



Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition

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

Изделие	RU.АЛДЕ.03.01.020-01
Документ	32 01-2
Версия	2.0.1.406
Автор	Липатова Ю.А.
Листов	173
Дата	14.05.2024

Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является субъектом 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 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.

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, заключённым 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.), подтверждённые или включённые в приложенные/взаимосвязанные/имеющие отношение к данному руководству, данные, содержащиеся в нём, а также все права на ПО являются и будут являться собственностью исключительно Компании.

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

Лицензия

описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного Соглашения:

Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении. Вы можете добавить/присоединить Программное обеспечение к программам для мобильных устройств с единственной целью, описанной в данном Соглашении. Принимая условия настоящего соглашения, Вы соглашаетесь:

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

Требования к использованию

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

Использование ПО

Пользователь вправе:

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

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникать в связи с экспортом шифровальных (криптографических) средств с территории Российской Федерации и (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

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как

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

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 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.

обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.» за это ПО.

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

- лицензия, предоставленная Вам данным Соглашением, прекращает своё действие, и Вы после её прекращения не сможете продолжать дальнейшее использование данного Программного обеспечения и других лицензионных Продуктов;

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии 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 реэкспорт ПО.

Разное

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

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ, И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ. Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ. ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНОВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

АННОТАЦИЯ

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

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

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

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

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

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

Содержание

¹ Далее по документу – программа, программное средство, Aladdin eCA CE

Аннотация.....	4
1 Запуск программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».....	9
1.1 Проверка состояния сервера в терминале.....	9
1.2 Автоматический запуск программы.....	9
1.3 Запуск программы в терминале.....	9
1.4 Завершение работы программы в терминале.....	10
2 Лицензирование программы.....	11
2.1 Первичное лицензирование.....	11
2.2 Ограничение лицензии.....	13
2.3 Окончание срока действия лицензии.....	14
2.4 Продление срока действия лицензии.....	15
3 Начало работы с программой.....	17
3.1 Создание Центра сертификации Корневого и Подчинённого.....	17
3.1.1 Инициализация Центра сертификации (шаг 2).....	17
3.1.2 Инициализация Центра сертификации (шаг 3).....	19
3.1.3 Инициализация Центра сертификации (шаг 4).....	20
4 Доступ к программе.....	22
4.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск.....	22
4.2 Аутентификация с использованием сертификата на ключевом носителе.....	26
4.2.1 Настройка СВТ для двухфакторной аутентификации администратора по сертификату на ключевом носителе.....	26
4.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе.....	28
5 Безопасность соединения.....	29
5.1 Настройка доверенного соединения.....	29
6 Технологические составляющие программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».....	31
6.1 Назначение технологических составляющих.....	31
6.2 Установка и настройка технологических составляющих.....	31
6.3 Удаление технологических составляющих.....	32
6.4 Восстановление доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certificate Authority» в случае некорректного удаления технологических составляющих и/или блокировки доступа...32	32
7 Функции управления программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».....	33
7.1 Верхняя панель «Центра сертификации Aladdin Enterprise Certificate Authority».....	33
7.2 Боковая панель «Центра сертификации».....	34
7.3 Раздел «Центр сертификации».....	36
7.3.1 Вкладка «Свои сертификаты».....	36
7.3.1.1 Карточка сертификата ЦС.....	38
7.3.1.2 Создание Центра сертификации.....	39
7.3.1.3 Скачивание запроса на сертификат для ЦС в состоянии «Запрос».....	39
7.3.1.4 Импорт сертификата Подчиненного ЦС.....	40
7.3.1.5 Удаление Центра сертификации.....	42
7.3.2 Вкладка «Сертификаты Подчиненных центров».....	44
7.3.2.1 Карточка сертификата подчинённого ЦС.....	45
7.3.2.2 Подписание запроса на Корневом ЦС.....	46
7.4 Раздел «Сертификаты».....	48
7.4.1 Выпуск сертификата.....	49

7.4.2	Поиск сертификатов.....	50
7.4.3	Сортировка сертификатов.....	50
7.4.4	Фильтрация сертификатов.....	51
7.4.4.1	Применение фильтров.....	51
7.4.4.2	Сброс применённых фильтров.....	51
7.4.5	Скачивание сертификатов.....	51
7.4.6	Статус сертификатов.....	52
7.4.7	Карточка сертификата.....	53
7.4.8	Экспорт списка выпущенных сертификатов.....	55
7.4.9	Массовые операции с сертификатами.....	57
7.5	Настройка уведомлений об истечении срока действия сертификата.....	59
7.5.1	Настройка параметров конфигурационного файла config.sh.....	60
7.5.2	Настройка шаблонов уведомлений об истечении срока действия сертификата.....	61
7.5.3	Настройка параметров почтового ящика пользователя.....	62
7.5.3.1	Настройка почтовой программы Яндекс.Почта.....	62
7.5.3.2	Настройка почтовой программы MS Exchange.....	64
7.6	Раздел «Учётные записи».....	65
7.6.1	Вкладка «Учётные записи».....	65
7.6.1.1	Создание учётной записи пользователя локального ресурса.....	66
7.6.1.2	Создание учётной записи для подключенного субъекта.....	66
7.6.1.3	Изменение статуса учётной записи.....	66
7.6.1.4	Редактирование учётной записи.....	67
7.6.1.5	Назначение прав оператору.....	67
7.6.1.6	Удаление учётной записи.....	68
7.6.1.7	Выпуск сертификата для учётной записи.....	68
7.6.2	Вкладка «Группы».....	69
7.6.2.1	Добавление группы пользователей с ролью «Оператор».....	69
7.6.2.2	Назначение прав участникам групп.....	70
7.6.2.3	Просмотр участников группы.....	70
7.6.2.4	Удаление группы.....	71
7.7	Раздел «Субъекты».....	71
7.7.1	Просмотр субъектов ресурсных систем.....	72
7.7.2	Поиск субъектов.....	72
7.7.3	Сортировка субъектов.....	73
7.7.4	Карточка субъекта.....	73
7.7.4.1	Редактирование атрибутов субъекта.....	77
7.7.5	Субъекты локальной ресурсной системы.....	78
7.7.5.1	Создание нового субъекта локальной ресурсной системы.....	79
7.7.6	Субъекты внешнего ресурса.....	80
7.7.7	Создание сертификата для субъекта ресурсной системы.....	82
7.7.8	Создание учётной записи для субъекта.....	83
7.8	Раздел «Ресурсная система».....	83
7.8.1	Регистрация ресурсной системы.....	84
7.8.2	Обновление зарегистрированной ресурсной системы.....	90
7.8.2.1	Виды обновления ресурсной системы.....	90
7.8.2.2	Режимы обновления ресурсной системы.....	90
7.8.3	Редактирование зарегистрированной ресурсной системой.....	91

7.8.4	Удаление зарегистрированной ресурсной системой	92
7.9	Раздел «Центры валидации»	92
7.9.1.1	Настройка периода автообновления.....	93
7.9.1.2	Моментальная публикация списка отозванных сертификатов CRL.....	95
7.9.1.3	Экспорт актуального списка отозванных сертификатов CRL	95
7.9.2	Вкладка «Центры валидации»	96
7.9.2.1	Регистрация Центра валидации на сервере Центра сертификации	97
7.9.2.2	Подписание запроса OCSP-сервера	99
7.9.2.3	Карточка центра валидации (доступ к функциям управления)	101
7.9.2.4	Состояния центра валидации и действия над ним	102
7.9.3	Вкладка «Точки распространения»	103
7.9.3.1	Создание пользовательской точки распространения.....	104
7.9.3.2	Редактирование пользовательской точки распространения.....	104
7.9.3.3	Удаление пользовательской точки распространения	105
7.9.4	Вкладка «Службы OCSP».....	106
7.9.5	Настройка технического решения «Центра валидации»	107
7.9.5.1	С использованием web-сервера Nginx.....	107
7.9.5.2	С использованием web -сервера Apache.....	110
7.9.6	Получение файлов CRL, Delta CRL и AIA.....	115
7.9.6.1	Получение файлов посредством запуска скрипта из состава программы	115
7.9.6.2	Получение файлов посредством использования методов REST API.....	116
7.9.7	Параметры точек распространения в сертификате	118
7.9.7.1	Указание точек распространения списка отозванных сертификатов CRL.....	118
7.9.7.2	Указание точек распространения списка изменений последнего опубликованного CRL	118
7.9.7.3	Указание точек распространения сертификатов издающих Центров сертификации.....	118
7.9.7.4	Указание на службы OCSP	118
7.10	Раздел «Журнал событий»	118
7.10.1	Управление экранной таблицей.....	119
7.10.2	Фильтрация событий.....	120
7.10.3	Сортировка событий.....	121
7.10.4	Поиск событий.....	121
7.10.5	Экспорт журнала событий.....	122
7.10.6	Архивирование и очистка журнала событий	130
7.11	Раздел «Шаблоны».....	130
7.11.1	Поиск шаблонов.....	131
7.11.2	Сортировка шаблонов	132
7.11.2.1	Карточка шаблона	132
7.11.2.2	Вкладка шаблона «Свойства»	132
7.11.2.3	Вкладка шаблона «Расширения»	133
7.11.2.4	Вкладка шаблона «Компоненты имени сертификата».....	133
7.11.3	Создание нового шаблона	133
7.11.3.1	Клонирование шаблона	134
7.11.4	Редактирование шаблона	134
7.11.4.1	Сохранение внесённых изменений в шаблон	138
7.11.5	Удаление шаблона	139
7.11.6	Массовая операция (удаления) с шаблонами.....	139
7.11.7	Шаблоны MSCS.....	141

7.11.7.1 Экспорт шаблонов из MSCS.....	141
7.11.7.2 Загрузка шаблона MSCS	141
7.11.8 Работа с шаблонами сертификатов	142
7.11.8.1 Идентификатор шаблона.....	142
7.12 Раздел «Настройки»	143
7.12.1 Установка сертификата web-сервера.....	144
7.12.2 Разрешённые издатели	145
8 Поиск и устранение неисправностей	147
Приложение 1. Создание сертификата для субъекта	151
1.1 Способы создания сертификатов.....	151
1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации	152
1.3 Публикация сертификата в ресурсную систему.....	152
1.4 Создание сертификата с закрытым ключом pkcs#12	153
1.5 Создание сертификата субъекта по запросу.....	156
1.6 Создание сертификата субъекта на ключевом носителе	161
1.6.1 Сообщения об ошибках при создании сертификата на ключевом носителе.....	164
Приложение 2. Описание обязательных полей предустановленных шаблонов сертификатов	166
Обозначения и сокращения	171
Термины и определения	172
Лист регистрации изменений.....	174

1 ЗАПУСК ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

1.1 Проверка состояния сервера в терминале

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

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

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

1.2 Автоматический запуск программы

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

1.3 Запуск программы в терминале

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

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

Модули программного компонента³, запускаемые поочерёдно, при выполнении команды приведены в Таблица 1.

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

Порядок запуска	Исполняемый файл	Наименование	Назначение
1	logs-service.jar	Модуль журнала событий	Обеспечивает фиксацию событий в журнале и получение событий из журнала, просмотра и поиск записей журнала событий, экспорт и архивацию записей журнала событий
2	store-service.jar	Модуль хранения сертификатов	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

² Далее по документу – программный компонент, Центр сертификации Aladdin Enterprise Certificate Authority, Центр сертификации Aladdin eCA

³ Далее по документу - сервис

Порядок запуска	Исполняемый файл	Наименование	Назначение
6	export-service.jar	Модуль экспорта данных	Обеспечивает управление экспортом файлов программы
7	security-service.jar	Модуль безопасности	Обеспечивает управление учётными записями пользователей
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-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 сертификатов	Обеспечивает обслуживание точек публикации CRL, Delta CRL и AIA
12	validation-service.jar	Модуль валидации сертификатов	Обеспечивает взаимодействия с точками распространения, а также для валидации сертификатов
13	backward-compatibility-service.jar	Модуль обратной совместимости	Предназначен для обеспечения обратной совместимости с API Центра сертификатов доступа AeCA CE версии 1.2.0.
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

1.4 Завершение работы программы в терминале

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

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

2 ЛИЦЕНЗИРОВАНИЕ ПРОГРАММЫ

2.1 Первичное лицензирование

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

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

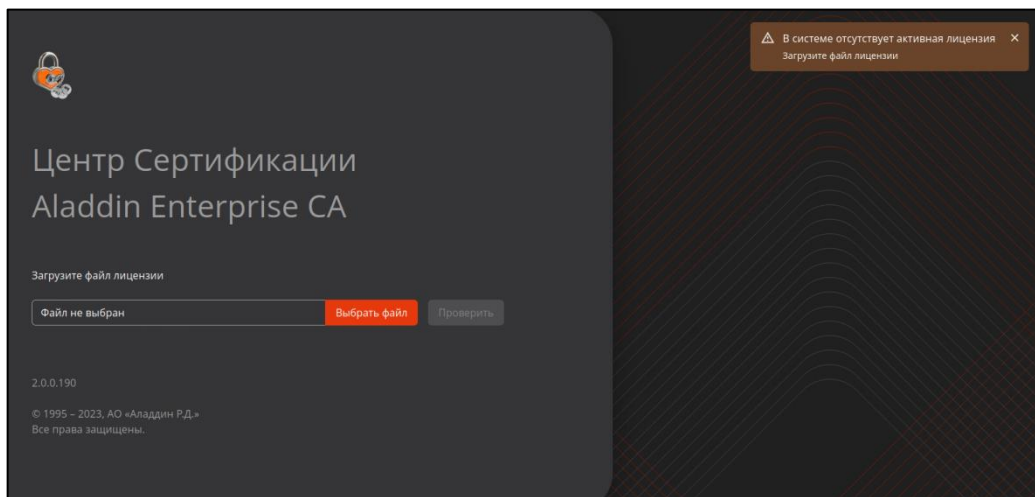


Рисунок 1 – Окно инициализации Центра сертификации. Шаг 1 – выбор лицензии

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

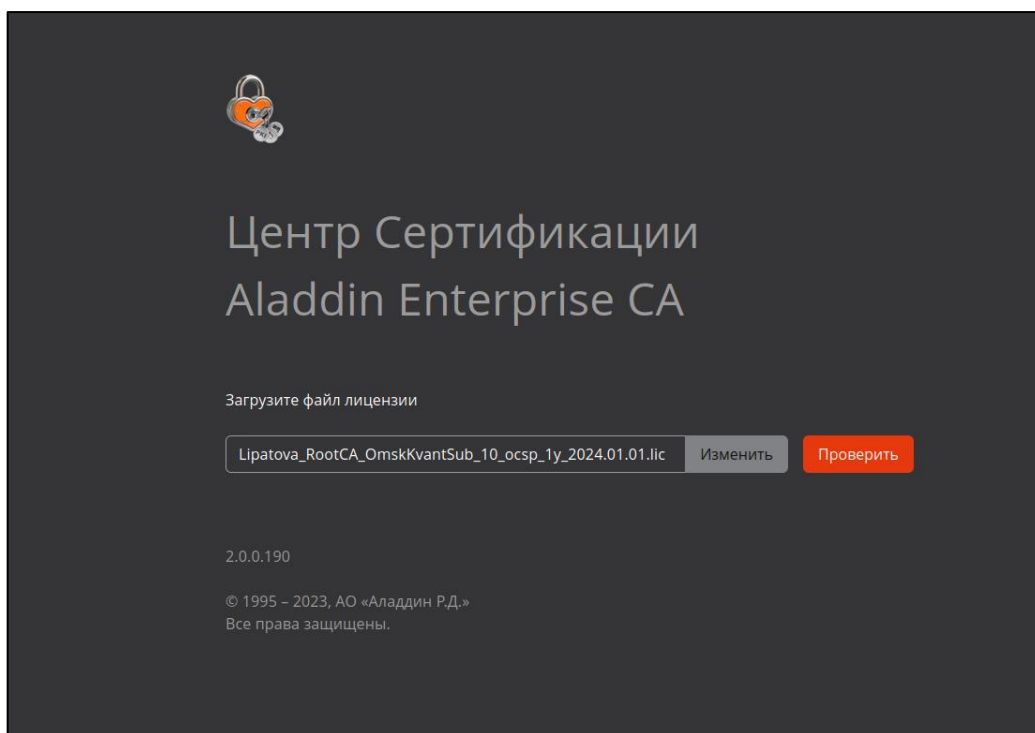


Рисунок 2 – Окно инициализации Центра сертификации. Шаг 1 – проверка лицензии

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

- при несовпадении ключевых полей – productId и id, администратор будет уведомлён сообщением на экране «Данная лицензия не предназначена для продукта Aladdin Enterprise CA» (см. Рисунок 15);

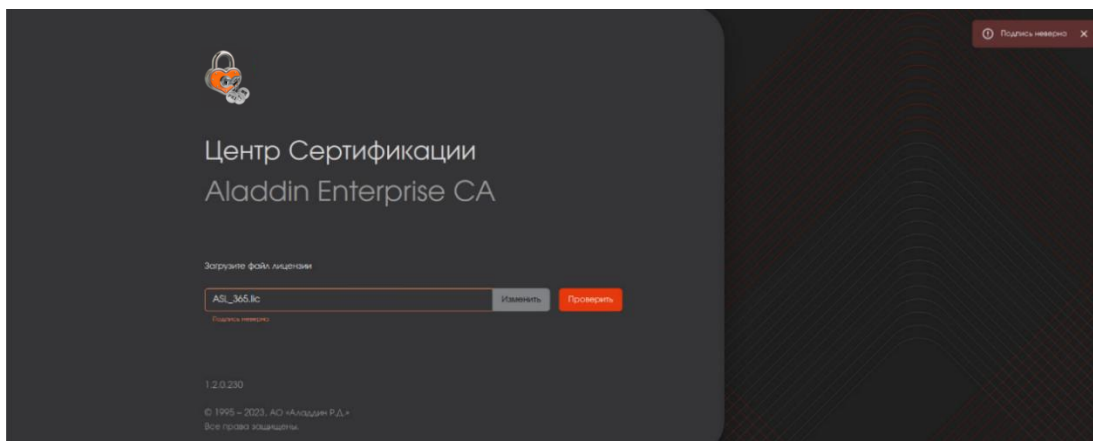


Рисунок 3 - Окно инициализации Центра сертификации. Проверка лицензии. Несовпадение полей

- при несовпадении подписи лицензии администратор будет уведомлён сообщением на экране «Подпись не верна» (см. Рисунок 16);

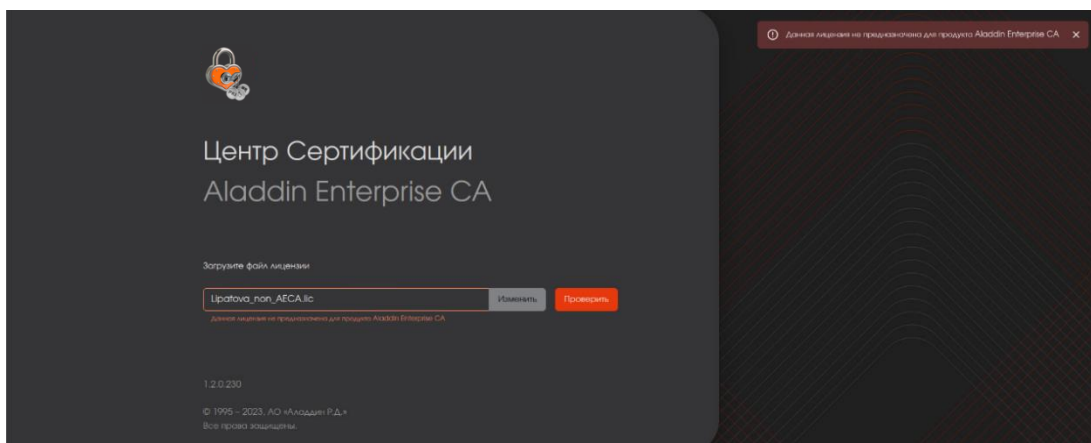


Рисунок 4 – Окно инициализации Центра сертификации. Лицензия предназначена для другого продукта

- при истечении срока действия лицензии администратор будет уведомлён сообщением на экране «Срок лицензии истёк» (см. Рисунок 17);

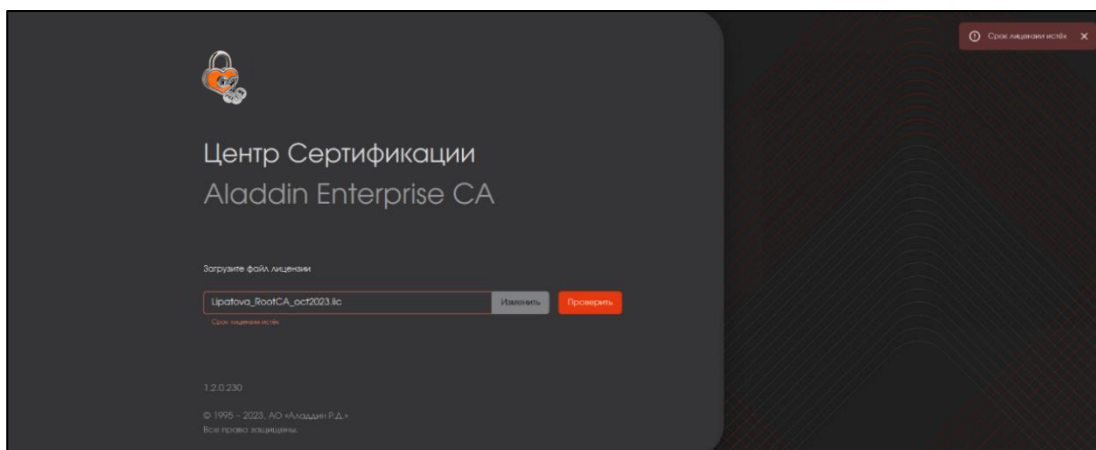


Рисунок 5 - Окно инициализации Центра сертификации. Срок лицензии истёк

- в случае ранее установленной лицензии на текущем рабочем месте и новой установке ПО Aladdin eCA администратор будет уведомлён сообщением на экране «В системе уже присутствует лицензия»;

- при невозможности чтения содержимого файла лицензии администратор будет уведомлён сообщением на экране «Некорректный файл».
- Если лицензия продукта «Центр сертификации» Aladdin eCA успешно проходит проверку на валидность, то активируется кнопка <Создать центр сертификации> (см. Рисунок 6).

На экране будут отображены параметры лицензии:

- имя Корневого центра сертификации в поле «Root Common Name»;
- имя создаваемого Подчинённого центра сертификации в поле «Common name» (в случае загрузки лицензии Подчинённого ЦС);
- срок действия лицензии в поле «Действует до».

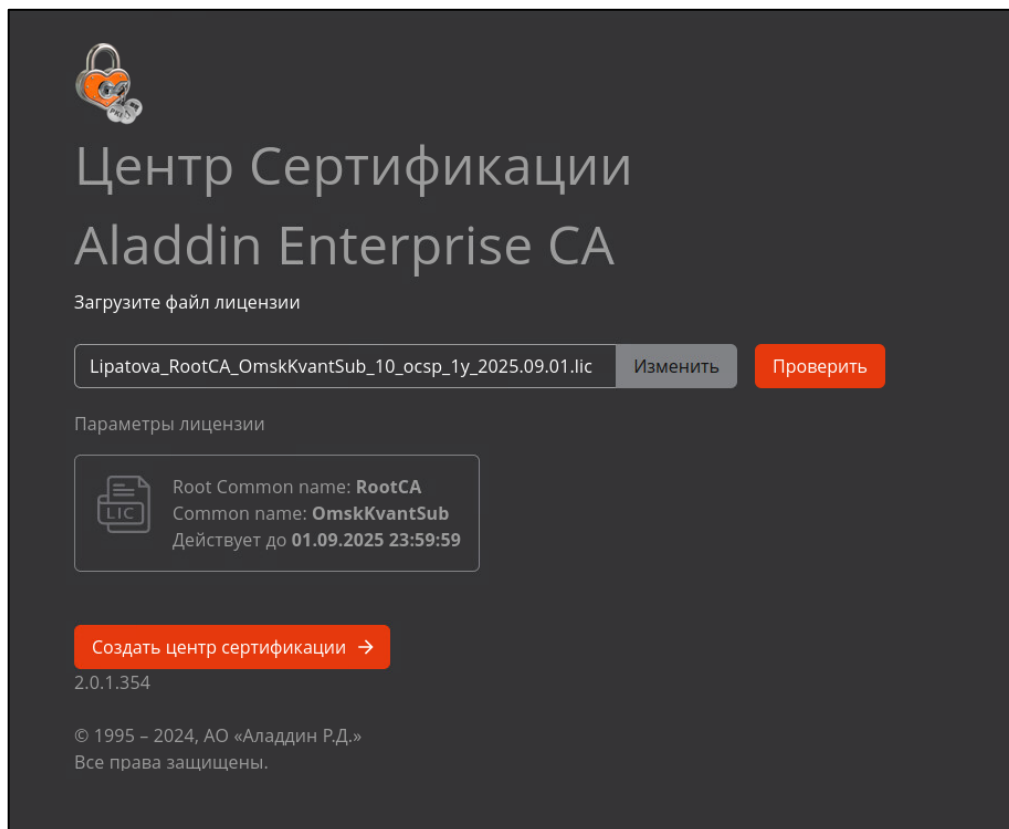


Рисунок 6 – Окно инициализации. Проверка на валидность файла лицензии прошла успешно

- Далее нажмите кнопку <Создать центр сертификации> для перехода к созданию Центра сертификации, процедура которого приведена в пункте 3.1 настоящего руководства.

2.2 Ограничение лицензии

- Лицензию необходимо импортировать для каждого разворачиваемого Центра сертификации.
- Лицензия может быть предоставлена для развёртывания Корневого ЦС или Подчинённого ЦС.
- Лицензия на право использования программы ограничена сроком действия.
- Сведения об установленной лицензии Корневого или Подчинённого ЦС доступны для просмотра в окне «О программе» (см. Рисунок 7, Рисунок 8), вызываемом на верхней панели экранной формы Центра сертификации и содержащим следующие данные:

Для Корневого ЦС:

- срок, до которого действует установленная лицензия;

Для Подчинённого ЦС:

- срок, до которого действует установленная лицензия;

- имя Корневого центра сертификации, указанное в установленной лицензии;
 - контактные данные предприятия – разработчика
- имя Корневого центра сертификации, выдавшего сертификат Подчинённому центру сертификации;
 - имя Подчинённого ЦС, указанное в установленной лицензии;
 - контактные данные предприятия – разработчика.

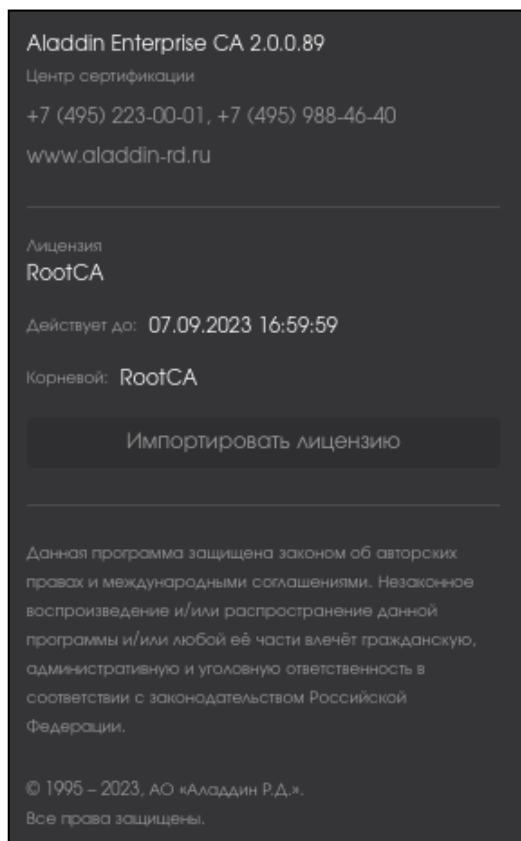


Рисунок 7 – Окно «О программе» для Корневого ЦС

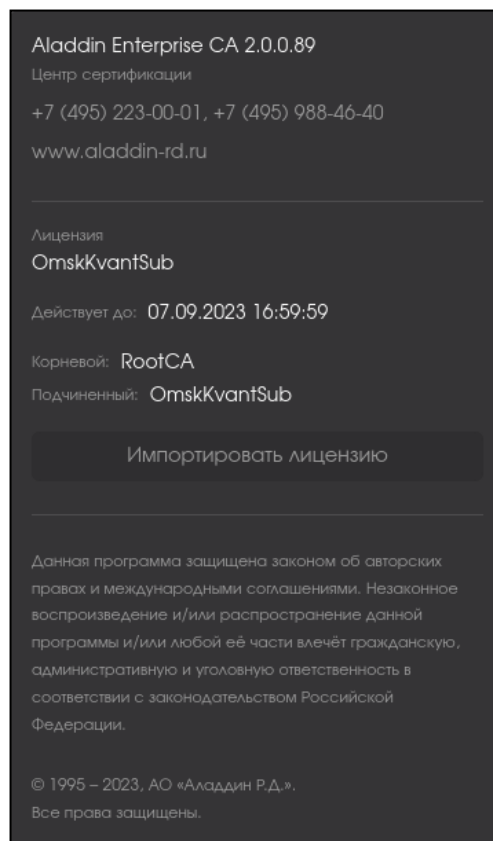


Рисунок 8 – Окно «О программе» для Подчинённого ЦС

2.3 Окончание срока действия лицензии

- После истечения срока действия лицензии функция выпуска сертификатов субъектов станет недоступна. Кнопки <Создать сертификат> в разделах «Центр сертификации» и «Сертификаты», кнопка <Подписать запрос> в разделе «Центр сертификации» будут заблокированы. При наведении на заблокированные кнопки будет показано сообщение о причинах блокировки «Срок действия лицензии истёк» (см. Рисунок 9).

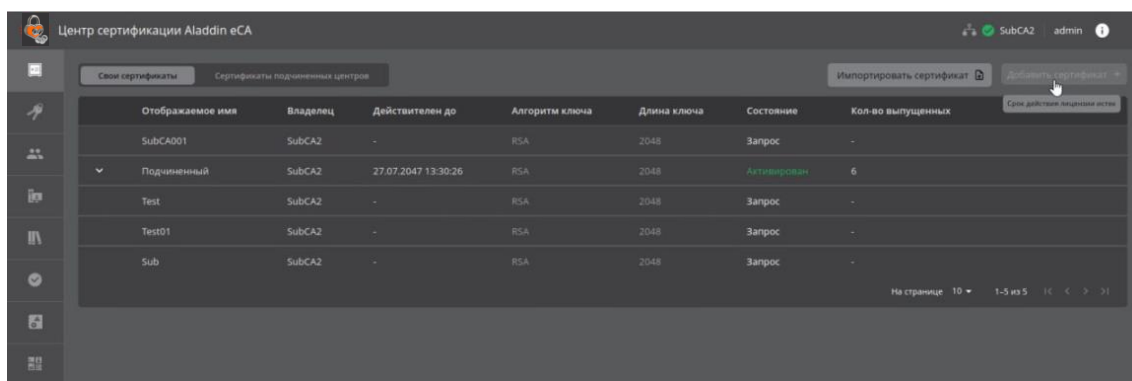


Рисунок 9 – Заблокированная кнопка <Создать сертификат> по истечении срока действия лицензии

2.4 Продление срока действия лицензии

- Для доступа к полному функционалу компонента «Центр сертификации Aladdin eCA» необходимо загрузить действительную лицензию, нажав кнопку <Импортировать лицензию> в окне «О программе» (см. Рисунок 7, Рисунок 8), расположенном на верхней панели экранной формы «Центра сертификации».
- В открывшемся окне импорта лицензии (см. Рисунок 10) будет доступна информация о текущей установленной лицензии.
- Выберите файл лицензии в формате .lic.

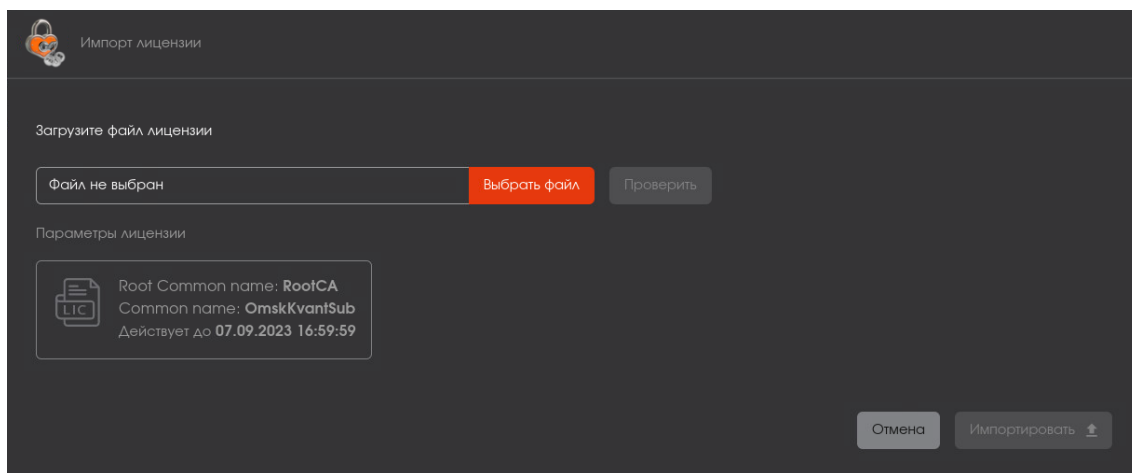


Рисунок 10 – Окно импорта лицензии

- 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:
 - имя Корневого центра сертификации в поле «Root Common name»;
 - имя текущего центра сертификации в поле «Common name» для Подчинённого ЦС;
 - срок действия лицензии в поле «Действует до».

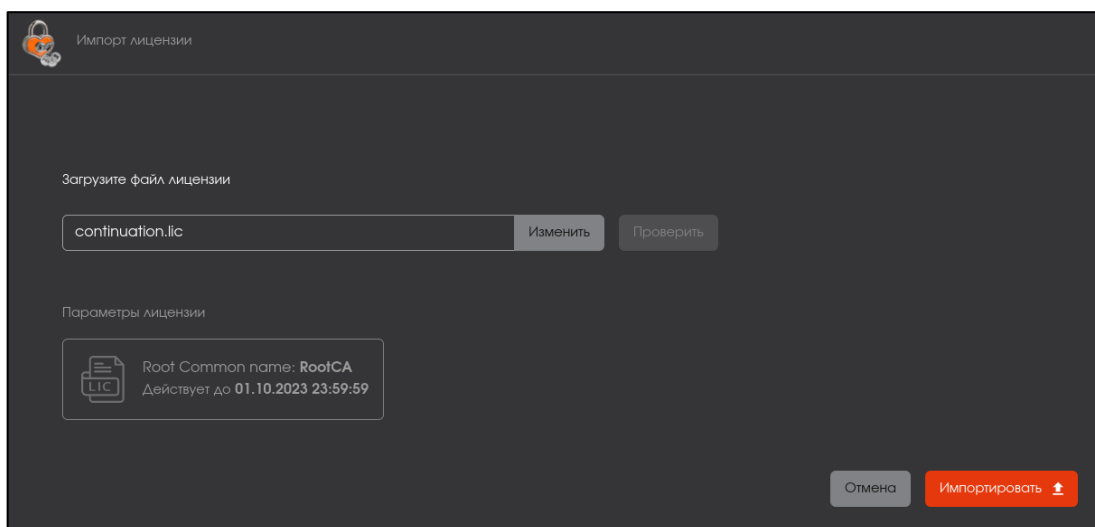


Рисунок 11 – Окно импорта лицензии после успешной проверки на валидность

- Нажмите кнопку <Импортировать> для установки лицензии.
- После успешного импорта лицензии будет:
 - выведено на экран уведомление об успешной установке лицензии «Успешно сохранено»;

- обновлены данные лицензии в поле «Действует до» окна «О программе»;
- произведена запись в Журнал событий CAENV002.
- После успешной установки лицензии функционал программного обеспечения «Центр сертификации» доступен в полном объеме.
- В случае неуспешной загрузки лицензии возможны следующие уведомления об ошибке:
 - «Указанный в лицензии сертификат не соответствует используемому Корневому сертификату»;
 - «Корень цепочки сертификатов отсутствует».

3 НАЧАЛО РАБОТЫ С ПРОГРАММОЙ

3.1 Создание Центра сертификации Корневого и Подчинённого

3.1.1 Инициализация Центра сертификации (шаг 2)

- После успешной установки лицензии, на следующем шаге, в зависимости от типа загруженной лицензии, создаётся Корневой или Подчинённый Центр сертификации (см. Рисунок 12, Рисунок 13).
- Отображаемое имя создаваемого центра сертификации задаётся путём ввода в соответствующее поле и может содержать буквы латинского и/или кириллического алфавита, цифры от 0 до 9, символы таблицы ASCII, максимальной длиной 200 символов.
- Имя центра сертификации (Common Name) задается автоматически, согласно данным лицензии, и не подлежит изменению.

Инициализация центра сертификации

Шаг 2 / 3

Укажите отображаемое имя и суффикс различающегося имени для сертификата

Отображаемое имя

Обязательно к заполнению

Имя центра сертификации

RootCA

Суффикс различающегося имени

Обязательно к заполнению

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

Имя соответствует указанному в лицензии.

Формат ввода: O=organization, OU=Department, L=City,
DC=Component, C=RU...

Назад

Продолжить

Рисунок 12 – Окно инициализации центра сертификации. Создание Корневого ЦС. Шаг 2

Инициализация центра сертификации

Шаг 2 / 3

Укажите отображаемое имя и суффикс различающегося имени для сертификата

Отображаемое имя

Обязательно к заполнению

Имя центра сертификации

OmskKvantSub

Суффикс различающегося имени

Обязательно к заполнению

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

Имя соответствует указанному в лицензии.

Формат ввода: O=organization, OU=Department, L=City,
DC=Component, C=RU...

Назад

Продолжить

Рисунок 13 – Окно инициализации центра сертификации. Создание Подчиненного ЦС. Шаг 2

- В поле «Суффикс различающегося имени» необходимо ввести суффикс различающегося имени ЦС. Для указания значений атрибутов суффикса SDN допустимо использование только следующих символов: A-Z, a-z, A-Я, а-я, 0-9, а также @ _ ' = () + , - . / : ? и пробел. Ограничители ввода между параметрами – запятые и запятые с пробелами. Длина вводимого суффикса различающегося имени не должна превышать 250 байт. Ввод атрибутов возможен в любом порядке, но в сертификате порядок атрибутов будет установлен в соответствии с номерами пунктов в таблице 2.

Поддерживаемые варианты атрибутов суффикса различающегося имени приведены в Таблица 2.

Таблица 2 – Поддерживаемые атрибуты суффикса различающегося имени

№ пп.	Наименование атрибута	Описание атрибута
1	EMAILADDRESS=	// E-mail address (электронная почта)
2	CN=	//name (дополнительное имя)
3	UID=	//Unique Identifier (уникальный идентификатор)
4	SERIALNUMBER =	//Serial number (серийный номер)
5	OU=	//Organizational Unit (отдел(организации))
6	O=	//Organization (организация)
7	L=	//Locality (район)
8	ST=	//State or Province (область, край, республика)
9	C=	// C, Country (страна, вводить согласно - ISO 3166)
10	T=	//title (заглавие)
11	SURNAME=	//Surname (фамилия)
12	STREET=	//streetAddress (адрес - улица)
13	INITIALS=	//First name abbreviation (инициалы)
14	GIVENNAME=	//Given name (first name – имя)
15	DC=	//Domain Component(first) (первый доменный компонент, при повторном вводе – второй)
16	UNSTRUCTUREDADDRESS=	//IP address (IP-адрес)
17	UNSTRUCTUREDNAME=	//Domain name (доменное имя - FQDN)
18	POSTALCODE=	//postalCode (почтовый индекс)
19	BUSINESSCATEGORY=	//Organization type (категория(тип) организации)
20	TELEPHONENUMBER=	// telephoneNumber (телефонный номер)
22	POSTALADDRESS=	//postalAddress (почтовый адрес)
21	PSEUDONYM=	//pseudonym (псевдоним)
24	DN=	//DN Qualifier (признак отличительного имени для идентификации субъекта)
25	DESCRIPTION=	//Description (краткое описание)

- После ввода суффикса различающегося имени нажмите ставшую активной кнопку <Продолжить>.

3.1.2 Инициализация Центра сертификации (шаг 3)

При выпуске сертификата доступа Центра сертификации рекомендуется выбирать алгоритмы хэш-суммы **SHA256**, **SHA384** или **SHA512**. Криптографическая хэш-функция **SHA1** не обеспечивает требуемой безопасности и может быть выбрана только при необходимости обеспечения совместимости.

• В открывшемся окне (см. Рисунок 14, Рисунок 15) в соответствующих полях установить параметры криптографии:

- алгоритм ключа RSA (выбран по умолчанию), ECDSA;
- длина ключа 2048, 3072, 4096 (выбран по умолчанию);
- алгоритм хэш-суммы SHA1 (не рекомендован), SHA256 (выбран по умолчанию), SHA384, SHA512.

• Для Корневого ЦС задайте срок действия сертификата (по умолчанию – 10 лет). Ввод осуществляется вручную или выбором даты окончания действия сертификата в открывшемся календаре. Максимальный срок действия Корневого сертификата 25 лет.

• Для Подчинённого ЦС срок действия сертификата по умолчанию устанавливается равным сроку действия, заданному в шаблоне, используемом при выпуске сертификата (подписании запроса), но не превышает срок действия сертификата Корневого ЦС. В случае, если в шаблоне не указан данный параметр, то срок действия сертификата подчинённого ЦС – 10 лет.

- После задания значений нажать ставшую активной кнопку <Создать ЦС>.

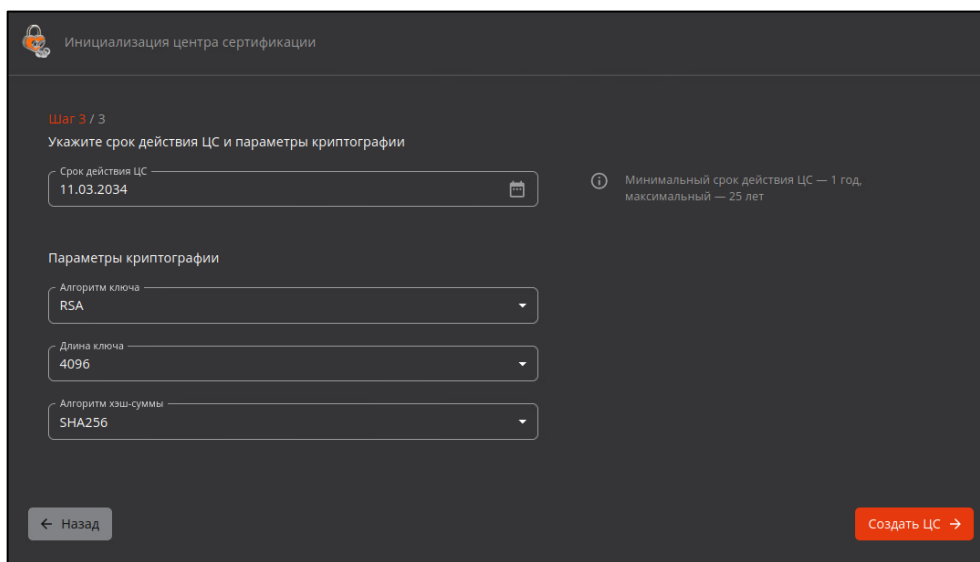


Рисунок 14 – Окно инициализации центра сертификации. Создание Корневого ЦС. Шаг 3

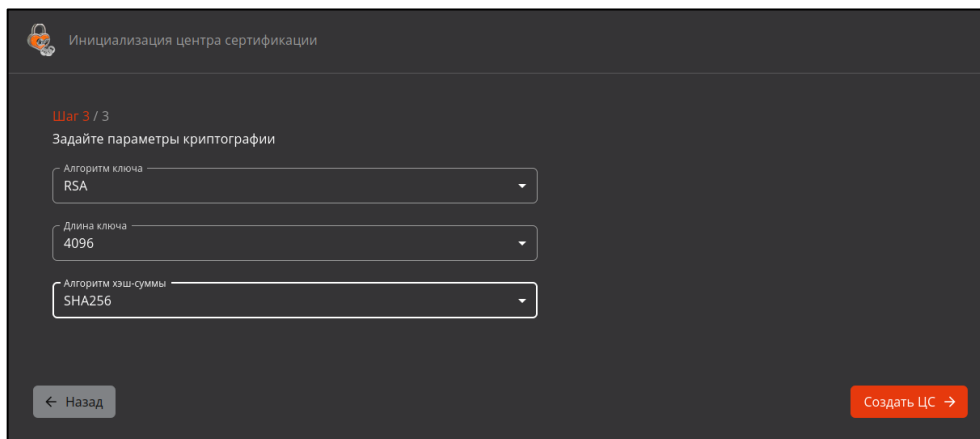


Рисунок 15 – Окно инициализации центра сертификации. Создание Подчиненного ЦС. Шаг 3

- В случае неудачной попытки создания ЦС администратор будет уведомлен сообщением (см. Таблица 3).

Таблица 3 – Перечень сообщений в случае неудачной попытки создания ЦС

Текст ошибки	Причина
Ошибка. Некорректный компонент суффикса различающегося имени – <Имя компонента>	Ошибка ввода неизвестного имени компонента суффикса различающегося имени
Ошибка. Лицензионные ограничения не позволяют создать ЦС используя данное имя	Ошибка несоответствия значения в компоненте «CN» суффикса различающегося имени значению, указанному в лицензии
Ошибка при создании Центра сертификации. Неизвестная ошибка	Внутренняя ошибка ПО

3.1.3 Инициализация Центра сертификации (шаг 4)

- При успешном создании Корневого ЦС и завершении инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 16). Возможно скачать сертификат созданного Корневого ЦС, цепочку сертификатов в формате .pem или открыть интерфейс Центра сертификации.

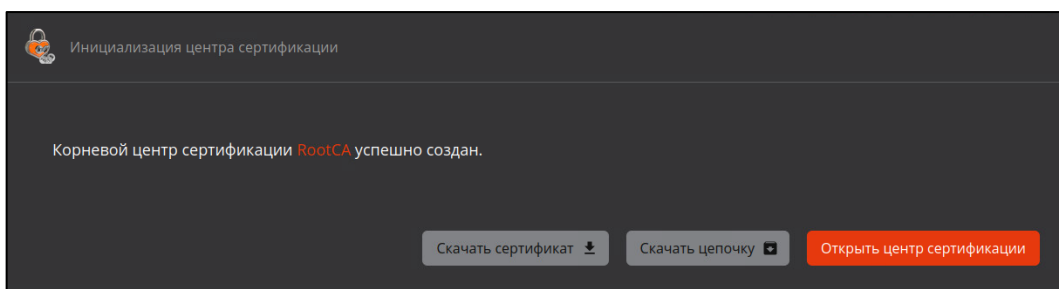


Рисунок 16 – Окно завершения работы инициализации по созданию Корневого ЦС

- При успешном создании Подчиненного ЦС и завершении инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 17).

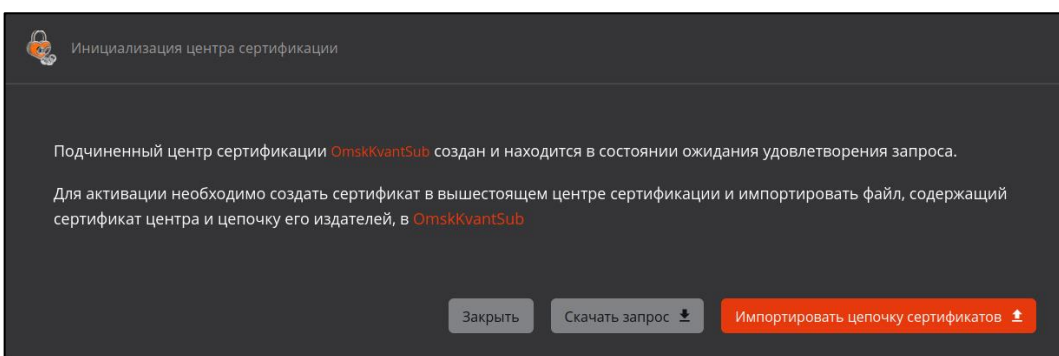


Рисунок 17 – Окно завершения инициализации по созданию Подчиненного ЦС

- Скачайте созданный запрос на сертификат Подчиненного ЦС в формате .csr.
- На данном этапе Подчиненный ЦС создан, отображается на вкладке «Свои сертификаты» и имеет статус «Запрос».

- Для перевода ЦС в состояние «Активирован», при котором становится доступен полный функционал ПО «Центра сертификации», необходимо выполнить подписание запроса на Корневом ЦС (пункт о настоящего руководства) и импорт подписанного сертификата Подчиненного ЦС (пункт 7.3.1.4 настоящего руководства).

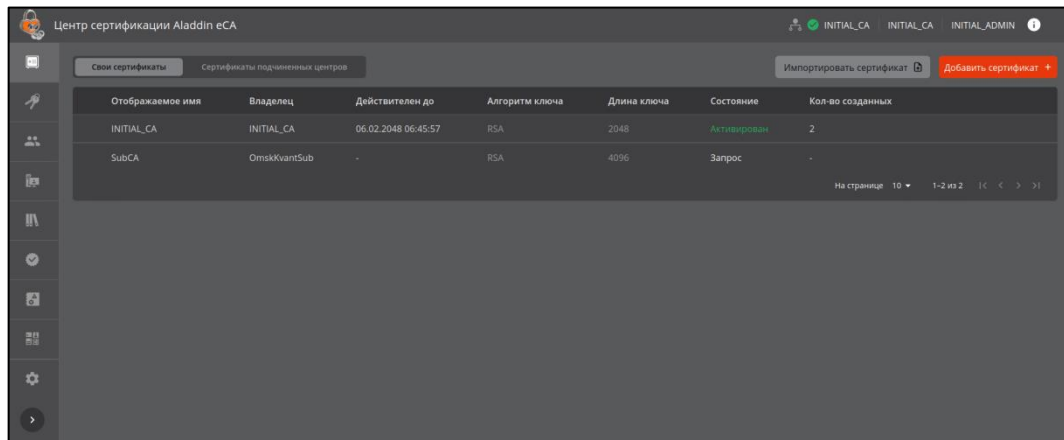


Рисунок 18 – Окно Центра сертификации. Подчинённый ЦС в состоянии «Запрос»

4 ДОСТУП К ПРОГРАММЕ

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

4.1 Аутентификация с использованием сертификата, перенесённого на жесткий диск

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

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

- Откройте браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 19). Нажмите кнопку <Просмотр сертификатов>.

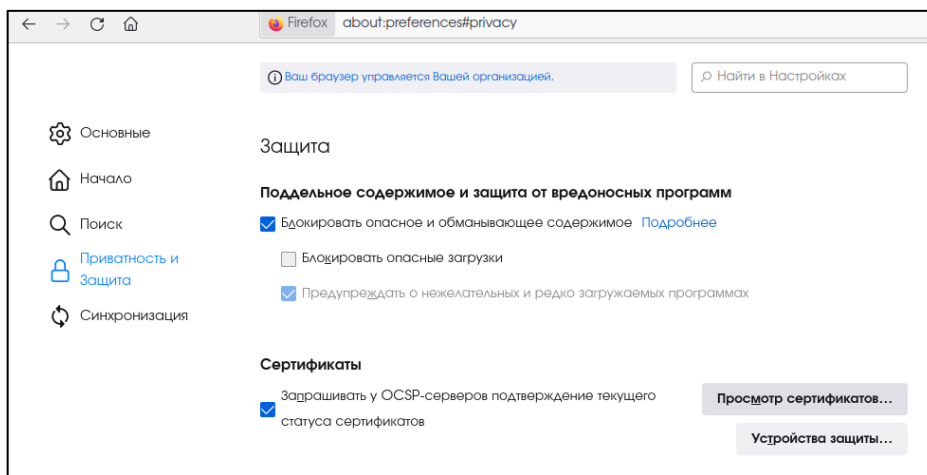


Рисунок 19 – Окно настроек браузера

- Выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать> (см. Рисунок 20).

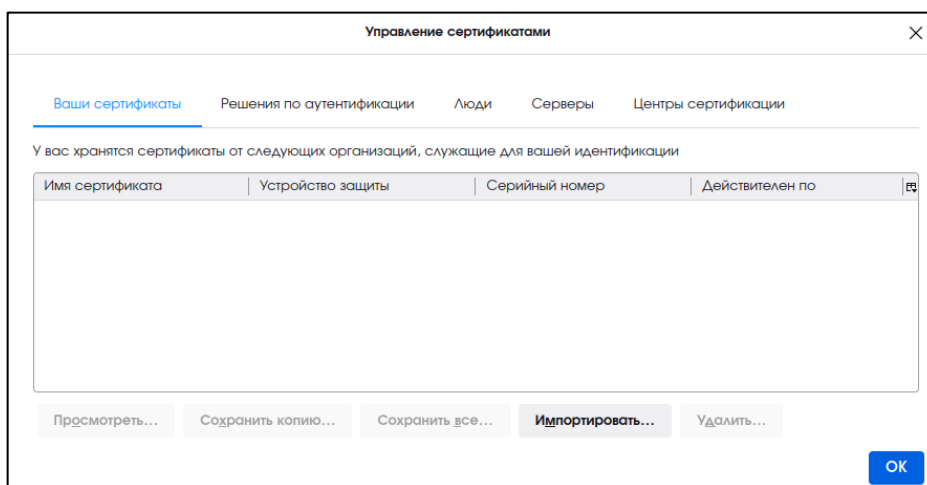


Рисунок 20 – Окно управления сертификатами

- Выберите контейнер .p12, содержащий закрытый ключ и сертификат доступа, перенесённый на жесткий диск, выпущенный для учётной записи пользователя (см. Рисунок 21).

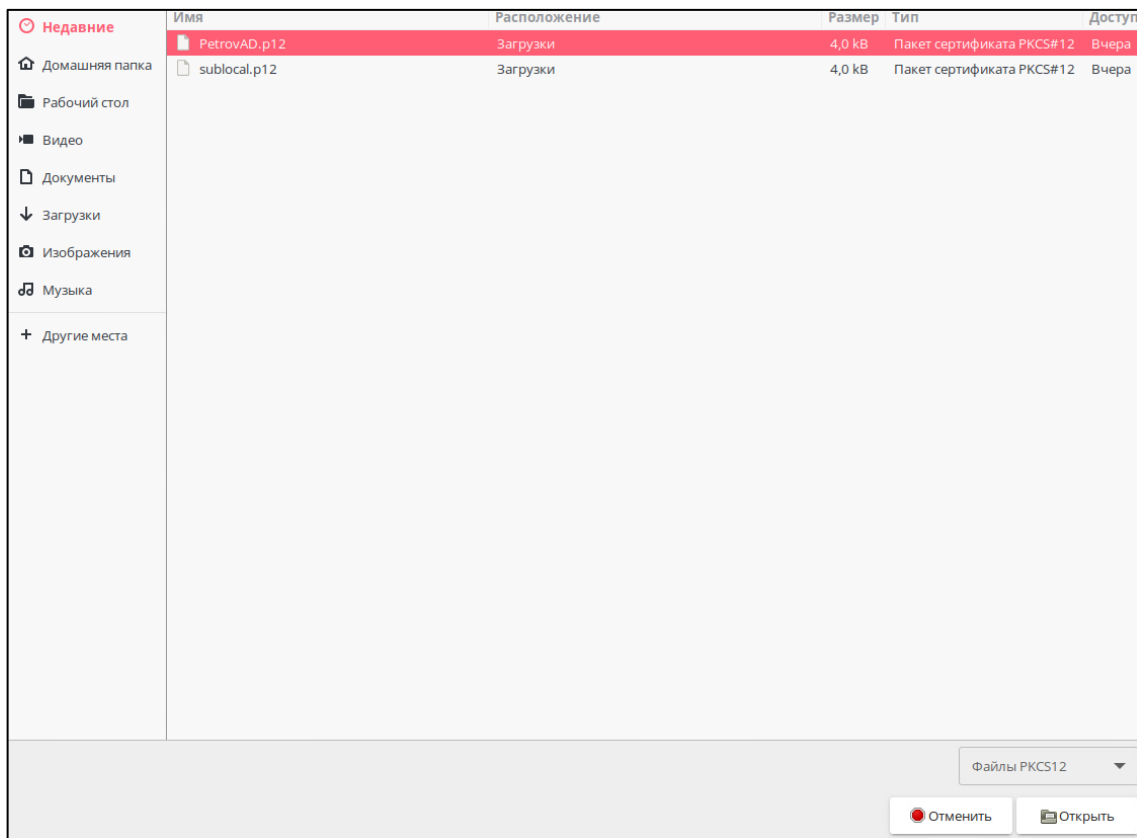


Рисунок 21 – Окно выбора импортируемого файла сертификата

- Введите PIN-код загружаемого контейнера .p12 в открывшемся окне и нажмите кнопку <Ок> (см. Рисунок 22). PIN-код сертификата является атрибутом безопасности и должен быть передан администратором с контейнером закрытого ключа и сертификата.

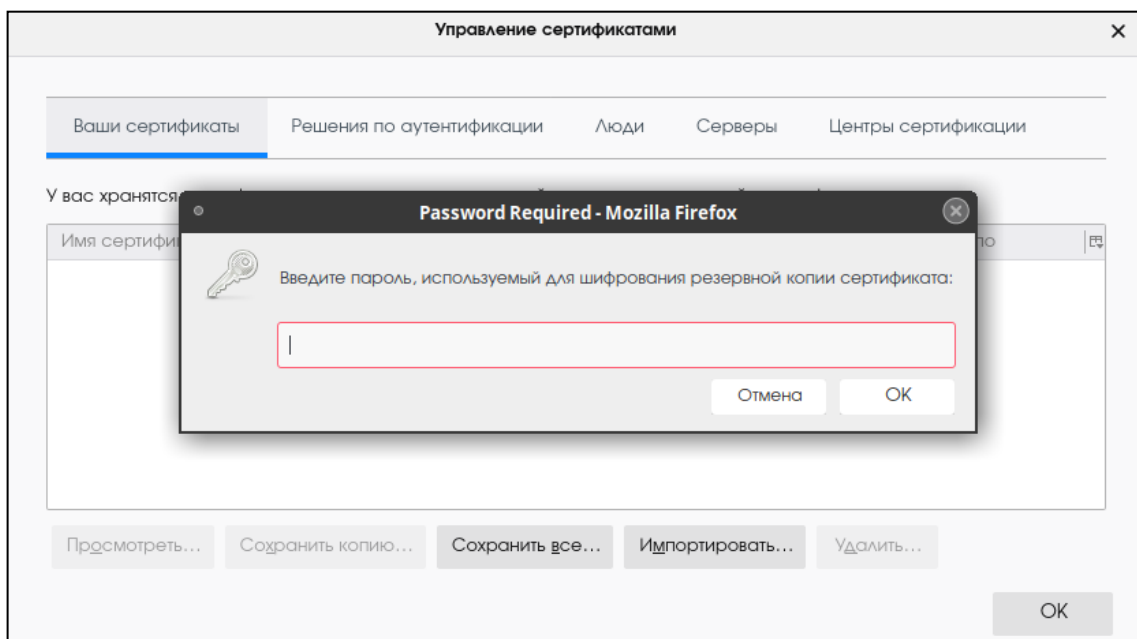


Рисунок 22 – Окно ввода PIN-кода сертификата

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 23). Нажмите кнопку <ОК>.

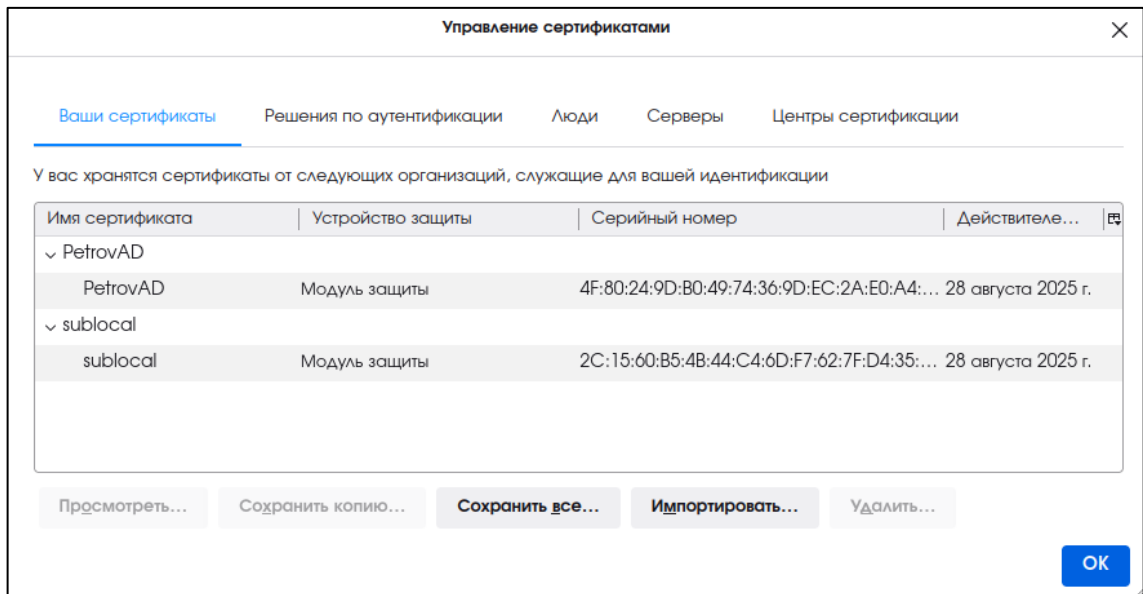


Рисунок 23 – Окно «Управление сертификатами»

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

Например:

`https://172.22.5.21`

- В открывшемся окне выберите сертификат для аутентификации на веб-сервере Центра сертификации Aladdin Enterprise Certificate Authority (см. Рисунок 24). Нажмите кнопку <ОК>.

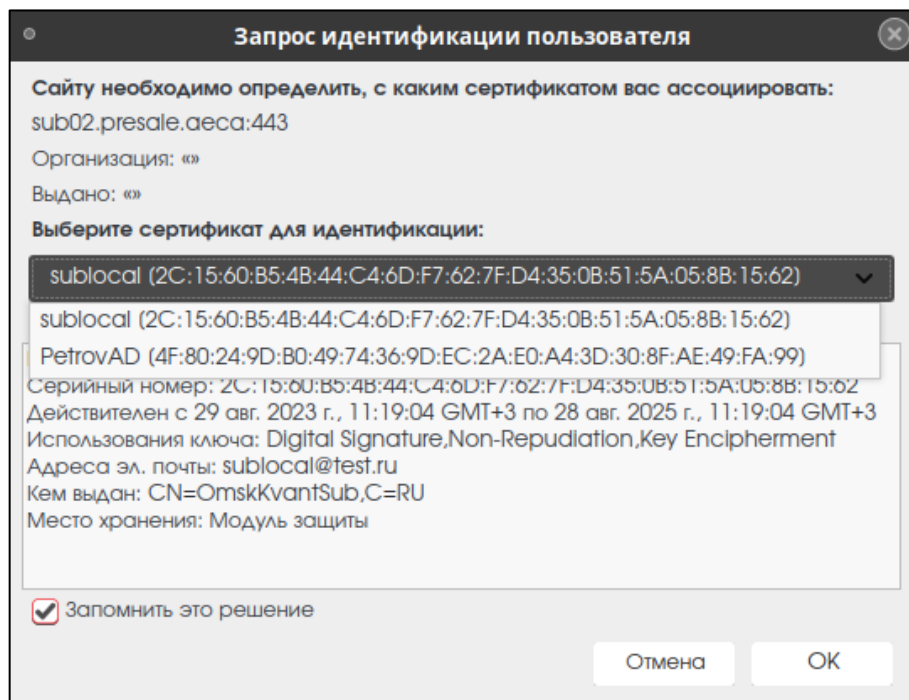


Рисунок 24 – Окно выбора сертификата для аутентификации

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 25). Нажмите кнопку <Дополнительно>.

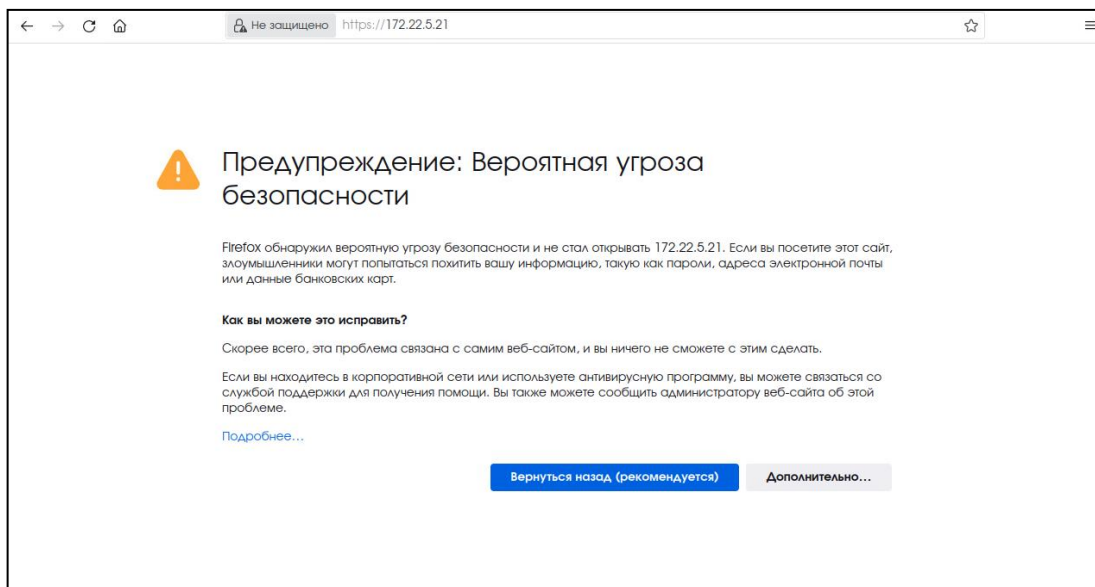


Рисунок 25 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Дополнительно> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 26). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

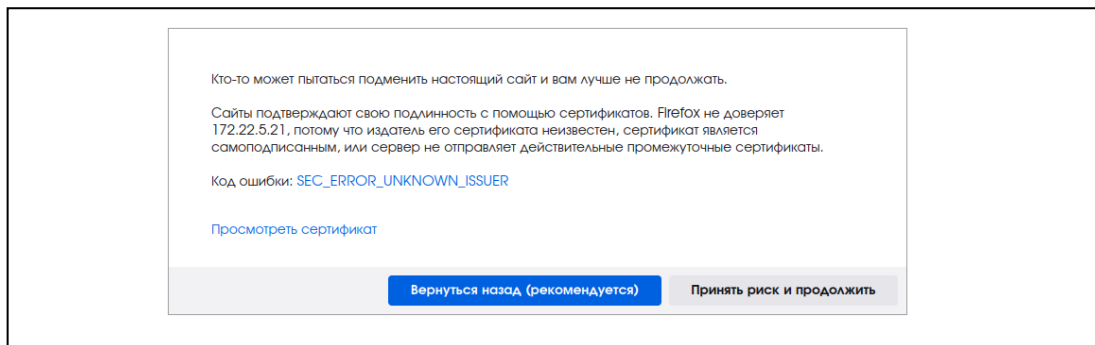


Рисунок 26 – Страница ошибки распознавания сертификата

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

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

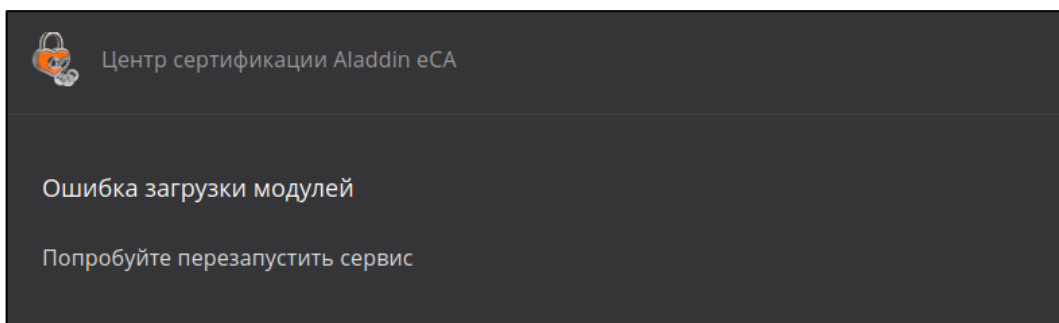


Рисунок 27 – Окно «Управление сертификатами»

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

4.2 Аутентификация с использованием сертификата на ключевом носителе

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

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

```
cd .../.../...
```

- Установите Единый Клиент JaCarta, выполнив команду:

```
bash install.sh
```

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

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

```
apt install libnss3-tools
```

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

- Рекомендуется очистить кэш браузера и ранее применённые решения по аутентификации в браузере (для браузера Firefox: Настройки -> Приватность и защита -> Сертификаты -> Просмотр сертификатов).
- Выполните настройку браузера **Firefox**, если подключение к серверу Центра сертификации Aladdin Enterprise Certificate Authority будет выполнено в этом браузере:
 - откройте Настройки -> Приватность и защита -> Сертификаты -> Устройства защиты;
 - в диалоговом окне нажмите кнопка <Загрузить>;
 - в окне загрузки драйвера нажмите кнопку <Обзор> и выберите файл модуля `/lib64/libjcpkcs11-2.so` (см. Рисунок 28) и подтвердите загрузку модуля, нажав кнопку <ОК>;

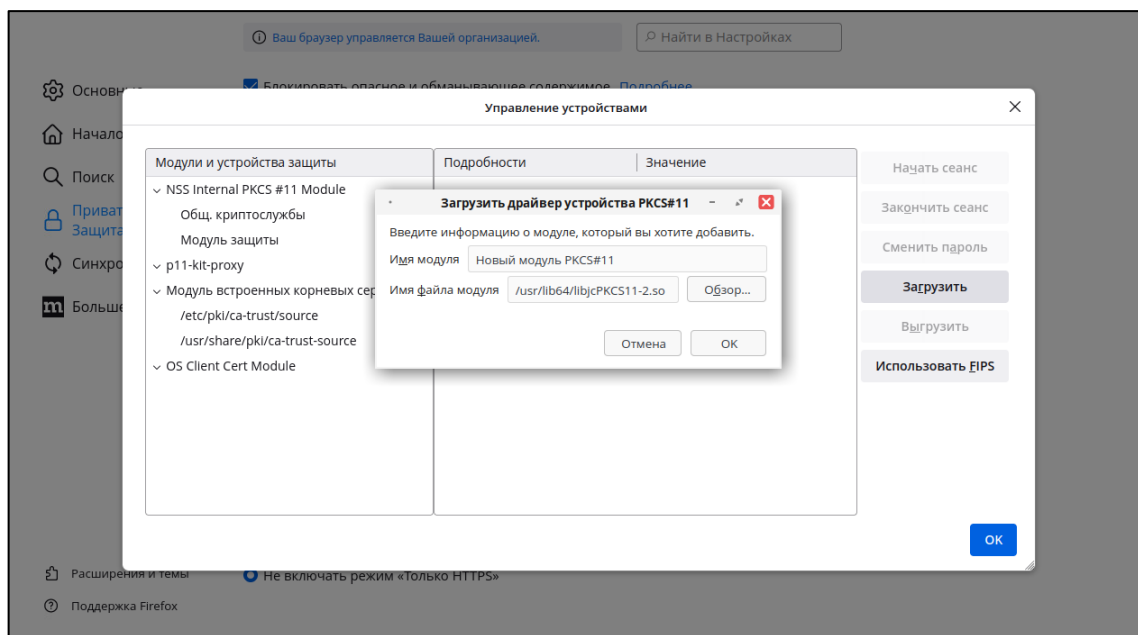


Рисунок 28 – Настройка браузера Firefox

- перезапустите браузер.

- Выполните настройку браузера **Chromium**, если подключение к серверу Центра сертификации Aladdin Enterprise Certificate Authority будет выполнено в этом браузере посредством **ОС РЕД ОС 7.3** или **Альт 8 СП, релиз 10**:

- удалите каталог локальной библиотеки сертификатов, выполнив команду:

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

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

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

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

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

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

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

- перезапустите браузер.

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

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

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

- перезапустите браузер.

4.2.2 Двухфакторная аутентификация администратора по сертификату на ключевом носителе

- Полученный оператором ключевой носитель с записанным на нём сертификатом доступа для аутентификации на web-сервере Центра сертификации Aladdin Enterprise Certificate Authority необходимо подключить в USB-порт предварительного настроенного средства вычислительной техники – рабочего места оператора/администратора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.

- Откройте браузер, для которого была выполнена первичная настройка двухфакторной аутентификации (согласно п. 4.2.1 настоящего руководства), и введите в адресную строку ip-адрес или полное доменное имя сервера (в зависимости от SAN, указанного в сертификате web-сервера), выдавшего импортированный сертификат доступа, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».

Например:

`https://172.22.5.21`

- В появившемся окне введите PIN-код ключевого носителя.

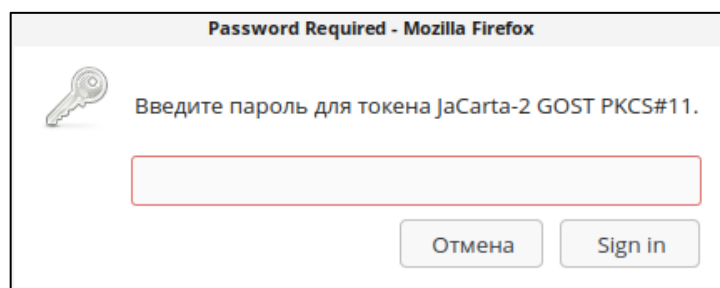


Рисунок 29 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

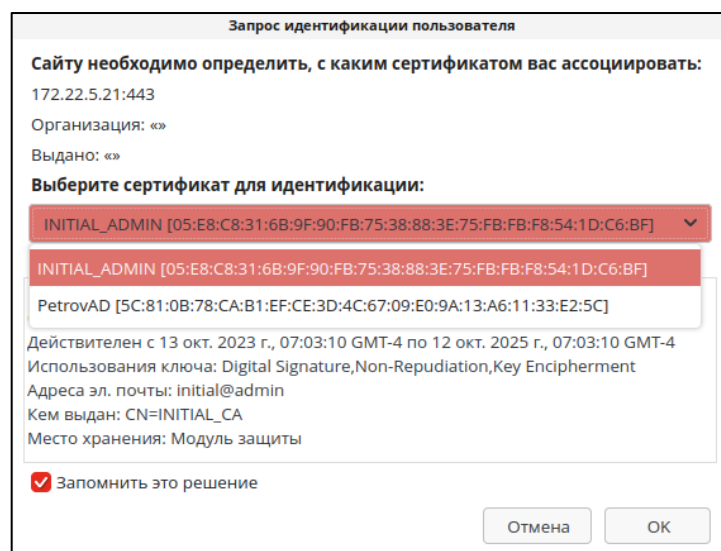


Рисунок 30 – Окно выбора сертификата пользователя для аутентификации на сервере

Время действия токена доступа – 3 минуты.

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

5 БЕЗОПАСНОСТЬ СОЕДИНЕНИЯ

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

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

5.1 Настройка доверенного соединения

Для настройки доверенного соединения:

- Подготовьте сертификаты Центров сертификации, на основе которых строится цепочка доверия сертификатам, или цепочку сертификатов Центра сертификации, с которым требуется установить безопасное соединение (см. пункт 7.3.1.1 настоящего руководства).

- Установите сертификаты Центров сертификации цепочки доверия в доверенное хранилище браузера. Процесс установки сертификатов рассмотрим на примере браузера Firefox:

- Откройте браузер Firefox – Настройки – Приватность и Защита – Сертификаты (см. Рисунок 31). Нажмите кнопку <Просмотр сертификатов>.

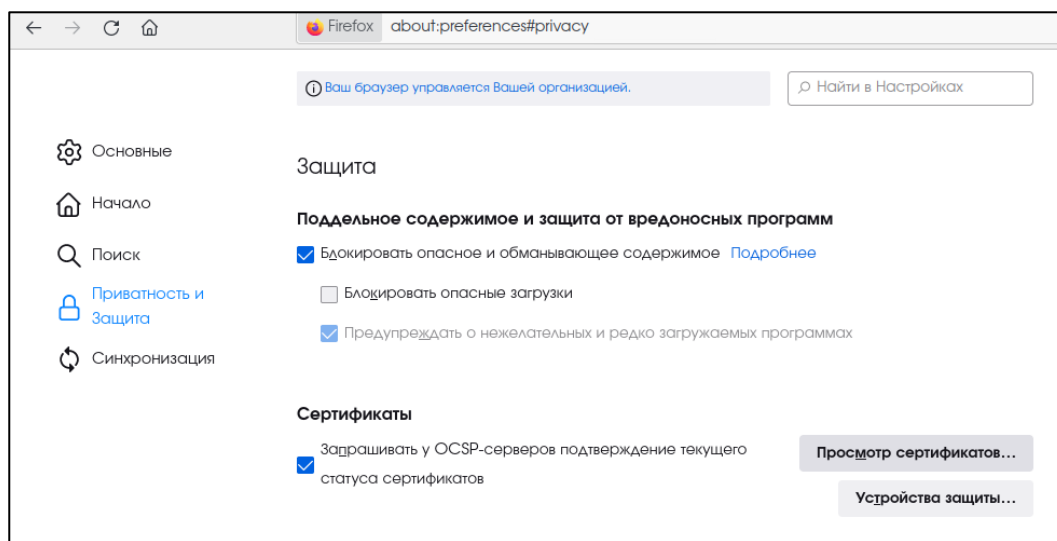


Рисунок 31 – Окно настроек браузера

- Выберите вкладку «Центры сертификации», в открывшейся вкладке нажмите кнопку <Импортировать> и выберите предварительно подготовленный сертификат Центра сертификации, поставьте флажки в чек-боксах «Доверять при идентификации веб-сайтов» и «Доверять при идентификации пользователей электронной почты». Поочередно импортируйте все сертификаты Центров сертификации, участвующие в построении цепочки доверия (см. Рисунок 32) или импортируйте цепочку сертификатов.

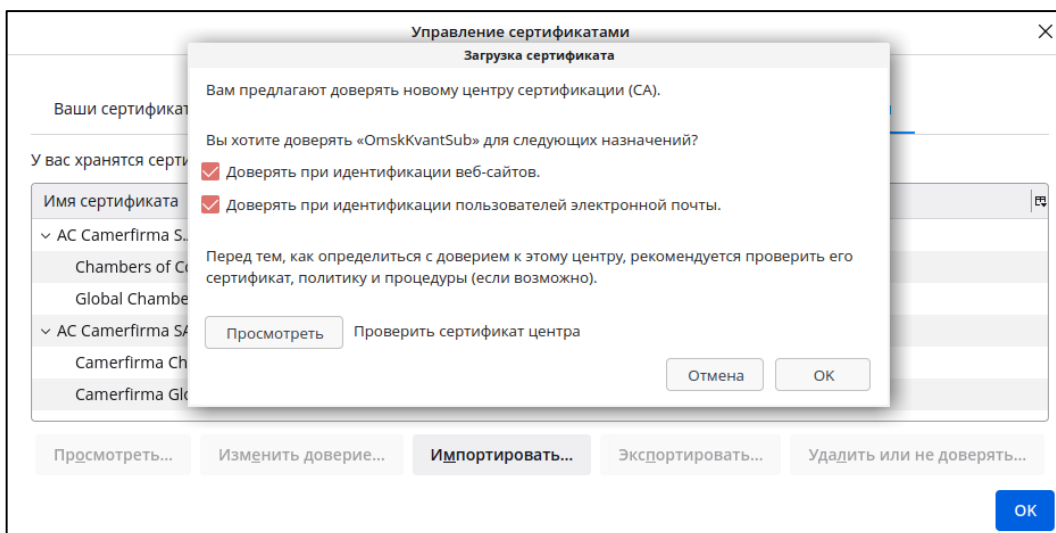


Рисунок 32 – Окно управления сертификатами

- Выпустите (см. пункт 7.4.1 настоящего руководства) для локального субъекта web-сервера и установите сертификат web-сервера (см. пункт 7.12.1 настоящего руководства), если это не сделано ранее.
- Перезапустите браузер.
- Для безопасного доверенного соединения при обращении к серверу Центра сертификации используйте доменное имя (см. Рисунок 33), указанное в атрибуте сертификата web-сервера Subject alternative name (SAN) (см. Рисунок 34) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера.



Рисунок 33 – Адресная строка в браузере

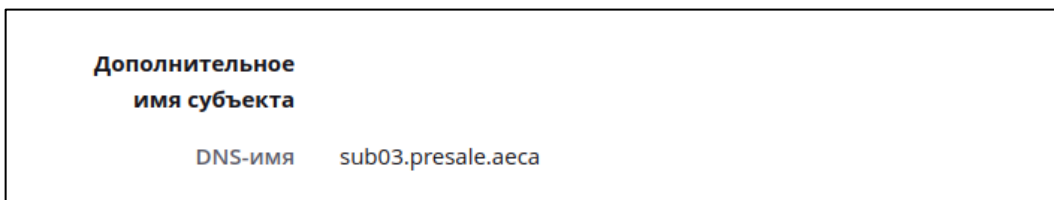


Рисунок 34 – Сертификат web-сервера

6 ТЕХНОЛОГИЧЕСКИЕ СОСТАВЛЯЮЩИЕ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

6.1 Назначение технологических составляющих

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

6.2 Установка и настройка технологических составляющих

- Перед установкой программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» возможно задать в файле конфигурации `/opt/aecaCa/scripts/config.sh` переменные окружения, используемые сервисом «settings-service» (см. Руководство администратора. Часть 1. Установка):

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

- В процессе установки программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» будут автоматически созданы технологические компоненты:

- технологический Центр сертификации «INITIAL_CA» (по умолчанию);
- локальные субъекты (локальный субъект web-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 web-сервера со сроком действия 2 года.

- После завершения развёртывания программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» в каталоге `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.p12` будет размещён сертификат администратора инициализации INITIAL_ADMIN.p12, необходимый для дальнейшей аутентификации на web-сервере. PIN-код сертификата администратора, заданный по умолчанию в конфигурационном файле `config.sh`, «INITIAL».

- Первичная авторизация в открывшемся интерфейсе установленного программного компонента «Центр Сертификации Aladdin Enterprise Certificate Authority» по умолчанию выполняется под учетной записью «INITIAL_ADMIN» с правами администратора.

- В открывшемся интерфейсе программного средства «Центр Сертификации Aladdin Enterprise Certificate Authority» отображены:

- Сертификат технологического Центра сертификации в разделе «Центр сертификации» на вкладке «Свои сертификаты».

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

6.3 Удаление технологических составляющих

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

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

- 1) Выпустите и импортируйте сертификат для созданного подчинённого Центра сертификации в состоянии «Запрос» (согласно пунктам о и 7.3.1.4 настоящего руководства).
- 2) Удостоверьтесь в том, что созданный Центр сертификации активирован.
- 3) Создайте учётную запись с ролью «Администратор» (см. пункт 7.6.1.1 настоящего руководства).
- 4) Выпустите сертификат для созданной учётной записи (см. пункт 7.6.1.7 настоящего руководства).
- 5) Выполните аутентификацию по выпущенному сертификату учётной записи (см. раздел 7.3.1.5 Руководства администратора. Часть 1. Установка).
- 6) Выключите проверку издателя технологического Центра сертификации (см. пункт 7.12 настоящего руководства).
- 7) Выпустите сертификат web-сервера, сохранив контейнер с ключевой парой (сертификат и закрытый ключ) в формате. pkcs12 (см. пункт 7.4.1 настоящего руководства).
- 8) Выполните смену ключей web-сервера в целях безопасности (см. пункт 7.12.1 настоящего руководства).
- 9) Удалите технологический Центр сертификации (см. пункт 7.3.1.5 настоящего руководства).

6.4 Восстановление доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certificate Authority» в случае некорректного удаления технологических составляющих и/или блокировки доступа

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

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

7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

7.1 Верхняя панель «Центра сертификации Aladdin Enterprise Certificate Authority»

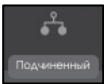


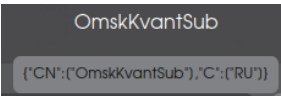
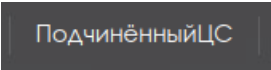
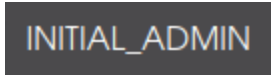
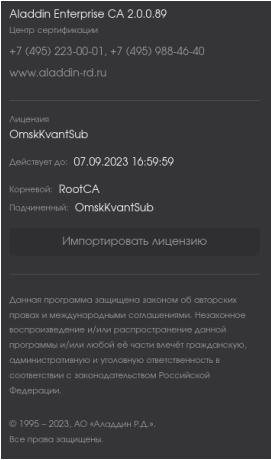
Верхняя панель (см. Рисунок 35) Центра сертификации фиксирована и отображается на любом шаге или переходе между разделами.



Рисунок 35 – Верхняя панель окна «Центра сертификации»

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


Верхняя панель содержит следующие элементы:

- 

 - тип активного ЦС (возможные варианты: Корневой или Подчиненный);
- 
 - обозначение статуса ЦС, возможные варианты:
 - «активный» – соответствует зеленому цвету иконки,
 - «не инициализирован» – соответствует красному цвету иконки,
 - «истек срок действия сертификата» – соответствует оранжевому цвету иконки,
 - «истек срок действия лицензии» – соответствует красному цвету иконки);
- 
 - имя текущего активного ЦС, заданное в применённой лицензии (не изменяемое). При наведении курсора всплывают заданные имя и значения суффикса различающегося имени ЦС;
- 
 - отображаемое имя текущего активного ЦС (задаётся при первичной активации лицензии);
- 
 - текущая авторизация учётной записи пользователя;
- 
 - сведения о текущей версии программного компонента, контактная информация разработчика, информация о лицензии.

По нажатию на кнопку <Импортировать лицензию> возможно загрузить обновление лицензии.

7.2 Боковая панель «Центра сертификации»

Боковая панель Центра сертификации закреплена и отображается на любом шаге или переходе между разделами.

Полный вид боковой панели показан на Рисунок 36, компактный вид боковой панели приведен на Рисунок 37. Выбор вида боковой панели происходит по нажатию кнопки , расположенной внизу данной панели.

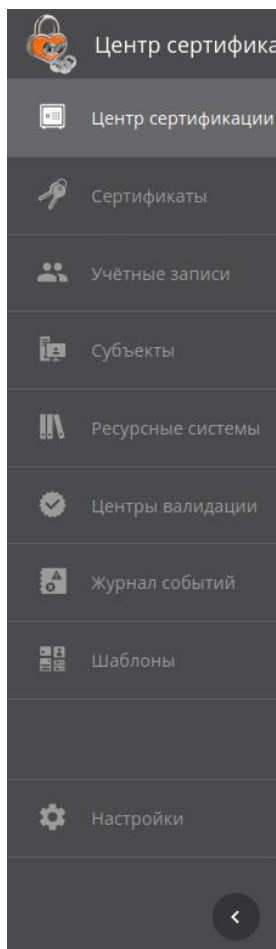


Рисунок 36 – Полный вид боковой панели



Рисунок 37 – Компактный вид боковой панели

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

- Раздел «Центр сертификации» – в данном разделе возможно:
 - выпустить сертификат Центра сертификации;
 - подписать запрос на выпуск сертификата Подчиненного Центра сертификации;
 - скачать цепочку сертификатов активного Центра сертификации;
 - скачать сертификат Корневого и Подчиненного ЦС в формате .pem;
 - отозвать сертификат Подчиненного ЦС;
 - посмотреть карточку Центра сертификации;
- Раздел «Сертификаты» – в данном разделе возможно:
 - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
 - выпустить сертификат на основании запроса для субъекта;
 - выпустить сертификат на ключевом носителе для субъекта;

- посмотреть список всех выпущенных сертификатов субъектов, выпущенных активным ЦС, с отображением статуса сертификата, срока действия, типа субъекта, имени субъекта и серийного номера сертификата;
- произвести поиск выпущенных сертификатов по имени субъекта;
- отозвать или приостановить действие выпущенного сертификата субъекта;
- посмотреть карточку выпущенного сертификата субъекта;
- скачать сертификат субъекта в формате .pem;
- скачать цепочку сертификатов;
- скачать текущий CRL;
- скачать список всех выпущенных сертификатов в формате .csv;
- применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);
- Раздел «Учетные записи» – в данном разделе возможно:
 - создать новую учетную запись;
 - отредактировать существующую учетную запись;
 - заблокировать или активировать существующую учетную запись;
 - задать группы, на которые предоставляются права для управления сертификатами субъектов, для учетной записи, выполняющей роль «Оператор»;
 - выпустить сертификат для пользователя учётной записи;
- Раздел «Субъекты» – в данном разделе возможно:
 - произвести поиск субъекта по его имени (или части имени);
 - обновить список групп и субъектов;
 - посмотреть организационные группы субъектов локальной и подключенных ресурсных систем;
 - посмотреть существующие субъекты;
 - 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;
 - зарегистрировать Центры валидации;
 - просмотреть список уже зарегистрированных центров валидации.
- 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 web-серверу и смена сертификата текущего web-сервера.

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

7.3 Раздел «Центр сертификации»

Переход на экран управления центра сертификации осуществляется по выбору раздела «Центр сертификации» бокового меню, расположенного слева на главном экране (см. Рисунок 36).

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

Данный раздел доступен только для пользователя с ролью «Администратор».

7.3.1 Вкладка «Свои сертификаты»

Вид раздела меню раздела «Центр сертификации» – вкладка «Свои сертификаты» показан на Рисунок 38.

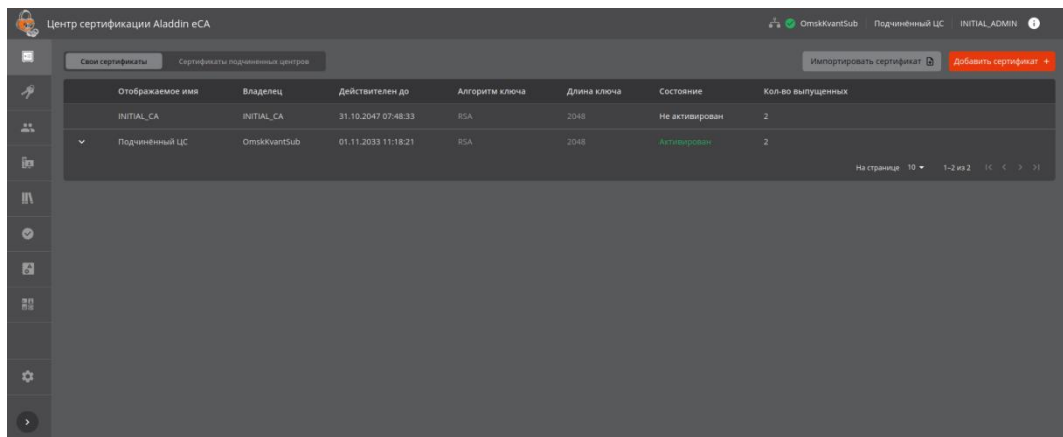


Рисунок 38 - Экран раздела "Центр сертификации" – вкладка «Свои сертификаты»

- На данной вкладке после инициализации отображены сертификат технологического Центра сертификации, создаваемый по умолчанию при установке программного компонента «Центр сертификации Aladdin eCA» на сервер, и сертификат Центра сертификации, созданный при инициализации.
- Сертификаты Центров сертификации в формате .pem хранятся в базе данных «aecasа» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`), схема базы данных «store», таблица «file_registry».
- Открытый и закрытый ключи Центров сертификации хранятся в контейнере pkcs#12 в папке `/opt/aeca/cryptotoken` по умолчанию, если не изменена конфигурация развёртывания в конфигурационном файле `/opt/aecaCa/scripts/config.sh`.

- Пароль контейнера pkcs#12 хранится в базе данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`), схема базы данных «certificate», таблица «crypto_token».


- 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».

- Информационные элементы вкладки «Свои сертификаты» - неуправляемые (табличные поля):

- отображаемое имя;
- владелец;
- действителен по (дата);
- алгоритм ключа;
- длина ключа;
- состояние (варианты состояния: активирован, запрос, отозван, истёк срок, не активирован);
- количество созданных сертификатов доступа не зависимо от статуса сертификата.


- Для управления Центрами сертификации администратору доступны действия, приведённые в Таблица 4.

Таблица 4 – Возможные операции, совершаемые над ЦС на вкладке «Свои сертификаты» и необходимые действия для выполнения

Операция	ЦС в состоянии «Запрос»	ЦС в состоянии «Активирован»	ЦС в состоянии «Не активирован»	Необходимое действие для выполнения операции
скачать сертификат	-	+	+	выделить сертификат и нажать кнопку  <Скачать>
скачать цепочку сертификатов	-	+	+	
скачать список отозванных сертификатов	-	+	+	
скачать запрос на сертификат	+	-	-	
удалить ЦС	+	-	+	выделить сертификат и нажать кнопку  <Удалить>
импортировать сертификат	+	-	-	выделить сертификат и нажать кнопку  <Загрузить> или кнопку 

Операция	ЦС в состоянии «Запрос»	ЦС в состоянии «Активирован»	ЦС в состоянии «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

- Технологический центр сертификации может быть удалён после выпуска и загрузки нового сертификата для текущего сервера (см. пункт 6.3 настоящего руководства).

- На вкладке «Свои сертификаты» по нажатию на кнопку  «Добавить сертификат +» доступна функция выпуска нового сертификата для Центра сертификации, созданного при инициализации на основании текущей лицензии, и может служить заменой текущего активного ЦС в случае компрометации его закрытого ключа. Описание процедуры приведено в пункте 7.3.1.2 настоящего руководства.

7.3.1.1 Карточка сертификата ЦС

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» в состоянии «Активирован» или «Не активирован» (см. Рисунок 39).

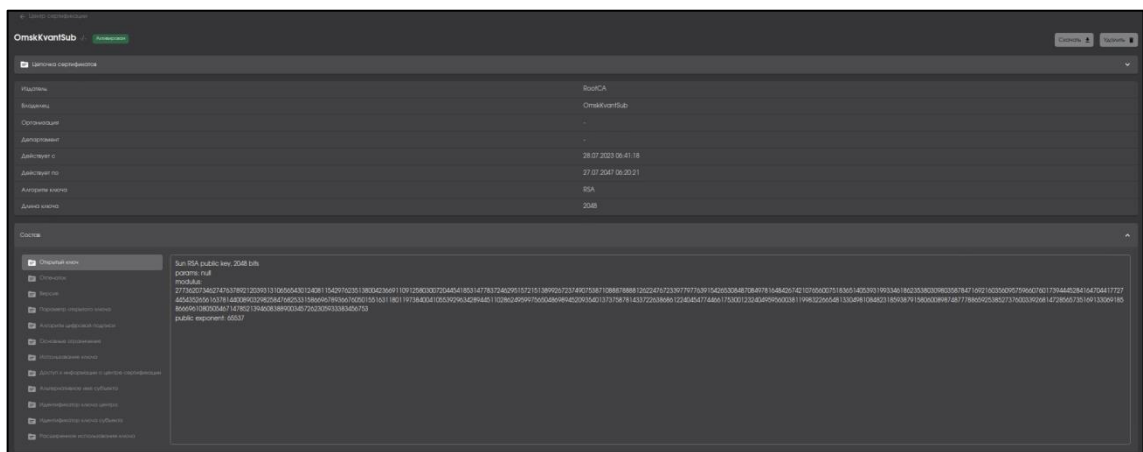



Рисунок 39 – Карточка ЦС в состоянии «Активирован»

- ID Центра Сертификации возможно определить, как крайний параметр URL-адреса Центра сертификации, например: <https://sub01.presale.aeca/access-certificates/4a660253-09bf-4cc6-a363-871a9c4cbd8c>, где 4a660253-09bf-4cc6-a363-871a9c4cbd8c является идентификатором Центра сертификации).

- В карточке активного ЦС доступны следующие действия:
 - выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки <Скачать>;
 - удалить Центр сертификации по нажатию кнопки <Удалить>.
- В карточке не активного ЦС доступны следующие действия:
 - выгрузить сертификат, цепочку сертификатов или текущий список отозванных сертификатов по нажатию кнопки <Скачать>;
 - удалить Центр сертификации по нажатию кнопки <Удалить>;
 - активировать Центр сертификации.
- В карточке Центра сертификации отображаются следующие сведения:
 - издатель;
 - владелец;
 - организация;
 - департамент;
 - срок действия («действует с», «действует до»);
 - алгоритм ключа;
 - длина ключа;
 - состав:
 - открытый ключ (поле «Subject Public Key Info»);
 - отпечаток (вычисляемое значение, отсутствует в сертификате);
 - версия (поле «Version»);
 - параметры открытого ключа (всегда «X509»);
 - алгоритм цифровой подписи (поле «Signature Algorithm»);
 - основные ограничения (поле «X509v3 Basic Constraints»);
 - использование ключа (поле «X509v3 Key Usage» сертификата);
 - доступ к информации о центре сертификации (поле «Authority Information Access»);
 - альтернативное имя субъекта (поле «X509v3 Subject Alternative Name» сертификата);
 - идентификатор ключа центра (поле «X509v3 Authority Key Identifier» сертификата);
 - идентификатор ключа субъекта (поле «X509v3 Subject Key Identifier» сертификата);
 - расширенное использование ключа (поле «X509v3 Extended Key Usage» сертификата).

7.3.1.2 Создание Центра сертификации

- Для создания Центра сертификации на вкладке «Свои сертификаты» нажмите кнопку  <Добавить сертификат +>.
- Дальнейшие шаги создания Центра сертификации описаны в пункте 3.1 настоящего Руководства.
- Новый Центр сертификации будет создан на основании текущей лицензии.

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

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

- На вкладке «Свои сертификаты» выбрать созданный Подчиненный ЦС в состоянии «Запрос» (см. Рисунок 40).

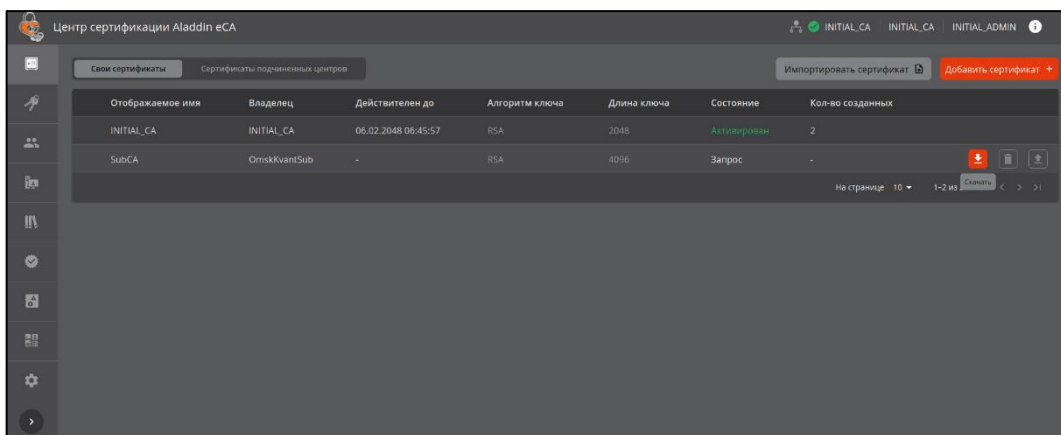




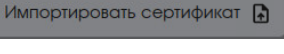
Рисунок 40 – Окно скачивания запроса на сертификат для Подчинённого ЦС

- Нажать появившуюся в строке выбранного ЦС кнопку  и скачать запрос в формате .csr.
- Далее следует подписать скачанный запрос на Корневом Центре сертификации согласно пункту о настоящего руководства администратора.

7.3.1.4 Импорт сертификата Подчиненного ЦС

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

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

На вкладке «Свои сертификаты» выбрать Подчиненный ЦС в состоянии «Запрос», по запросу которого был сформирован сертификат и цепочка сертификатов в формате .pem в п. 7.3.1.3 данного руководства. Нажать кнопку  <Загрузить> (см. Рисунок 40) или кнопку  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 41) выбрать скачанный ранее файл цепочки сертификата для загрузки в формате .pem. Нажать кнопку <Загрузить>, активированную после выбора файла цепочки сертификатов.

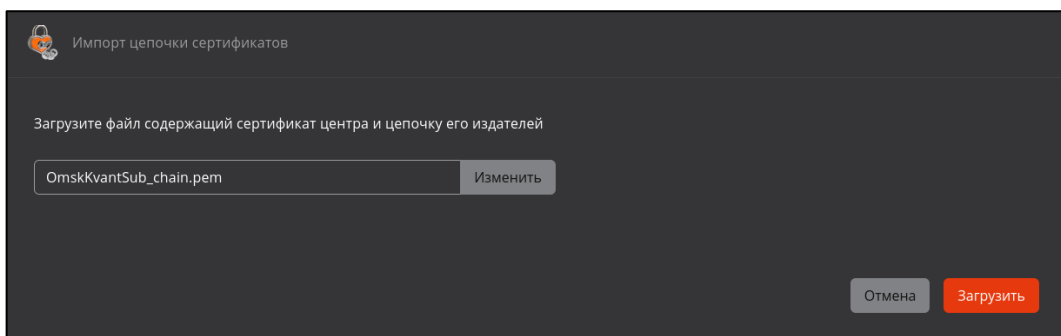


Рисунок 41 - Окно импорта цепочки сертификатов

- В процессе загрузки будет осуществлена проверка загружаемого сертификата, а именно:
 - имени подчиненного ЦС, указанного в импортируемом сертификате (компонент «Common name» в поле «Subject») на соответствие имени, указанному в лицензии подчиненного ЦС;
 - имени корневого ЦС, указанного в его сертификате (компонент «Common name» в поле «Subject») на соответствие имени корневого ЦС, указанному в лицензии;

- соответствия порядка расположения компонентов SDN в поле «Subject» в сертификате подчиненного ЦС порядку, указанному в Таблица 2;
 - соответствие структуры сертификата стандарту X.509;
 - срока действия всех сертификатов в составе цепочки;
 - аутентичность цепочки (проверка осуществляется криптографическими методами);
 - соответствие открытого ключа в сертификате закрытому ключу в Подчинённом Центре сертификации.
- В запросах на сертификат и сертификатах Центров сертификации, создаваемых Aladdin eCA компоненты SDN в поле «Subject» расположены в следующем порядке:

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

- В случае несоответствия каких-либо параметров импортируемого сертификата (цепочки сертификатов) администратор будет уведомлён сообщением об ошибке импорта сертификата Подчинённого ЦС (см. Таблица 5).

Таблица 5 – Перечень сообщений в случае неудачной попытки импорта сертификата подчинённого ЦС

Текст ошибки	Причина
Ошибка. Недействительный сертификат	Ошибка истечения срока действия сертификата, входящего в состав цепочки. Ошибка несоответствия имени подчиненного ЦС, указанного в его сертификате (компонент «Common name» в поле «Subject» сертификата подчиненного ЦС) имени, указанному в лицензии
Ошибка.	Ошибка несоответствия имени корневого ЦС, указанного

Текст ошибки	Причина
Имя корневого ЦС, указанное в сертификате, не соответствует лицензии	в его сертификате (компонент «Common name» в поле «Subject» сертификата корневого ЦС) имени корневого ЦС, указанному в лицензии
Ошибка. Сертификат ЦС содержит некорректный порядок компонентов суффикса различающегося имени	Сертификат ЦС содержит некорректный порядок компонентов суффикса различающегося имени (корректный порядок указан в функциональном требовании 3)
Ошибка. Неизвестная ошибка	Внутренняя ошибка ПО

• После успешной загрузки цепочки сертификатов открывается окно с уведомлением об успешной загрузке сертификата (см. Рисунок 42) и отображается следующая информация о сертификате ЦС:

- издатель;
- субъект;
- срок действия сертификата.

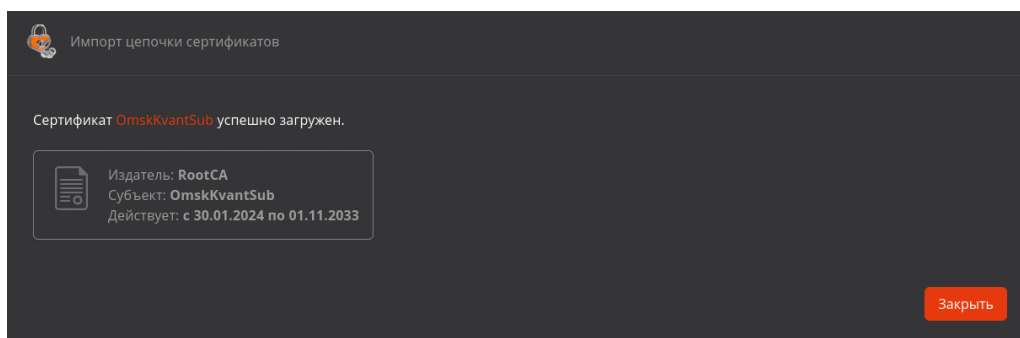


Рисунок 42 – Окно уведомления об успешном загрузке сертификата

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

7.3.1.5 Удаление Центра сертификации

- Условия удаления Центра сертификации:
 - удаляемый Центр сертификации находится в состоянии «Не активирован» (см. Рисунок 43);

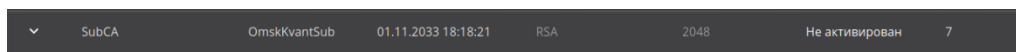


Рисунок 43 – Раздел «Центр сертификации» – Вкладка «Свои сертификаты» – Состояние удаляемого ЦС

- выключена проверка издателя – удаляемого Центр сертификации (см. Рисунок 44, пункт 7.12.2 настоящего руководства).

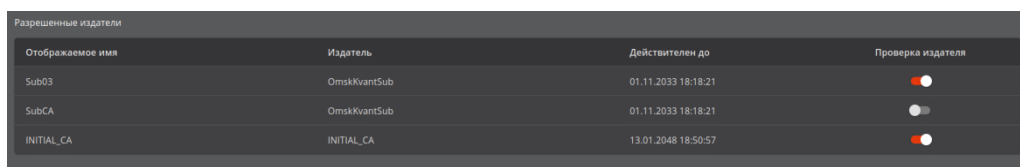

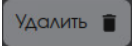


Рисунок 44 – Раздел «Настройки» – Поле «Разрешённые издатели» - Выключение издателя из разрешённых

- создан новый Центр сертификации (см. пункт 7.3.1.2 настоящего руководства);

- импортирован сертификат вновь созданного Центра сертификации (см. пункт 7.3.1.4 настоящего руководства). После активации вновь созданного Центра сертификации будут восстановлены:
 - o ранее зарегистрированные ресурсные системы;
 - o загруженные субъекты ранее зарегистрированных ресурсных систем;
 - o шаблоны;
 - o учётные записи;
 - o журнал событий, также содержащий событие удаления ЦС с кодом CAENV038.
- выпущен сертификат доступа вновь созданным Центром сертификации для учётной записи пользователя с целью авторизации в программе;
- выпущен сертификат доступа web-сервера вновь созданным Центром сертификации;
- установлен сертификат доступа web-сервера.
- Для удаления Центра сертификации, наведите указатель мыши на строку с выбранным ЦС и нажмите кнопку  или откройте карточку выбранного ЦС и нажмите кнопку  **Удалить**.
- В появившемся окне подтверждения внимательно ознакомьтесь с рекомендациями (см. Рисунок 45).

Внимание! После удаления Центра сертификации будут также удалены:

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

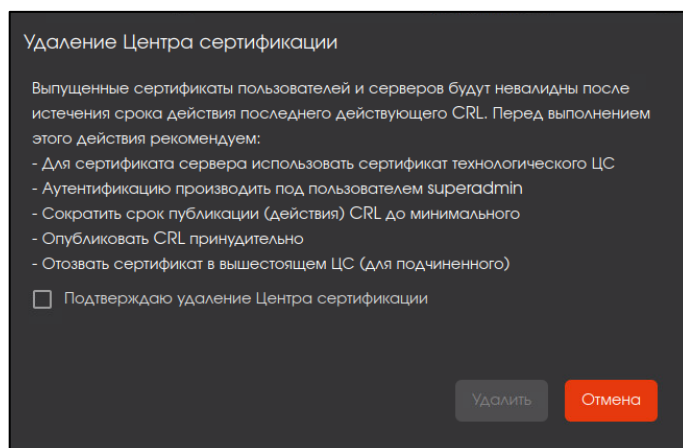


Рисунок 45 – Окно подтверждения удаления Центра сертификации

- Сертификаты, ранее выпущенные удалённым ЦС, будут действительны до следующего запланированного обновления списка отозванных сертификатов.
- Центр валидации, ранее зарегистрированный удалённым ЦС, необходимо самостоятельно удалить на сервере отзыва.
- Для подтверждения удаления ЦС установите флаг в чек-боксе «Подтверждаю удаление Центра сертификации» и нажмите ставшую активной кнопку <Удалить> (см. Рисунок 46). Для прерывания процесса удаления ЦС нажмите кнопку <Отмена>.

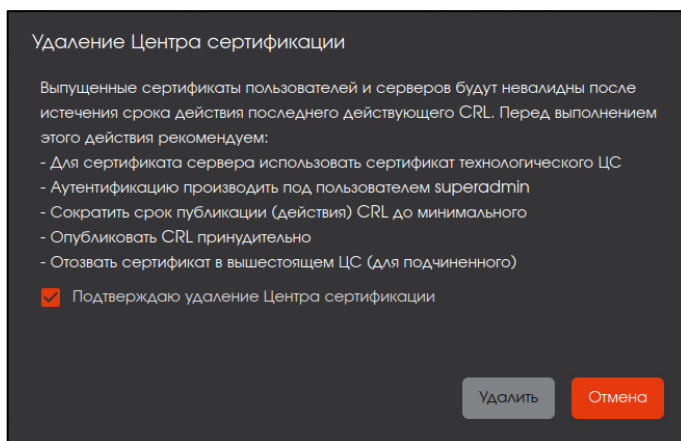


Рисунок 46 – Окно подтверждения удаления Центра сертификации. Чек-бокс подтверждения активирован

- В результате удаления центра сертификации в журнал событий будут занесены записи:
 - с кодом CAENV059;
 - с кодом CAENV038 (изменение списка издателей);
 - с кодом CAENV060.
- При попытке удаления активного или разрешённого издателя ЦС будет выведено сообщение (см. Рисунок 47).

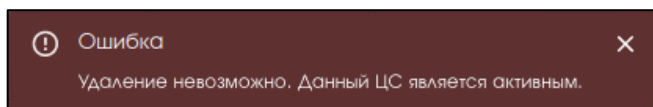


Рисунок 47 – Уведомление об ошибке при попытке удаления активного или разрешённого издателя ЦС

7.3.2 Вкладка «Сертификаты Подчиненных центров»

- Вкладка «Сертификаты Подчиненных центров» (см. Рисунок 48) предназначена для работы с Сертификатами Подчиненных ЦС нижнего уровня, сертификаты которых подписаны ЦС из категории «Свои сертификаты».
- Варианты состояния и возможных операций над сертификатами из категории «Сертификаты Подчиненных центров» с учетом наведенного указателя мыши и без приведены в Таблица 6.
- Нажатие на кнопку <Подписать запрос> запускает сценарий подписи запроса Подчиненного ЦС из категории «Сертификаты Подчиненных центров».

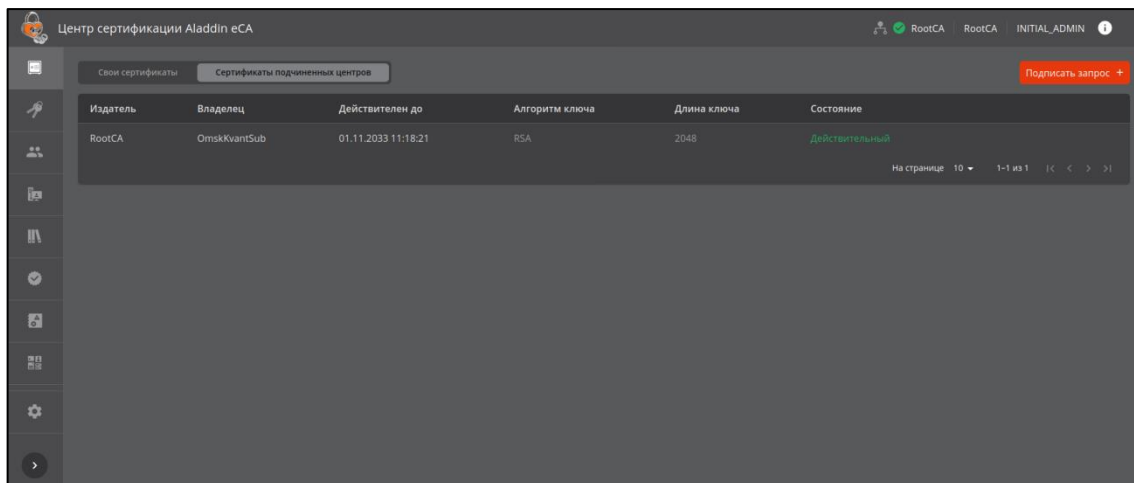


Рисунок 48 - Экран «Сертификаты Подчиненных центров»

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

- издатель;
- владелец;
- действителен до (дата);
- алгоритм ключа;
- длина ключа;
- состояние (варианты состояний: действительный, отозван, истёк срок).

• Управляемые поля. В соответствии с состоянием Подчиненного сертификата при помощи кнопок управления, расположенных на табличных полях, возможны действия, приведенные в Таблица 6.

Таблица 6 – Действия над сертификатами Подчиненных центров

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

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

7.3.2.1 Карточка сертификата подчинённого ЦС

• Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» (см. Рисунок 39).

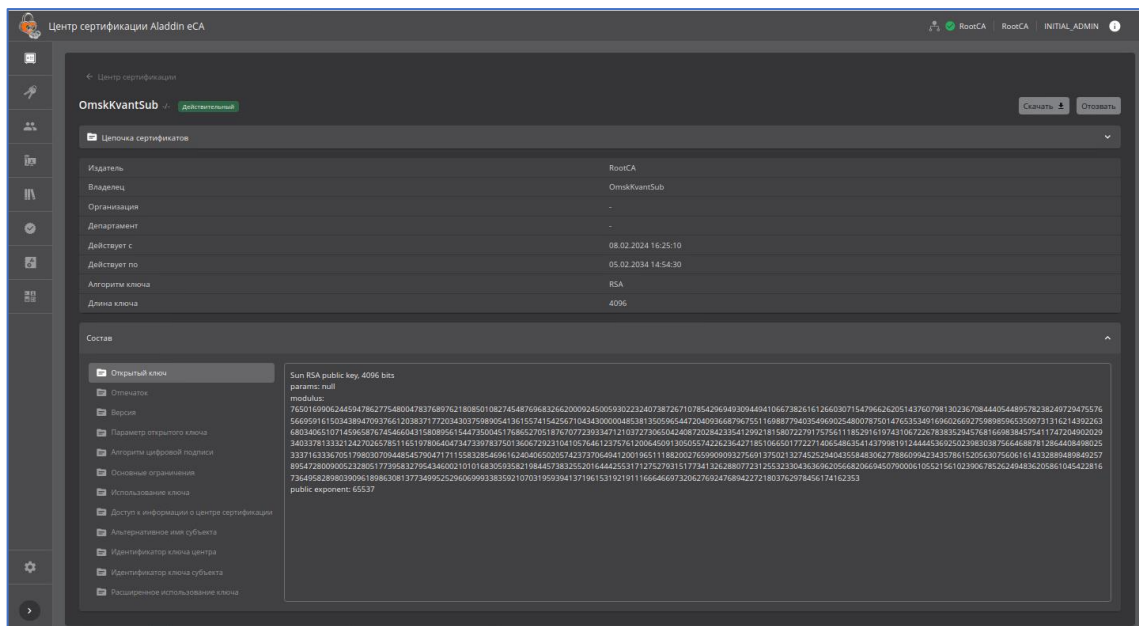


Рисунок 49 – Экран карточки сертификата Подчинённого ЦС в состоянии «Действительный»

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

- отозвать сертификат ЦС по нажатию кнопки <Отозвать>.

Набор кнопок в карточке ЦС в зависимости от статуса сертификата ЦС соответствует приведённым действиям в Таблица 6.

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

7.3.2.2 Подписание запроса на Корневом ЦС

- После предварительного скачивания запроса на сертификат Подчинённого ЦС и переноса его на Корневой ЦС выполните подписание согласно нижеприведённой инструкции.
- При активном Корневом ЦС, от имени которого будет выдан сертификат, на вкладке «Сертификаты Подчинённых центров» нажать кнопку <Подписать запрос+> (см. Рисунок 50)

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

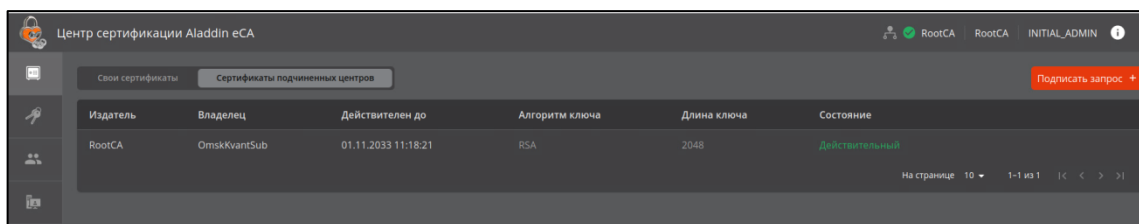


Рисунок 50 – Окно «Сертификаты Подчинённых ЦС»

- Далее загрузите запрос в формате .csr, скачанный на шаге 7.3.1.3, нажав кнопку <Выбрать файл> (см. Рисунок 51).

- Выберите шаблон сертификата Подчинённого центра сертификации (например, предварительно подготовленный шаблон путём редактирования клонированного предустановленного шаблона Подчинённого центра сертификации в разделе «Шаблоны»)

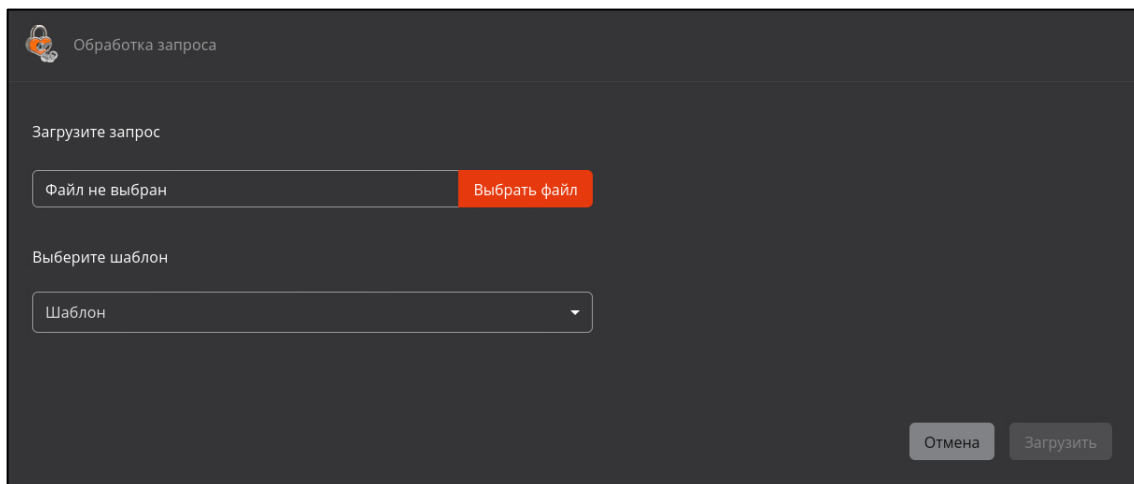


Рисунок 51 – Окно выбора файла запроса

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку <Изменить> (см. Рисунок 52).

- Нажмите ставшую активной кнопку <Загрузить> (см. Рисунок 52).

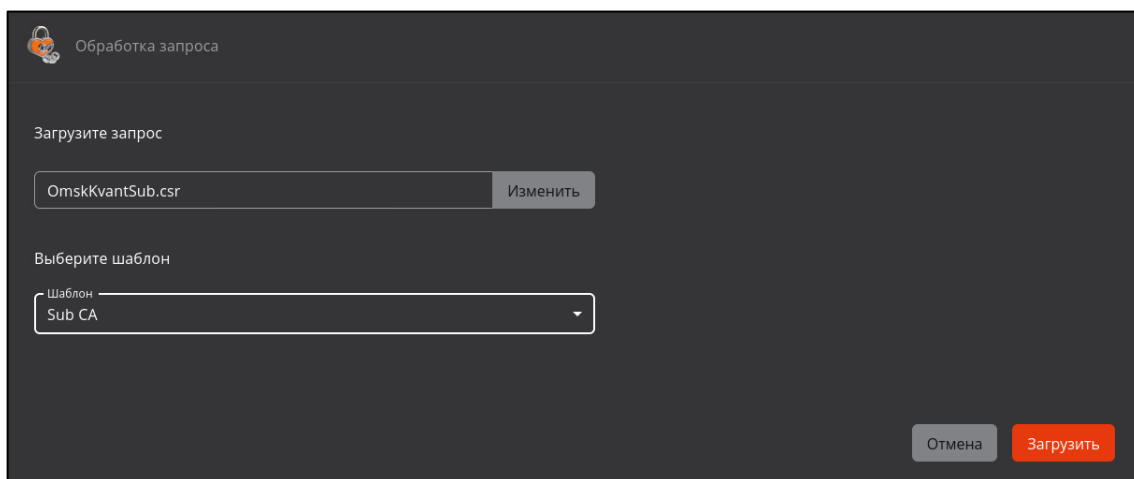


Рисунок 52 – Окно загрузки файла запроса

• При нажатии кнопки <Загрузить> происходит загрузка файл запроса в Корневой ЦС (текущий активный Корневой ЦС из категории «Свои сертификаты»). Далее администратор видит уведомление о том, что сертификат Подчиненного ЦС успешно сформирован и подписан Корневым ЦС (см. Рисунок 53).

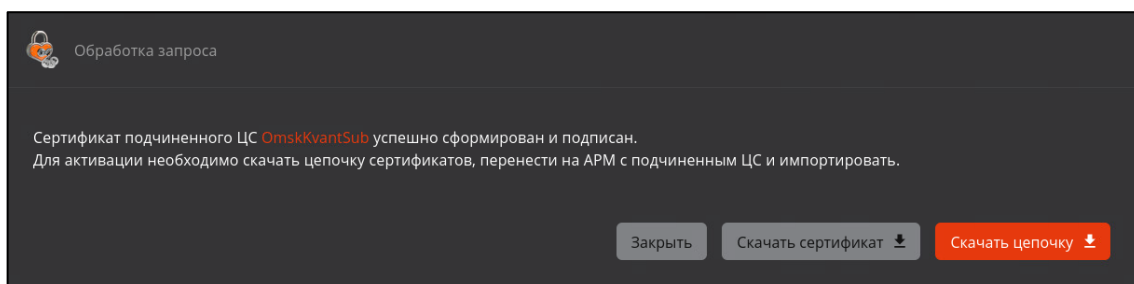


Рисунок 53 – Окно успешного формирования и подписи сертификата

- В случае если на основании загруженного запроса ранее был выпущен сертификат Подчинённого ЦС администратор будет уведомлён сообщением (см. Рисунок 54).

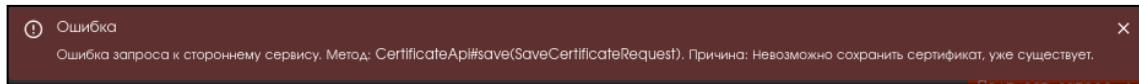



Рисунок 54 – Уведомление о том, что по загруженному запросу ранее выпущен сертификат

- Необходимо скачать цепочку сертификатов ЦС в формате .pem, нажав кнопку <Скачать цепочку сертификатов>, в окне «Обработка запроса» на данном шаге для дальнейшего импорта на Подчинённом центре сертификации.
- Скачать сформированный и подписанный сертификат, а также цепочку сертификатов можно позднее, открыв вкладку «Сертификаты Подчиненных центров», выбрав нужный сертификат и нажав появившуюся кнопку  для скачивания сертификата или цепочки сертификатов, выбрав соответствующий пункт в раскрывшемся меню (см. Рисунок 55).

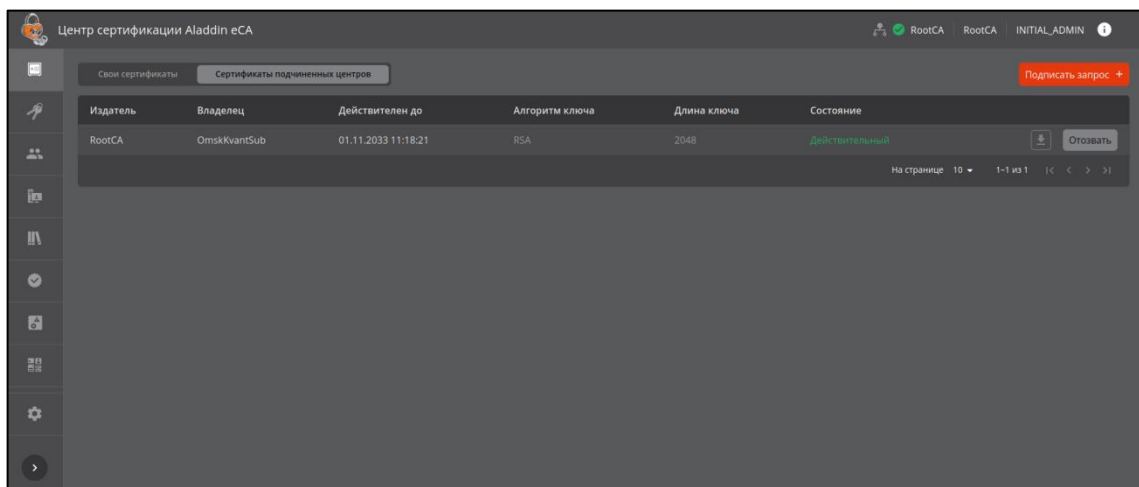


Рисунок 55 – Окно вкладки «Сертификаты Подчиненных центров» с выбранным сертификатом

- Далее перенесите сертификат на Подчинённый ЦС и выполните импорт цепочки сертификатов согласно пункту 7.3.1.4 настоящего руководства.

7.4 Раздел «Сертификаты»

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

Переход на экран управления центра сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 36).

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

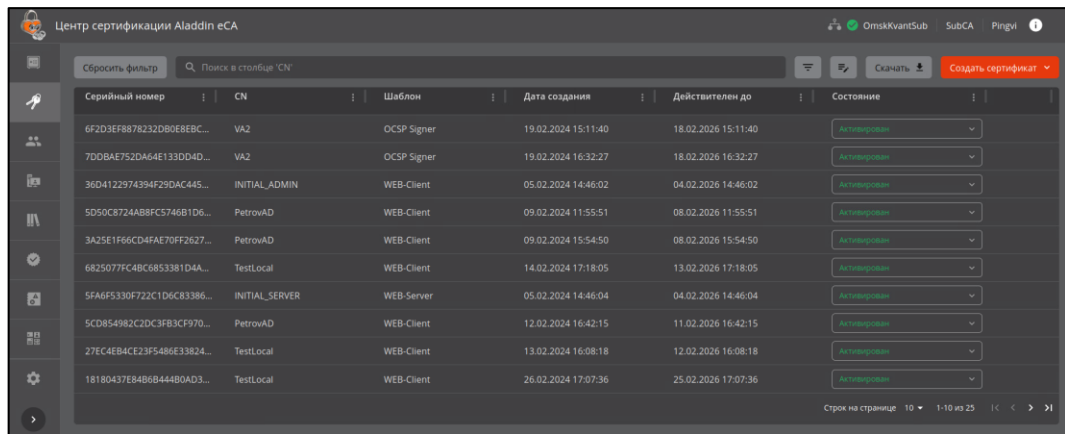


Рисунок 56 - Экран раздела меню «Сертификаты»

- На экране раздела «Сертификаты» отображены информационные элементы (табличные поля):
 - серийный номер сертификата;
 - имя субъекта (CN);
 - тип шаблона сертификата (шаблон);
 - дата выпуска сертификата;
 - дата срока окончания действия сертификата (действителен до);
 - текущий статус сертификата (состояние).
- Доступны следующие операции по работе с сертификатами:
 - выпуск нового сертификата;
 - поиск выпущенных сертификатов;
 - сортировка сертификатов;
 - просмотр списка сертификатов с заданными критериями;
 - сброс всех применённых фильтров или выборочная отмена выбранного фильтра;
 - скачивание сертификатов в формате .pem;
 - скачивание цепочки сертификатов;
 - изменение статуса сертификатов;
 - просмотр карточки сертификата;
 - экспорт списка всех выпущенных сертификатов с атрибутами;
 - массовые операции с выпущенными сертификатами.
- Все созданные сертификаты (в формате .pem) и закрытые ключи (в формате pkcs#12) субъектов будут сохранены в базе данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`), схема базы данных «store», таблица «file_registry».
 - 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.

7.4.1 Выпуск сертификата

- Для выпуска сертификата для существующего или нового субъекта нажмите кнопку «Создать сертификат» и выберите способ создания из выпадающего списка (см. Рисунок 57):
 - с закрытым ключом;
 - на основании запроса;

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

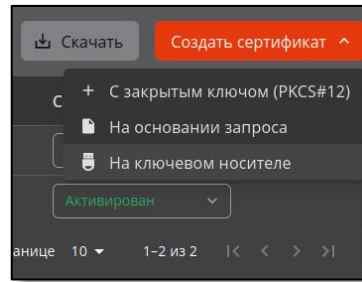


Рисунок 57 – Выпуск сертификата в разделе «Сертификаты»

7.4.2 Поиск сертификатов

Строка поиска (см. Рисунок 58) 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.

Серийный номер	CN	Шаблон	Дата создания	Действителен до	Состояние
5D50C8724AB8FC5746B1D6...	PetrovAD	WEB-Client	09.02.2024 11:55:51	08.02.2026 11:55:51	Активирован
3A25E1F66CD4FAE70FF2627...	PetrovAD	WEB-Client	09.02.2024 15:54:50	08.02.2026 15:54:50	Активирован

Рисунок 58 – Поисковая строка в разделе «Сертификаты»

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

7.4.3 Сортировка сертификатов


- Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 59):
 - «Серийный номер» – сортировка осуществляется в порядке возрастания или убывания значения;
 - «CN» – сортировка осуществляется в алфавитном порядке;
 - «Шаблон» – осуществляется группировка по типу шаблона;
 - «Дата выпуска», «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 59 – Поля сортировки содержимого раздела «Сертификаты»

- Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатию кнопки <Действия в колонке>, выбрав и нажав в раскрывшемся меню «Сортировать...» (см. Рисунок 61).

7.4.4 Фильтрация сертификатов

7.4.4.1 Применение фильтров

• Для выборочного просмотра сертификатов на экране раздела «Сертификаты» возможно применение фильтров. Для отображения параметров фильтрации для всех колонок таблицы нажмите кнопку <Фильтр> , заголовки колонок экранной таблицы будут дополнены полями фильтра для каждой колонки (см. Рисунок 156):

- шаблон. Выберите шаблоны сертификатов для отображения списка сертификатов, которые были выпущены на основании выбранных шаблонов;
- дата создания. Выберите за какой период создания отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
- действителен до. Выберите за какой период даты окончания действия отобразить сертификаты на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
- состояние. Выберите состояния сертификатов для отображения (активирован, приостановлен, отозван).

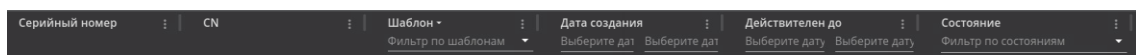



Рисунок 60 – Поля фильтра заголовков экранной таблицы


• Выберите одно или несколько значений фильтров, после выбора фильтр будет применён сразу автоматически.

• Повторное нажатие кнопки <Фильтр>  скроет поля выбора критериев фильтрации, но не отменяет применённые фильтры.

• Заголовки таблицы, для которых применён фильтр, будут отмечены знаком .

7.4.4.2 Сброс применённых фильтров

• Для очистки применённых фильтров для каждого заголовка колонки:

- нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 61);

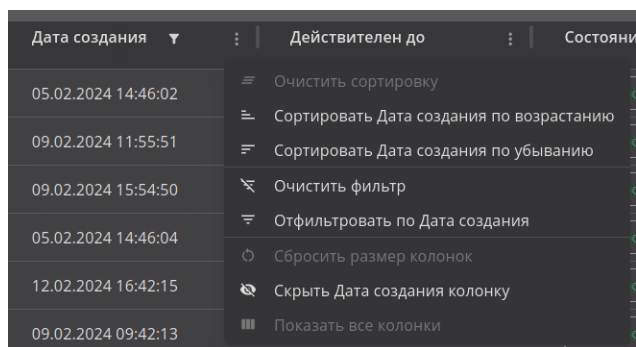
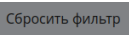



Рисунок 61 – Кнопка <Очистить> фильтр

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

7.4.5 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 56) и в раскрывшемся подменю выберите пункт <Скачать сертификат> или <Скачать цепочку> в формате .pem (см. Рисунок 62).

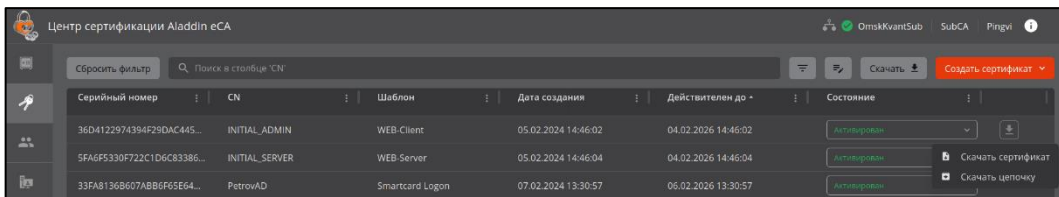


Рисунок 62 – Подменю «Скачать сертификат/цепочку»

7.4.6 Статус сертификатов

- Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 7.

Таблица 7 – 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 63).

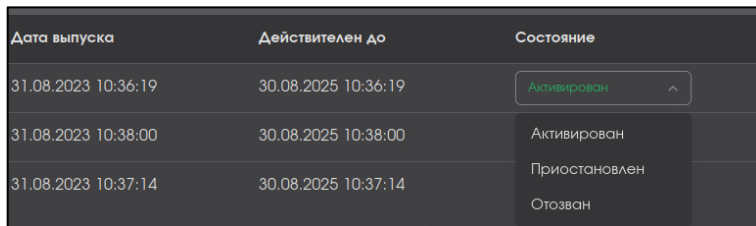


Рисунок 63 – Выпадающее меню смены состояния сертификата

- 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 64)

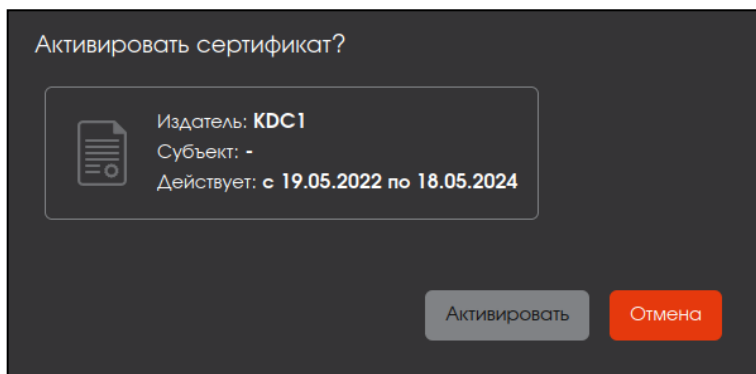


Рисунок 64 – Окно активации сертификата

- отзыв (см. Рисунок 65);

ВНИМАНИЕ! Данную операцию нельзя отменить.

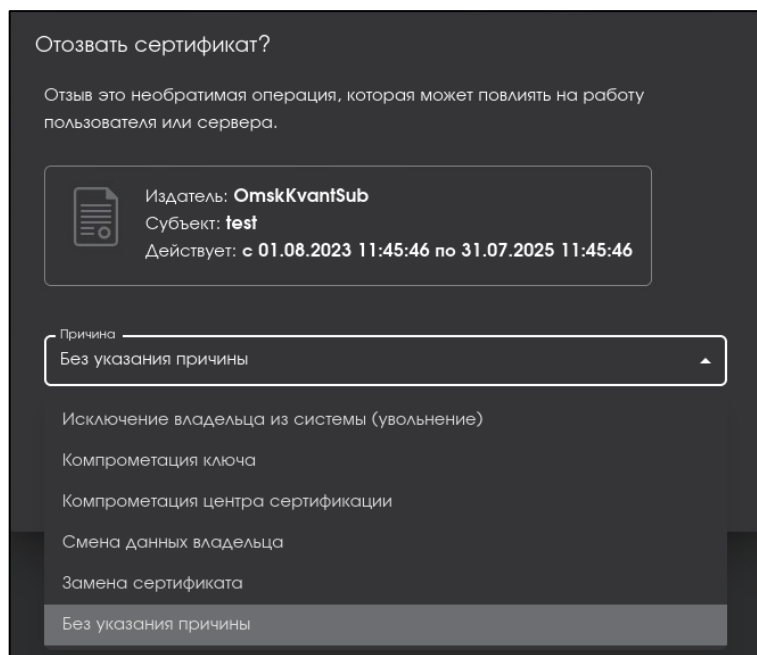


Рисунок 65 – Окно отзыва сертификата

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

- неиспользуемый (unused) – исключение владельца из системы/увольнение;
 - принадлежность изменена (affiliation Changed) – смена данных владельца;
 - компрометация ключа (keyCompromise);
 - компрометация центра сертификации (cACompromise);
 - заменен (сертификат) – заменен на иной сертификат;
 - без указания причины (unspecified).
- Приостановка действия сертификата (см. Рисунок 66):

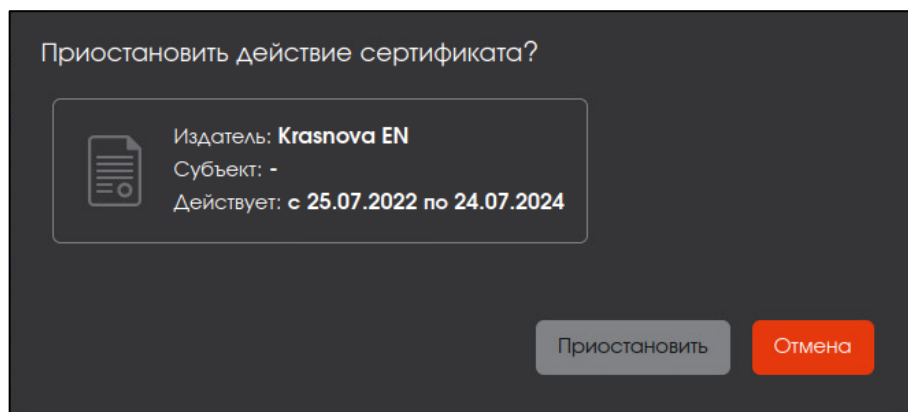


Рисунок 66 – Окно приостановки действия сертификата

7.4.7 Карточка сертификата

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см. Рисунок 67) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 56).

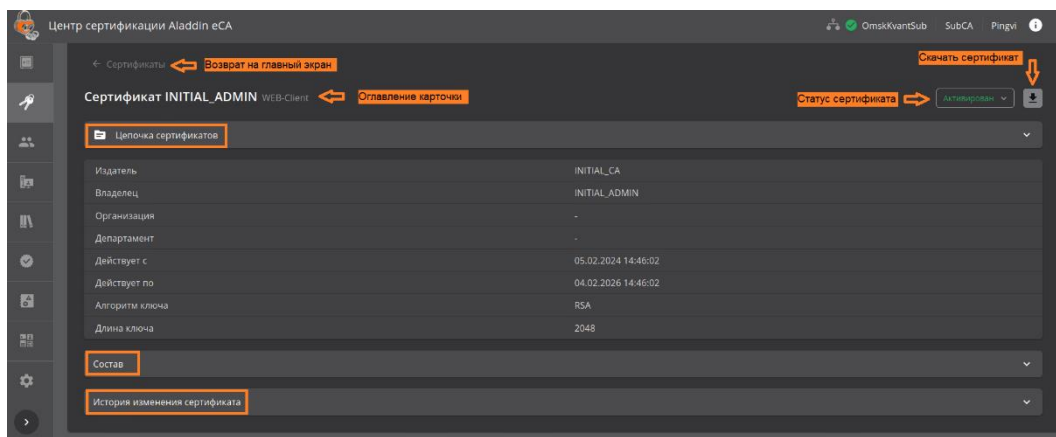


Рисунок 67 – Окно «Карточка сертификата»





- Оглавление карточки сертификата включает в себя:
 - тип-сертификата;
 - принадлежность;
 - тип субъекта.
- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке .
- Для изменения статуса сертификата выбрать из выпадающего списка действие в соответствии с Таблица 7.
- Для скачивания сертификата наведите указатель мыши на кнопку , во всплывающем меню выберите <Скачать сертификат> субъекта или <Скачать цепочку> сертификатов.
- Карточка сертификата содержит раскрывающиеся вкладки:
 - «Цепочка сертификатов». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены все Центры сертификации, участвующие в построении цепочки сертификатов, начиная с Корневого ЦС, на основе которого строится цепочка доверия сертификатам, до конечного Центра сертификации, выдавшего текущий сертификат субъекта (см. Рисунок 68).



Рисунок 68 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 69):
 - серийный номер;
 - открытый ключ;
 - отпечаток;
 - версия;
 - параметр открытого ключа;
 - алгоритм цифровой подписи
 - основные ограничения;
 - использование ключа;

- доступ информации о центре сертификации;
- альтернативное имя субъекта;
- идентификатор ключа центра;
- идентификатор ключа субъекта;
- расширенное использование ключа.

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

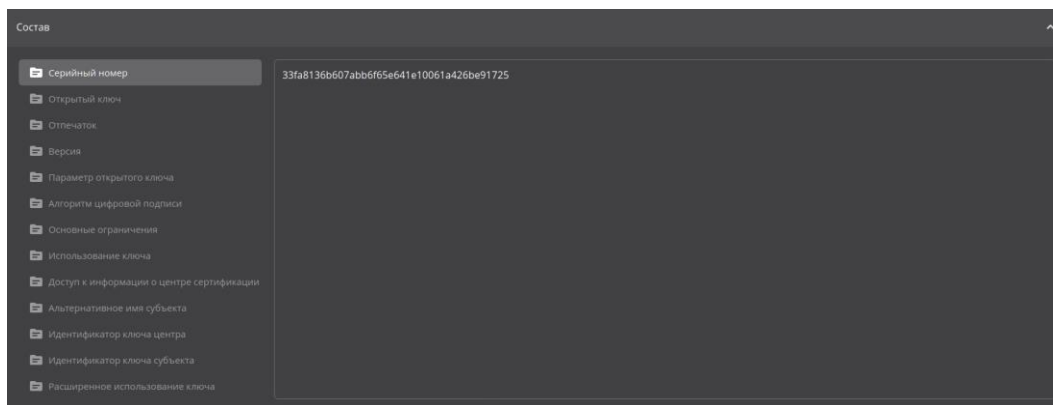



Рисунок 69 – Окно карточки сертификатов. Вкладка «Состав»

- «История изменения сертификата». Раскройте вкладку, нажав в строке с именем вкладки символ . На данной вкладке зафиксирована информация о всех совершённых над сертификатом действиях в хронологическом порядке. На раскрывшемся экране отображены поля (см. Рисунок 70):
 - дата – дата совершенного действия;
 - пользователь – учётная запись, под которой было совершено данное действие;
 - событие – действие, совершённое над сертификатом.

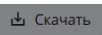
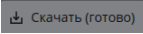
Дата	Пользователь	Событие
01.08.2023 11:45:45	INITIAL_ADMIN	Выпущен
01.08.2023 11:51:58	INITIAL_ADMIN	Приостановлен Приостановка полномочий владельца
01.08.2023 12:00:12	INITIAL_ADMIN	Активирован Удален из CRL

Рисунок 70 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

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

7.4.8 Экспорт списка выпущенных сертификатов

- При использовании учётной записи с ролью «Администратор» можно сохранить полный список всех выпущенных сертификатов в виде .csv файла.
- При использовании учётной записи «Оператор» в список .csv файла будут собраны только выпущенные сертификаты тех субъектов, права доступа на которые назначены данному оператору.

- Для выгрузки списка сертификатов нажмите кнопку  <Скачать все сертификаты в формате CSV>. Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние . Нажмите кнопку <Скачать (готово)> для сохранения подготовленного списка сертификатов.
- Сохранение списка сертификатов в виде zip-архива происходит по выбранному пути в открывшемся окне сохранения файла (см. Рисунок 71).

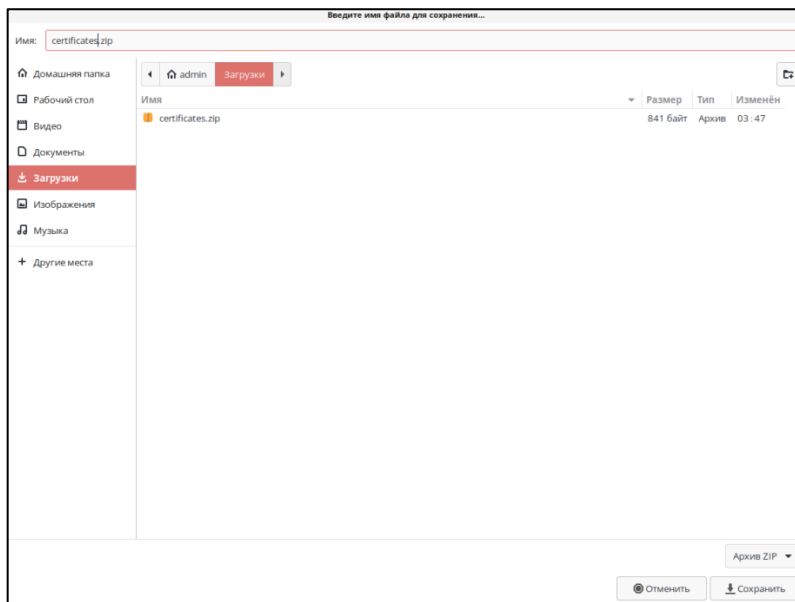


Рисунок 71 – Окно указания пути сохранения файла

- Выгруженный файл .csv (заархивированный при выгрузке) представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделённые запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 72):
 - fingerprint – содержит уникальный числовой отпечаток сертификата;
 - cafingerprint – содержит уникальный числовой отпечаток сертификата центра, подписавшего сертификат;
 - expire date – содержит значение даты «годен до»;
 - issuerdn – содержит отличительное имя издателя;
 - revocation date – содержит дату отзыва;
 - revocation reason – содержит причину отзыва;
 - serialnumber – содержит серийный номер сертификата;
 - status – содержит текущий статус сертификата;
 - subjectdn – содержит отличительное имя держателя сертификата;
 - create date – содержит дату выпуска сертификата;
 - username – содержит имя держателя сертификата;
 - subject alt name – содержит дополнительные имена держателя;
 - template – содержит наименование шаблона;
 - algorithm – содержит обозначение алгоритма;
 - key length – содержит длину ключа;
 - history – содержит историю изменений сертификата в формате JSON.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
1	fingerprint	ca:fingerprint	expire date	issuerrdn	revocation date	revocation reason	serialnumber	status	subjectdn	create date	username	subject alt name	template	algorithm key length	
2	532af36b56567	0f83238c98d881	#####	CN=SubCA242,	02.09.2022 13:18	Revoked: Cessation c	7f7b2814f9a1e1	HOLD	CN=SubCA242	#####	SubCA242	null	OCSP Signer	RSA 2048	
3	c32484f9822d6f	0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	29644f71ac761c	HOLD	CN=DC	#####	DC	dNSName=DC, gu	Domain Cont	RSA 2048	
4	5258bc09c2061f	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	699edc111e1c1e	REVOKED	CN=cheburger	#####	cheburger	rfc822name=cheb	Smartcard Loj	RSA 1024	
5	47b18421ec4d2	0f83238c98d881	#####	CN=SubCA242,		Active	5110646ee2431	ACTIVE	CN=SubCA242	#####	SubCA242-web	dNSName=SubCA	WEB-Server	RSA 2048	
6	7c13052621aff	0f83238c98d881	#####	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	6772c7275957b1	REVOKED	CN=OP1_242	#####	OP1_242	rfc822name=op1@	WEB-Client	RSA 2048	
7	52f46cc8e30f6	0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	79878f39e5d30c	REVOKED	CN=OP2_242	#####	OP2_242	rfc822name=op2@	WEB-Client	RSA 2048	
8	c411492ef40dc	0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	171a95d06d320	REVOKED	CN=koltakova	#####	koltakovav	rfc822name=eaca	Smartcard Loj	RSA 2048	
9	f83c0f0ccb22a0	0f83238c98d881	#####	CN=SubCA242,	04.09.2022 14:46	Revoked: Cessation c	659787b69d9f9	HOLD	CN=tushkan	#####	tushkan	rfc822name=tushl	Smartcard Loj	RSA 2048	
10	dec1c1520014;	0f83238c98d881	#####	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	6360503883063;	HOLD	CN=SUBCA	#####	SUBCA	dNSName=SUBCA	Domain Cont	RSA 3072	
11	110ffbd7a6f1a	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	560f36c6f48609	REVOKED	CN=ttttttt	#####	ttttttt	rfc822name=tt@t	Smartcard Loj	RSA 2048	
12	bd8e4c11e4e36	0f83238c98d881	#####	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	09f6b09eaf14e1	REVOKED	CN=OP1_242	#####	OP1_242	rfc822name=test@	WEB-Client	RSA 2048	
13	f9c9f93951e7c	0f83238c98d881	#####	CN=SubCA242,	02.09.2022 10:03	Suspended: Certifica	549b9e8b41de	REVOKED	CN=ushkan	#####	ushkan	rfc822name=ushk	Smartcard Loj	RSA 2048	
14	8c32419d620b;	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	360c2020731a1	REVOKED	CN=tushkan	#####	tushkan	dNSName=tushka	Domain Cont	RSA 2048	
15	bed018556dbt	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 12:38	Suspended: Certifica	6a60f1d27e71	REVOKED	CN=SUBCA	#####	SUBCA	dNSName=SUBCA	Domain Cont	RSA 3072	
16	d93b3f0eb9dc	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 12:37	Suspended: Certifica	3bf0b012fbd3f	REVOKED	CN=OCSP	#####	OCSP	02.09.2022 9:54	OCSP	Domain Cont	RSA 2048
17	3e352d5bf4f9c	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	1dc1aac2042d3f	REVOKED	CN=paukan	#####	paukan	rfc822name=pauk	Smartcard Loj	RSA 2048	
18	4810c3f5cbbbc	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 13:28	Suspended: Certifica	35e5f0c041cc8	REVOKED	CN=testop	#####	testop	rfc822name=sauk	Smartcard Loj	RSA 1024	
19	3614f6c6e324e5	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 15:01	Suspended: Certifica	201fe17d371d	REVOKED	CN=DC	#####	DC	dNSName=DC, gu	Domain Cont	RSA 2048	
20	4f2b63a93d73f	0f83238c98d881	#####	CN=SubCA242,		Active	762a8430c0356f	ACTIVE	CN=operator	#####	operator	rfc822name=swsd	WEB-Client	RSA 2048	
21	8b5c6e050346;	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 17:30	Suspended: Certifica	7061a34d5576b	REVOKED	CN=operator	#####	operator	rfc822name=test@	WEB-Client	RSA 2048	
22	06335097415b	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 15:57	Suspended: Certifica	2df664eb41687	REVOKED	CN=paukan	#####	paukan	rfc822name=pauk	Smartcard Loj	RSA 2048	
23	01f4dade2341;	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 16:37	Suspended: Certifica	124f06965c59bc	REVOKED	CN=Guest	#####	Guest	dNSName=Guest,	Domain Cont	RSA 2048	
24	07e080b9ca0b	0f83238c98d881	#####	CN=SubCA242,	01.09.2022 17:49	Suspended: Certifica	5fa7bd4816ce9	REVOKED	CN=test	#####	test	rfc822name=test@	Smartcard Loj	RSA 2048	
25	fc8bcd2875a1e	0f83238c98d881	#####	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	6ed38ad110043d	HOLD	CN=kruchinin	06.09.2022 0:37	kruchinina	rfc822name=alex	Smartcard Loj	RSA 2048	
26	ad3e9bed85d1	0f83238c98d881	#####	CN=SubCA242,	04.09.2022 8:50	Suspended: Certifica	365612cc14a7f9	REVOKED	CN=C-PIP* PIP	#####	C-PIP* PIP*	rfc822name=dfsd	Smartcard Loj	RSA 2048	
27	23421a1f5bdc;	0f83238c98d881	#####	CN=SubCA242,		Active	513c1b4479c38c	ACTIVE	CN=OP2_242	#####	OP2_242	rfc822name=swsd	WEB-Client	RSA 2048	
28	8defcb24f54df	0f83238c98d881	#####	CN=SubCA242,	04.09.2022 12:02	Revoked: Cessation c	4d70c1e01f42f	HOLD	CN=CLIENT2	#####	CLIENT2	dNSName=CLIENT	Domain Cont	RSA 2048	
29	9ba4eecd5179	0f83238c98d881	#####	CN=SubCA242,	05.09.2022 15:58	Active	666cbb74489eaf	ACTIVE	CN=OCSP	#####	OCSP	02.09.2022 9:54	OCSP	Domain Cont	RSA 2048
30	c73f85322b4e8	0f83238c98d881	#####	CN=SubCA242,		Active	17b0c9697f993f	ACTIVE	CN=OP1_242	#####	OP1_242	rfc822name=op1@	WEB-Client	RSA 2048	
31	4f1f61efba662	0f83238c98d881	#####	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	3c31d8839d6f6	HOLD	CN=koltakova	#####	koltakovav	rfc822name=eaca	Smartcard Loj	RSA 2048	
32	88bb73a7ae71	0f83238c98d881	#####	CN=SubCA242,	05.09.2022 16:11	Revoked: Cessation c	7aae5b17f1c57	HOLD	CN=testuser2	#####	testuser2	rfc822name=testu	Smartcard Loj	RSA 2048	

Рисунок 72 – Пример экспортированного файла списка выпущенных сертификатов.csv

7.4.9 Массовые операции с сертификатами

- Для массовой операции, применяемой к выбранному множеству сертификатов доступа, нажмите кнопку



<Массовые операции>, которая запускает окно выполнения массовой операции (см. Рисунок 73).

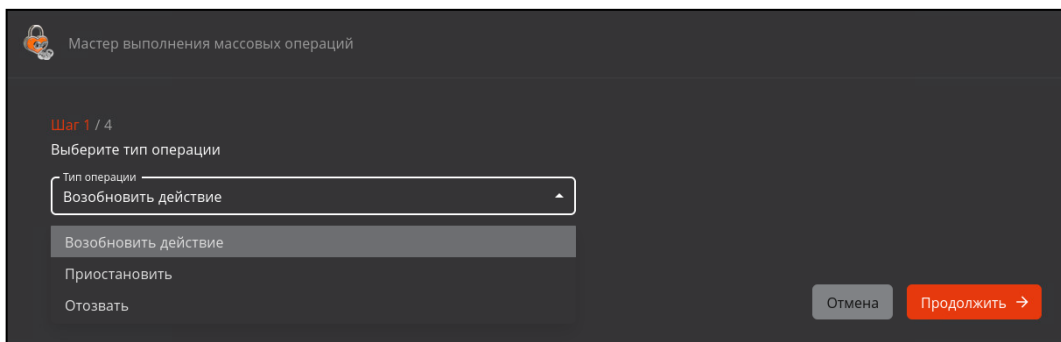




Рисунок 73 – Окно выполнения массовых операций. Шаг 1

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

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

- Нажмите ставшую активной кнопку <Продолжить>.
- Далее необходимо осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом поле окна Шага 2 (см. Рисунок 74). 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 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.

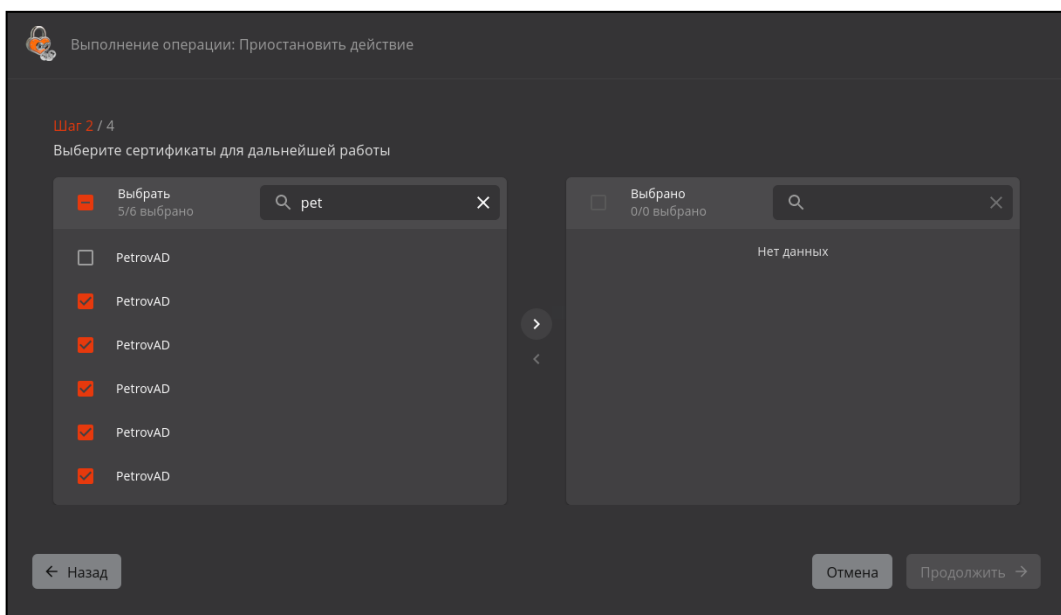



Рисунок 74 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

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

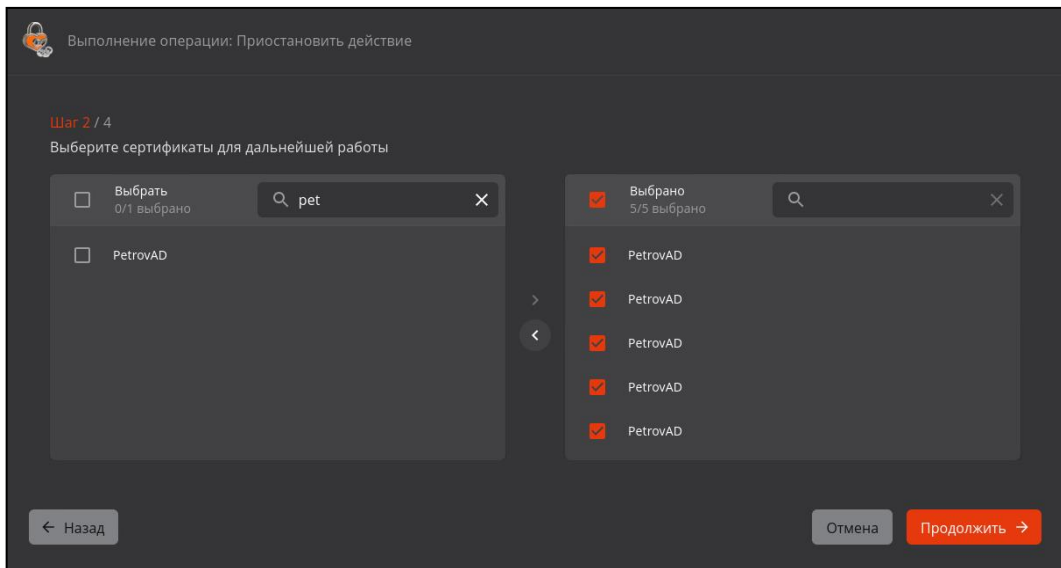


Рисунок 75 – Окно выполнения массовых операций. Шаг 2. Редактирование списка выбранных сертификатов

- Для перехода на следующий шаг нажмите кнопку <Продолжить>.
- В открывшемся окне подтвердите действие, нажав кнопку «Применить» (см. Рисунок 76).

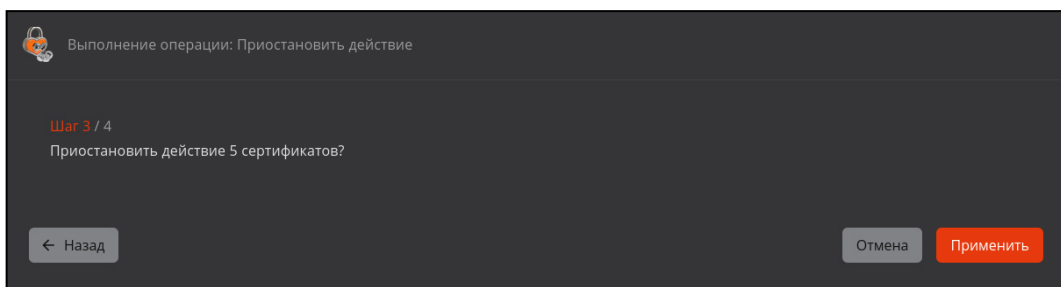


Рисунок 76 – Окно выполнения массовых операций. Шаг 3

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

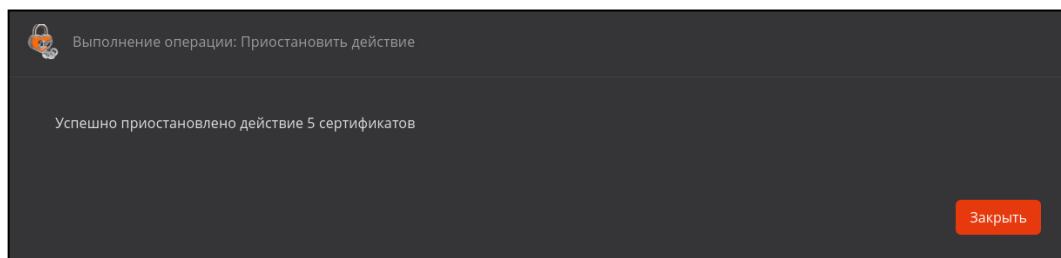


Рисунок 77 – Окно выполнения массовых операций. Шаг 4

7.5 Настройка уведомлений об истечении срока действия сертификата

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

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

7.5.1 Настройка параметров конфигурационного файла config.sh

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

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

- Блок настройки уведомлений об истечении срока действия сертификата конфигурационного файла `/opt/aecaCa/scripts/config.sh` и описание настроек приведены в Таблица 8.

Таблица 8 – Переменные окружения, используемые сервисом event-delivery-service, файла `config.sh`

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

- Для применения внесенных настроек (обновления конфигурационного файла `/opt/aecaCa/configuration/environment/event-delivery-service.env`) следует запустить сценарий обновления, выполнив команду:

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

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

7.5.2 Настройка шаблонов уведомлений об истечении срока действия сертификата

- В базе данных в таблице «`delivery.delivery_template`» хранится набор шаблонов рассылки уведомлений.
 - Каждый шаблон определяет следующие параметры отправки уведомления:
 - наименование шаблона;
 - признак необходимости запуска выполнения действий по этому шаблону;
 - отслеживание времени окончания срока действия сертификата, для отправки уведомлений в установленный в шаблоне срок.
 - тему письма, указанную при отправке уведомления.
 - По умолчанию созданы шаблоны, описанные в Таблица 9.

Таблица 9 – Шаблоны, настроенные по умолчанию

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

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

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

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

- Для просмотра списка существующих шаблонов уведомлений выполните команду:

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

- Отредактируйте существующий шаблон при необходимости, выполнив команду:

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

где:

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

Пример редактирования шаблона уведомления:

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

- Для создания нового шаблона уведомлений выполните команду:

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

где:

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

- Пример создания нового шаблона уведомлений:

```
./email_config.sh -new "1 час" "Истекает через час" 3600000 INACTIVE
INSERT 0 1
id |      template_name      |      subject      |      interval      |      status
---+-----+-----+-----+-----+-----
 1 | 30 дней                | Срок истекает через 30 дней. | 2592000000 | ACTIVE
 2 | 7 дней                 | Срок истекает через 7 дней. | 604800000 | ACTIVE
 3 | 1 день                 | Срок истекает через 1 день. | 86400000 | ACTIVE
 4 | 1 час                  | Истекает через час          | 3600000 | INACTIVE
(4 строки)
```

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

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

7.5.3 Настройка параметров почтового ящика пользователя

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

7.5.3.1 Настройка почтовой программы Яндекс.Почта

- Настройка почтовой программы показана на примере настройки Яндекс.Почта (см. Рисунок 78).

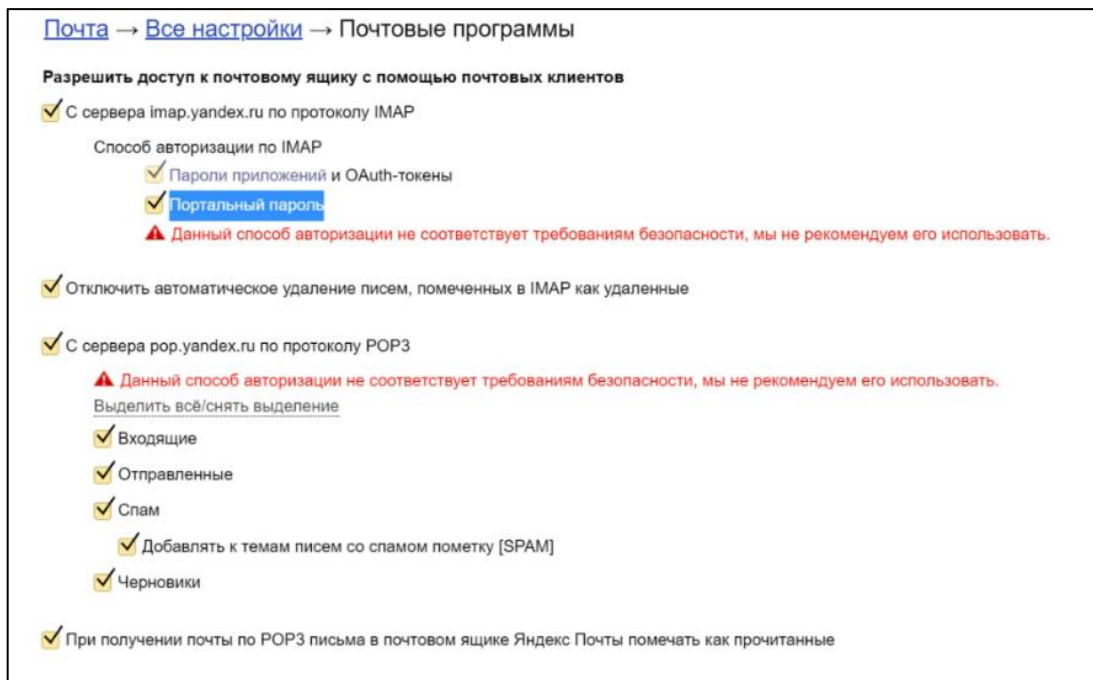
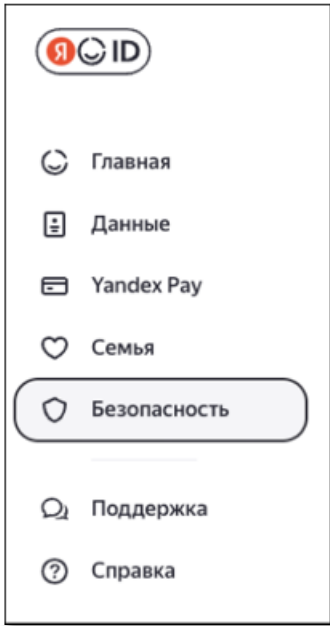
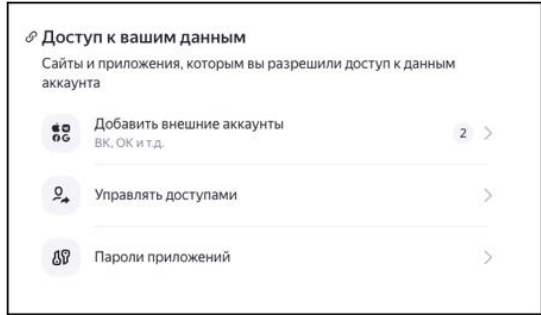


Рисунок 78 – Настройки почтового ящика Яндекс.Почта для получения уведомления об истечении срока сертификата

<p>1 • В настройках аккаунта Яндекс.Почты выберете пункт меню «Безопасность» (см. Рисунок 182).</p>  <p>Рисунок 79 – Раздел «Безопасность» аккаунта почтового ящика Yandex</p>	<p>2 • Перейдите в раздел «Доступ к вашим данным» (см. Рисунок 80).</p>  <p>Рисунок 80 – Подраздел «Доступ к вашим данным» аккаунта почтового ящика Yandex</p>
<p>3 • Перейдите в подраздел «Пароли приложений» (см. Рисунок 81)</p>	<p>4 • Перейдите в подраздел «Почта», «Создать пароль приложения» (см. Рисунок 82)</p>

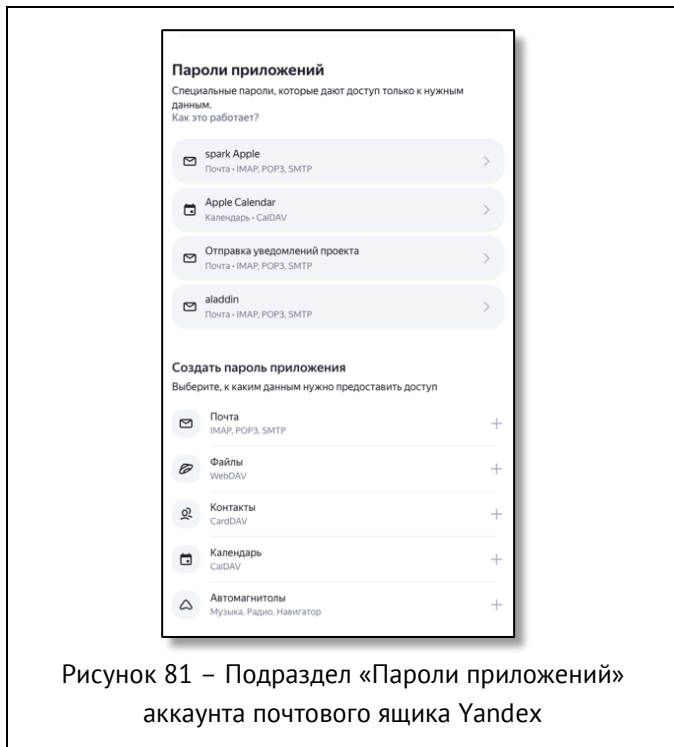


Рисунок 81 – Подраздел «Пароли приложений» аккаунта почтового ящика Yandex

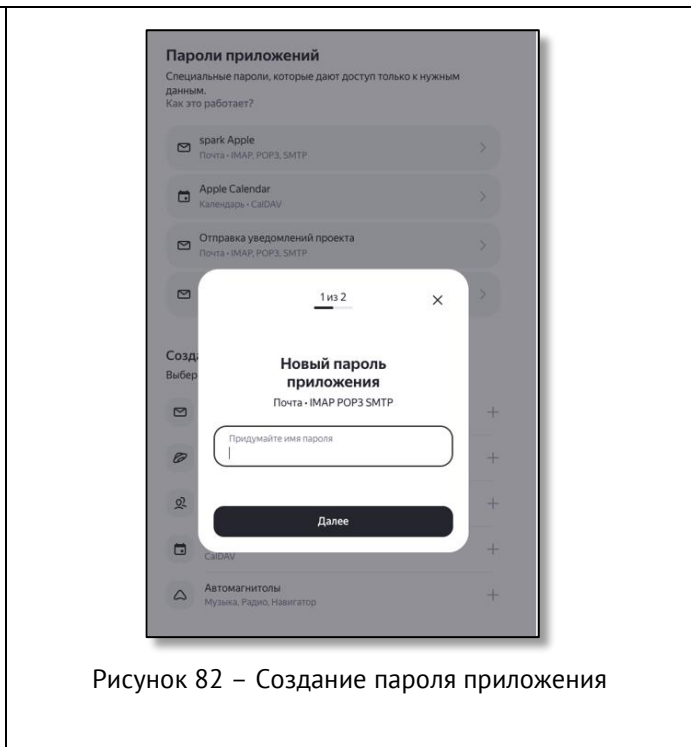


Рисунок 82 – Создание пароля приложения

5 Новый пароль необходимо сохранить. При потере восстановление невозможно. Возможен сброс и создание нового.

6 Данный пароль необходимо внести в конфигурационный файл `config.sh` в параметр `email_password`

7.5.3.2 Настройка почтовой программы MS Exchange

- Настройка почтовой программы показана на примере настройки MS Exchange (см. Рисунок 83). Убедитесь, что настроен протокол SMTP в настройках MS Exchange.

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

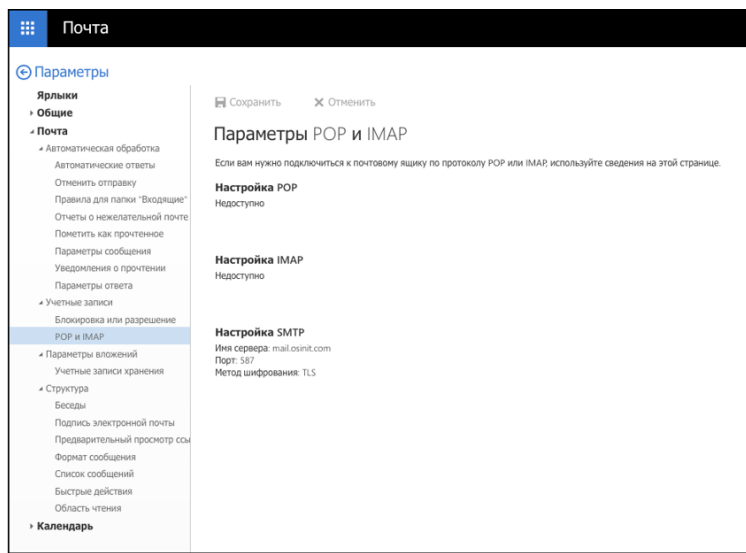


Рисунок 83 – Настройки почтового ящика MS Exchange для получения уведомления об истечении срока сертификата

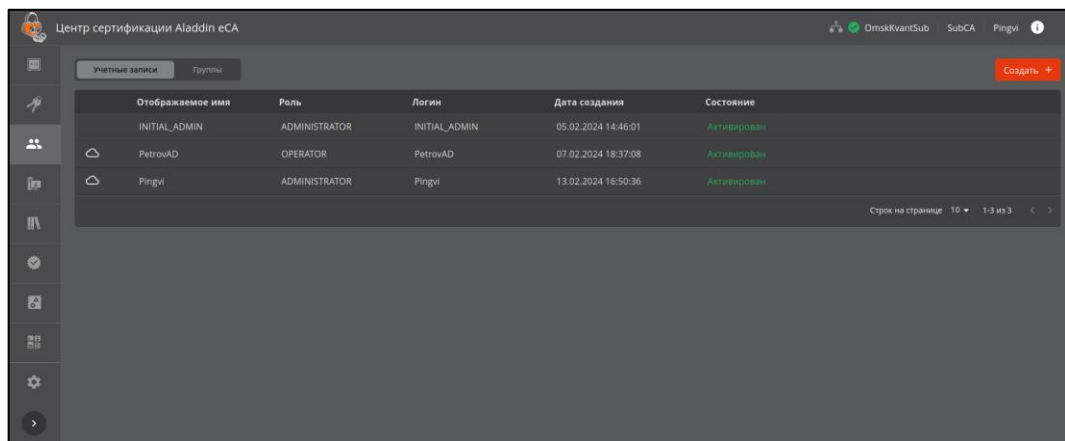
7.6 Раздел «Учётные записи»

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

Переход к разделу «Учётные записи» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 38).


7.6.1 Вкладка «Учётные записи»

На экране раздела «Учётные записи» отображены следующие поля (см. Рисунок 84):



Отображаемое имя	Роль	Логин	Дата создания	Состояние
INITIAL_ADMIN	ADMINISTRATOR	INITIAL_ADMIN	05.02.2024 14:46:01	Активирован
PetrovAD	OPERATOR	PetrovAD	07.02.2024 18:37:08	Активирован
Pingvi	ADMINISTRATOR	Pingvi	13.02.2024 16:50:36	Активирован

Рисунок 84 – 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 AeCA CE:
 - «Сертификаты», где сертификаты могут быть выпущены только по шаблону и с выбором субъекта из локальной системы, формируемой ранее выпущенными сертификатами для новых пользователей.
 - «Субъекты», где сертификаты могут быть выпущены только по шаблону и с выбором субъекта из ресурсной системы. Доступ к группам ресурсной системы определяется администратором при редактировании учётной записи оператора.
 - «Ресурсные системы», где доступны запуск синхронизации субъектов ресурсной системы и выпуск сертификатов только для субъектов, права на которые были предоставлены администратором.
 - Администратор – обладает неограниченными возможностями, в том числе имеет доступ к управлению учетными записями и может делегировать полномочия Оператору на работу с определёнными группами субъектов;

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

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

7.6.1.1 Создание учётной записи пользователя локального ресурса

- По нажатию кнопки <Создать +> на главном экране раздела «Учётные записи» происходит запуск сценария создания учетной записи (см. Рисунок 84).
- В открывшемся окне заполните следующие поля (см. Рисунок 85):
 - выберите роль создаваемой учётной записи – администратор или оператор;
 - отображаемое имя – параметр учетной записи, отображаемый на верхней панели Центра сертификации после авторизации;
 - логин – данные для поля сертификата «Common Name».

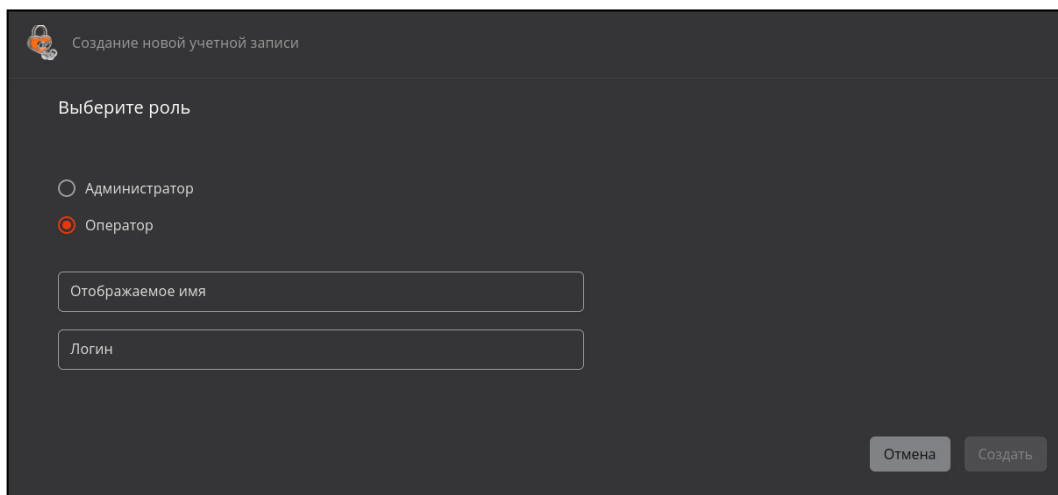


Рисунок 85 – Окно создания новой учётной записи локального пользователя

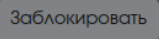
- Нажмите ставшую активной кнопку <Создать>. В результате успешного создания новой учётной записи будет выведено соответствующее уведомление на экран.
- Для созданной учетной записи Оператора произведите настройку прав доступа к группам и объектам ресурсной системы согласно пункту 7.6.1.5 настоящего руководства.
- Для созданной учетной записи Администратора настройка прав не требуется, так как ограничений для этой роли не будет.

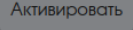
7.6.1.2 Создание учетной записи для подключенного субъекта

Для создания учётной записи доменного пользователя перейдите в раздел «Субъекты» Центра сертификации и создайте учётную запись в соответствии с п. 7.7.8 настоящего руководства.

7.6.1.3 Изменение статуса учётной записи

При наведении курсора на строку добавленной учётной записи появляется возможность управления статусом текущей учётной записи (см. Рисунок 86):

- по нажатию кнопки <Заблокировать>  возможно приостановить действие активной выбранной учётной записи или

- по нажатию кнопки <Активировать>  действие заблокированной ранее учётной записи будет возобновлено.

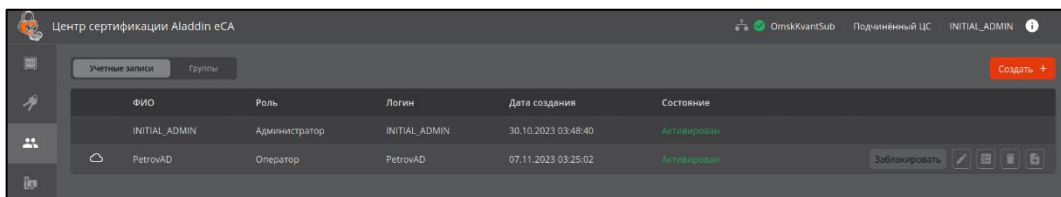



Рисунок 86 – Доступные действия над учетными записями

7.6.1.4 Редактирование учётной записи

- По нажатию на кнопку <Редактировать>  (в строке учётной записи) открывается карточка учётной записи, содержащая следующие поля (см. Рисунок 87):
 - редактируемый выбор назначенной роли;
 - редактируемое отображаемое имя (ФИО);
 - редактируемый статус связанного сертификата (доступные действия приведены в Таблица 7);
 - кнопку для скачивания сертификат в формате .pem.
- Переход в карточку связанного сертификата возможен по двойному нажатию на строку выбранного сертификата в карточке учётной записи.

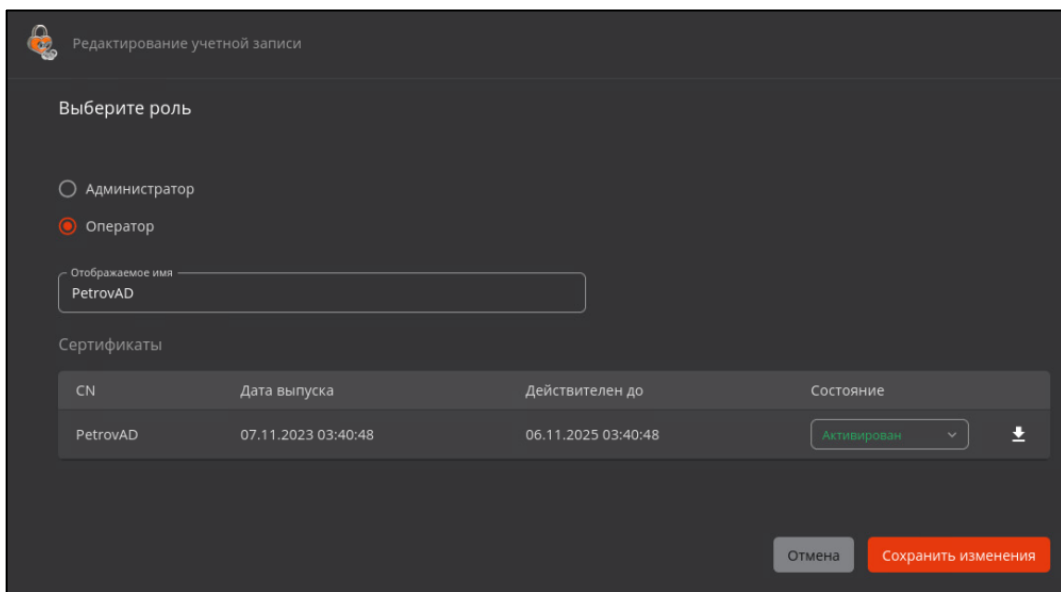



Рисунок 87 – Окно редактирование учётной записи

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

7.6.1.5 Назначение прав оператору

- По нажатию на кнопку <Права>  (в строке учётной записи) открывается окно назначения прав оператору (см. Рисунок 88). Администратор назначает для субъектов, каких ресурсных систем, их организационных групп и групп безопасности возможны операции, обусловленные назначенной ролью. Доступ производится путем проставления чекбоксов группы или выбранного субъекта/группы субъектов и дальнейшим нажатии кнопки <Применить>.

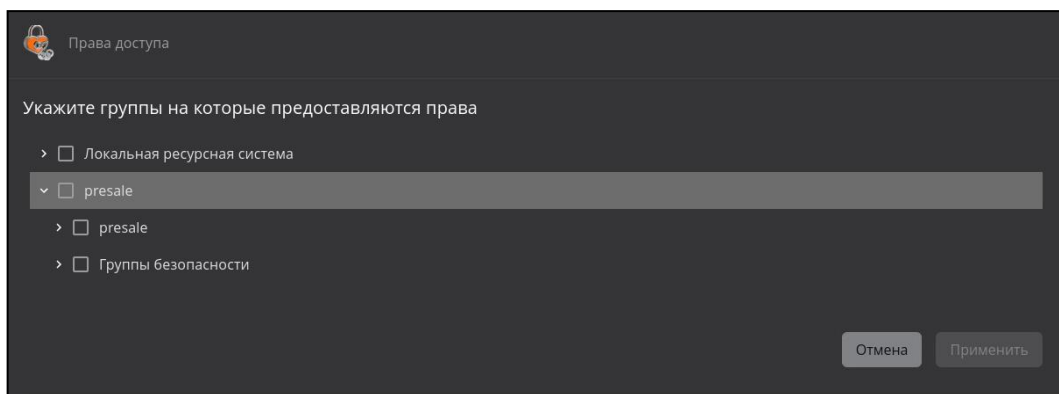



Рисунок 88 – Окно назначения прав учётной записи Оператора

7.6.1.6 Удаление учётной записи

- По нажатию на кнопку <Удалить>  (в строке учётной записи) открывается окно подтверждения удаления учётной записи (см. Рисунок 89)

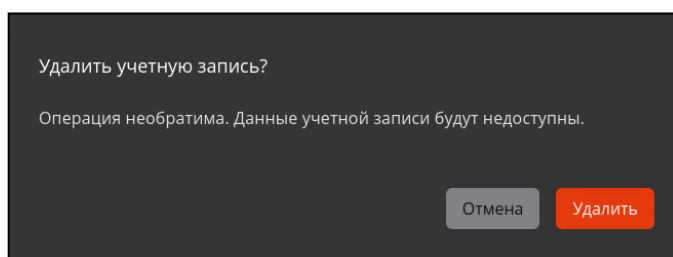



Рисунок 89 – Окно подтверждения удаления учётной записи

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

7.6.1.7 Выпуск сертификата для учетной записи

- По нажатию на кнопку <Создать сертификат>  (в строке учётной записи) в выпадающем меню выберите способ выпуска (см. Рисунок 90):
 - с закрытым ключом;
 - на ключевом носителе.
- Сертификат будет создан с использованием внутреннего шаблона ECA-Auth. Значение поля «Common Name», будет заполнено автоматически и соответствовать логину учетной записи, для которой выпускается сертификат.
- Более подробно процедура выпуска сертификата приведена в «Приложение 1. Создание сертификата для субъекта».

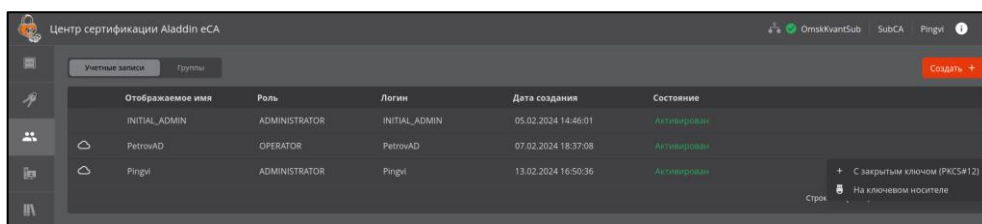


Рисунок 90 – Раздел «Учетные записи». Кнопка выпуска сертификата

7.6.2 Вкладка «Группы»

На данной вкладке возможно назначение прав, определяющих роль оператора, сразу нескольким пользователям, находящимся в одной группе безопасности или подразделении (OU) внешней ресурсной системы.

7.6.2.1 Добавление группы пользователей с ролью «Оператор»

- Нажмите кнопку <Добавить группы +> на вкладке «Группы» (см. Рисунок 91).

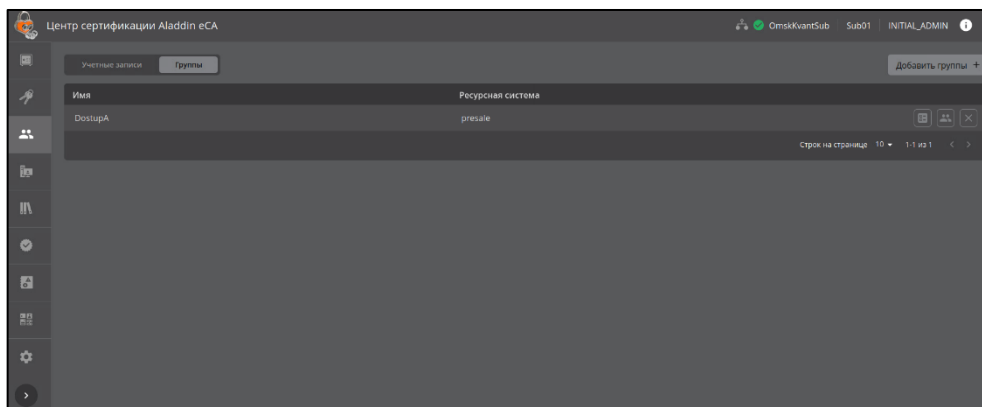


Рисунок 91 – Окно вкладки «Группы»

- В открывшемся окне (см. Рисунок 92) отображается иерархическое дерево групп безопасности ресурсных систем. Выберите в окне:
 - ресурсную систему;
 - в раскрывшемся списке – группы безопасности, субъектам которых будет назначена роль «Оператор». В левом нижнем углу окна показано сколько групп выбрано в данный момент.
- Подтвердите выбор, нажав кнопку <Добавить>.

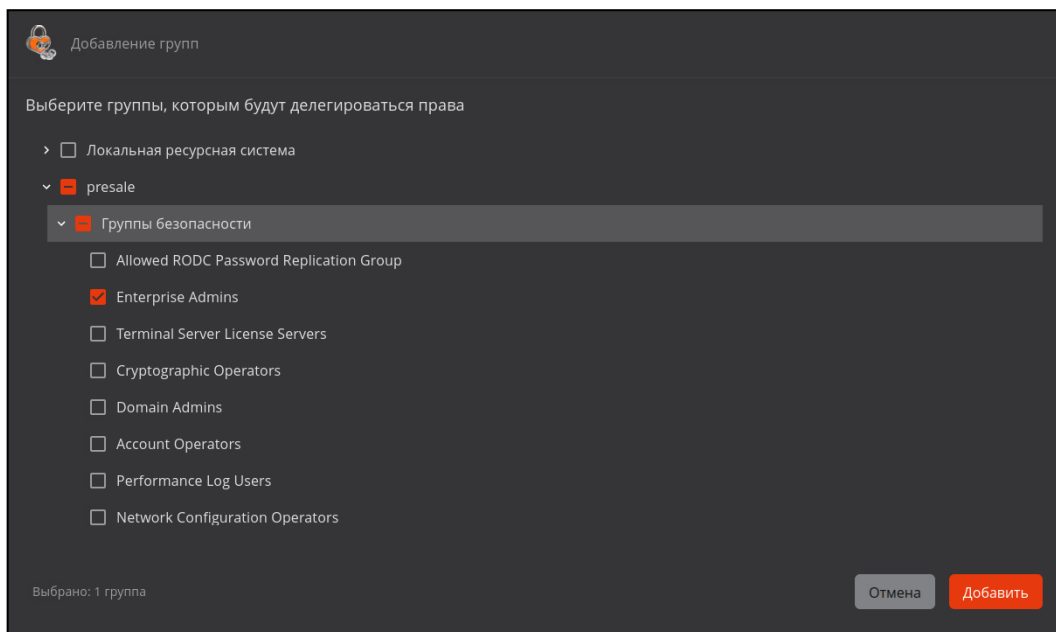



Рисунок 92 – Окно добавления групп

- В результате на экранной форме вкладки «Группы» будут добавлены выбранные группы безопасности и будет отображена информация (см. Рисунок 91):
 - в столбце «Имя» – название выбранной группы безопасности;
 - в столбце «Ресурсная система» – тип ресурсной системы, которой принадлежат выбранные группы безопасности.

- Ранее добавленные группы безопасности при следующем добавлении групп безопасности по нажатию кнопки <Добавить группы +> не будут отображены в иерархическом дереве групп безопасности ресурсных систем.

7.6.2.2 Назначение прав участникам групп

Для настройки прав доступа необходимо:

- выделить в экранной форме добавленную группу, для которой необходимо настроить права доступа;
- нажать на появившуюся кнопку  <Назначить права>;
- в окне предоставления прав доступа в иерархии групп ресурсной системы выбрать организационные группы и/или группы безопасности, на которые будут назначены права доступа. (см. Рисунок 93);
- подтвердить выбор, нажав кнопку <Применить>.

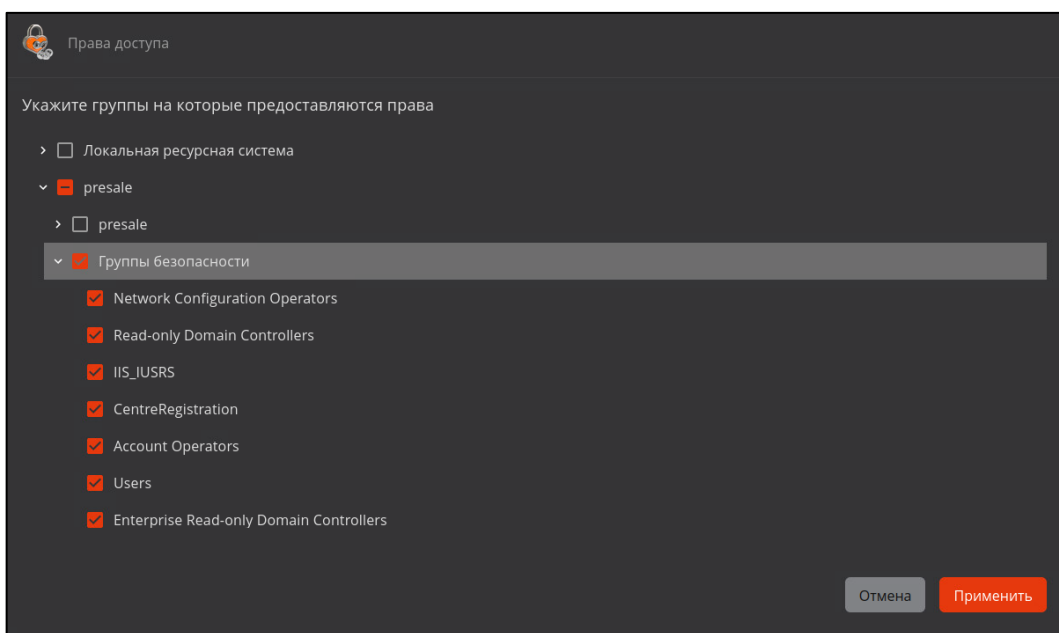



Рисунок 93 – Окно предоставления прав доступа для группы

7.6.2.3 Просмотр участников группы

Для просмотра состава группы безопасности:

- выделите в экранной форме добавленную группу, учётные записи которой необходимо просмотреть;
- нажмите на появившуюся кнопку  <Учётные записи>;
- в открывшемся окне будут отображены все учётные записи, созданные для участников выбранной группы.

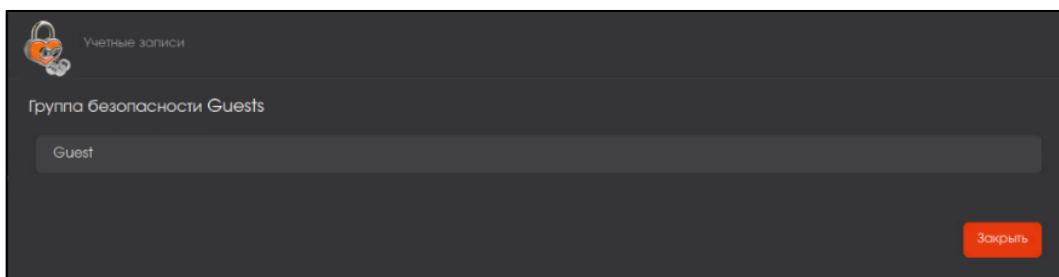



Рисунок 94 – Окно учётных записей, созданных для группы безопасности

7.6.2.4 Удаление группы

Для удаления всех учётных записей выбранной группы безопасности:

- выделите в экранной форме добавленную группу, которую необходимо удалить;
- нажмите на появившуюся кнопку  <Убрать из списка>. Удаление выбранной группы происходит без подтверждения.

7.7 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 38).

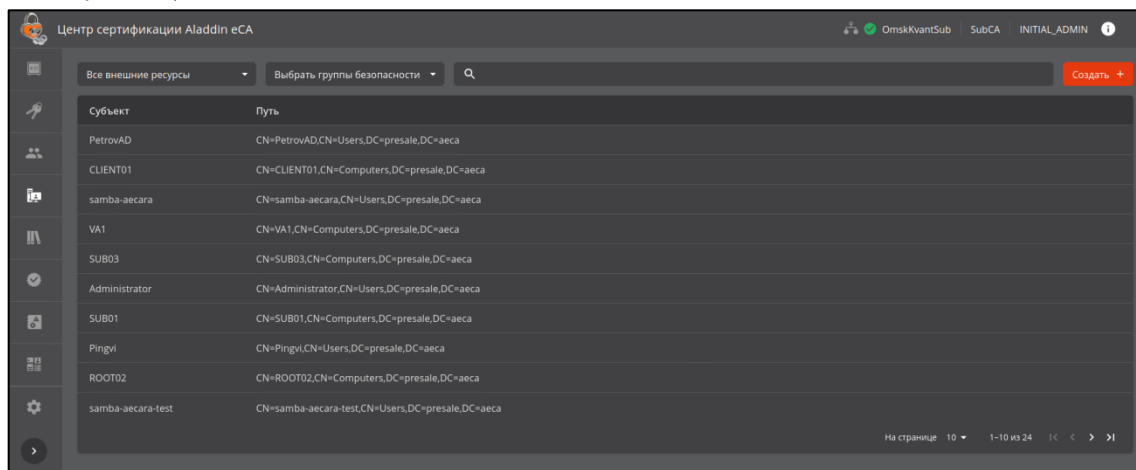


Рисунок 95 – Экран раздела «Субъекты»

- Список субъектов на экране раздела отображается в виде таблицы с пагинацией и сортировкой по заголовку табличного поля экранной формы.
- На экране раздела «Субъекты» отображены информационные элементы (табличные поля):
 - субъект – полное имя субъекта;
 - путь, состоящий из компонентов: отличительного имени субъекта (например, CN=Puma), контейнера отличительного имени (например, CN=Users, DC=presale, DC=aeca), состоящего из организационной группы (например, CN=Users) и доменных компонентов (полного DNS-имени) (например, DC=presale, DC=aeca).
- В разделе «Субъекты» доступны следующие действия:
 - просмотр субъектов подключенных ресурсных систем с выбором группы безопасности;
 - просмотр субъектов локальной ресурсной системы;
 - поиск субъекта;
 - создание нового субъекта локальной ресурсной системы;
 - редактирование значения атрибутов субъекта локальной ресурсной системы;
 - просмотр карточки субъекта;

- просмотр списка сертификатов, выпущенных Центром сертификации для субъекта;
 - управление статусом сертификатов, выпущенных Центром сертификации для субъекта;
 - публикация сертификата субъекта в ресурсную систему;
 - экспорт сертификата субъекта;
 - создание сертификата для субъекта;
 - создание учётной записи для субъекта.
- Идентификация локальных и подключенных субъектов в Центре сертификации осуществляется по атрибуту **UUID**.

7.7.1 Просмотр субъектов ресурсных систем

- Просмотр субъектов осуществляется посредством выбора источника:
 - все внешние ресурсы – подключенные службы каталогов;
 - локальный ресурс – появляется в случае, если в локальной базе данных Центра сертификации присутствует хотя бы один субъект;
 - внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.
- В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 96):
 - поле «ресурсная система», по нажатию на которое в выпадающем меню выберите локальную ресурсную систему, подключенный ресурс или все внешние ресурсы для отображения всех субъектов внешних ресурсных систем;
 - поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в выпадающем меню выберите необходимую группу. В случае если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. Для локального ресурса группы безопасности отсутствуют. В списке «Выбрать группу безопасности» отображаются только те группы безопасности, которые содержат один или более субъектов. Группы безопасности, не имеющие членов, не будут показаны в списке и не доступны для выбора.

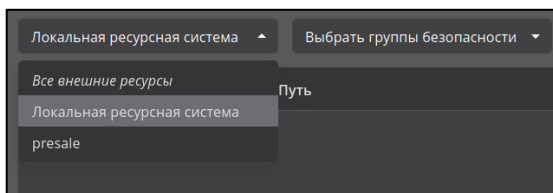


Рисунок 96 – Верхняя панель экранной формы вкладки «Субъекты»


7.7.2 Поиск субъектов

- В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 97):
 - в поле поиска осуществляется поиск субъектов по компонентам SubjectDN и SubjectAltName в выбранной ресурсной системе. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры. Для сброса поиска и отображения всех субъектов выбранной ресурсной системы очистите строку поиска.



Рисунок 97 – Поле поиска субъектов

7.7.3 Сортировка субъектов

- Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 98):
 - «Субъект» – сортировка осуществляется в алфавитном порядке;
 - «Путь» – сортировка осуществляется в алфавитном порядке содержимого атрибута Common Name.
- 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.

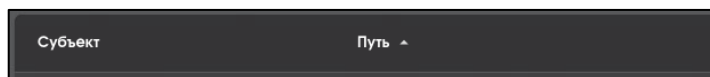
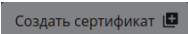
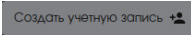


Рисунок 98 – Поля сортировки содержимого экрана раздела «Субъекты»

7.7.4 Карточка субъекта

- Просмотр данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 100) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 95).
- Карточка субъекта включает в себя следующие информационные поля:
 - сведения о субъекте:
 - из какой ресурсной системы получен субъект;
 - статус пользователя в ресурсной системе;
 - идентификатор UUID;
 - атрибуты SAN и SDN (см. Таблица 10);
 - сведения обо всех сертификатах субъекта, ранее выпущенных Центром сертификации:
 - серийный номер;
 - Common Name владельца сертификата;
 - шаблон;
 - дата создания;
 - дата окончания действия;
 - дата публикации в ресурсную систему;
 - состояние сертификата.
- Доступные действия в карточке субъекта:
 - создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку «Создать сертификат»  (см. п. 7.7.7, 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 99);

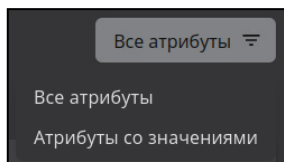




Рисунок 99 – Фильтрация отображаемых атрибутов в карточке субъекта

- 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 Таблица 7 в поле сертификата «Состояние»;
- редактировать значения в полях атрибутов (только для локальных субъектов).

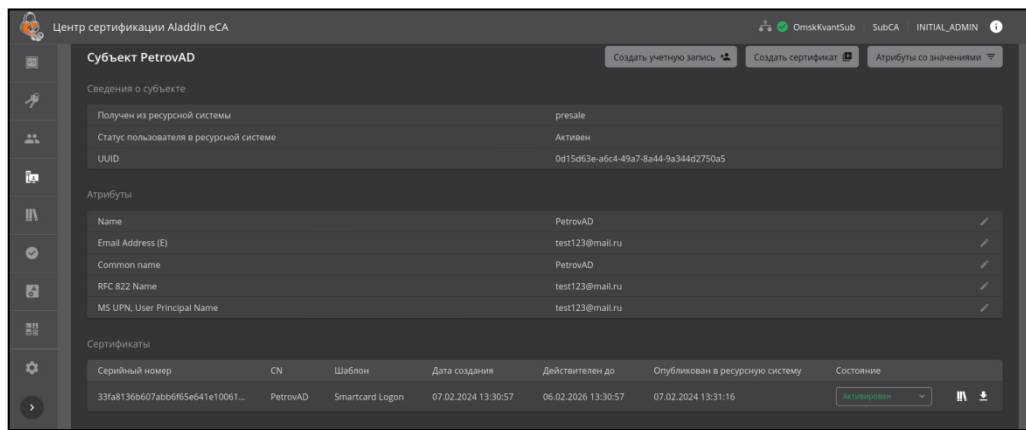


Рисунок 100 – Окно просмотра карточки подключенного субъекта (включено отображение «Атрибуты со значениями»)


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

Таблица 10 – Атрибуты субъекта

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

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
	Локальный субъект (false)	"isConnected": false	Отображение субъекта в списке субъектов локальной ресурсной системы.
Флаг блокировки в PC	Для подключенных к PC субъектов: субъект заблокирован в PC (true) или субъект не заблокирован в PC (false)	"isBlocked"	Поле «Статус в ресурсной системе» в карточке субъекта. Для локальных субъектов всегда отображается символ «-».
	Для локальных субъектов: всегда false		
UUID	string(\$uuid)	"id"	Поле «UUID» карточки субъекта
Расположение субъекта в структуре 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"	-
Атрибуты SDN			
Common name	Список строк	"CN"	Поле «Common name» в карточке субъекта
Unique Identifier (UID)	Список строк	"UID"	Поле «Unique Identifier (UID)» в карточке субъекта
Email Address (E)	Список строк	"E"	Поле «Email Address (E)» в карточке субъекта
Email Address (Mail)	Список строк	"EMAILADDRESS"	Поле «Email Address (Mail)» в карточке субъекта
Mail	Список строк	"MAIL"	Поле «Mail» в карточке субъекта
Serial number	Список строк	"SN"	Поле «Serial number» в карточке субъекта
Given name	Список строк	"GIVENNAME"	Поле «Given name» в карточке субъекта
Initials	Список строк	"INITIALS"	Поле «Initials» в карточке субъекта
Surname	Список строк	"SURNAME"	Поле «Surname» в карточке субъекта
Organizational unit	Список строк	"OU"	Поле «Organizational unit» в карточке субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
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 «Postalcode» в карточке субъекта
Business category	Список строк	"BUSINESSCATEGORY"	Поле «Business category» в карточке субъекта
Telephone number	Список строк	"TELEPHONENUMBER"	Поле «Telephone number» в карточке субъекта
Pseudonym	Список строк	"PSEUDONYM"	Поле «Pseudonym» в карточке субъекта
Postal address	Список строк	"POSTALADDRESS"	Поле «Postal address» в карточке субъекта
Street	Список строк	"STREET"	Поле «Street» в карточке субъекта
Name	Список строк	"NAME"	Поле «Name» в карточке субъекта
Title	Список строк	"T"	Поле «Title» в карточке субъекта
Domain Qualifier	Список строк	"DN"	Поле «Domain Qualifier» в карточке субъекта
Description	Список строк	"DESCRIPTION"	Поле «Description» в карточке субъекта
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

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


7.7.4.1 Редактирование атрибутов субъекта

- Для субъектов локальной ресурсной системы доступно редактирование всех атрибутов SDN и SAN.
- Для субъектов подключенной ресурсной системы редактирование атрибутов SDN или SAN, значения которых получены Центром сертификации из ресурсной системы, недоступно. Все остальные атрибуты SDN или SAN доступны для редактирования.
 - Для субъектов любой ресурсной системы редактирование сведений о субъектах в их карточках (поля «Получен из ресурсной системы», «Статус в ресурсной системе», «UUID») недоступны для редактирования.
 - При вводе/редактировании значений атрибутов, указанных в Таблица 11, осуществляется валидация. Для всех остальных атрибутов субъекта валидация отсутствует.

Таблица 11 – Допустимые значения атрибутов

Атрибут	Допустимый формат	Регулярное выражение
Атрибуты SDN		
Common name	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., _ , @, (,), пробел	$^[\backslashs\ -A-Яa-яA-Za-z0-9\._\@(\)+\$$
Organization	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., _ , @, (,), пробел	$^[\backslashs\ -A-Яa-яA-Za-z0-9\._\@(\)+\$$
Атрибуты SAN		
MS GUID, Globally Unique Identifier	Длина строки равна 32 символа; Только указанные символы: А-F, а-f, 0-9	$^[A-Fa-f0-9]{32}\$$

Атрибут	Допустимый формат	Регулярное выражение
RFC 822 NAME	Строка вида "text@text" и только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., @, _ , -	$^[_A-Яа-яА-Zа-z0-9\.\@_-\]+\$$
MS UPN, UserPrincipalName	Строка вида "text@text" и только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., @, _ , -	$^[_\A-Яа-яА-Zа-z0-9\._]+\@[_A-Яа-яА-Zа-z0-9\._]+\$$
DNS Name	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., -, *	$^[_A-Яа-яА-Zа-z0-9\.*_-\]+\$$
Kerberos KPN, Kerberos 5 Principal	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., @, /, _ , -	$^[_\A-Яа-яА-Zа-z0-9\._]+\@[_A-Яа-яА-Zа-z0-9\._]+\$$

- 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 101). При необходимости добавьте значение атрибута (будет указано в поле атрибута через запятую), нажав кнопку <Добавить значение+>. Нажмите ставшую активной кнопку <Сохранить> для сохранения результата или нажмите кнопку <Заккрыть> для выхода из режима редактирования значения атрибута без сохранения изменений.

- При синхронизации отредактированное поле атрибута будет заменено значением соответствующего атрибута субъекта синхронизированной ресурсной системы, если оно заполнено для этого доменного субъекта в ресурсной системе!

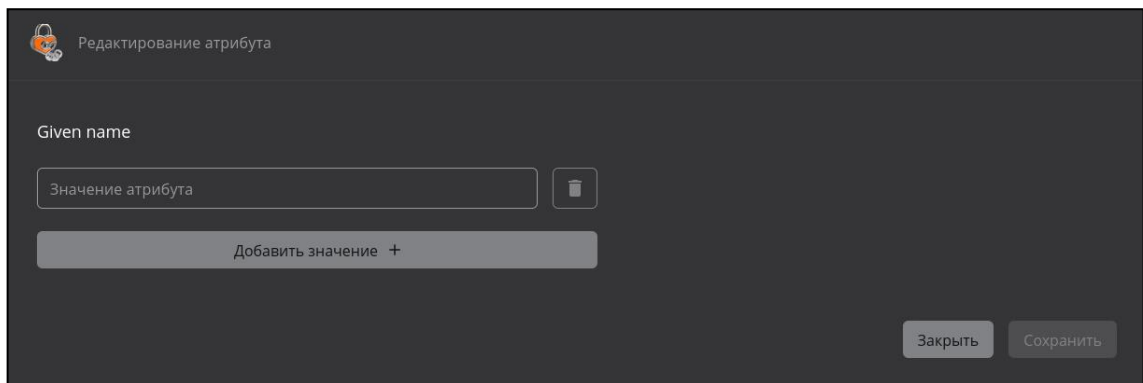


Рисунок 101 – Окно редактирования значения атрибута в карточке субъекта

7.7.5 Субъекты локальной ресурсной системы

- Локальную базу субъектов формируют:
 - субъекты, созданные Администратором путём вызова метода API;
 - субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы), атрибут субъекта «isBlocked» принимает значение «false». В случае повторного подключения ресурсной системы связи субъектов с группами будут восстановлены, обновлены атрибуты в соответствии с данными из ресурсной системы;
 - субъекты, загруженные в базу данных Aladdin eCA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false»;
 - субъект web-сервера, автоматически созданный при развёртывании Центр сертификации, с параметрами, указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:

- параметр `hostname` задаёт значение атрибутов «Common name» и «DNS Name» локального субъекта;
 - параметры `initial_server_key_algorithm` и `initial_server_key_bits` задают значения криптографических параметров сертификата web-сервера;
 - параметр `initial_server_password` задаёт значение пароля контейнера сертификата web-сервера.
- Локальный субъект отключенной ресурсной системы при подключении ресурсной системы, где существует данный субъект, будет перенесён из базы локальной ресурсной системы (атрибут субъекта «isConnected» примет значение «true»). При этом будет выполнено обновление атрибутов субъекта в соответствии с его атрибутами из ресурсной системы (см. Таблица 13 – Преобразование данных субъектов ресурсной системы), остальные текущие атрибуты (то есть те, которые не были получены из ресурсной системы) не изменятся.
 - Проверка субъектов осуществляется по атрибуту «id».

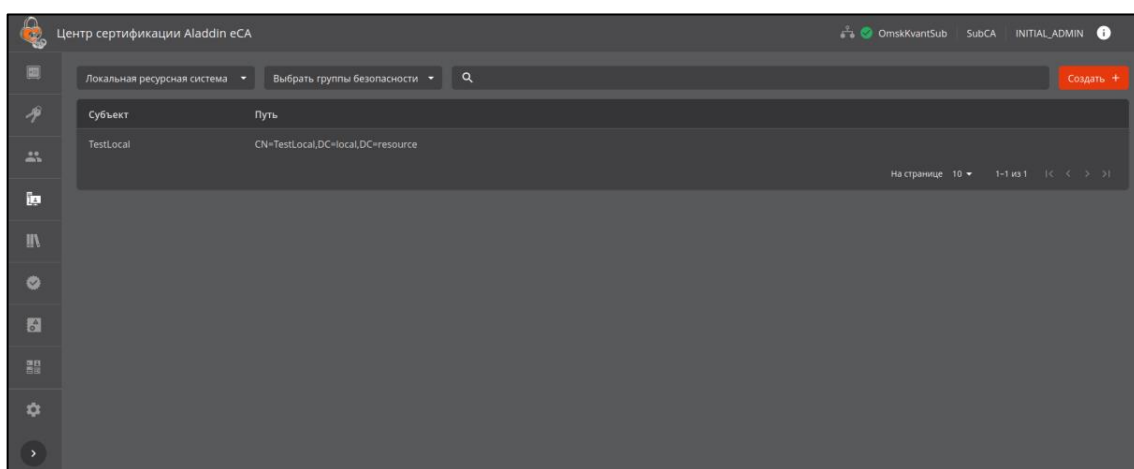


Рисунок 102 – Экран раздела меню «Субъекты». Локальный ресурс

7.7.5.1 Создание нового субъекта локальной ресурсной системы

- Доступно только пользователю с ролью «Администратор».
- Для создания нового локального субъекта нажмите кнопку «Создать» (см. Рисунок 102), в открывшемся окне (см. Рисунок 103) введите имя создаваемого субъекта (CN), добавьте необходимые атрибуты, нажав в окне создания субъекта кнопку «Добавить атрибут+», при необходимости прокрутив список всех возможных атрибутов SDN и SAN вниз и выбрав атрибут.

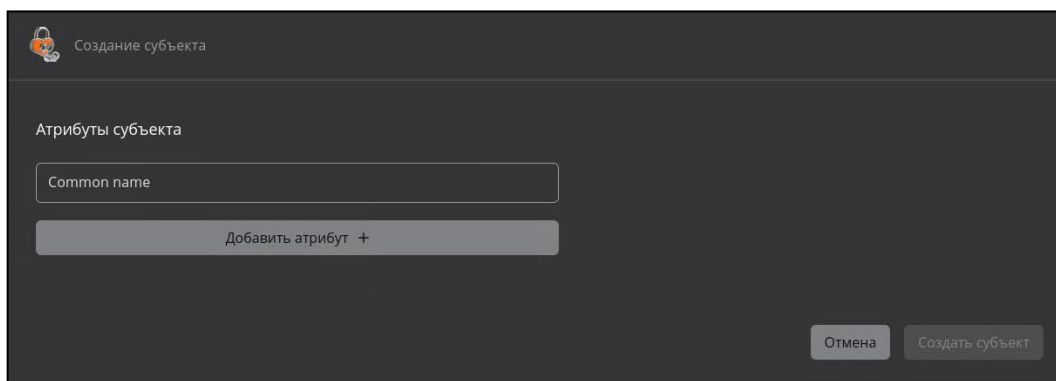



Рисунок 103 – Создание субъекта

- Полный список доступных атрибутов приведён в Таблица 10.

- Далее необходимо указать значения в полях выбранных атрибутов или удалить атрибут, нажав кнопку <Удалить> . При отсутствии значения в поле «Common name» или несоответствии введенного значения допустимому формату создание субъекта запрещено.
- После корректного заполнения всех выбранных полей атрибутов будет доступно создание субъекта по нажатию на кнопку <Создать субъект> (см. Рисунок 104).

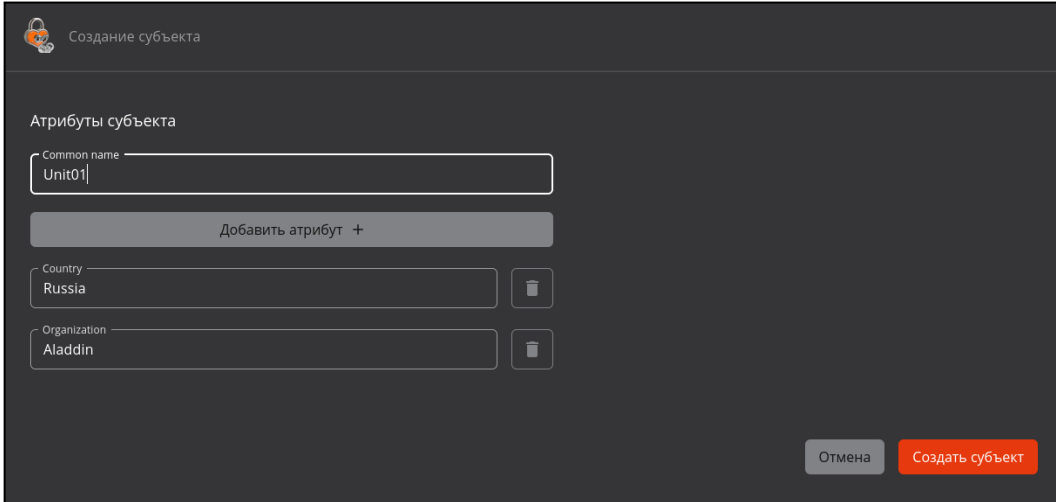


Рисунок 104 – Создание субъекта. Заполнение полей

- При создании локального субъекта Центр сертификации автоматически назначает новому субъекту идентификатор (UUID), если он не был передан во входном параметре «MS_GUID». Идентификатор (UUID) – уникальный, создание субъекта с существующим UUID в Центра сертификации недоступно.
- В случае неудачной попытки создания нового субъекта администратор будет уведомлен сообщением (см. Таблица 12).

Таблица 12 – Перечень сообщений в случае неудачной попытки создания нового субъекта

Текст ошибки	Причина
Используйте корректный формат	Ввод значения атрибута, не соответствующего допустимому формату
Ошибка. Субъект с указанным MS GUID уже существует	При указании для атрибута «MS GUID, Globally Unique Identifier» значения, соответствующего идентификатору существующего в Центре сертификации субъекта

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

7.7.6 Субъекты внешнего ресурса

- Внешний (подключенный) ресурс формируется в результате регистрации службы каталогов доменных служб Samba DC, РЕД АДМ, ALD PRO, FreeIPA или MS Active Directory.
- Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система» (см. пункт 7.8.1 настоящего руководства).
- Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в пункте 7.8.2 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 105).

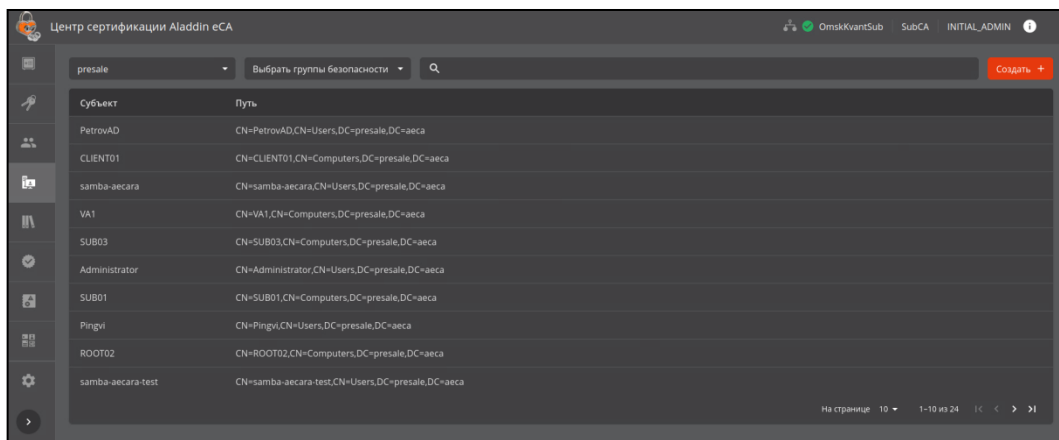


Рисунок 105 – Экран раздела меню «Субъекты». Подключенный ресурс

- Загрузка данных осуществляется из всей ресурсной системы, начиная с точки подключения, указанной в настройках подключения Корневого каталога.
- Для каждого загруженного пользователя и компьютера будет создан субъект и подгружены все поля, относящиеся к SubjectDN и SubjectAltName. Преобразование содержимого записи LDAP в поля базы субъектов ресурсной системы происходит в соответствии с Таблица 13.


Таблица 13 – Преобразование данных субъектов ресурсной системы

Атрибут субъекта Aladdin eCA	Поле в базах Samba DC, MS AD, РЕД АДМ 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

Атрибут субъекта Aladdin eCA	Поле в базах Samba DC, MS AD, РЕД АДМ для типов субъектов		Поле в базах ALD PRO, FreeIPA для типов субъектов		
	Пользователь	Компьютер	Пользователь	Компьютер	Сервис
	userPrincipalName		krbPrincipalName	krbPrincipalName	
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-

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

7.7.7 Создание сертификата для субъекта ресурсной системы

- Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку  <Выпустить сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 106):
 - с закрытым ключом (см. Приложение 1. Создание сертификата для субъекта);
 - на основании запроса (см. Приложение 1. Создание сертификата для субъекта);
 - на ключевом носителе (см. Приложение 1. Создание сертификата для субъекта).

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

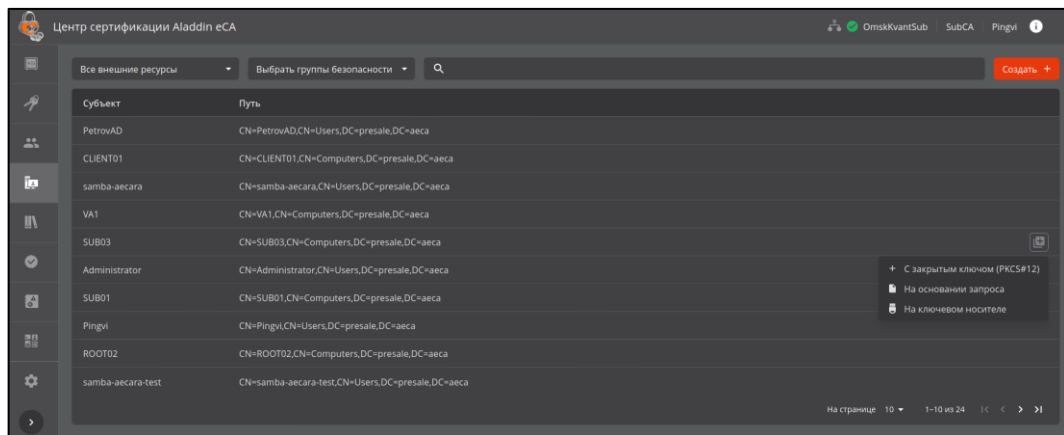


Рисунок 106 - Окно выпуска сертификата для субъекта ресурсной системы

- При выпуске сертификатов для субъектов внешних (подключенных) ресурсных систем возможно публиковать сертификат в формате LDIF в атрибут `userCertification` субъекта ресурсной системы (путём добавления, а не перезаписи атрибута), проставив флаг в чек-боксе «Публиковать сертификат в ресурсную систему» окна выпуска сертификата. По умолчанию флаг выполнения публикации сертификата включен.
- После выбора шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта в соответствии с Таблица 13.
- Если значения атрибутов отсутствуют, то необходимо их ввести в соответствующие поля в карточке субъекта.

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

7.7.8 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 107).

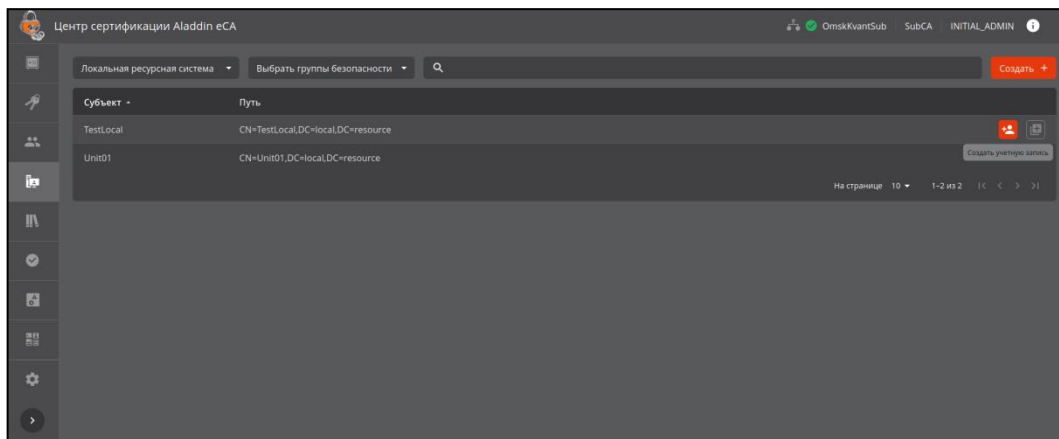


Рисунок 107 – Выбор субъекта для создания учётной записи

- В открывшемся окне создания новой учетной записи (см. Рисунок 108) поле «Отображаемое имя» автоматически заполнено данными атрибута «Common Name» субъекта, но доступно для редактирования, и соответствует полю «ФИО» в разделе «Учётные записи». Поле «Логин» не отображается в окне создания новой учётной записи и заполняется по умолчанию в соответствии со значением атрибута «Common Name» выбранного субъекта.
- Выберите роль, применяемую к создаваемой учетной записи.
- Нажмите кнопку <Создать> для создания учетной записи для субъекта.

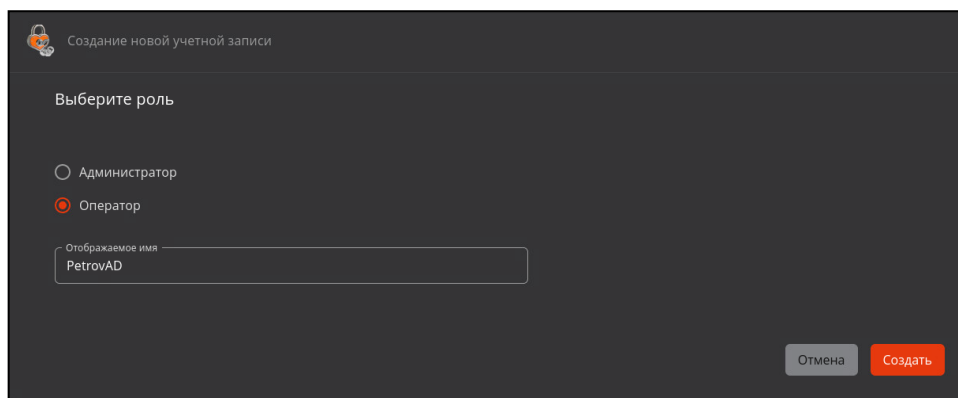


Рисунок 108 – Окно создания новой учётной записи

- Для созданной учетной записи Оператора произведите настройку прав доступа к группам и объектам ресурсной системы в соответствии с пунктом 7.6.1.5 настоящего руководства.
- Если учётная запись для выбранного пользователя существует, то при следующем создании новой учётной записи для этого же субъекта логин пользователя будет иметь префикс «_1».

7.8 Раздел «Ресурсная система»

Раздел «Ресурсная система» обеспечивает получение данных субъектов с целью упрощенного выпуска сертификатов субъектам служб каталогов Linux и Microsoft, а также централизованную публикацию выпущенных сертификатов в карточку субъекта службы каталогов.

Переход в раздел «Ресурсная система» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 38).

- На основном экране «Ресурсной системы» отображены информационные поля (см. Рисунок 109):
 - подключаемая ресурсная система – Samba DC, РЕД АДМ, MS AD, FreeIPA и/или ALD PRO;
 - отображаемое имя – показывает отображаемое имя ресурса;
 - логин – отображается полный параметр учетной записи Администратора домена, имеющего права доступа к домену;
 - последнее обновление – отображается дата и время последней синхронизации базы субъектов источника с базой данных программного компонента;
 - статус – отображается статус подключения к источнику;
 - субъекты – показывает количество загруженных субъектов из источника.

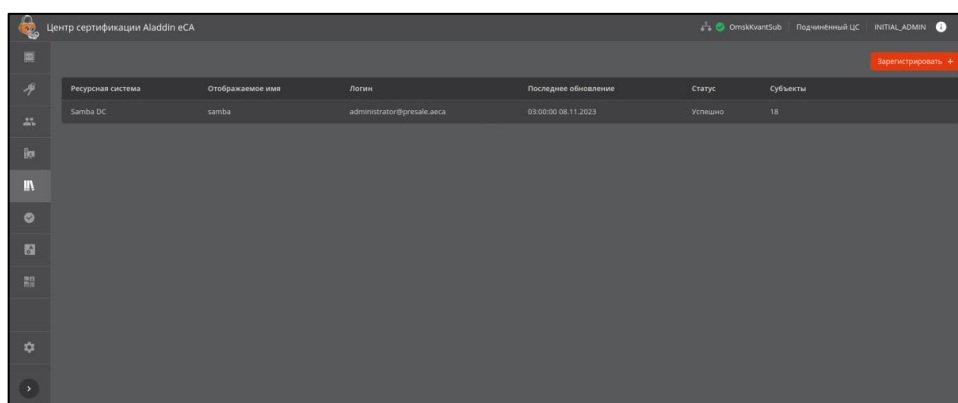


Рисунок 109 – Экран раздела «Ресурсная система»

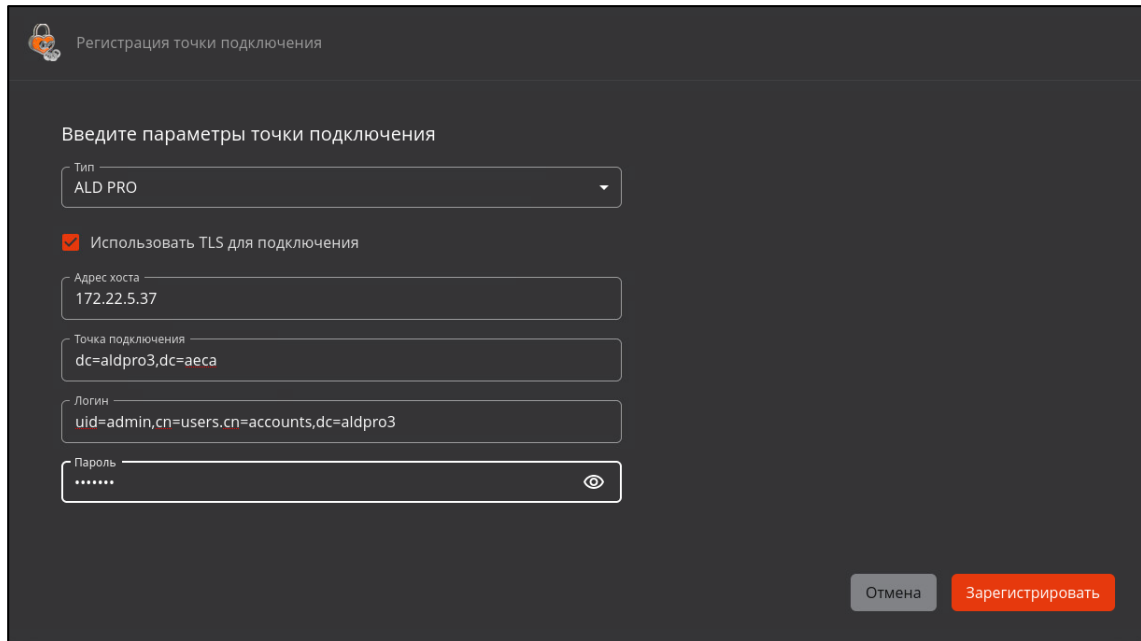
- Центр сертификации Aladdin Enterprise Certificate Authority позволяет загрузить из нескольких ресурсных систем Samba DC, РЕД АДМ, MS AD, FreeIPA или ALD PRO:
 - список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA)), их атрибуты и сертификаты;
 - список и состав организационных групп;
 - список и состав групп безопасности.
- Идентификация загружаемых субъектов ресурсной системы производится по их атрибуту «id».
- Работа с разделом «Ресурсные системы» предусматривает выполнение следующих сценариев использования:
 - регистрация (подключение) ресурсной системы для выпуска сертификатов и учётных записей субъектам служб каталогов;
 - обновление списка субъектов и их данных в ручном и автоматических режимах;
 - удаление зарегистрированной ресурсной системы.

7.8.1 Регистрация ресурсной системы

- По нажатию кнопки <Зарегистрировать +> на главном экране управления «Ресурсной системы» происходит запуск сценария создания ресурсной системы.
- В открывшемся окне заполните следующие поля:
 - тип – выберите тип подключаемой ресурсной системы из выпадающего списка: Samba DC, 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 отмету чек-бокса;
 - отображаемое имя – задайте отображаемое имя ресурса в разделе «Ресурсная система». Отображаемое имя должно начинаться с буквы, может содержать буквы и цифры. Ограничение длины отображаемого имени: не более 255 символов;
 - URL – укажите полное доменное имя или ip-адрес ресурса, к которому выполняется подключение;
 - укажите точку подключения в формате: `DC={первое доменное имя},DC={второе доменное имя}` и т.д.;
 - логин – укажите соответствующий параметр учетной записи администратора контроллера домена. Для Samba DC, РЕД АДМ и MS AD учетная запись администратора вводится в формате RFC822Name, для ALD PRO и FreeIPA соответственно в формате Distinguished Names. Успешное подключение к ресурсной системе ALD PRO или FreeIPA возможно с минимальным набором прав пользователя:
 - наличие роли «Service Role»⁴ 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.
 - пароль – укажите соответствующий параметр учетной записи администратора контроллера домена.
- Пример заполненной формы окон создания ресурсной системы для разных типов источников приведены далее (см. Рисунок 110, Рисунок 111, Рисунок 112, Рисунок 113).
 - Нажмите ставшую активной кнопку <Зарегистрировать>. В результате успешного создания будет выведено соответствующее уведомление на экран.
 - После создания ресурсной системы будут отображены дата и время последней синхронизации, статус подключенной ресурсной системы и количество загруженных субъектов.

⁴ Подключается на КД ALD PRO только через cli командой: `# ipa role-add-member "Service Role" --users=username`



Регистрация точки подключения

Введите параметры точки подключения

Тип
ALD PRO

Использовать TLS для подключения

Адрес хоста
172.22.5.37

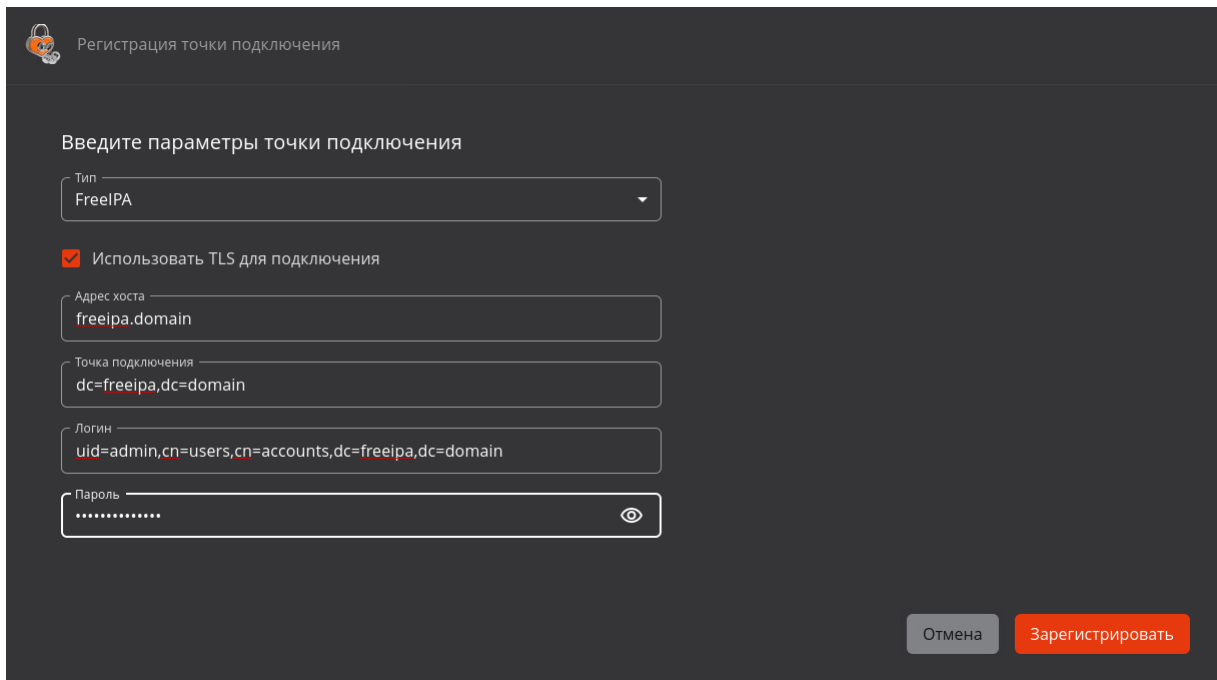
Точка подключения
dc=aldpro3,dc=aeca

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

Пароль
.....

Отмена Зарегистрировать

Рисунок 110 – Пример создания ресурсной системы типа ALD PRO



Регистрация точки подключения

Введите параметры точки подключения

Тип
FreeIPA

Использовать TLS для подключения

Адрес хоста
freeipa.domain

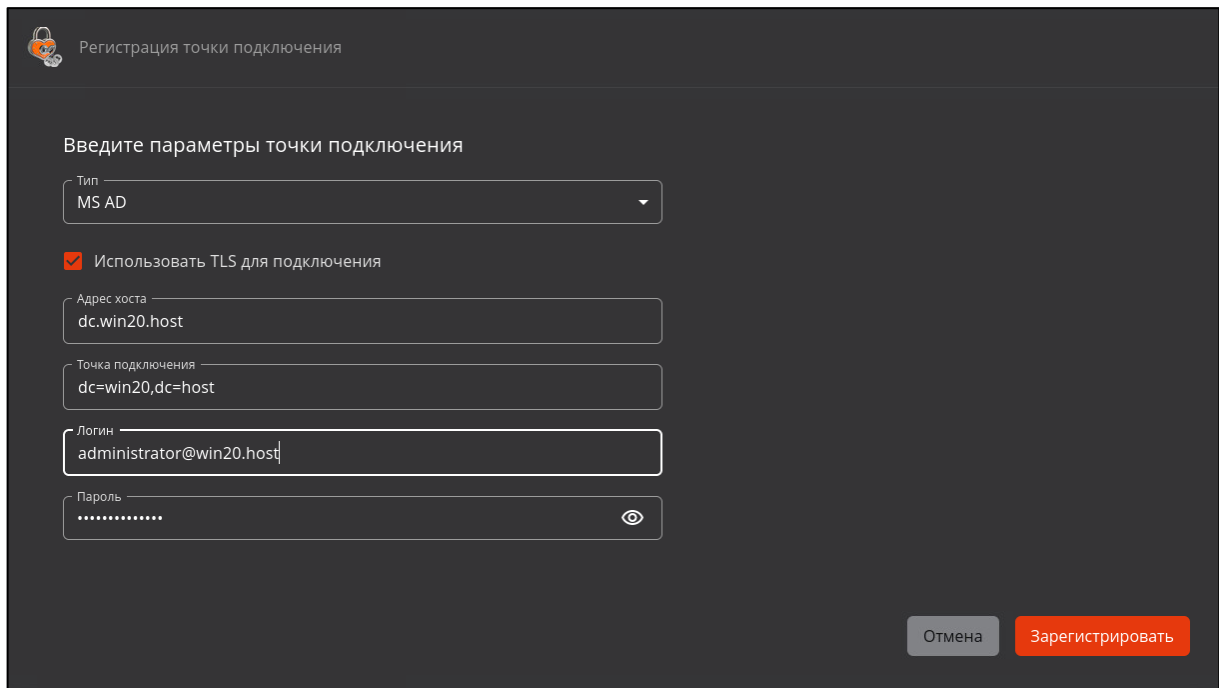
Точка подключения
dc=freeipa,dc=domain

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

Пароль
.....

Отмена Зарегистрировать

Рисунок 111 – Пример создания ресурсной системы типа FreeIPA



Регистрация точки подключения

Введите параметры точки подключения

Тип
MS AD

Использовать TLS для подключения

Адрес хоста
dc.win20.host

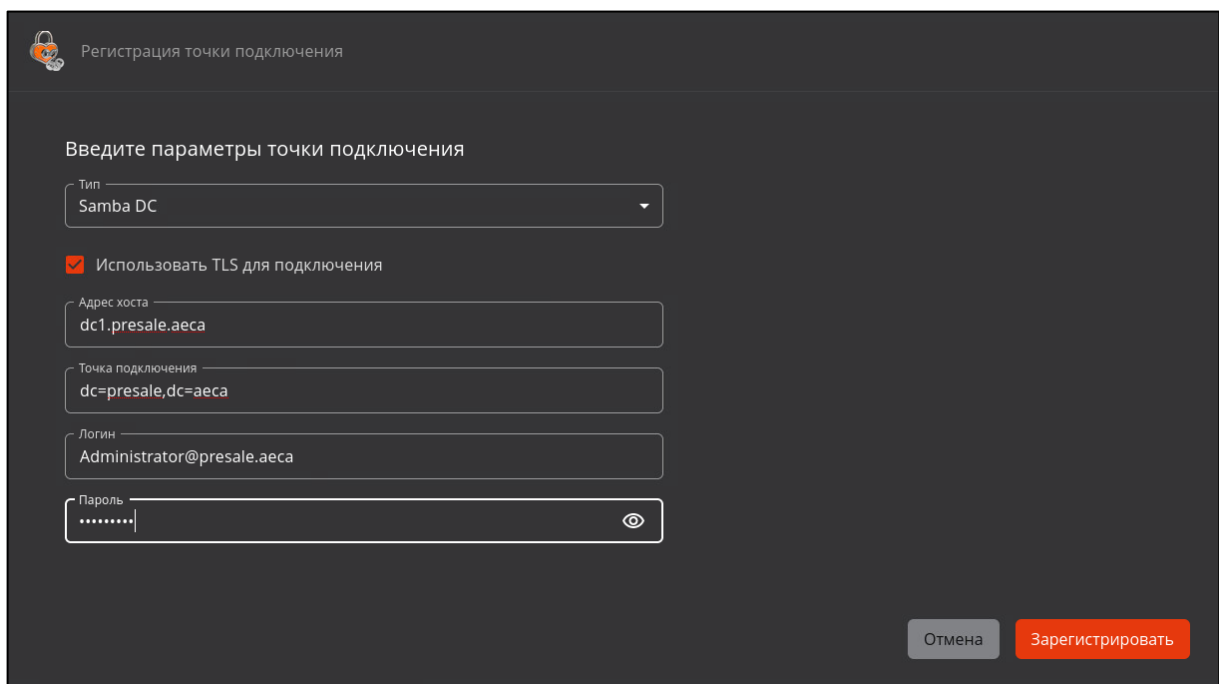
Точка подключения
dc=win20,dc=host

Логин
administrator@win20.host

Пароль
.....

Отмена **Зарегистрировать**

Рисунок 112 – Пример создания ресурсной системы типа 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 113 – Пример создания ресурсной системы типа Samba DC

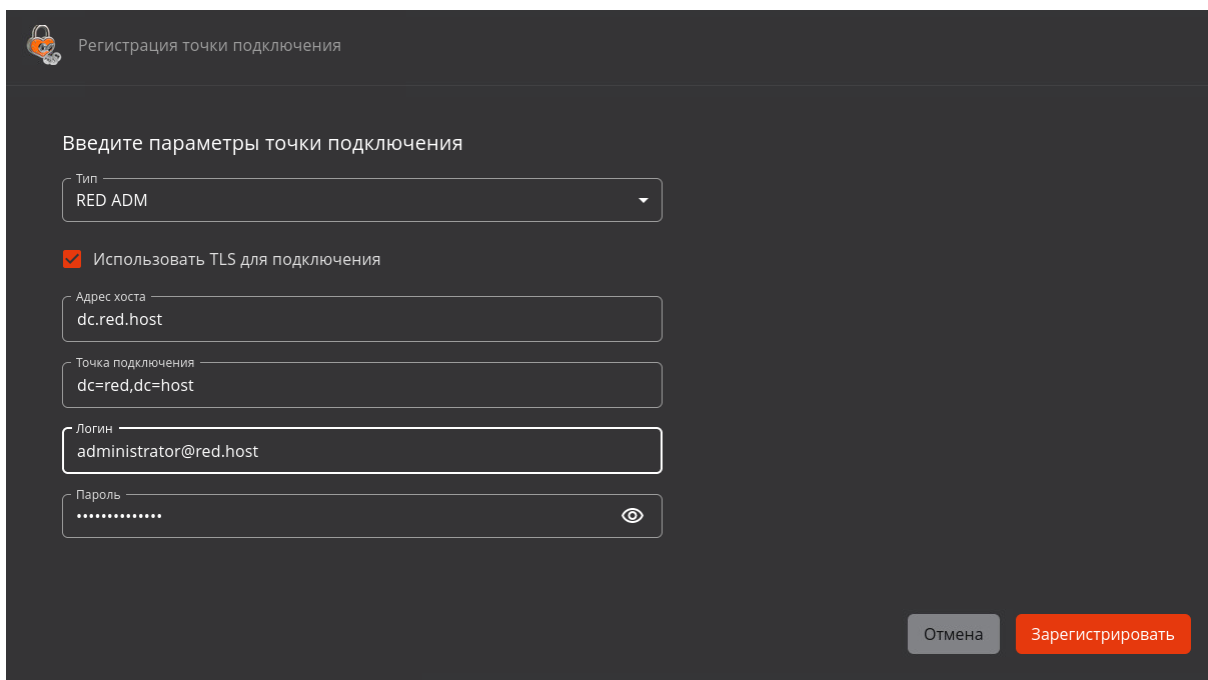


Рисунок 114 – Пример создания ресурсной системы типа РЕД АДМ

- В случае, если в поля формы подключения ресурсной системы введены неверные данные, то при нажатии кнопки <Зарегистрировать> администратор будет уведомлен соответствующим сообщением:
 - сообщение «Ошибка LDAP аутентификации: Неправильный логин или пароль» – при вводе неверных данных учётной записи администратора домена (см. Р и с у н о к 115);
 - сообщение об ошибке при вводе в поле «URL» (см. Рисунок 116);
 - сообщение об ошибке при настройке TLS-соединения (см. Рисунок 117);
 - сообщение об ошибке при совпадении регистрационных данных создаваемой и существующей ресурсных систем (см. Рисунок 118);
 - сообщение «Ошибка подключения к ресурсной системе» при возникновении других ошибок подключения к ресурсной системе.

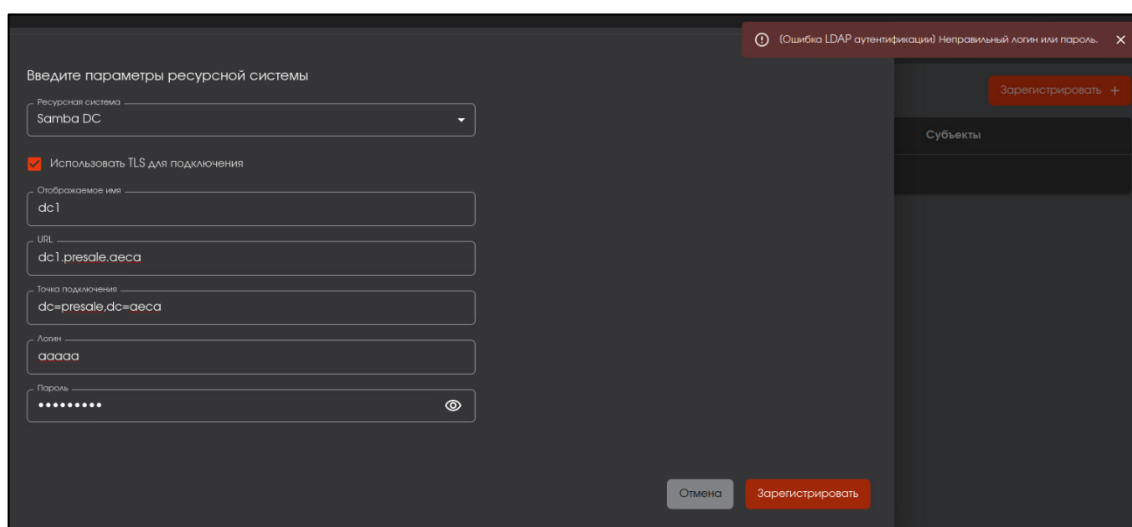


Рисунок 115 – Окно создания ресурсной системы. Уведомление об ошибке при вводе не верного логина или пароля администратора домена

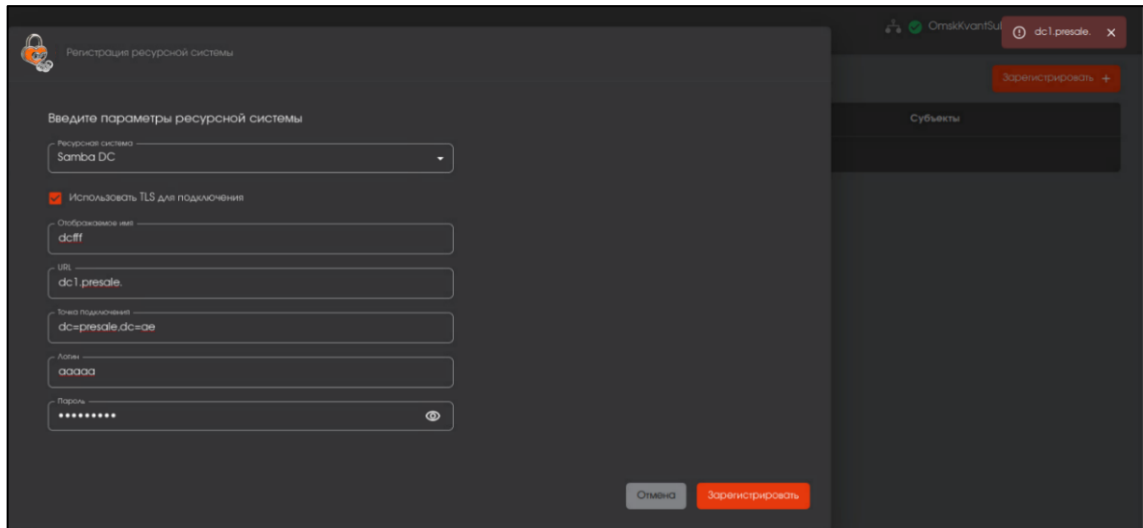


Рисунок 116 – Окно создания ресурсной системы. Уведомление об ошибке в поле «URL»

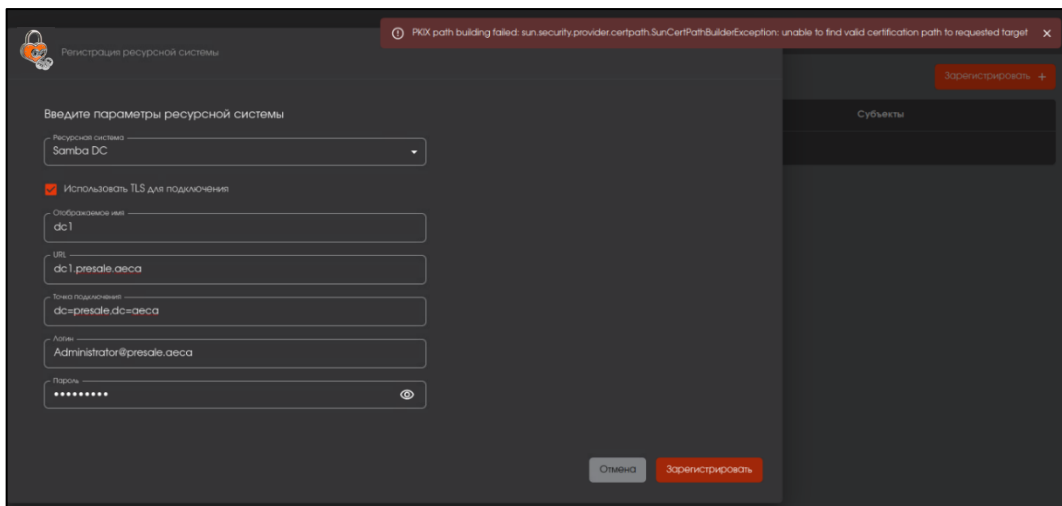


Рисунок 117 – Окно создания ресурсной системы. Уведомление об ошибке настройки TLS-соединения

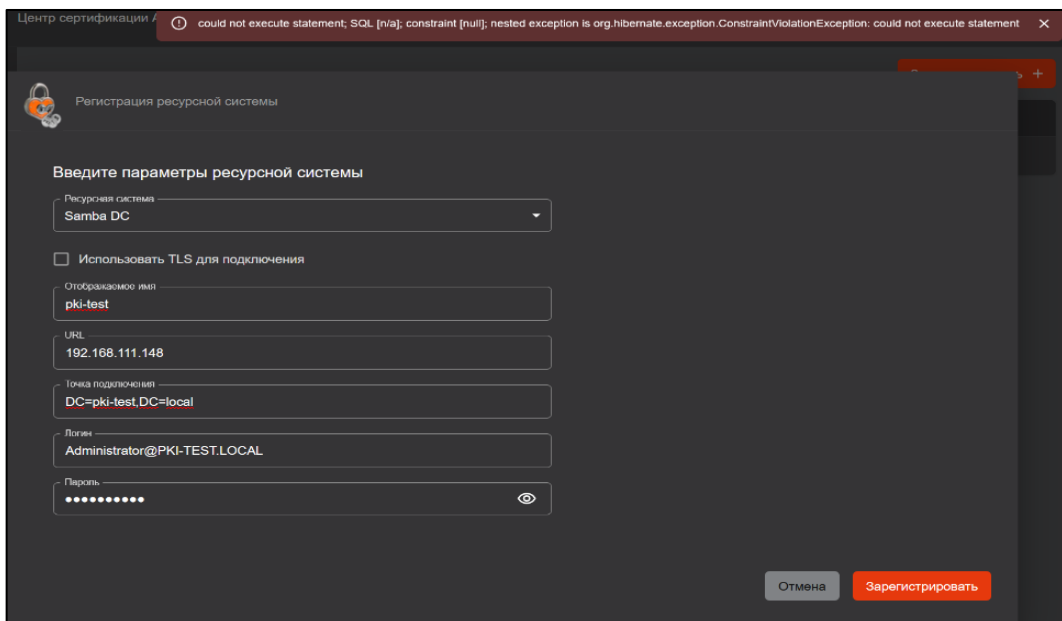


Рисунок 118 – Окно создания ресурсной системы. Уведомление об ошибке при создании ресурсной системы с одинаковыми регистрационными данными

- При успешном подключении к ресурсной системе выполняется получение данных из точки подключения, указанной при регистрации Base DN (dc=...).

7.8.2 Обновление зарегистрированной ресурсной системы

7.8.2.1 Виды обновления ресурсной системы

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

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

При запуске полной синхронизации нескольких точек подключения процесс выполняется поочередно. Статус ресурсной системы, обновление которой выполняется, будет отображен как «В процессе». Статус ресурсной системы, обновление которой запущено, но не выполняется, будет отображён как «В очереди».


По результатам обновления ресурсной системы будут:

- обновлены дата и время в поле «Последнее обновление» экранной формы «Ресурсная система»;
- в поле «Статус» экранной формы «Ресурсная система» будет отображён результат синхронизации «Успешно» или «Ошибка»;
- выведено всплывающее сообщение по результату синхронизации «Успешно» или «Ошибка».
- частичная. При частичной синхронизации выполняется обновление всех данных, полученных при полной синхронизации, за исключением сведений об удалении субъектов, организационных групп и групп безопасности из ресурсной системы.

7.8.2.2 Режимы обновления ресурсной системы

- Автоматический режим обновления ресурсной системы, при котором 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 `full_synchronization_cron` (значение по умолчанию `'0 0 0 * * *'` – запуск полной синхронизации каждую полночь);
- для задания расписания частичной синхронизации укажите значение CRON-выражения для параметра `part_synchronization_cron` (значение по умолчанию `'0 */30 * * * *'` – запуск частичной синхронизации каждые полчаса).

- Ручной запуск полной синхронизации ресурсной системы. Для ручного обновления подключенной ресурсной системы наведите курсор на созданный ресурс и нажмите появившуюся в строке кнопку  «Обновить», расположенную в правой части строки с названием подключаемого ресурса (см. Рисунок 119) - осуществляется загрузка данных для каждого существующего субъекта из ресурсной системы:

- список пользователей;
- список ПК в домене;
- список сервисов (только для ALD PRO и FreeIPA);
- список организационных групп;
- список групп безопасности.
- В результате обновления ресурсной системы состав объектов будет синхронизирован:
 - переименованы существующие объекты;
 - изменены существующие связи (включения в группы и т.д.);

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

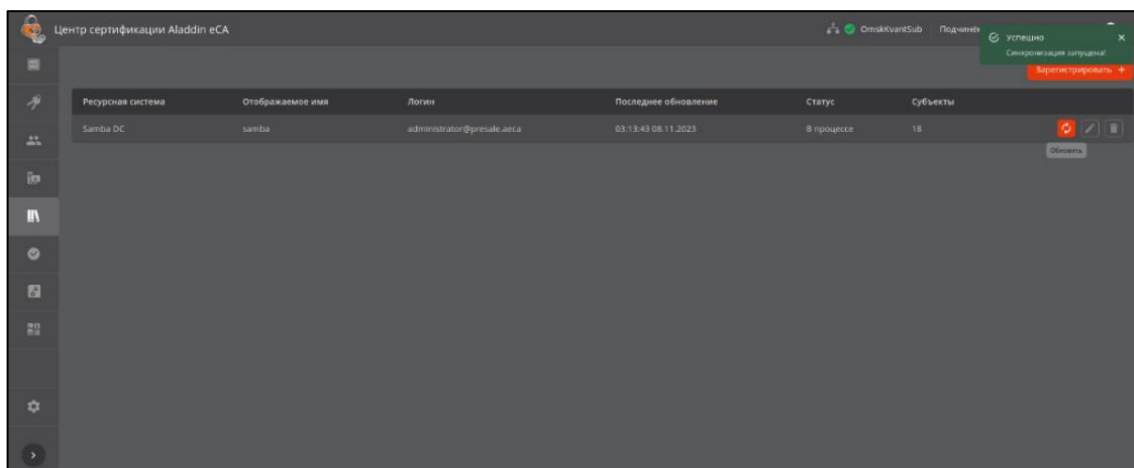



Рисунок 119 – Окно успешного обновления ресурсной системы

7.8.3 Редактирование зарегистрированной ресурсной системой

После добавления источника ресурсной системы, при наведении курсора на строку добавленного ресурса появляется возможность редактирования – при нажатии на кнопку <Редактировать>  (см. Рисунок 120) открывается окно для редактирования полей, заполненных при создании ресурсной системы. Тип подключаемого ресурса изменить невозможно (см. Рисунок 121).

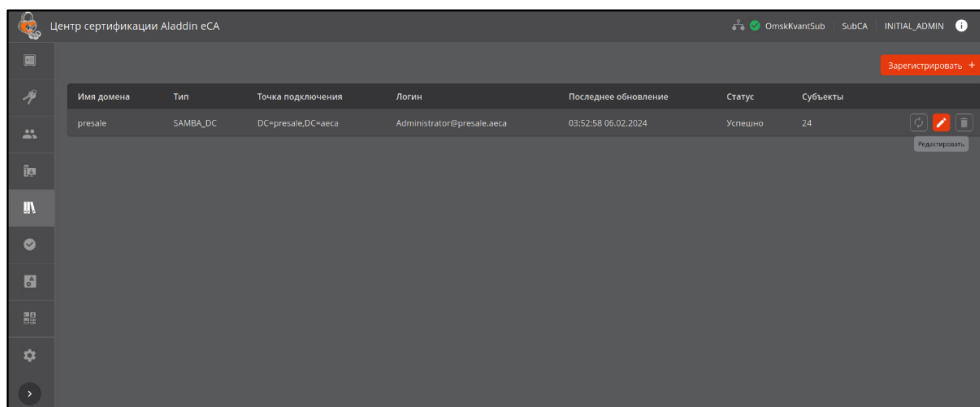


Рисунок 120 – Окно раздела «Ресурсная система». Кнопка редактирования РС

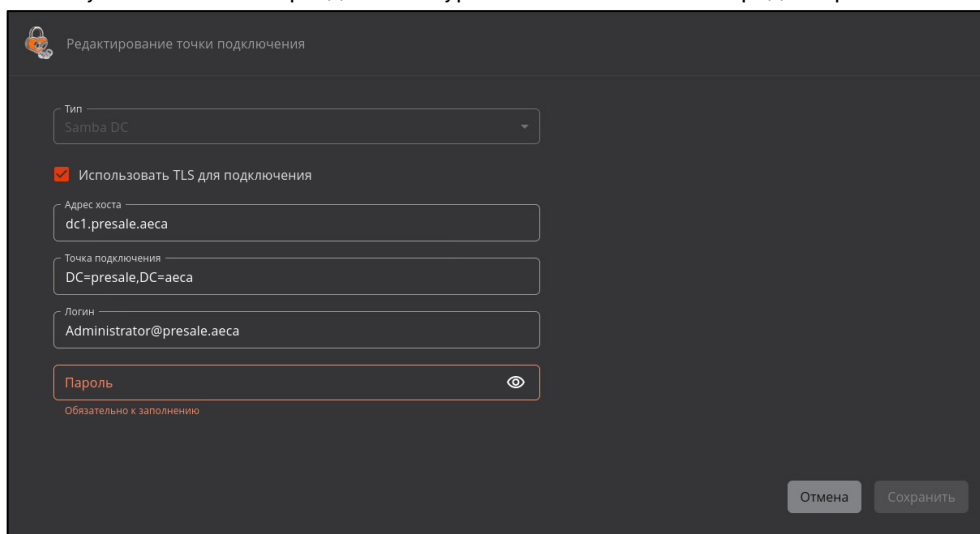



Рисунок 121 – Окно редактирования подключения к РС

7.8.4 Удаление зарегистрированной ресурсной системой

- После добавления источника ресурсной системы, при наведении курсора на строку добавленного ресурса появляется возможность удаления – при нажатии на кнопку <Удалить>  на экран будет выведено окно подтверждения выбранного действия (см. Рисунок 122).
- В результате удаления точки подключения:
 - все субъекты, полученные из этой точки подключения к ресурсной системе, будут переведены в отключенное от ресурсной системы состояние;
 - будут удалены группы ресурсной системы, полученные из точки подключения;
 - будут удалены связи групп с субъектами;
 - операторы, которым были назначены полномочия через группу ресурсной системы, потеряют права на управление данными субъектами.

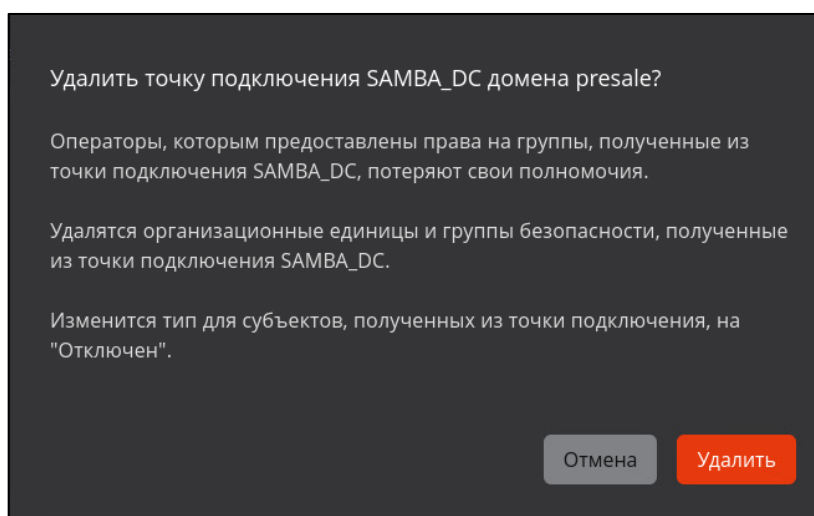


Рисунок 122 – Окно подтверждения удаления ресурсной системы

7.9 Раздел «Центры валидации»

- Переход в раздел «Центры валидации» (см. Рисунок 123) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 38).
- Данный раздел доступен только для пользователя с ролью «Администратор».

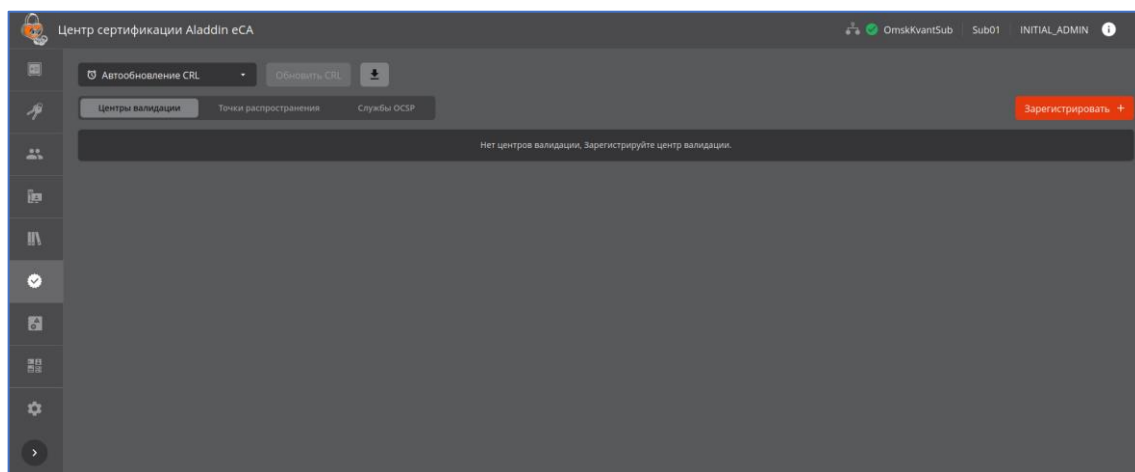


Рисунок 123 – Экран раздела «Центр валидации»

- Работа с разделом «Центры валидации» предусматривает выполнение следующих сценариев использования:
 - моментальная публикация списков отозванных сертификатов CRL (с уведомлением о результатах публикации);
 - регистрация центра валидации;
 - настройка параметров центра валидации;
 - удаление центра валидации (с подтверждением);
 - изменение периода авто-обновления точек публикации CRL и срока действия перекрытия Delta CRL для текущего активного Центра сертификации;
 - экспорт крайнего списка отозванных сертификатов;
 - экспорт сертификата текущего издающего Центра сертификации (из карточки Центра валидации, см. подраздел 7.9.2.3 настоящего руководства);
 - создание пользовательских точек распространения CRL, Delta CRL и AIA;
 - просмотра в табличном виде служб OCSP, зарегистрированных Центров валидации Aladdin Enterprise Certificate Authority.
- В разделе «Центры валидации» доступны следующие функции, вне зависимости от выбора вкладки («Центры валидации», «Точки распространения» или «Сервисы OCSP»):
 - настройка периода автообновления разностного и полного списков отозванных сертификатов;
 - моментальная публикация полного списка отозванных сертификатов;
 - экспорт актуального списка отозванных сертификатов.

7.9.1.1 Настройка периода автообновления

- Нажатие на поле <Автообновление CRL> на экране «Центр валидации» вызывает всплывающее меню, содержащее: (см. Рисунок 124):
 - поле «период/перекрытие» содержит период обновления публикации CRL/срок действия перекрытия. Значение периода обновления CRL должно быть больше значения периода обновления Delta CRL.
 - поле «Последнее», которое содержит дату и время последней публикации в формате «дд.мм.гггг чч.мм» (24-часовой формат);
 - поле «Следующее», которое содержит дату и время следующей публикации в формате «дд.мм.гггг чч.мм» (24-часовой формат);
 - поле «Delta CRL» содержит период обновления публикации Delta CRL. Значение периода обновления Delta CRL должно быть меньше значения периода обновления CRL. Значение «Delta CRL»

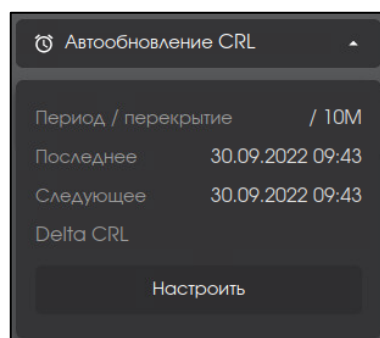


Рисунок 124 - Подменю "Следующая публикация"

ВНИМАНИЕ! При перенастройке периода точки публикации текущего ЦС перенастраивается время публикации всех списков CRL текущего ЦС. Время публикации CRL синхронизировано при настройке периода публикации, при создании нового сервиса публикации, при публикации по команде (включая REST) и одинаково для всех точек публикации текущего ЦС.

• При нажатии на кнопку <Настроить> (см. Рисунок 124) открывается окно с настройками (см. Рисунок 125):

- периода обновления публикации CRL (`crlperiod`) – задается период обновления CRL в формате час, день, месяц, год – время между публикациями;
- срока действия перекрытия (`crlOverlapTime`) – задается время до истечения срока действия текущего CRL, за которое будет публиковаться новый CRL;
- возможность поставить флаговую кнопку в поле «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 сохранить настройки будет невозможно до ввода корректного значения Delta CRL. Период обновления DeltaCRL может быть не задан - тогда DeltaCRL не публикуется.

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

Рисунок 125 – Окно настройки автообновления CRL

• Значения периодов обновления публикаций CRL и Delta CRL (`crlperiod` и `deltacrlperiod`) следует выбирать исходя из интенсивности обновления списка сертификатов в конкретных условиях эксплуатации.

• Значение срока действия перекрытия (`crlOverlapTime`) стоит выбирать исходя из следующих рекомендации:

- Срок действия перекрытия (`crlOverlapTime`) должно составлять 1/10 от значения периода обновления публикаций CRL (`crlperiod`), но не более 12 часов, и выполняются две нижеприведенные рекомендации;
- Срок действия перекрытия (`crlOverlapTime`) не должно быть больше периода обновления Delta CRL (`deltacrlperiod`), если выполняется следующее нижеприведенное условие;

- Срок действия перекрытия (`crlOverlapTime`) не должно быть меньше 1.5 от интервала рассинхронизации времени в сети (обычная рассинхронизация до 10 мин).
- В файлах CRL указываются следующие поля, указывающие на время действия списка отозванных сертификатов:
 - <Last Update> – дата вступления в силу CRL, указывающая на начало его действия;
 - <Next Update> – дата следующего обновления CRL, указывающая на дату истечения срока действия CRL и, когда CRL становится недействительным для проверки.
- При планировании срока действия CRL требуется также учитывать время следующей публикации (Next Publish), где следующая публикация (Next Publish) – это момент времени, указывающий дату и время, когда Центр сертификации выпускает новый CRL. Этот момент времени не записывается в CRL, но вычисляется для определения момента генерации, следующего CRL.
- Между настроенными значениями и значениями, которые указываются в файле CRL/DeltaCRL и выводятся в интерфейсе пользователя, должна быть следующая связь:
 - для CRL:

```
<Last Update> = <время создания CRL>
<Next Publish> = < Last Update> + <crlperiod>
<Next Update> = <Next Publish> + <crlOverlapTime>
```

- для DeltaCRL:

```
<Last Update> = <время создания DeltaCRL>
<Next Publish> = <Last Update> + <deltacrlperiod>
<Next Update> = <Next Publish>
```

- При каждой новой генерации CRL увеличивается значение номера версии (CRLNumber).
- При каждой новой генерации DeltaCRL увеличивается значение CRLNumber индикатора DeltaCRLIndicator и соответствует тому CRL, для которого указана разница.
- Служба CRL DP начинает распространять CRL/DeltaCRL с большим номером (версии и индикатора) сразу после его поступления и проверки подписи издателя.

7.9.1.2 Моментальная публикация списка отозванных сертификатов CRL

- Для того, чтобы не ждать наступление времени публикации, указанного в элементе «Следующее», можно нажать кнопку «Обновить CRL» (см. Рисунок 126). При нажатии на кнопку «Обновить CRL» публикуется внеплановый список отзыва, при этом таймер публикации списка отзыва сбрасывается и начинается новый отсчет времени публикации.
- Все сгенерированные списки отозванных сертификатов (в формате .crl) будут сохранены в базе данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`), схема базы данных «store», таблица «file_registry».

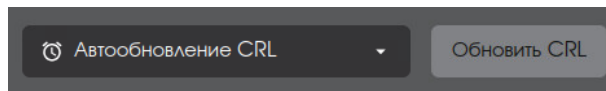



Рисунок 126 – Кнопка «Обновить CRL»

7.9.1.3 Экспорт актуального списка отозванных сертификатов CRL

- Для загрузки списка отозванных сертификатов в Центре сертификации необходимо нажать кнопку «Скачать CRL»  на верхней панели раздела «Центры валидации». В открывшемся окне выберите нужное действие из предложенных:

- введите срок действия CRL, сгенерируйте и скачайте список отозванных сертификатов в случае, если ранее не зарегистрирован Центр валидации и список CRL не публиковался (см. Рисунок 127);

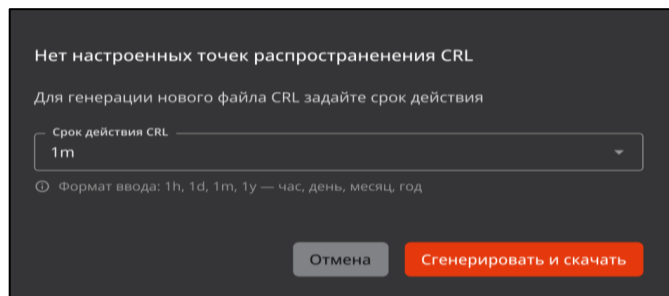


Рисунок 127 – Окно скачивания списка CRL, если нет зарегистрированных Центров валидации

- скачайте последний список CRL или сгенерируйте новый список отозванных сертификатов в случае, если Центр валидации не создан, но ранее список CRL был опубликован (см. Рисунок 128). Возможно задать срок действия CRL;

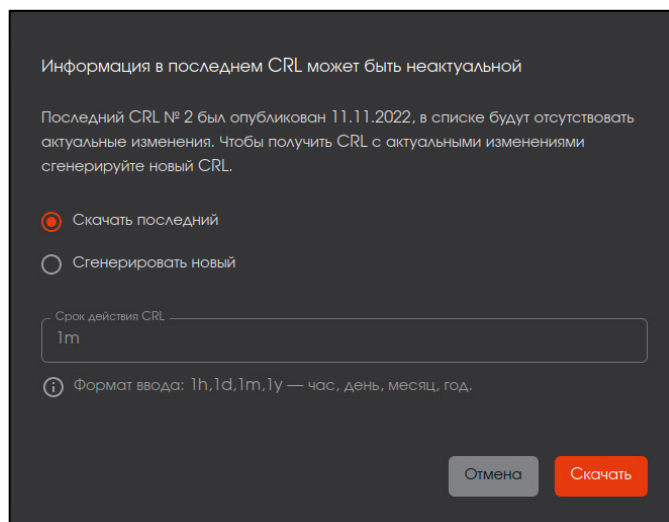


Рисунок 128 – Окно скачивания списка CRL, если ранее список был опубликован, но Центр валидации не зарегистрирован

- скачайте последний список CRL, если есть активные зарегистрированные Центры валидации (см. Рисунок 129).

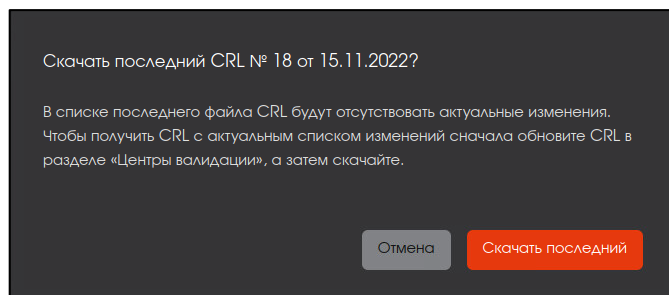


Рисунок 129 – Окно скачивания списка CRL, если есть активный Центр валидации

В скачанном списке отозванных сертификатов указано время в формате GMT+0.

7.9.2 Вкладка «Центры валидации»

- Данная вкладка предназначена для управления Центрами валидации Aladdin Enterprise Certificate Authority, развёрнутыми на серверах в информационной системе.

- На вкладке отображаются url-адреса всех зарегистрированных центров валидации.
- Возможно создание нескольких записей для разных Центров валидации, включающих точки распространения списков отозванных сертификатов (CRL DP) и информации о центре сертификации (AIA).

7.9.2.1 Регистрация Центра валидации на сервере Центра сертификации

Для выполнения автоматической инициализации служб CRL DP, AIA и OCSP выполните регистрацию центра валидации.

- Предварительно требуется:
 - развернуть компонент «Центр валидации Aladdin eCA» на сервере-OCSP;
 - скопировать сертификат учётной записи администратора «Центра валидации» `/opt/aeca/p12/superadmin.p12`;
 - скопировать пароль из файла `generated_passwords.txt`, данные строки `superadmin_password`, полученный после установки ПО AeCA VA;
 - перенести подготовленные данные на сервер «Центра сертификации»;
 - настроить автообновление CRL согласно п. 7.9.1.1 настоящего руководства;
 - опубликовать CRL согласно пункту 7.9.1.2 настоящего руководства.
- Регистрация «Центра валидации» состоит из двух последовательных действий:
 - активация служб AIA и CRL DP;
 - активация службы OCSP.
- Для активации служб AIA и CRL DP на текущей вкладке «Центр валидации» нажмите кнопку <Зарегистрировать+>.
- В открывшемся окне регистрации центра валидации (см. Рисунок 130) укажите параметры центра валидации:
 - в поле «Имя хоста» укажите ip-адрес или имя хост-сервера с указанием доменной зоны, на котором развёрнут компонент «Центр валидации» Aladdin eCA;
 - загрузите предварительно скачанный сертификат `superadmin.p12` сервера Центр валидации, нажав кнопку <Выбрать файл> и введя соответствующий пароль сертификата в поле «Пароль контейнера».
- Нажмите ставшую активной кнопку <Зарегистрировать> для создания Центра валидации или отмените действие нажав кнопку <Отмена>.

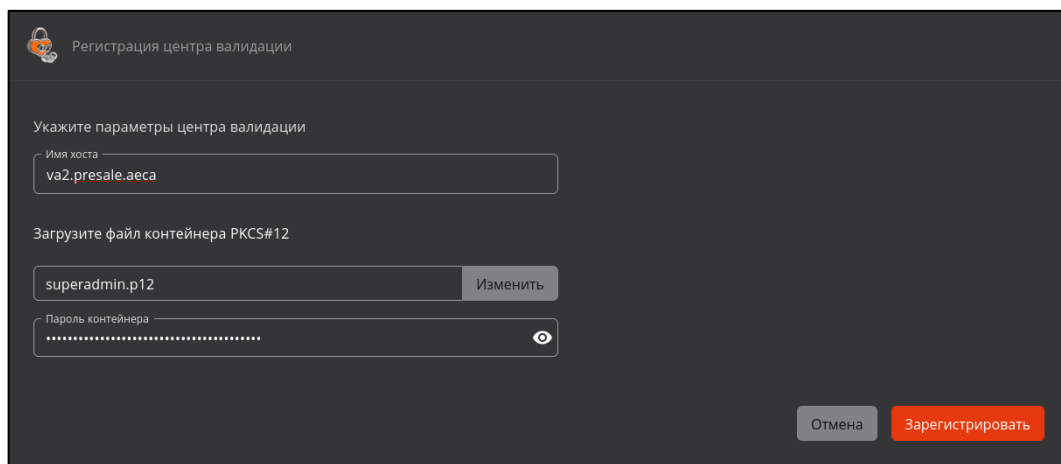


Рисунок 130 – Окно регистрации центра валидации

- В случае успешной регистрации Центра валидации, администратор будет уведомлён сообщением в окне регистрации центра валидации (см. Рисунок 131).

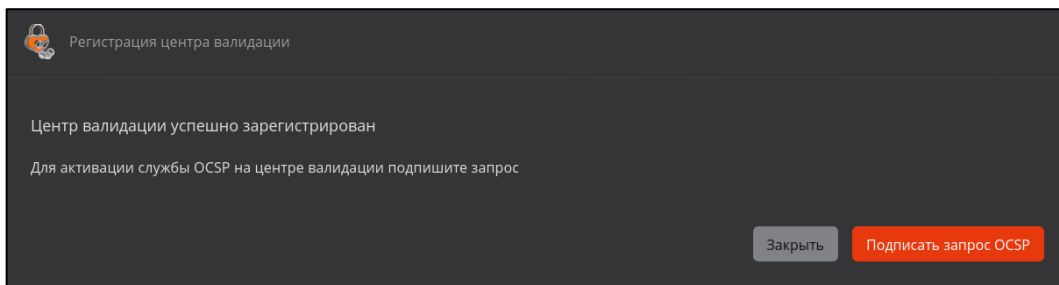


Рисунок 131 – Окно регистрации центра валидации. Сообщение об успешном создании Центра валидации

- В текущем окне возможно сразу подписать запрос OCSP, нажав одноимённую кнопку, или выполнить данное действия позже, статус созданного Центра валидации при этом будет «Ожидает подпись запроса OCSP» (см. Рисунок 132).

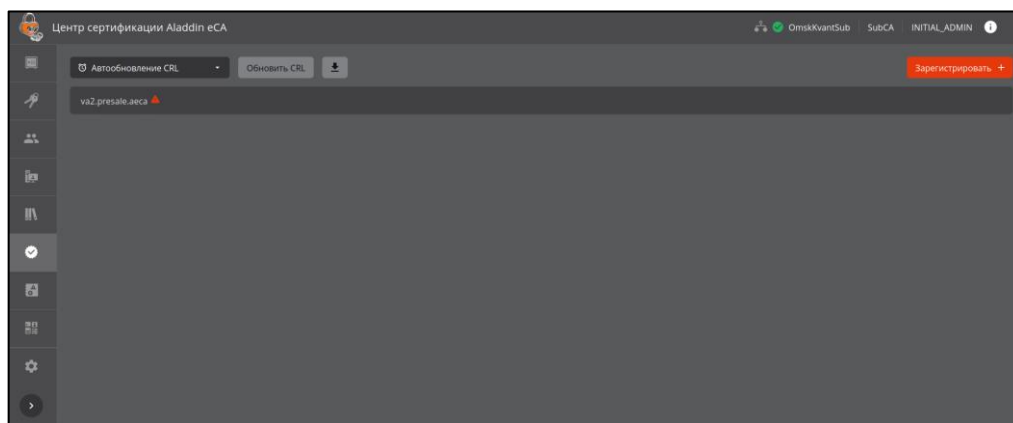


Рисунок 132 – Созданный центр валидации в статусе «Ожидает подпись запроса OCSP»

- После активации служб AIA и CRL DP на сервере «Центра валидации» появляется запись на вкладке «Издатель» (см. Рисунок 133).

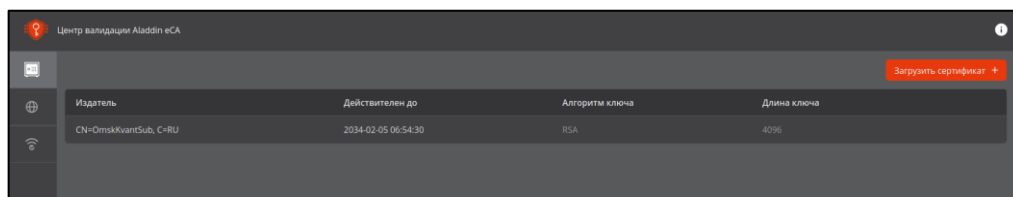


Рисунок 133 – Сервис «Центр валидации» после активации служб AIA и CRL DP

- Службы CRL DP и AIA создаются удаленно через панель управления «Центра сертификации».
- Схема взаимодействия программного компонента «Центр сертификации Aladdin eCA» и программного компонента «Центр валидации Aladdin eCA» при инициализации служб CRL DP, AIA и OCSP представлена на Рисунок 134.

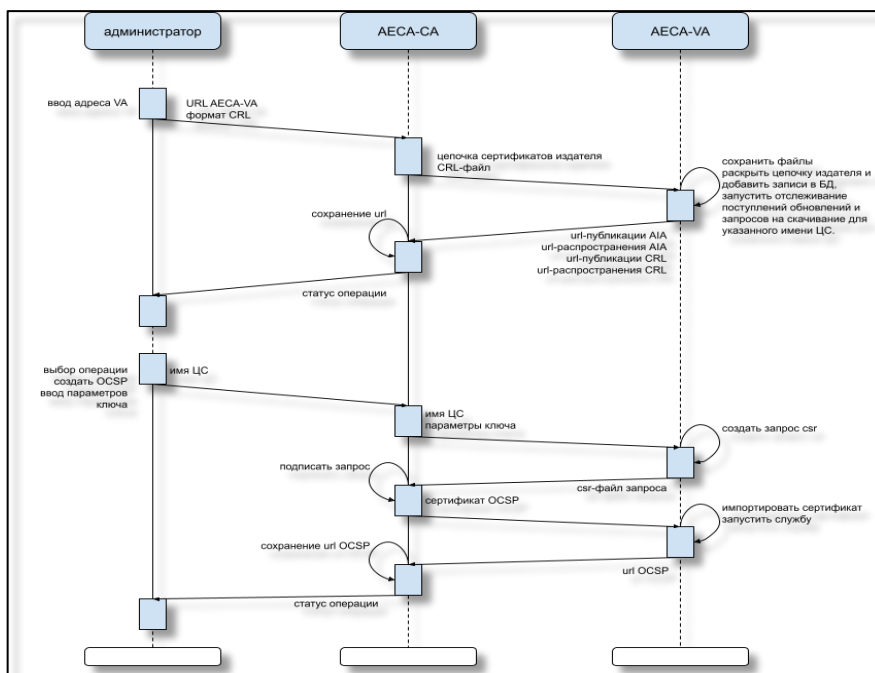


Рисунок 134 – Схема взаимодействия ПО «Центр сертификации» и ПО «Центр валидации»

- В случае безуспешной регистрации Центра валидации, администратор будет уведомлён сообщением в окне регистрации центра валидации с рекомендацией проверить доступность сетевого соединения (см. Рисунок 120).

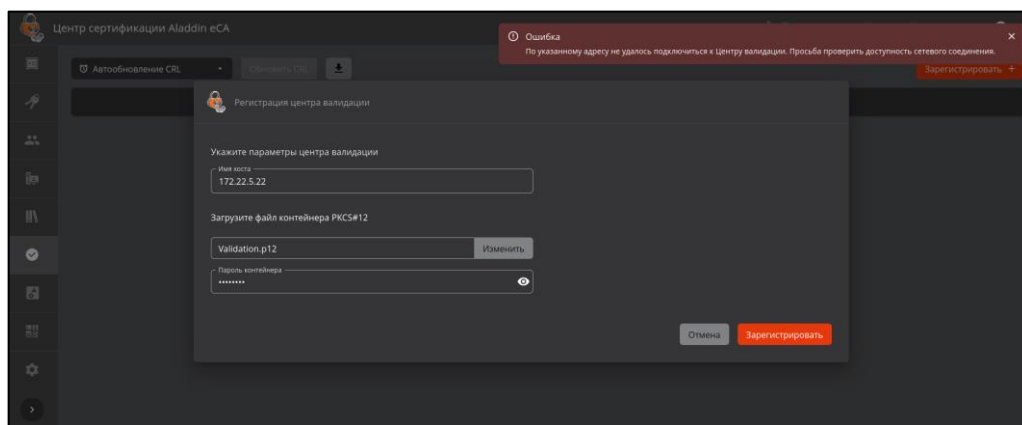


Рисунок 135 – Окно регистрации центра валидации. Сообщение об ошибке

7.9.2.2 Подписание запроса OCSP-сервера

Перед активацией службы OCSP необходимо настроить автообновление CRL!

- Для активации службы подпишите запрос OCSP:
 - продолжив работу в Мастере регистрации центра валидации после нажатия кнопки <Подписать запрос OCSP> (см. Рисунок 131), или
 - открыв карточку созданного сервиса OCSP в состоянии «Ожидает подпись запроса», и нажав кнопку <Подписать запрос +> в поле карточки «OCSP» (см. Рисунок 139).
- В открывшемся окне обработки запросов OCSP (см. Рисунок 136) укажите:

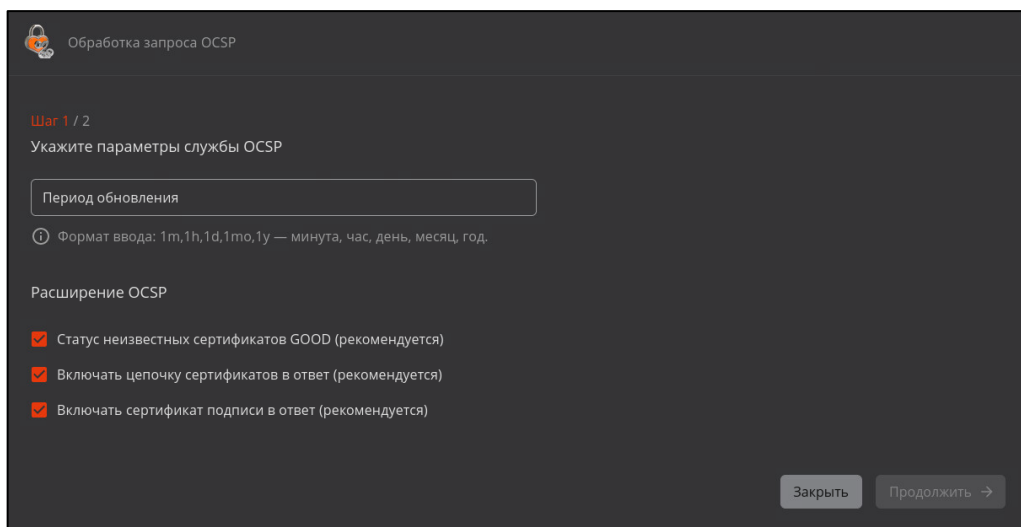


Рисунок 136 – Окно обработки запроса OSCP. Шаг 1

- период обновления – задание периода опроса службы распространения CRL. Формат ввода: 1h,1d,1m,1y - час, день, месяц, год;
- выберите дополнительные расширения OSCP (по умолчанию рекомендовано выбрать все расширения):
 - <статус неизвестных сертификатов GOOD> – для любого сертификата не указанного в CRL ответ: good; для любого сертификата не указанного в CRL ответ: unknown (off);
 - галочки <Включать цепочку сертификатов...> и <Включать сертификат подписи...> определяют включать или нет сертификат подписи (сертификат OSCP) в ответ и включать ли его цепочку.
- Нажать, ставшую активной кнопку, <Продолжить>.
- На втором шаге в окне обработки запроса OSCP (см. Рисунок 137) укажите параметры криптографии:
 - алгоритм ключа;
 - длину ключа.
- Для активации и запуска Центра валидации нажмите кнопку <Подписать и запустить>, для отмены прогресса нажмите кнопку <Закреть>.

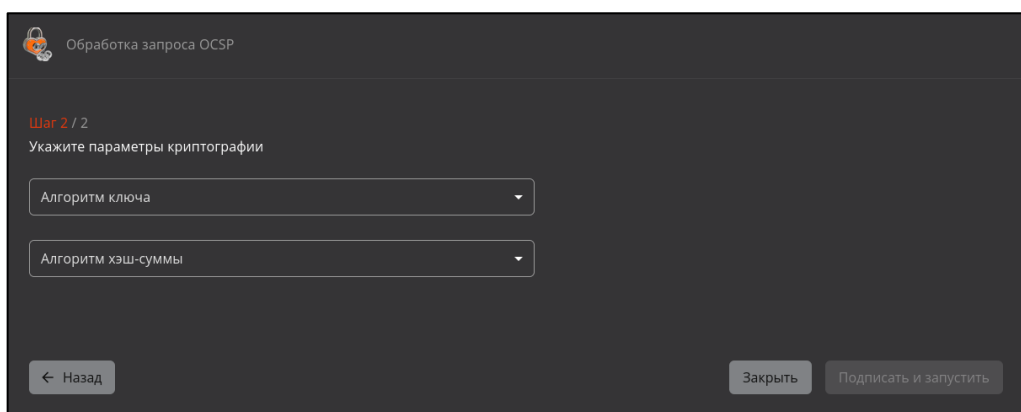


Рисунок 137 – Окно обработки запроса OSCP. Шаг 2

- После успешной активации администратор будет уведомлен информационным сообщением (см. Рисунок 138).

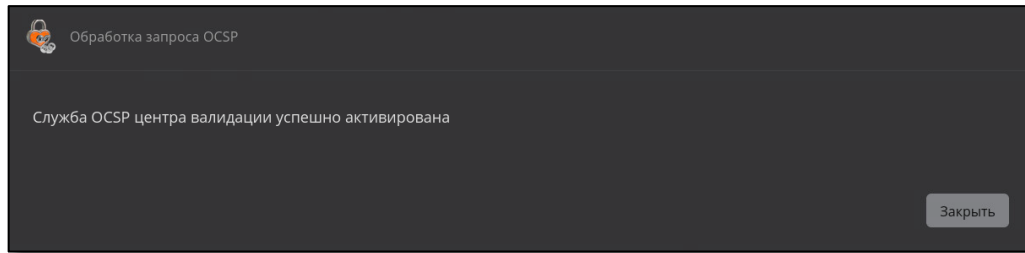


Рисунок 138 – Окно обработки запроса OSCP

- В результате выполненных действий будет выпущен сертификат OSCP-сервера сроком действия на 2 года, просмотр карточки и скачивание которого доступны на вкладке «Сертификаты».

7.9.2.3 Карточка центра валидации (доступ к функциям управления)

- Для просмотра карточки зарегистрированного центра валидации (см. Рисунок 139) необходимо щёлкнуть левой кнопкой мыши на нужном сервисе на главном экране вкладки «Центр валидации».

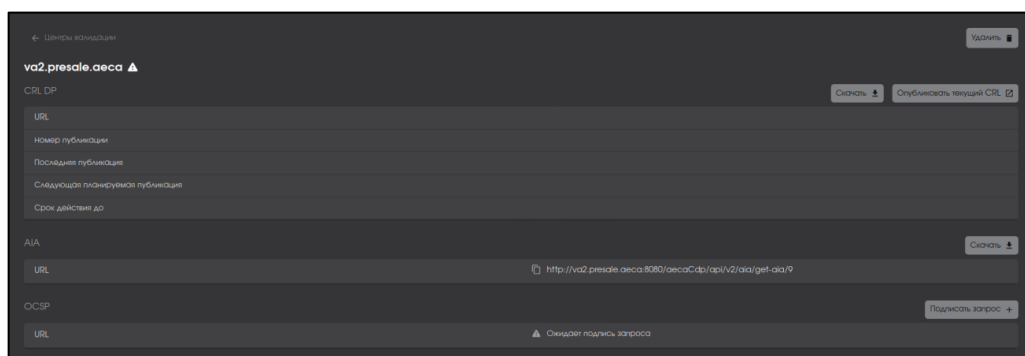


Рисунок 139 – Карточка зарегистрированного Центра валидации

- При регистрации Центра валидации происходит созданию служб CRL DP и AIA в карточке Центра валидации появляются адреса CRL DP и AIA.
- В открывшемся окне администратору доступны:
 - кнопка <Удалить> для удаления сервиса через подтверждение действия;
 - для службы CRL DP доступны:
 - загрузка списка отозванных сертификатов по нажатию кнопки <Скачать>;
 - публикация на Центре валидации последнего сгенерированного списка CRL по нажатию кнопки <Опубликовать>;
 - просмотр и копирование URL-адреса загрузки CRL, который будет включаться в сертификаты, в буфер обмена путём двойного нажатия мышкой на адрес;
 - просмотр номера публикации;
 - просмотр даты и времени последней публикации;
 - просмотр даты и времени следующей публикации;
 - просмотр даты и времени срока действия текущего CRL;
 - для службы AIA доступны:
 - загрузка опубликованного сертификата текущего издающего Центра сертификации по нажатию кнопки <Скачать>;
 - просмотр и копирование URL-адреса, который будет включаться в сертификаты, в буфер обмена путём двойного нажатия мышкой на адрес;

- для службы OCSP доступны:
 - просмотр и копирование URL-адреса OCSP, который будет включаться в сертификаты, в буфер обмена путём двойного нажатия мышкой на адрес;
 - просмотр статуса OCSP, если активация не завершена
 - кнопка <Подписать запрос>, если активация не завершена.

7.9.2.4 Состояния центра валидации и действия над ним

Состояние «Ожидает подпись запроса OCSP»

После регистрации Центр валидации переходит в состояние «Ожидает подпись запроса OCSP» (см. Рисунок 140), то есть служба OCSP не инициализирована и выводится соответствующая отметка с предупреждением.

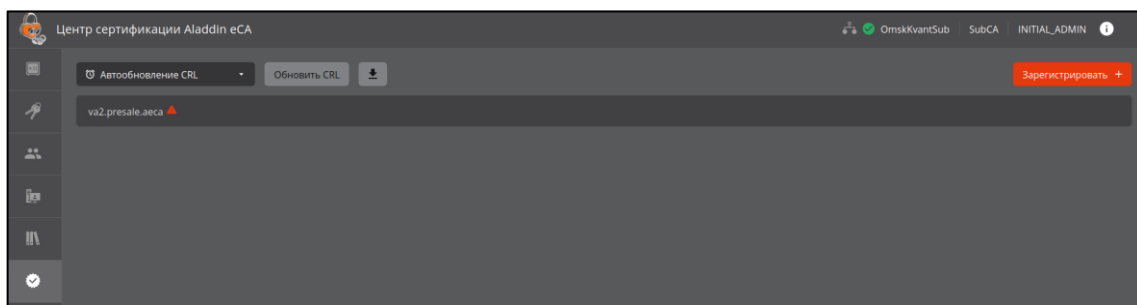



Рисунок 140 – Центр валидации в статусе «Ожидает подпись запроса OCSP»

При наведении на строку с нужным центром валидации будет доступна иконка  <Удалить>. После нажатия на кнопку <Удалить> будет выведено на экран окно подтверждения действия (см. Рисунок 141), где возможно отменить выбранное действие, нажав кнопку <Отмена>, или подтвердить удаление выбранного центра валидации, нажав кнопку <Удалить>.

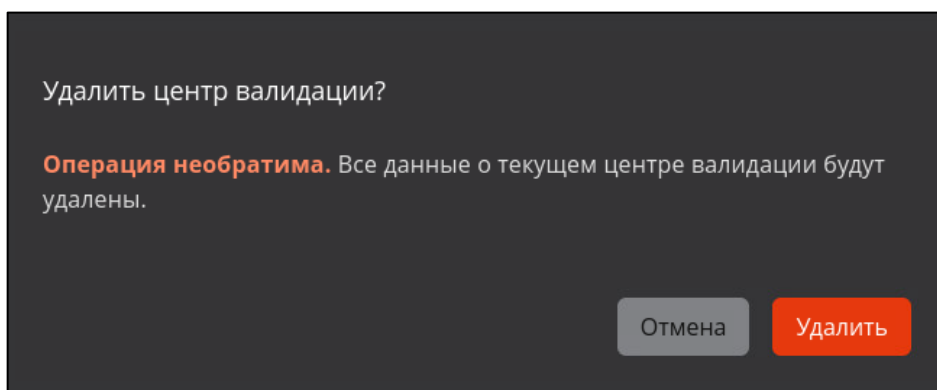


Рисунок 141 – Окно подтверждения удаления центра валидации

Состояние «Запущен»

После подписания запроса OCSP-сервера на сертификат Центр валидации переходит в состояние «Запущен» (см. Рисунок 142).

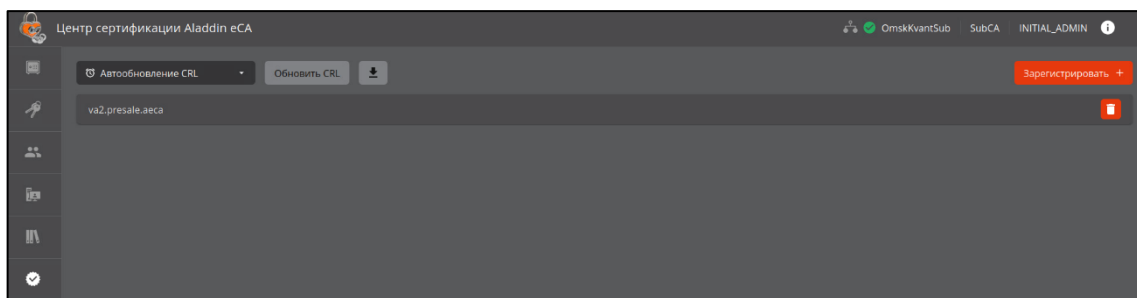




Рисунок 142 – Центр валидации в состоянии «Запущен»

7.9.3 Вкладка «Точки распространения»

- Данная вкладка предназначена для:
 - просмотра URL-адресов точек распространения CRL, Delta CRL и AIA, зарегистрированных Центров валидации Aladdin Enterprise Certificate Authority (на вкладке «Центры валидации»), образующих **автоматические точки**, обозначенные на экране вкладки пиктограммой ;
 - регистрации сторонних точек распространения CRL, Delta CRL и AIA, существующих или развертываемых на серверах в информационной системе, образующих **пользовательские точки**, обозначенные на экране вкладки пиктограммой .
- На вкладке (см. Рисунок 143) отображены точки распространения (автоматические и пользовательские), сгруппированные по назначению распространяемой информации (CRL, Delta CRL, AIA) в табличном формате с указанием:
 - типа точки распространения с соответствующей пиктограммой (автоматическая или пользовательская);
 - Центра валидации – имя сервера (hostname) Центра валидации Aladdin Enterprise Certificate Authority, которому принадлежит точка распространения (только для автоматической точки);
 - URL – ip-адреса сервера точки распространения.

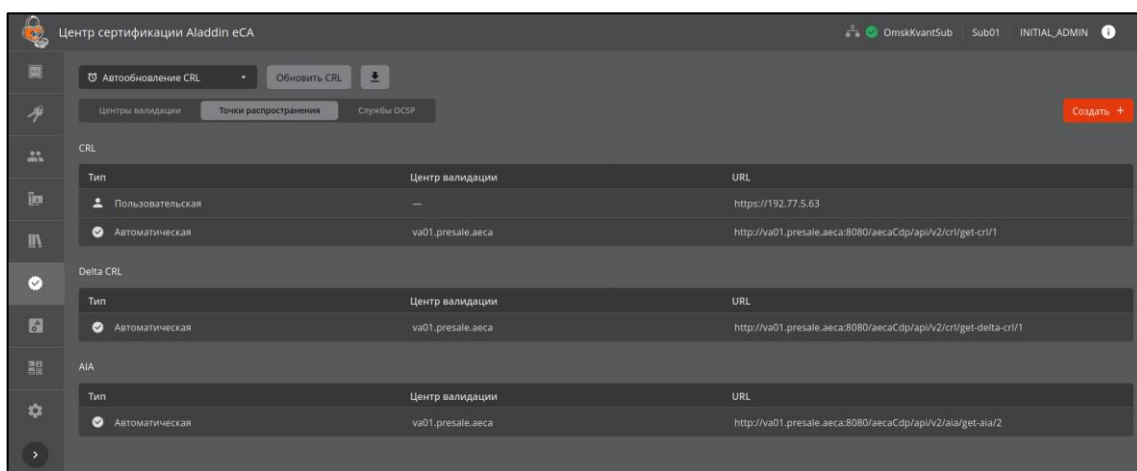



Рисунок 143 – Окно вкладки «Точки распространения» в разделе «Центры валидации»

- Для точки распространения типа «Автоматическая» действия не предусмотрены, доступен только просмотр данных точки на экране текущей вкладки.
- Для точки распространения типа «Пользовательская» возможны следующие действия:
 - создание (регистрация) новой точки распространения;
 - редактирование созданной точки распространения;

- удаление созданной точки распространения.

7.9.3.1 Создание пользовательской точки распространения

- Предварительно требуется подготовить URL незарегистрированной точки распространения.
- Для создания пользовательской точки распространения списка отзыва сертификатов (CRL), разностного списка отзыва сертификатов (Delta CRL) или сертификатов издающих Центров сертификации (AIA) выполните регистрацию точки распространения, нажав кнопку <Создать>  (см. Рисунок 143).
 - В открывшемся окне (см. Рисунок 144) выберите назначение распространяемой информации в поле «Тип» из выпадающего списка:
 - CRL – распространение списка отозванных сертификатов;
 - Delta CRL – распространение разностного списка отозванных сертификатов;
 - AIA – распространение сертификатов издающих Центров сертификации.
 - Укажите предварительно подготовленный URL точки распространения в поле «URL». Сообщения о возможных ошибках в поле «URL»:
 - если введённый URL точки распространения совпадает с URL существующей (зарегистрированной) точкой распространения (любого типа), то в поле «URL» будет отображено сообщение о данной ошибке: «Указан URL существующей точки распространения»;
 - если введённый URL точки распространения содержит пробел, то в поле «URL» будет отображено сообщение о данной ошибке: «Некорректный ввод».

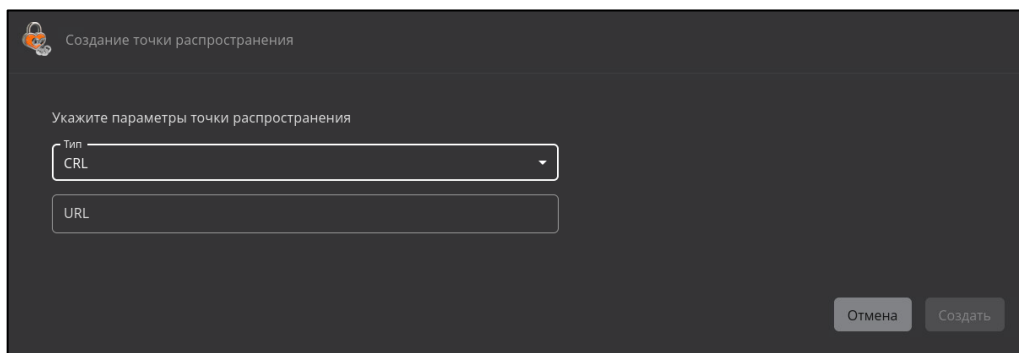


Рисунок 144 – Окно создания точки распространения

- После корректного заполнения всех полей окна, нажмите, ставшую активной кнопку <Создать>.
- В результате создания пользовательской точки распространения администратор будет уведомлён соответствующим сообщением (см. Рисунок 145).

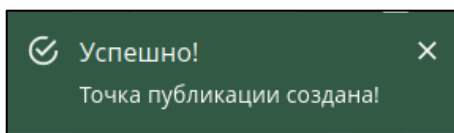


Рисунок 145 – Сообщение об успешном создании пользовательской точки публикации

7.9.3.2 Редактирование пользовательской точки распространения

- Для редактирования зарегистрированной пользовательской точки необходимо выделить нужную точку в текущем окне и нажать появившуюся кнопку <Редактировать> (см. Рисунок 146).

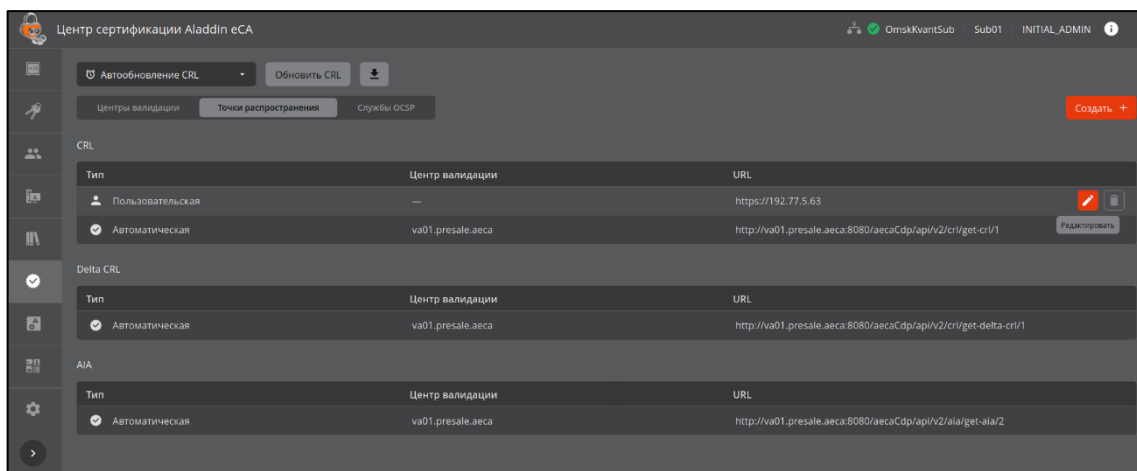


Рисунок 146 – Кнопка действий над пользовательской точкой распространения (Редактировать)

- В открывшемся окне (см. Рисунок 147) возможно изменить указанный URL пользовательской точки распространения и применить изменения, нажав активировавшуюся кнопку <Сохранить изменения>, или выйти без сохранения результатов изменения или окна редактирования, нажав кнопку <Отмена>.
- Если URL точки распространения будет отредактирован не корректно, то кнопка <Сохранить изменения> будет недоступна, и администратор будет уведомлён о возможных ошибках в поле «URL»:
 - если введённый URL точки распространения совпадает с URL существующей (зарегистрированной) точкой распространения (любого типа), то в поле «URL» будет отображено сообщение о данной ошибке: «Указан URL существующей точки распространения»;
 - если поле «URL» пустое, то будет отображено сообщение об ошибке: «Обязательно к заполнению»;
 - если введённый URL точки распространения содержит пробел, то в поле «URL» будет отображено сообщение о данной ошибке: «Некорректный ввод».

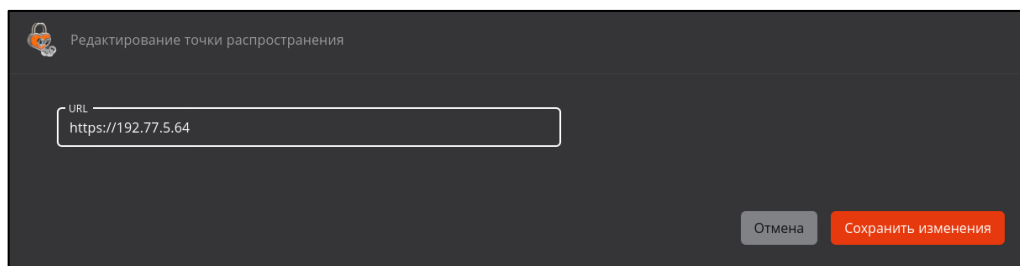


Рисунок 147 – Окно редактирования пользовательской точки

- В результате успешного редактирования пользовательской точки распространения и сохранения результата администратор будет уведомлён соответствующим сообщением (см. Рисунок 148).

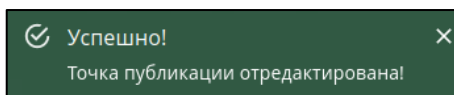


Рисунок 148 – Сообщение об успешном редактировании пользовательской точки публикации

7.9.3.3 Удаление пользовательской точки распространения

- Для удаления зарегистрированной пользовательской точки необходимо выделить нужную пользовательскую точку распространения в текущем окне и нажать появившуюся кнопку <Удалить> (см. Рисунок 149).

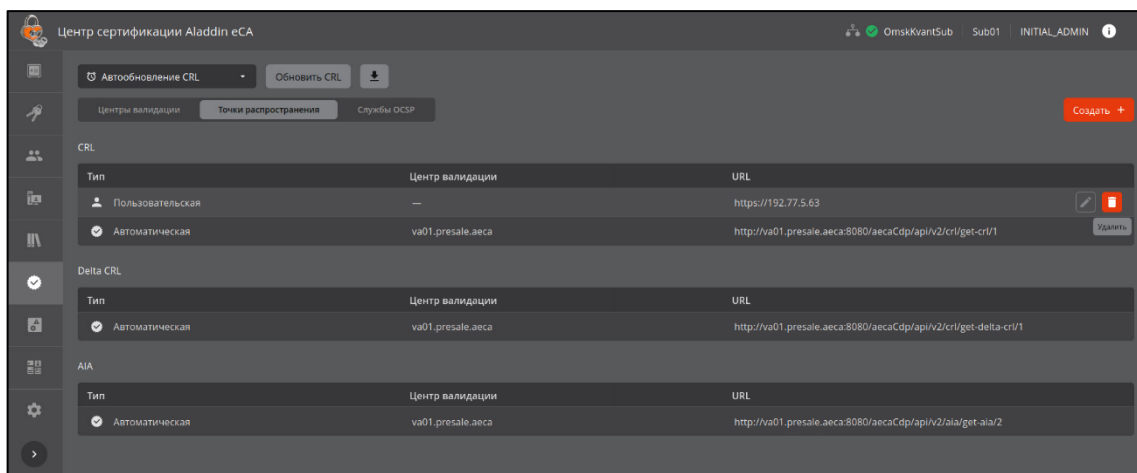


Рисунок 149 – Кнопка действий над пользовательской точкой распространения (Удалить)

- В открывшемся окне (см. Рисунок 150) подтвердите действие, нажав кнопку <Удалить>.

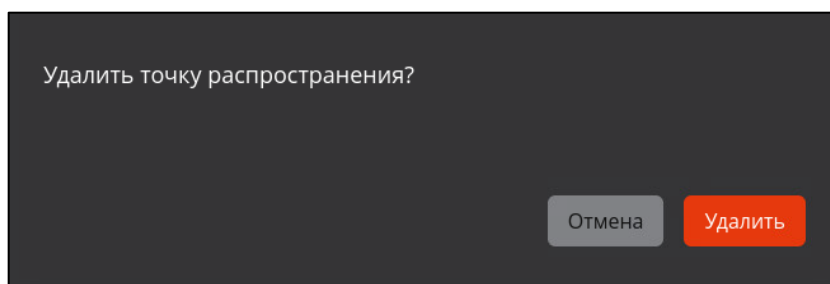


Рисунок 150 – Окно подтверждения удаления пользовательской точки

- В результате успешного удаления пользовательской точки распространения администратор будет уведомлён соответствующим сообщением (см. Рисунок 151).

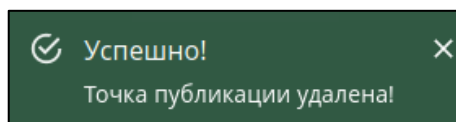


Рисунок 151 – Сообщение об успешном удалении пользовательской точки публикации

7.9.4 Вкладка «Службы OCSP»

- Данная вкладка (см. Рисунок 152) предназначена для просмотра автоматических точек распространения, зарегистрированных Центров валидации Aladdin Enterprise Certificate Authority (на вкладке «Центры валидации»).
- Информация о службах OCSP отображена в табличной форме с указанием:
 - типа службы OCSP;
 - центра валидации – имя сервера (hostname) Центра валидации Aladdin Enterprise Certificate Authority, которому принадлежит служба OCSP;
 - URL – ip-адреса сервера, где развёрнута служба OCSP.

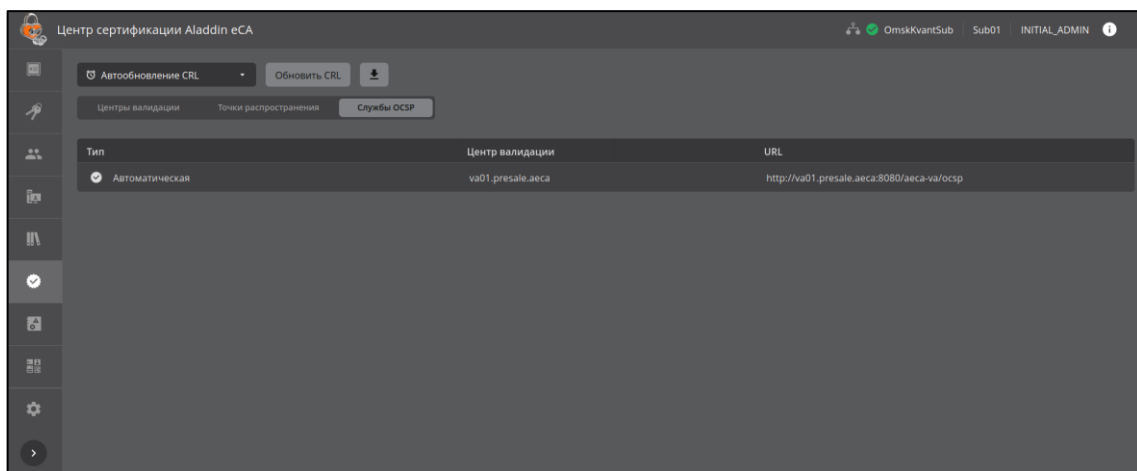


Рисунок 152 – Окно вкладки «Службы OCSP» в разделе «Центры валидации»

7.9.5 Настройка технического решения «Центра валидации»

7.9.5.1 С использованием web-сервера Nginx

для ОС РЕД ОС 7.3 и Astra Linux SE 1.7

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

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

РЕД ОС 7.3 `sudo dnf install nginx`

Astra Linux SE 1.7 `sudo apt install nginx`

- Запустите установленный web-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте web-сервер в автозагрузку, выполнив команду:

```
systemctl is-enabled nginx
```

- Создайте файл конфигурации, выполнив команду:

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

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

```
server {
    listen 80;
    server_name localhost;

    location /crl-dp/ {
        root /var/www;
```

```
    autoindex off;
}
}
```

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

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

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

- Только для ОС РЕД ОС 7.3! Расширьте политики selinux, выполнив команду:

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

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

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

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

```
sudo systemctl restart nginx
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.9.6 настоящего руководства, для распространения следующие файлы:

- список отозванных сертификатов CRL;
- список изменений последнего опубликованного CRL – DeltaCRL;
- сертификаты центров сертификации.

- Разместите в каталоге `/var/www/crl-dp` полученные с помощью скрипта файлы CRL, Delta CRL и/или AIA.

- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

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

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

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

для ОС АЛЪТ 8 СП

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

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

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

- Запустите установленный web-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте web-сервер в автозагрузку, выполнив команду:


```
systemctl is-enabled nginx
```

- Создайте файл конфигурации, выполнив команду:

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

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

```
server {  
    listen 80;  
    server_name localhost;  
  
    location /crl-dp/ {  
        root /var/www;  
        autoindex off;  
    }  
}
```

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

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

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

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

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

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

```
sudo systemctl restart nginx
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.9.6 настоящего руководства, для распространения следующие файлы:

- список отозванных сертификатов CRL;
- список изменений последнего опубликованного CRL – DeltaCRL;
- сертификаты центров сертификации.

- Разместите в каталоге `/var/www/crl-dp` полученные с помощью скрипта файлы CRL, Delta CRL и/или AIA.

- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

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

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

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

7.9.5.2 С использованием web-сервера Apache

для ОС Astra Linux SE 1.7

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

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

```
sudo apt install apache2
```

- Активируйте модули, выполнив команды:

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

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

```
sudo systemctl is-enabled apache2
```

- Создайте файл конфигурации, выполнив команду:

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

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

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

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

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

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

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

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

- Активируйте модуль `headers`, выполнив команду:

```
sudo a2enmod headers
```

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

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

- Выполните перезапуск web-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart apache2
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.9.6 настоящего руководства, для распространения следующие файлы:

- список отозванных сертификатов CRL;
- список изменений последнего опубликованного CRL – DeltaCRL;
- сертификаты центров сертификации.

- Разместите в каталоге `/var/www/crl-dp` полученные с помощью скрипта файлы CRL, Delta CRL и/или AIA.

- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

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

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

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

для ОС РЕД ОС 7.3

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

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

```
sudo dnf install httpd
```

- Установите дополнительный модуль для использования протокола `ssl` в `apache`, выполнив команду с правами суперпользователя (от имени пользователя `root`, либо с использованием `sudo`):

```
sudo dnf install mod_ssl
```

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

```
sudo systemctl is-enabled httpd
```

- Создайте файл конфигурации, выполнив команду:

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

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

```
<VirtualHost *:80>
    ServerName localhost

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

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

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

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

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

- Выполните перезапуск web-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart httpd
```

- Экпортируйте из Центра сертификации, согласно подразделу 7.9.6 настоящего руководства, для распространения следующие файлы:

- список отозванных сертификатов CRL;
- список изменений последнего опубликованного CRL – DeltaCRL;
- сертификаты центров сертификации.

- Разместите в каталоге `/var/www/crl-dp` полученные с помощью скрипта файлы CRL, Delta CRL и/или AIA.

- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

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

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

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

для ОС АЛБТ 8 СП

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

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

```
sudo apt-get install apache2-mod_http2
```

- Создайте файлы:

- `/etc/httpd2/conf/mods-available/http2.load`, выполнив команду с правами суперпользователя:

```
sudo cat /etc/httpd2/conf/mods-available/http2.load
```

Внесите следующий текст в созданный файл:

```
LoadModule http2_module /usr/lib64/apache2/modules/mod_http2.so
```

- `/etc/httpd2/conf/mods-available/http2.conf` выполнив команду с правами суперпользователя:

```
sudo cat /etc/httpd2/conf/mods-available/http2.conf
```

Внесите следующий текст в созданный файл:

```
/etc/httpd2/conf/mods-available/http2.conf
# mod_http2 doesn't work with mpm_prefork
<IfModule !mpm_prefork>
    Protocols h2 h2c http/1.1

    # # HTTP/2 push configuration
    #
    # H2Push          on
    #
    # # Default Priority Rule
    #
    # H2PushPriority * After 16
    #
    # # More complex ruleset:
    #
    # H2PushPriority *          after
    # H2PushPriority text/css   before
    # H2PushPriority image/jpeg after 32
    # H2PushPriority image/png  after 32
    # H2PushPriority application/javascript interleaved
    #
    # # Configure some stylesheet and script to be pushed by the webserver
    #
    # <FilesMatch "\.html$">
    #     Header add Link "</style.css>; rel=preload; as=style"
    #     Header add Link "</script.js>; rel=preload; as=script"
    # </FilesMatch>
    # Since mod_http2 doesn't support the mod_logio module (which provide the %O
format),
```

```
# you may want to change your LogFormat directive as follow:
#
# LogFormat "%v:%p %h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
# LogFormat "%h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
combined
# LogFormat "%h %l %u %t \"%r\" %>s %B" common
</IfModule>
```

- Активируйте модули, выполнив команды:

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

- Включите https порт по умолчанию, выполнив команду с правами суперпользователя:

```
sudo a2enport https
```

- Создайте файл конфигурации, выполнив команду:

```
nano /etc/httpd2/conf/sites-available/crl-dp.conf
```

Добавьте в созданный конфигурационный файл `/etc/httpd2/conf/sites-available/crl-dp.conf` следующее содержимое:

```
<VirtualHost *:80>
    ServerName localhost

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

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

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

- Создайте в каталоге `/etc/httpd2/conf/sites-enabled` ссылку на созданный конфигурационный файл `/etc/httpd2/conf/sites-available/crl-dp.conf`, выполнив команду:

```
ln -s /etc/httpd2/conf/sites-available/crl-dp.conf /etc/httpd2/conf/sites-enabled/
```

- Удалите из каталога `/etc/httpd2/conf/sites-enabled` ссылку на файл `000-default.conf`, выполнив команду:

```
sudo rm /etc/httpd2/conf/sites-enabled/000-default.conf
```

- Активируйте модуль `headers`, выполнив команду:

```
a2enmod headers
```

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

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

- Выполните перезапуск web-сервера Apache для применения изменений конфигурации, выполнив команду:

```
sudo systemctl restart httpd2
```

- Экспортируйте из Центра сертификации, согласно подразделу 7.9.6 настоящего руководства, для распространения следующие файлы:

- список отозванных сертификатов CRL;
- список изменений последнего опубликованного CRL – DeltaCRL;
- сертификаты центров сертификации.

- Разместите в каталоге `/var/www/crl-dp` полученные с помощью скрипта файлы CRL, Delta CRL и/или AIA.

- Убедитесь, что файлы CRL, Delta CRL или AIA доступны для скачивания. Для этого необходимо на любом другом АРМ, для которого сервер пользовательской точки распространения CRL DP является достижимым, перейти в браузере по ссылке:

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

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

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

7.9.6 Получение файлов CRL, Delta CRL и AIA

7.9.6.1 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:

- ID Центра Сертификации, файлы CRL, Delta CRL и AIA которого будут экспортированы (параметр `CA_ID` можно выделить, как крайний параметр URL-адреса Центра сертификации, например: `https://sub01.presale.aeca/access-certificates/4a660253-09bf-4cc6-a363-871a9c4cbd8c`, где `4a660253-09bf-4cc6-a363-871a9c4cbd8c` – идентификатором ЦС);
- путь к папке хранения сертификата для авторизации в ЦС (параметр `CERTIFICATE_PATH`), в случае использования значений по умолчанию для этих параметров необходимо создать каталог `/opt/aecaCa/dist/account`;
- путь к файлу контейнера p12 для авторизации в ЦС (параметр `P12_PATH`);

- пароль от контейнера p12 для авторизации в ЦС (параметр `P12_PASSWORD`);
- путь к файлу сертификата для авторизации в ЦС (параметр `CERT_PATH`), в случае использования значений по умолчанию необходимо создать каталог `/opt/aecaCa/dist/account`;
- путь к файлу ключа сертификата для авторизации в ЦС (параметр `KEY_PATH`), в случае использования значений по умолчанию для этих параметров необходимо создать каталог `/opt/aecaCa/dist/account`;
- хост ЦС (может быть как localhost, так и внешний адрес, параметр `SERVICE_HOST`);
- путь к папке экспорта файлов CRL, Delta CRL и AIA (параметр `DOWNLOAD_PATH`);
- задержка между проверками статуса в секундах (параметр `STATUS_CHECK_DELAY`).
- Для экспорта файлов запустите скрипт, выполнив команду (с правами суперпользователя или sudo):

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

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

7.9.6.2 Получение файлов посредством использования методов REST API

- Для получения файлов CRL, Delta CRL и AIA необходимо аутентифицироваться в программе по сертификату доступа. Аутентификация осуществляется путем обращения к методу идентификации и аутентификации по сертификату доступа публичного API (см. описание метода и пример его использования в разделе 1.1 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020-01 32 01-2).

В результате аутентификации по сертификату доступа будет получен маркер доступа, который будет использоваться далее.

Если при дальнейшем использовании маркера доступа в ответе на обращение к методам API будет содержаться сообщение об ошибке «Срок действия JWT токена истек», необходимо использовать метод обновления маркера доступа (см. описание метода и пример его использования в разделе 1.2 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020-01 32 01-2).

- Для получения файла CRL необходимо использовать метод получения CRL по идентификатору Центра сертификации (см. описание метода в разделе 6.7 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API» RU.АЛДЕ.03.01.020-01 32 01-2).

Пример использования метода (через утилиту curl):

```
curl -k --location 'https://192.168.111.100/export-service/api/v2/public/export/certificate-authorities/e5291624-fac6-4d5f-ae7-d57be0372489/crl' --header 'Cookie: token=eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiaOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZGQ1MGE3ZjUiLCJpYXQiOiJlZ3M0MTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyycCqr89HeahIsnsn_vUXxeSqwFV1WRJUtpIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMBuwHmjX4aODGnPWCSFc18DUCqFA-85BTYgvGL5ns5kXfCe2Wxmr7oPj-7XMAzBI98JydXkLEbmRx7F10TeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXegC0xEv2UK8mhF7Um4od9B1LW1CuNqKExyqTGr1DDKJcYjowBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm_scA_l-gARBh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

`192.168.111.100` – IP-адрес хоста АЕСА-СА;


```
curl -k --location 'https://192.168.111.100/export-  
service/api/v2/public/export/certificate-authorities/e5291624-fac6-4d5f-ae7-  
d57be0372489/certificate' --header 'Cookie:  
token=eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZG  
Q1MGE3ZjUiLCJpYXQiOiJlMzMTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn_vUXxeSqw  
FV1WRJUtPIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-  
85BTYgvGL5ns5kXfCe2Wxmr7oPj-  
7XMAzBI98JydXkLEbmRx7F10TeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXeg  
C0xEv2UK8mhF7Um4od9B1LW1CuNqKExyqTGr1DDKJcYjowBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm  
_scA_1-gARbh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA'
```

где:

192.168.111.100 – IP-адрес хоста АЕСА-СА;

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

eyJhbGciOiJSUzUxMiJ9.eyJzZXNzaW9uSWQiOiI2Njc3NGU1ZS1jODkzLTRmOWQtODM4Yy1lMzQzZG
Q1MGE3ZjUiLCJpYXQiOiJlMzMTAzMTIzODAsImV4cCI6MTcxMDMxMjU2MH0.MyyCQr89HeahIsnsn_vUXxeSqw
FV1WRJUtPIkVMTbxq7BrzjG1cjFNJ9rEXx9jGKeSaTMbuwhmjX4aODGnPWCSFc18DUCqFA-
85BTYgvGL5ns5kXfCe2Wxmr7oPj-
7XMAzBI98JydXkLEbmRx7F10TeNW1ZY3JKwKvi9yFxbWrojB3yNq2ak39cvNj4AFKCEBF0nE8UxKPoyXKDXeg
C0xEv2UK8mhF7Um4od9B1LW1CuNqKExyqTGr1DDKJcYjowBh49pQFAc3mG_bv7pBtTY7_vwuVNAelBAqj1kUm
_scA_1-gARbh-oaU_ZTGXNe-zpXKIiTDM-uFXLTuImZXRA – маркер доступа, полученный в результате аутентификации.

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

7.9.7 Параметры точек распространения в сертификате

7.9.7.1 Указание точек распространения списка отозванных сертификатов CRL

В создаваемых продуктом сертификатах субъектов в разделе «x509v3 extensions» в подразделе «x509v3 CRL Distributions Points» должны быть указаны URL-адреса точек распространения CRL в соответствии с перечнем и порядком точек распространения CRL, отображаемым в разделе «Центры валидации» – вкладка «Точки распространения» – группа «CRL».

7.9.7.2 Указание точек распространения списка изменений последнего опубликованного CRL

В создаваемых продуктом сертификатах субъектов в разделе «x509v3 extensions», в подразделе «x509v3 Freshest CRL» указаны URL-адреса точек распространения Delta CRL в соответствии с перечнем и порядком, отображаемым в разделе «Центры валидации» – вкладка «Точки распространения» – группа «Delta CRL».

7.9.7.3 Указание точек распространения сертификатов издающих Центров сертификации

В создаваемых продуктом сертификатах субъектов в разделе «x509v3 extensions», в подразделе «Authority Information Access», в полях «CA Issuers» указаны URL-адреса точек распространения AIA в соответствии с перечнем и порядком, отображаемым в разделе «Центры валидации» – вкладка «Точки распространения» – группа «AIA».

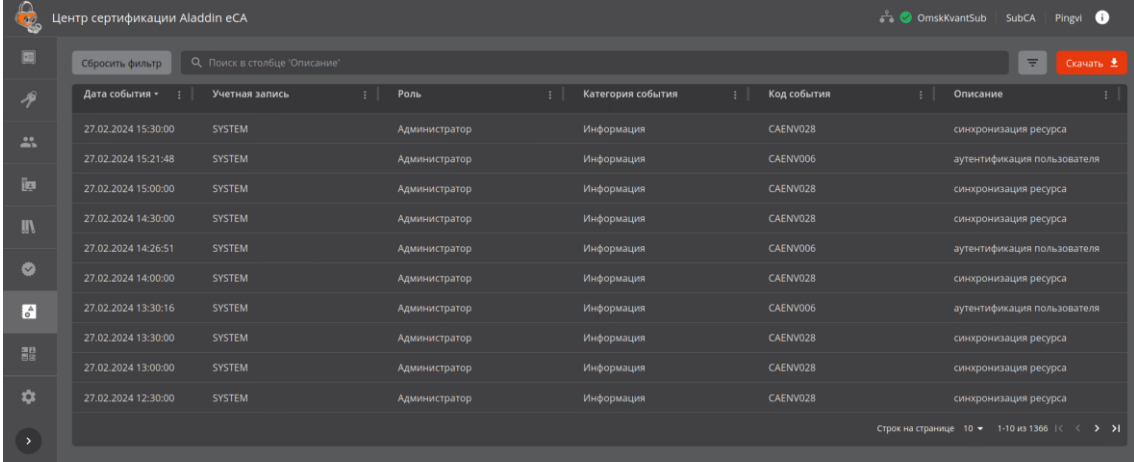
7.9.7.4 Указание на службы OCSP

В создаваемых продуктом сертификатах субъектов в разделе «x509v3 extensions», в подразделе «Authority Information Access», в полях «OCSP» указаны URL-адреса служб OCSP в соответствии с перечнем и порядком служб OCSP, отображаемым в разделе «Центры валидации» – вкладка «OCSP».

7.10 Раздел «Журнал событий»

Раздел «Журнал событий» предназначен для полного или выборочного просмотра истории событий сервера, формирования и выгрузки журнала событий по заданным критериям.

- Переход в раздел «Журнал событий» (см. Рисунок 153) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 38).
- Данный раздел доступен только в режиме администратора.



Скриншот интерфейса «Журнал событий» в Центре сертификации Aladdin eCA. Вверху экрана отображены логотип, название «Центр сертификации Aladdin eCA», статус подключения к серверу (OmskKvantSub, SubCA, Ping) и кнопка «Скачать». В центре находится таблица с заголовками: «Дата события», «Учетная запись», «Роль», «Категория события», «Код события» и «Описание». В таблице перечислены события от 27.02.2024 15:30:00 до 27.02.2024 12:30:00, все с ролью «Администратор» и категорией «Информация». Внизу экрана отображены параметры пагинации: «Строк на странице 10», «1-10 из 1366» и кнопки для навигации.

Дата события	Учетная запись	Роль	Категория события	Код события	Описание
27.02.2024 15:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 15:21:48	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 15:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 14:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 14:26:51	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 14:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 13:30:16	SYSTEM	Администратор	Информация	CAENV006	аутентификация пользователя
27.02.2024 13:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 13:00:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса
27.02.2024 12:30:00	SYSTEM	Администратор	Информация	CAENV028	синхронизация ресурса

Рисунок 153 – Экран раздела «Журнал событий»


- Программный компонент «Центр сертификации Aladdin eCA» оснащен функцией сбора диагностической информации, которая получает и аккумулирует записи о событиях для последующего анализа в базе данных «аесаса» (имя базы данных по умолчанию, конфигурация базы данных указана в файле `/opt/aecaCa/scripts/config.sh`).

- В процессе работы программного компонента «Центр сертификации Aladdin eCA» системные службы и компоненты приложения записывают все производимые действия. Произошедшие события записываются в файлы регистрации событий с расширением `.log`, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaCa/dist/logs/'имя сервиса'`. Доступ к папке осуществляется от имени администратора ОС. Срок хранения файлов регистрации событий составляет 10 дней с ограничением размера в 50 Мб.

- На данном экране (см. Рисунок 153) отображаются все произошедшие события (из списка **Ошибка! Источник ссылки не найден.**) в виде таблицы с пагинацией.

- На экране сервиса публикации отображены информационные элементы (табличные поля):
 - дата события;
 - учётная запись – логин учётной записи, действия которой повлекли событие;
 - роль (администратор, оператор);
 - категория события (информационное, ошибка);
 - код события (см. **Ошибка! Источник ссылки не найден.**);
 - описание.
- Доступны следующие операции в разделе «Журнал событий»:
 - скачать журнал событий в формате `.csv` файла;
 - полный или выборочный просмотр журнала событий.

7.10.1 Управление экранной таблицей

- Для каждой колонки экранной таблицы (справа от названия заголовка) доступна кнопка управления действиями  «Действия в колонке». По нажатию данной кнопки разворачивается меню (см. Рисунок 154) в котором возможно (в зависимости от применённых ранее действий – фильтр, сортировка, изменение ширины, скрытие колонки):

- очистить сортировку, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
- сортировать по возрастанию/убыванию значений в колонке;
- очистить фильтр, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
- отфильтровать, отобразив поле для выбора критерия фильтрации;
- сбросить размер колонок, сбросив ширину колонок к значению «по умолчанию»;
- скрыть колонку из отображаемых на экране;
- показать все колонки, отобразив на экране ранее скрытые колонки.

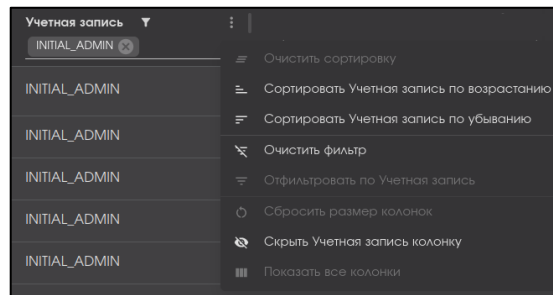
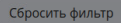


Рисунок 154 – Кнопка <Действия в колонке>

- Для сброса применённых фильтров следует нажать кнопку <Сбросить фильтр>  в результате чего в экранной таблице раздела «Журнал событий» будут отображены все произошедшие события.

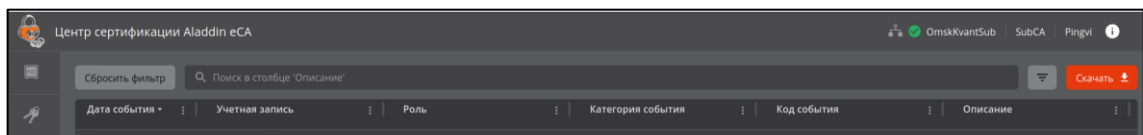



Рисунок 155 – Кнопка <Сбросить фильтр>

7.10.2 Фильтрация событий

- Для выборочного просмотра событий на экране раздела «Журнал событий» 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 156):
 - дата события. Выберите за какой период отразить события на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
 - учётная запись. Выберите учётные записи, чьи действия повлекли события;
 - роль. Выберите роль учётных записей, чьи действия повлекли события;
 - выберите категории событий для отображения (ошибка, информация);
 - выберите коды событий для отображения.

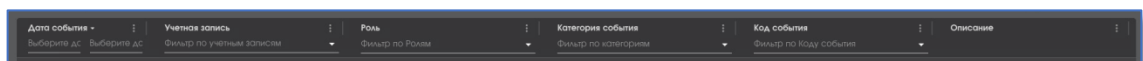



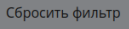


Рисунок 156 – Поля фильтра заголовков экранной таблицы

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

- Заголовки таблицы, для которых применён фильтр, будут отмечены знаком .
- Для очистки применённых фильтров для каждого заголовка колонки:
 - нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 154);
- Для полной отмены всех применённых фильтров по всем колонкам воспользуйтесь кнопкой <Сбросить фильтр>  на экране раздела «Журнал событий».

7.10.3 Сортировка событий

Средства сортировки событий на экране раздела «Журнал событий» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 157):

- дата события – упорядочивание осуществляется от старых к новым или от новых к старым записям событий;
- учётная запись – упорядочивание осуществляется в алфавитном порядке;
- роль – упорядочивание осуществляется в алфавитном порядке;
- код события – упорядочивание данных в порядке возрастания или убывания кода.

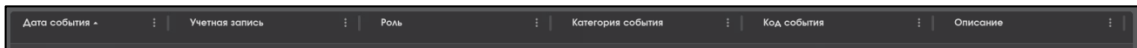




Рисунок 157 – Поля сортировки содержимого экрана раздела «Журнал событий»

- Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки> (см. п. 7.10.1).
- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок колонки таблицы.
- Активное поле таблицы, по которому выполнена сортировка, обозначено знаком  с правой стороны от заголовка таблицы.
- Для сброса сортировки в каждой колонке:
 - нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить сортировку» (см. Рисунок 154);
 - или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

7.10.4 Поиск событий

Строка поиска (см. Рисунок 159) предназначена для поиска записей событий в журнале по содержимому колонки «Описание». Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

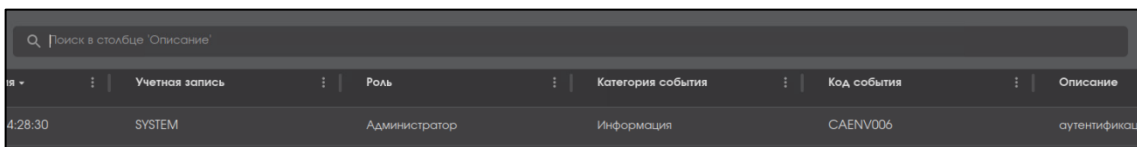


Рисунок 158 – Поисковая строка в разделе «Журнал событий»

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

7.10.5 Экспорт журнала событий


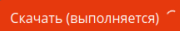
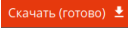
- Определите параметры экспортируемого журнала событий, для этого настройте фильтры в соответствии с заданными критериями:
 - датой (выбранным периодом);
 - учётной записью. Значение учётной записи пользователя и его роли записываются в момент совершения события. В случае редактирования учётной записи пользователя (изменения отображаемого имени или роли учётной записи) запись события остаётся неизменной;
 - ролью;
 - категорией события;
 - кодом события.
- Без применения фильтров, будут экспортированы все события.
- Для выгрузки журнала событий нажмите кнопку <Скачать>, расположенную на верхней панели экрана раздела «Журнал событий». Кнопка меняет своё состояние в зависимости от статуса процесса:
 - скачать  – система готова к новому формированию и скачиванию журнала событий;
 - скачивание выполняется  – начинается подготовка файла, содержащего записи журнала событий, соответствующие критериям фильтра или слову для поиска (при отсутствии заданных в фильтре или строке поиска значений будут экспортированы все записи журнала событий). Нажатие на кнопку в текущем состоянии не повлечёт никаких действий;
 - скачать (готово)  – файл журнала событий готов для скачивания. Нажатие на кнопку запускает скачивание файла журнала событий по указанному пути (в соответствии с настройками браузера). После завершения скачивания файла, статус кнопки возвращается в состояние «Скачать».
- Выгруженный файл имеет формат .csv, содержимое файла представлено в кодировке UTF-8 с разделителем полей “;” и доступно для открытия любым текстовым редактором (рекомендуемая программа просмотра записей журнала событий – MS Exel).
- Время хранения записей в журнале событий составляет 180 дней по умолчанию с момента создания журнала (см. п. 7.10.6 настоящего руководства).
- Возможные сообщения журнала событий приведены в **Ошибка! Источник ссылки не найден..**

Таблица 14 – Сообщения журнала событий

событие, вызвавшее запись в журнал	категория события	код события	описание события
запуск службы	CAENV000	INFO	запуск службы:<наименование сервиса>:<параметры запуска если есть>
остановка службы	CAENV001	INFO	остановка службы:<наименование сервиса>
импорт лицензии	CAENV002	INFO	импорт лицензии:<CN-Корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>
ошибка импорта лицензии	CAENV003	ERROR	ошибка импорта лицензии:<CN-Корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>:<текст ошибки>
проверка лицензии	CAENV004	INFO	аутентификация пользователя:<имя>:<роль>:<сер.номер сертификата>

ошибка проверка лицензии	CAENV005	ERROR	ошибка проверки лицензии:<CN-Корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>:<текст ошибки>
аутентификация пользователя	CAENV006	INFO	аутентификация пользователя:<имя>:<роль>:<сер.номер сертификата>
ошибка аутентификации	CAENV007	ERROR	ошибка аутентификации:<сер.номер сертификата>:<текст ошибки>
активация центра сертификации	CAENV008	INFO	активация центра сертификации:<CN>:<DNS>
ошибка активации	CAENV009	ERROR	ошибка активации центра сертификации:<CN>:<DNS>:<текст ошибки>
создание запроса на сертификат ЦС	CAENV010	INFO	успешное создание запроса на сертификат центра сертификации:<CN>:<DNS>
ошибка создания запроса	CAENV011	ERROR	ошибка создания запроса на сертификат центра сертификации:<CN>:<DNS>:<текст ошибки>
импорт сертификата центра сертификации	CAENV012	INFO	успешный импорт сертификата центра сертификации и цепочки сертификатов, успешная проверка сопоставления открытых ключей:<CN>:<CN-Корневого>

событие, вызвавшее запись в журнал	категория события	код события	описание события
ошибка импорта сертификата центра сертификации	CAENV013	ERROR	ошибка импорта сертификата центра сертификации:<CN>:<CN-Корневого>:<текст ошибки>
выпуск сертификата	CAENV014	INFO	выпуск сертификата:<CN>:<SAN>:<шаблон>:<вид операции>:<сценарий>:<ресурсная система>:<алгоритм> где: <вид операции> - один из вариантов "PKCS12", "по запросу"; <сценарий> - один из вариантов "подпись запроса Подчиненного ЦС", "сертификат учетной записи", "сертификат субъекта"
ошибка выпуска сертификата	CAENV015	ERROR	ошибка выпуска сертификата:<CN>:<SAN>:<шаблон>:<вид операции>:<сценарий>:<ресурсная система>:<алгоритм>:<текст ошибки>
регистрация центра валидации	CAENV016	INFO	регистрация центра валидации:<указанный адрес центра валидации>
ошибка регистрации	CAENV017	ERROR	ошибка регистрации центра валидации:<указанный адрес центра валидации>:<текст ошибки>
активация OCSP центра валидации	CAENV018	INFO	активация OCSP:<адрес центра валидации>:<сер.номер сертификата>
ошибка активации	CAENV019	ERROR	ошибка активации OCSP:<адрес центра валидации>:<сер.номер сертификата>:<текст ошибки>
настройка периода CRL	CAENV020	INFO	настройка периода CRL:<периода CRL>:<перекрытие CRL>:<период DeltaCRL>
ошибка настройки	CAENV021	ERROR	ошибка настройки периода CRL:<периода CRL>:<перекрытие CRL>:<период DeltaCRL>:<текст ошибки>
публикация CRL	CAENV022	INFO	публикация CRL:<номер CRL>:<срок действия>:<адрес точки публикации>
ошибка публикации	CAENV023	ERROR	ошибка публикации CRL:<номер CRL>:<срок действия>:<адрес точки публикации>:<текст ошибки>
добавление ресурсной системы	CAENV024	INFO	добавление ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>
ошибка добавления	CAENV025	ERROR	ошибка добавления ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>:<текст ошибки>

событие, вызвавшее запись в журнал	категория события	код события	описание события
изменение ресурсной системы	CAENV026	INFO	изменение ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>
ошибка изменения	CAENV027	ERROR	ошибка изменения ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>:<текст ошибки>
синхронизация ресурса	CAENV028	INFO	синхронизация ресурса:<наименование>:<кол-во субъектов>
ошибка синхронизации	CAENV029	ERROR	ошибка синхронизации ресурса:<наименование>:<кол-во субъектов>:<текст ошибки>
создание учетной записи	CAENV030	INFO	создание учетной записи:<лог.имя>:<роль>
ошибка создания	CAENV031	ERROR	ошибка создания учетной записи:<лог.имя>:<роль>:<текст ошибки>
изменение учетной записи	CAENV032	INFO	изменение учетной записи:<лог.имя>:<роль>:<сер.номер сертификата>
ошибка изменения	CAENV033	ERROR	ошибка изменения учетной записи:<лог.имя>:<роль>:<сер.номер сертификата>:<текст ошибки>
сохранение прав оператора	CAENV034	INFO	ввод прав оператора:<лог.имя>:<[список прав]>
ошибка сохранения	CAENV035	ERROR	ошибка сохранения прав оператора:<лог.имя>:<[список прав]>:<описание ошибки>
установка сертификата web-сервера	CAENV036	INFO	установка сертификата web-сервера:<сер.номер сертификата>
ошибка установки	CAENV037	ERROR	ошибка установки сертификата web-сервера:<сер.номер сертификата>:<описание ошибки>
изменение списка издателей	CAENV038	INFO	изменение списка разрешенных издателей:<имя издателя>:<"добавлен" или "удален">
ошибка изменения	CAENV039	ERROR	ошибка изменения списка разрешенных издателей:<имя издателя>:<"добавлен" или "удален">:<текст ошибки>
перезагрузка web-сервера	CAENV040	INFO	перезагрузка web-сервера
ошибка выполнения перезагрузки	CAENV041	ERROR	ошибка выполнения перезагрузки web-сервера:<описание ошибки>
подключение к ключевому носителю	CAENV042	INFO	подключение к ключевому носителю:<маркировка носителя>:<тип носителя>

событие, вызвавшее запись в журнал	категория события	код события	описание события
ошибка подключения	CAENV043	ERROR	подключение к ключевому носителю:<маркировка носителя>:<тип носителя>:<описание ошибки>
создание контейнера на ключевом носителе	CAENV044	INFO	создание контейнера на ключевом носителе:<маркировка носителя>:<ID-контейнера>:<алгоритм>
ошибка создания	CAENV045	ERROR	ошибка создания контейнера на ключевом носителе:<маркировка носителя>:<ID-сертификата>:<алгоритм>:<описание ошибки>
запись сертификата на ключевой носитель	CAENV046	INFO	запись сертификата на ключевой носитель:<маркировка носителя>:<ID-сертификата>
ошибка записи	CAENV047	ERROR	ошибка запись сертификата на ключевой носитель:<маркировка носителя>:<ID-сертификата>:<описание ошибки>
публикация сертификата в ресурсной системе	CAENV048	INFO	публикация сертификата в ресурсной системе:<ресурс>:<CN-субъекта>:<сер.номер сертификата>
ошибка публикации	CAENV049	ERROR	ошибка публикации сертификата в ресурсной системе:<ресурс>:<CN-субъекта>:<сер.номер сертификата>:<текст ошибки>
сохранение журнала в CSV	CAENV050	INFO	сохранение журнала в CSV:<фильтр>
ошибка сохранения	CAENV051	ERROR	ошибка сохранения журнала в CSV:<фильтр>:<текст ошибки>
генерация CRL	CAENV052	INFO	генерация CRL:<номер CRL>:<срок действия>
ошибка генерации	CAENV053	ERROR	ошибка генерации CRL:<номер CRL>:<срок действия>:<текст ошибки>
отправка уведомления на почту	CAENV054	INFO	отправка уведомления на почту:<CN>:<email>:<шаблон>
ошибка отправки	CAENV055	ERROR	ошибка отправки уведомления на почту:<CN>:<email>:<шаблон>:<текст ошибки>
отзыв сертификата	CAENV056	INFO	отзыв сертификата: после обновления: certSerialNumber: <ID-сертификата>
приостановка сертификата	CAENV057	INFO	приостановка сертификата: после обновления: certSerialNumber:<ID-сертификата>

событие, вызвавшее запись в журнал	категория события	код события	описание события
реактивация сертификата	CAENV058	INFO	активация сертификата: после обновления: certSerialNumber: <ID-сертификата>: revocationReason: <Причина отзыва>
начало удаления центра сертификации	CAENV059	INFO	начало удаления центра сертификации: после обновления: <CN>:<CN-Корневого или Подчиненного>, DNS<"суффикс различающегося имени">
окончание удаления центра сертификации	CAENV060	INFO	конец удаления центра сертификации: после обновления <CN>:<CN-Корневого или Подчиненного>, DNS<"суффикс различающегося имени">
ошибка при удалении центра сертификации	CAENV061	ERROR	ошибка удаления центра сертификации:<CN>:<CN-Корневого или Подчиненного>, DNS<"суффикс различающегося имени"> :<текст ошибки>
начало очистки журнала событий	CAENV064	INFO	Начало очистки журнала событий
окончание очистки журнала событий	CAENV065	INFO	Конец очистки журнала событий
ошибка при очистке журнала событий	CAENV066	ERROR	Ошибка очистки журнала события: <фильтр>:<текст ошибки>
начало архивации журнала событий	CAENV067	INFO	Начало архивации журнала событий
окончание архивации журнала событий	CAENV068	INFO	Конец архивации журнала событий
ошибка при архивации журнала событий	CAENV069	ERROR	Ошибка архивации журнала события: <фильтр>:<текст ошибки>
добавить шаблон сертификата в "Центр регистрации"	CAENV070	INFO	Добавить шаблон сертификата <наименование шаблона> в "Центр регистрации"
ошибка при добавлении шаблона сертификата в "Центр регистрации"	CAENV071	ERROR	Ошибка при добавлении шаблона сертификата <наименование шаблона> в "Центр регистрации"

событие, вызвавшее запись в журнал	категория события	код события	описание события
убрать шаблон сертификата в "Центр регистрации"	CAENV072	INFO	Убрать шаблон сертификата <наименование шаблона> в "Центр регистрации"
ошибка при уборке шаблона сертификата в "Центр регистрации"	CAENV073	ERROR	Ошибка при уборке шаблона сертификата <наименование шаблона> в "Центр регистрации"
успешная проверка контрольных сумм	CAENV074	INFO	Успешная проверка целостности исполняемых файлов.
неуспешная проверка контрольных сумм	CAENV075	ERROR	Проверка целостности исполняемых файлов прошла неуспешно: <список файлов, которые не удалось проверить>
распаковка ключей ЦС	CAENV076	INFO	Успешная проверка целостности контейнеров закрытых ключей центра сертификации при распаковке.
ошибка при распаковке ключей ЦС	CAENV077	ERROR	Неуспешная проверка целостности контейнеров закрытых ключей центра сертификации при распаковке: <текст ошибки>
скачан контейнер PKCS#12	CAENV078	INFO	Успешный экспорт контейнера закрытого ключа за пределы программы <серийный номер сертификата в контейнере>
скачен сертификат	CAENV079	INFO	Скачан сертификат
скачена цепочка сертификата	CAENV080	INFO	Скачана цепочка сертификата
экспорт запроса на сертификат ЦС	CAENV081	INFO	Успешный экспорт запроса на сертификат центра сертификации за пределы программы
ошибка экспорта запроса на сертификат ЦС	CAENV082	ERROR	Неуспешный экспорт запроса на сертификат центра сертификации за пределы программы

событие, вызвавшее запись в журнал	категория события	код события	описание события
назначение полномочий оператору	CAENV083	INFO	Успешное назначение полномочий оператору: <имя оператора>, <перечень групп, субъектов>
ошибка назначения полномочий оператору	CAENV084	ERROR	Ошибка назначения полномочий оператору: <имя оператора>, <перечень групп, субъектов>, <текст ошибки>.
ошибка экспорта контейнера PKCS#12	CAENV085	ERROR	Ошибка экспорта контейнера закрытого ключа за пределы программы <серийный номер сертификата в контейнере>
успешное создание резервной копии	CAENV086	INFO	Успешное создание резервной копии <путь к созданной резервной копии>
ошибка создания резервной копии	CAENV087	ERROR	Ошибка создания резервной копии: <текст ошибки>
успешное восстановление из резервной копии	CAENV088	INFO	Успешное восстановление из резервной копии <путь к использованной резервной копии>
ошибка восстановления из резервной копии	CAENV089	ERROR	Ошибка восстановления из резервной копии: <текст ошибки>

7.10.6 Архивирование и очистка журнала событий

- Программный компонент «Центр сертификации Aladdin eCA» обеспечивает настраиваемое архивирование событий с одновременной очисткой Журнала событий в части заархивированных событий.
- Для настройки параметров архивации и очистки отредактируйте переменные окружения, используемые сервисом logs-service в конфигурационном файле `/opt/aecaCa/scripts/config.sh`:
 - `archive_millis_ago` – время хранения событий (по умолчанию 180 дней) в миллисекундах. Записи со сроком давности большим или равным времени хранения будут заархивированы;
 - `archive_cron` – периодичность запуска архивации (значение указывается в формате CRON-выражения, значение по умолчанию – '0 0 0 1 * *'). По умолчанию процесс архивации будет запущен при наступлении первого числа каждого месяца;
 - `archive_path` – путь сохранения сформированного архива.
- Архив в формате .zip, содержащий .csv файл, с именем `logs-<дата и время создания архива>.zip` будет сохранён на сервере, где развёрнут Центр сертификации, в папке (по умолчанию) `/opt/aecaCa/dist/archive`.

7.11 Раздел «Шаблоны»

Расширить возможности Центра сертификации возможно при помощи создания специализированных индивидуальных шаблонов сертификатов.

- Переход в раздел «Шаблоны» (см. Рисунок 159) осуществляется через боковое меню, расположенное слева на экране (см. Рисунок 38).
- Данный раздел доступен только для учётной записи с ролью «Администратор».

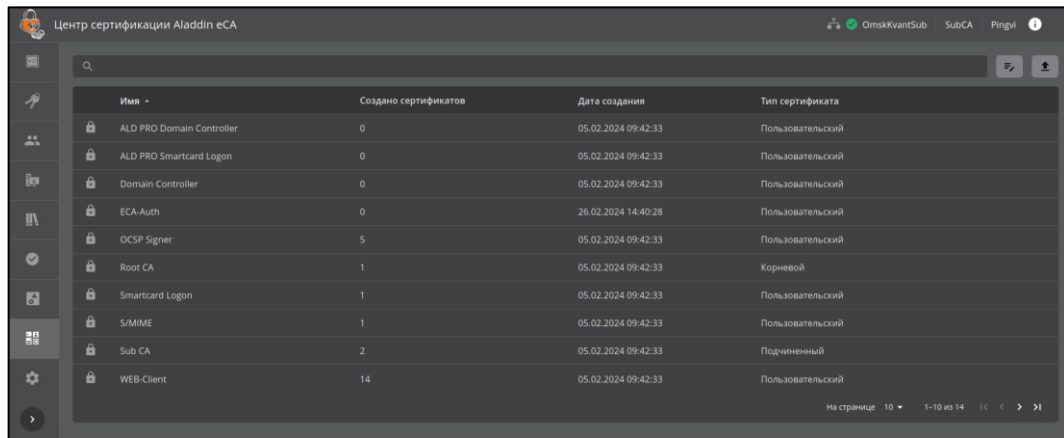





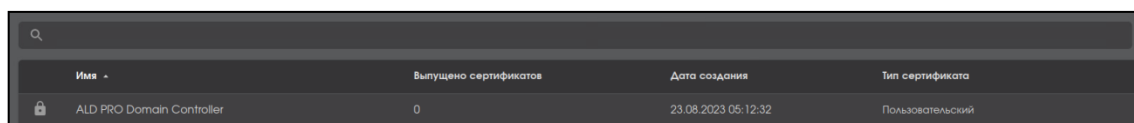
Рисунок 159 – Экран раздела «Шаблоны»

- На экранной таблице раздела «Шаблоны» отображены следующие колонки:
 - условное обозначение вида шаблона:
 -  – предустановленные по умолчанию шаблоны, созданные в момент установки Центра сертификации Aladdin eCA. Данный вид шаблонов не подлежит редактированию;
 -  – клонированные шаблоны для редактирования с целью создания нового шаблона с заданными параметрами;
 -  – импортированные шаблоны (например, из MS CS).

- имя – содержит название шаблона. В случае клонирования предустановленного шаблона или импортированного по умолчанию будет предложено имя в формате «Копия_имя исходного шаблона», при клонировании импортированного шаблона по умолчанию будет предложено имя шаблона в формате «`»;
 - выпущено сертификатов – количество сертификатов, выпущенных по данному шаблону;
 - дата создания – дата создания (клонирования) шаблона;
 - тип сертификата – определяет предназначение сертификата (корневой и подчинённый – для выпуска сертификата Центра сертификации, пользовательский – для выпуска сертификата субъекта).
- Просмотр набора полей предустановленных шаблонов возможен по клику «мышкой» на выбранный шаблон. Список предустановленных шаблонов:
 - Domain Controller;
 - Smartcard Logon;
 - WEB-Client;
 - WEB-Server;
 - S/MIME;
 - ECA-Auth;
 - ALD PRO Domain Controller;
 - ALD PRO Smartcard Logon;
 - OCSP Signer;
 - Root CA;
 - Sub CA.
 - Действия доступные над всеми видами шаблонов:
 - просмотр полного списка шаблонов или по результатам поиска;
 - загрузка новых шаблонов сертификатов MS CS;
 - клонирование (создание) шаблона;
 - поиск шаблонов;
 - сортировка шаблонов.
 - Действия доступные над клонированными и импортированными видами шаблонов:
 - редактирование шаблона;
 - сохранение результатов редактирования шаблона;
 - удаление шаблона или массовое удаление шаблонов.
 - Добавленные шаблоны доступны для использования на вкладке
 - Все шаблоны на экране раздела отображаются в виде таблицы с пагинацией.

7.11.1 Поиск шаблонов

Строка поиска (см. Рисунок 160) предназначена для поиска шаблонов в экранной таблице по содержимому колонки «Имя». Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.



Имя	Выпущено сертификатов	Дата создания	Тип сертификата
ALD PRO Domain Controller	0	23.08.2023 05:12:32	Пользовательский


Рисунок 160 – Поисковая строка в разделе «Шаблоны»

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

7.11.2 Сортировка шаблонов

- Средство сортировки списка шаблонов представлено элементом выбора направления сортировки в заголовках колонок экранной таблицы (см. Рисунок 159) – полями «Имя» (сортировка в алфавитном порядке), «Дата создания» (сортировка в порядке убывания/возрастания), «Тип сертификата» (упорядочивание по типу корневой/пользовательский).

- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок колонки таблицы.

- Активное поле таблицы, по которому выполнена сортировка, обозначено знаком  с правой стороны от заголовка таблицы.

- Для сброса сортировки в колонке несколько раз нажмите на заголовке колонки, для которой применена сортировка.

7.11.2.1 Карточка шаблона

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

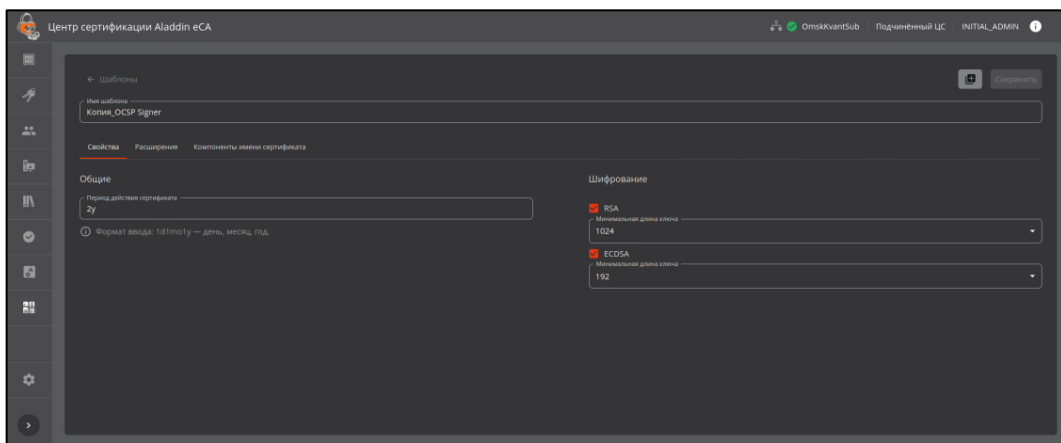


Рисунок 161 – Окно карточки шаблона

- В открывшемся окне администратору доступны:
 - кнопка возврата на вкладку «Шаблоны»;
 - кнопка «Клонировать» текущий шаблон;
 - кнопка «Сохранить» для записи изменений полей текущего шаблона, доступная для всех шаблонов, кроме предустановленных;
 - поле «Имя шаблона»;
 - информация, сформированная в виде вкладок «Свойства», «Расширения», «Компоненты имени субъекта».

7.11.2.2 Вкладка шаблона «Свойства»

На вкладке шаблона «Свойства» доступны поля (см. Рисунок 162):

- общие:
 - поле «Период действия сертификата». Формат ввода: 1d,1m,1y - час, день, месяц, год.
- шифрование:
 - RSA;

– ECDSA.

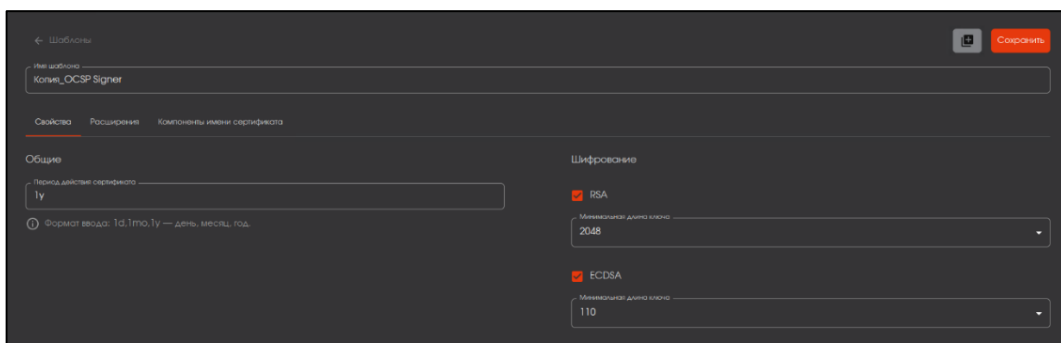


Рисунок 162 – Вкладка «Свойства» шаблона сертификата

7.11.2.3 Вкладка шаблона «Расширения»

На вкладке шаблона «Расширения» доступны:

- поле «Использование ключа»;
- поле «Расширенное использование ключа»;
- OID политики сертификата.

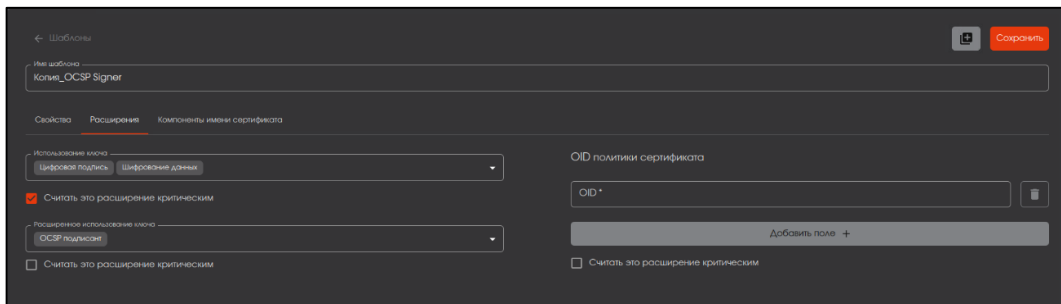


Рисунок 163 – Вкладка «Расширения» шаблона сертификата

7.11.2.4 Вкладка шаблона «Компоненты имени сертификата»

На вкладке шаблона «Расширения» доступны (см. Рисунок 164):

- отличительное имя субъекта;
- альтернативное имя субъекта.

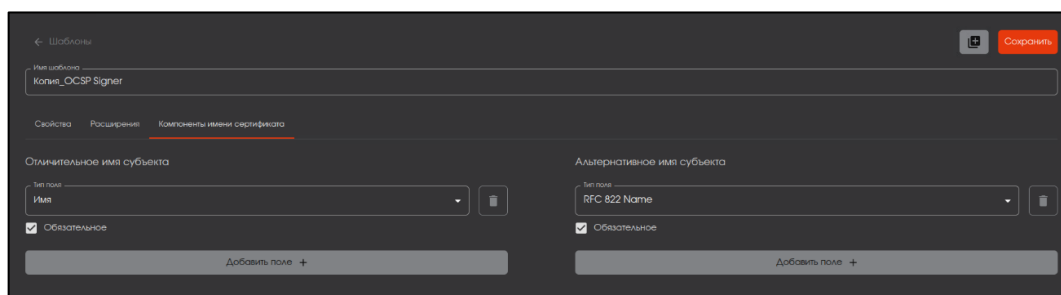



Рисунок 164 – Вкладка «Компоненты имени сертификата» шаблона сертификата

7.11.3 Создание нового шаблона

- Создание индивидуального шаблона возможно на базе существующих в системе шаблонов и состоит из трёх этапов:
 - клонирования выбранного шаблона;

- редактирование клонированного шаблона в соответствии со спецификой индивидуального шаблона;
- сохранения изменений, внесённых в клонированный шаблон.

7.11.3.1 Клонирование шаблона

- Выделите предустановленный шаблон на вкладке «Шаблоны» указателем «мышь».
- Нажмите появившуюся в строке кнопку <Клонировать> .
- В открывшемся окне подтверждения действия (см. Рисунок 165) при необходимости отредактируйте имя нового шаблона в соответствующем поле и нажмите кнопку <Клонировать> для создания нового шаблона на основании выбранного предустановленного шаблона.
 - Имя нового шаблона должно быть уникально, может содержать кириллицу, латиницу, любые символы, ограничители ввода между параметрами – пробелы, длина вводимого имени не ограничена с максимальной памятью до 1 Гб.
 - Если имя сохраняемого шаблона не уникально, ниже поля ввода имени шаблона появится текстовое предупреждение, и операция сохранения не будет выполнена.
 - Для прерывания действия клонирования шаблона нажмите кнопку <Отмена>.

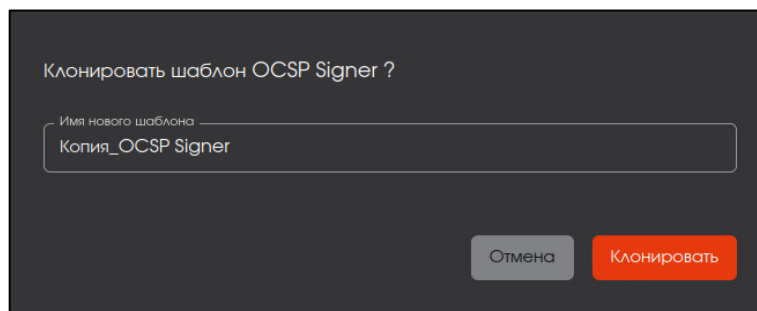


Рисунок 165 – Экран раздела меню «Шаблоны»

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

7.11.4 Редактирование шаблона

- Редактирование применимо для клонированного шаблона или импортированного (загруженного) шаблона MS CS.
- Редактирование предустановленных шаблонов недоступно.
- Для выбранного шаблона доступны для редактирования элементы, указанные в Таблица 15.

Таблица 15 – Поля шаблона, доступные для изменения через графический интерфейс

Название	Тип	Допустимые значения
Имя шаблона	Строка	Ограничение: 255 символов
Вкладка «Свойства»		
Раздел «Свойства»	Период действия сертификата	Строка *y *mo *d
Раздел «Шифрование»	Алгоритм ключа	Два чек-боксы <ul style="list-style-type: none"> • RSA • ECDSA Доступно включение обоих чек-боксов

Название		Тип	Допустимые значения
			одновременно
	Минимальная длина ключа	Два списка (список для каждого чек-бокса)	RSA: <ul style="list-style-type: none"> • 1024 • 1536 • 2048 • 3072 • 4096 • 6144 • 8192 ECDSA: <ul style="list-style-type: none"> • 192 • 224 • 256 • 384 • 521
Вкладка «Расширения сертификата»			
Использование ключа		Список с множественным выбором	<ul style="list-style-type: none"> • Цифровая подпись • Подтверждение подлинности • Шифрование ключей • Шифрование данных • Согласование ключей • Подпись сертификатов • Подпись списков отзыва • Только шифрование • Только расшифрование
Чек-бокс «Считать это расширение критическим» для поля «Использование ключа»		Чек-бокс	<ul style="list-style-type: none"> • Включен • Выключен
Расширенное использование ключа		Список с множественным выбором	<ul style="list-style-type: none"> • 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

Название	Тип	Допустимые значения
		<ul style="list-style-type: none"> кода ● Подписание MS документа ● Восстановление MS EFS ● Зашифрованная MS файловая система ● Подписание индивидуального MS кода ● Вход с MS смарт-картой ● OCSP подписант ● Подписание Adobe PDF ● Аутентификация PIV карты ● SCVP клиент ● SCVP сервер ● Домен SIP ● SSH клиент ● SSH сервер ● Аутентификация сервера ● Отметка времени ● ICAO подписание основного списка
Чек-бокс «Считать это расширение критическим» для поля «Расширенное использование ключа»	Чек-бокс	<ul style="list-style-type: none"> ● Включен ● Выключен
OID политики сертификата	Поле ввода	OID в формате, определенном стандартом ITU X.660
Чек-бокс «Считать это расширение критическим» для поля «OID политики сертификата»	Чек-бокс	<ul style="list-style-type: none"> ● Включен ● Выключен
Вкладка «Компоненты имени сертификата»		
Различающееся имя субъекта (SDN)	Список с множественным выбором	<ul style="list-style-type: none"> ● 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

Название	Тип	Допустимые значения
		<ul style="list-style-type: none"> Title Domain qualifier Description Unstructured address Unstructured name Email Address (E) Serial number
Чек-бокс «Обязательное» для полей различающегося имени субъекта (SDN)	Чек-бокс	<ul style="list-style-type: none"> Включен Выключен <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для каждого поля различающегося имени субъекта.</p>
Чек-бокс «Валидация» для полей различающегося имени субъекта (SDN)	Чек-бокс	<ul style="list-style-type: none"> Включен Выключен <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для включения у следующих полей различающегося имени субъекта:</p> <ul style="list-style-type: none"> Common name Organization
Альтернативное имя субъекта (SAN)	Список с множественным выбором	<ul style="list-style-type: none"> 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
Чек-бокс «Обязательное» для полей альтернативного имени субъекта (SAN)	Чек-бокс	<ul style="list-style-type: none"> Включен Выключен <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для каждого поля альтернативного имени субъекта.</p>
<ul style="list-style-type: none"> Чек-бокс «Валидация» для полей различающегося имени субъекта. Чек-бокс Включен Выключен 	Чек-бокс	<ul style="list-style-type: none"> Включен Выключен <p>Значение по умолчанию (при добавлении нового поля) – выключен. Доступен для включения у следующих</p>

Название	Тип	Допустимые значения
Доступен для каждого поля альтернативного имени субъекта. Чек-бокс «Валидация» для полей альтернативного имени субъекта (SAN)		полей альтернативного имени субъекта: <ul style="list-style-type: none"> • RFC 822 Name • DNS Name • MS UPN, User Principal Name • MS GUID, Globally Unique Identifier • Kerberos KPN, Kerberos 5 Principal Name

- При выборе параметров шифрования выбирается минимальная длина ключа, т.е. при выпуске сертификата по данному шаблону для выбора минимальной длины ключа будут доступны значения начиная от установленного минимального и все значения более установленного минимального значения длины ключа.

- Формат ввода периода действия сертификата: 1d,1m,1y - час, день, месяц, год.
- Используйте предлагаемые чек-боксы для дополнительной настройки шаблона сертификата:
 - Если включен чек-бокс «Считать это расширение критическим» для расширения, оно помечается как критическое при создании сертификата по данному шаблону (см. Рисунок 166). При обработке сертификата, имеющего атрибуты, для которых установлены чек-боксы «Считать это расширение критическим», могут быть отклонены, если правила обработки полей сертификатов системы не содержат отмеченных атрибутов (подробнее см. стандарт RFC 5280).

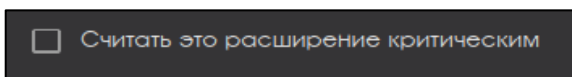


Рисунок 166 – Поле чек-бокса «Считать это расширение критическим»

- При включенном чек-боксе «Обязательное» для поля будет необходимо указать минимум одно значение в процессе создания сертификата по данному шаблону, а при выключенном чек-боксе значения для данного поля могут быть не указаны. При включенном чек-боксе «Валидации» для поля будет выполняться валидация значений, указываемых пользователем для данного поля в процессе создания сертификата (см. Рисунок 167).

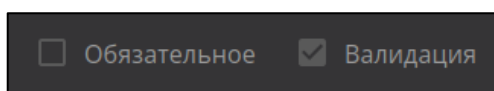


Рисунок 167 – Поле чек-бокса «Обязательное» и «Валидация»

- Используйте кнопки «Добавить поле» (см. Рисунок 168) на вкладках шаблона «Расширения» и «Компоненты имени сертификата» для формирования специализированного шаблона сертификата.

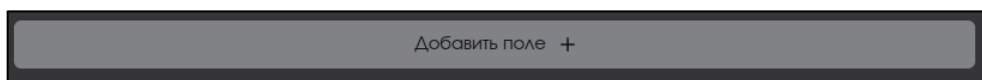



Рисунок 168 – Кнопка «Добавить поле» шаблона специализированного сертификата

7.11.4.1 Сохранение внесённых изменений в шаблон

- Для сохранения внесённых изменений в шаблоне нажмите кнопку в карточке шаблона «Сохранить» , расположенную в правом верхнем углу экранной формы. Сохранение изменений происходит без подтверждения.

- При переходе обратно на текущую вкладку «Шаблоны» или другую вкладку Центра сертификации в случае, если предварительно внесённые в редактируемый шаблон изменения не были сохранены, появляется окно подтверждения действия (см. Рисунок 169), в котором при нажатии кнопки:
 - <Покинуть страницу> внесённые изменения в текущем шаблоне будут утеряны и осуществлён выход из карточки шаблона;
 - <Отмена> будет осуществлено закрытие окна подтверждения и возврат к редактируемой карточке шаблона.

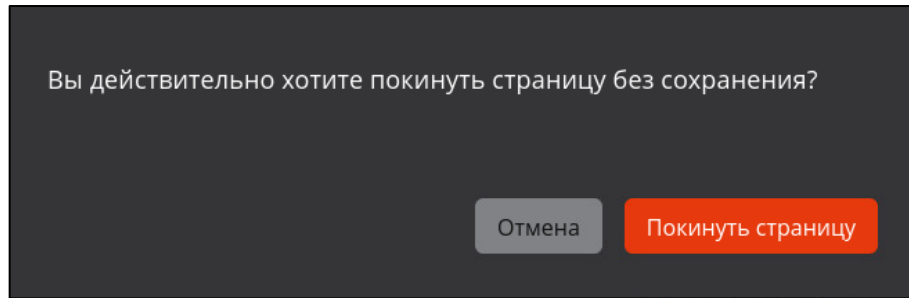



Рисунок 169 – Подтверждение выхода из карточки шаблона без сохранения изменений

7.11.5 Удаление шаблона

- Данная функция применима только для созданных, клонированных и загруженных шаблонов.
- Данная функция НЕ применима для предустановленных шаблонов.
- При наведении на строку с нужным шаблоном будет доступна иконка  <Удалить>. После нажатия на кнопку <Удалить> будет выведено на экран окно подтверждения действия (см. Рисунок 170), где возможно отменить выбранное действие, нажав кнопку <Отмена>, или подтвердить удаление выбранного шаблона, нажав кнопку <Удалить>.

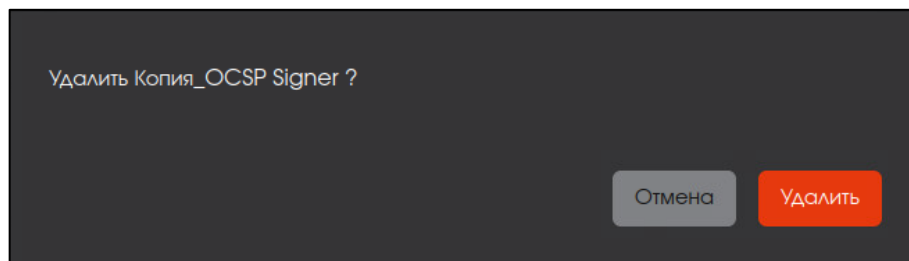




Рисунок 170 – Окно подтверждения удаления шаблона сертификата

- В случае успешного выполнения удаления шаблона сертификата администратор будет уведомлен сообщением на экране «Шаблон успешно удалён».
- Выбранный шаблон удаляется из системы и становится недоступным для всех операций. Сертификаты, выпущенные на этом шаблоне, остаются действительными.

7.11.6 Массовая операция (удаления) с шаблонами

- Для массовой операции удаления, применяемой к выбранному множеству шаблонов, нажмите кнопку  <Массовые операции>, которая запускает окно выполнения массовой операции.
 - В открывшемся окне необходимо осуществить поиск по имени шаблонов, для которых требуется применить выбранную операцию, в левом поле окна Шага 1 (см. Рисунок 171). Поиск производится для видов шаблонов: импортированный и клонированный, к которым применима операция удаления.
 - Выберите, найденные сертификаты, отметив их флажками .

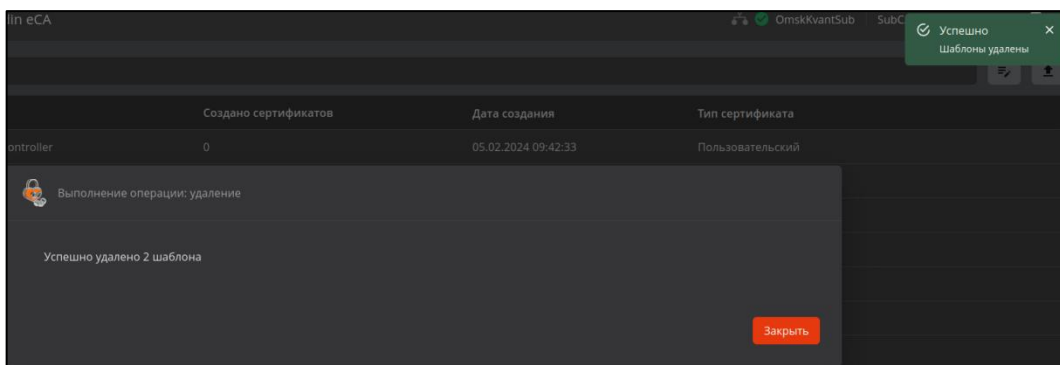


Рисунок 174 – Окно выполнения массовых операций. Шаг 4


7.11.7 Шаблоны MSCS

7.11.7.1 Экспорт шаблонов из MSCS

- Для экспорта шаблонов запустите скрипт `mcs2aeca.ps1` из комплекта поставки на рабочем месте с установленным Центром сертификации MSCS от имени администратора.
- Для успешного выполнения скрипта необходимо интернет-соединение. Для успешного выполнения скрипта в офлайн режиме требуется предварительно скачать и установить пакет NuGet.
- Скрипт запускается как консольное приложение и работает в режиме командной строки, графический интерфейс не предусмотрен. Запуск скрипта произвести от имени администратора.
- Результатом работы скрипта является сохранение всех шаблонов сертификатов из MSCS в папку `C:\temp\` на хосте.
- Шаблоны сохраняются в формате `.csv` с разделителем точка с запятой.
- При импорте шаблона из MSCS к названию шаблона должен добавляться префикс «MSCS_». Если в системе уже существует шаблон, совпадающий с именем импортируемого, то к имени импортируемого должен добавляться суффикс «_1» и т.д. (счетчик копий).

7.11.7.2 Загрузка шаблона MSCS

Для загрузки полученных шаблонов MSCS в Центр Сертификации Aladdin Enterprise CA:

- нажмите кнопку <Загрузить шаблоны> . В открывшемся окне выберите `.csv` файл шаблонов MSCS в локальной папке и нажмите кнопку <Открыть>.
- В результате шаблоны MSCS будут импортированы, и администратор будет уведомлен сообщением на экране «XX шаблонов успешно загружено», где «XX» - количество успешно загруженных шаблонов (см. Рисунок 175).

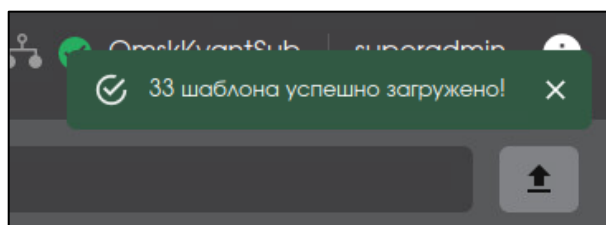


Рисунок 175 – Уведомление об успешной загрузке шаблонов MSCS

- В случае, если шаблоны не были импортированы, администратор будет уведомлен сообщением «Невозможно загрузить шаблоны» (см. Рисунок 175).

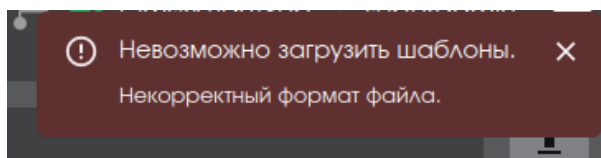


Рисунок 176 – Уведомление о неудачной загрузке шаблонов MSCS

- Поля, загружаемые из файла импорта шаблонов MSCS, приведены в Таблица 16.

Таблица 16 – Поля, загружаемые из файла шаблонов MSCS

Название поля в файле	Описание	Название поле в АЕСА
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”
Algoritm	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”
Policies, CritExts	Политики	OID политики сертификата; флажок “считать это расширение критическим”

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

7.11.8 Работа с шаблонами сертификатов

- Загруженные и созданные шаблоны доступны для использования при выпуске сертификатов на вкладке «Сертификаты» и «Субъекты» (см. подраздел 7.4 и 7.7 настоящего Руководства администратора).

7.11.8.1 Идентификатор шаблона

- При формировании заявки на сертификат необходимо указывать идентификатор шаблона – название шаблона или его идентификатор.
- Идентификатор нового (клонированного) шаблона возможно выделить из URL шаблона. Откройте созданный шаблон, выделите адрес, указанный в строке браузера, определите идентификатор шаблона, исходя из структуры URL-адреса. Например:

```
https://172.22.5.21/template/8548d5dc-c063-40f9-842d-3e35326fca01
```

имеет структуру

```
протокол://ip-адрес или имя сервера ЦС/наименование раздела/идентификатор шаблона
```

Таким образом, идентификатор созданного шаблона имеет вид 8548d5dc-c063-40f9-842d-3e35326fca01.

- Для предустановленных шаблонов идентификаторы приведены в Таблица 17.

Таблица 17 – Идентификаторы предустановленных шаблонов

Название шаблона	Идентификатор
ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffe
ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874
Domain Controller	bf2dac0a-f05f-49dd-95b4-e50691489b6a
ECA-Auth	8ecba810-7f48-4c4e-b803-99a97146e2ba
OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab
Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb
Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647
S/MIME	0c234243-18cf-4c05-b699-537731b2436f
Sub CA	af3b0355-1798-4c64-98f7-a9c70407db1c
WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68
WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1

7.12 Раздел «Настройки»

Раздел «Настройки» обеспечивает управление работой web-сервера и доступом к нему: возможность смены ключей web-сервера и управление издателями сертификатов учётных записей для доступа к нему.

- Переход в раздел «Настройки» (см. Рисунок 177) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 38).
- Данный раздел доступен только в режиме администратора.

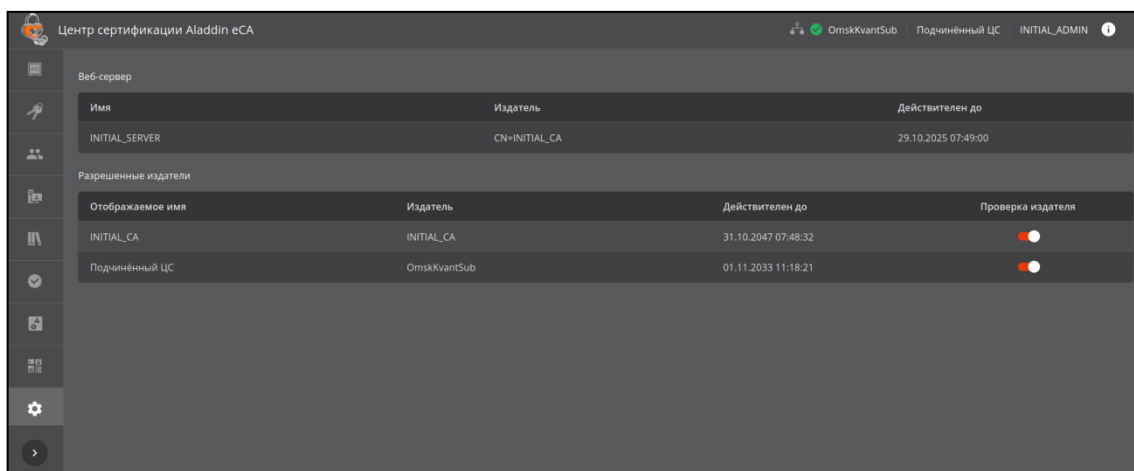


Рисунок 177 – Экран раздела «Настройки»

- На экране раздела «Настройки» отображены:
 - поле «Веб-сервер», в котором отображен текущий сертификат web-сервера с отображением его имени, издателя текущего сертификата и срока действия текущего сертификата web-сервер.


После установки программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» будет автоматически установлен сертификат web-сервера, выпущенный технологическим Центром сертификации;

- поле «Разрешенные издатели», где указаны все издатели текущего Центра сертификации. По умолчанию в «доверенных издателях» находится самоподписанный сертификат технологического ЦС, созданный при развертывании «Центра сертификации» и используемый для внутренних взаимодействий «INITIAL_CA».
- Доступны следующие операции в разделе «Настройки»:
 - установка (смена) сертификата web-сервера;
 - включение/отключение «разрешённых» издателей сертификатов учётных записей для доступа к web-серверу.

7.12.1 Установка сертификата web-сервера

- Предварительно необходимо выпустить сертификат для **субъекта локальной ресурсной системы** (для автоматически созданного локального субъекта при развёртывании Центра сертификации (см. 7.7.5 настоящего руководства) или нового созданного субъекта) (см. Приложение 1) со значениями в полях шаблона web-server при выпуске сертификата:

- «общее имя» – имя web-сервера, отображаемое на экране, в разделе «Настройки», рекомендуется указать имя сервера;
- «доменное имя» – имя хоста, на котором развёрнут Центр сертификации, должно совпадать указанным в файле `/etc/hosts`.

- Для смены ключей выберите web-сервер и нажмите появившуюся кнопку .
- В появившемся окне (см. Рисунок 178) выберите файл сертификата и введите пароль файла контейнера, заданный при выпуске сертификата web-сервера.
- Нажмите активировавшуюся кнопку <Сменить ключи>.

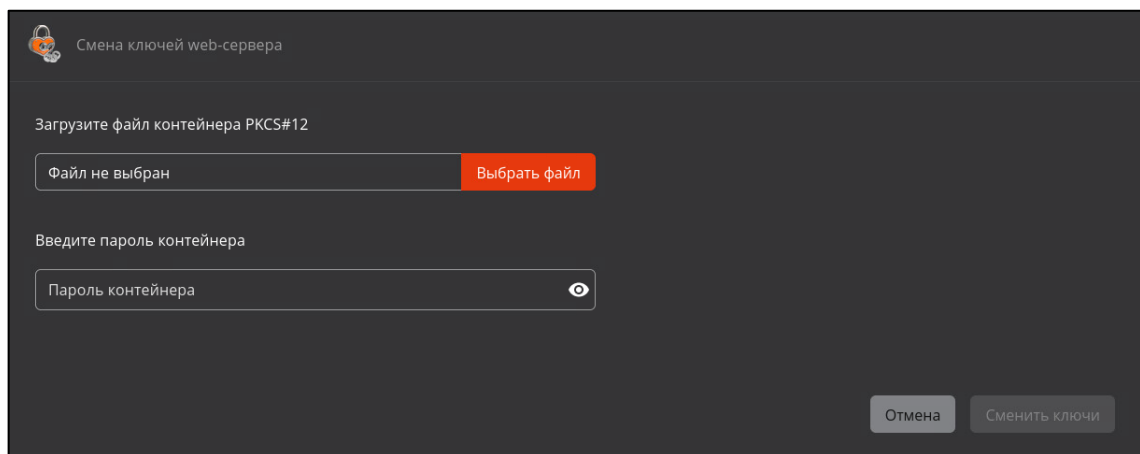


Рисунок 178 – Окно смены ключей web-сервера

- После смены сертификата web-сервера администратор будет уведомлён сообщением «Сертификат изменён» (см. Рисунок 179).

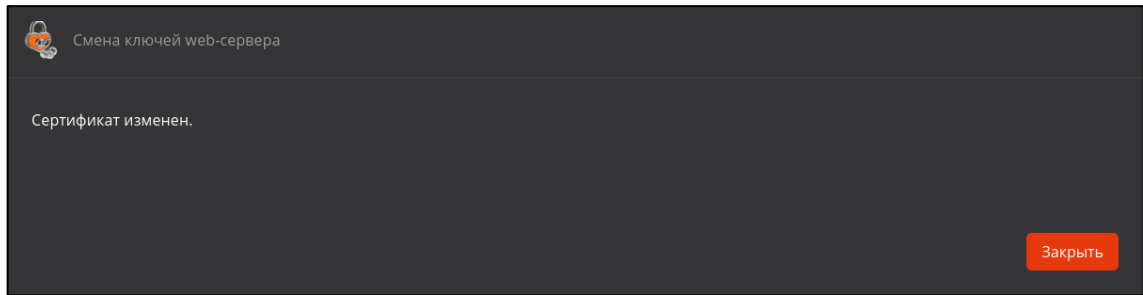


Рисунок 179 – Окно уведомления об успешной смене ключей web-сервера

- Далее будет выполнена автоматическая перезагрузка web-сервера. В результате перезагрузки web-сервера в «Журнал событий» будет записано событие с кодом CAENV040 в случае успешной перезагрузки web-сервера или событие с кодом CAENV041 в случае ошибки в процессе перезагрузки web-сервера.
- Для установки безопасного соединения с серверной частью Центра сертификации (после установки нового сертификата web-сервера) снова запустите браузер и выполните подключение к Центру сертификации.
- Администратору будет предложено выбрать сертификат для идентификации и аутентификации (или оставить текущий, издатель, которого активирован в «Разрешённых издателях») (см. Рисунок 180). Более подробно процедура аутентификации по сертификату приведена в разделе 6, «Руководства администратора. Установка и обслуживание Центра сертификации Aladdin Enterprise Certificate Authority. «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». RU.АЛДЕ.03.01.020-01 32 01-1»

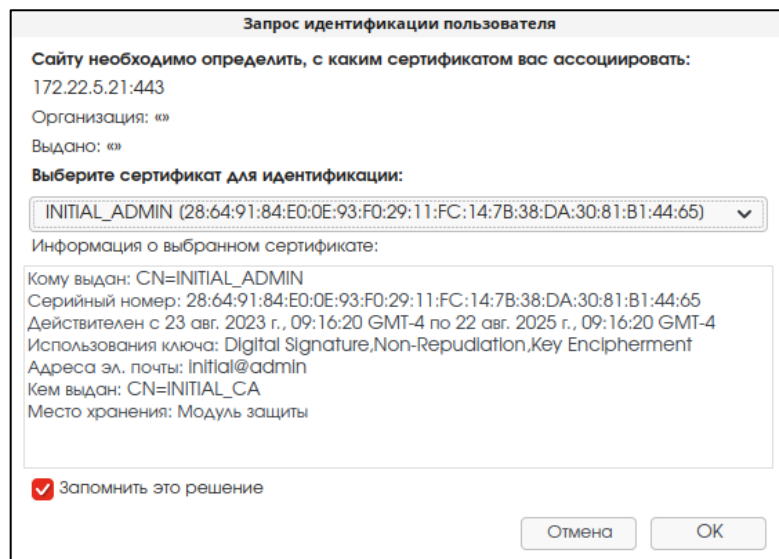




Рисунок 180 – Выбор сертификата пользователя

7.12.2 Разрешённые издатели

- На экранной таблице в поле «Разрешённые издатели» отображены текущие сертификаты Центров сертификации (технологического и созданного, при установке программного средства и загрузки лицензии).
- Для доступа аутентифицирующегося пользователя с ролью администратор/оператор к текущему web-серверу необходимо активировать издателя сертификата учётной записи, передвинув ползунок вправо .
- Для исключения издателя из «разрешённых» необходимо выделить издателя и деактивировать в поле «Проверка издателя», передвинув ползунок влево . С сертификатом пользователя, выпущенным исключённым издателем, аутентификация не будет успешной, в доступе к web-серверу будет отказано.

В случае, если издатель текущей учётной записи будет исключён из разрешённых издателей, то администратор будет уведомлён об ошибке, о чём будет внесена запись CAENV039 в «Журнал событий» (см. Рисунок

181). В случае активного сеанса пользователя (администратора/оператора) доступ к клиентской части центра сертификации будет заблокирован через 3 минуты после исключения издателя сертификата учётной записи пользователя из разрешённых.

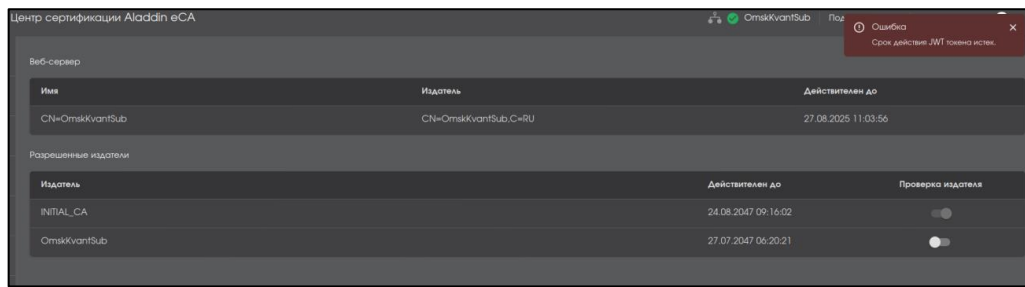


Рисунок 181 – Ошибка изменения списка разрешённых издателей

8 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения
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. п. 3.1)
Прекращение установки ПО или обновление Aladdin eSA	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	<p>Проверьте наличие установленного ПО согласно разделу 3 Руководства администратора RU.АЛДЕ.03-01.020-01 32.</p> <p>Также проверьте и при необходимости переключите текущую версию java-компонентов, выполнив команды:</p> <pre>sudo update-alternatives --config java sudo update-alternatives --config javac</pre> <p>sudo update-alternatives --config javap</p>
Нет подключения к ресурсной системе	1. Включен протокол TLS	<p>Измените настройку конфигурационного файла контроллера домена <code>/etc/samba/smb.conf</code>, добавив в раздел <code>[global]</code>:</p> <pre>ldap server require strong auth = no</pre>
	2. Проверить подключение к контроллеру домена Samba	<p>Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code>:</p> <ul style="list-style-type: none"> - получение списка пользователей <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=user)"</pre> <ul style="list-style-type: none"> - получение списка компьютеров <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=computer)"</pre> <ul style="list-style-type: none"> - получение списка групп безопасности <pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC= pki-test " -H "ldap://192.168.111.148" "(objectCategory=group)"</pre> <p>где:</p> <p><code>Administrator@pki-test.local</code> – имя администратора домена;</p>

Проблема	Возможная причина	Способы решения
		<p><code>Qwerty1234</code> – пароль администратора домена; <code>pki-test, pki-test</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>
3. Проверить подключение к контроллеру домена ALD PRO		<p>Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code>:</p> <ul style="list-style-type: none"> - получение списка пользователей <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=x-ald-user) "</pre> <ul style="list-style-type: none"> - получение списка компьютеров <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=nshost) "</pre> <ul style="list-style-type: none"> - получение списка групп безопасности <pre>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=ipausergroup) "</pre> <p>где:</p> <p><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>
Вход в интерфейс Центра сертификации с выпущенным сертификатом невозможен в браузере Chromium	Браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой браузер
Вход в интерфейс Центра сертификации невозможен.	Удалён сертификат	Проверить файл <code>opt/aeca/p12/truststore.jks</code> на предмет содержания записи о сертификате технологического центра сертификации, созданного при установке ПО Aladdin eCA.

Проблема	Возможная причина	Способы решения
Ошибка 500	технологическо-го ЦС	<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>
Невозможно подключиться к токену для выпуска сертификата после установки JC-WebClient. Сообщение «ПО JCWebClient не установлено»	Требуется разрешить ПО JC-WebClient доступ к ресурсу	<ol style="list-style-type: none"> В адресную строку браузера введите: <code>https://localhost:24738/admin/token_manager.html</code> Во всплывающем окне предупреждения браузера подтвердите действия.
Пустой файл шаблонов по завершению работы скрипта <code>mscs2aeca.ps1</code> экспорт а шаблонов MSCS	Требуется настройка <code>tls</code>	<p>Откройте Powershell от имени администратора и задайте версию протокола безопасности, выполнив команду:</p> <pre>[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12</pre>
Невозможно применить выпущенный Центром сертификации Aladdin eCA сертификат в операционной системе Windows (в частности, WinServer2012/2016)	Сертификат доступа сгенерирован с использованием алгоритма хеширования <code>sha256</code> , и операционная система Windows не поддерживает данный алгоритм	<p>Конвертируйте сертификат, сгенерированный с использованием алгоритма хеширования <code>sha256</code>, в формате <code>.p12</code> в формат <code>.pem</code> с помощью <code>openssl</code>:</p> <pre>openssl pkcs12 -in <имя контейнера>.p12 -out <имя декодированного файла>.pem</pre> <pre>openssl pkcs12 -keypbe PBE-SHA1-3DES -certpbe PBE-SHA1-3DES -export -in <имя декодированного файла>.pem -out <имя контейнера>.p12</pre>
Ошибка Cannot read properties of undefined (reading `data`)	Установленное ранее <code>ssl</code> соединение недействительно. Возникает, если в момент обновления сертификата <code>web-сервера</code> было открыто несколько вкладок, либо	Перезагрузите страницу браузера

Проблема	Возможная причина	Способы решения
	был перезапущен (по каким-либо причинам) web-сервер	
Ошибка запроса к стороннему сервису. ...	Ошибка подключения к Центру сертификации по протоколу https	Выполните настройку безопасного соединения согласно разделу 5 «Безопасность соединения» настоящего руководства

ПРИЛОЖЕНИЕ 1. СОЗДАНИЕ СЕРТИФИКАТА ДЛЯ СУБЪЕКТА

Внимание! Создание сертификата (любым способом) возможно только для существующего субъекта локальной (см. п. 7.7.5 настоящего руководства) или подключенных ресурсных систем (см. п. 7.7.6 настоящего руководства)!

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 182):

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

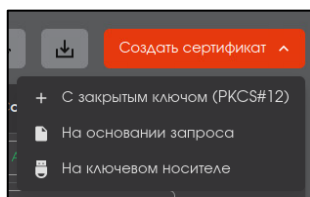


Рисунок 182 - Кнопка «Создать сертификат» на вкладке «Сертификаты»

- На вкладке «Учётные записи» при выделении строки учётной записи и нажатии кнопки <Создать сертификат> доступен выпуск сертификата для учётной записи (см. Рисунок 183):

- 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.

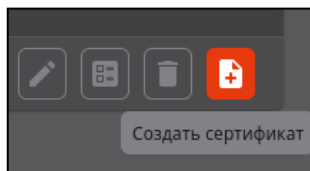


Рисунок 183 - Кнопка «Создать сертификат» на вкладке «Учётные записи»

- На вкладке «Субъекты» при выделении строки субъекта и нажатии кнопки <Создать сертификат> доступен выпуск сертификата (см. Рисунок 184):

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

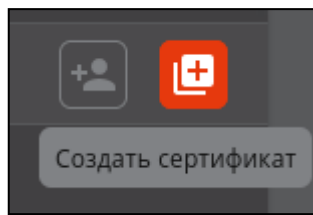


Рисунок 184 - Кнопка «Создать сертификат» на вкладке «Субъекты»

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

1.2 Параметры криптографии сертификатов учётных записей пользователей и Центров сертификации

В таблице определены комбинации сертификатов Центра сертификации, к которому происходит подключение пользователя (оператора/администратора), и используемого для аутентификации сертификата учётной записи пользователя, при которых будет происходить успешная аутентификация пользователя Aladdin eCA.

Таблица 18 – Успешные комбинации сертификатов Центра сертификации и учётной записи пользователя при аутентификации на сервере

Операционная система	Алгоритм и длина ключа сертификата Центра сертификации	Алгоритм и длина ключа сертификата учётной записи пользователя
Astra Linux Special Edition 1.7 Смоленск	RSA: 2048-4096, SHA256-SHA512	RSA: 2048-8196.
	ECDSA: 256-521, SHA256-SHA512	ECDSA: 256-521
РЕД ОС 7.3	RSA: 2048-4096, SHA1-SHA512	RSA: 1024-8196.
	ECDSA: 256-521, SHA1-SHA512	ECDSA: 256-521
ОС Альт 8 СП, релиз 10, Сервер	RSA: 2048-4096, SHA1-SHA512	RSA: 1024-8196.
	ECDSA: 256-521, SHA1-SHA512	ECDSA: 256-521

1.3 Публикация сертификата в ресурсную систему

- При создании сертификата для субъекта внешней ресурсной системы имеется возможность публикации его в ресурсную систему при установке соответствующего чек-бокса (см. Рисунок 185)

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

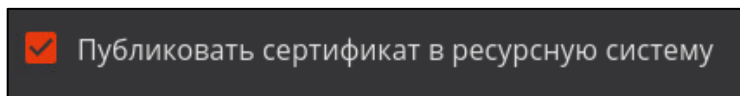



Рисунок 185 - Окно создания сертификата PKCS#12. Поиск субъекта

- Для успешной публикации сертификатов в ресурсную систему ALD Pro и Free IPA требуется подключение к ресурсной системе от имени пользователя, с минимальным набором прав пользователя:
 - наличие роли «Service Role» для подключения к ресурсной системе;
 - наличие роли «helpdesk» или роли «User Administrator» для публикации сертификатов пользователей;
 - наличие роли «Enrollment Administrator» для публикации сертификатов контроллеров домена.

1.4 Создание сертификата с закрытым ключом pkcs#12

Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. п. 7.7.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. п. 7.7.6 настоящего руководства).

- В появившемся окне (см. Рисунок 186):
 - при выпуске сертификата в разделе «Сертификаты» необходимо на нулевом шаге ввести частичное или полное значение Common Name, UPN или UUID субъекта, для которого будет выпущен сертификат доступа. В результате будут отображены найденные субъекты с указанием CN, UPN, UUID и пиктограммы наличия подключения субъекта к ресурсной системе  (см. Рисунок 186). Выберите субъект и нажмите кнопку <Продолжить> для перехода к шагу 1;
 - при выпуске сертификата в разделах «Субъекты» и «Учётные записи» нулевой шаг не требуется и первым шагом будет выбор ключевого носителя и шаблона для выпуска сертификата (см. Рисунок 187).

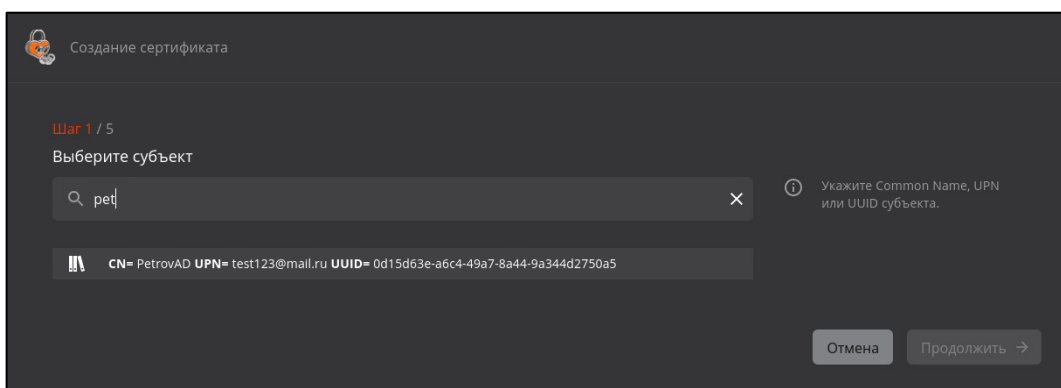


Рисунок 186 - Окно создания сертификата PKCS#12. Поиск субъекта

- В открывшемся окне (см. Рисунок 187) необходимо выбрать шаблон из выпадающего списка в поле «Выберите шаблон» для выпуска сертификата. 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.

- Чек-бокс «Публиковать сертификат в ресурсную систему» для субъектов внешних ресурсных систем, и активирован по умолчанию для публикации сертификата во внешнюю/подключенную ресурсную систему.

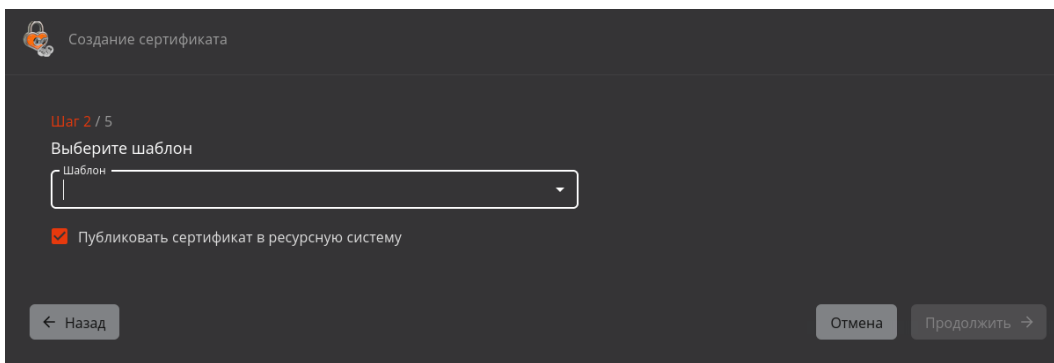




Рисунок 187 - Окно создания сертификата PKCS#12. Выбор шаблона сертификата

- В окне Шага 2 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей шаблона приведено в Приложение 2. Описание обязательных полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 7.7.4 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 188).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. п. 0 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку «Продолжить» для перехода к следующему шагу.

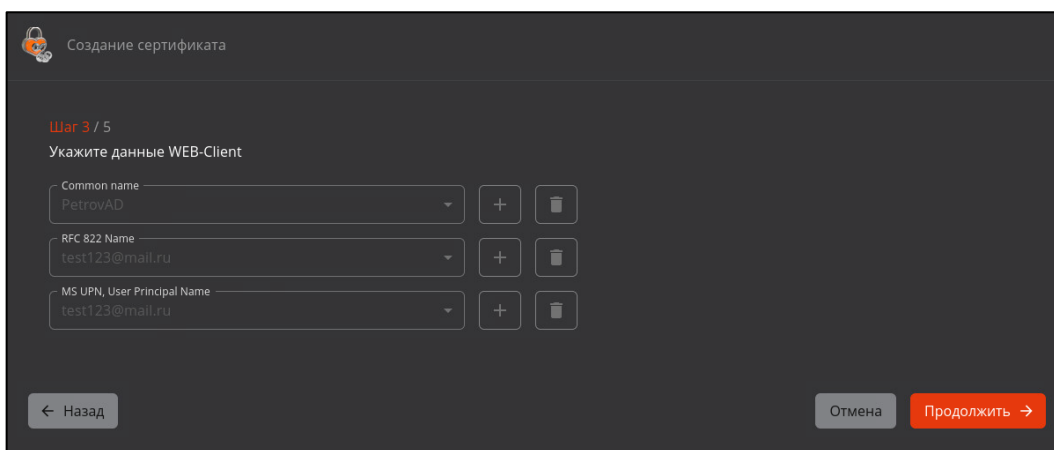



Рисунок 188 - Окно создания сертификата PKCS#12. Атрибуты сертификата

- Далее необходимо создать пароль с подтверждением (см. Рисунок 189) в соответствии с правилами ввода пароля:
 - для просмотра вводимых символов необходимо нажать кнопку  на текущей строке;
 - пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;

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

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

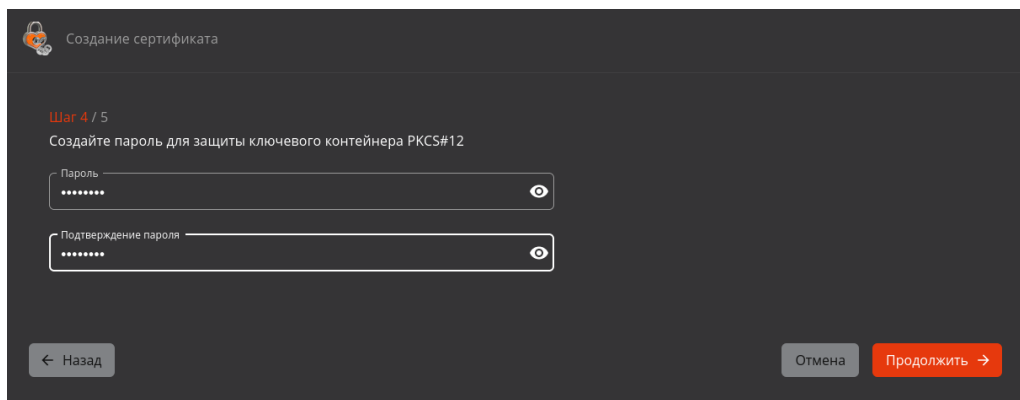


Рисунок 189 - Окно создания сертификата PKCS#12. Ввод пароля контейнера

- Далее необходимо выбрать параметры криптографии из выпадающего списка значений алгоритма ключа (см. Рисунок 190). По умолчанию выбрано значение «RSA-2048».
- После выбора алгоритма нажмите кнопку <Создать сертификат>.

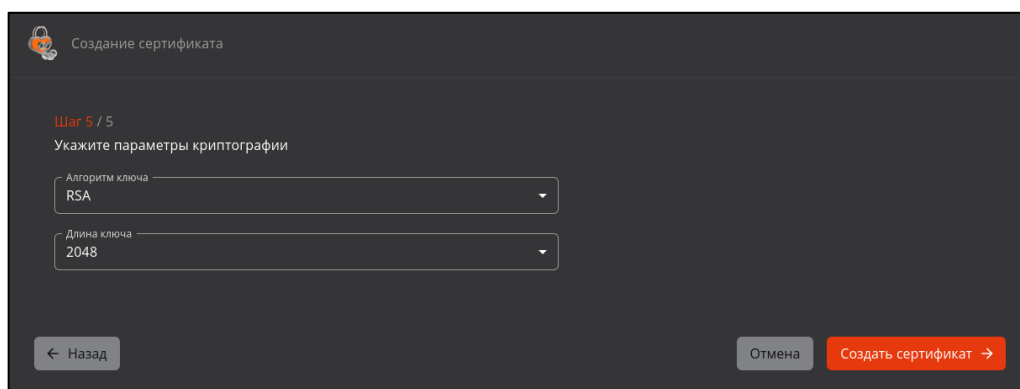


Рисунок 190 – Окно создания сертификата PKCS#12. Выбор параметров криптографии

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 196).

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.

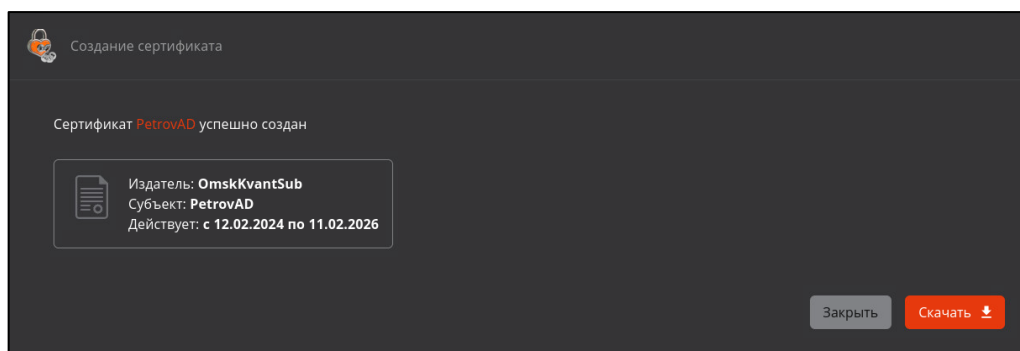



Рисунок 191 – Окно создания сертификата PKCS#12. Информирование об успешном создании сертификата

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

1.5 Создание сертификата субъекта по запросу

Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. п. 7.7.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. п. 7.7.6 настоящего руководства).

- Предварительные условия выполнения сценария:
 - файл-запрос для субъекта должен быть подготовлен заранее на стороннем ЦС (например, при помощи ПО «Единый клиент JaCarta»);
 - расширение файл-запроса не имеет существенного значения, но предполагается, что оно будет `***.csr` или `***.req`;
 - файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона компонента «Центр сертификации Aladdin Enterprise Certification Authority». Например, для использования шаблона «Domain Controller» в запросе должны быть указаны параметры DNS Name и MS GUID;
 - по файлу-запроса ранее не был выпущен сертификат.
- В открывшемся окне (см. Рисунок 192) введите частичное или полное значение Common Name, UPN или UUID субъекта, имя которого указано в запросе на сертификат. В результате будут отображены найденные субъекты с указанием CN, UPN или UUID и пиктограмма наличия подключения субъекта к ресурсной системе . Выберите субъект и нажмите кнопку <Продолжить> для перехода к следующему шагу.

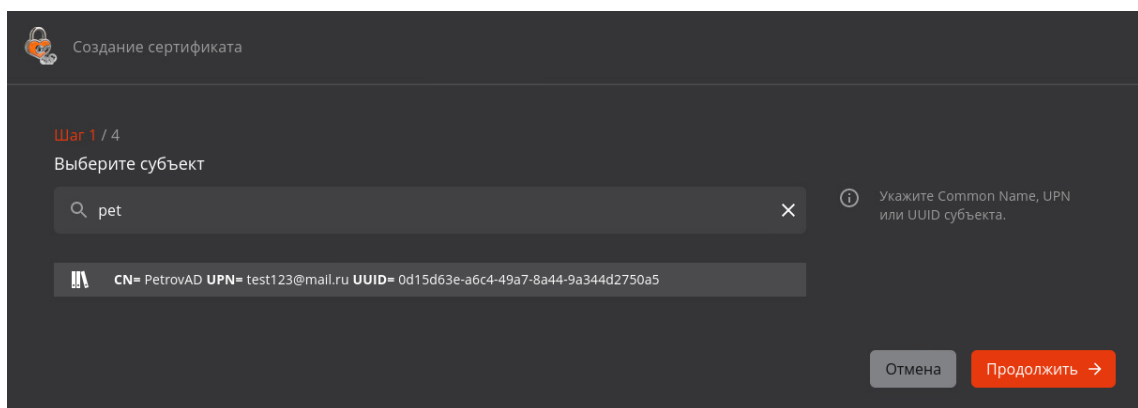


Рисунок 192 – Окно создания сертификата по запросу. Поиск субъекта

- На следующем шаге загрузить файл-запрос, а также выберите шаблон сертификата в соответствии с запросом (предполагается, что администратор заранее знает, для какого субъекта загружается файл-запрос и какой шаблон необходимо выбрать). По файлу запроса возможен только одноразовый выпуск сертификата.
- Чек-бокс «Публиковать сертификат в ресурсную систему» доступен только при выпуске сертификата для субъектов внешних ресурсных систем, и активирован по умолчанию для публикации сертификата во внешнюю ресурсную систему путём добавления, а не перезаписи атрибута. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат.
- 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>.

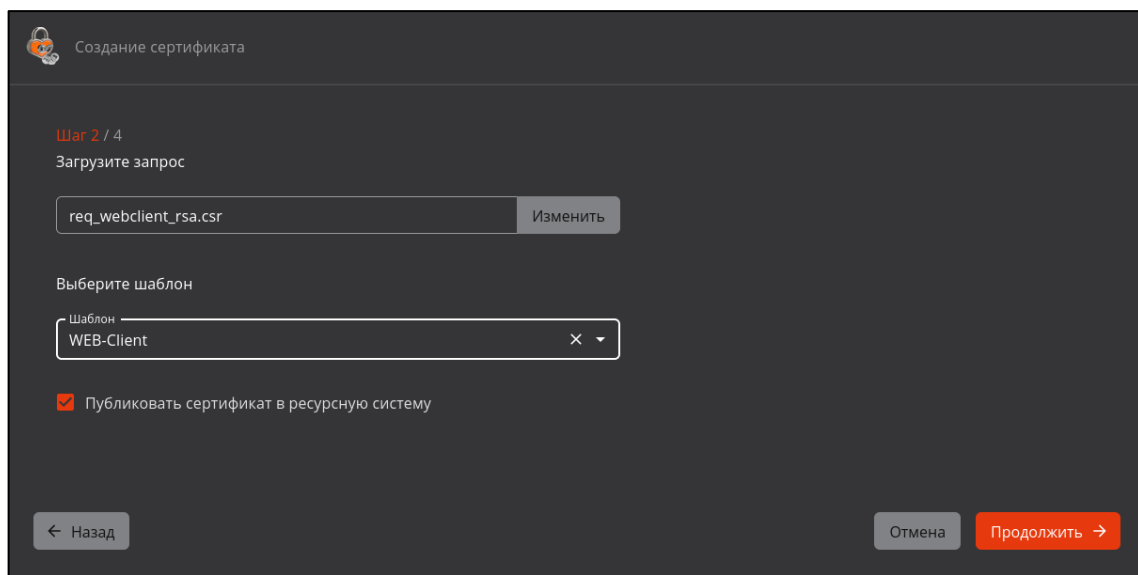


Рисунок 193 – Окно создания сертификата по запросу. Загрузка запроса и выбор шаблона

- Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 19.

Таблица 19 – Соответствие полей запроса шаблону выпускаемого сертификата

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Правила проверки соответствия SDN полей					
Есть, обязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, обязательное	Нет	Нет	Нет	-	Ошибка №1
Есть, обязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута субъекта
Есть, обязательное	Нет	Есть	Нет	-	Ошибка №1
Есть, необязательное	Есть	Нет	Нет	-	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Отсутствует	-
Нет	Есть	Нет	Нет	-	Ошибка №3

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

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Нет	Нет	Есть	Да	Отсутствует	-

• В случае выявления ошибки в запросе на сертификат доступа для субъекта возможны следующие сообщения:

- «Отсутствует обязательное поле» (ошибка №1);
- «Значение в поле не соответствует регулярному выражению: \"%s\","", где \"%s\"» (ошибка №2), регулярное выражение для валидации значений в соответствии с Приложением 2;
- «Поле отсутствует в шаблоне» (ошибка №3);
- «Значение в поле не соответствует значению атрибута в субъекте» (ошибка №4).

Если создание сертификата невозможно, то существует две возможности:

- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>.

• В результате успешной обработки запроса на сертификат субъекта на следующем шаге будут отображены (см. Рисунок 194):

- 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»);
- должна быть доступна кнопка «Продолжить» для перехода к следующему шагу;
- должен быть предусмотрен возврат к предыдущему шагу (путем нажатия на кнопку «Назад») с возможностью изменения выбора запроса и/или шаблона сертификата;
- должна быть доступна кнопка «Отмена» для завершения работы мастера создания сертификата без сохранения результатов.

• Отображение данных в окне создания сертификата для существующего и нового субъектов разделены на две основные части:

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

• В случае, если в файле-запросе существуют дополнительные поля субъектных идентификаторов, отсутствующие в текущей реализации (для справки - <http://oidref.com/2.5.4>, таблица children), то они идентифицируются по параметру OID.

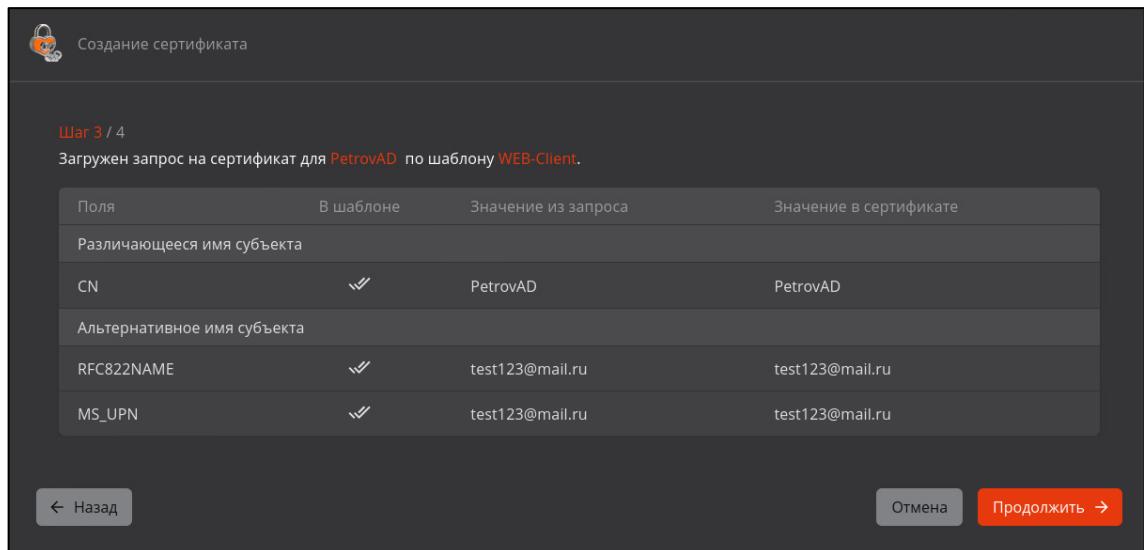




Рисунок 194 – Окно создания сертификата по запросу. Результат обработки запроса

- После успешной загрузки файла запроса нажмите кнопку <Продолжить> для продолжения процедуры выпуска сертификата для субъекта, кнопку <Отмена> для прекращения процедуры выпуска сертификата или кнопку <Назад> для возврата на предыдущий шаг.
- В открывшемся окне указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей шаблона приведено в Приложение 2. Описание обязательных полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 7.7.4 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 195).
- При отсутствии доступных для указания значений в поле обязательного атрибута будет отображаться ошибка «У субъекта отсутствует указанный атрибут».
- Необязательные поля могут оставаться незаполненными.

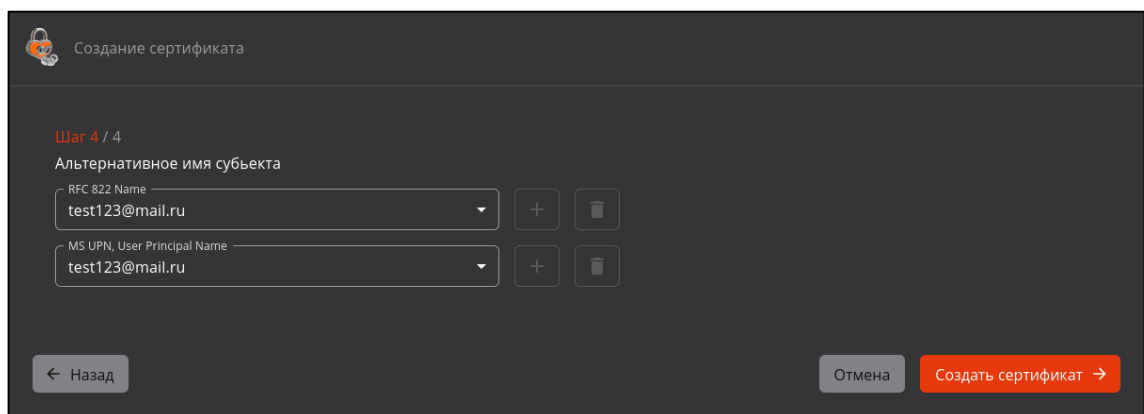


Рисунок 195 – Окно создания сертификата на основании запроса. Атрибуты сертификата

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 196).

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.

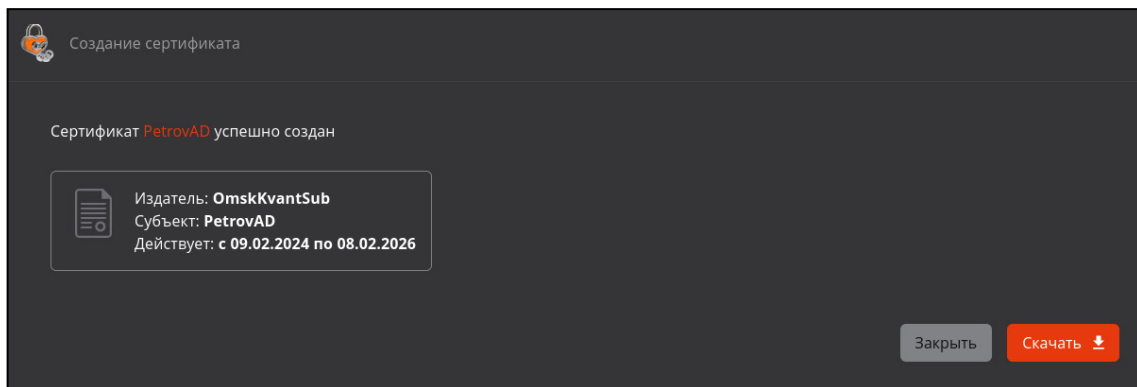



Рисунок 196 – Окно создания сертификата по запросу. Информирование об успешном создании сертификата

1.6 Создание сертификата субъекта на ключевом носителе

Создание сертификата возможно только для существующего субъекта! Предварительно создайте локальный субъект (см. п. 7.7.5.1 настоящего руководства) или выберите субъект внешней ресурсной системы (см. п. 7.7.6 настоящего руководства).

Предварительные условия выполнения сценария:

- Убедитесь, что поддерживаемый электронный ключ присоединен к АРМ выпускающего Центра сертификации;
- Убедитесь, что на сервере выпускающего Центра сертификации установлено ПО JC-WebClient версии 4.3.2 или 4.3.3 для дальнейшей работы с ключевыми носителями из браузера.
- Нажатие кнопки <Создать сертификат> - «На ключевом носителе» запускает сценарий по созданию сертификата на ключевом носителе. Осуществляется проверка подключения ключевого носителя, определяется наличие свободной памяти, достаточной для записи создаваемого сертификата.
- В случае если электронный ключ успешно подключен, в открывшемся окне:
 - при выпуске сертификата в разделе «Сертификаты» необходимо на нулевом шаге ввести частичное или полное значение Common Name, UPN или UUID субъекта, для которого будет выпущен сертификат доступа. В результате будут отображены найденные субъекты с указанием CN, UPN, UUID и пиктограммы наличия подключения субъекта к ресурсной системе  (см. Рисунок 197). Выберите субъект и нажмите кнопку <Продолжить> для перехода к шагу 1;
 - при выпуске сертификата в разделах «Субъекты» и «Учётные записи» нулевой шаг не требуется и первым шагом будет выбор ключевого носителя и шаблона для выпуска сертификата (см. Рисунок 198).

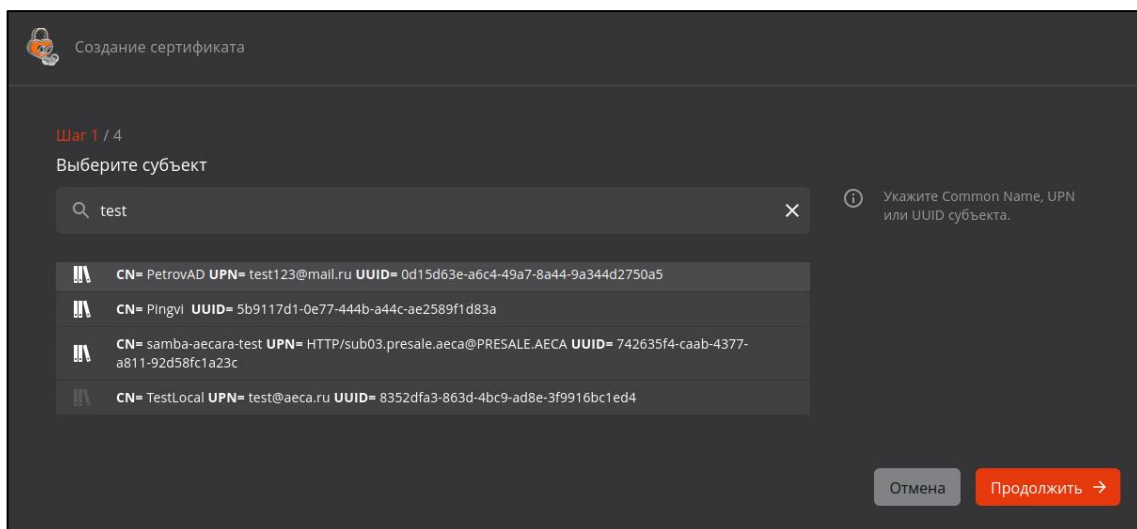


Рисунок 197 – Окно создания сертификата на электронном ключе в разделе «Сертификаты». Шаг 1

- В открывшемся окне (см. Рисунок 198) 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. Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> в случае ввода корректного PIN-кода электронного ключа и заполнении всех полей.

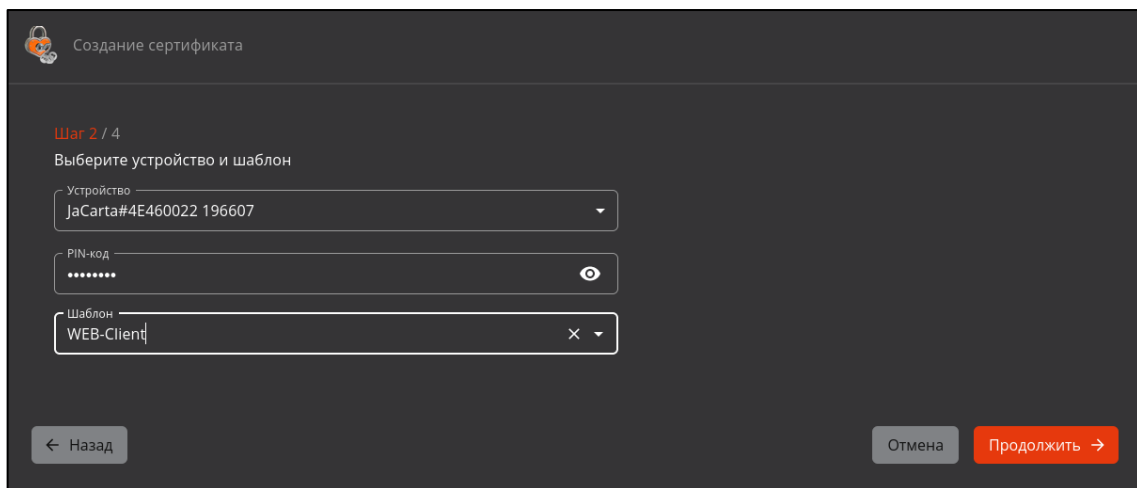




Рисунок 198 – Окно создания сертификата на электронном ключе. Шаг 1

- В окне Шага 2 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей шаблона приведено в Приложение 2. Описание обязательных полей предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 7.7.4 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 199).

- Необязательные поля могут оставаться незаполненными.

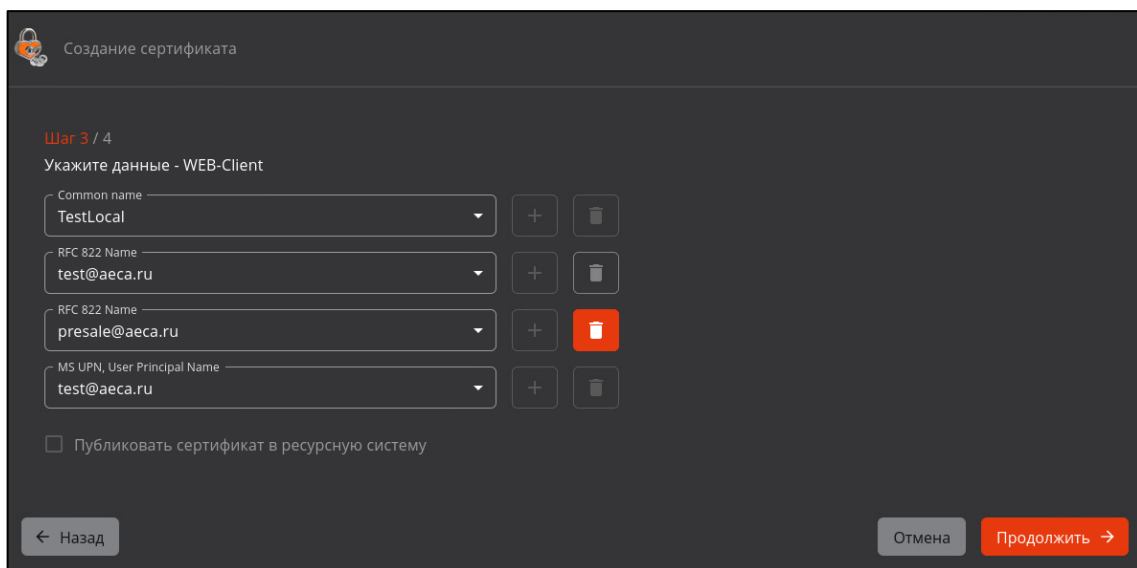


Рисунок 199 – Окно создания сертификата на электронном ключе. Шаг 2. Удаление добавленного значения атрибута

- Чек-бокс «Публиковать сертификат в ресурсную систему» для субъектов внешних ресурсных систем, и активирован по умолчанию для публикации сертификата во внешнюю/подключенную ресурсную систему. Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат, путём добавления, а не перезаписи атрибута.
- Нажмите кнопку «Продолжить», ставшую активной, после заполнения всех обязательных полей шаблона сертификата на втором шаге (см. Рисунок 199).
- Далее необходимо выбрать параметры криптографии из выпадающего списка значений алгоритма ключа (см. Рисунок 200). По умолчанию выбрано значение «RSA-2048». После выбора алгоритма нажмите кнопку «Создать сертификат».

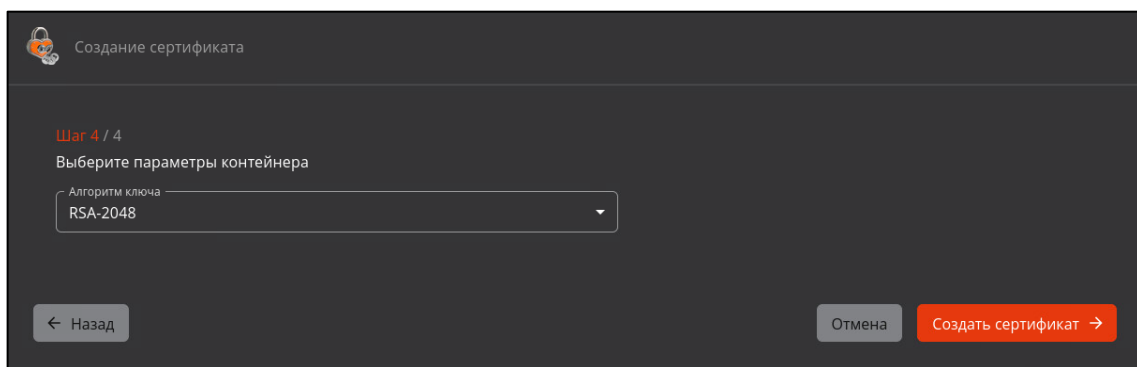


Рисунок 200 – Окно создания сертификата на электронном ключе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
 - генерация ключевой пары на основе данных заполненного шаблона сертификата на предыдущем шаге;
 - генерация запроса на основе данных заполненного шаблона сертификата на предыдущем шаге;
 - создание сертификата;
 - запись сертификата на ключевой носитель.
- Процессы выполняются автоматически и после завершения станут доступны кнопки «Скачать сертификат» (контейнер сертификата `pkcs#12`) и «Скачать цепочку сертификатов» (см. Рисунок 201).

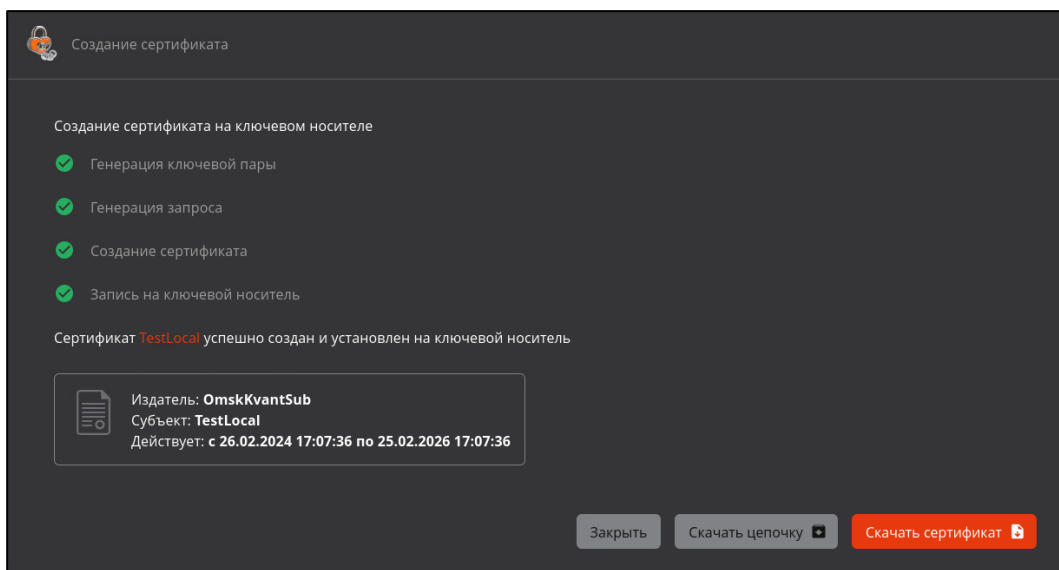


Рисунок 201 – Окно успешного создания сертификата субъекта на электронном ключе

1.6.1 Сообщения об ошибках при создании сертификата на ключевом носителе

- В случае, если ПО JC-WebClient предварительно не установлено, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 202). Для выпуска сертификата на электронном ключе установите ПО JC-WebClient версии 4.3.2 или 4.3.3.

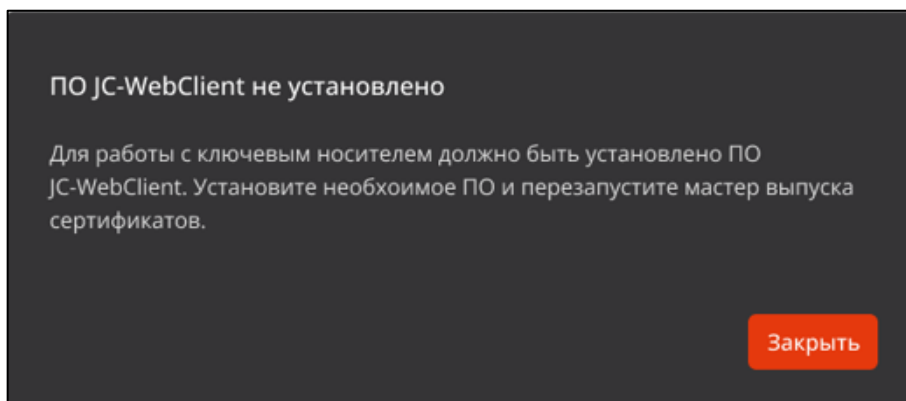


Рисунок 202 – Окно информационного сообщения «ПО JC-WebClient не установлено»

- В случае, если электронный носитель не подключен, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 203). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

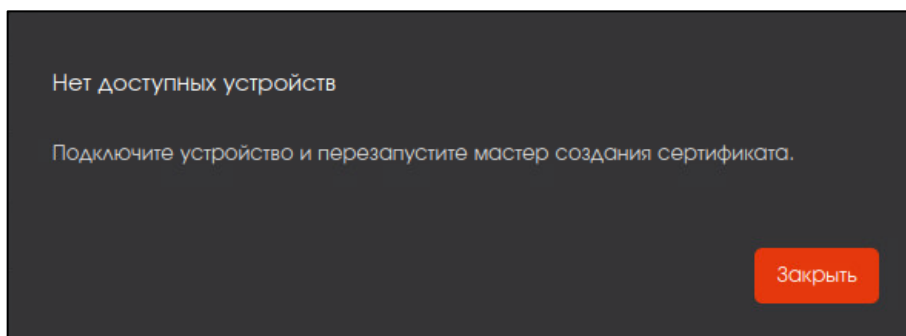


Рисунок 203 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя, администратор будет уведомлён об этом информационным сообщением.
- В случае возникновения ошибок, связанных с работой JC-WebClient, администратор будет уведомлён сообщением, согласно с описанием ошибки в документации JC-WebClient SDK:
 - <https://developer.aladdin-rd.ru/archive/jc-webclient/4.0.0/api/addendum/errors.html>
 - <https://developer.aladdin-rd.ru/archive/jc-webclient/3.1.1/api/addendum.html>

ПРИЛОЖЕНИЕ 2. ОПИСАНИЕ ОБЯЗАТЕЛЬНЫХ ПОЛЕЙ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Domain controller – шаблон сертификата контроллера домена				
CommonName	CommonName	имя контроллера домена	DC01	A-Я, а-я, A-Z, a-z, 0-9, ,, _ -, пробел, ()
DNS Name	Domain Name System	FQDN (полное доменное имя вашего сервера)	dc1.presale.aeca	Только указанные символы: A-Я, а-я, A-Z, a-z, 0-9, ,, -, *
MS GUID, Globally Unique Identifier	objectGUID / ipaUniqueID	<p>глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена</p> <p>Для получения значения идентификатора в среде РЕД ОС выполните команду:</p> <pre>samba-tool computer show <hostname> grep objectGUID</pre> <p>Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду:</p> <pre>ipa host-show <hostname> --all grep ipauniqueid</pre> <p>где [hostname] – короткое имя контроллера домена.</p>	92625ee510e248479554779d1f43f751 (32 знака)	ввод символов в рамках шестнадцатеричной системы счисления; длина строго 32 знака; A-Z, a-z, 0-9

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите значение из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите значение из выпадающего списка	-	1024,1536,2048,3072,4096,6144,8192 192,224,256,384,521
ALD PRO Domain controller – шаблон сертификата контроллера домена ALD PRO				
CommonName	CommonName	имя контроллера домена ALD PRO	dc.ald.pro	A-Я, а-я, A-Z, a-z, 0-9, ,, _ - , пробел, ()
Organization	-	организация	test	A-Я, а-я, A-Z, a-z, 0-9, ,, _ - , пробел
MS UPN, UserPrincipalName	objectGUID / ipaUniqueID	данные в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	Строка вида “text@text” A-Я, а-я, A-Z, a-z, 0-9, ,, @, /, _ -
Kerberos KPN	-	в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	A-Я, а-я, A-Z, a-z, 0-9, ,, @, /, _ -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144,8192 192,224,256,384,521
Smartcard Logon ALD PRO – шаблон сертификата пользователя ALD PRO				
CommonName	CommonName	имя пользователя ALD PRO		A-Я, а-я, A-Z, a-z, 0-9, ,, _ - , пробел, ()

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Organization	-	организация	test	А-Я, а-я, А-Z, а-z, 0-9, ,, _ , пробел
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	Строка вида "text@text" и только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ,, @, _ , -
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида "text@text" и только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ,, @, _ , -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	А-Z, а-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144, 8192 192,224,256,384,521
Smartcard Logon – шаблон сертификата пользователя				
CommonName	CommonName	имя пользователя	IvanovaAN	А-Я, а-я, А-Z, а-z, 0-9, ,, _ , пробел, ()
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@ald.pro	Строка вида "text@text" А-Я, а-я, А-Z, а-z, 0-9, ,, @, _ , -
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@ald.pro	Строка вида "text@text" А-Я, а-я, А-Z, а-z, 0-9, ,, @, _ , -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	А-Z, а-z, 0-9

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144, 8192 192,224,256,384,521
Web-client – шаблон сертификата учетной записи				
CommonName	CommonName	имя web-клиента	Operator01	А-Я, а-я, А-Z, а-z, 0-9, ., _ , пробел, ()
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., -, *
MS UPN, UserPrincipalName	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида “text@text” А-Я, а-я, А-Z, а-z, 0-9, ., @, _ , -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	А-Z, а-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144, 8192 192,224,256,384,521
Web-server – шаблон сертификата web-сервера				
CommonName	CommonName	имя web-сервера	Center01	А-Я, а-я, А-Z, а-z, 0-9, ., _ , пробел, ()
DNS Name	Domain Name System	FQDN (полное доменное имя вашего сервера)	dc1.presale.aeca	Только указанные символы: А-Я, а-я, А-Z, а-z, 0-9, ., -, *

Наименование поля Aladdin ECA	Поле в базе SambaDC, РЕД АДМ, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144,8192 192, 224, 256, 384, 521
S/MIME – шаблон сертификата электронной почты				
CommonName	CommonName	имя пользователя	ivanova	A-Я, а-я, A-Z, a-z, 0-9, ,, _ , -, пробел, ()
RFC 822 Name	userPrincipalName / krbPrincipalName	почтовый адрес пользователя, может совпадать с MS UPN	ivanova@example.com	Строка вида “text@text A-Я, а-я, A-Z, a-z, 0-9, ,, @, _ , -
пароль	-	должен содержать не менее 8 знаков с использованием латинских букв разного регистра и цифр	Example123	A-Z, a-z, 0-9
алгоритм ключа	-	выберите из выпадающего списка	-	RSA, ECDSA
длина ключа	-	выберите из выпадающего списка	-	1024,1536,2048,3072,4096,6144,8192 192,224,256,384,521

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦС	–	Центр сертификатов
АеСА СА	–	Центр сертификатов Aladdin Enterprise Certificate Authority Certified Edition
АеСА VA	–	Aladdin Enterprise Certificate Authority Validation Authority
CN	–	Common Name
CRL	–	Certificate Revocation List, список отозванных сертификатов
Delta CRL	–	список изменений последнего опубликованного списка отозванных сертификатов (CRL)
AIA	–	Authority Information Access
SSL	–	Secure Sockets Layer – протокол безопасности, создающий зашифрованное соединение между web-сервером и web-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.

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.

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.

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.

Разрешённые издатели – это список Центров сертификации, сертификаты которых клиент может использовать для авторизации на сервере, на котором развёрнут Центр сертификации с актуальным списком разрешённых издателей.

Ресурсная система (внешняя) – это подключаемая служба каталогов, которая предоставляет информацию об имеющихся субъектах.

Ресурсная система (локальная) – это ресурсная система, создаваемая автоматически при установке программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», представляющая собой базу данных субъектов и формируемая из сведений, вводимых при выпуске сертификата для нового субъекта.

Сервис валидации – служба, составная часть Центра сертификации, отвечающая за предоставление информации о действительности сертификатов. Предоставляет сервисы CRL DP, OCSP.

Сервис регистрации – служба, составная часть Центра сертификации, отвечающая за обработку запросов на выдачу сертификатов от субъектов информационной системы.

Сервис сертификатов – служба, составная часть Центра сертификации, непосредственно отвечающая за жизненный цикл сертификатов (выдача, отзыв).

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

Сертификат web-сервера – это сертификат, с помощью которого сервер, на котором развёрнут программный компонент «Центр сертификации Aladdin Enterprise Certificate 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 Certificate 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.).

