АКЦИОНЕРНОЕ ОБЩЕСТВО

«Аладдин Р.Д.»

УТВЕРЖДЕН

RU.АЛДЕ.03.01.020-01 32 01-2–ЛУ

ЦЕНТР СЕРТИФИКАТОВ
ALADDIN ENTERPRISE CERTIFICATE AUTHORITY

Руководство администратора. Функции управления

RU.АЛДЕ.03.01.020-01 32 01-2

Листов 142

Содержание

1 ВВЕДЕНИЕ

1.1 Назначение документа

Настоящий документ представляет собой часть 2 руководства администратора Центра сертификатов Aladdin Enterprise Certificate Authority.

1.2 На кого ориентирован данный документ

Документ предназначен для администраторов ПО «Центра сертификатов Aladdin Enterprise Certificate Authority», 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.

1.3 Рекомендации по использованию документа

Документ рекомендуется использовать в качестве подробного руководства по настройке ПО «Центра сертификатов Aladdin Enterprise Certificate Authority», а также в качестве справочника при работе с ПО «Центра сертификатов Aladdin Enterprise Certificate Authority».

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

1.4 Соглашения по оформлению

В данном документе для представления ссылок, терминов и наименований, примеров кода программ используются различные шрифты и средства оформления. Основные типы начертаний текста приведены в таблице 1.

Таблица 1 — Элементы оформления

[Поле]	Используется для выделения наименований полей, блоков, закладок экранных форм
<Кнопка>	Используется для выделения наименований кнопок
Меню:	Используется для выделения наименований пунктов меню
Ctrl+X	Используется для выделения сочетаний клавиш
`file.exe`	Используется для выделения имен файлов, каталогов, текстов программ
Термин	Используется для выделения первого и последующих вхождений определяемого в документе термина в тексте документа
Выделение	Используется для выделения отдельных значимых слов и фраз в тексте
Ссылка (Рисунок 5)	Используется для выделения перекрестных ссылок
Важно	Используется для выделения информации, на которую следует обратить внимание
Рамка	Используется для выделения важной информации, вывод, резюме

1.5 Обозначения и сокращения

Таблица 2 — Обозначения и сокращения

ОС	Операционная система
ПО	Программное обеспечение
СУБД	Система управления базами данных
УЦ	Удостоверяющий центр
ЦС	Центр сертификатов
AeCA, Aladdin eCA	Центр сертификатов Aladdin Enterprise Certificate Authority
AeCA VA	Aladdin Enterprise Certificate Authority Validation Authority
CRL	Certificate Revocation List
AIA	Authority Information Access
URL	Uniform Resource Locator

1.6 Ключевые слова

Администратор безопасности – сотрудник (специалист) и соответствующая роль в центре сертификации отвечающая за администрирование и управление настройками изделия. Физическое лицо (уполномоченный пользователь), имеющее роль «Администратор», должно быть указано в организационно-распорядительных документах организации, эксплуатирующей ПО.

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

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

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.

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

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

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.

Права доступа – набор возможных действий, которые субъекты могут выполнять над субъектами в конкретной среде функционирования.

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.

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).

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. Центр сертификации является частью Центра сертификатов Aladdin Enterprise Certificate Authority.

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.).

OCSP (Online Certificate Status Protocol) – онлайн протокол получения статуса сертификата,RFC2560.

1.7 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 ни явных, ни подразумеваемых гарантий.

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

Государственное регулирование и экспортный контроль

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

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

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

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

1.8 Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

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

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

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

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

Использование ПО

Пользователь вправе:

- воспроизводить ПО путём записи его в память электронно-вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

- встраивать ПО любым способом в продукты и решения Пользователя;

- распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

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

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

- дизайна (графики, расположения элементов оформления и т.п.);

- всех иных элементов, в том числе изображений, фонограмм, текстов.

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

- заменить ПО, если это не противоречит вышеупомянутому ограничению гарантии;

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

- вы незамедлительно вернёте в Компанию все экземпляры ПО и все копии такового и/или сотрёте/удалите любую информацию, содержащуюся в электронном виде.

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

2 ПЕРВИЧНАЯ НАСТРОЙКА ПО ALADDIN ECA

Первичная настройка выполняется для каждого компонента ПО Aladdin eCA – «Центра сертификации» и «Центра валидации».

В результате установки Программного компонента «Центр Сертификации Aladdin eCA» или программного компонента «Центр валидации Aladdin eCA» в консоли ОС отобразится информация о конфигурации установленного приложения и пин-код сертификата, импортируемого в браузер.

Для первичной настройки ПО необходимо установить сертификат в доверенное хранилище сертификатов вашего браузера.

Процесс установки сертификата рассмотрим на примере браузера Firefox:

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

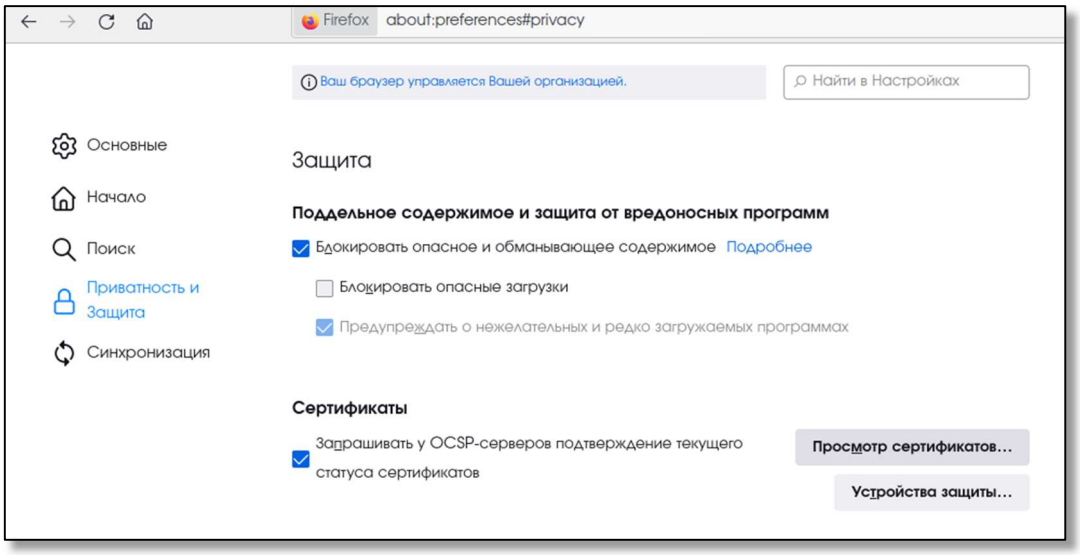


Рисунок 1 – Окно настроек браузера

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

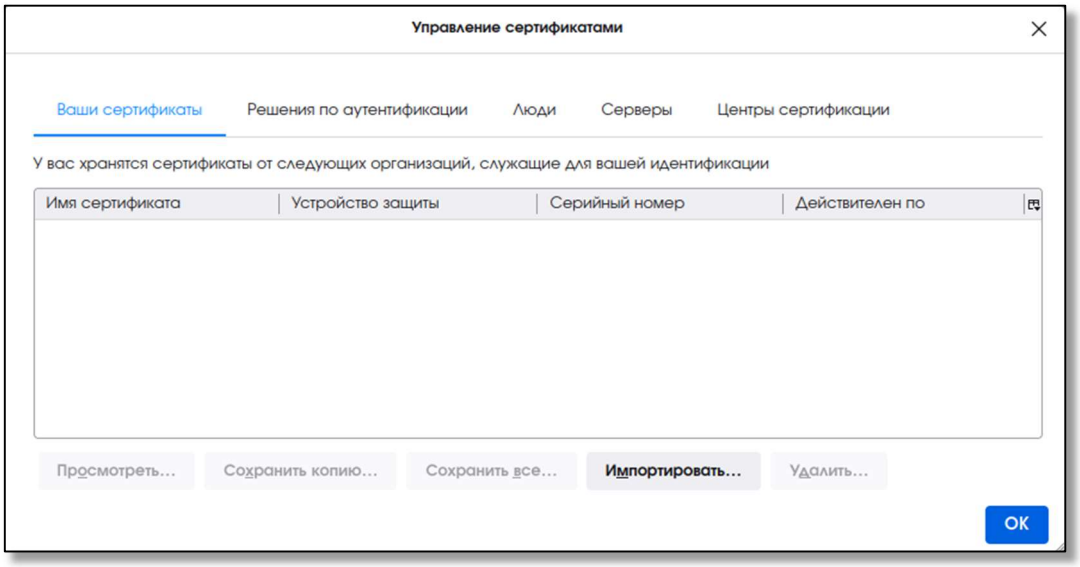


Рисунок 2 – Окно управления сертификатами

- Выберите файл сертификата `/opt/aeca/p12/superadmin.p1` самоподписанный ЦС «ManagmentCA», созданный на этапе установки ПО Aladdin eCA. Нажмите кнопку <Открыть> (см. Рисунок 3).

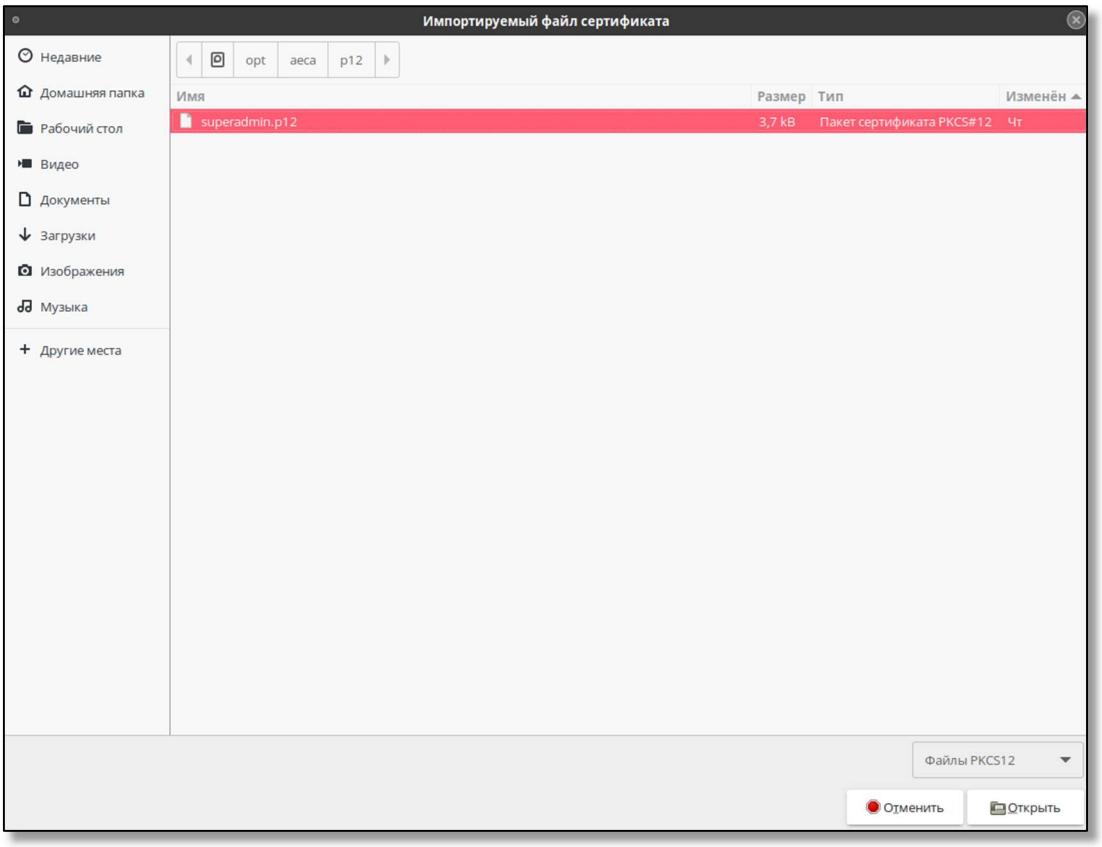


Рисунок 3 – Окно выбора импортируемого файла сертификата

- Введите пин-код сертификата в открывшемся окне и нажмите кнопку <Ок> (см. Рисунок 4). Пин-код предоставляется по завершению установки в окне терминала или доступен в директории установленного приложения `opt\aeca\p12\generated_passwords.txt`, из файла `generated_passwords.txt` данные строки `superadmin_password` (см. Рисунок 5).

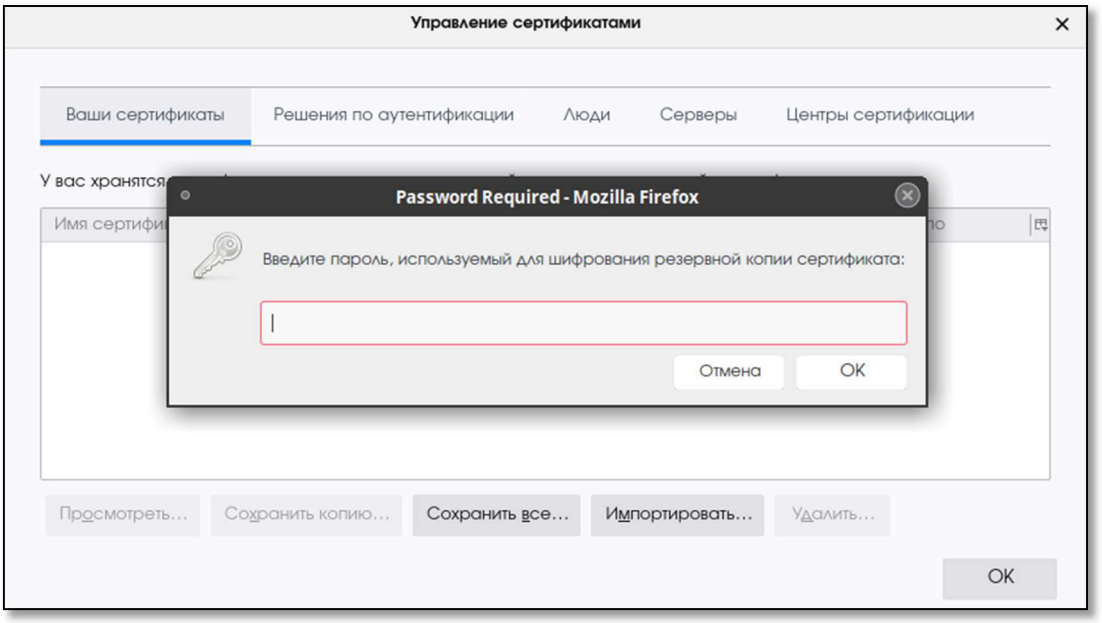


Рисунок 4 – Окно ввода пин-кода сертификата

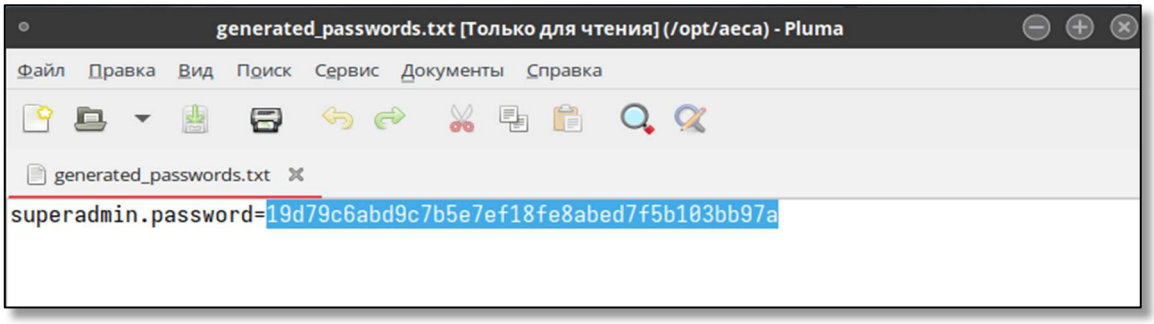


Рисунок 5 – Окно файла generated_passwords.txt

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 6). Нажать кнопку <ОК>.

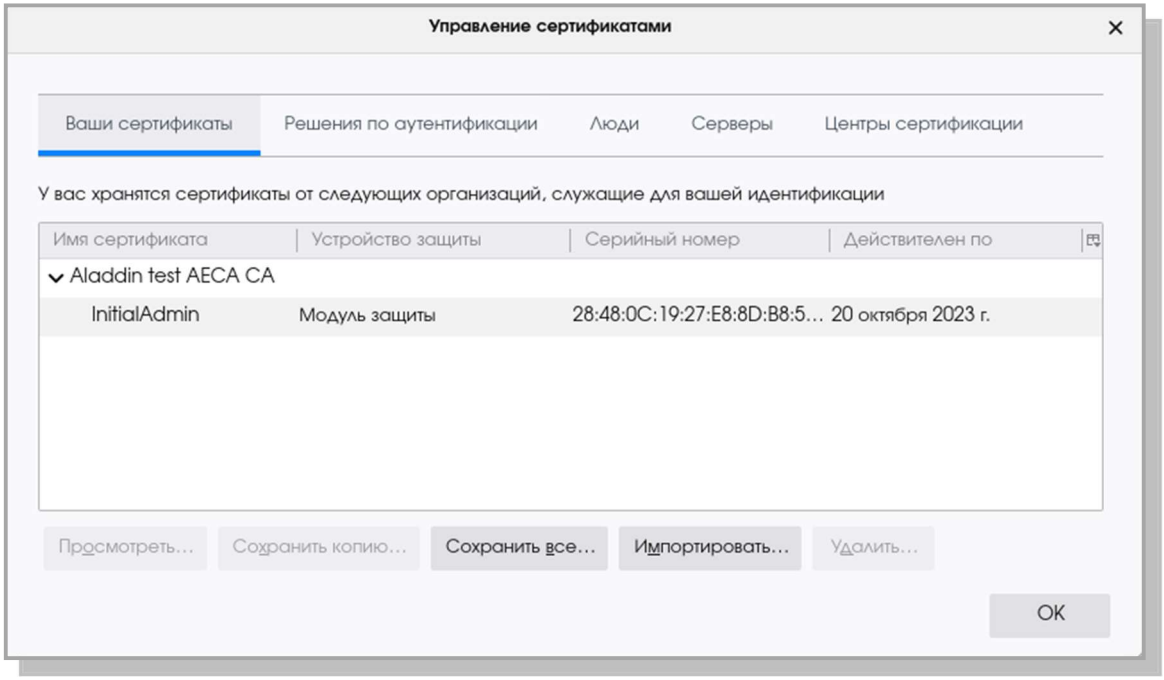


Рисунок 6 – Окно «Управление сертификатами»

- В адресную строку браузера ввести URL-адрес:
  - при настройке «Центра сертификации» ввести адрес в формате:

```
<адрес_хоста_развертывания_продукта>:<порт>/<aecaCa>/
```

где [адрес_хоста_развертывания_продукта] – имя ПК, на котором установлена СУБД, указанное в /opt/aecaCa/scripts/config.sh.

Например:

```
https://localhost:8888/aecaCa/
```

  - при настройке «Центра валидации» ввести адрес в формате:

```
<адрес_хоста_развертывания_продукта>:<порт>/<aecaVa>/
```

где [адрес_хоста_развертывания_продукта] – имя ПК, на котором установлена СУБД, указанное в /opt/aecaVa/scripts/config.sh.

Например:

```
https://localhost:8888/aecaVa/
```

- Если сертификат пользователя не импортирован, то откроется страница с сообщением об ошибке (см. Рисунок 7).

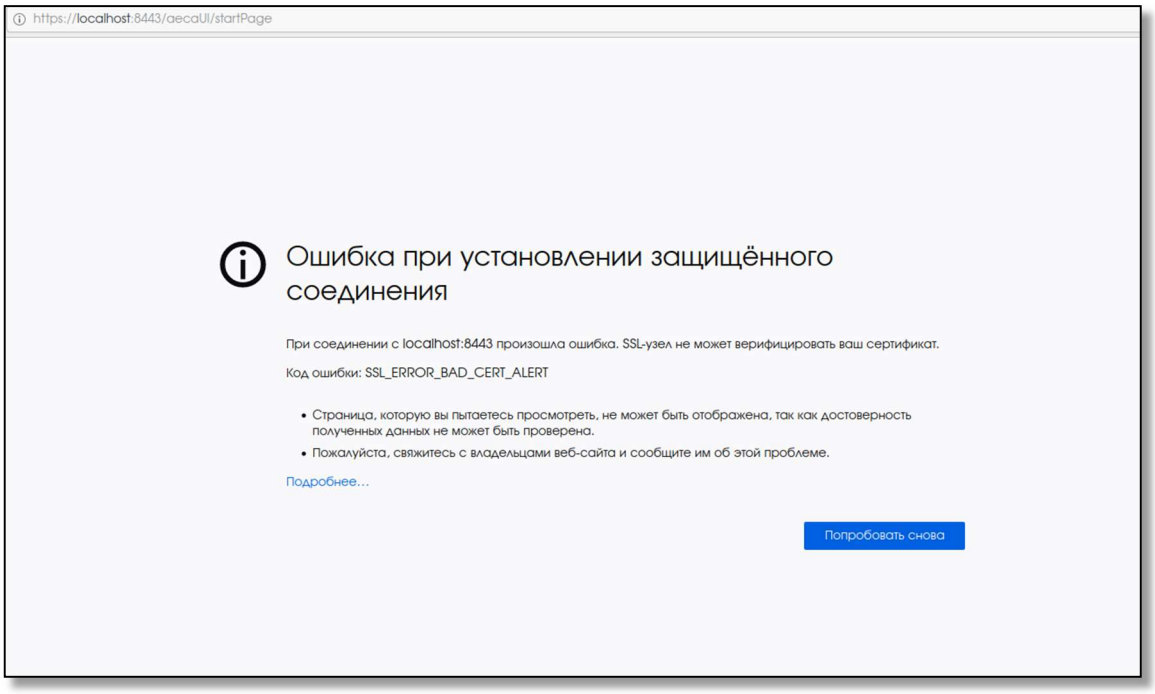


Рисунок 7 – Страница с сообщением об ошибке

- В случае успешной установки сертификата откроется страница с предупреждением системы безопасности (см. Рисунок 8). Нажмите кнопку <Advanced>.

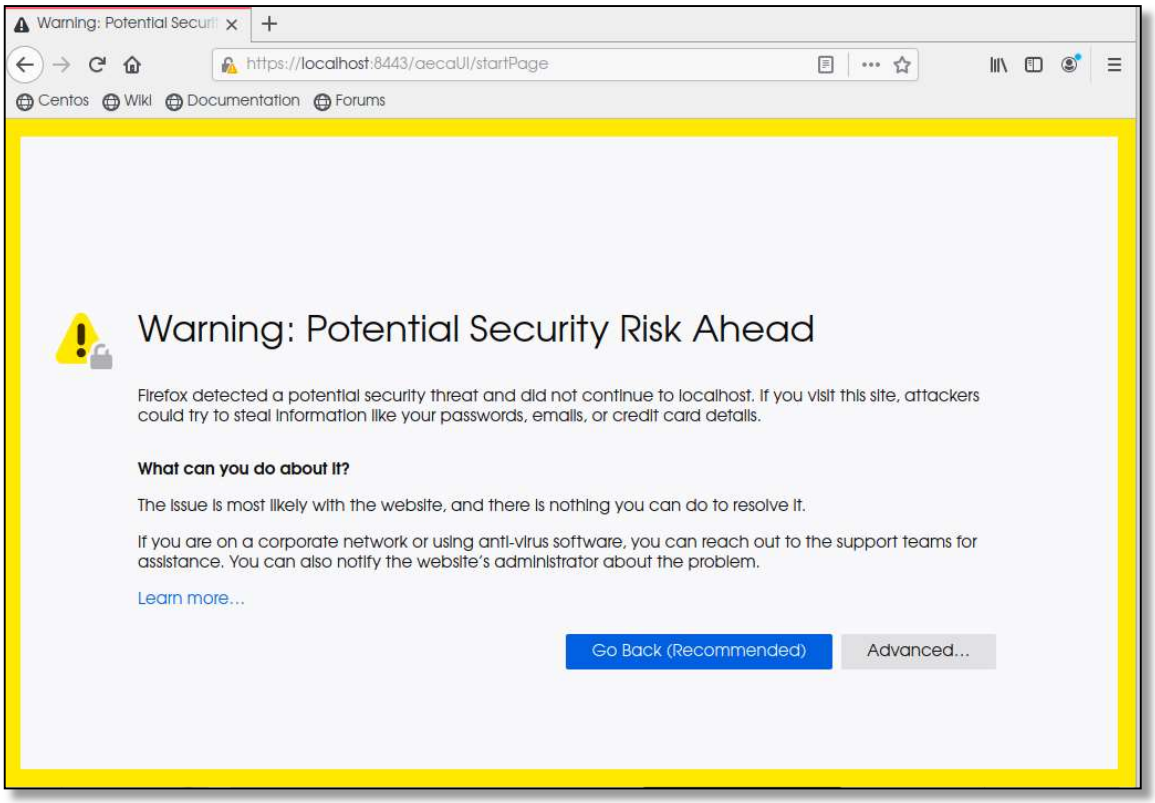


Рисунок 8 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Advanced> на странице предупреждения системы безопасности (см. Рисунок 8) осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 9). Нужно принять риски, нажав кнопку <Accept the Risk and Continue> на текущей странице.

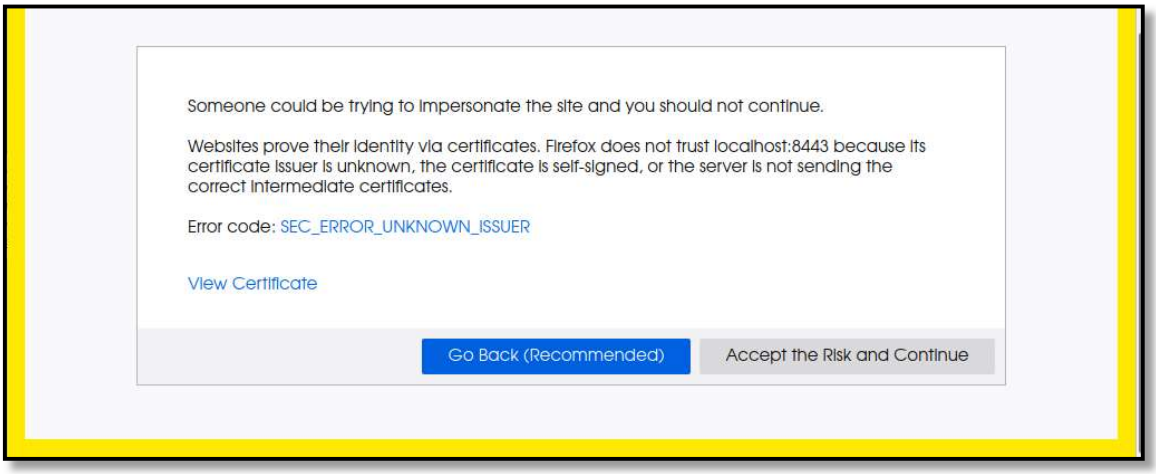


Рисунок 9 – Страница ошибки распознавания сертификата

- Установка и предварительный ввод в эксплуатацию ПО Aladdin eCA завершены, далее следует установить лицензию для компонента «Центр Сертификации» Aladdin eCA с помощью Мастера инициализации.
- Первичная авторизация в открывшемся интерфейсе установленного программного компонента «Центр Сертификации Aladdin eCA» по умолчанию выполняется под учетной записью «supeadmin» с правами администратора (см. Рисунок 10).

Рисунок 10 – Учетная запись пользователя superadmin AeCA CA

- Для работы с ПО Aladdin eCA подключение к глобальной сети Интернет не требуется.

3 ЛИЦЕНЗИРОВАНИЕ «ЦЕНТРА СЕРТИФИКАЦИИ» ALADDIN ECA

3.1 Первичное лицензирование

- После установки компонента ««Центр Сертификации» Aladdin eCA в появившемся окне инициализации необходимо выбрать файл лицензии с расширением .lic (см. Рисунок 11).

Один экземпляр программной лицензии предназначен для работы одного экземпляра компонента «Центр сертификации» Aladdin eCA.

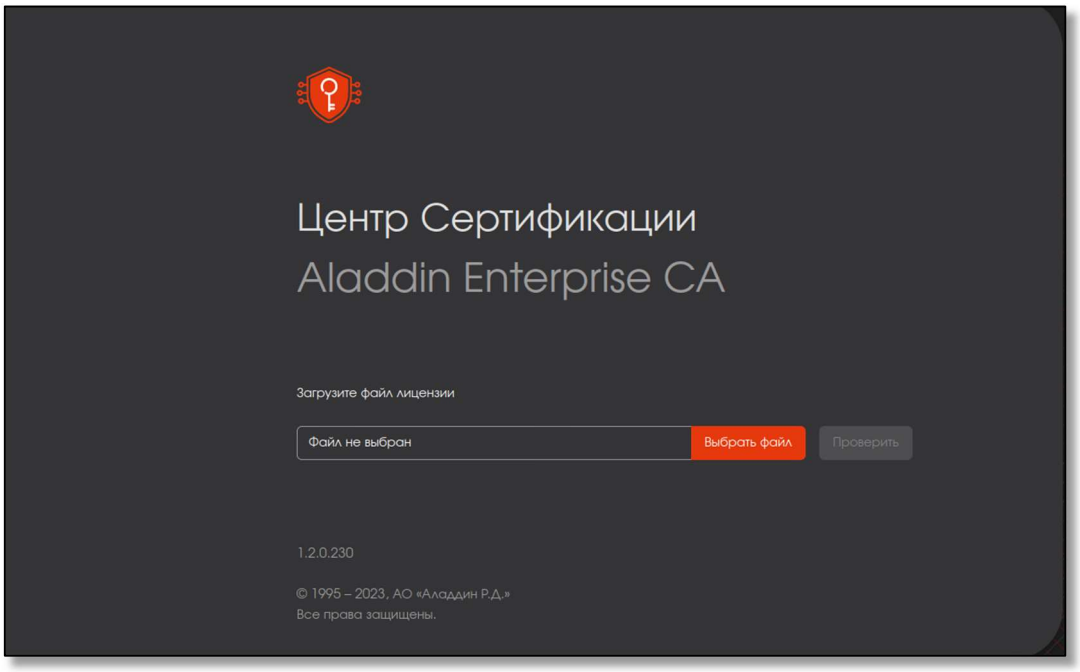


Рисунок 11 – Окно инициализации Центра сертификации. Шаг 1 – выбор лицензии

- Далее нажмите ставшую активной кнопку <Проверить> для проверки валидности файла лицензии (см. Рисунок 12).

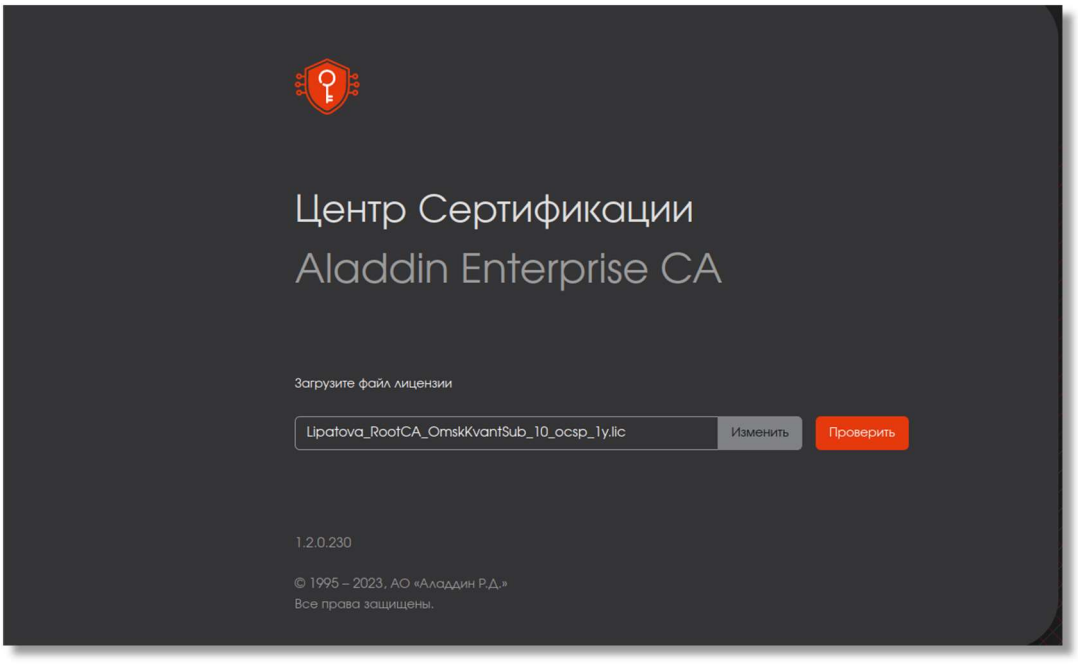


Рисунок 12 – Окно инициализации Центра сертификации. Шаг 1 – проверка лицензии

- 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 13);

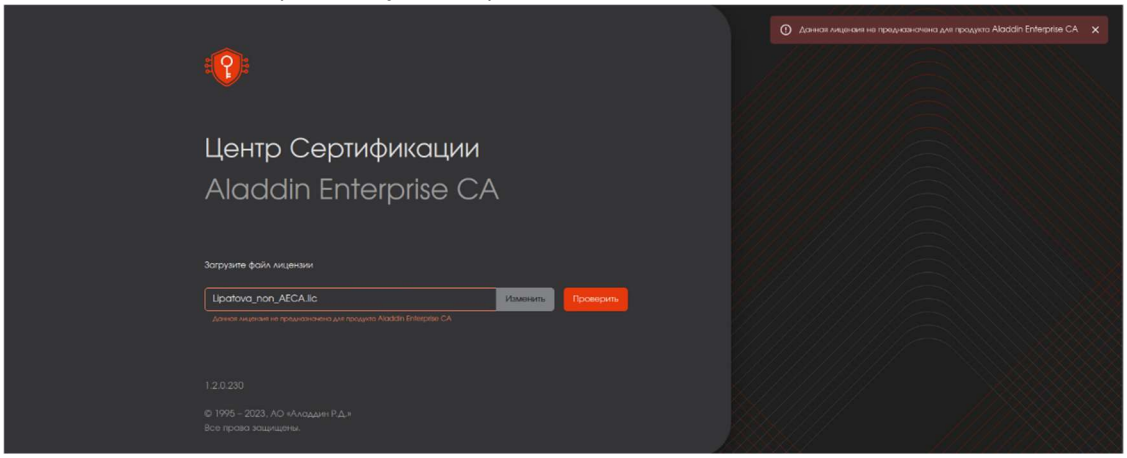


Рисунок 13 - Окно инициализации Центра сертификации. Проверка лицензии. Несовпадение полей

  - при несовпадении подписи лицензии администратор будет уведомлён сообщением на экране «Подпись не верна» (см. Рисунок 14);

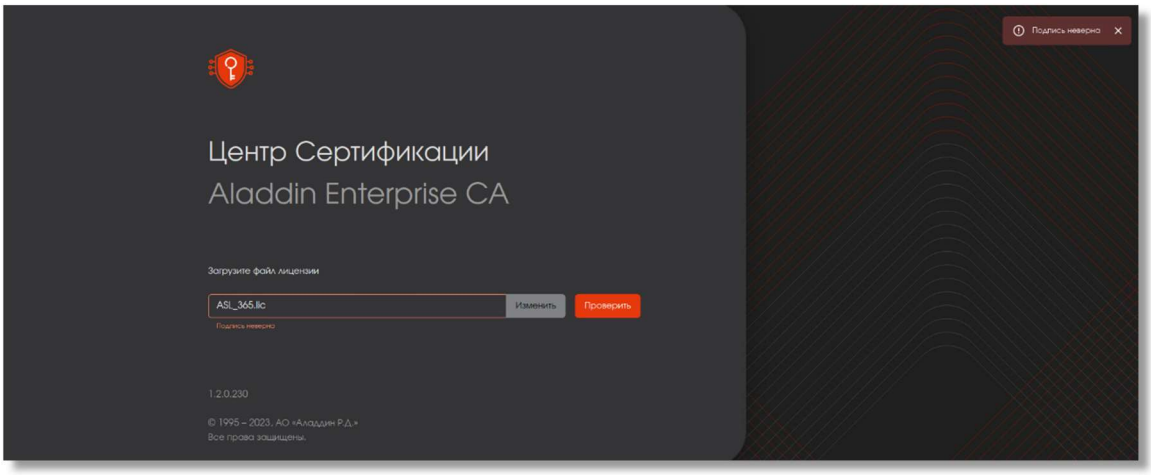


Рисунок 14 – Окно инициализации Центра сертификации. Лицензия предназначена для другого продукта

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

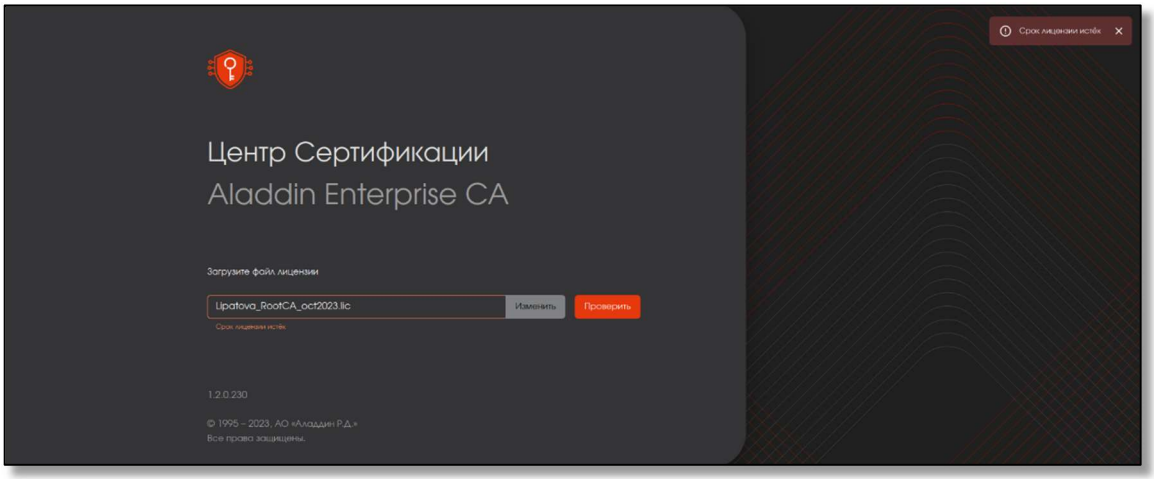


Рисунок 15 - Окно инициализации Центра сертификации. Срок лицензии истёк

- в случае ранее установленной лицензии на текущем рабочем месте и новой установке ПО АеСА 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 16). На экране будут отображены параметры лицензии – имя корневого центра сертификации в поле «Root Common Name» и срок действия лицензии в поле «Действует до».

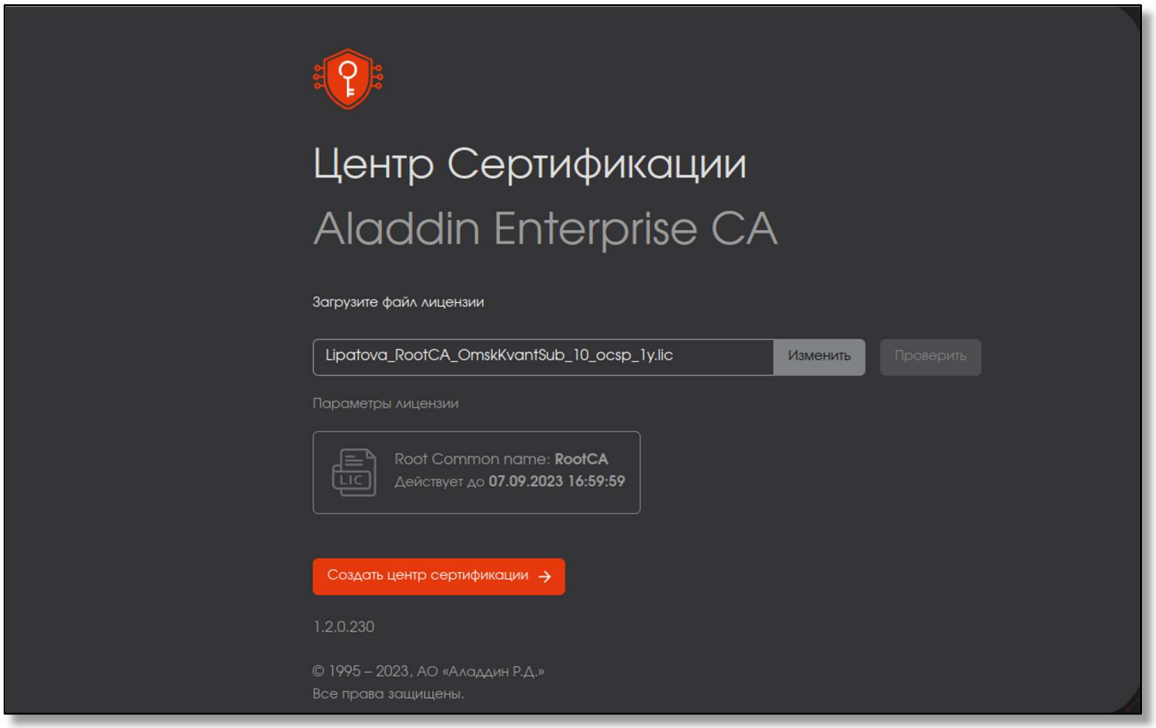


Рисунок 16 – Окно инициализации. Проверка на валидность файла лицензии прошла успешно

- Далее нажмите кнопку <Создать центр сертификации> для перехода к следующему шагу.

3.2 Создание Центра сертификации корневого и подчинённого

3.2.1 **Шаг 2 инициализации центра сертификации**

- На следующем шаге, в зависимости от типа загруженной лицензии, создаётся корневой или подчинённый Центр сертификации (см. Рисунок 17, Рисунок 18).

- Имя центра сертификации (Common Name) задается автоматически, согласно данным лицензии, и не подлежит изменению.

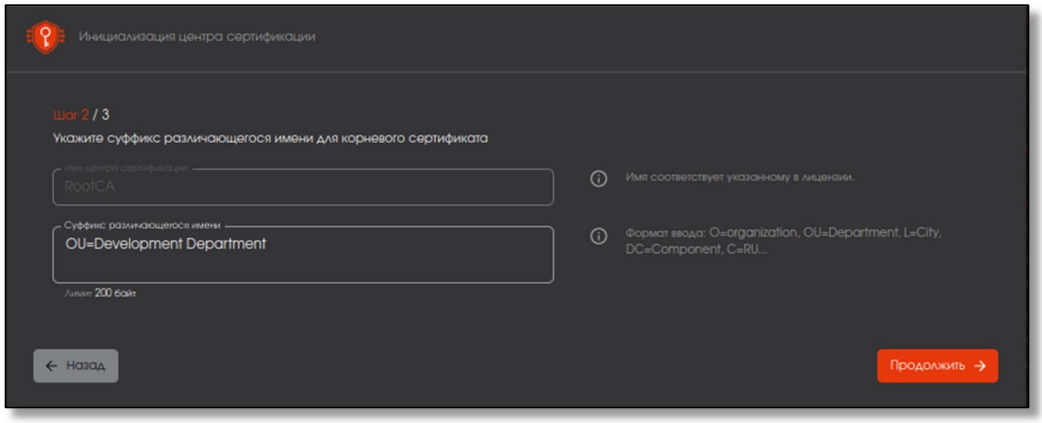


Рисунок 17 – Окно инициализации центра сертификации. Создание корневого ЦС. Шаг 2

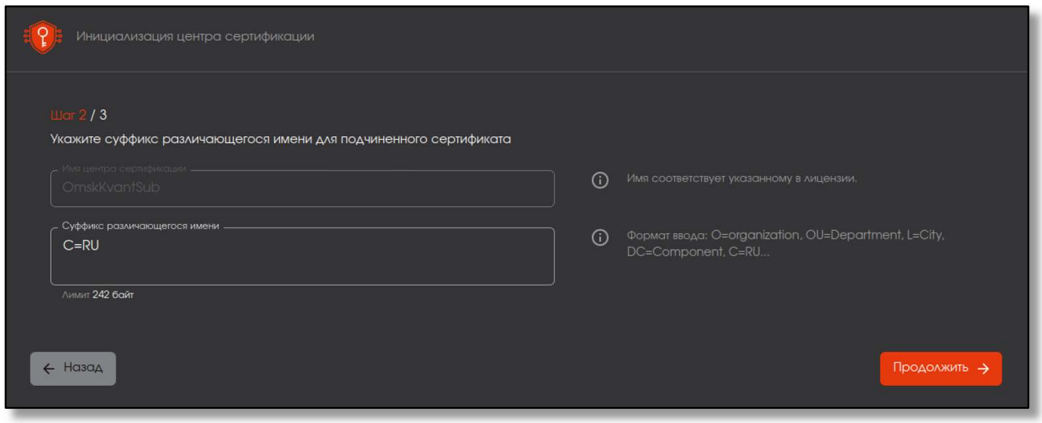


Рисунок 18 – Окно инициализации центра сертификации. Создание подчиненного ЦС. Шаг 2

- В поле «Суффикс различающегося имени» необходимо ввести суффикс различающегося имени ЦС. Суффикс различающегося имени не должно содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами – запятые и запятые с пробелами, ограничение на длину вводимого имени – 250 байт. Поддерживаемые варианты атрибутов суффикса различающегося имени приведены в Таблица 3.

Таблица 3 – Поддерживаемые атрибуты суффикса различающегося имени

Наименование атрибута	Описание атрибута
E=	// E-mail address(электронная почта)
UID=	//Unique Identifier(уникальный идентификатор)
SN=	//Serial number(серийный номер)
GIVENNAME=	//Given name (first name – имя)
INITIALS=	//First name abbreviation(инициалы)
SURNAME=	//Surname (фамилия)
T=	//title(заглавие)
OU=	//Organizational Unit(отдел(организации))
O=	//Organization(организация)
L=	//Locality(район)
ST=	//State or Province(область, край, республика)

Наименование атрибута	Описание атрибута
DC=	//Domain Component(first)(первый доменный компонент, если вводить второй раз, добавит во второй)
C=	// C, Country (страна, вводить согласно - ISO 3166)
UNSTRUCTUREDADDRESS=	//IP address(IP-адрес)
UNSTRUCTUREDNAME=	//Domain name(доменное имя - FQDN)
POSTALCODE=	//postalCode(почтовый индекс)
BUSINESSCATEGORY=	//Organization type(категория(тип) организации)
DN=	//DN Qualifier
POSTALADDRESS=	//postalAddress(почтовый адрес)
TELEPHONENUMBER=	// telephoneNumber(телефонный номер)
PSEUDONYM=	//pseudonym(псевдоним)
STREET=	//streetAddress(адрес - улица)
NAME=	//name(дополнительное имя)
DESCRIPTION=	//Description(краткое описание)

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

3.2.2 **Шаг 3 инициализации**

В открывшемся окне (см. Рисунок 19, Рисунок 20) в соответствующих полях установить:

- параметры криптографии:
  - алгоритм ключа:
    - RSA;
    - ECDSA;
  - длина ключа:
    - 2048;
    - 3072;
    - 4096;
    - 256;
    - 384;
    - 521;
  - алгоритм хэш-суммы:
    - SHA1;
    - SHA256;
    - 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.
- Для подчинённого ЦС срок действия сертификата по умолчанию задаётся равным сроку действия сертификата корневого ЦС.
- После задания значений нажать ставшую активной кнопку <Создать ЦС>.

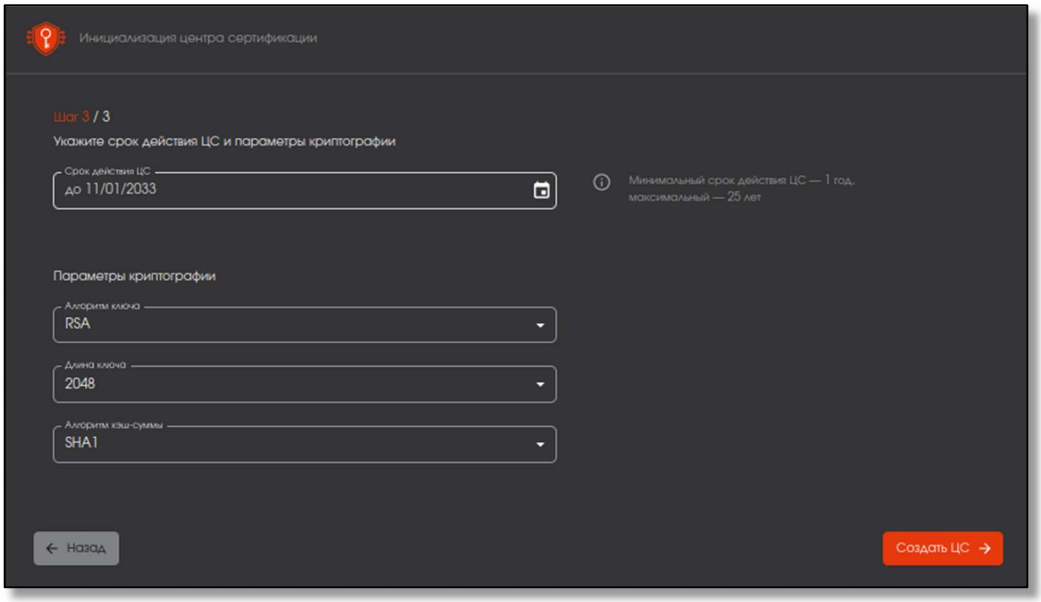


Рисунок 19 – Окно инициализации центра сертификации. Создание корневого ЦС. Шаг 3

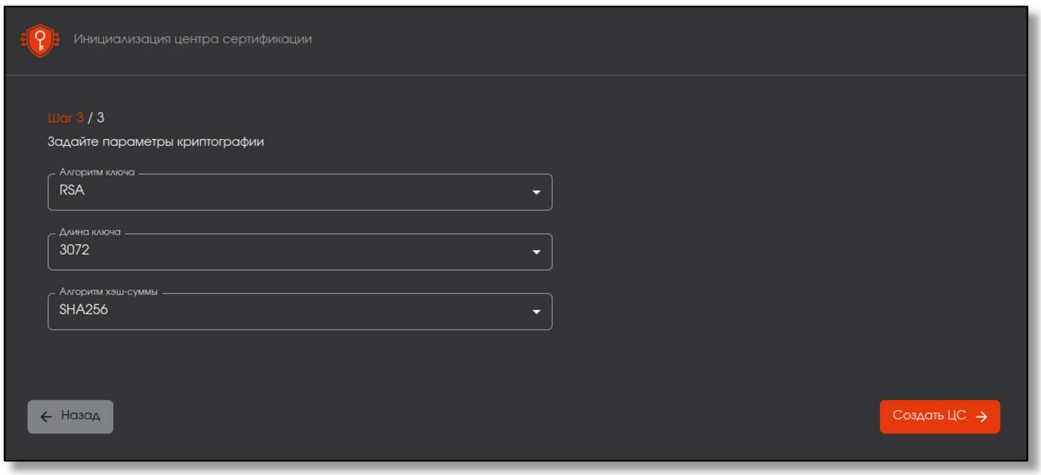


Рисунок 20 – Окно инициализации центра сертификации. Создание подчиненного ЦС. Шаг 3

- В случае неудачной попытки создания ЦС администратор будет уведомлен сообщением (см. Таблица 4).

Таблица 4 – Перечень сообщений в случае неудачной попытки создания ЦС

Текст ошибки	Причина
Ошибка при создании Центра сертификации. Указанное имя уже используется.	Имя, указываемое для ЦС, не является уникальным. Возможно, оно занято технологическим ЦС (имя ЦС, заданное в файле /opt/aecaVa/scripts/config.sh)
Ошибка при создании Центра сертификации <имя>. Введены некорректные данные.	Ошибка валидации из-за ввода некорректных данных
Ошибка при создании подчиненного Центра сертификации <имя>. Введены некорректные данные.	Ошибка валидации из-за ввода некорректных данных
Ошибка при создании Центра сертификации. Неизвестная ошибка.	Внутренняя ошибка ПО.

3.2.3 **Шаг 4 инициализации**

- При успешном создании корневого ЦС и завершении инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 21). Возможно скачать сертификат созданного корневого ЦС.

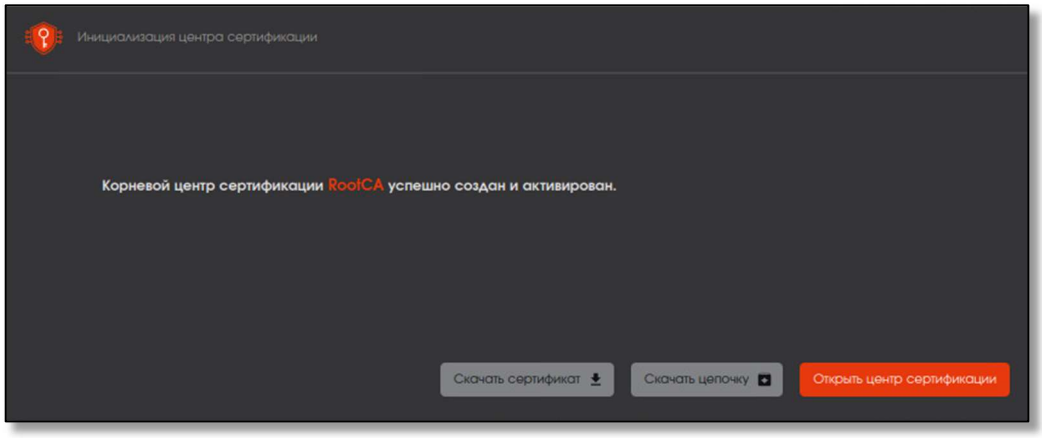


Рисунок 21 – Окно завершения работы инициализации по созданию корневого ЦС

- При успешном создании подчиненного ЦС и завершении инициализации центра сертификации администратор видит соответствующее сообщение (см. Рисунок 22).

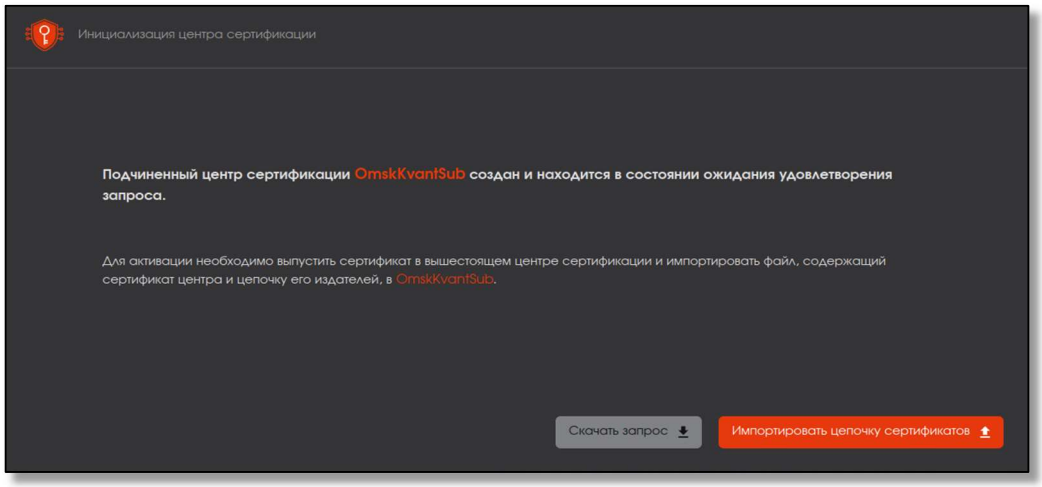


Рисунок 22 – Окно завершения инициализации по созданию подчиненного ЦС

- Скачайте созданный запрос на сертификат подчиненного ЦС.
- 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 4.3.2.2 настоящего руководства администратора) и импорт подписанного сертификата подчиненного ЦС (пункт 4.3.1.3 настоящего документа).

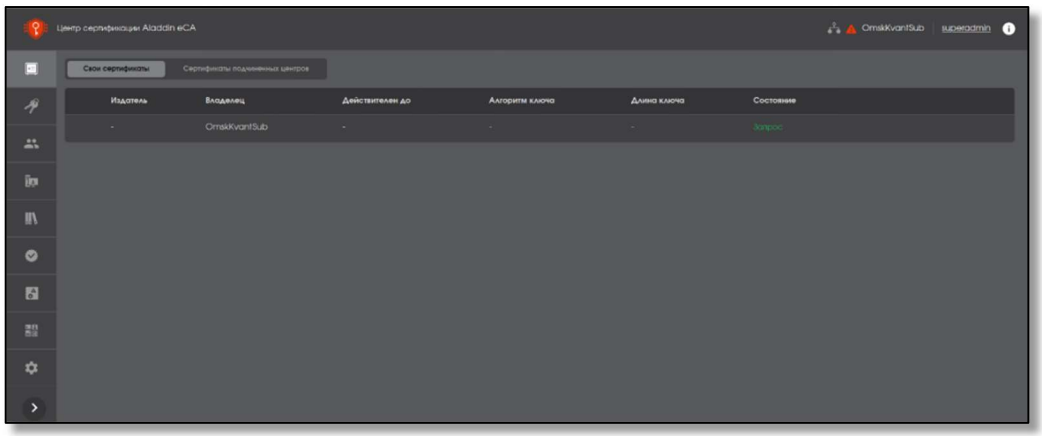


Рисунок 23 – Окно Центра сертификации. Подчинённый ЦС в состоянии «Запрос»

3.3 Ограничение лицензии

- Лицензию необходимо импортировать для каждого разворачиваемого Центра сертификации.
- После установки лицензии на одном рабочем месте возможно развернуть только корневой ЦС с установленным в лицензии именем или подчинённый ЦС с установленным в лицензии именем.
- Лицензия ограничена количеством выпущенных активных сертификатов со сроком окончания действия не менее 30 дней.
- Учёт количества сертификатов отображается на вкладке «О программе» верхней панели экранной формы Центра сертификации (см. Рисунок 24), где:
  - поле «сертификатов активных разрешено» – это максимальное количество активных сертификатов со сроком действия не менее 30 дней;
  - поле «выпущенных» отображает количество активных выпущенных сертификатов без учёта срока действия;
  - поле «истекает срок» отображает количество активных выпущенных сертификатов, у которых срок действия менее 30 дней;
  - поле «для выпуска доступно» отображает количество доступных для выпуска сертификатов, которое рассчитывается, как разность между количеством разрешенных лицензией для выпуска сертификатов и активных выпущенных сертификатов со сроком действия не менее 30 дней.

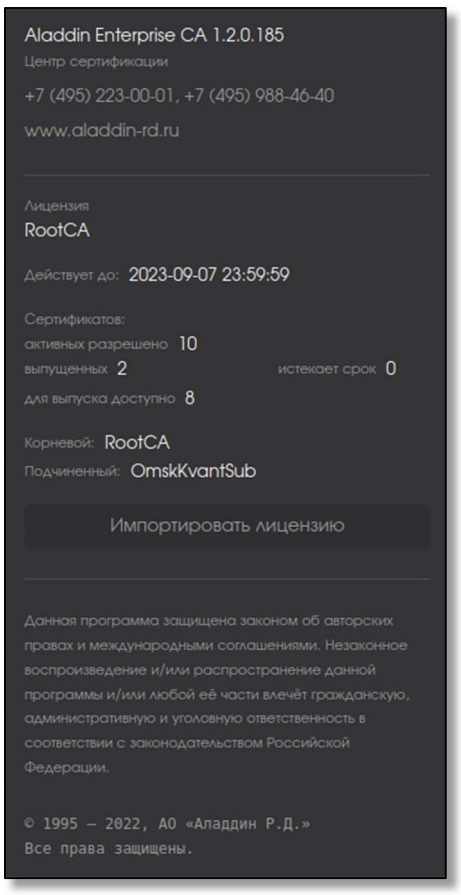


Рисунок 24 – Окно «О программе»

3.4 Окончание срока действия лицензии

- После истечения срока действия лицензии функция выпуска сертификатов субъектов станет недоступна. Кнопки <Создать сертификат> на вкладке «Центр сертификации» и «Сертификаты», кнопка <Подписать запрос> на вкладке «Центр сертификации» будут заблокированы. При наведении на заблокированные кнопки будет показано сообщение о причинах блокировки «Вы достигли лимита лицензии на количество сертификатов» (см. Рисунок 25).

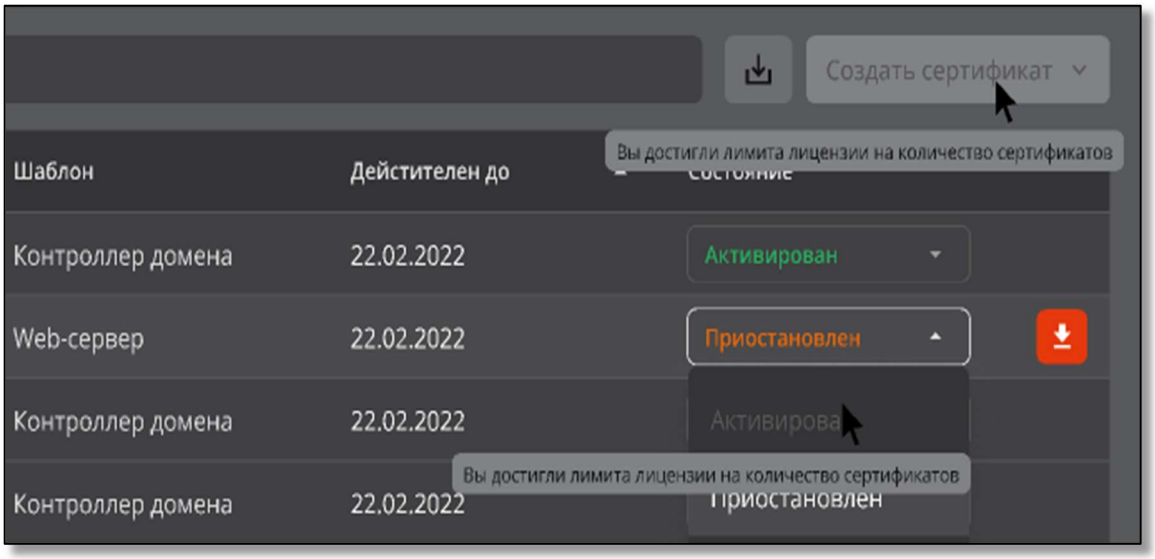


Рисунок 25 – Заблокированная кнопка <Создать сертификат> по истечении срока действия лицензии

3.5 Продление срока действия лицензии

- Для доступа к полному функционалу ПО «Центр сертификации» Aladdin eCA необходимо загрузить действительную лицензию, нажав кнопку <Импортировать лицензию> в окне «О программе» (см. Рисунок 26), расположенном на верхней панели экранной формы «Центра сертификации».

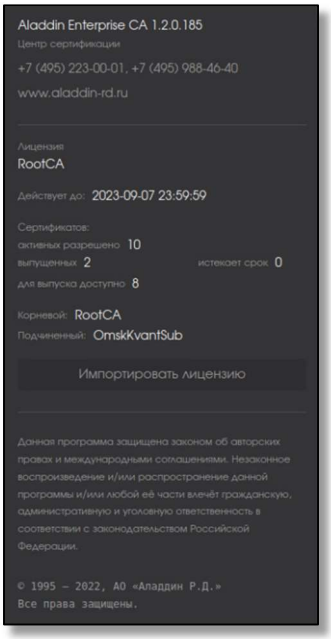


Рисунок 26 – Окно «о программе»

- В открывшемся окне импорта лицензии выберите файл лицензии в формате .lic.

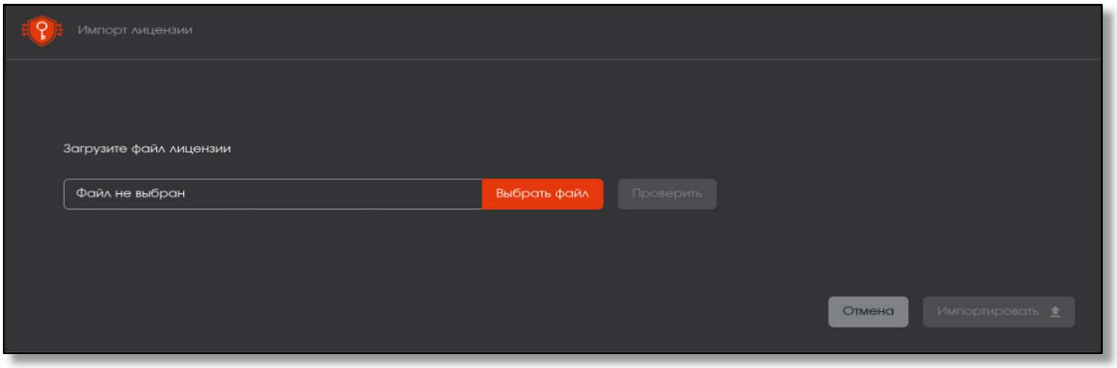


Рисунок 27 – Окно импорта лицензии

- После выбора файла лицензии нажмите ставшую активной кнопку <Проверить> (см. Рисунок 28). Происходит проверка цифровой подписи файла лицензии, срока действия лицензии и ключевых полей файла лицензии «productId» и «id».

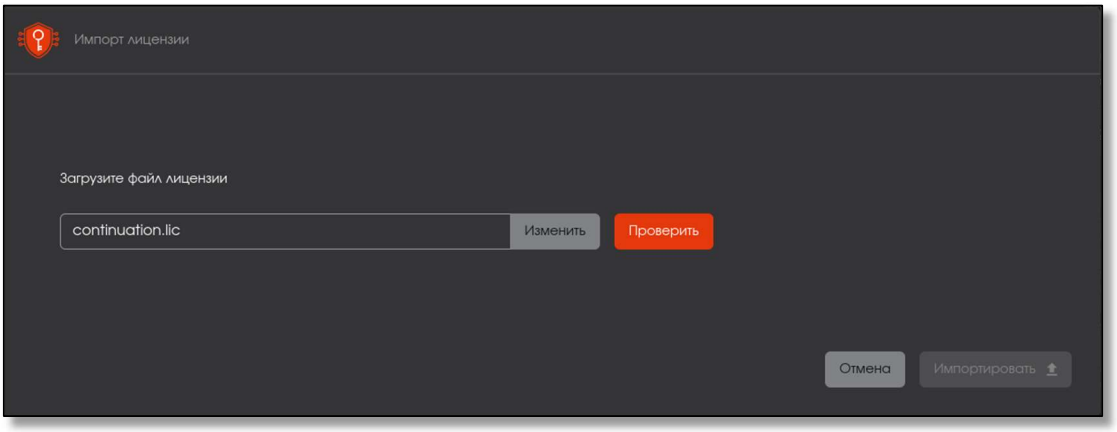


Рисунок 28 – Окно импорта лицензии после выбора файла лицензии

- По результатам успешной проверки на валидность в текущем окне будут показаны параметры загружаемой лицензии:
  - имя корневого центра сертификации в поле «Root Common Name»;
  - срок действия лицензии в поле «Действует до».

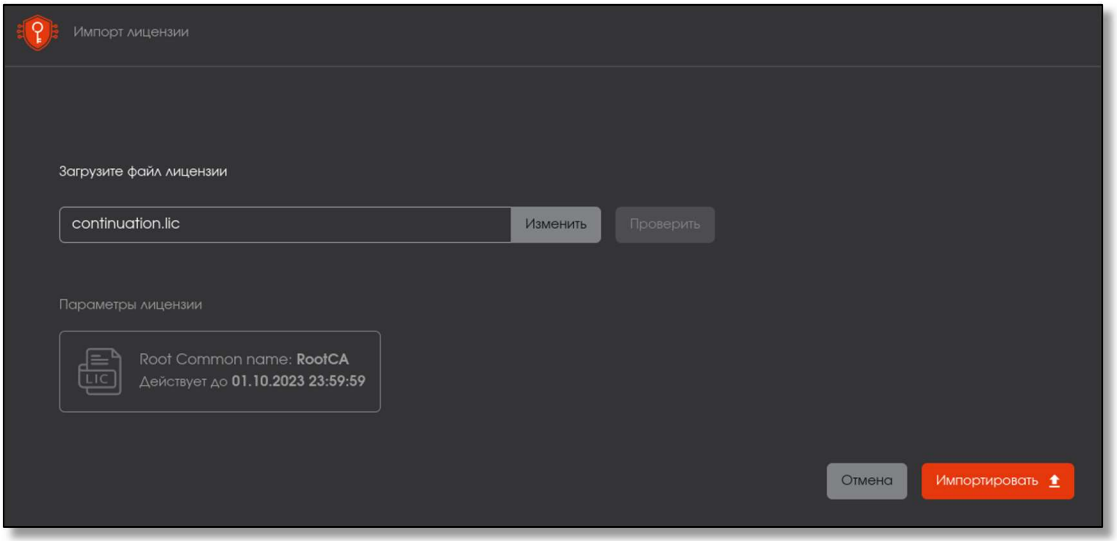


Рисунок 29 – Окно импорта лицензии после успешной проверки на валидность

- Нажмите кнопку <Импортировать> для установки лицензии.
- После успешного импорта лицензии будет выведено на экран уведомление об успешной установке лицензии «Успешно сохранено» и обновлены данные лицензии в поле «Действует до» окна «О программе».
- 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».

4 НАСТРОЙКА «ЦЕНТРА СЕРТИФИКАЦИИ ALADDIN ECA»

4.1 Описание верхней панели «Центра сертификации»

Верхняя панель (см. Рисунок 30) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.

Рисунок 30 – 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);

- 

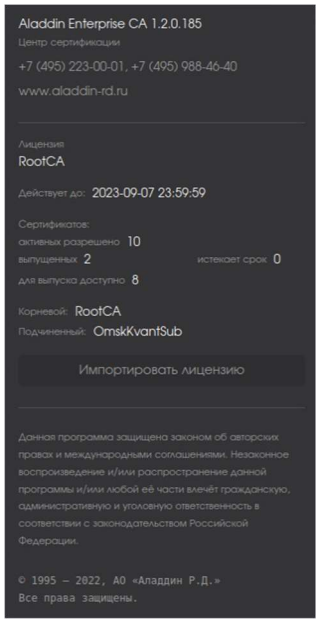
- обозначение статуса ЦС, возможные варианты:
  - «активный» – соответствует зеленому цвету иконки,
  - «не инициализирован» – соответствует красному цвету иконки,
  - «истек срок действия сертификата» – соответствует оранжевому цвету иконки,
  - «истек срок действия лицензии» – соответствует красному цвету иконки);

- 

- имя текущего активного ЦС (при наведении курсора всплывают заданные имя и значения суффикса различающегося имени ЦС);

- 

- текущая авторизация учётной записи пользователя;

- 

- сведения о текущей версии ПО, контактная информация разработчика, информация о лицензии.
По нажатию на кнопку <Импортировать лицензию> возможно загрузить обновление лицензии.

4.2 Описание боковой панели «Центра сертификации»

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

Полный вид боковой панели показан на Рисунок 31, компактный вид боковой панели приведен на Рисунок 32. Выбор вида боковой панели происходит по нажатию кнопки , расположенной внизу данной панели.

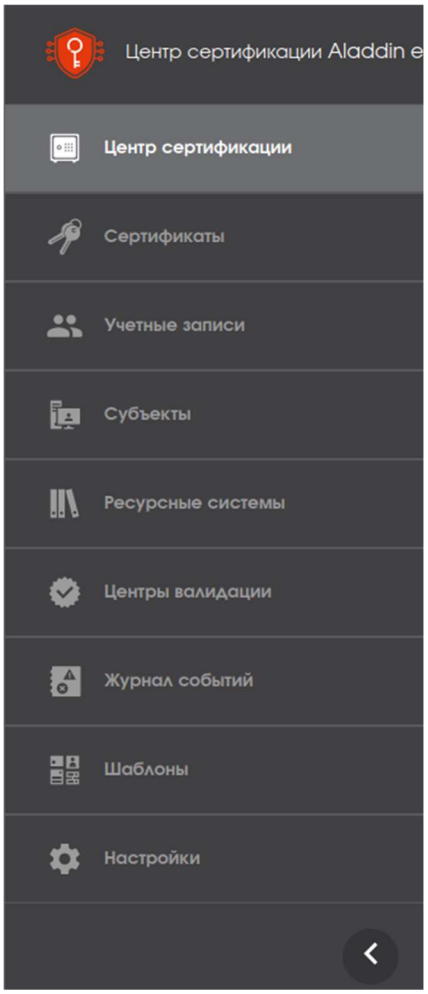


Рисунок 31 – Полный вид боковой панели

Рисунок 32 – Компактный вид боковой панели

Боковая панель состоит из вкладок, определяющих соответствующие функции ПО АЕСА СА и созданы для организации управления Центром сертификации:

- Вкладка «Центр сертификации» – на данной вкладке 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;
- Вкладка «Сертификаты» – на данной вкладке 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 для активного 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 список всех выпущенных сертификатов в формате .csv;

- Вкладка «Учетные записи» – на данной вкладке 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»;
- Вкладка «Субъекты» – на данной вкладке возможно:
  - произвести поиск субъекта по его имени (или части имени);
  - обновить список групп и субъектов;
  - посмотреть организационные группы с субъектами локальной и подключенных ресурсных систем;
  - посмотреть существующие субъекты;
  - выпустить сертификат с закрытым ключом PKCS#12 для каждого субъекта;
  - выпустить сертификат на ключевом носителе для каждого субъекта;
  - посмотреть все выпущенные сертификаты для каждого субъекта;
  - создать учётную запись для субъекта из группы «Users»;
  - посмотреть карточку субъекта;
- Вкладка «Ресурсная система» – на данной вкладке возможно:
  - подключить ресурсную систему для управления сертификатами доменных пользователей и других субъектов.
- Вкладка «Центры валидации» – на данной вкладке возможно:
  - настроить параметры рассылки CRL;
  - зарегистрировать Центры валидации;
  - просмотреть список уже зарегистрированных центров валидации.

- Вкладка «Журнал событий» – на данной вкладке возможно скачать журнал событий в формате .csv по выбранным параметрам экспорта.

- Вкладка «Шаблоны» – на данной вкладке 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.

- Вкладка «Настройки» – на данной вкладке производится настройка аутентификации при подключении в веб-серверу и смена сертификата текущего веб-сервера.

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

4.3 Описание вкладки «Центр сертификации»

Переход на экран управления центра сертификации осуществляется по выбору вкладки «Центр сертификации» бокового меню, расположенного слева на главном экране (см. Рисунок 31).

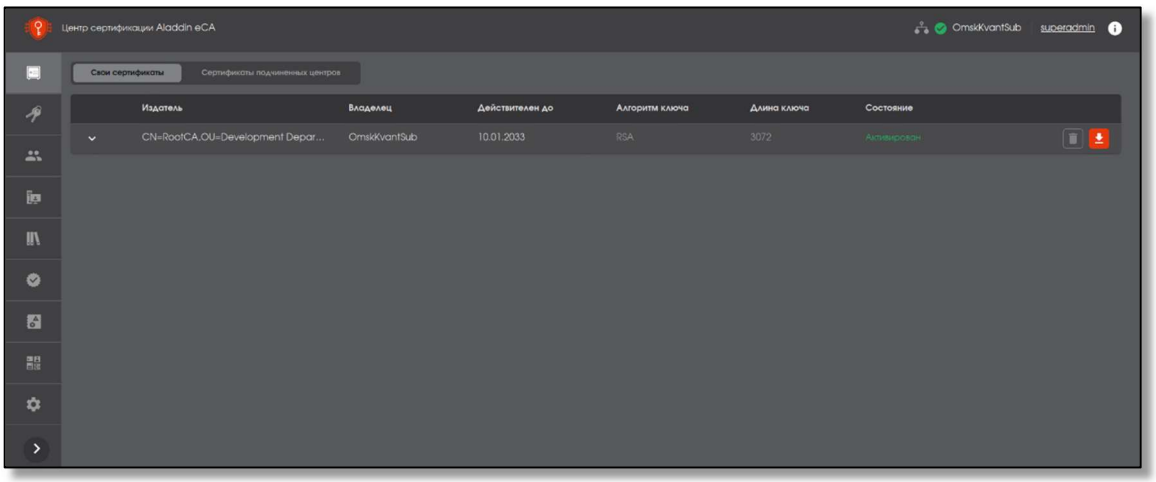


Рисунок 33 - Экран раздела меню "Центр сертификации"

4.3.1 **Вкладка «Свои сертификаты»**

- Вкладка «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).
- Для сертификата ЦС АЕСА из категории «Свои сертификаты», имеющего статус «активный», доступны настройки, в том числе создание и перенастройка сервисов публикации CRL DP и службы OCSP на вкладке «Центры валидации».
- Информационные элементы вкладки «Свои сертификаты» - неуправляемые (табличные поля):
  - издатель;
  - владелец;
  - действителен по (дата);
  - алгоритм ключа;
  - длина ключа;
  - состояние (варианты состояния: активирован, запрос, отозван, истёк срок).
- При наведении указателя мыши на Центр сертификации доступны действия:
  - по нажатию на кнопку  <Удалить> удалить Центр сертификации;
  - по нажатию на кнопку  <Скачать> в сплывающем подменю возможно выполнить действия:

- скачать сертификат;
- скачать цепочку сертификатов;
- скачать список отозванных сертификатов.

В обычном состоянии, без наведения указателя, управляемые элементы сертификата не отображаются.

- Для каждого сертификата возможно просмотреть цепочку сертификатов (см. Рисунок 34), нажав кнопку в строке слева от имени сертификата.

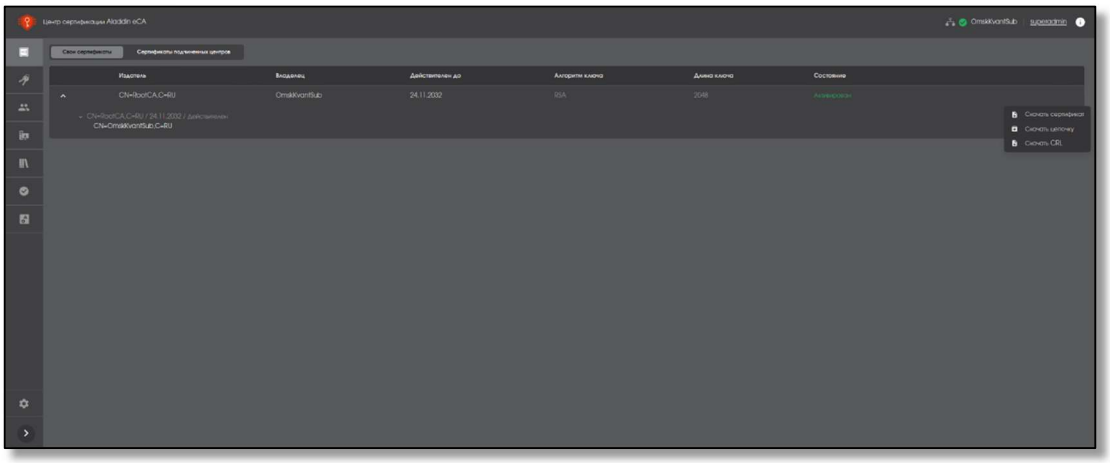


Рисунок 34 – Просмотр цепочки сертификатов

4.3.1.1 Карточка сертификата ЦС

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» (см. Рисунок 35).

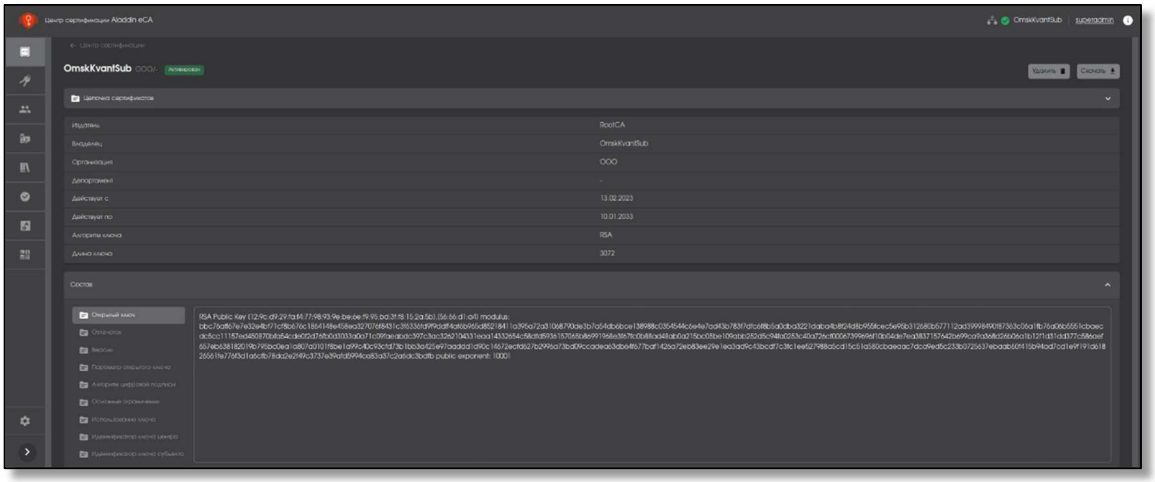


Рисунок 35 - Состояние «Активирован»

- В карточке активного ЦС доступны следующие действия:
  - выгрузить сертификат по нажатию кнопки <Скачать>;
  - удалить Центр сертификаци по нажатию кнопки <Удалить>.
- В карточке Центра сертификации отображаются следующие сведения:
  - издатель;
  - владелец;
  - организация;

- департамент;
- срок действия («действует с», «действует до»);
- алгоритм ключа;
- длина ключа;
- состав:
    - открытый ключ;
    - отпечаток;
    - версия;
    - параметры открытого ключа;
    - алгоритм цифровой подписи;
    - основные ограничения;
    - использование ключа;
    - идентификатор ключа центра;
    - идентификатор ключа субъекта.

4.3.1.2 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 36).
- Нажать появившуюся в строке выбранного ЦС кнопку  и скачать запрос в формате .csr.

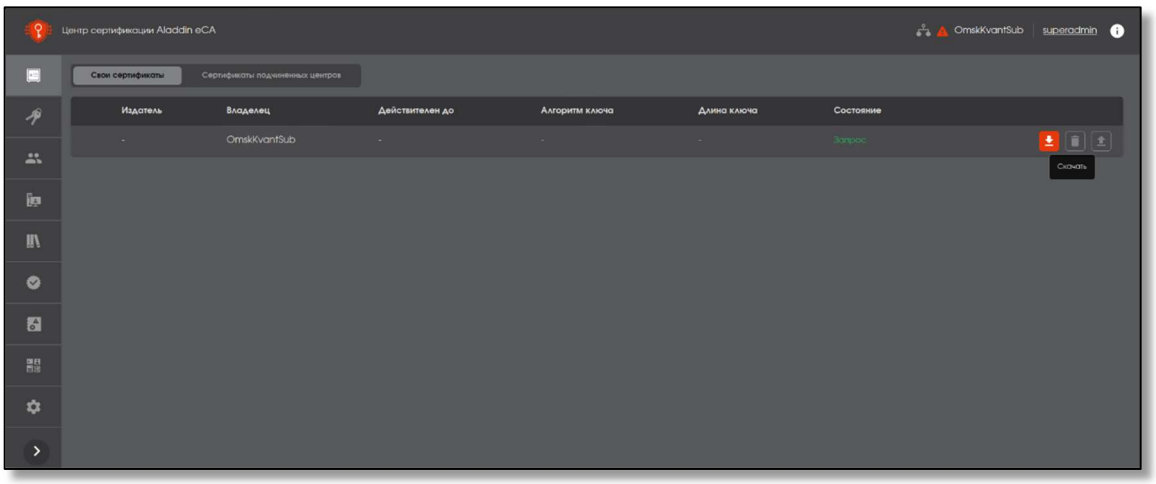


Рисунок 36 – Окно скачивания запроса на сертификат для подчинённого ЦС

- Далее следует подписать скачанный запрос на корневом Центре сертификации согласно пункту 4.3.2.2 настоящего руководства администратора.

4.3.1.3 Импорт сертификата подчиненного ЦС

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

- После подписания запроса на сертификат на корневом ЦС необходимо импортировать данный сертификат для ЦС в состоянии «Запрос».
- На вкладке «Свои сертификаты» выбрать подчиненный ЦС в состоянии «Запрос», по запросу которого был сформирован сертификат формата .pem и цепочка сертификатов в формате .chain.pem в подразделе 4.3.2.2 данного руководства. Нажать кнопку <Загрузить> (см. Рисунок 36).
- Далее в появившемся окне импорта цепочки сертификатов (см. Рисунок 37) выбрать скачанный ранее файл цепочки сертификата для загрузки в формате .chain.pem. Нажать кнопку <Загрузить>, активированную после выбора файла цепочки сертификатов.

Рисунок 37 - Окно импорта цепочки сертификатов

- После успешной загрузки цепочки сертификатов открывается окно с уведомлением об успешной загрузке сертификата (см. Рисунок 38) и отображается следующая информация:
  - издатель;
  - субъект;
  - срок действия сертификата.

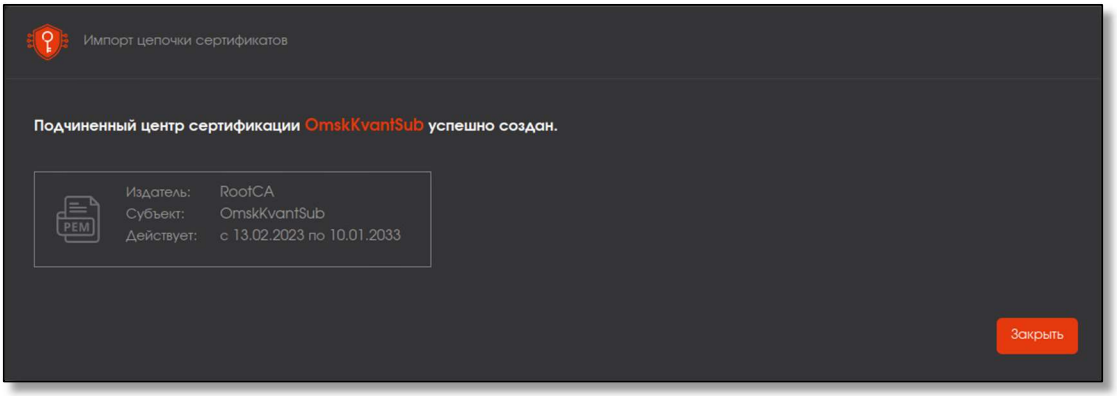


Рисунок 38 – Окно уведомления об успешном загрузки сертификата

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

4.3.1.4 Удаление активного ЦС

- 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 39).

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;**
- **настроенные Центры валидации AeCA CA.**

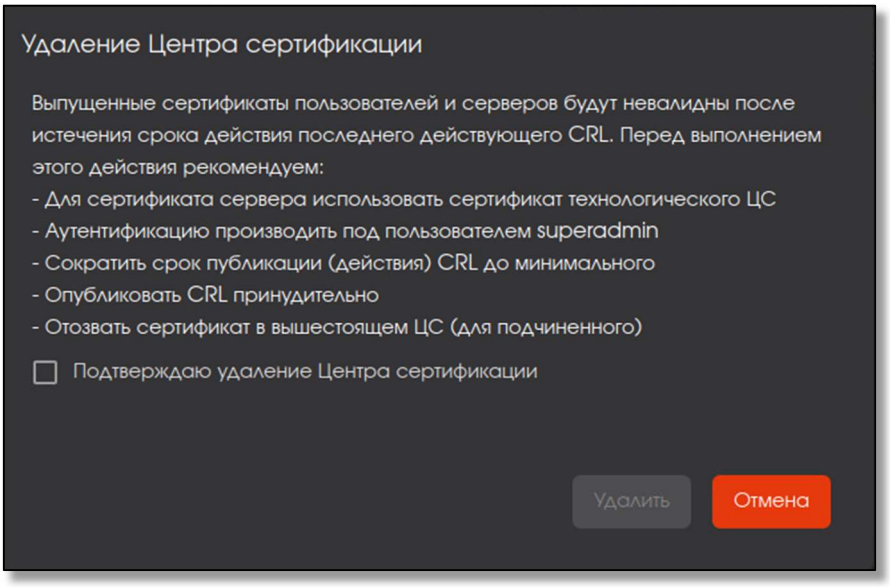


Рисунок 39 – Окно подтверждения удаления Центра сертификации

- 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 40). Для прерывания процесса удаления ЦС нажмите кнопку <Отмена>.

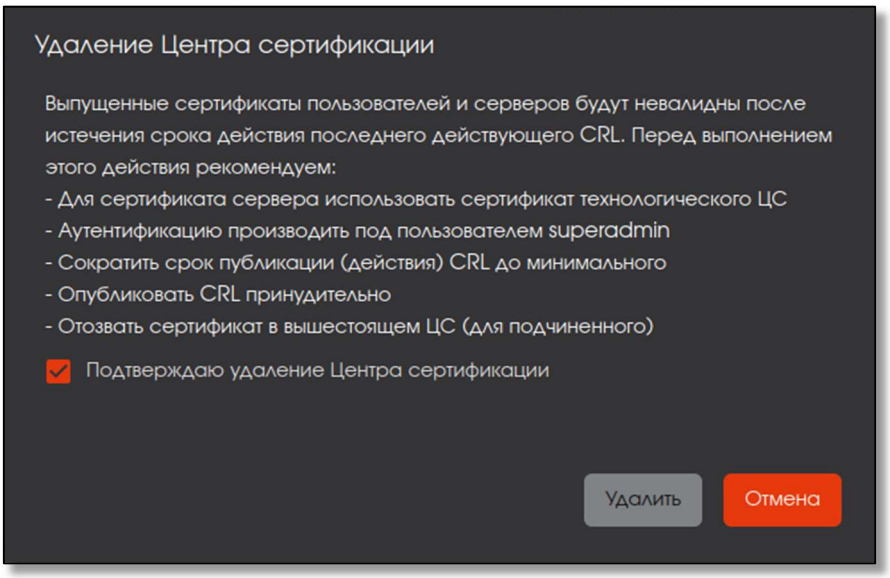


Рисунок 40 – Окно подтверждения удаления Центра сертификации. Чек-бокс подтверждения активирован

- После удаления Центра сертификации происходит переход к окну загрузки лицензии. Текущая лицензия установлена, но есть возможность при необходимости загрузить и установить новую лицензию (см. Рисунок 41).

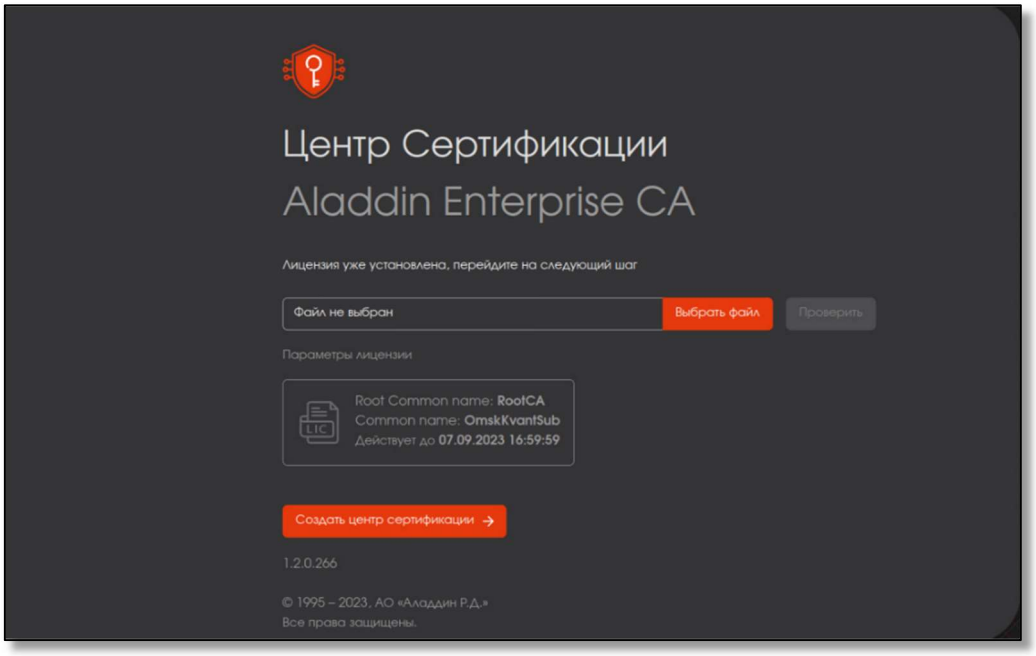


Рисунок 41 – Окно загрузки лицензии после удаления ЦС

- После создания Центра сертификации с использованием текущей установленной или новой лицензии будут восстановлены:
  - ранее зарегистрированные ресурсные системы;
  - загруженные субъекты ранее зарегистрированных ресурсных систем;
  - шаблоны;
  - учётные записи;
  - журнал событий, также содержащий событие удаления ЦС с кодом CAENV038.

4.3.2 **Вкладка «Сертификаты подчиненных центров»**

- Вкладка «Сертификаты подчиненных центров» (см. Рисунок 42) 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 5.
- Нажатие на кнопку <Подписать запрос+> запускает сценарий подписи запроса подчиненного ЦС из категории «Сертификаты подчиненных центров».

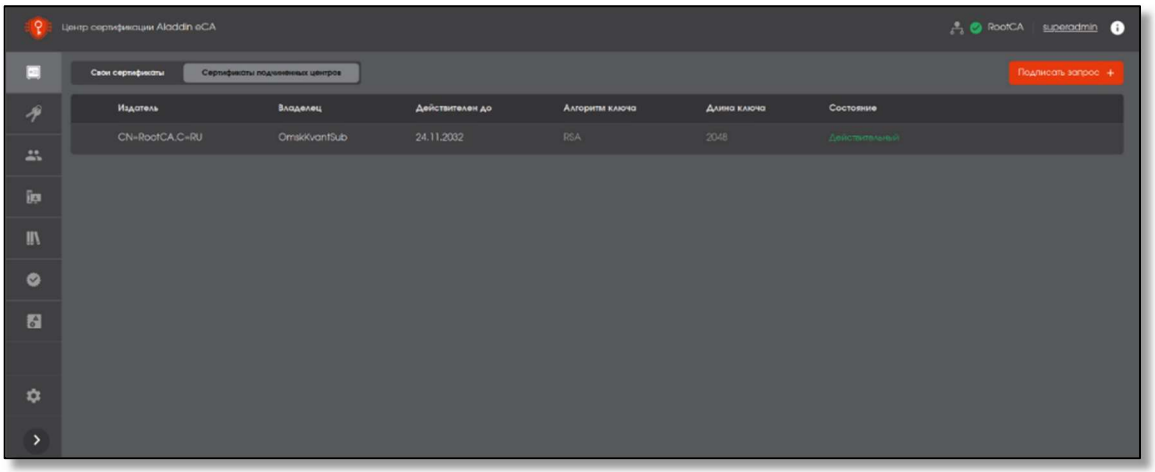


Рисунок 42 - Экран «Сертификаты подчиненных центров»

- Информационные элементы экрана «Сертификаты подчиненных центров» – неуправляемые табличные поля:
  - издатель;
  - владелец;
  - действует с (дата);
  - действует по (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 5.

Таблица 5 – 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.

4.3.2.1 Карточка сертификата ЦС

- Переход к экрану «Карточка сертификата ЦС» осуществляется при нажатии на строку сертификата таблицы на вкладке «Свои сертификаты» (см. Рисунок 35).

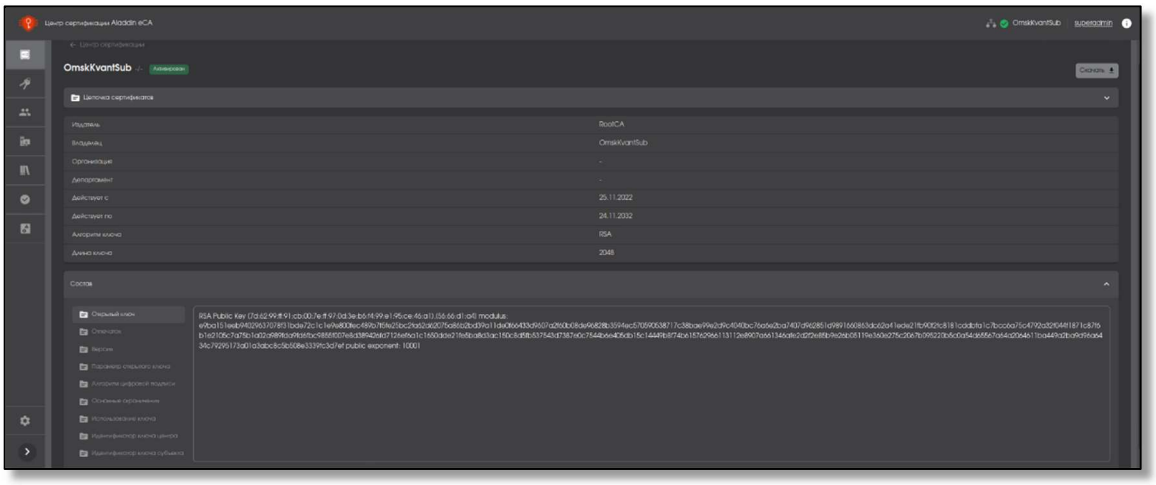


Рисунок 43 – Экран карточки сертификата подчинённого ЦС в состоянии «Действительный»

- В карточке ЦС со статусом сертификата «Действительный» возможно выгрузить сертификат по нажатию кнопки <Скачать> и отозвать сертификат ЦС по нажатию кнопки <Отозвать>. Набор кнопок в карточке ЦС в зависимости от статуса сертификата ЦС соответствует приведённым действиям в Таблица 5.
- В карточке Центра сертификации отображаются следующие сведения:
  - издатель;

- владелец;
- организация;
- департамент;
- срок действия («действует с», «действует до»);
- алгоритм ключа;
- длина ключа;
- состав:
    - открытый ключ;
    - отпечаток;
    - версия;
    - параметры открытого ключа;
    - алгоритм цифровой подписи;
    - основные ограничения;
    - использование ключа;
    - идентификатор ключа центра;
    - идентификатор ключа субъекта.

4.3.2.2 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 подчиненных центров» нажать кнопку <Подписать запрос+> (см. Рисунок 44)

Внимание! Подписание файл-запроса и выдача подписанного сертификата производится от ЦС в состоянии «Активирован» на вкладке «Свои сертификаты».

Рисунок 44 – Окно «Сертификаты подчиненных ЦС»

- Далее загрузите запрос в формате .csr, скачанный на шаге 3.2.3 или 4.3.1.2, нажав кнопку <Выбрать файл> (см. Рисунок 45).

На текущем шаге, после выбора файла запроса, возможно изменить выбор, нажав кнопку <Изменить> (см. Рисунок 46).

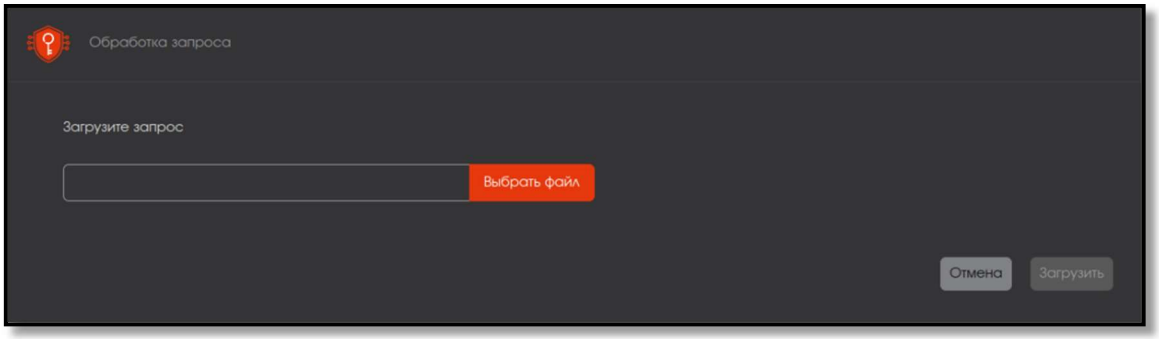


Рисунок 45 – Окно выбора файла запроса

- Нажмите ставшую активной кнопку <Загрузить> (см. Рисунок 46).

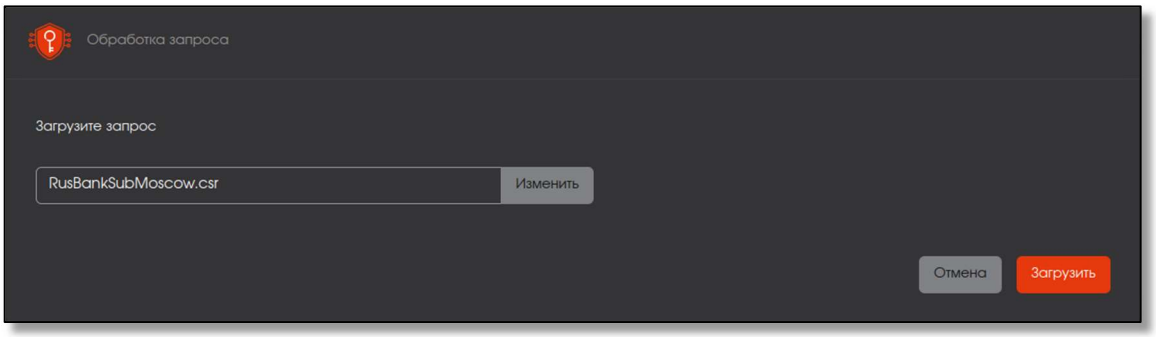


Рисунок 46 – Окно загрузки файла запроса

- 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 47).

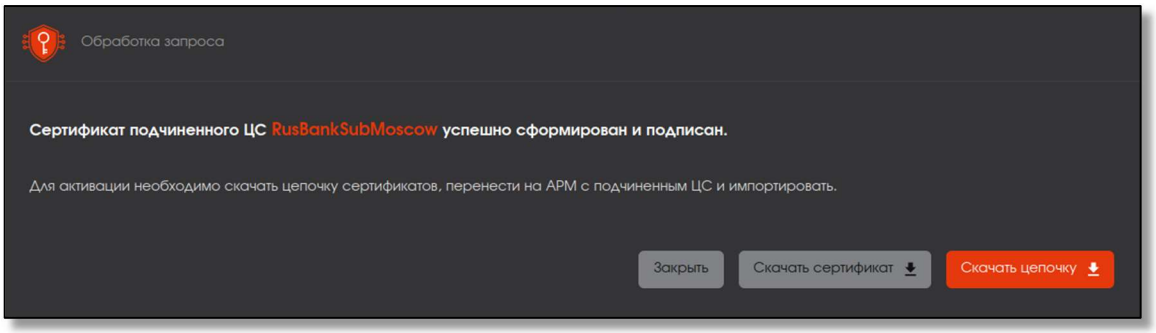


Рисунок 47 – Окно успешного формирования и подписи сертификата

- Необходимо скачать цепочку сертификатов ЦС в формате .chain.pem, нажав кнопку <Скачать цепочку сертификатов>, в окне Обработки запроса на данном шаге для дальнейшего импорта.
- 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 48).

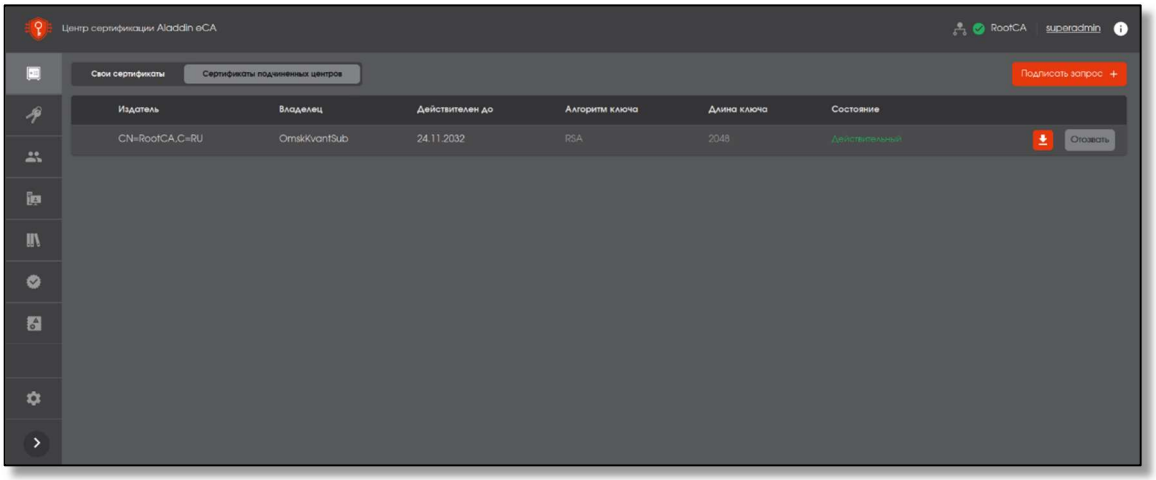


Рисунок 48 – Окно вкладки «Сертификаты подчиненных центров» с выбранным сертификатом

- Далее перенесите сертификат на подчинённый ЦС и выполните импорт сертификата согласно пункту 4.3.1.3 настоящего руководства.

4.4 Описание вкладки «Сертификаты»

Переход на экран управления центра сертификации осуществляется по выбору вкладки «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 31).

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

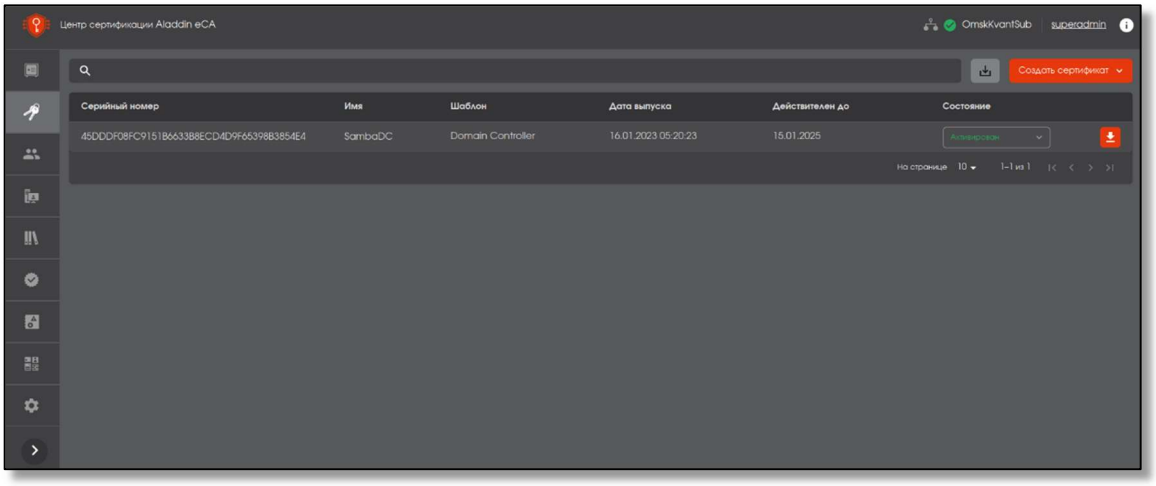


Рисунок 49 - Экран раздела меню «Сертификаты»

На основном экране сервиса публикации отображены информационные элементы (табличные поля):

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

- Все созданные сертификаты субъектов отображаются в виде таблицы с постраничным выводом данных. Ссылочный блок для разграничения содержимого размещен внизу страницы (см. Рисунок 50) 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.

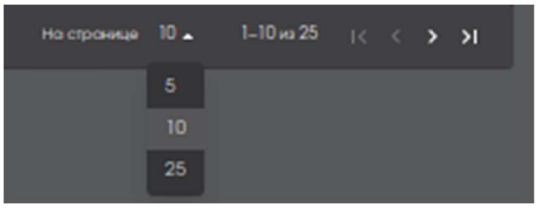


Рисунок 50 – Пагинация на вкладке «Сертификаты»

4.4.1 **Поиск сертификатов**

Строка поиска (см. Рисунок 51) предназначена для поиска сертификатов по полям SubjectDN, SubjectAltName и серийному номеру сертификата.

Рисунок 51 – Поисковая строка на вкладке «Сертификаты»

4.4.2 **Сортировка сертификатов**

- Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 52):
  - «Серийный номер» – сортировка осуществляется в порядке возрастания или убывания значения;
  - «Имя» – сортировка осуществляется в алфавитном порядке;
  - «Шаблон» – осуществляется группировка по типу шаблона;
  - «Действует 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 52 – Поля сортировки содержимого вкладки «Сертификаты»

4.4.3 **Скачивание сертификатов**

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку (см. Рисунок 49) и в раскрывшемся подменю выберите пункт <Скачать сертификат> или «Скачать цепочку» (см. Рисунок 53).

Рисунок 53 – Подменю «Скачать сертификат/цепочку»

4.4.4 **Статус сертификатов**

Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в Таблица 6. Смена состояния сертификата производится посредством выбора нужного значения из выпадающего меню при выделении строки сертификата (см. Рисунок 54).

Таблица 6 – Доступные действия над сертификатами в зависимости от состояния

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

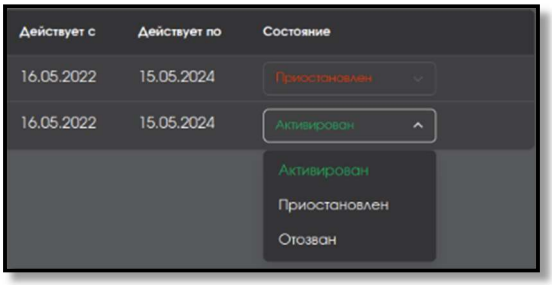


Рисунок 54 – Выпадающее меню смены состояния сертификата

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 55);

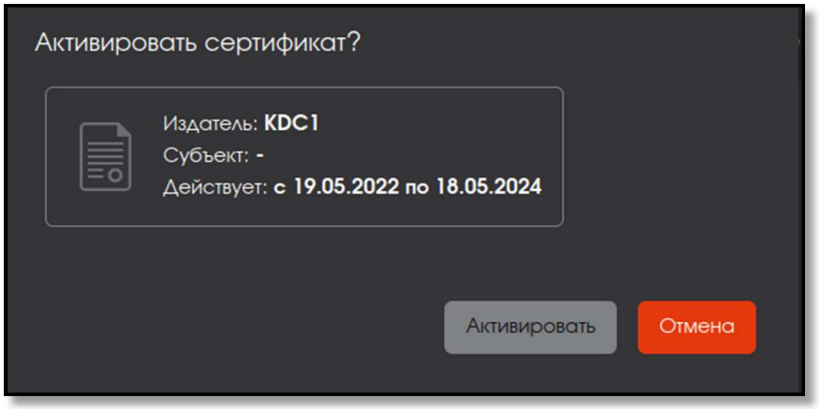


Рисунок 55 – Окно активации сертификата

- отзыв (см. Рисунок 56);

ВНИМАНИЕ! Данную операцию нельзя отменить.

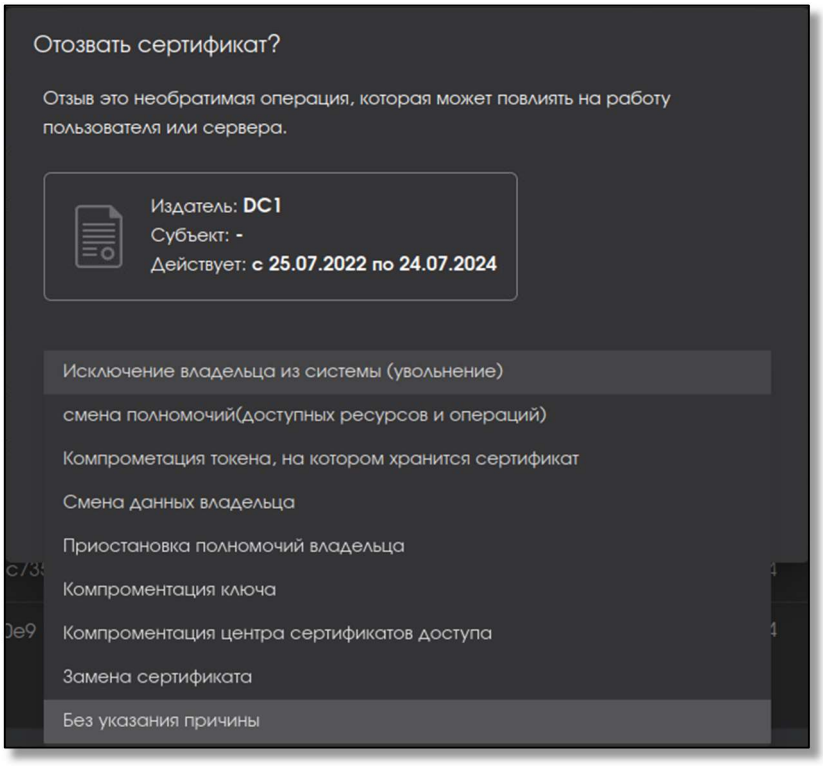


Рисунок 56 – Окно отзыва сертификата

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

- неиспользуемый (unused) – исключение владельца из системы/увольнение;
- компрометация ключа (keyCompromise);
- компрометация центра сертификации (cACompromise);
- принадлежность изменена (affiliation Changed) – смена данных владельца;
- заменен (сертификат) – заменен на иной сертификат;
- приостановка полномочий владельца сертификата (certificateHold);
- без указания причины (unspecified).

- Приостановка действия сертификата (см. Рисунок 57):

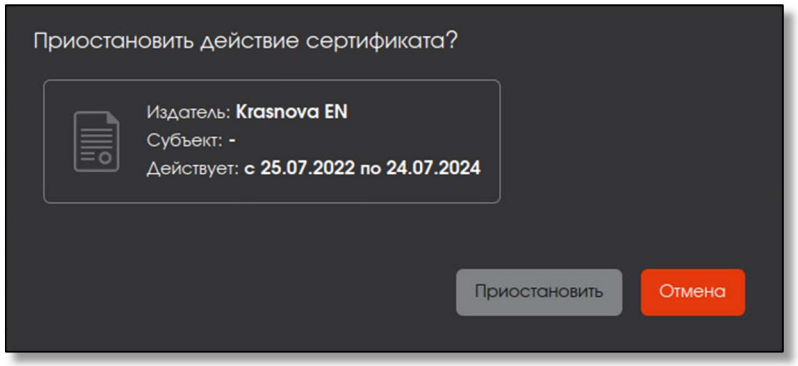


Рисунок 57 – Окно приостановки действия сертификата

4.4.5 **Карточка сертификата**

- Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».
- Переход к экрану «Карточка сертификата» (см. Рисунок 58) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 49).

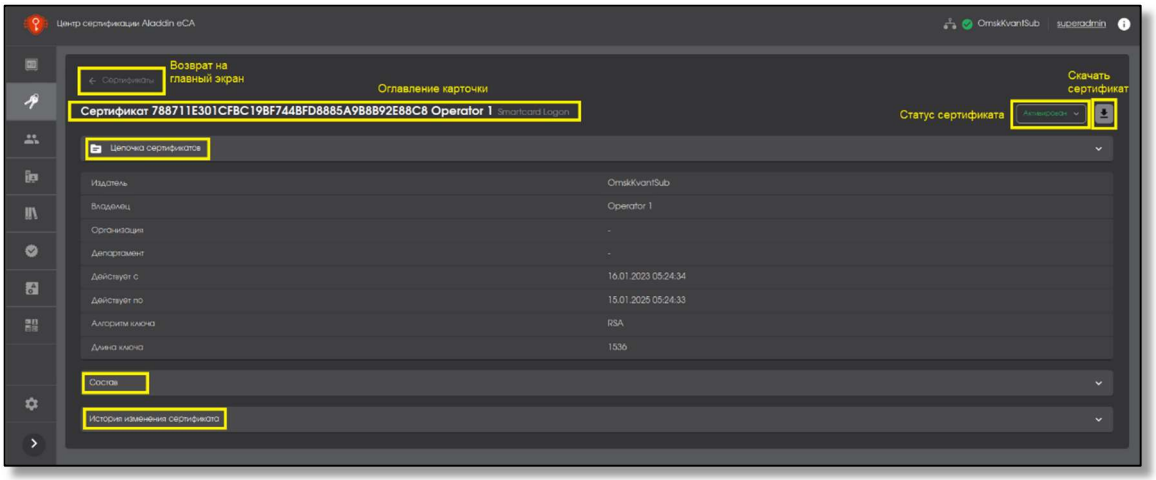


Рисунок 58 – Окно «Карточка сертификата»

- Оглавление карточки сертификата включает в себя:
  - тип-сертификат;
  - серийный номер;
  - принадлежность;
  - тип субъекта.

- Для возврата на главный экран раздела «Сертификаты» проследовать по стрелке ← Сертификаты.
- Для изменения состояния сертификата выбрать из выпадающего списка действие в соответствие с Таблица 6.
- Для скачивания сертификата наведите указатель мыши на выбранный сертификат и скачайте по нажатию появившейся кнопки <Скачать сертификат>.
- 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 59).

Рисунок 59 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

  - «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены поля (см. Рисунок 60):
    - открытый ключ;
    - отпечаток;
    - версия;
    - параметр открытого ключа;
    - алгоритм цифровой подписи
    - основные ограничения;
    - использование ключа;
    - 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 60 – 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. На раскрывшемся экране отображены поля (см. Рисунок 61):
  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершенно данное действие;
  - событие – действие, совершённое над сертификатом.

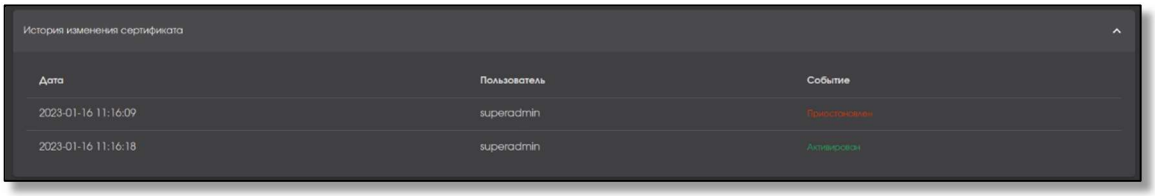


Рисунок 61 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

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

4.4.6 **Экспорт списка выпущенных сертификатов**

- При использовании учётной записи «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.

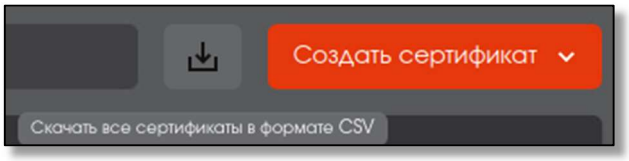


Рисунок 62 – Кнопка <Скачать все сертификаты в формате CSV>

- Для выгрузки списка сертификатов нажмите кнопку <Скачать все сертификаты в формате CSV> (см. Рисунок 62).
- В появившемся окне выберите «Сохранить файл» и нажмите кнопку <ОК>.

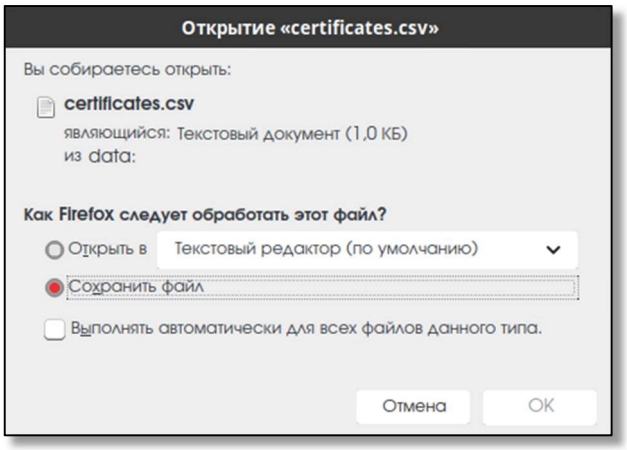


Рисунок 63 – Окно выбора действия при нажатии на кнопку <Скачать все сертификаты>

- Введите имя файла и выберите папку для сохранения файла списка сертификатов. Нажмите кнопку <Сохранить>.

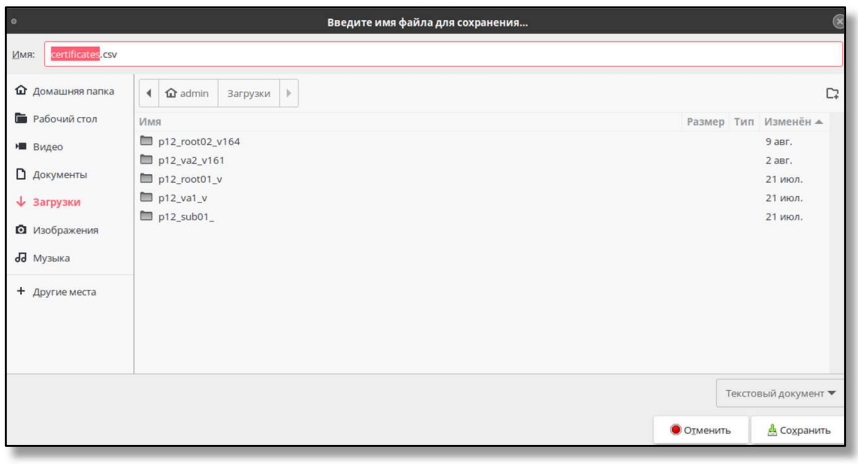
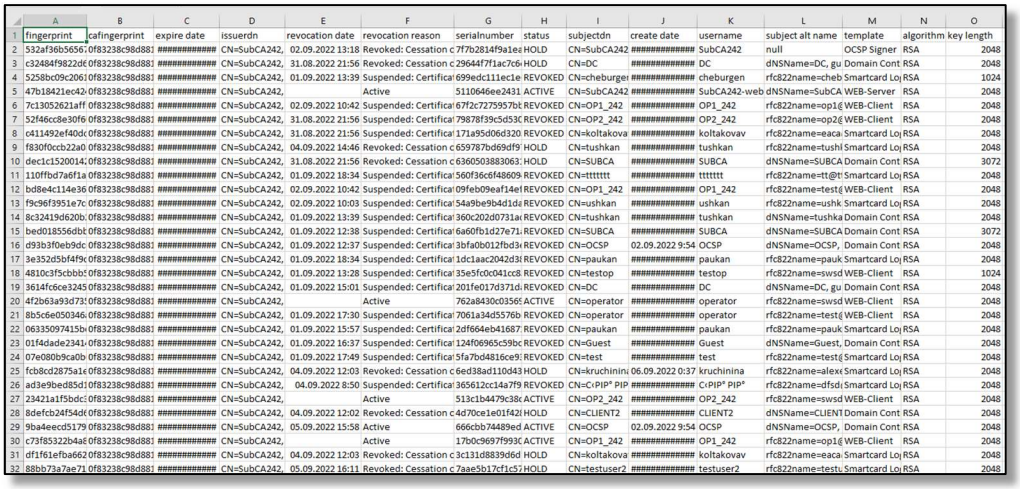


Рисунок 64 – Окно указания пути сохранения списка выпущенных сертификатов

- Выгруженный файл .csv представлен в текстовом формате для представления табличных данных, где строки текста содержат поля таблицы, разделённые запятыми. Сформированная таблица содержит следующие столбцы (см. Рисунок 65):
  - 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.



fingerprint	cafingerprint	expire date	issuerdn	revocation date	revocation reason	serialnumber	status	subjectdn	create date	username	subject alt name	template	algorithm	key length
532af36b5656	0f83238c98d88	##########	CN=SubCA242,	02.09.2022 13:18	Revoked: Cessation c	7f7b2814f9a1e4	HOLD	CN=SubCA242	##########	SubCA242	null	OCSP Signer	RSA	2048
c32484f9822d6	0f83238c98d88	##########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	29644f7f1ac7c6	HOLD	CN=DC	##########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
5258bc09c206	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	699edc111ec1e	REVOKED	CN=cheburge	##########	cheburgen	rfc822name=cheb	Smartcard Lo	RSA	1024
47b18421ec42	0f83238c98d88	##########	CN=SubCA242,		Active	5110646ee2431	ACTIVE	CN=SubCA242	##########	SubCA242-web	dNSName=SubCA	WEB-Server	RSA	2048
7c13052621aff	0f83238c98d88	##########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	67f2c7275957bf	REVOKED	CN=OP1_242	##########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
52f46cc8e30f6	0f83238c98d88	##########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	79878f39c5d53(	REVOKED	CN=OP2_242	##########	OP2_242	rfc822name=op2@	WEB-Client	RSA	2048
c411492ef40dc	0f83238c98d88	##########	CN=SubCA242,	31.08.2022 21:56	Suspended: Certifica	171a95d06d320	REVOKED	CN=koltakova	##########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
f830f0ccb22a0	0f83238c98d88	##########	CN=SubCA242,	04.09.2022 14:46	Revoked: Cessation c	659787bd69df9	HOLD	CN=tushkan	##########	tushkan	rfc822name=tush	Smartcard Lo	RSA	2048
dec1c1520014	0f83238c98d88	##########	CN=SubCA242,	31.08.2022 21:56	Revoked: Cessation c	6360503883063	HOLD	CN=SUBCA	##########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
110ffbd7a6f1a	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	560f36c6f48609	REVOKED	CN=ttttttt	##########	ttttttt	rfc822name=tt@t	Smartcard Lo	RSA	2048
bd8e4c114e36	0f83238c98d88	##########	CN=SubCA242,	02.09.2022 10:42	Suspended: Certifica	09feb09eaf14e	REVOKED	CN=OP1_242	##########	OP1_242	rfc822name=test(	WEB-Client	RSA	2048
f9c96f3951e7c	0f83238c98d88	##########	CN=SubCA242,	02.09.2022 10:03	Suspended: Certifica	54a9be9b4d1da	REVOKED	CN=ushkan	##########	ushkan	rfc822name=ushk	Smartcard Lo	RSA	2048
8c32419d620b	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 13:39	Suspended: Certifica	360c202d0731a	REVOKED	CN=tushkan	##########	tushkan	dNSName=tushka	Domain Cont	RSA	2048
bed018556db8	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 12:38	Suspended: Certifica	6a60fb1d27e71	REVOKED	CN=SUBCA	##########	SUBCA	dNSName=SUBCA	Domain Cont	RSA	3072
d93b3f0eb9dc	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 12:37	Suspended: Certifica	3bfa0b012fbd3(	REVOKED	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
3e352d5bf4f9c	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 18:34	Suspended: Certifica	1dc1aac2042d3	REVOKED	CN=paukan	##########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
4810c3f5cbbb	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 13:28	Suspended: Certifica	35e5fc0c041cc8	REVOKED	CN=testop	##########	testop	rfc822name=swsd	WEB-Client	RSA	1024
3614fc6ce3245	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 15:01	Suspended: Certifica	201fe017d371d	REVOKED	CN=DC	##########	DC	dNSName=DC, gu	Domain Cont	RSA	2048
4f2b63a93d73	0f83238c98d88	##########	CN=SubCA242,		Active	762a8430c0356	ACTIVE	CN=operator	##########	operator	rfc822name=swsd	WEB-Client	RSA	2048
8b5c6e050346	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 17:30	Suspended: Certifica	7061a34d5576b	REVOKED	CN=operator	##########	operator	rfc822name=test(	WEB-Client	RSA	2048
06335097415b	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 15:57	Suspended: Certifica	2df664eb41687	REVOKED	CN=paukan	##########	paukan	rfc822name=pauk	Smartcard Lo	RSA	2048
01f4dade2341	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 16:37	Suspended: Certifica	124f06965c59bc	REVOKED	CN=Guest	##########	Guest	dNSName=Guest,	Domain Cont	RSA	2048
07e080b9ca0b	0f83238c98d88	##########	CN=SubCA242,	01.09.2022 17:49	Suspended: Certifica	5fa7bd4816ce9	REVOKED	CN=test	##########	test	rfc822name=test(	Smartcard Lo	RSA	2048
fcb8cd2875a1e	0f83238c98d88	##########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	6ed38ad110d43	HOLD	CN=kruchinin	06.09.2022 0:37	kruchinina	rfc822name=alex(	Smartcard Lo	RSA	2048
ad3e9bed85d1	0f83238c98d88	##########	CN=SubCA242,	04.09.2022 8:50	Suspended: Certifica	365612cc14a7f9	REVOKED	CN=C‹PIP° PIP	##########	C‹PIP° PIP°	rfc822name=dfsd	Smartcard Lo	RSA	2048
23421a1f5bdc	0f83238c98d88	##########	CN=SubCA242,		Active	513c1b4479c38(	ACTIVE	CN=OP2_242	##########	OP2_242	rfc822name=swsd	WEB-Client	RSA	2048
8defcb24f54d6	0f83238c98d88	##########	CN=SubCA242,	04.09.2022 12:02	Revoked: Cessation c	4d70ce1e01f42(	HOLD	CN=CLIENT2	##########	CLIENT2	dNSName=CLIENT	Domain Cont	RSA	2048
9ba4eecd5179	0f83238c98d88	##########	CN=SubCA242,	05.09.2022 15:58	Active	666cbb74489ed	ACTIVE	CN=OCSP	02.09.2022 9:54	OCSP	dNSName=OCSP,	Domain Cont	RSA	2048
c73f85322b4a6	0f83238c98d88	##########	CN=SubCA242,		Active	17b0c9697f993(	ACTIVE	CN=OP1_242	##########	OP1_242	rfc822name=op1@	WEB-Client	RSA	2048
df1f61efba662	0f83238c98d88	##########	CN=SubCA242,	04.09.2022 12:03	Revoked: Cessation c	3c131d8839d6d	HOLD	CN=koltakova	##########	koltakovav	rfc822name=eaca	Smartcard Lo	RSA	2048
88bb73a7ae71	0f83238c98d88	##########	CN=SubCA242,	05.09.2022 16:11	Revoked: Cessation c	7aae5b17cf1c57	HOLD	CN=testuser2	##########	testuser2	rfc822name=testu	Smartcard Lo	RSA	2048

Рисунок 65 – Пример экспортированного файла списка выпущеных сертификатов.csv

4.4.7 **Выпуск сертификата с закрытым ключом pkcs#12 для нового субъекта**

В результате выпуска сертификата с закрытым ключом pkcs#12 для нового субъекта будет сгенерирована ключевая пара в соответствии с заданными параметрами криптографии и создана запись о новом субъекте в локальной ресурсной системе.

- Нажатие кнопки <Создать сертификат> на главном экране раздела «Сертификаты» разворачивает подменю. Выбор варианта <+ С закрытым ключом (PKCS#12)> стартует сценарий по созданию сертификата для нового субъекта (см. Рисунок 66).

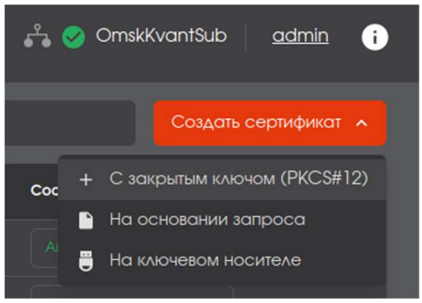


Рисунок 66 - Кнопка «Создать сертификат»

- Для нового пользователя осуществляется выбор по радиокнопке <Создать нового пользователя или устройство>, из выпадающего списка администратор выбирает шаблон вида субъекта и по ставшей активной кнопке <Продолжить> переходит к следующему шагу (см. Рисунок 67).
- Описание полей для каждого шаблона приведено в Приложение А. Описание полей шаблонов сертификатов настоящего документа.

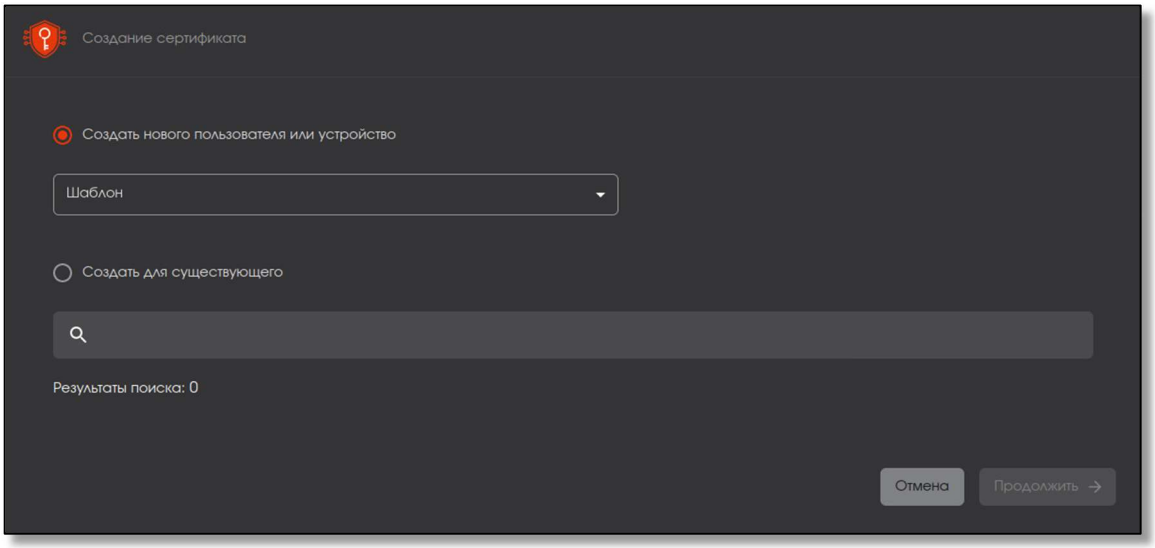


Рисунок 67 - Окно создания сертификата PKCS#12 для нового пользователя

- После выбора шаблона для субъекта открывается окно ввода данных для шаблона (см. Рисунок 68). После ввода всех данных кнопка «Продолжить» становится активной.

Вводимые данные не должны содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами.

Рисунок 68 – Окно создания сертификата PKCS#12 для нового пользователя. Шаг 1

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 69).

Правила ввода пароля:

- для просмотра вводимых символов необходимо нажать кнопку на текущей строке;
- пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;
- если в пароле используются запрещенные символы, то рамка поля ввода приобретает красный цвет;
- если пароли не совпадают, то рамка поля подтверждения окрашивается в красный цвет.

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

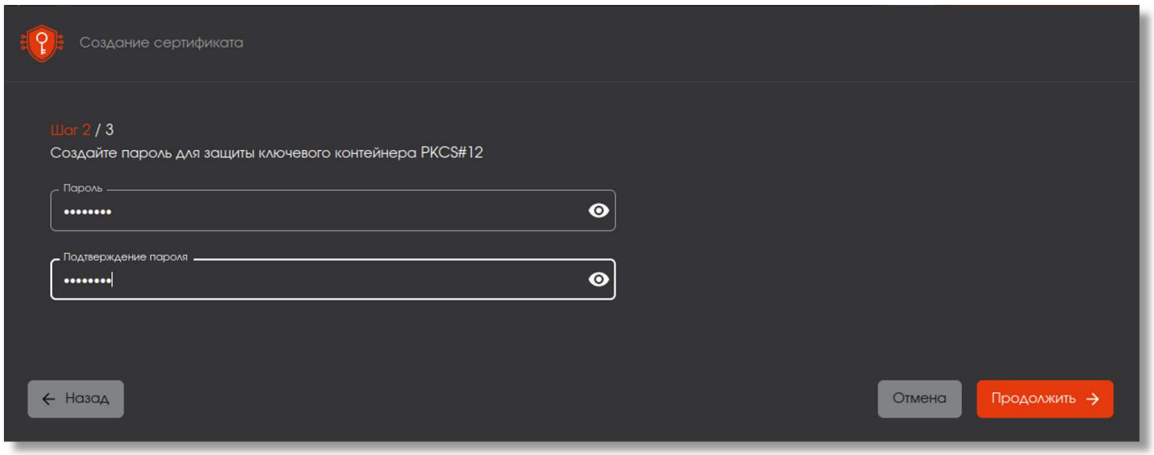


Рисунок 69 – Окно создания сертификата PKCS#12 для нового пользователя. Шаг 2

- В следующем окне требуется определить параметры шифрования (см. Рисунок 70):
  - алгоритм ключа;
  - длину ключа.

Параметры определяются шаблоном сертификата и выбираются в соответствии с техническими требованиями шаблона.

После определения всех параметров шифрования становится доступной для нажатия кнопка <Создать сертификат>.

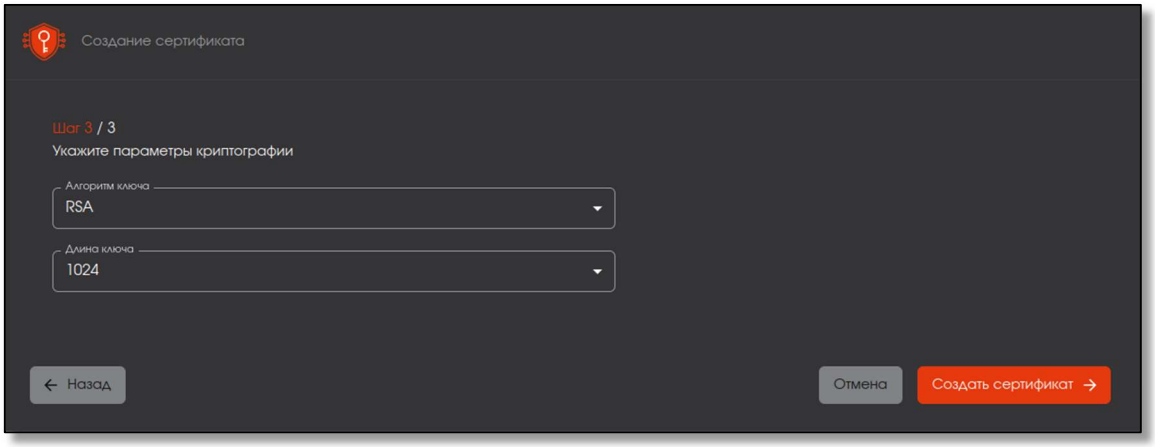


Рисунок 70 - Окно создания сертификата PKCS#12 для нового пользователя. Шаг 3

- По завершению работы мастера создания сертификата субъекта администратор видит окно, изображенное на Рисунок 71. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия) и возможность скачать созданный сертификат.

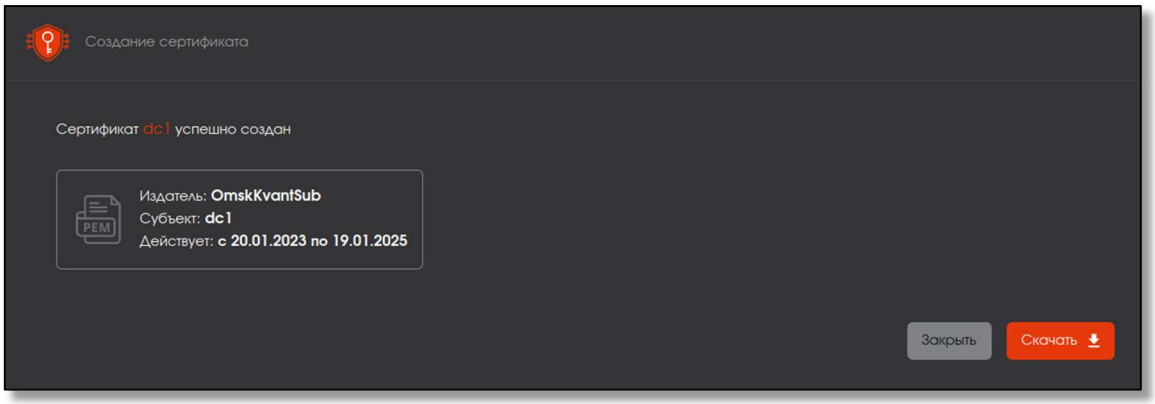


Рисунок 71 – Окно по результату успешного завершения создания сертификата PKCS#12 для нового пользователя

4.4.7.1 Выпуск сертификата с закрытым ключом pkcs#12 для контроллера ALD PRO

Для выпуска сертификата контроллеру ALD PRO:

- Нажмите кнопку <Создать сертификат> на главном экране раздела «Сертификаты» и в развернувшемся подменю выберите вариант <+ С закрытым ключом (PKCS#12)> стартует сценарий по созданию сертификата для нового субъекта.
- В открывшемся окне выбираем шаблон сертификата «ALD PRO Domain Controller» и нажимаем ставшую активной кнопку «Продолжить» (см. Рисунок 72).

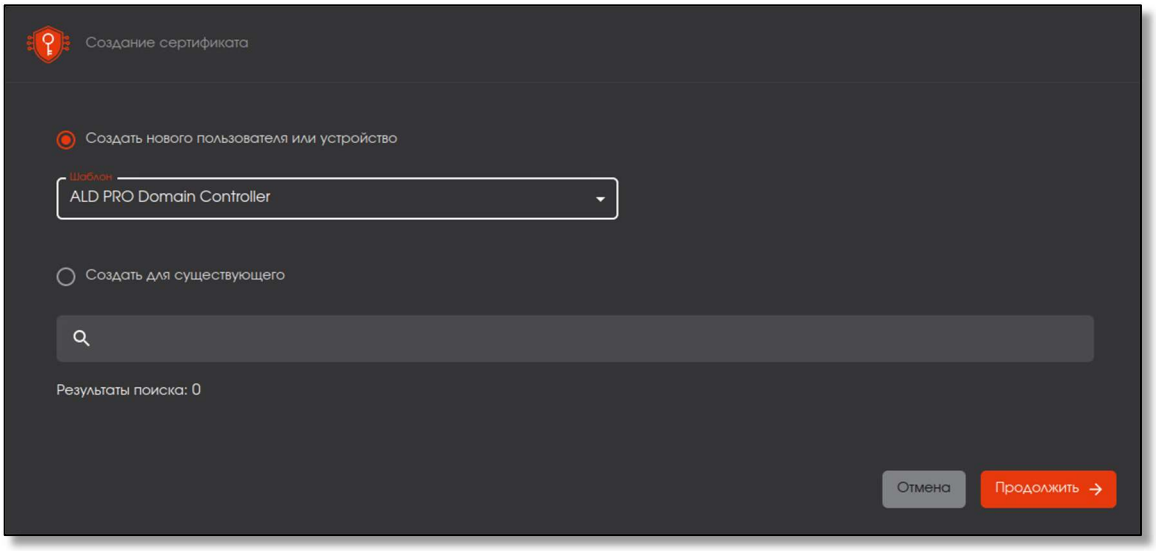


Рисунок 72 – Окно создания сертификата. Выбор шаблона контроллера домена ALD PRO

- В открывшемся окне необходимо ввести данные контроллера домена ALD PRO в соответствующие поля (см. Рисунок 73):
  - в поле «Имя» укажите имя контроллера домена ALD PRO, для которого выпускается сертификат;
  - в поле «Организация» укажите полное имя домена;
  - в поле «MS UPN» укажите данные в формате «krbtgt/полное имя домена@полное имя домена»;
  - в поле «Kerberos 5 Principal Name» укажите в формате «krbtgt/полное имя домена@полное имя домена»;

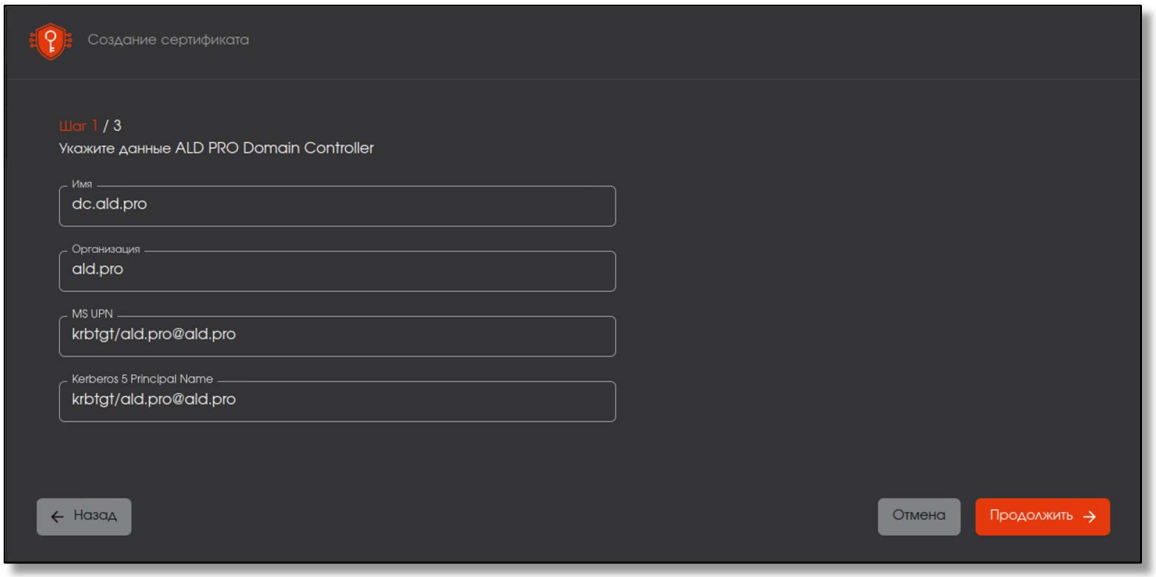


Рисунок 73 – Окно создания сертификата. Ввод данных контроллера домена ALD PRO

- На следующем шаге создайте пароль для защиты ключевого контейнера PKCS#12 и нажмите ставшую активной кнопку «Продолжить» (см. Рисунок 74).

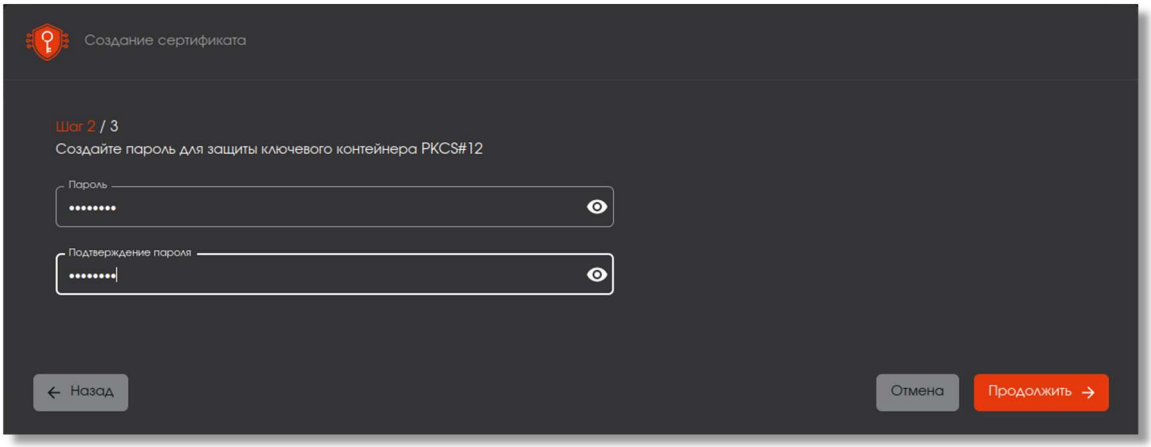


Рисунок 74 – Окно создания сертификата. Установка пароля контейнера PKCS#12

- Далее в открывшемся окне выберите параметры криптографии и нажмите ставшую активной кнопку «Создать сертификат» (см. Рисунок 75).

Рисунок 75 – Окно создания сертификата. Выбор параметров криптографии сертификата

- После создания сертификата в открывшемся окне необходимо скачать сертификат контроллера домена ALD PRO по кнопке «Скачать» (см. Рисунок 76).

Внимание! Скачать контейнер PKCS#12 возможно только на этом шаге.

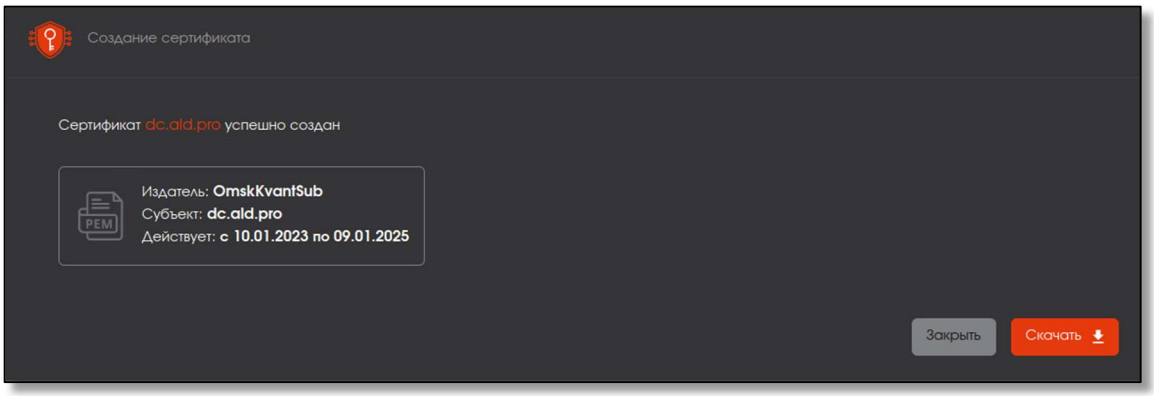


Рисунок 76 – Окно создания сертификата. Успешное создание сертификата контроллера домена ALD PRO

4.4.8 **Выпуск сертификата с закрытым ключом pkcs#12 для существующего субъекта**

- Нажатие кнопки <Создать сертификат> на главном экране раздела «Сертификаты» стартует сценарий по созданию сертификата для существующего субъекта (см Рисунок 77).

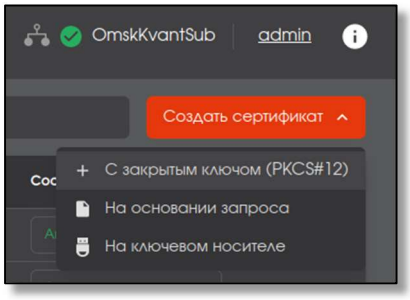


Рисунок 77 - Кнопка «Создать сертификат +»

- Далее необходимо выбрать вариант <Создать для существующего> (см. Рисунок 78).
- После выбора поля активируется строка поиска для субъекта.

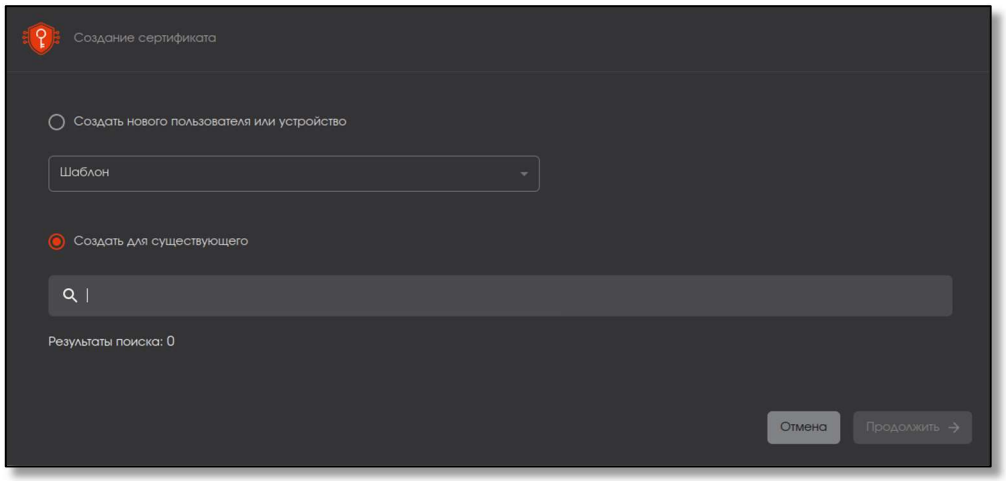


Рисунок 78 - Экран с выбранным значением «Создать для существующего»

- Поиск осуществляется путем ввода части известного параметра субъекта (id, имени, суффикса дополнительного имени), далее нажать на клавишу ENTER. При условии, что найдено не более трех субъектов, открывается страница с отображением результатов упрощенного поиска (см. Рисунок 79), из которых возможно выбрать нужный субъект. Поиск осуществляется среди субъектов локального ресурса, для которых ранее были выпущены сертификаты.

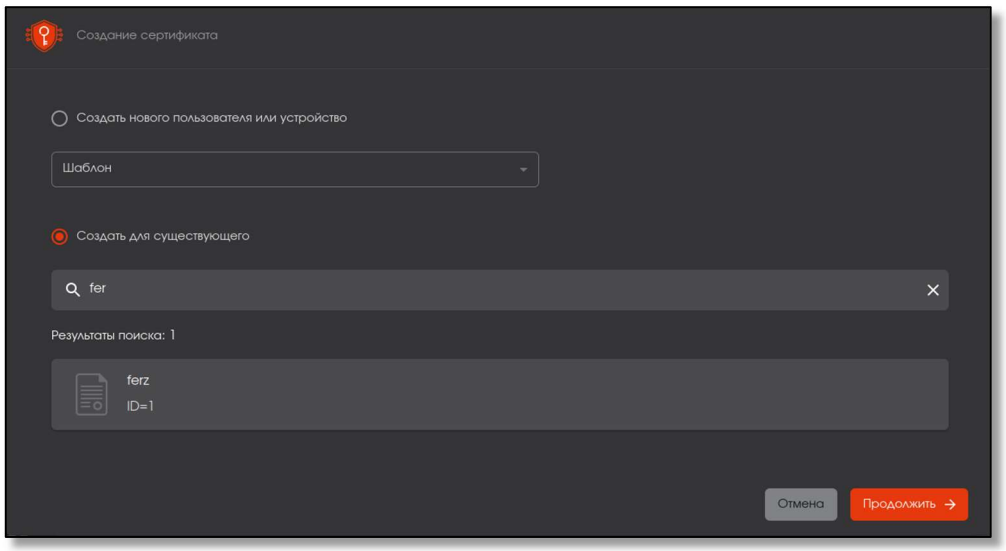


Рисунок 79 - Окно результатов поиска менее 3-х субъектов

- Если количество найденных субъектов более трех, то система предлагает перейти к расширенному поиску (поиск по полям в формате SN=******, DN=******, OU=******, O=*****, UID=******, DC=******, C=********) (см. Рисунок 80).

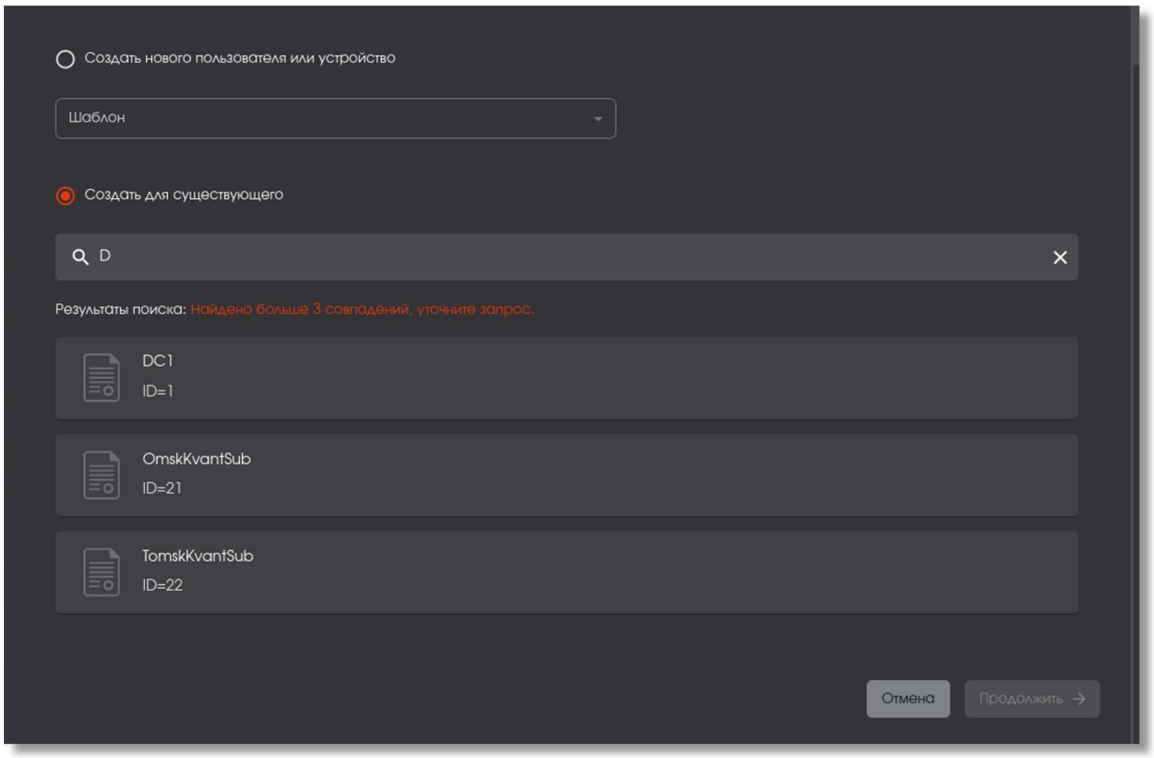


Рисунок 80 - Окно результатов поиска более 3-х субъектов

- После поиска и выбора необходимого субъекта активизируется мастер создания сертификата.

- На первом шаге необходимо выбрать шаблон сертификата из списка доступных (см. Рисунок 81). Описание полей шаблонов приведено в Приложение А. Описание полей шаблонов сертификатов. После выбора шаблона нажать активировавшуюся кнопку <Продолжить> и перейти к следующему шагу;

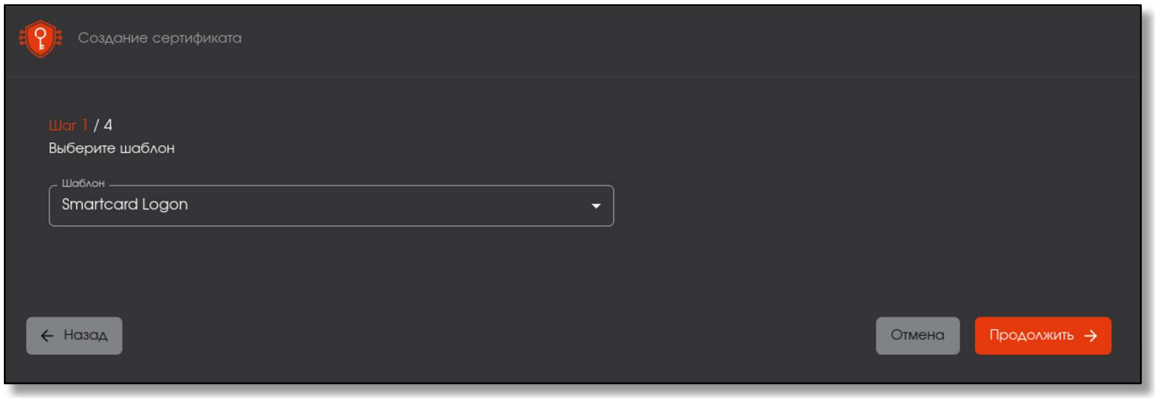


Рисунок 81 - Окно создания сертификата. Выбор шаблона

- Далее необходимо ввести данные согласно шаблону сертификата (см. Рисунок 82). Некоторые поля уже заполнены в соответствии с имеющимися данными о субъекте из ранее выпущенного сертификата. Данные можно изменять в соответствии с поставленными задачами.

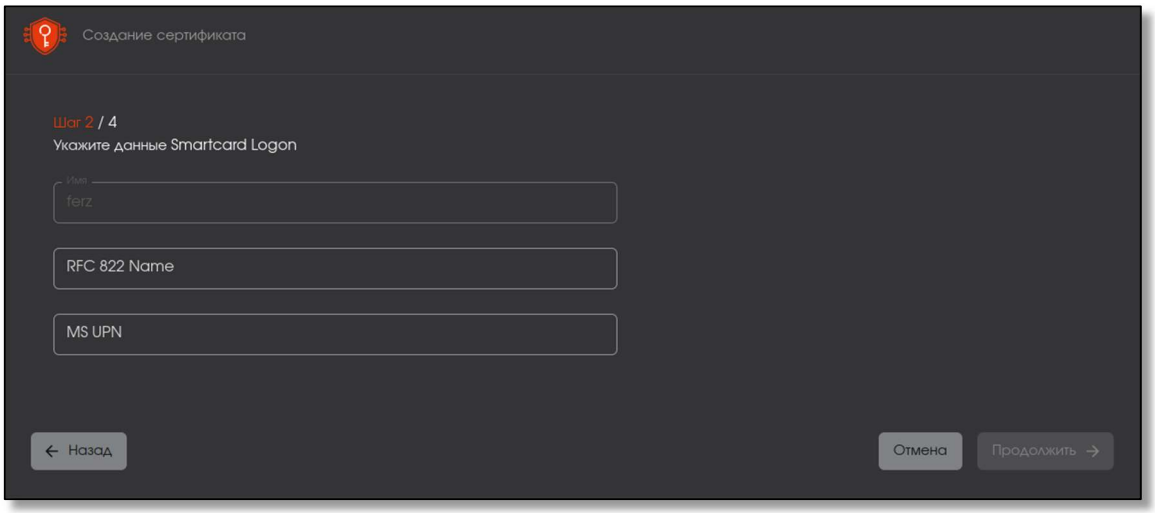


Рисунок 82 – Окно создания сертификата. Ввод данных

- Далее необходимо создать пароль с подтверждением (см. Рисунок 83) 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 83 – Окно создания сертификата. Задание пароля

- В следующем окне требуется определить параметры шифрования (см. Рисунок 84):
  - алгоритм ключа;
  - длину ключа.

Параметры определяются шаблоном сертификата и выбираются в соответствии с техническими требованиями шаблона.

Кнопка <Создать сертификат> доступна после выбора всех параметров.

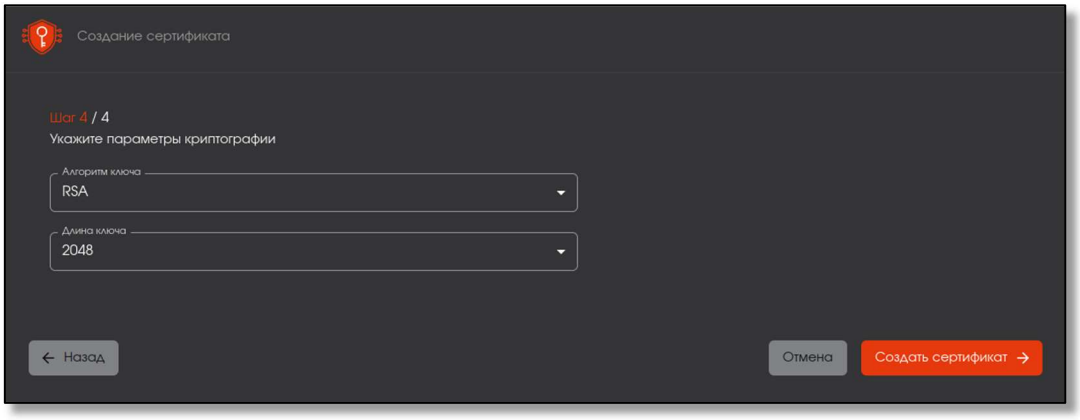


Рисунок 84 – Окно создания сертификата. Задание параметров криптографии

- По завершению работы мастера создания сертификата субъекта администратор видит окно, изображенное на Рисунок 85. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия).

Существует возможность скачать созданный сертификат.

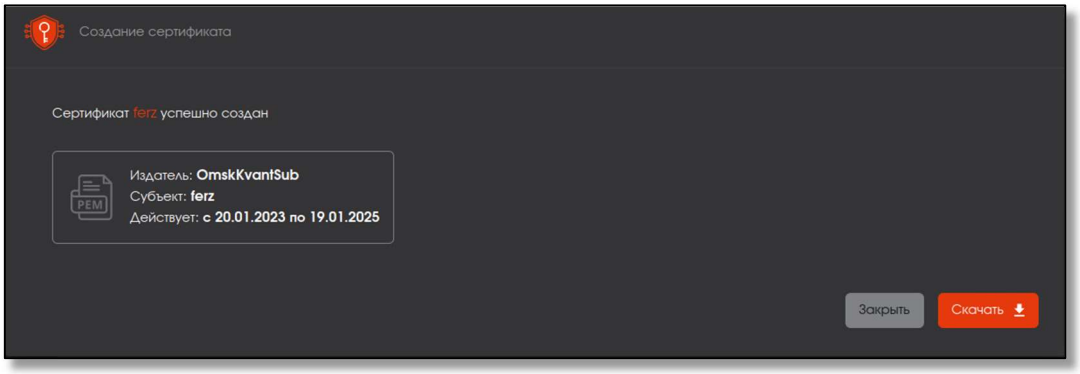


Рисунок 85 – Окно уведомления о успешном создании сертификата

4.4.9 **Выпуск сертификата субъекта по запросу**

- Предварительные условия выполнения сценария:
  - файл-запрос для субъекта должен быть подготовлен заранее на стороннем ЦС (например, при помощи ПО «Единый клиент JaCarta»);
  - расширение файл-запроса не имеет существенного значения, но предполагается, что оно будет `***.csr` или `***.pem`;
  - файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона АеСА. Например, для использования шаблона «Domain Controller» в запросе должны быть указаны параметры DNS Name и MS GUID.
- Нажатие кнопки <Создать сертификат> на главном экране раздела «Сертификаты» стартует сценарий по созданию сертификата по запросу (см. Рисунок 86) посредством мастера создания сертификата по запросу.

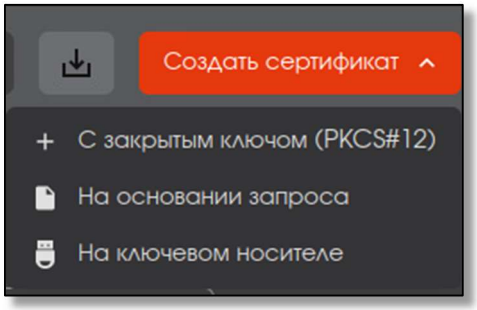


Рисунок 86 - Кнопка создания сертификата на основании запроса

- В открывшемся окне (см. Рисунок 87) необходимо выбрать и загрузить файл-запрос, а также выбрать шаблон сертификата в соответствии с запросом (предполагается, что администратор АеСА заранее знает для какого субъекта загружается файл-запрос и какой шаблон необходимо выбрать).

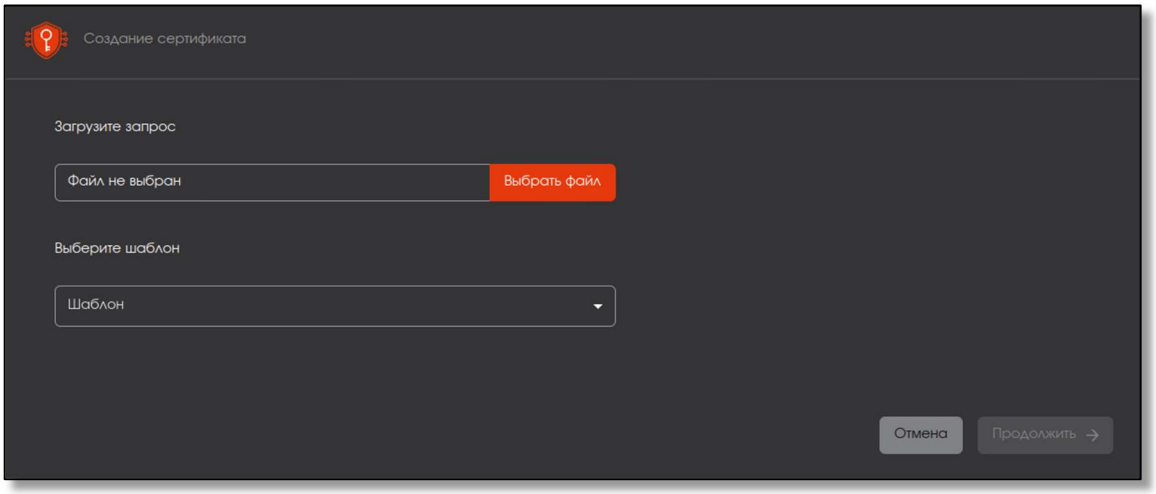


Рисунок 87 – Окно создания сертификата. Загрузка запроса и выбор шаблона

- После загрузки файла запроса и выбора шаблона нажать активировавшуюся кнопку <Продолжить> (см. Рисунок 88).

При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.

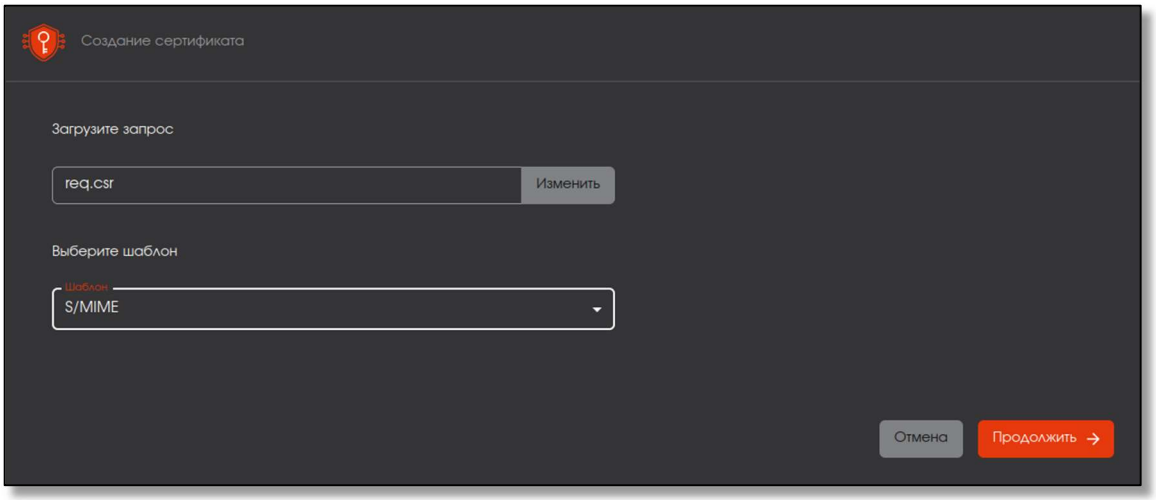


Рисунок 88 – Окно по созданию сертификата. Загруженный файл-запрос

- Приложение проверяет запрос на наличие субъекта:
  - при соответствии данных запроса и выбранного шаблона открывается окно с данными шаблона и принятыми данными из файла запроса (см. Рисунок 89).
  - если субъект не обнаружен – создается новый субъект, для которого выдается сертификат.

ВНИМАНИЕ! Окно с данными шаблона на Рисунок 89 и Рисунок 90 приведено в ознакомительных целях, количество и наименование полей зависят от выбранного шаблона.

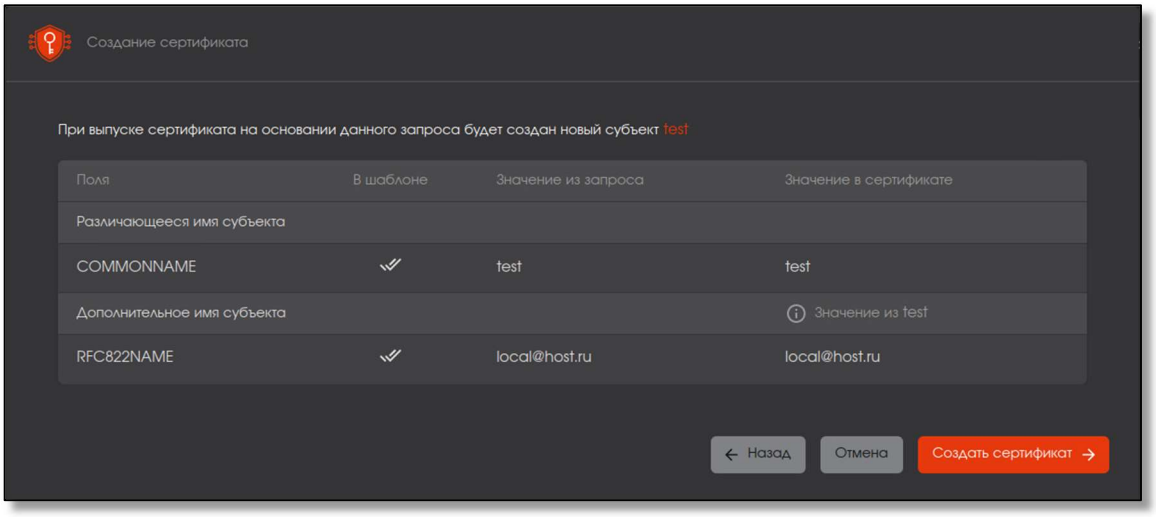


Рисунок 89 – Окно создания сертификата на основании запроса для нового субъекта

ВНИМАНИЕ! ! Поле «общее имя» (CN) всегда идет на первом месте.

В окне создания сертификата для существующего и нового субъектов обозначены:

- обязательные к заполнению поля шаблона, отмеченные знаком ✓✓ и необязательные поля шаблон, отмеченные знаком ✓;
- значения запроса, соответствующие полям шаблона сертификата;
- финальное представление данных, попадающих в сертификат.

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.

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификатов и отображается краткая информация о созданном сертификате (см. Рисунок 90).

Существует возможность скачать сертификат.

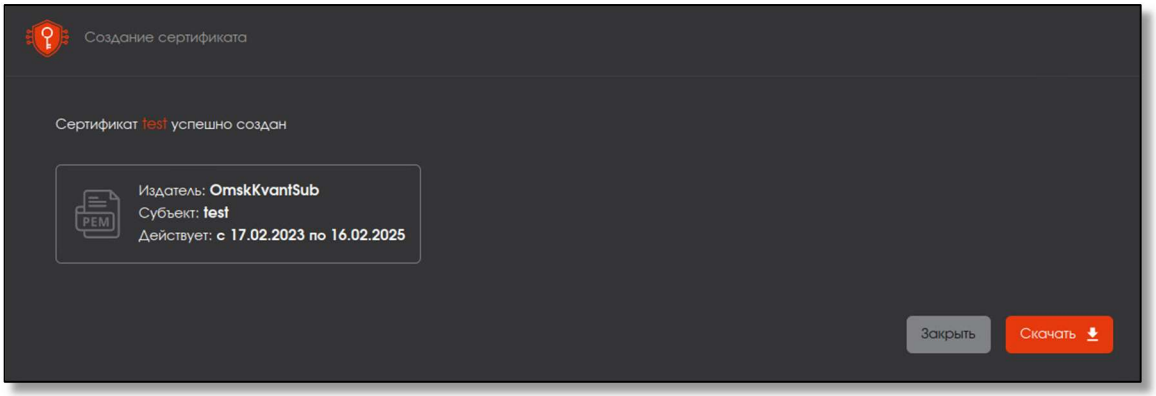


Рисунок 90 – Окно успешного создания сертификата субъекта на основании запроса

- В случае обнаружения ошибок или несоответствия обязательных полей параметров шаблона в файле запроса при проверке мастером создания сертификата в таблице сравнения появляется ошибка:

- «Не задано обязательное поле» в случае, если в загружаемом запросе отсутствует поле, которое является обязательным в выбранном шаблоне (см. Рисунок 91);
- «Поле не соответствует формату, указанному в шаблоне» в случае, если загружаемый запрос содержит поле, которое отсутствует в выбранном шаблоне.

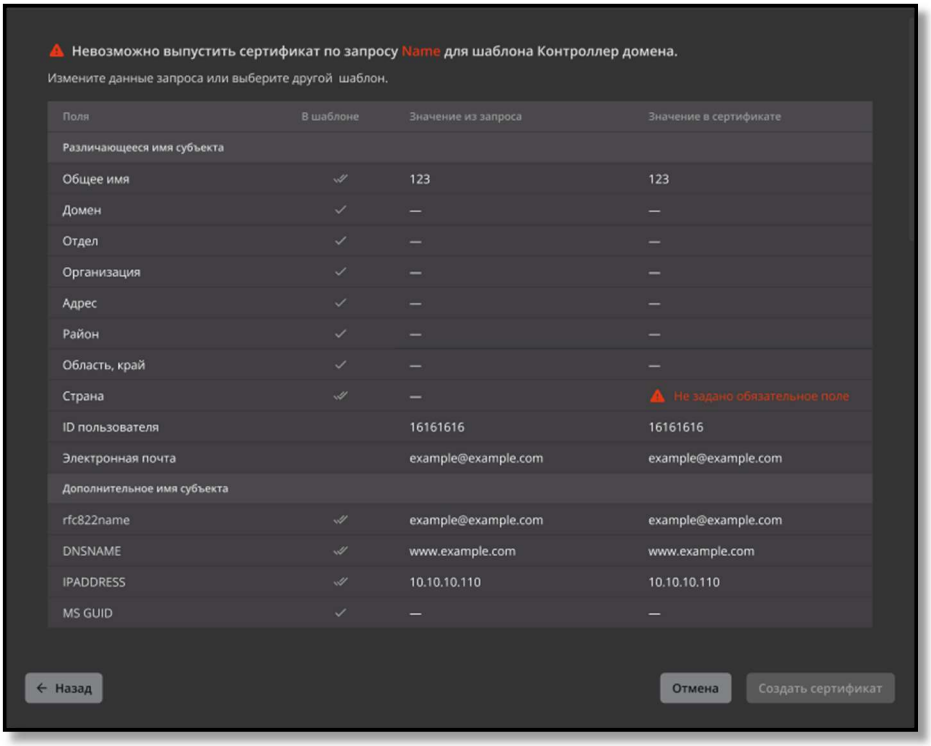


Рисунок 91 - Экран ошибки «Не задано обязательное поле»

- В таком случае создание сертификата невозможно и 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 в АЕСА.

4.4.10 **Выпуск сертификата субъекта на ключевом носителе**

4.4.10.1 Предварительные условия выполнения сценария:

- Убедитесь, что электронный ключ присоединен к АРМ выпускающего Центра сертификации;
- Убедитесь, что на АРМ веб-клиента установлено ПО JC-WebClient версии 4.3.2 или 4.3.3 для дальнейшей работы с токенами из браузера.

4.4.10.2 Нажатие кнопки <Создать сертификат> на главном экране раздела «Сертификаты» стартует сценарий по созданию сертификата на ключевом носителе (см. Рисунок 92) посредством мастера создания сертификата.

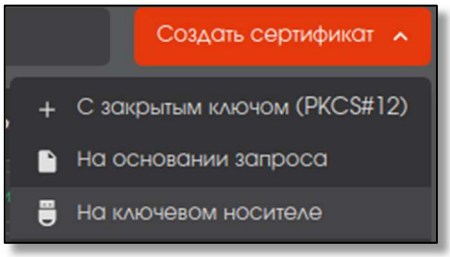


Рисунок 92 – Кнопка создания сертификата на ключевом носителе

- В случае, если ПО JC-WebClient предварительно не установлено, администратор будет уведомлен об этом информационным сообщением (см. Рисунок 93). Для выпуска сертификата на электронном ключе установите ПО JC-WebClient версии 4.3.2 или 4.3.3.

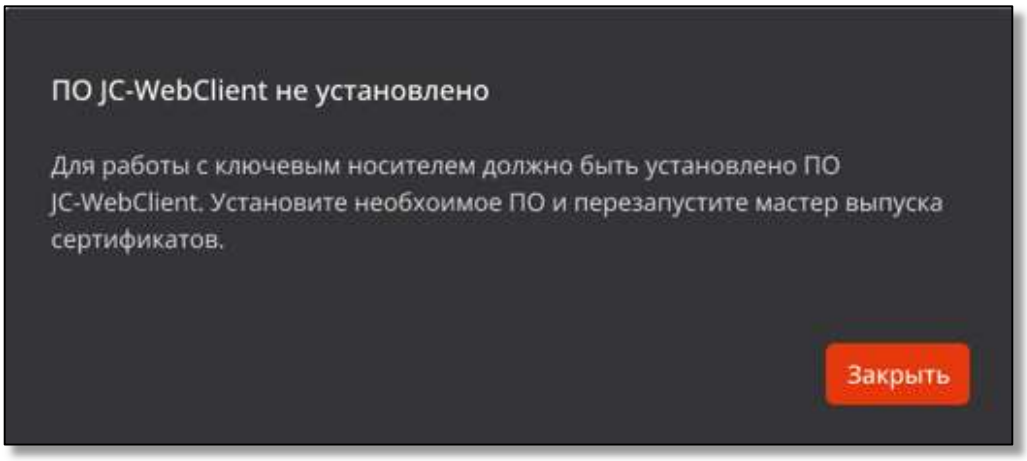


Рисунок 93 – Окно информационного сообщения «ПО JC-WebClient не установлено»

- В случае, если электронный носитель не подключен, администратор будет уведомлен об этом информационным сообщением (см. Рисунок 94). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

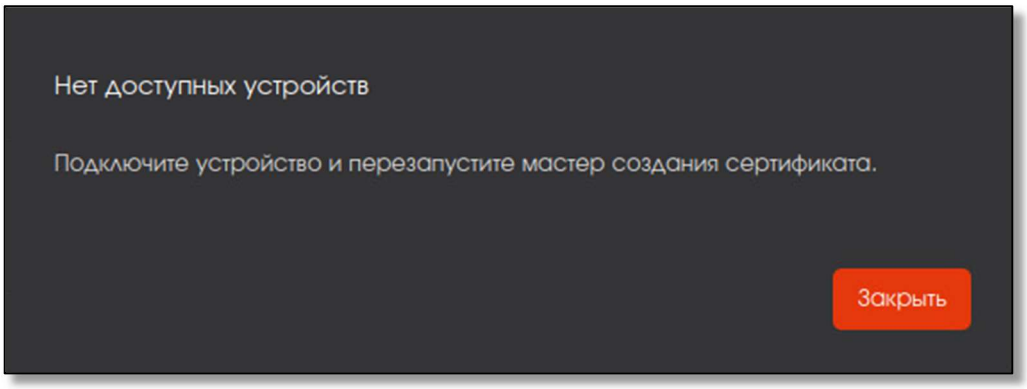


Рисунок 94 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если электронный ключ успешно подключен, в открывшемся окне (см. Рисунок 95) необходимо выбрать ключевой носитель, ввести его пин-код и указать шаблон для выпуска сертификата. В случае, если ключевых носителей более одного, то необходимо выбрать нужный из выпадающего списка в поле «Устройство».

После ввода всех данных кнопка «Продолжить» становится активной.

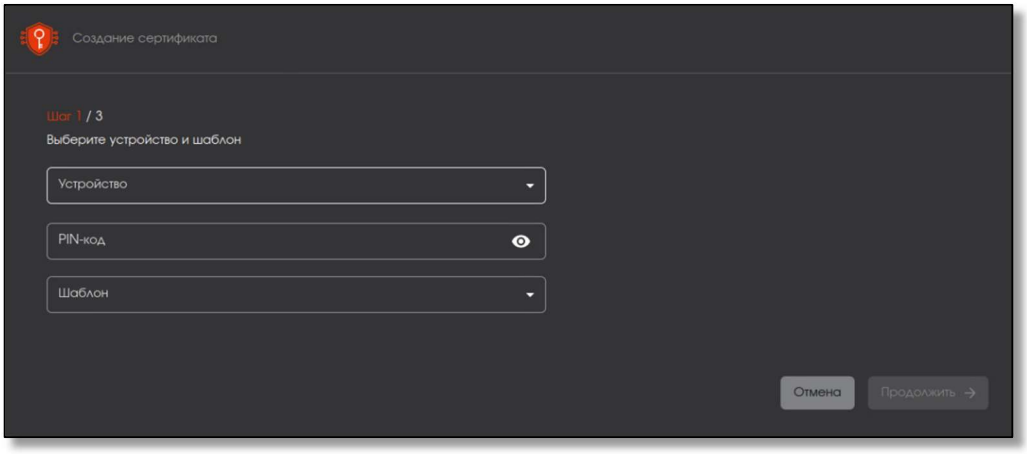


Рисунок 95 – Окно создания сертификата на электронном ключе. Шаг 1

- В зависимости от выбранного шаблона выпускаемого сертификата на предыдущем шаге заполняем поля на следующем шаге (см. Рисунок 96). Более подробное описание полей шаблона приведено в Приложение А. Описание полей шаблонов сертификатов.

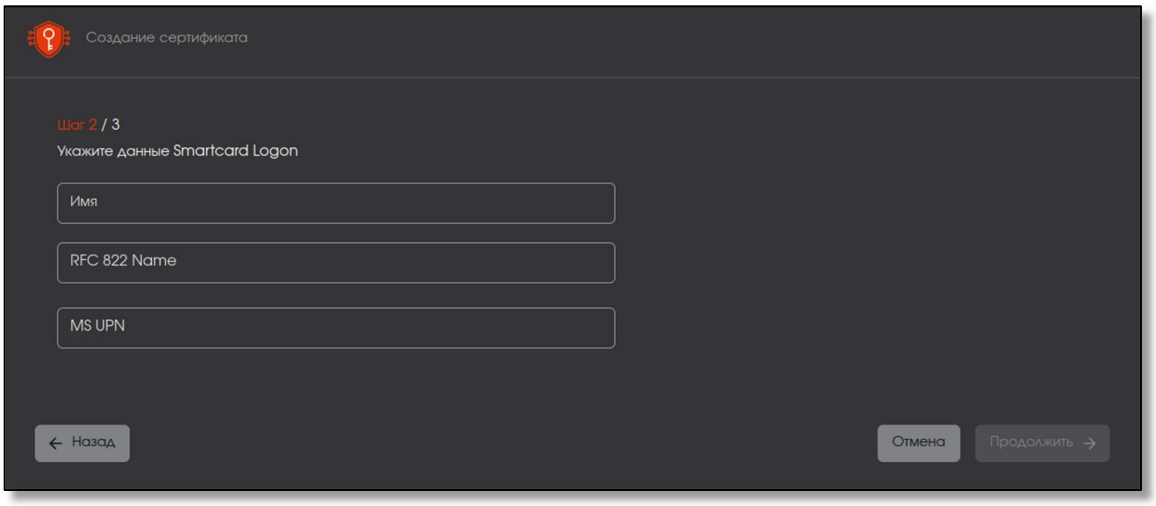


Рисунок 96 – Окно создания сертификата на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии алгоритм ключа (см. Рисунок 97). После выбора алгоритма нажмите кнопку <Создать сертификат>.

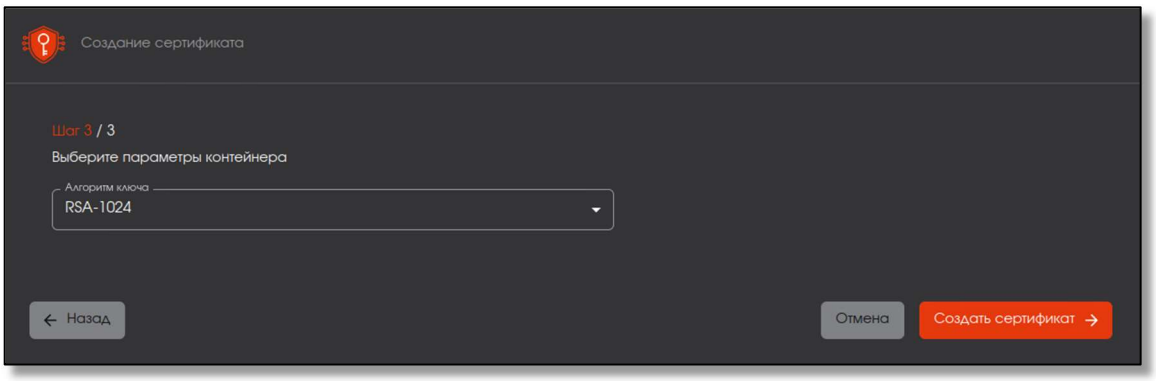


Рисунок 97 – Окно создания сертификата на электронном ключе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
  - генерация ключевой пары на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - генерация запроса на основе данных заполненного шаблона сертификата на предыдущем шаге;
  - выпуск сертификата;
  - запись на ключевой носитель.

Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов> (см. Рисунок 98).

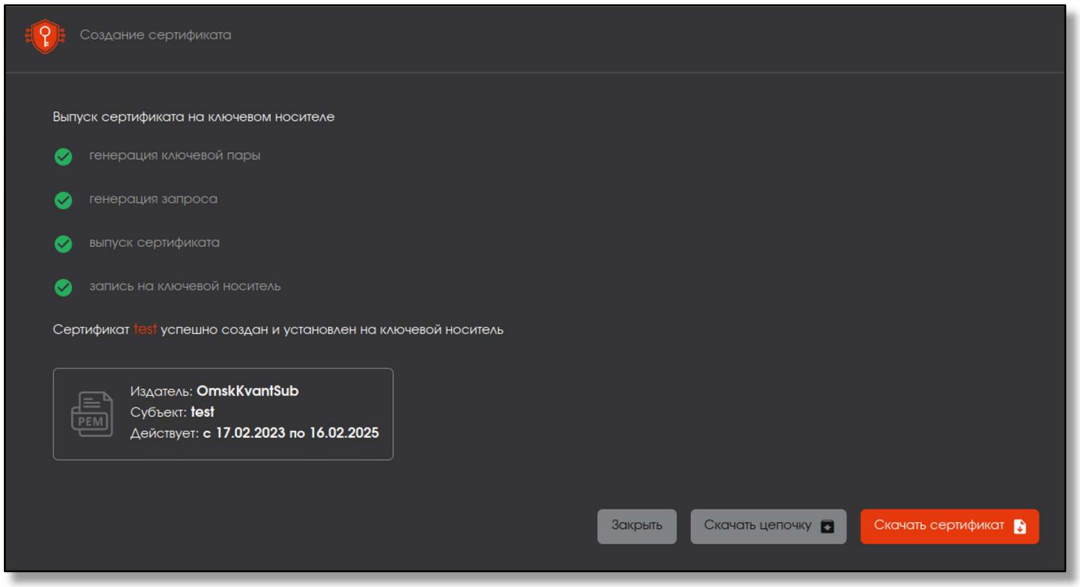


Рисунок 98 – Окно успешного создания сертификата субъекта на электронном ключе

4.5 Описание вкладки «Учётные записи»

Переход на вкладку «Учётные записи» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).

4.5.1 **Вкладка «Учётные записи»**

На основном экране «Учётные записи» отображены следующие поля (см. Рисунок 99):

-  – соответствующий символ обозначает, что данная учётная запись создана для субъекта ресурсной системы;
- ФИО – идентифицирует владельца учетной 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 АЕСА СА:
    - «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 администратор при редактировании учётной записи оператора.
  - Администратор – обладает неограниченными возможностями, в том числе имеет доступ к управлению учетными записями и может делегировать полномочия Оператору на работу с определёнными группами субъектов;

- Superadmin – Учётная запись создана по умолчанию при установке программного обеспечения АЕСА СА, имеет неограниченные права и не может быть отредактирована или удалена. Прочие учётные записи могут быть созданы, отредактированы, удалены или заблокированы пользователем учетной записи «superadmin»;

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

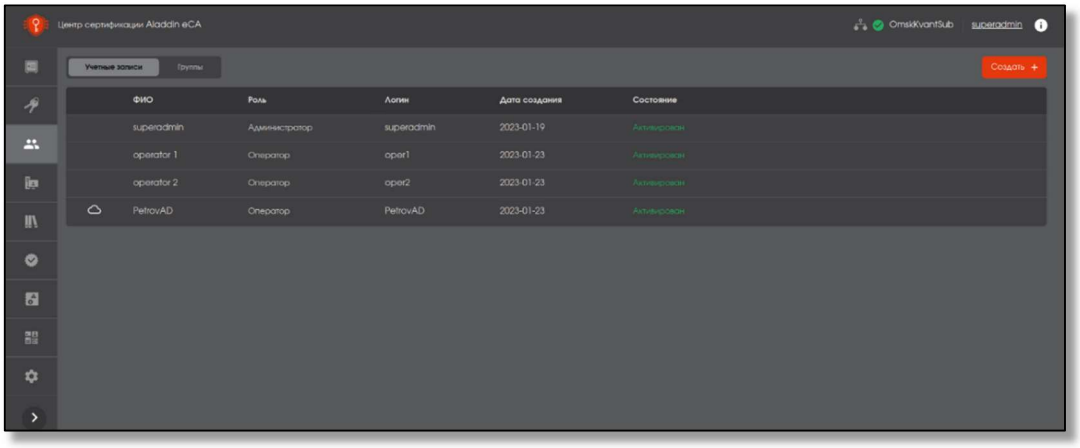


Рисунок 99 – Экран раздела меню «Учётные записи»

Вход в учётные записи пользователя на сервере осуществляется при помощи сертификатов, выпущенных с использованием шаблона «Web-client». Подробнее о настройке аутентификации для входа в учётную запись см. п. 4.10.2 настоящего руководства.

4.5.1.1 Создание новой учётной записи пользователя локального ресурса

- По нажатию кнопки <Создать +> на главном экране управления «Учётные записи» происходит запуск сценария создания учетной записи.
- В открывшемся окне заполните следующие поля (см. Рисунок 100):
  - выберите роль создаваемой учётной записи из предложенных – администратор или оператор
  - отображаемое имя – параметр учетной записи, отображаемый на верхней панели после авторизации;
  - логин – данные для поля сертификата «Common Name»;

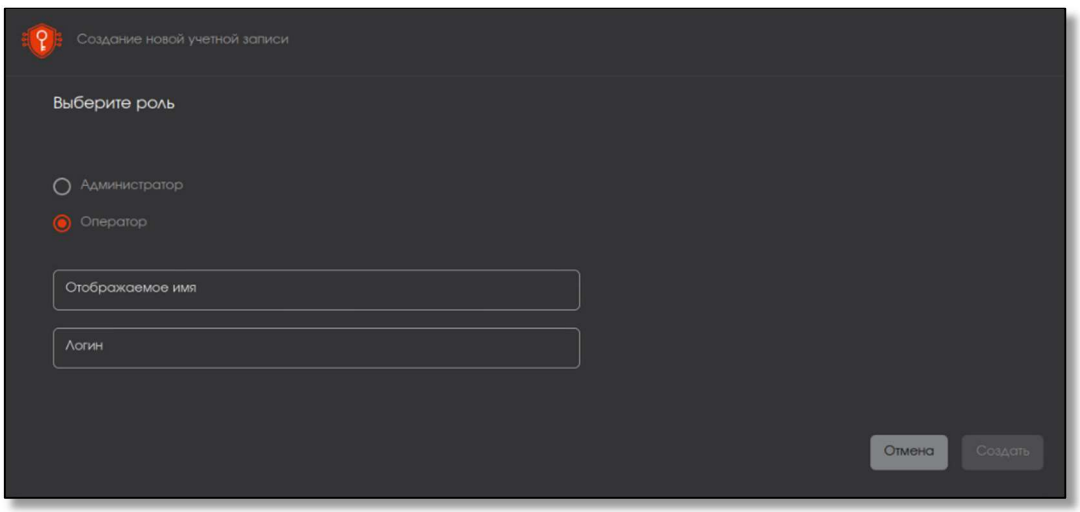


Рисунок 100 – Окно создания новой учётной записи

- 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 4.7.3 настоящего Руководства администратора.
- Для созданной учетной записи Администратора настройка прав не требуется, так как ограничений для этой роли не будет.

4.5.1.2 Создание учетной записи для субъекта ресурсной системы

Для создания учётной записи доменного пользователя воспользуйтесь ресурсной системой:

- Перейдите на вкладку «Субъекты» Центра сертификации;
- Выберите нужный ресурс ;
- Выберите группу безопасности ;
- Выберите пользователя, для которого необходимо создать учетную запись и нажмите кнопку в строке выбранного пользователя <Создать учетную запись> (см. Рисунок 101);

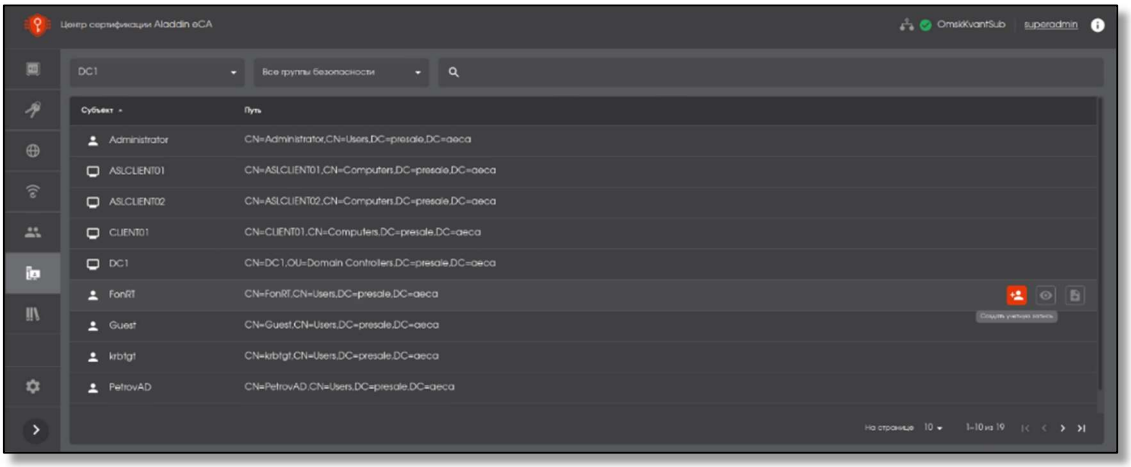


Рисунок 101 – Окно субъектов ресурсной системы

- В открывшемся окне Мастера создания новой учетной записи (см. Рисунок 100) автоматически заполнено, но доступно для редактирования поле «Отображаемое имя», поле «Логин» не отображается и заполняется по умолчанию в соответствии со значением Common Name выбранного доменного пользователя.

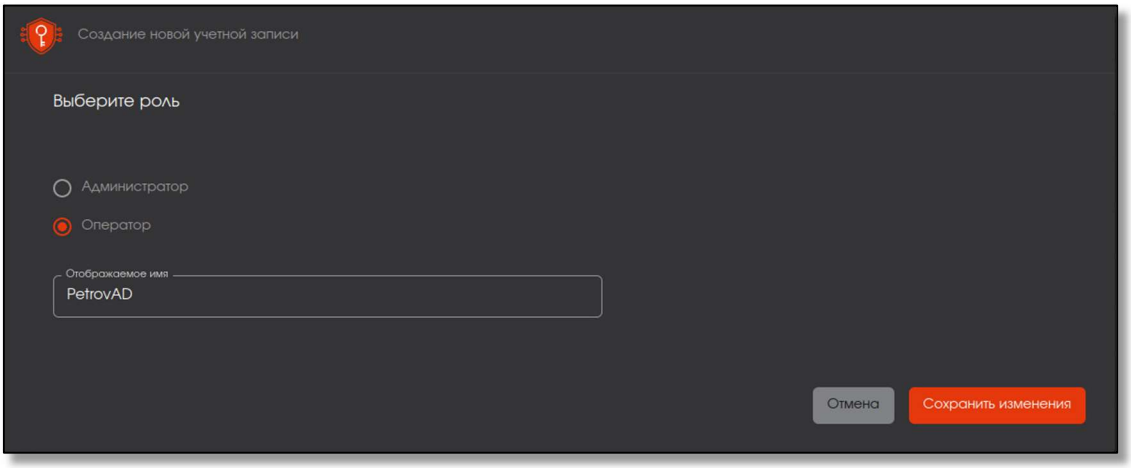


Рисунок 102 – Создание учетной записи для субъекта ресурсной системы

- Выберите роль, применяемую к создаваемой учетной записи.
- Нажмите кнопку <Сохранить> изменения для создания учетной записи доменного пользователя.
- Для созданной учетной записи Оператора произведите настройку прав доступа к группам и объектам ресурсной системы в соответствии с пунктом 4.7.3 настоящего руководства.

4.5.1.3 Доступные действия над учётными записями

После добавления учётной записи, при наведении курсора на строку добавленного пользователя центра сертификации появляются возможности (см. Рисунок 103):

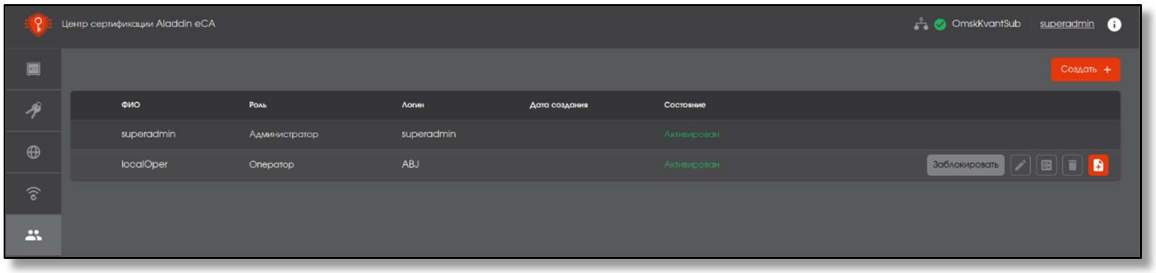


Рисунок 103 – Доступные действия над учетными записями

- Заблокировать / Активировать по нажатию кнопки <Заблокировать> возможно приостановить действие активной выбранной учётной записи или по нажатию кнопки <Активировать> возобновить действие заблокированной ранее учётной записи;
- редактирования – при нажатии на кнопку <Редактировать> открывается окно для редактирования полей, заполненных при создании ресурсной системы (см. Рисунок 104):
  - возможно изменение выбора назначенной роли;
  - поля «Отображаемое имя».
  - параметры связанного сертификата доступны только в режиме просмотра.
- Карточка учётной записи суперадмина доступна только для просмотра.

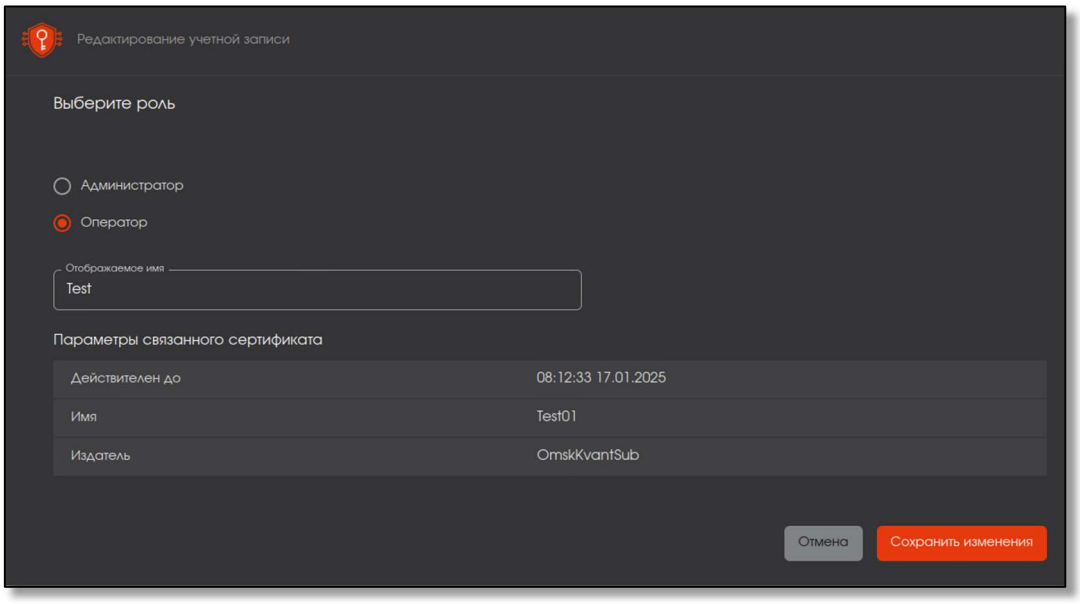


Рисунок 104 – Окно редактирование учётной записи

- права – определяются только для оператора. Администратор назначает для субъектов каких ресурсных систем, их организационных групп и групп безопасности возможны операции, обусловленные назначенной ролью (см. Рисунок 105). Доступ производится путем проставления отметки в пустом поле около названия группы или выбранного субъекта/группы субъектов и дальнейшим нажатии кнопки <Применить>.

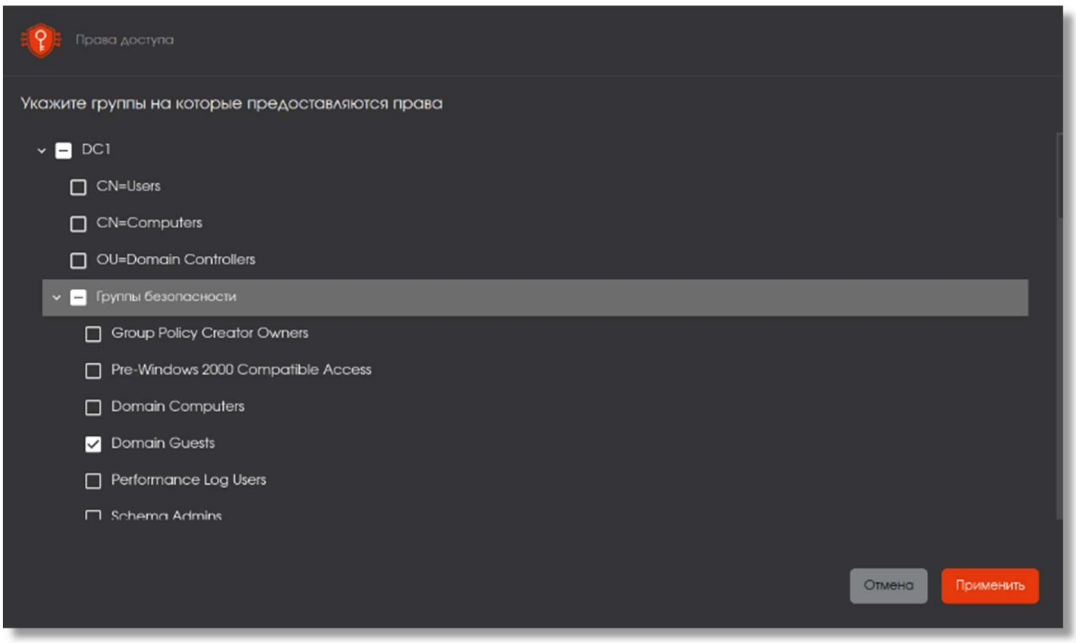


Рисунок 105 – Окно редактирования прав учётной записи

удаления – при необходимости возможно удалить добавленную учётную запись. Процесс удаления происходит без подтверждения, сразу по нажатию кнопки <Удалить>;

выпуск сертификата с закрытым ключом в контейнере pkcs#12 или на ключевом носителе для дальнейшей авторизации учетной записи.

4.5.1.4 Выпуск сертификата с закрытым ключом pkcs#12 для учетной записи

- Выделите учетную запись, сертификат для которой необходимо создать, и нажмите появившуюся кнопку <Выпустить сертификат>, в раскрывшемся меню выберите пункт «С закрытым ключом pkcs#12» (см. Рисунок 106).

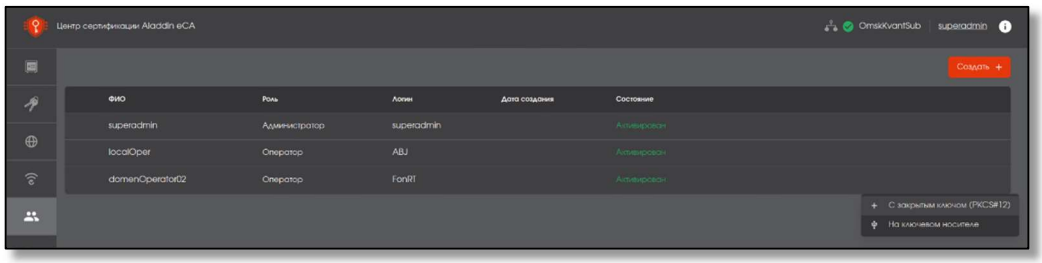


Рисунок 106 – Вкладка «Учетные записи». Кнопка выпуска сертификата с закрытым ключом

- В открывшемся окне создания сертификата заполните данные в соответствии с шаблоном web-клиента (подробное описание полей шаблона см. в Приложение А. Описание полей шаблонов сертификатов) для выбранной учетной записи. (см. Рисунок 107) и нажмите кнопку <Продолжить> для перехода на следующий шаг.

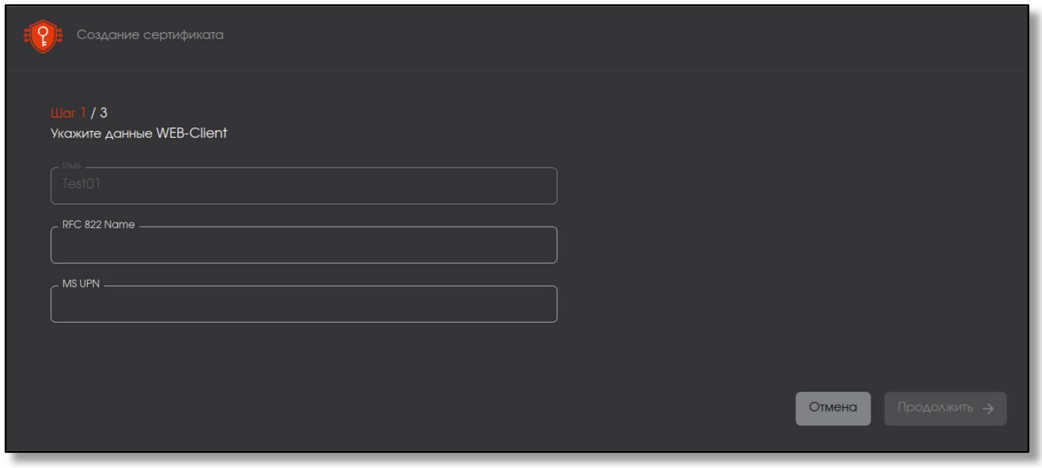


Рисунок 107 – Окно создания сертификата pkcs#12 учетной записи. Шаг 1

- Далее введите пароль и подтвердите его (см. Рисунок 108). Пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице. Пароль необходим для дальнейшего импорта сертификата учетной записи в браузер.

Нажмите ставшую активной при верном вводе пароля кнопку <Продолжить>.

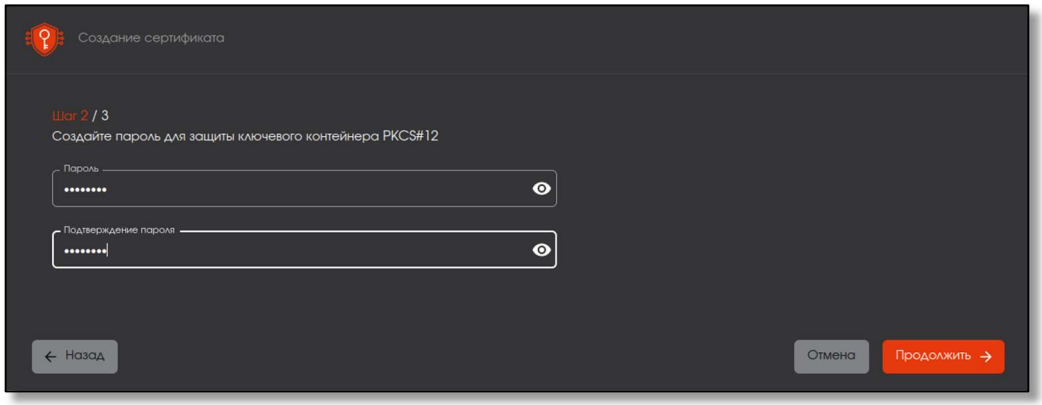


Рисунок 108 – Окно создания сертификата pkcs#12 учетной записи. Шаг 2

- В окне следующего шага выберите параметры криптографии доступные для данного шаблона (см. Рисунок 109):
  - алгоритм ключа;
  - длину ключа.

После выбора параметров криптографии нажмите ставшую активной кнопку <Создать сертификат>.

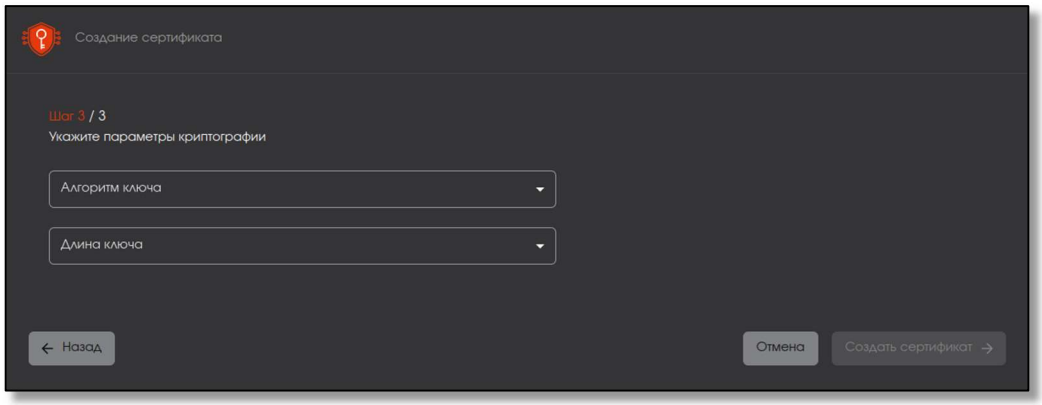


Рисунок 109 – Окно создания сертификата pkcs#12 учетной записи. Шаг 3

- На экране уведомления о успешном создании сертификата для учетной записи пользователя возможно сразу сохранить сертификат в формате .p12, нажав кнопку <Скачать> (см. Рисунок 110), или скачать сертификат позднее на вкладке «Сертификаты».

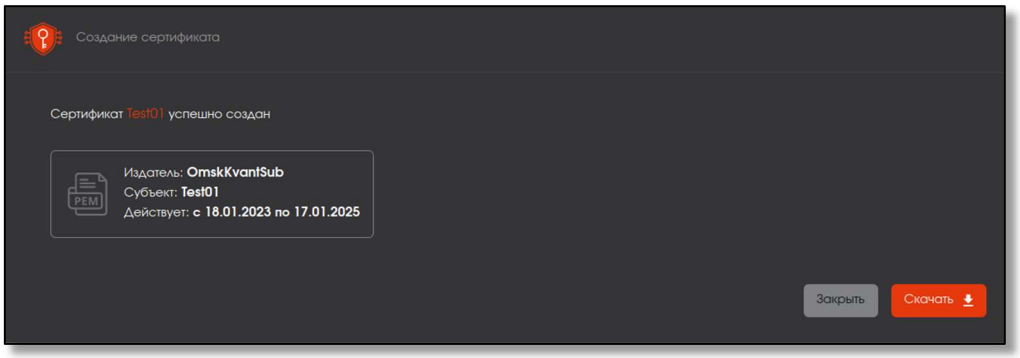


Рисунок 110 – Окно создания сертификата pkcs#12 учетной записи. Шаг 4

4.5.1.5 Выпуск сертификата на ключевом носителе для учетной записи

- Вставьте электронный ключ в usb-порт АРМ, на котором происходит выпуск сертификата.
- Выделите учетную запись, сертификат для которой необходимо создать, и нажмите появившуюся кнопку  <Выпустить сертификат>, в раскрывшемся меню выберите пункт «Ключевом носителе» (см. Рисунок 111).

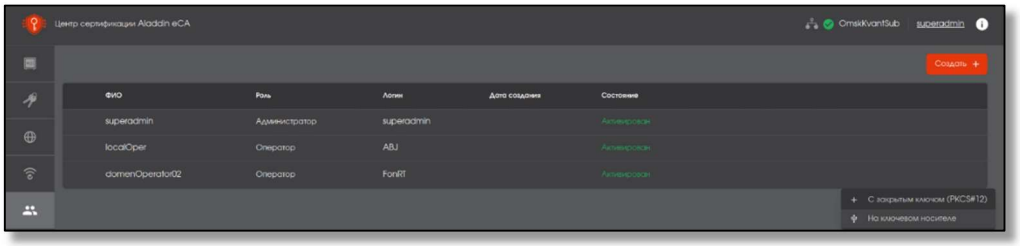


Рисунок 111 – Вкладка «Учетные записи». Кнопка выпуска сертификата на ключевом носителе

- В открывшемся окне создания сертификатов в поле «Устройство» выберите доступный электронный ключ, на который будет записан сертификат, в поле «PIN-код» введите PIN-код выбранного электронного ключа, шаблон сертификата для учетной записи пользователя выбран по умолчанию и не доступен для изменения (см. Рисунок 112).

По умолчанию активирован чек-бокс «Публиковать сертификат в ресурсную систему», при необходимости снимите флаг, чтобы не публиковать сертификат во внешнюю ресурсную систему.

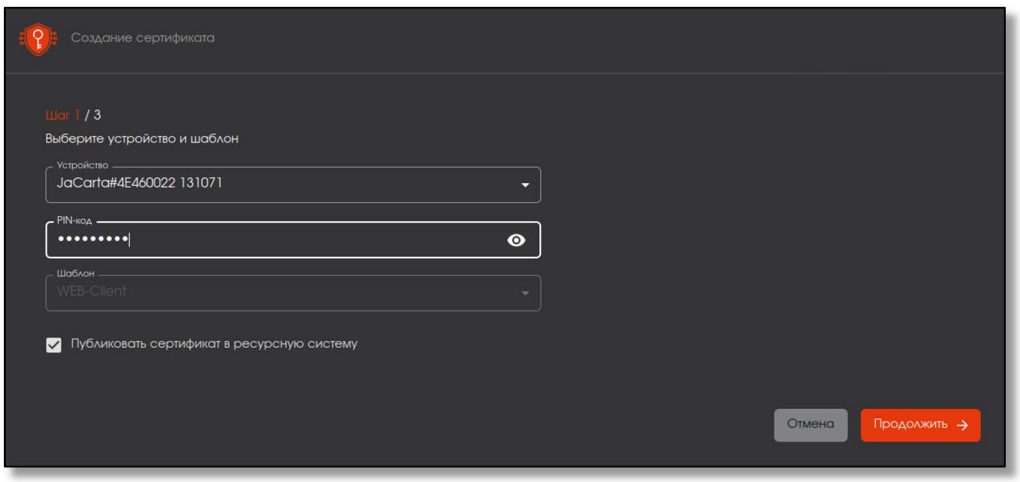


Рисунок 112 – Окно создания сертификата учетной записи на электронном носителе. Шаг 1

Нажмите ставшую активной кнопку <Продолжить> для продолжения создания сертификата.

- Переход на следующий шаг осуществляется в случае корректного PIN-код электронного ключа. В открывшемся окне поле «Имя» заполнено данными Common Name пользователя учётной записи и не подлежит редактированию, поля «RFC 822» и «Name MS UPN» подлежат редактированию и автоматически заполнены, если сертификат выпускается для учетной записи доменного пользователя и в атрибутах доменного пользователя указан `userPrincipalName`, в случае, если данный атрибут не задан или сертификат выпускается для учетной записи пользователя локального ресурса, то данные поля будут пустыми (см. Рисунок 113).

Далее нажмите кнопку <Продолжить>, ставшую активной, после заполнения всех полей экранной формы создания сертификата на втором шаге.

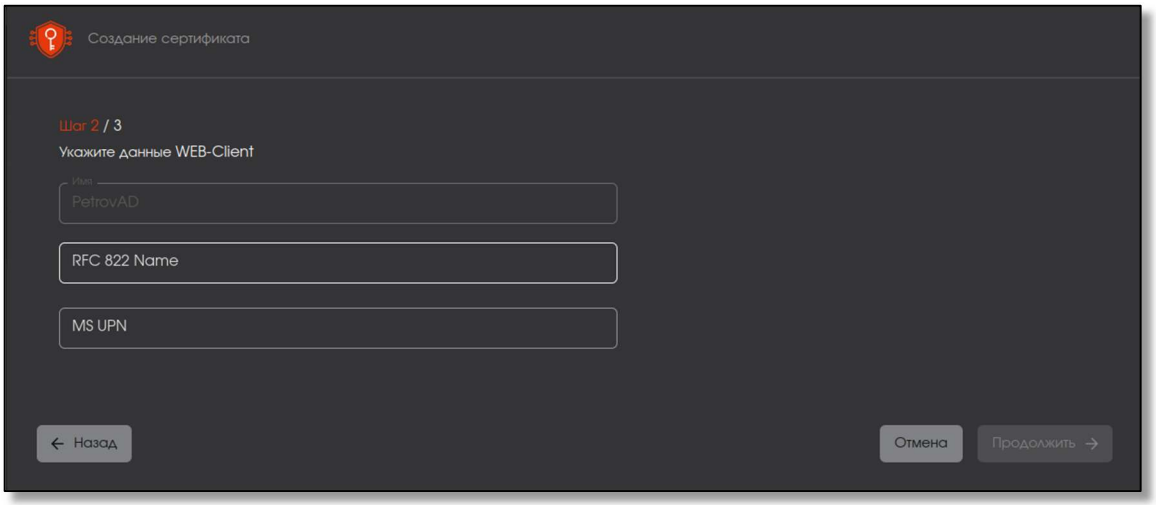


Рисунок 113 – Окно создания сертификата учетной записи на электронном носителе. Шаг 2

- Далее выберите алгоритм ключа из выпадающего меню, при этом предоставляется выбор алгоритмов в соответствии с установленной версией ПО JC-WebClient и моделью ключевого носителя (см. Рисунок 114).

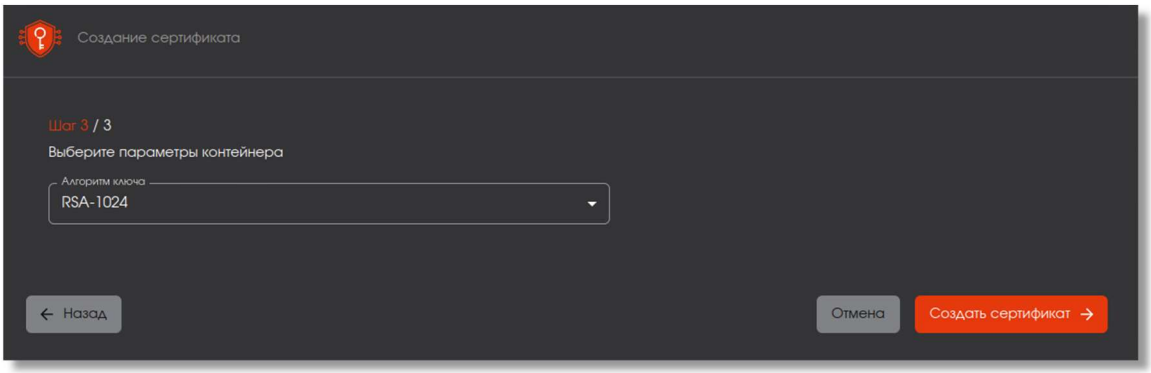


Рисунок 114 – Окно создания сертификата учетной записи на электронном носителе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
  - генерация ключевой пары;
  - генерация запроса;
  - выпуск сертификата;
  - запись на ключевой носитель.

Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов> (см. Рисунок 115).

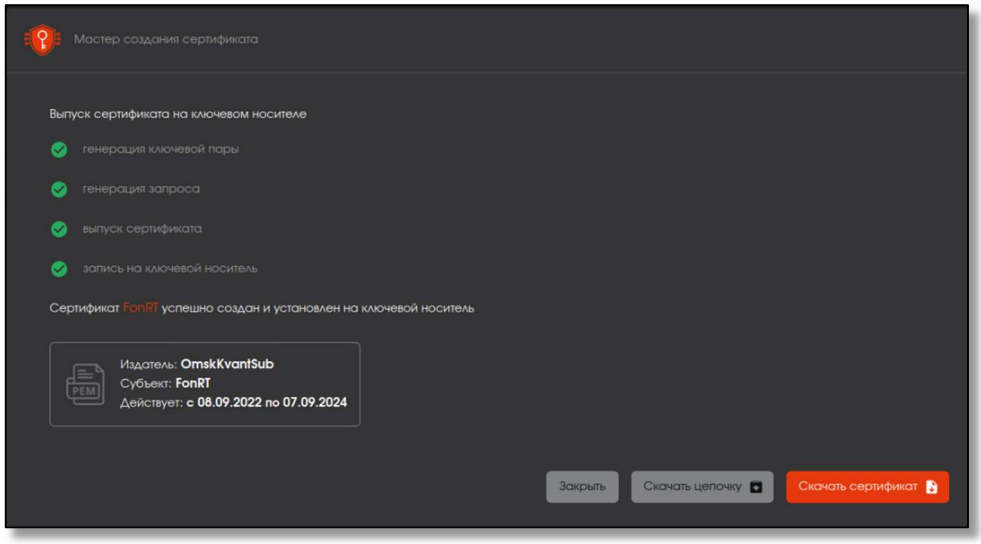


Рисунок 115 – Окно успешного создания сертификата учетной записи пользователя на электронном ключе

4.5.2 **Вкладка «Группы»**

На данной вкладке возможно назначение прав, определяющих роль оператора, сразу нескольким пользователям, находящихся в одной группе безопасности.

4.5.2.1 Добавление группы пользователей с ролью «Оператор»

- Нажмите кнопку <Добавить группы +> на вкладке «Группы» (см. Рисунок 116).

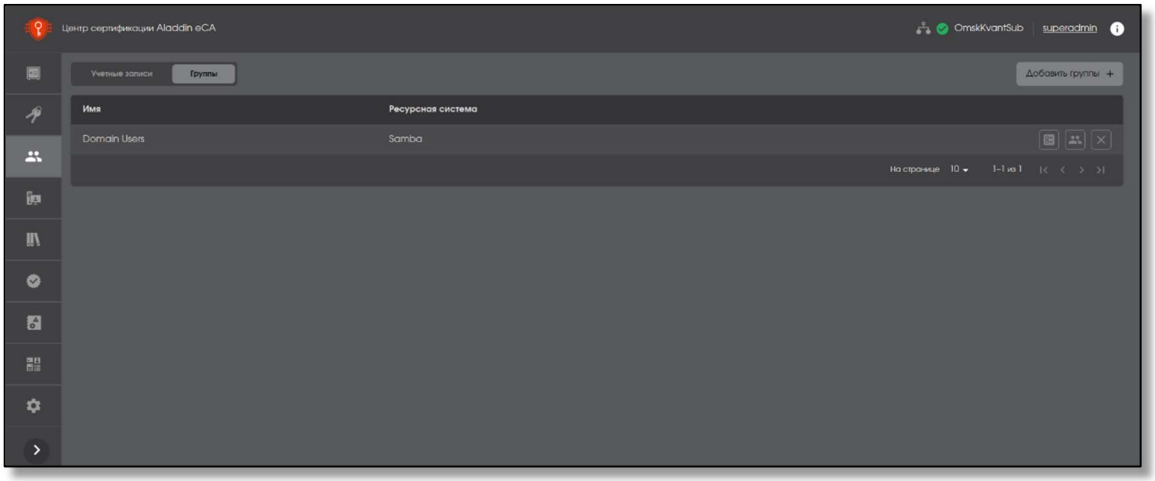


Рисунок 116 – Окно вкладки «Группы»

- В открывшемся окне (см. Рисунок 117) отображается иерархическое дерево групп безопасности ресурсных систем. Выберите в окне:
  - ресурсную систему;
  - в раскрывшемся списке – группы безопасности, субъектам которых будет назначена роль «Оператор».
- Подтвердите выбор, нажав кнопку <Добавить>.

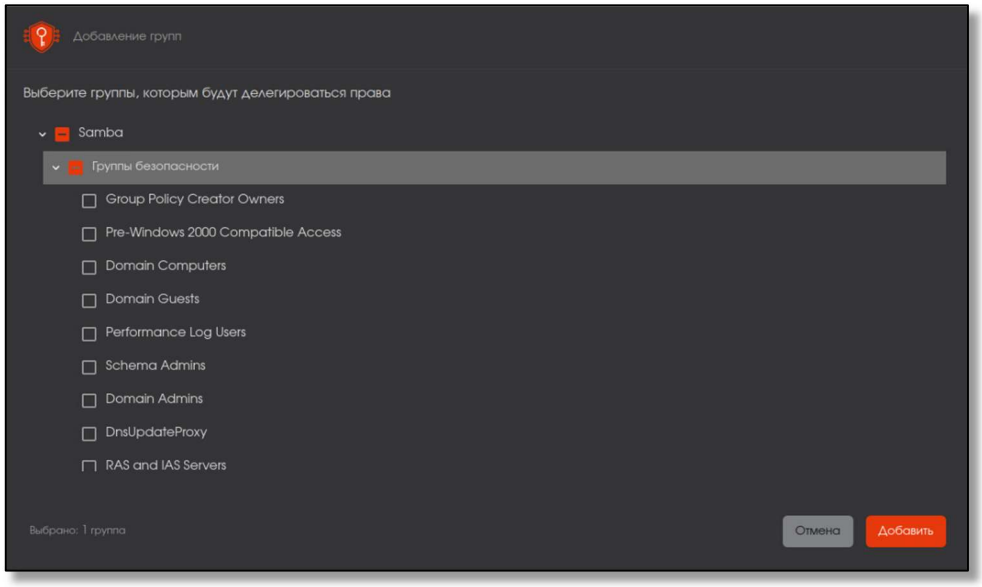


Рисунок 117 – Окно добавления групп

- В результате на экранной форме вкладки «Группы» будут добавлены выбранные группы безопасности и будет отображена информация (см. Рисунок 116):
  - 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.

4.5.2.2 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 118);
- подтвердить выбор, нажав кнопку <Добавить>.

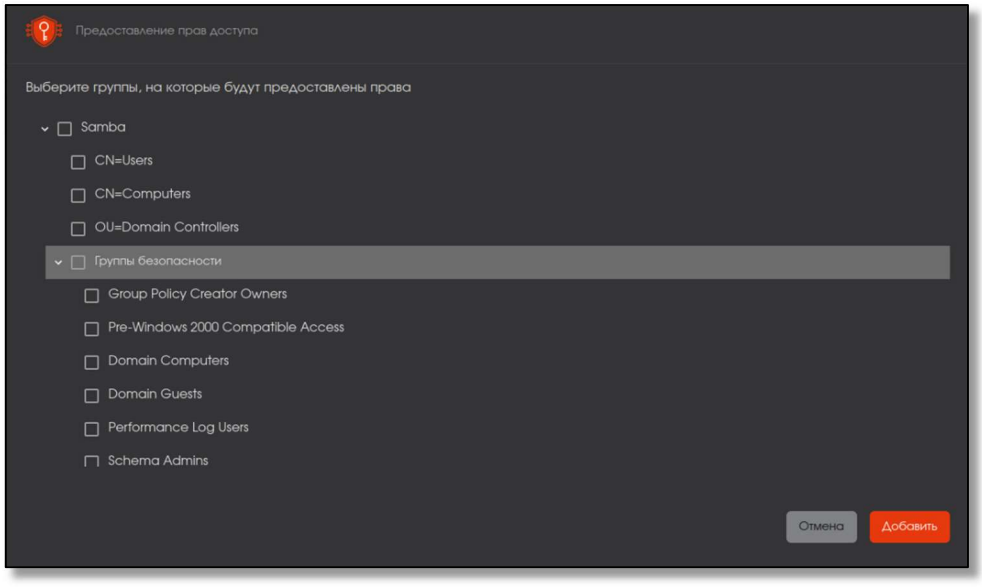


Рисунок 118 – Окно предоставления прав доступа для группы

4.5.2.3 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 119 – Окно учётных записей, созданных для группы безопасности

4.5.2.4 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.

4.5.3 Настройка аутентификации для входа в учётную запись

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.

Для настройки аутентификации:

- выпустите сертификат для учетной записи в соответствии с пунктом 4.5.4 или 4.5.5 настоящего документа;
- на вкладке «Настройка» в поле «Разрешенные издатели» выберите издателя, от имени которого был выпущен сертификат учетной записи, и активируйте проверку издателя, передвинув ползунок вправо;
- на вкладке «Настройки» нажмите кнопку Перезагрузить для применения настроек веб-сервера;
- загрузите сертификат учетной записи во встроенное хранилище веб-браузера на АРМ. Для браузера Firefox:
  - откройте новое приватное окно, в меню браузера выберите Настройки – Приватность и Защита – Сертификаты. Нажмите кнопку <Просмотр сертификатов>;
  - выберите вкладку «Ваши сертификаты», в открывшейся вкладке нажмите кнопку <Импортировать>;

- выберите файл созданного сертификата учетной записи на электронном ключе или локальном диске. Нажмите кнопку <Открыть>;
- введите пароль, указанный при создании сертификата учетной записи в открывшемся окне, и нажмите кнопку <Ок>;
- для входа в Центр сертификации по учетной записи введите в адресную строку: `<адрес_хоста_развертывания_продукта>:<порт>/<aecaCa>/`;
- в появившемся окне «Запрос идентификации пользователя» выберите установленный сертификат учетной записи;
- в случае успешной установки сертификата откроется страница с предупреждением системы безопасности. Нажмите кнопку <Advanced>;
- по нажатию кнопки <Advanced> на странице предупреждения системы безопасности осуществляется переход на страницу ошибки распознавания сертификата. Нужно принять риски, нажав кнопку <Accept the Risk and Continue> на текущей странице;

- аутентификация выполнена успешно, в случае перехода в Центр сертификации с указанием отображаемого имени на верхней панели соответствующей учетной записи.

4.6 Описание вкладки «Субъекты»

- Переход на вкладку «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).
- На вкладке «Субъекты» в верхней панели расположены элементы (см. Рисунок 120):
  - поле «ресурсная система», по нажатию на поле выберите локальную ресурсную систему или подключенный ресурс (см. пункт 4.9.1 настоящего документа) для отображения всех субъектов ресурса;
  - поле «выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в развернувшемся 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;
  - в поле поиска осуществляется поиск субъектов по компонентам SubjectDN и SubjectAltName. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры.

Рисунок 120 – Верхняя панель экранной формы вкладки «Субъекты»

- Источники ресурсной системы подразделяются на:
  - локальный ресурс;
  - внешние ресурсы.
- Публикация сертификатов в ресурсную систему возможна только на данной вкладке:
  - при выпуске сертификата для субъекта путем установления флага «Публиковать сертификат в ресурсную систему» на шаге выбора шаблона сертификата;
  - из карточки субъекта по кнопке <Опубликовать в ресурсную систему> в поле «Сертификаты».

- Сертификат публикуется в формате LDIF в атрибут `userCertification` выбранного субъекта ресурсной системы, для которого выпущен сертификат.

4.6.1 **Субъекты локальной ресурсной системы**

- Новые субъекты, для которых выпускается сертификат, формируют локальную базу данных субъектов AECA CA. Локальная ресурсная система автоматически создается при установке ПО AECA CA. Субъекты представлены в виде списка с сортировкой по заголовку табличного поля экранной формы.
- По нажатию соответствующих кнопок в строке субъекта возможны следующие действия (см. Рисунок 121):
  - выпустить сертификат – нажатие кнопки  открывает подменю для выбора выпуска сертификата с закрытым ключом (PKCS#12) или на ключевом носителе с последующим вызовом Мастера создания сертификата.
- Действия применимые к субъектам ресурсных систем приведены в Таблица 8.

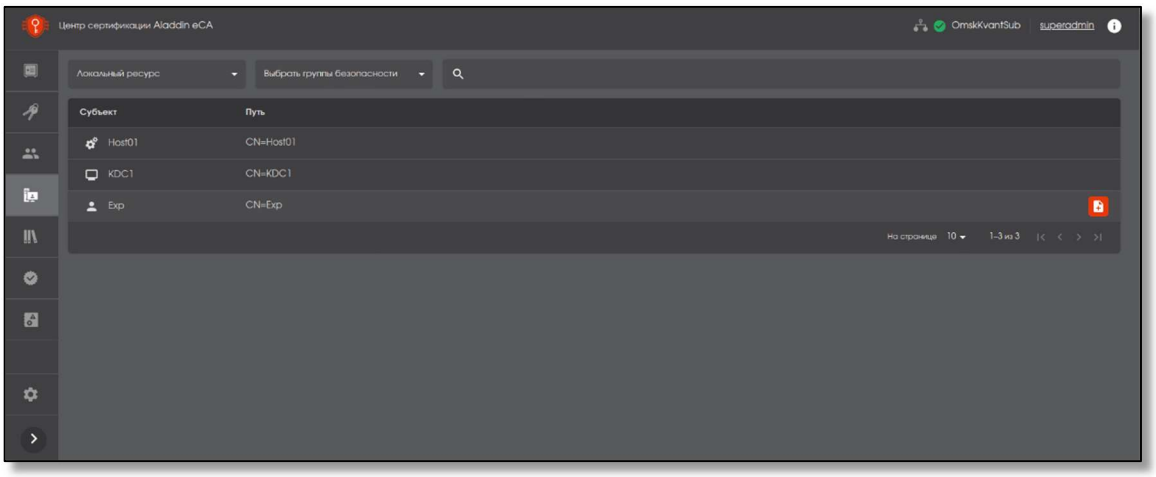


Рисунок 121 – Экран раздела меню «Субъекты». Локальный ресурс

4.6.2 **Субъекты подключаемого ресурса**

- Внешний ресурс формируется в результате подключения к службе каталогов доменных служб Samba DC, ALD PRO, FreeIPA или MS Active Directory.
- Внешний ресурс будет отображен только после создания ресурсной системы на вкладке «Ресурсная система» (см. пункт 4.7.1 настоящего руководства).
- Обновление субъектов ресурсной системы происходит на вкладке «Ресурсная система» или автоматическая синхронизация каждые 30 минут (см. п. 4.7.2 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 122).

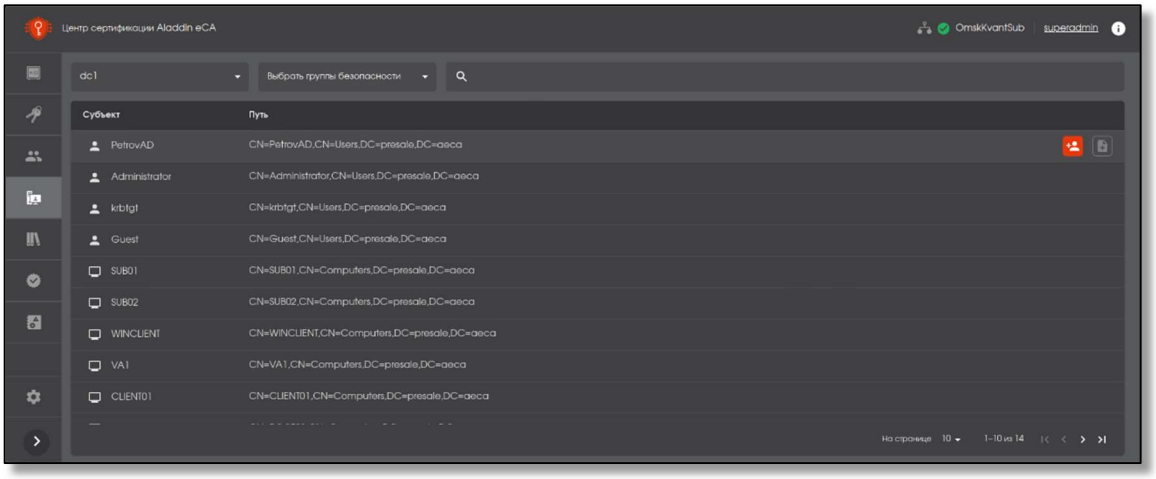


Рисунок 122 – Экран раздела меню «Субъекты». Подключенный ресурс

- 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 7.

Таблица 7 – Преобразование данных субъектов ресурсной системы

Поле в базе субъектов ресурсной системы	**Поле в базах Samba DC MS AD**	**Поле в базах ALD PRO FreeIPA**
name	name	serverHostName/CN
MS_GUID	objectGUID	ipaUniqueID
MS UPN	userPrincipalName	krbPrincipalName
CommonName	CN	CN
RFC822Name	name или dNSHostName	CN или ServerHostName
CountryCode	C или CountryCode (в формате DCC)	-
objectGuid	objectGUID	ipaUniqueID
Organization	Organization	Organization
Department	Department	Department

- Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.
- По нажатию соответствующих кнопок в строке субъекта возможны следующие действия (см. Рисунок 122):
  - создать учётную запись – нажатие кнопки  запускает Мастер создания новой учетной записи (см. п.3.6.2), созданная учетная запись будет отображена на вкладке «Учётные записи»;
  - выпустить сертификат – нажатие кнопки  открывает подменю для выбора выпуска сертификата с закрытым ключом (PKCS#12), на основании запроса или на ключевом носителе с последующим вызовом Мастера создания сертификата.

При выпуске сертификата значения полей заполняются автоматически соответственно атрибутам, указанным для субъекта в ресурсной системе .

Действия применимые к субъектам ресурсных систем приведены в Таблица 8.

Таблица 8 – Доступные действия над субъектами

Ресурсная система	Группа субъектов	Показать сертификаты	Выпустить сертификат	Создать учетную запись
Локальный ресурс	–	в карточке субъекта	✚	□
Ресурс Samba DC	Users	в карточке субъекта	✚	✚
	Computers	в карточке субъекта	✚	□
	Domain Controllers	в карточке субъекта	✚	□

4.6.3 **Сортировка субъектов**

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 123):

- «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 фильтрация обозначен знаком ▲ с правой стороны от заголовка таблицы.

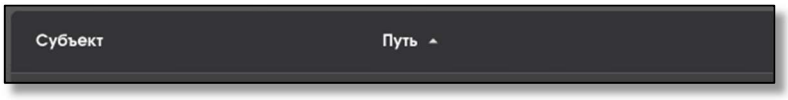
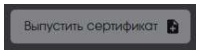


Рисунок 123 – Поля сортировки содержимого вкладки «Сертификаты»

4.6.4 **Карточка субъекта**

- Просмотра данных субъекта возможен посредством страницы «Карточка субъекта».
- Переход к экрану «Карточка субъекта» (см. Рисунок 124) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 122).
- Карточка субъекта включает в себя следующие информационные поля:
  - имя;
  - objectGUID;
  - UserPrincipleName;
  - CommonName;
  - код страны;
  - организацию;
  - отдел;
  - e-mail;
  - сведения обо всех выпущенных ранее для субъекта сертификатах:

- номер;
- шаблон;
- дата окончания действия;
- дата публикации в ресурсную систему.

- Доступные действия в карточке субъекта:
  - выпуск сертификата для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку <Выпустить сертификат> 

(см. п. 4.6.5, 4.6.6, 4.6.7 настоящего Руководства администратора);
  - опубликовать сертификат в ресурсную систему. 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;
  - скачать сертификат выбранного субъекта по указанному для сохранения файла пути.

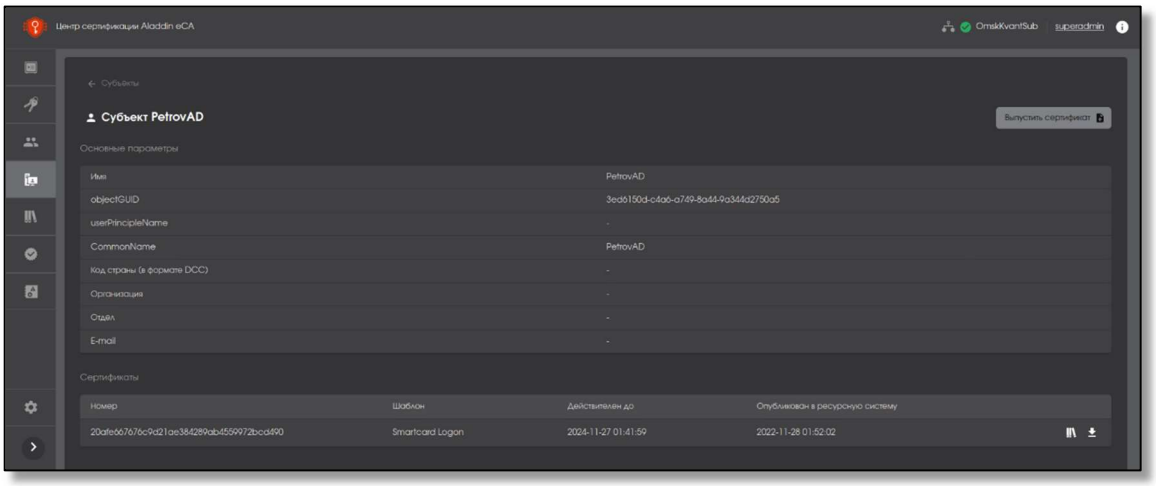


Рисунок 124 – Окно просмотра карточки субъекта

- Для возврата на главный экран раздела «Субъекты» проследовать по стрелке 

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

4.6.5 **Выпуск сертификата с закрытым ключом для субъекта ресурсной системы**

- Откройте ресурс, выберите субъект, для которого будет выпущен сертификат, нажмите кнопку  <Выпустить сертификат> и из выпадающего списка выберите пункт <С закрытым ключом (PKCS#12)> (см. Рисунок 125). Стартует сценарий по созданию сертификата с закрытым ключом посредством мастера создания сертификата.

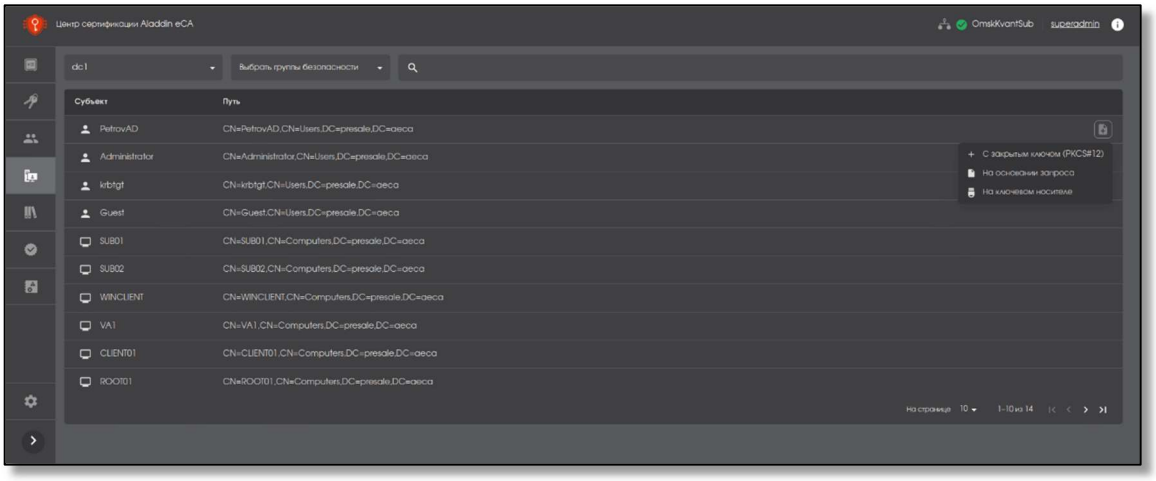


Рисунок 125 - Окно выпуска сертификата для субъекта ресурсной системы

- Далее администратор выбирает из выпадающего списка шаблон субъекта ресурсной системы (см. Рисунок 126).

На данном шаге можно выбрать публикацию сертификата в формате LDIF в атрибут `userCertification` субъекта ресурсной системы. По умолчанию флаг выполнения публикации сертификата включен.

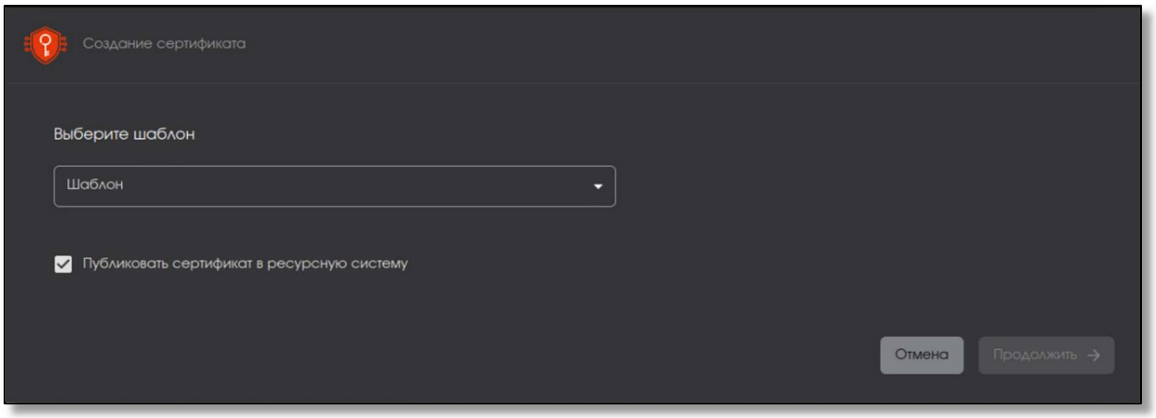


Рисунок 126 - Окно создания сертификата PKCS#12 для субъекта ресурсной системы

Далее по ставшей активной кнопке <Продолжить> осуществляется переход к следующему шагу.

- После выбор шаблона субъекта ресурсной системы на следующем шаге поля автоматически заполняются данными субъекта (см. Рисунок 127) в соответствии:
  - в поле «Имя» передаются данные атрибута Common name содержимого записи LDAP. Поле не изменяемое;
  - в поле «RFC 822 Name» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение;
  - в поле «MS UPN» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение.

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля вручную.
- Описание шаблонов смотри в Приложение А. Описание полей шаблонов сертификатов.
- Вводимые данные не должны содержать кириллицу, знаки: «+», «\», «,», ограничители ввода между параметрами.

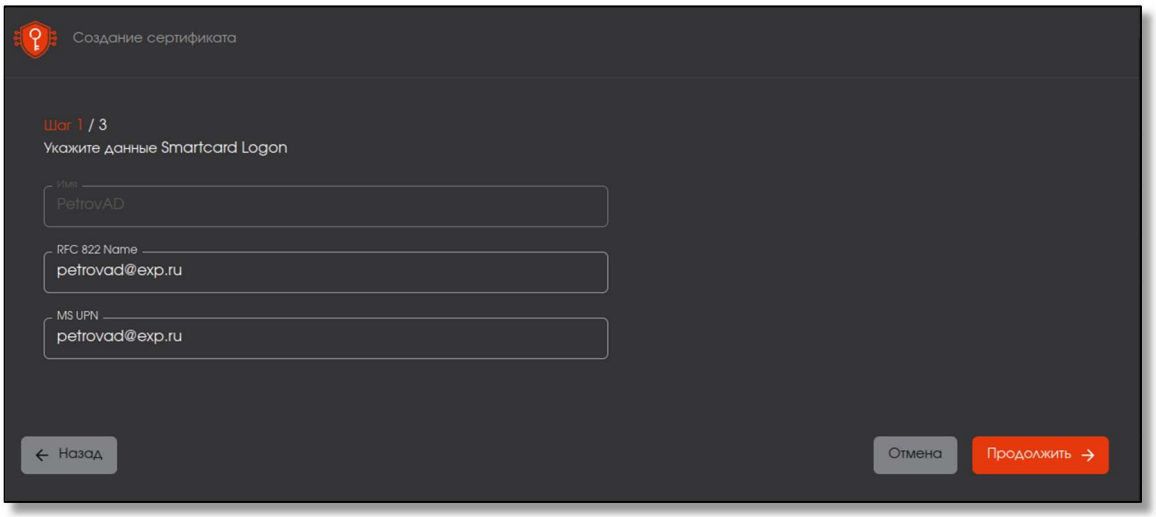


Рисунок 127 – Окно создания сертификата PKCS#12 для субъекта ресурсной системы. Шаг 1

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 128).
- Правила ввода пароля:
  - для просмотра вводимых символов необходимо нажать кнопку на текущей строке;
  - пароль должен содержать не менее 8 символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;
  - если в пароле используются запрещенные символы, то рамка поля ввода приобретает красный цвет;
  - если пароли не совпадают, то рамка поля подтверждения окрашивается в красный цвет.
- Кнопка <Продолжить> доступна только после ввода и верного повторения пароля в соответствии с правилами ввода.

Рисунок 128 – Окно создания сертификата PKCS#12 для субъекта ресурсной системы. Шаг 2

- В следующем окне требуется определить параметры шифрования (см. Рисунок 129):
  - алгоритм ключа;
  - длину ключа.
- Параметры определяются шаблоном сертификата и выбираются в соответствии с техническими требованиями шаблона.
- После определения всех параметров шифрования становится доступной для нажатия кнопка <Создать сертификат>.

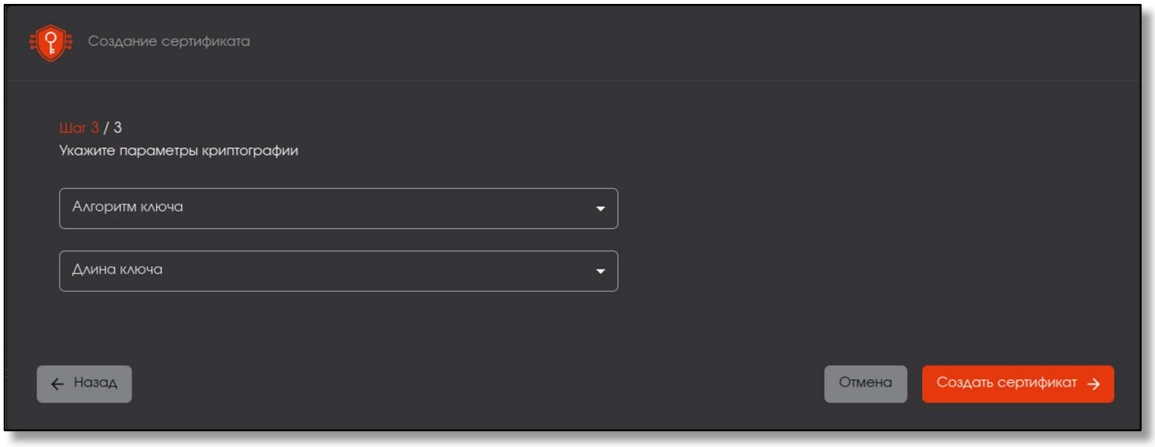


Рисунок 129 - Окно создания сертификата PKCS#12 для нового пользователя. Шаг 3

- По завершению работы мастера создания сертификата субъекта администратор видит окно, изображенное на Рисунок 130. В окне отображена общая информация о созданном сертификате (издатель, субъект, срок действия). Возможно скачать данный сертификат.
- Существует возможность скачать созданный сертификат на вкладке «Сертификаты» или в карточке субъекта на вкладке «Субъекты».

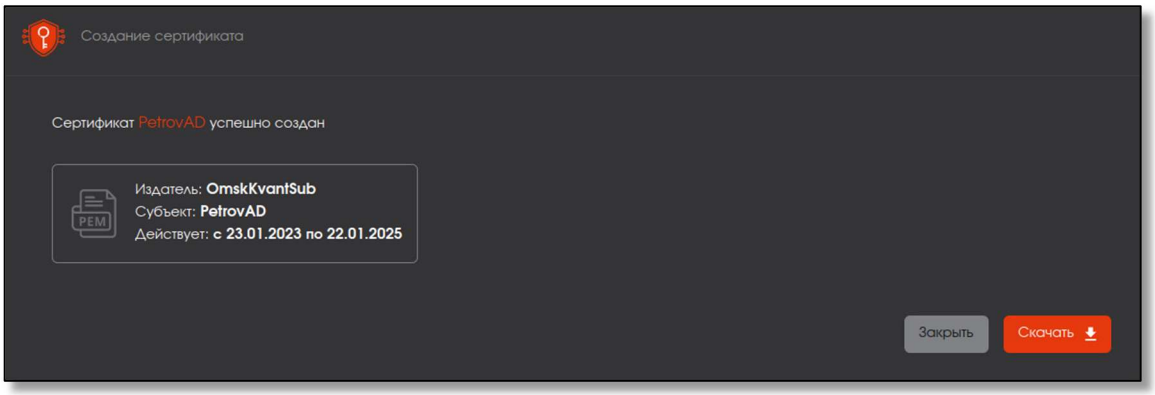


Рисунок 130 – Окно по результату успешного завершения создания сертификата PKCS#12 для субъекта ресурсной системы

4.6.6 **Выпуск сертификата на основании запроса**

- Откройте ресурс, выберите субъект, для которого будет выпущен сертификат, нажмите кнопку  <Выпустить сертификат> и из выпадающего списка выберите пункт <На основании запроса> (см. Рисунок 125). Стартует сценарий по созданию сертификата по запросу посредством мастера создания сертификата.

Далее администратор выбирает из выпадающего списка шаблон субъекта ресурсной системы и загружает файл запроса на сертификат (см. Рисунок 125). При необходимости,

возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.

- На данном шаге можно выбрать публикацию сертификата в формате LDIF в атрибут `userCertification` субъекта ресурсной системы. По умолчанию флаг выполнения публикации сертификата включен.

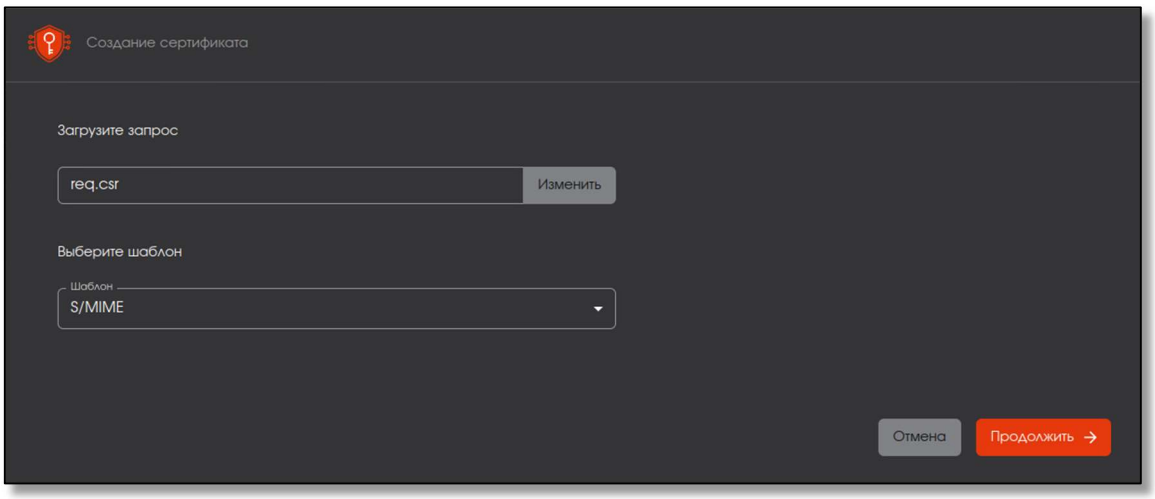


Рисунок 131 – Окно создания сертификата субъекта ресурсной системы по запросу. Шаг 1

- Далее по ставшей активной кнопке <Продолжить> осуществляется переход к следующему шагу.
- Приложение проверяет запрос на наличие субъекта:
  - при соответствии данных запроса и выбранного шаблона открывается окно с данными шаблона и принятыми данными из файла запроса (см. Рисунок 132).

ВНИМАНИЕ! Окно с данными шаблона приведен в ознакомительных целях, количество и наименование полей зависят от выбранного шаблона.

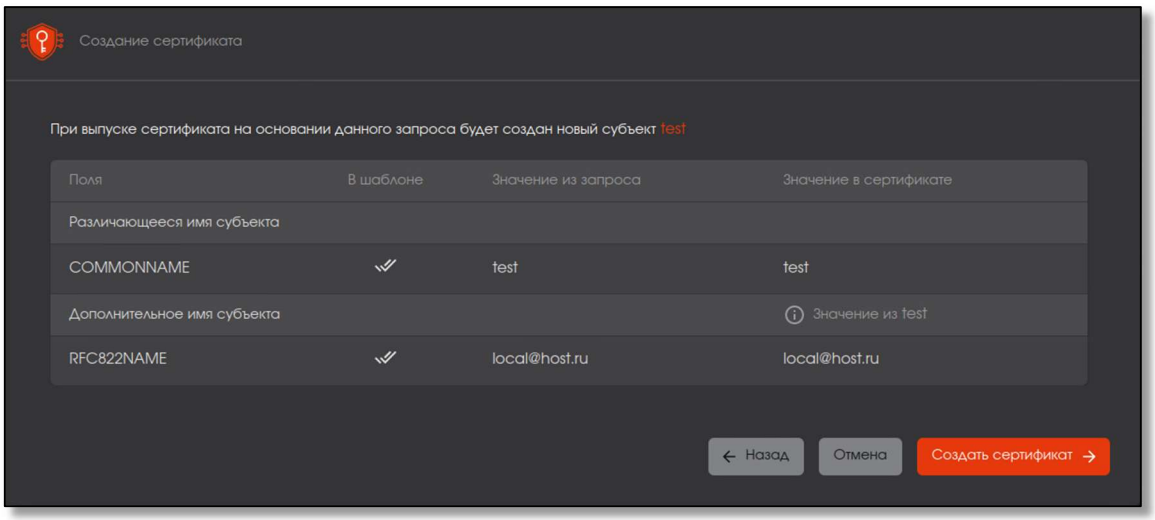


Рисунок 132 – Окно создания сертификата на основании запроса для субъекта ресурсной системы

- В случае неудачной проверки на соответствие полей запроса на сертификат и выбранного шаблона администратор буде уведомлён сообщениями об ошибке:
  - «Не задано обязательное поле» в случае, если в загружаемом запросе отсутствует поле, которое является обязательным в выбранном шаблоне;

- «Поле не соответствует формату, указанному в шаблоне» в случае, если загружаемый запрос содержит поле, которое отсутствует в выбранном шаблоне.

4.6.7 **Выпуск сертификата субъекта ресурсной системы на ключевом носителе**

- Предварительные условия выполнения сценария:
  - убедитесь, что электронный ключ присоединен к АРМ выпускающего Центра сертификации;
  - убедитесь, что на АРМ веб-клиента установлено ПО JC-WebClient версии 4.3.2 или 4.3.3 для дальнейшей работы с токенами из браузера.
- Выберите ресурс, выберите субъект, для которого будет выпущен сертификат, нажмите кнопку  <Выпустить сертификат> и из выпадающего списка выберите пункт <На ключевом носителе> (см. Рисунок 125). Стартует сценарий по созданию сертификата на ключевом носителе посредством мастера создания сертификата.
- В случае, если электронный носитель не подключен, администратор будет уведомлен об этом информационным сообщением (см. Рисунок 133). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

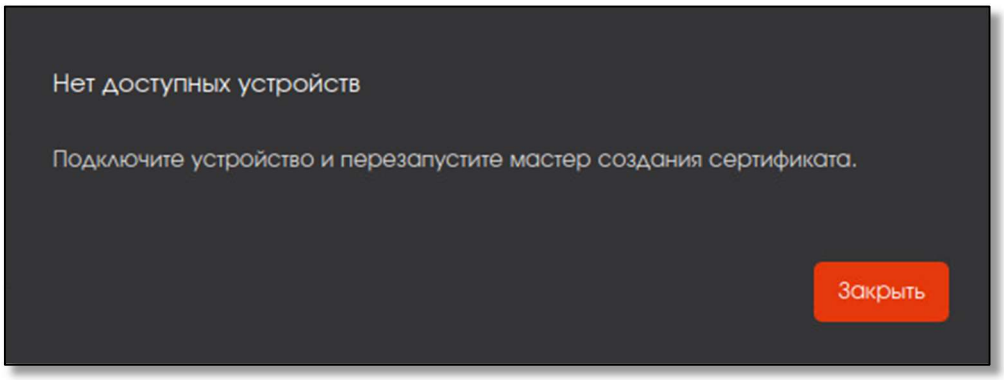


Рисунок 133 – Окно информационного сообщения «Нет доступных устройств»

- В случае, если электронный ключ успешно подключен, в открывшемся окне (см. Рисунок 134) необходимо выбрать ключевой носитель, ввести его пин-код и указать шаблон для выпуска сертификата. В случае, если ключевых носителей более одного, то необходимо выбрать нужный из выпадающего списка в поле «Устройство».
- На данном шаге можно выбрать публикацию сертификата в формате LDIF в атрибут `userCertification` субъекта ресурсной системы. По умолчанию флаг выполнения публикации сертификата включен.
- После ввода всех данных кнопка «Продолжить» становится активной.

Рисунок 134 – Окно создания сертификата субъекта ресурсной системы на электронном ключе. Шаг 1

- На втором шаге поля (в зависимости от выбранного шаблона выпускаемого сертификата на предыдущем шаге) автоматически заполнены данными субъекта (см. Рисунок 135):
  - в поле «Имя» передаются данные атрибута Common name содержимого записи LDAP. Поле не изменяемое;
  - в поле «RFC 822 Name» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение;
  - в поле «MS UPN» передается содержимое атрибута userPrincipalName записи LDAP. Данные в этом поле можно отредактировать. Если атрибут userPrincipalName не задан, то необходимо ввести в пустое поле окна создания сертификата нужное значение.
- Более подробное описание полей шаблона приведено в Приложение А. Описание полей шаблонов сертификатов.

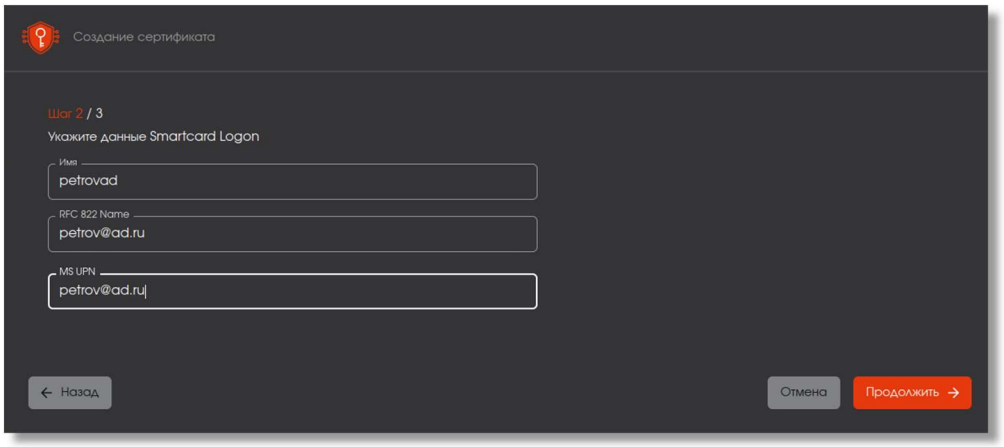


Рисунок 135 – Окно создания сертификата субъекта ресурсной системы на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии алгоритм ключа (см. Рисунок 136).

После выбора алгоритма нажмите кнопку <Создать сертификат>.

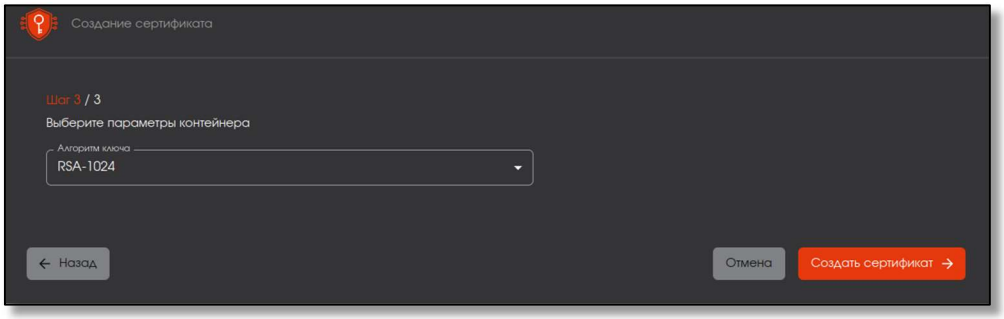


Рисунок 136 – Окно создания сертификата субъекта ресурсной системы на электронном ключе. Шаг 3

- Далее осуществляются все необходимые операции для выпуска и записи сертификата на ключевой носитель:
  - генерация ключевой пары;
  - генерация запроса;
  - выпуск сертификата;
  - запись на ключевой носитель.

Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов> (см. Рисунок 137).

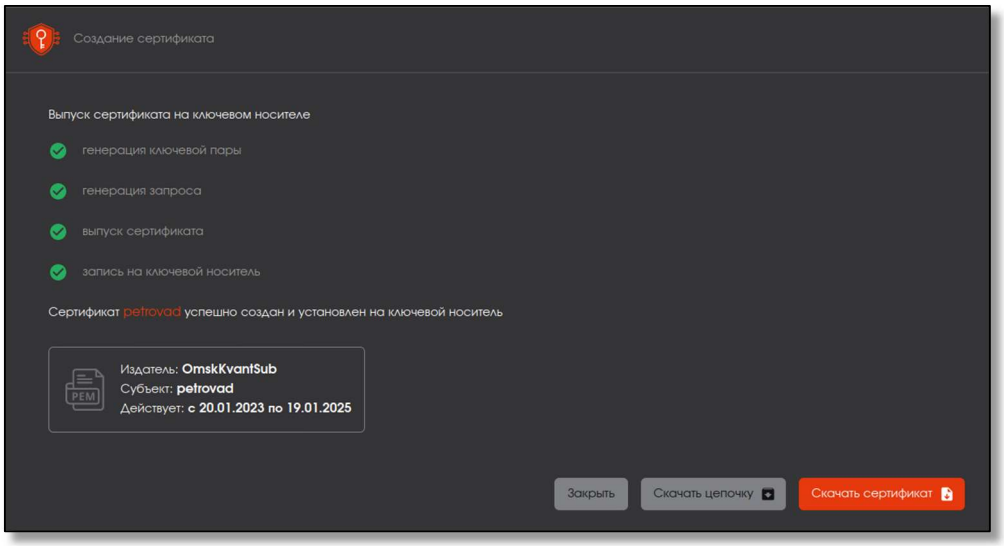


Рисунок 137 – Окно успешного создания сертификата субъекта ресурсной системы на электронном ключе

4.7 Описание вкладки «Ресурсная система»

Переход на вкладку «Ресурсная система» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).

На основном экране «Ресурсной системы» отображены информационные поля (см. Рисунок 138):

- подключаемая ресурсная система – Samba DC, MS AD, FreeIPA 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 АЕСА;
- статус – отображается статус подключения к источнику;
- субъекты – показывает количество загруженных субъектов из источника.

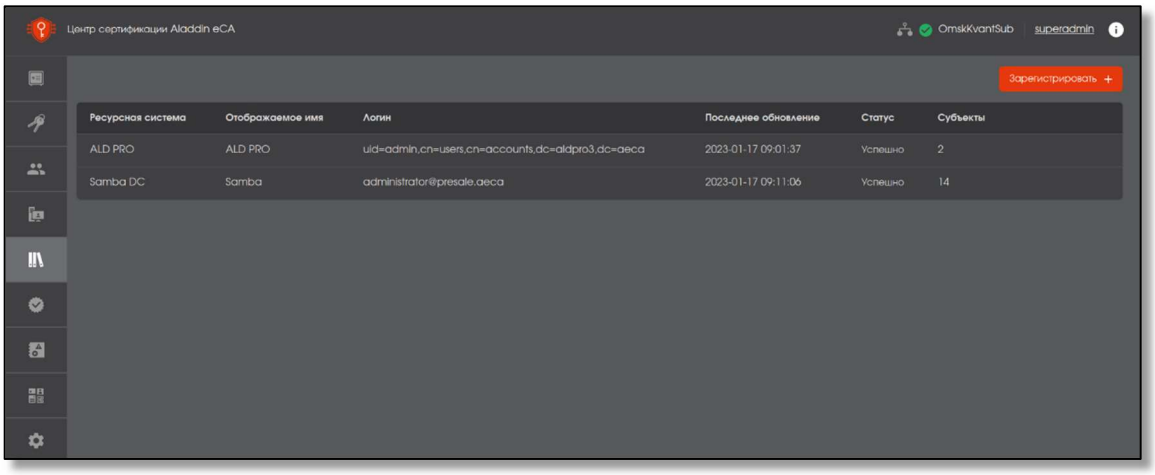


Рисунок 138 – Экран раздела меню «Ресурсная система»

- Aladdin Enterprise CA позволяет загрузить из нескольких ресурсных систем Samba DC, MS AD, FreeIPA или ALD PRO:

- список пользователей;
- список компьютеров;
- список организационных групп;
- список групп безопасности.

- Идентификация загружаемый субъектов ресурсной системы производится по полю objectGuid/ ipaUniqueID.

4.7.1 **Предварительная настройка подключения по протоколу TLS**

При дальнейшем выборе подключения к ресурсной системе с использованием протокола TLS, необходимо:

- на хосте, где развёрнут контроллер домена:
  - скопировать текущий сертификат контроллера домена, к которому будет производиться подключение, для tls соединений в файловой системе. В Таблица 9 приведено стандартное расположение сертификата контроллера домена.

Таблица 9 – Расположение сертификата контроллера домена

Контроллер домена	**Путь расположения файла сертификата контроллера домена**
ALD PRO	/etc/ipa/ca.crt
FreeIPA	/etc/ipa/ca.crt
Samba DC	/var/lib/samba/private/tls/cert.pem
MS AD	При стандартной установке MS AD: 1) добавьте оснастку «Certificates»: - в окне «Выполнить» введите mmc; - в открывшейся консоли откройте File-add-Certificates-Add-Computer account-Next (Local Computer)-OK; 2) откройте установленную оснастку Console Root-Certificates; 3) выбираем сертификат со свойством Intended Purposes=Server Authentication; 4) экспортируйте сертификат, выбрав формат DER Export-Der (.CER)

- на хосте, где развёрнут Центр Сертификации Aladdin CA:
  - перенести скопированный сертификат контроллера домена, к которому выполняется tls подключение, в домашний каталог пользователя, который будет выполнять команды в терминале;
  - выполнить команды, находясь в каталоге с сертификатом, в соответствии с Таблица 10.

Таблица 10 – Установка сертификата контроллера домена для tls соединения

Тип сертификата контроллера домена	**Действия**
1.	Конвертируйте сертификат контроллера домена в формат .DER
ALD PRO	`openssl x509 -outform der -in ca.crt -out aldpro.der`
FreeIPA	`openssl x509 -outform der -in ca.crt -out aldpro.der`
MS AD	`openssl x509 -inform DER -in WINMSCS.cer -out winca.crt` `openssl x509 -outform der -in WINMSCS.crt -out winca.der`
Samba DC	`openssl x509 -outform der -in cert.pem -out smbdc.der`

Тип сертификата контроллера домена	Действия
2. Получите путь к каталогу с установленным java одним из способов для переменной среды JAVA_HOME	
способ 1	`dirname $(dirname $(readlink -f $(which javac)))`
способ 2	`update-alternatives --config javac`
3. При необходимости удалите ранее установленный сертификат контроллера домена	
ALD PRO	`sudo keytool -delete -alias ald-cert -keystore 'поставьте полученное значение JAVA_HOME'\lib\security\cacerts`
FreeIPA	`sudo keytool -delete -alias ipa-cert -keystore 'поставьте полученное значение JAVA_HOME'\lib\security\cacerts`
MS AD	`sudo keytool -delete -alias ms-cert -keystore 'поставьте полученное значение JAVA_HOME'\lib\security\cacerts`
Samba DC	`sudo keytool -delete -alias smb-cert -keystore 'поставьте полученное значение JAVA_HOME'\lib\security\cacerts`
4. Импортируйте полученный сертификат контроллера домена в хранилище keystore java	
ALD PRO	`sudo keytool -import -alias ald-cert -keystore 'поставьте полученное значение JAVA_HOME'/lib/security/cacerts -file ~/aldpro.der`
FreeIPA	`sudo keytool -import -alias ipa-cert -keystore 'поставьте полученное значение JAVA_HOME'/lib/security/cacerts -file ~/freeipa.der`
MS AD	`sudo keytool -import -alias ms-cert -keystore 'поставьте полученное значение JAVA_HOME'/lib/security/cacerts -file ~/msad.der`
Samba DC	`sudo keytool -import -alias smb-cert -keystore 'поставьте полученное значение JAVA_HOME'/lib/security/cacerts -storepass changeit -file ~/smbdc.der`
где:	
`JAVA_HOME` - переменная среды, указывающая на каталог с установленным JAVA (например, `JAVA_HOME="/usr/lib/jvm/java-11-openjdk-amd64/"`);	
`alias ald-cert, ipa-cert, ms-cert, smb-cert` - псевдоним сертификата в хранилище ключей (присвоить имя в зависимости от ресурсной системы);	
`keystore cacerts` - имя файла хранилища для хранения сгенерированной пары ключей;	
`file ~/ca.der` – путь к импортируемому сертификату.	
5. Перезапустите службу AeCA CA	
---	`sudo systemctl restart aecaca`

4.7.2 **Создание 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;

- чек-бокс «Использовать TLS для подключения» – выберите тип соединения. По умолчанию чек-бокс для соединения по протоколу tls всегда включен. При использовании tls-соединения выполните пред настройку в соответствии с п.п. 4.7.1 настоящего руководства. В случае использования незащищённого соединения снимите отмету чек-бокса;
- отображаемое имя – задайте отображаемое имя ресурса на вкладке «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 и MS AD учетная запись администратора вводится в формате RFC822Name, для ALD PRO и FreeIPA соответственно в формате Distinguished Names;
- пароль – укажите соответствующий параметр учетной записи администратора контроллера домена.

- Пример заполненной формы окон создания ресурсной системы для разных типов источников приведены далее (см. Рисунок 139, Рисунок 140, Рисунок 141, Рисунок 142).
- 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.

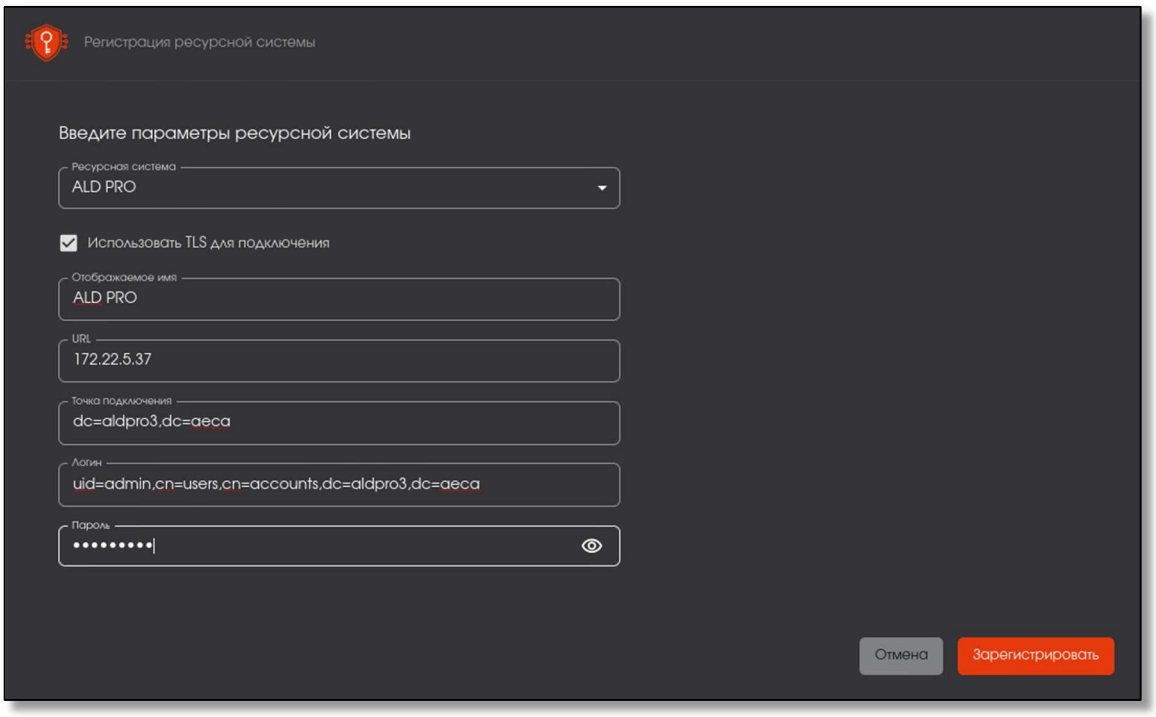


Рисунок 139 – Окно создания ресурсной системы типа ALD PRO

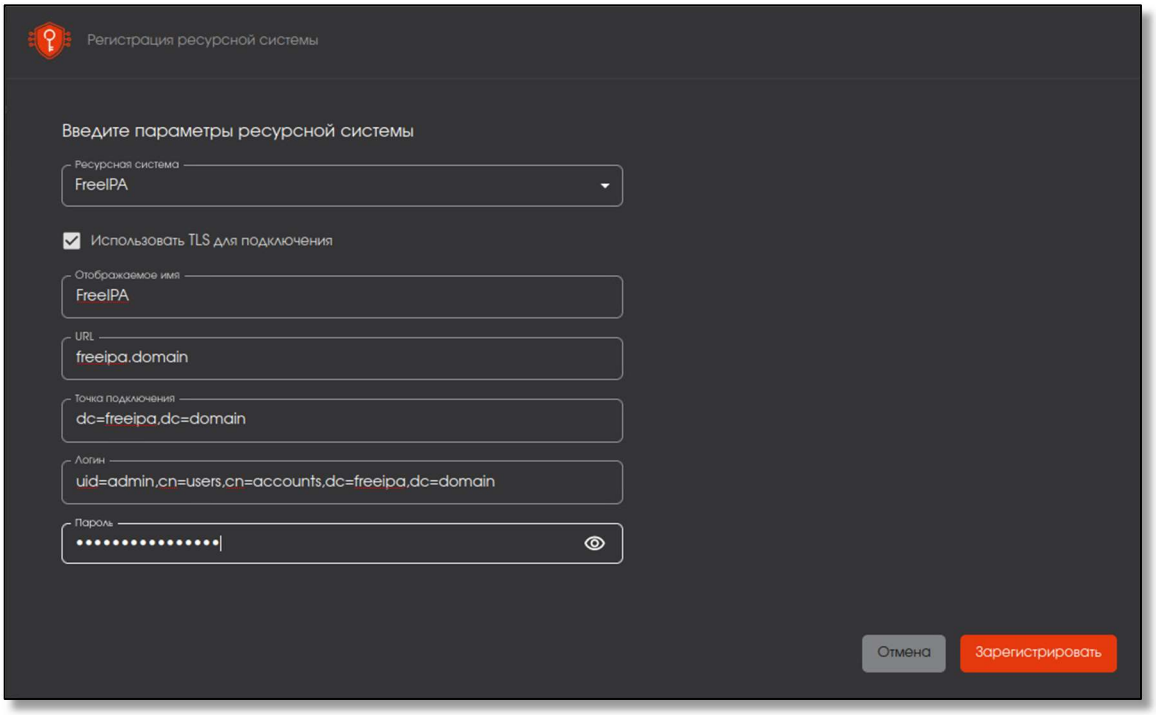


Рисунок 140 – Окно создания ресурсной системы типа FreeIPA

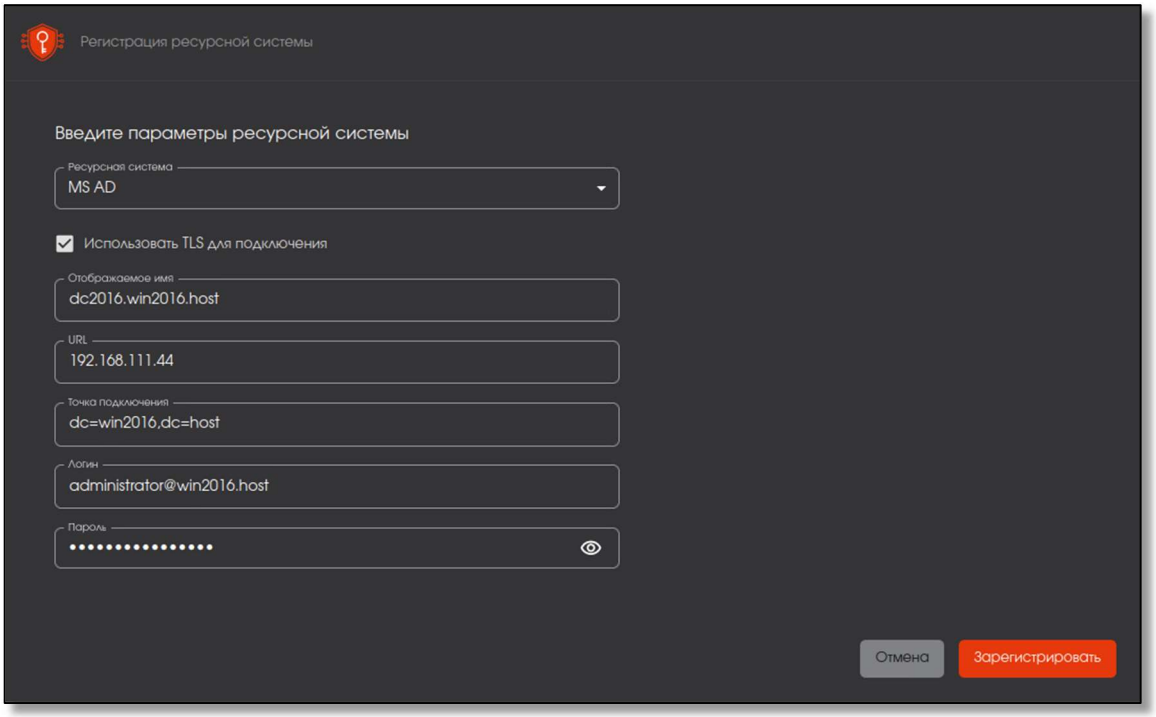


Рисунок 141 – Окно создания ресурсной системы типа MS AD

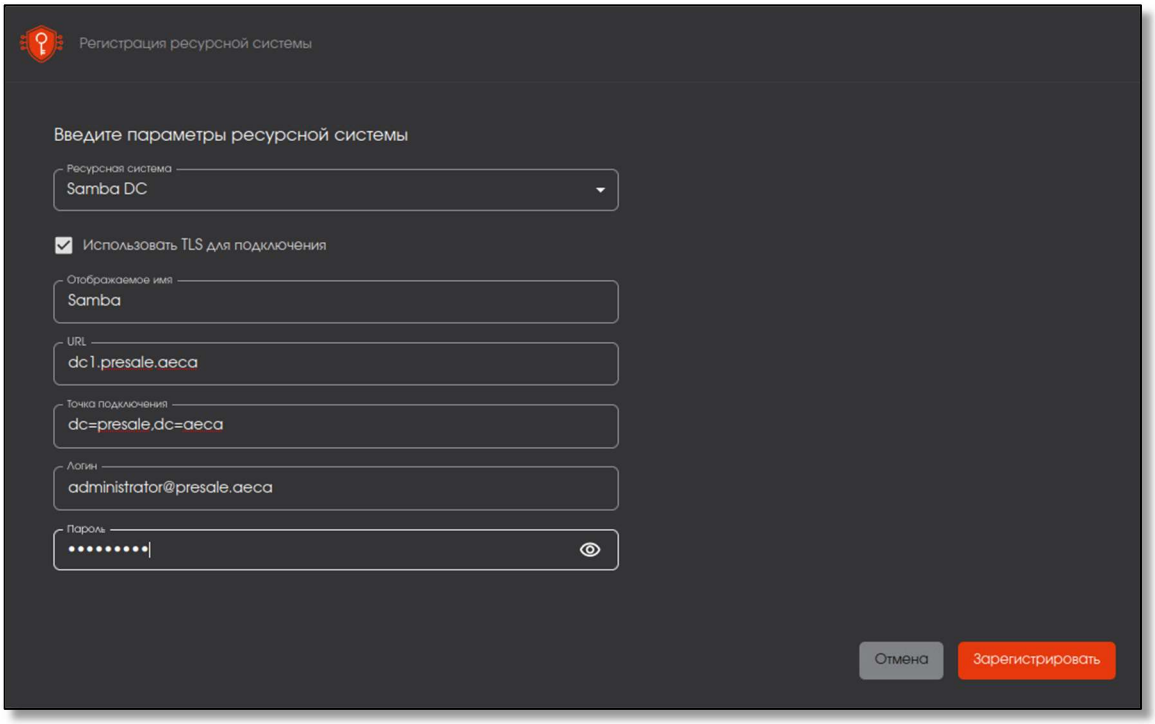


Рисунок 142 – Окно создания ресурсной системы типа Samba DC

- 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. Рисунок 143);
  - сообщение об ошибке при вводе в поле «URL» (см. Рисунок 144);
  - сообщение об ошибке при настройке TLS-соединения (см. Рисунок 145);
  - сообщение об ошибке при совпадении регистрационных данных создаваемой и существующей ресурсных систем (см. Рисунок 146).

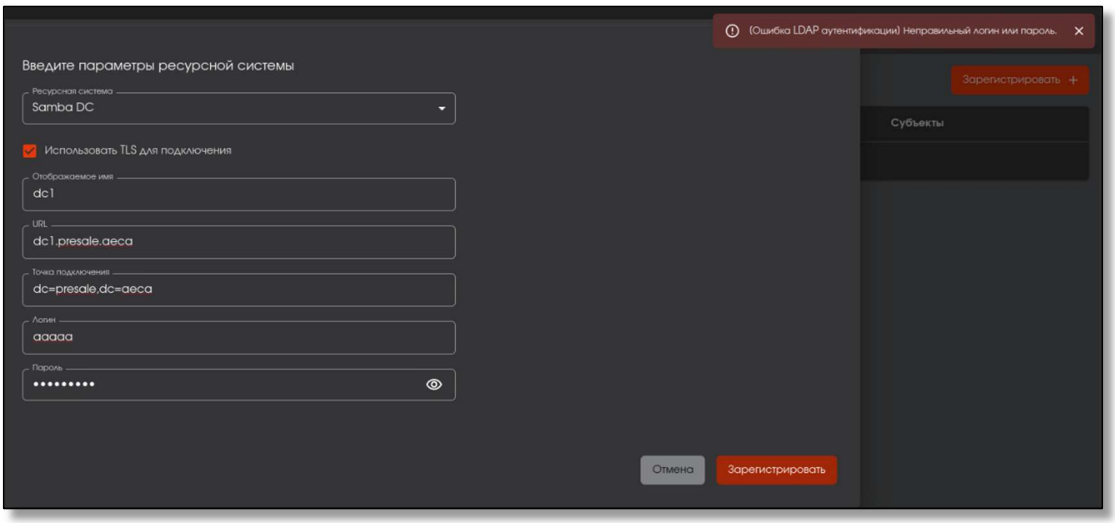


Рисунок 143 – Окно создания ресурсной системы. Уведомление об ошибке при вводе не верного логина или пароля администратора домена

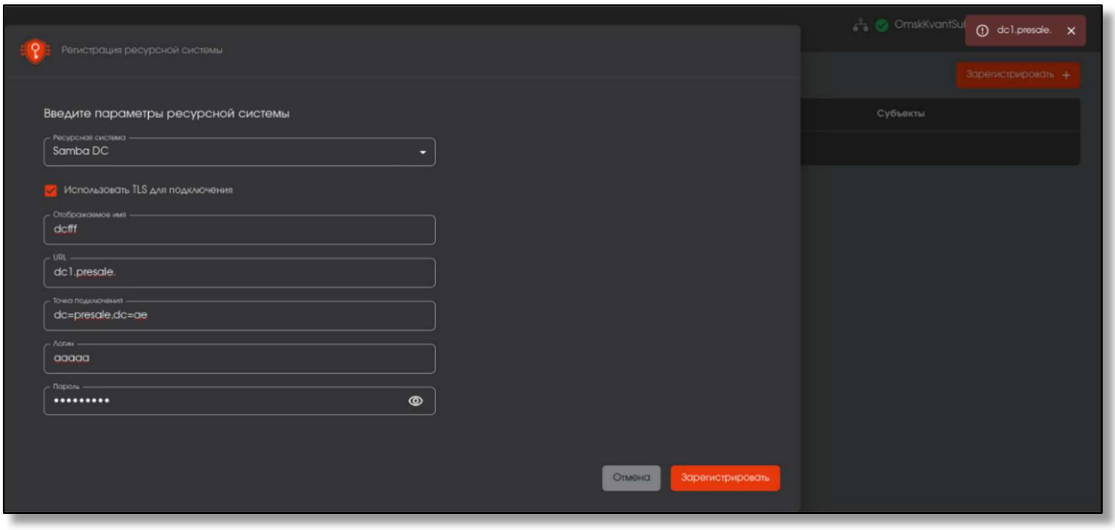


Рисунок 144 – Окно создания ресурсной системы. Уведомление об ошибке в поле «URL»

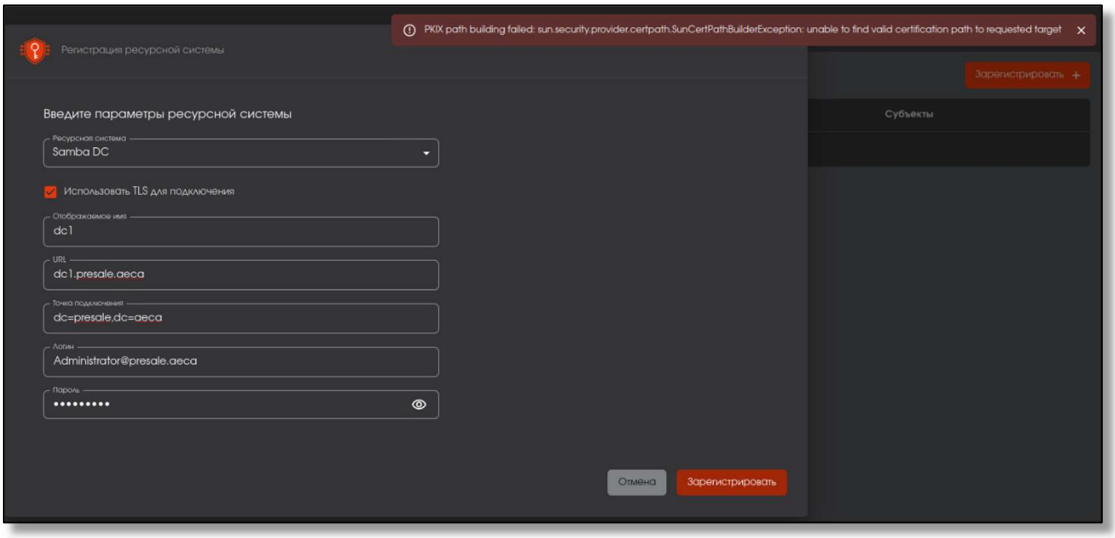


Рисунок 145 – Окно создания ресурсной системы. Уведомление об ошибке настройки TLS-соединения

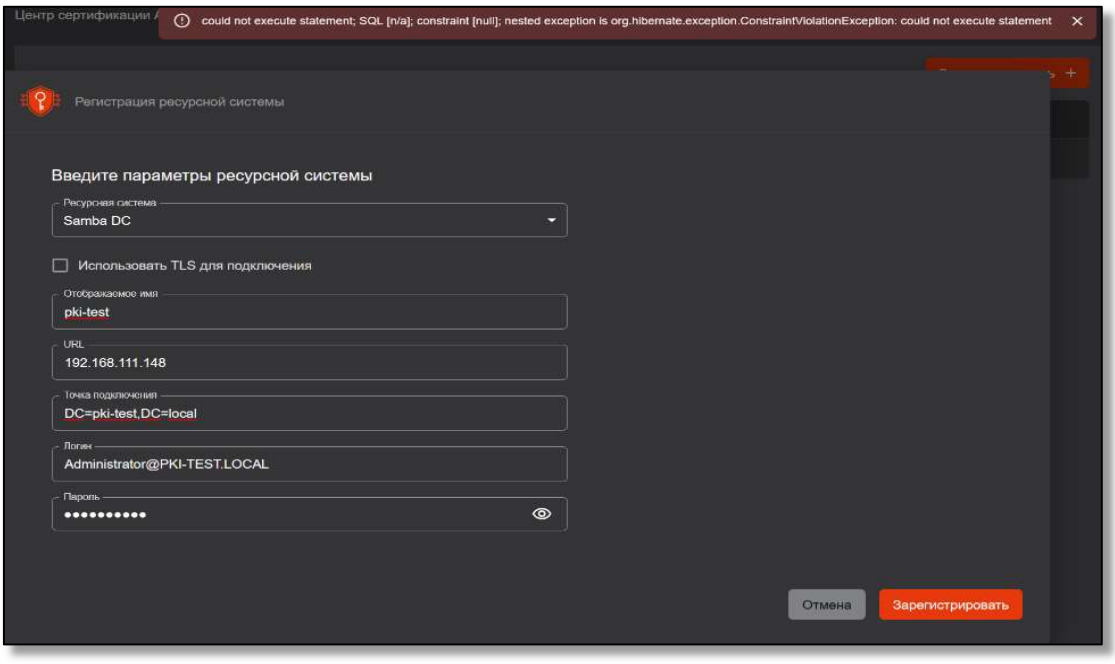


Рисунок 146 – Окно создания ресурсной системы. Уведомление об ошибке при создании ресурсной системы с одинаковыми регистрационными данными

4.7.3 **Обновление ресурсной системы**

- Автоматическая синхронизация списка субъектов из ресурсной системы осуществляется каждые 30 минут.
- Помимо автоматической синхронизации возможно ручное обновление списка субъектов 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 147) - осуществляется загрузка данных для каждого существующего субъекта из ресурсной системы:
    - список пользователей;
    - список ПК в домене;
    - список организационных групп.

Статус ресурса обновлен, информация о субъектах успешно загружена.

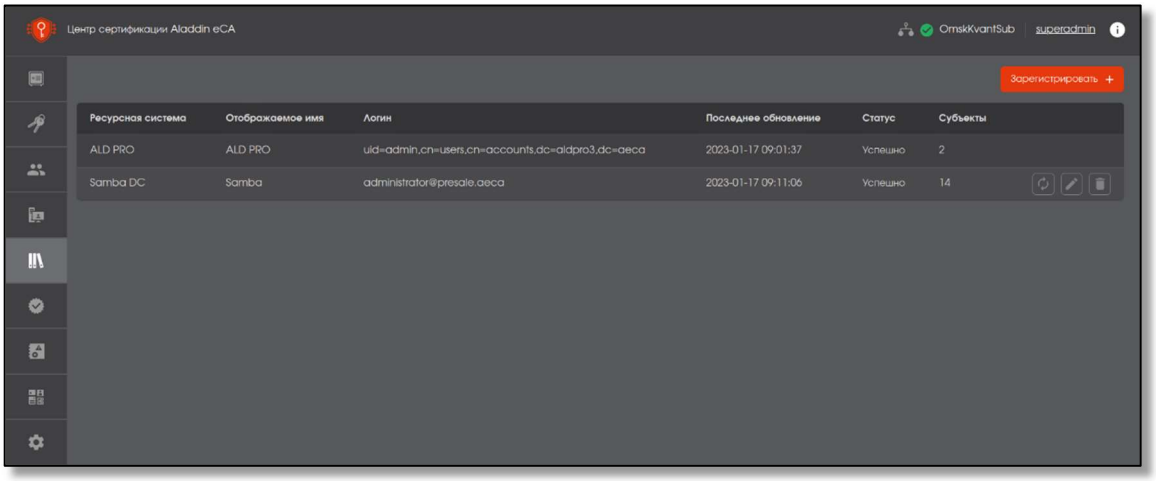


Рисунок 147 – Окно успешного обновления ресурсной системы

4.7.4 **Доступные действия над добавленной ресурсной системой**

После добавления источника ресурсной системы, при наведении курсора на строку добавленного ресурса появляются возможности (см. Рисунок 147):

-  обновления – при нажатии на кнопку <Обновить> выполняется синхронизация с базой данной АЕСА;
-  редактирования – при нажатии на кнопку <Редактировать> открывается окно для редактирования полей, заполненных при создании ресурсной системы. Тип подключаемого ресурса изменить невозможно;
-  удаления – при необходимости возможно удалить добавленный источник ресурсной системы. При нажатии на кнопку <Удалить> на экран будет выведено окно подтверждения выбранного действия (см. Рисунок 148).

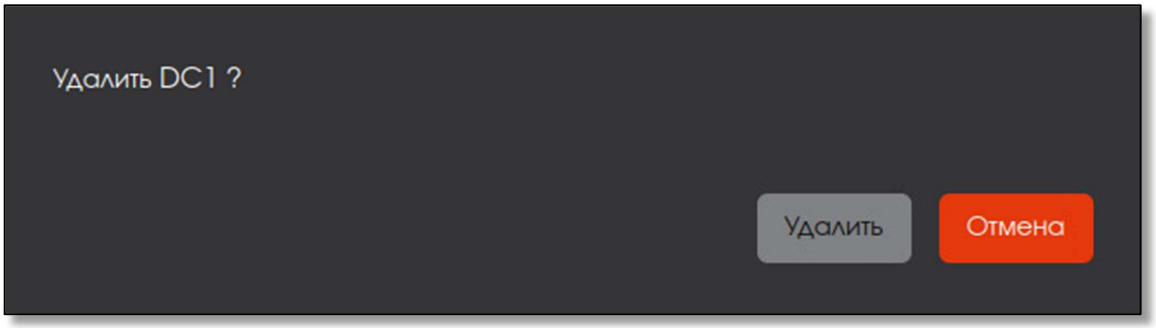


Рисунок 148 – Окно подтверждения удаления ресурсной системы

4.8 Описание вкладки «Центры валидации»

- Переход на вкладку «Центры валидации» (см. Рисунок 149) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).
- Данная вкладка доступна только в режиме администратора.

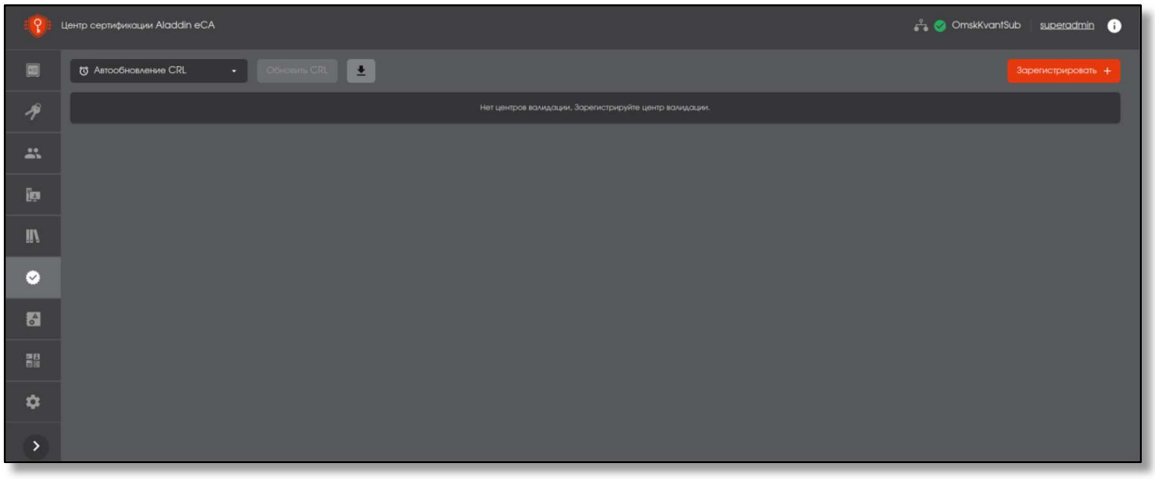


Рисунок 149 – Экран раздела меню «Центр валидации»

- На данной вкладке отображаются все url-адреса зарегистрированных центров валидации.
- Возможно создание нескольких записей для разных Центров валидации, включающих CRL DP и AIA.
- Чтобы не ждать наступление времени публикации, указанного в элементе «Автообновление CRL» можно нажать кнопку <Обновить CRL>, предварительно зарегистрировав центр валидации.
- Работа с разделом «Центры валидации» предусматривает выполнение следующих сценариев использования:
  - моментальная публикация списков 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.
- Службы CRL DP и AIA создаются удаленно через панель управления «Центра сертификации».

- Схема взаимодействия ПО «Центр сертификации» и ПО «Центр валидации» при инициализации служб CRL DP, AIA и OCSP представлена на Рисунок 150.

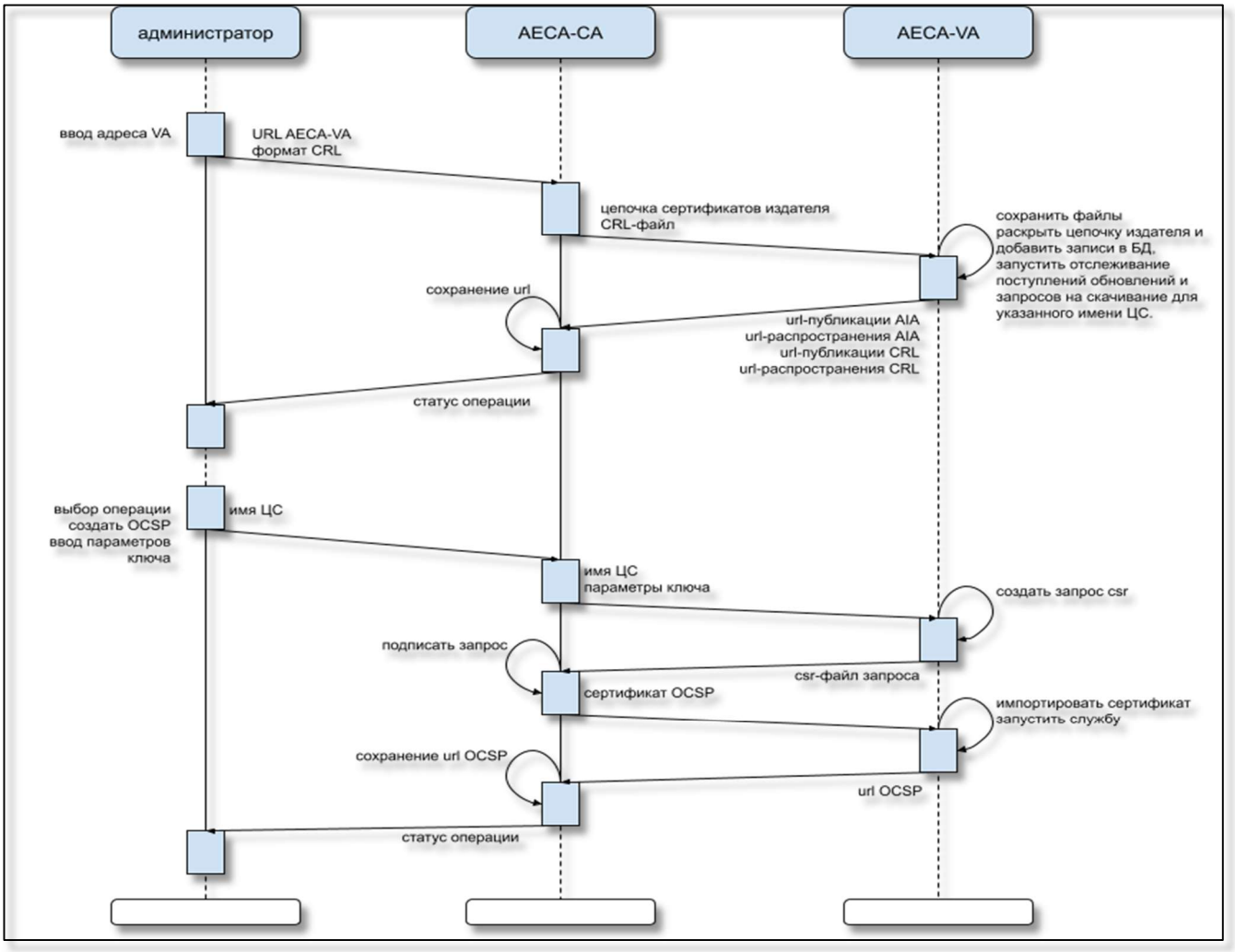


Рисунок 150 – Схема взаимодействия ПО «Центр сертификации» и ПО «Центр валидации»

4.8.1 **Настройка периода автообновления**

- Нажатие на поле <Автообновление CRL> на экране «Центр валидации» вызывает всплывающее меню, содержащее: (см. Рисунок 151):
  - поле «период/перекрытие» содержит период обновления публикации CRL/срок действия перекрытия;
  - 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.

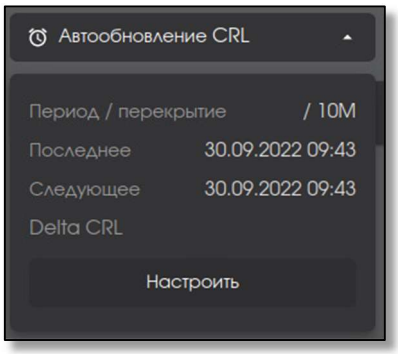


Рисунок 151 - Подменю "Следующая публикация"

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 151) открывается окно с настройками (см. Рисунок 152):
  - периода обновления публикации CRL (`crlperiod`) – задается период обновления CRL в формате час, день, месяц, год – время между публикациями;
  - срока действия перекрытия (`crlOverlapTime`) – задается период действия текущего списка CRL до публикации нового списка CRL, согласно настроенному периоду;
  - возможность поставить флаговую кнопку в поле «Рассылать Delta CRL»;
  - период обновления Delta CRL (`deltacrlperiod`) – время между публикациями Delta CRL.

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

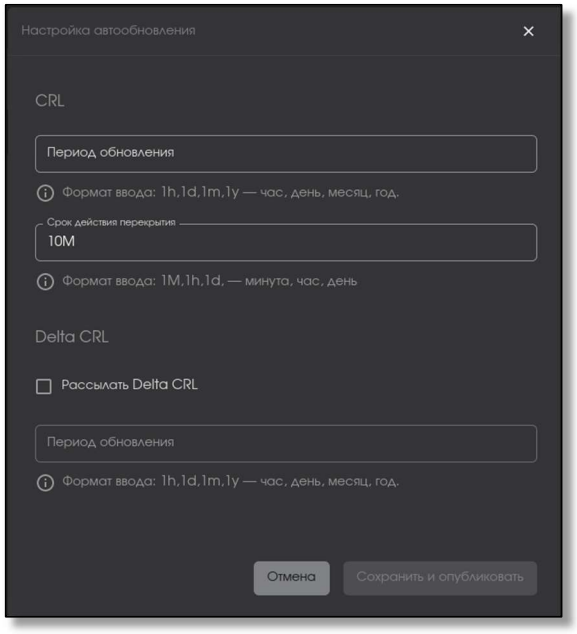


Рисунок 152 – Окно настройки автообновления CRL

- Значения `crlperiod` и `deltacrlperiod` следует выбирать исходя из интенсивности обновления списка сертификатов в конкретных условиях эксплуатации.
- После выбора этих значений значение `crlOverlapTime` стоит выбирать исходя из следующих рекомендации:

- `crlOverlapTime` должно составлять 1/10 от `crlperiod`, но не более 12 часов, и выполняются две нижеприведенные рекомендации;
- `crlOverlapTime` не должно быть больше `deltacrlperiod`, если выполняется следующее нижеприведенное условие ;
- `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 бóльшим номером (версии и индикатора) сразу после его поступления и проверки подписи издателя.

4.8.2 **Моментальная публикация списков CRL**

Для того, чтобы не ждать наступление времени публикации, указанного в элементе «Следующее», можно нажать кнопку <Обновить CRL> (см. Рисунок 153). При нажатии на кнопку <Обновить CRL> публикуется внеплановый список отзыва, при этом таймер публикации списка отзыва сбрасывается и начинает новый отсчет времени публикации.

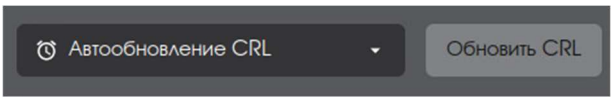


Рисунок 153 – Кнопка «Обновить CRL»

4.8.3 **Выгрузка актуальных списков CRL**

- Для выгрузки списка CRL в Центре сертификации необходимо нажать кнопку <Скачать CRL>  на верхней панели вкладки «Центры сертификации». 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 154);

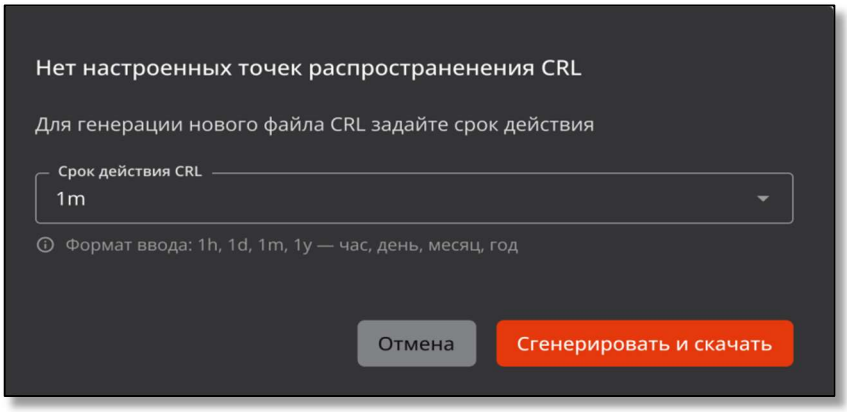


Рисунок 154 – Окно скачивания списка CRL, если нет зарегистрированных Центров валидации

  - 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 155). Возможно задать срок действия CRL;

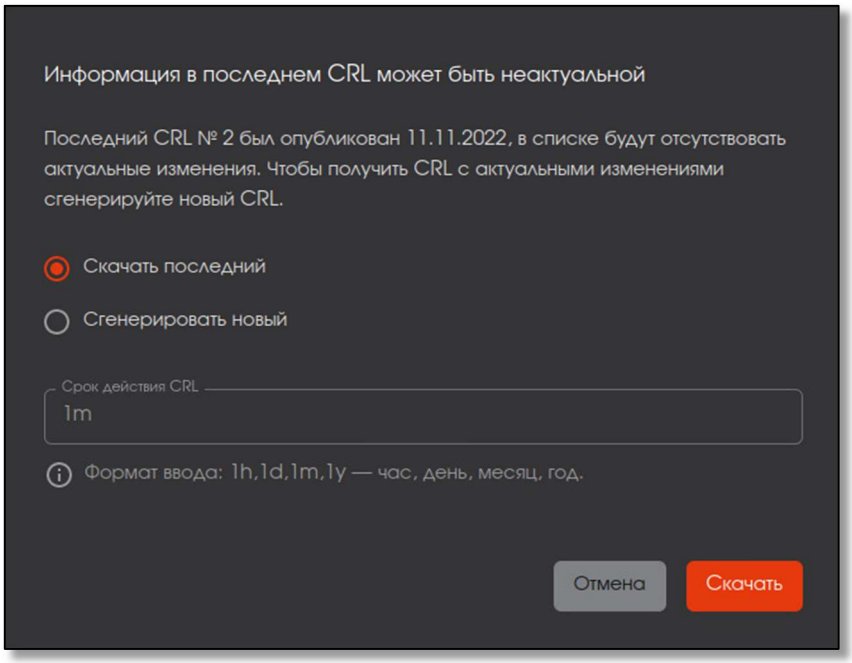


Рисунок 155 – Окно скачивания списка CRL, если ранее список был опубликован, но Центр валидации не зарегистрирован

  - скачайте последний список CRL, если есть активные зарегистрированные Центры валидации (см. Рисунок 156);

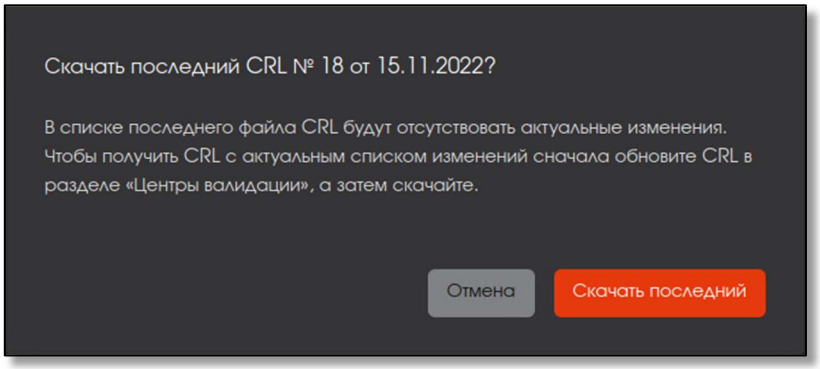


Рисунок 156 – Окно скачивания списка CRL, если есть активный Центр валидации

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

4.8.4 **Создание 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 суперадмина «Центра валидации» `/opt/aeca/p12/superadmin.p12`;
  - скопировать пароль из файла `generated_passwords.txt`, данные строки `superadmin_password`, полученный после установки ПО АеСА VA;
  - перенести подготовленные данные на сервер «Центра сертификации»;
  - настроить автообновление CRL согласно п.4.8.1 настоящего руководства;
  - опубликовать CRL согласно пункту 4.8.2 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 157) 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>.

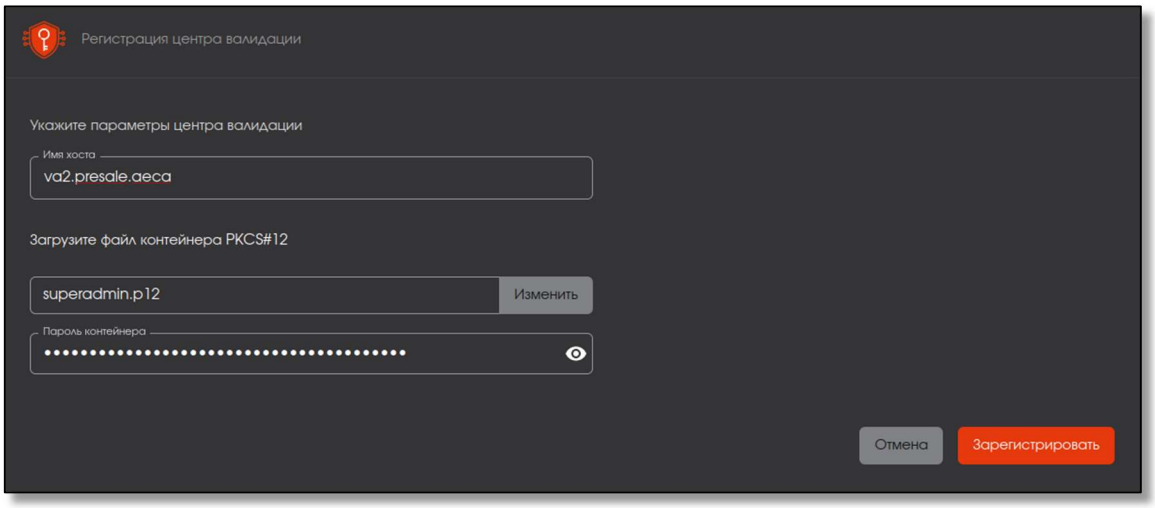


Рисунок 157 – Окно регистрации центра валидации

- В случае успешной регистрации Центра валидации, администратор будет уведомлён сообщением в окне регистрации центра валидации (см. Рисунок 158).

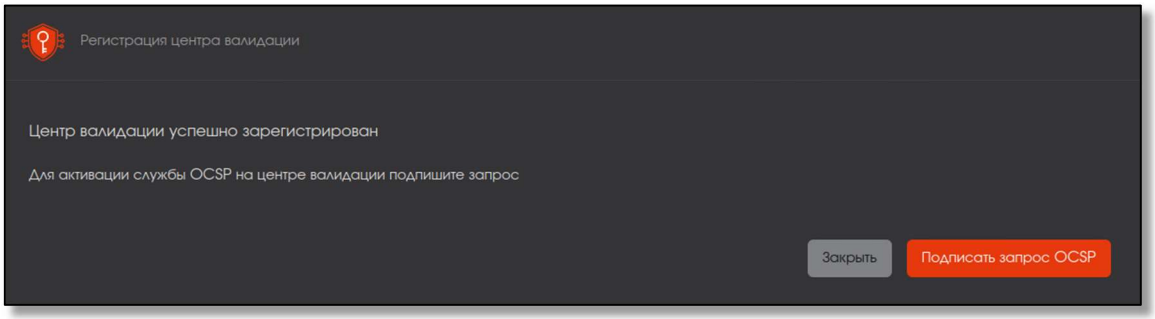


Рисунок 158 – Окно регистрации центра валидации. Сообщение об успешном создании Центра валидации

- 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 159).

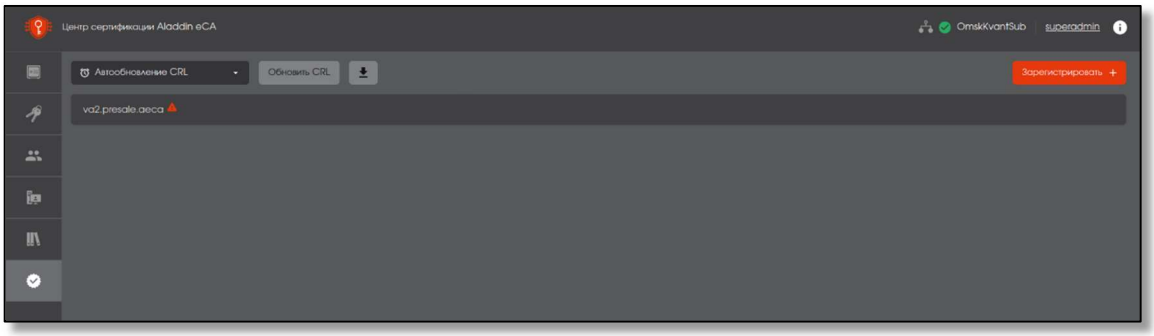


Рисунок 159 – Созданный центр валидации в статусе «Ожидает подпись запроса OCSP»

- После активации служб AIA и CRL DP на сервере «Центра валидации» появляется запись на вкладке «Издатель» (см. Рисунок 160).

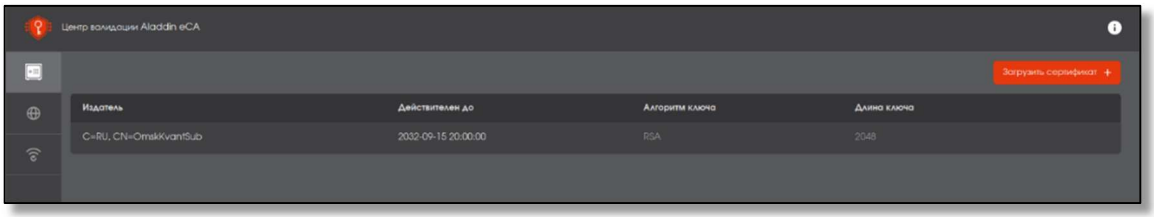


Рисунок 160 – Сервис «Центр валидации» после активации служб AIA и CRL DP

4.8.5 **Подписание запроса OCSP-сервера**

Перед активацией службы OCSP необходимо настроить автообновление CRL!

- Для активация службы OCSP подпишите запрос OCSP, продолжив работу в Мастере регистрации центра валидации после нажатия кнопки <Подписать запрос OCSP> (см. Рисунок 158), или, открыв карточку созданного сервиса OCSP в состоянии «Ожидает подпись запроса», и нажав кнопку <Подписать запрос +> в поле карточки «OCSP» (см. Рисунок 164).
- В открывшемся окне обработки запросов OCSP (см. Рисунок 161) укажите:
  - период обновления – задание периода опроса службы распространения CRL. Формат ввода: 1h,1d,1m,1y - час, день, месяц, год;
  - выберите дополнительные расширения OCSP (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 OCSP) в ответ и включать ли его цепочку.

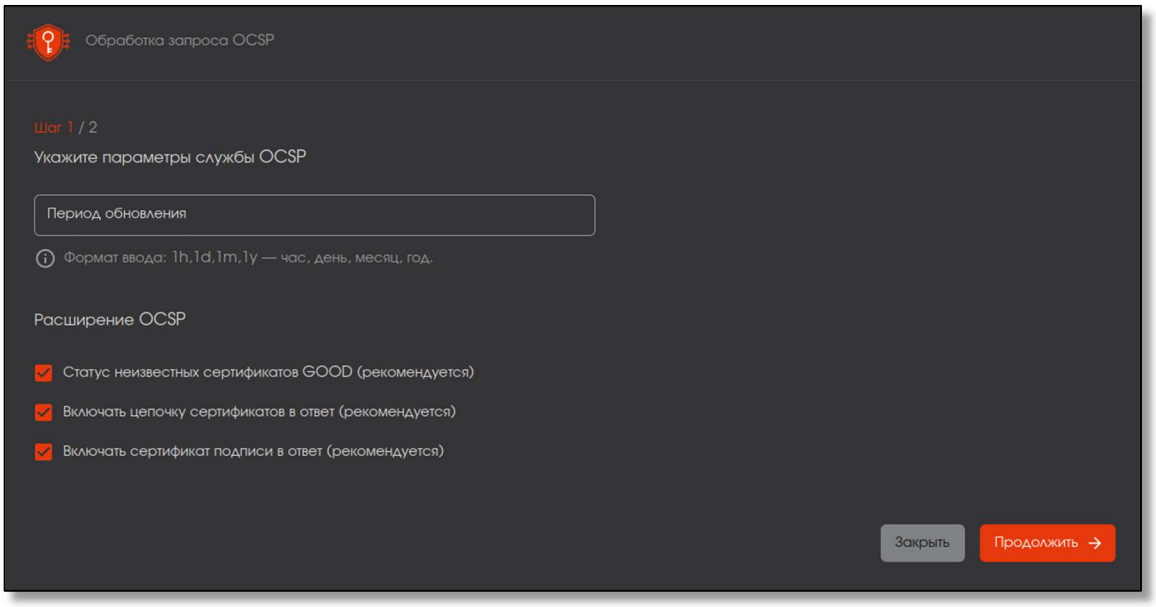


Рисунок 161 – Окно обработки запроса OCSP. Шаг 1

- Нажать, ставшую активной кнопку, <Продолжить>.
- На втором шаге в окне обработки запроса OCSP (см. Рисунок 162) укажите параметры криптографии:
  - алгоритм ключа;
  - длину ключа.
- Для активации и запуска Центра валидации нажмите кнопку <Подписать и запустить>, для отмены прогресса нажмите кнопку <Закрыть>.

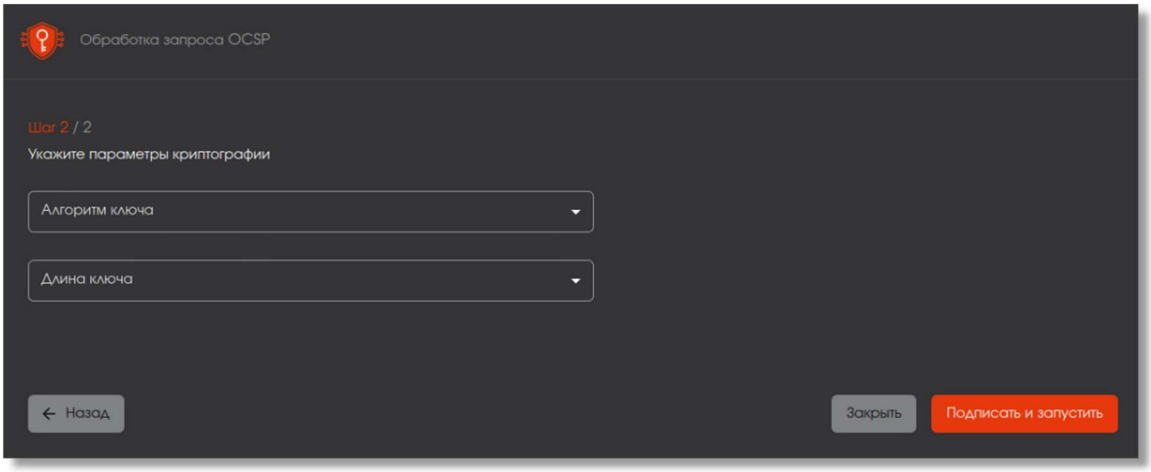


Рисунок 162 – Окно обработки запроса OCSP. Шаг 2

- После успешной активации администратор будет уведомлен информационным сообщением (см. Рисунок 163).

Рисунок 163 – Окно обработки запроса OCSP

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

4.8.6 **Карточка центра валидации (доступ к функциям управления)**

- Для просмотра карточки зарегистрированного центра валидации (см. Рисунок 164) необходимо щёлкнуть левой кнопкой мыши на нужном сервисе на главном экране вкладки «Центр валидации».

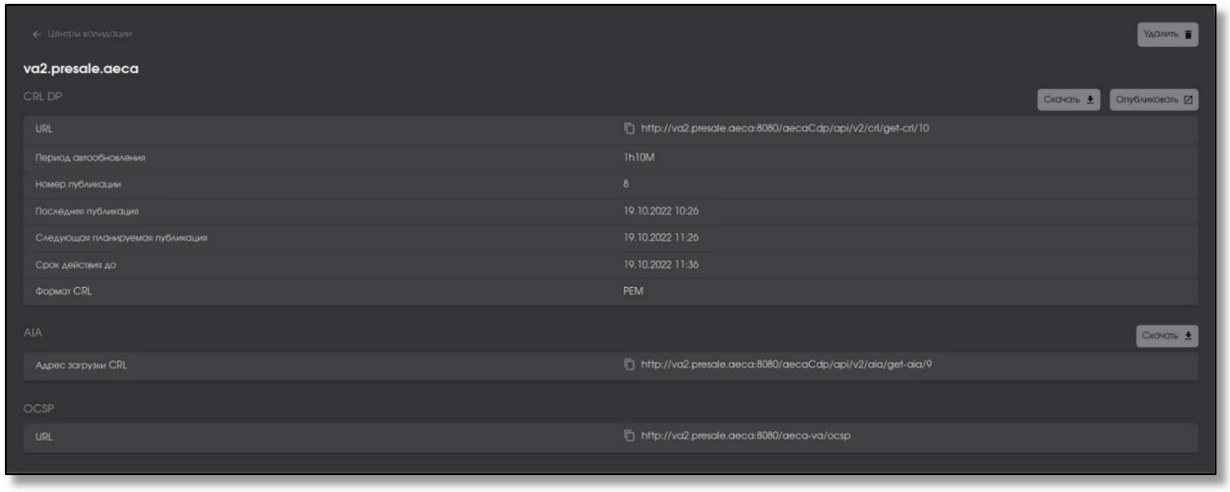


Рисунок 164 – Карточка зарегистрированного Центра валидации

- При регистрации Центра валидации происходит создании 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>;
    - досрочная генерация и публикация 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 следующего обновления CRL;
    - просмотр номера публикации;
    - просмотр даты и времени последней публикации;
    - просмотр даты и времени следующей публикации;
    - просмотр формата публикуемого файла 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 CRL DP 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.

4.8.7 **Состояния центра валидации и действия над ним**

4.8.7.1 Состояние «Ожидает подпись запроса OCSP»

После регистрации Центр валидации переходит в состояние «Ожидает подпись запроса OCSP» (см. Рисунок 165), то есть служба OCSP не инициализирована и выводится соответствующая отметка с предупреждением.

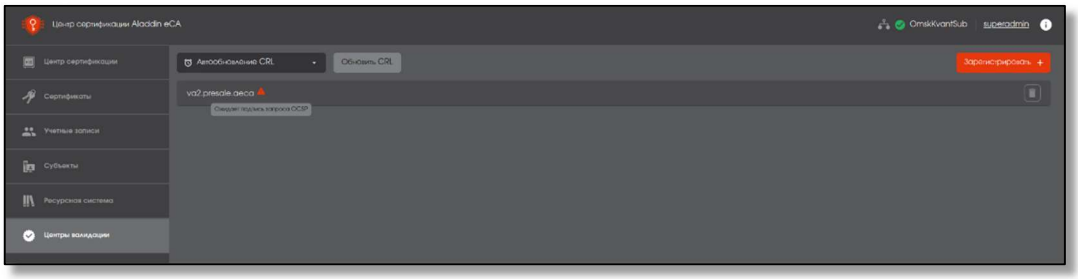


Рисунок 165 – Центр валидации в статусе «Ожидает подпись запроса OCSP»

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 166), где возможно отменить выбранное действие, нажав кнопку <Отмена>, или подтвердить удаление выбранного центра валидации, нажав кнопку <Удалить>.

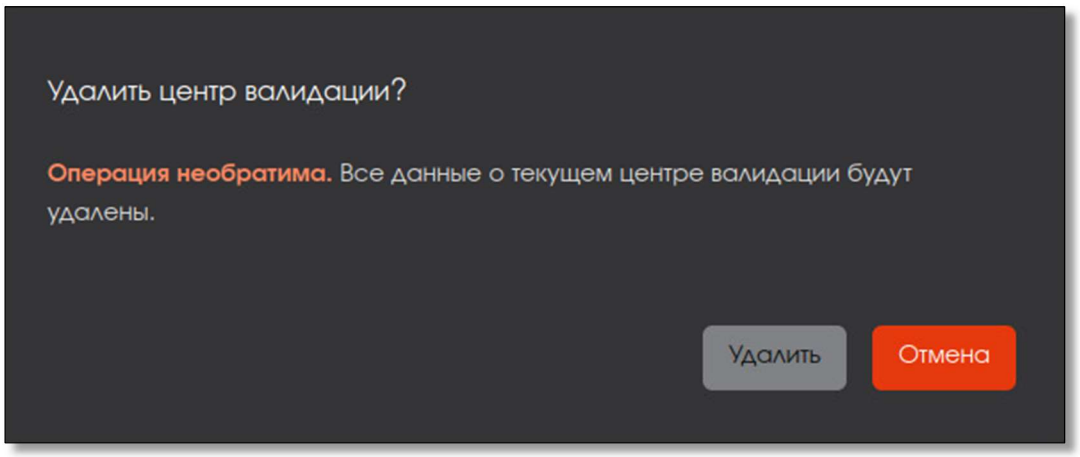


Рисунок 166 – Окно подтверждения удаления центра валидации

4.8.7.2 Состояние «Запущен»

После подписания запроса OCSP-сервера на сертификат Центр валидации переходит в состояние «Запущен» (см. Рисунок 167).

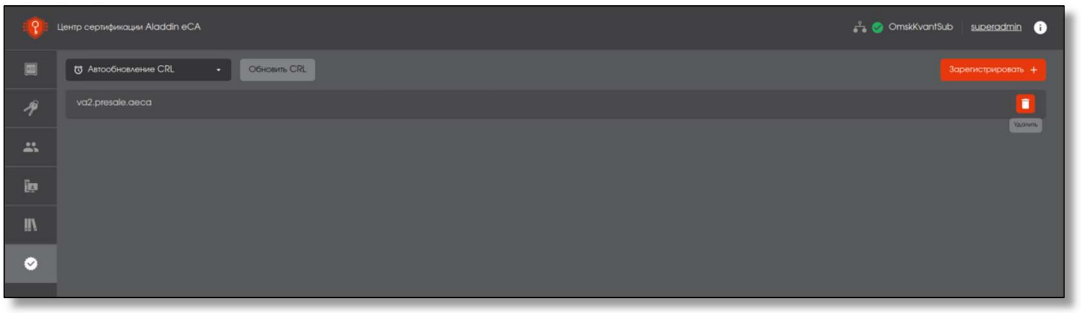


Рисунок 167 – Центр валидации в состоянии «Запущен»

4.9 Описание вкладки «Журнал событий»

- Переход на вкладку «Журнал событий» (см. Рисунок 168) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).
- Программа Aladdin eCA оснащена функцией сбора диагностической информации, которая получает необходимые системные журналы, конфигурационные файлы и аккумулирует их в одном месте для последующего анализа.
- Данная вкладка доступна только в режиме администратора.

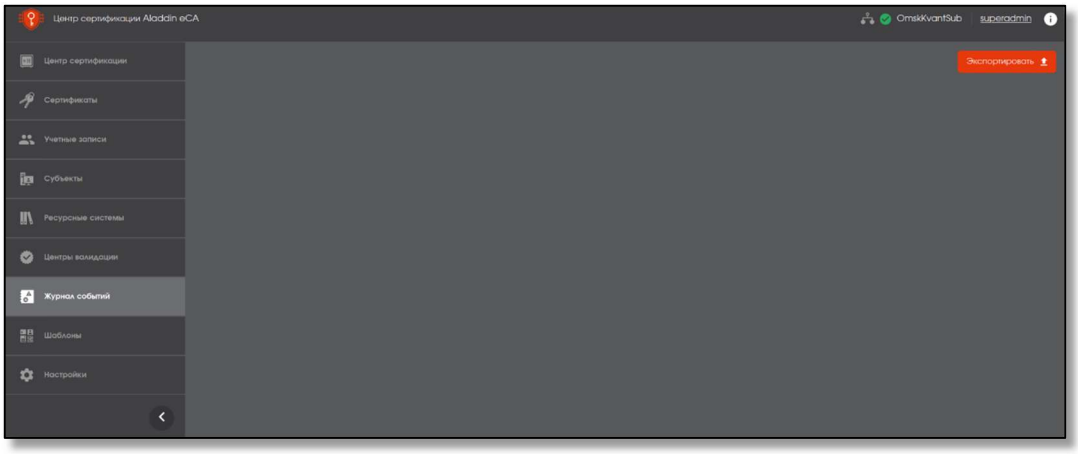


Рисунок 168 – Экран раздела меню «Журнал событий»

- На данной вкладке возможно скачать журнал событий в формате .csv файла.
- Журнал событий предназначен для просмотра истории событий сервера.
- В процессе работы ПО Aladdin eCA системные службы и компоненты приложения записывают все производимые действия.

4.9.1 **Выгрузка журнала событий**

- Для выгрузки журнала событий нажмите кнопку <Экспортировать>, расположенную на вкладке «Журнал событий».
- В открывшемся окне (см. Рисунок 169) задайте параметры экспорта, формирующие скачиваемый файл журнала событий в формате .csv:
  - выберите действия какой учётной записи будут выгружены:
    - все учётные записи;
    - системные учётные записи;
    - учётная запись superadmin;
  - выберите категорию выгружаемых сообщений:
    - информация;
    - ошибка;
    - предупреждение;
    - отладка;
  - выберите необходимый период, за который необходимо вывести сообщения.

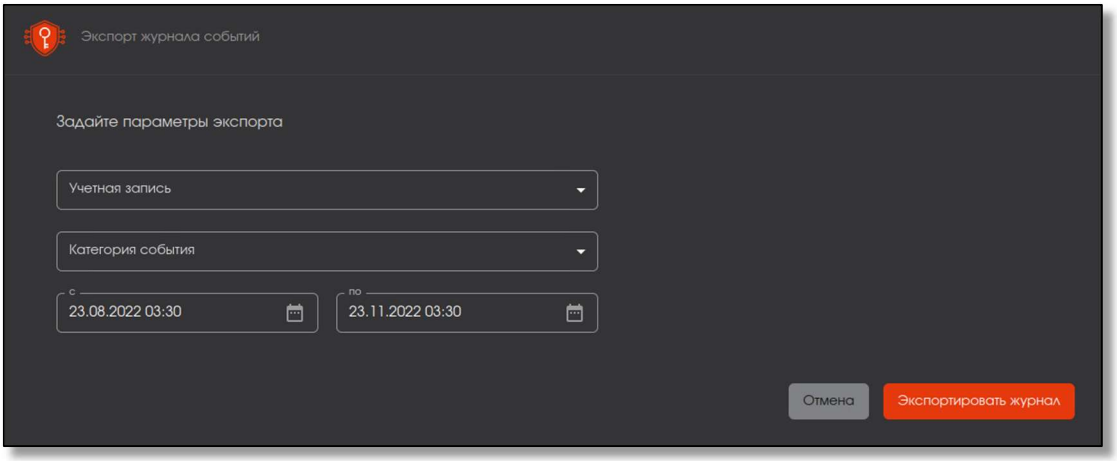


Рисунок 169 – Окно экспорта журнала событий

- Нажмите кнопку <Экспортировать журнал>.

4.9.2 **Состав журнала событий**

- Журнал событий отображает ранее определенный параметрами экспорта набор событий.
- События можно сортировать, выделив строку заголовков и включив соответствующую функцию в MS Exel по следующим полям:
  - дата и время события;
  - учетная запись;
  - роль пользователя;
  - категория сообщения;
  - код сообщения;
  - описание.
- Возможные сообщения журнала событий приведены в Таблица 11.

Таблица 11 – 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	проверка лицензии:<CN-корневого>:<CN-CA>:<срок действия>:<флаг OCSP>:<кол-во активных>
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	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	импорт сертификата центра сертификации:<CN>:<CN-корневого>
ошибка импорта сертификата центра сертификации	CAENV013	ERROR	ошибка импорта сертификата центра сертификации:<CN>:<CN-корневого>:<текст ошибки>

событие, вызвавшее запись в журнал	категория события	код события	описание события
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>
изменение ресурсной системы	CAENV026	INFO	изменение ресурсной системы:<наименование>:<тип>:<адрес>:<точка>:<служебный логин>

событие, вызвавшее запись в журнал	категория события	код события	описание события
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>
ошибка подключения	CAENV043	ERROR	подключение к ключевому носителю:<маркировка носителя>:<тп носителя>:<описание ошибки>

событие, вызвавшее запись в журнал	категория события	код события	описание события
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>
реактивация сертификата	CAENV058	INFO	Активация сертификата:после обновления:certSerialNumber:<ID-сертификата>:revocationReason:<Причина отзыва>

4.10 Описание вкладки «Шаблоны»

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

- Переход на вкладку «Шаблоны» (см. Рисунок 170) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).
- Данная вкладка доступна только в режиме администратора.

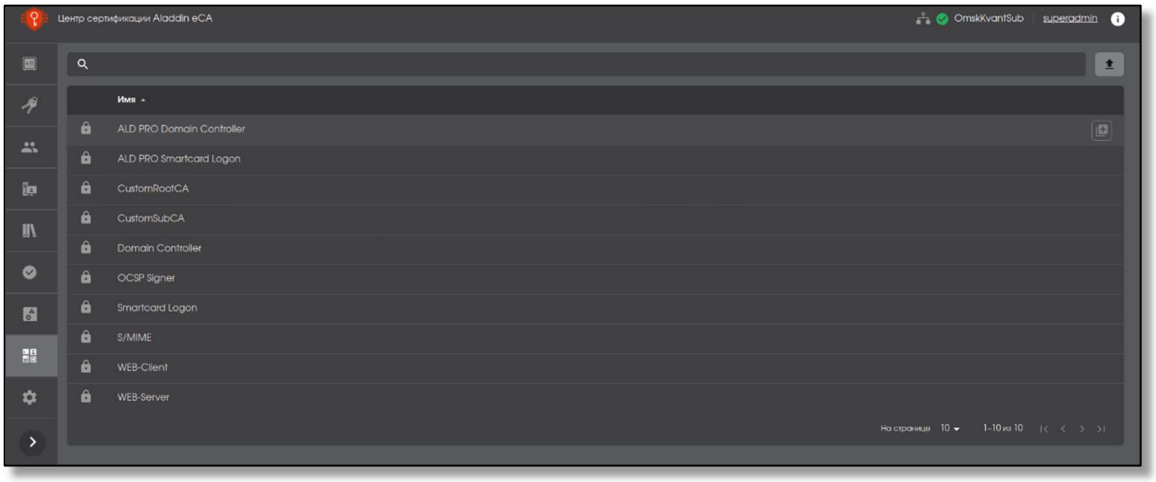


Рисунок 170 – Экран раздела меню «Шаблоны»

- Первоначально на основном экране «Шаблоны» в виде списка отображены шаблоны, предустановленные в системе, и выделены в списке шаблонов символом  . Предустановленные шаблоны нельзя редактировать или удалить.
- 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;
  - ALD PRO Domain Controller;
  - ALD PRO Smartcard Logon;
  - OCSP Signer.
- На данной вкладке возможно:
  - загрузить новые шаблоны сертификатов MS CS;
  - клонировать предустановленный шаблон.
  - осуществить поиск шаблонов в верхнем поле экранной формы автоматически через несколько секунд после ввода одного или нескольких элементов (символа, буквы и т.д.), содержащихся в имени искомого шаблона. Для возврата к полному списку шаблонов очистите поле поиска.
- Действия доступные над прочими шаблонами (загруженные и созданные, в результате клонирования):
  - редактирование шаблона;

- сохранение результатов редактирования шаблона;
- удаление шаблона.

Добавленные шаблоны доступны для использования на вкладке

- Все шаблоны сертификатов отображаются в виде таблицы с постраничным выводом данных. Ссылочный блок для разграничения содержимого размещен внизу страницы (см. Рисунок 50) 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.

4.10.1 Сортировка шаблонов

- Средство сортировки списка шаблонов представлено элементом выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 170) – полем «Имя».
- Сортировка осуществляется в алфавитном порядке при нажатии на соответствующий заголовок экранной таблицы. Символ фильтрации в поле «Имя» обозначен знаком  с правой стороны от заголовка таблицы.

4.10.2 Карточка шаблона

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

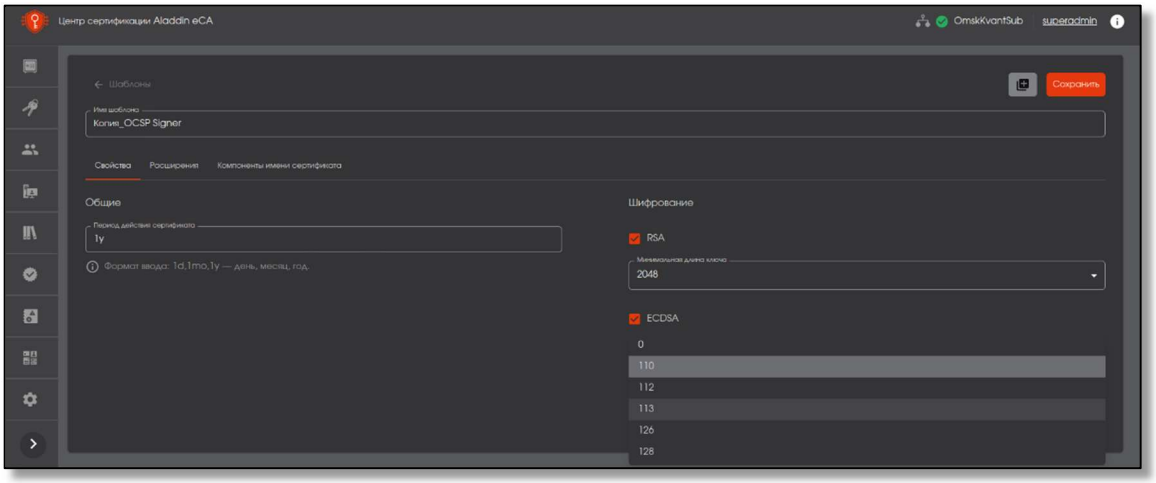


Рисунок 171 – Окно карточки шаблона

- 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».

4.10.2.1 Вкладка шаблона «Свойства»

На вкладке шаблона «Свойства» доступны поля (см. Рисунок 172):

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

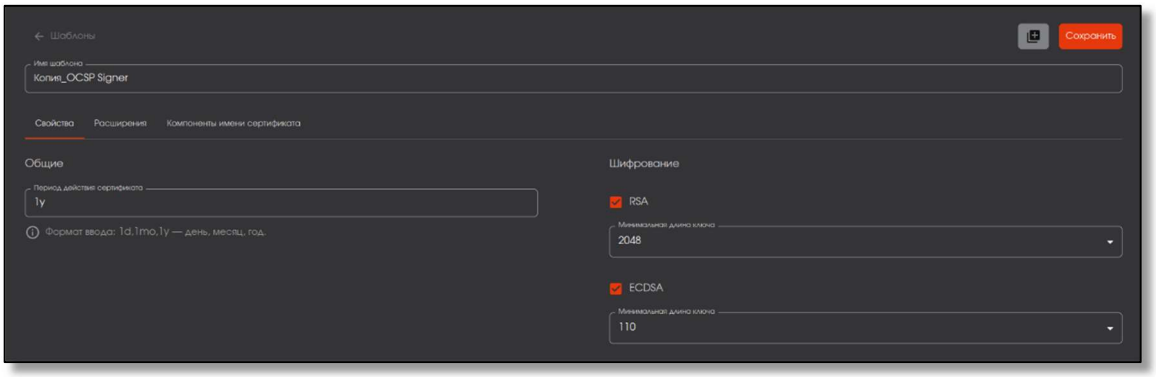


Рисунок 172 – Вкладка «Свойства» шаблона сертификата

4.10.2.2 Вкладка шаблона «Расширения»

На вкладке шаблона «Расширения» доступны:

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

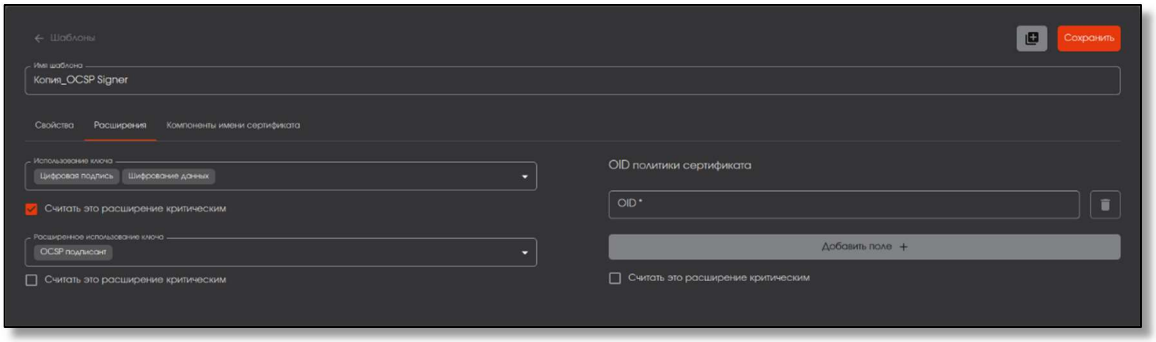


Рисунок 173 – Вкладка «Расширения» шаблона сертификата

4.10.2.3 Вкладка шаблона «Компоненты имени сертификата»

На вкладке шаблона «Расширения» доступны (см. Рисунок 174):

- отличительное имя субъекта;
- альтернативное имя субъекта.

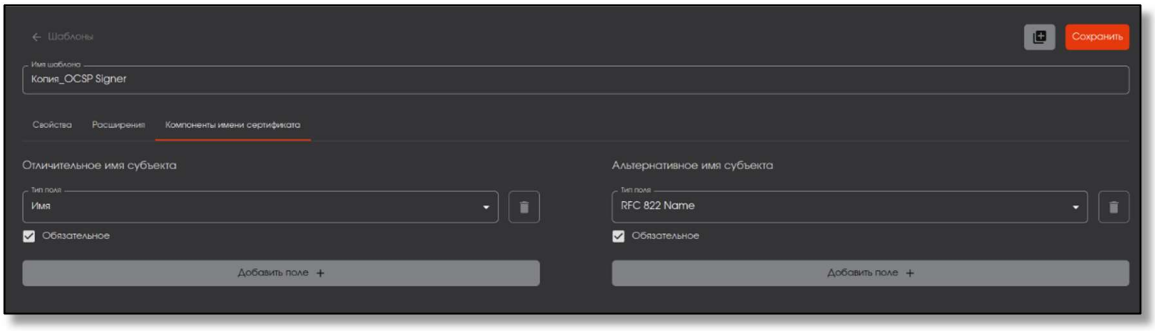


Рисунок 174 – Вкладка «Компоненты имени сертификата» шаблона сертификата

4.10.3 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.

4.10.3.1 Клонирование шаблона

- Выделите предустановленный шаблон на вкладке «Шаблоны» указателем «мышь».
- Нажмите появившуюся в строке кнопку <Клонировать>  .
- В открывшемся окне подтверждения действия (см. Рисунок 175) 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 175 – 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.

4.10.3.2 Редактирование шаблона

- Редактирование применимо для клонированного шаблона или загруженного шаблона MS CS.
- Редактирование предустановленных шаблонов недоступно.
- Для выбранного шаблона доступны для редактирования элементы, указанные в Таблица 12.

Таблица 12 – Поля шаблона, доступные для изменения через графический интерфейс

Название	Тип	Допустимые значения
Вкладка шаблона «Свойства»		
Имя шаблона	Строка	Ограничение: 255 символов
Период действия	Строка	*y *mo *d
Алгоритм ключа	Список с множественным выбором	RSA ECDSA
Минимальная длина ключа	Два списка	RSA: • 1024 • 1536 • 2048 • 3072 • 4096 • 6144 • 8192 ECDSA: • 110 • 112 • 113 • 126 • 128 • 131 • 160 • 161 • 162 • 163 • 189 • 190 • 191 • 192 • 193 • 224 • 225 • 232 • 233 • 236 • 237 • 238

Название	Тип	Допустимые значения
		• 239 • 256 • 257 • 281 • 282 • 289 • 320 • 353 • 384 • 407 • 409 • 418 • 512 • 521 • 570
Вкладка «Расширения сертификата»		
Использование ключа	Список с множественным выбором	• Цифровая подпись • Подтверждение подлинности • Шифрование ключей • Шифрование данных • Согласование ключей • Подпись сертификатов • Подпись списков отзыва • Только шифрование • Только расшифрование
«Критическое»	Флажок	Для поля «Использование ключа» (вкл)
Политики сертификата	Поле ввода со списком	Список OID
«Критическое»	Флажок	Для поля «Политики сертификата»
Расширенное использование ключа	Список с множественным выбором	• Any Extended Key Usage • CSN 369791 TLS client • CSN 369791 TLS server • Client Authentication • Code Signing • EAP over LAN (EAPOL) • EAP over PPP • ETSI TSL Signing • Email Protection • ICAO Deviation List Signing • ICAO Master List Signing • Intel AMT management • Internet Key Exchange for IPsec • Kerberos Client Authentication • Kerberos KDC (Key Distribution Center) • MS Commercial Code Signing • MS Document Signing • MS EFS Recovery • MS Encrypted File System (EFS) • MS Individual Code Signing • MS Smart Card Logon

Название	Тип	Допустимые значения
		• OCSP Signer • PDF Signing • PIV Card Authentication • SCVP Client • SCVP Server • SIP Domain • SSH Client • SSH Server • Server Authentication • Time Stamping
«Критическое»	Флажок	Для поля «Расширенное использование ключа»
Вкладка «Компоненты имени сертификата»		
Альтернативное имя субъекта	Список и флажок, указывающий обязательность каждого элемента списка	• RFC 822 Name (e-mail address) • DNS Name • IP Address • Directory Name (Distinguished Name) • Uniform Resource Identifier (URI) • Registered Identifier (OID) • MS UPN, User Principal Name • MS GUID, Globally Unique Identifier • Kerberos KPN, Kerberos 5 Principal Name • Permanent Identifier • XmppAddr • Service Name
Отличительное имя субъекта	Список и флажок, указывающий обязательность каждого элемента списка	• emailAddress, E-mail address in DN • CN, Common name • serialNumber, Serial number (in DN) • givenName, Given name (first name) • initials, First name abbreviation • surname, Surname (last name) • title, Title • OU, Organizational Unit • O, Organization • L, Locality • ST, State or Province • DC, Domain Component • C, Country (ISO 3166) • unstructuredAddress, IP address • unstructuredName, Domain name (FQDN) • postalCode • businessCategory, Organization type • dnQualifier, DN Qualifier • telephoneNumber • pseudonym • streetAddress • name • description, Description

- 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 (см. Рисунок 176)

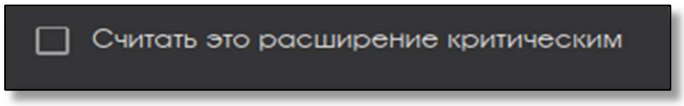


Рисунок 176 – Поле чек-бокса

- Используйте кнопки <Добавить поле> (см. Рисунок 177) на вкладках шаблона «Расширения» и «Компоненты имени сертификата» для формирования специализированного шаблона сертификата.

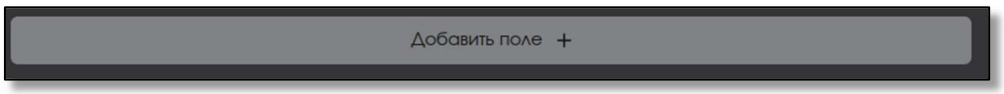


Рисунок 177 – Кнопка <Добавить поле> шаблона специализированного сертификата

4.10.3.3 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 выбора действий (см. Рисунок 178), в котором при нажатии кнопки:
  - <Сохранить> будут сохранены внесённые изменения в текущий шаблон и осуществлён переход на выбранную вкладку;
  - <Не сохранять> внесённые изменения в текущем шаблоне будут утеряны и осуществлён переход на выбранную вкладку;
  - <Отмена> будет осуществлено закрытие окна подтверждения и возврат к редактируемой карточке шаблона.

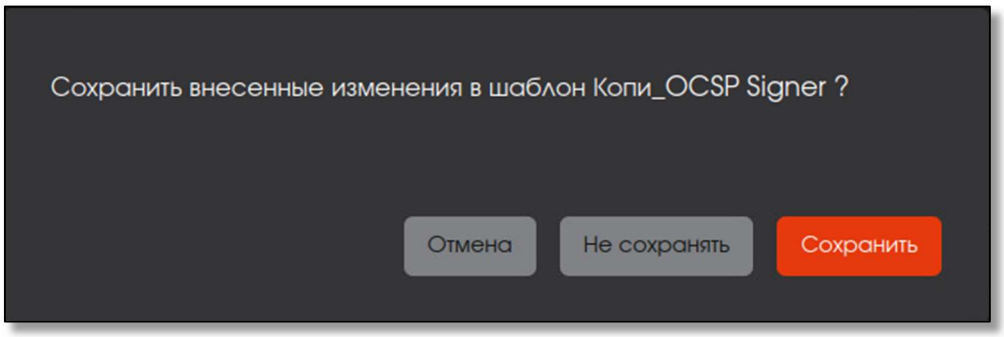


Рисунок 178 – Окно выбора действий в редактируемом шаблоне при переходе на другую вкладку ЦС

4.10.4 Экспорт шаблонов MSCS

- Для экспорта шаблонов запустите скрипт mscs2aeca.ps1 из комплекта поставки на рабочем месте с установленным Центром сертификации MSCS от имени администратора.
- Скрипт запускается как консольное приложение и работает в режиме командной строки, графический интерфейс не предусмотрен.

- Для успешного выполнения скрипта необходимо интернет-соединение. Для успешного выполнения скрипта в оффлайн режиме требуется предварительно скачать и установить пакет NuGet.
- Скрипт запускается как консольное приложение и работает в режиме командной строки, графический интерфейс не предусмотрен.
- 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).

4.10.5 Загрузка шаблона MSCS

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

- нажмите кнопку <Загрузить шаблоны>  . В открывшемся окне выберите .csv файл шаблонов MSCS в локальной папке и нажмите кнопку <Открыть>.
- В результате шаблоны MSCS будут импортированы, и администратор будет уведомлён сообщением на экране «XX шаблонов успешно загружено», где «XX» - количество успешно загруженных шаблонов (см. Рисунок 179).

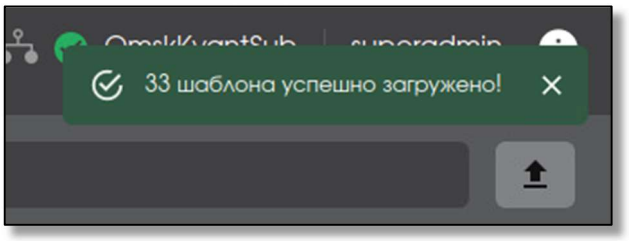


Рисунок 179 – Уведомление об успешной загрузке шаблонов MSCS

- В случае, если шаблоны не были импортированы, администратор будет уведомлен сообщением «Невозможно загрузить шаблоны» (см. Рисунок 179).

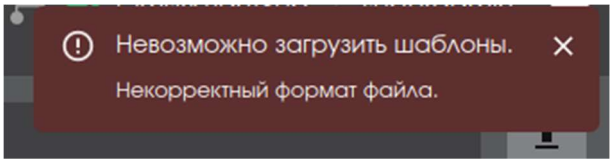


Рисунок 180 – Уведомление о неудачной загрузке шаблонов MSCS

- Поля, загружаемые из файла импорта шаблонов MSCS, приведены в Таблица 13.

Таблица 13 – 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	• Альтернативное имя субъекта

Название поля в файле	Описание	Название поле в АЕСА
	требование обязательности в одной строке	• флажок “Обязательное”
Alghoritm	Алгоритм шифрования	Алгоритм шифрования
AlgMinLen	Минимальная длина ключа	Минимальная длина ключа
ValidPeriod	Период действия	Период действия
KeyUsage, CritExts	Использование ключа	• Использование ключа • флажок “считать это расширение критическим”
EKU, CritExts	Расширенное использование ключа	• Расширенное использование ключа • флажок “считать это расширение критическим”
Polices, CritExts	Политики	• OID политики сертификата • флажок “считать это расширение критическим”

- При 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).

4.10.6 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 181), где возможно отменить выбранное действие, нажав кнопку <Отмена>, или подтвердить удаление выбранного шаблона, нажав кнопку <Удалить>.

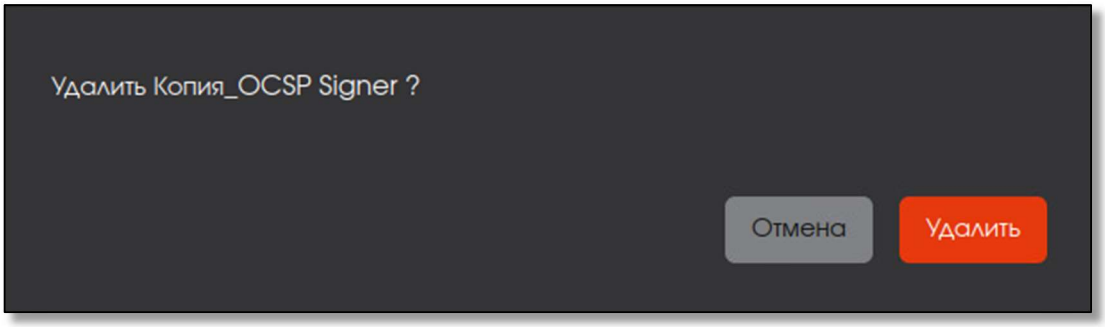


Рисунок 181 – Окно подтверждения удаления шаблона сертификата

- 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.

4.10.7 Работа с шаблонами сертификатов

- Загруженные и созданные шаблоны доступны для использования при выпуске сертификатов на вкладке «Сертификаты» и «Субъекты» (см. подраздел 4.4. и 4.6 настоящего Руководства администратора).

4.11 Описание вкладки «Настройки»

- Переход на вкладку «Настройки» (см. Рисунок 182) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 33).
- Данная вкладка доступна только в режиме администратора.

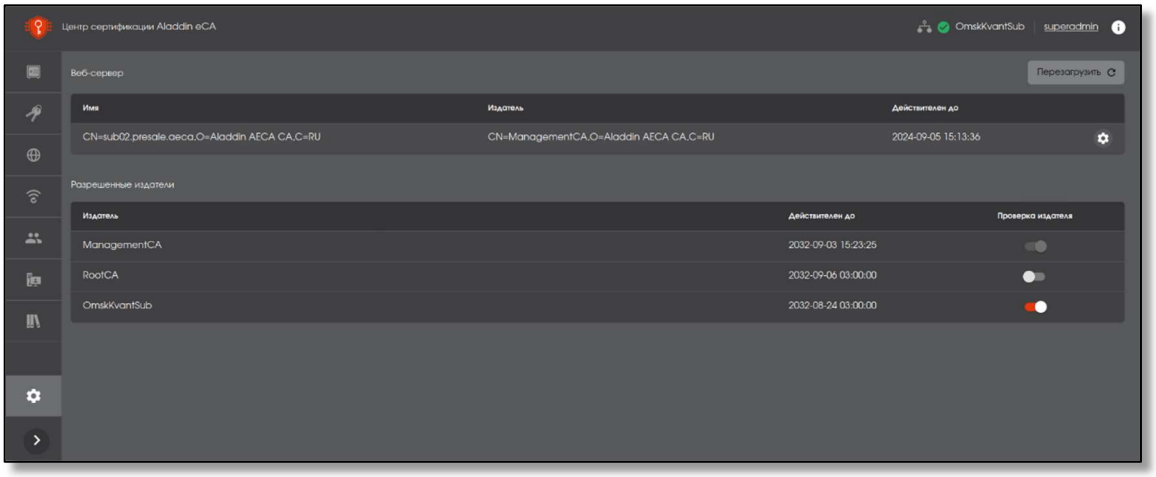


Рисунок 182 – Экран раздела меню «Настройки»

- На основном экране «Настройки» отображены:
  - поле «Веб-сервер», в котором отображен текущий сертификат корневого ЦС, с возможностью сменить ключи веб-сервера;
  - поле «Разрешенные издатели», где указаны все издатели текущего Центра сертификации. По умолчанию в «доверенных издателях» находится самоподписанный сертификат, созданный при развертывании «Центра сертификации» и используемый для внутренних взаимодействий «ManagementCA», этот служебный ЦС не может быть деактивирован.

4.11.1 Установка сертификата веб-сервера

- Для смены ключей выберите нужный веб-сервер и нажмите появившуюся кнопку  .
- В появившемся окне (см. Рисунок 183) выберите файл сертификата и введите пароль файла контейнера, заданный при выпуске сертификата веб-сервера.
- Нажмите кнопку <Сменить ключи>.
- Перезагрузите сервер, нажав кнопку 

на экране вкладки «Настройка».

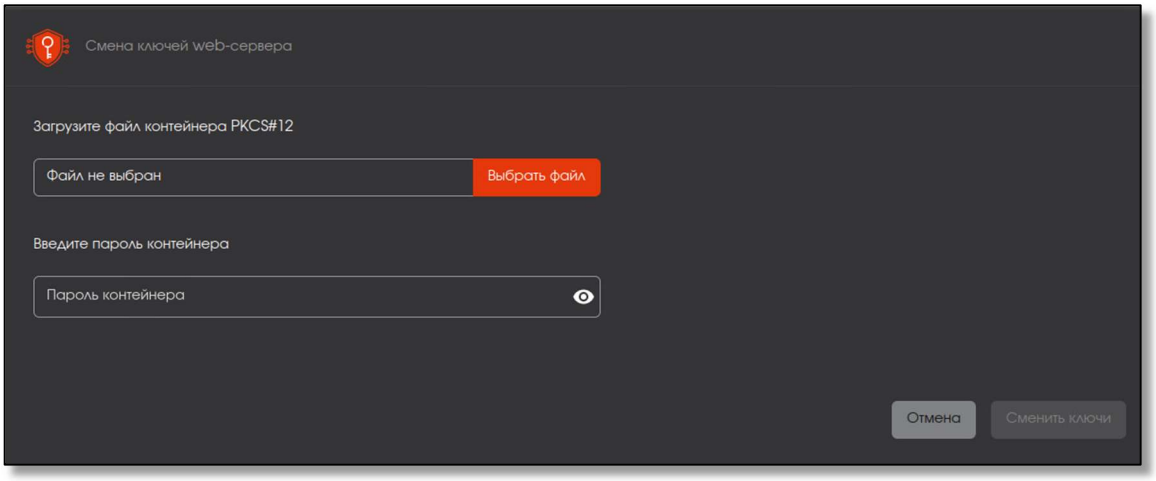


Рисунок 183 – Окно смены ключей веб-сервера

4.12 Настройка уведомлений об истечении срока действия сертификата

- ПО Aladdin eCA поддерживает возможность уведомления пользователей об истечении срока действия сертификатов.
- При использовании настроек по умолчанию AeCA 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 сертификат 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 email.env;
  - создан и настроен хотя бы один шаблон уведомлений.

4.12.1 Настройка параметров конфигурационного файла email.env

- Отредактируйте конфигурационный файл `email.env`, размещенный по адресу `/opt/aecaCa/env/email.env`, выполнив команду:

```
sudo nano /opt/aecaCa/env/email.env
```

- Листинг файла и описание настроек приведены в Таблица 14.

Таблица 14 – Листинг файла `email.env`

Листинг файла	Настраиваемые параметры подключения
`#Настройки сервиса рассылки сообщений`	
`#Хост почтового сервера` `EMAIL_HOST=""`	укажите адрес почтового сервера, например: `mail.example.com`

Листинг файла	Настраиваемые параметры подключения
`#Порт почтового сервера` `EMAIL_PORT="25"`	укажите порт почтового сервера
`#Логин пользователя` `EMAIL_LOGIN=""`	укажите логин пользователя, под которым производится авторизация в почтовом сервере
`#Пароль пользователя` `EMAIL_PASSWORD=""`	введите пароль пользователя, под которым производится авторизация в почтовом сервере
`#Почтовый адрес, с которого отправлено сообщение` `EMAIL_FROM="no_reply@aeca.ru"`	укажите адрес почты, с которой будет производиться рассылка уведомлений
`#CRON для запуска метода отправки почтовых уведомлений` `EMAIL_SCHEDULE="0 */30 * * * *"`	укажите период проверки в виде CRON-выражения, по которому будет выполняться проверка сроков действия сертификатов и рассылка уведомлений (по умолчанию раз в 30 минут)
`#Флаг отправки почтовых уведомлений, если выкл, то сообщения не отправляются, но>` `EMAIL_ENABLED="true"`	флаг отправки уведомлений (если false, то уведомления рассылаться не будут, но будут отмечаться отправленными)
`#Протокол рассылки сообщений` `EMAIL_PROTOCOL="smtp"`	протокол, по которому происходит подключение к почтовому серверу (по умолчанию SMTP)
`#Авторизация по SMTP` `EMAIL_SMTP_AUTH="false"`	флаг авторизации при подключении к почтовому серверу
`#Использовать TLS` `EMAIL_START_TLS="false"`	флаг использования TLS при подключении к почтовому серверу

- Для применения внесенных настроек следует перезапустить сервис:
  - при использовании ПО «Центр сертификации» на отдельном сервере, выполнив команду:

```
sudo systemctl restart aecaca.service
```

  - при использовании ПО «Центр сертификации» и «Центра валидации» на одном сервере, выполнив команду:

```
sudo systemctl restart aeca.service
```

4.12.2 **Настройка шаблонов уведомлений об истечении срока действия сертификата**

- В базе данных в таблице «`public.aeca_email_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 15.

Таблица 15 – 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:

```
email_config.sh -list
```

- Отредактируйте существующий шаблон при необходимости, выполнив команду:

```
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:

```
./email_config.sh -edit 4 "2 часа" "Истекает через 2 часа" 7200000 INACTIVE
UPDATE 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 | 2 часа                | Истекает через 2 часа        |    7200000 | INACTIVE
(4 строки)
```

- Для создания нового шаблона уведомлений выполните команду:

```
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:
  - при использовании ПО «Центр сертификации» на отдельном сервере, выполнив команду:

```
sudo systemctl restart aecaca.service
```

  - при использовании ПО «Центр сертификации» и «Центра валидации» на одном сервере, выполнив команду:

```
sudo systemctl restart aeca.service
```

4.12.3 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.
- Настройка почтовой программы показана на примере настройки Яндекс.Почта (см. Рисунок 184).

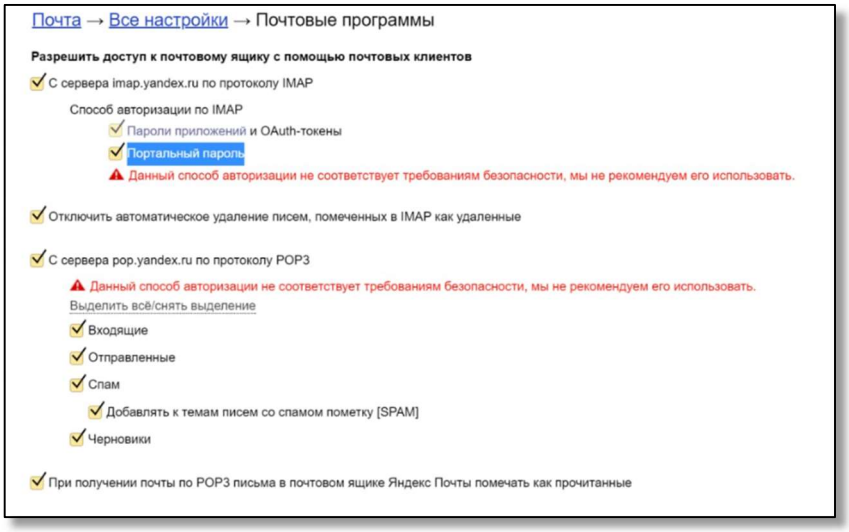


Рисунок 184 – Настройки почтового ящика для получения уведомления об истечении срока сертификата

5 НАСТРОЙКА «ЦЕНТРА ВАЛИДАЦИИ» ALADDIN ECA

5.1 Описание верхней панели «Центра валидации»

- Верхняя панель (см. Рисунок 185) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.

Рисунок 185 – Верхняя панель окна «Центра валидации»

- При наведении курсора на иконку  панели всплывает соответствующее текстовое пояснение, содержащее контактную информацию компании-разработчика и номер текущей версии ПО (см. Рисунок 186).

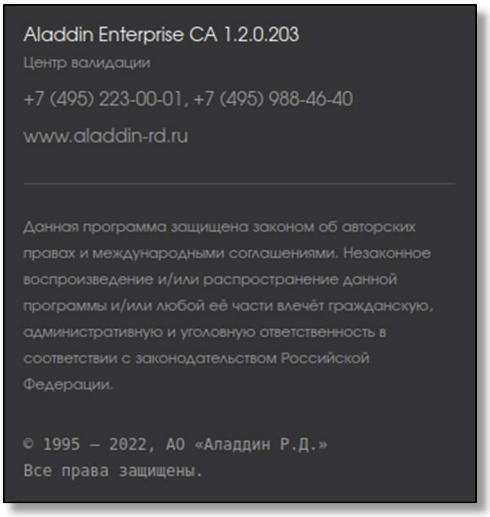


Рисунок 186 – Окно «О программе» Центра валидации

5.2 Описание боковой панели «Центра валидации»

Боковая панель Центра валидации закреплена и отображается на любом шаге или переходе между вкладками.

Полный вид боковой панели показан на Рисунок 187, компактный вид боковой панели приведен на Рисунок 188. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

Боковая панель состоит из вкладок, определяющих соответствующие функции ПО AECA VA и созданы для организации управления Центром валидации:

- Вкладка «Издатели» – на данной вкладке возможно:
  - добавить корневой сертификат Центра сертификации;
  - скопировать url-адрес для распространения сертификата издателя;
  - скачать сертификат издателя.
- Вкладка «CRL DP» – на данной вкладке возможно:
  - скопировать url-адрес для распространения списка отозванных сертификатов;
  - скопировать url-адрес публикации CRL
  - скопировать url-адрес для распространения DeltaCRL;
  - скачать текущий CRL.

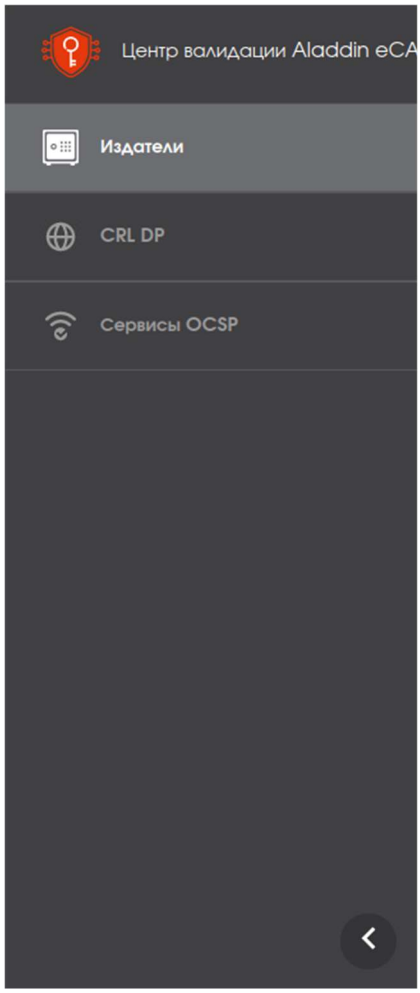


Рисунок 187 – Полный вид боковой панели

Рисунок 188 – Компактный вид боковой панели

- Вкладка «Сервисы OCSP» – на данной вкладке возможно:
  - создать новый сервис OCSP;
  - скопировать URL-адрес OCSP сервиса;
  - обновить CRL;
  - произвести настройку сервиса OCSP;
  - скачать сертификат издателя;
  - скачать цепочку сертификатов.

5.3 Описание вкладки «Издатели»

- Переход на вкладку «Издатели» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 187).
- На данной вкладке отображён список издателей, сертификаты которых может рассылать служба доступа к информации о центрах сертификации (AIA).
- На основном экране сервиса публикации отображены информационные поля экранной формы (см. Рисунок 189):
  - поле «Издатель» – в данном поле записан суффикс различающегося имени Центра сертификации;

- поле «Действителен до» – в данном поле указано окончание срока действия сертификата издателя – Центра сертификации;
- поле «Алгоритм ключа» и поле «Длина ключа» – в данном поле отображены выбранные параметры криптографии сертификата Издателя.

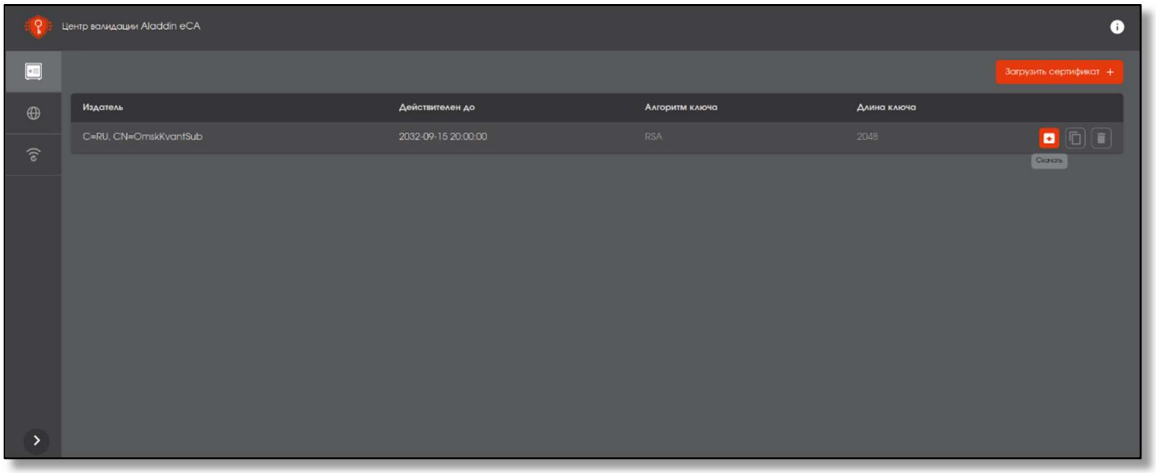


Рисунок 189 – Экран «Издатели»

5.3.1 **Добавление новой записи об издателе**

- Для добавления записи в список издателей:
  - нажмите кнопку <Загрузить сертификат +> (см. Рисунок 189);
  - выберите файл сертификата центра сертификации в формате .pem и нажмите кнопку <Открыть>.
- В случае успешной загрузки сертификата администратор будет уведомлён соответствующим сообщением (см. Рисунок 190) и добавлена строка с новым издателем.

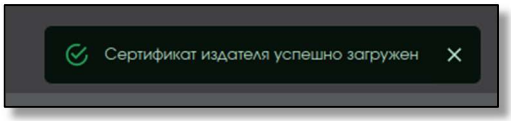


Рисунок 190 – Сообщение об успешном добавлении сертификата издателя

- В случае, если сертификат издателя был загружен ранее, администратор будет уведомлен соответствующим сообщением (см. Рисунок 191) и файл сертификата ранее зарегистрированного издателя будет обновлён.

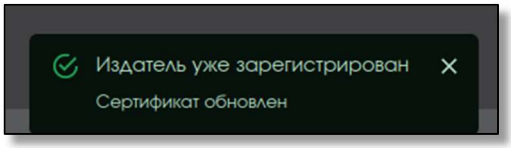


Рисунок 191 – Сообщение об обновлении сертификата издателя

- В случае, если сертификат издателя в формате .pem был загружен в отличном формате, то администратор будет уведомлен соответствующим сообщением (см. Рисунок 192).

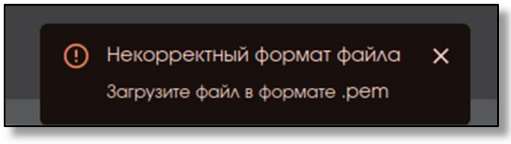


Рисунок 192 – Сообщение о некорректном формате файла сертификата издателя

5.3.2 **Доступные действия над добавленными записями издателей**

При наведении курсора на строку издателя появляются возможности выполнить следующие действия:

- скачать сертификат издателя, нажав кнопку <Скачать>  , выбрав место сохранения файла сертификата и нажав кнопку <Сохранить>;
- скопировать в буфер обмена url-адрес для распространения (откуда можно скачать сертификат издателя), нажав кнопку <Копировать URL распространения>  ;
- удалить запись из списка издателей, нажав кнопку <Удалить>  . Процесс удаления происходит с подтверждением и предупреждением о необратимости операции.

При удалении издателя произойдет удаление служб AIA, CRL DP и OCSP!

5.4 Описание вкладки «CRL DP»

- Переход на вкладку «CRL DP» осуществляется через боковое меню, расположенное слева на главном экране Центра валидации (см. Рисунок 187).
- На данной вкладке отображён сервис публикации CRL, созданный при регистрации Центра валидации на сервере Центра сертификации.
- На основном экране сервиса публикации отображены информационные элементы (см. Рисунок 189):
  - поле «Издатель» – в данном поле записан суффикс различающегося имени Центра сертификации;
  - поле «№» – в данном поле записан номер последнего опубликованного CRL и номер последнего опубликованного DeltaCRL (в котором DeltaCRLIndicatore указывает на текущий CRL);
  - поле «Действителен до» – в данном поле указан срок действия последнего опубликованного CRL/DeltaCRL;
  - поле «Отозванных сертификатов» показывает количество отозванных сертификатов в последнем опубликованном CRL, включая количество отозванных сертификатов в последнем DeltaCRL;
  - поле «Последняя публикация» показывает дату создания последнего опубликованного CRL/DeltaCRL.

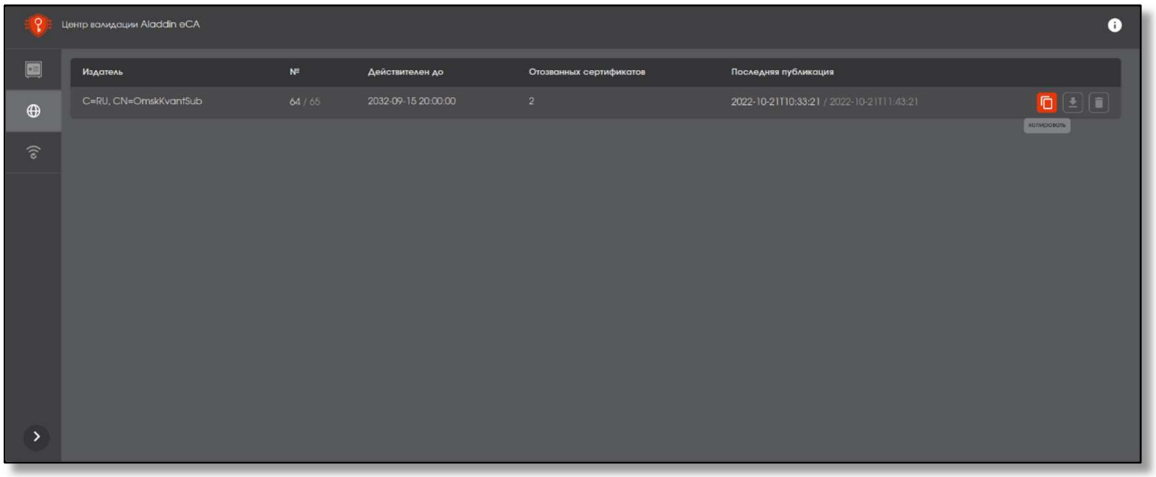


Рисунок 193 – Экран «CRL DP»

5.4.1 **Доступные действия CRL DP**

При наведении курсора на строку сервиса публикации появляется возможность выполнить следующие действия:

- скопировать в буфер обмена url-адрес  и выбрав из выпадающего меню (см. Рисунок 194):
  - публикации CRL;
  - для распространения CRL;
  - для распространения DeltaCRL;

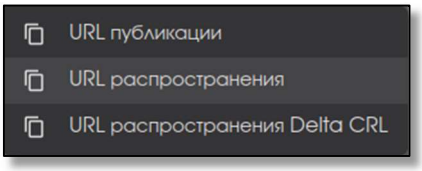


Рисунок 194 – Подменю «Копировать» CRL DP

- скачать текущий CRL, нажав кнопку <Скачать>  , выбрав место сохранения файла сертификата и нажав кнопку <Сохранить>;
- удалить сервис публикаций, нажав кнопку <Удалить>  . Процесс удаления происходит с подтверждением и предупреждением о необратимости операции.

При удалении сервиса публикации произойдет удаление службы OCSP!

5.5 Описание вкладки «Сервисы OCSP»

- Переход на вкладку «Сервисы OCSP» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 187).
- На основном экране сервиса OCSP отображены информационные элементы (см. Рисунок 195):
  - в поле «Издатель» указано имя Центра сертификации, подписавшего запрос на сертификат OCSP;
  - поле «Имя сервиса» сгенерировано случайно в случае регистрации центра валидации на сервере, где развёрнут Центр сертификации, и заданное имя сервиса при создании сервиса OCSP на сервере, где развёрнут Центр валидации»;
  - в поле «Действителен до» указано окончание срока действия сертификата сервиса OCSP;
  - в поле «CRL действителен до» указано окончание срока действия текущего списка отозванных сертификатов;
  - поле «Состояние» показывает текущее состояние сервиса OCSP. Возможные состояния сервиса OCSP: запущен, остановлен, ошибка CRL, недействителен, ожидает сертификат (см. пункт настоящего руководства администратора).

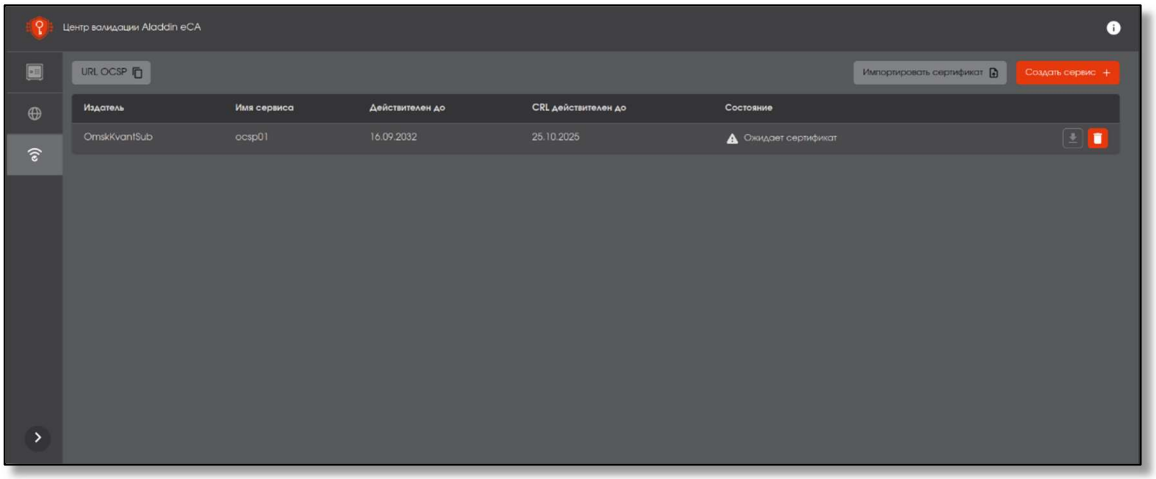


Рисунок 195 – Экран «Сервисы OCSP»

- Создание сервиса OCSP возможно двумя способами:
  - при регистрации Центра валидации на сервере, где развёрнут Центр сертификации (см. п.4.8.3 настоящего руководства);
  - создание сервиса OCSP на сервере, где развёрнут Центр валидации (см. п.5.6 настоящего руководства).
- Для настройки параметров доступа к службе OCSP необходимо выполнить процедуры:
  - создания сервиса OCSP;
  - подписания запроса на сертификат сервиса OCSP в ЦС;
  - импортирования подписанного сертификата сервиса OCSP.
- Кнопка 

– по нажатию на кнопку <URL OCSP> происходит копирование URL службы OCSP (по этому URL будет доступен каждый OCSP) (см. Рисунок 196).

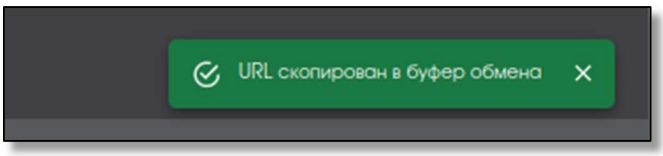


Рисунок 196 - Уведомление об успешном копировании URL службы OCSP

- Кнопка 

– по нажатию кнопки <Создать сервис +> на главном экране управления сервисами OCSP происходит запуск сценария создания сервиса OCSP.
- Кнопка 

<Импортировать сертификат> будет доступной при наличии сервисов на главном экране управления сервисами OCSP в состоянии «Ожидает сертификат».

5.6 Создание сервиса OCSP на сервере Центра валидации

- На каждом шаге создания сервиса OCSP администратору доступны кнопки:
  - <Назад> - для возврата на предыдущий шаг;
  - <Отмена> - для прекращения процесса создания сервиса;
  - <Продолжить> - становится активной и доступной для нажатия только в случае верного заполнения всех полей на текущем шаге.
- Перед созданием сервиса OCSP требуется предварительно:

- скачать цепочку сертификатов Центра сертификации (издателя), для которого создаем сервис OCSP и перенести цепочку сертификатов на АРМ, на котором происходит настройка «Центра валидации».
- настроить сервис публикации на вкладке «CRL DP», для которого создаем сервис OCSP и скопировать указатель ресурса точки распространения CRL в буфер обмена.

• Нажмите на кнопку <Создать сервис +> на экране управления сервисами. В открывшемся окне (см. Рисунок 197) заполнить следующие поля:

- имя сервиса – имя, которое должно попасть в `Common Name` запроса на сертификат службы OCSP и соответствующего сертификата службы OCSP;
- указать файл формата `.pem`, содержащий цепочку сертификатов ЦС.

После выбора файла и нажатия кнопки <Продолжить> файл импортируется.

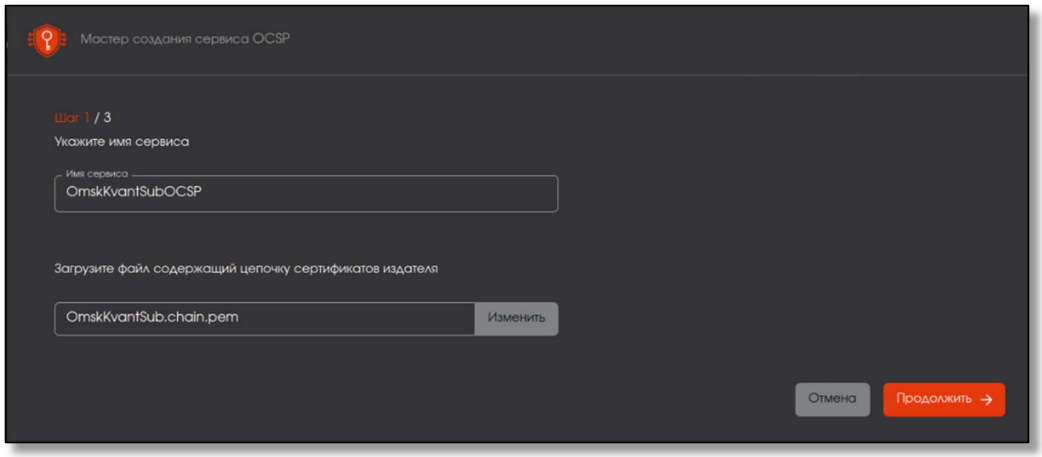


Рисунок 197 – Окно создания сервиса OCSP. Шаг 1

• Возможные ошибки, которые могут привести к завершению создания сервиса:

- файл неверного формата. Загрузите, пожалуйста, файл в формате PEM;
- сертификат не действителен. Загрузите, пожалуйста, файл, содержащий валидную цепочку сертификатов.

• В рамках данного сценария не проверяется валидность CRL.

• В случае успешного импорта файла, администратор переходит на следующий экран создания сервиса OCSP (см. Рисунок 198).

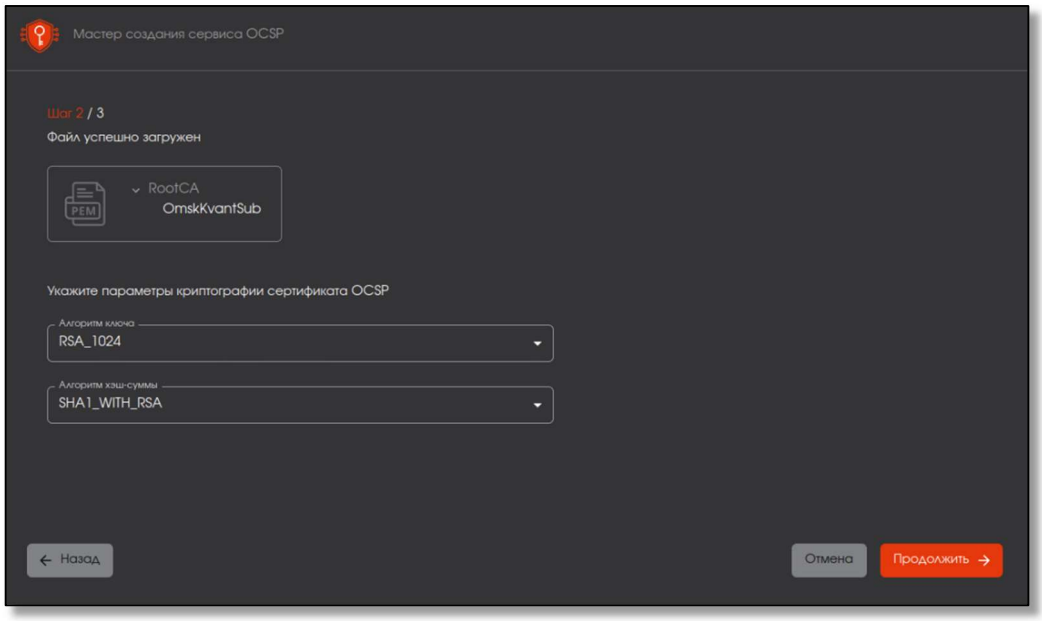


Рисунок 198 – Окно создания сервиса OCSP. Шаг 2

- На экране появится подтверждение успешной загрузки с отображением полной цепочки сертификатов, а также полей с выпадающими списками, где администратор указывает параметры криптографии создаваемого сервиса:
  - алгоритм ключа;
  - алгоритм хэш-суммы.

После указания параметров криптографии создаваемого сервиса нажать кнопку <Продолжить>.

- Следующим шагом является задание параметров CRL на экране создания сервиса OCSP (см. Рисунок 199).

В открывшемся окне заполните следующие поля:

- <URL точки распространения CRL> – укажите путь скачивания CRL того ЦС, статус сертификатов которого будет проверяться;
- <Период обновления> - задание периода опроса CRL DP. Формат ввода: 1h,1d,1m,1y — час, день, месяц, год.

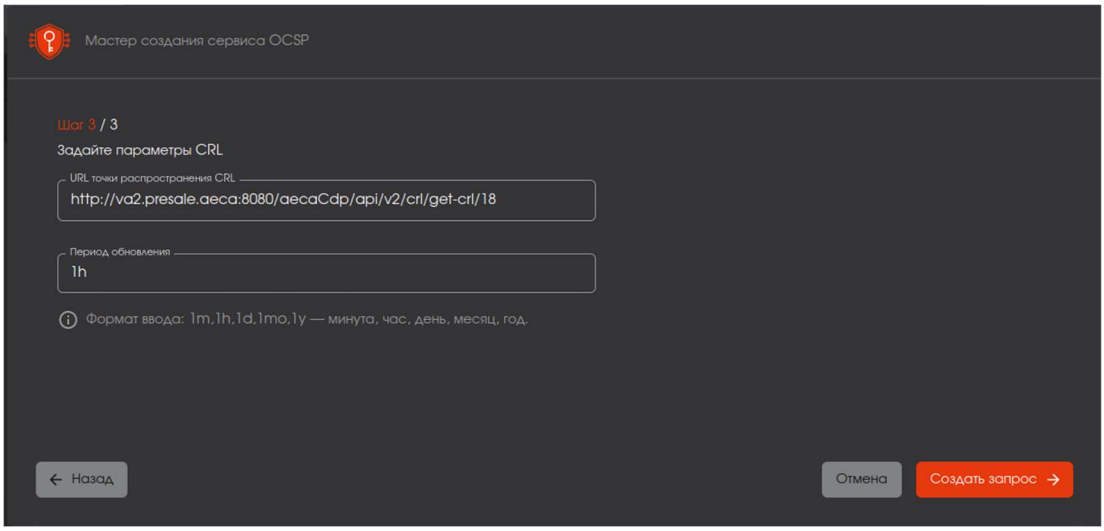


Рисунок 199 – Окно создания сервиса OCSP. Шаг 3

После указания параметров CRL нажмите ставшую активной кнопку <Создать запрос>.

- Финальным шагом является экран с результатом успешного создания запроса на сертификат для службы OCSP (см. Рисунок 200), где администратору доступны кнопки:
  - <Скачать> - для скачивания сформированного запроса на сертификат;
  - <Закрыть> - окно создания сервиса закрывается и происходит возврат в главное окно.

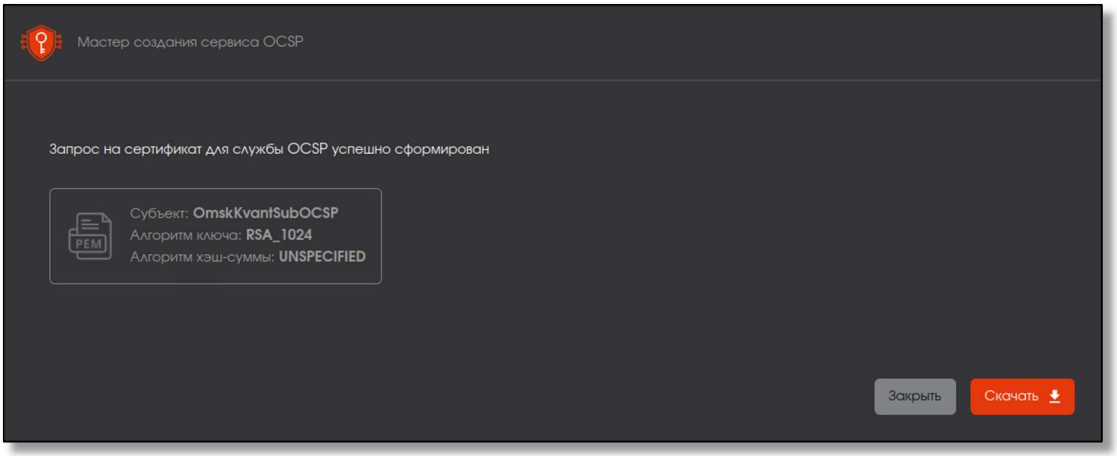


Рисунок 200 - Окно создания сервиса OCSP. Шаг 4

- Созданный сервис отобразиться в списке сервисов OCSP на вкладке «Сервисы OCSP» в состоянии «Ожидает сертификат» (см. Рисунок 201).

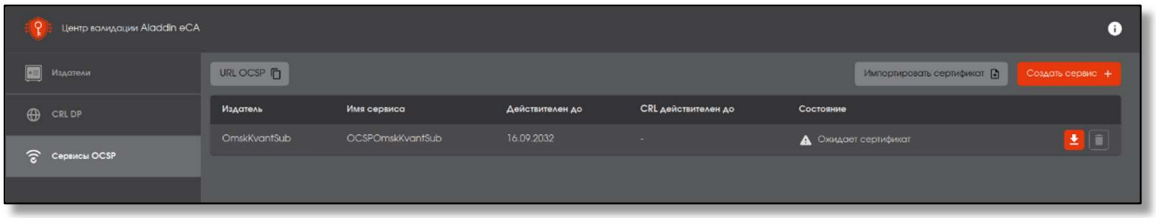


Рисунок 201 – Список сервисов OCSP

- Для дальнейшего подписания запроса на сертификат для службы OCSP необходимо скачать созданный запрос и перенести его на АРМ ЦС, для которого создается сервер-OCSP.

5.7 Подписание запроса на сертификат для службы OCSP

Для подписания запроса:

- открыть «Центр сертификации» АеСА;
- на вкладке «Свои сертификаты» убедиться, что ЦС, для которого создается сервер-OCSP, находится в состоянии «Активирован»;
- выполнить подписание запроса на сертификат сервиса OCSP согласно пункту 4.4.9 настоящего руководства администратора, выбирая в соответствующем поле окна создания сертификата шаблон «OCSP Signer» (см. Рисунок 202).

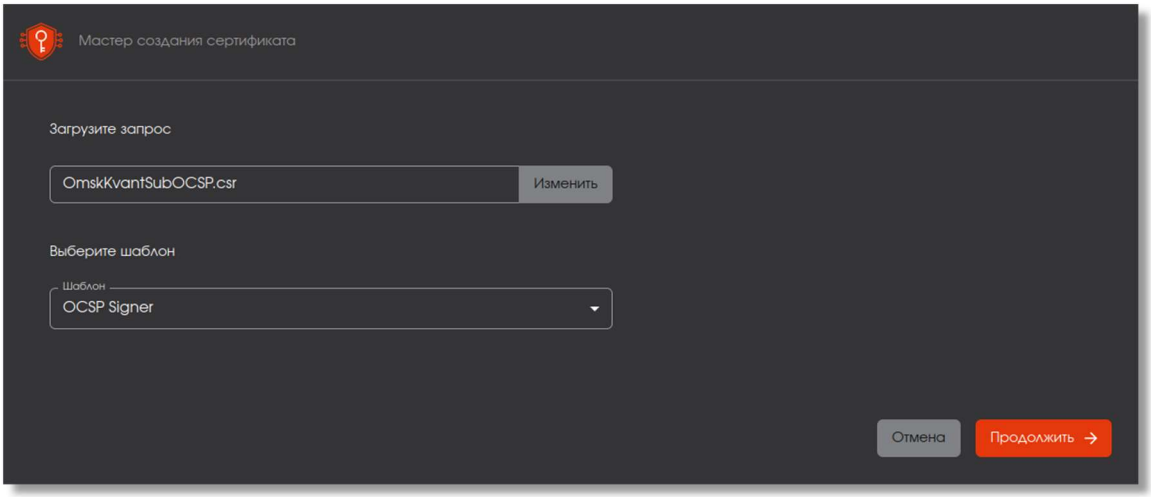


Рисунок 202 – Окно создания сертификата. Загрузка запроса и выбор шаблона

- Далее необходимо скачать файл сформированного сертификата сервиса OCSP в формате .pem.
- Перенести созданный сертификат на АРМ «Центра валидации», для которого был выпущен данный сертификат.
- Произвести импорт сертификата сервиса OCSP.

5.8 Импорт сертификата службы OCSP

- Импорт сертификата инициируется по нажатию на кнопку 

<Импортировать сертификат> на вкладке «Сервисы OCSP» (см. Рисунок 201) для сервиса в состоянии «Ожидает сертификат», также кнопка «Импортировать сертификат» доступна в карточке сервиса со статусом «Ожидает сертификат» и на главном экране раздела.

- По нажатию на кнопку <Импортировать сертификат> открывается окно для загрузки файла сертификата (см. Рисунок 203). Прием файла осуществляться в формате .pem.

При необходимости, возможно перезагрузить подписанный файл сертификата через кнопку <Изменить>.

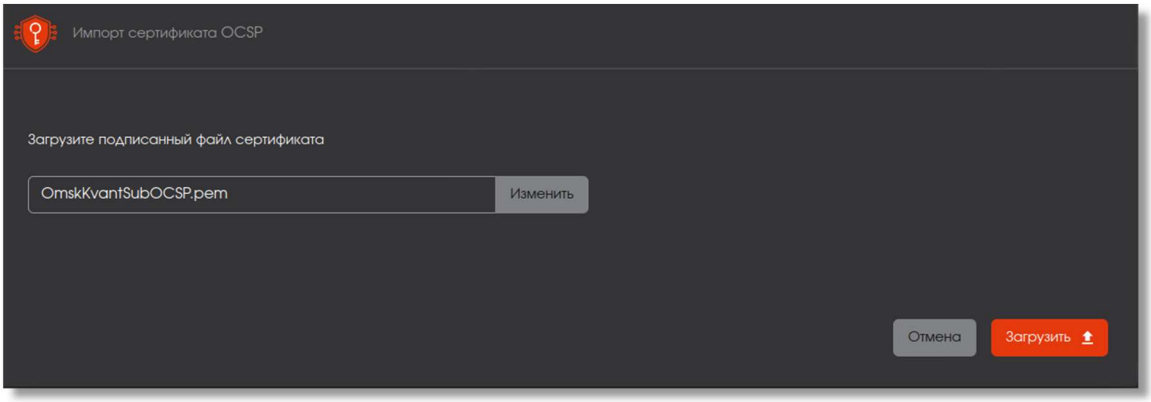


Рисунок 203 – Окно импорта сертификата OCSP

После того, как будет выбран сформированный файл сертификата, нажать на кнопку <Загрузить>.

Если загрузка файла сертификата была произведена с ошибкой, то администратору будет выведено уведомление с ошибкой.

- В случае успешной загрузки откроется окно с результатом (см. Рисунок 204).

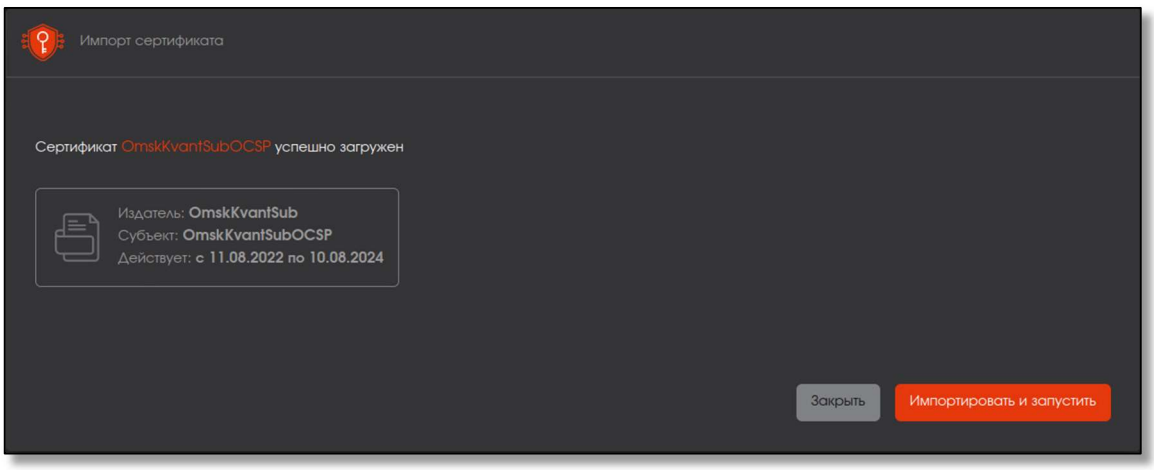


Рисунок 204 - Окно импорта сертификата OCSP. Успешная загрузка файла

После успешного импорта по нажатию на кнопку <Импортировать и запустить> происходят следующие действия:

- запускается сервис OCSP;
- запускается служба CRL updater (служба обновления CRL).

- Далее необходимо открыть карточку созданной службы OCSP и нажать кнопку <Обновить CRL>, дождаться перевода сервиса OCSP в состояние «Запущен».

5.9 Карточка сервиса, возможные действия над сервисом в зависимости от состояния

Для просмотра карточки созданного сервиса, необходимо выбрать нужный сервис в списке и дважды кликнуть по выбранной строке.

Общие возможные действия в карточке сервиса OCSP (в зависимости от статуса сервиса):

- кнопка <Импортировать сертификат> для сервиса в состоянии запроса – по нажатию данной кнопки в открывшемся окне выберите сертификат сервиса OCSP, полученный в результате подписания запроса на сертификат сервиса на сервере Центра сертификации;
- кнопка <Удалить> для удаления сервиса через подтверждение действия (более подробно в пункте 5.12);
- кнопка <Настроить> (более подробно в пункте 5.11);
- кнопка <Обновить CRL> для обновления списка отзыва в произвольный момент времени;
- имя сервиса, заданное при создании;
- ссылка <Скачать запрос> для скачивания запроса без подтверждения (для сервиса в состоянии запроса);
- состояние (для сервисов в состоянии ожидания сертификата, будет значение <Нужно импортировать сертификат сервиса>);
- поле <Алгоритм подписи ответа> по умолчанию:
- RSA для алгоритма сертификата RSA;
- ECDSA для алгоритма сертификата ECDSA.
- поле <Адрес загрузки CRL> и <Период обновления> для отображения значений, заданных в окне создания;
- поле <Следующее обновление CRL> показывает дату следующего обновления по таймеру;
- данные в полях <Номер текущего CRL> и «CRL действителен до» (Next Update) отображаются в случае, если удалось скачать сертификат по указанному адресу загрузки;
- расширения OCSP, заданные в настройках сервиса (все галочки по умолчанию заданы):
  - 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 OCSP) в ответ и включать ли его цепочку.

- Набор доступных действий в карточке сервиса OCSP определяется состоянием сервиса OCSP:

- Сервис в состоянии «Ожидает сертификат»

Сервис OCSP не инициализирован.

При наведении на строку с нужным сервисом будут доступны иконки (см. Рисунок 205):

-  <Скачать> запрос на сертификат сервиса OCSP для дальнейшей его подписи Центром сертификации;
-  <Удалить> сервис OCSP.

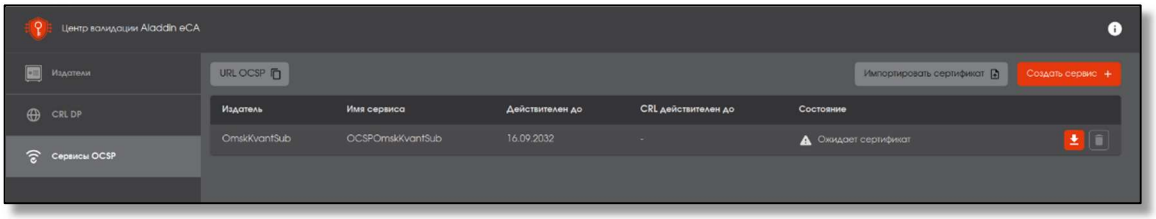


Рисунок 205 – доступные действия над сервисом OCSP в состоянии «Ожидает сертификат»

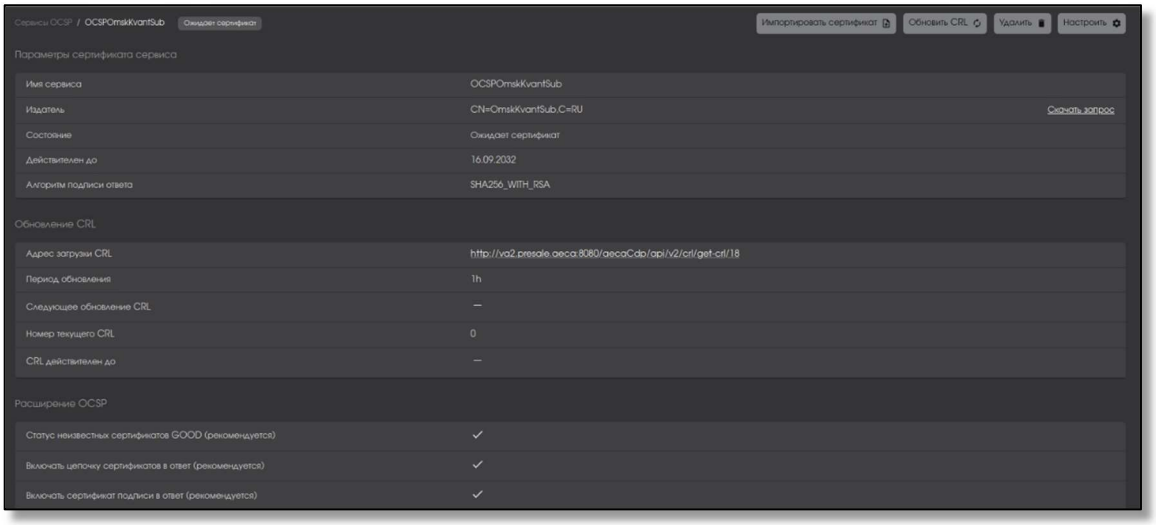


Рисунок 206 – Карточка сервиса в состоянии «Ожидает сертификат»

- Сервис в состоянии «Запущен»

После успешного импорта сертификата сервис переходит в состояние «Запущен» (см. Рисунок 207, Рисунок 208).

После скачивания CRL, если он валиден, сервис OCSP будет отвечать на запросы о статусе сертификата ЦС, подписавшего сертификат этого сервиса, в соответствии с настройками.

При наведении на строку с нужным сервисом будут доступны иконки (см. Рисунок 207):

- <Остановить> для остановки служб сервиса OCSP без подтверждения;
-  <Удалить> сервис OCSP с подтверждением.

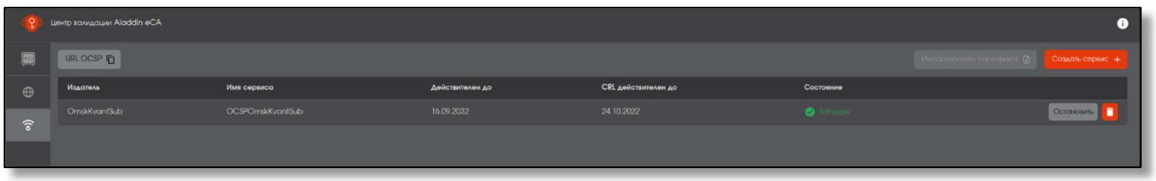


Рисунок 207 - Сервис в состоянии "Запущен"

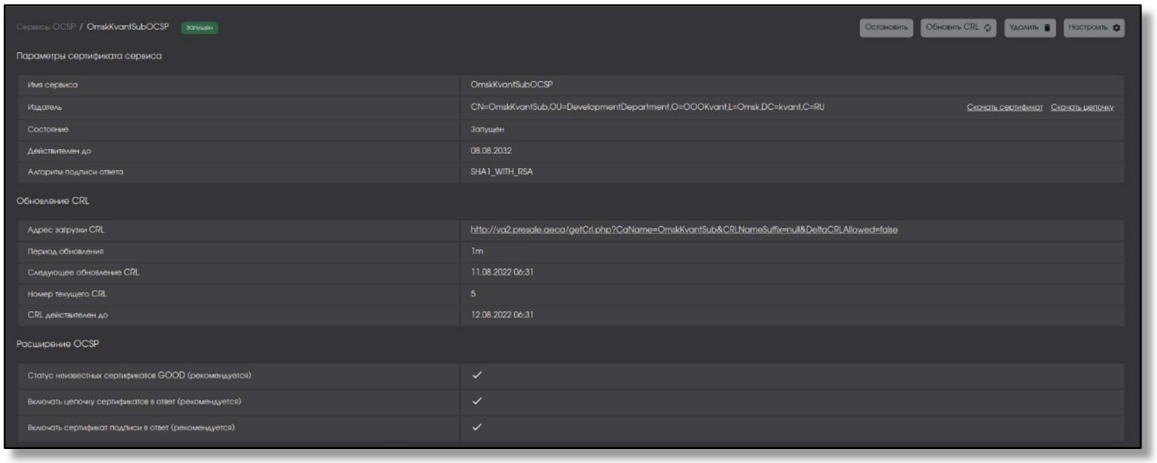


Рисунок 208 - Карточка сервиса в состоянии "Запущен"

- Сервис в состоянии «Остановлен»

В состоянии «Остановлен» сервис не работает (см. Рисунок 209, Рисунок 210). Обновление CRL не происходит.

При наведении на строку с нужным сервисом будут доступны иконки (см. Рисунок 209):

- <Запустить> по нажатию кнопки остановленный сервис может перейти в состояние «Запущен». После нажатия кнопки <Запустить> производятся следующие действия:
  - запускается сервис OCSP;
  - запускается служба CRL updater;
  - осуществляет отображение статуса «Запущен» в столбце «Состояние».
-  <Удалить> сервис OCSP с подтверждением.

Рисунок 209 - Сервис в состоянии "Остановлен"

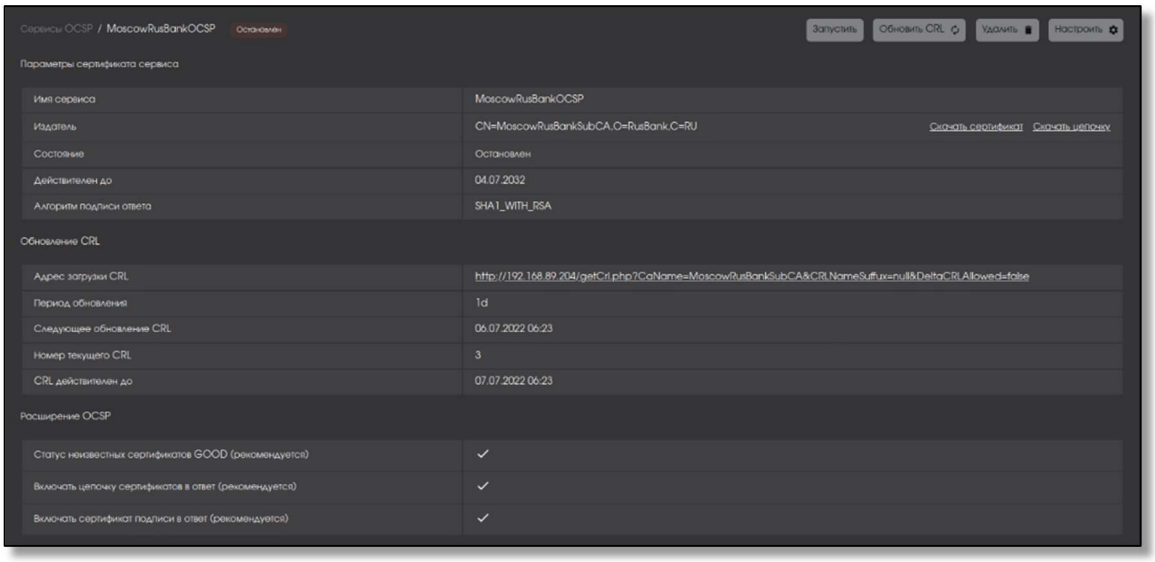


Рисунок 210 – Карточка сервиса в состоянии «Остановлен»

- Работа сервиса в состоянии «Ошибка CRL»

В это состояние сервис переходит, если по указанному URL-адресу CRL недоступен, просрочен или не валиден (см. Рисунок 211, Рисунок 212).

В этом состоянии сервис отвечает на запросы OCSP ошибкой: interlaError(2) или tryLater(3) в соответствии с https://datatracker.ietf.org/doc/html/rfc6960#section-4.2

При наведении на строку с нужным сервисом будут доступна иконка (см. Рисунок 211):

-  <Удалить> сервис OCSP с подтверждением.

Рисунок 211 - Сервис в состоянии «Ошибка CRL»

Служба обновления CRL продолжает работать и, если CRL обновился и валиден, то сервис автоматически переходит в состояние «Запущен».

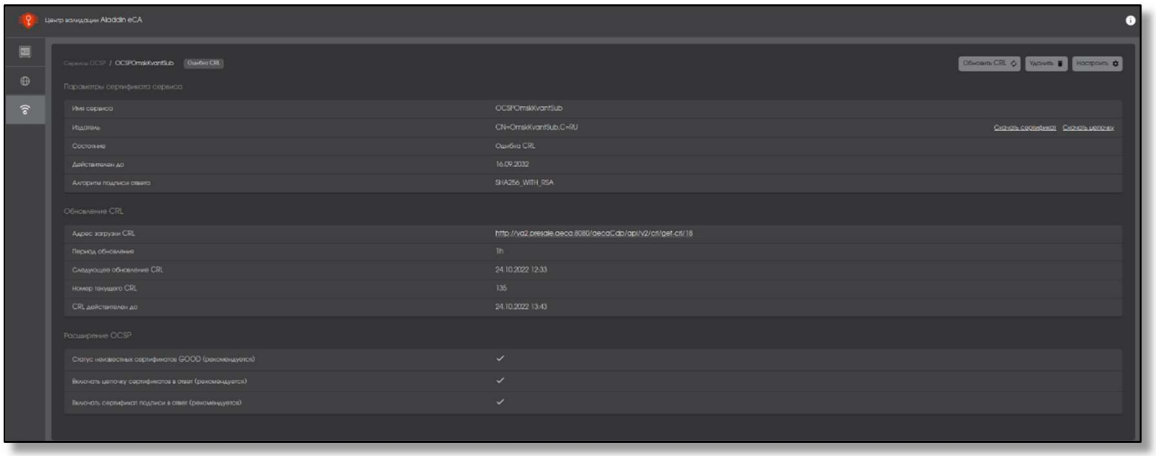


Рисунок 212 – Карточка сервиса в состоянии «Ошибка CRL»

- Сервис в состоянии «Недействителен»

В этом состоянии сервис можно только удалить через подтверждение.

5.10 Редактирование сервиса OCSP

- Сценарий редактирования сервиса инициируется по нажатию кнопки <Настроить> (см. Рисунок 213) в карточке сервиса (п. 5.9 настоящего руководства администратора).
- При необходимости администратор может внести изменения в поля:
  - алгоритм подписи ответа;
  - адрес загрузки CRL;
  - период обновления;
  - статус неизвестных сертификатов GOOD (рекомендуется);
  - включать цепочку сертификатов в ответ (рекомендуется);
  - включать сертификат подписи в ответ (рекомендуется).
- По умолчанию проставлены все галочки в блоке «Расширение OCSP»:

- 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 OCSP) в ответ и включать ли его цепочку.

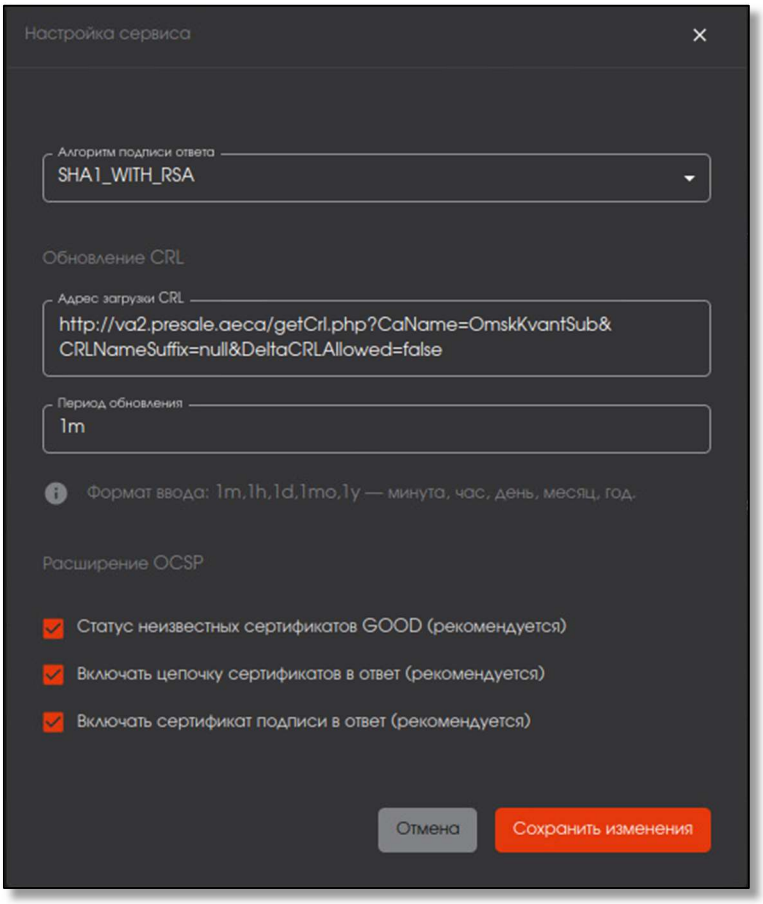


Рисунок 213 – Экран с настройками сервиса OCSP

5.11 Удаление сервиса OCSP

Удаление сервиса доступно на главном экране по клику на иконку <Удалить> в соответствующей строке с сервисом (см. Рисунок 201), а также по нажатию на кнопку <Удалить> в карточке просмотра сервиса.

При клике на кнопку <Удалить> будет запрошено подтверждение действия (см. Рисунок 214).

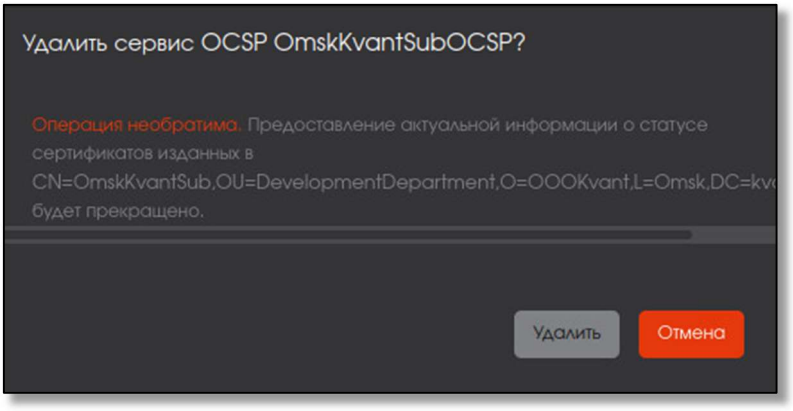


Рисунок 214 – Окно подтверждения удаления сервиса OCSP

6 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

<table>
<tr><th>Проблема</th><th>Возможная причина</th><th>Способы решения</th></tr>
<tr><td>Заблокированы кнопки выпуска сертификатов</td><td>Истёк срок действия лицензии или исчерпан лимит доступных для выпуска сертификатов</td><td>Проверьте в окне «О программе» срок действия лицензии и количество доступных для выпуска сертификатов (см. п. 3.1)</td></tr>
<tr><td rowspan="2">Прекращение установки ПО или обновление АеСА</td><td>1. Не хватка аппаратных ресурсов</td><td>Произведите оценку ресурса вашего ПК в соответствии с требованием к аппаратным ресурсам, указанным в первой части Руководства администратора</td></tr>
<tr><td colspan="2">2. Не корректная установка или отсутствие программного компонента, указанного в требовании
Проверьте наличие установленного ПО согласно разделу 3 Руководство администратора RU.АЛДЕ.03-01.020-01 32.

Также проверьте и при необходимости переключите текущую версию java-компонентов, выполнив команды:
<pre>sudo update-alternatives --config java
sudo update-alternatives --config javac
sudo update-alternatives --config javap</pre></td></tr>
<tr><td rowspan="3">Нет подключения к ресурсной системе</td><td>1. Включен протокол TLS</td><td>Измените настройку конфигурационного файла контроллера домена <code>/etc/samba/smb.conf</code>, добавив в раздел <code>[global]</code>:
<pre>ldap server require strong auth = no</pre></td></tr>
<tr><td>2. Проверить подключение к контроллеру домена Samba</td><td>Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:
- получение списка пользователей
<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=user)"</pre>- получение списка компьютеров
<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=computer)"</pre>- получение списка групп безопасности
<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC= pki-test " -H "ldap://192.168.111.148" "(objectCategory=group)"</pre>где:
<code>Administrator@pki-test.local</code> – имя администратора домена;</td></tr>
</table>

Проблема	Возможная причина	Способы решения
		`Qwerty1234` – пароль администратора домена; `pki-test, pki-test` – доменное имя; `192.168.111.148` – ip-адрес контроллера домена. В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.

	3. Проверить подключение к контроллеру домена ALD PRO	Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:
		- получение списка пользователей
		`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)"`
		- получение списка компьютеров
		`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)"`
		- получение списка групп безопасности
		`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)"`
		где:
		`admin` – имя администратора домена;
		`users`, `accounts`
		`Qwerty1234` – пароль администратора домена;
		`domain, local` – доменное имя;
		`192.168.111.148` – ip-адрес контроллера домена.
		В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.

Вход в интерфейс Центра сертификации с выпущенным сертификатом невозможен в браузере Chromium	Браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой браузер
Невозможно подключиться к токену для выпуска сертификата после установки JC-WebClient. Сообщение «ПО JCWebClient не установлено»	Требуется разрешить ПО JC-WebClient доступ к ресурсу	1. В адресную строку браузера введите: https://localhost:24738/admin/token_manager.html 2. Во всплывающем окне предупреждения браузера подтвердите действия.

Проблема	Возможная причина	Способы решения
Пустой файл шаблонов по завершению работы скрипта mscs2aeca.ps1экспорта шаблонов MSCS	Требуется настройка tls	- Откройте Powershell от имени администратора и задайте версию протокола безопасности, выполнив команду: `[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12`

7 КОНТАКТЫ

7.1 Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, 7 этаж, компания "Аладдин Р.Д."

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

Факс: +7 (495) 646-08-82

E-mail: aladdin@aladdin-rd.ru (общий)

Web: https://www.aladdin-rd.ru

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней.

7.2 Техподдержка

Служба техподдержки принимает запросы только в письменном виде через веб-сайт: www.aladdin-rd.ru/support/index.php.

ПРИЛОЖЕНИЕ А. ОПИСАНИЕ ПОЛЕЙ ШАБЛОНОВ СЕРТИФИКАТОВ

Наименование поля АЕСА	Поле в базе SambaDC, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Domain controller – шаблон сертификата контроллера домена				
имя	CommonName	имя контроллера домена	DC01	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
доменное имя	DC	домен	example.com	А-Я, а-я, A-Z, a-z, 0-9, ., -
MS GUID	objectGUID / ipaUniqueID	глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена	92625ee510e248479554779d1f43f751 (32 знака)	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	2048, 3072, 4096, 256, 384, 521	-
ALD PRO Domain controller – шаблон сертификата контроллера домена ALD PRO				
имя	CommonName	имя контроллера домена ALD PRO	dc.ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
MS UPN	objectGUID / ipaUniqueID	данные в формате «krbtgt/полное имя домена@полное имя домена»	krbtgt/ald.pro@ald.pro	Строка вида “text@text” А-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	А-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

Наименование поля АЕСА	Поле в базе SambaDC, 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	-
Smartcard Logon ALD PRO – шаблон сертификата пользователя ALD PRO				
имя	CommonName	имя пользователя ALD PRO		А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-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	А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
Smartcard Logon – шаблон сертификата пользователя				
имя	CommonName	имя пользователя	IvanovaAN	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
организация	-	полное имя домена	ald.pro	А-Я, а-я, A-Z, a-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, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@ald.pro	Строка вида “text@text” А-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	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	2048, 3072, 4096	-

Наименование поля АЕСА	Поле в базе SambaDC, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
Web-client – шаблон сертификата учетной записи				
имя	CommonName	имя веб-клиента	Operator01	А-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” и только указанные символы: А-Я, а-я, A-Z, a-z, 0-9, ., @, _, -
MS UPN	userPrincipalName / krbPrincipalName	имя входа пользователя в формате e-mail адреса	ivanova@example.com	Строка вида “text@text” А-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	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	1024,1536,2048,3072,4096,6144, 8192	-
Web-server – шаблон сертификата веб-сервера				
имя	CommonName	имя веб-сервера	Center01	А-Я, а-я, A-Z, a-z, 0-9, ., _, -, пробел
доменное имя	DC	домен	example.com	А-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	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	1024,1536,2048,3072,4096,6144, 8192	-
S/MIME – шаблон сертификата электронной почты				

Наименование поля АЕСА	Поле в базе SambaDC, MS AD / ALD PRO, FreeIPA	Описание	Пример заполнения	Допустимые символы
имя	CommonName	имя пользователя	ivanova	А-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 А-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	-
алгоритм ключа	-	выберите из выпадающего списка	RSA, ECDSA	-
длина ключа	-	выберите из выпадающего списка	192,224,256,384,521,1024, 1536,2048,3072,4096,6144,8192	-

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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