Центр сертификатов доступа

Aladdin Enterprise Certificate Authority

Certified Edition

Руководство оператора

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 34 01
Версия	2.3 (AeCA), 2.3 (AeRA)
Листов	136
Дата	01.09.2025

Авторские права, товарные знаки, ограничения

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.

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 ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

АННОТАЦИЯ

Настоящий документ представляет собой руководство оператора программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» [1].

Настоящий документ является эксплуатационным документом, содержащим описание действий пользователя с ролью «Оператор» (далее по документу – Оператор) при работе с программными комплексами «Центр сертификации Aladdin Enterprise Certification Authority» [2] и «Центр регистрации Aladdin Enterprise Registration Authority [3]», входящими в состав Центра сертификатов доступа.

Настоящий документ содержит сведения о назначении программного средства, условиях его применения, порядке действий Оператора при работе с Центром сертификации Aladdin eCA и Центром регистрации Aladdin eCA, сообщениях, выдаваемых Оператору в процессе работы.

Настоящий документ соответствует разделу 16 «Требования к разработке эксплуатационной документации» методического документа «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённого приказам ФСТЭК России от 02 июня 2020 г. №76 по 4 уровню доверия.

Таблица 1 – Соответствие документации требованиям доверия

Требования доверия (16.1 Руководство пользователя должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
режимов работы средства	раздел 2 «Условия выполнения программы»
принципов безопасной работы средств	раздел 2 «Условия выполнения программы»
функций и интерфейсов функций средства, доступных каждой роли пользователей	раздел 4 «Функции управления Центра сертификации Aladdin eCA» раздел 5 «Функции управления Центра регистрации Aladdin eRA»
параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их безопасных значений	раздел 3 «Выполнение программы»
типов событий безопасности, связанных с доступными пользователю функциями средства	раздел 6 «Сообщения оператору»
действий после сбоев и ошибок эксплуатации средства	раздел 6 «Сообщения оператору»

Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

[1] Далее по документу – Центр сертификатов доступа, программное средство

[2] Далее по документы – программа, Центр сертификации Aladdin eCA

[3] Дале по документу – программа, Центр регистрации Aladdin eCA

СОДЕРЖАНИЕ

1 НАЗНАЧЕНИЕ ПРОГРАММЫ

1.1 Область применения

Центр сертификатов доступа применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификации при управлении доступом субъектов [1] доступа к объектам [2] доступа в автоматизированной (информационной) системе.

Центр регистрации Aladdin eRA предназначен для формирования и обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов) [3], выпускаемых Центром сертификации Aladdin eCA из состава Центра сертификатов доступа Aladdin eCA CE.

1.2 Состав

Центр сертификатов доступа включает:

- Программный комплекс «Центр сертификации Aladdin Enterprise Certification Authority» (далее по тексту – программа или Центр сертификации Aladdin eCA), состоящий из следующих программных компонентов:
  - Программный компонент «Серверная часть Центра сертификации».

    Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов безопасности цифровых сертификатов) (далее – сертификаты), выпуска и обслуживания сертификатов, приостановки и/или возобновления действия сертификатов, предоставления информации о сертификатах и их статусах.
  - Программный компонент «Клиентская часть Центра сертификации».

    Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра сертификации».
- Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority» (далее по тексту – Центр валидации Aladdin eVA), состоящий из следующих программных компонентов:
  - Программный компонент «Серверная часть Центра валидации».

    Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части предоставления информации о сертификатах и их статусах.
  - Программный компонент «Клиентская часть Центра валидации».

    Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра валидации».

---

[1] Субъект доступа представляет собой одну из сторон информационного взаимодействия, которая инициирует получение и получает доступ. Субъектами доступа могут являться как физические лица (пользователи), так и средства вычислительной техники (устройства), а также вычислительные процессы, инициирующие получение и получающие доступ от имени пользователей, программ, средств вычислительной техники и других программно-аппаратных устройств информационно-телекоммуникационной инфраструктуры.

[2] Объект доступа представляет собой одну из сторон информационного взаимодействия, предоставляющую доступ. Объектами доступа могут являться как средства вычислительной техники (устройства), так и их вычислительные процессы.

[3] Далее по документу – сертификаты.

- Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» (далее по тексту – Центр регистрации Aladdin eRA), состоящий из следующих программных компонентов:
  - Программный компонент «Серверная часть Центра регистрации».

    Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов, выпуска и обслуживания сертификатов.
  - Программный компонент «Клиентская часть Центра регистрации».

    Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации».
- Программное средство «Утилита контроля целостности 2.0» RU.АЛДЕ.02.13.002–09.

  Программное средство предназначена для контроля целостности исполняемых файлов и дистрибутивов программных комплексов из состава Центра сертификатов доступа.

1.3 Основные функции

Центр сертификатов доступа реализует следующие функции, для выполнения которых он предназначен в заданных условиях применения:

- Формирование идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств) (далее по тексту – СВТ) на основе данных, полученных при первичной идентификации непосредственно от пользователей и СВТ через заявку на выпуск сертификатов, либо полученных от доменной службы каталогов или уполномоченных пользователей. Первичная идентификация пользователей и СВТ в программном средстве завершается созданием для них субъектов. Идентификационная информация, необходимая для выпуска сертификатов, представляет собой атрибуты субъекта, значения которых записываются в поля сертификатов, создаваемых для данного субъекта.
- Выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
  - Создание ключевых пар (открытый и закрытый ключи) пользователей и СВТ.

    Создание ключевых пар для пользователей и средств вычислительной техники (устройств) выполняется при формировании для них сертификатов с закрытым ключом (PKCS#12) [1].
  - Формирование сертификатов для пользователей и СВТ.

    В программном средстве реализовано формирование сертификатов для пользователей и СВТ:
    - С закрытым ключом (PKCS#12).
    - На основании запроса PKCS#10 [2].
  - Формирование заявок на выпуск сертификатов для пользователей и СВТ.

    В программном средстве реализовано:
    - Создание заявок пользователями с ролями «Администратор» и «Оператор» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации»

[1] В соответствии с документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1».

[2] В соответствии с документом «RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7».

- Создание заявок пользователем с ролью «Получатель сертификата» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации», включая заявки, создаваемые через программный интерфейс по протоколу WS-Trust X.509v3 Token Enrollment Extensions (WSTEP) [1].
- Создание заявок через программный интерфейс программного компонента «Серверная часть Центра регистрации» по протоколу Simple Certificate Enrollment Protocol (SCEP) [2].
- Автоматическое создание заявок на основании запросов PKCS#10 из локального или сетевого каталога в соответствии с настройками Offline-выпуска.

– Выдача сертификатов для их использования владельцами.

  Выдача сертификатов для их использования владельцами доступна:
  - Путем их экспорта за пределы программного средства пользователями с ролями «Администратор» или «Оператор».
  - Путем их экспорта за пределы программного средства инициатором заявки на выпуск сертификата, если по данной заявке успешно выпущен сертификат.
  - Путем их автоматического экспорта за пределы программного средства в локальный или сетевой каталог в соответствии с настройками Offline-выпуска.

– Централизованное автоматическое (автоматизированное) отслеживание актуальности (с уведомлением владельцев о сроках действия) сертификатов.

  Уведомление владельцев о сроках действия их сертификатов выполняется по электронной почте. По умолчанию программное средство уведомляет владельца сертификата в случае, если срок его действия истекает через 30 суток, через 7 суток или через 1 сутки. В программном средстве доступно формирование шаблонов рассылок уведомлений владельцев о сроках действия их сертификатов. Для каждого шаблона рассылки доступно указание времени, отслеживаемого до окончания действия сертификата, а также текста отправляемого уведомления.

- Выпуск и обслуживание сертификатов центров сертификации инфраструктуры открытых ключей, в том числе:

– Создание, экспорт, импорт и удаление ключевой пары (открытый и закрытый ключи) центра сертификации (корневого и/или подчиненного).

  Создание ключевой пары центра сертификации (корневого и/или подчиненного) выполняется при создании собственного центра сертификации в программном средстве. В программном средстве доступно создание центра сертификации (корневого и/или подчиненного) на основании импортированного контейнера закрытого ключа PKCS #12 центра сертификации, содержащего его ключевую пару. Для центра сертификации доступен экспорт ключевой пары за пределы программного средства, если его ключевая пара уже не экспортирована за пределы программного средства, и для данной ключевой пары при ее создании не был установлен запрет на экспорт. При экспорте ключевая пара центра сертификации удаляется из программного средства. Для центра сертификации, ключевая пара которого экспортирована за пределы программного средства, доступна возможность импорта его ключевой пары в программное средство. Удаление ключевой пары центра сертификации выполняется при удалении данного центра сертификации из программного средства, если его ключевая пара уже не экспортирована за пределы программного средства.

[1] В соответствии с документом «OASIS WS-Trust 1.3. WS-Trust X.509 Token Profile (WSTEP)».

[2] В соответствии с документом «RFC 8894. Simple Certificate Enrolment Protocol».

- Создание, импорт, просмотр, экспорт и удаление корневого (самоподписанного) сертификата центра сертификации.

  Создание корневого (самоподписанного) сертификата центра сертификации выполняется при создании в программном средстве собственного корневого центра сертификации. Импорт корневого (самоподписанного) сертификата центра сертификации выполняется при создании в программном средстве корневого центра сертификации на основании импортированного контейнера закрытого ключа PKCS #12 корневого центра сертификации. В программном средстве доступен просмотр значений полей корневого (самоподписанного) сертификата центра сертификации. Для каждого корневого центра сертификации доступен импорт его самоподписанного сертификата. Удаление корневого (самоподписанного) сертификата центра сертификации выполняется при удалении данного корневого центра сертификации.
- Создание, просмотр, экспорт и удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации.

  Создание запроса на сертификат центра сертификации в вышестоящий центр сертификации выполняется при создании в программном средстве подчиненного центра сертификации. Запрос на сертификат центра сертификации в вышестоящий центр сертификации доступен для просмотра средствами из состава операционной системы (среды функционирования) (далее – ОС). Запрос на сертификат центра сертификации в вышестоящий центр сертификации доступен для экспорта за пределы программного средства. Удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации выполняется при удалении в программном средстве данного подчиненного центра сертификации.
- Создание на основании запроса, импорт, просмотр, экспорт, удаление и отзыв сертификата для подчиненного центра сертификации.

  Создание сертификата для подчиненного центра сертификации на основании запроса выполняется в вышестоящем центре сертификации при подписании запроса на сертификат данного подчиненного центра сертификации. Импорт сертификата для подчиненного центра сертификации выполняется при создании в программном средстве подчиненного центра сертификации на основании импортированного контейнера закрытого ключа PKCS #12 подчиненного центра сертификации. В программном средстве доступен просмотр значений полей созданного сертификата для подчиненного центра сертификации. Сертификат для подчиненного центра сертификации доступен для экспорта за пределы программного средства как отдельно, так и в составе его цепочки сертификатов. Удаление сертификата подчиненного центра сертификации выполняется при удалении данного центра сертификации из программного средства. В вышестоящем центре сертификации, подписавшем запрос на сертификат подчиненного центра сертификации, доступен отзыв сертификата данного подчиненного центра сертификации.

- Приостановка и/или возобновление действия пользователей и СВТ, в том числе:
  - Блокирование, возобновление действия, отзыв и перевыпуск сертификатов.

    Блокирование, возобновление действия и отзыв сертификатов выполняется путем формирования списка (основного и разностного) отозванных сертификатов. В данный список программным средством заносятся заблокированные и отозванные сертификаты. Операция блокирования сертификата обратима путем возобновления действия данного сертификата. Операция отзыва сертификата необратима. В программном средстве доступен повторный выпуск сертификатов пользователей и СВТ на основании ранее использованной идентификационной информации.
  - Формирование, экспорт и публикация списка отозванных сертификатов.

Формирование списка отозванных сертификатов выполняется автоматически с задаваемой пользователем с ролью «Администратор» периодичностью и/или при любом изменении статуса сертификата. В программном средстве доступен экспорт списка отозванных сертификатов. При каждом формировании списка отозванных сертификатов безопасности выполняется его публикация в зарегистрированные точки распространения. В программном средстве доступна публикация списка отозванных сертификатов и сертификатов центров сертификации в точки распространения центров валидации, создаваемых в Центре валидации Aladdin eVA, и точки распространения доменной службы каталогов.

- Предоставление информации о сертификатах центров сертификации, пользователей и СВТ, а также информации об их статусах, в том числе:
  - Формирование и экспорт реестра сертификатов.

    В программном средстве реализовано формирование реестра сертификатов, содержащего значения полей всех созданных сертификатов. При экспорте реестра сертификатов доступен выбор критериев, которым должны соответствовать сертификаты в экспортируемом реестре.
  - Проверка статусов сертификатов на основании данных, опубликованных в точке распространения.

    Программное средство позволяет экспортировать опубликованные списки отозванных сертификатов и сертификаты центров сертификации из точек распространения, реализованных программным средством.
  - Проверка статусов сертификатов в режиме реального времени.

    Программное средство позволяет выполнять проверку статусов сертификатов в режиме реального времени по протоколу Online Certificate Status Protocol (OCSP) [1].

Центр сертификатов доступа выпускает сертификаты в следующих форматах:

- Формат сертификата открытого ключа X.509v3 [2].

  Сертификат включает в себя следующие данные:
  - Версия сертификата.
  - Серийный номер сертификата.
  - Идентификатор алгоритма подписи сертификата.
  - Отличительное имя издателя сертификата.
  - Период действия сертификата.
  - Отличительное имя субъекта.
  - Информация об открытом ключе, включающая алгоритм открытого ключа и сам открытый ключ.
  - Расширения сертификата, включая следующие возможные поля:
    - Идентификатор ключа издателя сертификата.
    - Идентификатор ключа субъекта.
    - Идентификаторы использования ключа.
    - Политики сертификата.
    - Альтернативное имя субъекта.
    - Альтернативное имя издателя сертификата.
    - Базовые ограничения.

[1] В соответствии с документом «RFC 6960. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP».

[2] Формат определяется документом «ITU-T Recommendation X.509 (10/2019). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks».

        - Точки распространения списков отзыва.
        - Доступ к информации о центрах сертификации.
        - Идентификаторы расширенного использования ключа.
    - Подпись сертификата.
- Формат списка отозванных сертификатов безопасности (CRL) [1].

  Список отозванных сертификатов включает в себя следующие данные:
  - Версия CRL.
  - Отличительное имя издателя CRL.
  - Дата и время издания текущего CRL.
  - Дата и время издания следующего CRL.
  - Расширения CRL, включая следующие возможные поля:
    - Идентификатор ключа издателя CRL.
    - Номер CRL.
  - Перечень отозванных сертификатов, где для каждого сертификата указаны:
    - Серийный номер.
    - Дата и время отзыва.
    - Причина отзыва (может отсутствовать).
  - Алгоритм подписи CRL.
  - Подпись CRL.
- Формат контейнера закрытого ключа PKCS #12 [2].

  Контейнеры закрытого ключа включают в себя следующие данные:
  - Цепочка сертификатов владельца закрытого ключа.
  - Закрытый ключ.

Центр сертификатов доступа реализовывает следующие криптографические алгоритмы:

- Алгоритмы генерации ключевой пары:
  - RSA с длинами ключей 1024, 1536, 2048, 3072, 4096, 6144 и 8192 бит.
  - ECDSA с длинами ключей 256, 384 и 521 бит.
  - ГОСТ Р 34.10-2012 с ключом 256 или 512 бит.
- Алгоритмы генерации цифровой подписи:
  - RSA PKCS#1 Ver 1.5 (длины ключей: 1024, 1536, 2048, 3072, 4096, 6144 и 8192 бит; хэш-алгоритмы: SHA256, SHA384, SHA512).
  - ECDSA (длины ключей: 256, 384, 521 бит; хэш-алгоритмы: SHA256, SHA384, SHA512).
  - ГОСТ Р 34.10-2012 с ключом 256 или 512 бит (хэш-алгоритм: ГОСТ Р 34.11-2012 с длиной хэш-кода 256 или 512 бит).

[1] Формат определяется документом «ITU-T Recommendation X.509 (10/2019). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks».

[2] Формат определяется документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1»

1.4 Полномочия оператора

Доступные действия для Оператора Центра сертификации Aladdin eCA:

- Создание сертификатов доступа для ограниченного набора субъектов ресурсных систем.
- Просмотр списка сертификатов доступа для ограниченного набора субъектов ресурсных систем.
- Экспорт списка выпущенных сертификатов для ограниченного набора субъектов ресурсных систем.
- Скачивание сертификата доступа для ограниченного набора доступных субъектов ресурсных систем.
- Изготовление и экспорт документа, содержащего значения полей сертификата, (сертификат на бумажном носителе) для ограниченного набора доступных субъектов ресурсных систем.
- Скачивание сертификата доступа субъекта в контейнере #pkcs12 для ограниченного набора субъектов ресурсных систем
- Скачивание цепочки сертифи.катов для ограниченного набора субъектов ресурсных систем.
- Управление статусом сертификата доступа субъекта для ограниченного набора субъектов ресурсных систем.
- Просмотр ограниченного списка субъектов ресурсных систем.
- Просмотр списка ограниченного набора зарегистрированных ресурсных систем.
- Обновление ограниченного набора субъектов ресурсных систем.
- Просмотр ограниченного набора идентификаторов расширенного использования ключа.
- Просмотр ограниченного количества шаблонов.

> **Внимание! Оператору Центра сертификации Aladdin eCA доступны субъекты (в том числе и выпущенные для них сертификаты) и шаблоны, на которые ему предоставлены полномочия в соответствии с назначенными уполномоченным пользователем Центра сертификации Aladdin eCA правилами доступа.**

Доступные действия для Оператора Центра регистрации Aladdin eRA:

- Просмотр информации о своих заявках на выпуск сертификатов.
- Просмотр информации об ограниченном наборе чужих заявок на выпуск сертификатов.
- Создание заявок на выпуск сертификатов для субъекта своей учётной записи.
- Создание заявок на выпуск сертификатов для субъекта любой учётной записи.
- Скачивание файла запроса на сертификат для своих заявок на выпуск сертификата по запросу.
- Скачивание файла запроса на сертификат для ограниченного набора чужих заявок на выпуск сертификата по запросу.
- Скачивание сертификата для своих заявок.
- Скачивание сертификата для ограниченного набора чужих заявок.
- Отзыв сертификатов для своих заявок.
- Отзыв сертификатов для ограниченного набора чужих заявок.
- Скачивание цепочки сертификатов для своих заявок.
- Скачивание цепочки сертификатов для ограниченного набора чужих заявок.
- Скачивание контейнера закрытого ключа PKCS#12 для своих заявок.
- Скачивание контейнера закрытого ключа PKCS#12 для ограниченного набора чужих заявок.
- Импорт сертификата на ключевой носитель для своих заявок.
- Импорт сертификата на ключевой носитель для ограниченного набора чужих заявок.
- Скачивание цепочки сертификатов издателя для своих заявок.
- Скачивание цепочки сертификатов издателя для ограниченного набора чужих заявок.
- Скачивание списка отозванных сертификатов.
- Отмена своих заявок.
- Обработка ограниченного набора заявок.
- Просмотр ограниченного количества записей журнала событий.

- Экспорт ограниченного количества записей журнала событий.

Внимание! **Оператор Центра регистрации Aladdin eCA может создать заявку на выпуск сертификата для любого субъекта. Создание заявок на выпуск сертификатов для субъектов ресурсных систем может быть выполнена только по шаблонам, назначенным данным субъектам на основе правил выпуска. Оператор может обрабатывать заявки на выпуск сертификатов (в том числе и управлять выпущенными по ним сертификатами) для субъектов, на которые ему предоставлены полномочия в соответствии с назначенными уполномоченным пользователем Центра сертификации Aladdin eCA правилами доступа.**

1.5 Уровень подготовки оператора

Операторы Центра сертификации Aladdin eCA и Цента регистрации Aladdin eRA должны иметь навыки в работе с применением технических средств уровня семейства операционных систем Windows и семейства операционных систем Linux.

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Поддерживаемые браузеры

Работа с Центром сертификации Aladdin eCA и Центром регистрации Aladdin eRA поддерживается через веб-браузеры операционных систем РЕД ОС, Astra Linux Special Edition, Альт Сервер и ОС «Platform V SberLinux OS Server».

2.2 Поддерживаемые ключевые носители

Поддерживаемые модели электронных ключей (ключевых носителей):

- JaCarta:
  - JaCarta PKI.
  - JaCarta PRO.
  - JaCarta-2 PKI/ГОСТ.
  - JaCarta-2 ГОСТ.
  - JaCarta-3.
- Рутокен [1]:
  - Рутокен ЭЦП 3.0.
  - Рутокен ЭЦП 2.0.
  - Рутокен ЭЦП 2.0 Flash.
  - Рутокен ЭЦП PKI.

Для работы с ключевыми носителями JaCarta используется приложение JC-WebClient. Рекомендуется использовать приложение последней версии для 64-битных систем.

Для работы с ключевыми носителями Рутокен используется ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин».

Порядок установки JC-WebClient и ПО «Рутокен Плагин» приведен в Приложении 3.

2.3 Режим функционирования программы

Центр сертификации Aladdin eCA и Центр регистрации Aladdin eRA функционируют в следующих режимах:

- Штатный режим, при котором программа должна исправно функционировать, обеспечивая возможность круглосуточного выполнение задач и функций в полном объёме.
- Сервисный режим, необходимый для проведения обслуживания (обновления программы).

Основным режимом функционирования Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA является штатный режим.

Аварийный режим работы, при отказах/сбоях серверного общесистемного и специального программного обеспечения и оборудования, не предусматривается.

[1] Возможность использования ключевых носителей Рутокен может быть ограничена лицензией.

2.4 Доступ к программе

Для получения доступа к Центру сертификации Aladdin eCA и Центру регистрации Aladdin eRA необходимо обратиться к уполномоченному лицу, исполняющему обязанности администратора для:

- Создания новой учётной записи Оператора и выпуска сертификата в контейнере p12 для созданной учётной записи.
- Передачи сертификата лицу, исполняющему обязанности Оператора, в контейнере p12 с атрибутом безопасности (паролем от контейнера) для дальнейшей аутентификации на веб-серверах Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA.

2.5 Принципы безопасной работы программы

К основным принципам безопасной работы Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA относятся:

- Выполнение ограничений по эксплуатации программного средства, приведённых в разделе 2 «Условия выполнения программы» настоящего документа.
- Контроль физической сохранности средств вычислительной техники с установленным Средством двухфакторной аутентификации.
- Сохранение в секрете пароля (PIN-кода) пользователя.
- Исключение доступа посторонних лиц к персональному идентификатору.

3 ВЫПОЛНЕНИЕ ПРОГРАММЫ

3.1 Запуск программы

Запуск служб серверов Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA осуществляет администратор на сервере, где развёрнут соответствующий компонент.

Оператору предоставляется доступ к клиентским частям посредством веб-интерфейса. Для запуска клиентской части Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA:

- Запустите веб-браузер.
- В адресной строке веб-браузера введите IP-адрес или полное доменное имя сервера, на котором соответственно установлен Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA (например: https://172.22.5.21).
- Выберите сертификат доступа аутентифицирующегося пользователя.

3.2 Подключение к веб-интерфейсу

Веб-интерфейс представляется собой графический интерфейс в виде совокупности динамических веб-страниц, отображаемых в веб-браузере. Веб-интерфейсы реализованы клиентскими компонентами Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA и предназначены для управления серверными компонентами Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA (выполнения доступных пользователю в рамках его полномочий действий).

Подключение к веб-интерфейсу Центра сертификации Aladdin и Центра регистрации Aladdin eRA выполняется из веб-браузера удаленно по сети передачи данных с выделенного компьютера.

Канал управления является защищенным — организован по протоколу HTTPS/TLS с двусторонней аутентификацией и шифрованием передаваемых данных. Идентификация и аутентификация Операторов выполняется по предъявленному сертификату, который должен быть предварительно установлен в хранилище веб-браузера или хранилище сертификатов используемой ОС.

3.2.1 Установка сертификата оператора

Полученный Оператором контейнер сертификата доступа для аутентификации на веб-сервере Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA необходимо перенести любым удобным способом на жёсткий диск компьютера, с которого выполняется подключение к веб-интерфейсу, для его дальнейшей установки в хранилище сертификатов браузера для сохранения информации о доверенных сертификатах с целью успешного подключения к серверу на клиентской стороне.

Процесс установки сертификата представлен на примере веб-браузера Firefox:

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

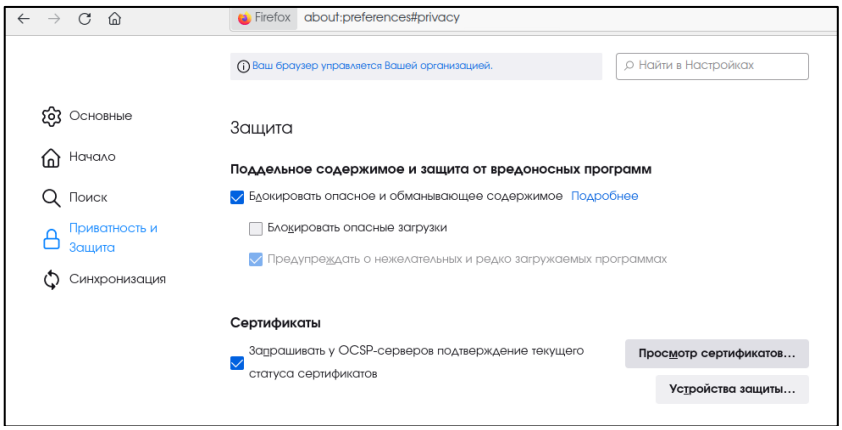


Рисунок 1 – Окно настроек браузера

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

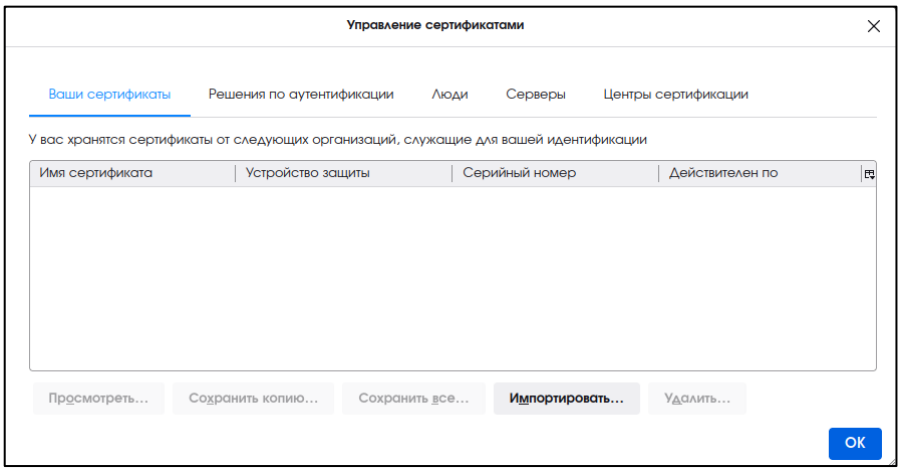


Рисунок 2 – Окно управления сертификатами

- Выберите предварительно подготовленный файл сертификата, подписанный Центром сертификации Aladdin eCA, который будет принимать обработанные Центром сертификации Aladdin eCA или Центра регистрации Aladdin eRA запросы на сертификаты доступа и находящийся в списке разрешённых Издателей. Нажмите кнопку <Открыть> (см. Рисунок 3).

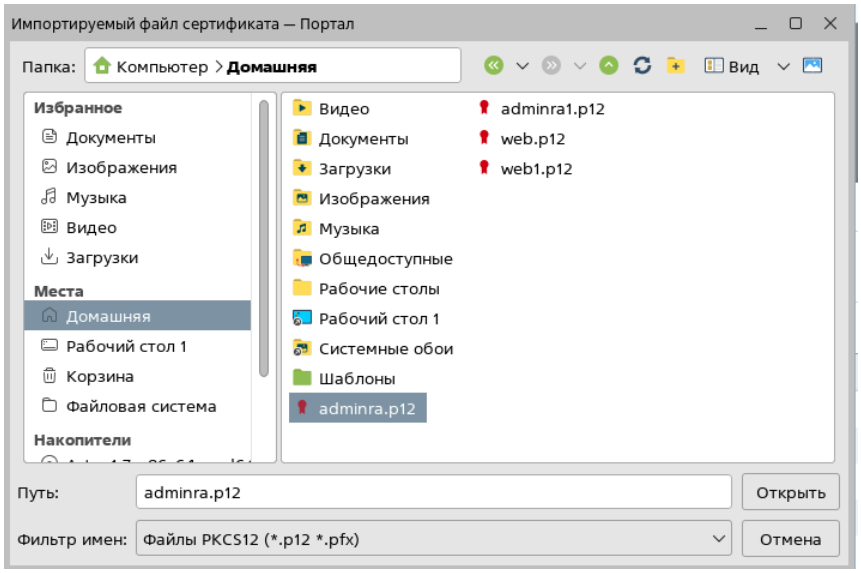


Рисунок 3 – Окно выбора импортируемого файла сертификата

- Введите PIN-код сертификата доступа в открывшемся окне и нажмите кнопку **<OK>** (см. Рисунок 4).

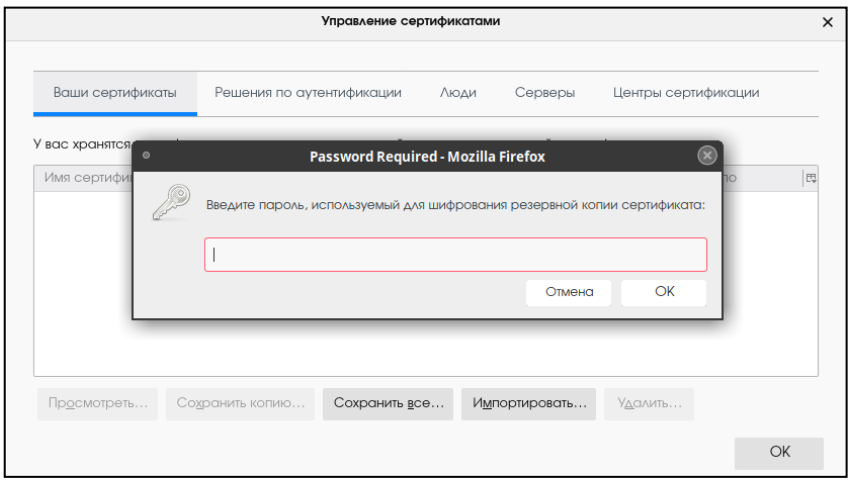


Рисунок 4 – Окно ввода PIN-кода сертификата

Внимание! PIN-код сертификата устанавливается администратором Центра сертификации Aladdin eCA при выпуске сертификата доступа.

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 5). Нажать кнопку **<OK>**.

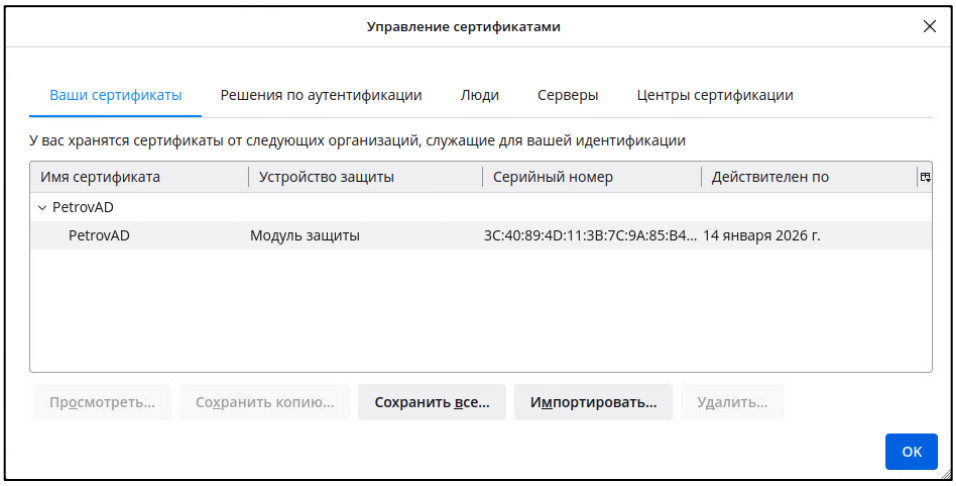


Рисунок 5 – Окно «Управление сертификатами»

3.2.2 Подключение к веб-интерфейсу

Порядок подключения к веб-интерфейсу:

- Запустите веб-браузер и в адресной строке введите IP-адрес или доменное имя компьютера, на котором установлен соответственно Центр сертификации Aladdin eCA или Центр регистрации Aladdin eRA (например, `https://172.22.5.21` или `https://sub02.presale.aeca)`.

- Для безопасного доверенного соединения при обращении к серверу Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA используйте доменное имя, указанное в атрибуте сертификата веб-сервера Subject alternative name (SAN) и соответственно указанное в конфигурационном файле `/etc/hosts/` сервера.

- В открывшемся окне выберите сертификат для аутентификации в Центре сертификации Aladdin eCA или Центр регистрации Aladdin eRA (см.). Нажмите кнопку **<OK>**.

- Далее на открывшейся странице с предупреждением системы безопасности нажмите кнопку **<Дополнительно>**, примите риск и продолжите подключение.

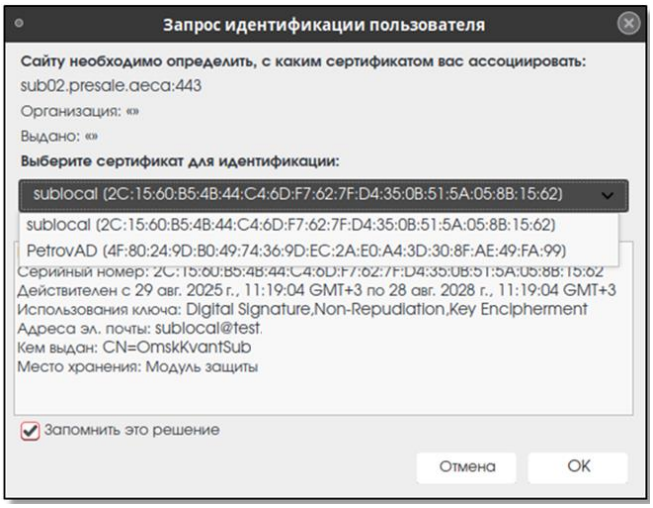


Рисунок 6 – Окно выбора сертификата для аутентификации

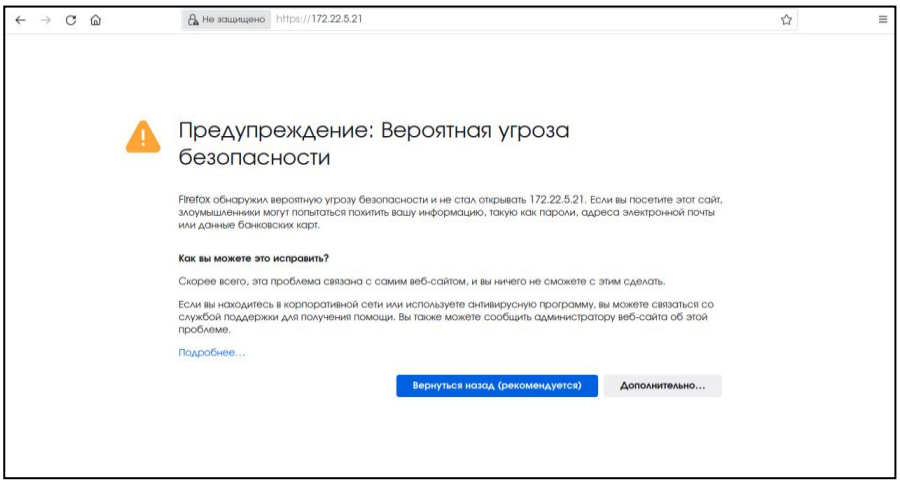


Рисунок 7 – Страница с предупреждением системы безопасности

В результате вы подключитесь соответственно к веб-интерфейсу Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA.

При подключении к веб-интерфейсу Центра сертификации Aladdin eCA аутентификация по сертификату выполняется автоматически.

При подключении к веб-интерфейсу Центра регистрации Aladdin eRA пройдите аутентификацию, нажав в окне авторизации кнопку **<Сертификат>**.

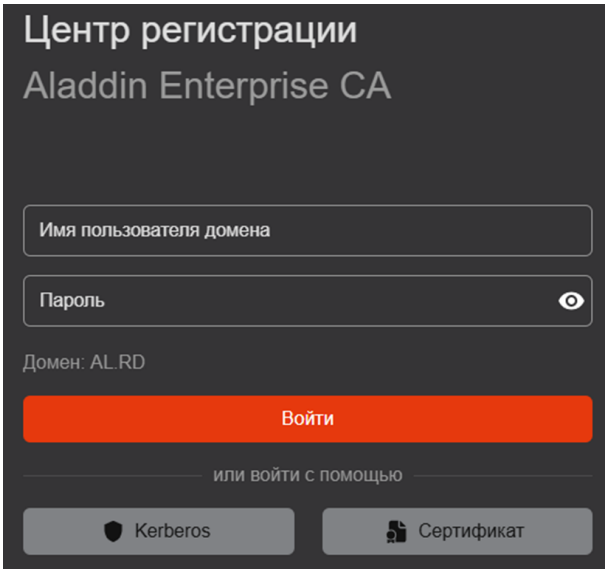


Рисунок 8 – Окно авторизации

В случае отказа в доступе к веб-интерфейсу Оператор будет уведомлен сообщением об ошибке. Возможные причины отказа:

- сертификат доступа пользователя не импортирован в доверенное хранилище браузера;
- отсутствие издателя сертификата доступа, импортированного в доверенное хранилище браузера, в списке разрешённых издателей веб-сервера;
- невозможно выполнить авторизацию с использованием сертификата. Сертификат не привязан к пользователю;
- остановка работы служб на веб-сервере;
- срок действия сертификата доступа истёк;
- действия сертификата было приостановлено или сертификат отозван;
- аккаунт заблокирован;
- достигнуто предельное число сессий аккаунта.

В случае отказа в доступе обратитесь соответственно к администратору Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA.

3.2.3 Аутентификация с использованием сертификата на ключевом носителе

3.2.3.1 Первичная настройка СВТ для двухфакторной аутентификации оператора по сертификату на ключевом носителе

Для настройки сначала выполните установку Единого Клиента JaCarta (см. подраздел 3.2.3.2), а затем выполните настройку браузера (настройку Firefox см. в подразделе 3.2.3.3, настройку Chromium в зависимости от ОС см. в подразделах 3.2.3.4 и 3.2.3.5).

3.2.3.2 Установка Единого Клиента JaCarta

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

```
cd …/…/…
```

  - Установите Единый Клиент JaCarta, выполнив команду:

```
bash install.sh
```

Подробное описание процедуры установки Единого Клиента JaCarta приведено в разделе 4 «Единый Клиент JaCarta. Руководства администратора».

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

```
apt install libnss3-tools
```

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

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

3.2.3.3 Настройка веб-браузера Firefox

Выполните настройку браузера **Firefox** в следующем порядке:

- откройте **Настройки -> Приватность и защита -> Сертификаты -> Устройства защиты**;
- в диалоговом окне нажмите кнопку **<Загрузить>**;
- в окне загрузки драйвера нажмите кнопку **<Обзор>** и выберите файл модуля `/lib64/libjcPKCS11-2.so` (см. Рисунок 9) и подтвердите загрузку модуля, нажав кнопку **<ОК>**;

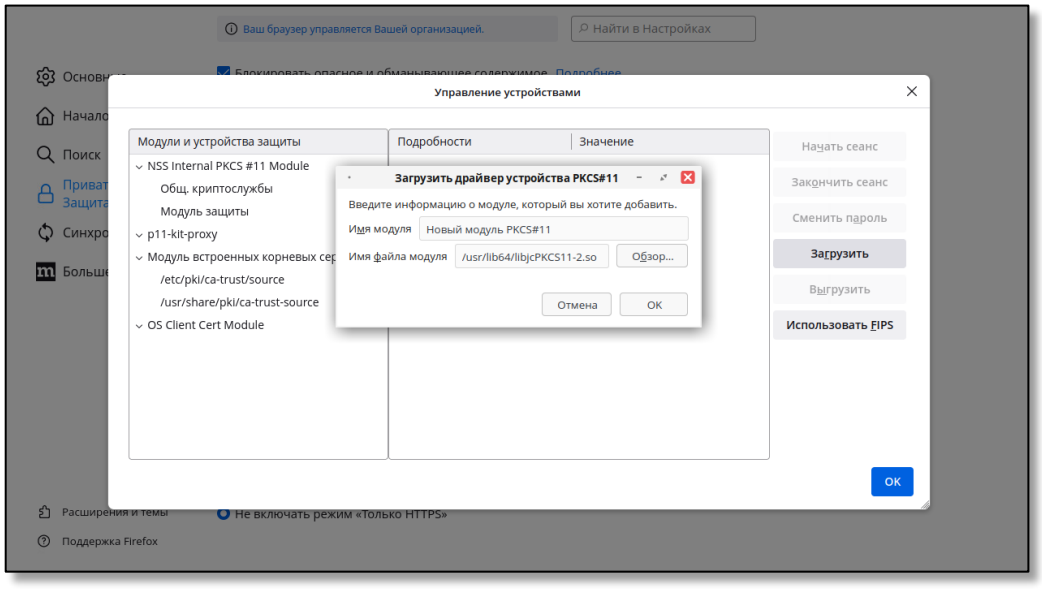


Рисунок 9 – Настройка браузера Firefox

– перезапустите веб-браузер.

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

Выполните настройку браузера **Chromium** в следующем порядке:

- удалите каталог локальной библиотеки сертификатов, выполнив команду:

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

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

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

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

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

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

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /usr/lib64/libjcPKCS11-2.so
```

- перезапустите браузер.

3.2.3.5 Настройка веб-браузера Chromium для Astra Linux Special Edition-

Выполните настройку браузера **Chromium** в следующем порядке:

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

```
modutil -dbdir sql:.pki/nssdb/ -add "JaCarta" -libfile /lib/libjcPKCS11-2.so
```

- перезапустите браузер.

3.2.3.6 Двухфакторная аутентификации оператора по сертификату на ключевом носителе

Полученный Оператором ключевой носитель с записанным на нём сертификатом доступа для аутентификации на веб-сервере Центра сертификации Aladdin eCA или Центра регистрации Aladdin eRA необходимо подключить в USB-порт предварительного настроенного средства вычислительной техники – рабочего места Оператора для его дальнейшей аутентификации с целью успешного подключения к серверу на клиентской стороне.

- Запустите веб-браузер и в адресной строке введите IP-адрес или доменное имя компьютера, на котором установлен соответственно Центр сертификации Aladdin eCA или Центр регистрации Aladdin eRA (например, `https://172.22.5.21 или https://sub02.presale.aeca`).
- В появившемся окне введите PIN-код ключевого носителя.

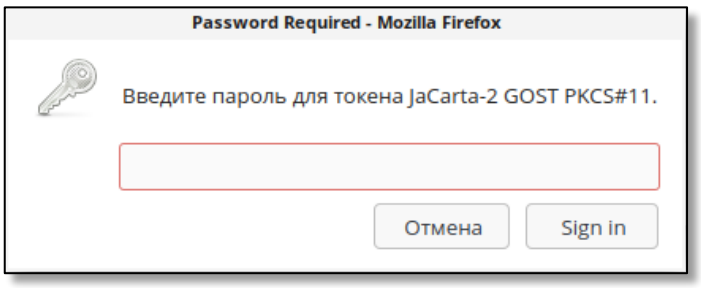


Рисунок 10 – Окно ввода PIN-кода ключевого носителя

- В появившемся окне выберите сертификат с подключенного ключевого носителя.

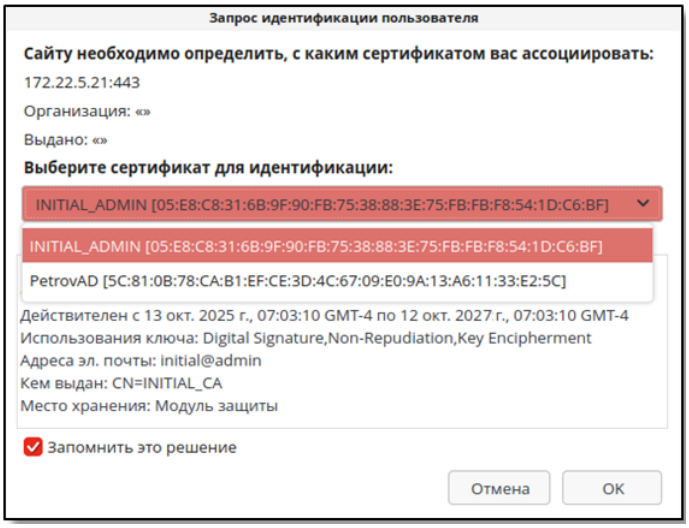


Рисунок 11 – Окно выбора сертификата пользователя для аутентификации на сервере

Внимание! Время действия токена доступа – 3 минуты. Время действия токена обновления – 24 часа, то есть по истечению времени действия токена обновления будет требоваться повторная аутентификация пользователя для доступа к серверу Центра сертификации.

4 ФУНКЦИИ УПРАВЛЕНИЯ ЦЕНТРА СЕРТИФИКАЦИИ ALADDIN ECA

4.1 Описание верхней панели

Верхняя панель (см. Рисунок 12) Центра сертификации фиксирована и отображается на любом шаге или переходе между вкладками.

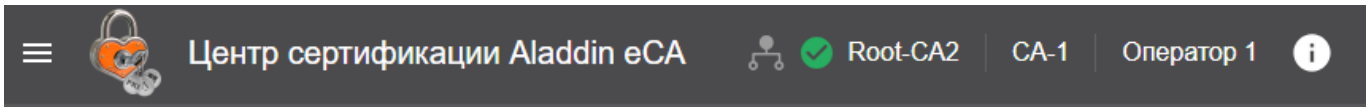


Рисунок 12 – Верхняя панель окна «Центра сертификации»

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.

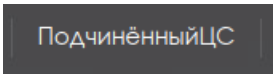
  При отсутствии ошибок и предупреждений отображается активный статус:
  - активный  . При наведении курсора отображается всплывающее сообщение «Активный»;

  Индикатор «треугольник с восклицательным знаком» присутствует в следующих случаях:
  - истёк срок действия сертификата текущего активного ЦС  . При наведении курсора отображается всплывающее сообщение «Истек срок действия сертификата ЦС»;
  - истекает[1] срок действия сертификата текущего активного ЦС  . При наведении курсора отображается всплывающее сообщение «Истекает срок действия сертификата ЦС»;
  - закрытый ключ ЦС недоступен[2]  . При наведении курсора отображается всплывающее сообщение «Закрытый ключ центра сертификации недоступен».
  - истёк срок действия лицензии  . При наведении курсора отображается всплывающее сообщение «Истек срок действия лицензии»;

[1] До истечения остаётся менее 90 дней.

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

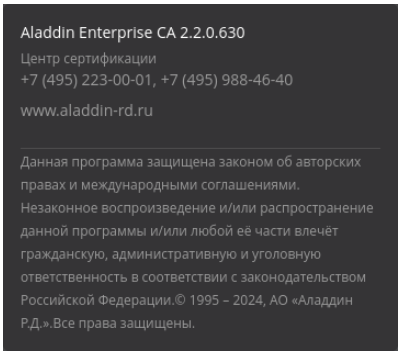
- достигнуто лицензионное ограничение на количество субъектов с действующими сертификатами  . При наведении курсора отображается всплывающее сообщение «Достигнуто предельное количество субъектов с действующими сертификатами по лицензии».

- 

- отображаемое имя текущего активного ЦС;

- 

- текущая авторизация учётной записи пользователя;

- 

- сведения о текущей версии программного компонента, контактная информация разработчика.

4.2 Описание боковой панели

В зависимости от ширины окна браузера боковая панель может:

- либо быть закрепленной и отображаться на любом шаге или переходе между разделами (при ширине окна браузера более или равной 1200px). При этом боковая панель отображается в полном (см. Рисунок 13) или компактном (см. Рисунок 14) виде. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели;
- либо быть скрытой и отображаться только после нажатия на кнопку  на верней панели, которая отображается только в данном режиме (при ширине окна браузера менее 1200px).

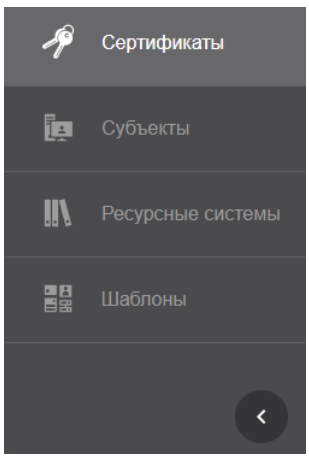


Рисунок 13 – Полный вид боковой панели

Рисунок 14 – Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции программы, доступные Оператору, и созданы для организации управления выпуском и жизненным циклом сертификатов доступа:

- Раздел «Сертификаты» – в данном разделе возможно:
  - посмотреть список всех выпущенных сертификатов субъектов, издателем которых является активный ЦС, с отображением статуса сертификата, срока действия, типа субъекта, имени субъекта и серийного номера сертификата;

- произвести поиск выпущенных сертификатов по имени субъекта или серийному номеру;
- отозвать или приостановить действие выпущенного сертификата субъекта;
- посмотреть карточку выпущенного сертификата субъекта;
- скачать сертификат субъекта в формате .pem;
- скачать цепочку сертификатов;
- скачать бумажный сертификат (файл, содержащий сведения из сертификата);
- скачать список выпущенных сертификатов в формате .csv;
- применить массовые операции к выбранным сертификатам (отзыв, приостановка, возобновление);

- Раздел «Субъекты» – в данном разделе возможно:
  - произвести поиск субъекта по его имени (или части имени);
  - обновить список групп и субъектов;
  - посмотреть организационные группы субъектов локальной и подключенных ресурсных систем;
  - посмотреть существующие субъекты;
  - выпустить сертификат с закрытым ключом PKCS#12 для субъекта;
  - выпустить сертификат на основании запроса для субъекта;
  - выпустить сертификат на ключевом носителе для субъекта;
  - посмотреть все выпущенные сертификаты для каждого субъекта;
  - создать учётную запись для субъекта из группы «Users»;
  - посмотреть карточку субъекта;
  - опубликовать сертификат субъекта в ресурсную систему;

- Вкладка «Ресурсная система» – на данной вкладке возможно обновить список субъектов ресурсной системы и их данных в ручном режиме.
- Вкладка «Шаблоны», доступная Оператору только при наличии у него доступа к шаблонам, – на данной вкладке возможно просмотреть шаблоны, доступные Оператору для использования при создании сертификатов.

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

4.3 Раздел «Сертификаты»

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

Раздел «Сертификаты» обеспечивает просмотр и управление сертификатами субъектов в соответствии с правами учётной записи Оператора. Авторизованному Оператору доступны только сертификаты тех субъектов, на которые ему прямо или косвенно[1] предоставлены полномочия в соответствии с назначенными правилами доступа.

Переход на экран управления Центра сертификации осуществляется по выбору раздела «Сертификаты» бокового меню, расположенного слева на главном экране (см. Рисунок 13).

На данном экране отображаются все созданные сертификаты субъектов (см. Рисунок 15).

[1] Путем наследования от группы безопасности куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

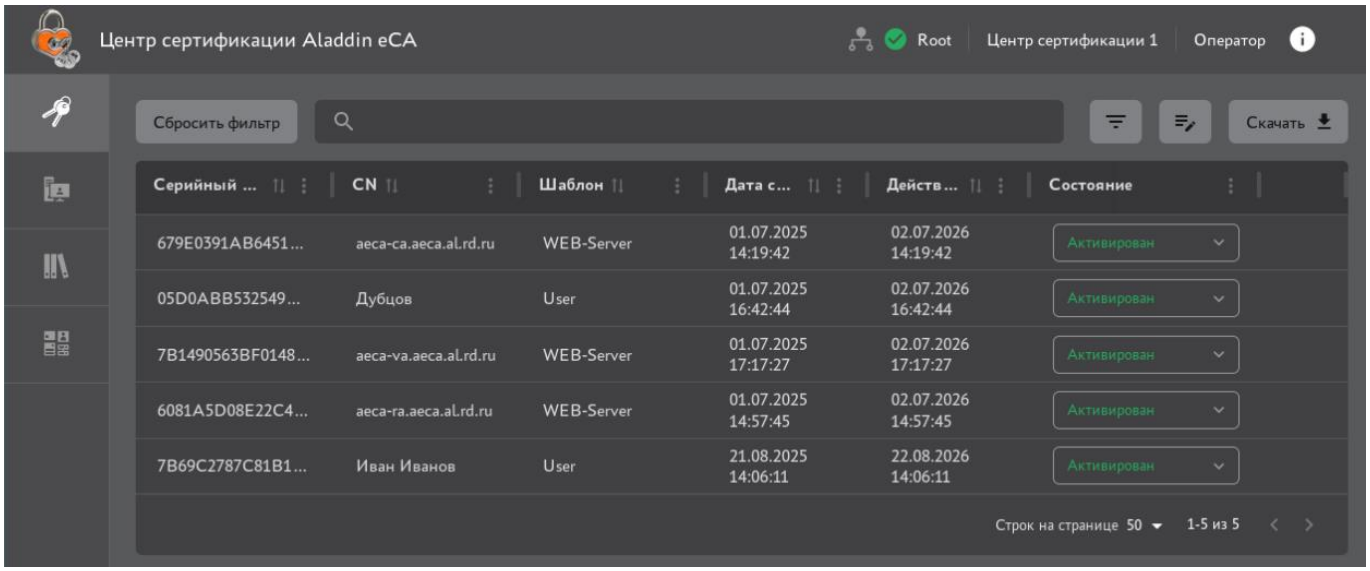


Рисунок 15 - Экран раздела меню «Сертификаты»

- На экране раздела «Сертификаты» отображены информационные элементы (табличные поля):
  - серийный номер сертификата;
  - имя субъекта (CN);
  - тип шаблона сертификата (шаблон);
  - дата выпуска сертификата;
  - дата срока окончания действия сертификата (действителен до);
  - текущий статус сертификата (состояние).
- Доступны следующие операции по работе с сертификатами:
  - поиск выпущенных сертификатов;
  - сортировка сертификатов;
  - скачивание сертификатов;
  - скачивание бумажного сертификата (файл, содержащий сведения из сертификата).
  - изменение статуса сертификатов в формате .pem;
  - просмотр списка сертификатов с заданными критериями;
  - сброс всех применённых фильтров или выборочная отмена выбранного фильтра;
  - просмотр карточки сертификата;
  - экспорт списка выпущенных сертификатов с атрибутами;
  - массовые операции с выпущенными сертификатами.
- Все созданные сертификаты субъектов на экране раздела отображаются в виде таблицы с пагинацией.

4.3.1 Поиск сертификатов

Строка поиска (см. Рисунок 16) предназначена для поиска сертификатов по имени (поле Common Name), альтернативному имени субъекта (поле SubjectAltName) и серийному номеру сертификата (поле Serial Number). Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

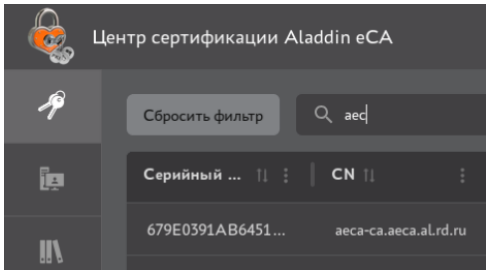


Рисунок 16 – Поисковая строка в разделе «Сертификаты»

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

4.3.2 Сортировка сертификатов

Средства сортировки выпущенных сертификатов представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 17):

- «Серийный номер» – сортировка осуществляется в порядке возрастания или убывания значения;
- «CN» – сортировка осуществляется в алфавитном порядке;
- «Шаблон» – осуществляется группировка по типу шаблона;
- «Дата создания», «Действителен до» – сортировка осуществляется в порядке возрастания или убывания значения даты.

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

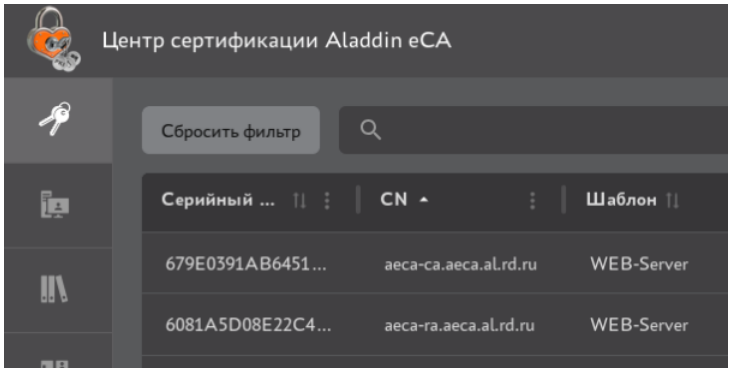


Рисунок 17 – Сортировка сертификатов

Также отобразить в определённом порядке список сертификатов (отсортировать) в колонке возможно по нажатию кнопки **<Действия в колонке>**, выбрав и нажав в раскрывшемся меню «Сортировать...» (см. Рисунок 19).

4.3.3 Фильтрация сертификатов

4.3.3.1 Применение фильтров

Для выборочного просмотра сертификатов на экране раздела «Сертификаты» возможно применение фильтров. Для отображения параметров фильтрации для всех колонок таблицы нажмите кнопку **<Фильтр>** , заголовки колонок экранной таблицы будут дополнены полями фильтра для каждой колонки (см. Рисунок 18):

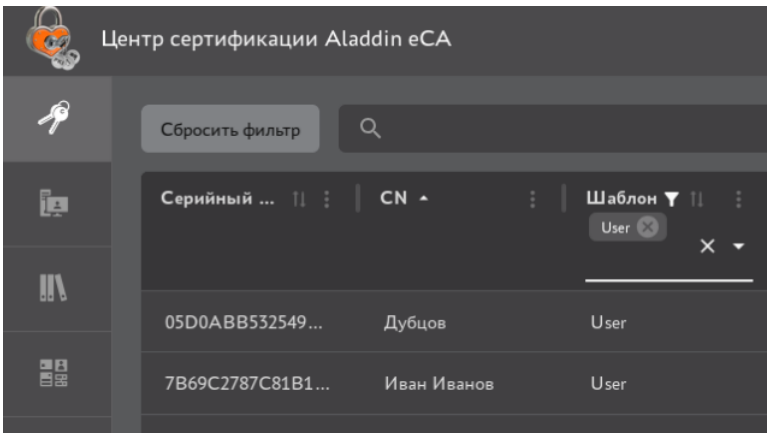


Рисунок 18 – Фильтры заголовков экранной таблицы

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

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

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

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

4.3.3.2 Сброс применённых фильтров

Для очистки применённых фильтров для каждого заголовка колонки нажмите кнопку  **<Действия в колонке>** и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 19);

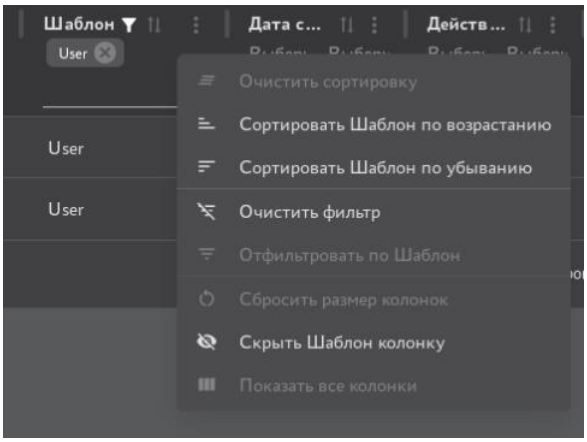
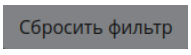


Рисунок 19 – Кнопка <Очистить> фильтр

Для полной отмены всех применённых фильтров по всем колонкам воспользуйтесь кнопкой **<Сбросить фильтр>** 

на экране раздела «Сертификаты».

4.3.4 Скачивание сертификатов

Для скачивания наведите указатель мыши на выбранный сертификат в экранной таблице, нажмите появившуюся кнопку  (см. Рисунок 15) и в раскрывшемся подменю выберите пункт **<Скачать сертификат>** или **<Скачать цепочку>** в формате .pem (см. Рисунок 20).

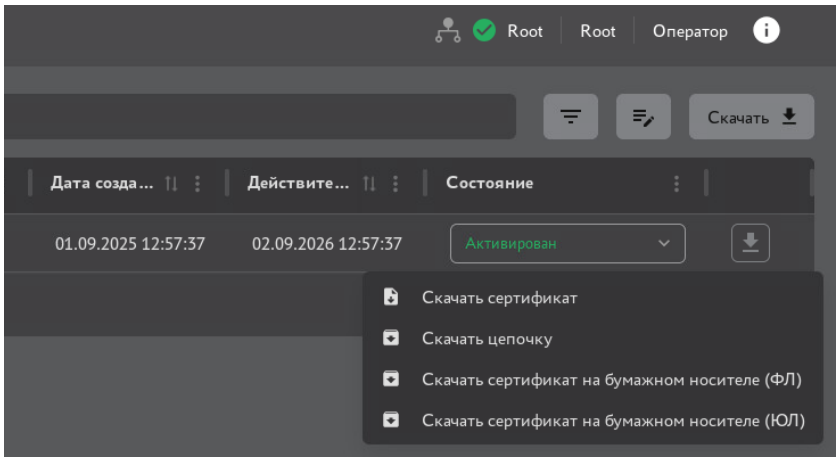


Рисунок 20 – Скачивание сертификата

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

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

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

4.3.5 Статус сертификатов

Возможные варианты состояния и доступные действия над сертификатами в зависимости от состояния приведены в таблице ниже (Таблица 2).

Таблица 2 – Доступные действия над сертификатами в зависимости от состояния

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

Смена состояния сертификата производится посредством выбора нужного значения из выпадающего меню при выделении строки сертификата (см. Рисунок 21).

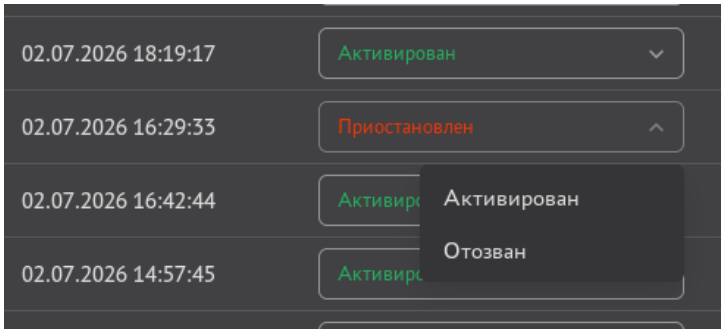


Рисунок 21 – Выпадающее меню смены состояния сертификата

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 22)

Внимание! Если достигнуто предельное количество субъектов с действующими сертификатами в соответствии с лицензией, при попытке активации сертификата субъекта, у которого отсутствуют действующие сертификаты, будет отображаться сообщение об ошибке «Лицензионные ограничения не позволяют активировать данный сертификат. Достигнуто предельное количество субъектов с действующими сертификатами».

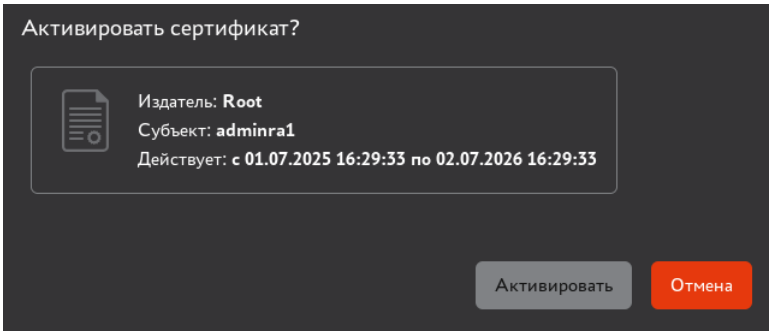


Рисунок 22 – Окно активации сертификата

- приостановка действия сертификата (см. Рисунок 23):

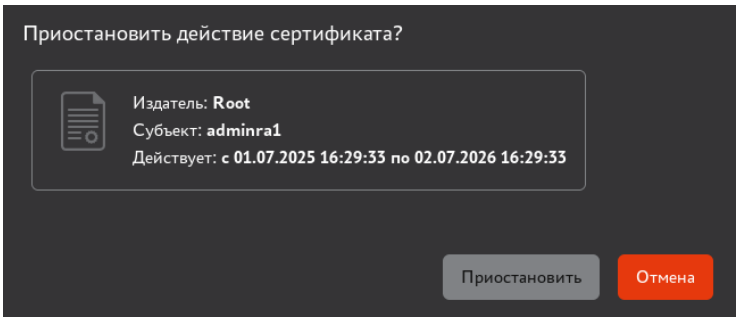


Рисунок 23 – Окно приостановки действия сертификата

- отзыв (см. Рисунок 24);

ВНИМАНИЕ! Данную операцию нельзя отменить.

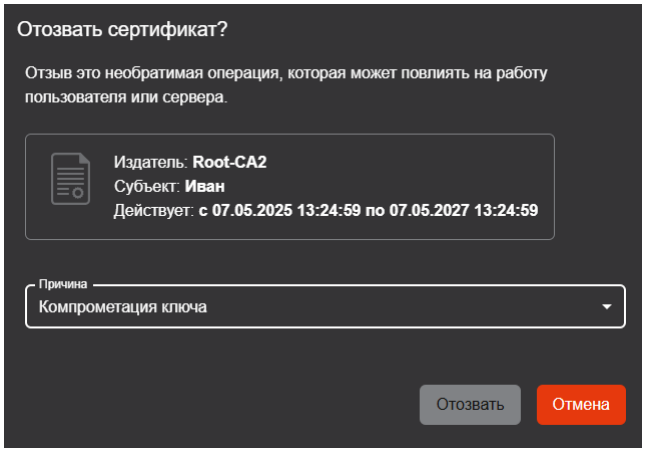


Рисунок 24 – Окно отзыва сертификата

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

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

4.3.6 Карточка сертификата

Просмотр данных сертификата возможен посредством страницы «Карточка сертификата».

Переход к экрану «Карточка сертификата» (см. Рисунок 25) осуществляется при нажатии на строку сертификата таблицы главного экрана раздела «Сертификаты» (см. Рисунок 15).

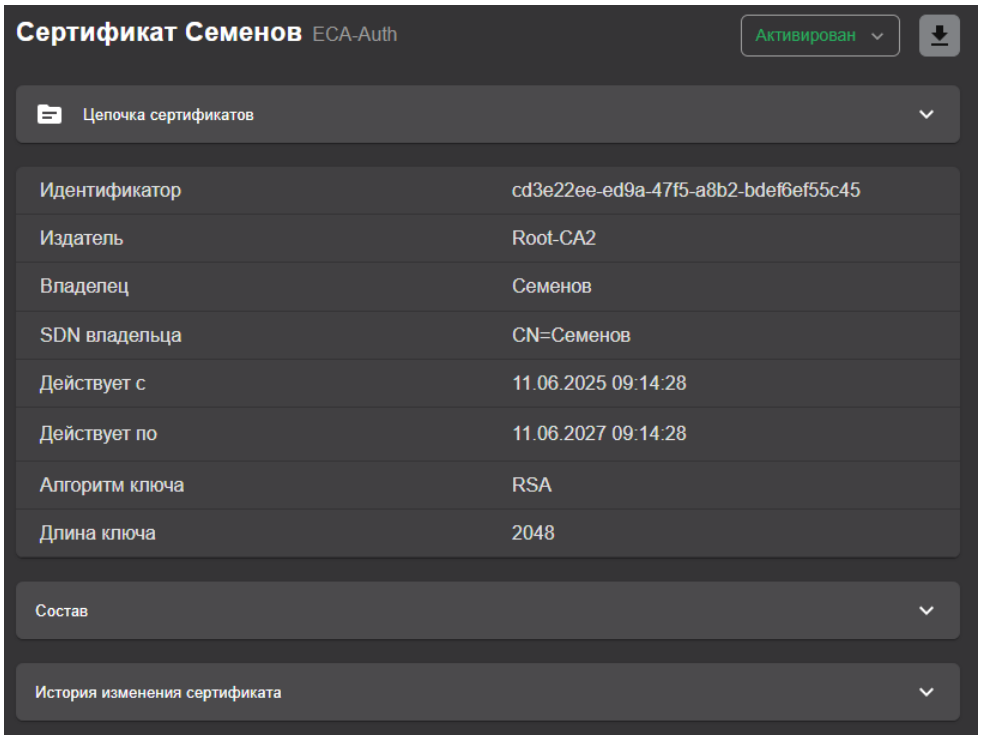


Рисунок 25 – Окно «Карточка сертификата»

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

Для изменения статуса сертификата выбрать из выпадающего списка действие 

в соответствие с таблицей выше (Таблица 2).

> **Внимание! Если достигнуто предельное количество субъектов с действующими сертификатами в соответствии с лицензией, при попытке активации сертификата субъекта, у которого отсутствуют действующие сертификаты, будет отображаться сообщение об ошибке «Лицензионные ограничения не позволяют активировать данный сертификат. Достигнуто предельное количество субъектов с действующими сертификатами».**

Для скачивания сертификата нажмите кнопку  и во всплывающем меню (см. Рисунок 26) выберите **<Скачать сертификат>** субъекта или **<Скачать цепочку сертификатов>**.

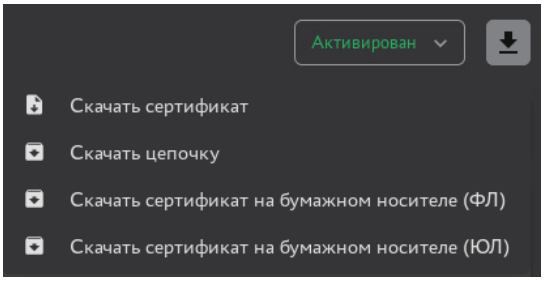


Рисунок 26 – Скачивание сертификата

Для изготовления и экспорта документа, содержащего значения полей данного сертификата (далее – сертификат на бумажном носителе) нажмите кнопку  и во всплывающем меню (см. Рисунок 26) выберите

<Скачать сертификат на бумажном носителе (ФЛ)> (для физических лиц) субъекта или <Скачать сертификат на бумажном носителе (ЮЛ)> (для юридических лиц).

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

Формат сертификата на бумажном носителе для каждого типа, а также правила записи значений в поля сертификата на бумажном носителе представлены в Приложении 4.

В карточке сертификата отображаются следующие сведения:

- идентификатор;
- издатель;
- владелец;
- SDN владельца;
- срок действия («действует с», «действует по»);
- алгоритм ключа;
- длина ключа.

Карточка сертификата содержит раскрывающиеся вкладки:

- «Цепочка сертификатов». Раскройте 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 27).

Рисунок 27 – Окно карточки сертификата. Вкладка «Цепочка сертификатов»

- «Состав». Раскройте вкладку, нажав в строке с именем вкладки символ . На раскрывшемся экране отображены следующие поля (см. Рисунок 28):

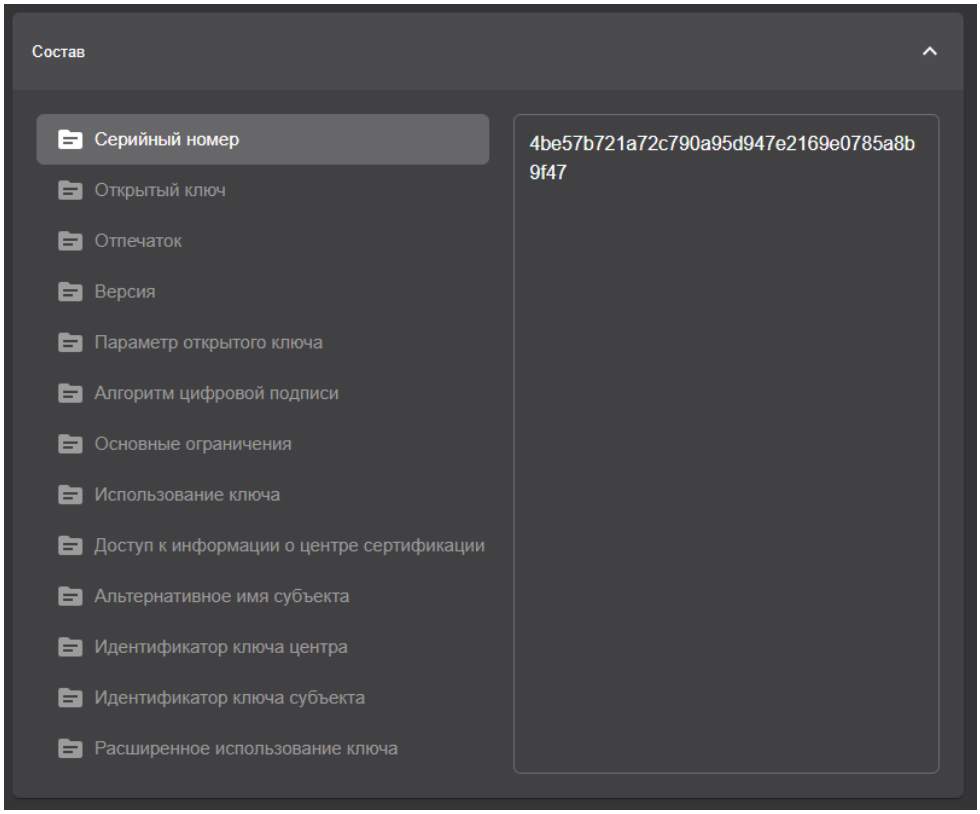


Рисунок 28 – Окно карточки сертификатов. Вкладка «Состав»

- серийный номер;
- открытый ключ;
- отпечаток;
- версия;
- параметр открытого ключа;
- алгоритм цифровой подписи
- основные ограничения;
- использование ключа;
- доступ информации о центре сертификации;
- альтернативное имя субъекта;
- идентификатор ключа центра;
- идентификатор ключа субъекта;
- расширенное использование ключа.

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

- «История изменения сертификата». Раскройте вкладку, нажав в строке с именем вкладки символ . На данной вкладке зафиксирована информация о всех совершённых над сертификатом действиях в хронологическом порядке. На раскрывшемся экране отображены поля (см. Рисунок 29):
  - дата – дата совершенного действия;
  - пользователь – учётная запись, под которой было совершенно данное действие;
  - событие – действие, совершённое над сертификатом.

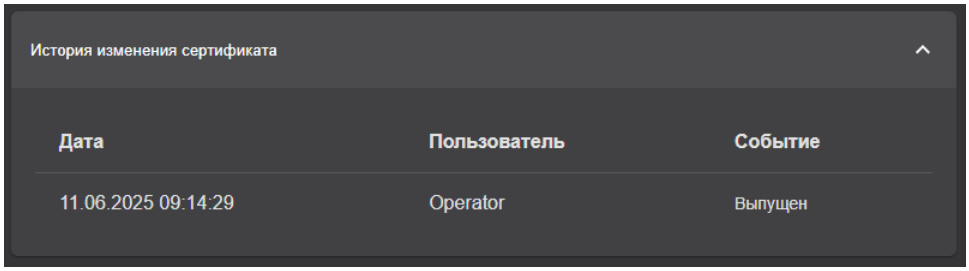


Рисунок 29 – Окно карточки сертификатов. Вкладка «История изменения сертификата»

Выход из карточки сертификата осуществляется по кнопке <Возврат> и по кнопкам разделов на боковой панели.

4.3.7 Экспорт списка выпущенных сертификатов

Оператору доступен экспорт выпущенные сертификаты только тех субъектов, права доступа на которые ему назначены.

Для выгрузки списка сертификатов нажмите кнопку Скачать **<Скачать все сертификаты в формате CSV>**. Происходит формирование списка сертификатов, по завершению действия и готовности к выгрузке списка сертификатов кнопка переходит в состояние Скачать (готово). Нажмите кнопку **<Скачать (готово)>** для сохранения подготовленного списка сертификатов.

Сохранение списка сертификатов в виде zip-архива происходит по выбранному пути в открывшемся окне сохранения файла.

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

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

4.3.8 Массовые операции с сертификатами

Порядок выполнения массовых операций с сертификатами:

- Для массовой операции, применяемой к выбранному множеству сертификатов доступа, нажмите кнопку  **<Массовые операции>**, которая запускает окно выполнения массовой операции (см. Рисунок 30).

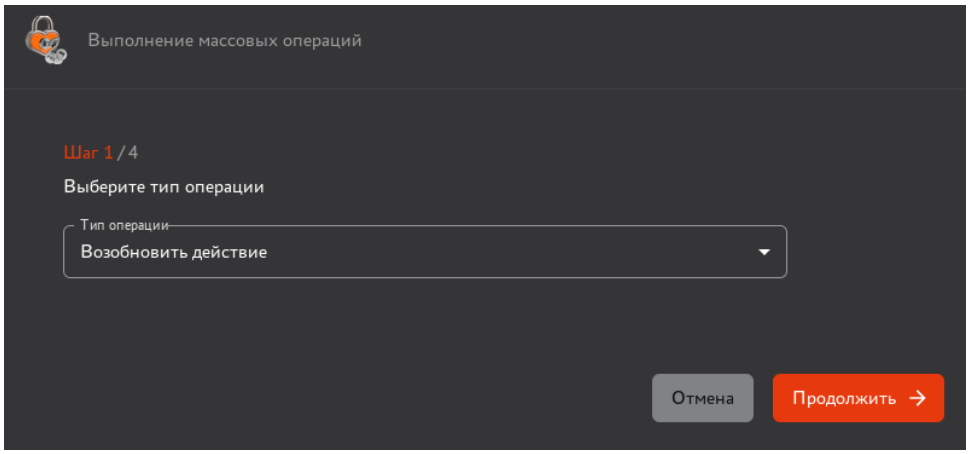


Рисунок 30 – Окно выполнения массовых операций. Шаг 1

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

    При выборе операции «Отозвать» дополнительно необходимо будет указать причину отзыва из выпадающего списка.
- Нажмите кнопку **<Продолжить>**.

Далее необходимо осуществить поиск сертификатов по отличительному имени субъекта Subject Distinguished Names, для которых требуется применить выбранную операцию, в левом поле окна Шага 2 (см. Рисунок 31). Поиск сертификатов производится с учётом текущего статуса сертификата и выбранного типа операции на шаге 1. Например, при выборе типа операции «Возобновить» поиск осуществляется только среди сертификатов со статусом «Приостановлен», для которых допустимо выполнить данный тип операции.

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

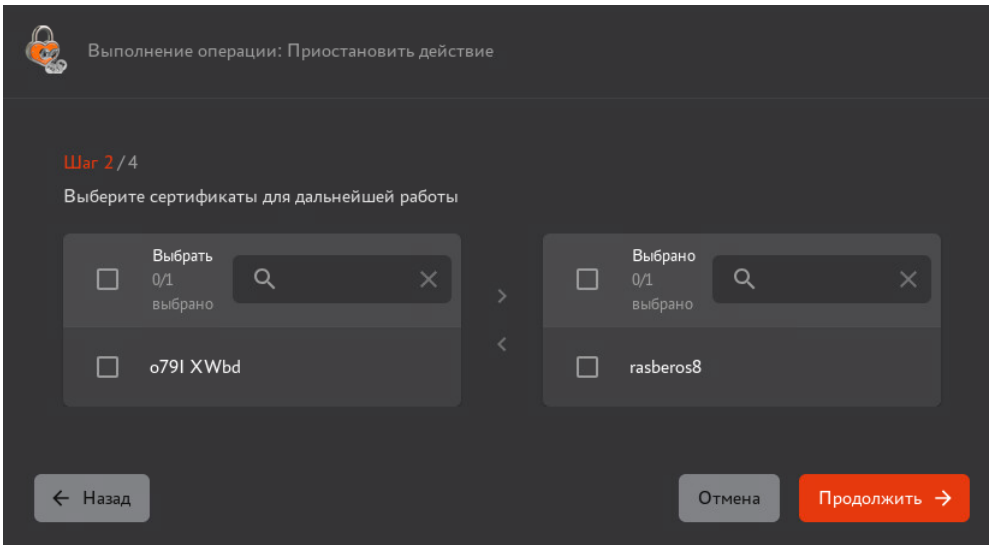


Рисунок 31 – Окно выполнения массовых операций. Шаг 2. Создание списка выбранных сертификатов

- В случае необходимости исключения из выбранных сертификатов, к которым будет применена массовая операция, отметьте флажками сертификата из списка в правой части окна, и нажмите кнопку ‹.
- Для перехода на следующий шаг нажмите кнопку **<Продолжить>**.
- В открывшемся окне подтвердите действие, нажав кнопку <**Применить>** (см. Рисунок 32).

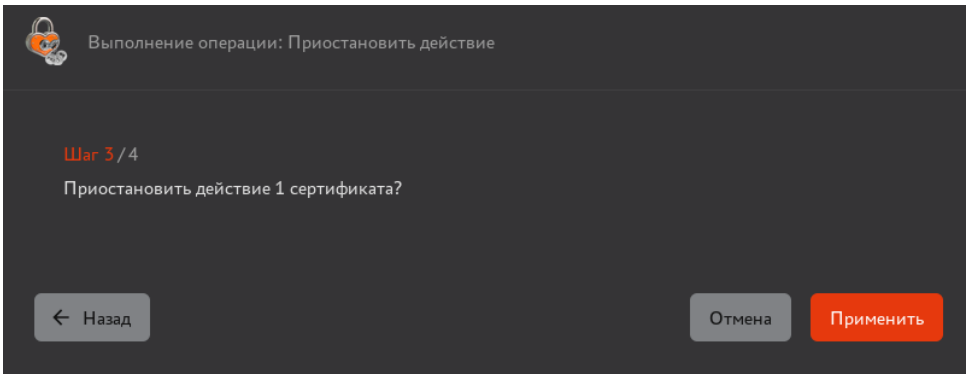


Рисунок 32 – Окно выполнения массовых операций. Шаг 3

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

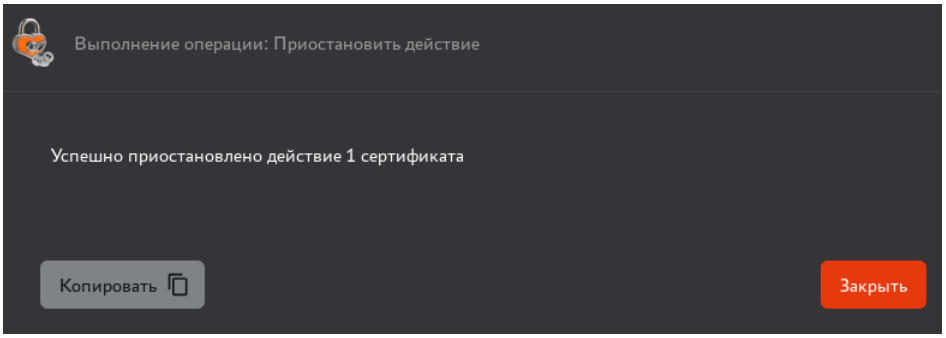


Рисунок 33 – Окно выполнения массовых операций. Шаг 4

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

4.4 Раздел «Субъекты»

Раздел «Субъекты» обеспечивает возможность просмотра субъектов подключенных служб каталога, выпуска сертификатов для субъектов. Для авторизованного Оператора в разделе «Субъекты» доступны только те субъекты, на которые ему прямо или косвенно[1] предоставлены полномочия в соответствии с назначенными правилами доступа.

Переход в раздел «Субъекты» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 34).

После выбора источника в поле «Внешние ресурсные системы», субъекты будут отображены в виде списка в окне раздела «Субъекты (см. Рисунок 34).

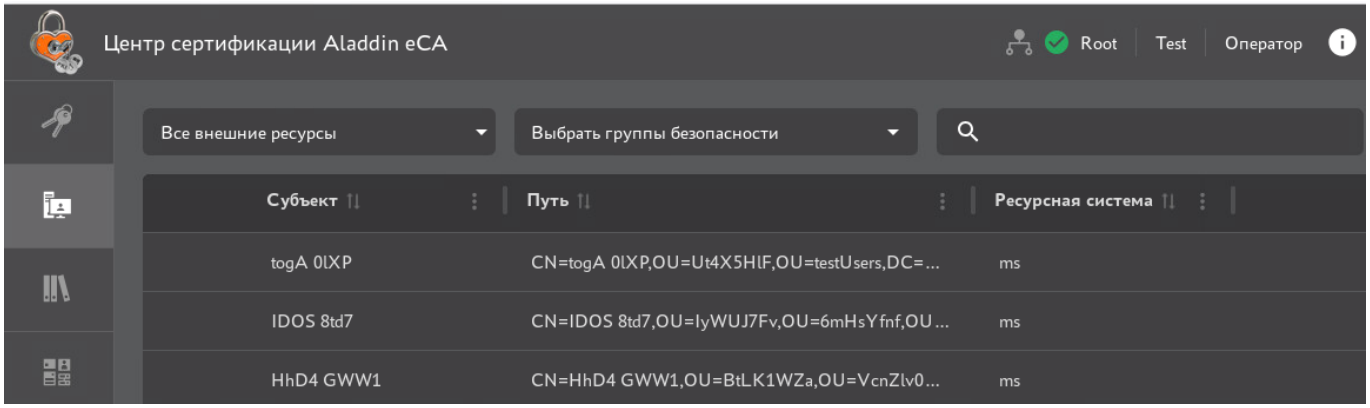


Рисунок 34 – Экран раздела меню «Субъекты». Подключенный ресурс

В разделе доступны следующие элементы:

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

В разделе «Субъекты» доступны следующие действия:

- просмотр субъектов подключенных ресурсных систем с выбором группы безопасности;
- просмотр субъектов локальной ресурсной системы;

[1] Путем наследования от группы безопасности, куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

- поиск субъекта;
- редактирование значения атрибутов субъекта;
- просмотр карточки субъекта;
- просмотр списка сертификатов, выпущенных Центром сертификации для субъекта;
- управление статусом сертификатов субъектов;
- публикация сертификата субъекта в ресурсную систему;
- экспорт сертификата субъекта;
- создание сертификата для субъекта.

Идентификация локальных и подключенных субъектов в Центре сертификации осуществляется по атрибуту «UUID».

4.4.1 Просмотр субъектов ресурсных систем

Просмотр субъектов осуществляется посредством выбора источника:

- все внешние ресурсы – подключенные службы каталогов, на субъекты которых назначены права авторизованному Оператору;
- локальный ресурс – появляется в случае, если назначены права хот бы на один субъект в локальной базе данных Центра сертификации;
- внешний ресурс, отображаемое имя которого соответствует имени контроллера домена.

В разделе «Субъекты» в верхней панели расположены элементы выбора ресурса и фильтрации (см. Рисунок 35):

- поле «Ресурсная система», по нажатию на которое в выпадающем меню выберите локальную ресурсную систему, подключенный ресурс или все внешние ресурсы для отображения всех субъектов внешних ресурсных систем;
- поле «Выбрать группу безопасности», для отображения на экране субъектов определенной группы нажмите на поле и в выпадающем меню выберите необходимую группу. В случае если группа безопасности не выбрана, то будут отображены все субъекты выбранного источника. Для локального ресурса группы безопасности отсутствуют. В списке «Выбрать группу безопасности» отображаются только те группы безопасности, которые содержат один или более субъектов. Группы безопасности, не имеющие членов, не будут показаны в списке и не доступны для выбора.

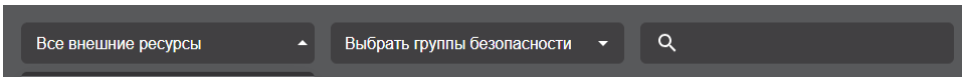


Рисунок 35 – Верхняя панель экранной формы вкладки «Субъекты»

4.4.2 Поиск субъектов

В разделе «Субъекты» в верхней панели расположены элементы (см. Рисунок 35). Поле поиска, в котором осуществляется поиск субъектов по компонентам SubjectDN и SubjectAltName в выбранной ресурсной системе. Для поиска начните ввод имени субъекта в строке, поиск начинается автоматически через 1 секунду после прекращения ввода с клавиатуры. Для сброса поиска и отображения всех субъектов выбранной ресурсной системы очистите строку поиска.

4.4.3 Сортировка субъектов

Средства сортировки субъектов выбранной ресурсной системы представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 36):

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

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

Рисунок 36 – Поля сортировки содержимого экрана раздела «Сертификаты»

4.4.4 Карточка субъекта

Просмотра данных субъекта возможен посредством страницы «Карточка субъекта».

Переход к экрану «Карточка субъекта» (см. Рисунок 37) осуществляется при нажатии на строку субъекта главного экрана раздела «Субъекты» (см. Рисунок 34).

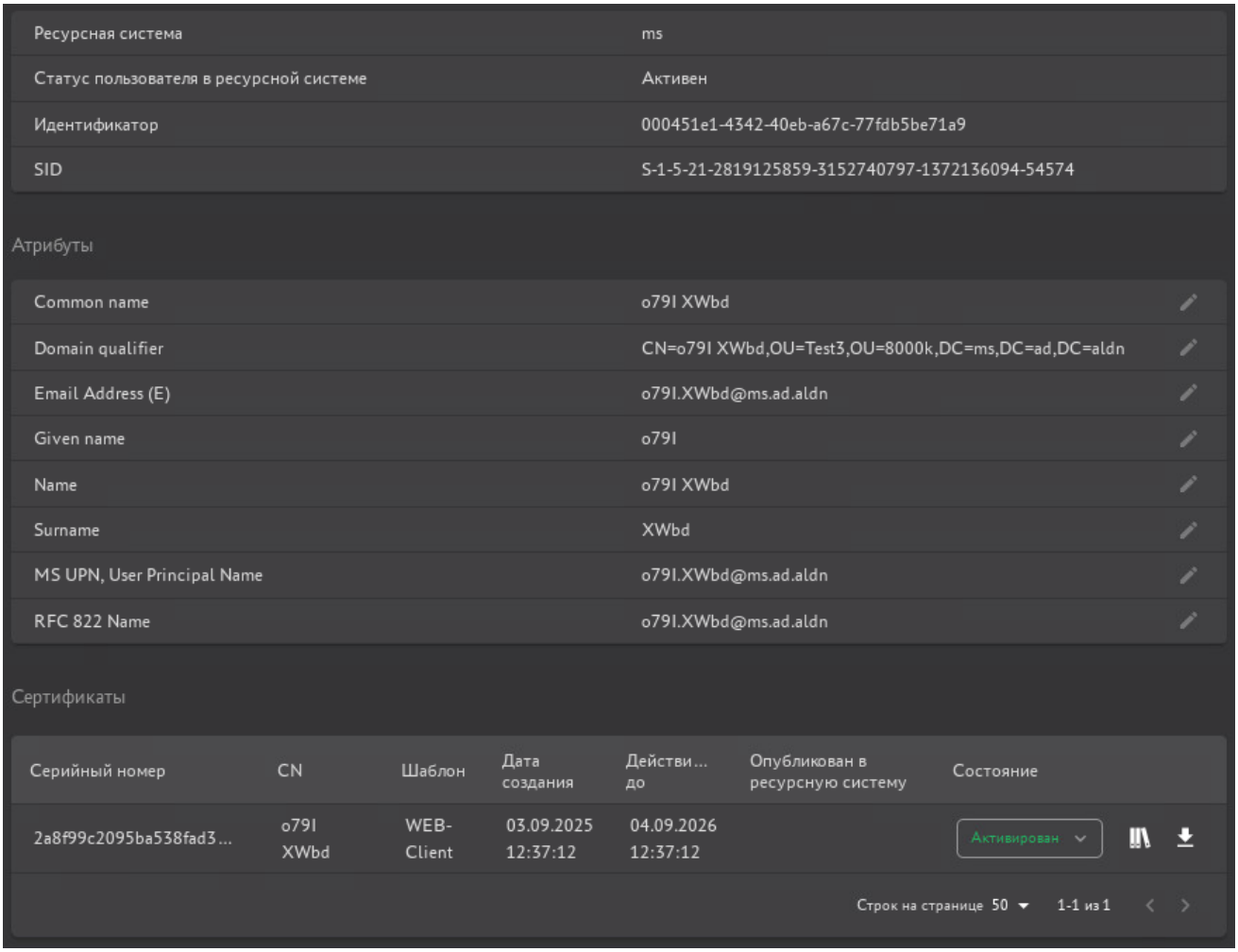


Рисунок 37 – Окно просмотра карточки субъекта (включено отображение «Атрибуты со значениями»)

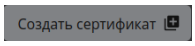
Карточка субъекта включает в себя следующие информационные поля:

- сведения о субъекте:
  - из какой ресурсной системы получен субъект;
  - статус пользователя в ресурсной системе;
  - идентификатор UUID;
- SID (идентифкатор безопасности)[1];

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

- атрибуты SAN и SDN (см. Таблица 3);
- сведения обо всех сертификатах субъекта, ранее выпущенных Центром сертификации:
  - серийный номер;
  - Common Name владельца сертификата;
  - шаблон;
  - дата создания;
  - дата окончания действия;
  - дата публикации в ресурсную систему;
  - состояние сертификата.

Доступные действия в карточке субъекта:

- создать сертификат для выбранного субъекта с закрытым ключом, на основании запроса или на ключевом носителе по нажатию на кнопку <Создать сертификат> 

(см. п. 4.4.8, настоящего руководства);
- выбрать набор атрибутов SDN и SAN, отображаемых в карточке субъекта, в выпадающем меню (см. Рисунок 38);

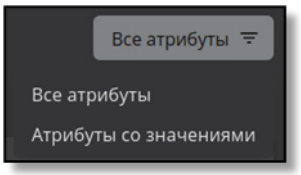


Рисунок 38 – Фильтрация отображаемых атрибутов в карточке субъекта

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

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

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

Таблица 3 – Атрибуты субъекта

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Сведения о субъекте			
Ресурсная система, к которой подключен	Ресурсная система, к которой подключен субъект	resource: { id (UUID), commonName (string), name (string)}	Поле «Получен из ресурсной системы» в карточке субъекта Для локальных субъектов всегда отображается значение «Локальная

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
субъект			ресурсная система».
Флаг подключения к РС	Субъект подключен к ресурсной системе (true)	"isConnected": true	Отображение субъекта в списке субъектов ресурсной системы, к которой он подключен.
	Локальный субъект (false)	" isConnected": false	Отображение субъекта в списке субъектов локальной ресурсной системы.
Флаг блокировки в РС	Для подключенных к РС субъектов: субъект заблокирован в РС (true) или субъект не заблокирован в РС (false)	"isBlocked"	Поле «Статус в ресурсной системе» в карточке субъекта. Для локальных субъектов всегда отображается символ «-».
	Для локальных субъектов: всегда false		
UUID	string($uuid)	"id"	Поле «UUID» карточки субъекта
Расположение субъекта в структуре РС	Строка	"distinguishedName"	Поле «Путь» в списке субъектов в разделе «Субъекты»
Время обновления субъекта	Дата в формате ISO 8601	"updated"	-
Время создания субъекта	Дата в формате ISO 8601	"created"	-
SID[1]	Строка	"sid"	Поле «SID» карточки субъекта
Атрибуты SDN			
Common name	Список строк	"CN"	Поле «Common name» в карточке субъекта
Unique Identifier (UID)	Список строк	"UID"	Поле «Unique Identifier (UID)» в карточке субъекта
Email Address (E)	Список строк	"E"	Поле «Email Address (E)» в карточке субъекта
Email Address (Mail)	Список строк	"EMAILADDRESS"	Поле «Email Address (Mail)» в карточке субъекта
Mail	Список строк	"MAIL"	Поле «Mail» в карточке субъекта

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

Атрибут	Возможные значения	Представление в API	Представление в клиентском компоненте
Serial number	Список строк	"SN"	Поле «Serial number» в карточке субъекта
Given name	Список строк	"GIVENNAME"	Поле «Given name» в карточке субъекта
Initials	Список строк	"INITIALS"	Поле «Initials» в карточке субъекта
Surname	Список строк	"SURNAME"	Поле «Surname» в карточке субъекта
Organizational unit	Список строк	"OU"	Поле «Organizational unit» в карточке субъекта
Organization	Список строк	"O"	Поле «Organization» в карточке субъекта
Locality	Список строк	"L"	Поле «Locality» в карточке субъекта
State or province	Список строк	"ST"	Поле «State or province» в карточке субъекта
Domain component	Список строк	"DC"	Поле «Domain component» в карточке субъекта
Country	Список строк	"C"	Поле «Country» в карточке субъекта
Unstructured address	Список строк	"UNSTRUCTUREDADDRESS"	Поле «Unstructured address» в карточке субъекта
Unstructured name	Список строк	"UNSTRUCTUREDNAME"	Поле «Unstructured name» в карточке субъекта
Postalcode	Список строк	"POSTALCODE"	Поле «Postalcode» в карточке субъекта
Business category	Список строк	"BUSINESSCATEGORY"	Поле «Business category» в карточке субъекта
Telephone number	Список строк	"TELEPHONENUMBER"	Поле «Telephone number» в карточке субъекта
Pseudonym	Список строк	"PSEUDONYM"	Поле «Pseudonym» в карточке субъекта
Postal address	Список строк	"POSTALADDRESS"	Поле «Postal address» в карточке субъекта
Street	Список строк	"STREET"	Поле «Street» в карточке субъекта
Name	Список строк	"NAME"	Поле «Name» в карточке субъекта
Title	Список строк	"T"	Поле «Title» в карточке субъекта
Domain Qualifier	Список строк	"DN"	Поле «Domain Qualifier» в карточке субъекта
Description	Список строк	"DESCRIPTION"	Поле «Description» в карточке субъекта
Дата рождения	Список строк	«DATEOFBIRTH»	Поле «Дата рождения» в карточке субъекта
Место рождения	Список строк	«PLACEOFBIRTH»	Поле «Место рождения» в карточке субъекта
ИНН	Список строк	"INN"	Поле «ИНН» в карточке субъекта

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

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

4.4.5 Редактирование атрибутов субъекта

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

- Для субъектов любой ресурсной системы редактирование сведений о субъектах в их карточках (поля «Получен из ресурсной системы», «Статус в ресурсной системе», «UUID») недоступны для редактирования.
- При вводе/редактировании значений атрибутов, указанных в Таблица 4, осуществляется валидация. Для всех остальных атрибутов субъекта валидация отсутствует.

Таблица 4 – Допустимые значения атрибутов

Атрибут	Правило валидации
Country	Допустимые символы: "A"-"Z", "a"-"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
Serial number	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", ".", "@", "_", "-". Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле. При этом преобразовывать можно только доменную часть. Формат значения: "text@text".
DNS Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "-", ".", "*". Если необходимо использовать кириллицу, то кириллицу необходимо преобразовать в латиницу с помощью Punycode (подробнее см. RFC 3492) и ввести полученное значение в поле.
IP address	Допустимые символы: "A"-"F", "a"-"f", "0"-"9", ".", ":". Формат значения: IPv4-адрес или IPv6-адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component, C=RU...). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"-"9", ".". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
MS GUID, Globally Unique Identifier	Допустимые символы: "A"-"F", "a"-"f", "0"-"9". Длина значения должна составлять 32 символа.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.
Дата рождения	Формат значения: дата в формате «DD.MM.YYYY».
ИНН	Допустимые символы: "0"-"9". Длина значения должна составлять 12 или 14 символов.
ОГРН	Допустимые символы: "0"-"9". Длина значения должна составлять 13 символов.

Атрибут	Правило валидации
ОГРНИП	Допустимые символы: "0"-"9". Длина значения должна составлять 15 символов.
СНИЛС	Допустимые символы: "0"-"9". Длина значения должна составлять 11 символов.
ИНН ЮЛ	Допустимые символы: "0"-"9". Длина значения должна составлять 10 или 14 символов.

Для редактирования значения атрибута в карточке субъекта нажмите кнопку <Редактировать> , в открывшемся окне введите новое значение атрибута в соответствующем поле, в соответствии с условиями валидации (см. Рисунок 39).

- Для добавления значения атрибута (будет указано в поле атрибута через запятую) нажмите кнопку **<Добавить значение +>**;

Для удаления значения атрибута нажмите кнопку **<Удалить значение атрибута>** . При этом у атрибута «Common name» нельзя удалить последнее значение;

- Для сохранения результата нажмите кнопку **<Сохранить>**;
- Для выхода из режима редактирования без сохранения изменений или нажмите кнопку **<Закрыть>**.

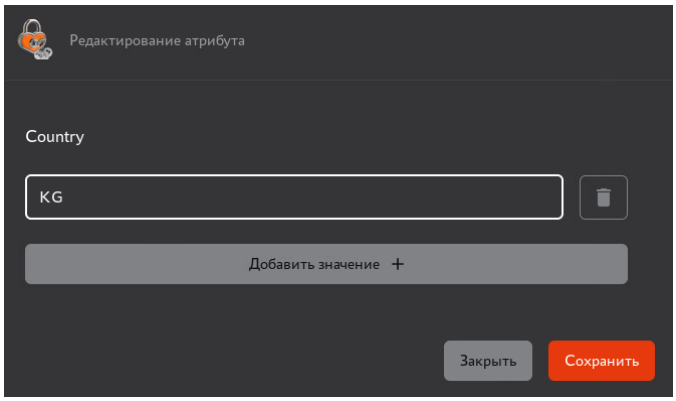


Рисунок 39 – Окно редактирования значения атрибута в карточке субъекта

4.4.6 Субъекты локальной ресурсной системы

Локальную базу субъектов формируют:

- субъекты, созданные Администратором путём вызова метода API;
- субъекты отключенной ресурсной системы (удалённой ранее зарегистрированной ресурсной системы), атрибут субъекта «isBlocked» принимает значение «false». В случае повторного подключения ресурсной системы связи субъектов с группами будут восстановлены, обновлены атрибуты в соответствии с данными из ресурсной системы;
- субъекты, загруженные в базу данных Центра сертификации Aladdin eCA при подключении ресурсной системы, но отсутствующие в списке субъектов, полученном по результатам выполнения полной синхронизации ресурсной системы. Атрибут субъекта «isBlocked» принимает значение «false».

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

4.4.7 Субъекты внешнего ресурса

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

Подключенный ресурс будет отображен только после регистрации ресурсной системы на вкладке «Ресурсная система».

Обновление списков и данных субъектов ресурсной системы происходит по правилам, приведённым в пункте 4.5.1 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 34).

- 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 9.

Таблица 5 – Преобразование данных субъектов ресурсной системы

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

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

- Идентификация подключенных субъектов в Центре сертификации осуществляется по атрибуту `UUID`.

4.4.8 Создание сертификата для субъекта ресурсной системы

Создание сертификата для локального субъекта доступно авторизованному Оператору, которому в соответствии с правилами доступа предоставлены полномочия на доступ к субъектам локальной ресурсной системы. Создание сертификата для подключенного к ресурсной системе субъекта доступно авторизованному Оператору, которому в соответствии с правилами доступа предоставлены полномочия на доступ к субъектам группы безопасности ресурсной системы, куда входит данный субъект.

Выберите субъект, для которого необходимо создать сертификат, нажмите появившуюся кнопку <Создать сертификат> и выберите способ создания из выпадающего списка (см. Рисунок 40).

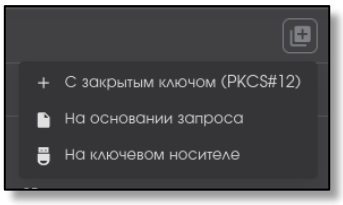


Рисунок 40 - Окно выпуска сертификата для субъекта ресурсной системы

4.4.8.1 Создание сертификата с закрытым ключом pkcs#12

- В открывшемся окне создания сертификата (см. Рисунок 41) выберите шаблон создаваемого сертификата из выпадающего списка. В выпадающем списке будут присутствовать только те шаблоны, на использование которых данному Оператору предоставлен доступ администратором путем создания правил доступа. Описание полей для шаблонов по умолчанию приведено в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.

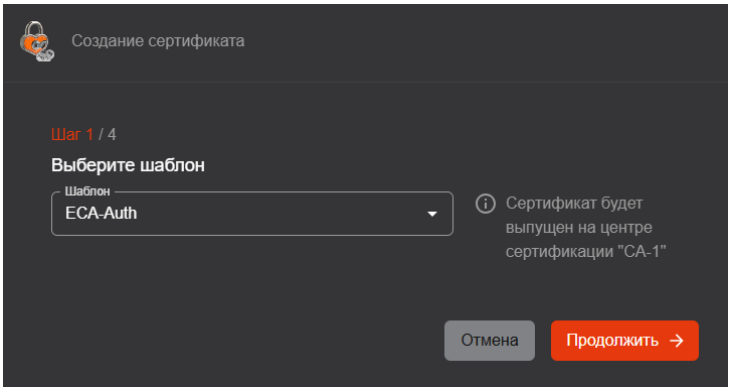


Рисунок 41 – Окно создания сертификата PKCS#12. Шаг 1. Выбор шаблона

- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.
- Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов).

В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. Рисунок 42).

- Если данные атрибутов отсутствуют, то необходимо ввести значения в соответствующие поля в карточке субъекта (см. п. 4.4.5 настоящего руководства).
- Необязательные поля могут оставаться незаполненными.
- Нажмите ставшую активной кнопку <Продолжить> для перехода к следующему шагу.

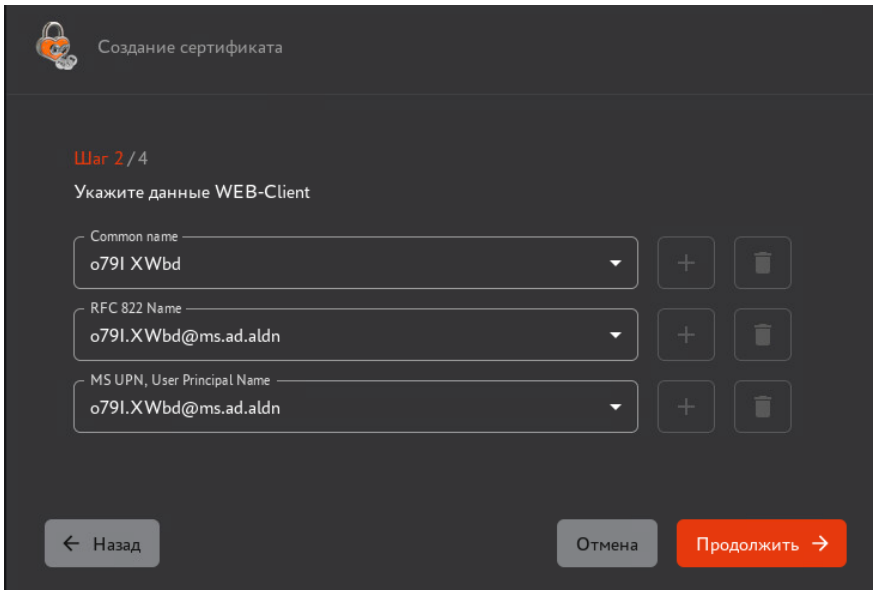


Рисунок 42 – Окно создания сертификата PKCS#12. Шаг 2. Атрибуты сертификата

- Далее администратору необходимо создать пароль с подтверждением для ключевого контейнера (см. Рисунок 43). 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.

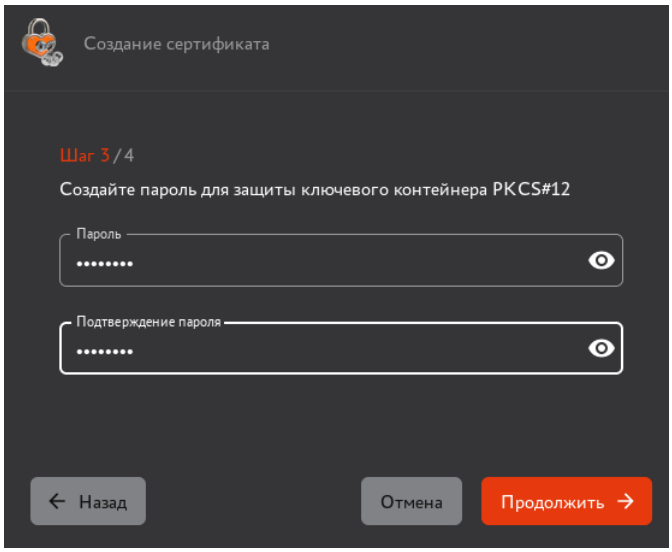


Рисунок 43 – Окно создания сертификата PKCS#12. Шаг 3. Задание пароля контейнера сертификата

- В следующем окне требуется определить параметры шифрования (см. Рисунок 44):
  - алгоритм ключа;
  - длину ключа.

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

- После выбора алгоритма нажмите кнопку <Создать сертификат>.

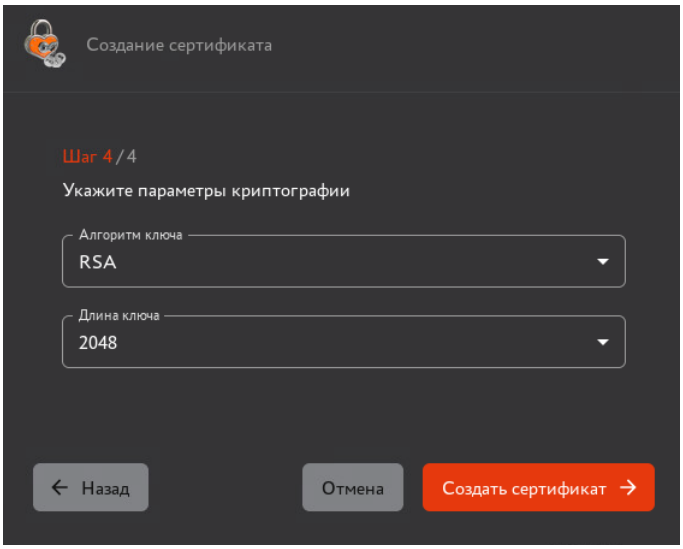


Рисунок 44 - Окно создания сертификата PKCS#12. Шаг 4. Выбор параметров криптографии

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 51).

Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате PEM.

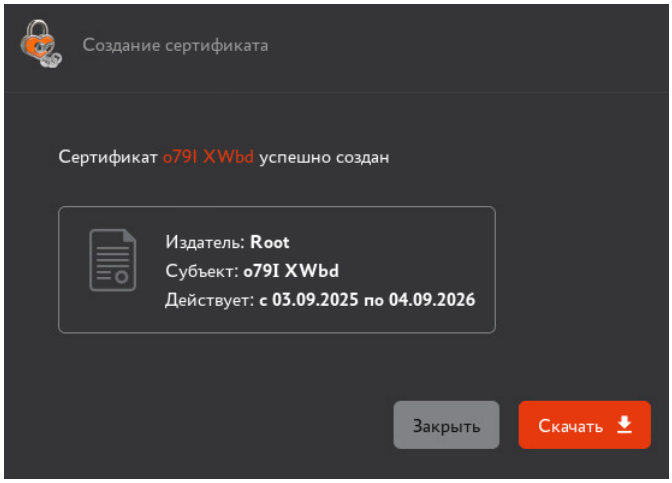


Рисунок 45 – Окно по результату успешного завершения создания сертификата PKCS#12

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».

В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

4.4.8.2 Создание 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 должно быть `.csr` или `.pem`;
  - файл-запрос должен быть сформирован с учетом известных данных выбранного шаблона Центра сертификации Aladdin eCA. Например, для использования шаблона «Domain Controller» в запросе должны быть указаны параметры DNS Name и MS GUID;
  - по файлу-запроса ранее не был выпущен сертификат.
- В открывшемся окне (см. Рисунок 46) необходимо выбрать и загрузить файл-запрос, а также выбрать шаблон сертификата в соответствии с запросом (предполагается, что Оператор заранее знает какой шаблон необходимо выбрать). В списке шаблонов будут присутствовать только те шаблоны, на использование которых данному Оператору предоставлен доступ администратором путем создания правил доступа. По файлу запроса возможен только одноразовый выпуск сертификата. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.
- При необходимости, возможно перезагрузить файл-запрос в мастере создания сертификата без сброса текущего прогресса по кнопке <Изменить>.

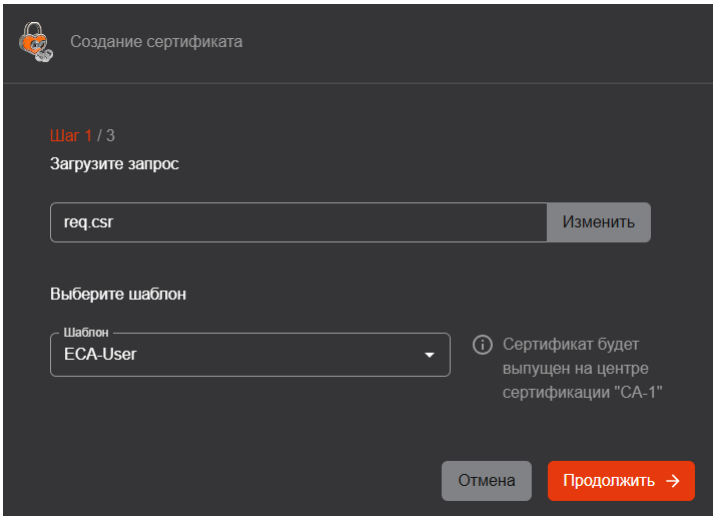


Рисунок 46 – Окно создания сертификата по запросу. Шаг 1. Загрузка запроса и выбор шаблона

- После загрузки файла запроса и выбора шаблона нажмите активировавшуюся кнопку <Продолжить>.
- Программа проверяет запрос на соответствие полей запроса на сертификат и атрибутов субъекта по правилам, приведённым в Таблица 6. Проверка является регистронезависимой.

Таблица 6 – Соответствие полей запроса шаблону выпускаемого сертификата

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

Поле в шаблоне	Значение поля в запросе	Атрибут субъекта АЕСА	Возможность создания сертификата	Поле в сертификате	Возможные ошибки*
Есть, необязательное	Есть	Нет	Да	Отсутствует	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка №4
Есть, необязательное	Нет	Нет	Да	Отсутствует	-
Есть, необязательное	Есть	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	1) Ошибка №2, если значение в запросе не проходит валидацию по шаблону 2) Ошибка 4, если значение в запросе не соответствует значению атрибута
Есть, необязательное	Нет	Есть	Да	Присутствует, если поле не было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне или Отсутствует, если поле было удалено на этапе переопределения значений для полей SAN, указанных в шаблоне	-
Нет	Есть	Нет	Да	Отсутствует	Ошибка №3
Нет	Нет	Нет	Да	Отсутствует	-
Нет	Есть	Есть	Да	Отсутствует	Ошибка №3
Нет	Нет	Есть	Да	Отсутствует	-

- Если во время обработки запроса произошла ошибка, в окне результата обработки запроса отображаются сообщения об ошибках в полях запроса, где они были обнаружены, с цветовой (красной) индикацией и предупреждающей иконкой (см. Рисунок 47 и Рисунок 48).

- В случае выявления ошибки в запросе на сертификат доступа для субъекта возможны следующие сообщения:
  - «Отсутствует обязательное поле» (ошибка №1)[1];
  - «Значение в поле не соответствует регулярному выражению: \"%s\"", где \"%s\» (ошибка №2)[2];
  - «Поле отсутствует в шаблоне» (ошибка №3);
  - «Значение в поле не соответствует значению атрибута субъекта» (ошибка №4).

Если создание сертификата невозможно, то существует две возможности:
- вернуться на предыдущий шаг и сменить шаблон на подходящий;
- пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>.

[1] Описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов.

[2] Правила валидации значений полей предустановленных шаблонов см. в Приложение 2. Правила валидации значений полей по умолчанию предустановленных шаблонов сертификатов.

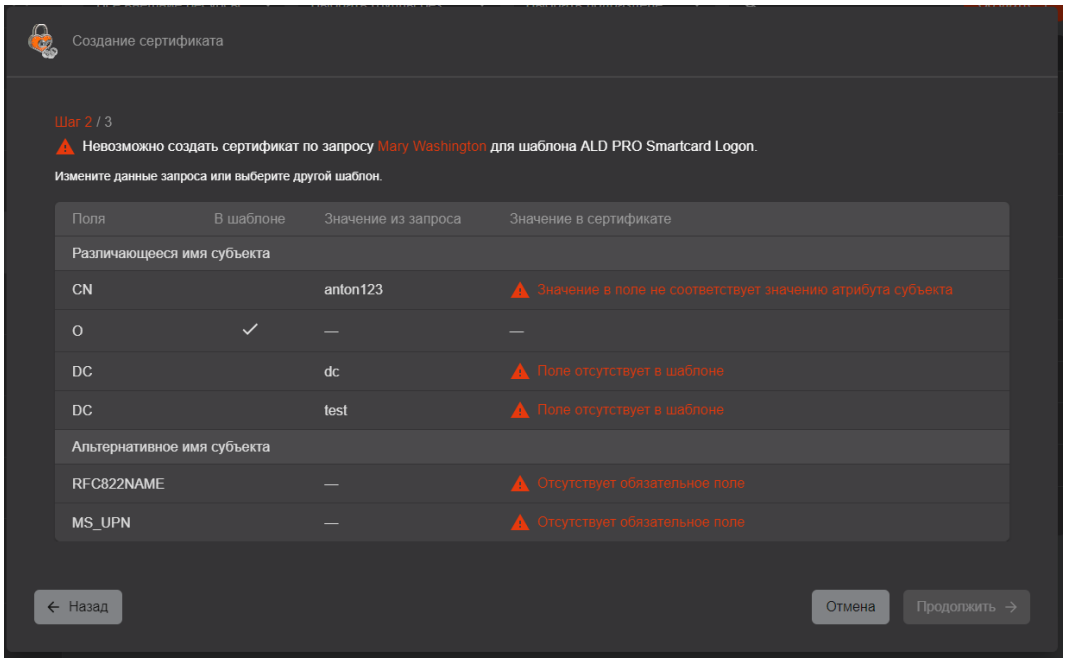


Рисунок 47 – Окно создания сертификата по запросу. Шаг 2. Результат обработки запроса с ошибкой в поле различающегося имени субъекта

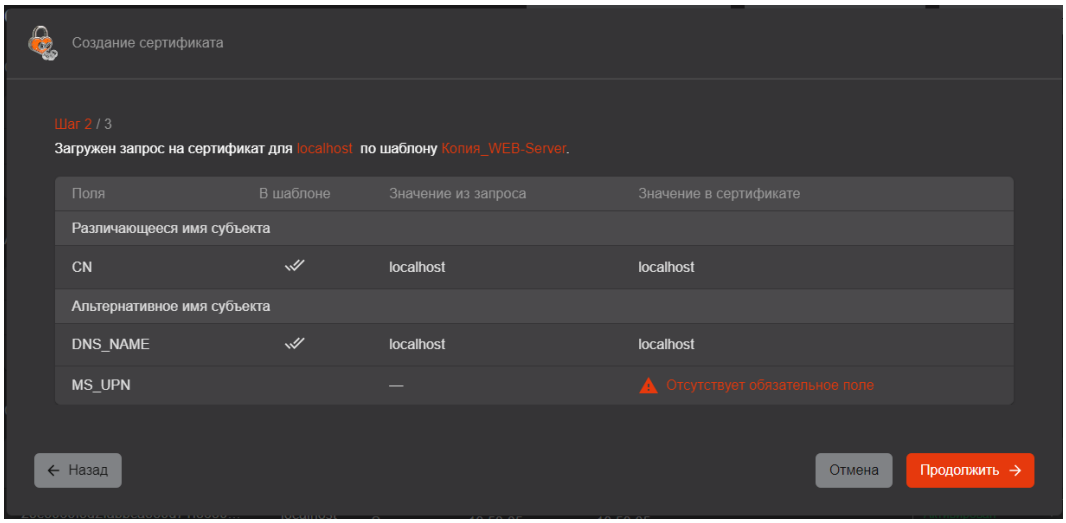


Рисунок 48 – Окно создания сертификата по запросу. Шаг 2. Результат обработки запроса с ошибками в полях альтернативного имени субъекта

- В результате успешной обработки запроса на сертификат субъекта на следующем шаге отображаются (см. Рисунок 49):
  - таблица, содержащая:
    - перечень полей, заданных в шаблоне (в столбце «Поля»);
    - пиктограммы, отображающие обязательные и необязательные поля шаблона (в столбце «В шаблоне»). Пиктограмма «Галка» ✓ указывает на необязательность поля, а пиктограмма «Двойная галка» ✓✓ указывает на обязательность поля;
    - значения для полей, заданных шаблоном, полученные из запроса на сертификат (в столбце «Значение из запроса»);
    - значения, которые будут указаны в полях создаваемого сертификата (в столбце «Значение в сертификате»).
  - данные таблицы разделена на две основные части:
    - различающееся имя субъекта (Subject DN);
    - дополнительное имя субъекта (Subject AltName).

- кнопка <Продолжить> для перехода к следующему шагу;
- кнопка <Назад> для возврата к предыдущему шагу;
- кнопка <Отмена> для завершения работы мастера создания сертификата без сохранения результатов.

- В случае, если в файле-запросе существуют дополнительные поля субъектных идентификаторов, отсутствующие в текущей реализации[1], то они идентифицируются по параметру OID.

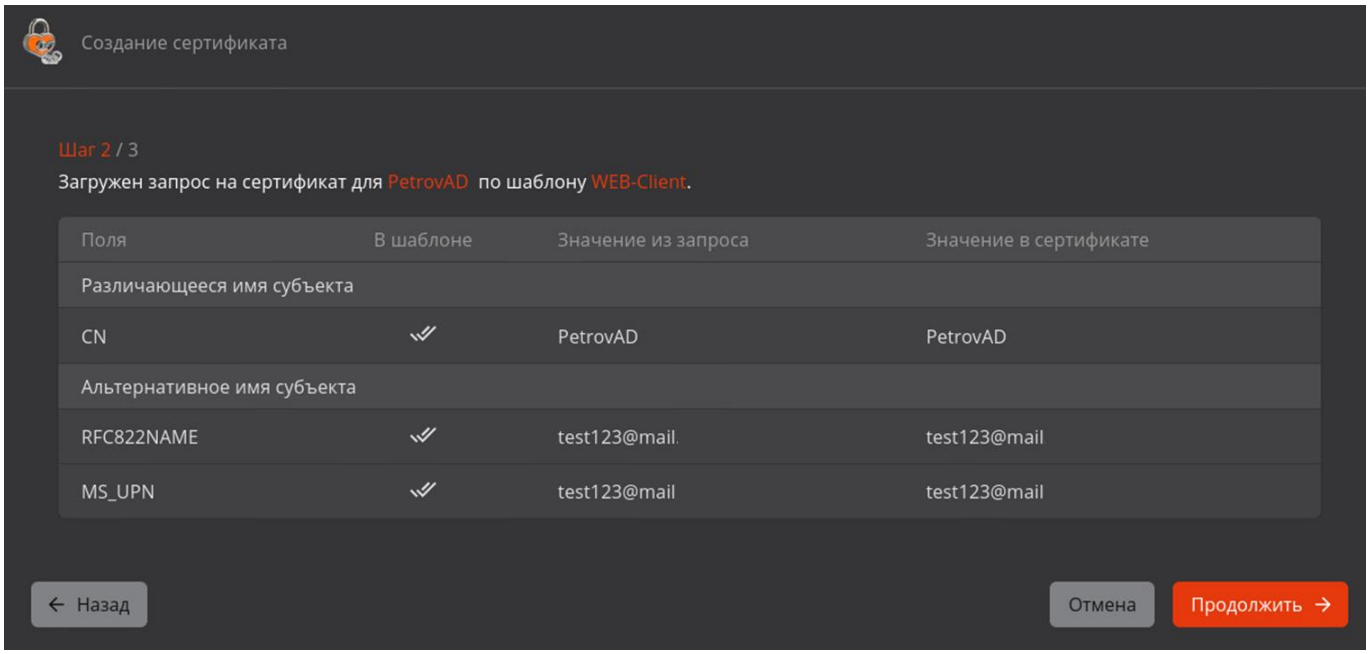


Рисунок 49 – Окно создания сертификата по запросу. Шаг 2. Результат успешной обработки запроса

- После успешной загрузки файла запроса нажмите кнопку <Продолжить> для продолжения процедуры выпуска сертификата для субъекта, кнопку <Отмена> для прекращения процедуры выпуска сертификата или кнопку <Назад> для возврата на предыдущий шаг.

- В окне следующего шага указаны атрибуты в соответствии с шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута (см. Рисунок 50).

- Перечень доступных для выбора значений в полях SAN включает в себя:
  - значения соответствующего полю атрибута субъекта;
  - значения данного поля из запроса, если у субъекта в соответствующем атрибуте есть аналогичное значение, отличающееся от значения в запросе только регистрами символов (такие значения отмечены пиктограммой «Запрос»).

- При отсутствии доступных для указания значений в поле обязательного атрибута будет отображаться ошибка «У субъекта отсутствует указанный атрибут».

- Необязательные поля могут оставаться незаполненными.

[1] Для справки – https://www.alvestrand.no/objectid/2.5.4.html, раздел Subdirectory references.

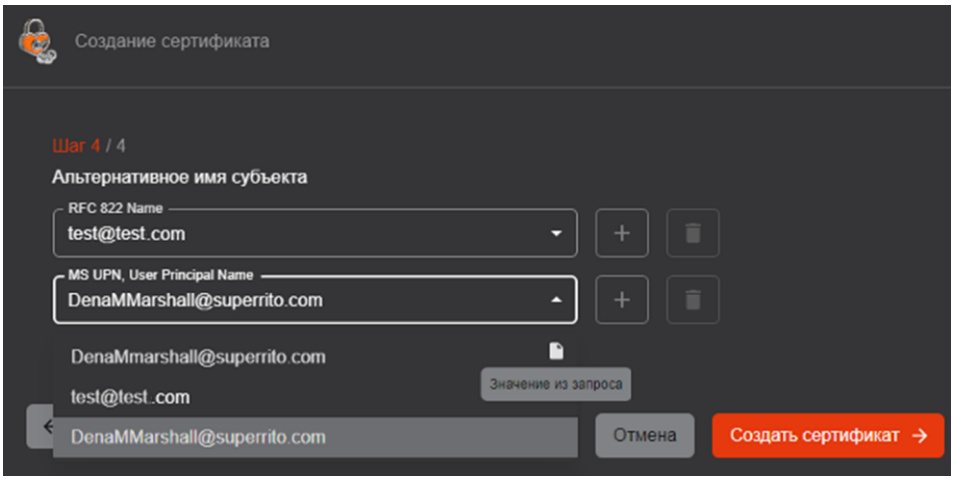


Рисунок 50 – Окно создания сертификата на основании запроса. Шаг 3. Атрибуты сертификата

- Далее по нажатию кнопки <Создать сертификат> открывается финальное окно создания сертификата и отображается краткая информация о созданном сертификате (см. Рисунок 51). У созданного сертификата значения в полях SDN соответствуют значениям в соответствующих полях SDN запроса, на основе которого был создан сертификат.
- При попытке повторного создания сертификата на основании одного запроса на данном шаге отображается ошибка.

> **Внимание! Только в данном окне возможно скачать сертификат и закрытый ключ в контейнере pkcs#12, после закрытия окна скачать сертификат возможно только в формате .pem.**

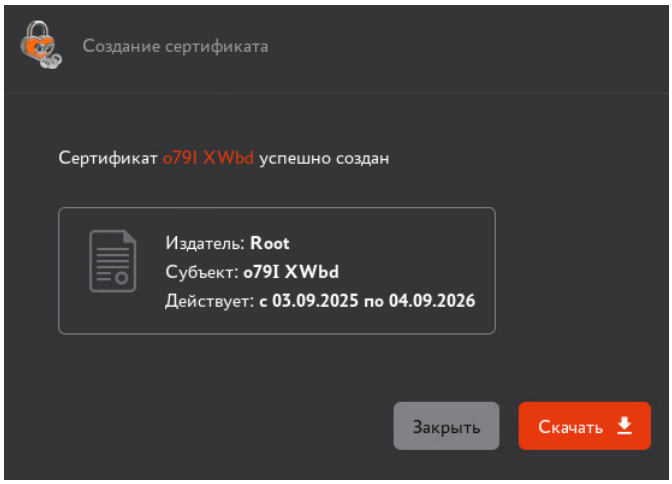


Рисунок 51 – Окно создания сертификата по запросу. Информирование об успешном создании сертификата

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».

  В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

4.4.8.3 Создание сертификата субъекта на ключевом носителе

> **Внимание! Выпуск сертификатов с алгоритмом ключа ГОСТ Р 34.10-2012 и длиной ключа 512 возможен только на ключевых носителях JaCarta-3.**

> **Внимание! Ограничения по возможностям генерации для ключевых носителей Рутокен приведены на официальном сайте производителя.**

Предварительные условия выполнения сценария:

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- Нажатие кнопки <Создать (Выпустить) сертификат> - «на ключевом носителе» стартует сценарий по созданию сертификата на ключевом носителе.
- В случае если электронный ключ успешно подключен, в открывшемся необходимо выбрать ключевой носитель из выпадающего списка в поле «Устройство», ввести PIN-код пользователя ключевого носителя и указать шаблон для выпуска сертификата. В списке шаблонов будут присутствовать только те шаблоны, на использование которых данному Оператору предоставлен доступ администратором путем создания правил доступа. После выбора шаблона в окне отображается информация о центре сертификации, в котором будет выпущен сертификат. Центр сертификации, в котором будет выпущен сертификат, определяется при создании шаблона. Если в шаблоне в качестве центра сертификации выбрано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использован активный в данный момент центр сертификации.
- Переход на следующий шаг осуществляется по ставшей активной кнопке <Продолжить> в случае ввода корректного PIN-кода электронного ключа и заполнении всех полей.

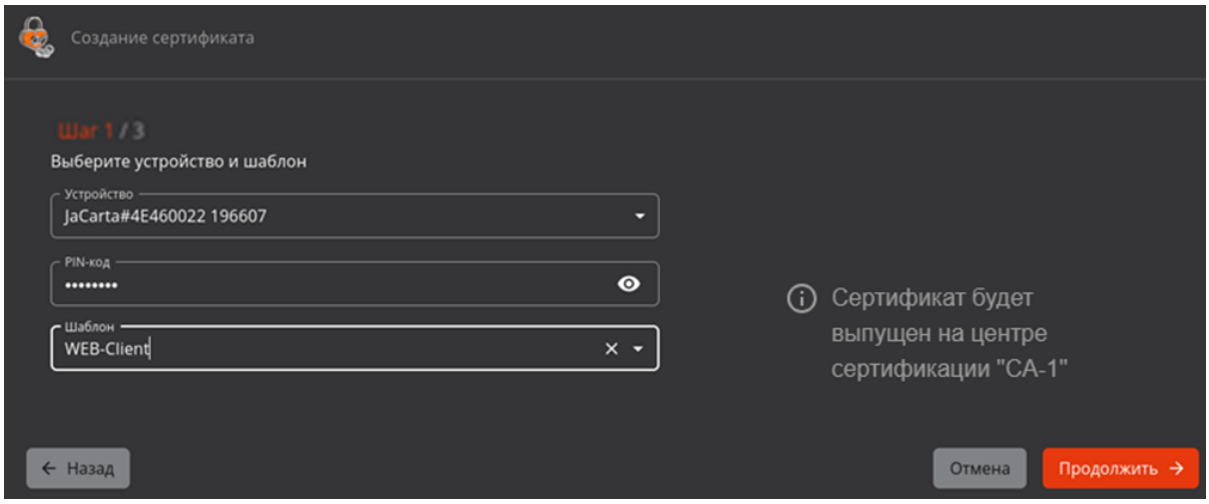


Рисунок 52 – Окно создания сертификата на электронном ключе. Шаг 1

- В окне Шага 2 указаны атрибуты в соответствии с выбранным (на предыдущем шаге) шаблоном сертификата (подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов). Значение атрибутов заполняется автоматически в соответствии с данными в карточке субъекта (см. п. 4.4.4 настоящего руководства) и изменению не подлежит. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить> справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становиться активной – красного цвета). Также дополнительно добавленное значение атрибута можно удалить по кнопке справа от соответствующего поля атрибута.

- Необязательные поля могут оставаться незаполненными.

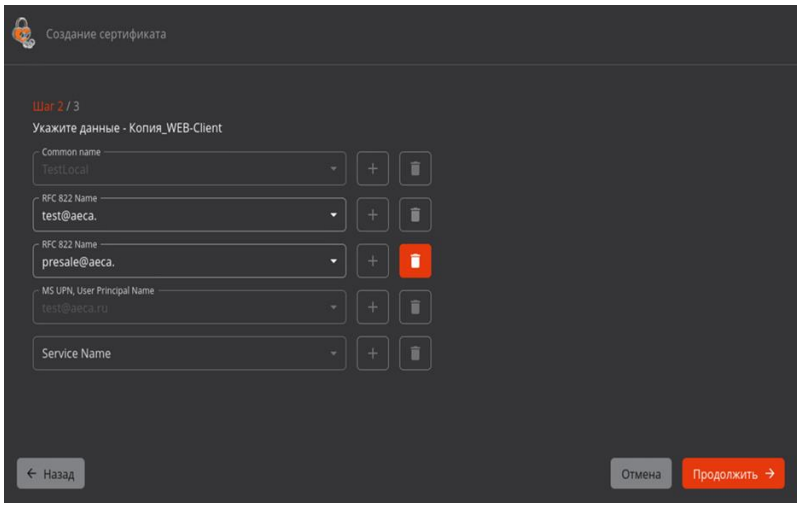


Рисунок 53 – Окно создания сертификата на электронном ключе. Шаг 2

- Далее необходимо выбрать параметры криптографии:
  - выберите алгоритм генерации ключевой пары из раскрывающегося списка. Список алгоритмов ключа определяется шаблоном. При этом алгоритмы, для которых на активном центре сертификации отключен криптопровайдер, не будут отображены в списке. По умолчанию указан первый алгоритм из списка в используемом шаблоне, для которого не отключен криптопровайдер;
  - выберите длину ключа из раскрывающегося списка. Минимальная доступная для выбора длина ключа определяется выбранным шаблоном. По умолчанию указана минимальная длина ключа по шаблону;
  - после выбора алгоритма нажмите кнопку <Создать сертификат>.

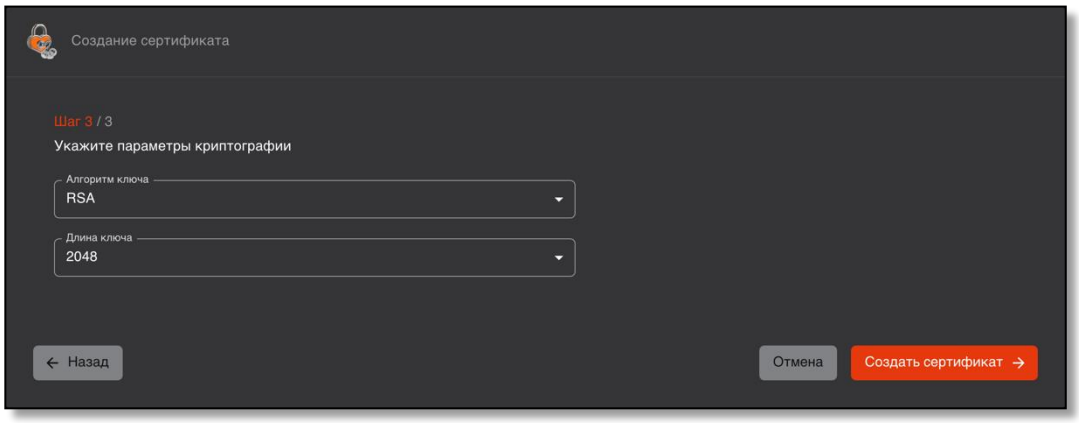


Рисунок 54 – Окно создания сертификата на электронном ключе. Шаг 3

- 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 сертификата на ключевой носитель.
- Процессы выполняются автоматически и после завершения процессов станут доступны кнопки <Скачать сертификат> и <Скачать цепочку сертификатов>.

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

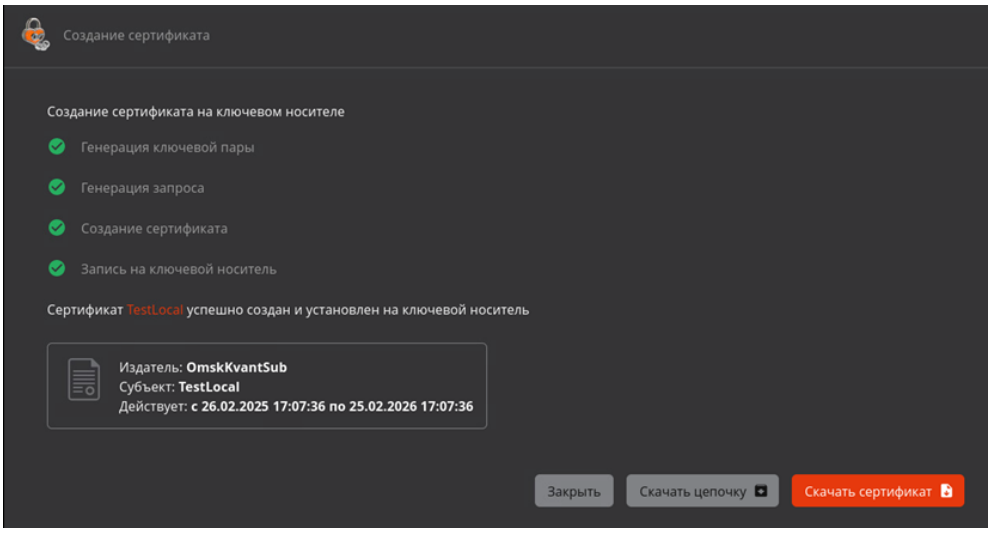


Рисунок 55 – Окно успешного создания сертификата субъекта на электронном ключе

- При успешном создании сертификата и выполнении всех условий ниже происходит его публикация в ресурсную систему:
  - сертификат был создан для субъекта, подключенного к ресурсной системе;
  - сертификат создан по шаблону, в котором включена публикация сертификата в ресурсную систему.

  В случае успешной публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Сертификат успешно опубликован в ресурсную систему».

  В случае ошибки публикации сертификата в ресурсную систему отобразится всплывающее сообщение «Ошибка публикации сертификата в ресурсную систему», также сертификат будет помечен, как требующий публикации. И при включенной настройке автопубликации будет произведена попытка его публикации в соответствии с расписанием.

Сообщения об ошибках при создании сертификата на ключевом носителе:

- В случае, если ПО JC–WebClient или или ПО «Рутокен Плагин» предварительно не установлено, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 56). Для выпуска сертификата на электронном ключе установите ПО JC–WebClient или «Рутокен Плагин».

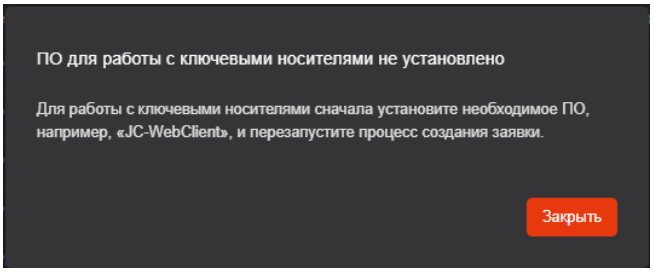


Рисунок 56 – ПО для работы с ключевыми носителями не установлено

- В случае, если электронный носитель не подключен, то администратор будет уведомлен об этом информационным сообщением (см. Рисунок 57). Для выпуска сертификата подключите электронный ключ и перезапустите мастер создания сертификата.

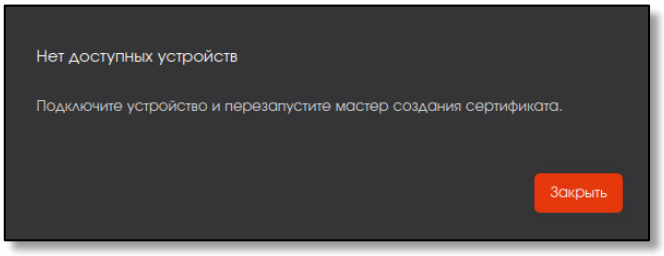


Рисунок 57 – Окно информационного сообщения «Нет доступных устройств»

В случае, если выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя, администратор будет уведомлён об этом информационным сообщением.

4.5 Раздел «Ресурсные системы»

Раздел «Ресурсные системы» обеспечивает получение данных субъектов с целью упрощенного выпуска сертификатов субъектам служб каталогов Linux и Microsoft, а также централизованную публикацию выпущенных сертификатов в карточку субъекта службы каталогов. Для авторизованного Оператора в списке присутствуют только те ресурсные системы, на субъекты которых ему прямо или косвенно[1] предоставлены полномочия в соответствии с текущими правилами доступа.

Переход в раздел «Ресурсные системы» осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 58).

- На основном экране «Ресурсной системы» отображены информационные поля (см. Рисунок 58):
  - имя домена – домен подключенной ресурсной системы;
  - последнее обновление – отображается дата и время последней синхронизации базы субъектов источника с базой данных программного компонента;
  - статус –статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице ниже;

Таблица 7 – Статусы ресурсной системы и критерии их присвоения

Статус ресурсной системы	Критерии присвоения статуса ресурсной системе
Ожидание обработки	Все точки подключения к данной ресурсной системе ожидают первой синхронизации (при регистрации ресурсной системы)
Успешно	Все точки подключения к ресурсной системе успешно синхронизированы
В процессе	Какая-либо точка подключения к ресурсной системе находится в процессе синхронизации или удаления
Ошибка	У ресурсной системы нет точек, находящихся в процессе синхронизации, и есть хотя бы одна точка, синхронизация которой завершена с ошибкой

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

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

[1] Путем наследования от группы безопасности, куда входит субъект, на основе которого создана учетная пользователя с ролью «Оператор».

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

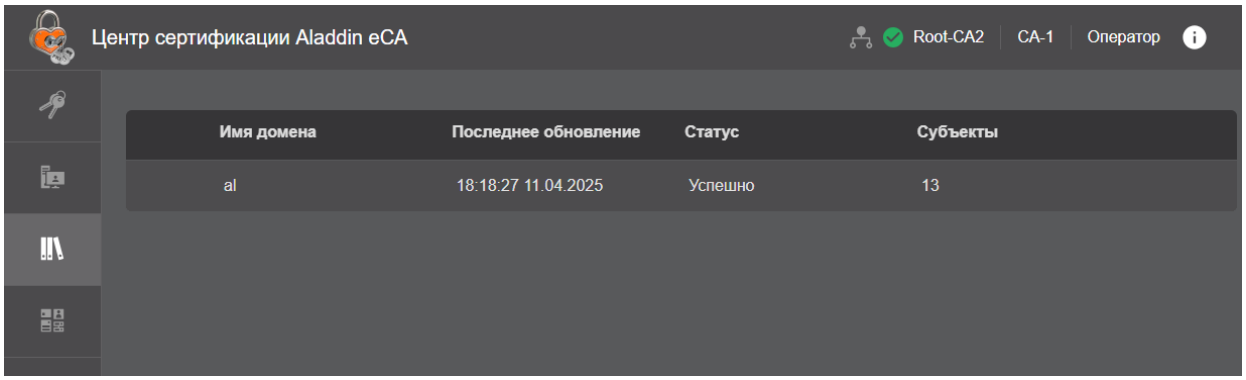


Рисунок 58 – Экран раздела «Ресурсная система»

- Центр сертификации Aladdin Enterprise Certification Authority позволяет загрузить из нескольких ресурсных систем Samba DC, РЕД АДМ, MS AD, FreeIPA, ALD PRO или Альт Домен:
  - список субъектов (пользователей, компьютеров и сервисов (только для ALD PRO и FreeIPA)), их атрибуты и сертификаты;
  - список и состав групп безопасности.
- В разделе «Ресурсные системы» доступны следующие возможности:
  - переход в карточку ресурсной системы (см. п. 4.5.1);
  - запуск полной синхронизации ресурсной системы (см. п. 4.5.2.3).

4.5.1 Карточка ресурсной системы

Просмотр информации о ресурсной системе возможен посредством окна «Карточка ресурсной системы».

- Переход к «Карточке ресурсной системы» (см. Рисунок 59) осуществляется при нажатии на строку ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 58).

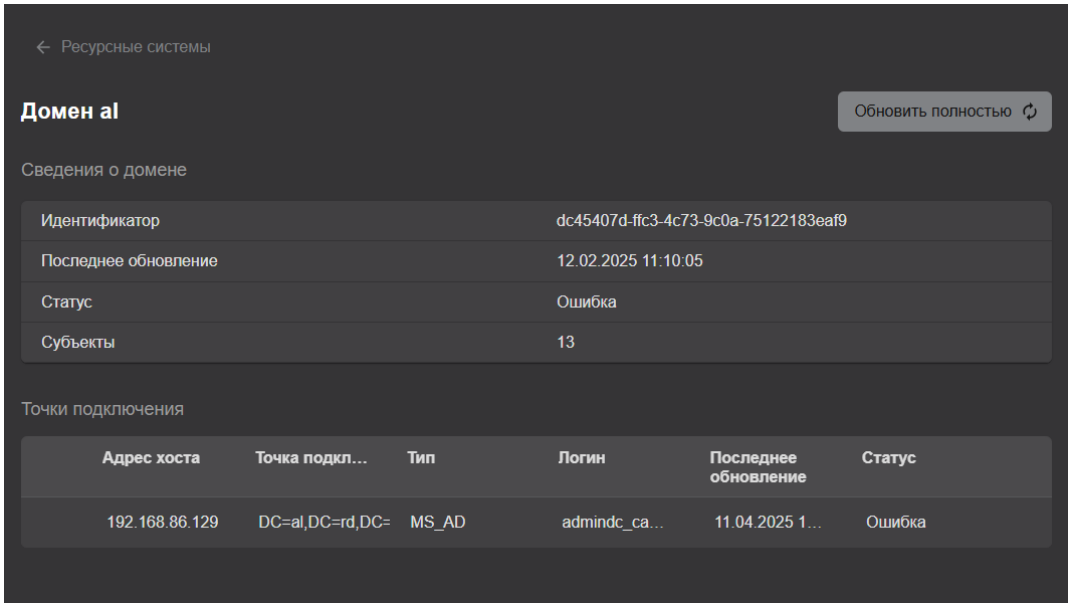


Рисунок 59 – Окно «Ресурсная система»

- Карточка ресурсной системы включает в себя следующую информацию:
  - Заголовок с именем домена в формате «Домен DomainName», где «DomainName» – имя домена;
  - Подраздел «Сведения о домене», включающий в себя таблицу со следующими полями:

- «Идентификатор». В данном поле указан идентификатор ресурсной системы;
- «Последнее обновление». В данном поле указаны дата и время последней попытки полной синхронизации ресурсной системы;
- «Статус». Статус ресурсной системы, который назначается в соответствии с критериями, приведенными в таблице выше (Таблица 7);
- «Субъекты». В данном поле указано количество субъектов, полученных из ресурсной системы.

– Подраздел «Точки подключения», содержащий таблицу со списком точек подключения к данной ресурсной системе, которая включает в себя поля:
  - «Адрес хоста» - полное доменное имя или IP-адрес точки подключения ресурсной системы;
  - «Точка подключения» – Base DN, который содержит в своем DN объекты, получаемые из точки подключения; указывается при регистрации точки подключения в формате Distinguished Name;
  - «Тип» – значение из списка: SambaDC, ALD PRO, MS AD, FreeIPA, RED ADM или Альт Домен.
    Указывается при регистрации точки подключения;
  - «Логин» – логин уполномоченного пользователя контроллера домена, указанный при регистрации точки подключения);
  - «Последнее обновление» – дата последней успешной полной синхронизации точки подключения;
  - «Статус» – статус точки подключения, который назначается в соответствии с критериями, приведенными в таблице ниже;

Таблица 8 – Статусы точки подключения и критерии их присвоения

Статус точки подключения	Критерии присвоения статуса точке подключения
Ожидание обработки	Точка подключения ресурсной системы ожидает первой синхронизации (при регистрации ресурсной системы)
Успешно	Точка подключения к ресурсной системе успешно синхронизирована
В процессе	Точка подключения к ресурсной системе находится в процессе синхронизации или удаления
Ошибка	Последняя синхронизация точки подключения завершена с ошибкой

- Доступные действия в карточке ресурсной системы:
  – запуск полной синхронизации ресурсной системы (см. п. 4.5.2);
  – запуск частичной синхронизации точки подключения (см. п. 4.5.2.3).

4.5.2 Синхронизация ресурсных систем

4.5.2.1 Виды синхронизации ресурсных систем

Центр сертификации Aladdin eCA поддерживает следующие виды синхронизации:

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

  При запуске полной синхронизации нескольких точек подключения процесс выполняется поочерёдно. Статус ресурсной системы, обновление которой выполняется, будет отображен как «В процессе».

По результатам обновления ресурсной системы будут:

- обновлены дата и время в поле «Последнее обновление» экранной формы «Ресурсная система»;
- в поле «Статус» экранной формы «Ресурсная система» будет отображён результат синхронизации «Успешно» или «Ошибка»;
- выведено всплывающее сообщение по результату синхронизации «Успешно» или «Ошибка».

- частичная. При частичной синхронизации выполняется обновление всех данных, полученных при полной синхронизации, за исключением сведений об удалении субъектов, организационных групп и групп безопасности из ресурсной системы.

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

4.5.2.2 Режимы обновления ресурсной системы

- Автоматическая частичная и полная синхронизация всех зарегистрированных точек подключения к ресурсным системам выполняется по расписанию в соответствии с заданным CRON-выражением администратором.
- Ручной запуск полной синхронизации ресурсной системы (см. п. 4.5.2.3);
- Ручной запуск частичной синхронизации точки подключения (см. п. 4.5.2.4);
- В результате обновления ресурсной системы состав объектов будет синхронизирован:
  - переименованы существующие объекты;
  - изменены существующие связи (включения в группы и т.д.);
  - обновлён список субъектов (добавлены новые группы и объекты, удалены субъекты).
- 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 9. Если данные поля отсутствуют в описании субъекта в подключенном домене, то в шаблоне при выпуске сертификата соответствующие поля заполняются пустыми значениями.

Таблица 9 – Преобразование данных субъектов ресурсной системы

Атрибут субъекта АЕСА-CA	**Поле в MS AD, SambaDC, RED ADM, Альт Домен**		**Поле в ALD PRO, FreeIPA**		
	Тип субъекта		**Тип субъекта**		
	Пользователь	**Компьютер**	**Пользователь**	**Компьютер**	**Сервис**
Id	ObjectGUID	ObjectGUID	ipaUniqueID	ipaUniqueID	ipaUniqueID
Common name	cn	cn	cn	cn	krbPrincipalName
			uid		
Initials	-	-	initials	-	-
Surname	sn	-	sn	-	-
Given Name	givenName	-	givenName	-	-
Organization	-	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Name	name	name	-	serverHostName	-
MS GUID	-	ObjectGUID	-	-	-
Domain Qualifier	distigushedName	distigushedName	entrydn	entrydn	entrydn
Description	description	-	-	-	-

Атрибут субъекта АЕСА-CA	Поле в MS AD, SambaDC, RED ADM, Альт Домен		Поле в ALD PRO, FreeIPA		
	Тип субъекта		Тип субъекта		
	Пользователь	Компьютер	Пользователь	Компьютер	Сервис
DNS Name	-	dNSHostName	-	fqdn	-
Email Address (Mail)	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
RFC 822 NAME	mail	-	mail	-	-
	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
MS UPN	userPrincipalName	-	krbPrincipalName	krbPrincipalName	krbPrincipalName
Unique Identifier (UID)	-	-	uid	-	-
Kerberos KPN, Kerberos 5 Principal	-	-	-	krbPrincipalName	-
SID	objectSid	objectSid	-	-	-

4.5.2.3 Ручной запуск полной синхронизации ресурсной системы

Запуск полной синхронизации ресурсной системы может осуществляться путем нажатия на кнопку <Обновить> для ресурсной системы в разделе «Ресурсные системы» (см. Рисунок 60) или путем нажатия на кнопку <Обновить полностью> в карточке ресурсной системы (см. Рисунок 60). Ресурсная система, для которой выполняется полная синхронизация, имеет статус «В процессе».

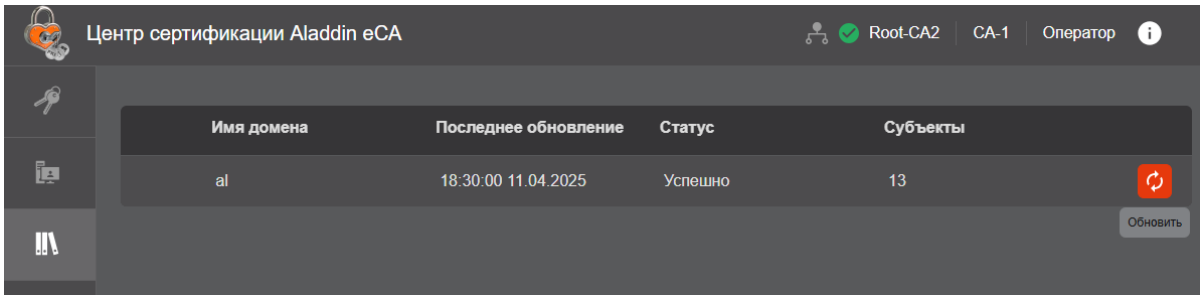


Рисунок 60 – Запуск полной синхронизации ресурсной системы из раздела «Ресурсные системы»

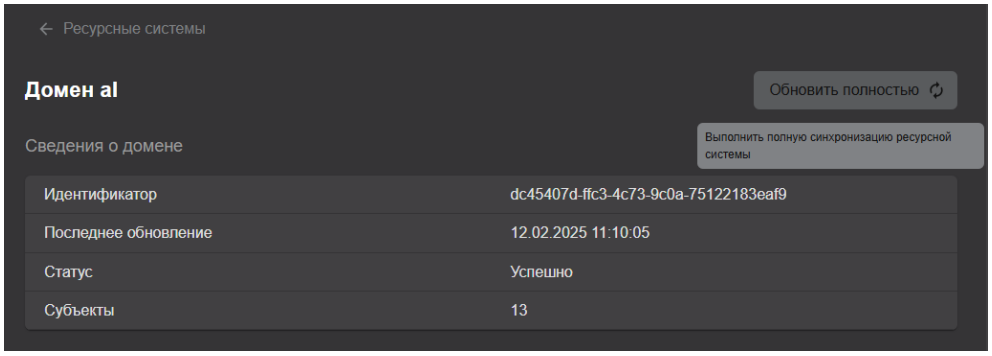


Рисунок 61 – Запуск полной синхронизации ресурсной системы из карточки ресурсной системы

4.5.2.4 Ручной запуск частичной синхронизации точки подключения

Запуск частичной синхронизации точки подключения осуществляться путем нажатия на кнопку <Обновить> для точки подключения в карточке ресурсной системы (см. Рисунок 62).

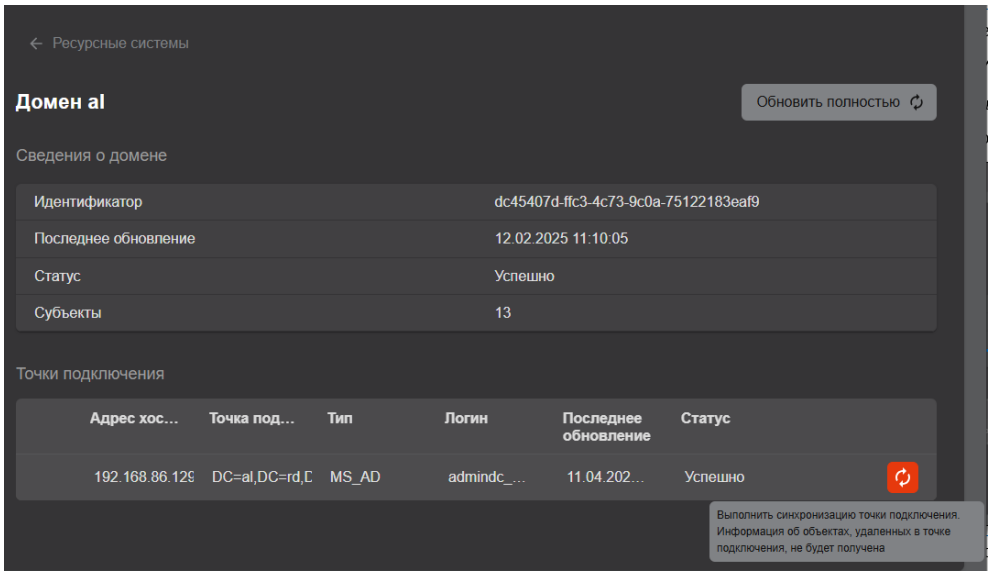


Рисунок 62 – Запуск частичной синхронизации точки подключения

4.6 Раздел «Шаблоны»

Раздел «Шаблоны» позволяет Операторам просматривать шаблоны, доступ к которым им предоставлен в соответствии с назначенными правилами доступа.

- Переход в раздел «Шаблоны» (см. Рисунок 63) осуществляется через боковое меню, расположенное слева на экране.

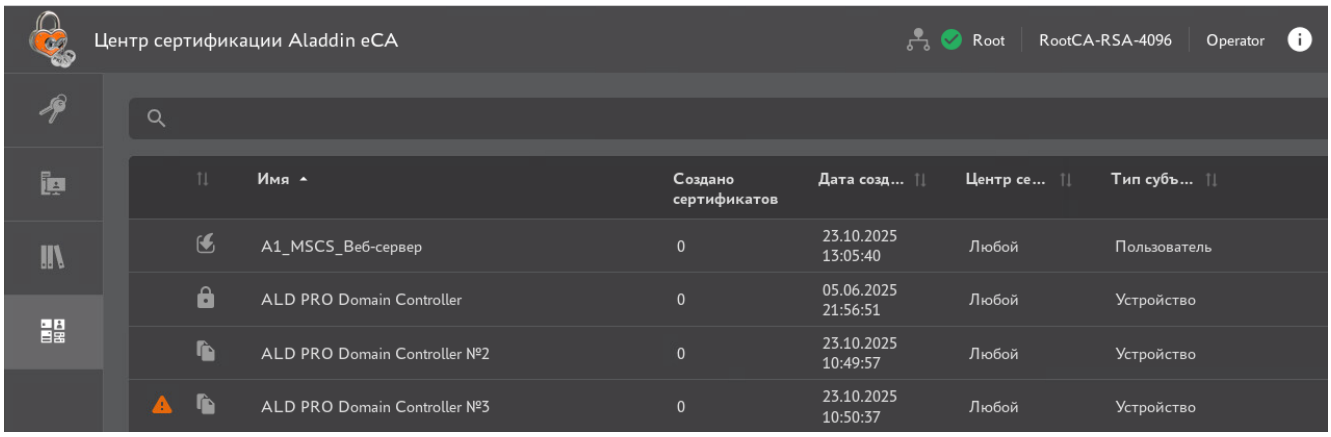


Рисунок 63 – Раздел «Шаблоны»

- На экранной таблице раздела «Шаблоны» отображены следующие колонки:
  -  - Признак отсутствия контроля соответствия полей в сертификате атрибутам субъекта при выпуске сертификата по данному шаблону.

> **Внимание! Контроль соответствия полей не выполняется только при выпуске сертификатов через REST API. Использование таких шаблонов в информационных системах крайне не рекомендуется. При использовании таких шаблонов контроль соответствия значений в SDN и SAN полях сертификатов необходимо обеспечивать средствами внешней системы, и доступ к таким шаблонам в Центре сертификатов Aladdin eCA должен быть строго ограничен.**

  - условное обозначение вида шаблона:

-  – предустановленные по умолчанию шаблоны, созданные в момент установки Центра сертификации Aladdin eCA. Данный вид шаблонов не подлежит редактированию;
-  – клонированные шаблоны для редактирования с целью создания нового шаблона с заданными параметрами;
-  – импортированные шаблоны (например, из MS CS).

– имя – содержит название шаблона;

– создано сертификатов – количество сертификатов, выпущенных по данному шаблону, владельцами которых являются субъекты, на управление которыми данному Оператору назначены полномочия;

– дата создания – дата создания (клонирования) шаблона;

– центр сертификации – центр сертификации, в котором будет выполняться выпуск сертификатов по данному шаблону. Если в данном параметре шаблона указано значение «Любой», то выпуск сертификатов по данному шаблону доступен в любом центре сертификации. При этом для выпуска сертификатов будет использоваться активный в данный момент центр сертификации. Для предустановленных шаблонов данный параметр всегда имеет значение «Любой»;

> **Внимание! При обновлении ПО с версии 2.1.2 до версии 2.3 всем шаблонам для параметра «Центр сертификации» устанавливается значение «Любой».**

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

> **Внимание! При обновлении ПО с версии 2.1.2 до версии 2.3 ранее применяемый для шаблонов параметр «Тип сертификата» преобразовывается в параметр «Тип субъекта» по следующим правилам. Шаблон с типом сертификата «Корневой» принимает значение для типа субъекта «Корневой ЦС». Шаблон с типом сертификата «Подчиненный» принимает значение для типа субъекта «Подчиненный ЦС». Шаблон с типом сертификата «Пользовательский» принимает значение для типа субъекта «Пользователь» (за исключением шаблонов по умолчанию «WEB-Server», «ECA-WEB-Server», «OCSP Signer», «Domain Controller», «ALD PRO Domain Controller», «SCEP Management», для которых устанавливается заначение типа субъекта «Устройство»).**

Список предустановленных шаблонов[1]:

- User;
- WEB-Client;
- WEB-Server;
- Domain Controller;
- Smartcard Logon;
- S/MIME;
- ALD PRO Domain Controller;
- ALD PRO Smartcard Logon;
- OCSP Signer;
- Root CA;

[1] Подробное описание полей предустановленных шаблонов см. в Приложение 1. Описание полей по умолчанию предустановленных шаблонов сертификатов

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

Внимание! При обновлении ПО до версии 2.3 все предустановленные в версии 2.1.2 шаблоны считаются устарешими (в названия шаблонов добавлена пометка [Deprecated]). В набор шаблонов добавлены копии устаревших шаблонов с измененными параметрами (за исключением шаблонов «ECA-WEB-Server» и «ECA-Auth»). Шаблон «ECA-User» переименован в «User».

- Действия доступные над всеми видами шаблонов для операторов:
  - просмотр полного списка доступных шаблонов или по результатам поиска;
  - просмотр параметров шаблона в его карточке.
- Все шаблоны на экране раздела отображаются в виде таблицы с пагинацией.

4.6.1 Поиск шаблонов

Строка поиска (см. Рисунок 64) предназначена для поиска шаблонов в экранной таблице по содержимому колонки «Имя». Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

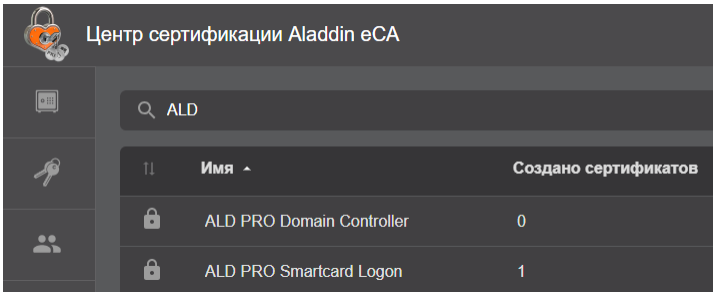


Рисунок 64 – Поисковая строка в разделе «Шаблоны»

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

4.6.2 Сортировка шаблонов

- Средство сортировки списка шаблонов представлено элементом выбора направления сортировки в заголовках колонок экранной таблицы (см. Рисунок 63) – полями «Имя» (сортировка в алфавитном порядке), «Дата создания» (сортировка в порядке убывания/возрастания), «Тип субъекта» (упорядочивание по типу субъекта в алфавитном порядке), по виду шаблона (предустановленный, импортированный, клонированный), «Центр сертификации» (упорядочивание по названию центра сертификации в алфавитном порядке).

- Сортировка происходит только по одному значению при нажатии на соответствующий заголовок колонки таблицы.
- Активное поле таблицы, по которому выполнена сортировка, обозначено знаком с правой стороны от заголовка таблицы.
- Для сброса сортировки в колонке несколько раз нажмите на заголовке колонки, для которой применена сортировка.

4.6.3 Карточка шаблона

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

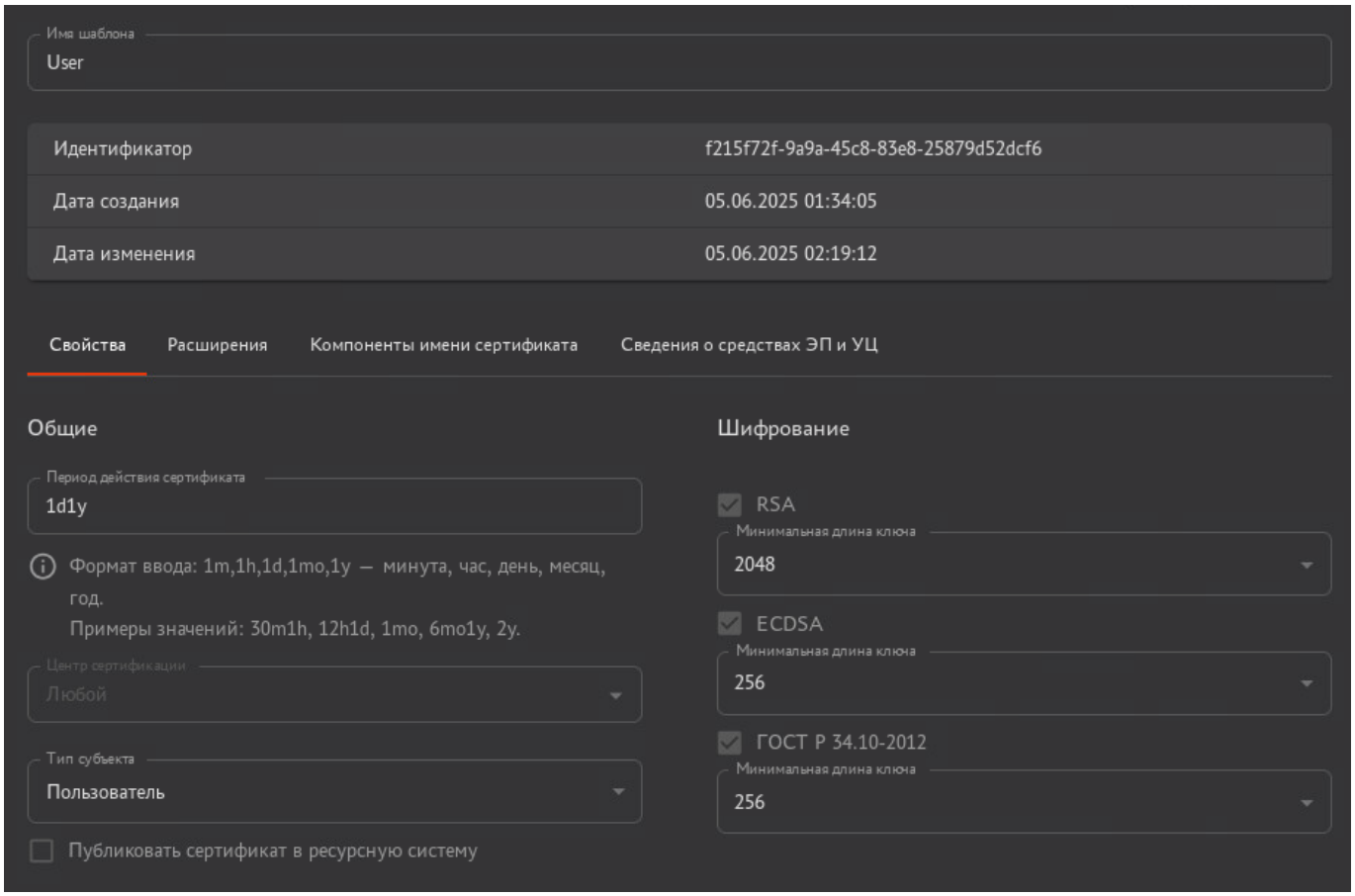


Рисунок 65 – Окно карточки шаблона

- В открывшемся окне оператору доступны:
  - поле «Имя шаблона»;
  - поле «Идентификатор», содержащее постоянный идентификатор шаблона;
  - поле «Дата создания шаблона»;
  - поле «Дата изменения шаблона»;
  - информация о шаблоне, сформированная в виде вкладок «Свойства», «Расширения», «Компоненты имени субъекта».

4.6.3.1 Вкладка шаблона «Свойства»

На вкладке шаблона «Свойства» для просмотра доступны поля (см. Рисунок 66):

- общие:
  - поле «Период действия dсертификата». Формат значения в поле: 1m, 1h, 1d, 1mo, 1y - , минута, час, день, месяц, год (примеры: 1d1y, 30m1h);

- чек-бокс «Публиковать сертификат в ресурсную систему».
- поле «Центр сертификации» - центр сертификации, в котором возможен выпуск сертификатов по данному шаблону;
- поле «Тип субъекта» - определяет тип субъекта, для которого предназначен данный шаблон (корневой Центр сертификации, подчинённый Центр сертификации, устройство, пользователь).

- шифрование:
  - RSA;
  - ECDSA;
  - ГОСТ Р 34.10-2012.

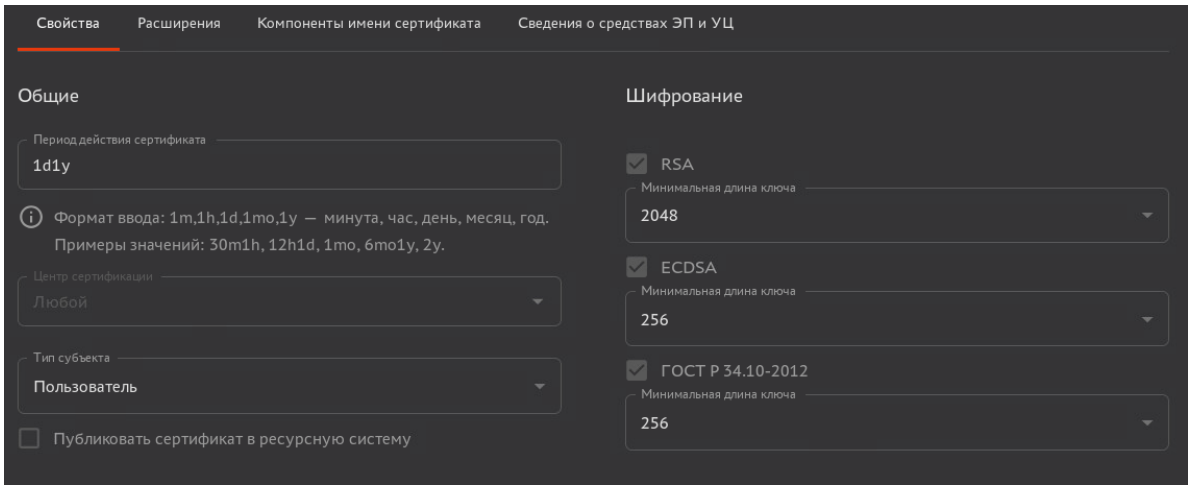


Рисунок 66 – Вкладка «Свойства» шаблона сертификата

4.6.3.2 Вкладка шаблона «Расширения»

На вкладке шаблона «Расширения» для просмотра доступны (см. Рисунок 67):

- поле «Использование ключа»;
- поле «Расширенное использование ключа»;
- OID политики сертификата;
- чек-бокс «Считать это расширение критическим» для списка «Использование ключа»;
- чек-бокс «Считать это расширение критическим» для списка «Расширенное использование ключа».
- чек-бокс «Включить SID субъекта в сертификат». При включенной опции в поле сертификата субъекта с OID 1.3.6.1.4.1.311.25.2 будет записан его SID (при наличие данного атрибута у субъекта). SID может быть получен только для субъектов ресурсных систем MS AD, SambaDC, РЕД АДМ и Альт Домен.

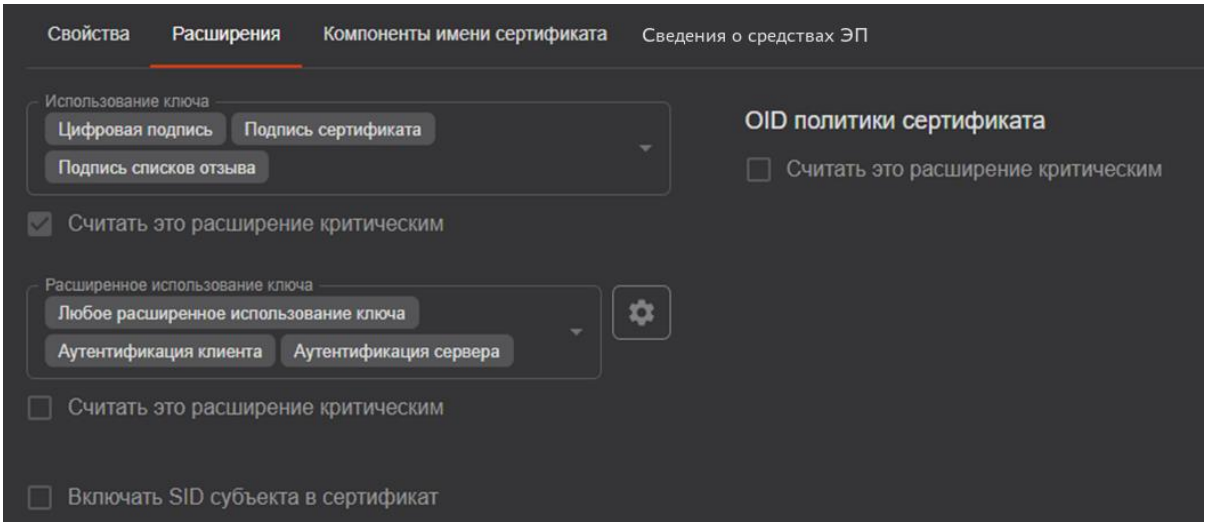


Рисунок 67 – Вкладка «Расширения» шаблона сертификата

4.6.3.3 Вкладка шаблона «Компоненты имени сертификата»

На вкладке шаблона «Компоненты имени сертификата» для просмотра доступны (см. Рисунок 68):

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

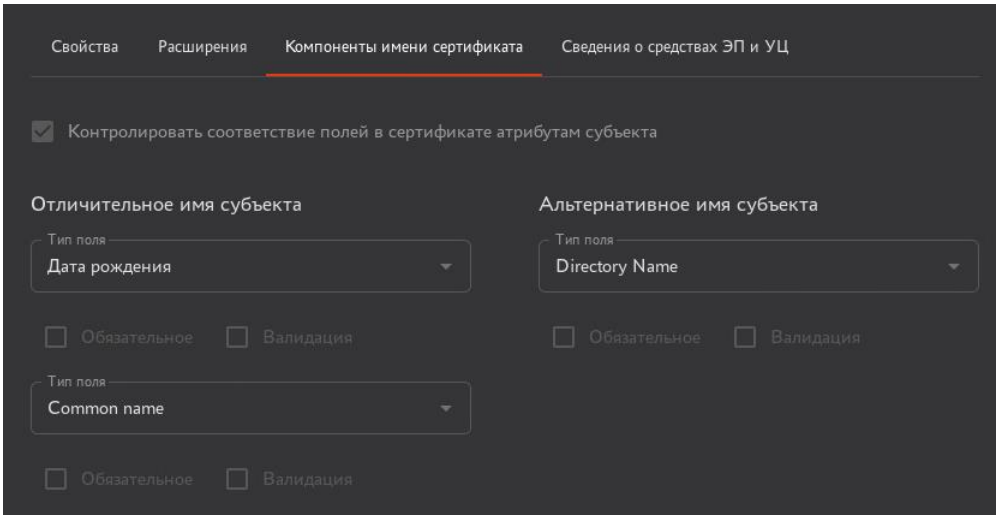


Рисунок 68 – Вкладка «Компоненты имени сертификата» шаблона сертификата

4.6.3.4 Вкладка шаблона «Сведения о средствах ЭП»

На вкладке шаблона «Сведения о средствах ЭП» доступны:

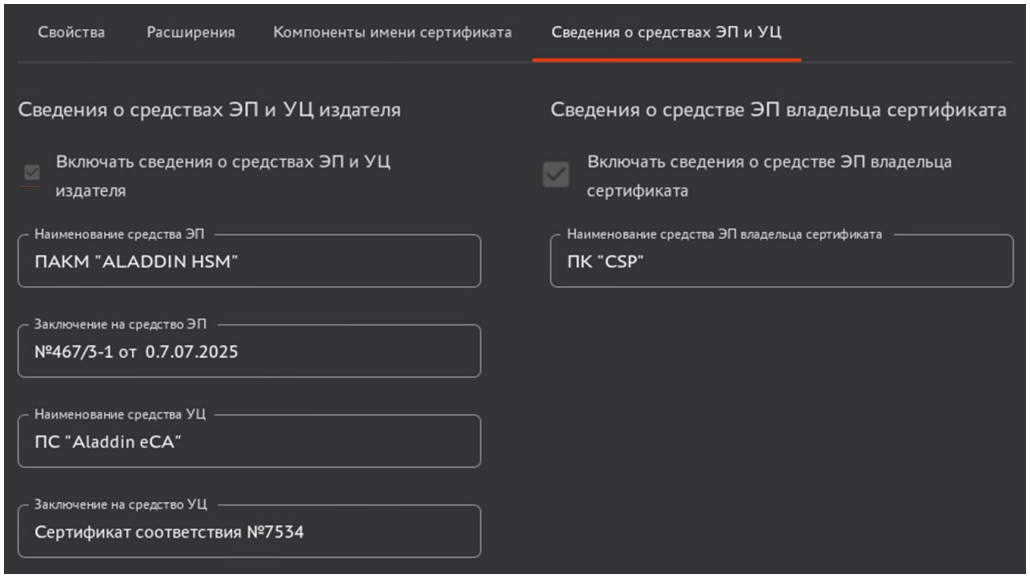


Рисунок 69 – Вкладка «Сведения о средствах ЭП»

- В подразделе «Сведения о средствах ЭП и УЦ издателя» доступны:
  - Чек-бокс «Включать сведения о средствах ЭП и УЦ издателя» - при включенной опции все поля данного подраздела, сведения из которых будут включены в сертификаты, должны быть заполнены.
  - Поле «Наименование средства ЭП» - в поле указывается наименование средства ЭП удостоверяющего центра (далее -УЦ) издателя.
  - Поле «Заключение на средство ЭП» - в поле указывается номер и дата выдачи заключения на средство ЭП удостоверяющего центра издателя.
  - «Наименование средства УЦ» - в поле указывается наименование средства УЦ издателя.

  - «Заключение на средство УЦ» - в поле указывается номер и дата выдачи заключения на УЦ издателя.
- Если в подразделе «Сведения о средстве ЭП владельца сертификата» включен чек-бокс «Включать сведения о средстве ЭП владельца сертификата», то поле «Наименование средства ЭП владельца сертификата» заполнено и сведения из него будут включены в сертификаты, выпущенные по данному шаблону.

5 ФУНКЦИИ УПРАВЛЕНИЯ ЦЕНТРА РЕГИСТРАЦИИ ALADDIN ERA

Данный раздел описывает функции управления Центра регистрации Aladdin eRA, доступные учётной записи с ролью «Оператор».

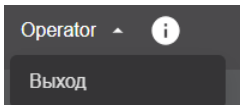
5.1 Верхняя панель

Верхняя панель Центра регистрации фиксирована и отображается на любом шаге или переходе между разделами.

Рисунок 70 – Верхняя панель окна «Центра регистрации»

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

Верхняя панель содержит следующие элементы:

• 	- текущая авторизация учётной записи пользователя, при нажатии неё отображается меню с кнопкой <Выход>
• 	- сведения о текущей версии программы, контактная информация разработчика, права на программное обеспечение.

5.2 Боковая панель

Боковая панель Центра регистрации Aladdin eRA закреплена и отображается на любом шаге или переходе между разделами при ширине окна браузера больше или равной 1200px. При ширине окна браузера менее 1200px боковая панель скрыта и отображается только при нажатии на кнопку  , которая отображается только в данном режиме.

Полный и компактный виды боковой панели показаны на рисунке ниже. Компактный вид боковой панели приведён на рисунке ниже. Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

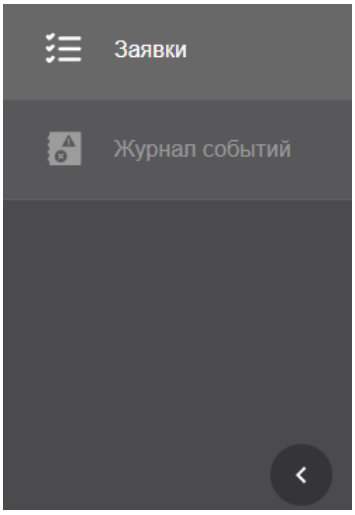


Рисунок 71 – Полный вид боковой панели

Рисунок 72 – Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции программы, и предназначена для организации управления Центром регистрации:

- Раздел «Заявки» – в данном разделе возможно:
  - просмотреть существующие заявки;
  - произвести поиск заявки по номеру заявки;
  - создать заявку на выпуск сертификата на основании запроса;
  - создать заявку на выпуск сертификата с закрытым ключом PKCS#12;
  - создать заявку на выпуск сертификата на ключевом носителе;
  - отменить заявку;
  - обработать заявку (выпустить сертификат или отклонить заявку);
  - скачать сертификат;
  - импортировать сертификат на ключевой носитель;
  - скачать цепочку сертификатов;
  - скачать контейнер закрытого ключа PKCS#12;
  - скачать CRL издателя;
  - скачать цепочку сертификатов издателя;
  - просмотреть карточку заявки;
  - отозвать сертификаты.
- Раздел «Журнал событий» - в данном разделе возможно:
  - посмотреть в интерактивном режиме полный или выборочный (с применением фильтров) журнал событий;
  - произвести поиск событий по описанию;
  - скачать журнал событий в формате .csv по выбранным параметрам экспорта.

5.3 Раздел «Заявки»

Внимание! Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

5.3.1 Общие сведения о заявках

Раздел «Заявки» обеспечивает возможности создания, отслеживания, обработки заявок на выпуск сертификатов, а также получения файлов, являющихся результатом выполнения заявки, включая скачивание и импорт сертификатов на ключевой носитель.

Пользователь с ролью «Оператор» (далее – Оператор) может просматривать созданные им заявки, просматривать и обрабатывать заявки для доступных ему субъектов[1], создавать заявки для любых субъектов Центра сертификации Aladdin eCA, к которому подключён Центре регистрации Aladdin eRA, скачивать и отзывать сертификаты, выпущенные по заявкам доступным ему субъектов.

Процесс подачи заявки на выпуск сертификата включает:

- Выбор шаблона, по которому будет выпущен сертификат.

Оператору доступны шаблоны в соответствии с установленными для субъекта РС в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно субъекту РС, так и группе безопасности, в которую входит субъект. Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA Оператором как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме (подтверждение или отклонение заявки).

- Редактирование (при необходимости) атрибутов сертификата согласно выбранному шаблону (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10 [2]).
- Указание пароля для защиты контейнера PKCS#12 (только при подаче заявки с закрытым ключом PKCS#12 [3]).
- Выбор алгоритма и длины ключа для генерации ключевой пары (не выполняется при подаче заявки на основание запроса на сертификат PKCS#10).

Оператору доступны следующие действия по управлению заявками на выпуск сертификатов:

- Подача (создание) новой заявки для любого субъекта РС:
  - На основании запроса PKCS#10 (см. раздел 5.3.4.1).
  - С закрытым ключом PKCS#12 (см. раздел 5.3.4.2).
  - На ключевом носителе (см. раздел 5.3.4.3).
- Просмотр информации о созданных заявках для доступных ему субъектов РС (см. раздел 5.3.2).
- Просмотр карточек заявок с подробной информацией (в том числе информации о сертификате после его выпуска в Центре сертификации Aladdin eCA по данной заявке) для доступных ему субъектов РС (см. раздел 5.3.3).
- Отмена созданной заявки, которая еще не рассмотрена уполномоченными пользователями Центра регистрации Aladdin eRA с ролями «Администратор» и «Оператор» или обработана после создания Центром регистрации Aladdin eRA с ошибкой (см. раздел 5.3.5).
- Обработка заявок на сертификаты от доступных ему согласно правилам доступа субъектов РС.

Заявка на выпуск сертификата имеет следующие атрибуты:

- Номер заявки – уникальный идентификатор, назначаемый заявке при создании.
- Статус – текущий статус заявки:

---

[1] Заявки, у которых получателем сертификата является субъект, доступный данному Оператору в соответствии с правилами доступа, назначенными в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA

[2] В соответствии с документом «RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7».

[3] В соответствии с документом «RFC 7292. PKCS #12: Personal Information Exchange Syntax v1.1»

- Ошибка выпуска – выпуск сертификата по данной заявке завершился ошибкой.
- Отклонена – заявка отклонена уполномоченным пользователем Центра регистрации Aladdin eRA.
- Ожидает подтверждения – заявка создана, получателю сертификатов (субъекту) назначены правила выпуска с автоматизированной (ручной) обработкой заявок уполномоченным пользователем Центра регистрации Aladdin eRA.
- Выполнена – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат.
- Отменена – заявка отменена получателем сертификатов (субъектом) или иным уполномоченным пользователем Центра регистрации Aladdin eRA.
- Ожидает импорта на КН – заявка обработана, в Центре сертификации Aladdin eCA для получателя сертификатов (субъекта) успешно выпущен сертификат, который ожидает импорта на ключевой носитель.
- Новая – статус присваивается заявке при ее регистрации, сразу после этого происходит обработка заявки и её статус изменяется. Данный статус может быть отображен в веб-интерфейсе в случае ошибки при первичной обработке заявки.

- Общая информация о заявке:
  - Сценарий – наименование сценария, по которому была создана заявка на выпуск сертификата:
    - На основании запроса (PKCS#10).
    - С закрытым ключом (PKCS#12).
    - На ключевом носителе.
    - WSTEP [1].
  - Шаблон – шаблон, по которому будет или уже выпущен сертификат.
  - Центр сертификации - центр сертификации, в котором будет или уже выпущен сертификат по данной заявке, на основании используемого в сценарии создания заявки шаблона.
  - Внешний идентификатор – идентификатор из запроса на выпуск сертификата PKCS#10.
  - Дата создания – дата и время создания заявки.
  - Дата обработки – дата и время последней смены статуса (обработки) заявки (например, создание или отмена заявки).
  - Комментарий – комментарий, указанный уполномоченным пользователем Центра регистрации Aladdin eRA при обработке заявки.
- Информация о получателе сертификата:
  - Идентификатор субъекта в Центре сертификации Aladdin eCA.
  - Название ресурсной системы субъекта.
  - «Common Name», указанное в заявке на сертификат.
  - Имя получателя (UPN) – содержит User Principal Name получателя сертификата по данной заявке.
- Информация об истории изменения заявки:
  - Дата – дата и время события, связанного с изменением заявки.
  - Имя учётной записи – отображаемое имя пользователя (получателя сертификатов), сделавшего изменение в заявке.
  - Событие – описание события, связанного с изменениями заявки (например, создание заявки).

[1] Заявки с типом «WSTEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов клиентов по протоколу MS-WSTEP.

5.3.2 Просмотр записей о заявках

Оператору доступен просмотр своих заявок и заявок от доступных ему согласно правилам доступа субъектов.

Для просмотра информации о заявках на сертификаты подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.

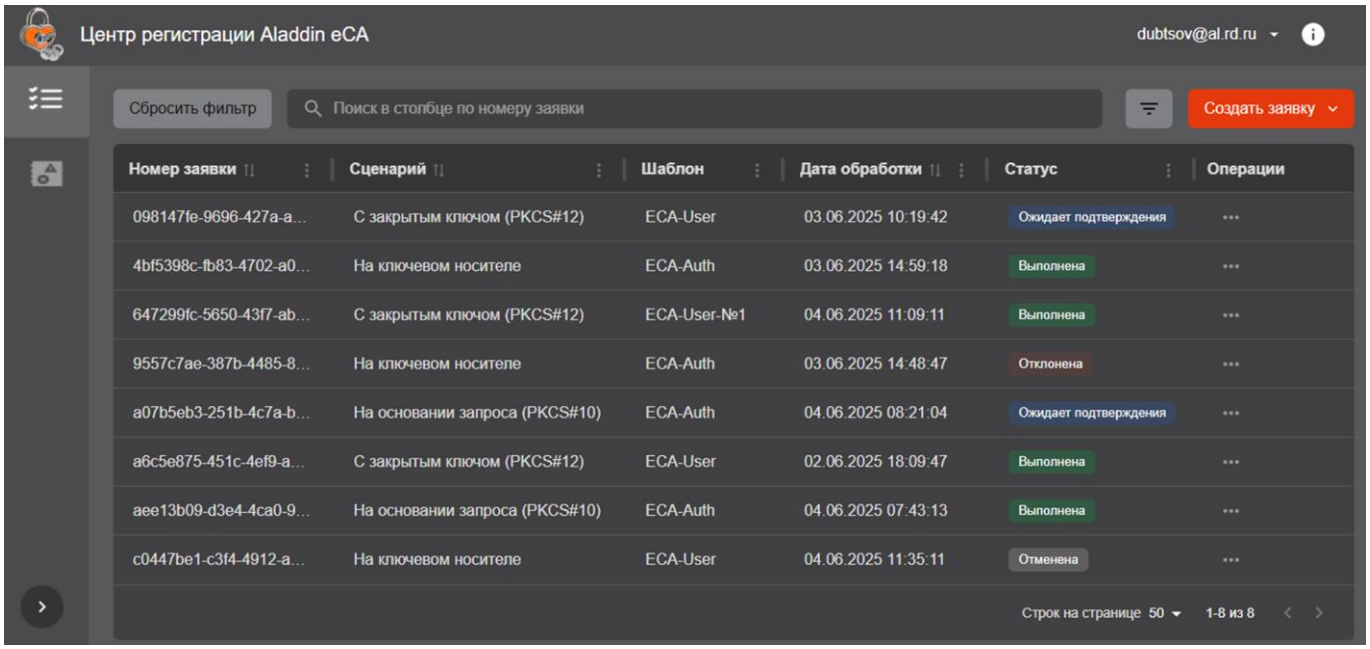


Рисунок 73 – Просмотр списка заявок [1]

Информация о заявках отображается списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты заявок на выпуск сертификатов:

- Номера заявок.
- Сценарии, по которым заведены заявки.
- CN – содержит «Common Name», указанный в заявке на сертификат.
- Имена получателей (UPN) – содержит User Principal Name получателя сертификата по данной заявке.
- Наименования шаблонов, по которым будут и уже выпущены сертификаты по заявкам.
- Дата и время последней смены статуса (обработки) заявок.
- Текущие статусы заявок.

Записи о заявках выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 74).

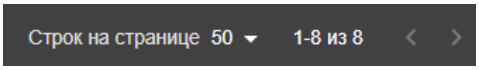


Рисунок 74 – Инструменты навигации списка заявок

Описание инструментов навигации:

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

[1] Некоторые колонки скрыты для наглядности списка заявок.

Для удобства анализа информации о заявках в списке вы можете управлять видимостью колонок таблицы с заявками. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок **<Действие колонки>** и в открывшемя списке [1] выберите **<Скрыть [название колонки] колонку>** (см. Рисунок 75). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок **<Действие колонки>** и в открывшемя списке выберите **<Показать все колонки>** (см. Рисунок 75).

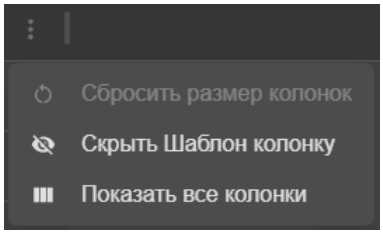


Рисунок 75 – Список действий с колонкой **[Шаблон]**

Для поиска заявок в списке вы можете выполнить сортировку (упорядочивание) записей о заявках по выбранному атрибуту, представленному в соответствующей колонке. В зависимости от информации, представленной в колонке списка, упорядочивание записей может выполняться по следующим принципам:

- В алфавитном порядке.
- В порядке убывания или возрастания временных меток.

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

- По номеру заявки в алфавитном порядке.
- По сценариям заведения заявок в алфавитном порядке.
- По содержимому полей «CN» и «Имя получателя (UPN)» в алфавитном порядке.
- По дате и времени последней смены статуса (обработки) заявок в порядке убывания или возрастания временных меток.

По умолчанию сортировка записей о заявках в списке выполнена по номеру заявки в алфавитном порядке (в порядке возрастания).

Чтобы выполнить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [2] выберите:

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

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками [3]:

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

[1] Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

[2] Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

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

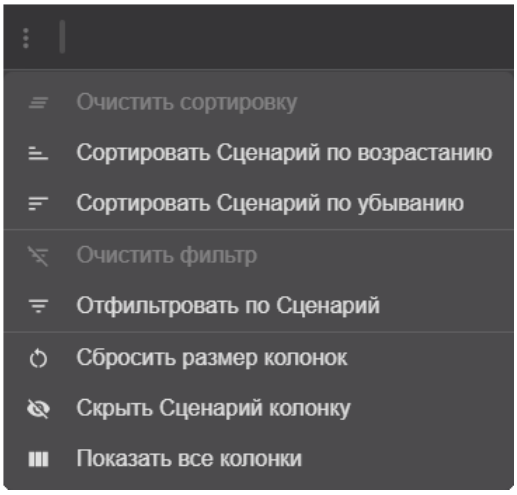


Рисунок 76 – Список действий с колонкой **[Сценарий]**

Чтобы отменить сортировку записей о заявках по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [1] выберите **<Очистить сортировку>**.

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

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

- По сценариям заведения заявок.
- По дате и времени последней смены статуса (обработки) заявок.
- По статусам заявок.

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

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

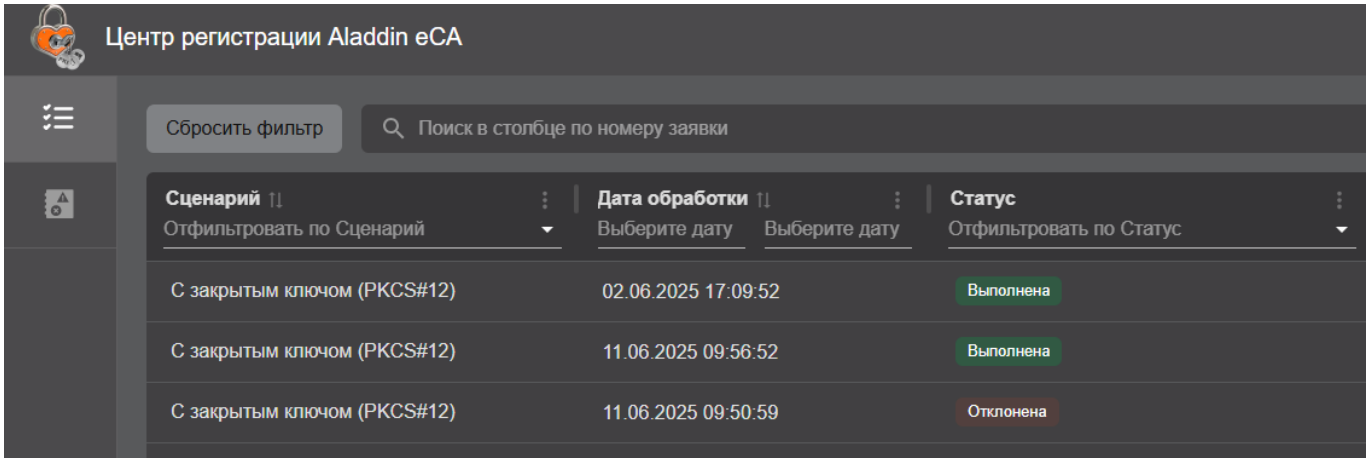


Рисунок 77 – Отображение фильтров в заголовках колонок включено

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

[1] Набор действий колонок отличается в зависимости от атрибута заявки, представленного в данной колонке.

Фильтры по атрибутам заявок, представленным в колонках **[Сценарий]** и **[Статус]**, обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов.

Фильтр по атрибуту заявок, представленном в колонке **[Дата обработки]**, обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок.

Признаком применения фильтра является значок в заголовке соответствующей колонки.

а) б) в)

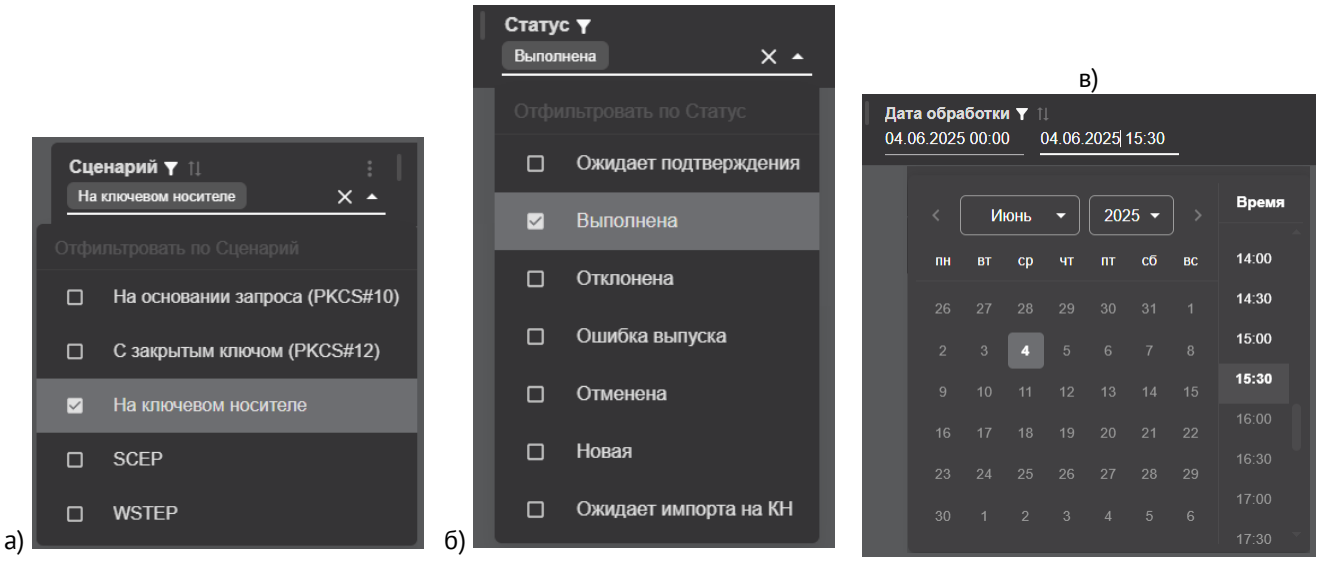


Рисунок 78 – Указание критериев выборки в фильтрах

Чтобы отменить действие определенного фильтра, щелкните в заголовке колоноки значок **<Действие колонки>** и в открывшемя списке выберите **<Очистить фильтр>** или щелкните в заголовке колонки значок (только для колонок **[Сценарий]** и **[Статус]**.

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

Чтобы выполнить выборку записей о заявках по их номерам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в номере заявки. Для отмены выборки заявок по их номерам щелкните в поисковой строке значок .

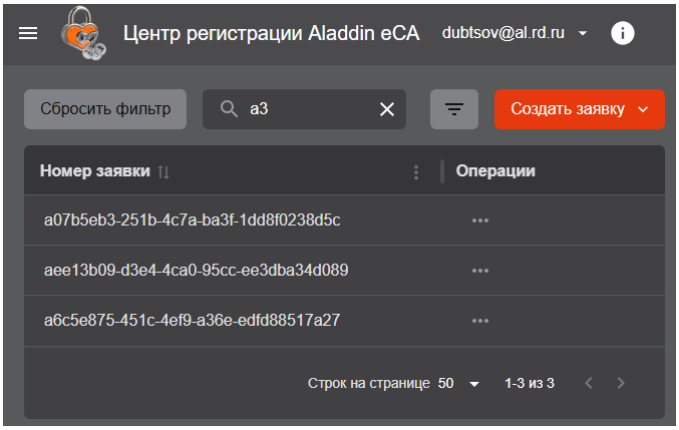


Рисунок 79 – Выборка заявок по их номерам с помощью поисковой строки

5.3.3 Просмотр карточки заявки на выпуск сертификата

Карточка заявки содержит представленную в удобном для анализа виде подробную информацию о заявке, а также информацию о сертификате в случае, если по заявке уже выпущен сертификат.

Чтобы открыть карточку заявки:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.

- Найдите нужную заявку (см. раздел 5.3.2) и щелкните запись о ней в списке.

В результате откроется карточка заявки.

Карточка заявки, по которой еще не выпущен сертификат, представлена на рисунке ниже. Описание атрибутов заявки приведено в разделе 5.3.1.

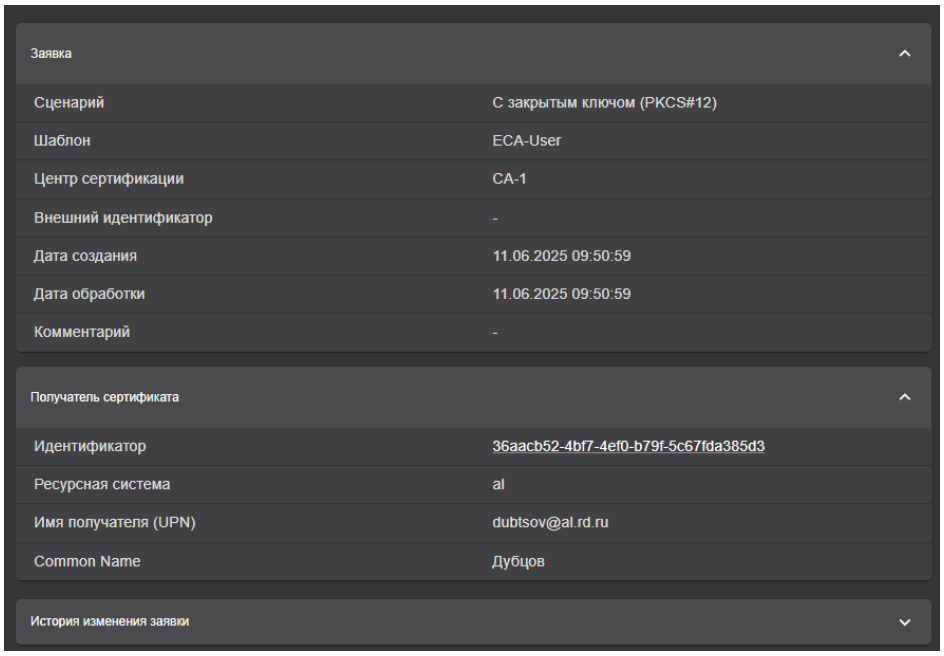


Рисунок 80 – Карточка заявки, по которой еще не выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат, представлена на рисунке ниже. Описание атрибутов заявки приведено в разделе 5.3.1.

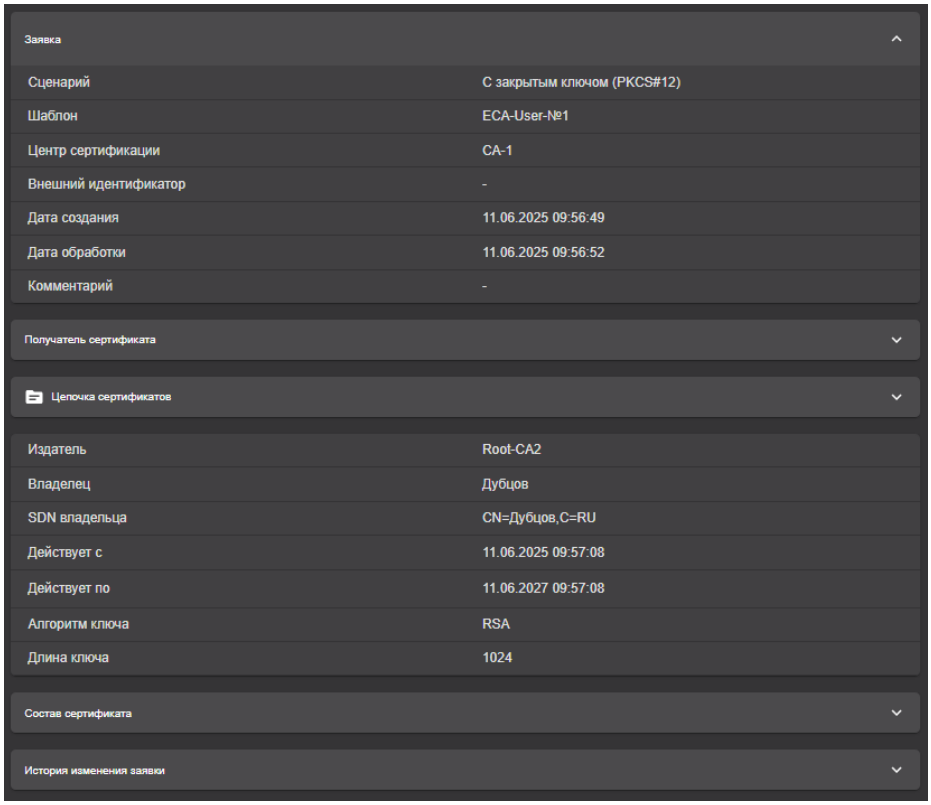


Рисунок 81 – Карточка заявки, по которой выпущен сертификат

Карточка заявки, по которой уже выпущен сертификат, содержит также информацию о выпущенном по ней сертификате (статус сертификата, блоки «Цепочка сертификатов», «Информация о сертификате» и «Состав сертификата»).

Статус сертификата отображен на панели инструментов карточки заявки. После выпуска сертификату назначается статус «Активирован». Оператор уполномочен при необходимости отозвать сертификат (см. раздел 5.3.7.7).

В блоке «Цепочка сертификатов» (см. Рисунок 82) представлена иерархическая коллекция сертификатов, которая ведёт от сертификата, выпущенного по данной заявке, к корню доверия (корневому центру сертификации).

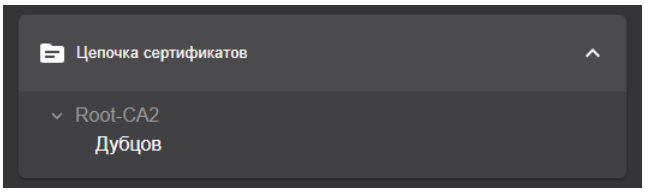


Рисунок 82 – Блок «Цепочка сертификатов»

В блоке «Информация о сертификате» представлена следующая информацию о сертификате:

- Издатель – поле «Issuer» сертификата.
- Владелец – атрибут «CN» из поля «Subject» сертификата.
- SDN владельца – поле «Subject» сертификата.
- Действует с – атрибут «Not Before» из поля «Validity» сертификата.
- Действует по – атрибут «Not After» из поля «Validity» сертификата.
- Алгоритм ключа –атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата.
- Длина ключа – атрибут «Public Key Algorithm» из поля «Subject Public Key Info» сертификата.

В блоке «Состав сертификата» представлена следующая информацию о сертификате:

- Серийный номер – поле «Serial Number» сертификата.
- Открытый ключ – поле «Subject Public Key Info».
- Отпечаток – вычисляемое значение, отсутствует в сертификате.
- Версия – поле «Version» сертификата.
- Параметр открытого ключа – всегда «X509».
- Алгоритм цифровой подписи– поле «Signature Algorithm».
- Основные ограничения – поле «X509v3 Basic Constraints».
- Использование ключа – поле «X509v3 Key Usage» сертификата.
- Доступ к информации о центре сертификации – поле «Authority Information Access».
- Идентификатор ключа центра – поле «X509v3 Authority Key Identifier» сертификата.
- Альтернативное имя субъекта – поле «X509v3 Subject Alternative Name» сертификата.
- Идентификатор ключа субъекта – поле «X509v3 Subject Key Identifier» сертификата.
- Расширенное использование ключа – поле «X509v3 Extended Key Usage» сертификата.

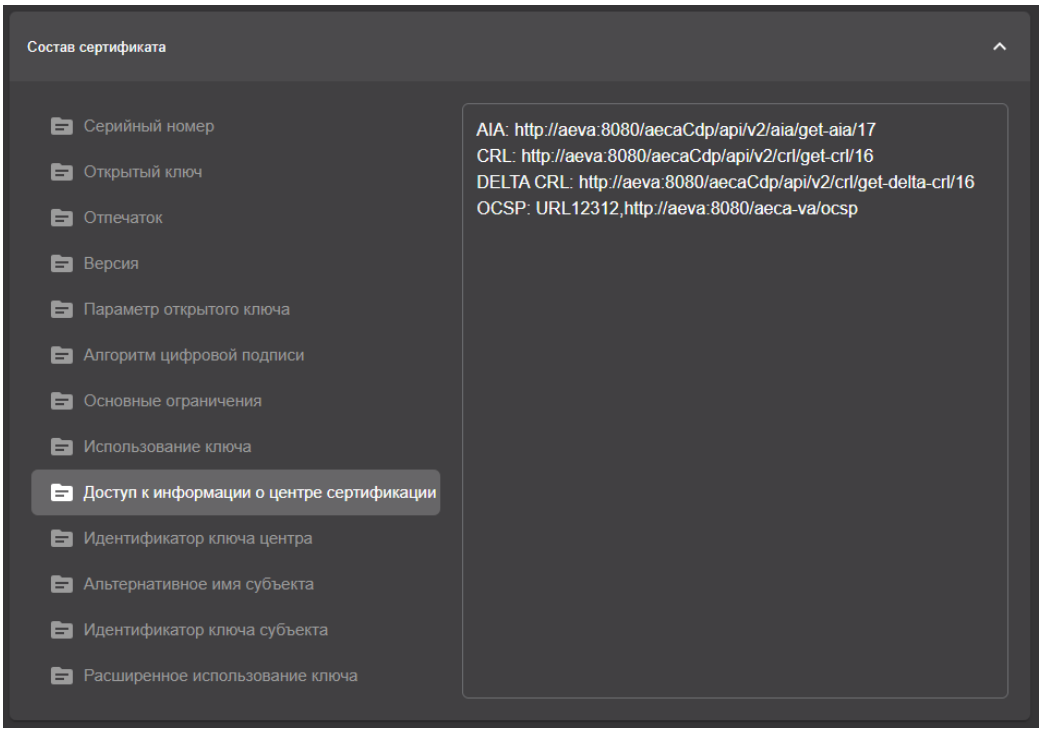


Рисунок 83 – Блок «Состав сертификата»

5.3.4 Создание заявок на выпуск сертификатов

5.3.4.1 Создание заявки на основании запроса PKCS#10

Предварительные условия для создания заявки на основании запроса на выпуск сертификата PKCS#10:

- Файл с запросом на выпуск сертификата PKCS#10 в формате CSR или REQ для получателя сертификата (субъекта РС) должен быть предварительно подготовлен средствами стороннего ПО (например, с помощью приложения Единый клиент JaCarta).
- Файл с запросом на выпуск сертификата PKCS#10 должен быть сформирован с учетом известных данных шаблонов Центра сертификации Aladdin eCA, доступных получателю сертификатов (субъекту РС) на основании назначенных ему уполномоченным пользователем Центра регистрации Aladdin eRA правил выпуска сертификатов (например, для использования шаблона «Domain Controller» для создания заявки на выпуск сертификата в запросе должны быть указаны атрибуты «DNS Name» и «MS GUID»).
- На основании предоставленного при создании заявки файла с запросом ранее в Центре сертификации Aladdin eCA, к которому подключен Центр регистрации Aladdin eRA, не было выпущено сертификатов.

Порядок создания заявки на выпуск сертификата на основании запроса PKCS#10:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<На основании запроса>**.

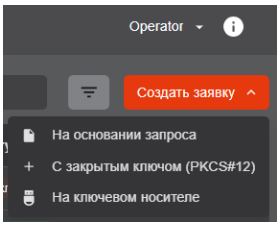


Рисунок 84 – Выбор сценария создания заявки

- В открывшемся окне «Создание заявки» на шаге 1 выберите субъект, для которого выпускается сертификат и нажмите кнопку Продолжить →.
  - в поле поиска введите частичное или полное значение любого атрибута субъекта;
  - поиск субъектов выполняется по атрибутам и является регистронезависимым;
  - в результате будут отображены найденные субъекты с указанием краткой информации:
    - «CN» – значение атрибута «Common Name» субъекта;
    - «ID» – идентификатор субъекта;
    - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
    - «DNS» – значение атрибута «DNS Name» субъекта;
    - пиктограммы наличия подключения субъекта к ресурсной системе .
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;

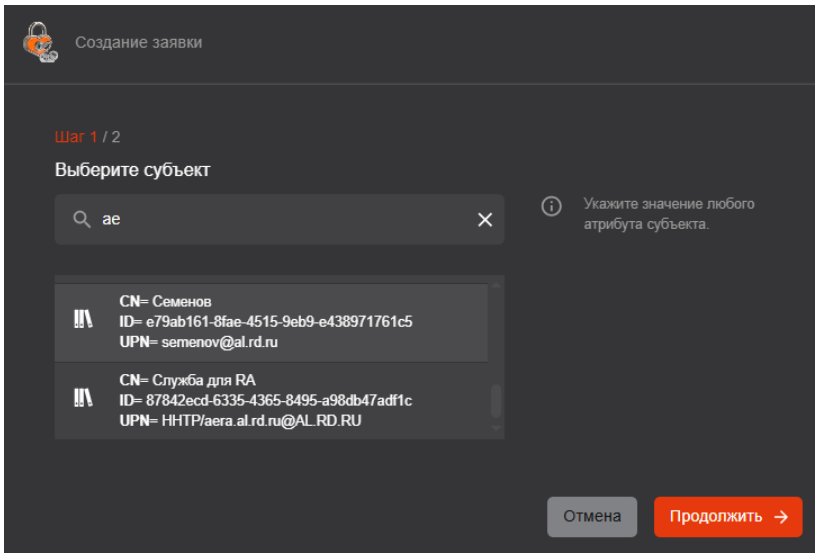


Рисунок 85 – Выбор субъекта для создания заявки на сертификат

- В открывшемся окне «Создание заявки» (см. Рисунок 86):
  - Нажмите кнопку Выбрать файл и укажите путь к файлу с запросом на сертификат.
  - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [1].
  - Нажмите кнопку Создать заявку.

[1] Получателю сертификатов (субъекту РС) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту РС), так и группе безопасности, в которую входит получатель сертификатов (субъект РС). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

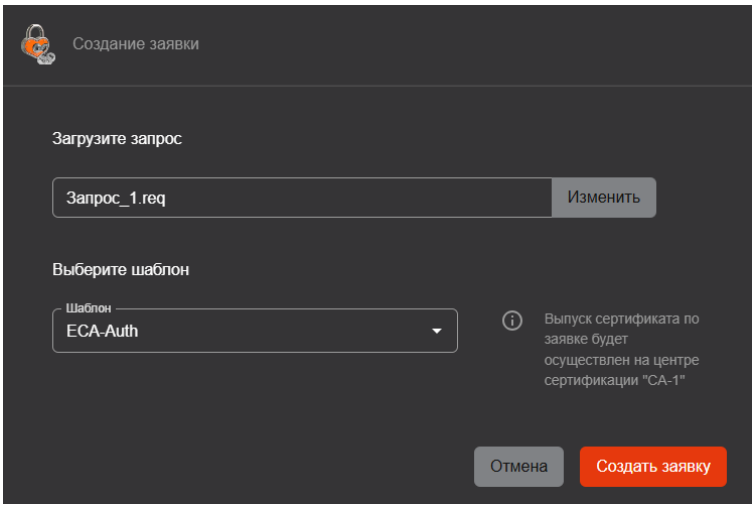


Рисунок 86 – Выбор файла с запросом и шаблона для выпуска сертификата

После заведения заявки файл с запросом на выпуск сертификата PKCS#10 можно выгрузить из Центра регистрации Aladdin eRA. Выгрузка доступна при любом статусе заявки. Выгрузку файла с запросом возможно выполнить как при просмотре списка заявок, так и из карточки заявки:

- Найдите заявку, из которой нужно выгрузить запрос, в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 87).

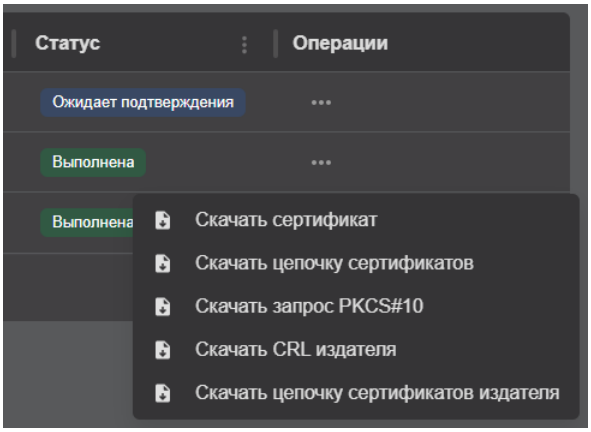


Рисунок 87 – Выгрузка запроса на выпуск сертификата

- Откройте карточку заявки, из которой нужно выгрузить запрос, (см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать запрос PKCS#10>** (см. Рисунок 88).

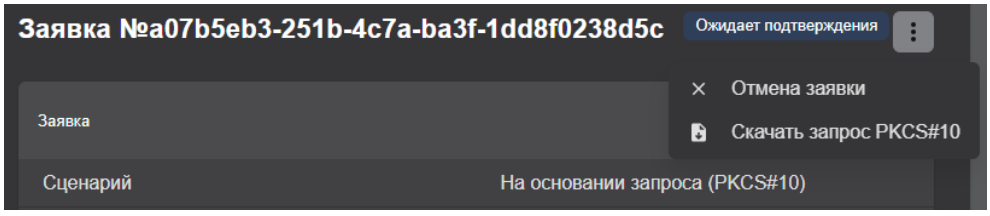


Рисунок 88 – Выгрузка запроса на выпуск сертификата

5.3.4.2 Создание заявки с закрытым ключом PKCS#12

Порядок создания заявки с закрытым ключом PKCS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<С закрытым ключом (PKCS#12)>**.

- В открывшемся окне «Создание заявки» на шаге 1 выберите субъект, для которого выпускается сертификат и нажмите кнопку Продолжить →.
  - в поле поиска введите частичное или полное значение любого атрибута субъекта;
  - поиск субъектов выполняется по атрибутам и является регистронезависимым;
  - в результате будут отображены найденные субъекты с указанием краткой информации:
    - «CN» – значение атрибута «Common Name» субъекта;
    - «ID» – идентификатор субъекта;
    - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
    - «DNS» – значение атрибута «DNS Name» субъекта;
    - пиктограммы наличия подключения субъекта к ресурсной системе .
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;

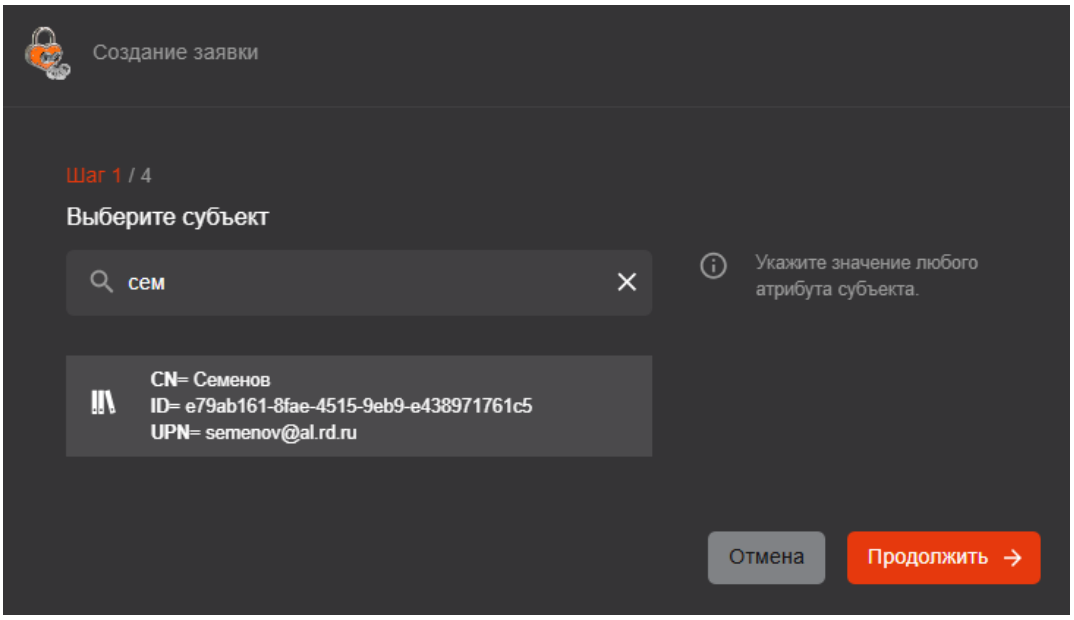


Рисунок 89 – Выбор субъекта для создания заявки на сертификат

- В открывшемся окне «Создание заявки» (шаг 2 сценария) в списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [1], и нажмите кнопку Продолжить →.

[1] Получателю сертификатов (субъекту РС) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту РС), так и группе безопасности, в которую входит получатель сертификатов (субъект РС). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

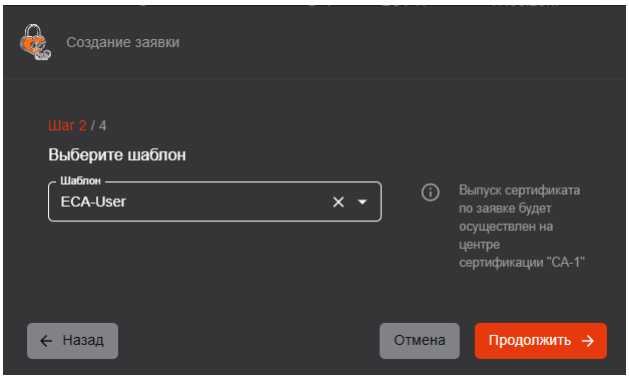


Рисунок 90 – Выбор шаблона для выпуска сертифката

- В открывшемся окне «Создание заявки» (шаг 3 сценария) (см. Рисунок 91) укажите атрибуты получателя сертификатов (субъекта РС):

Значения атрибутов заполняются автоматически в соответствии с данными получателя сертификатов (субъекта РС), полученными из Центра сертификации Aladdin eCA. Выберите в списке атрибута нужное значение или добавьте новый такой же атрибут с другим значением.

– При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений (см. Рисунок 91).

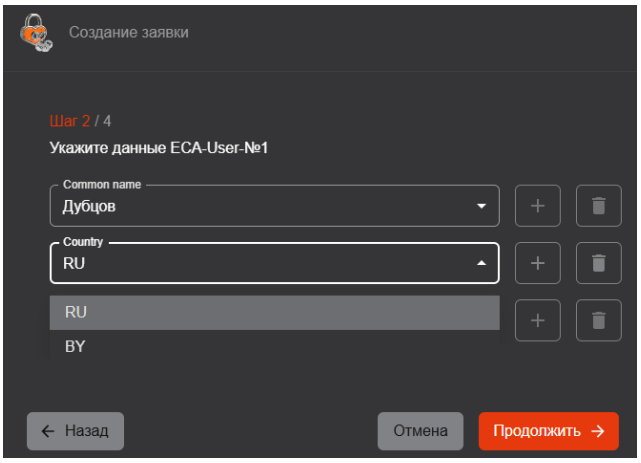


Рисунок 91 – Редактирование атрибутов получателя сертификатов (субъекта РС)

– При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку + и выберите в списках новых атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений) (см. Рисунок 92).

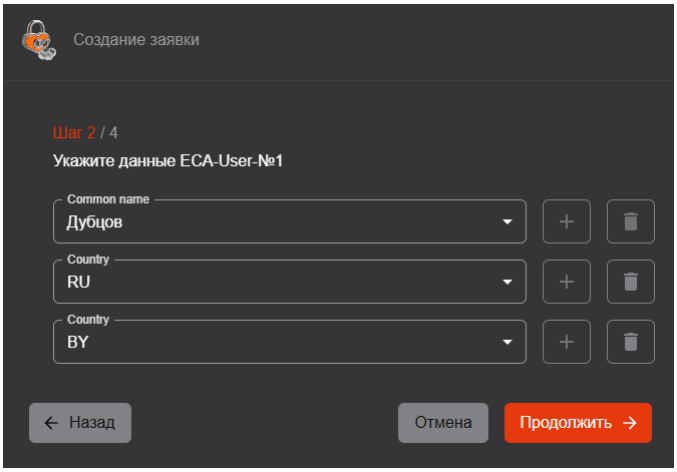


Рисунок 92 – Добавлен новый атрибут

– При необходимости добавленные атрибуты можно удалять. Для этого нажмите рядом со списком атрибута кнопку .

В случае отсутствия у получателя сертификатов (субъекта РС) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 93). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

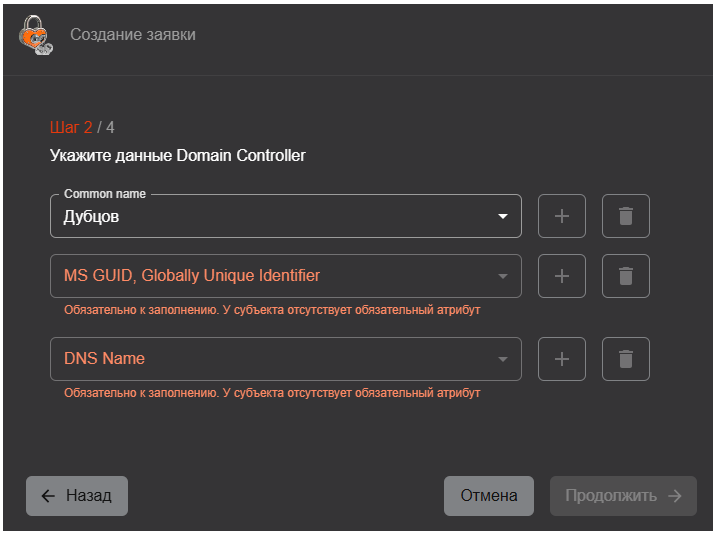


Рисунок 93 – У получателя сертификатов (субъекта РС) отсутствуют обязательные по шаблону атрибуты

Если у получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 94).

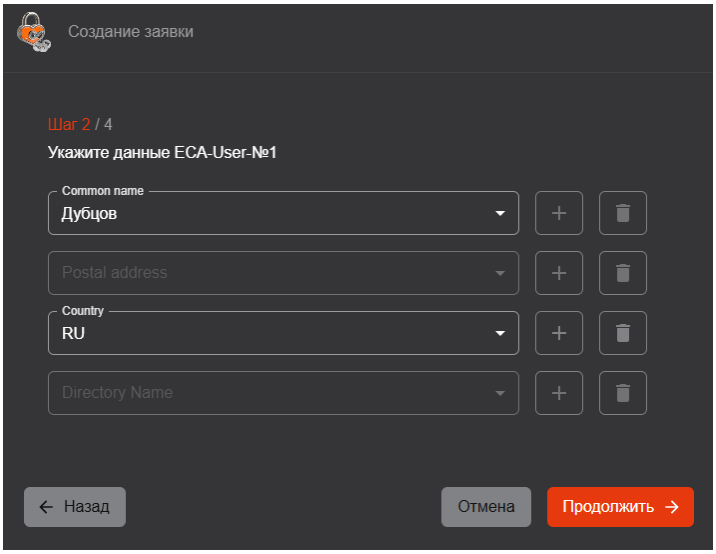


Рисунок 94 – У получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты

– После редактирования атрибутов получателя сертификатов (субъекта РС) нажмите кнопку Продолжить.

- В открывшемся окне «Создание заявки» (шаг 4 сценария) в соответствующих полях задайте и подтвердите пароль для контейнера PKCS#12 и нажмите кнопку Продолжить.

  Пароль должен удовлетворять следующим требованиям:

  – Длина – не менее **8** символов.
  – Пароль должен содержать не менее одного символа из следующих категорий:
    - Строчные буквы английского алфавита от **a** до **z**.
    - Прописные буквы английского алфавита от **A** до **Z**.
    - Десятичные цифры от **0** до **9**.

Для просмотра вводимых символов пароля щелкните в поле значок .

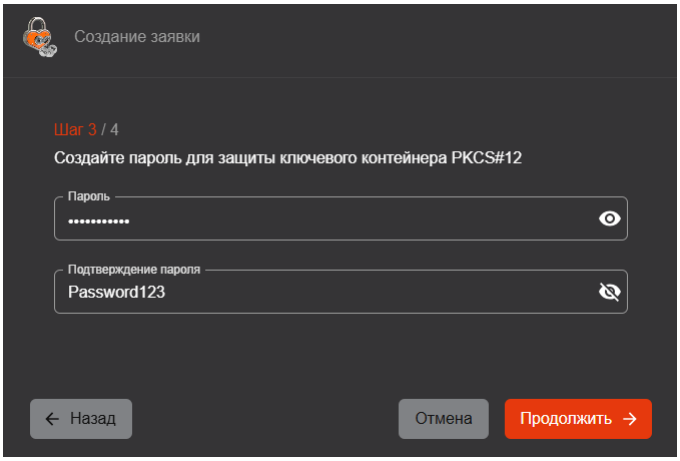


Рисунок 95 – Установка пароля для контейнера PKCS#12

- В открывшемся окне «Создание заявки» (шаг 5 сценария):
  - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
  - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
  - Нажмите кнопку Создать заявку.

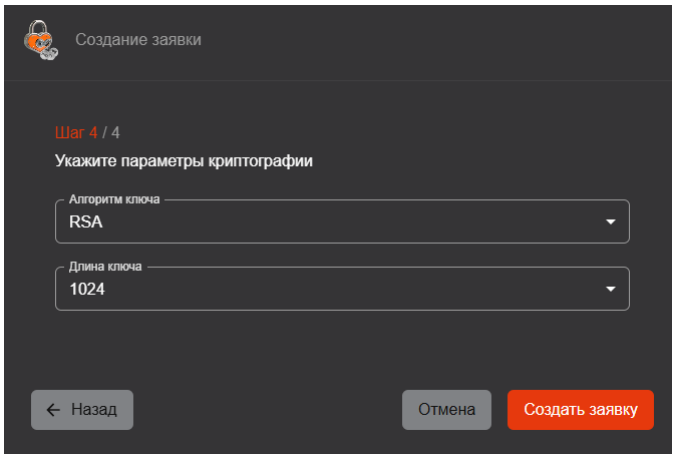


Рисунок 96 – Выбор алгоритма выработки ключевой пары и длины ключа

5.3.4.3 Создание заявки на ключевом носителе

Внимание! Выпуск сертификатов с алгоритмом ключа ГОСТ Р 34.10-2012 и длиной ключа 512 возможен только на ключевых носителях JaCarta-3.

Внимание! Ограничения по возможностям генерации для ключевых носителей Рутокен приведены на официальном сайте производителя.

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должен быть подключен поддерживаемый ключевой носитель (электронный ключ).

Предварительные условия для создания заявки на выпуск сертификата на ключевом носителе:

Порядок создания заявки для импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку Создать заявку и выберите в открывшемся списке сценарий создания заявки **<На ключевом носителе>**.

Если приложение JC-WebClient или ПО «Рутокен Плагин» не установлено или к компьютеру не подключен ключевой носитель, создать заявку на ключевом носителе невозможно.

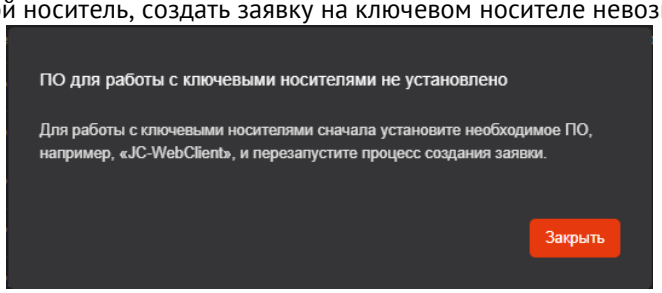


Рисунок 97 – Приложение для работы к ключевыми носителями не установлено

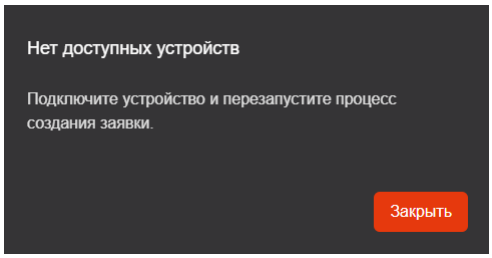


Рисунок 98 – Ключевой носитель не подключен к компьютеру

- В открывшемся окне «Создание заявки» на шаге 1 выберите субъект, для которого выпускается сертификат и нажмите кнопку Продолжить →.
  - в поле поиска введите частичное или полное значение любого атрибута субъекта;
  - поиск субъектов выполняется по атрибутам и является регистронезависимым;
  - в результате будут отображены найденные субъекты с указанием краткой информации:
    - «CN» – значение атрибута «Common Name» субъекта;
    - «ID» – идентификатор субъекта;
    - «UPN» – значение атрибута «MS UPN, User Principal Name» субъекта;
    - «DNS» – значение атрибута «DNS Name» субъекта;
    - пиктограммы наличия подключения субъекта к ресурсной системе .
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;

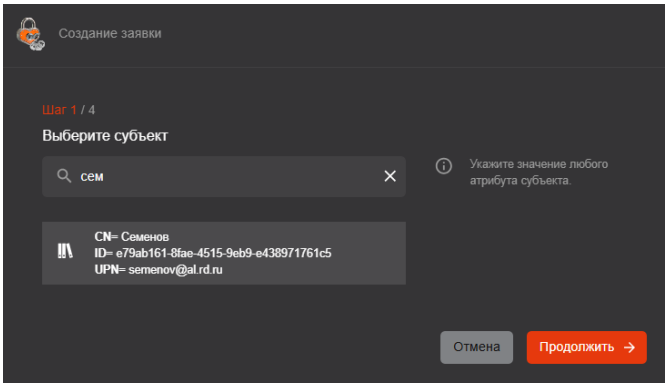


Рисунок 99 – Выбор субъекта для создания заявки на сертификат

- В открывшемся окне «Создание заявки на сертификат» (шаг 2 сценария):

– В списке «Устройство» выберите подключенный ключевой носитель.
– В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
– В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат [1].
– Нажмите кнопку Продолжить →.

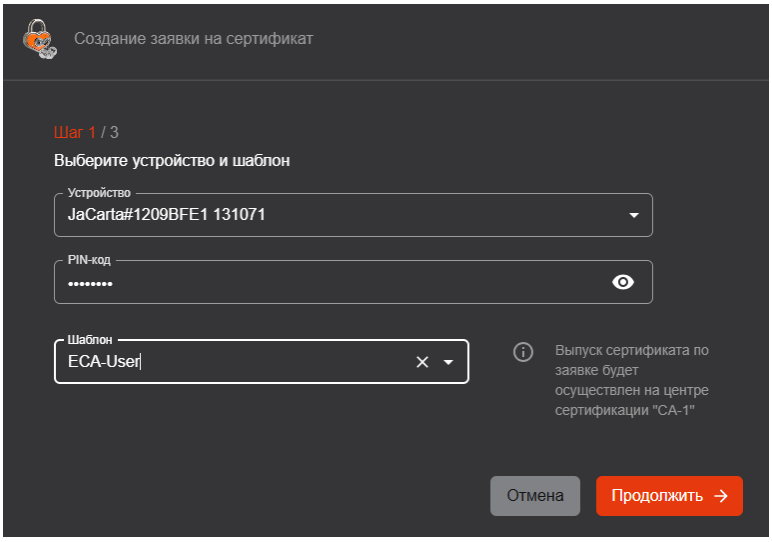


Рисунок 100 – Выбор ключевого носителя и шаблона для выпуска сертификата

- В открывшемся окне «Создание заявки на сертификат» (шаг 3 сценария) укажите атрибуты получателя сертификатов (субъекта РС):

Значения атрибутов заполняются автоматически в соответствии с данными получателя сертификатов (субъекта РС), полученными из Центра сертификации Aladdin eCA. Выберите в списке атрибута нужное значение или добавьте новый такой же атрибут с другим значением.

– При необходимости выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений.

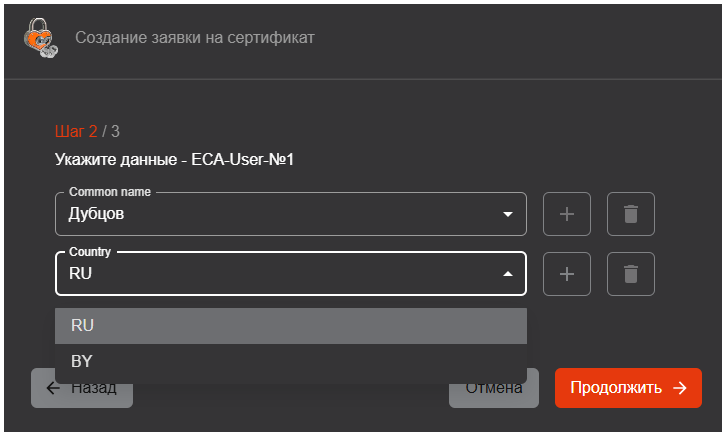


Рисунок 101 – Редактирование атрибутов получателя сертификатов (субъекта РС)

[1] Получателю сертификатов (субъекту РС) доступны шаблоны в соответствии с установленными для него в Центре регистрации Aladdin eRA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту РС), так и группе безопасности, в которую входит получатель сертификатов (субъект РС). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в Центре сертификации Aladdin eCA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

– При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку + и выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах получателя сертификатов (субъекта РС) содержится несколько значений) (см. Рисунок 102).

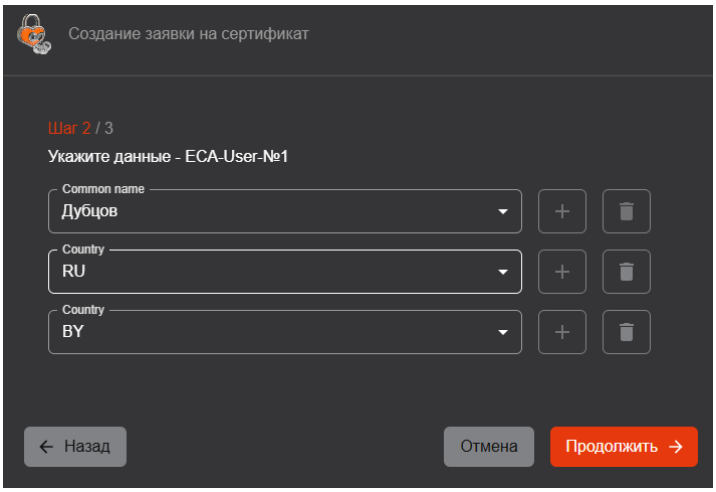


Рисунок 102 – Добавлен новый атрибут

– Добавленные новые атрибуты можно удалять. Для этого нажмите рядом с атрибутом кнопку .

В случае отсутствия у получателя сертификатов (субъекта РС) обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке (см. Рисунок 93). При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

Если у получателя сертификатов (субъекта РС) отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить (см. Рисунок 94).

– После редактирования атрибутов пользователя (субъекта) нажмите кнопку Продолжить →.

- В открывшемся окне «Создание заявки на сертификат» (шаг 4 сценария):
  – В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
  – В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
  – Нажмите кнопку Создать заявку →.

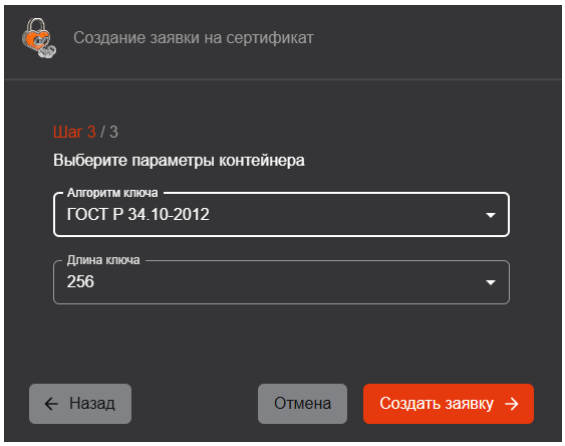


Рисунок 103 – Выбор алгоритма выработки ключевой пары и длины ключа

- В открывшемся окне «Создание заявки на сертификат» (процесс формирования заявки и его результат отображаются процессы:
  – Генерации ключевой пары.

– Генерации запроса.
– Создания заявки.

Успешное завершения каждого процесса помечается значком .

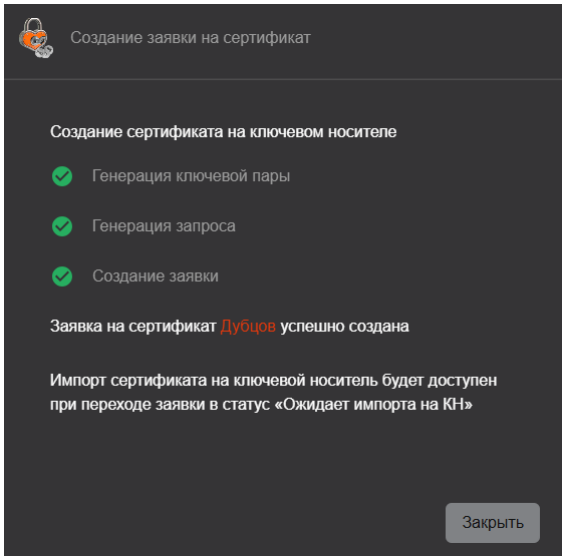


Рисунок 104 – Заявка на выпуск сертификата на ключевом носителе заведена успешно

В случае возникновения ошибок при формировании заявки процесс помечается значком .

Некоторые типы ключевых носителей поддерживают определенный набор алгоритмов выработки ключевых пар (например, в приведенном ниже примере при создании заявки на выпуск сертификата на электронном ключе JaCarta-2 ГОСТ был выбран неподдерживаемый алгоритм RSA) (см. Рисунок 105).

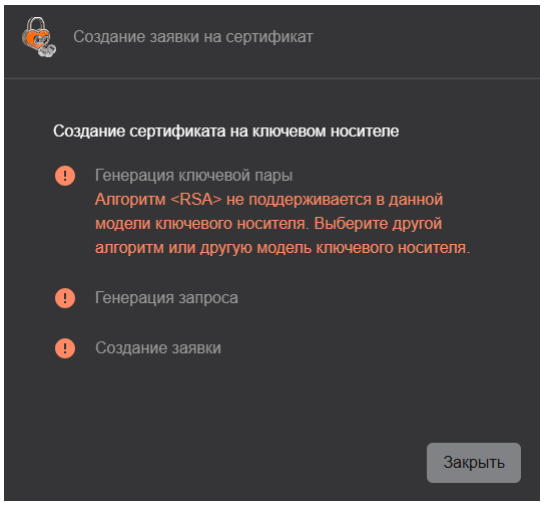


Рисунок 105 – Выбранный алгоритм не поддерживается в используемом ключевом носителе

Для завершения процесса создания заявки в независимости от его результата нажмите кнопку Закрыть.

Импорт сертификата на ключевой носитель (см. раздел 5.3.7.8) будет доступен (статус заявки «Ожидает импорта на КН») после одного из следующих событий:

- Подтверждение заявки уполномоченным пользователем и выпуск сертификата в Центре сертификации Aladdin eCA.
- Автоматическое подтверждение заявки и выпуск сертификата в Центре сертификации Aladdin eCA.

5.3.5 Отмена заявки

Оператор может отменить только созданные им заявки (например, по причине указания в заявке некорректных данных). Отменить заявку возможно, если ее статус «Ожидает подтверждения» или «Ошибка выпуска».

Выполнить отмену заявки возможно как при просмотре списка заявок, так и из карточки заявки.

Порядок отмены заявки, созданной получателем сертификатов (субъектом РС), способом №1:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Инициируйте процесс отмены заявки одним из следующих способов:
  - Найдите заявку, которую необходимо отменить, в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Отмена заявки>** (см. Рисунок 106).

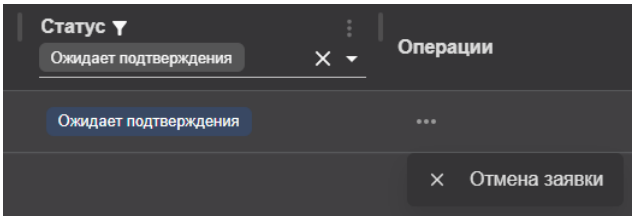


Рисунок 106 – Инициализация процесса отмены заявки на выпуск сертификата в спсике

  - Откройте карточку заявки, которую необходимо отменить (см. раздел 5.3.3), на панели инструментов карточки заявки щелкните значок и выберите в открывшемся списке **<Отмена заявки>** (см. Рисунок 107).

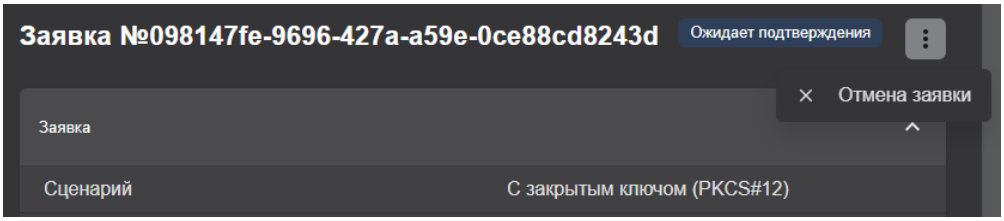


Рисунок 107 – Инициализация процесса отмены заявки на выпуск сертифката из ее карточки

- В открывшемся окне в поле «Комментарий» укажите причину отмены заявки и нажмите кнопку Отменить.

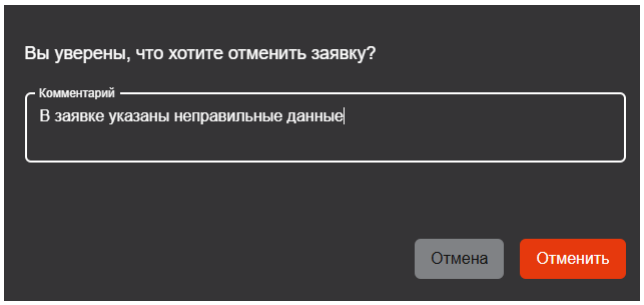


Рисунок 108 – Указание причинs перед отменой заявки на выпуск сертификата

После отмены заявки указанный комментарий будет доступен для просмотра в карточке заявки (см. раздел 5.3.3) в атрибуте «Комментарий» блока «Заявка» (см. Рисунок 109).

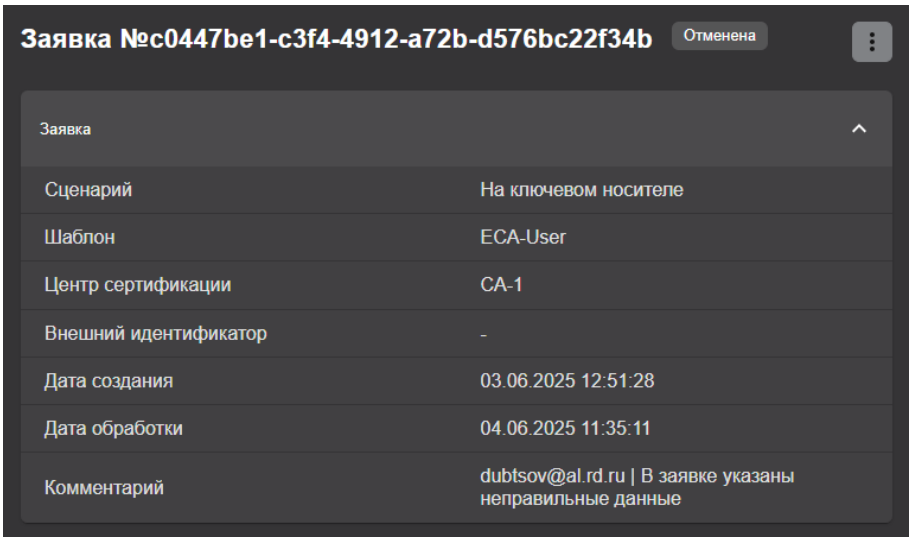


Рисунок 109 – Комментарий занесен в карточку отменной заявки

5.3.6 Обработка заявки

Статус заявки, участвующей в сценарии, должен быть «Ожидает подтверждения».

Для обработки заявки выполните следующие шаги:

Обработать заявку возможно как при просмотре списка заявок, так и из карточки заявки.
Порядок обработки заявки способом №1:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Найдите заявку, которую необходимо обработать, в списке (см. раздел 5.3.2),
- Инициируйте процесс отмены заявки одним из следующих способов - щелкните в колонке **[Операции]** значок **<Операции строки>** или откройте карточку заявки и щелкните значок на панели инструментов.
- Выберите в открывшемся списке необходимый вариант обработки заявки:
  - Отклонить выпуск;
  - Выпустить сертификат.

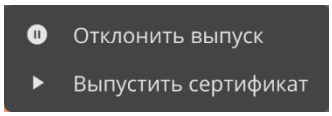


Рисунок 110 – Обработка заявки

- В появившемся окне введите комментарий к действию и нажмите на соответствующую кнопку **<Выпустить>** или **<Отклонить>**.

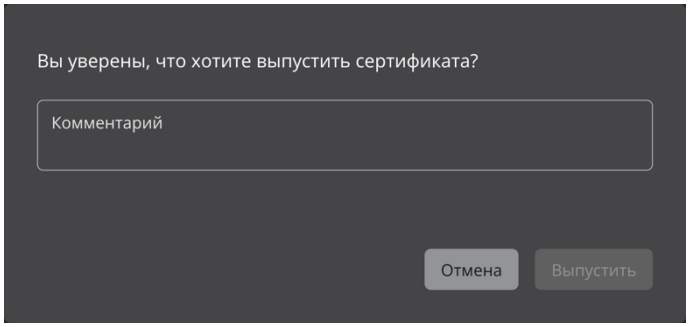


Рисунок 111 – Окно комментария к подтверждению выпуска сертификата

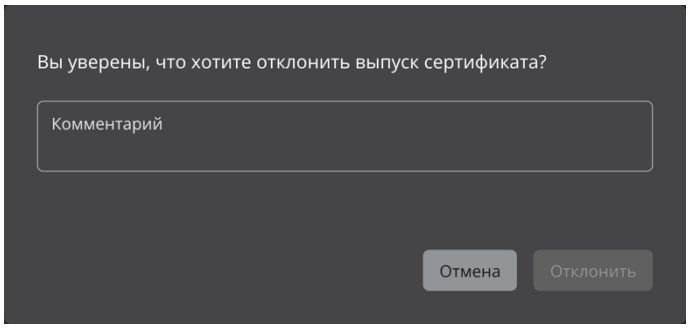


Рисунок 112 – Окно комментария к отклонению выпуска сертификата

5.3.7 Управление выпущенными по заявкам сертификатами

5.3.7.1 Общие сведения о работе с сертификатами

Инициализация процесса выпуска сертификата в Центре сертификации Aladdin eCA выполняется:

- После подтверждения заявки уполномоченными пользователями Цента регистрации Aladdin eRA с ролями «Администратор» или «Оператор» в ручном режиме (режим определяется правилами выпуска, установленными для получателя сертификатов (субъекта РС)).
- В автоматическом режиме (режим определяется правилами выпуска, установленными для получателя сертификатов (субъекта РС)).

После успешного выпуска сертификата заявке, по которой он был выпущен, назначается статус «Выполнена».

Заявкам, заведенным по сценарию на ключевом носителе, после успешного выпуска сертификатов назначается статус «Ожидает импорта на КН». Статус «Выполнен» назначается таким заявками после импорта сертификата на ключевой носитель (см. раздел 5.3.7.8).

После выпуска сертификата Оператору доступны следующие операции:

- Выгрузка файла с сертификатом в формате PEM (см. раздел 5.3.7.2).
- Выгрузка файла цепочки сертификатов в формате PEM (см. раздел 5.3.7.3).
- Выгрузка файла со списком отозванных сертификатов (CRL) в формате CRL (см. раздел 5.3.7.5).
- Выгрузка файла с цепочкой сертификатов издателя в формате PEM (см. раздел 5.3.7.6).
- Выгрузка файла с контейнером закрытого ключа PKCS#12 в формате P12 (см. раздел 5.3.7.4).

Выгрузка доступна только для заявок, заведенных по сценарию с закрытым ключом PKCS#12 (см. раздел 5.3.4.2).

- Отзыв сертификатов, выпущенных по заявкам (см. раздел 5.3.7.7).

Оператору доступен отзыв сертификатов, выпущенных по заявкам, у которых получателями сертификатов является субъект, доступный данному Оператору в соответствии с правилами доступа.

- Импорт сертификата на ключевой носитель (см. раздел 5.3.7.8).

Импорт доступен только для заявок, заведенных по сценарию на ключевом носителе (см. раздел 5.3.4.3).

Если по подтвержденной заявке или обрабатываемой в автоматическом режиме сертификат не выпущен по какой-ли причине, такой заявке назначается статус «Ошибка выпуска».

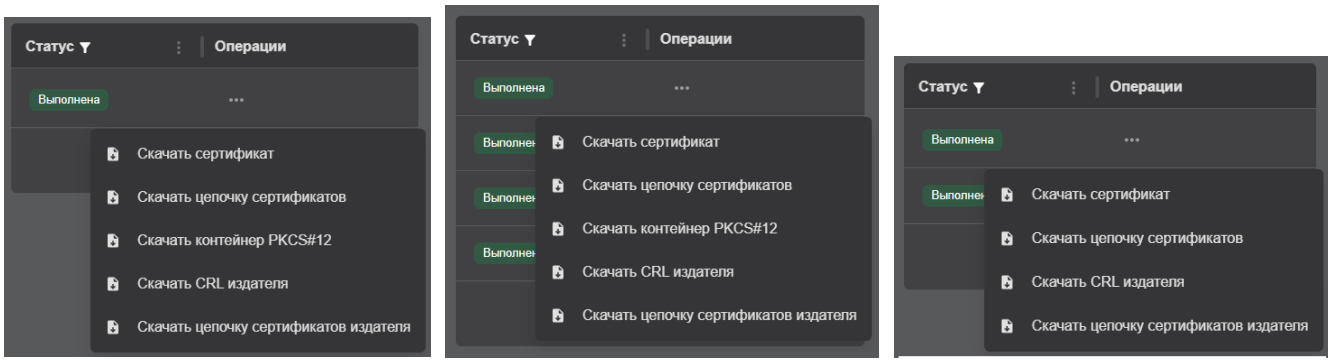
5.3.7.2 Выгрузка сертификата

Выгрузку файла с сертификатом возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки сертификата получателя сертификатов (субъекта РС):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.

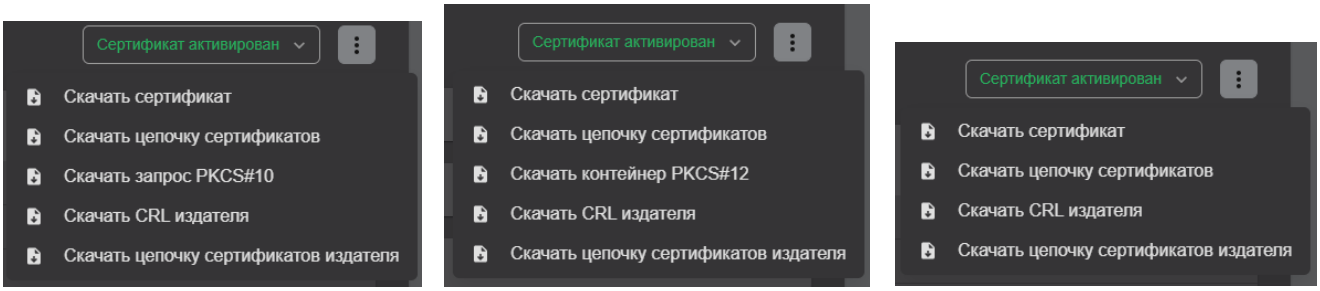
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать сертификат>** (см. Рисунок 113).



а) Заявка на основании запроса PKCS#10 **б) Заявка с закрытым ключом PRCS#12** **в) Заявка на ключевом носителе[1]**

Рисунок 113 – Выгрузка сертификата, выпущенного по заявкам с разными сценариями создания

  - Откройте карточку заявки (см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать сертификат>** (см. Рисунок 114).



а) Заявка на основании запроса PKCS#10 **б) Заявка с закрытым ключом PRCS#12** **в) Заявка на ключевом носителе[2]**

Рисунок 114 – Выгрузка сертификата, выпущенного по заявкам с разными сценариями создания

5.3.7.3 Выгрузка цепочки сертификатов

Выгрузку файла с цепочкой сертификатов возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки цепочки сертификата получателя сертификатов (субъекта РС):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать цепочку сертификатов>** (см. Рисунок 113).
  - Откройте карточку заявки (см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать цепочку сертификатов>** (см. Рисунок 114).

[1] Заявка на ключевом носителе после импорта сертификата на ключевой носитель.

[2] Заявка на ключевом носителе после импорта сертификата на ключевой носитель.

5.3.7.4 Выгрузка контейнера PCKS#12

Выгрузку файла с контейнером PCKS#12 возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки контейнера PCKS#12:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать контейнер PCKS#12>** (см. Рисунок 113).
  - Откройте карточку заявки (см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать контейнер PCKS#12>** (см. Рисунок 114).

5.3.7.5 Выгрузка списка отозванных сертификатов (CRL)

Выгрузку файла со списком отозванных сертификатов (CRL) возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки списка отозванных сертификатов (CRL):

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать CRL издателя>** (см. Рисунок 113).
  - Откройте карточку заявки (см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **<Скачать CRL издателя>** (см. Рисунок 114).

5.3.7.6 Выгрузка цепочки сертификатов издателя

Выгрузку файла с цепочкой сертификатов издателя возможно выполнить как при просмотре списка заявок, так и из карточки заявки.

Порядок выгрузки цепочки сертификатов издателя:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Выгрузите файл одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Скачать цепочку сертификатов издателя>** (см. Рисунок 113).
  - Откройте карточку заявки см. раздел 5.3.3), на панели инструментов щелкните значок и выберите в открывшемся списке **< Скачать цепочку сертификатов издателя>** (см. Рисунок 114).

5.3.7.7 Отзыв сертификата

Чтобы отозвать сертификат, заявка по которой он был выпущен должна быть в статусе «Выполнена», а статус сертификата «Активирован».

Отзыв сертификата является необратимой операцией, которая может повлиять на работу получателя сертификатов (субъекта РС).

Порядок отзыва сертификата:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.

- Откройте карточку заявки, по которой был выпущен сертификат, требующий отзыва (см. раздел 5.3.3).
- На панели инструментов карточки заявки нажмите кнопку Сертификат активирован и выберите в открывшемся списке **<Сертификат отозван>**.

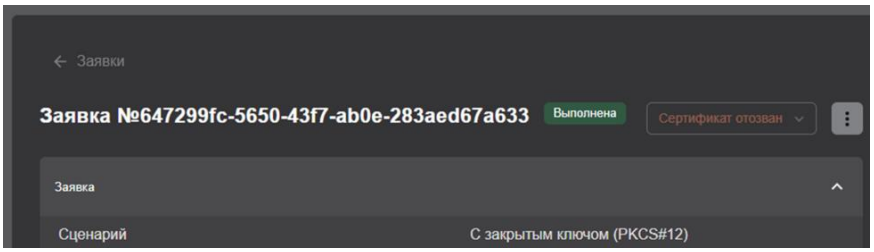


Рисунок 115 – Отзыв сертификата

- В открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в поле «Комментарий» и нажмите кнопку Отозвать.

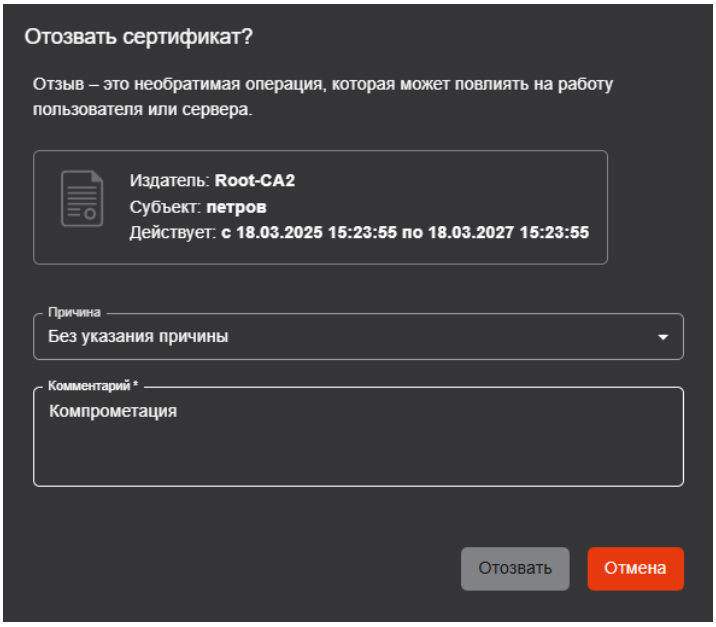


Рисунок 116 – Указание причины отзыва сертификата

В результате сертификат будет отозван (см. Рисунок 117).

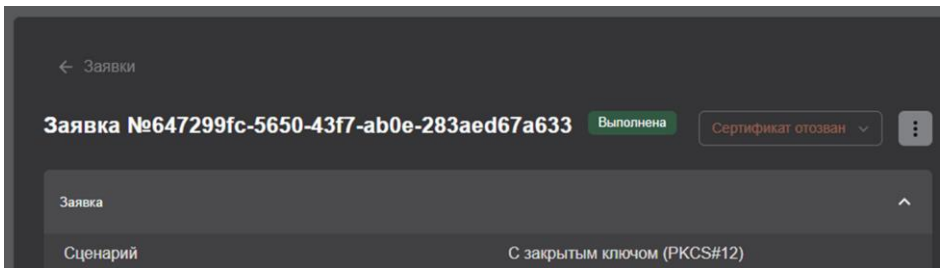


Рисунок 117 –Сертификат отозван

5.3.7.8 Импорт сертификата на ключевой носитель

Предварительные условия для импорта сертификата на ключевой носитель:

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должен быть подключен поддерживаемый ключевой носитель (электронный ключ).

- Заявка, по которой был выпущен сертификат для последующего импорта на ключевой носитель, должна иметь статус «Ожидает импорта на КН».

Порядок импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Заявки**.
- Инициируйте процесс отмены заявки одним из следующих способов:
  - Найдите заявку в списке (см. раздел 5.3.2), щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Импортировать на КН>** (см. Рисунок 118).

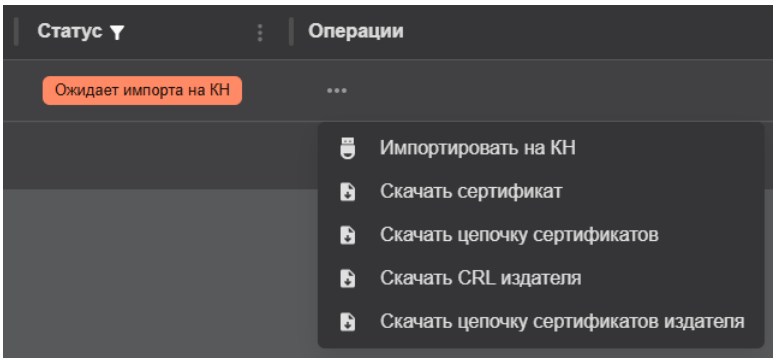


Рисунок 118 – Инициализация процесса импорта сертификата на ключевой носитель из списка

Если приложение JC-WebClient или ПО «Рутокен Плагин» не установлено или к компьютеру не подключен ключевой носитель, создать заявку на ключевом носителе невозможно.

  - Откройте карточку заявки, на панели инструментов карточки заявки щелкните значок и выберите в открывшемся списке **< Импортировать на КН >** (см. Рисунок 119).

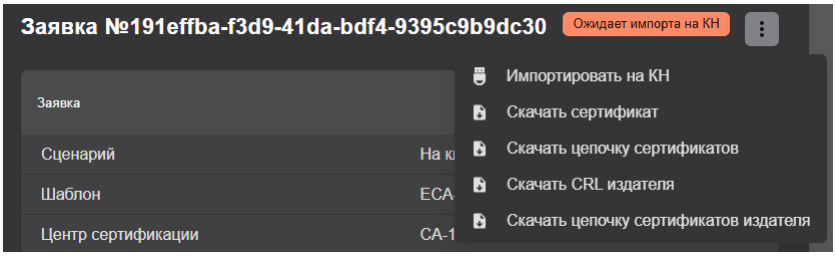


Рисунок 119 – Инициализация процесса импорта сертификата на ключевой носитель из карточки заявки

- В открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 120):
  - В списке «Устройство» выберите подключенный ключевой носитель.
  - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
  - Нажмите кнопку Импортировать.

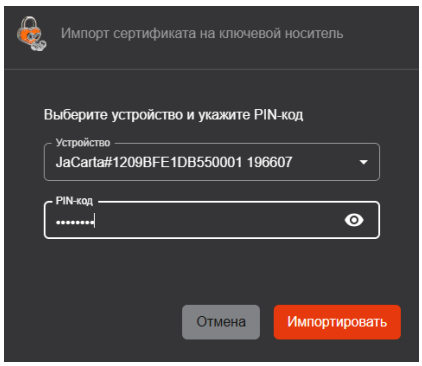


Рисунок 120 – Импорт сертификата на ключевой носитель

При импорте сертификата, открытый ключ которого не соответствует закрытому ключу на ключевом носителе возникает ошибка «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата».

Центр регистрации Aladdin eRA последовательно проходит по списку ключевых пар на выбранном при импорте ключевом носителе. Все неуспешные попытки создания контейнера завершаются ошибкой, возвращаемой приложением JC-WebClient или ПО «Рутокен Плагин». При этом Центр регистрации Aladdin eRA не отображает ошибку для каждой ключевой пары, генерируемую приложением JC-WebClient или ПО «Рутокен Плагин», а выводит общую ошибку «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата».

- В случае успешного импорта сертификата на ключевой носитель в открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 121) проверьте данные сертификата и нажмите кнопку Закрыть.

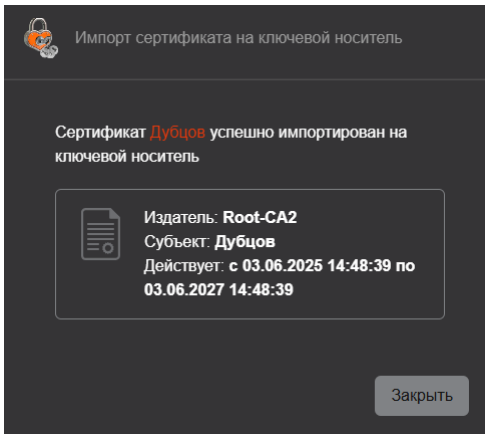


Рисунок 121 – Импорт сертификата на ключевой носитель успешно выполнен

5.4 Раздел «Журнал событий»

5.4.1 О журнале событий

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

Каждая запись в журнале событий содержит следующую информацию:

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

События, доступные Оператору, приведены в таблице ниже.

Таблица 10 – События, доступные Оператору

Причина, вызвавшая запись в журнал	**Код события**	**Категория события**	**Описание в журнале**
Аутентификация пользователя	RAENV0100	INFO	Краткое описание: Аутентификация пользователя Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя – Аутентификатор – Тип аутентификации – IP адрес
Ошибка аутентификации	RAENV0101	ERROR	Краткое описание: Ошибка аутентификации пользователя Атрибуты: – Id пользователя (может отсутствовать) – Отображаемое имя пользователя (может отсутствовать) – Роль пользователя (может отсутствовать) – Аутентификатор (может отсутствовать) – Тип аутентификации – IP адрес – Причина ошибки
Выход пользователя	RAENV0102	INFO	Краткое описание: Выход пользователя Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя – Аутентификатор – Тип аутентификации – IP адрес
Создание заявки	RAENV0300	INFO	Краткое описание: Создание заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать)
Ошибка создания заявки	RAENV0301	ERROR	Краткое описание: Ошибка создания заявки Атрибуты: – Сценарий (может отсутствовать) – CN в заявке (может отсутствовать) – Id шаблона (может отсутствовать) – Имя шаблона (может отсутствовать) – Id получателя сертификата (может отсутствовать) – Имя получателя сертификата (может отсутствовать) – Внешний ключ (может отсутствовать) – Причина ошибки
Обработка заявки	RAENV0302	INFO	Краткое описание: Обработка заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			– Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Режим обработки – Id правил
Выпуск сертификата по заявке	RAENV0303	INFO	Краткое описание: Выпуск сертификата по заявке Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата
Ошибка выпуска сертификата по заявке	RAENV0304	ERROR	Краткое описание: Ошибка выпуска сертификата по заявке Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Причина ошибки
Отмена заявки	RAENV0305	INFO	Краткое описание: Отмена заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать)
Ошибка отмены заявки	RAENV0306	ERROR	Краткое описание: Ошибка отмены заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Причина ошибки
Отклонение заявки	RAENV0307	INFO	Краткое описание: Отклонение заявки Атрибуты: – Id заявки – Сценарий – CN в заявке

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			– Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать)
Ошибка отклонения заявки	RAENV0308	ERROR	Краткое описание: Ошибка отклонения заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Причина ошибки
Импорт сертификата на носитель	RAENV0309	INFO	Краткое описание: Импорт сертификата на носитель Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата
Ошибка импорта сертификата на носитель	RAENV0310	ERROR	Краткое описание: Ошибка импорта сертификата на носитель Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата (может отсутствовать)
Отзыв сертификата	RAENV0311	INFO	Краткое описание: Отзыв сертификата Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата – Причина отзыва – Комментарий к отзыву

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка отзыва заявки	RAENV0312	ERROR	Краткое описание: Ошибка отзыва сертификата Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата (может отсутствовать) – Причина ошибки
Подключение ключевого носителя	RAENV0400	INFO	Краткое описание: Подключение ключевого носителя Атрибуты: – Свойства носителя
Ошибка подключения ключевого носителя	RAENV0401	ERROR	Краткое описание: Ошибка подключения ключевого носителя Атрибуты: – Свойства носителя – Причина ошибки
Экспорт файла	RAENV0500	INFO	Краткое описание: Экспорт файла Атрибуты: – ID заявки – Тип файла (возможные значения: «PKCS#10», «Сертификат», «Цепочка сертификатов», «PKCS#12», «Сертификат издателя», «Цепочка сертификатов издателя», «CRL издателя»)
Ошибка экспорта файла	RAENV0501	ERROR	Краткое описание: Ошибка экспорта файла Атрибуты: – ID заявки – Тип файла (возможные значения: «PKCS#10», «Сертификат», «Цепочка сертификатов», «PKCS#12», «Сертификат издателя», «Цепочка сертификатов издателя», «CRL издателя») Причина ошибки
Экспорт журнала событий	RAENV0502	INFO	Краткое описание: Экспорт журнала событий Атрибуты: – Параметры фильтрации
Ошибка экспорта журнала событий	RAENV0503	ERROR	Краткое описание: Ошибка экспорта журнала событий Атрибуты: – Параметры фильтрации – Причина ошибки

5.4.2 Просмотр журнала событий

Оператору доступен просмотр только следующих событий журнала:

- события, для которых он является инициатором;
- события по заявкам, которые были созданы данным пользователем;
- события по заявкам, у которых получателем сертификата является субъект, доступный данному пользователю в соответствии с правилами доступа Центра сертификации, к которому подключён Центр регистрации Aladdin eRA.

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

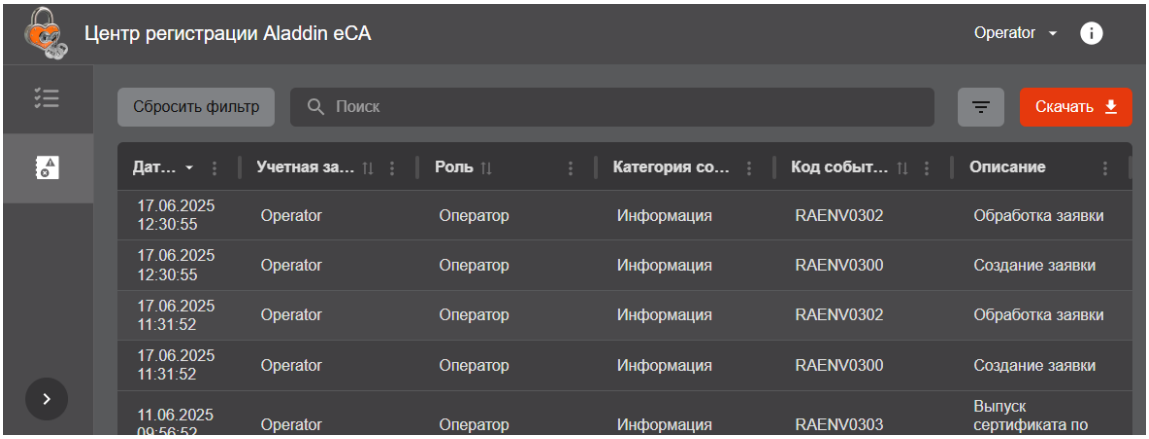


Рисунок 122 – Просмотр записей журнала событий

Записи о событиях отображаются списком в табличном виде. По умолчанию в колонках таблицы отображаются следующие атрибуты событий:

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

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

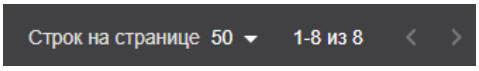


Рисунок 123 – Инструменты навигации

Описание инструментов навигации:

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

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

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

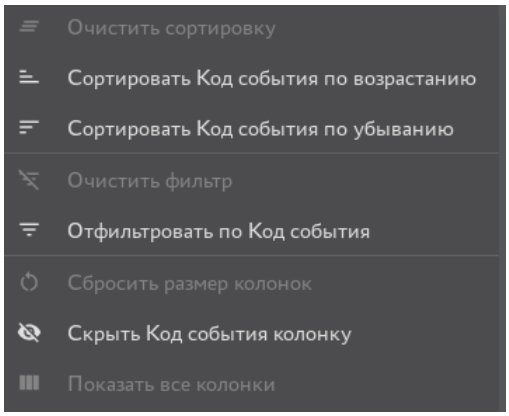


Рисунок 124 – Список действий с колонкой **[Код события]**

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

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

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

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

Чтобы выполнить сортировку записей о событиях по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [1] выберите:

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

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками [2]:

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

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

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

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

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

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

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

- По коду события.

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

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

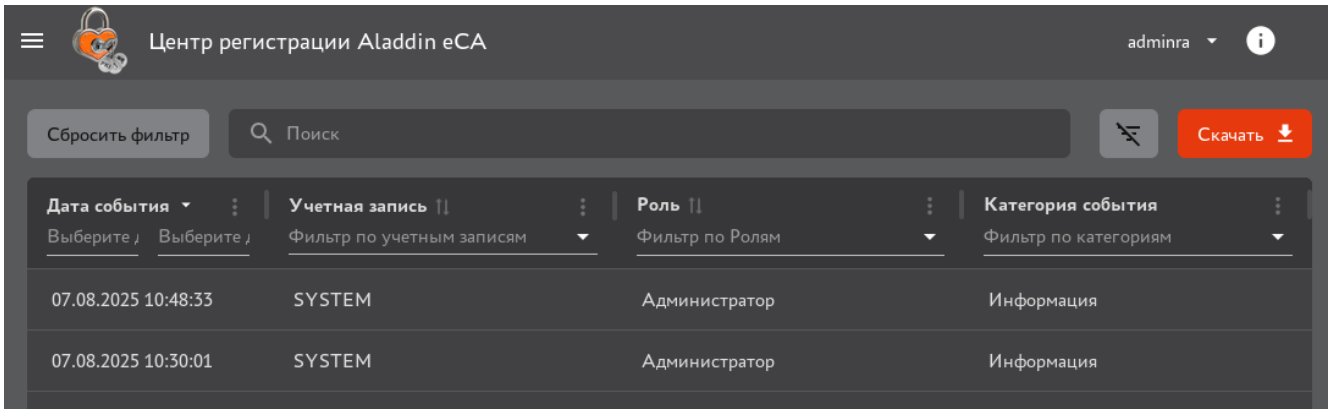


Рисунок 125 – Отображение фильтров в заголовках колонок включено

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

Фильтры по атрибутам событий, представленный в колонках **[Учетная запись]** (см. Рисунок 126а), **[Роль]** (см. Рисунок 126б), **[Категория события]** (см. Рисунок 126в) и **[Код события]** (см. Рисунок 126г) обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов. Фильтр по атрибуту события, представленном в колонке **[Дата события]** (см. Рисунок 126д), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок. Признаком применения фильтра является значок в заголовке соответствующей колонки (см. Рисунок 126д).

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

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

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

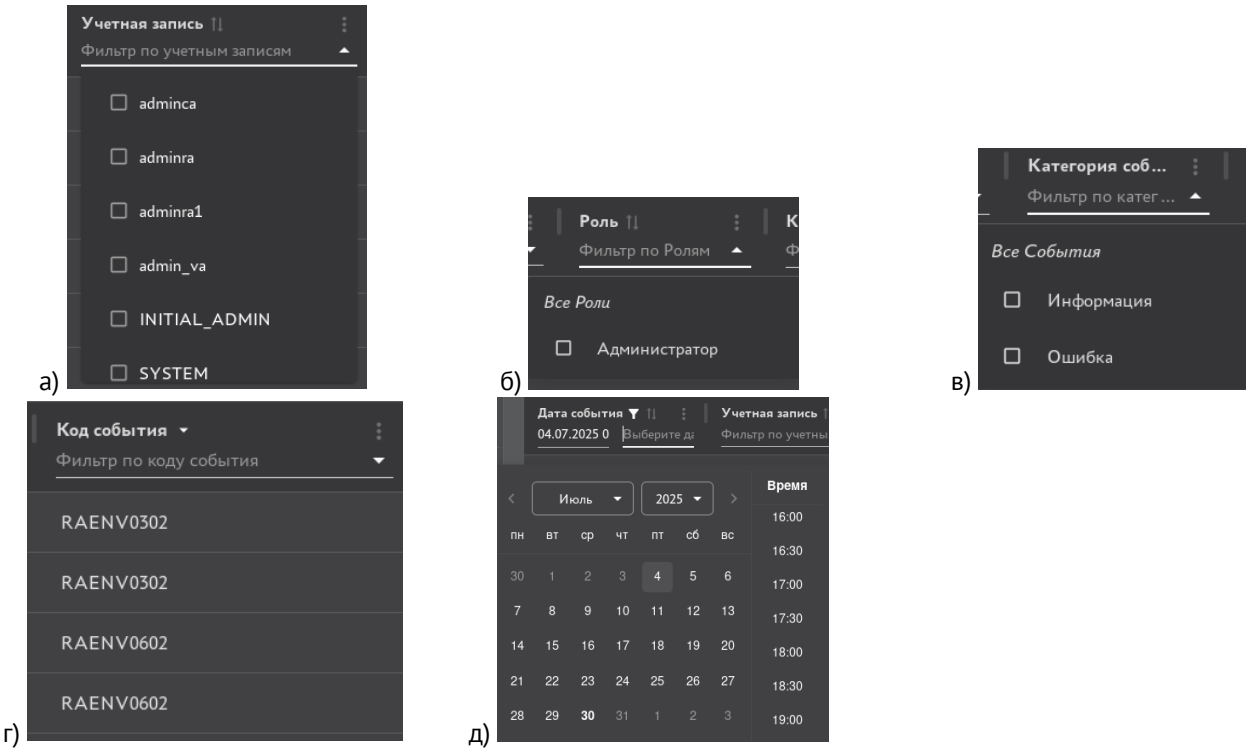


Рисунок 126 – Указание критериев выборки в фильтрах

5.4.3 Просмотр карточки события

Карточка события содержит представленную в удобном для анализа виде подробную информацию о событии.

Чтобы открыть карточку события:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел **Журнал событий.**
- Найдите нужное событие и щелкните запись о нем в списке (см. Рисунок 127).

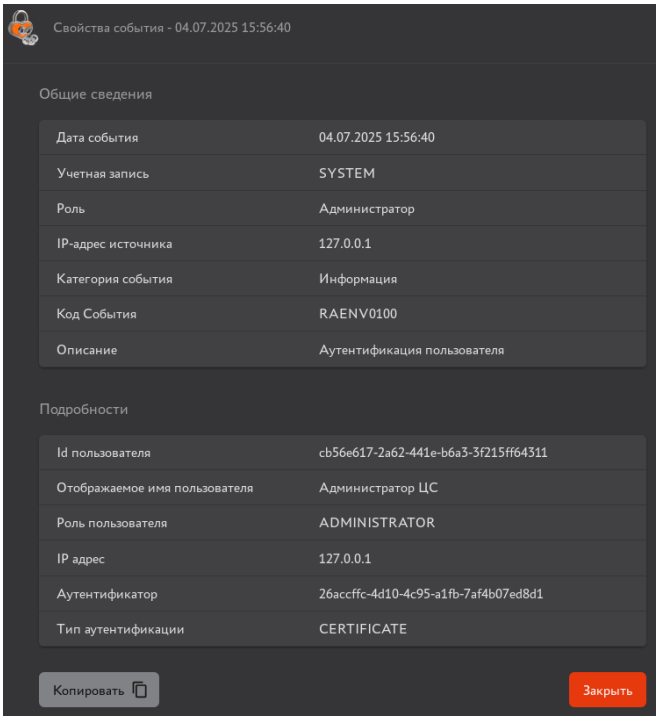
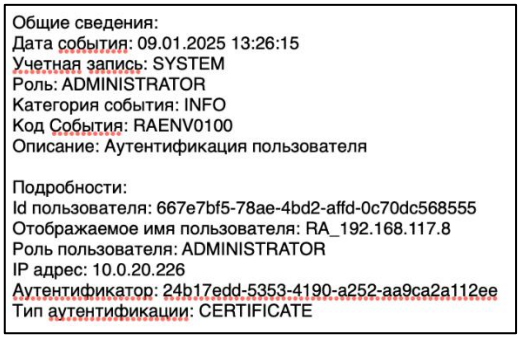


Рисунок 127 – Окно «Свойства события» (карточка события)

Для копирования информации о событии в буфер обмена нажмите кнопку Копировать. Содержимое события из буфера обмена можно вставить, например, в текстовый файл (см. Рисунок 128).


Общие сведения:
Дата события: 09.01.2025 13:26:15
Учетная запись: SYSTEM
Роль: ADMINISTRATOR
Категория события: INFO
Код События: RAENV0100
Описание: Аутентификация пользователя

Подробности:
Id пользователя: 667e7bf5-78ae-4bd2-affd-0c70dc568555
Отображаемое имя пользователя: RA_192.168.117.8
Роль пользователя: ADMINISTRATOR
IP адрес: 10.0.20.226
Аутентификатор: 24b17edd-5353-4190-a252-aa9ca2a112ee
Тип аутентификации: CERTIFICATE

Рисунок 128 – Пример копирования события в текстовый файл

5.4.4 Экспорт записей журнала событий

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

Порядок экспорта журнала событий:

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

6 СООБЩЕНИЯ ОПЕРАТОРУ

Сообщения оператору представляют собой текст сообщения в модальном окне под полем ввода пароля или пин-кода, которое появляется по центру текущего окна входа в систему и сообщает об ошибке или обязательном действии, которое не выполнено. Список всех возможных сообщения для оператора приведён в таблице ниже (Таблица 11).

Таблица 11 – Оповещения программы

№ п/п	Сообщение об ошибке/ уведомление	Описание	Действие оператора
1	Не задано обязательное поле	Сообщение об ошибке при выпуске сертификата по запросу. В загружаемом запросе отсутствует поле, которое является обязательным в выбранном шаблоне	Вернуться на предыдущий шаг и сменить шаблон на подходящий или пересоздать файл-запрос с учетом выявленных при сверке ошибок и перезагрузить файл-запрос, вернувшись на предыдущие шаги по нажатию кнопки <Назад>
2	Поле не соответствует формату, указанному в шаблоне	Сообщение об ошибке при выпуске сертификата по запросу. Загружаемый запрос содержит поле, которое отсутствует в выбранном шаблоне	
3	Для работы с ключевым носителем сначала установите необходимое ПО. Например, «JC-WebClient», и перезапустите процесс создания заявки.	Сообщение об ошибке при выпуске сертификата на ключевом носителе ПО JC-WebClient или «Рутокен Плагин» предварительно не установлено	Для выпуска сертификата на электронном ключе установить ПО JC-WebClient или «Рутокен Плагин»
4	Нет доступных устройств. Подключите устройство и перезапустите мастер создания сертификата	Сообщение об ошибке при выпуске сертификата на ключевом носителе Электронный носитель не подключен	Для выпуска сертификата на электронном ключе подсоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
5	Алгоритм не поддерживается выбранной моделью ключевого носителя	Сообщение об ошибке при выпуске сертификата на ключевом носителе Выбранный для выпуска сертификата алгоритм не поддерживается выбранной моделью ключевого носителя	Для выпуска сертификата на электронном ключе выберите поддерживаемый ключевой носитель, присоедините ключевой носитель к USB-порту и запустите мастер создания сертификатов
6	Синхронизация запущена	Уведомление о успешном запуске обновления ресурсной системы	—
7	Ресурс с указанным идентификатором не найден	Ошибка при запуске обновления ресурсной системы	Выбрать актуальную ресурсную систему
8	Не удалось найти объект сущности по идентификатору: ${id}	Сообщение об ошибке при выпуске сертификата	Выбрать актуальный и активный субъект
9	Не должны присутствовать одновременно параметры SubjectId и UserId.	Сообщение об ошибке при выпуске сертификата. Ошибка присутствия одновременно параметров субъекта и юзера	Выбрать только одни параметры
10	Ошибка получения шаблона	Сообщение об ошибке при выпуске сертификата. Ошибка при выборе шаблона	Выбрать актуальный и активный шаблон
11	Время действия активной лицензии истекло	Сообщение об ошибке при приостановке, отзыве и активации сертификата.	Использовать актуальную лицензию

ПРИЛОЖЕНИЕ 1. ОПИСАНИЕ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Примечание - Для всех предустановленных шаблонов контроль соответствия значений отличительного и альтернативного имен значениям аналогичных атрибутов у субъекта при выпуске сертификата включен.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ECA–Auth	8ecba810–7f48–4c4e–b803–99a97146e2ba	2y	–	–	RSA ECDSA ГОСТ Р34.10–2012	1024 256 Выключен	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name	+	+	–		
[Deprecated] ECA–User	2d58b30c-3965-4555-9af4-fec4552af21e	2y	–	–	RSA ECDSA ГОСТ Р 34.10–2012	1024 256 256	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиент – Защита электронной почты	–	Common name	+	+	–		
[Deprecated] ECA–WEB–Server	25bbd733-4d8c-43ce-ba5a-e9826eb7b16c	2y	–	–	RSA ECDSA ГОСТ Р 34.10–2012	1024 256 256	– Цифровая подпись – Шифрование ключей	+	– Аутентификация сервера	–	Common name	+	+	DNS name	+	+
[Deprecated] Domain Controller	bf2dac0a–f05f–49dd–95b4–e50691489b6a	2y	–	–	RSA ECDSA ГОСТ Р 34.10–2012	1024 256 Выключен	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Центр распространения ключей Kerberos – SSH сервер	–	Common name[44]	+	+	DNS name[45] MS GUID[46]	+ +	+ +

[44] Имя контроллера домена.

[45] FQDN –полное доменное имя вашего сервера.

[46] Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Smartcard Logon	aa03e458-50cd-46b8-82cd-d5612ed3b647	2y	–	–	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name[47]	+	+	MS UPN[48]	+	+
					ECDSA	256								RFC 822 Name[49]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Client	059a38f5-f345-4275-b79f-e7e6cc3cbb68	2y	–	–	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name[50]	+	+	MS UPN[51]	+	+
					ECDSA	256								RFC 822 Name[52]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] WEB-Server	08c66f99-218a-46ef-bdee-6a2b3b26a4f1	2y	–	–	RSA	1024	– Цифровая подпись – Шифрование ключей	+	Аутентификация сервера	–	Common name[53]	+	+	DNS name[54]	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] S/MIME	0c234243-18cf-4c05-b699-537731b2436f	2y	–	–	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт-картой	–	Common name[55]	+	+	RFC 822 Name[56]	+	+
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										

[47] Имя пользователя.

[48] Имя входа пользователя в формате e-mail адреса.

[49] Почтовый адрес пользователя, может совпадать с MS UPN.

[50] Имя веб-клиента.

[51] Имя входа пользователя в формате e-mail адреса.

[52] Почтовый адрес пользователя, может совпадать с MS UPN.

[53] Имя веб-сервера.

[54] FQDN – полное доменное имя вашего сервера.

[55] Имя пользователя.

[56] почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] ALD PRO Domain Controller	11ec34a4-d03e-4059-92f0-9c09b08bffea	2y	–	–	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name[57]	+	+	MS UPN[58]	+	+
					ECDSA	256					Organization[59]	–	+	Kerberos KPN[60]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] ALD PRO Smartcard Logon	18d9bd4e-6f15-423f-8137-ac8416ad6874	2y	–	–	RSA	1024	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name[61]	+	+	MS UPN[62]	+	+
					ECDSA	256					Organization[63]	–	+	RFC 822 Name[64]	+	+
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] OCSP Signer	aac2e49b-9c8e-4869-80c1-eef526ba75ab	2y	–	–	RSA	1024	Цифровая подпись	+	OCSP подписант	–	Common name	+	+	–		
					ECDSA	256										
					ГОСТ Р 34.10-2012	Выключен										
[Deprecated] Root CA	9129245a-eaad-4ebc-a2a4-8845ac0336fb	7d24y	–	–	RSA	1024	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
					ECDSA	256					Unique Identifier (UID)	–	+	DNS name	–	+
					ГОСТ Р 34.10-2012	256					Given name	–	+	MS UPN	–	+
											Initials	–	+	MS GUID	–	+

[57] Имя контроллера домена ALD PRO.

[58] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[59] Организация.

[60] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[61] Имя пользователя ALD PRO.

[62] Имя входа пользователя в формате e-mail адреса.

[63] Организация.

[64] Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Surname	–	+	IP address	–	+
											Organizational unit	–	+	Directory Name	–	+
											Locality	–	+	Uniform resource identifier	–	+
											State or province	–	+	Registered Identifier (OID)	–	+
											Domain component	–	+	Permanent identifier	–	+
											Country	–	+	Xmpp address	–	+
											Postal code	–	+	Service Name	–	+
											Business category	–	+	Subject Identification Method	–	+
											Telephone number	–	+	Kerberos KPN	–	+
											Pseudonym	–	+			
											Postal address	–	+			
											Street	–	+			
											Name	–	+			
											Title	–	+			
											Domain qualifier	–	+			
											Description	–	+			
											Unstructured address	–	+			
											Unstructured name	–	+			
											Email Address (E)	–	+			
											Serial number	–	+			
											Organization	–	+			
											ИНН	–	+			
											ОГРН	–	+			
											ОГРНИП	–	+			
											СНИЛС	–	+			
											ИНН ЮЛ	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
[Deprecated] Sub CA	af3b0355–1798–4c64–98f7–a9c70407db1c	7d24y	–	–	RSA	1024	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
											Unique Identifier (UID)	–	+	DNS name	–	+
					ECDSA	256					Given name	–	+	MS UPN	–	+
					ГОСТ Р 34.10–2012	256					Initials	–	+	MS GUID	–	+
											Surname	–	+	IP address	–	+
											Organizational unit	–	+	Directory Name	–	+
											Locality	–	+	Uniform resource identifier	–	+
											State or province	–	+	Registered Identifier (OID)	–	+
											Domain component	–	+	Permanent identifier	–	+
											Country	–	+	Xmpp address	–	+
											Postal code	–	+	Service Name	–	+
											Business category	–	+	Subject Identification Method	–	+
											Telephone number	–	+	Kerberos KPN	–	+
											Pseudonym	–	+			
											Postal address	–	+			
											Street	–	+			
											Name	–	+			
											Title	–	+			
											Domain qualifier	–	+			
											Description	–	+			
											Unstructured address	–	+			
											Unstructured name	–	+			
											Email Address (E)	–	+			
											Serial number	–	+			
											Organization	–	+			
											ИНН	–	+			
											ОГРН	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											ОГРНИП	–	+			
											СНИЛС	–	+			
											ИНН ЮЛ	–	+			
[Deprecated] SCEP Management	3e5df3d4–683c–4252–b862–467589c2225b	25y	–	–	RSA	1024	– Цифровая подпись – Шифрование ключей – Шифрование данных	+	–	–	Common name	+	–	–		
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										
User	f215f72f-9a9a-45c8-83e8-25879d52dcf6	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиент – Защита электронной почты	–	Common name	+	+	–		
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										
Domain Controller	eca2ad3d-944e-48ce-ba7b-114f16ad8fd4	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Центр распространения ключей Kerberos – SSH сервер	–	Common name[65]	+	+	DNS name[66]	+	+
					ECDSA	256								MS GUID[67]	+	+
					ГОСТ Р 34.10–2012	256										

[65] Имя контроллера домена.

[66] FQDN –полное доменное имя вашего сервера.

[67] Глобальный уникальный идентификатор контроллера домена, данные должны быть получены из контроллера домена. Для получения значения идентификатора в среде РЕД ОС и SberLinux OS Server выполните команду: `samba-tool computer show <hostname> | grep objectGUID`. Для получения значения идентификатора в среде Astra Linux Special Edition выполните команду: `ipa host-show <hostname> --all | grep ipauniqueid`, где `hostname` – короткое имя контроллера домена.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
Smartcard Logon	682225f6-f189-412f-a456-c480d42efaa8	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт–картой	–	Common name[68]	+	+	MS UPN[69]	+	+
					ECDSA	256								RFC 822 Name[70]	+	+
					ГОСТ Р 34.10–2012	256										
WEB–Client	18ecaacc-43d6-4aaa-afcc-1bc8e547e6f5	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей	+	– Аутентификация клиента – Защита электронной почты	–	Common name[71]	+	+	MS UPN[72]	+	+
					ECDSA	256								RFC 822 Name[73]	+	+
					ГОСТ Р 34.10–2012	256										
WEB–Server	61c901fa-c823-4899-87a0-df4035291fa0	1y	–	–	RSA	2048	– Цифровая подпись – Шифрование ключей	+	Аутентификация сервера	–	Common name[74]	+	+	DNS name[75]	+	+
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										

[68] Имя пользователя.

[69] Имя входа пользователя в формате e-mail адреса.

[70] Почтовый адрес пользователя, может совпадать с MS UPN.

[71] Имя веб-клиента.

[72] Имя входа пользователя в формате e-mail адреса.

[73] Почтовый адрес пользователя, может совпадать с MS UPN.

[74] Имя веб-сервера.

[75] FQDN – полное доменное имя вашего сервера.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат		Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
S/MIME	0a7c4a9f-b260-46c5-94c5-58de5e977678	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Защита электронной почты – Вход с MS смарт–картой	–	Common name[76]	+	+	RFC 822 Name[77]	+	+
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										
ALD PRO Domain Controller	83afddde-5729-4562-a7ed-260f1c0f73d7	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name[78]	+	+	MS UPN[79]	+	+
					ECDSA	256					Organization[80]	–	+	Kerberos KPN[81]	+	+
					ГОСТ Р 34.10–2012	256										
ALD PRO Smartcard Logon	85e99e47-479f-407e-98f8-ad13d51435a7	1y	–	–	RSA	2048	– Цифровая подпись – Подтверждение подлинности – Шифрование ключей – Шифрование данных	+	– Аутентификация клиента – Центр распространения ключей Kerberos – Аутентификация сервера	–	Common name[82]	+	+	MS UPN[83]	+	+
					ECDSA	256					Organization[84]	–	+	RFC 822 Name[85]	+	+
					ГОСТ Р 34.10–2012	256										
OCSP Signer	eeb625cb-861e-458c-94ae-79b2e05090e5	1y	–	–	RSA	2048	Цифровая подпись	+	OCSP подписант	–	Common name	+	+	–		
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										

[76] Имя пользователя.

[77] почтовый адрес пользователя, может совпадать с MS UPN.

[78] Имя контроллера домена ALD PRO.

[79] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[80] Организация.

[81] Данные в формате «krbtgt/полное имя домена@полное имя домена».

[82] Имя пользователя ALD PRO.

[83] Имя входа пользователя в формате e-mail адреса.

[84] Организация.

[85] Почтовый адрес пользователя, может совпадать с MS UPN.

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
Root CA	a1eb9d3a-b9b5-4e6d-8f2d-587ca9cc6554	15y	–	–	RSA	4096	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
					ECDSA	384					Unique Identifier (UID)	–	+	DNS name	–	+
					ГОСТ Р 34.10–2012	512					Given name	–	+	MS UPN	–	+
											Initials	–	+	MS GUID	–	+
											Surname	–	+	IP address	–	+
											Organizational unit	–	+	Directory Name	–	+
											Locality	–	+	Uniform resource identifier	–	+
											State or province	–	+	Registered Identifier (OID)	–	+
											Domain component	–	+	Permanent identifier	–	+
											Country	–	+	Xmpp address	–	+
											Postal code	–	+	Service Name	–	+
											Business category	–	+	Subject Identification Method	–	+
											Telephone number	–	+	Kerberos KPN	–	+
											Pseudonym	–	+			
											Postal address	–	+			
											Street	–	+			
											Name	–	+			
											Title	–	+			
											Domain qualifier	–	+			
											Description	–	+			
											Unstructured address	–	+			
											Unstructured name	–	+			
											Email Address (E)	–	+			
											Serial number	–	+			
											Organization	–	+			
											Дата рождения	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Место рождения	–	+			
											ИНН	–	+			
											ОГРН	–	+			
											ОГРНИП	–	+			
											СНИЛС	–	+			
											ИНН ЮЛ	–	+			
Sub CA	4f56589e-7e80-4fbe-b49f-662c9ba9a335	7y	–	–	RSA	3072	– Цифровая подпись – Подпись сертификата – Подпись списка отзыва	+	– Любое расширенное использование ключа – Аутентификация клиента – Аутентификация сервера	–	Common name	+	+	RFC 822 Name	–	+
											Unique Identifier (UID)	–	+	DNS name	–	+
					ECDSA	256					Given name	–	+	MS UPN	–	+
					ГОСТ Р 34.10–2012	256					Initials	–	+	MS GUID	–	+
											Surname	–	+	IP address	–	+
											Organizational unit	–	+	Directory Name	–	+
											Locality	–	+	Uniform resource identifier	–	+
											State or province	–	+	Registered Identifier (OID)	–	+
											Domain component	–	+	Permanent identifier	–	+
											Country	–	+	Xmpp address	–	+
											Postal code	–	+	Service Name	–	+
											Business category	–	+	Subject Identification Method	–	+
											Telephone number	–	+	Kerberos KPN	–	+
											Pseudonym	–	+			
											Postal address	–	+			
											Street	–	+			
											Name	–	+			
											Title	–	+			
											Domain qualifier	–	+			
											Description	–	+			

Имя шаблона	Идентификатор	Период действия сертификата	Включать SID в сертификат	Публиковать сертификат в ресурсную систему	Шифрование		Использование ключа		Расширенное использование ключа		Компоненты имени сертификата					
											Отличительное имя субъекта			Альтернативное имя субъекта		
					Алгоритм	Минимальная длина ключа	Значения	Крит.	Значения	Крит.	Поле	Обязат.	Валидац.	Поле	Обязат.	Валидац.
											Unstructured address	–	+			
											Unstructured name	–	+			
											Email Address (E)	–	+			
											Serial number	–	+			
											Organization	–	+			
											Дата рождения	–	+			
											Место рождения	–	+			
											ИНН	–	+			
											ОГРН	–	+			
											ОГРНИП	–	+			
											СНИЛС	–	+			
											ИНН ЮЛ	–	+			
SCEP Management	77004b9d-e195-40a3-aee0-dca5ad403f49	25y	–	–	RSA	2048	– Цифровая подпись – Шифрование ключей – Шифрование данных	+	–	–	Common name	+	–	–		
					ECDSA	256										
					ГОСТ Р 34.10–2012	256										

ПРИЛОЖЕНИЕ 2. ПРАВИЛА ВАЛИДАЦИИ ЗНАЧЕНИЙ ПОЛЕЙ ПО УМОЛЧАНИЮ ПРЕДУСТАНОВЛЕННЫХ ШАБЛОНОВ СЕРТИФИКАТОВ

Поле	Правило валидации
Поля SDN	
Country	Допустимые символы: "A"-"Z", "a"-"z". Длина значения должна составлять 2 символа.
Domain qualifier	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
Email Address (E)	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text".
Serial number	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "'", "(", ")", "+", ",", "-", ".", "/", ":", "=", "?", пробел.
ИНН	Допустимые символы: "0"-"9". Длина значения должна составлять 12 или 14 символов.
ОГРН	Допустимые символы: "0"-"9". Длина значения должна составлять 13 символов.
ОГРНИП	Допустимые символы: "0"-"9". Длина значения должна составлять 15 символов.
СНИЛС	Допустимые символы: "0"-"9". Длина значения должна составлять 11 символов.
ИНН ЮЛ	Допустимые символы: "0"-"9". Длина значения должна составлять 10 или 14 символов.
Postal code	Допускается любая последовательность символов, в которой отсутствуют непарные двойные кавычки (").
Дата рождения	Формат значения: дата в формате «DD.MM.YYYY».
Поля SAN	
RFC 822 Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", ".", "@", "_", "-". Формат значения: "text@text". Пример заполнения: “ivanova@example.com”.
DNS Name	Допустимые символы: "A"-"Z", "a"-"z", "0"-"9", "-", ".", "*".

Поле	Правило валидации
	Пример значения: “dc1.presale.aeca”.
IP address	Допустимые символы: "A"-"F", "a"-"f", "0"-"9", ".", ":". Формат значения: IPv4-адрес или IPv6-адрес.
Directory Name	Формат значения: последовательность идентификаторов относительных отличительных имен (RDN) и их значений, отделенных запятой или запятой с пробелом (например, O=organization, OU=Department, L=City, DC=Component, C=RU...). Допускается использование следующих идентификаторов RDN: EMAILADDRESS, CN, UID, SERIALNUMBER, OU, O, L, ST, C, T, SURNAME, STREET, INITIALS, GIVENNAME, DC, UNSTRUCTUREDADDRESS, UNSTRUCTUREDNAME, POSTALCODE, BUSINESSCATEGORY, TELEPHONENUMBER, PSEUDONYM, POSTALADDRESS, NAME, DN, DESCRIPTION. В качестве идентификатора RDN допускается указание OID (формат OID должен соответствовать рекомендации ITU X.660).
Registered Identifier (OID)	Допустимые символы: "0"-"9", ".". Формат значения: OID в соответствии с рекомендацией ITU X.660.
MS UPN, User Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".Пример заполнения: “krbtgt/ald.pro@ald.pro”.
MS GUID, Globally Unique Identifier	Допустимые символы: "A"-"F", "a"-"f", "0"-"9". Длина значения должна составлять 32 символа. Пример значения: “92625ee510e248479554779d1f43f751”.
Kerberos KPN, Kerberos 5 Principal Name	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text". Пример заполнения: “krbtgt/ald.pro@ald.pro”.
Permanent Identifier	Формат значения: "value/OID", где "value" – любая последовательность символов, а "OID" – OID в соответствии с рекомендацией ITU X.660. Допускается отсутствие значения "text", например, "/1.2.2.3.4.5".
Xmpp address	Допустимые символы: "A"-"Z", "a"-"z", "А"-"Я", "а"-"я", "ё", "Ё", "0"-"9", ".", "@", "_", "-", "/". Формат значения: "text@text".
Subject Identification Method	Формат значения: "OID::text::text", где "OID" – OID в соответствии с рекомендацией ITU X.660, а "text" – любая последовательность символов.

ПРИЛОЖЕНИЕ 3. УСТАНОВКА ПО ДЛЯ РАБОТЫ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

6.1 3.1 Установка JC-WebClient

JC-WebClient обеспечивает выпуск сертификатов на электронных ключевых носителях JaCarta. JC-WebClient необходимо установить на компьютер, с которого будет выполняется подключение к Клиентской части Центра регистрации Aladdin eRA.

> **Внимание! При установке и использовании JC-WebClient сертифицированная среда функционирования не обеспечивается.**

Скачайте дистрибутив JC-WebClient с веб-сайта производителя и установите зависимости.

Установите JC-WebClient, выполнив следующую команду с правами суперпользователя:

РЕД ОС	`sudo dnf install JC-WebClient-x64-x.x.x.xxxx.rpm`
Astra Linux SE	`sudo apt install -f JC-WebClient-x64-x.x.x.xxxx.deb`
Альт Сервер	`sudo apt-get install JC-WebClient-x64-x.x.x.xxxx.rpm`

Перейдите в каталог `/etc/rc.d/init.d/`, выполнив команду:

```
cd /etc/rc.d/init.d/
```

Выполните запуск JC-WebClient, выполнив следующую команду с правами суперпользователя:

```
sudo sh jcmon start
```

6.2 3.2 Установка Рутокен плагина и его расширения

ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключевых носителях Рутокен. ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин» необходимо установить на компьютер, с которого будет выполняется подключение к Клиентской части Центра регистрации Aladdin eRA.

> **Внимание! При установке и использовании ПО «Рутокен Плагин» и его браузерного расширения «Адаптер Рутокен Плагин» сертифицированная среда функционирования не обеспечивается.**

Скачайте дистрибутив ПО «Рутокен Плагин» с официального сайта производителя.

Установите ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен по инструкции с официального сайта производителя.

ПРИЛОЖЕНИЕ 4. ФОРМАТ И ПРАВИЛА ЗАПИСИ ЗНАЧЕНИЙ В ПОЛЯ СЕРТИФИКАТА НА БУМАЖНОМ НОСИТЕЛЕ

4.1 Формат сертификата на бумажном носителе для физического лица

Сертификат ключа проверки электронной подписи

1. Номер квалифицированного сертификата: _____

2. Действие квалифицированного сертификата: с _____ по _____

3. Сведения о владельце квалифицированного сертификата

- Фамилия, имя, отчество: _____

- ПИН: _____

4. Сведения об издателе квалифицированного сертификата

- Наименование УЦ: _____

- Место нахождения УЦ: _____

- Доверенное лицо УЦ: _____

5. Номер квалифицированного сертификата УЦ: _____

6. Наименование средства ЭП: _____

7. Реквизиты заключения о подтверждении соответствия средства ЭП:_____

8. Наименование средства УЦ: _____

9. Реквизиты заключения о подтверждении соответствия средства УЦ:_____

10. Сведения о ключе проверки ЭП

- Используемый алгоритм: _____

- Используемое средство ЭП: _____

- Область использования ключа: _____

- Значение ключа: _____

11. ЭП под квалифицированным сертификатом

- Используемый алгоритм: _____

- Значение ЭП: _____

Подпись уполномоченного лица _____ /_____/

4.2 Формат сертификата на бумажном носителе для юридического лица

Сертификат ключа проверки электронной подписи

1. Номер квалифицированного сертификата: _____

2. Действие квалифицированного сертификата: с _____ по _____

3. Сведения о владельце квалифицированного сертификата

- Наименование юридического лица: _____
- ИНН: _____
- Место нахождения юридического лица: _____
- Уполномоченный представитель юридического лица: _____
- ПИН: _____

4. Сведения об издателе квалифицированного сертификата

- Наименование УЦ: _____
- Место нахождения УЦ: _____
- Доверенное лицо УЦ: _____

5. Номер квалифицированного сертификата УЦ: _____

6. Наименование средства ЭП: _____

7. Реквизиты заключения о подтверждении соответствия средства ЭП: _____

8. Наименование средства УЦ: _____

9. Реквизиты заключения о подтверждении соответствия средства УЦ: _____

10. Сведения о ключе проверки ЭП

- Используемый алгоритм: _____
- Используемое средство ЭП: _____
- Область использования ключа: _____
- Значение ключа: _____

11. ЭП под квалифицированным сертификатом

- Используемый алгоритм: _____
- Значение ЭП: _____

Подпись уполномоченного лица _____ /_____/

4.3 Правила записи значений в поля сертификата на бумажном носителе для физического лица

Поле	Значение
1. Номер квалифицированного сертификата	Серийный номер сертификата
2. Действие квалифицированного сертификата	
с	Дата и время начала действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
по	Дата и время окончания действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
3. Сведения о владельце квалифицированного сертификата	
Фамилия, имя, отчество	CN в сертификате
ПИН	INN в сертификате
4. Сведения об издателе квалифицированного сертификата	
Наименование УЦ	CN в сертификате ЦС, издавшего данный сертификат
Место нахождения УЦ	Строка вида «{поле «C» в сертификате ЦС}, {поле «ST» в сертификате ЦС}, {поле «L» в сертификате ЦС}, {поле «STREET» в сертификате ЦС}»
Доверенное лицо УЦ	Строка вида «{поле «T» в сертификате ЦС} {поле «SURNAME» в сертификате ЦС} {поле «GIVENNAME» в сертификате ЦС}»
5. Номер квалифицированного сертификата УЦ	Серийный номер сертификата ЦС
6. Наименование средства ЭП	issuerSignTool.signTool (1.2.643.100.112 [0]) из сертификата
7. Реквизиты заключения о подтверждении соответствия средства ЭП	issuerSignTool.signToolCert (1.2.643.100.112 [2]) из сертификата
8. Наименование средства УЦ	issuerSignTool.cATool (1.2.643.100.112 [1]) из сертификата
9. Реквизиты заключения о подтверждении соответствия средства УЦ	issuerSignTool.cAToolCert (1.2.643.100.112 [3]) из сертификата
10. Сведения о ключе проверки ЭП	
Используемый алгоритм	Алгоритм ключа в сертификате

Поле	Значение
Используемое средство ЭП	subjectSignTool (1.2.643.100.111) из сертификата
Область использования ключа	Список keyUsage
Значение ключа	Отрытый ключ (hex; разделитель - пробелы)
11. ЭП под квалифицированным сертификатом	
Используемый алгоритм	Алгоритм подписи сертификата
Значение ЭП	Подпись (hex; разделитель - пробелы)

Примечания:

1 В случае, если для поля сертификата на бумажном носителе в преобразуемом сертификате отсутствуют значения (в случае составных полей – для всех компонентов составного поля отсутствуют значения), то для данного поля в качестве значения указан прочерк «-».

2 Формат значения в поле «Используемый алгоритм» в разделе «Сведения о ключе проверки ЭП»:
<Название алгоритма> (<длина ключа>)
Примеры:
- RSA (2048)
- ECDSA (384)
- ГОСТ Р 34.10-2012 (256)

3 Формат значения в поле «Используемый алгоритм» в разделе «ЭП под квалифицированным сертификатом»:
- «Алгоритм хеш-суммы» «Алгоритм ключа» - для подписи, формируемой с помощью RSA или ECDSA ключа.
Примеры:
- SHA512RSA
- SHA512ECDSA
- ГОСТ Р 34.11-2012/34.10-2012 (длина ключа)» - для подписи, формируемой с помощью ГОСТ ключа.
Примеры:
- ГОСТ Р 34.11-2012/34.10-2012 (256)
- ГОСТ Р 34.11-2012/34.10-2012 (512)

4.4 Правила записи значений в поля сертификата на бумажном носителе для юридического лица

Поле	Значение
1. Номер квалифицированного сертификата	Серийный номер сертификата
2. Действие квалифицированного сертификата	
с	Дата и время начала действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
по	Дата и время окончания действия сертификата в формате «ДД.ММ.ГГГГ ЧЧ:ММ:СС (UTC)»
3. Сведения о владельце квалифицированного сертификата	
Наименование юридического лица	CN в сертификате
ИНН	INNLE в сертификате
Место нахождения юридического лица	Строка вида «{поле «C» в сертификате}, {поле «ST» в сертификате}, {поле «L» в сертификате}, {поле «STREET» в сертификате}»
Уполномоченный представитель юридического лица	Строка вида «{поле «T» в сертификате} {поле «SURNAME» в сертификате} {поле «GIVENNAME» в сертификате}»
ПИН	INN в сертификате
4. Сведения об издателе квалифицированного сертификата	
Наименование УЦ	CN ЦС
Место нахождения УЦ	Строка вида «{поле «C» в сертификате ЦС}, {поле «ST» в сертификате ЦС}, {поле «L» в сертификате ЦС}, {поле «STREET» в сертификате ЦС}»
Доверенное лицо УЦ	Строка вида «{поле «T» в сертификате ЦС} {поле «SURNAME» в сертификате ЦС} {поле «GIVENNAME» в сертификате ЦС}»
5. Номер квалифицированного сертификата УЦ	Серийный номер сертификата ЦС
6. Наименование средства ЭП	issuerSignTool.signTool (1.2.643.100.112 [0]) из сертификата
7. Реквизиты заключения о подтверждении соответствия средства ЭП	issuerSignTool.signToolCert (1.2.643.100.112 [2]) из сертификата
8. Наименование средства УЦ	issuerSignTool.cATool (1.2.643.100.112 [1]) из сертификата
9. Реквизиты заключения о подтверждении	issuerSignTool.cAToolCert (1.2.643.100.112 [3]) из

Поле	Значение
соответствия средства УЦ	сертификата
10. Сведения о ключе проверки ЭП	
Используемый алгоритм	Алгоритм ключа в сертификате
Используемое средство ЭП	subjectSignTool (1.2.643.100.111) из сертификата
Область использования ключа	Список keyUsage
Значение ключа	Отрытый ключ (hex; разделитель - пробелы)
11. ЭП под квалифицированным сертификатом	
Используемый алгоритм	Алгоритм подписи сертификата
Значение ЭП	Подпись (hex; разделитель - пробелы)

Примечания:

1 В случае, если для поля сертификата на бумажном носителе в преобразуемом сертификате отсутствуют значения (в случае составных полей – для всех компонентов составного поля отсутствуют значения), то для данного поля в качестве значения указан прочерк «-».

2 Формат значения в поле «Используемый алгоритм» в разделе «Сведения о ключе проверки ЭП»:
<Название алгоритма> (<длина ключа>)
Примеры:
- RSA (2048)
- ECDSA (384)
- ГОСТ Р 34.10-2012 (256)

3 Формат значения в поле «Используемый алгоритм» в разделе «ЭП под квалифицированным сертификатом»:
- «Алгоритм хеш-суммы» «Алгоритм ключа» - для подписи, формируемой с помощью RSA или ECDSA ключа.
Примеры:
- SHA512RSA
- SHA512ECDSA
- ГОСТ Р 34.11-2012/34.10-2012 (длина ключа)» - для подписи, формируемой с помощью ГОСТ ключа.
Примеры:
- ГОСТ Р 34.11-2012/34.10-2012 (256)
- ГОСТ Р 34.11-2012/34.10-2012 (512)

4.5 Пример сертификата на бумажном носителе для физического лица

Сертификат ключа проверки электронной подписи

1. Номер квалифицированного сертификата: 1389df28647548cd880ebfa2ad6c22ddff14f6da
2. Действие квалифицированного сертификата: с 02.09.2025 14:16:23 UTC по 03.09.2026 14:16:23 UTC
3. Сведения о владельце квалифицированного сертификата
   - Фамилия, имя, отчество: Иванов Иван Иванович
   - ПИН: 01234567891234
4. Сведения об издателе квалифицированного сертификата
   - Наименование УЦ: Root
   - Место нахождения УЦ: Страна, Область, Город, Ул. Тест 3, д. 123
   - Доверенное лицо УЦ: Директор Петров Петр Петрович
5. Номер квалифицированного сертификата УЦ: 3afef9c1f4b24b4d9afd0e0bb5f9befd24c1d65e
6. Наименование средства ЭП: КриптоПро HSM
7. Реквизиты заключения о подтверждении соответствия средства ЭП: Заключение на КриптоПро HSM
8. Наименование средства УЦ: КриптоПро УЦ
9. Реквизиты заключения о подтверждении соответствия средства УЦ: Заключение на КриптоПро УЦ
10. Сведения о ключе проверки ЭП
    - Используемый алгоритм: RSA (2048)
    - Используемое средство ЭП: КриптоПро CSP
    - Область использования ключа: Цифровая подпись, Подтверждение подлинности, Шифрование ключей
    - Значение ключа: 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 BC C2 E8 BC 6E 23 B5 42 35 88 57 1E 18 8B BE D4 99 87 8B A3 C9 12 C8 8A 89 91 D6 07 37 B9 98 90 4B 90 97 A7 07 81 E8 CC 69 EF EC B4 03 D4 41 DA 16 FD 3E 0F BA D0 5A 52 4F 4B D7 0E CB 42 7E AD 73 8B 52 7C E7 71 AE 84 D0 DD 92 1B 4A F6 1E 3C F4 55 59 FA 1B E8 60 03 40 CB 6A 68 E1 54 01 34 ED 61 5E CA 10 B4 83 5E 02 99 E5 3F C6 69 43 19 6D AF 4E B1 0F D3 40 2A B6 53 6F 70 64 26 07 15 5F 94 BD 2F CF 0C 00 4B 71 61 43 8C 8D 9D E3 4C 11 9C 94 E3 B8 4F 85 14 3F 15 DF EA 9B 8F 3F 48 57 22 36 E3 FE 40 19 9B 90 1F A1 19 E5 12 41 31 98 B2 97 F0 0C 74 74 CD BF D9 C3 20 1A 42 9C 1B 4A A7 FA D1 DA C9 31 23 55 A6 EB 30 8D 34 0E D4 38 3A EB 36 A2 3B 56 A2 0F 0C 03 AC 1A DD 54 C5 5B 09 D0 F0 00 CB 2B E1 DD 67 03 CB 52 C0 73 C1 0F 14 9B 7D C8 EB 2D 69 6B 82 B0 10 95 D9 55 B3 02 03 01 00 01
11. ЭП под квалифицированным сертификатом
    - Используемый алгоритм: SHA512RSA
    - Значение ЭП: 76 4C C2 F3 6A 78 81 03 2B F9 CF 99 76 BB 4F 03 82 FC 89 7C 48 66 94 9A 6B E0 5A 6B E5 55 C4 A4 78 FC DC 2B DB 5A 9B CB DE 95 89 AD CB 30 23 A8 F3 31 6F F4 AD 85 B8 71 9B FB 44 ED AB B3 78 39 F3 75 03 3B 8B 92 48 C2 39 D1 FB CF E5 79 53 52 77 77 FD 2B 2A D2 E6 5E BA 0C B8 FE 2F 13 32 0F A6 5D B9 77 46 8D C3 A4 65 5E 52 07 D8 42 AF 72 11 F2 F6 03 4D 82 4F 36 A5 6E C1 3E 8F 16 B0 D9 C2 A7 EA 8D 91 79 EB D8 26 CA DF 96 67 99 5A 73 E2 70 AC B3 D3 ED 4F E8 B9 B5 62 A4 5F 9E FE 4A 20 F5 27 38 7A 48 ED C4 BA C3 59 6D 67 C9 08 3C 5F 82 81 C8 AE 4B 20 88 87 C1 79 BC EF 77 F5 FA 44 E0 25 1B B9 20 38 9B 6A B6 AB 27 D8 19 33 04 52 47 5A A9 8D 06 C4 38 3B E3 DB FD 00 3B F7 F1 BA 66 65 8D 26 C6 02 E4 8C 5C E7 CC 24 7A A2 32 CD B9 FD BA 22 A5 4B 84 14 BB 97 DA 28 B9 4E F1 CF 1E 73 E7 A8 11 8E 75 B2 F6 3A 27 5C D4 67 55 03 5E F3 B6 E3 B9 26 65 34 DB 51 87 4D 9B 07 D3 83 41 D7 3F 18 21 94 DF C4 FA 23 6A 4D A0 1F 86 3E D3 D4 A8 9F FA 1C 15 5C 49 35 38 CD 02 CB 2F C5 F7 10 B2 66 A4 CE 40 F8 2B 17 0A EE 7F 37 66 C8 5F 38 86 0F 11 CD 8A 38 FF 23 B2 3B B1 62 E6 16 6E 69 C2 43 86 11 EE B9 64 4A 1C FD 6F 03 1B 10 E5 95 73 82 CF 37 EA B1 FB 72 EA D6 2A 45 99 F7 01 A4 EA 53 27 C9 C4 D1 2C 2C AE 9C 50 27 EC E2 B7 1B 61 60 A8 63 7A 4B B3 D9 8F C8 19 C0 B6 9A C1 6C 02 FB 81 0D 79 3C 87 37 FA 17 37 B2 E7 15 58 D0 F8 05 57 79 BA 57 C2 66 56 78 40 B5 EA 8F C3 4C 31 5B D7 8F 53 B5 C0 7E 0C 8B 73 0F 74 17 0F D2 FC 67 3B 23 3B 9A C8 FB A0 69 80 48 2B F0 C6 55 C4 C0 56 1D 93 DE 5E 69 2A 8B 05 B3 D5 D2 CB DC E9 95 72 84 90 AD 7B 8B BC 41 4F 2A 2D

Подпись уполномоченного лица _____ /_____ /

4.6 Пример сертификата на бумажном носителе для юридического лица

Сертификат ключа проверки электронной подписи

1. Номер квалифицированного сертификата: 5b4d309e9baee870703354096d6580c9bbf11f10
2. Действие квалифицированного сертификата: с 02.09.2025 14:15:16 UTC по 03.09.2026 14:15:16 UTC
3. Сведения о владельце квалифицированного сертификата
   - Наименование юридического лица: ОсОО Тест
   - ИНН: 01234567891234
   - Место нахождения юридического лица: Страна, Область, Город, Пер. Тест 32 д. 456
   - Уполномоченный представитель юридического лица: Директор Антонов Антон Антонович
   - ПИН: 01234567891234
4. Сведения об издателе квалифицированного сертификата
   - Наименование УЦ: Root
   - Место нахождения УЦ: Страна, Область, Город, Пер. Тест 32 д. 123
   - Доверенное лицо УЦ: Директор Петров Петр Петрович
5. Номер квалифицированного сертификата УЦ: 3afef9c1f4b24b4d9afd0e0bb5f9befd24c1d65e
6. Наименование средства ЭП: КриптоПро HSM
7. Реквизиты заключения о подтверждении соответствия средства ЭП: Заключение на КриптоПро HSM
8. Наименование средства УЦ: КриптоПро УЦ
9. Реквизиты заключения о подтверждении соответствия средства УЦ: Заключение на КриптоПро УЦ
10. Сведения о ключе проверки ЭП
    - Используемый алгоритм: RSA (2048)
    - Используемое средство ЭП: КриптоПро CSP
    - Область использования ключа: Цифровая подпись, Подтверждение подлинности, Шифрование ключей
    - Значение ключа: 30 82 01 22 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05 00 03 82 01 0F 00 30 82 01 0A 02 82 01 01 00 AF 2E 5F 8A 22 28 4B 1C 8E 71 EC 96 BD E4 F6 2E 14 73 AE FC 1D 1E 13 88 BA E4 B8 DD 54 05 0E 14 48 CD C4 A8 68 81 7F 18 22 D6 B4 4C 7B 17 EA 1A 60 50 12 41 11 70 BC 60 04 B8 61 03 2C 5F 67 17 D0 33 55 DF 65 59 E7 EE 53 82 91 D6 BC 81 02 BB DF 2C 06 74 07 6A AC 18 91 E9 5D 3C CC 6C 11 A1 19 D1 6F BE A7 57 B2 14 FE E3 A2 C1 C8 8F 42 DA 1B 88 C8 B6 62 EE EE 78 7E 1F 75 99 D9 5E AE 9D CC 75 C5 34 2A AF 9D 4D D4 27 B5 9A 75 4E AE D3 95 E2 CF 3C DD 6D 36 7C AC 98 6D 99 D1 DE FB AF 60 B6 92 DF 97 17 AC 2C 18 B1 47 3C D7 C4 D0 6A E7 50 26 DF 8D F7 7A 72 45 AA 74 B2 09 22 9F C0 1A 77 2A D1 4A 2D A2 3D D6 85 E2 BE FD 25 3B 20 FF 1D 0A A4 13 91 E3 70 C9 62 5B FB 57 0E 39 B1 B5 18 3C C2 4D A6 35 06 86 57 FC F4 9E 80 AC 59 82 B7 6B 2F A5 7B 9B 7C 82 CC B2 6A 59 79 31 F5 02 03 01 00 01
11. ЭП под квалифицированным сертификатом
    - Используемый алгоритм: SHA512RSA
    - Значение ЭП: 86 A5 1D 7E 93 F2 43 FB 4A C4 59 38 C5 69 C9 B0 46 23 16 AF EE A2 2C 4F 9F BD D8 EE 1A 3B B5 DF 22 5D 3F 22 FC AF 4F C4 BD C2 50 B7 F5 AB 1C E9 BA A1 FF 40 03 32 5A E6 09 CF FF 79 90 ED 68 38 DD C5 84 A9 43 A0 5B 73 80 C6 48 BD D4 55 86 79 09 9B 07 50 06 7F 61 DD E5 2F A9 F8 3B BC C1 B5 C1 2A F5 85 74 87 42 60 F2 BB F4 47 9E E7 9C 7C 2D 0D DD 3D 14 5C B2 82 5C A6 DB 50 43 0A 06 F2 FF C8 2F 31 95 68 01 64 3C 78 9E B6 A3 9F 42 0F 9C D0 20 0F FC 17 95 08 59 74 45 22 A0 09 18 80 3B 36 27 A2 29 70 DC 7F 90 38 48 73 68 9F 2E 04 34 24 09 91 A9 17 FC 7E 5E 90 20 6C 61 C7 7B 38 8E 8B 6B 7C 55 6C 76 02 EB 96 BA 8F 59 34 22 95 E0 B4 30 3F 02 C3 CE EA 63 EA 50 49 7B 83 2A 0A 16 58 6F 4F EB 30 BD 1E 4A BF 95 D1 A9 44 99 1C 0E B8 08 0A 90 97 B2 A4 9A 61 F7 A3 05 E0 61 29 9A 3C A1 F3 83 9B AE 3B 5B 1D 06 C5 47 CE FB 7D B1 BE 3D 9C 0A 09 33 DE 37 BA 3E A6 87 9C 2E 44 26 42 F9 11 9A 03 6F EB B3 C0 9F CC 46 23 0D D1 14 04 4E BE C7 BA B1 2D 94 E6 FD A9 BF AB E3 E8 5C 99 74 FC 0C 52 F3 5E F6 7A 63 83 9F 50 FD 94 E2 F0 F1 6E 0B 75 0A F4 8D 03 97 0F E8 42 1D CF 80 51 35 19 C4 E3 91 19 58 5D C2 A9 FE 15 A2 B3 07 7F 85 52 60 DA 55 F2 B9 09 9C D8 C1 B5 E2 26 7F DC DF 5E 5B A3 86 A0 01 18 94 B4 22 53 FA 95 9D 7B 5C C0 B0 D6 DB 4E 5B 36 BD F8 D0 AC 57 BF EF 93 6C 98 65 1A 3E FB 63 7F 6C 10 59 F2 EC C0 50 A9 07 F6 61 65 C0 F8 FD 28 98 7F EE 2D 43 9E F2 08 26 EC FC B4 6F 68 29 A0 8E 1A 61 A8 4C BE 9F 32 91 C1 08 BD EC C5 57 8B 48 B8 7E A2 22 E9 0F F4 69 62 B7 61 83 93 D9 9C 76 B8 78 80 88 D1 28 38 8A 04 F2 75 F7 F2 CF 05 CC 0B 77 C7 30 17

Подпись уполномоченного лица _____ /_____ /

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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.

Ключевой носитель – 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.

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.

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).

Токен доступа – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен доступа используется для передачи данных для аутентификации в клиент-серверных приложениях. Токены создаются сервером, подписываются секретным ключом и передаются клиенту, который в дальнейшем использует данный токен для подтверждения своей личности.

Токен обновления – это уникальная последовательность символов (букв, цифр и символов), основанная на формате JSON. Токен обновления выдается сервером в результате успешной аутентификации и используется для получения нового токена доступа и обновления токена обновления.

Центр сертификации – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения процессов идентификации и строгой аутентификации в информационной системе. Программный компонент «Центр сертификации» является частью Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition.

Шаблон субъекта – шаблон, на основании которого необходимо создавать субъекты. Шаблон определяет свойства субъекта (subject name, alternative name), свойства сертификата (криптографию, срок действия, назначение, политики и проч.), а также инфраструктурные характеристики (реквизиты для доставки сертификатов, возможности отзыва, хранения и проч.).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
СВТ	–	Средство вычислительной техники
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦС	–	Центр сертификатов
CRL	–	Certificate Revocation List
AIA	–	Authority Information Access
URL	–	Uniform Resource Locator

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводи-тельного документа и дата	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					
1	-	Все	-	-	-	АЛДЕ.28.1.010-24ИИ	-		24.03.2025
6	-	Все	-	-	-	АЛДЕ.28.1.015.3/3-25ИИ	-		30.05.2025