



Центр сертификатов доступа

# Aladdin Enterprise Certificate Authority Certified Edition

Руководство администратора. Часть 5. Центр регистрации  
Aladdin Enterprise Registration Authority

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-5
Версия	2.4
Листов	190
Дата	28.05.2026

## Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации.

Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р.Д.».

Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ. При перепечатке и использовании данных материалов либо любой их части ссылки на АО «Аладдин Р.Д.» обязательны.

Владельцем зарегистрированных товарных знаков "Аладдин", Aladdin, JaCarta, JMS, JAS, Secret Disk, SecurLogon, "Крипто БД", логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является АО «Аладдин Р.Д.».

Названия прочих технологий, продуктов, компаний, упоминающиеся в данном документе, могут являться товарными знаками своих законных владельцев.

### Ограничение ответственности

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены АО «Аладдин Р.Д.» без предварительного уведомления.

АО «Аладдин Р.Д.» не гарантирует ни отсутствия ошибок в данном документе, ни того, что описанное программное обеспечение (ПО) не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

АО «Аладдин Р.Д.» не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется по закону.

Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе АО «Аладдин Р.Д.» не предоставляет никаких ни явных, ни подразумеваемых гарантий.

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

### Государственное регулирование и экспортный контроль

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

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

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

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

© АО «Аладдин Р.Д.», 1995—2026. Все права защищены

## Лицензионное соглашение

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

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

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

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

### Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ.

Программное обеспечение, включая все доработки, 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.), подтвержденные или включенные в приложения/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, приведенными в данном и других документах Компании, в том числе на портале онлайн документации для разработчиков Компании (<http://developer.aladdin-rd.ru/>).

### Использование ПО

Пользователь вправе:

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

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

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

- дизайна (графики, расположения элементов оформления и т.п.);
  - всех иных элементов, в том числе изображений, фонограмм, текстов.
- Получаемые Пользователем неисключительные имущественные права не включают права на передачу третьим лицам каких-либо прав на встраивание, воспроизведение, распространение и использование программ для ЭВМ не в составе продуктов и решений Пользователя.

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

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

## Обслуживание и поддержка

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

## Ограниченная гарантия

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

## Отказ от гарантии

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

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

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

## Ограничение возмещения

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

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

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

## Исключение косвенных убытков

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

## Ограничение ответственности

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

## Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

## Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

## Разное

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

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

## АННОТАЦИЯ

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

Документ определяет порядок подготовки, установки и эксплуатации программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority»<sup>1</sup> из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»<sup>2</sup>. Перед эксплуатацией программы рекомендуется внимательно ознакомиться с настоящим руководством.

Сведения о составе, комплектности и функциях Центра сертификатов доступа приведены в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority».

Инструкции по установке стороннего программного обеспечения из состава среды функционирования программы приведены в ознакомительных целях, для получения более точной информации рекомендуем ознакомиться с актуальными инструкциями по установке и настройке продуктов на официальных сайтах производителей.

Характер изложения материала данного руководства предполагает, что вы знакомы с операционными системами (далее - ОС) семейства Linux и владеете базовыми навыками администрирования для работы в них.

Руководство администратора соответствует требованиям к разработке эксплуатационной документации, определённым в методическом документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий», утверждённого приказом ФСТЭК России от 02 июня 2020 г. №76 по 4 уровню доверия.

Таблица 1 – Соответствие документации требованиям доверия

Требования доверия (16.1 Руководство администратора должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
Действий по приёмке поставленного средства	Раздел 3 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»
Действий по безопасной установке и настройке средства	Раздел 1.8 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»
Действий по реализации функций безопасности среды функционирования средства	Раздел 1.9 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»

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

<sup>1</sup> Далее по документу - программа, eCA-RA.

<sup>2</sup> Далее по документу - программное средство, eCA.

## СОДЕРЖАНИЕ

Аннотация .....	5
1 Введение .....	9
1.1 Назначение программы.....	9
1.2 Состав программы.....	9
1.3 Функции программы .....	9
1.4 Роли управления.....	10
1.5 Режимы функционирования программы.....	13
2 Условия выполнения программы.....	14
2.1 Требования к программному обеспечению .....	14
2.1.1 Требования к среде функционирования Серверной части программы.....	14
2.1.2 Требования к среде функционирования Клиентской части программы .....	15
2.2 Требования к аппаратным средствам .....	15
3 Подготовка к установке программы.....	17
3.1 Подготовка среды функционирования с РЕД ОС и РОСА «ХРОМ» 12 Сервер .....	19
3.1.1 Подключение репозитория и установка зависимостей .....	19
3.1.2 Установка среды исполнения Java .....	19
3.1.3 Установка и настройка СУБД .....	20
3.1.4 Установка веб-сервера.....	23
3.2 Подготовка среды функционирования с ОС Astra Linux Special Edition 1.8.....	24
3.2.1 Подключение репозитория и установка зависимостей .....	24
3.2.2 Установка среды исполнения Java .....	25
3.2.3 Установка и настройка СУБД .....	25
3.2.4 Установка веб-сервера.....	28
3.3 Подготовка среды функционирования с ОС Альт 8 СП релиз 10 вариант исполнения Сервер и ОС «Альт Сервер» 11.....	29
3.3.1 Подключение репозитория и установка зависимостей ОС Альт 8 СП релиз 10 вариант исполнения Сервер .....	29
3.3.2 Установка среды исполнения Java .....	29
3.3.3 Установка и настройка СУБД .....	29
3.3.4 Установка веб-сервера.....	32
3.4 Подготовка среды функционирования с ОС «Platform V SberLinux OS Server».....	33
3.4.1 Установка среды исполнения Java .....	33
3.4.2 Установка и настройка СУБД .....	33
3.4.3 Установка веб-сервера.....	36
3.5 Создание службы HTTP и keytab-файла .....	37
3.6 Установка веб-сервера Cppnginx.....	37
3.7 Установка JC-WebClient .....	38
3.8 Установка Рутокен плагина и его расширения .....	38
4 Установка программы .....	39
4.1 Распаковка инсталляционного комплекта .....	39
4.2 Настройка конфигурации программы .....	40
4.3 Настройка веб-сервера при ограничении доступа к его файлам.....	53
4.4 Создание и настройка базы данных .....	53
4.4.1 Создание и настройка базы данных в автоматическом режиме.....	53
4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме .....	54
4.4.3 Создание и настройка базы данных Jatoba в ручном режиме .....	55
4.5 Установка программы .....	57
4.6 Порядок совместной установки программы с другими компонентами Центра сертификатов доступа на одном сервере.....	59
5 Запуск и завершение программы .....	60
6 Подключение к веб-интерфейсу .....	62
6.1 Общие сведения.....	62
6.2 Установка сертификата администратора .....	62
6.3 Подключение к веб-интерфейсу .....	65

6.4	Переопределение сведений, отображаемых в окне авторизации и в заголовке вкладки браузера	66
6.5	Аутентификация с использованием сертификата	67
6.6	Аутентификация по имени и паролю доменной учётной записи	68
6.7	Аутентификация с использованием Kerberos-билета	68
6.8	Завершение рабочей сессии пользователя	69
7	Функции управления программы	70
7.1	Верхняя панель	70
7.2	Боковая панель	70
7.3	Раздел «Центр регистрации»	73
7.4	Раздел «Заявки»	73
7.4.1	Управление экранной таблицей	76
7.4.2	Фильтрация заявок	77
7.4.3	Сортировка заявок	78
7.4.4	Поиск заявок	78
7.4.5	Карточка заявки	78
7.4.6	Создание заявки на основании запроса	83
7.4.7	Создание заявки с закрытым ключом PKCS#12	85
7.4.8	Создание заявки на ключевом носителе	88
7.4.9	Отмена заявки	92
7.4.10	Обработка заявки	93
7.4.11	Импорт сертификата на ключевой носитель	94
7.4.12	Отзыв сертификата	96
7.5	Раздел «Учётные записи»	98
7.5.1	Вкладка «Учётные записи eCA»	98
7.5.2	Вкладка «Получатели сертификатов»	98
7.5.3	Блокировка доменной учётной записи	99
7.5.4	Активация доменной учётной записи	99
7.6	Раздел «Журнал событий»	100
7.6.1	О журнале событий	100
7.6.2	Просмотр записей журнала событий	100
7.6.3	Просмотр карточки события	104
7.6.4	Экспорт записей журнала событий	105
7.6.5	Передача информации о событиях в сторонние системы по протоколу Syslog	105
7.7	Раздел «Управление»	108
7.7.1	Вкладка «Правила выпуска»	108
7.7.2	Вкладка «SCEP»	120
7.8	Смена сертификата веб-сервера	127
7.9	Просмотр информации о разрешённых издателях	129
8	Поддержка протокола SCEP	130
8.1	Настройка SCEP-сервера	130
8.2	Обработка запросов по протоколу SCEP	131
8.2.1	Обработка запроса клиента PKCSReq/RenewalReq	131
8.2.2	Обработка запроса клиента CertPoll	132
8.2.3	Обработка запроса клиента GetCert	132
8.2.4	Обработка запроса клиента GetCRL	132
8.2.5	Обработка запроса клиента GetCACert	132
8.2.6	Обработка запроса клиента GetCACaps	132
9	Поддержка протоколов MS-XCEP и MS-WSTEP	133
9.1	Обработка запроса на получение политики «GetPolicies»	133
9.2	Обработка запроса на выпуск сертификата «RequestSecurityToken»	135
9.3	Создание политики регистрации сертификатов	136
9.4	Запрос нового сертификата	137
9.5	Перевыпуск сертификатов	139
10	Офлайн выпуск сертификатов	140
10.1	Поддерживаемые расширения и кодировки файлов запросов	140
10.2	Сценарий офлайн выпуска сертификатов	140

10.3 Включение офлайн выпуска сертификатов .....	141
10.4 Отключение офлайн выпуска сертификатов .....	141
11 Контроль целостности.....	142
11.1 Автоматический контроль целостности при запуске eCA-RA .....	142
12 Сбор диагностической информации .....	143
13 Резервное копирование и восстановление данных .....	145
13.1 Резервное копирование данных .....	145
13.2 Настройка расписания резервного копирования.....	145
13.3 Восстановление данных из резервной копии .....	146
14 Обновление программы.....	147
15 Удаление программы .....	149
16 Удаление базы данных Postgres.....	150
16.1 Удаление базы данных .....	150
16.2 Удаление пользователя базы данных .....	150
17 Поиск и устранение неисправностей.....	151
Приложение 1. Разрешение конфликта при установке СУБД PostgreSQL и СУБД Postgres Pro .....	153
Приложение 2. Настройка подключения к внешней СУБД .....	154
2.1 Настройка на хосте СУБД .....	154
2.1.1 Настройка на хосте СУБД для Astra Linux .....	154
2.1.2 Настройка на хосте СУБД для РЕД ОС, РОСА «ХРОМ» 12 Сервер, SberLinux OS Server и Альт Сервер .....	154
2.2 Настройка на хосте eCA-RA.....	155
Приложение 3. Настройка TLS-соединения с СУБД .....	156
3.1 Настройка на хосте СУБД .....	156
3.2 Настройка на хосте eCA-RA.....	157
Приложение 4. Развёртывание кластера.....	158
4.1 Развертывание кластера в виртуальной среде с холодным резервированием «active-passive»... ..	158
4.2 Развертывание кластера с холодным резервированием «active-passive».....	160
4.3 Развертывания кластера в виртуальной среде с горячим резервированием «active-active» .....	163
4.4 Развертывание кластера с горячим резервированием «active-active».....	165
4.3 Обновление ПО узлов кластера .....	167
Приложение 5. Настройка Kerberos в веб-браузере .....	169
5.1 Настройка веб-браузера Firefox.....	169
5.2 Настройка веб-браузера Chromium .....	170
Приложение 6. Перечень регистрируемых событий .....	171
6.1 События запуска/остановки служб, применения параметров конфигурационного файла .....	171
6.2 События аутентификации пользователей.....	171
6.3 События работы с УЗ получателей сертификатов.....	172
6.4 События работы с заявками .....	173
6.5 События работы с ключевыми носителями.....	175
6.6 События экспорта.....	176
6.7 События работы с правилами выпуска .....	176
6.8 События работы с веб-сервером и издателями.....	178
6.9 События Offline-выпуска.....	178
6.10 События работы с резервными копиями .....	179
6.11 События контроля целостности.....	179
6.12 События архивации и очистки записей аудита .....	179
6.13 События работы с Syslog .....	180
6.14 События перевыпуска сертификатов технологической учётной записи eCA-RA для связи с eCA-CA .....	181
6.15 События SCEP .....	181
Приложение 7. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP» .....	185
Обозначения и сокращения.....	187
Термины и определения .....	188
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	190



# 1 ВВЕДЕНИЕ

## 1.1 Назначение программы

Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», которое применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификацию при управлении доступом субъектов<sup>1</sup> доступа к объектам<sup>2</sup> доступа в автоматизированной (информационной) системе.

еCA-RA предназначен для обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов)<sup>3</sup>, выпускаемых программным комплексом «Центр сертификации Aladdin Enterprise Certification Authority»<sup>4</sup> из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

## 1.2 Состав программы

еCA-RA является клиент-серверным веб-приложением и состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра регистрации»<sup>5</sup>.  
Программный компонент реализует функции еCA-RA, для выполнения которых оно предназначено в заданных условиях применения, в части формирования идентификационной информации, необходимой для выпуска сертификатов безопасности, выпуска и обслуживания сертификатов.
- Программный компонент «Клиентская часть Центра регистрации»<sup>6</sup>.  
Программный компонент реализует интерфейс, с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации».

## 1.3 Функции программы

Основные функции еCA-RA:

- Формирование и обработка заявок на выпуск сертификатов, в том числе:
  - Создание, просмотр и обработка заявок на выпуск сертификатов.
  - Создание заявок через программный интерфейс по протоколу WS-Trust X.509v3 Token Enrollment Extensions (WSTEP) <sup>7</sup>.
  - Создание заявок через программный интерфейс по протоколу Simple Certificate Enrollment Protocol (SCEP) <sup>8</sup>.
  - Автоматическое создание заявок на основании запросов PKCS#10 из локального или сетевого каталога в соответствии с настройками Offline-выпуска.

<sup>1</sup> 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.

<sup>2</sup> 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.

<sup>3</sup> Далее по документу - сертификаты.

<sup>4</sup> Далее по документу – еCA-CA.

<sup>5</sup> Далее по документу - Серверная часть программы.

<sup>6</sup> Далее по документу - Клиентская часть программы.

<sup>7</sup> В соответствии с документом «OASIS WS-Trust 1.3. WS-Trust X.509 Token Profile (WSTEP)».

<sup>8</sup> В соответствии с документом «RFC 8894. Simple Certificate Enrollment Protocol».

- Загрузка файлов запросов для заявок на выпуск сертификатов по запросу.
- Выгрузка файлов сертификатов, цепочки сертификатов, списка отозванных сертификатов (CRL) и цепочки сертификатов eCA-CA, издавшего данный сертификат.
- Импорт сертификатов на ключевые носители.
- Выгрузка контейнера закрытого ключа для заявок на выпуск сертификата с закрытым ключом.
- Отзыв сертификатов.
- Управление учётными записями подключённого eCA-CA и доменными учётными записями служб каталогов (ресурсных систем), в том числе:
  - Просмотр учётных записей.
  - Блокировка и активация учётных записей.
- Формирование и управление правилами выпуска сертификатов, позволяющими определить режим обработки заявки, в том числе:
  - Создание, просмотр, редактирование и удаление правил выпуска.
  - Запуск и остановка действия правил выпуска.
- Регистрация, хранение, просмотр и хранение записей аудита, а также их публикация по протоколу Syslog.
- Управление профилями <sup>3</sup> и политиками SCEP, в том числе:
  - Создание, изменение и удаление SCEP-политик, а также управления их статусами.
  - Создание, остановка, запуск и удаление SCEP-профилей.

## 1.4 Роли управления

Роли определяют полномочия пользователей при работе с eCA-RA.

Пользователями eCA-RA являются:

- Пользователи, учётные записи и сертификаты которых были созданы в eCA-CA, подключённом к eCA-RA.
- Пользователи, учётные записи которых созданы в доменной службе каталогов, подключённой к eCA-RA и eCA-CA.

В eCA-RA определены следующие роли:

- Администратор.  
Пользователь с данной ролью обладает максимальными полномочиям. Пользователь с данной ролью может взаимодействовать с eCA-RA через веб-интерфейс и программный интерфейс API <sup>1</sup>. Идентификация и аутентификация пользователей с данной ролью выполняется по сертификату, выпущенному в eCA-CA.
- Оператор.  
Пользователь с данной ролью может взаимодействовать с eCA-RA через веб-интерфейс и программный интерфейс API <sup>2</sup>. Пользователь с данной ролью имеет может подавать заявки для любых субъектов, просматривать свои заявки, просматривать и обрабатывать заявки для доступных ему субъектов<sup>3</sup>. Идентификация и аутентификация пользователей с данной ролью выполняется по сертификату, выпущенному в eCA-CA.
- Получатель сертификатов.

<sup>1</sup> См. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 6. Описание методов REST API Центра регистрации Aladdin Enterprise Registration Authority».

<sup>2</sup> См. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 6. Описание методов REST API Центра регистрации Aladdin Enterprise Registration Authority».

<sup>3</sup> Доступ пользователя с ролью «Оператор» к субъектам определяется в eCA-CA, к которому подключён eCA-RA.

Пользователь с данной ролью является субъектом ресурсной системы (доменной службы каталогов). Пользователь с данной ролью может взаимодействовать с eCA-RA через веб-интерфейс и программный интерфейс API. Пользователь с данной ролью обладает правами на подачу заявки, просмотр своих заявок, просмотр карточки заявок, отзыв своих сертификатов, получение сертификатов по заявке, скачивания запросов на сертификат. Пользователь с данной ролью создаётся программой автоматически при первой авторизации в eCA-RA. Идентификация и аутентификация пользователя с данной ролью выполняется по имени и паролю доменной учётной записи или Kerberos-билету.

- Аноним (анонимный субъект доступа).

Пользователь с данной ролью может управлять eCA-RA через программный интерфейс по протоколу SCEP, а также путем размещения заявок на выпуск сертификатов в удалённом сетевом каталоге (офлайн выпуск сертификатов). Идентификация пользователей с данной ролью выполняется по атрибуту «ChallengePassword» SCEP-запроса на регистрацию при подключении через программный интерфейс по протоколу SCEP и по атрибуту «Common Name», содержащемуся в запросе на выпуск сертификата, при офлайн выпуске сертификатов. Аноним (анонимный субъект доступа) процедуру аутентификации не проходит. В зависимости от значения параметра `actuator_authenticate` конфигурационного файла Анониму могут быть доступны методы получения информации о сервисах и метод получения версии сервиса внешних интеграций (по умолчанию методы доступны).

Доступные действия для существующих ролей пользователей eCA-RA приведены в таблице 2.

Таблица 2 - Полномочия пользователей eCA-RA

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей			
	Аноним	Получатель сертификата	Оператор	Администратор
Установка или обновление программы	-	-	-	✓
Просмотр информации о конфигурации центра регистрации	-	-	-	✓
Просмотр статистической информации об обработке заявок и выпуске сертификатов	-	-	-	✓
Просмотр информации о своих заявках на выпуск сертификатов	-	✓	✓	✓
Просмотр информации об ограниченном наборе чужих заявок на выпуск сертификатов	-	-	✓	✓
Просмотр информации о всех заявках на выпуск сертификатов	-	-	-	✓
Получение статуса своих заявок по протоколу SCEP	✓	-	-	-
Создание заявок на выпуск сертификатов для субъекта своей учётной записи	-	✓	✓	✓
Создание заявок на выпуск сертификатов для субъекта любой учётной записи	-	-	✓	✓
Создание заявок на выпуск сертификатов по протоколу SCEP (PKCS#7)	✓	-	-	-
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 файла запроса на сертификат для всех заявок на выпуск сертификата по запросу	-	-	-	✓
Скачивание сертификата для своих заявок	-	✓	✓	✓
Скачивание сертификата для своих заявок по протоколу SCEP	✓	-	-	-
Скачивание сертификата для ограниченного набора чужих заявок	-	-	✓	✓

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей			
	Аноним	Получатель сертификата	Оператор	Администратор
Скачивание сертификата для всех заявок	-	-	-	✓
Отзыв сертификатов для своих заявок	-	✓	✓	✓
Отзыв сертификатов для ограниченного набора чужих заявок	-	-	✓	✓
Отзыв сертификатов для всех заявок	-	-	-	✓
Скачивание цепочки сертификатов для своих заявок	-	✓	✓	✓
Скачивание цепочки сертификатов для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание цепочки сертификатов для всех заявок	-	-	-	✓
Скачивание контейнера закрытого ключа PKCS#12 для своих заявок	-	✓	✓	✓
Скачивание контейнера закрытого ключа PKCS#12 для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание контейнера закрытого ключа PKCS#12 для всех заявок	-	-	-	✓
Импорт сертификата на ключевой носитель для своих заявок	-	✓	✓	✓
Импорт сертификата на ключевой носитель для ограниченного набора чужих заявок	-	-	✓	✓
Импорт сертификата на ключевой носитель для всех заявок	-	-	-	✓
Скачивание цепочки сертификатов издателя для своих заявок	-	✓	✓	✓
Скачивание цепочки сертификатов издателя для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание цепочки сертификатов издателя для всех заявок	-	-	-	✓
Скачивание списка отозванных сертификатов	-	✓	✓	✓
Скачивание списка отозванных сертификатов по протоколу SCEP	✓	-	-	-
Отмена своих заявок	-	✓	✓	✓
Обработка ограниченного набора заявок	-	-	✓	✓
Обработка всех заявок	-	-	-	✓
Настройка оффлайн выпуска сертификатов по запросам	-	-	-	✓
Оффлайн выпуск сертификатов по запросам	✓	-	-	✓
Просмотр учётных записей	-	-	-	✓
Управление учётными записями	-	-	-	✓
Создание, изменение, просмотр и удаление правил выпуска сертификатов	-	-	-	✓
Запуск и остановка действия правил выпуска сертификатов	-	-	-	✓
Просмотр ограниченного журнала событий	-	-	✓	✓
Просмотр журнала событий	-	-	-	✓
Архивация журнала событий	-	-	-	✓
Экспорт ограниченного журнала событий	-	-	✓	✓
Экспорт всего журнала событий	-	-	-	✓
Создание, редактирование, просмотр и удаление SCEP-политик	-	-	-	✓

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей			
	Аноним	Получатель сертификата	Оператор	Администратор
Запуск и остановка SCEP-политик	-	-	-	✓
Создание, редактирование, просмотр, копирование URL и удаление SCEP-профилей	-	-	-	✓
Запуск и остановка SCEP-профилей	-	-	-	✓
Скачивание цепочки сертификатов технологического сертификата SCEP-профиля по протоколу SCEP	✓	-	-	-
Добавление, редактирование, просмотр и удаление Syslog-серверов	-	-	-	✓
Смена сертификата веб-сервера	-	-	-	✓
Контроль целостности исполняемых файлов программы	-	-	-	✓

## 1.5 Режимы функционирования программы

Основным режимом функционирования eCA-RA является нормальный режим.

В нормальном режиме должны штатно функционировать программные компоненты eCA-RA, обеспечивая возможность круглосуточного функционирования, с перерывами на обслуживание (обновление программы). То есть должны штатно функционировать Клиентская и Серверная части программы, а также программный компонент «Серверная часть Центр сертификации»<sup>1</sup>, с которым взаимодействует eCA-RA.

Сетевой режим работы обеспечивает возможность кластеризации eCA-RA с целью повышения отказоустойчивости<sup>2</sup>.

<sup>1</sup> Входит в состав программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority».

<sup>2</sup> Порядок развёртывания кластера eCA-RA в приложении 4

## 2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

### 2.1 Требования к программному обеспечению

#### 2.1.1 Требования к среде функционирования Серверной части программы

Среда функционирования Серверной части eCA-RA:

- Поддерживаемые ОС:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Орёл».
  - РЕД ОС версия 7.3, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
  - ОС «Альт Сервер» 11.
  - Platform V SberLinux OS Server.
  - РОСА «ХРОМ» 12 Сервер.
- Поддерживаемые СУБД:
  - PostgreSQL из состава ОС.
  - Postgres Pro.
  - Jatoba.
- Поддерживаемые среды исполнения Java:
  - Java Axiom JDK Certified (компонент JRE).
  - OpenJDK версии 17 и выше из состава поддерживаемых ОС.
- Поддерживаемые веб-серверы:
  - Apache2 из состава ОС.
  - Nginx из расширенного репозитория.
  - Cpnginx <sup>1</sup>.
- Поддерживаемые ресурсные системы (доменные службы каталогов):
  - Samba DC.
  - Dynamic Directory.
  - Free IPA.
  - ALD PRO.
  - РЕД АДМ.
  - Microsoft AD.
  - Альт Домен.
- Поддерживаемый eCA-CA версии 2.4 <sup>2</sup>.

---

<sup>1</sup> Из состава средства криптографической защиты (далее - СКЗИ) «КриптоПро CSP». СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно.

<sup>2</sup> Входит в состав программного средства.

- СКЗИ «КриптоПро CSP»<sup>1</sup> - криптопровайдер, обеспечивающий подпись маркеров доступа пользователей еCA-CA по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит.

## 2.1.2 Требования к среде функционирования Клиентской части программы

Среда функционирования Клиентской части еCA-RA:

- Поддерживаемые ОС:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Орёл».
  - РЕД ОС версия 7.3, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
  - ОС «Альт Сервер» 11.
  - Platform V SberLinux OS Server.
  - РОСА «ХРОМ» 12 Сервер.
- Веб-браузер из состава ОС.
- JC-WebClient последней версии (для 64-битных систем)<sup>2</sup>.
- ПО «Рутокен Плагин» и браузерное расширение «Адаптер Рутокен Плагин»<sup>3</sup>.

## 2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования еCA-RA:

- Накопитель HDD или SSD - не менее 50 Гбайт.
- Оперативная память - не менее 6 Гбайт.
- Процессорные ядра с архитектурой x86, x64 - не менее 4 шт.
- VGA-совместимый видеоадаптер.
- Устройства взаимодействия с пользователем: клавиатура и мышь.
- USB 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей:
  - JaCarta:
    - JaCarta PKI.
    - JaCarta PRO.
    - JaCarta-2 PKI/ГОСТ.
    - JaCarta-2 ГОСТ.
    - JaCarta-3.

<sup>1</sup> СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки еCA и при необходимости приобретается заказчиком самостоятельно. Порядок настройки взаимодействия еCA-RA с СКЗИ «КриптоПро CSP» описан в приложении 7 настоящего руководства.

<sup>2</sup> JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) JaCarta. Официальный сайт производителя [JC-WebClient](http://jc-webclient.ru).

<sup>3</sup> ПО «Рутокен Плагин» через браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) Рутокен. Официальный [сайт производителя](http://ruutoken.ru).

- Рутокен <sup>1</sup>:
  - Рутокен ЭЦП 3.0.
  - Рутокен ЭЦП 2.0.
  - Рутокен ЭЦП 2.0 Flash.
  - Рутокен ЭЦП PKI.

---

<sup>1</sup> Возможность использования ключевых носителей Рутокен может быть ограничена лицензией.



## 3 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

При установке eCA-RA выполняется конфигурирование установленного в среде функционирования веб-сервера, в результате чего для внешнего доступа открывается порт, используемый для подключения по протоколу HTTPS (по умолчанию 443). Изменение порта веб-сервера для подключения к нему по протоколу HTTPS выполняется путём редактирования конфигурационного файла eCA-RA (см. раздел 4.2).

В таблице 3 приведён список портов, которые должны быть открыты в eCA-RA и взаимодействующих компонентах.

Таблица 3 - Таблица сетевого взаимодействия

Порт	Транспорт	Протокол	Назначение	Возможность изменения
443	TCP	TLS/HTTPS	Порт для подключения к веб-интерфейсу eCA-RA, а также для взаимодействия с eCA-CA.	Да
			Порт используется для подключения SCEP-клиентов (при соответствующих настройках конфигурационного файла), а также для обращения к CEP- и CES-серверам по протоколам MS-XCEP и MS-WSTEP.	
80	TCP	HTTP	Порт для подключения SCEP-клиентов (по умолчанию). Если в конфигурационном файле отключена передача данных по протоколу HTTP, с данного порта выполняется переадресация пакетов на порт 443.	Да
389	TCP	LDAP	Порт для взаимодействия с доменной службой каталогов (ресурсной системой) по протоколу LDAP.	Нет
88, 464	TCP	Kerberos	Порты для взаимодействия со службой аутентификации Kerberos ресурсной системы.	Нет
5432	TCP	TCP	Порт для подключения к СУБД.	Да
	TCP	TLS		
514	UDP	Syslog	Порт для отправки сообщений на Syslog-серверы (порт 514, как правило, используется по умолчанию).	Да
	TCP			

В таблице 4 приведен список портов, которые используются в eCA-RA. Доступ к данным портам для внешних подключений ограничивается автоматически при установке eCA-RA с помощью утилиты **iptables** из состава ОС.

**Внимание!** Во избежание возникновения ошибок в работе eCA-RA переназначение данных портов запрещено.

Таблица 4 — Таблица входящих внутренних сетевых портов

Порт	Транспорт	Протокол	Назначение
1051	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «api-gateway-service» (сервис проксирования)
1101	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «sa-adapter-service» (адаптер для подключения к программе)
1151	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «discovery-service» (сервис обнаружения)
1201	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «export-service» (сервис экспорта)
1251	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «external-integration-service» (сервис публичного API)
1301	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (сервис журнализации)

Порт	Транспорт	Протокол	Назначение
1351	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «middleware-service» (связующий сервис для взаимодействия с внутренним контуром программы)
1401	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «policies-service» (сервис правил выпуска)
1451	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «scep-enrollment-service» (сервис SCEP)
1501	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «security-service» (сервис безопасности)
1551	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «settings-service» (сервис настройки)
1601	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «storage-service» (сервис хранения файлов)
1651	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «tasks-service» (сервис заявок)
1701	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «wstep-enrollment-service» (сервис WSTEP)

Подготовка среды функционирования для eCA-RA заключается в установке и настройке следующего ПО:

- Зависимостей и подключение репозитория ОС.
- Среды исполнения Java.
- СУБД.
- Веб-сервера.
- JC-WebClient (при необходимости работы с электронными ключами JaCarta).
- ПО «Рутокен Плагин» и браузерное расширение «Адаптер Рутокен Плагин» (при необходимости работы с электронными ключами Рутокен).

Предварительно необходимо выполнить следующие действия:

- Ввести компьютер, на котором будет выполнена установка eCA-RA, в домен ресурсной системы (доменной службы каталогов).
- Создать службу HTTP и keytab-файл <sup>1</sup> на контроллере домена ресурсной системы (см. раздел 3.5).
- Создать в eCA-CA технологическую учетную запись с правами «Администратор» для взаимодействия eCA-RA с eCA-CA, выпустить для нее сертификат по шаблону «User» и выгрузить контейнер PKCS#12 <sup>2</sup>.
- Создать в eCA-CA субъект для веб-сервера eCA-RA, выпустить для него сертификат по шаблону «WEB-Server» и выгрузить контейнер PKCS#12.
- Перенести подготовленные контейнеры PKCS#12 на компьютер, где будет выполнено развертывание eCA-RA.

<sup>1</sup> Keytab-файл используется для аутентификации доменных пользователей в eCA-RA с использованием Kerberos-билетов без ввода пароля.

<sup>2</sup> Порядок создания субъектов, учетных записей и выпуска сертификатов приведен в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA eCA-RA может взаимодействовать с криптопровайдером СКЗИ «КриптоПро CSP». При этом в eCA-RA необходимо применять СКЗИ «КриптоПро CSP» для:

- Организации канала взаимодействия Серверных частей eCA-CA и eCA-RA по протоколу TLS ГОСТ.
- Организации канала взаимодействия Клиентской и Серверной части eCA-RA по протоколу TLS ГОСТ.
- Обеспечения TLS-аутентификации пользователей eCA-CA в eCA-RA с использованием отечественных криптографических алгоритмов.
- Подписи маркеров доступа пользователей eCA-CA по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит.

Порядок установки и настройки СКЗИ «КриптоПро CSP» представлен в приложении 7. Установка и настройка СКЗИ «КриптоПро CSP» могут быть выполнены после установки eCA-RA в процессе его эксплуатации.

При применении СКЗИ «КриптоПро CSP»:

- В качестве веб-сервера должен использоваться веб-сервер «Cpengine» из состава СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP». Порядок установки веб-сервера «cprengine» приведен в разделе 3.6. После установки веб-сервера необходимо установить на СКЗИ «КриптоПро CSP» серверную лицензию, обеспечивающую возможность использования СКЗИ «КриптоПро CSP» в качестве TLS-сервера.
- Сертификаты для веб-сервера и учётной записи с ролью «Администратор» для взаимодействия с eCA-CA должны быть выпущены по алгоритму ГОСТ Р 34.11-2012/ 34.10-2012 256/512 Бит.

## 3.1 Подготовка среды функционирования с РЕД ОС и РОСА «ХРОМ» 12 Сервер

### 3.1.1 Подключение репозитория и установка зависимостей

Для РЕД ОС и РОСА «ХРОМ» 12 Сервер репозитории настроены по умолчанию для скачивания из сети Интернет. Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС выполнив следующую команду с правами суперпользователя:

```
dnf install tar unzip iptables
```

Если доступ к сети Интернет отсутствует, то зависимости возможно установить с USB-носителя из комплекта поставки ОС выполнив следующие действия:

- Перейдите в корневой каталог USB-носителя.
- Выполните следующую команду с правами суперпользователя:

```
dnf install tar
```

### 3.1.2 Установка среды исполнения Java

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified.

#### 3.1.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

#### 3.1.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией по установке пакета с официального сайта РЕД ОС:

- [Инструкция для РЕД ОС 7.3.](#)
- [Инструкция для РЕД ОС 8.](#)

### 3.1.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL из состава ОС.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в приложении 1.

Порядок настройки взаимодействия с СУБД, размещенной на отдельном узле, приведен в приложении 2.

еСА-РА может быть настроен на взаимодействие с СУБД по протоколу TLS. Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведен в приложении 3.

#### 3.1.3.1 Установка СУБД PostgreSQL<sup>1</sup>

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL выполнив команду с правами суперпользователя:

```
dnf install postgresql-server
```

- Выполните установку последней доступной версии пакета `postgresql-contrib` выполнив команду с правами суперпользователя:

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

```
postgresql-setup --initdb
```

В случае возникновения ошибки `Data directory in '/var/lib/pgsql/data' is not empty...` очистите каталог командой ниже с правами суперпользователя и повторить инициализацию СУБД.

```
rm -rf /var/lib/pgsql/data
```

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`<sup>2</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>3</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgsql/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

<code>host all all 127.0.0.1/32 ident</code>	заменить на	<code>host all all 127.0.0.1/32 scram-sha-256</code>
<code>host all all ::1/128 ident</code>	заменить на	<code>host all all ::1/128 scram-sha-256</code>

<sup>1</sup> Подробное описание приведено на [официальном сайте производителя](#).

<sup>2</sup> Расположение файла может отличаться. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>3</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgresql
```

### 3.1.3.2 Установка СУБД Postgres Pro <sup>1</sup>

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду <sup>2</sup>:

```
wget --user [ключ] --password=' ' https://repo.postgrespro.ru/std/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

```
sh pgpro-repo-add.sh
```

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

```
dnf install postgrespro-std-16
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`<sup>3</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>4</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgpro/std-16/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident заменить на host all all ::1/128 scram-sha-256
```

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump` выполнив следующие команды с правами суперпользователя:

```
ln -s /opt/pgpro/std-16/bin/psql /usr/bin/psql
ln -s /opt/pgpro/std-16/bin/pg_dump /usr/bin/pg_dump
```

- Перезапустите СУБД Postgres Pro выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgrespro-std-16.service
```

### 3.1.3.3 Установка СУБД Jatoba <sup>5</sup>

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo` выполнив следующую команду с правами суперпользователя:

```
mkdir /localrepo
```

- Скопируйте в каталог `/localrepo` необходимые файлы для установки СУБД.

**Внимание!** Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с оптического диска напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога `/localrepo` во всех шагах далее

<sup>1</sup> Подробное описание приведено на [официальном сайте производителя](#).

<sup>2</sup> Команды ниже приведены для СУБД Postgres Pro версии 16.

<sup>3</sup> Расположение файла указано для СУБД Postgres Pro версии 16. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>4</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

<sup>5</sup> Подробное описание приведено на [официальном сайте производителя](#).

**указывать соответствующий путь до носителя и директорию репозитория СУБД на носителе для соответствующей ОС.**

- Дистрибутив СУБД содержит:
  - Каталог `/packages`.
  - Каталог `/repodata`.
  - Файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива СУБД. Для этого перейдите в каталог `/localrepo` и выполните следующую команду:

```
ls -l
```

- Установите открытый ключ репозитория выполнив следующую команду с правами суперпользователя:

```
rpm --import /localrepo/RPM-GPG-KEY-Jatoba
```

- Создайте файл `/etc/yum.repos.d/jatoba-[версия].repo` с описанием локального репозитория в системе, в котором разместите следующее описание:

```
[jatoba-[версия]]
name=Jatoba [версия] Official Repository
baseurl=file:///localrepo
enabled=1
gpgcheck=1
gpgkey=file:///localrepo/RPM-GPG-KEY-Jatoba
```

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

- Установите основные пакеты СУБД выполнив следующую команду с правами суперпользователя:

```
dnf install jatoba[версия]-client jatoba[версия]-contrib jatoba[версия]-libs
jatoba[версия]-server
```

**Внимание!** Пакеты `jatoba[версия]-client`, `jatoba[версия]-contrib`, `jatoba[версия]-libs` и `jatoba[версия]-server` являются обязательными для установки СУБД.

- Перейдите в каталог расположения исполняемых файлов СУБД выполнив следующую команду:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД выполнив следующую команду с правами суперпользователя:

```
./jatoba-setup initdb jatoba-[версия]
```

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>1</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/jatoba/[версия]/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например, `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке DATABASE указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

<sup>1</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable jatoba-[версия]
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart jatoba-[версия]
```

### 3.1.4 Установка веб-сервера

**Внимание!** РЕД ОС и РОСА «ХРОМ» 12 Сервер поддерживают веб-сервера Nginx и Apache, которые обеспечивают сертифицированную среду функционирования. Веб-серверы устанавливаются из основного репозитория ОС.

#### 3.1.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache для РЕД ОС:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install httpd
```

- Установите дополнительный модуль для использования протокола SSL выполнив следующую команду с правами суперпользователя:

```
dnf install mod_ssl
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable httpd
```

Порядок установки веб-сервера Apache для ОС РОСА «ХРОМ» 12 Сервер:

- Установите модуль поддержки шифрования при помощи команды с правами суперпользователя:

```
dnf install apache-mod_ssl
```

- Установите модуль прокси-сервера при помощи команды с правами суперпользователя:

```
urpmi apache-mod_proxy
```

- Установите модуль поддержку разделяемой памяти (shared memory) на основе слотов при помощи команды с правами суперпользователя:

```
dnf install apache-mod_slotmem_shm
```

#### 3.1.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

- Запустите установленный веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable nginx
```



## 3.2 Подготовка среды функционирования с ОС Astra Linux Special Edition 1.8

### 3.2.1 Подключение репозитория и установка зависимостей

#### 3.2.1.1 Подключение репозитория и установка зависимостей Astra Linux Special Edition 1.8<sup>1</sup>

Порядок подключения репозитория и зависимостей:

- Для обновления посредством сети Интернет перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториях<sup>2</sup>, отредактировав файл `/etc/apt/sources.list` выполнив следующую команду с правами суперпользователя:

```
nano /etc/apt/sources.list
```

- Укажите ссылки на следующие репозитории<sup>3</sup>:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.5/repository-main/  
1.8_x86-64 main contrib non-free
```

- Укажите нижеприведённый репозиторий, если в качестве веб-сервера будет использоваться Nginx:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.5/repository-extended/  
1.8_x86-64 main contrib non-free
```

Для установки необходимых компонентов в офлайн режиме предварительно необходимо настроить использование установочных дисков в качестве репозитория, отредактировав файл `/etc/apt/sources.list`.

Пример:

```
deb cdrom:[OS Astra Linux 1.8.5 1.8_x86-64 DVD ]/ 1.7_x86-64 contrib main non-free
```

- Зарегистрируйте физический оптический диск, установленный в оптический привод, выполнив команду:

```
apt-cdrom add
```

- Выполните обновление пакетов для операционной системы из указанных репозиториях выполнив следующую команду с правами суперпользователя:

```
apt update
```

- Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС выполнив следующую команду с правами суперпользователя:

```
apt install tar unzip iptables
```

В процессе установки в офлайн режиме может потребоваться заменить и вставить диск с нужным репозиторием («диск 1», «диск 2», «develop»).

#### 3.2.1.2 Поддержка активного режима замкнутой программной среды

еCA-RA обеспечивает работу ОС Astra Linux Special Edition 1.8 в активном режиме замкнутой программной среды (далее — ЗПС). Для этого в состав установочных пакетов еCA-RA включён публичный открытый ключ ОсОО «Аладдин КГ» — `aladdin_pub.key`. После распаковки установочного пакета ключ находится в каталоге `/opt/aecaRa/digisig/keys/aladdin_pub.key`.

Для обеспечения режима ЗПС открытый ключ необходимо скопировать в каталог `/etc/digisig/keys/`.

<sup>1</sup> Подробнее см. на официальном сайте производителя.

<sup>2</sup> Ссылки на репозитории приведены для Astra Linux SE 1.8.5

<sup>3</sup> При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозиториях в соответствии с [инструкцией по подготовке и присоединению хоста к домену ALD Pro](#).



## 3.2.2 Установка среды исполнения Java

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified.

### 3.2.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

### 3.2.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта Astra Linux (в инструкции описана установка Open JDK 17, установка Open JDK 21 аналогична).

## 3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

Порядок настройки взаимодействия с СУБД, размещённой на отдельном узле, приведён в приложении 2.

eCA-RA может быть настроен на взаимодействие с СУБД по протоколу TLS. Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведён в приложении 3.

### 3.2.3.1 Установка СУБД PostgreSQL<sup>1</sup>

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД выполнив следующую команду с правами суперпользователя:

```
apt install postgresql
```

- Выполните установку последней доступной версии пакета `postgresql-contrib`<sup>2</sup> выполнив следующую команду с правами суперпользователя:

```
apt install postgresql-contrib
```

- Установите пакет `postgresql-client` выполнив следующую команду с правами суперпользователя:

```
apt install postgresql-client
```

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable postgresql
```

- Отредактируйте файл `/etc/postgresql/15/main/postgresql.conf`<sup>3</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>4</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/etc/postgresql/15/main/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке DATABASE» указано значение `replication`.

<sup>1</sup> Подробное описание приведено на официальном сайте производителя.

<sup>2</sup> Для некоторых минорных версий ОС данный пакет может отсутствовать.

<sup>3</sup> Расположение файла может отличаться. Расположение файла указано для СУБД PostgreSQL версии 11. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>4</sup> Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

Примеры изменений:

```
host all all 127.0.0.1/32 ident заменить на host all all 127.0.0.1/32 scram-sha-256
host all all ::1/128 ident заменить на host all all ::1/128 scram-sha-256
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgresql
```

### 3.2.3.2 Установка СУБД Postgres Pro <sup>1</sup>

Порядок установки СУБД PostgreSQL Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду <sup>2</sup>:

```
wget --user [ключ] --password='' https://repo.postgrespro.ru/std/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

```
sh pgpro-repo-add.sh
```

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

```
apt install postgrespro-std-16
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`<sup>3</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>4</sup>.

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump` выполнив следующие команды с правами суперпользователя:

```
ln -s /opt/pgpro/std-16/bin/psql /usr/bin/psql
ln -s /opt/pgpro/std-16/bin/pg_dump /usr/bin/pg_dump
```

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgpro/std-16/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident заменить на host all all 127.0.0.1/32 scram-sha-256
host all all ::1/128 ident заменить на host all all ::1/128 scram-sha-256
```

- Перезапустите СУБД выполнив команду с правами суперпользователя:

```
systemctl restart postgrespro-std-16.service
```

### 3.2.3.3 Установка СУБД Jatoba <sup>5</sup>

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo` выполнив команду:

```
mkdir /localrepo
```

<sup>1</sup> Подробное описание приведено на официальном сайте производителя.

<sup>2</sup> Команды ниже приведены для СУБД Postgres Pro версии 16.

<sup>3</sup> Расположение файла указано для СУБД Postgres Pro версии 16. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>4</sup> Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

<sup>5</sup> Подробное описание приведено на официальном сайте производителя.

- В каталог `/localrepo` скопируйте необходимые файлы для установки СУБД Jatoba.

**Внимание!** Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с оптического диска напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога `/localrepo` во всех шагах далее указывать соответствующий путь до носителя и директорию репозитория СУБД на носителе для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
  - Каталог `/pool`.
  - Каталог `/dists`.
  - Файл ключа `DEB-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива СУБД. Для этого перейдите в каталог `/localrepo` и выполните следующую команду:

```
ls -l
```

- Установите открытый ключ репозитория выполнив следующую команду с правами суперпользователя:

```
apt-key add /localrepo/DEB-GPG-KEY-Jatoba
```

- Создайте файл `/etc/apt/sources.list.d/jatoba-[версия].list` с описанием локального репозитория в системе, в котором разместите следующее описание:

```
deb file:///localrepo stable non-free
```

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

- Установите основные пакеты СУБД выполнив следующую команду с правами суперпользователя:

```
apt install jatoba[версия]-client jatoba[версия]-contrib jatoba[версия]-libs  
jatoba[версия]-server
```

**Внимание!** Пакеты `jatoba[версия]-client`, `jatoba[версия]-contrib`, `jatoba[версия]-libs` и `jatoba[версия]-server` являются обязательными для установки СУБД.

- Перейдите в каталог расположения исполняемых файлов СУБД выполнив следующую команду:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД выполнив следующую команду с правами суперпользователя:

```
./jatoba-setup initdb jatoba-[версия]
```

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>1</sup>.

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable jatoba-[версия]
```

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/jatoba/[версия]/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident заменить на host all all 127.0.0.1/32 scram-sha-256
```

<sup>1</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

```
host all all ::1/128 ident
```

заменить на `host all all ::1/128 scram-sha-256`

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart jatoba-[версия]
```

В случае возникновения ошибки запуска следует проанализировать внутренние системные журналы СУБД:

```
ls /var/lib/jatoba/[версия]/data/log
```

```
cat /var/lib/jatoba/[версия]/data/log/[weekDay]
```

### 3.2.4 Установка веб-сервера

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить веб-сервер Apache из основного репозитория сертифицированной ОС.

#### 3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
apt install apache2
```

- Активируйте модули выполнив следующую команду с правами суперпользователя:

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

- Перезапустите веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl restart apache2.service
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable apache2
```

- Для проверки корректности запуска модулей выполните следующую команду с правами суперпользователя:

```
apachectl -M | grep -E 'ssl|proxy|proxy_http|headers|cgi|rewrite|http2'
```

#### 3.2.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет из расширенного репозитория ОС выполнив следующую команду с правами суперпользователя:

```
apt install nginx
```

- Запустите установленный веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable nginx
```

## 3.3 Подготовка среды функционирования с ОС Альт 8 СП релиз 10 вариант исполнения Сервер и ОС «Альт Сервер» 11

### 3.3.1 Подключение репозитория и установка зависимостей ОС Альт 8 СП релиз 10 вариант исполнения Сервер

Для развёртывания eCA-RA с использованием веб-сервера Apache перед началом установки необходимо установить путь нахождения необходимого репозитория:

- Отредактируйте файл `/etc/apt/sources.list` выполнив следующую команду с правами суперпользователя:

```
nano /etc/apt/sources.list.d/aptpsp.list
```

- Укажите в файле ссылку на следующий репозиторий:

```
rpm [cert8] http://update.altsp.su/pub/distributions/ALTLinux c10f/branch/x86_64-i586 classic
```

- После этого обновите список доступных пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

### 3.3.2 Установка среды исполнения Java

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified.

#### 3.3.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

#### 3.3.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС.

### 3.3.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

Порядок настройки взаимодействия с СУБД, размещённой на отдельном узле, приведён в приложении 2.

eCA-RA может быть настроен на взаимодействие с СУБД по протоколу TLS. Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведён в приложении 3.

#### 3.3.3.1 Установка СУБД PostgreSQL <sup>1</sup>

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL выполнив команду с правами суперпользователя:

```
apt-get install postgresql-server
```

- Выполните установку последней доступной версии пакета `postgresql-contrib` выполнив команду с правами суперпользователя:

```
dnf install postgresql-contrib
```

<sup>1</sup> Подробное описание приведено на официальном сайте производителя.

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

```
postgresql-setup --initdb
```

В случае возникновения ошибки `Data directory in '/var/lib/pgsql/data' is not empty...` очистите каталог командой с правами суперпользователя ниже и повторите инициализацию СУБД.

```
rm -rf /var/lib/pgsql/data
```

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`<sup>1</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>2</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgsql/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgresql
```

### 3.3.3.2 Установка СУБД Postgres Pro <sup>3</sup>

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду <sup>4</sup>:

```
wget --user [ключ] --password='' https://repo.postgrespro.ru/std/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

```
sh pgpro-repo-add.sh
```

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

```
dnf install postgrespro-std-16
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`<sup>5</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>6</sup>.

<sup>1</sup> Расположение файла может отличаться, для поиска используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>2</sup> Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

<sup>3</sup> Подробное описание приведено на официальном сайте производителя.

<sup>4</sup> Команды ниже приведены для СУБД Postgres Pro версии 16.

<sup>5</sup> Расположение файла указано для СУБД Postgres Pro версии 16. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>6</sup> Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump` выполнив команды с правами суперпользователя:

```
ln -s /opt/pgpro/std-16/bin/psql /usr/bin/psql
ln -s /opt/pgpro/std-16/bin/pg_dump /usr/bin/pg_dump
```

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgpro/std-16/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

- Перезапустите СУБД `Postgres Pro` выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgrespro-std-16.service
```

### 3.3.3.3 Установка СУБД `Jatoba` <sup>1</sup>

Порядок установки СУБД `Jatoba`:

- Создайте каталог `/localrepo` выполнив следующую команду с правами суперпользователя:

```
mkdir /localrepo
```

- Скопируйте в каталог `/localrepo` необходимые файлы для установки СУБД.

**Внимание!** Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с оптического диска напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога `/localrepo` во всех шагах далее указывать соответствующий путь до носителя и директорию репозитория СУБД на носителе для соответствующей ОС.

- Дистрибутив СУБД содержит:

- Каталог `/packages`.
- Каталог `/repodata`.
- Файл ключа `RPM-GPG-KEY-Jatoba`.

- Проверьте результат копирования всех файлов дистрибутива СУБД. Для этого перейдите в каталог `/localrepo` и выполните следующую команду:

```
ls -l
```

- Создайте файл `/etc/apt/sources.list.d/jatoba-[версия].list` под администратором с описанием локального репозитория в системе, в котором разместите следующее описание:

```
rpm file:///localrepo x86_64 classic
```

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

- Установите основные пакеты СУБД выполнив следующую команду с правами суперпользователя:

```
apt-get install jatoba[версия]-client jatoba[версия]-contrib jatoba[версия]-libs
jatoba[версия]-server
```

<sup>1</sup> Подробное описание приведено в [официальной документации на Jatoba](#).

**Внимание!** Пакеты `jatoba[версия]-client`, `jatoba[версия]-contrib`, `jatoba[версия]-libs` и `jatoba[версия]-server` являются обязательными для установки СУБД.

- Перейдите в каталог расположения исполняемых файлов СУБД выполнив следующую команду:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД выполнив следующую команду с правами суперпользователя:

```
./jatoba-setup initdb jatoba-[версия]
```

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>1</sup>.
- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable jatoba-[версия]
```

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/jatoba/[версия]/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart jatoba-[версия]
```

### 3.3.4 Установка веб-сервера

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить веб-сервер Nginx из основного репозитория сертифицированной ОС.

#### 3.3.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

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

- Установите модуль ssl выполнив следующую команду с правами суперпользователя:

```
apt-get install apache2-mod_ssl
```

- Создайте следующие файлы:

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

```
nano /etc/httpd2/conf/mods-available/http2.load
```

Внесите следующий текст в созданный файл:

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

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

```
nano /etc/httpd2/conf/mods-available/http2.conf
```

Внесите следующий текст в созданный файл:

```
# mod_http2 doesn't work with mpm_prefork
```

<sup>1</sup> Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.



```
<IfModule !mpm_prefork>
    Protocols h2 h2c http/1.1
</IfModule>
```

- Активируйте модули выполнив поочерёдно следующие команды с правами суперпользователя:

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

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

```
a2enport https
```

### 3.3.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
apt-get install nginx
```

- Запустите установленный веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable nginx
```

## 3.4 Подготовка среды функционирования с ОС «Platform V SberLinux OS Server»

### 3.4.1 Установка среды исполнения Java

**Внимание!** Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified.

#### 3.4.1.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

#### 3.4.1.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией по установке пакета с официального сайта Platform V SberLinux OS Server.

### 3.4.2 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL из состава ОС.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

Порядок настройки взаимодействия с СУБД, размещённой на отдельном узле, приведён в приложении 2.

еCA-RA может быть настроен на взаимодействие с СУБД по протоколу TLS. Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведён в приложении 3.

### 3.4.2.1 Установка СУБД PostgreSQL<sup>1</sup>

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL выполнив команду с правами суперпользователя:

```
dnf install postgresql-server
```

- Выполните установку последней доступной версии пакета `postgresql-contrib` выполнив команду с правами суперпользователя:

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

```
postgresql-setup --initdb
```

В случае возникновения ошибки `Data directory in '/var/lib/pgsql/data' is not empty...` очистите каталог командой с правами суперпользователя ниже и повторить инициализацию СУБД.

```
rm -rf /var/lib/pgsql/data
```

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`<sup>2</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>3</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgsql/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgresql
```

### 3.4.2.2 Установка СУБД Postgres Pro<sup>4</sup>

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду<sup>5</sup>:

```
wget --user [ключ] --password='' https://repo.postgrespro.ru/std/std-16/keys/pgpro-repo-add.sh
```

<sup>1</sup> Подробное описание приведено на официальном сайте производителя.

<sup>2</sup> Расположение файла может отличаться. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>3</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

<sup>4</sup> Подробное описание приведено на официальном сайте производителя.

<sup>5</sup> Команды ниже приведены для СУБД Postgres Pro версии 16.

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

```
sh pgpro-repo-add.sh
```

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

```
dnf install postgrespro-std-16
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`<sup>1</sup> с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>2</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgpro/std-16/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке DATABASE указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident заменить на host all all ::1/128 scram-sha-256
```

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump` выполнив следующие команды с правами суперпользователя:

```
ln -s /opt/pgpro/std-16/bin/psql /usr/bin/psql
ln -s /opt/pgpro/std-16/bin/pg_dump /usr/bin/pg_dump
```

- Перезапустите СУБД Postgres Pro выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgrespro-std-16.service
```

### 3.4.2.3 Установка СУБД Jatoba<sup>3</sup>

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo` выполнив следующую команду с правами суперпользователя:

```
mkdir /localrepo
```

- Скопируйте в каталог `/localrepo` необходимые файлы для установки СУБД.

**Внимание!** Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с оптического диска напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога `/localrepo` во всех шагах далее указывать соответствующий путь до носителя и директорию репозитория СУБД на носителе для соответствующей ОС.

- Дистрибутив СУБД содержит:

- Каталог `/packages`.
- Каталог `/repodata`.
- Файл ключа `RPM-GPG-KEY-Jatoba`.

- Проверьте результат копирования всех файлов дистрибутива СУБД. Для этого перейдите в каталог `/localrepo` и выполните следующую команду:

```
ls -l
```

<sup>1</sup> Расположение файла указано для СУБД Postgres Pro версии 16. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

<sup>2</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

<sup>3</sup> Подробное описание приведено на [официальном сайте производителя](#).

- Установите открытый ключ репозитория выполнив следующую команду с правами суперпользователя:

```
rpm --import /localrepo/RPM-GPG-KEY-Jatoba
```

- Создайте файл `/etc/yum.repos.d/jatoba-[версия].repo` с описанием локального репозитория в системе, в котором разместите следующее описание:

```
[jatoba-[версия]]
name=Jatoba [версия] Official Repository
baseurl=file:///localrepo
enabled=1
gpgcheck=1
gpgkey=file:///localrepo/RPM-GPG-KEY-Jatoba
```

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

- Установите основные пакеты СУБД выполнив следующую команду с правами суперпользователя:

```
dnf install jatoba[версия]-client jatoba[версия]-contrib jatoba[версия]-libs
jatoba[версия]-server
```

**Внимание!** Пакеты `jatoba[версия]-client`, `jatoba[версия]-contrib`, `jatoba[версия]-libs` и `jatoba[версия]-server` являются обязательными для установки СУБД.

- Перейдите в каталог расположения исполняемых файлов СУБД выполнив следующую команду:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД выполнив следующую команду с правами суперпользователя:

```
./jatoba-setup initdb jatoba-[версия]
```

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`<sup>1</sup>.

- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/jatoba/[версия]/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

```
host all all 127.0.0.1/32 ident    заменить на host all all 127.0.0.1/32 scram-sha-256
```

```
host all all ::1/128 ident       заменить на host all all ::1/128 scram-sha-256
```

- Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable jatoba-[версия]
```

- Выполните перезапуск СУБД для вступления изменений в силу выполнив следующую команду с правами суперпользователя:

```
systemctl restart jatoba-[версия]
```

### 3.4.3 Установка веб-сервера

**Внимание!** ОС «Platform V SberLinux OS Server» поддерживает веб-сервера Nginx и Apache, которые обеспечивают сертифицированную среду функционирования. Оба веб-сервера устанавливаются из основного репозитория сертифицированной ОС.

<sup>1</sup> Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

### 3.4.3.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install httpd
```

- Установите дополнительный модуль для использования протокола SSL выполнив следующую команду с правами суперпользователя:

```
dnf install mod_ssl
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable httpd
```

### 3.4.3.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

- Запустите установленный веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable nginx
```

## 3.5 Создание службы HTTP и keytab-файла

Создание службы HTTP и keytab-файла для eCA-RA выполняется аналогично созданию службы HTTP и keytab-файла для eCA-CA.

## 3.6 Установка веб-сервера Cpnginx

Пакеты веб-сервера `cpnginx` расположены в дистрибутиве СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP» (см. приложение 7).

Порядок установки веб-сервера `cpnginx`:

- Распакуйте архив с дистрибутивом СКЗИ «КриптоПро CSP» выполнив команду с правами суперпользователя:

```
tar -zxvf <имя_дистрибутива>.tgz && cd <имя_дистрибутива>
```

- Установите следующие пакеты:

- для ОС Astra Linux SE выполнив следующую команду с правами суперпользователя:

```
dpkg -i <наименование пакета>.deb;
```

- o `cprocsp-nginx-64_5.0.13000-7_amd64.deb`;
- o `lsb-cprocsp-rcrypt-64_5.0.13300-7_amd64.deb`;
- o `cprocsp-pki-plugin-64_2.0.15000-1_amd64.deb`.

- для ОС РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server выполнив следующую команду с правами суперпользователя:

```
dnf install <наименование пакета>.rpm:
```

- o `cprocsp-nginx-64-5.0.13000-7.x86_64.rpm`;
- o `lsb-cprocsp-rcrypt-64-5.0.13000-7.x86_64.rpm`.

- для ОС Альт Сервер выполнив следующую команду с правами суперпользователя:

```
apt-get install <наименование пакета>.rpm:
```

- o cprocsp-nginx-64-5.0.13000-7.x86\_64.rpm;
- o lsb-cprocsp-rcrypt-64-5.0.13000-7.x86\_64.rpm.

- Установите на СКЗИ «КриптоПро CSP» соответствующую лицензию (TLS-сервер) выполнив следующую команду с правами суперпользователя:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -set "Номер лицензии"
```

- Выполните проверку активации лицензии выполнив следующую команду с правами суперпользователя:

```
/opt/cprocsp/sbin/amd64/cpconfig -license -view
```

- Запустите установленный веб-сервер выполнив следующую команду с правами суперпользователя:

```
systemctl start cpnginx.service
```

- Добавьте веб-сервер в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable cpnginx.service
```

### 3.7 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 еCA-RA.

Скачайте дистрибутив JC-WebClient с веб-сайта АО «Аладдин Р.Д» и установите зависимости.

Установите JC-WebClient выполнив следующую команду с правами суперпользователя:

РЕД ОС, РОСА «ХРОМ» 12  
Сервер и SberLinux OS Server

```
dnf install JC-WebClient-x64-x.x.x.xxxx.rpm
```

Astra Linux SE

```
apt install -f JC-WebClient-x64-x.x.x.xxxx.deb
```

Альт Сервер

```
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:

```
sh jcmon start
```

### 3.8 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 еCA-RA.

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.

## 4 УСТАНОВКА ПРОГРАММЫ

**Внимание!** В случае повторной установки ПО рекомендуется произвести очистку кэш используемого веб-браузера.

### 4.1 Распаковка инсталляционного комплекта

Распакуйте инсталляционный пакет, находясь в папке, где он расположен выполнив следующую команду с правами суперпользователя

РЕД ОС, РОСА «ХРОМ» 12  
Сервер и SberLinux OS Server

```
dnf install <наименование пакета>.rpm
```

Astra Linux

```
dpkg -i <наименование пакета>.deb
```

Альт Сервер

```
apt-get install <наименование пакета>.rpm
```

Инсталляционный пакет будет автоматически распакован в директорию `/opt/aecaRa`.

Структура распакованного инсталляционного rpm/deb-пакета приведена в таблице 5.

Таблица 5 — Структура установочного комплекта eCA-RA

Структурный элемент	Назначение элемента
/opt/aecaRa	Установочный комплект eCA-RA, а также используемые дополнительные инструменты
/opt/aecaRa/bin	Каталог с дополнительными утилитами
..bin/jcverify	Каталог утилиты контроля целостности «jcverify»
..bin/jcverify/jcverify	Утилита контроля целостности «jcverify»
..bin/jcverify/jcverify.txt	Вспомогательный файл для работы утилиты целостности «jcverify»
/opt/aecaRa/dist	Путь развертывания продукта; содержит создаваемые временные файлы
..dist/backup/	Созданные резервные копии Центра регистрации
..dist/certificates/aeca-ca	Расположение сертификата для установки соединения с Центром сертификации Aladdin eCA
..dist/certificates/ssl	Расположение сертификатов для управления ssl-соединением
..dist/environment/	Расположение переменных окружения сервисов
..dist/logs/	Расположения технических логов сервисов
/opt/aecaRa/eula	Файл лицензионного соглашения
/opt/aecaRa/samples	Содержит шаблоны файлов конфигурации для внутреннего использования программным средством
/opt/aecaRa/scripts	Содержит скрипты управления программным средством eCA-RA
../scripts/internal	Скрипты для внутреннего использования программы, запускаемые автоматически при выполнении скриптов из каталога /opt/aecaRa/scripts
../scripts/backup.sh	Скрипт резервного копирования конфигурации eCA-RA
../scripts/config.sh	bash-скрипт конфигурации eCA-RA (развёртывание продукта, настройка подключения к БД, управление конфигурацией сервисов)
../scripts/database_create.sh	Скрипт создания базы данных на разворачиваемом сервере Центра регистрации с предустановленными параметрами по умолчанию (именем пользователя, наименованием базы данных и т.д.)
../scripts/diagnostics.sh	Скрипт сбора диагностической информации eCA-RA
../scripts/install.sh	Скрипт установки и обновления текущей версии eCA-RA
../scripts/integrity_check.sh	Скрипт контроля целостности исполняемых файлов eCA-RA

Структурный элемент	Назначение элемента
../scripts/restore.sh	Скрипт восстановления из резервной копии конфигурации eCA-RA
../scripts/jc_checksum	Файл с эталонами контрольных сумм исполняемых файлов eCA-RA
../scripts/uninstall.sh	Скрипт удаления eCA-RA
/opt/aecaRa/services	Сервисы Серверной части Центра регистрации
/opt/aecaRa/static	Артефакты Клиентской части Центра регистрации
/opt/aecaRa/digsig/keys/aladdin_pub.key	Открытый ключ АО «Аладдин Р.Д.», используемый для проверки подписи исполняемых файлов и библиотек eCA-RA на Astra Linux Special Edition в режиме замкнутой программной среды (ЗПС).

Владельцем распакованных файлов будет являться пользователь «root», другие пользователи не будут иметь прав доступа к инсталляционному комплекту.

## 4.2 Настройка конфигурации программы

Конфигурация eCA-RA задаётся с помощью параметров конфигурационного файла `/opt/aecaRa/scripts/config.sh`.

Перед установкой программы определите значения следующих параметров:

- `webserver` — используемый веб-сервер (``nginx``, ``apache`` или ``cprnginx``). Также значение параметра можно будет ввести после запуска инсталлятора установки, в интерактивном режиме выбрав веб-сервер.
- `webserver_path` — папка с файлами для развёртывания веб-сервера. Также значение параметра можно будет ввести при запуске инсталлятора, в интерактивном режиме указав путь к файлам веб-сервера:
  - конфигурация Nginx располагается по пути `/etc/nginx`;
  - конфигурация Apache располагается для Astra Linux SE по пути `/etc/apache2`, для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server — по пути `/etc/httpd`, для Альт Сервер по пути `/etc/httpd2`;
  - конфигурация Cprnginx располагается по пути `/etc/opt/cprosp/cprnginx`.
- `aeca_ca_host` — адрес (IP-адрес или доменное имя) eCA-CA, к которому будет подключён eCA-RA (пример, `172.22.5.21`).
- `kerberos_service_principal` — принципал HTTP-службы, используемой для валидации Kerberos-билетов в формате `HTTP/<доменное имя стенда>.<домен>` (например, `HTTP/ra01.presale.aeca`).
- `kerberos_krb5_location` — расположение `krb5.conf` файла (по умолчанию располагается по пути `/etc/krb5.conf`, не рекомендуется изменять без веской причины).
- `kerberos_ad_domain` — имя домена службы каталог в верхнем регистре (например, `PRESALE.AECA`).
- `kerberos_ad_server` — LDAP-адрес для подключения к домену в формате `ldap://<имя контроллера домена>.<домен>` (например, `ldap://dc1.presale.aeca`).<sup>1</sup>
- `resource_type` — тип подключаемой ресурсной системы (доступные значения: `FREE_IPA`, `ALD_PRO`, `SAMBA_DC`, `MS_AD`, `RED_ADM`, `ALT_DOMAIN`).
- `resource_base_dn` — точка подключения к ресурсной системе (например, `dc=presale,dc=aeca`).
- `certificate_raw_server_password` — пароль контейнера закрытого ключа веб-сервера.

<sup>1</sup> Вместо LDAP можно использовать LDAPS.



- `use_credentials_from_config` — значение флага использования пароля от контейнера для подключения к еСА-СА, имени и пароля пользователя СУБД из конфигурационного файла. Если установлено true (значение по умолчанию), то укажите значения параметров:<sup>1</sup>
  - `database_password` — пароль создаваемой базы данных (имя базы данных по умолчанию - aecara).
  - `aeca_ca_auth_password` — пароль от контейнера закрытого ключа учётной записи администратора, используемой для взаимодействия еСА-РА с еСА-СА.
- `kerberos_keytab_location` — расположение keytab-файла для принципа HTTP-службы для валидации Kerberos-билетов. Рекомендуется располагать данный файл по пути `/etc/http.keytab`.
- `root_cert_path` — абсолютный путь к сертификату корневого центра сертификации из цепочки сертификатов сервера СУБД. Значение параметра необходимо заполнить только при включённом флаге обязательного использования TLS для подключения к СУБД (при значении параметра `use_tls=true`).
- `hostname` — полное доменное имя компьютера, на котором будет развёрнут еСА-РА.

Для обеспечения корректности встраивания СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программы должен быть организован по протоколу TLS ГОСТ, должна обеспечиваться TLS-аутентификация пользователей в программе с использованием отечественных криптографических алгоритмов, а маркеров доступа пользователей еСА-СА должен быть подписан по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит. Для этого настройте конфигурационный файл в соответствии с таблицей 6.

Таблица 6 - Параметры для настройки TLS ГОСТ

Параметр	Значение
<code>webserver</code>	<code>'cpnginx'</code>
<code>webserver_path</code>	<code>'/etc/opt/cprocp/cpnginx'</code>
<code>sign_provider</code>	<code>'CRYPTO_PRO'</code>
<code>sign_key_algorithm</code>	<code>'GOST_R_34_10_2012'</code>
<code>sign_key_length</code>	<code>'256'</code> или <code>'512'</code>
<code>sign_hash_algorithm</code>	<code>'GOST_R_34_11_2012'</code>

Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh` выполнив следующую команду с правами суперпользователя:

```
nano /opt/aecaRa/scripts/config.sh
```

Настраиваемые параметры конфигурационного файла `/opt/aecaRa/scripts/config.sh` позволяют задавать:

- параметры конфигурации развёртывания сервисов центра регистрации;
- параметры конфигурации подключения к центру сертификации;
- параметры конфигурации подключаемой ресурсной системы;
- параметры конфигурации офлайн-выпуска сертификатов;
- параметры сертификата веб-сервера центра регистрации;
- расписание синхронизации разрешённых издателей;
- расписание архивации журнала событий;

<sup>1</sup> Если параметр `use_credentials_from_config` имеет значение `true`, то после установки или обновления еСА-РА параметры `database_password` и `aeca_ca_auth_password` отображаются в конфигурационном файле в зашифрованном виде (алгоритм шифрования AES-256 с использованием хранимого в файле `/opt/aecaRa/scripts/key` ключа шифрования).

- конфигурацию базы данных;
- конфигурация памяти.

Полный перечень и описание параметров конфигурации приведено в таблице 7.

Таблица 7 — Описание параметров конфигурации

Ключ	Значение по умолчанию	Описание
Конфигурация развёртывания		
webserver	'#CHANGEIT'	Используемый web-сервер Допустимые значения: "apache", "nginx", "cprnginx". '#CHANGEIT' означает, что параметр не задан. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
webserver_path	'#CHANGEIT'	Расположение конфигурации веб-сервера (папка с файлами для развёртывания сервиса). По умолчанию: конфигурация nginx располагается по пути /etc/nginx, для Astra Linux конфигурация apache располагается по пути /etc/apache2, для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server конфигурация apache располагается по пути /etc/httpd, конфигурация cprnginx располагается по пути /etc/opt/cproscsp/cprnginx '#CHANGEIT' означает, что параметр не задан. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
aeca_path	'/opt/aecaRa/dist'	Каталог установки eCA-RA. Указано значение по умолчанию.
environment_path	'/opt/aecaRa/dist/environmen t'	Конфигурация развёртывания. Указано значение по умолчанию.
webserver_config_path	'/opt/aecaRa/dist/webserver'	Расположение конфигурации eCA-RA для веб-сервера. Указано значение по умолчанию.
encryption_key_path	'/opt/aecaRa/scripts/key'	Ключ для шифрования конфигурационного файла
proxy_connect_timeout	'320'	Время ожидания подключения к прокси-серверу перед тем, как будет выдано сообщение об ошибке  Только для nginx. Настраивается разработчиком, редактировать не следует
proxy_send_timeout	'320'	Время ожидания ответа от прокси-сервера после отправки запроса. Если ответ не получен в течение этого времени, запрос считается неудачным.  Только для nginx. Настраивается разработчиком, редактировать не следует

Ключ	Значение по умолчанию	Описание
proxy_read_timeout	'720'	<p>Время ожидания чтения ответа от прокси-сервера после получения успешного запроса. Если ответ не получен в течение этого времени, запрос считается неудачным.</p> <p>Только для nginx. Настраивается разработчиком, редактировать не следует</p>
ssl_ciphers	"	<p>Поддерживаемые наборы шифров для TLS-соединения.</p> <p>Данный параметр позволяет ограничить наборы шифров (cipher suites), которые могут использоваться при TLS-соединении. Разделитель между наборами – двоеточие (:). Если клиент не поддерживает ни один из указанных в данном параметре наборов, TLS-соединение не будет установлено.</p> <p>По умолчанию значением данного параметра является пустая строка, что означает отсутствие управления со стороны eCA-RA перечнем допустимых наборов шифров (ciphersuites) TLS-соединения для веб-сервера. (Исходный набор шифров веб-сервера не переопределяется).</p> <p>В данном параметре могут быть указаны любые наборы шифров, поддерживаемые используемой на сервере eCA-RA версией Openssl для TLS v1.2. Получить список поддерживаемых используемым Openssl наборов шифров для TLS v1.2 можно с помощью команды «openssl ciphers -tls1_2 -s».</p> <p>Данный параметр учитывается только при использовании Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cprnginx осуществляется с помощью утилиты «cprconfig» из состава «КриптоПро CSP».<sup>1</sup></p>
ssl_protocols	'TLSv1.2 TLSv1.3'	<p>Поддерживаемые версии протокола TLS Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обеих версий необходимо указывать их через пробел).</p>
backup_path	'/opt/aecaRa/dist/backup'	Путь до места хранения резервных копий
logs_base	'/opt/aecaRa/dist/logs'	Путь хранения лог-файлов
archive_path	'/opt/aecaRa/dist/archive'	Путь до архивированных файлов. Можно менять. Только абсолютные пути. Права на

<sup>1</sup> Инструкция по установке и настройке cprnginx - <https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/440/0/nginx-gost-binary-packages>.

Ключ	Значение по умолчанию	Описание
		каталог должны быть предоставлены пользователю/группе аеса:аеса.
certificates_ssl_path	'/opt/aecaRa/dist/certificates/ssl'	Путь хранения контейнера, сертификата и ключа web-сервера, а также цепочек сертификатов разрешенных издателей
certificates_aeca_ca_path	'/opt/aecaRa/dist/certificates/aeca-ca'	Путь хранения контейнера сертификата для авторизации в eCA-CA
Конфигурация пользователя		
aeca_user	'aeca'	Имя локального пользователя, создаваемого при установке eCA-RA
aeca_group	'aeca'	Наименование группы, создаваемой при установке eCA-RA, в которую входит пользователь, создаваемый по параметру "aeca_user"
Конфигурация памяти		
memory	'6144'	Конфигурация памяти (значение в МБ)
enable_gc_diagnostic	'false'	Флаг сбора диагностической информации о памяти
enable_heap_dump	'false'	Флаг сбора дампов памяти для «упавших» приложений ЦР
Конфигурация БД		
max_db_pool_size	'200'	Максимальный размер пула подключений к СУБД  Настраивается разработчиком, редактировать не следует
use_tls	'false'	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя СУБД
database_password	'#CHANGEIT'	Пароль пользователя СУБД. '#CHANGEIT' означает, что параметр не задан. Пароль пользователя СУБД. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
database_host	'localhost'	Имя хоста СУБД. Указано значение по умолчанию.
database_port	'5432'	Порт для доступа к СУБД. Указано значение по умолчанию.
database_name	'aecara'	Имя БД. Указано значение по умолчанию.
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД.

Ключ	Значение по умолчанию	Описание
		'#CHANGEIT' означает, что параметр не задан
Конфигурация eCA-RA		
http_port	'80'	Порт для подключения к программе по протоколу http
https_port	'433'	Порт для подключения к программному комплексу по протоколу https
hostname	'localhost'	Имя сервера, на котором развёртывается eCA-RA
hostname_no_mtls	'#CHANGEIT'	Параметр используется только в конфигурации с CPNGINX. Имя хоста (должно отличаться от значения hostname), используемое для доступа к интерфейсу без использования mTLS '#CHANGEIT' означает, что параметр не задан
Параметры использования HTTP при работе по протоколу SCEP		
allow_scep_http	'true'	Флаг возможности использования HTTP при работе по протоколу SCEP Возможные значения: 'true' / 'false' При использовании значения 'false' взаимодействие с eCA-RA по протоколу SCEP будет возможно только по HTTPS
Переменные окружения, используемые всеми сервисами		
number_of_services	'14'	Количество активных сервисов в системе  Настраивается разработчиком, редактировать не следует
logging_response	'false'	—
logging_sql	'false'	—
Переменные окружения для logback		
logs_file_max_size	'10MB'	Максимальный размер файла лога сервиса перед его архивацией. При достижении данного значения текущий лог-файл (access.log или service.log) будет архивироваться – файл будет сохранен в текущем каталоге логов данного сервиса с именем {access или service}-{дата в формате YYYY-MM-DD}.{индекс лога}.log.
logs_max_history	'10'	Максимальный срок хранения архивов логов в днях. Архивы логов, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться.
logs_total_size_cap	'100MB'	Максимальный общий объем логов, включая архивы, каждого типа (access или service) для каждого сервиса

Ключ	Значение по умолчанию	Описание
		При достижении данного объема наиболее старые архивы логов данного типа будут удаляться.
Ключ для внутренней аутентификации		
api_key	'2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810'	—
Переменные окружения, используемые tasks-service		
offline_enrollment_enabled	'false'	Флаг включения offline-выпуска. Возможные значения: true/false
offline_enrollment_cron	'0 0 * * * *'	CRON выражение, по которому будет запускаться offline-выпуск
offline_enrollment_template_id	'682225f6-f189-412f-a456-c480d42efaa8'	Идентификатор шаблона, который будет использоваться для offline-выпуска
offline_enrollment_request_path	'/opt/aecaRa/dist/enrollment/csr/'	Путь к каталогу с файлами запросов на сертификат для offline-выпуска Путь должен быть задан в абсолютном формате. Пользователю аеса должны быть предоставлены права на чтение для данного каталога.
offline_enrollment_certificate_path	'/opt/aecaRa/dist/enrollment/certificates/'	Путь к каталогу, в который будут записываться сертификаты, созданные в результате offline-выпуска Путь должен быть задан в абсолютном формате. Пользователю аеса должны быть предоставлены права на чтение и запись для данного каталога.
offline_enrollment_error_path	'/opt/aecaRa/dist/enrollment/error/'	Путь к каталогу, в который будут записываться запросы на сертификат, создание сертификата по которым было отклонено или завершено с ошибкой Путь должен быть задан в абсолютном формате. Пользователю аеса должны быть предоставлены права на чтение и запись для данного каталога.
Переменные окружения, используемые ca-adapter-service		
aeca_ca_host	'#CHANGEIT'	IP адрес eCA-CA. '#CHANGEIT' означает, что параметр не задан
aeca_ca_auth_filename	'AECA_CA_AUTH'	Имя файла контейнера сертификата, используемого для авторизации в eCA-CA
aeca_ca_auth_password	'#CHANGEIT'	Пароль контейнера сертификата, используемого для авторизации в eCA-CA '#CHANGEIT' означает, что параметр не задан
Параметры технологической учётной записи		
service_user_cert_renewal_enabled	'false'	Флаг включения автоматического обновления сертификата технологической

Ключ	Значение по умолчанию	Описание
		учётной записи eCA-RA. Возможные значения: true/false
service_user_cert_renewal_cron	'0 0 0 * * *'	CRON-выражение, по которому запускается проверка срока действия сертификата технологической УЗ eCA-RA. Значение по умолчанию — запуск проверки раз в сутки
service_user_cert_renewal_threshold	'90'	Пороговое значение (в процентах) для проверки срока действия сертификата технологической УЗ eCA-RA
service_user_cert_template_id	'#CHANGEIT'	Идентификатор шаблона, который будет использоваться при автоматическом обновлении сертификата технологической УЗ eCA-RA '#CHANGEIT' означает, что параметр не задан
service_user_id	'#CHANGEIT'	Идентификатор технологической УЗ eCA-RA. '#CHANGEIT' означает, что параметр не задан
Переменные окружения, используемые settings-service		
certificate_server_name	'server'	Имя файла сертификата web-сервера
certificate_raw_server_password	'#CHANGEIT'	Пароль от контейнера сертификата web-сервера/ '#CHANGEIT' означает, что параметр не задан
issuers_name	'issuers'	Имя файла разрешенных издателей
issuers_sync	'0 */30 * * * *'	CRON-выражение, по которому выполняется синхронизация разрешенных издателей
refresh_token_expire	'86400000'	Время жизни JWT токена обновления в миллисекундах Значение по умолчанию: 86400000 мс (1 сутки).  В течение данного срока маркер обновления можно использовать для получения нового маркера доступа и маркера обновления. По истечению данного срока маркер обновления нельзя использовать для этого. И для получения нового маркера доступа и обновления потребуются повторная аутентификация.
token_expire	'180000'	Время жизни JWT токена доступа в миллисекундах Значение по умолчанию: 180000 мс (3 минуты).
self_service_portal_enabled	'true'	Флаг доступности личного кабинета для получателей сертификатов

Ключ	Значение по умолчанию	Описание
		При указании значения 'false' для пользователей с ролью «Получатель сертификатов» будет недоступно использование личного кабинета в eCA-RA. Данный флаг не влияет на доступность методов API eCA-RA для получателей сертификатов.
Переменные окружения, используемые security-service		
session_max_count	'100'	Максимальное число сессий аккаунта (-1 - ограничение отключено) Значение по умолчанию: 100. Допустимые варианты указания предельного количества сессий для учетных записей: 1) натуральное число, представленное в десятичной системе счисления; 2) число «0»; 3) число «-1» (для выключения ограничения на количество сессий).
kerberos_service_principal	'#CHANGEIT'	Имя принципа, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_keytab_location	'#CHANGEIT'	Расположение keytab файла, содержащего тикет принципа, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_krb5_location	'#CHANGEIT'	Расположение файла конфигурации krb5.conf '#CHANGEIT' означает, что параметр не задан
kerberos_ad_domain	'#CHANGEIT'	Имя подключаемого домена. '#CHANGEIT' означает, что параметр не задан
kerberos_ad_server	'#CHANGEIT'	Адрес сервера контроллера домена Доступно указание сервера в формате ldap://<адрес контроллера домена> (для подключения по протоколу LDAP) и ldaps://<адрес контроллера домена> (для подключения по протоколу LDAPS). По умолчанию eCA-RA при подключении к домену по протоколу LDAPS будет доверять любому сертификату, предоставленному контроллером домена. '#CHANGEIT' означает, что параметр не задан
resource_type	'#CHANGEIT'	Тип PC (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN) При подключении к ресурсной системе Dynamic Directory необходимо указывать значение 'FREE_IPA'.



Ключ	Значение по умолчанию	Описание
		'#CHANGEIT' означает, что параметр не задан
resource_base_dn	'#CHANGEIT'	Точка подключения ресурса. '#CHANGEIT' означает, что параметр не задан
ldap_sign_in_failure_max_count	'5'	Максимальное количество неудачных попыток аутентификации через LDAP
ldap_sign_in_failure_delay_millis	'3600000'	Время задержки после последней неудачной попытки аутентификации через LDAP
Дополнительные настройки для подключения к домену с усиленными требованиями по безопасности аутентификации		
channel_binding_enabled	'false'	Включает поддержку привязки к TLS-каналу (Channel Bindings). Только для подключения к домену по протоколу LDAPS. Флаг будет проигнорирован, если подключение осуществляется по протоколу LDAP. Включение данного флага требуется для удовлетворения требования домена к наличию токенов привязки канала при аутентификации по Kerberos.
ldap_starttls_enabled	'false'	Включает TLS-шифрование (директива STARTTLS) при подключении к домену по протоколу LDAP для аутентификации. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS. Включение данного флага требуется для возможности аутентификации доменных пользователей по логинам и паролям, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию.
kerberos_qop_enabled	'false'	Включает механизмы QOP (Quality of Protection) для защиты данных внутри протокола Kerberos при подключении к домену по протоколу LDAP. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS. Включение данного флага требуется для возможности аутентификации доменных пользователей по Kerberos-билетам, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию.

Ключ	Значение по умолчанию	Описание
sign_provider	'EMBEDDED'	Провайдер подписи (выбирается между стандартным - 'EMBEDDED' и КриптоПро - 'CRYPTO_PRO')
sign_key_algorithm	'RSA'	Алгоритм подписи ключа Для стандартного провайдера доступны алгоритмы 'RSA' и 'ECDSA'. Для провайдера КриптоПро доступны алгоритмы 'RSA' и 'GOST_R_34_10_2012'.
sign_key_length	'2048'	Длина ключа подписи
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи Доступные для выбора значения алгоритмов хэширования: 1) для стандартного провайдера (EMBEDDED): для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' 2) для провайдера КриптоПро (CRYPTO_PRO): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012' для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384'
Переменные окружения, используемые api-gateway-service		
max_requests_count	'30'	Максимальное число параллельных HTTP запросов При превышении числа запросов в систему данного значения, для последующих запросов будет возвращаться HTTP код ошибки 429 (Слишком много запросов). Настраивается разработчиком, редактировать не следует
actuator_authenticate	'false'	Флаг доступности без аутентификации методов получения информации о сервисах и метод получения версии сервиса внешних интеграций.  При включении данного флага методы получения информации о сервисах и метод получения версии сервиса внешних интеграций будут недоступны без аутентификации пользователя. Для аутентифицированного пользователя в любой роли (администратора, оператора, получателя сертификатов) останутся доступными.
Переменные окружения, используемые logs-service		

Ключ	Значение по умолчанию	Описание
archive_cron	'0 0 0 1 * *'	CRON выражение, по которому запускается архивация журнала событий.
archive_enabled	'true'	Флаг: включена архивация. Возможные значения: true/false
archive_millis_ago	'15778800000'	Архивировать записи старше
Переменные окружения, используемые scep-service		
scep_certificate_renewal_cron	'0 0 0 * * *'	CRON-выражение, по которому запускается проверка сроков действия технологических сертификатов SCEP-профилей. Значение по умолчанию – запуск проверки раз в сутки
integrity_check_startup_enabled	'true'	Флаг выполнения контроля целостности при запуске eCA-RA Допустимые значения: true, false
integrity_check_fail_block_startup	'true'	Флаг блокировки запуска служб eCA-RA при неуспешной проверке целостности Допустимые значения: true, false
Данные eCA-RA, отображаемые в окне авторизации		
login_window_product_name	'Aladdin Enterprise CA'	Название программы, отображаемое в окне авторизации
login_window_component_name	'Центр регистрации'	Название компонента, отображаемое в окне авторизации
tab_title	'Aladdin Enterprise Registration Authority'	Текст, отображаемый в заголовке вкладок браузера
use_credentials_from_config	'true'	Флаг использования имени и пароля пользователя СУБД, а также пароля от контейнера для подключения к eCA-CA из конфигурационного файла (указываются в параметрах «database_username», «database_password» и «aeca_ca_auth_password» соответственно). Допустимые значения: «true», «false». Если данный параметр имеет значение «false», eCA-RA будет требовать указывать имя и пароль пользователя СУБД при выполнении следующих скриптов: <ul style="list-style-type: none"> <li>– install.sh;</li> <li>– uninstall.sh;</li> <li>– integrity_check.sh;</li> <li>– database_create.sh;</li> <li>– backup.sh;</li> <li>– restore.sh.</li> </ul> Данные скрипты поддерживают следующие способы передачи в них имени и пароля пользователя СУБД:

Ключ	Значение по умолчанию	Описание
		<p>в параметрах запуска «--dbuser» или «-U» (имя пользователя СУБД) и «--dbpass» или «-P» (пароль пользователя СУБД);</p> <p>в диалоговом режиме. Если не был указан какой-либо из параметров запуска, приведённых выше, скрипты при их запуске запросят ввод имени и/или пароля пользователя СУБД («Укажите имя пользователя СУБД» и/или «Укажите пароль пользователя СУБД»).</p> <p>Дополнительно скрипты «install.sh» и «restore.sh» будут требовать указания пароля от контейнера для подключения к eCA-CA. При этом скрипт «restore.sh» требует указания пароля только при восстановлении из резервной копии без хранения паролей в конфигурационном файле. Данные скрипты поддерживают следующие способы передачи в них пароля от контейнера:</p> <p>в параметре запуска «--capass» или «-C»;</p> <p>в диалоговом режиме. Если параметр запуска «--capass» или «-C» не указан, скрипты при их запуске запросят ввод пароля от контейнера для связи с eCA-CA («Укажите пароль от контейнера для подключения к eCA-CA»).</p>
strong_permissions_to_exception_files	'false'	<p>Флаг установки прав доступа 640 на файлы-исключения.</p> <p>По умолчанию eCA-RA устанавливает права доступа 640 на все свои файлы, кроме исключений (см. список ниже) и утилиты «jsverify». Утилита «jsverify» имеет права 740 (-rwxr-----) для возможности ее запуска при выполнении КЦ.</p> <p>Исключения (файлы по умолчанию имеют права 775):</p> <ul style="list-style-type: none"> <li>• файлы в каталоге «/opt/aecaRa/static» и его подкаталогах. Они представляют собой файлы клиентского компонента, доступ к ним необходим для Web-сервера.</li> <li>• файлы в каталоге «/opt/aecaRa/dist/webserver» и его подкаталогах. Данные файлы представляют собой конфигурации, подключаемые к Web-серверу.</li> <li>• файлы в каталоге «/opt/aecaRa/dist/certificates/ssl». В данном каталоге располагается сертификат Web-сервера, его закрытый ключ, а также файл с разрешенными издателями.</li> </ul> <p>При включении данного флага права доступа 640 будут установлены на указанные выше файлы-исключения.</p> <p>Для обеспечения сертифицированной среды функционирования присвойте параметру значение 'true'</p>

## 4.3 Настройка веб-сервера при ограничении доступа к его файлам

Если доступ к файлам веб-сервера ограничен (параметр `strong_permissions_to_exception_files` конфигурационного файла имеет значение `true`):

1. Для веб-сервера Nginx: в файле `/etc/nginx/nginx.conf` укажите первой строкой `user aeca;`.
2. Для веб-сервера Cppnginx: в файле `/etc/opt/cprosp/cppnginx/cppnginx.conf` укажите первой строкой `user aeca;`.
3. Для веб-сервера Apache:
  - 3.1. Для ОС РЕД ОС, ОС РОСА «ХРОМ» 12 Сервер и ОС Platform V SberLinux OS Server: в файле `/etc/httpd/conf/httpd.conf` замените значения для параметров `user` и `group`, указав в них значение `aeca`.
  - 3.2. Для ОС Astra Linux Special Edition: в файле `/etc/apache2/envvars` в строках `export APACHE_RUN_USER` и `export APACHE_RUN_GROUP` после символа `=` укажите значение `aeca`.
  - 3.3. Для ОС Альт Сервер: в файле `/etc/httpd2/conf/httpd2.conf` замените значения для параметров `user` и `group`, указав в них значение `aeca`.

## 4.4 Создание и настройка базы данных

Перед установкой eCA-RA необходимо создать и настроить БД. Это может быть выполнено одним следующих из способов:

- В автоматическом режиме, посредством запуска скрипта.
- В ручном режиме.

Созданная БД (имя базы данных по умолчанию `aecara`) предназначена для хранения информации:

- Об учётных записях.
- О заявках.
- О правилах выдачи сертификатов.
- О событиях журнала аудита.
- О ролях пользователей.
- О правах, определённых для ролей пользователей.

### 4.4.1 Создание и настройка базы данных в автоматическом режиме

Перед созданием БД в конфигурационном файле `/opt/aecaRa/scripts/config.sh` должны быть заданы параметры создаваемой БД (см. раздел 4.2 настоящего руководства).

**Внимание!** Если в качестве операционной системы в среде функционирования eCA-CA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом мандатного разграничения доступа (МРД)<sup>1</sup>, то при использовании локальной СУБД имя пользователя СУБД в параметре `database_username` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (см. подраздел 4.2 настоящего руководства) должно отличаться от имени пользователя ОС, указанного в параметре `aeca_user` конфигурационного файла.

<sup>1</sup> Активность МРД в Astra Linux Special Edition 1.8 может быть определена путём выполнения в терминале с правами суперпользователя команды `astra-mac-control status`.

Для создания и настройки БД:

1. Запустите скрипт выполнив следующую команду с правами суперпользователя <sup>1</sup>:

```
bash /opt/aecaRa/scripts/database_create.sh
```

2. При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.

В результате выполнения скрипта будет создана БД с параметрами, указанными в конфигурационном файле `/opt/aecaRa/scripts/config.sh` (имя пользователя, пароль, имя БД).

Если в качестве операционной системы в среде функционирования eCA-RA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным МРД, то при использовании локальной СУБД необходимо:

- создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путём выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя СУБД`.
- назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя СУБД`;
- предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

#### 4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме

Требования к настройке предварительно установленной СУБД PostgreSQL:

- Создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД.
- Создание БД, используемой программой в процессе работы.
- Назначение созданному пользователю полных прав доступа к созданной БД.

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите PostgreSQL выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку выполнив команду с правами суперпользователя:

```
systemctl enable postgresql
```

- Зайдите под пользователем «postgres» в PostgreSQL выполнив следующую команду с правами суперпользователя:

```
-u postgres psql
```

- Создайте пользователя базы данных выполнив следующую команду с правами суперпользователя:

```
CREATE USER aeca
```

где `aeca` - задаваемое имя пользователя по умолчанию, в случае указания отличного имени пользователя, требуется соответственно отредактировать конфигурационный файл (см. раздел 4.2).

**Внимание!** Если в качестве операционной системы в среде функционирования eCA-CA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом мандатного разграничения доступа (МРД)<sup>2</sup>, то при использовании локальной СУБД имя пользователя СУБД в параметре `database_username` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (см. подраздел 4.2

<sup>1</sup> Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba[версия]-client`).

<sup>2</sup> Активность МРД в Astra Linux Special Edition 1.8 может быть определена путём выполнения в терминале с правами суперпользователя команды `astra-mac-control status`.

**настоящего руководства) должно отличаться от имени пользователя ОС, указанного в параметре `aeca_user` конфигурационного файла.**

- Задайте пароль пользователю выполнив команду:

```
ALTER USER aeca WITH PASSWORD 'aeca';
```

где `'aeca'` - задаваемый пароль пользователя по умолчанию. В случае указания отличного пароля, требуется соответственно отредактировать конфигурационный файл (см. раздел 4.2).

- Создайте базу данных выполнив команду:

```
CREATE DATABASE aecara;
```

где `aecara` - задаваемое имя базы данных по умолчанию, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационный файл (см. раздел 4.2).

- Назначьте владельцем созданной базы данных созданного пользователя выполнив команду:

```
ALTER DATABASE aecara OWNER TO aeca;
```

- Наделите созданного пользователя полными правами доступа к созданной базе данных и завершите действия выполнив команды:

```
GRANT ALL PRIVILEGES ON DATABASE aecara TO aeca;
\q
```

- Завершите работу под пользователем «postgres» и выйдите из терминала выполнив команду:

```
exit
```

- Перезапустите СУБД PostgreSQL выполнив следующую команду с правами суперпользователя:

```
systemctl restart postgresql
```

- Установите расширение `pgcrypto` в БД PostgreSQL выполнив команду от имени пользователя «postgres» с правами суперпользователя:

```
-u postgres psql -c "CREATE EXTENSION IF NOT EXISTS pgcrypto WITH SCHEMA
pg_catalog;" -d aecara
```

где `aecara` - имя созданной базы данных.

• Если в качестве операционной системы в среде функционирования eCA-RA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД<sup>1</sup>, при использовании локальной СУБД дополнительно необходимо:

- создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путем выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя СУБД`.
- назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя СУБД`;
- предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

### 4.4.3 Создание и настройка базы данных Jatoba в ручном режиме

Требования к настройке предварительно установленной СУБД Jatoba:

- Создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД.
- Создание БД, используемой программой в процессе работы.

<sup>1</sup> Активность МРД в Astra Linux Special Edition 1.8 может быть определена путём выполнения в терминале с правами суперпользователя команды `astra-mac-control status`.



- Назначение созданному пользователю полных прав доступа к созданной БД.  
Возможно использование локальной СУБД или удаленной, доступной для подключений.
- Запустите Jatoba выполнив следующую команду с правами суперпользователя:

```
systemctl start jatoba-[версия]
```

Добавьте запуск Jatoba в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable jatoba-[версия]
```

- Зайдите под пользователем «postgres» в Jatoba выполнив следующую команду с правами суперпользователя:

РЕД ОС, РОСА «ХРОМ» 12  
Сервер и SberLinux OS  
Server

```
-u postgres psql
```

Astra Linux SE

```
-u postgres psql
```

Альт Сервер

```
- postgres -s /bin/bash
-bash-4.4$ /usr/jatoba-[версия]/bin/psql
psql
```

- Создайте пользователя БД выполнив команду:

```
CREATE USER aeca;
```

где **aeca** - задаваемое имя пользователя.

**Внимание!** Если в качестве операционной системы в среде функционирования еСА-СА используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом мандатного разграничения доступа (МРД)<sup>1</sup>, то при использовании локальной СУБД имя пользователя СУБД в параметре `database_username` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (см. подраздел 4.2 настоящего руководства) должно отличаться от имени пользователя ОС, указанного в параметре `aeca_user` конфигурационного файла.

- Задайте пароль пользователю выполнив команду:

```
ALTER USER aeca WITH PASSWORD 'aeca';
```

где **'aeca'** - задаваемый пароль пользователя.

- Создайте БД выполнив команду:

```
CREATE DATABASE aecara;
```

где **aecara** - задаваемое имя БД.

- Назначьте владельцем созданной БД созданного пользователя выполнив команду:

```
ALTER DATABASE aecara OWNER TO aeca;
```

- Наделите созданного пользователя полными правами доступа к созданной БД и завершите действия выполнив команды:

```
GRANT ALL PRIVILEGES ON DATABASE aecara TO aeca;
\q
```

- Завершите работу под пользователем «postgres» и выйдите из терминала выполнив команду:

```
exit
```

<sup>1</sup> Активность МРД в Astra Linux Special Edition 1.8 может быть определена путём выполнения в терминале с правами суперпользователя команды `astra-mac-control status`.



- Перезапустите СУБД Jatoba выполнив следующую команду с правами суперпользователя:

```
systemctl restart jatoba-[версия]
```

- Установите расширение pgcrypto в БД Jatoba выполнив команду от имени пользователя «postgres» с правами суперпользователя:

```
-u postgres psql -c "CREATE EXTENSION IF NOT EXISTS pgcrypto WITH SCHEMA pg_catalog;" -d aecara
```

где `aecara` - имя созданной базы данных.

• Если в качестве операционной системы в среде функционирования eCA-RA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД<sup>1</sup>, при использовании локальной СУБД дополнительно необходимо:

- создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путем выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя СУБД`.
- назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя СУБД`;
- предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

## 4.5 Установка программы

Установка выполняется при помощи скрипта `install.sh`. Необходимые для работы переменные могут быть переданы при запуске скрипта (см. таблицу 8) или введены в диалоге.

Таблица 8 — Параметры запуска скрипта `/opt/aecaRa/scripts/install.sh`

Параметр	Описание
<code>--authp12 путь_к_контейнеру</code>	Параметр предназначен для передачи пути к контейнеру закрытого ключа для подключения к eCA-CA
<code>-A путь_к_контейнеру</code>	То же, что и <code>--authp12 путь_к_контейнеру</code>
<code>--capass пароль</code>	Параметр предназначен для передачи пароля к контейнеру закрытого ключа для подключения к eCA-CA
<code>-C пароль</code>	То же, что и <code>--capass пароль</code>
<code>--webp12 путь_к_контейнеру</code>	Параметр предназначен для передачи в скрипт пути к контейнеру закрытого ключа для веб-сервера
<code>-W путь_к_контейнеру</code>	То же, что <code>--webp12 путь_к_контейнеру</code>
<code>--dbuser имя_пользователя СУБД</code>	См. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-U имя_пользователя СУБД</code>	То же, что <code>--dbuser имя_пользователя СУБД</code>
<code>--dbpass пароль_пользователя СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-P пароль_пользователя СУБД</code>	То же, что <code>--dbpass пароль_пользователя СУБД</code>

Для инициализации процесса установки eCA-RA запустите скрипт `install.sh`<sup>2</sup> с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.

<sup>1</sup> Активность МРД в Astra Linux Special Edition 1.8 может быть определена путём выполнения в терминале с правами суперпользователя команды `astra-mac-control status`.

<sup>2</sup> Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba[версия]-client`).

Пример запуска скрипта без параметров:

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

После инициализации процесса установки интерактивный инсталлятор запущен и пользователю будет предложено (в случае, если ранее eCA-RA был установлен):

- Установить ПО.
- Обновить ПО.
- Завершить работу инсталлятора.

Подтвердите выбор действия, вводом цифры «1» и процесс установки ПО будет запущен.

В случае, если в конфигурационном файле `/opt/aecaRa/scripts/config.sh` не определён используемый веб-сервер или введено неверное значение параметра `webserver`, то в процессе установки пользователю будет предложено выбрать используемый веб-сервер:

- Apache.
- Nginx.
- Cpnginx.

Выберите веб-сервер вводом соответствующей цифры.

В случае, если в конфигурационном файле `/opt/aecaRa/scripts/config.sh` не определено расположение конфигурации выбранного веб-сервера (параметр `webserver_path`), то в процессе установки пользователю будет предложено ввести расположение конфигурации.

В процессе установки требуется ввести полный путь до ранее подготовленных и скопированных на жёсткий диск файлов:

- Контейнера сертификата PKCS#12, используемого для работы с eCA-CA.
- Контейнера сертификата PCS#12 веб-сервера.

В процессе установки выполняется:

- Создание системного пользователя и соответствующей группы, от имени которых функционирует eCA-RA.
- Установка прав для создаваемого пользователя eCA-RA.
- Установка контейнера сертификата, используемого для авторизации в Центре сертификации Aladdin eCA.
- Установка контейнера сертификата веб-сервера eCA-RA.
- Подготовка, установка параметров и служебных сервисов.
- Запуск служебных сервисов.
- Запись номера сборки eCA-RA в БД <sup>1</sup>.

Ход установки программы отображён в виде горизонтальной шкалы с указанием процентов выполнения установки. В случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

После первичной установки программного средства системному пользователю `aeca` будет назначена командная оболочка `/sbin/nologin`, которая запрещает интерактивный вход в ОС. При обновлении ПО командная оболочка не меняется. Чтобы сменить командную оболочку выполните с правами суперпользователя команду:

```
usermod -s /bin/bash aeca
```

<sup>1</sup> Значение номера сборки записывается в таблицу «build\_info» схемы «aeca\_ra\_info».

## **4.6 Порядок совместной установки программы с другими компонентами Центра сертификатов доступа на одном сервере**

В Центре сертификатов доступа поддерживается совместная работа eCA-CA, eCA-RA и eCA-VA на одном сервере. Также поддерживается совместная работа eCA-RA и eCA-VA, а также eCA-RA и eCA-CA на одном сервере.

Порядок совместной установки компонентов Центра сертификатов доступа на одном сервере приведен в разделе 5.5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority».

## 5 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

еCA-RA запускается автоматически:

- Автоматически в случае выполнения успешной установки программы.
- Автоматически в случае выполнения успешного обновления программы.
- Автоматически после запуска ОС.

Для проверки состояния еCA-RA в терминале выполните команду с правами суперпользователя:

```
systemctl status aeca-ra.service
```

Возможные варианты ответа:

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

Для проверки автозагрузки программы выполните команду с правами суперпользователя:

```
systemctl is-enabled aeca-ra.service
```

Для добавления программы в автозагрузку выполните команду с правами суперпользователя:

```
systemctl enable aeca-ra.service
```

Для запуска программы выполните команду с правами суперпользователя:

```
systemctl start aeca-ra.service
```

Для перезапуска программы выполните команду с правами суперпользователя:

```
systemctl restart aeca-ra.service
```

При запуске еCA-RA выполняются следующие проверки:

- Проверка возможности подключения к базе данных. Если не удаётся подключиться к базе данных, то программа не запускается.
- Проверка соответствия номера своей сборки и значения номера сборки, указанной в базе данных<sup>1</sup>:
  - Если в базе данных отсутствует номер сборки, то программа не запускается.
  - Если номер сборки не равен номеру сборки программы, то программа завершает запуск с ошибкой «Текущая версия схемы базы данных не позволяет выполнить запуск службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где «X.X.X.X» - номер сборки указанный в базе данных, а «Y.Y.Y.Y» - номер сборки запускаемой программы.

Модули еCA-RA запускаются поочерёдно в порядке, приведённом в таблице 9.

Таблица 9 - Модули программы

Порядок запуска	Исполняемый файл	Наименование	Назначение
1	logs-service.jar	Модуль журнала событий	Обеспечивает фиксацию событий в журнале и получение событий из журнала, просмотра и поиск записей журнала событий, экспорт и архивацию записей журнала событий
2	tasks-service.jar	Модуль заявок	Обеспечивает управление заявками на сертификаты
3	ca-adapter-service.jar	Адаптер для подключения к еCA-CA	Обеспечивает передачу обработанных запросов на сертификат доступа в Центр сертификации и выпущенных по запросу сертификатов доступа в Центр регистрации
4	policies-service.jar	Модуль правил выбора	Обеспечивает управление правилами выпуска сертификатов

<sup>1</sup> Значение номера сборки указано в таблице «build\_info» схемы «aeca\_ra\_info».

Порядок запуска	Исполняемый файл	Наименование	Назначение
5	security-service.jar	Модуль безопасности	Обеспечивает управление учётными записями пользователей
6	routes-service.jar	Модуль управления	Предоставляет пользовательские веб-интерфейсы, обеспечивает разграничение доступа на основе ролей пользователей
7	export-service.jar	Модуль экспорта данных	Обеспечивает управление экспортом файлов программы
8	middleware-service.jar	Модуль промежуточного слоя	Обеспечивает взаимодействие с внутренним контуром eCA-RA
9	kerberos-provider-service.jar	Модуль аутентификации по Kerberos	Предназначен для аутентификации пользователя домена по Kerberos (без запроса имени пользователя и его пароля)
10	settings-service.jar	Модуль настроек	Обеспечивает управление жизненным циклом программы, её состоянием и параметрами (данные о продукте, конфигурация серверного сертификата SSL, разрешённые издатели сертификатов)
11	x509-provider-service.jar	Модуль аутентификации по сертификату	Предназначен для аутентификации пользователей в программе по сертификату доступа
12	api-gateway-service.jar	Модуль проксирования	Предназначен для перенаправления поступающих в программу запросов в нужный сервис (на основании данных, указанных в URL запроса), а также для перенаправления запросов к модулю безопасности с целью аутентификации пользователя
13	external-integration-service.jar	Модуль публичного API	Предоставляет публичное API, через которое сторонние сервисы могут взаимодействовать с eCA-RA
14	scep-enrollment-service.jar	Модуль SCEP	Реализует серверный компонент по протоколу SCEP
15	wstep-enrollment-service.jar	Модуль WSTEP	Реализует серверный компонент по протоколу WSTEP
16	storage-service.jar	Модуль хранения файлов	Предназначен для хранения файлов программы

Для завершения работы eCA-RA выполните команду с правами суперпользователя:

```
systemctl stop aeca-ra.service
```

eCA-RA при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты<sup>1</sup>, используемые для доступа к eCA-RA (определяются параметрами «http\_port» и «https\_port» конфигурационного файла /opt/aecaRa/scripts/config.sh), если данные порты не используются иными программами.

<sup>1</sup> Порты будут закрыты только в том случае, если они были открыты eCA-RA.

## 6 ПОДКЛЮЧЕНИЕ К ВЕБ-ИНТЕРФЕЙСУ

### 6.1 Общие сведения

Веб-интерфейс представляется собой графический интерфейс в виде совокупности динамических веб-страниц, отображаемых в веб-браузере. Веб-интерфейс реализован клиентским компонентом eCA-RA и предназначен для управления серверным компонентом eCA-RA (выполнения доступных пользователю в рамках его полномочий действий).

Подключение к веб-интерфейсу eCA-RA выполняется из веб-браузера удаленно по сети передачи данных с выделенного компьютера, на котором развернута среда функционирования, удовлетворяющая требованиям раздела 2.1.2.

Канал управления является защищенным — организован по протоколу HTTPS/TLS с двусторонней аутентификацией <sup>1</sup> и шифрованием передаваемых данных.

Идентификация и аутентификация пользователей с ролями «Администратор» и «Оператор» выполняется по предъявленному сертификату, который должен быть предварительно установлен в хранилище веб-браузера или хранилище сертификатов используемой ОС. Пример установки сертификата администратора из контейнера закрытого ключа PKCS#12 приведен в разделе 6.2.

Идентификация и аутентификация пользователей с ролью «Получатель сертификатов» выполняется по имени и паролю доменной учётной записи или Kerberos-билету.

При использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента eCA-RA должен быть организован по протоколу TLS ГОСТ с использованием отечественных криптографических алгоритмов.

Для этого на компьютере, предназначенном для подключения к веб-интерфейсу, должны быть выполнены следующие действия:

- Установлен криптопровайдер СКЗИ «КриптоПро CSP» в соответствии с инструкцией, описанной в разделе 2 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.
- Установлена клиентская лицензия СКЗИ «КриптоПро CSP», дающая право использовать двустороннюю аутентификацию по протоколу TLS. Порядок установки лицензии описан в разделе 4 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.
- Сертификат учётной записи администратора для взаимодействия с eCA-CA из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, должен быть установлен в личное хранилище пользователя с помощью утилиты `cptools` из состава СКЗИ «КриптоПро CSP». Порядок установки сертификата из контейнера закрытого ключа приведён в разделе 2.6.5 документа «СКЗИ «КриптоПро CSP». Инструкция по использованию графического приложения Инструменты КриптоПро (cptools)» ЖТЯИ.00101-03 92 06.
- Установлен веб-браузер Chromium с поддержкой TLS ГОСТ из состава используемой ОС. Данный веб-браузер входит в состав базовых репозиториях ОС Astra Linux SE, Альт Сервер, РЕД ОС, ОС РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.

### 6.2 Установка сертификата администратора

Для первичной настройки программы необходимо установить сертификат учётной записи пользователя с ролью «Администратор» eCA-CA, к которому подключён eCA-RA, в доверенное хранилище сертификатов веб-браузера или ОС <sup>2</sup>.

<sup>1</sup> При подключении пользователей с ролью «Получатель сертификатов» по умолчанию обеспечивается односторонняя аутентификация.

<sup>2</sup> Сертификат администратора из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, устанавливается в личное хранилище пользователя с помощью утилиты «cptools» из состава СКЗИ «КриптоПро CSP».

Процесс установки сертификата представлен на примере веб-браузера Mozilla Firefox:

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

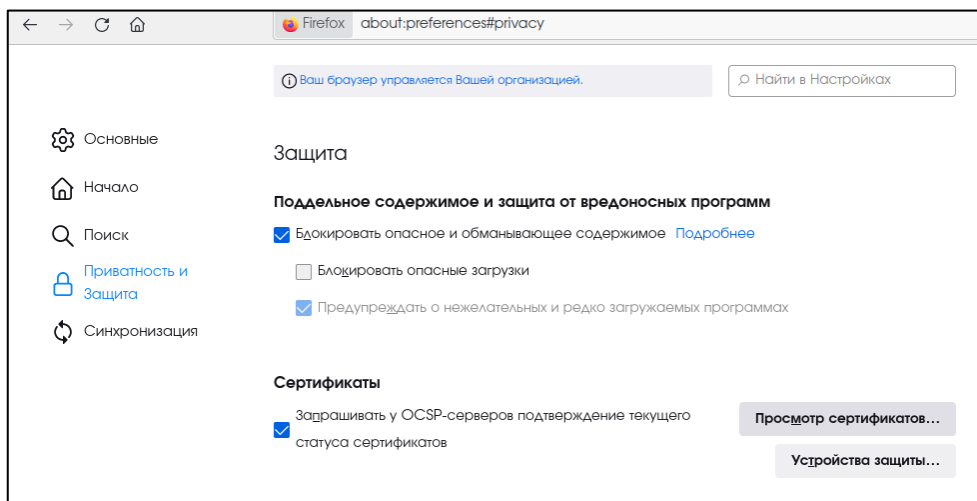


Рисунок 1 - Окно настроек браузера

- Выберите вкладку «Ваши сертификаты» и нажмите кнопку <Импортировать> (см. Рисунок 2).

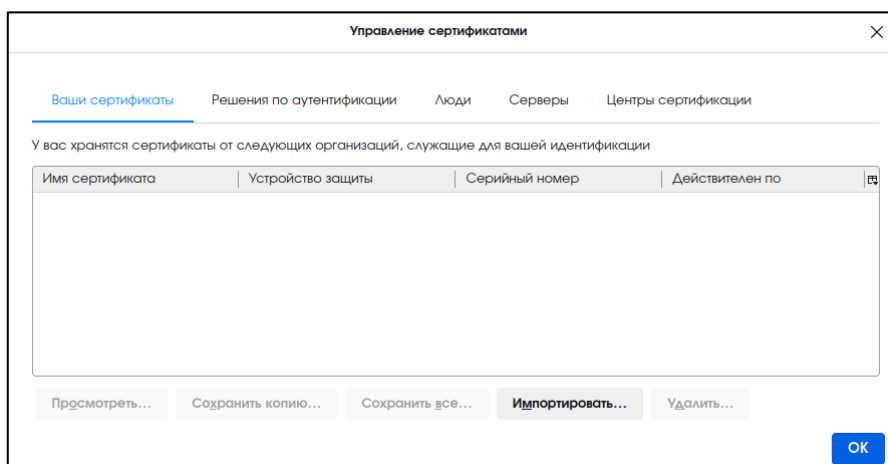


Рисунок 2 - Окно управления сертификатами

- Выберите предварительно подготовленный файл контейнера закрытого ключа PKCS#12, подписанный Центром сертификации, который будет принимать обработанные Центром регистрации запросы на сертификаты доступа и находящийся в списке разрешённых Издателей. Нажмите кнопку <Открыть> (см. Рисунок 3).

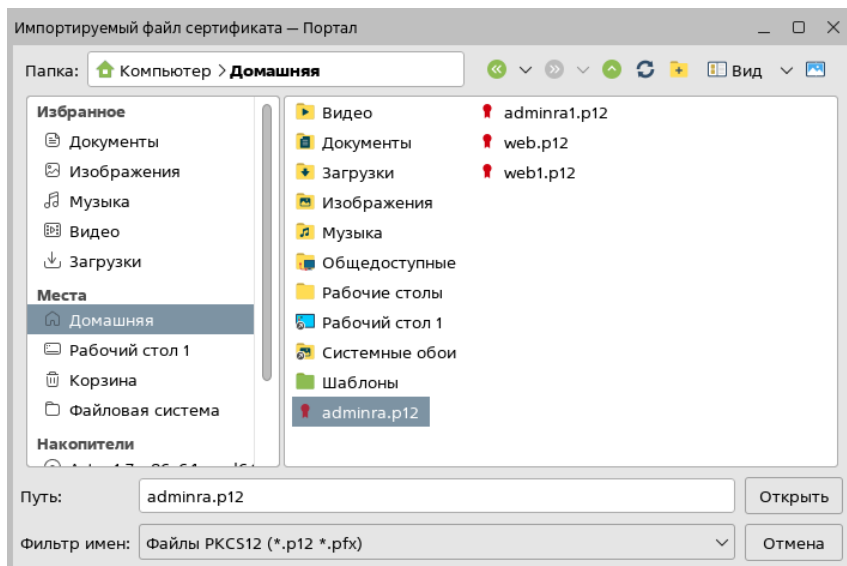


Рисунок 3 - Окно выбора импортируемого файла сертификата

- Введите пароль от контейнера закрытого ключа PKCS#12 в открывшемся окне и нажмите кнопку <OK> (см. Рисунок 4).

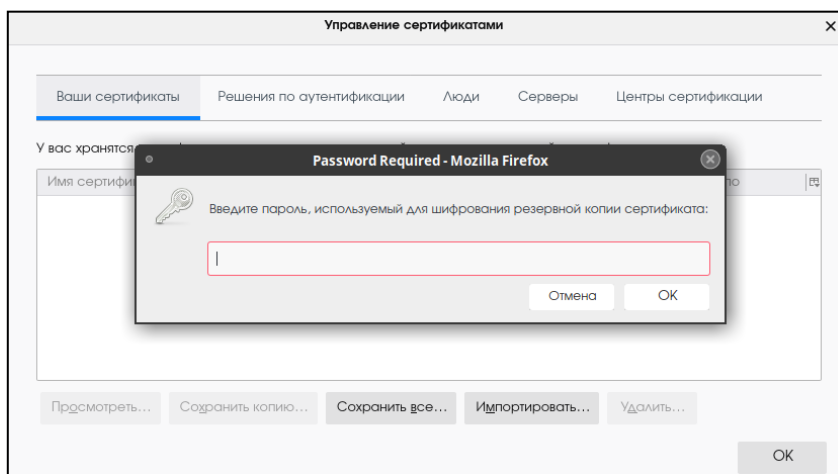


Рисунок 4 - Окно ввода PIN-кода сертификата

**Внимание!** Пароль устанавливается администратором еСА-СА при выпуске сертификата доступа.

- В результате сертификат будет установлен в хранилище веб-браузера (см. Рисунок 5). Нажмите кнопку <OK>.

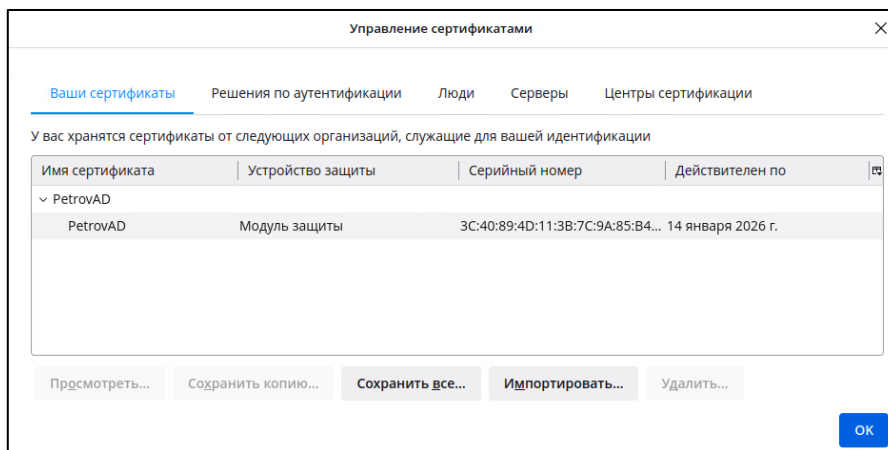


Рисунок 5 - Окно «Управление сертификатами»



## 6.3 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 eCA-RA (например, `https://172.22.5.21`).
- В открывшемся окне выберите сертификат администратора (см. Рисунок 6) и нажмите кнопку <OK>.

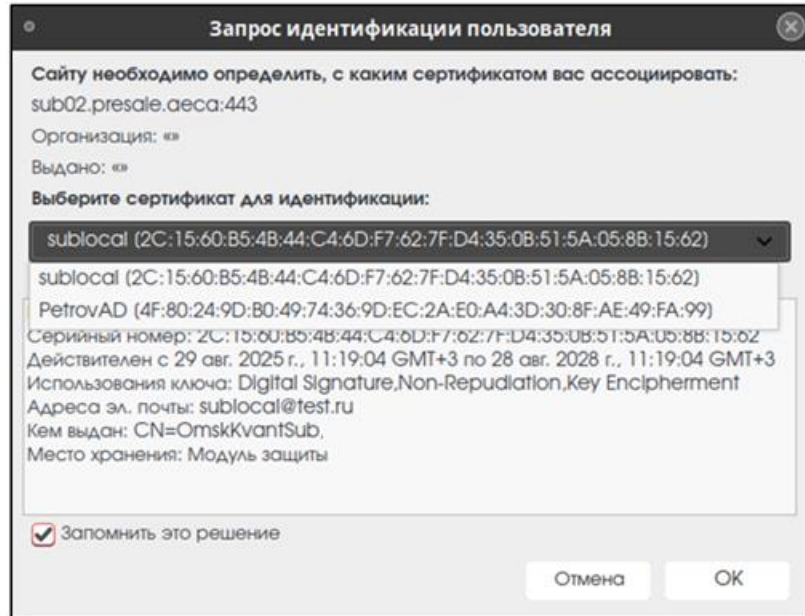


Рисунок 6 - Выбор сертификата для установки двустороннего TLS-соединения

При этом выбранный сертификат в дальнейшем будет использован для аутентификации, если пользователь выберет способ аутентификации с помощью сертификата. Если пользователь откажется от выбора сертификата, то будет установлено одностороннее TLS-соединение.

- На открывшейся странице с предупреждением системы безопасности (см. Рисунок 7) нажмите кнопку <Дополнительно>, примите риск и продолжите подключение.

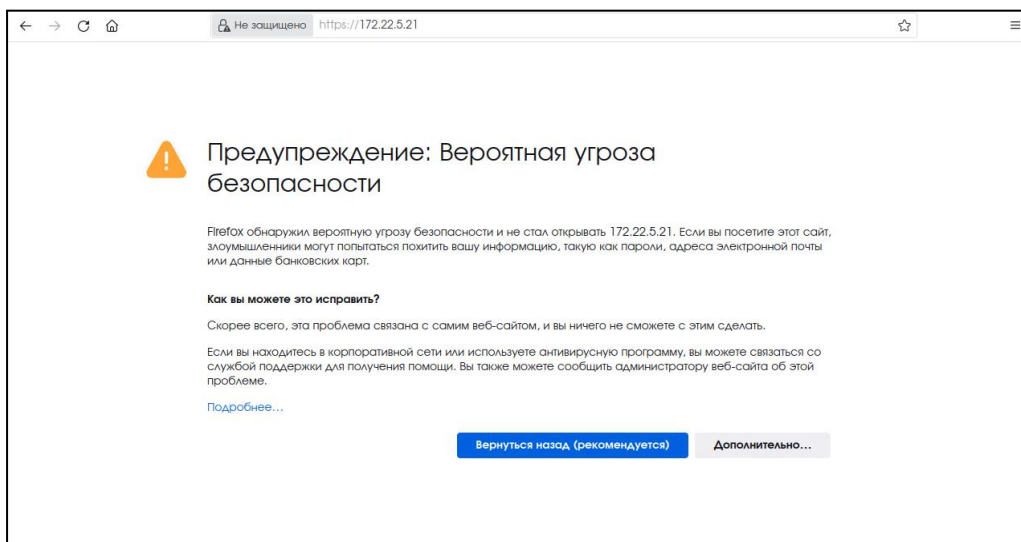


Рисунок 7 - Страница с предупреждением системы безопасности

После установки TLS-соединения для неаутентифицированного пользователя отображается окно авторизации (см. рисунок 8).

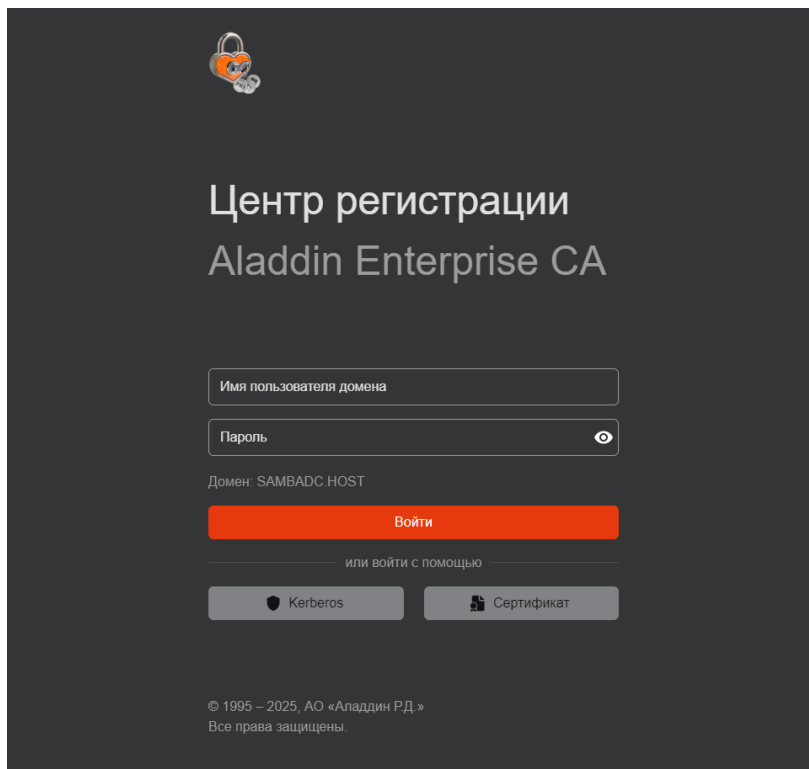


Рисунок 8 — Окно авторизации

еCA-RA поддерживает следующие способы аутентификации:

- С использованием сертификата учётной записи пользователя еCA-CA (см. раздел 6.5).
- С использованием Kerberos-билета пользователя ресурсной системы (см. раздел 6.7).
- По имени и паролю доменной учётной записи пользователя ресурсной системы (см. раздел 6.6).

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

Для переопределения сведений, отображаемых в окне авторизации и в заголовке вкладки браузера (см. рисунок 9):

1. В конфигурационном файле `/opt/aecaRa/scripts/config.sh` задайте необходимые значения параметрам:
  - `login_window_product_name` (для переопределения названия продукта, отображаемого в окне авторизации);
  - `login_window_component_name` (для переопределения названия компонента, отображаемого в окне авторизации);
  - `tab_title` (для переопределения текста, отображаемого в заголовке вкладок браузера).
2. Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.  
Пример запуска скрипта без параметров:  
`sudo bash /opt/aecaRa/scripts/install.sh`
3. Установщик предложит выбрать необходимое действие в интерактивном режиме.
4. Введите в терминале цифру «2».
5. Дождитесь окончания выполнения сценария обновления.

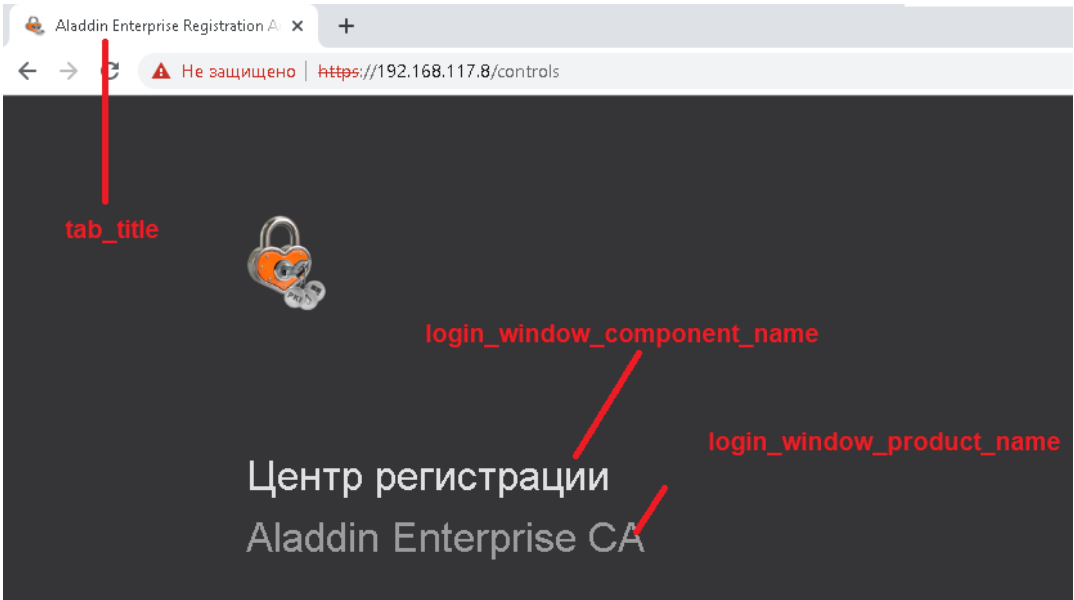
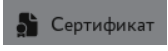


Рисунок 9 — Сведения, отображаемые в окне авторизации и в заголовке вкладки браузера

6.5 Аутентификация с использованием сертификата

Пользователи с ролями «Администратор» и «Оператор» eCA-CA могут аутентифицироваться в eCA-RA по сертификатам своих учетных записей. При этом роль учётной записи в eCA-RA соответствует роли в eCA-CA.

Для аутентификации по сертификату следует выполнить следующие действия:

- Подключитесь к веб-интерфейсу eCA-RA, выбрав при подключении в окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) установленный в хранилище веб-браузера или ОС ранее сертификат учётной записи.
- В открывшемся окне авторизации eCA-RA (см. Рисунок 8) нажмите кнопку .

В результате будет выполнена авторизация пользователя в eCA-RA. В ходе аутентификации по сертификату могут возникать ошибки, приведённые в таблице 10:

Таблица 10 - Типовые ошибки при аутентификации по сертификату

Ошибка	Описание
«Невозможно выполнить авторизацию с использованием сертификата. Сертификат не привязан к пользователю»	Учётная запись не найдена для данного сертификата
«Аккаунт заблокирован»	Учётная запись заблокирована
«Невозможно выполнить авторизацию с использованием сертификата, находящегося в данном состоянии»	Сертификат не является действующим (истек, приостановлен или отозван)
«Ошибка проверки издателя»	Сертификат был выпущен eCA-CA, не входящим в список разрешённых издателей сертификатов доступа, к которому подключён eCA-RA
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи (параметр <code>session_max_count</code> конфигурационного файла)

## 6.6 Аутентификация по имени и паролю доменной учётной записи

**Внимание!** Для аутентификации с помощью имени и пароля доменной учётной записи необходимо зарегистрировать в еCA-CA, к которому подключён еCA-RA, ресурсную систему, содержащую субъект, под которым будет проходить аутентификация, в соответствии с инструкцией в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».

Доменные учётные записи <sup>1</sup> могут аутентифицироваться в еCA-RA по имени и паролю доменной учётной записи пользователя. Информация о домене отображена в окне авторизации в поле «Домен».

Для аутентификации по имени и паролю выполните следующие действия:

- Подключитесь к веб-интерфейсу еCA-RA, пропустив при подключении в окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) выбор сертификата. Если используется `crnginx`, то подключение должно осуществляться по имени хоста из параметра `hostname_no_mtls` конфигурационного файла.
- В окне авторизации еCA-RA (см. Рисунок 8) в соответствующих полях введите имя и пароль доменной учётной записи и нажмите кнопку **Войти**.

В результате будет выполнена авторизация доменного пользователя в еCA-RA. Если в подключённом еCA-CA присутствует незаблокированная учётная запись, связанная с данным пользователем, то вход осуществляется под данной учётной записью с соответствующими ей правами.

Если у пользователя отсутствовала учётная запись в еCA-RA, то она будет автоматически создана с ролью «Получатель сертификатов».

Если в подключённом еCA-CA отсутствует незаблокированная учётная запись, связанная с данным пользователем (субъектом), вход субъекта должен осуществляться под УЗ с ролью «Получатель сертификатов».

При аутентификации по доменному имени и паролю могут возникать ошибки, приведённые в таблице 11.

Таблица 11 - Типовые ошибки при аутентификации по доменному имени и паролю

Ошибка	Описание
«Аккаунт заблокирован»	Доменная учётная запись или учётная запись в программе заблокирована
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи в еCA-RA (параметр <code>session_max_count</code> конфигурационного файла)

## 6.7 Аутентификация с использованием Kerberos-билета

**Внимание!** Для аутентификации пользоваля ресурсной системы с использованием Kerberos-билета необходимо зарегистрировать в еCA-CA, к которому подключён еCA-RA, ресурсную систему, содержащую субъект, под которым будет проходить аутентификация, в соответствии с инструкцией в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».


Доменные учётные записи <sup>2</sup> могут аутентифицироваться в еCA-RA по Kerberos-билету. Информация о домене отображена в окне авторизации в поле «Домен».

<sup>1</sup> Учётные записи, находящиеся в домене ресурсной системы, к которому подключён еCA-RA (адрес сервера доменной службы каталогов задан в параметре `kerberos_ad_server` конфигурационного файла).

<sup>2</sup> Учётные записи, находящиеся в домене, к которому еCA-RA (адрес сервера AD задан в параметре `kerberos_ad_server` конфигурационного файла).

Предварительно на компьютере доменного пользователя должен быть настроен веб-браузер с поддержкой Kerberos-аутентификации <sup>1</sup>, а также должен быть получен Kerberos-билет.

Для аутентификации по Kerberos-билету выполните следующие действия:

- Подключитесь к веб-интерфейсу eCA-RA, пропустив при подключении в окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) выбор сертификата. Если используется cnginx, то подключение должно осуществляться по имени хоста из параметра hostname\_no\_mtls конфигурационного файла.
- В открывшемся окне авторизации eCA-RA (см. Рисунок 8) нажмите кнопку .

В результате будет выполнена авторизация доменного пользователя в eCA-RA. Если в подключённом eCA-CA присутствует незаблокированная учётная запись, связанная с данным пользователем, то вход осуществляется под данной учётной записью с соответствующими ей правами.

Если у пользователя отсутствовала учётная запись в eCA-RA, то она будет автоматически создана с ролью «Получатель сертификатов».

При аутентификации по Kerberos-билету могут возникать ошибки, приведённые в таблице 12.

Таблица 12 - Типовые ошибки при аутентификации по Kerberos-билету

Ошибка	Описание
«Full authentication is required to access this resource»	Браузер не был настроен для аутентификации по Kerberos-билету - необходимо выполнить инструкцию по настройке веб-браузера
«Срок действия Kerberos-билета истек»	Срок действия Kerberos-билета истек - необходимо получить новый билет с помощью команды <code>kinit</code>
«Аккаунт заблокирован»	Доменная учётная запись или учётная запись в программе заблокирована
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи в программе (параметр <code>session_max_count</code> конфигурационного файла)

## 6.8 Завершение рабочей сессии пользователя

Для завершения рабочей сессии пользователя на верхней панели (см. Рисунок 10) веб-интерфейса eCA-RA нажмите на имя учётной записи пользователя и выберите в появившемся списке <Выход>. В результате рабочая сессия пользователя будет завершена - выполнен переход в окно авторизации eCA-RA (см. Рисунок 8).

**Внимание!** Для аутентификации по другому сертификату учётной записи необходимо перезагрузить веб-браузер.

<sup>1</sup> Инструкцию по настройке Kerberos-аутентификации в веб-браузерах см. в приложении 5 «Настройка Kerberos в веб-браузере».

## 7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

В данном раздел описаны функции управления еCA-RA, доступные пользователям с ролью «Администратор».

Функции управления еCA-RA, доступные пользователям с ролью «Оператор», описаны в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство оператора».

Функции управления еCA-RA, доступные пользователям с ролью «Получатель сертификатов», описаны в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство получателя сертификатов».

### 7.1 Верхняя панель

Верхняя панель (см. Рисунок 10) Центра регистрации фиксирована и отображается на любом шаге или переходе между разделами.

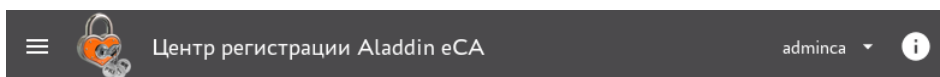
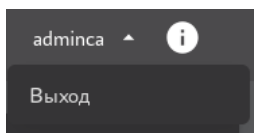
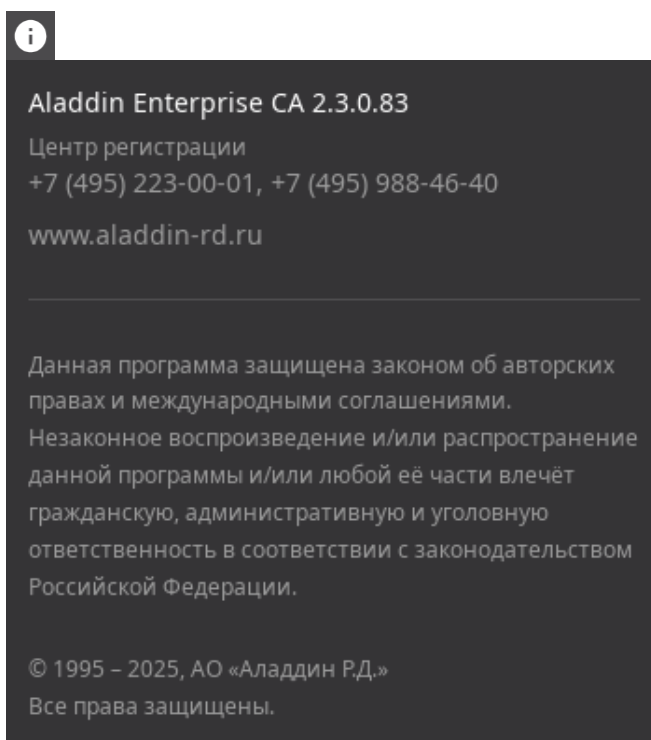


Рисунок 10 - Верхняя панель окна «Центра регистрации»

Верхняя панель содержит следующие элементы:





- имя учётной записи авторизованного пользователя.



- сведения о текущей версии программы, контактная информация разработчика, права на программное обеспечение.

### 7.2 Боковая панель

Боковая панель еCA-RA 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 вид боковой панели показан на рисунке ниже (Рисунок 11). Компактный вид боковой панели приведён на рисунке ниже (см. Рисунок 12). Выбор вида боковой панели происходит по нажатию кнопки , расположенной внизу данной панели.

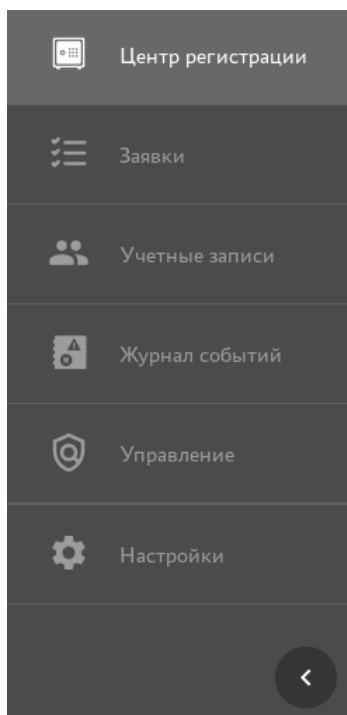


Рисунок 11 - Полный вид боковой панели

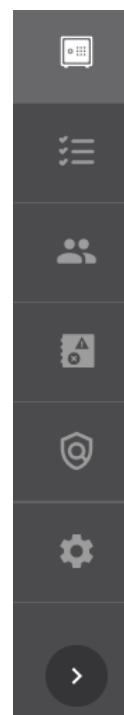


Рисунок 12 - Компактный вид боковой панели

Боковая панель состоит из разделов, определяющих соответствующие функции программы, и предназначена для организации управления еCA-RA:

- Раздел «Центр регистрации» - в данном разделе возможно:
  - посмотреть данные о подключённом Центре сертификации, который производит выпуск сертификатов по согласованным направленным заявкам на сертификаты Центром регистрации;
  - посмотреть данные о заявках на сертификаты за период от начала развёртывания Центра регистрации до настоящего момента (за всё время) и за последние 7 дней.
- 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.
- Раздел «Учётные записи» - в данном разделе возможно:
  - просмотреть существующие учётные записи;



- заблокировать или активировать существующую доменную учётную запись.
- 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.
- Раздел «Управление» - в данном разделе возможно:
  - просмотреть существующие правила выпуска;
  - создать новое правило выпуска;
  - отредактировать правило выпуска;
  - скопировать правило выпуска;
  - запустить или остановить правило выпуска;
  - удалить правило выпуска.
  - В разделе «Управление» на вкладке «SCEP» доступны следующие действия:
    - Управление SCEP-политиками:
      - Просмотр списка SCEP-политик;
      - Создание новой SCEP-политики;
      - Редактирование существующей SCEP-политики;
      - Запуск/остановка действия SCEP-политик;
      - Удаление существующей SCEP-политики.
    - Управление SCEP-профилями:
      - Просмотр списка SCEP-профилей;
      - Создание нового SCEP-профиля;
      - Редактирование существующего SCEP- профиля;
      - Запуск/остановка SCEP- профиля;
      - Копирование URL адреса SCEP-сервера для существующего SCEP-профиля;
      - Удаление существующего SCEP-профиля.
- Раздел «Настройки» - в данном разделе возможно:
  - на вкладке Веб-сервер выполнить:
    - просмотр данных текущего сертификата веб-сервера;
    - изменение текущего сертификата веб-сервера;
    - просмотр списка разрешённых издателей сертификатов.
  - на вкладке Syslog выполнить:
    - просмотр списка и параметров Syslog-серверов<sup>1</sup>;
    - добавление Syslog-сервера в список;
    - редактирование параметров Syslog-серверов из списка, включая управление (вкл./выкл.) отправкой сообщений на данный Syslog-сервер;
    - удаление Syslog-серверов из списка.

Доступность разделов в зависимости от ролей представлена в таблице 13.

Таблица 13 - Доступность раздела в зависимости от роли учётной записи

Раздел	Аноним	Получатель сертификатов	Оператор	Администратор
Центр регистрации	-	-	-	✓
Заявки	-	✓	✓	✓
Учётные записи	-	-	-	✓
Журнал событий	-	-	✓	✓
Управление	-	-	-	✓

<sup>1</sup> Syslog-сервер – программное обеспечение, осуществляющее регистрацию сообщений от клиентов по стандарту Syslog.



Раздел	Аноним	Получатель сертификатов	Оператор	Администратор
Настройки	-	-	-	✓

## 7.3 Раздел «Центр регистрации»

В разделе «Центр регистрации» присутствует следующая информация (см. Рисунок 13):

- Информация о Центре сертификации, с которым установлено подключение и который получает запросы от настоящего eCA-RA:
  - Подключённый ЦС (CN) - Common name Центра сертификации;
  - Подключённый ЦС (HostName) - IP-адрес или Hostname Центра сертификации;
  - Сертификат доступа к ЦС - расположение сертификата для доступа к eCA-CA.
- Информация об общем количестве созданных заявок.
- Информация о заявках на сертификаты:
  - Общее количество заявок на сертификаты, ожидающих подтверждения, и количество заявок на сертификаты, созданных за последнюю неделю.
  - Общее количество выпущенных сертификатов (количество выполненных заявок) и количество сертификатов, выпущенных за последнюю неделю.
  - Общее количество отклонённых заявок на сертификаты и количество отклонённых заявок на сертификаты за последнюю неделю.
  - Общее количество заявок на сертификаты, при обработке которых произошла ошибка, и количество заявок на сертификаты, при обработке которых произошла ошибка, за последнюю неделю.

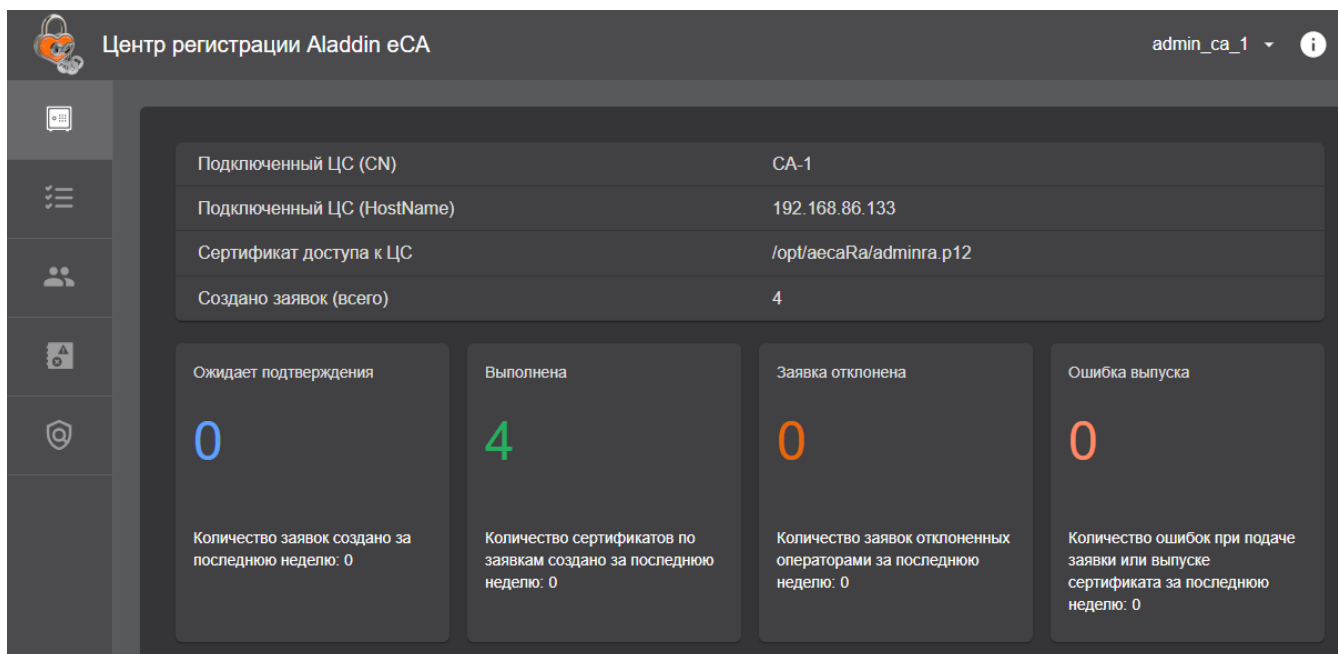


Рисунок 13 - Экран раздела «Центр регистрации»

## 7.4 Раздел «Заявки»

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

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:

- для пользователя с ролью «Администратор» на данном экране отображаются все созданные в eCA-RA заявки, а также у пользователя есть возможность обрабатывать заявки, попавшие под ручной режим обработки, скачивать и отзывать сертификаты, выпущенные по заявкам любых учётных записей (см. рисунок 14);
- пользователь с ролью «Оператор» может просматривать созданные им заявки, просматривать и обрабатывать заявки для доступных ему субъектов<sup>1</sup>, создавать заявки для любых субъектов eCA-CA, к которому подключён eCA-RA, скачивать и отзывать сертификаты, выпущенные по заявкам доступным ему субъектов (см. рисунок 15);
- пользователь с ролью «Получатель сертификатов», если параметр конфигурационного файла self\_service\_portal\_enabled имеет значение true, может просматривать только свои заявки, создавать новые заявки, получать выпущенные по своим заявкам сертификаты, а также отзывать их.

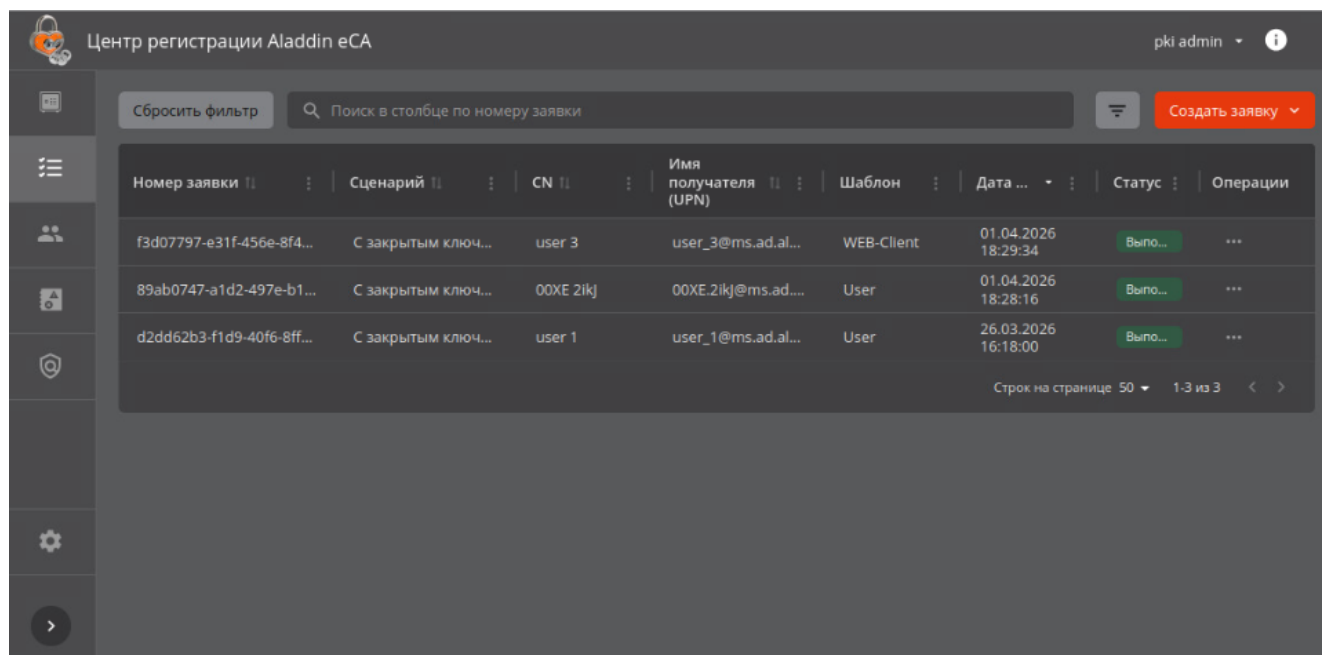


Рисунок 14 — Экран раздела «Заявки» для пользователя с ролью «Администратор»

<sup>1</sup> То есть заявки, у которых получателем сертификата является субъект, доступный данному оператору в соответствии с правилами доступа eCA-CA, к которому подключён eCA-RA.

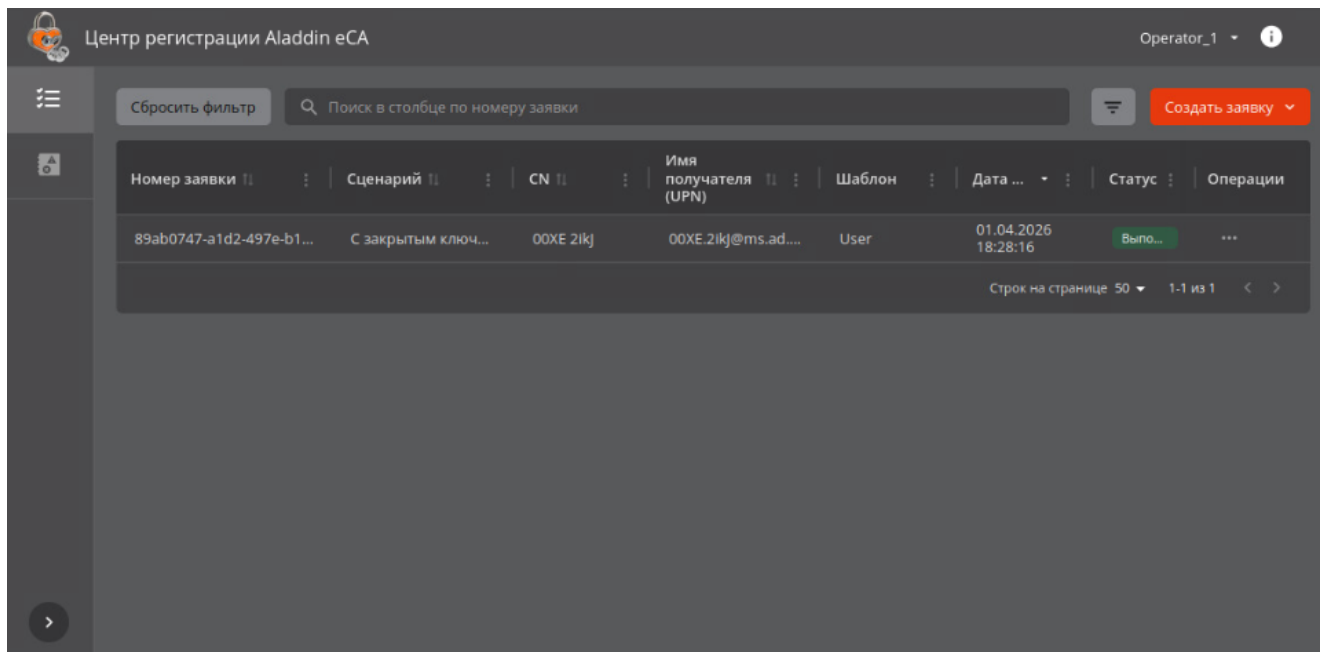


Рисунок 15 — Экран раздела «Заявки» для пользователя с ролью «Оператор»

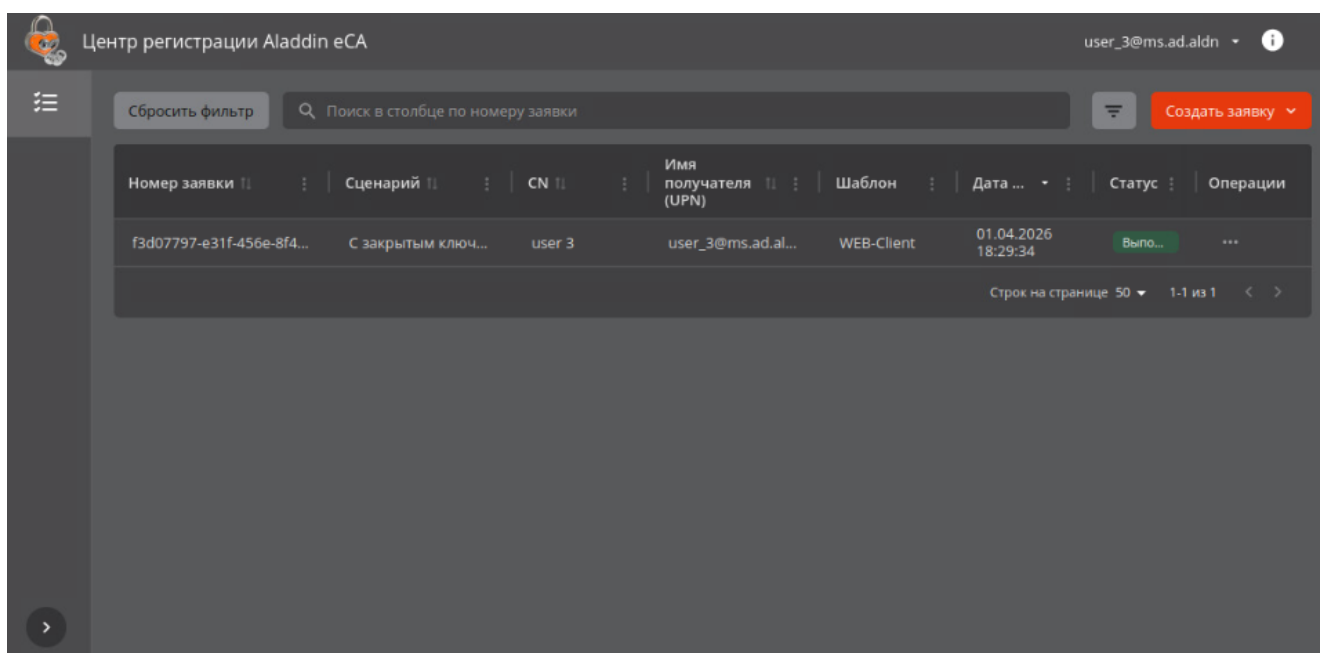


Рисунок 16 — Экран раздела «Заявки» для пользователя с ролью «Получатель сертификатов»

На экране раздела «Заявки» в табличной форме отображена следующая информация о заявках:

- Номер заявки - содержит номер заявки;
- Сценарий - содержит сценарий, по которому была создана заявка («На основании запроса (PKCS#10)», «С закрытым ключом (PKCS#12)», «На ключевом носителе», «SCEP»<sup>1</sup> или «WSTEP»<sup>2</sup>);
- CN - содержит CN, указанный в заявке на сертификат;
- Имя получателя (UPN) - содержит UPN отправителя заявки;

<sup>1</sup> Заявки с типом «SCEP» создаются в eCA-RA автоматически в результате обработки запросов клиентов по протоколу SCEP, подробнее см. раздел 8.


<sup>2</sup> Заявки с типом «WSTEP» создаются в eCA-RA автоматически в результате обработки запросов клиентов по протоколу MS-WSTEP, подробнее см. раздел 9.

- Шаблон - содержит шаблон, по которому должен быть выпущен сертификат;
- Дата обработки - содержит дату последней обработки заявки;
- Статус - содержит текущий статус заявки («Ошибка выпуска», «Отклонена», «Ожидает подтверждения», «Выполнена», «Отменена»<sup>1</sup>, «Ожидает импорта на КН»).

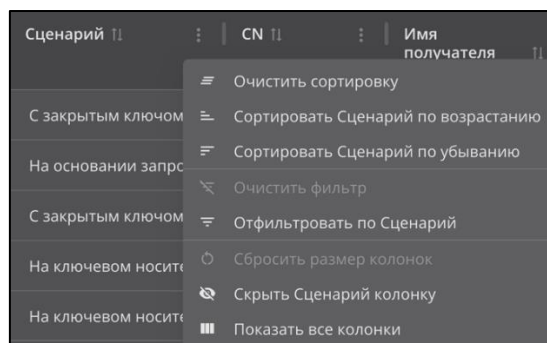
На экране раздела «Заявки» Доступны следующие действия:

- поиск заявок;
- просмотр карточки заявки;
- создание новой заявки на выпуск сертификата;
  - на основании запроса;
  - с закрытым ключом PKCS#12;
  - на ключевом носителе.
- действия над заявкой (подробнее см. в таблице 14.):
  - обработка ожидающих подтверждение заявок (выпустить сертификат или отменить заявку);
  - отмена созданных собой заявок;
  - импорт сертификата на ключевой носитель;
  - скачивание сертификата;
  - скачивание цепочки сертификатов;
  - скачивание контейнера закрытого ключа PKCS#12;
  - скачивание CRL издателя;
  - скачивание цепочки сертификатов издателя.

### 7.4.1 Управление экранной таблицей

Для каждой колонки экранной таблицы (справа от названия заголовка) доступна кнопка управления действиями  «Действия в колонке». По нажатию данной кнопки разворачивается меню (см. Рисунок 17, Рисунок 18 и Рисунок 19), в котором возможно (в зависимости от типа колонки и применённых ранее действий - фильтр, сортировка, изменение ширины, скрытие колонки):

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



<sup>1</sup> Статус «Отменена» подразумевает, что заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.

Рисунок 17 - Кнопка <Действия в колонке> в колонке «Сценарий»

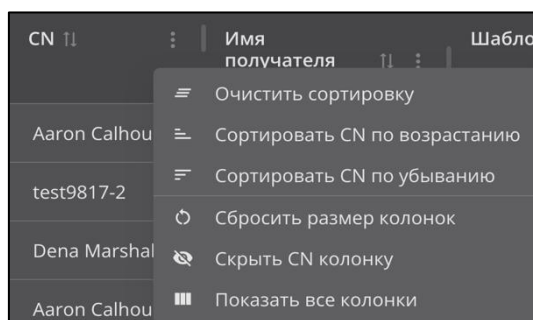


Рисунок 18 - Кнопка <Действия в колонке> в колонке «CN»

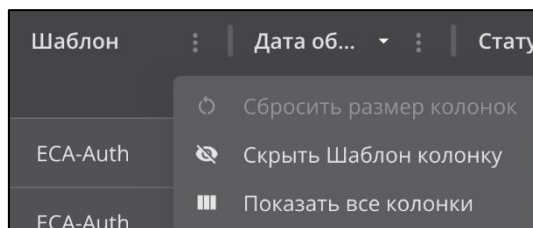



Рисунок 19 - Кнопка <Действия в колонке> в колонке «Шаблон»

Для сброса применённых фильтров следует нажать кнопку <Сбросить фильтр>  в результате чего в экранной таблице раздела «Заявки» будут отображены все произошедшие события (см. Рисунок 20).

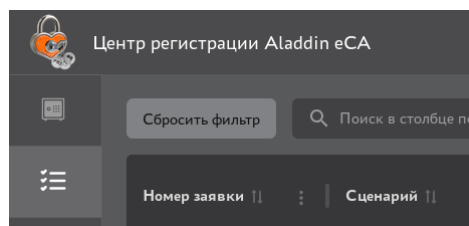



Рисунок 20 - Кнопка <Сбросить фильтр>

## 7.4.2 Фильтрация заявок

Для выборочного просмотра заявок на экране раздела «Заявки» 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 21):

- Сценарий - выберите сценарий выпуска сертификата («На основании запроса (PKCS#10)», «С закрытым ключом (PKCS#12)», «На ключевом носителе», «SCEP», «WSTEP»).
- Дата обработки - выберите период, в который должна попадать дата обработки заявки (введите дату с помощью клавиатуры или выберите в календаре).
- Статус - выберите статус заявки («Ошибка выпуска», «Отклонена», «Ожидает подтверждения», «Выполнена», «Отменена»<sup>1</sup>, «Ожидает импорта на КН», «Новая»).

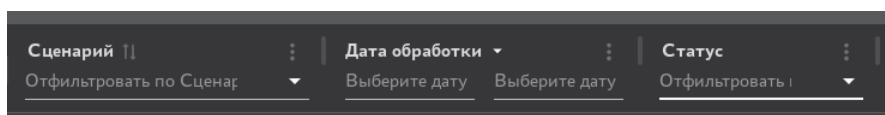





Рисунок 21 - Поля фильтра заголовков экранной таблицы


<sup>1</sup> Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.

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

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

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

Для очистки применённых фильтров для каждого заголовка колонки нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 17)

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

### 7.4.3 Сортировка заявок

Средства сортировки событий на экране раздела «Заявки» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 22):

- номер заявки - упорядочивание осуществляется в алфавитном порядке;
- сценарий - упорядочивание осуществляется в алфавитном порядке;
- CN - упорядочивание осуществляется в алфавитном порядке;
- имя получателя (UPN) - упорядочивание осуществляется в алфавитном порядке;
- дата обработки - упорядочивание осуществляется от старых к новым и от новых к старым.

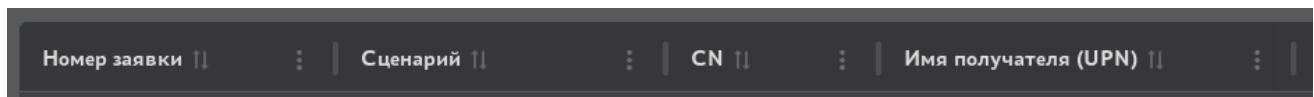




Рисунок 22 - Поля сортировки содержимого экрана раздела «Заявки»

Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки> (см. Рисунок 17, Рисунок 18).

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

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

Для сброса сортировки в каждой колонке:

- нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить сортировку» (см. Рисунок 17, Рисунок 18) или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

### 7.4.4 Поиск заявок

Строка поиска (см. Рисунок 23) предназначена для поиска заявок по содержимому колонки «Номер заявки». Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

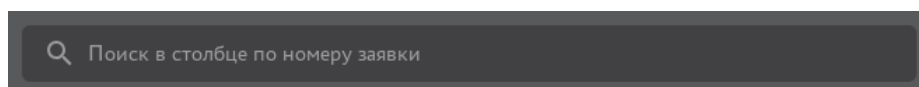


Рисунок 23 - Поисковая строка в разделе «Заявки»


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

### 7.4.5 Карточка заявки

Просмотр данных заявки возможен посредством страницы «Карточка заявки».

Переход к экрану «Карточка заявки» (см. Рисунок 24) осуществляется при нажатии на строку заявки главного экрана разделе «Заявки» (см. Рисунок 14).

Администратору доступны следующие информационные блоки на экране «Карточка заявки»:

- Заголовок с текстом «Заявка НОМЕР», где «НОМЕР» - номер заявки, и полем со статусом заявки. В поле статус заявки могут содержаться следующие значения: «Ошибка выпуска», «Отклонена», «Ожидает подтверждения», «Выполнена», «Отменена»<sup>1</sup>, «Ожидает импорта на КН»;
- Кнопка <Сертификат активирован>, отражающая текущий статус сертификата и предназначенная для отзыва сертификата, выпущенного по данной заявке. После отзыва сертификата кнопка меняет свое наименование на «Сертификат отозван» и становится неактивной.
- Кнопка  с контекстным меню действий (состав действий приведен в таблице 14, контекстное меню см. Рисунок 25, Рисунок 26 и Рисунок 27).

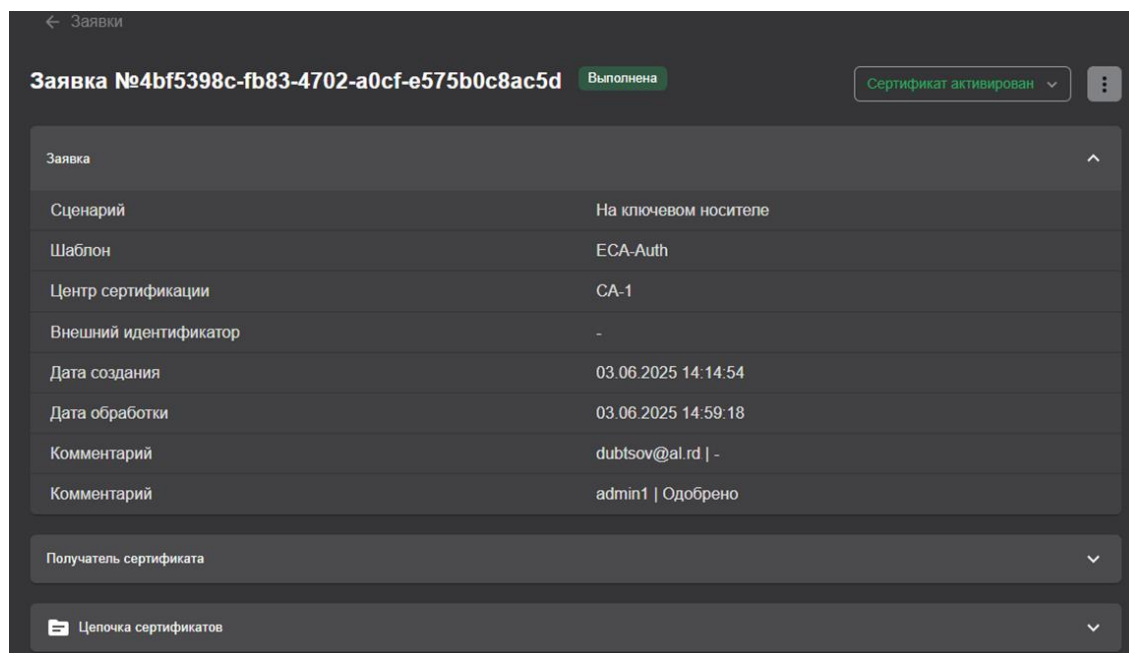


Рисунок 24 - Экран «Карточка заявки»

Таблица 14 - Доступные действия для заявок

Действия	Условие отображения действия	Выполнение
Выпустить сертификат	(Статус заявки «Ожидает подтверждения» или «Ошибка выпуска») и роль текущей учётной записи - Администратор	См. раздел 7.4.10
Отклонить выпуск		
Отмена заявки	(Статус заявки «Ожидает подтверждения» или «Ошибка выпуска») и получателем сертификата является субъект, связанный с текущей учётной записью	См. раздел 7.4.9
Скачать запрос PKCS#10	Поле «Сценарий» равно «На основании запроса (PKCS#10)» и (роль текущей учётной записи - Администратор или и получателем сертификата является субъект, связанный с текущей учётной записью)	Происходит скачивание запроса PKCS#10, указанного в заявке

<sup>1</sup> Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.



Действия	Условие отображения действия	Выполнение
Скачать сертификат	Статус заявки «Выполнена» или «Ожидает импорта на КН» и (роль текущей учётной записи - Администратор или получателем сертификата является субъект, связанный с текущей учётной записью)	Происходит скачивание сертификата, выпущенного по заявке
Скачать цепочку сертификатов		Происходит скачивание цепочки сертификатов при успешном выпуске сертификата
Скачать цепочку сертификатов издателя		Происходит скачивание цепочки сертификатов издателя при успешном выпуске сертификата
Скачать CRL издателя		Происходит скачивание CRL издателя при успешном выпуске сертификата
Скачать контейнер PKCS#12	Статус заявки «Выполнена» и поле «Сценарий» равно «С закрытым ключом (PKCS#12)» и (роль текущей учётной записи - Администратор или получателем сертификата является субъект, связанный с текущей учётной записью)	Происходит скачивание контейнера PKCS#12, указанного к заявке
Импортировать на ключевой носитель	Статус заявки «Ожидает импорта на КН» и (роль текущей учётной записи - Администратор или получателем сертификата является субъект, связанный с текущей учётной записью)	См. раздел 7.4.11

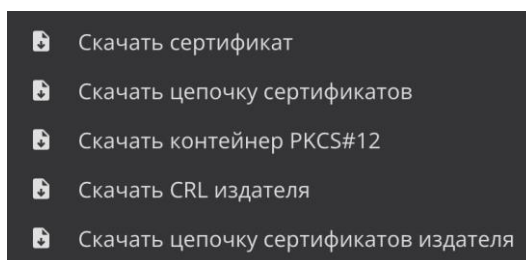


Рисунок 25 - Меню действий в карточке заявки

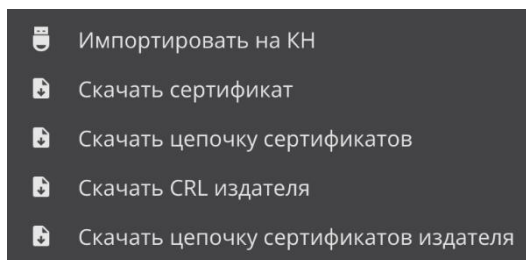


Рисунок 26 - Меню действий для заявки



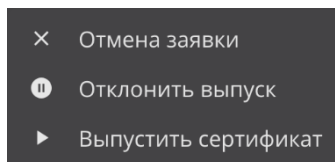


Рисунок 27 - Меню действий для заявки. Заявка в статусе «Ожидает подтверждения»

- Блок «Заявка», содержащий следующие строки в формате «ключ - значение» (см. Рисунок 28):
  - Сценарий - содержит сценарий, по которому была создана заявка («На основании запроса (PKCS#10)», «С закрытым ключом (PKCS#12)», «На ключевом носителе», «SCEP» или «WSTEP»);
  - Шаблон - содержит название шаблона, по которому должен быть выпущен сертификат;
  - Центр сертификации - центр сертификации, в котором будет выполняться выпуск сертификата по данной заявке, на основании используемого в сценарии создания заявки шаблона;
  - Внешний идентификатор - содержит значение внешнего идентификатора, указанного при создании заявки;
  - Дата создания - содержит дату создания заявки;
  - Дата обработки - содержит дату последней обработки заявки;
  - Комментарий - содержит комментарий, указанный при обработке заявки.

Заявка	
Сценарий	С закрытым ключом (PKCS#12)
Шаблон	ECA-Auth
Центр сертификации	CA-1
Внешний идентификатор	-
Дата создания	18.02.2025 14:53:14
Дата обработки	18.02.2025 14:53:48
Комментарий	admin_ca_1   213

Рисунок 28 - Экран «Карточка заявки». Блок «Заявка»

- Блок «Получатель сертификата», содержащий следующие строки в формате «ключ - значение» (см. Рисунок 29):
  - Идентификатор - содержит идентификатор субъекта. Значение поля является ссылкой, при нажатии на которую открывается карточка соответствующего субъекта ЦС в новой вкладке браузера;
  - Ресурсная система - содержит CN ресурсной системы субъекта;
  - Имя получателя (UPN) - содержит UPN отправителя заявки;
  - Common Name - содержит CN, указанный в заявке на сертификате.

Получатель сертификата	
Идентификатор	<a href="#">ccd5f712-03f9-4084-bba6-b5bbcb858b63</a>
Ресурсная система	al
Имя получателя (UPN)	petrov@al.rd
Common Name	петров

Рисунок 29 - Экран «Карточка заявки». Блок «Получатель сертификата»

- Блок «Информация о сертификате», содержащий (см. Рисунок 30):
  - Раскрывающийся список (дерево) «Цепочка сертификатов»;
  - Сведения о сертификате в табличной форме, содержащие следующие строки в формате «ключ - значение»:
    - 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.

Цепочка сертификатов	
Root-CA2 петров	
Издатель	Root-CA2
Владелец	петров
SDN владельца	CN=петров
Действует с	18.02.2025 16:17:44
Действует по	18.02.2027 16:17:44
Алгоритм ключа	RSA
Длина ключа	1024

Рисунок 30 - Экран «Карточка заявки». Вид для администратора. Блок «Информация о сертификате»

- Блок «Состав сертификата», содержащий следующую информацию о сертификате (см. Рисунок 31):

Состав сертификата	
Серийный номер	2bb8fb378b821b5af3f2f7aa54f20cc028ce42a9
Открытый ключ	
Отпечаток	
Версия	
Параметр открытого ключа	
Алгоритм цифровой подписи	
Основные ограничения	
Использование ключа	
Доступ к информации о центре сертификации	
Идентификатор ключа центра	
Альтернативное имя субъекта	
Идентификатор ключа субъекта	
Расширенное использование ключа	

Рисунок 31 - Экран «Карточка заявки». Блок «Состав сертификата»

- 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.

Блок «История изменения заявки», содержащий историю изменений заявки в табличном виде (см. Рисунок 32). В таблице изменений отображается следующая информация:

- Дата - содержит дату события изменения заявки;
- Имя учётной записи - содержит отображаемое имя пользователя, сделавшего изменение в заявке;
- Событие - содержит описание изменения.

История изменения заявки		
Дата	Имя учетной записи	Событие
18.02.2025 16:17:44	petrov@al.rd	Создание заявки
18.02.2025 16:17:45	petrov@al.rd	Выпуск сертификата по заявке
18.02.2025 16:17:44	petrov@al.rd	Обработка заявки

Рисунок 32 - Экран «Карточка заявки». Блок «История изменения заявки»

#### 7.4.6 Создание заявки на основании запроса

Для создания заявки на основании запроса выполните следующие шаги:

- Нажмите кнопку «Создать заявку» на главном экране раздела «Заявки» (см. Рисунок 14).
- В открывшемся контекстном меню выберите сценарий выпуска сертификата «На основании запроса» (см. Рисунок 33).

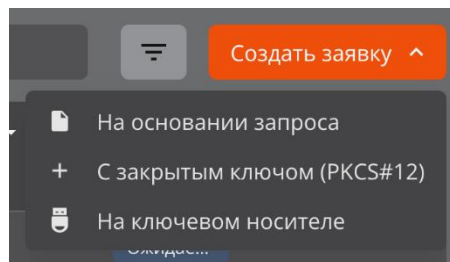



Рисунок 33 - Контекстное меню создания заявки

- В открывшемся окне «Создание заявки» на шаге 1 выберите субъект, для которого выпускается сертификат (см. Рисунок 34):
  - 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  (см. Рисунок 34).
- в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего поля атрибута субъекта, разделитель значений в поле - запятая с пробелом;
- в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному
- полю атрибуте у субъекта отсутствуют значения;
- выберите субъект и нажмите кнопку <Продолжить> для перехода к следующему шагу.

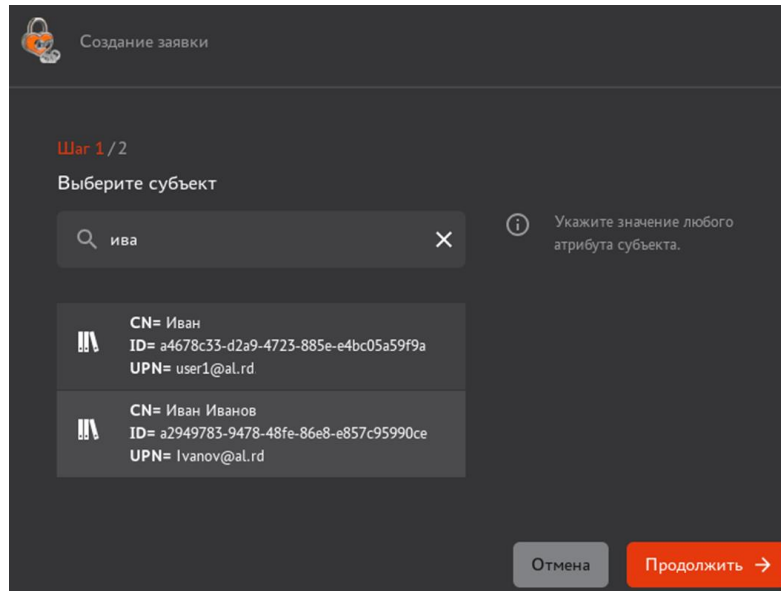


Рисунок 34 - Создание заявки на основании запроса. Шаг 1

- На втором шаге (см. Рисунок 35):
  - выберите файл-запрос (загружается по кнопке <Выбрать файл> с возможностью повторного выбора по кнопке <Изменить>);
  - выберите шаблон, на основании которого будет создан сертификат. В списке шаблонов присутствуют шаблоны, которые указаны в правилах выпуска с режимом обработки «Автоматический выпуск» или «Ручная обработка» для выбранного на шаге 1 субъекта<sup>1</sup>.

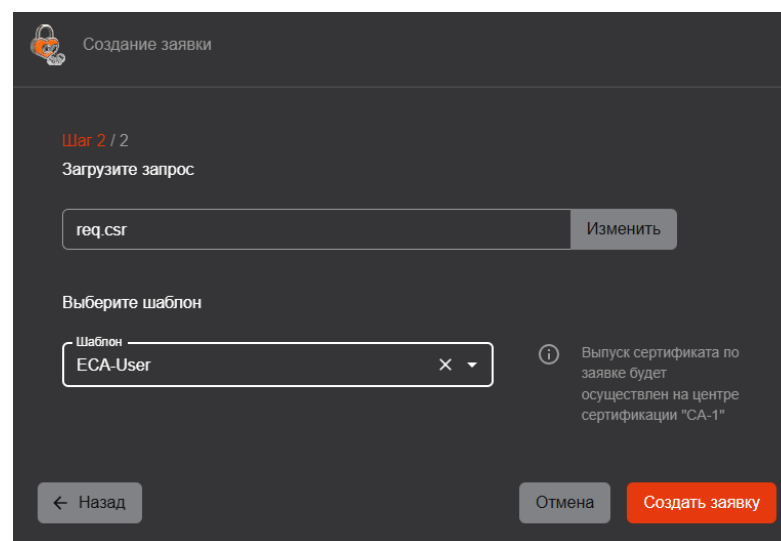


Рисунок 35 - Создание заявки на основании запроса. Шаг 2

<sup>1</sup> Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

- Для создания заявки нажмите на кнопку <Создать заявку>.

После этого заявка будет зарегистрирована и обработана в соответствии с правилом выпуска, под которое она попадает.

### 7.4.7 Создание заявки с закрытым ключом PKCS#12

Для создания заявки с закрытым ключом PKCS#12 выполните следующие шаги:

- Нажмите кнопку <Создать +> на главном экране раздела «Заявки» (см. Рисунок 14).
- В открывшемся контекстном меню выберите сценарий выпуска сертификата «С закрытым ключом (PKCS#12)» (см. Рисунок 36).

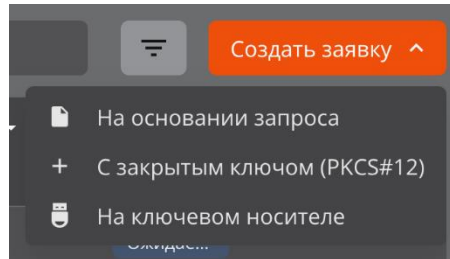



Рисунок 36 - Контекстное меню создания заявки

- В открывшемся окне «Создание заявки» на первом шаге выберите субъект, для которого выпускается сертификат (см. Рисунок 34):
  - 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  (см. Рисунок 37).
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего поля атрибута субъекта, разделитель значений в поле - запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному
  - полю атрибуте у субъекта отсутствуют значения.



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

Рисунок 37 - Создание заявки с закрытым ключом PKCS#12. Шаг 1

- На втором шаге выберите шаблон, на основании которого будет создан сертификат. В списке шаблонов присутствуют шаблоны, которые указаны в правилах выпуска с режимом обработки «Автоматический выпуск» или «Ручная обработка» для выбранного на шаге 1 субъекта<sup>1</sup>.

После выбора шаблона нажмите на кнопку <Продолжить> для перехода к следующему шагу.

Рисунок 38 - Создание заявки с закрытым ключом PKCS#12. Шаг 2

- На третьем шаге указаны атрибуты в соответствии с шаблоном сертификата (см. Рисунок 39). Значения атрибутов заполняются автоматически в соответствии с данными из субъекта ЦС, выбранного на шаге 1, и изменению не подлежат. В случае если в атрибуте указано несколько значений, в выпадающем меню будет предложен выбор значения из существующих или возможно добавление значения атрибута по нажатию кнопки <Добавить>  справа от соответствующего поля (если атрибут содержит несколько значений, то при наведении мышки на кнопку <Добавить>, она становится активной - красного цвета). Дополнительно добавленное значение атрибута можно удалить по кнопке <Удалить>  справа от соответствующего поля атрибута.


При отсутствии доступных для указания значений в обязательном по шаблону поле отображается ошибка «Обязательно к заполнению».

Необязательные поля могут оставаться незаполненными. При этом необязательные поля субъекта с отсутствующими значениями отображаются в выключенном состоянии.

<sup>1</sup> Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

После заполнения полей и нажмите кнопку <Продолжить> для перехода к следующему шагу.

Рисунок 39 - Создание заявки с закрытым ключом PKCS#12. Шаг 3

- На четвёртом шаге задайте пароль для ключевого контейнера PKCS#12 (см. Рисунок 40):
  - пароль должен содержать не менее восьми символов с использованием цифр, заглавных и прописных букв, ввод осуществляется на латинице;
  - если в пароле используются запрещённые символы, то рамка поля ввода приобретает красный цвет;
  - если пароль и подтверждение не совпадают, то рамка поля подтверждения окрашивается в красный цвет;
  - для просмотра вводимых символов следует нажать кнопку  на текущей строке;

После заполнения полей и нажмите кнопку <Продолжить> для перехода к следующему шагу.

Рисунок 40 - Создание заявки с закрытым ключом PKCS#12. Шаг 4

- На пятом шаге укажите параметры криптографии (см. Рисунок 41):
  - выберите алгоритм генерации ключевой пары. Список алгоритмов определяется выбранным шаблоном;
  - выберите длину ключа. Минимальная доступная для выбора длина ключа определяется выбранным шаблоном.

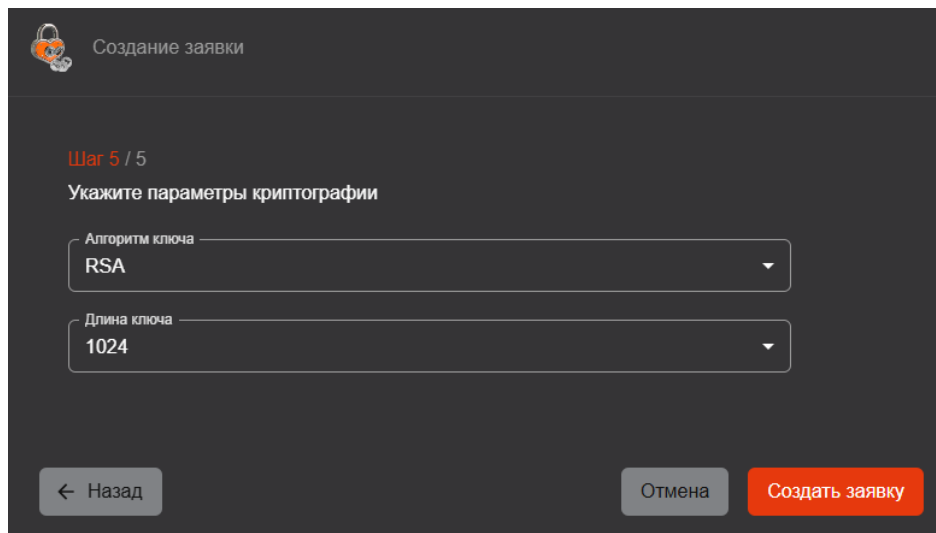


Рисунок 41 - Создание заявки с закрытым ключом PKCS#12. Шаг 5

- Для создания заявки нажмите на кнопку <Создать заявку>.  
После этого заявка будет зарегистрирована и обработана в соответствии с правилом выпуска, под которое она попадает.

#### 7.4.8 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](#). Возможность выпуска сертификатов на КН Рутокен должна быть указана в лицензии на eCA.

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

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

Для создания заявки на ключевом носителе выполните следующие действия:

- Подключитесь к веб-интерфейсу eCA-RA и перейдите в раздел **Заявки**.
- На панели инструментов нажмите кнопку **Создать заявку** и выберите в открывшемся списке сценарий создания заявки **<На ключевом носителе>** (см. Рисунок 42).

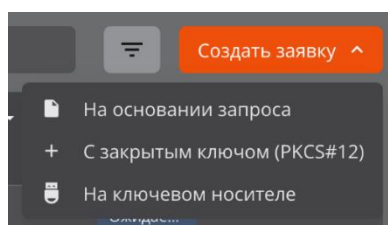


Рисунок 42 - Контекстное меню создания заявки

**Внимание!** Если JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 43) или к компьютеру не подключен ключевой носитель (см. Рисунок 44), создать заявку невозможно.



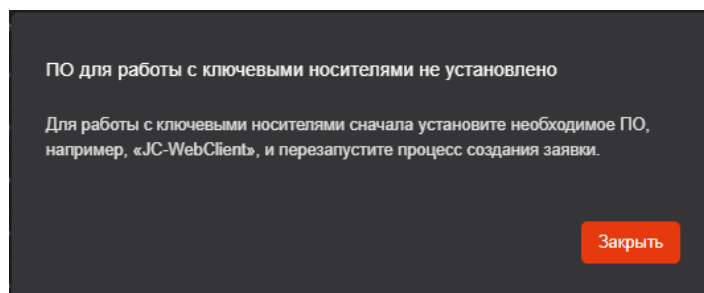


Рисунок 43 - ПО для работы с ключевыми носителями не установлено

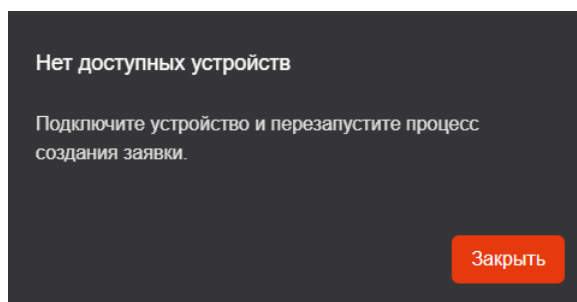



Рисунок 44 - Подключенные ключевые носители отсутствуют

- В открывшемся окне «Создание заявки на сертификат» (см. Рисунок 37) выберите субъекта и нажмите кнопку .

Чтобы найти субъекта в поле поиска введите ключевое слово, содержащееся в его любом атрибуте. Поиск является регистронезависимым. Для найденных субъектов отображаются следующие атрибуты:

- «CN» - значение атрибута «Common Name» субъекта.
- «ID» - идентификатор субъекта.
- «UPN» - значение атрибута «MS UPN, User Principal Name» субъекта.
- «DNS» - значение атрибута «DNS Name» субъекта
-  - признак подключения к ресурсной системе.
- В открывшемся окне «Создание заявки на сертификат» (шаг 1 сценария) (см. Рисунок 45):
  - В списке «Устройство» выберите подключённый ключевой носитель.
  - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
  - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат<sup>1</sup>.

В списке шаблонов присутствуют шаблоны, которые указаны в правилах выпуска с режимом обработки «Автоматический выпуск» или «Ручная обработка» для выбранного на шаге 1 субъекта<sup>2</sup>.

  - Нажмите кнопку .

<sup>1</sup> Получателю сертификатов (субъекту PC) доступны шаблоны в соответствии с установленными для него в eCA-RA уполномоченным пользователем с ролью «Администратор» правилами выпуска. Правило выпуска может быть назначено как непосредственно получателю сертификатов (субъекту PC), так и группе безопасности, в которую входит получатель сертификатов (субъект PC). Правило выпуска также определяет режим обработки (рассмотрения) заявки. В соответствии с правилом выпуска обработка заявки и выпуск сертификата может выполняться в eCA-CA как в автоматическом режиме (автоматическое подтверждение), так в ручном (автоматизированном) режиме пользователями с ролями «Администратор» или «Оператор» (подтверждение или отклонение заявки).

<sup>2</sup> Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

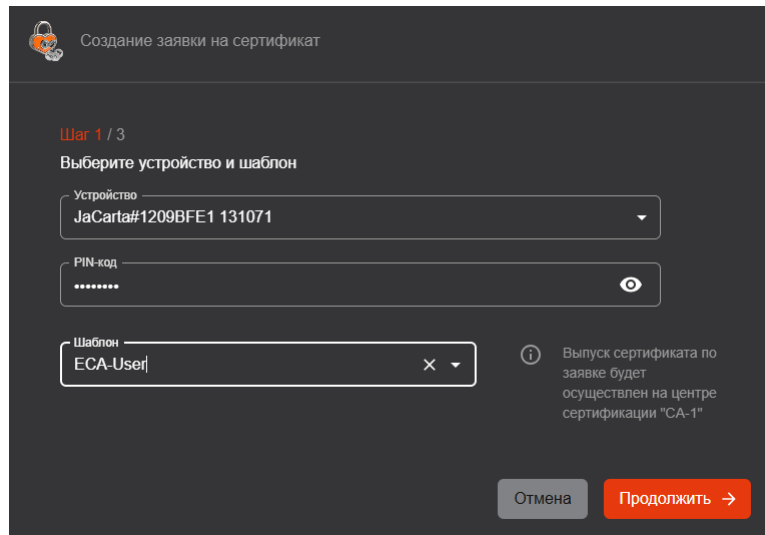


Рисунок 45 - Выбор ключевого носителя и шаблона для выпуска сертификата

- В открывшемся окне «Создание заявки на сертификат» (шаг 2 сценария) (см. Рисунок 46) укажите атрибуты получателя сертификатов (субъекта РС) и нажмите кнопку **Продолжить** →.

Значения атрибутов заполняются автоматически в соответствии с данными субъекта, полученными из еСА-СА, 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 субъекта РС содержится несколько значений).

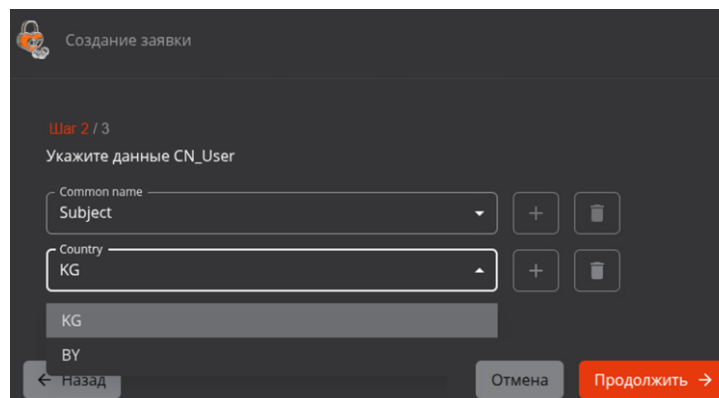


Рисунок 46 - Создание заявки на ключевом носителе. Шаг 3

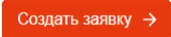
При необходимости добавьте новые атрибуты. Для этого нажмите рядом со списками атрибутов кнопку **+** и выберите в списках атрибутов нужные значения (выбор доступен, если в атрибутах субъекта содержится несколько значений).

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

В случае отсутствия у субъекта обязательных по шаблону атрибутов под списком атрибута отображается сообщение об ошибке. При этом создание заявки на выпуск сертификата по данному шаблону невозможно.

Если у субъекта отсутствуют необязательные по шаблону атрибуты, процесс заведения заявки на выпуск сертификата можно продолжить.

- В открывшемся окне «Создание заявки на сертификат» (шаг сценария 3) (см. Рисунок 47):
  - 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 .

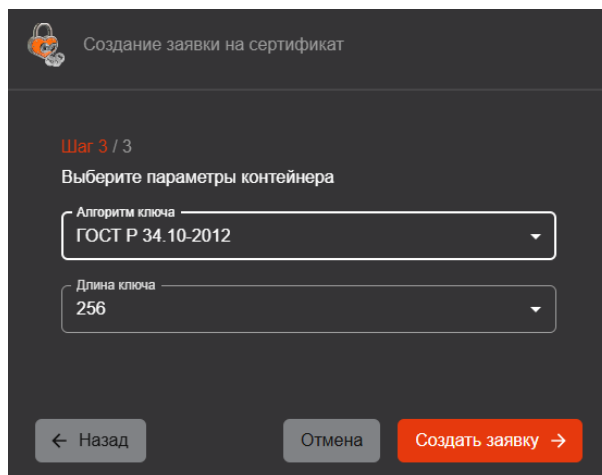



Рисунок 47 - Создание заявки на ключевом носителе. Шаг 4

- В открывшемся окне «Создание заявки на сертификат» (процесс формирования заявки и его результат) (см. Рисунок 48) отображаются следующие процессы:
  - Генерации ключевой пары.
  - Генерации запроса.
  - Создания заявки.

Успешное завершения каждого процесса помечается значком .

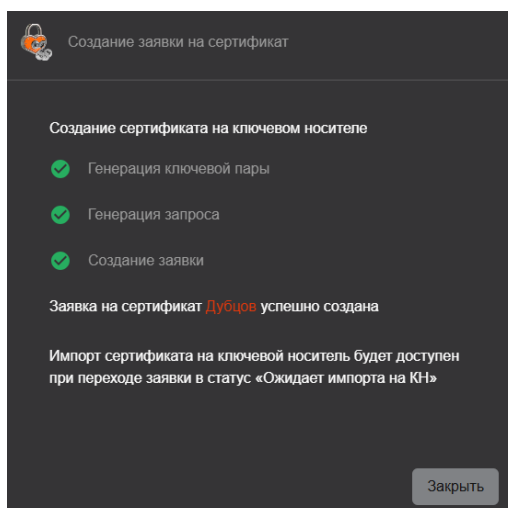


Рисунок 48 - Заявка на выпуск сертификата на ключевом носителе заведена успешно

**Внимание!** Некоторые типы ключевых носителей поддерживают определенный набор алгоритмов выработки ключевых пар (например, в приведённом ниже примере при создании заявки на выпуск сертификата на электронном ключе JaCarta-2 ГОСТ был выбран неподдерживаемый алгоритм RSA) (см. Рисунок 49).

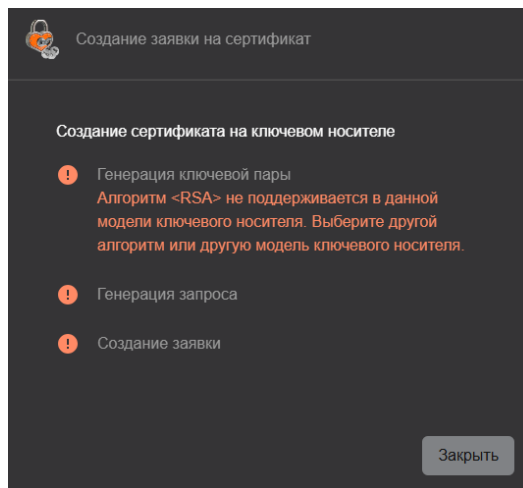



Рисунок 49 - Выбранный алгоритм не поддерживается в используемом ключевом носителе

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

Импорт сертификата на ключевой носитель (см. раздел 7.4.11) будет доступен (статус заявки «Ожидает импорта на КН») после одного из следующих событий:

- Подтверждение заявки уполномоченным пользователем и выпуск сертификата в еСА-СА.
- Автоматическое подтверждение заявки и выпуск сертификата в еСА-СА.



#### 7.4.9 Отмена заявки

**Внимание!** Статус заявки, участвующей в сценарии, должен быть «Ожидает подтверждения» или «Ошибка выпуска».

Отмена заявки может быть выполнена только учётной записью, создавшей данную заявку. Для отмены заявки выполните следующие шаги:

- На главном экране раздела «Заявки» найдите заявку, которую необходимо отменить. При этом заявка должна находиться в статусе «Ожидает подтверждения» или «Ошибка выпуска».

Далее необходимо нажать на кнопку выбора действий для заявки:

- в строке заявки нажмите на кнопку <Операции> .
- либо в карточке заявки нажмите на кнопку .
- В появившемся контекстном меню (см. Рисунок 50) выберите действие «Отмена заявки».

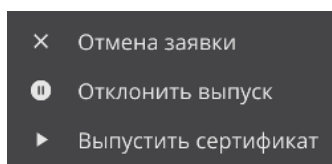


Рисунок 50 - Меню действий для заявки. Заявка в статусе «Ожидает подтверждения», создателем данной заявки является текущая учётная запись

- В появившемся окне введите комментарий к отмене заявки (см. Рисунок 51) и нажмите кнопку <Отменить> для подтверждения действия.

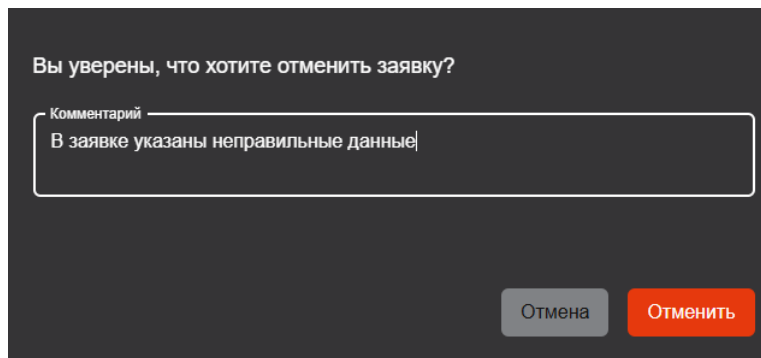


Рисунок 51 - Окно комментария к отмене заявки

- После подтверждения операции будет выполнена отмена заявки, в результате чего её статус будет изменён на «Отменена». Над заявками в статусе «Отменена» никаких действий в eCA-RA не предусмотрено.

Указанный комментарий будет отображаться в карточке заявки в поле «Комментарий».



#### 7.4.10 Обработка заявки

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

Для обработки заявки выполните следующие шаги:

- На главном экране раздела «Заявки» найдите заявку, которую необходимо обработать. При этом заявка должна находиться в статусе «Ожидает подтверждения».

Далее необходимо нажать на кнопку выбора действий для заявки:

- в строке заявки нажмите на кнопку «Операции» ;
- либо в карточке заявки нажмите на кнопку .
- В появившемся контекстном меню (см. Рисунок 52) выберите действие из перечня:
  - Отклонить выпуск.
  - Выпустить сертификат.

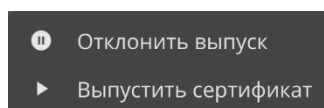


Рисунок 52 - Меню действий для заявки. Вид для администратора. Заявка в статусе Ожидает

- В появившемся окне введите комментарий к действию (см. Рисунок 53 и Рисунок 54).
- Нажмите на кнопку «Выпустить» или «Отклонить» для подтверждения действия.

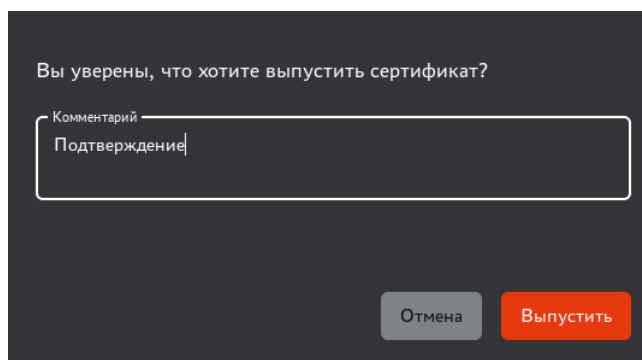


Рисунок 53 - Окно комментария к подтверждению выпуска сертификата

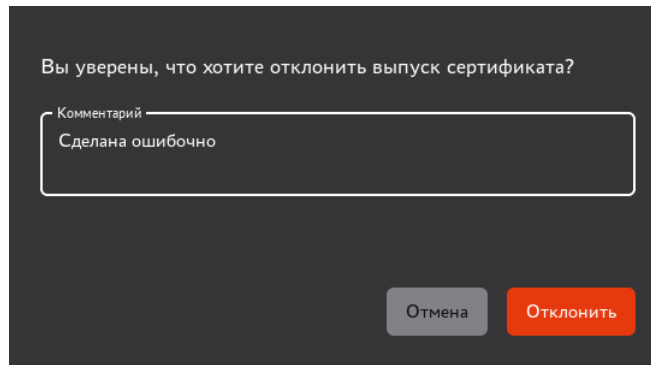


Рисунок 54 - Окно комментария к отклонению выпуска сертификата

- После подтверждения операции выбранное действие будет выполнено с заявкой, в результате чего её статус будет изменён.

Указанный комментарий будет отображаться в карточке заявки в поле «Комментарий».

В случае, если было выбрано действие «Выпустить сертификат», и выпуск не был завершён успешно (заявка в статусе «Ошибка выпуска»), будет доступно повторное выполнение данного сценария.

### 7.4.11 Импорт сертификата на ключевой носитель

Предварительные условия для импорта сертификата на ключевой носитель:

- На компьютере, с которого выполняется подключение к веб-интерфейсу eCA-RA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу eCA-RA, 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 eCA-RA и перейдите в раздел **Заявки**.
- Иницилируйте процесс импорта сертификата на ключевой носитель одним из следующих способов:
  - Найдите заявку в списке, щелкните в колонке **[Операции]** значок **<Операции строки>** и выберите в открывшемся списке **<Импортировать на КН>**.

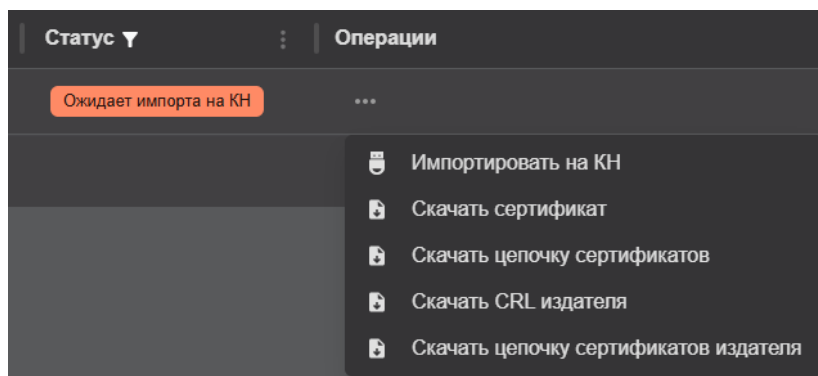


Рисунок 55 - Инициализация процесса импорта сертификата на ключевой носитель из списка

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

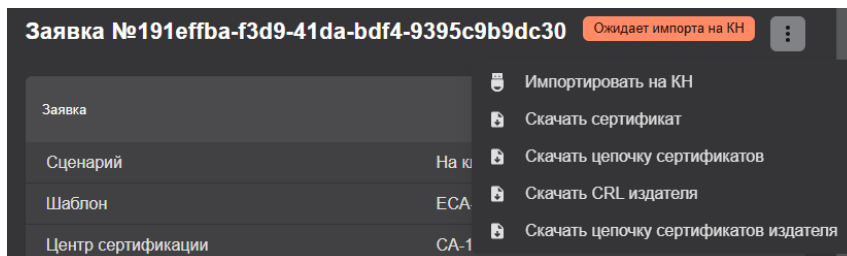


Рисунок 56 - Инициализация процесса импорта сертификата на ключевой носитель из карточки заявки

**Внимание!** Если JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 43) или к компьютеру не подключен ключевой носитель (см. Рисунок 44), создать заявку невозможно.

- В открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 57):
  - В списке «Устройство» выберите подключённый ключевой носитель.
  - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
  - Нажмите кнопку **Импортировать**.

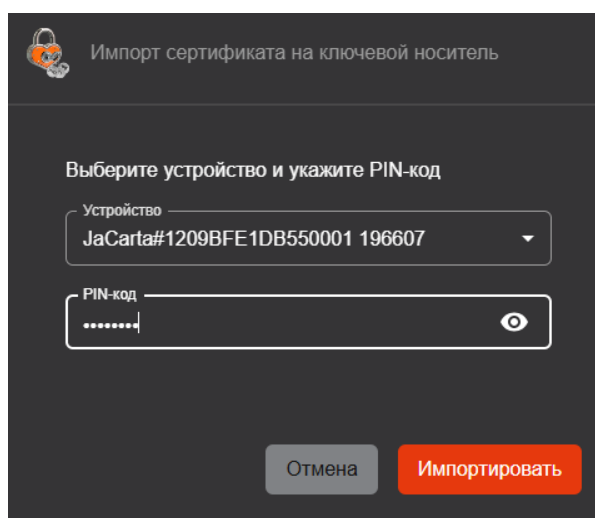


Рисунок 57 - Импорт сертификата на ключевой носитель

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».

еCA-RA 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 еCA-RA 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 58) проверьте данные сертификата и нажмите кнопку **Закрыть**.

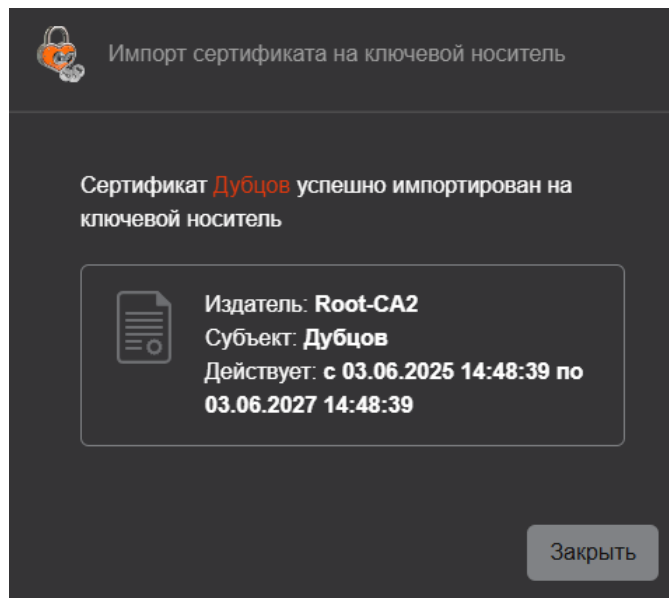


Рисунок 58 - Импорт сертификата на ключевой носитель успешно выполнен

#### 7.4.12 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 пользователя или устройства.

Для пользователя с ролью «Получатель сертификатов» доступен отзыв сертификатов, выпущенных только по собственным заявкам. Пользователю с ролью «Оператор» доступен отзыв сертификатов из заявок для субъектов, доступ к которым ему предоставлен в соответствии с правилами доступа, назначенными в eCA-CA, к которому подключен eCA-RA. Пользователю с ролью «Администратор» доступен отзыв сертификатов, выпущенных по любым заявкам.

Порядок отзыва сертификата:

- перейдите в раздел «Заявки» и найдите нужную заявку в списке;
- откройте карточку выбранной заявки;
- нажмите кнопку <Сертификат активирован> и выберите в контекстном меню «Сертификат отозван» (см. Рисунок 59);

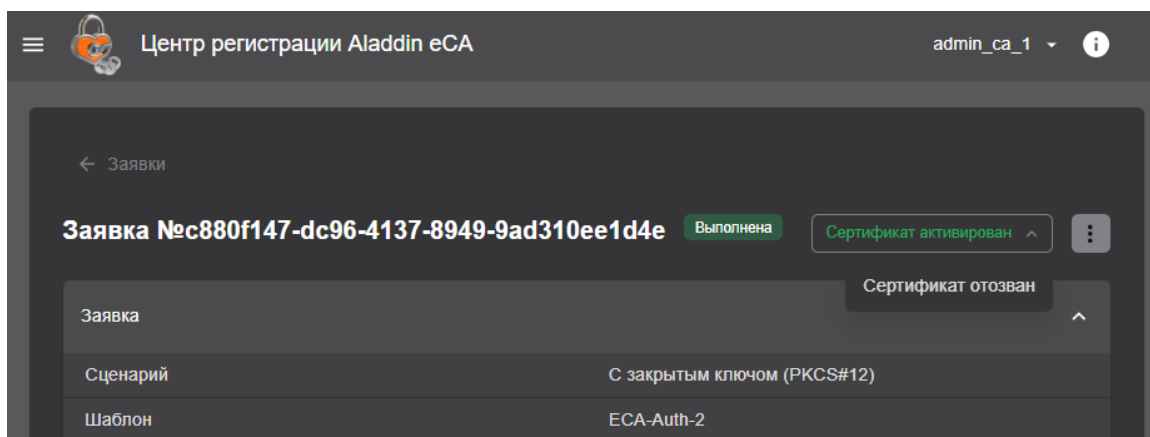



Рисунок 59 - Отзыв сертификата

- в открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в соответствующем поле и нажмите кнопку <Отозвать> (см. Рисунок 60);



### Отозвать сертификат?

Отзыв – это необратимая операция, которая может повлиять на работу пользователя или сервера.



Издатель: **Root-CA2**  
 Субъект: **петров**  
 Действует: с 18.03.2025 15:23:55 по 18.03.2027 15:23:55

Причина

Без указания причины

Комментарий \*



Компрометация

Отозвать

Отмена


Рисунок 60 - Указание причины отзыва сертификата

- В результате сертификат будет отозван.

Центр регистрации Aladdin eCA

dubtsov@al.rd.ru



← Заявки

**Заявка №647299fc-5650-43f7-ab0e-283aed67a633**

Выполнена

Сертификат отозван

Заявка

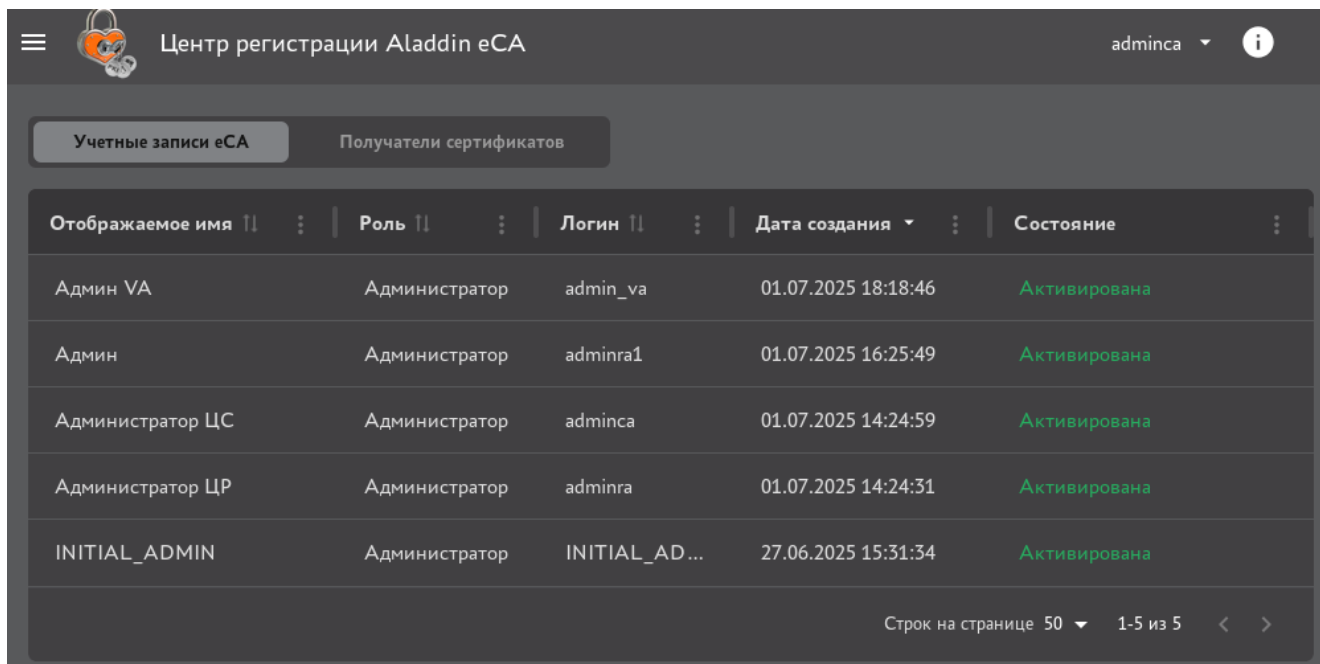
Сценарий

С закрытым ключом (PKCS#12)

Рисунок 61 -Сертификат отозван

## 7.5 Раздел «Учётные записи»

Раздел «Учётные записи» (см. Рисунок 62) предоставляет информацию об учётных записях eCA-RA, а также обеспечивает возможность блокировать и активировать учётные записи.



Отображаемое имя	Роль	Логин	Дата создания	Состояние
Админ VA	Администратор	admin_va	01.07.2025 18:18:46	Активирована
Админ	Администратор	adminra1	01.07.2025 16:25:49	Активирована
Администратор ЦС	Администратор	adminca	01.07.2025 14:24:59	Активирована
Администратор ЦР	Администратор	adminra	01.07.2025 14:24:31	Активирована
INITIAL_ADMIN	Администратор	INITIAL_AD...	27.06.2025 15:31:34	Активирована

Рисунок 62 - Экран раздела «Учётные записи». Вкладка «Учётные записи eCA»

На экране раздела «Учётные записи» отображаются следующие вкладки:

- «Учётные записи eCA».
- «Получатели сертификатов».

### 7.5.1 Вкладка «Учётные записи eCA»

На вкладке «Учётные записи eCA» в табличной форме отображена следующая информация об учётных записях из Центра сертификации, к которому подключён eCA-RA (см. Рисунок 62):

- отображаемое имя;
- роль (Оператор, Администратор);
- логин;
- дата создания;
- состояние (Активирована, Заблокирована).

Действия над учётными записями Центра сертификации Aladdin eCA производятся в eCA-CA (подробнее см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).

### 7.5.2 Вкладка «Получатели сертификатов»

На вкладке «Получатели сертификатов» в табличной форме отображена следующая информация о доменных учётных записях (см. Рисунок 63):

- отображаемое имя;
- дата создания;
- состояние (Активирована, Заблокирована).

На вкладке «Получатели сертификатов» доступны следующие действия:

- блокировка активированных учётных записей;

- активация заблокированных учётных записей.

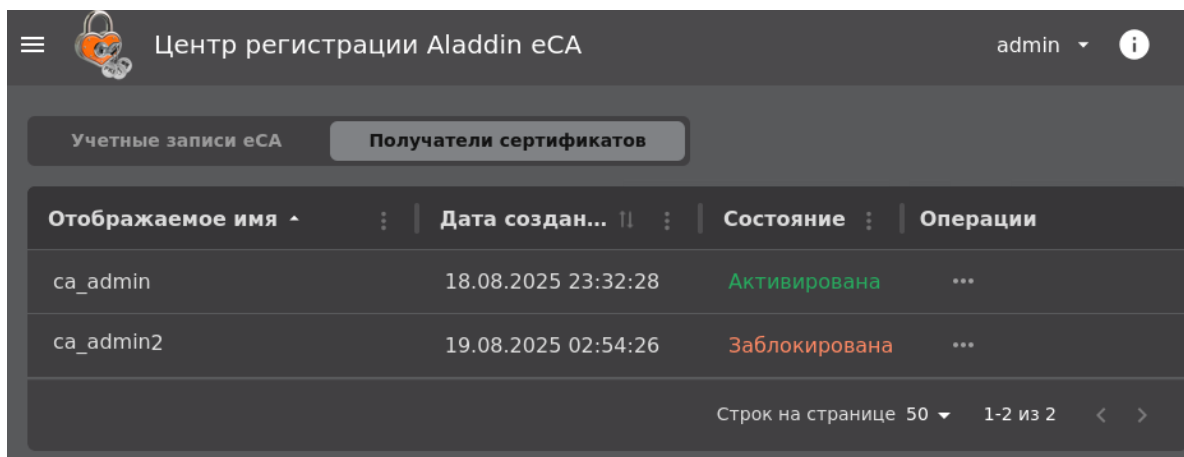


Рисунок 63 - Экран раздела «Учётные записи». Вкладка «Получатели сертификатов»

### 7.5.3 Блокировка доменной учётной записи

Администратор может заблокировать доменную учётную запись в состоянии «Активирована».

Для блокировки учётной записи найдите учётную запись, которую необходимо заблокировать, нажмите на кнопку <Операции> [...] и выберите опцию <Заблокировать> (см. Рисунок 64).

В результате блокировки доменной учётной записи:

- Все сессии данной учётной записи будут удалены из БД.
- Как следствие, при выполнении любых запросов (за исключением запросов на аутентификацию) будет выводиться ошибка: «Недействительный идентификатор сессии».
- Субъект заблокированной учётной записи не сможет выполнить вход в Центр регистрации - при аутентификации будет выводиться ошибка: «Аккаунт заблокирован».

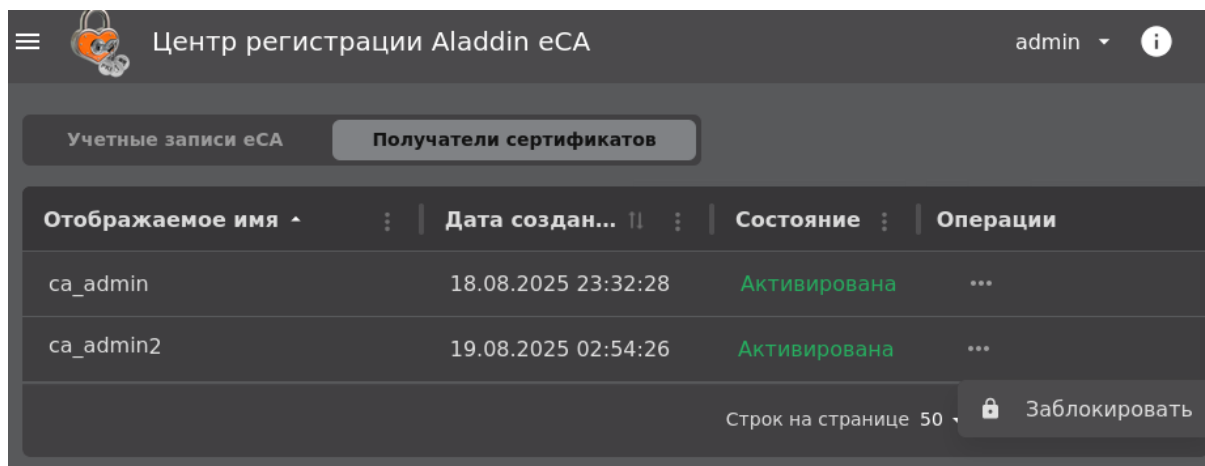


Рисунок 64 - Экран раздела «Учётные записи». Блокировка доменной учётной записи

### 7.5.4 Активация доменной учётной записи

Активация может быть выполнена для доменных учётных записей в состоянии «Заблокирована».

Для активации учётной записи найдите учётную запись, которую необходимо активировать, нажмите на кнопку <Операции> [...] и выберите опцию <Активировать> (см. Рисунок 65).

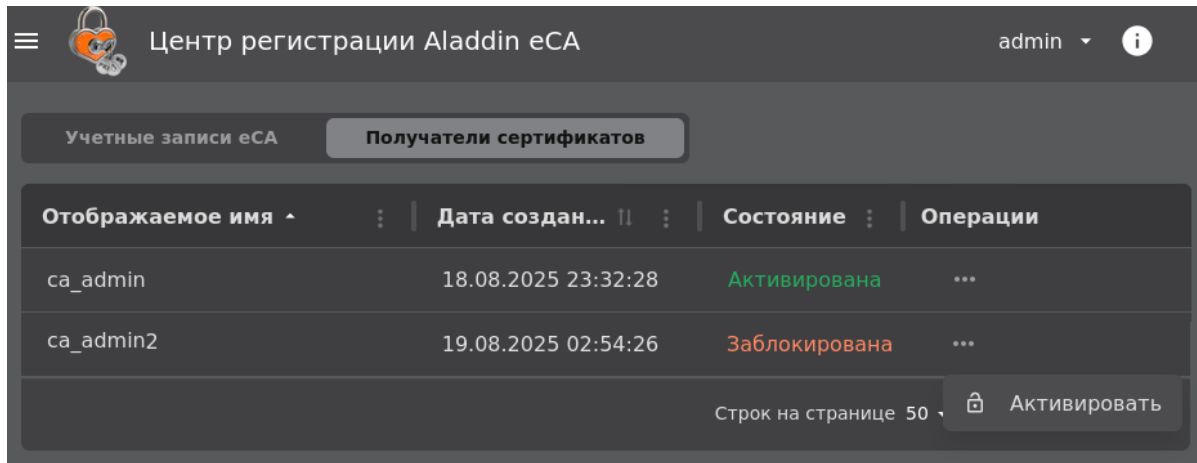


Рисунок 65 - Экран раздела «Учётные записи». Активация доменной учётной записи

## 7.6 Раздел «Журнал событий»

### 7.6.1 О журнале событий

Перечень событий приведён в приложении 6.

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


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

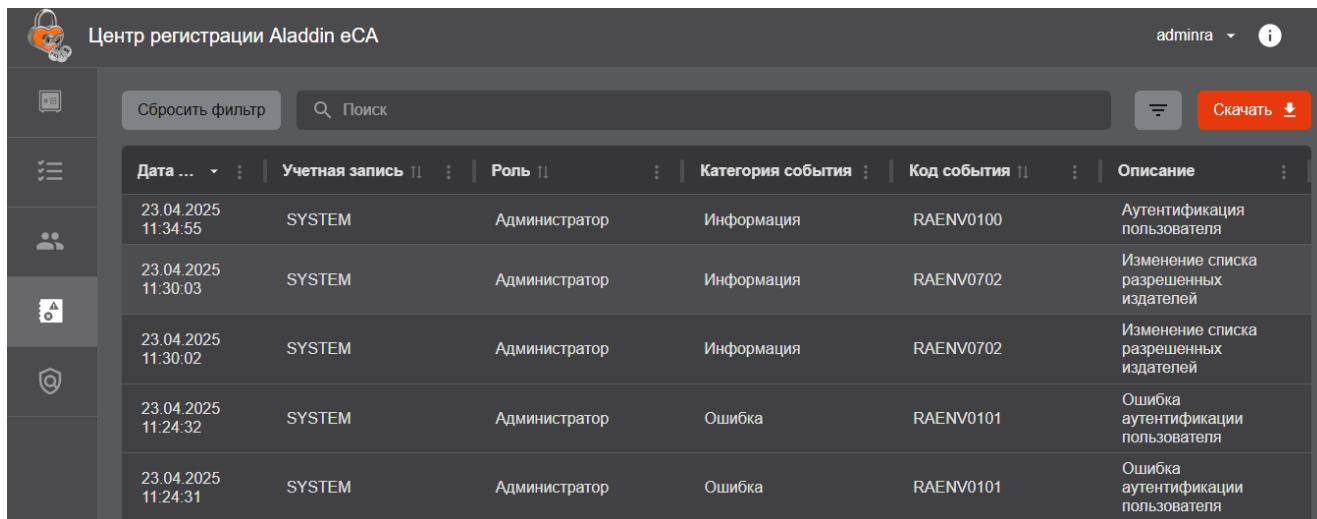
Архив в формате `.zip`, содержащий `.csv` файл, с именем `logs-<дата создания архива>.zip` будет сохранён в каталог, указанный в параметре `archive_path` конфигурационного файла (по умолчанию `/opt/aecaRa/dist/archive`).

### 7.6.2 Просмотр записей журнала событий

Данный раздел доступен для пользователей с ролями «Администратор» и «Оператор»:

- Для пользователя с ролью «Администратор» доступен просмотр всех событий журнала.
- Для пользователя с ролью «Оператор» 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 eCA-RA.

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



Дата ...	Учетная запись	Роль	Категория события	Код события	Описание
23.04.2025 11:34:55	SYSTEM	Администратор	Информация	RAENV0100	Аутентификация пользователя
23.04.2025 11:30:03	SYSTEM	Администратор	Информация	RAENV0702	Изменение списка разрешенных издателей
23.04.2025 11:30:02	SYSTEM	Администратор	Информация	RAENV0702	Изменение списка разрешенных издателей
23.04.2025 11:24:32	SYSTEM	Администратор	Ошибка	RAENV0101	Ошибка аутентификации пользователя
23.04.2025 11:24:31	SYSTEM	Администратор	Ошибка	RAENV0101	Ошибка аутентификации пользователя

Рисунок 66 - Просмотр записей журнала событий

Записи о событиях отображаются списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты событий:

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

Записи о событиях выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 67).

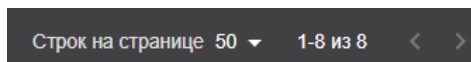









Рисунок 67 - Инструменты навигации

Описание инструментов навигации:

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

Для удобства анализа записей в списке вы можете управлять видимостью колонок таблицы. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок  **<Действие колонки>** и в открывшемся списке <sup>1</sup> выберите  **<Скрыть [название колонки] колонку>** (см. Рисунок 68). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок  **<Действие колонки>** и в открывшемся списке выберите  **<Показать все колонки>** (см. Рисунок 68).

<sup>1</sup> Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

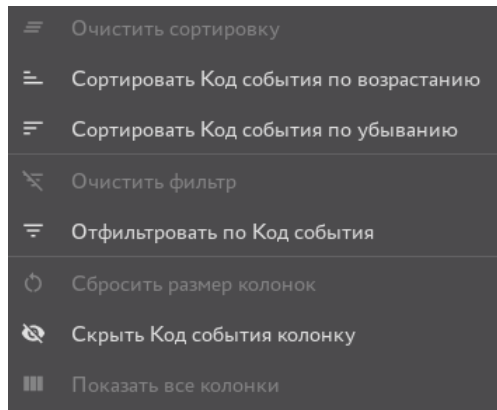


Рисунок 68 - Список действий с колонкой **[Код события]**

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 учётной записи инициатора события в алфавитном порядке.
- По роли инициатора события в алфавитном порядке.
- По коду события в порядке возрастания или убывания номера, содержащегося в коде.

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

Чтобы выполнить сортировку записей о событиях по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок ⓘ **<Действие колонки>** и в открывшемся списке <sup>1</sup> (см. Рисунок 68) 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 <sup>2</sup>:

- ▴ - сортировка выполнена в порядке возрастания.
- ▾ - сортировка выполнена в порядке убывания.
- ■ - сортировка не выполнена.

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




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


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

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

<sup>1</sup> Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

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

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку  **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок  **<Действие колонки>** и в открывшемся списке выберите  **<Отфильтровать по [название колонки]>** (см. Рисунок 68).

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

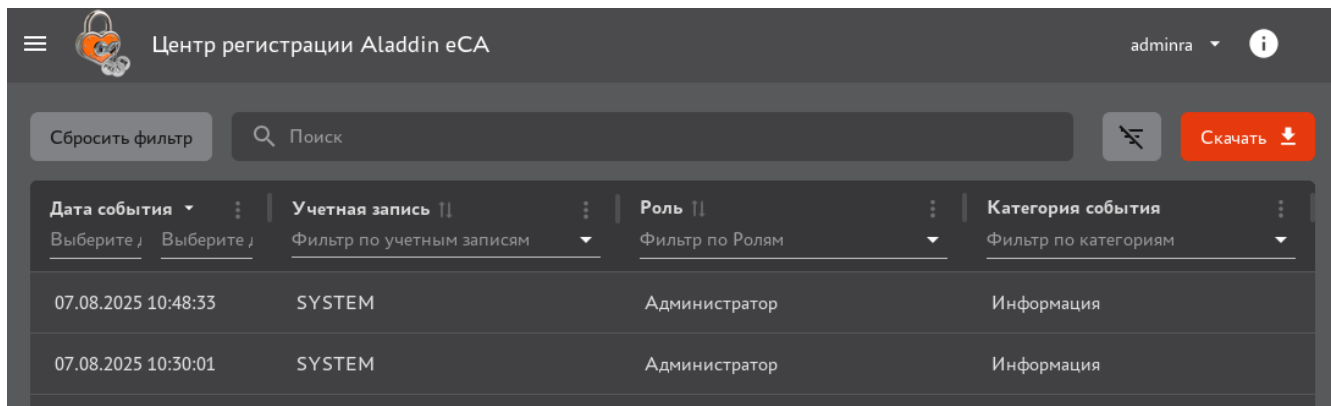






Рисунок 69 - Отображение фильтров в заголовках колонок включено


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 70а), **[Роль]** (см. Рисунок 70б), **[Категория события]** (см. Рисунок 70в) и **[Код события]** (см. Рисунок 70г) 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 70д), 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 70д).

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

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

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 .

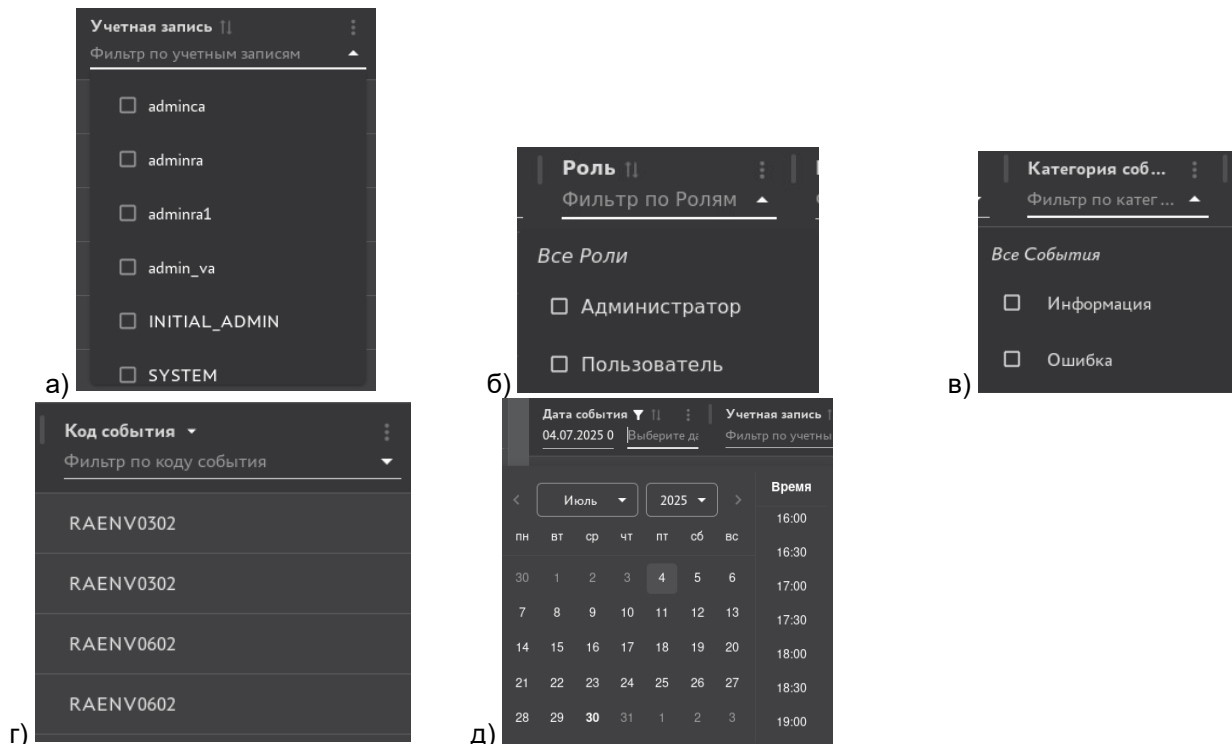


Рисунок 70 - Указание критериев выборки в фильтрах


### 7.6.3 Просмотр карточки события

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

Карточка события содержит подробную информацию о событии:

- В полях раздела «Общие сведения»:
  - «Идентификатор события»;
  - «Дата и время события»;
  - «Учётная запись» — инициатор события, логин учётной записи, действия которой повлекли событие (имя пользователя eCA-RA или «SYSTEM» для системных событий);
  - «Роль» — роль инициатора события. Для системных событий должна быть указана роль «ADMINISTRATOR»;
  - «IP-адрес источника» — IP-адрес инициатора события. Для системных событий значение в данном поле может отсутствовать;
  - «Категория события» — «INFO» для информационных событий или «ERROR» для ошибок;
  - «Код События» — (см. приложение 6);
  - «Описание» — описание события с атрибутами (см. приложение 6).
- В разделе «Подробности». Состав полей раздела «Подробности» соответствует составу полей списка «Атрибуты» в столбце «Описание в журнале» таблиц, представленных в приложении 6.

Чтобы открыть карточку события:

- Подключитесь к веб-интерфейсу eCA-RA и перейдите в раздел  **Журнал событий**.
- Найдите нужное событие и щёлкните запись о нем в списке (см. Рисунок 71).



Свойства события - 04.11.2025 15:31:34

Общие сведения

Идентификатор события	8e19c5e2-e167-41da-9734-f0f76760900e
Дата события	04.11.2025 15:31:34
Учетная запись	SYSTEM
Роль	Администратор
IP-адрес источника	192.168.0.104
Категория события	Информация
Код События	RAENV0100
Описание	Аутентификация пользователя

Подробности

Id пользователя	3d9b40c3-903b-4e11-894b-df772b030302
Отображаемое имя пользователя	INITIAL_ADMIN
Роль пользователя	ADMINISTRATOR
IP адрес	192.168.0.104
Аутентификатор	1a028620-4ee3-4930-884e-271c7974b829
Тип аутентификации	CERTIFICATE

Копировать Закрыть

Рисунок 71 — Окно «Свойства события» (карточка события)

Для копирования информации о событии в буфер обмена нажмите кнопку Копировать.

#### 7.6.4 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 eCA-RA 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)**.

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


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

Значения полей отправляемых Syslog-сообщений о зарегистрированных событиях представлены в таблице ниже.

Таблица 15 - Значения полей отправляемых Syslog-сообщений

Поле сообщения	Описание	Значение
PRIVAL	Priority Value - значение, вычисляемое на основе категории и важности события	Для информационных событий - 14, для ошибок - 11

Поле сообщения	Syslog-Описание	Значение
VERSION	Версия используемого стандарта Syslog	1
TIMESTAMP	Временная метка в соответствии с RFC3339	Текущее время на хосте eCA-RA в формате ISO 8601: YYYY-MM-DDThh:mm:ss[.SSS]
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста eCA-RA
APP-NAME	Тег, указывающий приложение или процесс, создавшего сообщение	AECA-RA
PROCID	Идентификатор процесса (PID) приложения	PID сервиса, являющегося источником события
MSGID	Идентификатор сообщения	Код события
[STRUCTURED-DATA]	Структурированные данные	<pre>[aece-ra eventId="eventId" actionCode="actionCode" category="category" id="id" serviceName="serviceName" system="system" username="username" role="role" ipAddress="ipAddress" attributes="attributes"]</pre> <p>где:</p> <ul style="list-style-type: none"> <li>– "eventId" – идентификатор события;</li> <li>– "actionCode" - код события;</li> <li>– "category" - категория события;</li> <li>– "id" - идентификатор типа события;</li> <li>– "serviceName" - имя сервиса, в котором произошло событие;</li> <li>– "system" - флаг системного события;</li> <li>– "username" - логин учётной записи инициатора события;</li> <li>– "role" - роль инициатора события;</li> <li>– "ipAddress" - IP-адрес инициатора события;</li> <li>– "attributes" - расширенное описание события. Состав полей расширенного описания события соответствует составу полей описания события, указанному в приложении 6</li> </ul>
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»).

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

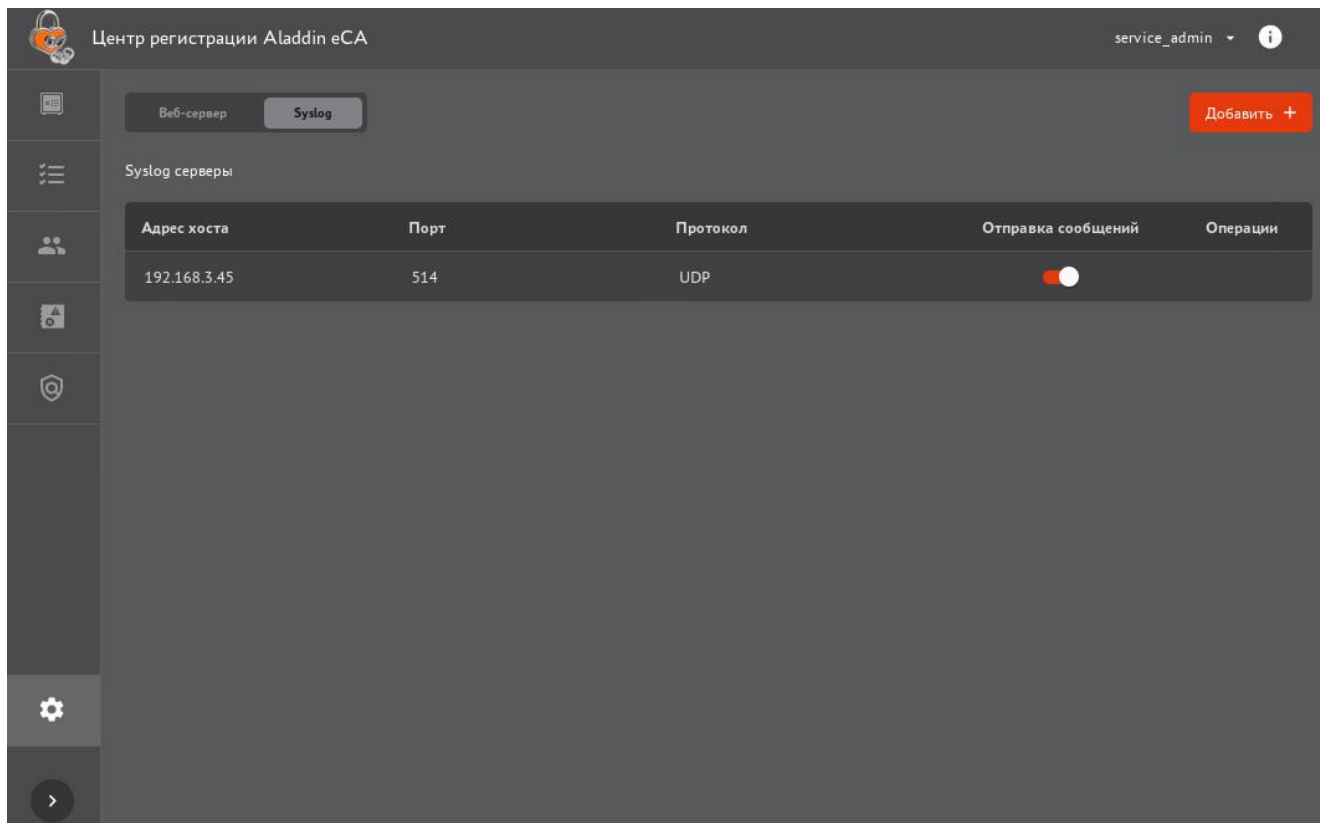


Рисунок 72 - Просмотр списка Syslog-серверов

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

- Адрес хоста - IP-адрес или доменное имя Syslog-сервера.
- Входящий порт Syslog-сервера, на который отправляются сообщения (число в диапазоне от 1 до 65535).
- Транспортный протокол, по которому выполняется передача данных.

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

Порядок добавления Syslog-сервера:

- На панели инструментов нажмите кнопку **Добавить +**.
- В открывшемся окне (см. Рисунок 73) выполните следующие действия:
  - В поле «Адрес хоста» укажите IP-адрес или доменное имя Syslog-сервера.
  - В поле «Порт» укажите входящий порт Syslog-сервера, на который будут отправляться сообщения (число в диапазоне от 1 до 65535).
  - В списке «Протокол» выберите транспортный протокол, по которому будет выполняться передача данных: UDP, TCP или TCP (TLS).
  - Нажмите кнопку **Добавить**.

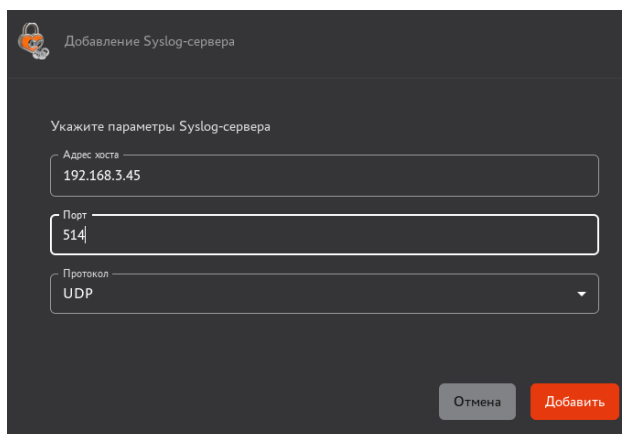






Рисунок 73 - Добавление Syslog-сервера

Если в качестве протокола используется TCP (как с TLS, так и без него), то при добавлении Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения новый Syslog-сервер не будет добавлен.

Чтобы изменить настройки Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Редактировать>** (Рисунок 74) и в открывшемся окне измените параметры Syslog-сервера.

Если в качестве протокола используется TCP (как с TLS, так и без него), то при изменении параметров Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения параметры Syslog-сервер не будут изменены.

Чтобы удалить Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Удалить>** (Рисунок 74) и в открывшемся окне подтвердите удаление Syslog-сервера.

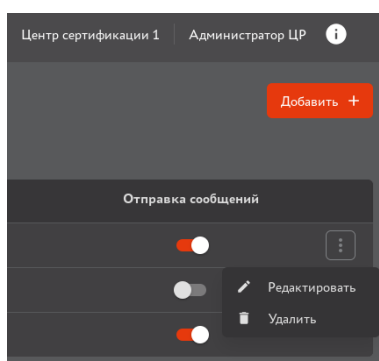


Рисунок 74 - Выбор действия с Syslog-сервером

## 7.7 Раздел «Управление»

Раздел «Управление» содержит вкладки «Правила выпуска» и «SCEP» (см. Рисунок 75). Данный раздел доступен только для администратора.

### 7.7.1 Вкладка «Правила выпуска»

Вкладка «Правила выпуска» (см. Рисунок 75) раздела «Управление» обеспечивает возможности создания, изменения, удаления правил выпуска сертификатов, также управления статусами правил выпуска.

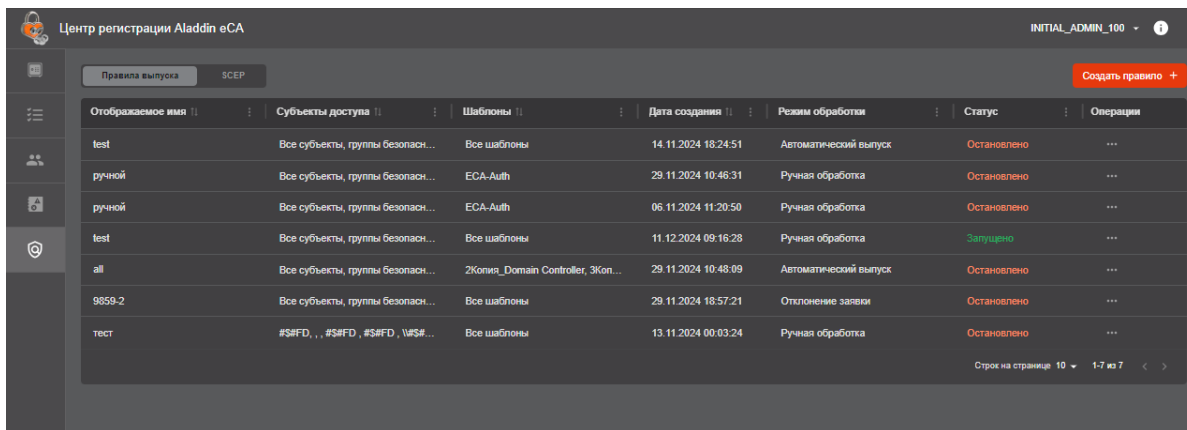


Рисунок 75 - Экран раздела «Управление». Вкладка «Правила выпуска»

Во вкладке «Правила выпуска» раздела «Управление» в табличной форме отображена информация о существующих правилах выпуска, представленная в таблице 16.

Таблица 16 - Описание полей таблицы «Правил выпуска сертификатов»

Поле	Описание
Отображаемое имя	Содержит отображаемое имя правила
Субъекты доступа	Содержит перечень субъектов и групп безопасности, являющихся субъектами доступа по данному правилу. Для групп безопасности указан домен, которому они принадлежат. В данном поле может содержаться значение «Все субъекты», обозначающее, что субъектами доступа по правилу являются все субъекты и группы безопасности еCA-CA, к которому подключён еCA-RA, включая локальных субъектов
Шаблоны	Содержит перечень шаблонов правила выпуска. В данном поле может содержаться значение «Все шаблоны», если при создании правила выпуска на шаге выбора шаблонов была выбрана опция «Все шаблоны»
Дата создания	Содержит дату и время создания правила выпуска
Режим обработки	Содержит режим обработки заявки по правилу выпуска. Допустимые значения в поле: «Автоматический выпуск», «Ручная обработка», «Отклонение заявки»
Статус	Содержит статус правила выпуска. Допустимые значения в поле: «Запущено», «Остановлено»

Во вкладке «Правила выпуска» раздела «Управление» доступны следующие действия:

- Создание нового правила выпуска;
- Редактирование правила выпуска;
- Запуск и остановка правила выпуска;
- Копирование правила выпуска;
- Удаление правила выпуска.

#### 7.7.1.1 Управление экранной таблицей

Для каждой колонки экранной таблицы (справа от названия заголовка) доступна кнопка управления действиями «Действия в колонке». По нажатию данной кнопки разворачивается меню (см. Рисунок 76), в котором возможно (в зависимости от применённых ранее действий - фильтр, сортировка, изменение ширины, скрытие колонки):

- очистить сортировку, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
- сортировать по возрастанию/убыванию значений в колонке;
- сбросить размер колонок, сбросив ширину колонок к значению «по умолчанию»;
- скрыть колонку из отображаемых на экране;

- показать все колонки, отобразив на экране ранее скрытые колонки.

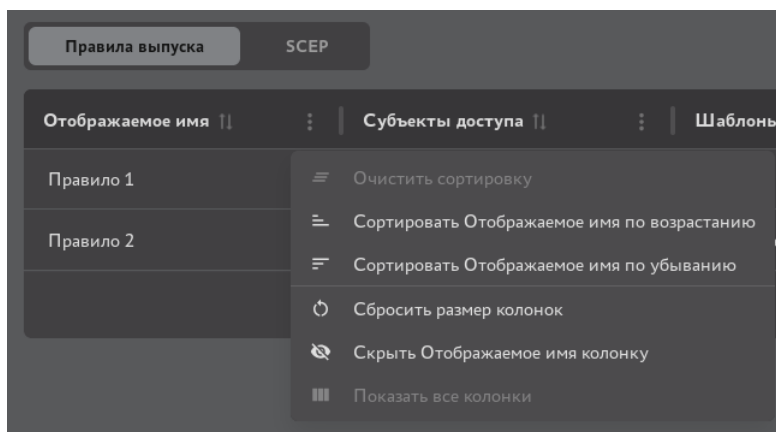


Рисунок 76 - Кнопка <Действия в колонке>

### 7.7.1.2 Сортировка правил

Средства сортировки правил в разделе «Правила выпуска» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 77)

- Отображаемое имя - упорядочивание осуществляется в алфавитном порядке.
- Субъекты доступа - упорядочивание осуществляется в алфавитном порядке.
- Шаблоны - упорядочивание осуществляется в алфавитном порядке.
- Дата создания - упорядочивание выполняется по дате и времени создания правила в порядке убывания или возрастания временных меток.

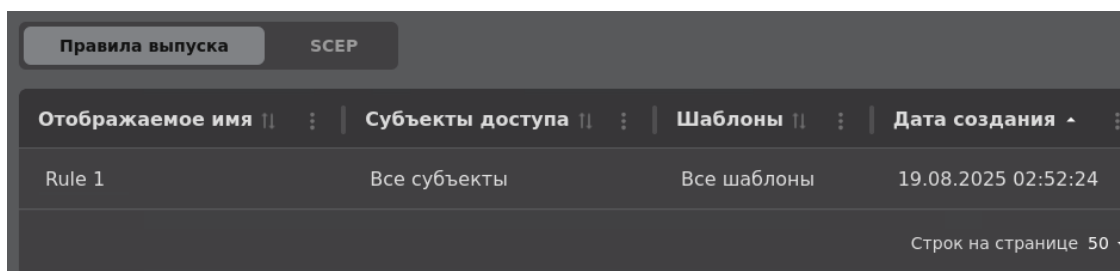




Рисунок 77 - Поля сортировки содержимого экрана раздела «Правила выпуска»

Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки>.

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

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

Для сброса сортировки в каждой колонке:

- нажмите кнопку  <Действия в колонке> и в раскрывшемся списке выберите пункт «Очистить сортировку»;
- или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

### 7.7.1.3 Создание правила выпуска

Для создания правила выпуска выполните следующие шаги:

- Нажмите кнопку <Создать правило +> на главном экране раздела «Управление» (см. Рисунок 75).
- В открывшемся окне укажите отображаемое имя для создаваемого правила выпуска (см. Рисунок 78). Далее нажмите кнопку <Продолжить> для перехода к следующему шагу.

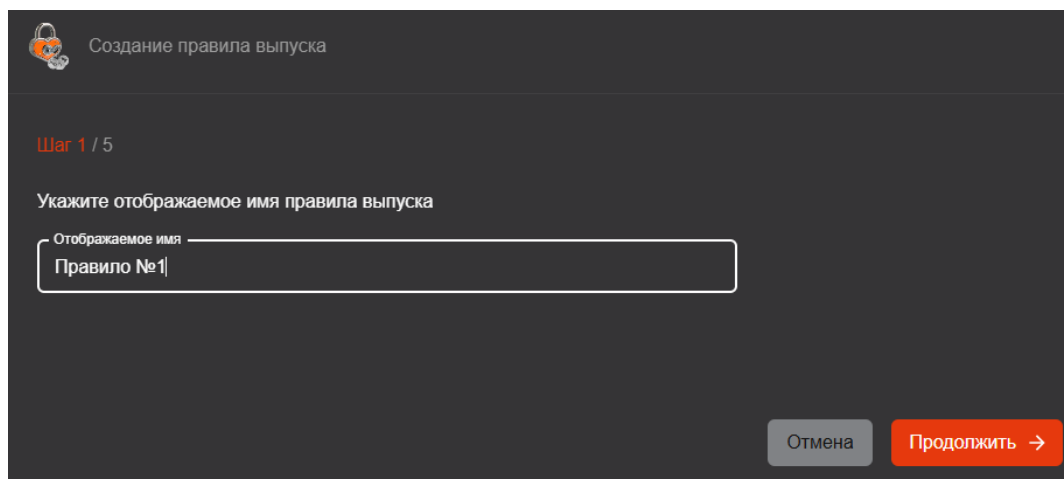


Рисунок 78 - Окно создания правила выпуска. Шаг 1. Отображаемое имя

- На втором шаге выберите субъекты доступа для создаваемого правила. Допустимые варианты выбора субъектов доступа:
  - «Все субъекты» (см. Рисунок 79). При выборе данного значения субъектами доступа будут являться все субъекты и группы безопасности ресурсных систем еСА-СА, к которому подключён еСА-РА, включая локальную ресурсную систему. При выборе данного значения указание отдельных субъектов или групп безопасности на данном шаге будет недоступно;

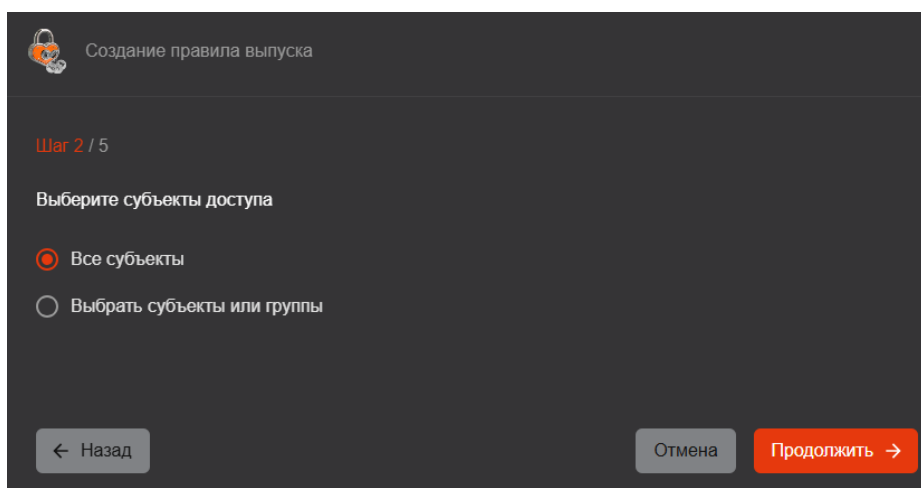


Рисунок 79 - Окно создания правила выпуска. Шаг 2. Выбор субъектов - Все субъекты

«Выбрать субъекты или группы» (см. Рисунок 80). При выборе данного значения становится доступен выбор типа (субъекты или группы), а также домена. Вложенные группы не наследуют правила выпуска от вышестоящих групп. Выбранные субъекты доступа необходимо перенести в правый столбец («Выбрано») путём нажатия на стрелку вправо. В случае, если в правый столбец («Выбрано») не добавлен ни один субъекта доступа, переход на следующий шаг недоступен.

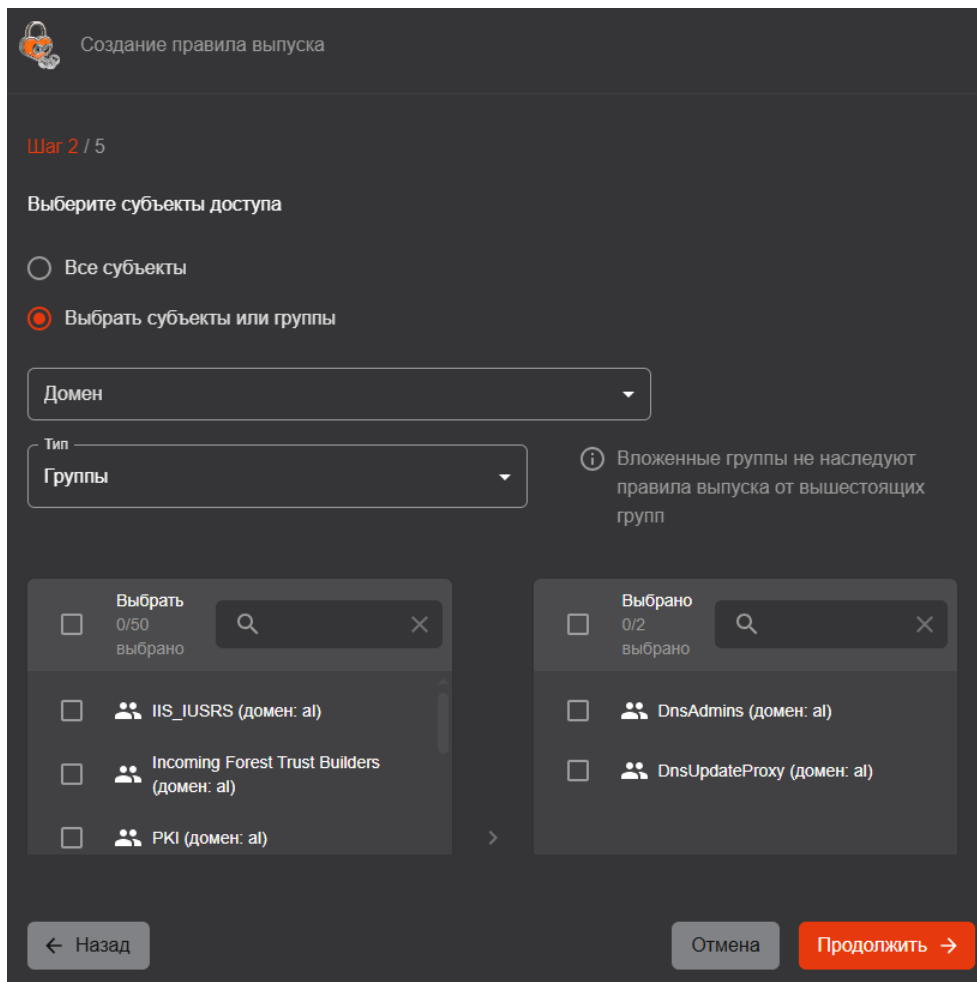


Рисунок 80 - Окно создания правила выпуска. Шаг 2. Выбор субъектов - Выбрать субъекты

- Для перехода к следующему шагу нажмите на кнопку <Продолжить>.
- На третьем шаге выберите шаблоны для создаваемого правила выпуска. Доступны следующие варианты выбора шаблонов для правила выпуска:
  - «Все шаблоны» (см. Рисунок 81). При выборе данного значения объектами доступа будут являться все шаблоны (в том числе те, которые будут созданы в eCA-CA позднее). При выборе данного значения указание отдельных шаблонов на данном шаге будет недоступно.

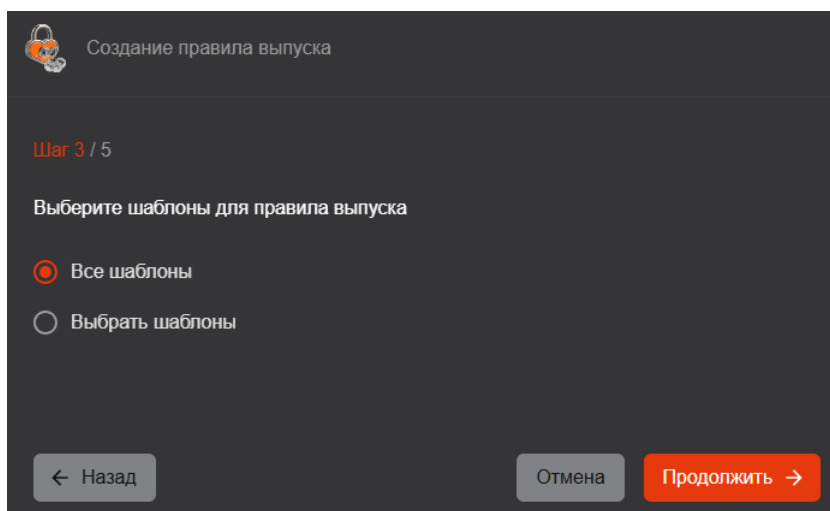


Рисунок 81 - Окно создания правила выпуска. Шаг 3. Выбор шаблонов - Все шаблоны

- «Выбрать шаблоны» (см. Рисунок 82). При выборе данного значения пользователю доступен выбор шаблонов.



Выбранные шаблоны необходимо перенести в правый столбец («Выбрано») путём нажатия на стрелку вправо.

В случае, если в правый столбец («Выбрано») не добавлен ни один шаблон, переход на следующий шаг недоступен.

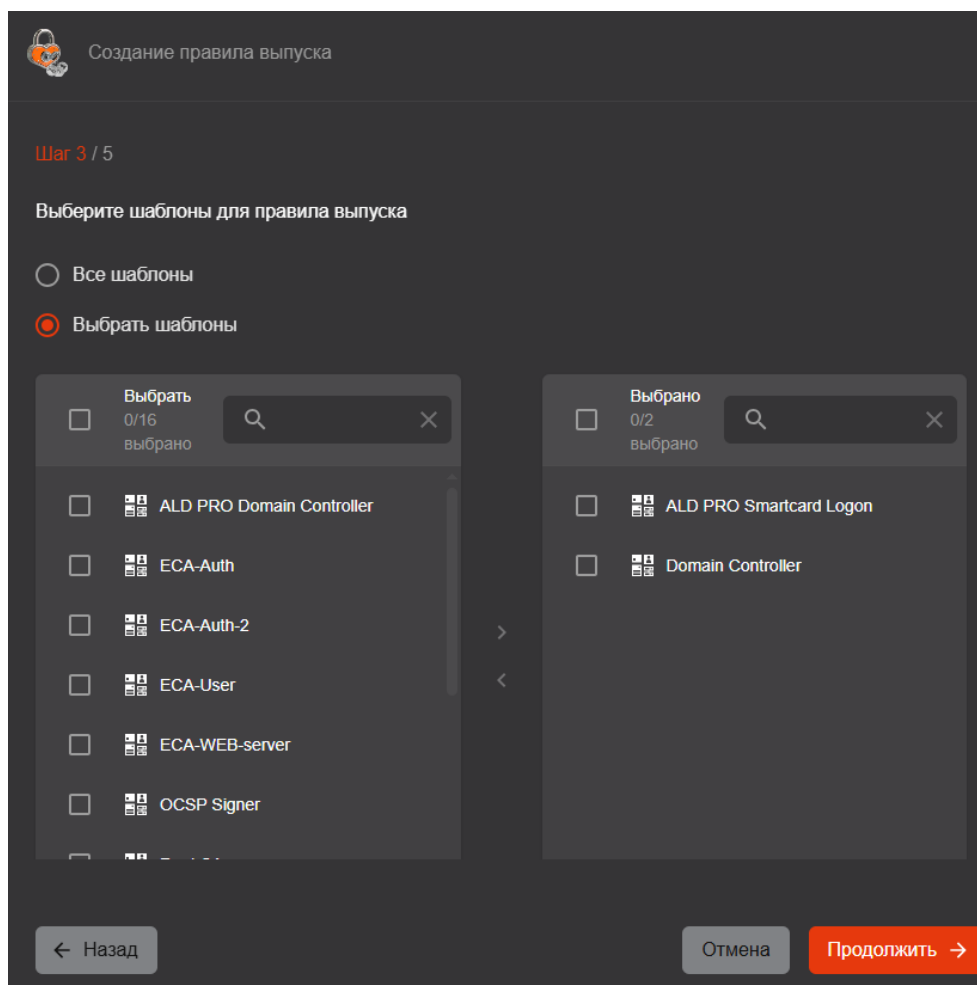


Рисунок 82 - Окно создания правила выпуска. Шаг 3. Выбор шаблонов - Выбрать шаблоны

- Для перехода к следующему шагу нажмите на кнопку <Продолжить>.
- На четвёртом шаге выберите режим обработки заявок для создаваемого правила выпуска (см. Рисунок 82). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка», «Отклонение заявки».

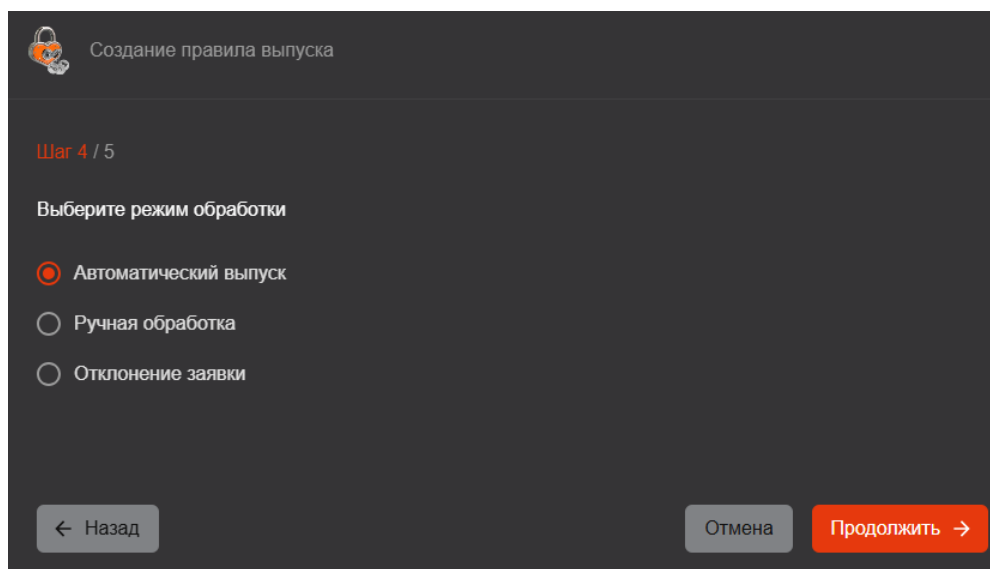


Рисунок 83 - Окно создания правила выпуска. Шаг 4. Выбор режима обработки

- Для перехода к следующему шагу нажмите на кнопку <Продолжить>.
- На пятом шаге отображена информация о создаваемом правиле выпуска, включающая в себя отображаемое имя, перечень выбранных субъектов доступа, шаблонов и режим обработки по правилу (см. Рисунок 84).

Создание правила выпуска

Шаг 5 / 5

Просмотр и подтверждение правила предоставления доступа

Отображаемое имя  
Правило 3

Субъекты доступа  
Все субъекты

Шаблоны  
Все шаблоны

Режим обработки  
Ручная обработка

← Назад      Отмена      Создать правило

Рисунок 84 - Окно создания правила выпуска. Шаг 5. Подтверждение перед созданием

- Для создания правила выпуска нажмите на кнопку <Создать правило>. После этого окно создания закроется, и созданное правило выпуска появится в списке правил выпуска в разделе «Управление».

#### 7.7.1.4 Редактирование правила выпуска

Для редактирования правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо отредактировать, нажмите на кнопку <Операции> [...] и выберите опцию <Редактировать> (см. Рисунок 85).

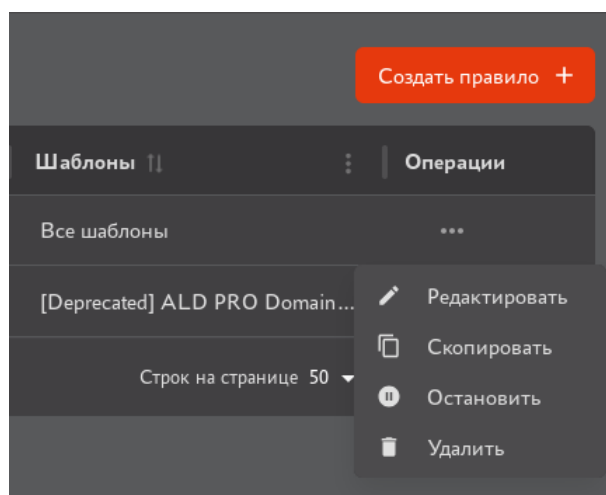


Рисунок 85 - Экран раздела «Управление». Вкладка «Правила выпуска». Редактирование правила выпуска

- В открывшемся окне «Редактирование правила выпуска» на первом шаге осуществляется редактирование отображаемого имени правила выпуска (см. Рисунок 86).

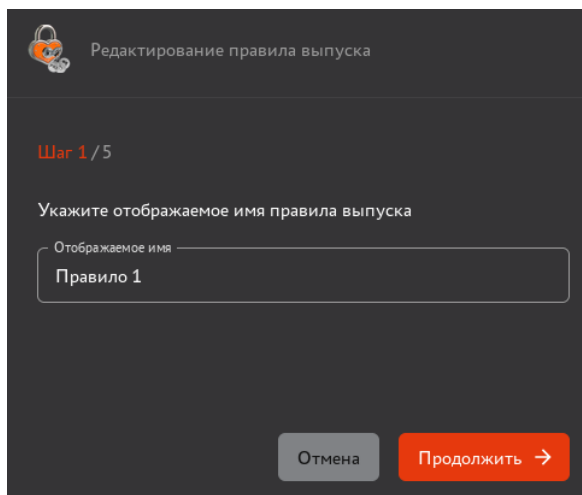


Рисунок 86 - Окно редактирования правила выпуска. Шаг 1. Отображаемое имя

- Далее нажмите кнопку <Продолжить> для перехода к следующему шагу.
- На шаге 2 окна «Редактирование правила выпуска» осуществляется редактирование субъектов доступа для правила выпуска (см. Рисунок 87 и Рисунок 88). Редактирование субъектов доступа для правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.3). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

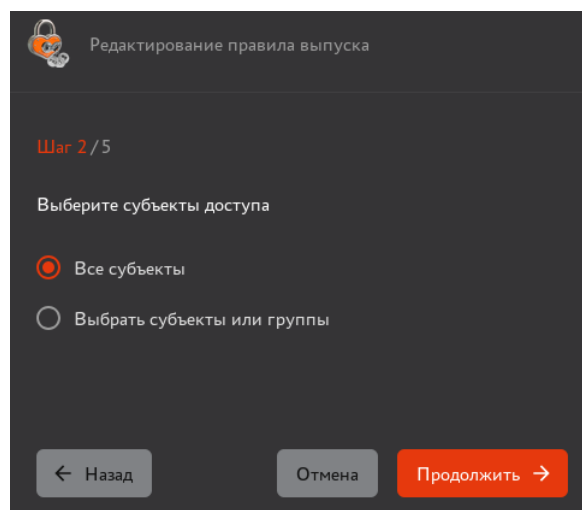


Рисунок 87 - Окно редактирования правила выпуска. Шаг 2. Выбор субъектов - Все субъекты

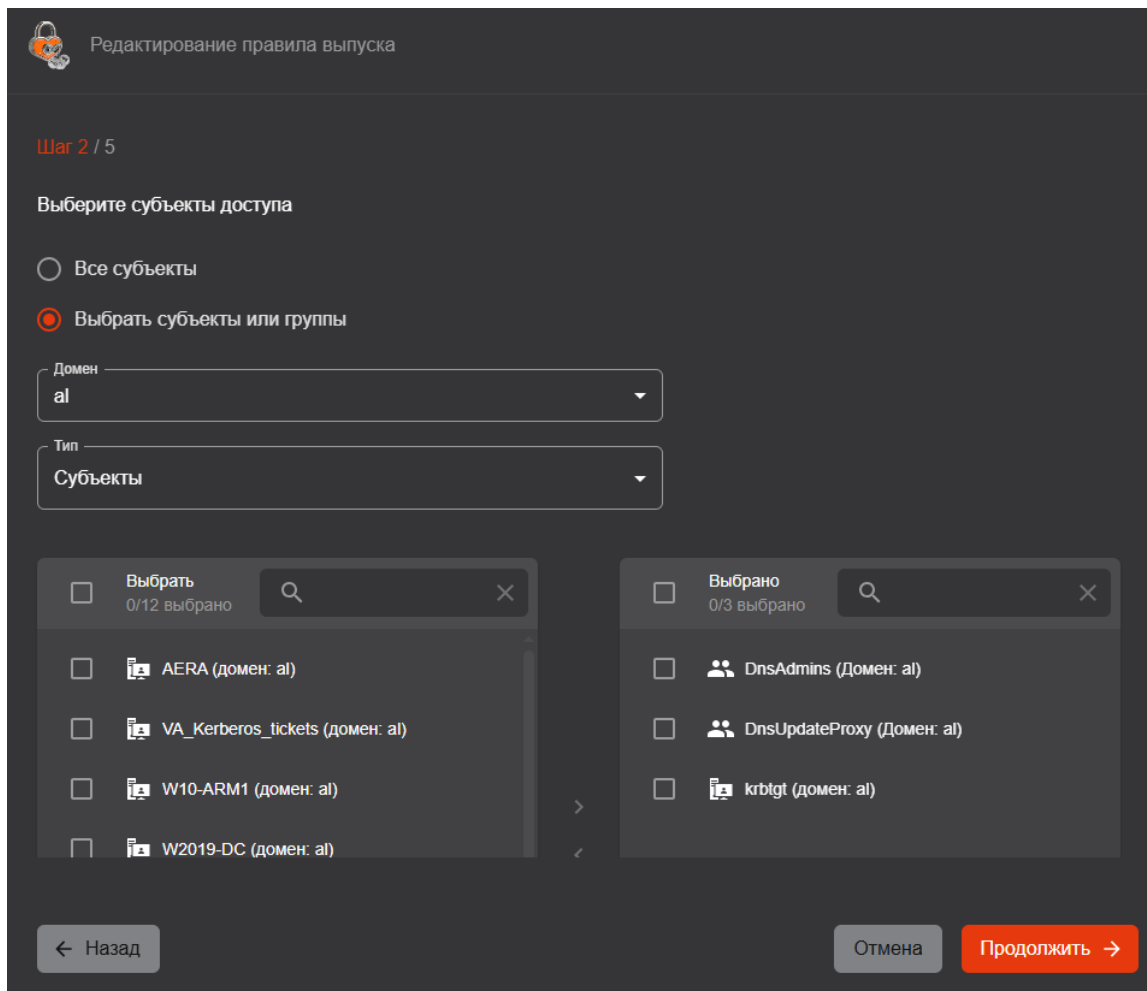


Рисунок 88 - Окно редактирования правила выпуска. Шаг 2. Выбор субъектов - Выбрать субъекты

- На шаге 3 окна «Редактирование правила выпуска» осуществляется редактирование шаблонов для правила выпуска (см Рисунок 89 и Рисунок 91). Редактирование перечня шаблонов правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.3). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

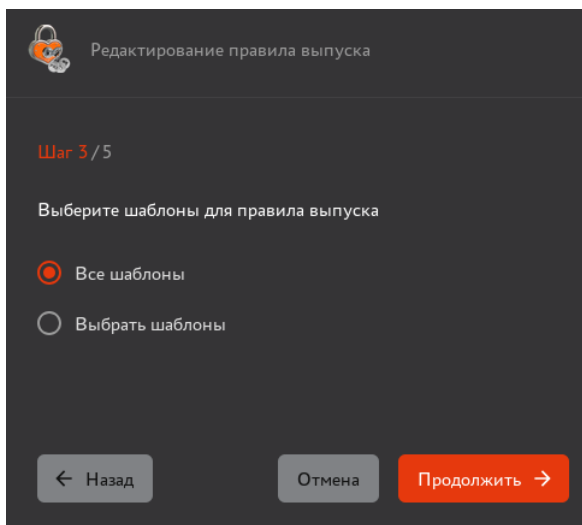


Рисунок 89 - Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов - Все шаблоны

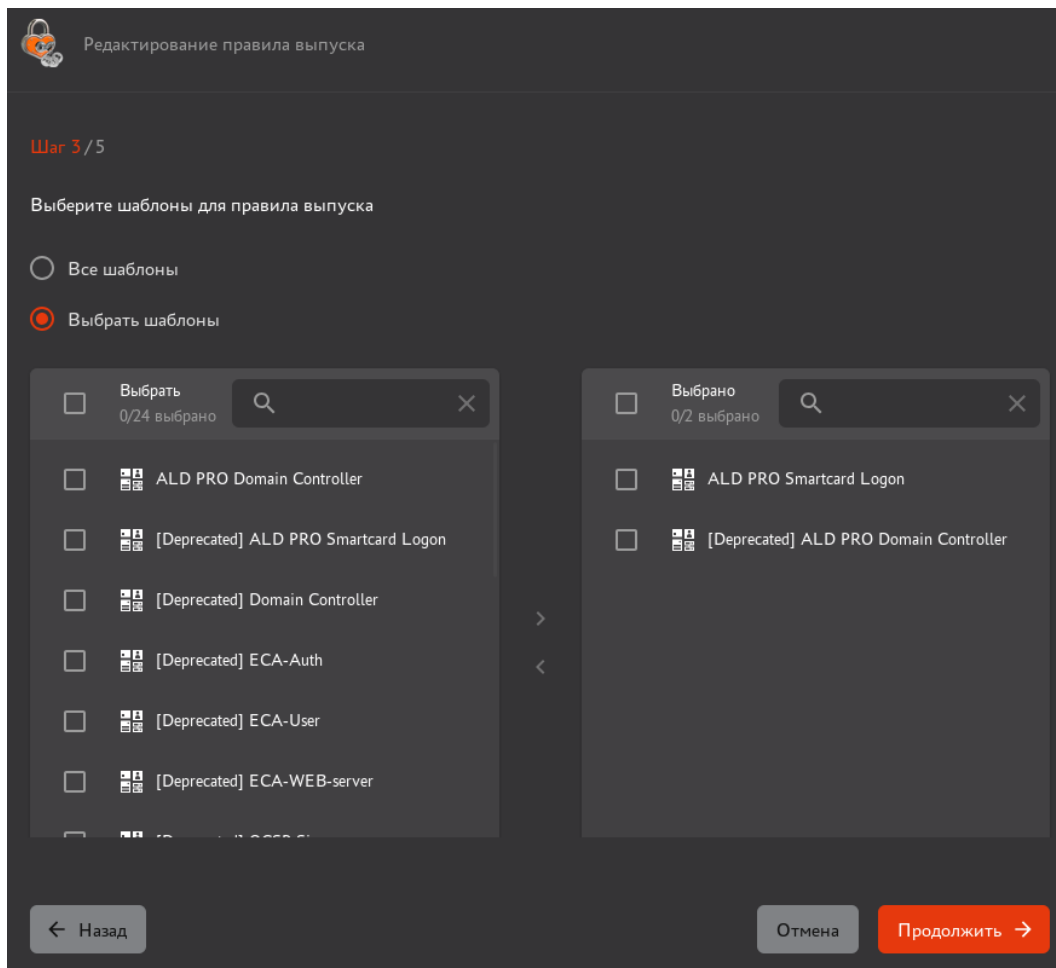


Рисунок 90 - Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов - Выбрать шаблоны

- На шаге 4 окна «Редактирование правила выпуска» осуществляется редактирование режима обработки заявок для правила выпуска (см. Рисунок 91). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка» и «Отклонение заявки».

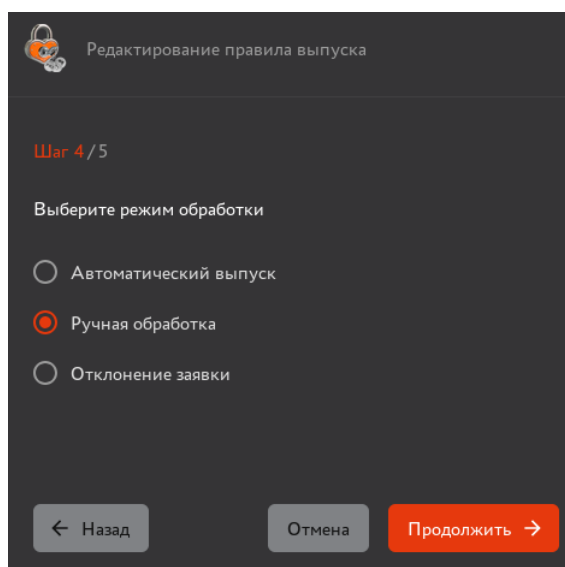


Рисунок 91 - Окно редактирования правила выпуска. Шаг 4. Выбор режима обработки

- На шаге 5 окна «Редактирование правила выпуска» отображена информация об отредактированном правиле выпуска, включающая в себя отображаемое имя, перечень субъектов доступа, шаблонов и режим обработки по правилу (см. Рисунок 92).

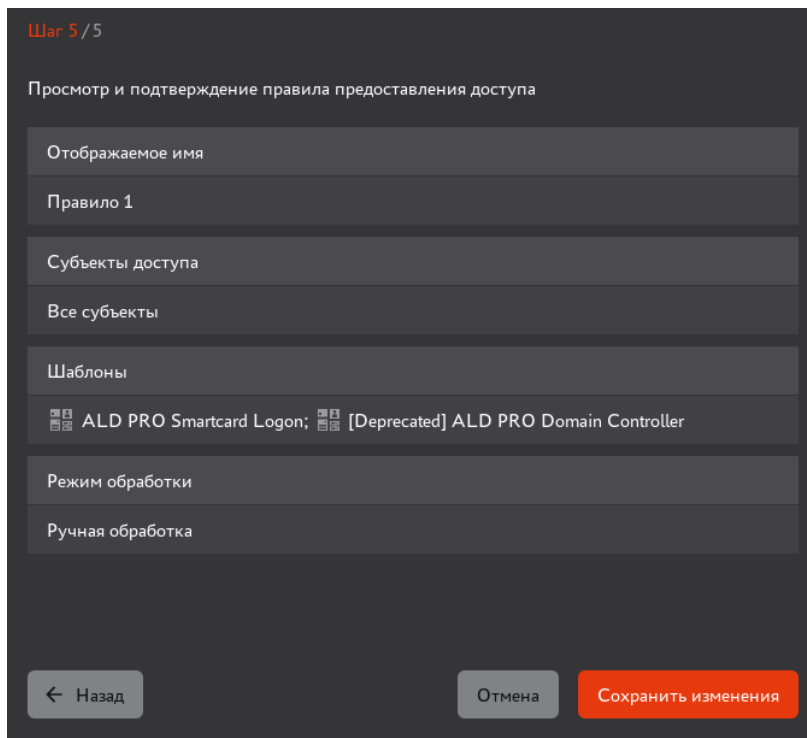


Рисунок 92 - Окно редактирования правила выпуска. Шаг 5. Подтверждение

- После нажатия на кнопку «Сохранить изменения» отредактированное правило выпуска будет обновлено.

#### 7.7.1.5 Запуск правила выпуска

Запуск может быть выполнен только для правил выпуска в статусе «Остановлено».

Для запуска правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо запустить, нажмите на кнопку «Операции» и выберите опцию «Запустить» (см. Рисунок 93).

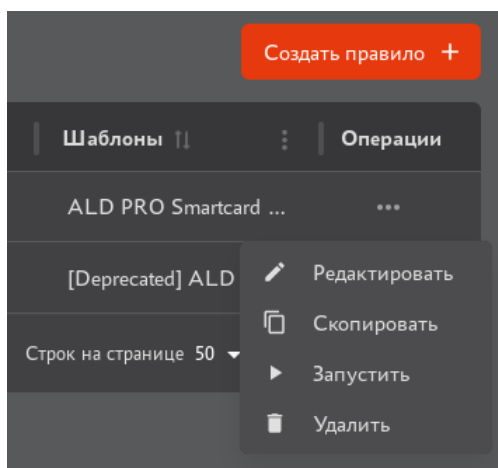


Рисунок 93 - Экран раздела «Управление». Вкладка «Правила выпуска». Запуск правила выпуска

- В появившемся окне подтверждения операции запуска (см. Рисунок 94) нажмите на кнопку «Запустить». После нажатия на неё правило выпуска будет запущено и будет использоваться при обработке заявок.

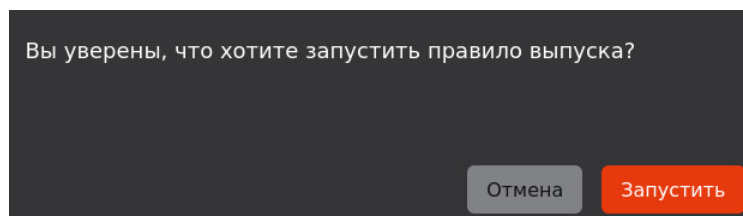



Рисунок 94 - Окно подтверждения запуска правила выпуска

### 7.7.1.6 Остановка правила выпуска

Остановка может быть выполнена только для правил выпуска в статусе «Запущено».

Для остановки правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо остановить, нажмите на кнопку <Операции>  и выберите опцию <Остановить> (см. Рисунок 95).

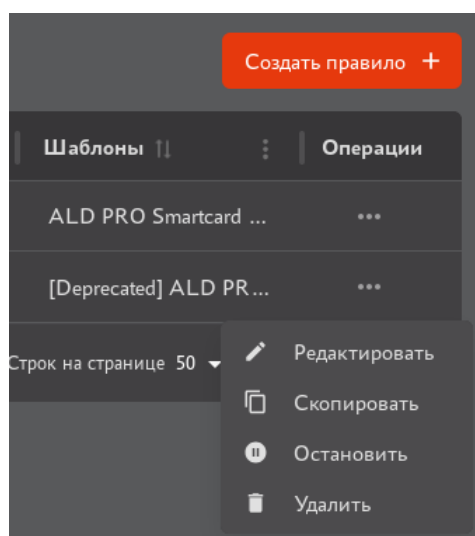


Рисунок 95 - Экран раздела «Управление». Вкладка «Правила выпуска». Остановка правила выпуска

- В появившемся окне подтверждения операции остановки (см. Рисунок 96) нажмите на кнопку <Остановить>. После нажатия на неё правило выпуска будет остановлено и не будет использоваться при обработке заявок.

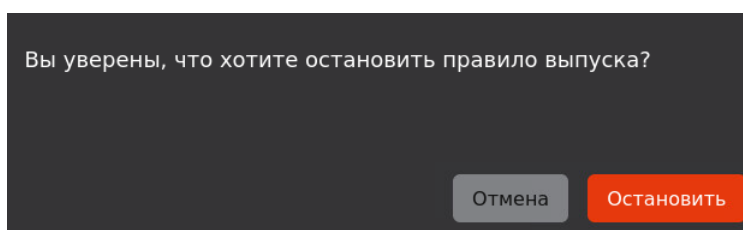



Рисунок 96 - Окно подтверждения остановки правила выпуска

### 7.7.1.7 Копирование правила выпуска

Для копирования правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо скопировать, нажмите на кнопку <Операции>  и выберите опцию <Скопировать> (см. Рисунок 95).
- В появившемся окне подтверждения операции копирования (см. Рисунок 97) нажмите на кнопку <Скопировать>. После нажатия на неё правило выпуска будет скопировано, при этом созданное правило выпуска будет находиться в статусе «Запущено».

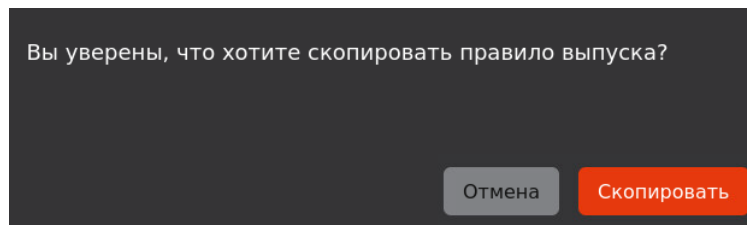



Рисунок 97 - Окно подтверждения копирования правила выпуска

#### 7.7.1.8 Удаление правила выпуска

Для удаления правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо удалить, нажмите на кнопку <Операции>  и выберите опцию <Удалить> (см. Рисунок 95).
- В появившемся окне подтверждения операции удаления (см. Рисунок 98) нажмите на кнопку <Удалить>. После нажатия на неё правило выпуска будет удалено.

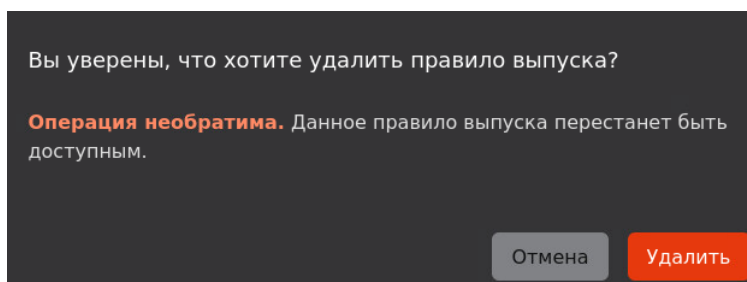


Рисунок 98 - Окно подтверждения удаления правила выпуска

#### 7.7.2 Вкладка «SCEP»

Во вкладке «SCEP» раздела «Управление» (см. рисунок 99) доступны:

- действия над SCEP-политиками:
  - Создание SCEP-политики (см. 7.7.2.1);
  - Редактирование SCEP-политики (см. 7.7.2.2);
  - Запуск SCEP-политики (см. 7.7.2.3);
  - Остановка SCEP-политики (см. 7.7.2.4);
  - Удаление SCEP-политики (см. 7.7.2.5).
- действия над SCEP-профилями:
  - Создание SCEP-профиля (см. 7.7.2.6);
  - Копирование URL адреса SCEP-сервера выбранного SCEP-профиля (см. 7.7.2.7);
  - Остановка и запуск SCEP-профиля (см. 7.7.2.9);
  - Удаление SCEP-профиля (см. 7.7.2.10).



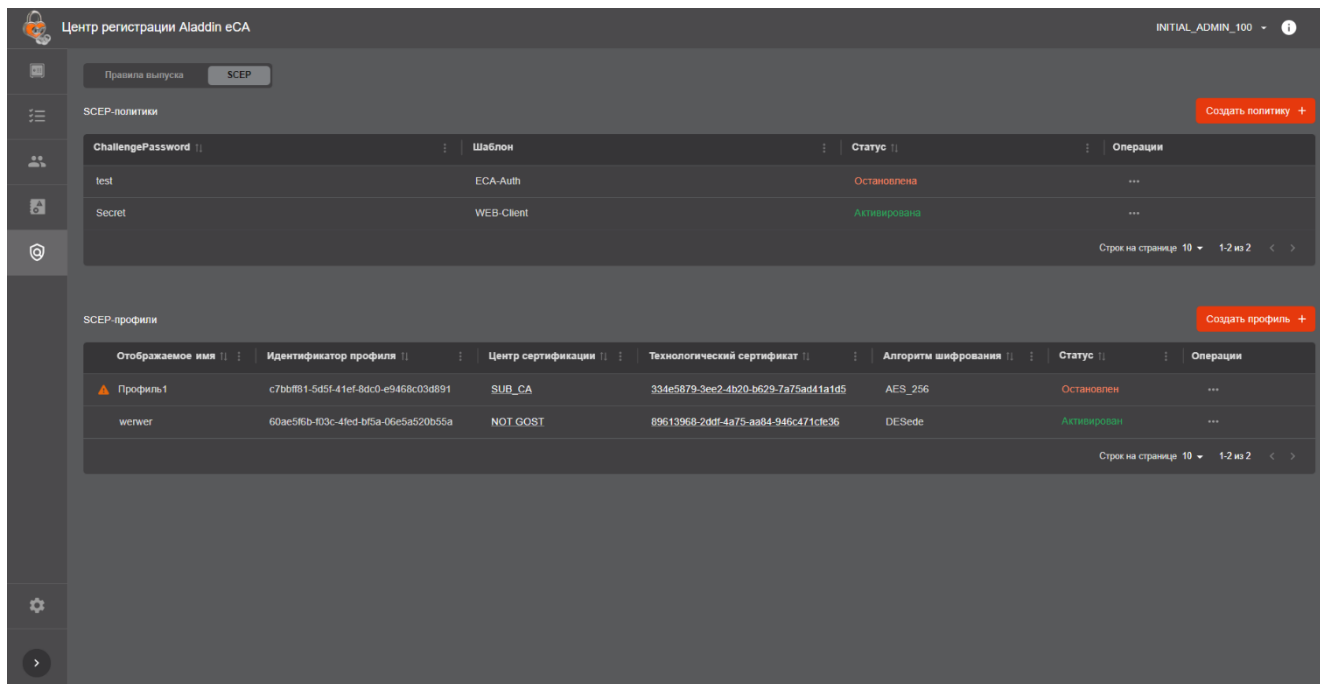


Рисунок 99 — Экран раздела «Управление». Вкладка «SCEP»

#### 7.7.2.1 Создание SCEP-политики

Для создания SCEP-политики выполните следующие шаги:

- В разделе «Управление» во вкладке «SCEP» нажмите на кнопку «Создать политику»
- В открывшемся окне «Создание SCEP-политики» (см. Рисунок 100) укажите «ChallengePassword» и выберите шаблон для создаваемой SCEP-политики.

При этом допускается оставить поле «ChallengePassword» пустым. Данная SCEP-политика будет использоваться при обработке запросов, в которых отсутствует «ChallengePassword».

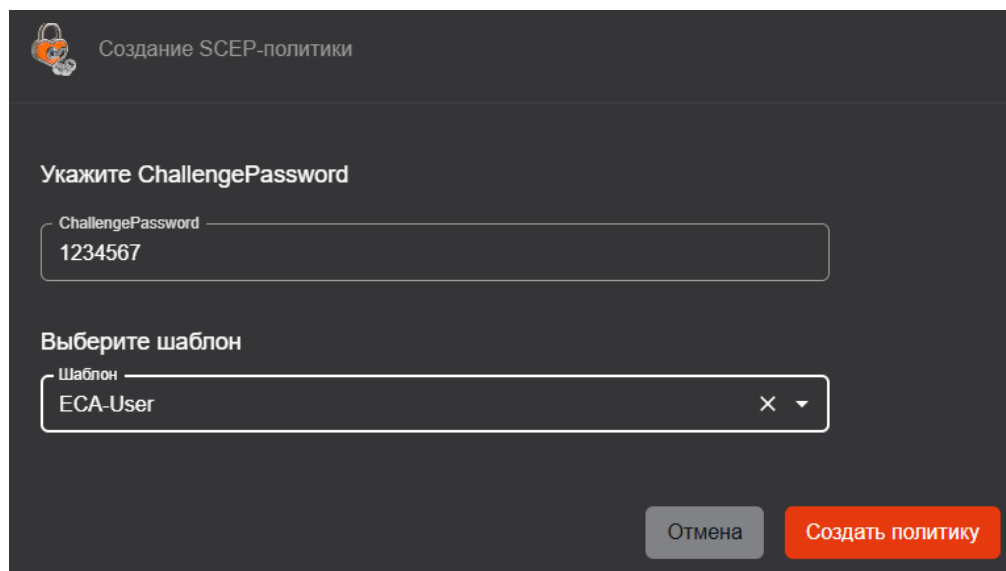


Рисунок 100 - Окно «Создание SCEP-политики»


- Далее нажмите на кнопку «Создать политику».
- При успешном создании созданная SCEP-политика будет отображаться в списке SCEP-политик на вкладке «SCEP» в разделе «Управление».

**Внимание!** В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском

интерфейсе еCA-RA будет отображено всплывающее сообщение об ошибке «Указанный ChallengePassword уже используется», и новая политика не будет создана. Данное ограничение применимо в том числе и к SCEP-политике, у которой ChallengePassword представляет собой пустую строку.

### 7.7.2.2 Редактирование SCEP-политики

Для редактирования SCEP-политики выполните следующие шаги:

- Найдите SCEP-политику, которую необходимо отредактировать, нажмите на кнопку <Операции>  и выберите опцию <Редактировать> (см. Рисунок 101).

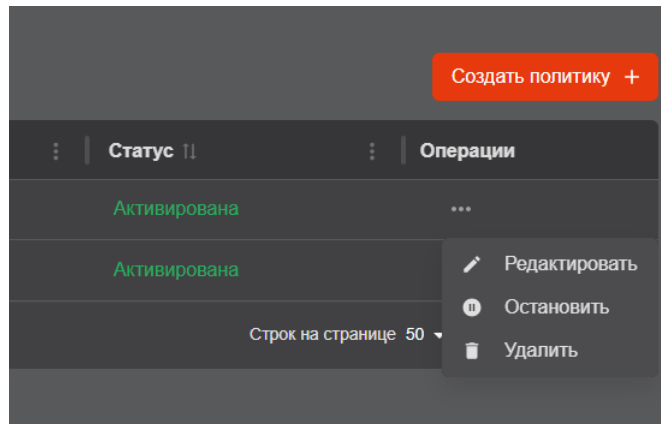


Рисунок 101 - Экран раздела «Управление». Вкладка «SCEP». Редактирование SCEP-политики

- В отрывшемся окне «Редактирование SCEP-политики» (см. Рисунок 102) осуществляется редактирование ChallengePassword и шаблона SCEP-политики.

При этом допускается оставить поле «ChallengePassword» пустым. Данная SCEP-политика будет использоваться при обработке запросов, в которых отсутствует «ChallengePassword».

Рисунок 102 - Окно «Редактирование SCEP-политики»

- После нажатия на кнопку «Сохранить изменения» отредактированная SCEP-политика будет обновлена.

**Внимание!** В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском интерфейсе еCA-RA будет отображено всплывающее сообщение об ошибке «Указанный ChallengePassword уже используется», и новая политика не будет создана. Данное ограничение применимо в том числе и к SCEP-политике, у которой ChallengePassword представляет собой пустую строку.

### 7.7.2.3 Запуск SCEP-политики

Запуск может быть выполнен только для SCEP-политик в статусе «Остановлена». Для запуска SCEP-политики выполните следующие шаги:

- Найдите SCEP-политику, которую необходимо запустить, нажмите на кнопку <Операции> и выберите опцию <Запустить> (см. Рисунок 103).

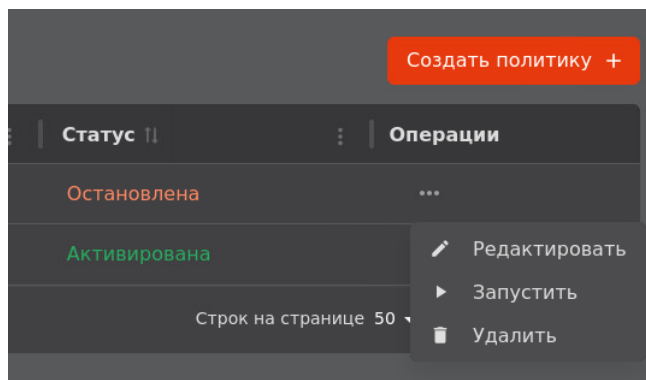


Рисунок 103 - Экран раздела «Управление». Вкладка «SCEP». Запуск SCEP-политики

- В открывшемся окне подтверждения операции запуска (см. Рисунок 104) нажмите на кнопку <Запустить>. После нажатия на неё SCEP-политика будет запущена.

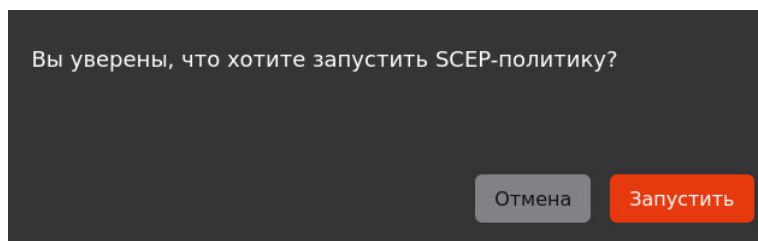


Рисунок 104 - Окно подтверждения запуска SCEP-политики

### 7.7.2.4 Остановка SCEP-политики

Остановка может быть выполнена только для SCEP-политик в статусе «Активирована». Для остановки SCEP-политики выполните следующие шаги:

- Найдите SCEP-политику, которую необходимо остановить, нажмите на кнопку <Операции> и выберите опцию <Остановить> (см. Рисунок 105).

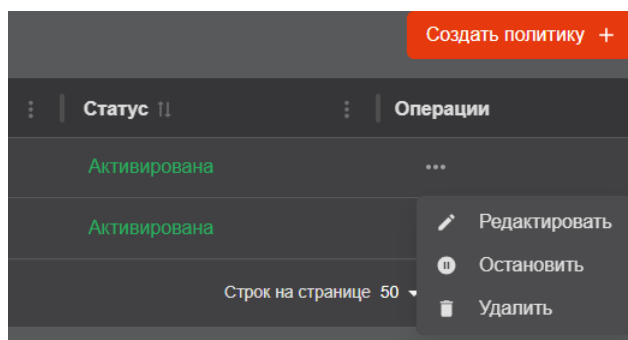


Рисунок 105 - Экран раздела «Управление». Вкладка «SCEP». Остановка SCEP-политики

- В появившемся окне подтверждения операции остановки (см. Рисунок 106) нажмите на кнопку <Остановить>. После нажатия на неё SCEP-политика будет остановлена.

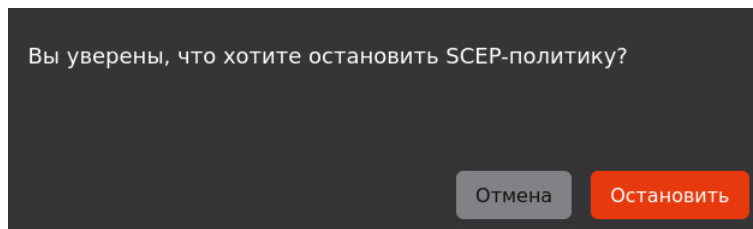



Рисунок 106 - Окно подтверждения остановки SCEP-политики

#### 7.7.2.5 Удаление SCEP-политики

Для удаления SCEP-политики выполните следующие шаги:

- Найдите SCEP-политику, которую необходимо удалить, нажмите на кнопку <Операции>  и выберите опцию <Удалить> (см. Рисунок 107).

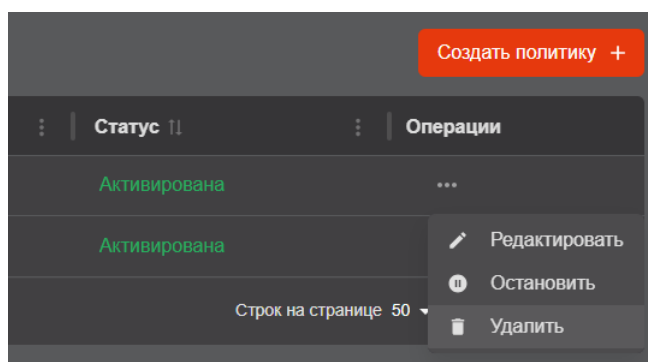


Рисунок 107 - Экран раздела «Управление». Вкладка «SCEP». Удаление SCEP-политики

- В появившемся окне подтверждения операции удаления (см. Рисунок 108) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-политика будет удалена.

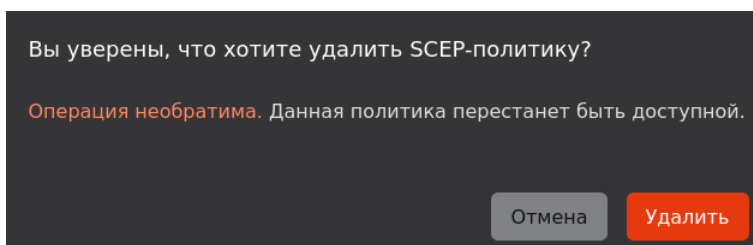


Рисунок 108 - Окно подтверждения удаления SCEP-политики

#### 7.7.2.6 Создание SCEP-профиля

Для создания SCEP-профиля:

- Перейдите в раздел «Управление» на вкладку «SCEP».
- Нажмите на кнопку «Создать профиль».
- В окне «Создание SCEP-профиля» (см. рисунок 109):
  - Укажите отображаемое имя для создаваемого SCEP-профиля.
  - Выберите Центр сертификации подключённого eCA-CA, для которого необходимо создать SCEP-профиль.<sup>1</sup>
  - Выберите алгоритм шифрования ответов SCEP-сервера.
  - Выберите шаблон технологического сертификата создаваемого SCEP-профиля.
  - При необходимости выключить автоматическое обновление технологического сертификата (по умолчанию данная возможность включена).
  - Нажмите на кнопку «Создать профиль».

<sup>1</sup> В выпадающем списке доступных для выбора Центров сертификации должны отсутствовать те Центры сертификации подключённого eCA-CA, для которых в eCA-RA уже существует SCEP-профиль.

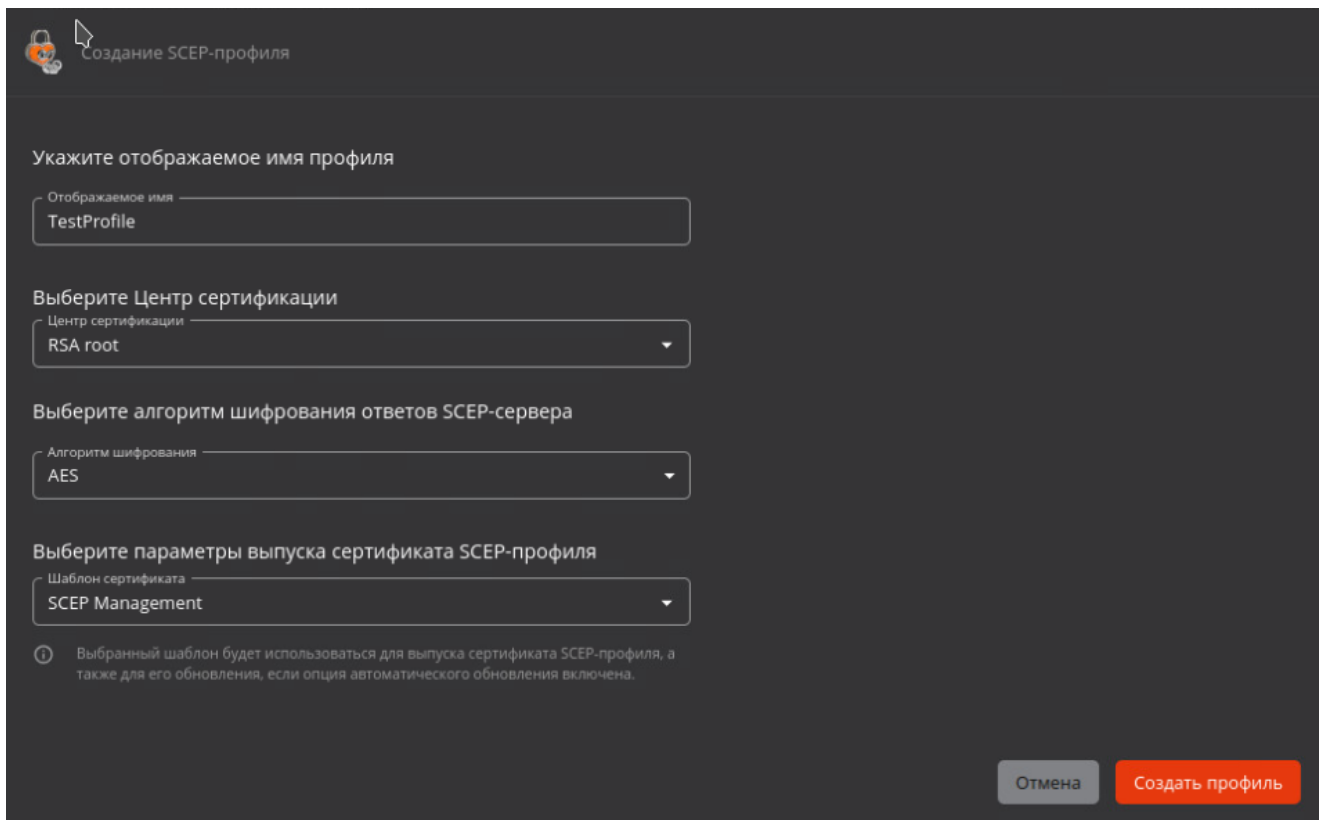


Рисунок 109 — Окно «Создание SCEP-профиля»

При успешном создании созданный SCEP-профиль будет отображаться в списке SCEP-профилей на вкладке «SCEP» в разделе «Управление».

**Внимание!** Работа со SCEP-профилями Центров сертификации подключённого eCA-CA, у которых криптопровайдером алгоритма ключа является СКЗИ «КриптоПро CSP», недоступна. Для такого SCEP-профиля сразу после его создания в пользовательском интерфейсе eCA-RA будет отображаться индикация о его неработоспособности.

#### 7.7.2.7 Редактирование SCEP-профиля

Для редактирования SCEP-профиля:

1. Перейдите в раздел «Управление» на вкладку «SCEP».
2. В строке SCEP-профиля, который необходимо отредактировать, нажмите кнопку отображения контекстного меню операций со SCEP-профилем;
3. Нажмите кнопку «Редактировать».
4. В окне «Редактирование SCEP-профиля» (см. рисунок 110) выполните редактирование параметров.<sup>1</sup>
5. Нажмите кнопку «Сохранить изменения».

<sup>1</sup> Параметр «Центр сертификации» доступен только на чтение. При отключении чекбокса «Обновлять сертификат SCEP-профиля автоматически» параметр «Шаблон» доступен только на чтение.

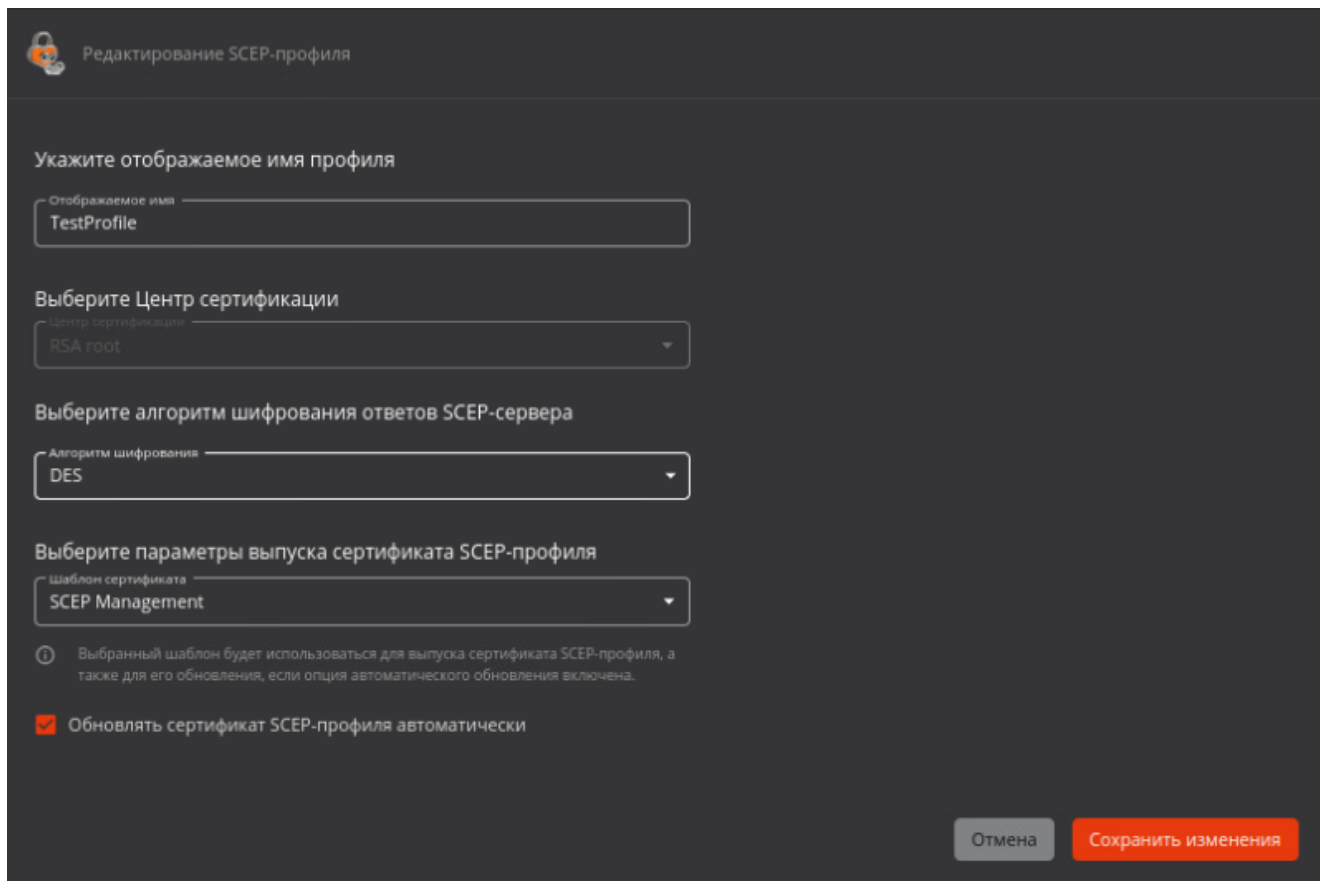



Рисунок 110 — Окно «Редактирование SCEP-профиля»

#### 7.7.2.8 Копирование URL адреса SCEP-сервера выбранного SCEP-профиля

Для копирования URL SCEP-сервера найдите SCEP-профиль в списке нажмите на кнопку <Операции>  и выберите опцию <Копировать URL> (см. Рисунок 111).

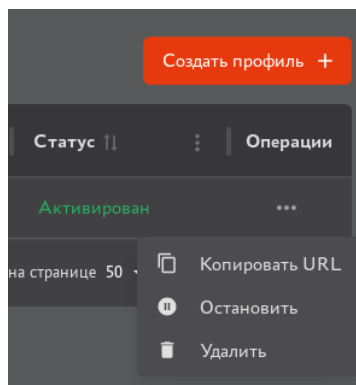


Рисунок 111 — Экран раздела «Управление». Вкладка «SCEP». Копирование URL


После этого буфер обмена будет содержать URL адреса SCEP-сервера выбранного SCEP-профиля (см. Рисунок 112).

`https://rasberos8.msad.aldn/scep-service/profiles/419d9801-e7a8-4ca6-82ab-f9570a55b704/engine`

Рисунок 112 - Пример URL адреса SCEP-сервера

#### 7.7.2.9 Остановка и запуск SCEP-профиля

Для остановки SCEP-профиля выполните следующие действия:

- Найдите SCEP-профиль в списке, нажмите на кнопку <Операции>  и выберите в списке <Остановить> (см. Рисунок 111).

- В появившемся окне подтверждения операции (см. Рисунок 115) нажмите на кнопку <Остановить>.

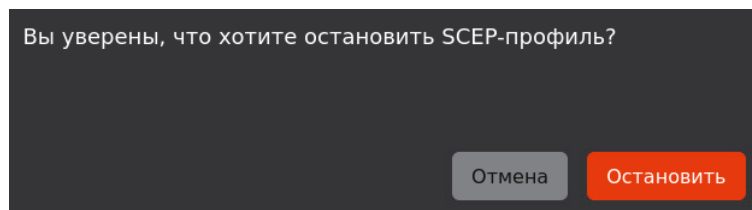



Рисунок 113 - Окно подтверждения остановки SCEP-профиля

В результате SCEP-профиль будет остановлен (статус «Остановлен»)

Чтобы активировать (запустить) SCEP-профиль найдите его в списке, нажмите на кнопку <Операции>  и выберите в списке <Запустить>. В открывшемся окне подтвердите запуск профиля, нажав кнопку <Запустить>.

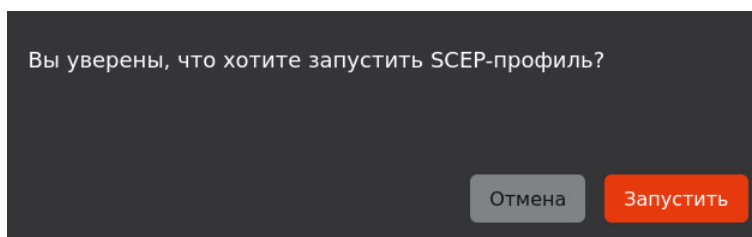



Рисунок 114 - Окно подтверждения запуска СЕР-профиля

#### 7.7.2.10 Удаление SCEP-профиля

Для удаления SCEP-профиля выполните следующие шаги:

- Найдите SCEP-профиль, который необходимо удалить, нажмите на кнопку <Операции>  и выберите опцию <Удалить> (см. Рисунок 111).
- В появившемся окне подтверждения операции удаления (см. Рисунок 115) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-профиль будет удален.

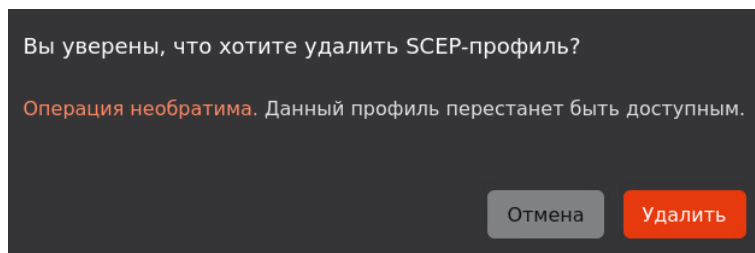


Рисунок 115 - Окно подтверждения удаления SCEP-профиля

## 7.8 Смена сертификата веб-сервера

Предварительно на подключённом eCA-CA необходимо выпустить сертификат для субъекта, соответствующего eCA-RA, с шаблоном «WEB-Server» и со следующими значениями в полях:


- «Common name» - имя веб-сервера, отображаемое на экране, в разделе «Настройки», рекомендуется указать имя сервера;
- «DNS Name» - имя хоста, на котором развёрнут Центр регистрации, должно совпадать с указанным в файле `/etc/hosts`.

Импортируемый сертификат должен отвечать следующим требованиям:

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

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

Для смены сертификата веб-сервера выполните следующие действия:

- Подключитесь к веб-интерфейсу eCA-RA и перейдите в раздел  **Настройка > Веб-сервер** (Рисунок 116).

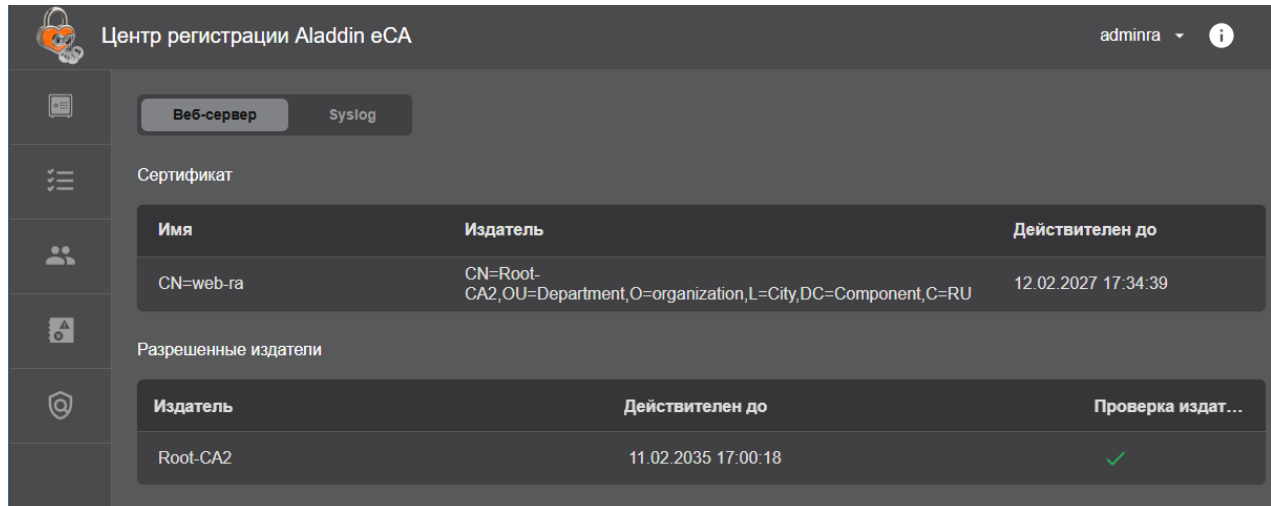




Рисунок 116 - Смена сертификата веб-сервера

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

- «Имя» - CN, указанный в сертификате.
- «Издатель» - SDN издателя сертификата.
- «Действителен до» - дата окончания действия сертификата.
- Наведите на запись о веб-сервере и нажмите появившуюся кнопку .
- В появившемся окне (см. Рисунок 117) выберите файл сертификата и введите пароль от контейнера.
- Нажмите кнопку  **Сменить ключи**.

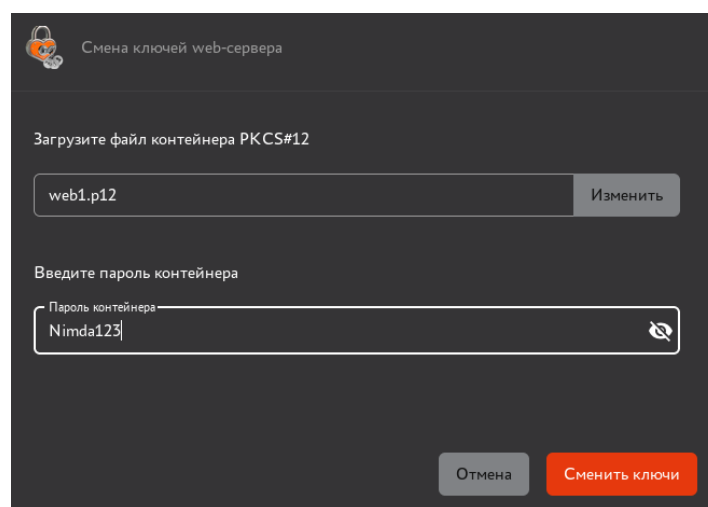


Рисунок 117 - Окно смены ключей веб-сервера


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




В результате будет выполнена автоматическая перезагрузка веб-сервера. В результате перезагрузки веб-сервера в журнале событий будет зарегистрировано событие с кодом RAENV0700 в случае успешной перезагрузки веб-сервера или событие с кодом RAENV0701 в случае ошибки в процессе перезагрузки веб-сервера.

## 7.9 Просмотр информации о разрешённых издателях

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

Для просмотра списка разрешенных издателей подключитесь к веб-интерфейсу eCA-RA и перейдите в раздел  **Настройка > Веб-сервер**.

Информация о разрешенных издателях отображается в разделе «Разрешенные издатели» (Рисунок 116) списком в табличном виде и содержит:

- «Издатель» - CN, указанный в сертификате Центра сертификации.
- «Действителен до» - дата окончания действия сертификата Центра сертификации.
- «Проверка издателя» - статус издателя (разрешенные издатели помечены значком ).

## 8 ПОДДЕРЖКА ПРОТОКОЛА SCEP

еCA-RA реализует серверный компонент по протоколу SCEP<sup>1</sup> (далее SCEP-сервер еCA-RA). SCEP-сервер еCA-RA поддерживает возможность подключения к нему клиентов по протоколам HTTP и HTTPS.

Доступ клиентов к SCEP-серверу еCA-RA осуществляется в контексте SCEP-профилей Центров сертификации подключённого еCA-CA (см. раздел 7.7.2). Чтобы Центр сертификации подключённого еCA-CA, мог быть использован в качестве издателя сертификатов по протоколу SCEP, необходимо для него создать SCEP-профиль.

При создании SCEP-профиля еCA-RA выполняет следующие действия:

- автоматически генерирует и назначает создаваемому профилю идентификатор в формате UUID;
- выпускает на Центре сертификации сертификат с закрытым ключом (PKCS#12) по шаблону «SCEP Management» (технологический сертификат SCEP-профиля), при этом:
  - сертификат не привязан к какому-либо субъекту;
  - имеет в поле «CN» значение «Технологический сертификат SCEP-профиля ID={profileId}», где profileId - идентификатор созданного SCEP-профиля;
  - алгоритм и длина ключа у сертификата соответствуют алгоритму и длине ключа Центра сертификации, на котором осуществляется выпуск;
  - пароль от создаваемого контейнера автоматически формирует еCA-RA и записывает его в свою базу данных в зашифрованном виде.
- экспортирует созданный контейнер закрытого ключа и сохраняет его в своей базе данных.

В дальнейшем технологический сертификат SCEP-профиля используется в обработке запросов по протоколу SCEP (см. раздел 8.2).

### 8.1 Настройка SCEP-сервера

Для настройки SCEP-сервера еCA-RA выполните следующие шаги:

- В разделе «Управление» на вкладке «SCEP» создайте SCEP-политики (см. раздел 7.7.2.1). SCEP-политика представляет собой совокупность «ChallengePassword + Шаблон» и служит для управления шаблонами, которые используются в рамках реализации сценария выпуска сертификата по протоколу SCEP.
- В разделе «Управление» на вкладке «SCEP» создайте новый SCEP-профиль (см. раздел 7.7.2.6). При его создании задайте Центр сертификации подключённого еCA-CA и алгоритм шифрования ответов SCEP-сервера.

После этого будет доступен соответствующий SCEP-сервер, доступный по адресу «`PROTOCOL://<HOSTNAME>/scep-service/profiles/{profileId}/engine`» (про получение URL SCEP-сервера еCA-RA см. раздел 7.7.2.7), где:

- «PROTOCOL» - протокол, по которому осуществляется подключение («http» или «https»). Возможность подключения по http определяется параметром `allow_scep_http` конфигурационного файла;
- «HOSTNAME» - адрес сервера еCA-RA;
- «profileId» - идентификатор существующего SCEP-профиля.
- Далее URL созданного SCEP-профиля следует использовать при добавлении конфигурации SCEP-сервера. Получить URL можно с помощью функции копирования URL адреса SCEP-профиля - см. раздел 7.7.2.7. Пример команды `certmonger`<sup>2</sup> для добавления SCEP-сервера<sup>3</sup>:

```
getcert add-scep-ca -c CA_Name -u SCEP_URL
```

<sup>1</sup> Протокол SCEP описан в RFC8894, см.: <https://datatracker.ietf.org/doc/html/rfc8894>

<sup>2</sup> Certmonger — это служба, которая управляет сертификатами и их жизненным циклом в системах Linux.

<sup>3</sup> Для выполнения команд ниже необходимо, чтобы был установлен пакет `certmonger`.

Для проверки следует использовать команду с правами суперпользователя:

```
getcert list-cas -c Name
```

## 8.2 Обработка запросов по протоколу SCEP

еCA-RA реализовывает обработку следующих запросов клиента по протоколу SCEP<sup>1</sup>:

- PKCSReq;
- CertPoll;
- RenewalReq;
- GetCert;
- GetCRL;
- GetCACert;
- GetCACaps.

### 8.2.1 Обработка запроса клиента PKCSReq/RenewalReq

еCA-RA по серийному номеру сертификата клиента (присутствует в составе сообщения формата PKCS#7) и идентификатору Центра сертификации (определяется автоматически на основании связи используемого клиентом SCEP-профиля и Центра сертификации) осуществляет поиск заявки на данный сертификат клиента в своей базе данных среди выполненных заявок (заявка должна иметь статус «Выполнена»). Далее в зависимости от результатов поиска заявки выполняется один из следующих сценариев:

- Если выполненная заявка на данный сертификат клиента найдена, еCA-RA создаёт новую заявку на основании запроса на сертификат из состава расшифрованного сообщения. Заявка создаётся для субъекта и по шаблону, указанному в найденной заявке. Выпуск сертификата по созданной заявке осуществляется на Центре сертификации Aladdin еCA, ассоциированном с используемым пользователем SCEP-профилем.
  - Если по созданной заявке успешно выпущен сертификат, еCA-RA в ответном сообщении возвращает клиенту выпущенный сертификат (SUCCESS).
  - Если созданная заявка ожидает подтверждения или по ней произошла ошибка выпуска, еCA-RA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
  - Если заявка не была создана или созданная заявка отклонена, еCA-RA возвращает клиенту сообщение об отклонении запроса (FAILURE).
- Если выполненная заявка на данный сертификат клиента не найдена, еCA-RA создаёт новую заявку на основании запроса на сертификат из состава расшифрованного сообщения. Шаблон, который используется при создании заявки, определяется на основании SCEP-политик по значению ChallengePassword, указанному в запросе на сертификат. Выпуск сертификата по созданной заявке осуществляется на Центре сертификации, ассоциированном с используемым пользователем SCEP-профилем.
  - Если в запросе на сертификат не указан ChallengePassword, и среди SCEP-политик отсутствует политика на «пустой» ChallengePassword, еCA-RA возвращает клиенту сообщение об отклонении запроса (FAILURE).
  - Если по созданной заявке успешно выпущен сертификат, еCA-RA в ответном сообщении возвращает клиенту выпущенный сертификат (SUCCESS).
  - Если созданная заявка ожидает подтверждения или по ней произошла ошибка выпуска, еCA-RA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
  - Если заявка не была создана или созданная заявка отклонена, еCA-RA возвращает клиенту сообщение об отклонении запроса (FAILURE).

<sup>1</sup> Запрос «GetNextCACert» на данный момент не поддерживается SCEP-сервером еCA-RA

еCA-RA записывает в свою базу данных «TransactionId» для каждой заявки, созданной в ходе обработки запросов «PKCSReq/RenewalReq».

### 8.2.2 Обработка запроса клиента CertPoll

еCA-RA осуществляет поиск в своей базе данных заявки, у которой «TransactionId» соответствует указанному в сообщении, и определять ее статус.

- Если по найденной заявке успешно выпущен сертификат, еCA-RA в ответном сообщении возвращает клиенту выпущенный сертификат по данной заявке (SUCCESS).
- Если данная заявка ожидает подтверждения или по ней произошла ошибка выпуска, еCA-RA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
- Если данная заявка отклонена или не была найдена, еCA-RA должен возвращать клиенту сообщение об ошибке (FAILURE).

### 8.2.3 Обработка запроса клиента GetCert

еCA-RA осуществляет поиск в своей базе данных заявки, по которой выпущенный сертификат имеет серийный номер, соответствующий указанному в сообщении серийному номеру. Поиск осуществляется только среди заявок, сертификат по которым выпущен еCA-CA, SCEP-профиль которого используется клиентом.

Если такая заявка найдена, еCA-RA в ответном сообщении возвращает клиенту выпущенный по данной заявке сертификат (SUCCESS), иначе - сообщение об ошибке (FAILURE).

### 8.2.4 Обработка запроса клиента GetCRL

еCA-RA в ответном сообщении возвращает CRL еCA-CA, SCEP-профиль которого используется клиентом.

### 8.2.5 Обработка запроса клиента GetCACert

еCA-RA в ответном сообщении возвращает цепочку сертификатов технологического сертификата SCEP-профиля, используемого клиентом.

### 8.2.6 Обработка запроса клиента GetCACaps

еCA-RA возвращает клиенту сообщение формата «CA Capabilities Response» в соответствии с RFC8894, перечисляющее следующие возможности SCEP-сервера:

- AES;
- DES3;
- POSTPKIOperation;
- Renewal;
- SHA-1;
- SHA-256;
- SHA-512;
- SCEPStandart.

## 9 ПОДДЕРЖКА ПРОТОКОЛОВ MS-XCEP И MS-WSTEP

еCA-RA реализует серверные компоненты по протоколам MS-XCEP<sup>1</sup> и MS-WSTEP<sup>2</sup>. Реализация данных серверных компонентов обеспечивает выполнение автоматического сценария распространения сертификатов клиентам и устройствам по протоколу MS-WSTEP.

Сервер политик выпуска сертификатов (CEP-сервер) и сервер выпуска сертификатов (CES-сервер), реализуемые еCA-RA в соответствии с протоколами MS-XCEP и MS-WSTEP, доступны по URL «<https://HOSTNAME/wstep-service/engine>», где «HOSTNAME» - адрес хоста еCA-RA.

еCA-RA в рамках реализации функций CEP-сервера (при получении запроса на политики «GetPolicies») и функций CES-сервера (при получении запроса на выпуск сертификата «RequestSecurityToken») обеспечивает следующие способы аутентификации пользователей домена, к которому он подключен:

- по имени пользователя и паролю;
- по Kerberos-билету.

### 9.1 Обработка запроса на получение политики «GetPolicies»

еCA-RA при получении запроса «GetPolicies» в случае успешной аутентификации пользователя, от имени которого был выполнен запрос, возвращает в ответе «GetPoliciesResponse» политику выпуска сертификатов.

Общие параметры возвращаемой политики соответствуют таблице ниже (Таблица 17).

Таблица 17 - Общие параметры возвращаемой политики

Параметр политики	Значение	Примечание
policyID	5817949c-a7cd-46ec-90ef-7782cd200b15	Уникальный идентификатор политики
policyFriendlyName	еCA enrollment policy	Отображаемое имя политики
nextUpdateHours	8	Время в часах, через которое клиент должен запросить обновление политики выпуска сертификатов с CEP-сервера. Значение «8» указано аналогично значению по умолчанию в MS CS.
policiesNotChanged	NULL	Параметр, используемый для указания факта изменения политики с момента последнего запроса клиентом. Значение «NULL» указано аналогично значению по умолчанию в MS CS.

Шаблоны, записываемые в поле «policies» ответа «GetPoliciesResponse», представляют собой шаблоны подключённого еCA-CA, преобразованные в шаблоны по протоколу MS-XCEP (далее - шаблоны CEP).

При этом в шаблоны CEP преобразовываются только шаблоны еCA-CA одновременно удовлетворяющие следующим условиям:

- которые присутствуют в правилах выпуска еCA-RA для данного пользователя с режимом обработки «Автоматический выпуск»;

<sup>1</sup> Описание протокола MS-XCEP доступно по ссылке: <https://winprotocoldoc.z19.web.core.windows.net/MS-XCEP/%5bMS-XCEP%5d.pdf>

<sup>2</sup> Описание протокола MS-WSTEP доступно по ссылке: <https://winprotocoldoc.z19.web.core.windows.net/MS-WSTEP/%5bMS-WSTEP%5d.pdf>

- у которых включен алгоритм генерации ключевой пары RSA.

В атрибуты возвращаемых шаблонов CEP записываются значения в соответствии с таблицей ниже (Таблица 18):

Таблица 18 - Значения атрибутов шаблонов в сообщении «GetPoliciesResponse»

Атрибут шаблона в сообщении «GetPoliciesResponse»	Примечание
commonName	Имя шаблона eCA-CA
policySchema	3
validityPeriodSeconds	Период действия сертификата по шаблону eCA-CA в секундах
renewalPeriodSeconds	10 % от периода действия сертификата по шаблону в секундах
enroll	true
autoEnroll	true <sup>1</sup>
minimalKeyLength	Минимальная длина ключа для алгоритма RSA по шаблону eCA-CA
keySpec	1
keyUsageProperty	NULL
permissions	NULL
algorithmOIDReference	NULL
provider	Microsoft Base Cryptographic Provider v1.0
majorRevision	1
minorRevision	0
supersededPolicies	NULL
privateKeyFlags	0
subjectNameFlags	2181038080 <sup>2</sup>
enrollmentFlags	0
generalFlags	0 - для типа субъекта шаблона «Пользователь», 64 - для типа субъекта шаблона «Устройство», 128 - для типа субъекта шаблона «Корневой ЦС», 2048 - для типа субъекта шаблона «Подчиненный ЦС»
hashAlgorithmOIDReference	NULL
rARequirements	NULL
keyArchivalAttributes	NULL
extensions	Строка вида «Имя_шаблона@ID_шаблона» <sup>3</sup>

Параметры издателя сертификатов в возвращаемой политике (блок «cAs») соответствуют таблице ниже (см. Таблица 19).

Таблица 19 - Параметры издателя сертификатов в возвращаемой политике

Параметр издателя	Записываемое значение	Примечание
clientAuthentication	2	Данное значение указывается, если пользователь аутентифицируется на CEP-сервере по Kerberos-билету.

<sup>1</sup> Указанное значение обозначает, что шаблон может использоваться при автоматическом запросе и обновлении цифровых сертификатов без ручного вмешательства пользователей.

<sup>2</sup> Указанное значение обозначает, что от пользователя при создании запроса на сертификат не должно требоваться указание значений для SDN и SAN.

<sup>3</sup> Данное значение будет записываться в расширения создаваемого на клиенте запроса на сертификат и будет использоваться в рамках реализации функций CES-сервера.

Параметр издателя	Записываемое значение	Примечание
	4	Данное значение указывается, если пользователь аутентифицируется на CEP-сервере по имени пользователя и паролю
uri	Адрес CES-сервера	URI CES-сервера. На данный адрес будут направляться запросы пользователя на выпуск сертификата (запрос «RequestSecurityToken» по протоколу MS-WSTEP). Адреса CEP- и CES-серверов, реализуемых eCA-RA, совпадают.
priority	1	Приоритет издателя. Прочие значения не применимы для политики, формируемой eCA-RA.
renewalOnly	False	Значение указывает, что издатель может обрабатывать не только запросы на продление существующих сертификатов, но и запросы на выпуск новых сертификатов.
certificate	Сертификат активного центра сертификации eCA-CA	Сертификат в Base64.
enrollPermission	True	Значение указывает, что пользователь может выполнять запросы к данному издателю.

## 9.2 Обработка запроса на выпуск сертификата «RequestSecurityToken»

eCA-RA при получении запроса на выпуск сертификата «RequestSecurityToken» в случае успешной аутентификации выполняет следующие действия:

- создаёт от имени пользователя новую заявку на сертификат на основании запроса из поля «BinarySecurityToken» по шаблону, указанному в данном запросе на сертификат.

Для заявок, создаваемых в ходе обработки запроса «RequestSecurityToken», указан сценарий «WSTEP».

При создании заявки и последующем выпуске сертификата в eCA-CA атрибуты запроса на сертификат автоматически переопределяются атрибутами субъекта из eCA-CA, требуемыми по шаблону.

Для поля, требуемого по шаблону, используются все имеющиеся у субъекта в соответствующем атрибуте значения.

В случае ошибки создания заявки eCA-RA возвращает сообщение об ошибке с кодом «RequestFailed»;

- в случае успешного выпуска сертификата по созданной заявке eCA-RA генерирует и отправляет пользователю ответное сообщение «RequestSecurityTokenResponse», записывая в поле «RequestedSecurityToken» выпущенный по заявке сертификат, а также цепочку данного сертификата в поле «BinarySecurityToken».

Если после создания заявки сертификат по ней не был успешно выпущен, eCA-RA возвращает сообщение об ошибке с кодом «RequestFailed».

- eCA-RA поддерживает перевыпуск сертификатов с новым ключом и с тем же ключом, на котором был выпущен текущий сертификат.

## 9.3 Создание политики регистрации сертификатов

Порядок создания политики регистрации сертификатов в ОС Windows:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Вызовите контекстное меню и выберите Все задачи > Дополнительные операции > Управление политиками регистрации сертификатов (см. Рисунок 118).

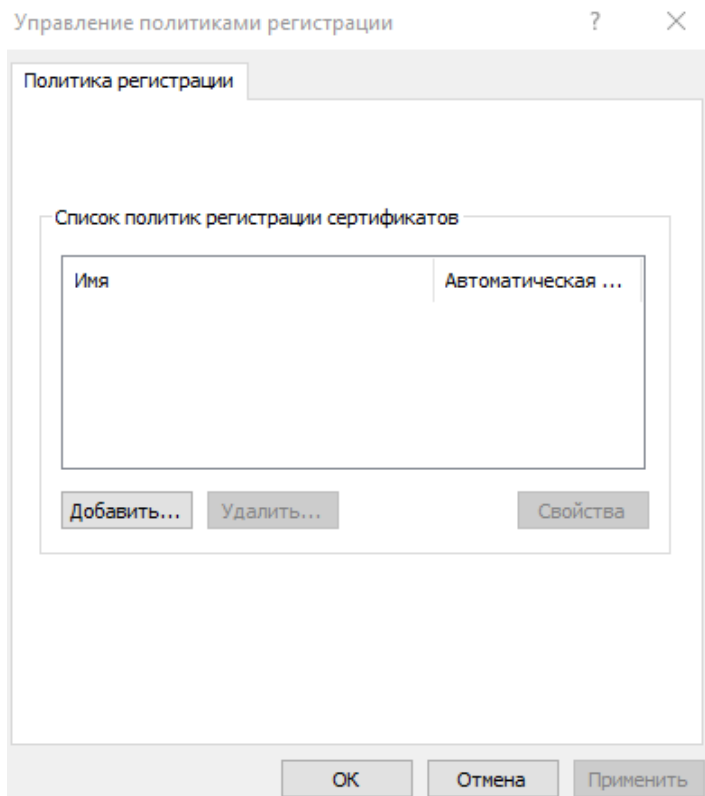


Рисунок 118 - Управление политиками регистрации сертификатов

- В открывшемся окне «Управление политиками регистрации» нажмите кнопку **<Добавить...>**.

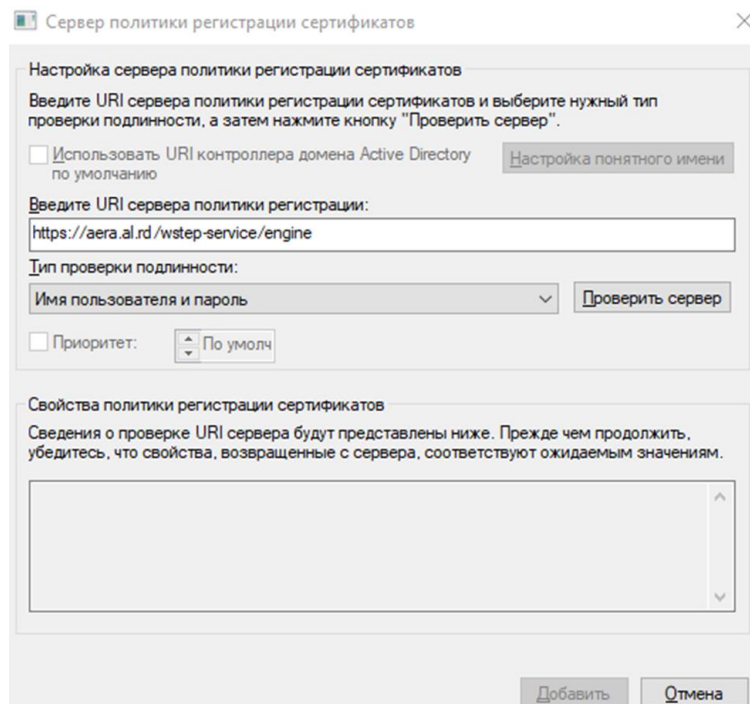




Рисунок 119 - Управление политиками регистрации сертификатов

- В открывшемся окне «Сервер политики регистрации сертификатов» выполните следующие действия:
  - В соответствующем поле введите URL сервера политик выпуска сертификатов eCA-RA.
  - В списке «Тип проверки подлинности» выберите:
    - «Имя пользователя и пароль» для аутентификации по имени и паролю вашей доменной учётной записи.
    - «Встроенная проверка подлинности Windows» для аутентификации по Kerberos-билету.
  - Нажмите кнопку **<Проверить сервер>**.

При выбранном способе аутентификации по имени и паролю укажите их в соответствующих поля открывшегося окна и нажмите кнопку **<ОК>**.

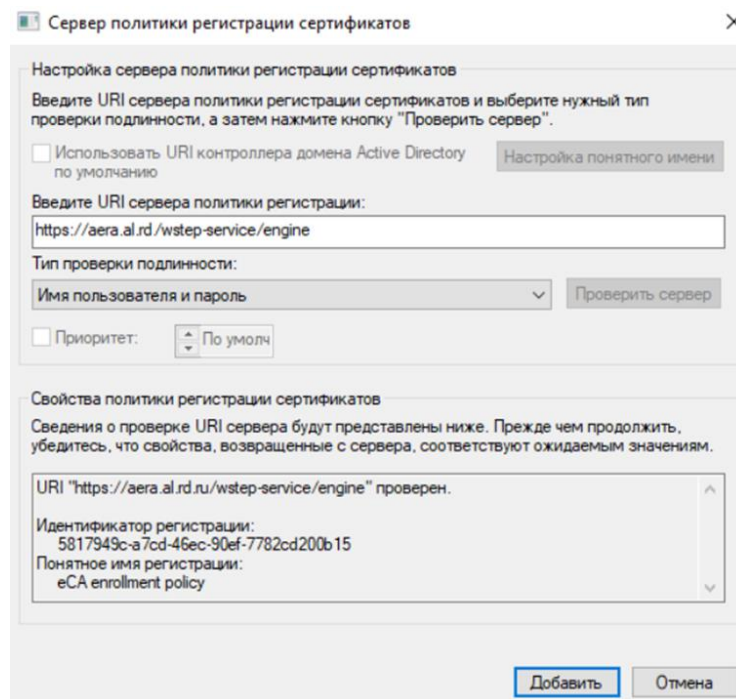


Рисунок 120 - Проверка сервера выполнена успешно

- В случае успешной проверки сервера нажмите кнопку **<Добавить>**.
- В окне «Управление политикам и регистрации» нажмите кнопку **<Применить>**, а затем **<ОК>**.

## 9.4 Запрос нового сертификата

Порядок запроса сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Для запроса нового сертификата вызовите контекстное меню каталога «Сертификаты» и выберите **Все задачи > Запросить новый сертификат**.
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

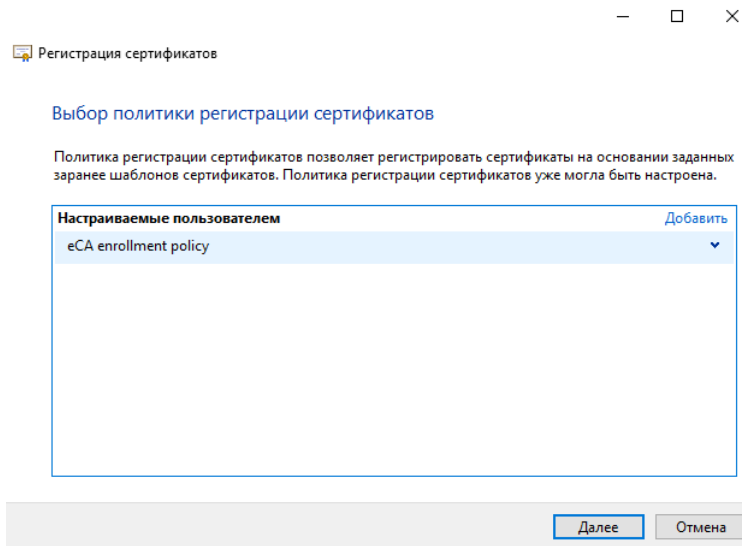


Рисунок 121 - Выбор политики регистрации сертификатов

- На 2 шаге мастера регистрации сертификатов выберите политику **eCA enrollment policy** и нажмите кнопку **<Далее>**.

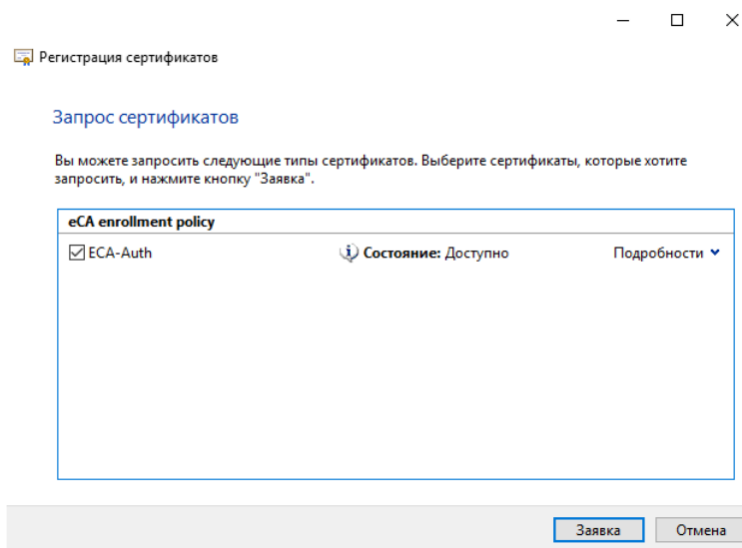


Рисунок 122 - Выбор шаблона для выпуска сертификата

- На 3 шаге мастера регистрации сертификатов выберите шаблоны, по которым необходимо выпустить сертификаты, и нажмите кнопку **<Заявка>**.
- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 123).

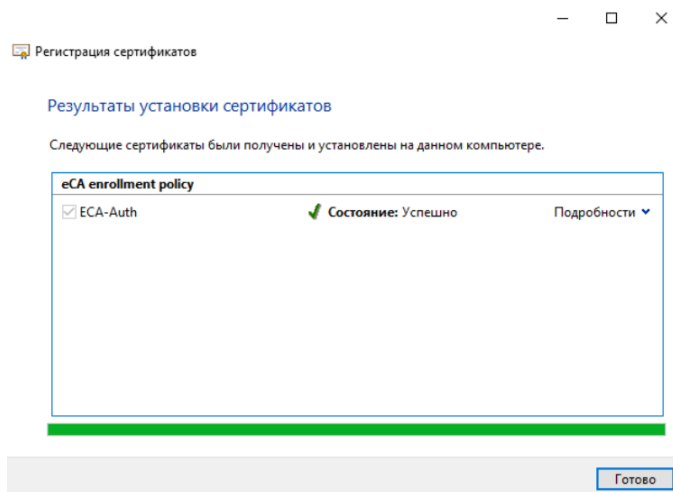


Рисунок 123 - Сертификат получен и успешно установлен в хранилище

## 9.5 Перевыпуск сертификатов

еCA-RA поддерживает перевыпуск сертификатов с новым ключом и с тем же ключом, на котором был выпущен текущий сертификат.

Порядок перевыпуска сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Для запроса нового сертификата вызовите контекстное меню выбранного сертификата и выберите необходимый сценарий перевыпуска или выпуска нового сертификата:
  - Все задачи > Обновить сертификат с новым ключом.
  - Все задачи > Запросить сертификат с новым ключом.
  - Все задачи > Дополнительные операции > Обновить сертификат с тем же ключом.
  - Все задачи > Дополнительные операции > Запросить новый сертификат с тем же ключом.
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

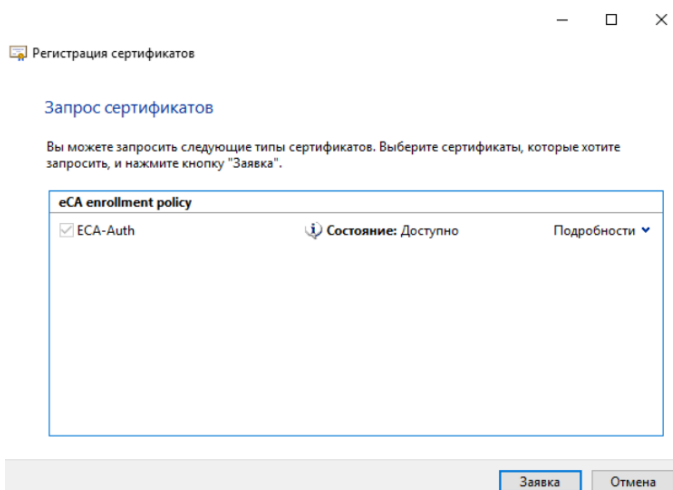


Рисунок 124 - Отправка заявки для выпуска сертификата

- На 2 шаге мастера регистрации сертификатов нажмите кнопку **<Заявка>**.  
На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 123).

## 10 ОФЛАЙН ВЫПУСК СЕРТИФИКАТОВ

еCA-RA обладает возможностью офлайн выпуска сертификатов. Данная возможность заключается в том, что еCA-RA автоматически по расписанию создаёт заявки на выпуск сертификатов на основании файлов запросов на выпуск сертификатов из определённого каталога, используя заранее заданный шаблон сертификата. Выпущенные сертификаты в результате выполнения таких заявок еCA-RA сохраняет в другой заранее заданный каталог.

Также с помощью офлайн выпуска сертификатов может быть настроена интеграция с JMS.

По умолчанию офлайн выпуск сертификатов отключён.

### 10.1 Поддерживаемые расширения и кодировки файлов запросов

еCA-RA поддерживает следующие расширения и кодировки файлов запросов на выпуск сертификатов:

- «.p10» (кодировки DER и PEM);
- «.смс» (кодировка PEM);
- «.req» (кодировки DER и PEM);
- «.pem» (кодировка PEM);
- «.der» (кодировка DER);
- «.dat» (кодировка PEM);
- «.csr» (кодировка PEM).

### 10.2 Сценарий офлайн выпуска сертификатов

Сценарий офлайн выпуска сертификатов запускается по расписанию, которое задается с помощью CRON-выражения в параметре «`offline_enroll_cron`» конфигурационного файла. Сценарий офлайн выпуска сертификатов заключается в обработке каждого файла с запросом (запрос) из каталога, указанного в параметре «`offline_enroll_req_path`» конфигурационного файла.

Если в каталоге сертификатов, заданном в параметре «`offline_enroll_cert_path`» конфигурационного файла, присутствует сертификат, выпущенный по данному запросу, а в каталоге ошибок, заданном в параметре «`offline_enroll_error_path`» конфигурационного файла, содержится данный запрос, то запрос пропускается.

Если по запросу ранее была создана заявка, то выполняется анализ её статуса:

- Если заявка в статусе «Отклонена», то запрос копируется в каталог ошибок.
- Если заявка в статусе «Ожидает подтверждения» или «Ошибка выпуска», то запрос пропускается. Статус данной заявки будет проанализирован при следующем выполнении сценария.
- Если заявка в статусе «Выполнена», то выпущенный по заявке сертификат записывается в каталог сертификатов.

Если заявки не было, то выполняется попытка создать заявку на основании запроса с использованием шаблона, указанного в параметре «`offline_enroll_template_id`» конфигурационного файла, с использованием системной учётной записи (SYSTEM). При этом, если создание заявки завершается с ошибкой, то запрос копируется в каталог ошибок.

## 10.3 Включение офлайн выпуска сертификатов

Для включения выполнения сценария офлайн выпуска сертификатов выполните следующие действия:

- На сервере, где функционирует eCA-RA, создайте следующие каталоги<sup>1</sup>:
  - ``requests`` - каталог, в который будут размещаться файлы запросов на выпуск сертификатов, обрабатываемые при офлайн выпуске;
  - ``certs`` - каталог, в который будут записываться выпущенные сертификаты;
  - ``errors`` - каталог, в который будут записываться файлы запросов, по которым выпуск был отклонен или завершён с ошибкой.
- Выдайте права пользователю `aeca` на запись и чтение для указанных выше каталогов;
- Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, задав следующие значения параметрам:
  - `«offline_enroll_enabled»` - укажите значение `'true'` для активации возможности офлайн выпуска;
  - `«offline_enroll_cron»` - укажите значение cron-выражения, в соответствии с которым будет запускаться офлайн выпуск;
  - `«offline_enroll_template_id»` - укажите значение идентификатора шаблона сертификата, который будет использован для выпуска сертификата. Идентификатор шаблона указан в карточке шаблона в eCA-CA, к которому подключён eCA-RA;
  - `«offline_enroll_req_path»` - укажите абсолютный путь к каталогу ``requests``;
  - `«offline_enroll_cert_path»` - укажите абсолютный путь к каталогу ``certs``;
  - `«offline_enroll_error_path»` - укажите абсолютный путь к каталогу ``errors``;
- Примените изменения конфигурационного файла:
  - Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.  
Пример запуска скрипта без параметров:  
`sudo bash /opt/aecaRa/scripts/install.sh`
  - Выберите действие «[Update]».

## 10.4 Отключение офлайн выпуска сертификатов

Для отключения офлайн выпуска сертификатов выполните следующие действия:

- Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, задав параметру `«offline_enroll_enabled»` значение `'false'`.
- Примените изменения конфигурационного файла:
  - Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.  
Пример запуска скрипта без параметров:  
`sudo bash /opt/aecaRa/scripts/install.sh`
  - Выберите действие «[Update]».

<sup>1</sup> Также можно примонтировать соответствующие сетевые каталоги к хосту eCA-RA

## 11 КОНТРОЛЬ ЦЕЛОСТНОСТИ

### 11.1 Автоматический контроль целостности при запуске eCA-RA

Контроль целостности eCA-RA при запуске регулируется путём редактирования параметров `integrity_check_startup_enabled` и `integrity_check_fail_block_startup` конфигурационного файла.

Для корректировки автоматического контроля целостности eCA-RA при запуске:

1. Укажите в конфигурационном файле необходимые значения для параметров `integrity_check_startup_enabled` и `integrity_check_fail_block_startup`.
2. Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.

Пример запуска скрипта без параметров:

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

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

Контроль целостности исполняемых файлов eCA-RA необходим для отслеживания неизменности и контроля состояния файлов, перечень которых приведён ниже:

- все файлы из каталога `/opt/aecaRa/samples` и его подкаталогов;
- все файлы из каталога `/opt/aecaRa/scripts` и его подкаталогов, кроме файлов `config.sh` и `jc_checksum`;
- все `.jar` файлы в каталоге `/opt/aecaRa/services` и его подкаталогов;
- все файлы в каталоге `/opt/aecaRa/static` и его подкаталогов;
- все файлы в каталоге `/opt/aecaRa/bin` и его подкаталогов;
- все файлы в каталоге `/opt/aecaRa/digsig` и его подкаталогов.

Контроль целостности осуществляется с помощью скрипта `integrity_check.sh`, находящегося в каталоге скриптов `/opt/aecaRa/scripts`. Скрипт `integrity_check.sh` осуществляет проверку целостности исполняемых файлов программного средства средствами утилиты «Утилита контроля целостности 2.0» `jcverify`<sup>1</sup>.

Скрипт `integrity_check.sh` принимает в качестве опционального входного параметра путь к файлу с контрольными суммами, на основании которого должна выполняться проверка. В случае, если путь к файлу не указан, то по умолчанию будет использоваться файл `/opt/aecaRa/scripts/jc_checksum`.

Файл с эталонами контрольными суммами `jc_checksum` формируется при сборке программного средства с помощью утилиты контроля целостности `jcverify`.

Для выполнения контроля целостности исполняемых файлов запустите скрипт `integrity_check.sh` с правами суперпользователя:

```
bash /opt/aecaRa/scripts/integrity_check.sh
```

При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.

В данном случае будет использован файл с эталонами контрольных сумм по умолчанию - `/opt/aecaRa/scripts/jc_checksum`.

После завершения работы скрипта необходимо проанализировать полученные данные.

<sup>1</sup> Данная утилита включена в состав Центра регистрации (каталог `/opt/aecaRa/bin/jcverify`).

## 12 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ

Сбор диагностической информации компонентов необходим для предоставления в службу поддержки. пользователей информации о проблемах в работе программы.

В процессе работы eCA-RA системные службы и компоненты приложения записывают все производимые действия. Произошедшие события записываются в файлы регистрации событий<sup>1</sup> с расширением `.log`, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaRa/dist/logs/` (определяется параметром `logs_base` конфигурационного файла). Максимальный размер лог-файла каждого сервиса перед его архивацией составляет 10 Мбайт (определяется параметром `logs_file_max_size` конфигурационного файла). Срок хранения архивов составляет 10 дней (определяется параметром `logs_max_history` конфигурационного файла). Максимальный общий объем файлов регистрации событий, включая архивы, каждого типа (`access.log` или `service.log`) для каждого сервиса составляет 100 Мбайт (определяется параметром `logs_total_size_cap` конфигурационного файла)

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- О работе сервисов программы (файлы в формате `.log`).
- Конфигурационный файл `/opt/aecaRa/scripts/config.sh`.
- О работе веб-сервера Nginx/Apache (в формате `.log` и `.gz`).
- О работе системы управления базой данных PostgreSQL.
- О работе системы управления базой данных Jatoba.
- О работе ОС (системная).
- Данные системных логов, представленные в таблице 18.

Таблица 20 - Данные системных логов

Системный лог	РЕД ОС	РОСА «ХРОМ» 12 Сервер	Astra Linux SE	Alt Сервер	SberLinux OS Server
<code>/var/log/audit/</code>	+	+	+	+	+
<code>/var/log/samba/</code>	+	+	+	+	+
<code>/var/log/httpd/</code>	+	+	-	-	+
<code>/var/log/messages/</code>	+	+	+	+	+
<code>/var/log/secure/</code>	+	+	-	-	+
<code>/var/log/cron/</code>	+	+	+	-	+
<code>/var/log/auth/</code>	-	-	+	-	-
<code>/var/log/syslog/</code>	-	-	+	+	-
<code>/var/log/httpd2/</code>	-	-	-	+	-
<code>/var/log/ahhttpd/</code>	-	-	-	+	-

При включенном флаге сбора диагностической информации о памяти (параметр `enable_gc_diagnostic` конфигурационного файла `/opt/aecaRa/scripts/config.sh`) архив диагностических данных дополнительно содержит:

- Лог сборщика мусора.
- Дампы памяти для завершивших работу с ошибкой модулей eCA-RA.

Предварительно выполните переход в каталог, где будет сохранён архив с диагностической информацией в формате `tar.gz`, выполнив команду:

```
cd /`папка размещения архива собранной диагностической информации`
```

<sup>1</sup> Файлы регистрации событий, создаваемые в подкаталогах `/opt/aecaRa/dist/logs/`, имеют права доступа 640 (rw-r-- ---).

Для сбора диагностической информации запустите скрипт от имени суперпользователя командой:

```
bash /opt/aecaRa/scripts/diagnostics.sh
```

Сформированный архив в формате `tar.gz` с диагностической информацией будет сохранён в каталоге, из которого был запущен скрипт.

Для вывода текущего каталога используйте команду: `pwd`



## 13 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

### 13.1 Резервное копирование данных

Резервное копирование данных eCA-RA выполняется при помощи скрипта `/opt/aecaRa/scripts/backup.sh`.

Резервная копия включает:

- обязательно:
  - сертификат и ключ веб-сервера, а также файл, содержащий сертификаты разрешённых издателей, из каталога, указанного в параметре `certificates_ssl_path` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию: `/opt/aecaRa/dist/certificates/ssl`);
  - ключи для шифрования пароля пользователя СУБД в конфигурационном файле (файл `/opt/aecaRa/scripts/key`);
  - конфигурационный файл программы `/opt/aecaRa/scripts/config.sh`;
- опционально: базу данных программы, указанную в параметре `database_name` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию `aecara`).

Путь к каталогу, в котором создаются резервные копии, определяется значением, указанным в параметре `backup_path` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию — `/opt/aecaRa/dist/backup/`).

Имена файлов резервных копий имеют следующий формат:

- `aeca-ra-backup-«дата-время-создания».tar` — для резервных копий, содержащих базу данных;
- `aeca-ra-backup-«дата-время-создания»-nodb.tar` — для резервных копий, не содержащих базу данных.

Параметры запуска скрипта `/opt/aecaRa/scripts/backup.sh` представлены в таблице 21.

Таблица 21 — Параметры запуска скрипта `/opt/aecaRa/scripts/backup.sh`

Параметр	Описание
<code>-nodb</code>	При указании параметра скрипт не вносит базу данных в создаваемую резервную копию
<code>--dbuser имя_пользователя СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-U имя_пользователя СУБД</code>	То же, что <code>--dbuser имя_пользователя СУБД</code>
<code>--dbpass пароль_пользователя СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-P пароль_пользователя СУБД</code>	То же, что <code>--P пароль_пользователя СУБД</code>

Для создания резервной копии:

- Запустите скрипт `/opt/aecaRa/scripts/backup.sh` с параметрами согласно таблице 21.
- При необходимости укажите параметры в диалоге.

Пример запуска скрипта `/opt/aecaRa/scripts/backup.sh` без параметров:

```
sudo bash /opt/aecaRa/scripts/backup.sh
```

### 13.2 Настройка расписания резервного копирования

Для снижения потерь данных во время сбоя выполните настройку автоматического резервного копирования, настроив системный планировщик расписания `crontab`.

Выполните переход в режим редактирования `crontab` выполнив команду с правами суперпользователя:

```
nano /etc/crontab
```

Укажите время и период запуска сценариев создания резервных копий:

```
0 0 1 * * /opt/aecaRa/scripts/backup.sh
0 0 1 12 * /opt/aecaRa/scripts/backup.sh
```

где:

- Первая строка описывает запуск резервного копирования один раз в месяц.
- Вторая строка описывает запуск резервного копирования один раз в год.

Для просмотра настроенного расписания используйте команду: `crontab -l`

**Внимание!** В случаях, когда изменений между резервными копиями обнаружено не было, возможно отображение сообщения о некорректном срабатывании функции `stat` следующего вида: `tar: /tmp/1/inc/copia_*`: Функция `stat` завершилась с ошибкой: No such file or directory

### 13.3 Восстановление данных из резервной копии

Восстановление данных eCA-RA из резервной копии выполняется при помощи скрипта `/opt/aecaRa/scripts/restore.sh`.

Параметры запуска скрипта `/opt/aecaRa/scripts/restore.sh` представлены в таблице 22.

Таблица 22 — Параметры запуска скрипта `/opt/aecaRa/scripts/restore.sh`

Параметр	Описание
<code>--backup</code> путь_к_файлу_резервной_копии	Параметр позволяет передать путь к резервной копии при запуске скрипта
<code>-В</code> путь_к_файлу_резервной_копии	То же, что <code>--backup</code> путь_к_файлу_резервной_копии
<code>--sypass</code> пароль	Параметр позволяет передать пароль от контейнера для подключения к eCA-CA при запуске скрипта
<code>-С</code> пароль	То же, что <code>--с</code> пароль
<code>-nodb</code>	При указании параметра скрипт не восстанавливает базу данных из резервной копии
<code>--dbuser</code> имя_пользователя_СУБД	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-U</code> имя_пользователя_СУБД	То же, что <code>--dbuser</code> имя_пользователя_СУБД
<code>--dbpass</code> пароль_пользователя_СУБД	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-Р</code> пароль_пользователя_СУБД	То же, что <code>--dbpass</code> пароль_пользователя_СУБД

Для восстановления данных из резервной копии:

- Запустите скрипт `/opt/aecaRa/scripts/restore.sh` с необходимыми параметрами согласно таблице 22.
- При необходимости укажите параметры в диалоге.

Пример запуска скрипта `/opt/aecaRa/scripts/restore.sh` без параметров:

```
sudo bash /opt/aecaRa/scripts/restore.sh
```

## 14 ОБНОВЛЕНИЕ ПРОГРАММЫ

Обновление базы данных и модулей eCA-RA обеспечивает актуальность версии программного обеспечения.

При обновлении программы решаются следующие задачи:

- Исправление обнаруженных за время существования программы недочетов и ошибок.
- Устранение выявленных уязвимостей.
- Изменение или улучшение функций программы.
- Добавление новых функций и возможностей.

Компания ведет учет покупателей Центра сертификатов доступа. Выполняется регистрация следующей информации:

- Наименование организации.
- Адрес организации.
- Контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).

Уведомление пользователей о выпуске новой версии Центра сертификатов доступа выполняется путем публикации информации на официальном сайте АО «Аладдин Р.Д.» и (или) рассылкой электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счет применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлами новой версии программного средства может предоставляться обновленная документация для использования программы.

Получение файлов для обновления программного средства и соответствующих им контрольных сумм возможно:

- С использованием электронной почты.
- Путем загрузки с веб-сайта АО «Аладдин Р.Д.»..

Проверка квалифицированной электронной подписи изготовителя (производителя) файлов для обновления программного средства и файлов соответствующих им контрольных сумм выполняется любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления.

Контроль целостности файлов для обновления программы выполняется путем расчета КС полученных установочных пакетов (дистрибутивов) с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0» или программного средства «Утилита контроля целостности 2.0» из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», и её сравнением со значением контрольной суммы для этого обновления (см. подраздел 1.5.2 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).

**Внимание!** На случай, если во время процесса обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию данных программы (см. раздел 13 настоящего руководства).

Порядок обновления программы:

- Перенесите дистрибутив с новой версией программы на компьютер с установленным eCA-RA.
- Выполните распаковку установочного пакета:
  - для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server командой с правами суперпользователя: `dnf install aeca-*.rpm`;
  - для ОС Astra Linux SE командой с правами суперпользователя: `dpkg -i aeca-*.deb`;
  - для Альт Сервер командой с правами суперпользователя: `apt-get install aeca-*.rpm`.

- Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.

Пример запуска скрипта без параметров:

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

- Установщик обнаружит текущую версию eCA-RA и предложит выбрать необходимое действие в интерактивном режиме:
  - Удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программы.
  - Выполнить обновление установленной версии до актуальной версии программы.
  - Прервать процесс установки.

Для продолжения процесса обновления введите в терминале цифру «2».

При обновлении программа проверяет соответствие номера сборки и значения номера сборки, указанной в БД<sup>1</sup>, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaRa/scripts/config.sh`:

- Если на момент обновления в БД отсутствует номер сборки, то программа записывает в БД номер устанавливаемой сборки.
- Если на момент обновления в базе данных присутствует номер сборки, и он меньше номера устанавливаемой сборки, то eCA-RA перезаписывает номер сборки в БД, заменив его номером устанавливаемой сборки.
- Если на момент обновления в БД записан номер сборки, и он равен номеру устанавливаемой сборки, программа не изменяет его.
- Если на момент обновления в БД записан номер сборки, и он больше номера устанавливаемой сборки, то программа завершает процесс обновления с ошибкой «Текущая версия схемы базы данных не позволяет выполнить установку или обновление службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где X.X.X.X - номер сборки, записанный в БД, а Y.Y.Y.Y - номер устанавливаемой сборки программы. Номер сборки в БД при этом не меняется.

После обновления программы запустите веб-браузер и очистите его данные.

Запустите обновленный eCA-RA, подключитесь к веб-интерфейсу и проверьте версию программы в окне «О программе».

<sup>1</sup> Значение номера сборки указано в таблице «`build_info`» схемы «`aeca_info`».

## 15 УДАЛЕНИЕ ПРОГРАММЫ

Для инициализации процесса удаления:

1. Выполните команду с правами суперпользователя:

```
bash /opt/aecaRa/scripts/uninstall.sh
```

2. При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге:

- имя пользователя СУБД;
- пароль пользователя СУБД.

В результате выполнения данного действия будут полностью уничтожены:

- Все добавленные при установке компонента системные службы.
- Все добавленные при установке компонента пользователи и группы.
- Все добавленные при установке компонента файлы и структура каталогов.
- Процесс удаления выполняется вне зависимости от наличия соединения с БД, имя которой указано в значении параметра `database_name` конфигурационного файла `/opt/aecaRa/scripts/config.sh`.

## 16 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

### 16.1 Удаление базы данных

Для удаления ранее созданной базы данных (по умолчанию «aecara») необходимо выполнить команды с правами суперпользователя:

- Зайдите под пользователем «postgres» в Postgres выполнив команду с правами суперпользователя:

```
-u postgres psql
```

- Для предотвращения возможности новых подключений выполните команду:

```
UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'aecara';
```

- Для закрытия всех текущих сессий выполните команду:

```
SELECT pg_terminate_backend(pg_stat_activity.pid)
FROM pg_stat_activity
WHERE pg_stat_activity.datname = 'aecara' AND pid <> pg_backend_pid();
```

- Для удаления базы данных выполните команду:

```
DROP DATABASE aecara;
```

- Завершите работу под пользователем «postgres» и выйдите из терминала выполнив команду:

```
exit
```

### 16.2 Удаление пользователя базы данных

Для удаления ранее созданного пользователя базы данных (по умолчанию «aeca») необходимо выполнить команды с правами суперпользователя:

- Зайдите под пользователем «postgres» в Postgres выполнив команду с правами суперпользователя:

```
-i -u postgres
```

- Удалите пользователя базы данных в Postgres выполнив команду:

```
dropuser aeca -i
```

- Завершите работу под пользователем «postgres» и выйдите из терминала выполнив команду:

```
exit
```

- Перезапустите СУБД Postgres выполнив команду с правами суперпользователя:

```
systemctl restart postgresql
```

## 17 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ид.	Проблема	Возможная причина	Способы решения
П001	Ошибка при запуске скрипта установки <code>install.sh</code> «error obtaining MAC configuration for user «имя пользователя СУБД»» в ОС Astra Linux Special Edition 1.8	Не выполнена дополнительная настройка пользователя СУБД для поддержки работы с активным механизмом МРД	Выполнить настройку пользователя СУБД для поддержки работы с активным механизмом МРД в соответствии с инструкциями подраздела 4.4 (в зависимости от использованного способа создания пользователя СУБД) и перезапустить скрипт установки <code>install.sh</code> .
П002	Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для установки eCA-RA	Нехватка аппаратных ресурсов	Проверьте показатель загруженности оперативной памяти. Для корректной работы программы требуется не менее 8 Гб свободной оперативной памяти
П003	Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для установки eCA-RA: «[ERROR] Не удалось запустить сервис aeca-ra-ca-adapter...»	Отсутствуют права на директории, которые указаны в файле <code>krb5.conf</code> в командах <code>includedir</code> . Пример: В файле <code>krb5.conf</code> используется команда <code>includedir /etc/krb5.conf.d/</code> , внутри этой директории есть файл <code>enable_ssd.conf_dir</code> , внутри которого есть команда <code>includedir /var/lib/sss/pubconf/krb5.include.d</code> , Соответственно должны быть права на: <ul style="list-style-type: none"> <li>▪ <code>krb5.conf</code>;</li> <li>▪ <code>/etc/krb5.conf.d/</code>, а также все файлы и директории внутри, включая файл <code>enable_ssd.conf_dir</code>;</li> <li>▪ <code>/var/lib/sss/pubconf/krb5.include.d/</code>, а также все файлы и директории внутри.</li> </ul>	Выдать права на все файлы и директории, используемые в <code>krb5.conf</code> при помощи команды с правами суперпользователя: <code>chmod 666 путь_к_файлу</code> Где «путь_к_файлу» - путь к файлу или директории.

Ид.	Проблема	Возможная причина	Способы решения
П004	Вход в интерфейс Центра регистрации невозможен в браузере Firefox. Ошибка SEC_ERROR_BAD_SIGNATURE	Проблема возникает при наличии в хранилище сертификатов ОС сертификата ЦС с аналогичным SDN издателю сертификата веб-сервера. Она связана с алгоритмом проверки сертификата веб-сервера браузером Firefox для решения уязвимости, связанной с подлогом серверного сертификата: 1. Firefox получает сертификат веб-сервера от сервера 2. После этого выполняет поиск в хранилище сертификатов ОС сертификата ЦС по SDN издателя сертификата 3. И далее выполняет проверку цепочки по открытым ключам	1. Проверьте состав сертификатов доверенных ЦС в хранилище ОС 2. В случае несоответствия установите сертификат издателя сертификата веб-сервера
П005	Вход в интерфейс ЦС невозможен. Ошибка 400. The SSL certificate error	Вход в интерфейс выполнялся в момент синхронизации разрешенных издателей. В параметре «issuers_sync» конфигурационного файла установлено слишком маленькое значение. Синхронизация выполняется слишком часто.	1. Увеличьте интервал синхронизации разрешенных издателей (по умолчанию - каждые 30 минут). 2. Обновите страницу веб-браузера.



## ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА ПРИ УСТАНОВКЕ СУБД POSTGRESQL И СУБД POSTGRES PRO

В случае, если другой продукт Postgres уже установлен, то для разрешения конфликта необходимо выполнить команды:

- Создайте начальную базу данных, запустив вспомогательный скрипт `pg-setup` с правами суперпользователя и ключом `initdb`:

```
/opt/pgpro/std-16/bin/pg-setup initdb [--tune=конфигурация] [параметры_initdb]
```

где

- аргумент `tune` выбирает вариант конфигурации базы данных;
- `параметры_initdb` — обычные параметры `initdb`.

- Для настройки автозапуска сервера запустите скрипт `pg-setup` со следующими параметрами:

```
/opt/pgpro/std-16/bin/pg-setup service enable
```

- Запустите сервер с помощью `pg-setup` выполнив следующую команду с правами суперпользователя):

```
/opt/pgpro/std-16/bin/pg-setup service start
```

## ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

Для подключения еСА-РА к внешней СУБД необходимо:

- выполнить настройку на хосте СУБД в соответствии с разделом 2.1 настоящего приложения;
- выполнить настройку на хосте еСА-РА в соответствии с разделом 2,2 настоящего приложения.

### 2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД в зависимости от используемой на нём ОС необходимо выполнить настройки ниже.

#### 2.1.1 Настройка на хосте СУБД для Astra Linux

Если в качестве ОС на хосте СУБД используется Astra Linux, то необходимо разрешить подключение по протоколу TCP для порта СУБД выполнив в терминале на данном хосте следующую команду с правами суперпользователя:

```
iptables -A INPUT -p tcp --destination-port port -j ACCEPT
```

где `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432). Данная команда разрешит подключение к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к порту СУБД, предоставив его только для определённого IP-адреса, необходимо использовать следующую команду с правами суперпользователя:

```
iptables -A INPUT -s IP -p tcp --destination-port port -j ACCEPT
```

где `IP` - IP-адрес, доступ с которого необходимо разрешить; `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432).

Затем на хосте СУБД необходимо перезапустить используемую СУБД выполнив команду с правами суперпользователя `systemctl restart postgresql` (или `systemctl restart jatoba-4`, если используется СУБД Jatoba).

Затем на хосте СУБД необходимо выполнить создание и настройку базы данных. В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

#### 2.1.2 Настройка на хосте СУБД для РЕД ОС, РОСА «ХРОМ» 12 Сервер, SberLinux OS Server и Альт Сервер

Если в качестве ОС на хосте с СУБД используется РЕД ОС, РОСА «ХРОМ» 12 Сервер или Альт Сервер, необходимо отредактировать файл `/var/lib/pgsql/15/data/pg_hba.conf` (или `var/lib/jatoba/[версия]/data/pg_hba.conf`, если используется СУБД Jatoba)<sup>1</sup>, приведя его к следующему виду:

# TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only				
local	all	all		peer
# IPv4 local connections:				
host	all	all	0.0.0.0/0	password
# IPv6 local connections:				
host	all	all	:::1/128	password
# Allow replication connections from localhost, by a user with the				
# replication privilege.				
local	replication	all		peer
host	replication	all	127.0.0.1/32	ident
host	replication	all	:::1/128	ident

<sup>1</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

Кроме того, необходимо отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)<sup>1</sup>, указав для параметра `listen_addresses` значение `listen_addresses = '*'`

Значение `'*'` позволит подключаться к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к СУБД, предоставив его только для определённого IP-адреса, необходимо указать данный IP-адрес в параметре `listen_addresses`, например:

```
listen_addresses = '192.168.111.100'
```

Затем на хосте СУБД необходимо перезапустить используемую СУБД выполнив с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-4` если используется СУБД Jatoba).

Затем на хосте СУБД необходимо выполнить создание и настройку базы данных.

## 2.2 Настройка на хосте eCA-RA

**Внимание!** На хосте eCA-RA предварительно должна быть выполнена установка СУБД. При этом не нужно настраивать СУБД, установленную на хосте eCA-RA.

На хосте eCA-RA необходимо отредактировать конфигурационный файл `/opt/aecaRa/scripts/config.sh`, указав в нём значения следующих параметров:

Параметр	Значение по умолчанию	Описание
<code>use_tls</code>	<code>false</code>	Флаг обязательного использования TLS для подключения к СУБД <sup>2</sup> . Допустимые значения: <code>true</code> , <code>false</code>
<code>database_username</code>	<code>'aeca'</code>	Имя пользователя базы данных, используемое для работы eCA-RA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>database_password</code>	<code>#CHANGEIT</code>	Пароль пользователя базы данных, используемый для работы eCA-RA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>database_host</code>	<code>'localhost'</code>	Сетевой адрес хоста СУБД
<code>database_port</code>	<code>'5432'</code>	Порт, используемый для подключения к базе данных
<code>database_name</code>	<code>'aecara'</code>	Имя базы данных, используемой eCA-RA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>root_cert_path</code>	<code>#CHANGEIT</code>	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД <sup>3</sup>

Затем на хосте eCA-RA примените изменения конфигурационного файла:

1. Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.

Пример запуска скрипта без параметров:

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

2. Выберите действие «[Update]».
3. Выберите действие «[Update]».

В случае, если eCA-RA не был установлен ранее, выбор действия не потребует, и будет выполнена установка с указанными в конфигурационном файле параметрами.

<sup>1</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

<sup>2</sup> Подробная информация о параметре `use_tls` приведена в Настройка TLS-соединения с СУБД

<sup>3</sup> Подробная информация о параметре `root_cert_path` приведена в Настройка TLS-соединения с СУБД

## ПРИЛОЖЕНИЕ 3. НАСТРОЙКА TLS-СОЕДИНЕНИЯ С СУБД

Для настройки TLS-соединения Центра регистрации Aladdin Enterprise Registration Authority с СУБД необходимо в предварительно развёрнутом и инициализированном еCA-CA создать сертификат с закрытым ключом (PKCS#12) для сервера СУБД. При этом в сертификате сервера СУБД в атрибуте Common Name или в атрибуте Subject Alternative Name типа `dnsName` обязательно должно быть указано доменное сервера СУБД (или IP-адрес)<sup>1</sup>, так как еCA-RA аутентифицирует сервер СУБД в режиме «verify-full», который предполагает проверку соответствия имени узла сервера имени, записанному в сертификате. Для создания сертификата может быть использован шаблон «WEB-Server» (необходимо предварительно создать локальный субъект в еCA-CA, указав ему необходимые атрибуты CN и DNS Name).

Во избежание ошибок в работе еCA-RA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу еCA-RA путём выполнения с правами суперпользователя команды `systemctl stop aeca-ra.service`.

Для настройки TLS-соединения еCA-RA с СУБД необходимо:

- выполнить настройку СУБД в соответствии с разделом 3.1 настоящего приложения, представленным ниже;
- выполнить настройку еCA-RA в соответствии с разделом 3.2 настоящего приложения, представленным ниже.

### 3.1 Настройка на хосте СУБД

На хосте с установленной и настроенной СУБД отредактировать файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)<sup>2</sup>, указав:

- в параметре «ssl» значение «on»;
- в параметре «ssl\_cert\_file» абсолютный путь к файлу сертификата сервера СУБД<sup>3</sup>;
- в параметре «ssl\_key\_file» абсолютный путь к файлу закрытого ключа сервера СУБД<sup>4</sup>;
- в параметре «ssl\_ca\_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД<sup>5</sup>.

При этом указанные выше файлы должны иметь метку доступа «600», установить которую можно с помощью команды с правами суперпользователя `chmod 600 путь_к_файлу` для каждого файла. Владелец всех указанных выше файлов необходимо назначить пользователя «postgres» выполнив команду с правами суперпользователя `chown postgres:postgres путь_к_файлу` для всех перечисленных файлов. Указанные файлы должны располагаться в каталоге, к которому имеет доступ пользователь `postgres` (например, `/tmp`). В случае использования ОС РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server на хосте СУБД указанные выше файлы должны располагаться в каталоге `/var/lib/pgsql` (или `/var/lib/jatoba`, если используется СУБД Jatoba). При этом указанные выше файлы должны быть скопированы в нужный каталог, а не перемещены.

Пример значений отредактированных параметров конфигурационного файла СУБД `postgresql.conf`:

<sup>1</sup> Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database\_host» конфигурационного файла еCA-RA.

<sup>2</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

<sup>3</sup> Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса еCA-CA. Например, в карточке локального субъекта сервера СУБД.

<sup>4</sup> Файл закрытого ключа сервера СУБД может быть получен из контейнера закрытого ключа сервера СУБД путём выполнения команды `openssl pkcs12 -in container.p12 -out key.key -nocerts -nodes`, где `container.p12` - путь к контейнеру закрытого ключа сервера СУБД, а «key.key» - путь к файлу для сохранения закрытого ключа.

<sup>5</sup> Файл цепочки сертификатов издателя сертификата СУБД может быть скачан в карточке ЦС, выпустившего сертификат сервера СУБД.

```
# - SSL -
ssl = on
ssl_cert_file = '/tmp/cert.pem'
ssl_key_file = '/tmp/key.key'
ssl_ca_file = '/tmp/chain.pem'
```

На хосте СУБД перезапустить СУБД выполнив с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-4` если используется СУБД Jatoba).

## 3.2 Настройка на хосте eCA-RA

На хосте eCA-RA отредактировать конфигурационный файл `/opt/aecaRa/scripts/config.sh`, указав в нём в параметре конфигурации БД `use_tls` значение `true`, а в параметре `root_cert_path` абсолютный путь к файлу сертификата корневого издателя из цепочки сертификатов сервера СУБД<sup>1</sup>.

При этом указанный выше файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен иметь метку доступа «600», установить которую можно с помощью команды с правами суперпользователя `chmod 600 путь_к_файлу`. Владелец файла сертификата корневого издателя из цепочки сертификатов сервера СУБД необходимо назначить пользователя «aeca» выполнив с правами суперпользователя команду `chown aeca:aeca путь_к_файлу`. Указанный файл должен располагаться в каталоге, к которому имеет доступ пользователь `aeca` (например, `/tmp`). В случае использования РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server на хосте eCA-RA файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен располагаться в каталоге `/opt/aecaRa` (или в его подкаталогах). Кроме того, в случае использования РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server на хосте eCA-RA необходимо дополнительно выполнить команду `restorecon -Rv "путь_к_файлу_сертификата_корневого_издателя_из_цепочки_сертификатов_сервера_СУБД"`.

На хосте eCA-RA применить изменения конфигурационного файла:

1. Запустите скрипт `install.sh` с параметрами согласно таблице 8 или введите параметры в диалоге при необходимости.

Пример запуска скрипта без параметров:

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

2. Выберите действие «[Update]».

По завершению выполнения указанной команды дальнейший обмен данными eCA-RA с СУБД будет осуществляться только по протоколу TLS. Если в СУБД, к которой выполняется подключение, отключён TLS, то eCA-RA не будет выполнять обмен данными с такой СУБД. При этом eCA-RA сможет установить соединение с СУБД только в случае, если её сертификат издан издателем, путь к сертификату которого указан в конфигурационном файле eCA-RA и только в случае, если имя хоста сервера СУБД соответствует указанному в сертификате.

<sup>1</sup> Если сертификат сервера СУБД выпущен подчинённым ЦС, необходимо указать путь до сертификата корневого ЦС.

## ПРИЛОЖЕНИЕ 4. РАЗВЁРТЫВАНИЕ КЛАСТЕРА

Программное средство обеспечивает объединение нескольких eCA-RA в кластер. Кластеризация обеспечивается в отказоустойчивом режиме с использованием внешнего средства балансировки нагрузки HAProxy<sup>1</sup>. Отказоустойчивый режим кластеризации обеспечивает как холодное «active-passive»<sup>2</sup>, так и горячее «active-active»<sup>3</sup> резервирование. Горячее «active-active» резервирование возможно только при «source»<sup>4</sup> балансировке.

**Внимание!** В кластере eCA-RA работает аутентификация по сертификату, а также по доменному логину и паролю. Аутентификация с использованием Kerberos-билета не поддерживается.

Развертывание кластера eCA-RA возможно в следующих вариантах:

- В виртуальной инфраструктуре путем клонирования виртуальной машины.
- С помощью переноса контейнера закрытого ключа.

### 4.1 Развертывание кластера в виртуальной среде с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Виртуальная машина с установленным eCA-RA (далее - BM1) - основной узел кластера.
- Клон BM1, созданный сразу установки на BM1 eCA-RA (далее - BM2) - резервный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - BM3).
- Клон BM1, созданный при необходимости при эксплуатации кластера (далее - BMP) – дополнительный резервный узел кластера.
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - BM4).

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации BM3 и BM4.

Порядок развертывания кластера:

- Выполните следующие действия на BM3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000<sup>5</sup> в файле<sup>6</sup>:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.

<sup>1</sup> Серверное программное обеспечение для обеспечения высокой доступности и балансировки нагрузки для TCP- и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов

<sup>2</sup> Это конфигурация отказоустойчивых кластеров, в которой одни узлы назначаются активными, а другие — резервными, готовыми взять на себя работу в случае отказа активного узла.

<sup>3</sup> Это архитектурный подход построения кластера, при котором оба или все узлы активны и работают одновременно, обрабатывая запросы и трафик.

<sup>4</sup> Это режим, при котором балансировщик выбирает узел кластера на основе хэш-суммы источника IP-адреса, с которого клиенты отправляют запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера.

<sup>5</sup> Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-RA взаимодействующего с СУБД.

<sup>6</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на ВМ1 установку eCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. приложение 2 настоящего руководства).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2 <sup>1</sup>.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-ra.service`.
- Выполните следующие действия на ВМ4:
  - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy` - для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy` - для ОС Astra Linux SE.
    - `apt-get install haproxy` - для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла HAProxy `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду, приведённому ниже:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- `DOMAINNAME_HOST1` – доменное имя ВМ1.
- `DOMAINNAME_HOST2` – доменное имя ВМ2.

<sup>1</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

- `admin:password` – имя и пароль учётной записи администратора для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя:  
`systemctl restart haproxy.service`.

В кластер можно подключать дополнительные резервные узлы ВМР. Для подключения нового резервного узла ВМР необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2 <sup>1</sup>:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР <sup>2</sup>.
- Запустите ВМР и дождитесь запуска службы `aeca-ra.service`.
- Выполните на ВМ4 редактирование конфигурационного файла HAProxy `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об доменном имени ВМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
```

где `DOMAINNAME_HOSTR` – доменное имя ВМР.

- Перезапустите HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя:  
`systemctl restart haproxy.service`

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки кластера все запросы, направляемые к еCA-RA через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера ВМ1. При недоступности основного узла кластера все запросы будут перенаправляться на резервный узел кластера ВМ2. При недоступности ВМ2 все запросы будут перенаправляться на дополнительный резервный узел кластера ВМР. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где `IP_VM4` - IP-адрес ВМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

## 4.2 Развертывание кластера с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Сервер с установленным еCA-RA (далее - АРМ1) - основной узел кластера.
- Сервер с установленным еCA-RA (далее - АРМ2) - резервный узел кластера.
- Сервер с установленным еCA-RA (далее - АРМР) – дополнительный резервный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - АРМ3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - АРМ4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1.1. Допускается использование одного сервера для реализации АРМ3 и АРМ4.

Порядок развертывания кластера:

<sup>1</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

<sup>2</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).



- Выполните следующие действия на АРМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС.
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000<sup>1</sup> в файле<sup>2</sup>:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.
    - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на АРМ1 установку еCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на АРМ3 (см. приложение 2 настоящего руководства).
- Выполните на АРМ2 установку еCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД<sup>3</sup>, установленной на АРМ3 (см. приложение 2 настоящего руководства)<sup>4</sup>.
- Скопируйте с АРМ1 содержимое каталога `/opt/aecaRa/dist/certificates` в каталог `/opt/aecaRa/dist/certificates` АРМ2<sup>5</sup>.
- Выполните следующие действия на ВМ4:
  - Выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy` для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy` для ОС Astra Linux SE.
    - `apt-get install haproxy` для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
```

<sup>1</sup> Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра еCA-RA, взаимодействующего с СУБД.

<sup>2</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

<sup>3</sup> В конфигурационном файле еCA-RA на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным для СУБД АРМ1.

<sup>4</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

<sup>5</sup> В случае, если на АРМ2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, выполните с правами суперпользователя следующую команду: `restorecon -Rv /opt/aecaRa/dist/certificates`

```

timeout client 50000
timeout server 50000
frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
    
```

где:

- DOMAINNAME\_HOST1 – доменное имя APM1.
  - DOMAINNAME\_HOST2 – доменное имя APM2.
  - admin:password – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя:
- ```
systemctl restart haproxy.service
```

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла необходимо выполнить действия, аналогичные действиям по подключению узла APM2<sup>1</sup>.

Выполните на APM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени APMР в соответствии с примером, представленном ниже:

```

backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
    
```

где DOMAINNAME\_HOSTR – доменное имя APMР.

На APM4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя:

```
systemctl restart haproxy.service
```

В результате в кластере появится дополнительный резервный узел.

В результате выполненной настройки кластера все запросы, направляемые к еCA-RA через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера APM1. При недоступности основного узла кластера все запросы будут перенаправляться на резервный узел кластера APM2. При недоступности APM2 все запросы будут перенаправляться на дополнительный резервный узел кластера APMР. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где IP\_VM4 - IP-адрес APM4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

<sup>1</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

## 4.3 Развертывания кластера в виртуальной среде с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Виртуальная машина с установленным eCA-RA (далее - BM1) - первый узел кластера.
- Клон BM1, созданный сразу завершения установки на BM1 eCA-RA (далее - BM2) - второй узел кластера.
- Клон BM1, созданный при необходимости при эксплуатации кластера (далее - BMP) - дополнительный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - BM3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - BM4).

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации BM3 и BM4.

Порядок развертывания кластера:

- Выполните следующие действия на BM3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000 <sup>1</sup> в файле <sup>2</sup>:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.
    - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на BM1 установку eCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на BM3 (см. приложение 2 настоящего руководства).
- Средствами используемого гипервизора клонируйте BM1, тем самым создав BM2 <sup>3</sup>.
- Запустите BM2 и дождитесь завершения запуска службы `aeca-ra.service`.
- Выполните следующие действия на BM4:
  - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy` - для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy` - для ОС Astra Linux SE.
    - `apt-get install haproxy` - для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
```

<sup>1</sup> Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-RA, взаимодействующего с СУБД.

<sup>2</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

<sup>3</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

```
stats socket /run/haproxy/admin.sock mode 660 level admin
stats timeout 30s
user haproxy
group haproxy
daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- DOMAINNAME\_HOST1 – доменное имя ВМ1.
  - DOMAINNAME\_HOST2 – доменное имя ВМ2.
  - admin:password – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя:
- ```
systemctl restart haproxy.service.
```

В кластер можно подключать дополнительные узлы ВМР. Для подключения нового узла ВМР необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР<sup>1</sup>.
- Запустите ВМР и дождитесь запуска службы `aeca-ra.service`.
- Выполните на ВМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени ВМР в соответствии с примером, представленном ниже:

---

<sup>1</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где `DOMAINNAME_HOSTR` - это доменное имя ВМР.

- Перезапустить HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя:  
`systemctl restart haproxy.service`.

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где `IP_VM4` - IP-адрес ВМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

## 4.4 Развертывание кластера с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Сервер с установленным eCA-RA (далее - АРМ1) – первый узел кластера.
- Сервер с установленным eCA-RA (далее - АРМ2) – второй узел кластера.
- Сервер с установленным eCA-RA (далее - АРМР) – дополнительный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - АРМ3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - АРМ4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1.1.

Допускается использование одного сервера для реализации АРМ3 и АРМ4.

Порядок развертывания кластера:

- Выполните следующие действия на АРМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000<sup>1</sup> в файле<sup>2</sup>:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.
    - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на АРМ1 установку eCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на АРМ3 (см. приложение 2 настоящего руководства).

<sup>1</sup> Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-CA, взаимодействующего с СУБД.

<sup>2</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- На АРМ2 выполните установку еCA-RA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД<sup>1</sup>, установленной на АРМ3 (см. приложение 2 настоящего руководства)<sup>2</sup>.
- Скопируйте с АРМ1 содержимое каталога `/opt/aecaRa/dist/certificates` в каталог `/opt/aecaRa/dist/certificates` АРМ2<sup>3</sup>.
- Выполните следующие действия на АРМ4:
  - Выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy`- для ОС Astra Linux SE.
    - `apt-get install haproxy`- для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

<sup>1</sup> В конфигурационном файле на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным СУБД АРМ1.

<sup>2</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

<sup>3</sup> В случае, если на АРМ2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, выполните с правами суперпользователя следующую команду: `restorecon -Rv /opt/aecaRa/dist/certificates`

- `DOMAINNAME_HOST1` – доменное имя APM1.
- `DOMAINNAME_HOST2` – доменное имя APM2.
- `admin:password` – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя:  
`systemctl restart haproxy.service`

В кластер можно подключать дополнительные резервные узлы APMР. Для подключения нового резервного узла APMР необходимо выполнить действия, аналогичные действиям по подключению узла APM2 <sup>1</sup>.

- Выполните на APM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени APMР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где `DOMAINNAME_HOSTR` - это доменное APMР.

- На APM4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя:  
`systemctl restart haproxy.service`

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_ARM4:8404/stats` (где `IP_ARM4` - IP-адрес APM4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

## 4.3 Обновление ПО узлов кластера

Процесс обновления кластера eCA-RA:

- Выполните резервное копирование данных на всех узлах кластера (см. раздел 13 настоящего руководства).
- Для кластера по схеме «active-passive» на всех резервных узлах выполните остановку службы eCA-RA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-ra.service`.
- Для кластера по схеме «active-active» на всех узлах кроме первого, выполните остановку службы eCA-RA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-ra.service`.
- Для кластера по схеме «active-passive» выполнить обновление ПО eCA-RA на основном узле (см. раздел 14 настоящего руководства).
- Для кластера по схеме «active-active» выполнить обновление ПО eCA-RA на первом узле кластера (см. раздел 14 настоящего руководства).

---

<sup>1</sup> Если на основном узле включен офлайн выпуск сертификатов, то отключите его на резервном узле (параметра `offline_enrollment_enabled` конфигурационного файла).

- Вне зависимости от схемы кластера выполните обновление ПО еСА-РА на всех остальных узлах кластера (см. раздел 14 настоящего руководства).

Критерием правильности установки обновления ПО кластера является отображение информации о новой версии в окне «О программе» веб-интерфейса и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_Haproxy:8404/stats` (где `IP_Haproxy` - IP-адрес ВМ4 или АРМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.



## ПРИЛОЖЕНИЕ 5. НАСТРОЙКА KERBEROS В ВЕБ-БРАУЗЕРЕ

**Внимание!** Предварительно на клиенте должен быть настроен Kerberos, клиент должен быть подключён к домену и клиент должен использовать браузер с поддержкой Kerberos.

Для того, чтобы в браузере клиента при работе с eCA-RA была доступна аутентификация по Kerberos необходимо внести доменное имя eCA-RA в список доверенных URI, для которых используется аутентификация Kerberos в соответствии с инструкциями ниже.

### 5.1 Настройка веб-браузера Firefox

Далее в примере:

- `aeca.al.rd.ru`, `aecal.al.rd.ru` - доменные имена eCA-RA
- `al.rd.ru` - домен, (`AL.RD.RU` - realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Запустите веб-браузер Mozilla Firefox.
- В адресной строке введите `about:config`.
- Нажмите на кнопку <Принять риск и продолжить>.
- В поле поиска введите `negotiate`, чтобы ограничить список отображаемых параметров.
- Установите параметру `network.negotiate-auth.trusted-uris` одно из следующих значений (см. Рисунок 125):
  - Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, введите полное доменное eCA-RA (например, `aeca.al.rd.ru`).
  - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.al.rd.ru`).
  - Чтобы разрешить SPNEGO аутентификацию для нескольких eCA-RA, введите их полные доменные имена через запятую (например, `aeca.al.rd.ru, aecal.al.rd.ru`).
- Продублируйте введённое значение параметра `network.negotiate-auth.trusted-uris` в параметре `network.negotiate-auth.delegation-uris`.

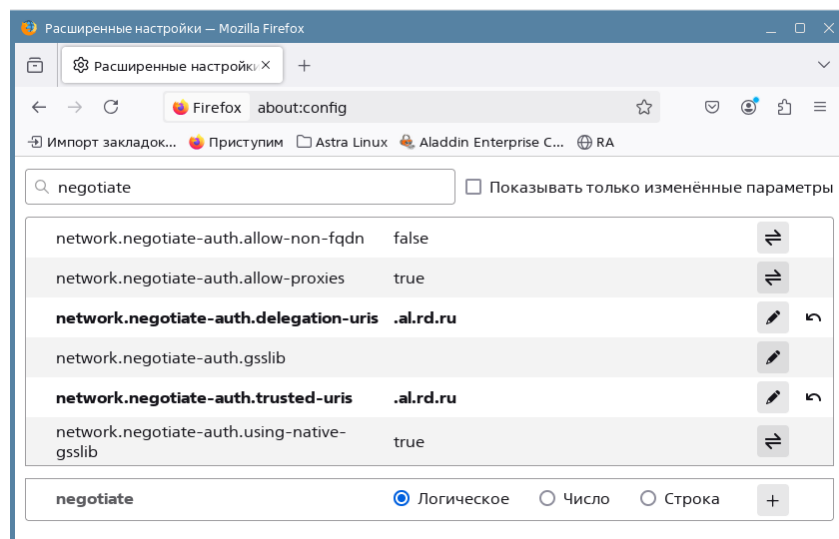


Рисунок 125 - Настройка Kerberos-аутентификации в веб-браузере Firefox

## 5.2 Настройка веб-браузера Chromium

Далее в примере:

- `aeca.al.rd.ru`, `aecal.al.rd.ru` - доменные имена eCA-RA.
- `al.rd.ru` - домен, (`AL.RD.RU` - realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Создайте в каталоге `/etc/chromium/policies/managed` файл `policies.json` выполнив следующую команду с правами суперпользователя:

```
touch /etc/chromium/policies/managed/policies.json
```

- Откройте файл для редактирования выполнив следующую команду с правами суперпользователя:

```
nano /etc/chromium/policies/managed/policies.json
```

- В файле `policies.json` укажите следующие политики в формате JSON:

```
{
  "AuthServerAllowlist": "*.al.rd.ru",
  "AuthSchemes": "ntlm,negotiate"
}
```

Примечания:

- Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, укажите для политики «AuthServerAllowlist» полное доменное eCA-RA (например, `aeca.al.rd.ru`).
- Чтобы разрешить SPNEGO аутентификацию для целого домена, укажите для политики «AuthServerAllowlist» имя домена (например, `*.al.rd.ru`).
- Чтобы разрешить SPNEGO аутентификацию для нескольких eCA-RA, укажите для политики «AuthServerAllowlist» их полные доменные имена через запятую (например, `aeca.al.rd.ru, aecal.al.rd.ru`).
- Запустите веб-браузер Chromium и введите в адресной строке `chrome://policy`.
- Убедитесь, что политики были применены (см. Рисунок 126).

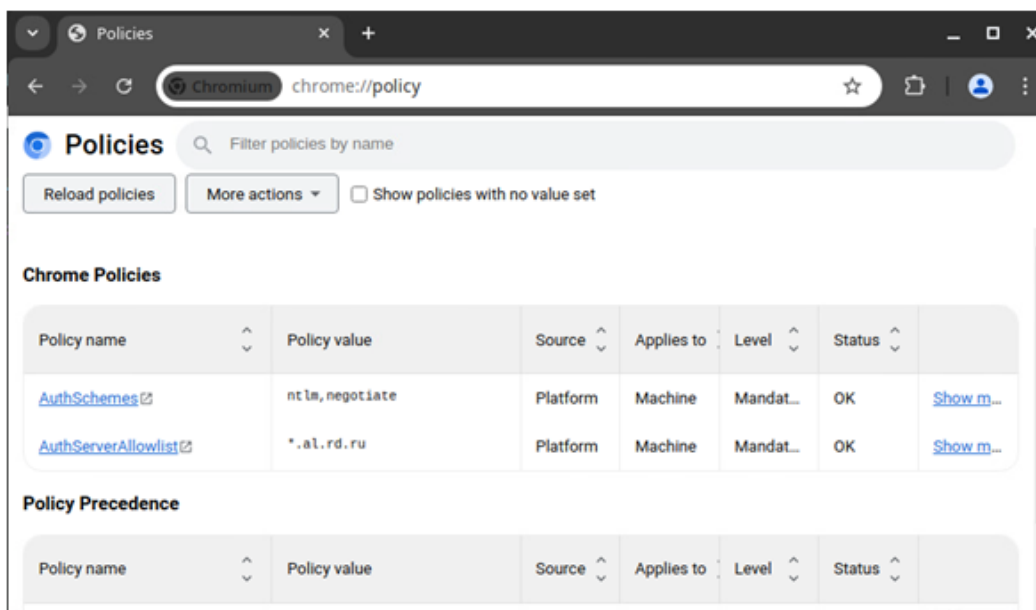


Рисунок 126 - Настройка Kerberos-аутентификации в веб-браузере Chromium

## ПРИЛОЖЕНИЕ 6. ПЕРЕЧЕНЬ РЕГИСТРИРУЕМЫХ СОБЫТИЙ

### 6.1 События запуска/остановки служб, применения параметров конфигурационного файла

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Запуск службы	RAENV0000	INFO	Краткое описание: Запуск службы Атрибуты: – Название службы
Остановка службы	RAENV0001	INFO	Краткое описание: Остановка службы Атрибуты: – Название службы
Применение параметров конфигурационного файла	RAENV0002	INFO	Описание: Применение параметров конфигурационного файла Атрибуты: – Наличие изменений в конфигурационном файле – Параметры конфигурационного файла. В данном атрибуте присутствуют все параметры и значения параметров применённого конфигурационного файла в формате «ключ=значение», кроме параметров «database_password», «aeca_ca_auth_password» и «certificate_raw_server_password»

### 6.2 События аутентификации пользователей

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

## 6.3 События работы с УЗ получателей сертификатов

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание УЗ получателя сертификата	RAENV0200	INFO	Краткое описание: Создание УЗ Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя
Ошибка создания УЗ получателя сертификата	RAENV0201	ERROR	Краткое описание: Ошибка создания УЗ Атрибуты: – Отображаемое имя пользователя (может отсутствовать) – Роль пользователя (может отсутствовать) – Причина ошибки
Блокировка УЗ получателя сертификата	RAENV0202	INFO	Краткое описание: Блокировка УЗ Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя
Ошибка блокировки УЗ получателя сертификата	RAENV0203	ERROR	Краткое описание: Ошибка блокировки УЗ Атрибуты: – Id пользователя (может отсутствовать) – Отображаемое имя пользователя (может отсутствовать) – Роль пользователя (может отсутствовать) – Причина ошибки
Активация УЗ получателя сертификата	RAENV0204	INFO	Краткое описание: Активация УЗ Атрибуты: – Id пользователя – Отображаемое имя пользователя – Роль пользователя
Ошибка активации УЗ получателя сертификата	RAENV0205	ERROR	Краткое описание: Ошибка активации УЗ Атрибуты: – Id пользователя (может отсутствовать) – Отображаемое имя пользователя (может отсутствовать) – Роль пользователя (может отсутствовать) – Причина ошибки

## 6.4 События работы с заявками

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание заявки	RAENV0300	INFO	<p>Краткое описание: Создание заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> </ul>
Ошибка создания заявки	RAENV0301	ERROR	<p>Краткое описание: Ошибка создания заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Сценарий (может отсутствовать)</li> <li>– CN в заявке (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Имя шаблона (может отсутствовать)</li> <li>– Id получателя сертификата (может отсутствовать)</li> <li>– Имя получателя сертификата (может отсутствовать)</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Обработка заявки	RAENV0302	INFO	<p>Краткое описание: Обработка заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Режим обработки</li> <li>– Id правил</li> </ul>
Выпуск сертификата по заявке	RAENV0303	INFO	<p>Краткое описание: Выпуск сертификата по заявке</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Id сертификата</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка выпуска сертификата по заявке	RAENV0304	ERROR	<p>Краткое описание: Ошибка выпуска сертификата по заявке</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Отмена заявки	RAENV0305	INFO	<p>Краткое описание: Отмена заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> </ul>
Ошибка отмены заявки	RAENV0306	ERROR	<p>Краткое описание: Ошибка отмены заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Отклонение заявки	RAENV0307	INFO	<p>Краткое описание: Отклонение заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> </ul>
Ошибка отклонения заявки	RAENV0308	ERROR	<p>Краткое описание: Ошибка отклонения заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Импорт сертификата на носитель	RAENV0309	INFO	<p>Краткое описание: Импорт сертификата на носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Id сертификата</li> </ul>
Ошибка импорта сертификата на носитель	RAENV0310	ERROR	<p>Краткое описание: Ошибка импорта сертификата на носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Id сертификата (может отсутствовать)</li> </ul>
Отзыв сертификата	RAENV0311	INFO	<p>Краткое описание: Отзыв сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Id сертификата</li> <li>– Причина отзыва</li> <li>– Комментарий к отзыву</li> </ul>
Ошибка отзыва заявки	RAENV0312	ERROR	<p>Краткое описание: Ошибка отзыва сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id заявки</li> <li>– Сценарий</li> <li>– CN в заявке</li> <li>– Id шаблона</li> <li>– Имя шаблона</li> <li>– Id получателя сертификата</li> <li>– Имя получателя сертификата</li> <li>– Статус</li> <li>– Внешний ключ (может отсутствовать)</li> <li>– Id сертификата (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>

## 6.5 События работы с ключевыми носителями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Подключение ключевого носителя	RAENV0400	INFO	<p>Краткое описание: Подключение ключевого носителя</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Свойства носителя</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка подключения ключевого носителя	RAENV0401	ERROR	Краткое описание: Ошибка подключения ключевого носителя Атрибуты: – Свойства носителя – Причина ошибки

## 6.6 События экспорта

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
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

## 6.7 События работы с правилами выпуска

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание правила выпуска	RAENV0600	INFO	Краткое описание: Создание правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа
Ошибка создания правила выпуска	RAENV0601	ERROR	Краткое описание: Ошибка создания правила выпуска Атрибуты: – Отображаемое имя правила (может отсутствовать) – Режим обработки (может отсутствовать) – Статус (может отсутствовать) – Субъекты доступа (может отсутствовать) – Объекты доступа (может отсутствовать) – Причина ошибки



Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Редактирование правила выпуска	RAENV0602	INFO	<p>Краткое описание: Редактирование правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> </ul>
Ошибка редактирования правила выпуска	RAENV0603	ERROR	<p>Краткое описание: Ошибка редактирования правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила (может отсутствовать)</li> <li>– Режим обработки (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Субъекты доступа (может отсутствовать)</li> <li>– Объекты доступа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Запуск правила выпуска	RAENV0604	INFO	<p>Краткое описание: Запуск правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> </ul>
Ошибка запуска правила выпуска	RAENV0605	ERROR	<p>Краткое описание: Ошибка запуска правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> <li>– Причина ошибки</li> </ul>
Остановка правила выпуска	RAENV0606	INFO	<p>Краткое описание: Остановка правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> </ul>
Ошибка остановки правила выпуска	RAENV0607	ERROR	<p>Краткое описание: Ошибка остановки правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> <li>– Причина ошибки</li> </ul>
Удаление правила выпуска	RAENV0608	INFO	<p>Краткое описание: Удаление правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка удаления правила выпуска	RAENV0609	ERROR	<p>Краткое описание: Ошибка удаления правила выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– ID правила</li> <li>– Отображаемое имя правила</li> <li>– Режим обработки</li> <li>– Статус</li> <li>– Субъекты доступа</li> <li>– Объекты доступа</li> <li>– Причина ошибки</li> </ul>

## 6.8 События работы с веб-сервером и издателями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Изменение сертификата веб-сервера	RAENV0700	INFO	<p>Краткое описание: Изменение сертификата веб-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Серийный номер</li> <li>– Отпечаток</li> <li>– CN в сертификате</li> <li>– SDN издателя</li> <li>– Действует с</li> <li>– Действует по</li> </ul>
Ошибка изменения сертификата веб-сервера	RAENV0701	ERROR	<p>Краткое описание: Ошибка изменения сертификата веб-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Серийный номер (может отсутствовать)</li> <li>– Отпечаток (может отсутствовать)</li> <li>– CN в сертификате (может отсутствовать)</li> <li>– Действует с (может отсутствовать)</li> <li>– Действует по (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение списка разрешённых издателей	RAENV0702	INFO	<p>Краткое описание: Изменение списка разрешённых издателей</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Обновлённый список разрешённых издателей</li> </ul>
Ошибка изменения списка разрешённых издателей	RAENV0703	ERROR	<p>Краткое описание: Ошибка изменения списка разрешённых издателей</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Обновлённый список разрешённых издателей (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>

## 6.9 События Offline-выпуска

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Запуск Offline-выпуска	RAENV0800	INFO	<p>Краткое описание: Запуск Offline-выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Каталог запросов</li> <li>– Каталог сертификатов</li> <li>– Каталог ошибок</li> <li>– Id шаблона</li> </ul>
Завершение Offline-выпуска	RAENV0801	INFO	<p>Краткое описание: Завершение Offline-выпуска</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Список Id заявок, созданных в результате Offline-выпуска</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			– Количество запросов, по которым заявки не были созданы

## 6.10 События работы с резервными копиями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Успешное создание резервной копии	RAENV0900	INFO	Краткое описание: Успешное создание резервной копии Атрибуты: – Абсолютное имя файла резервной копии – Наличие БД в резервной копии
Ошибка создания резервной копии	RAENV0901	ERROR	Краткое описание: Ошибка создания резервной копии Атрибуты: – Абсолютное имя файла резервной копии (может отсутствовать) – Причина ошибки
Успешное восстановление из резервной копии	RAENV0902	INFO	Краткое описание: Успешное восстановление из резервной копии Атрибуты: – Абсолютное имя файла резервной копии – Восстановление БД
Ошибка восстановления из резервной копии	RAENV0903	ERROR	Краткое описание: Ошибка восстановления из резервной копии Атрибуты: – Абсолютное имя файла резервной копии (может отсутствовать) – Причина ошибки

## 6.11 События контроля целостности

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Успешная проверка контрольных сумм	RAENV1000	INFO	Краткое описание: Успешная проверка контрольных сумм
Неуспешная проверка контрольных сумм	RAENV1001	ERROR	Краткое описание: Неуспешная проверка контрольных сумм Атрибуты: Причина ошибки

## 6.12 События архивации и очистки записей аудита

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Начало очистки записей аудита	RAENV1100	INFO	Краткое описание: Начало очистки записей аудита
Завершение очистки записей аудита	RAENV1101	ERROR	Краткое описание: Завершение очистки записей аудита
Ошибка очистки записей аудита	RAENV1102	INFO	Краткое описание: Ошибка очистки записей аудита Атрибуты: Причина ошибки
Начало архивации записей аудита	RAENV1103	ERROR	Краткое описание: Начало архивации записей аудита
Завершение архивации записей аудита	RAENV1104	INFO	Краткое описание: Завершение архивации записей аудита
Ошибка архивации записей аудита	RAENV1105	ERROR	Краткое описание: Ошибка архивации записей аудита

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			Атрибуты: Причина ошибки

## 6.13 События работы с Syslog

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Добавление Syslog-сервера	RAENV1200	INFO	Краткое описание: Добавление Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Флаг отправки сообщений</li> </ul>
Ошибка добавления Syslog-сервера	RAENV1201	ERROR	Краткое описание: Ошибка добавления Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста (может отсутствовать)</li> <li>– Порт (может отсутствовать)</li> <li>– Протокол (может отсутствовать)</li> <li>– Флаг отправки сообщений (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение параметров Syslog-сервера	RAENV1202	INFO	Краткое описание: Изменение параметров Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Флаг отправки сообщений</li> </ul>
Ошибка изменения параметров Syslog-сервера	RAENV1203	ERROR	Краткое описание: Ошибка изменения параметров Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста (может отсутствовать)</li> <li>– Порт (может отсутствовать)</li> <li>– Протокол (может отсутствовать)</li> <li>– Флаг отправки сообщений (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Удаление Syslog-сервера	RAENV1204	INFO	Краткое описание: Удаление Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Флаг отправки сообщений</li> </ul>
Ошибка удаления Syslog-сервера	RAENV1205	ERROR	Краткое описание: Ошибка удаления Syslog-сервера Атрибуты: <ul style="list-style-type: none"> <li>– Адрес хоста</li> <li>– Порт</li> <li>– Протокол</li> <li>– Флаг отправки сообщений</li> <li>– Причина ошибки</li> </ul>

## 6.14 События перевыпуска сертификатов технологической учётной записи eCA-RA для связи с eCA-CA

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Перевыпуск сертификата технологической учётной записи	RAENV1300	INFO	<p>Краткое описание: Перевыпуск сертификата технологической учётной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id технологической учётной записи</li> <li>– Id сертификата</li> <li>– Id шаблона</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> </ul>
Ошибка перевыпуска сертификата технологической учётной записи	RAENV1301	ERROR	<p>Краткое описание: Ошибка перевыпуска сертификата технологической учётной записи</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id технологической учётной записи (может отсутствовать)</li> <li>– Id сертификата (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>

## 6.15 События SCEP

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание SCEP-политики	RAENV1400	INFO	<p>Краткое описание: Создание SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики</li> <li>– ChallengePassword (может отсутствовать)</li> <li>– Id шаблона</li> <li>– Статус</li> </ul>
Ошибка создания SCEP-политики	RAENV1401	ERROR	<p>Краткое описание: Ошибка создания SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики (может отсутствовать)</li> <li>– ChallengePassword (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение параметров SCEP-политики.	RAENV1402	INFO	<p>Краткое описание: Изменение параметров SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики</li> <li>– ChallengePassword (Исходное значение; Конечное значение)</li> <li>– Id шаблона (Исходное значение; Конечное значение)</li> <li>– Статус</li> </ul>
Ошибка изменения параметров SCEP-политики	RAENV1403	ERROR	<p>Краткое описание: Ошибка изменения параметров SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики</li> <li>– ChallengePassword (может отсутствовать)</li> <li>– Id шаблона</li> <li>– Статус</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Удаление SCEP-политики	RAENV1404	INFO	<p>Краткое описание: Удаление SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики</li> <li>– ChallengePassword (может отсутствовать)</li> <li>– Id шаблона</li> <li>– Статус</li> </ul>
Ошибка удаления SCEP-политики	RAENV1405	ERROR	<p>Краткое описание: Ошибка удаления SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-политики</li> <li>– ChallengePassword (может отсутствовать)</li> <li>– Id шаблона</li> <li>– Статус</li> <li>– Причина ошибки</li> </ul>
Создание SCEP-профиля	RAENV1406	INFO	<p>Краткое описание: Создание SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля</li> <li>– Отображаемое имя SCEP-профиля</li> <li>– Отображаемое имя Центра сертификации подключённого eCA-CA</li> <li>– Алгоритм шифрования ответов SCEP-сервера</li> <li>– Id технологического сертификата</li> <li>– Id шаблона</li> <li>– Наименование шаблона</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> <li>– Обновлять технологический сертификат автоматически</li> <li>– Статус</li> </ul>
Ошибка создания SCEP-профиля	RAENV1407	ERROR	<p>Краткое описание: Ошибка создания SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля (может отсутствовать)</li> <li>– Отображаемое имя SCEP-профиля (может отсутствовать)</li> <li>– Отображаемое имя Центра сертификации подключённого eCA-CA (может отсутствовать)</li> <li>– Алгоритм шифрования ответов SCEP-сервера (может отсутствовать)</li> <li>– Id технологического сертификата (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Наименование шаблона (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Обновлять технологический сертификат автоматически (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Изменение параметров SCEP-профиля.	RAENV1408	INFO	<p>Краткое описание: Изменение параметров SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля</li> <li>– Отображаемое имя SCEP-профиля (Исходное значение; Конечное значение)</li> <li>– Отображаемое имя Центра сертификации подключённого eCA-CA</li> <li>– Алгоритм шифрования ответов SCEP-сервера (Исходное значение; Конечное значение)</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			<ul style="list-style-type: none"> <li>– Id технологического сертификата (Исходное значение; Конечное значение)</li> <li>– Id шаблона (Исходное значение; Конечное значение)</li> <li>– Наименование шаблона (Исходное значение; Конечное значение)</li> <li>– Алгоритм ключа (Исходное значение; Конечное значение)</li> <li>– Длина ключа (Исходное значение; Конечное значение)</li> <li>– Обновлять технологический сертификат автоматически (Исходное значение; Конечное значение)</li> <li>– Статус (может отсутствовать)</li> </ul>
Ошибка изменения параметров SCEP-политики	RAENV1409	ERROR	<p>Краткое описание: Ошибка изменения SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля (может отсутствовать)</li> <li>– Отображаемое имя SCEP-профиля (может отсутствовать)</li> <li>– Отображаемое имя Центра сертификации подключённого eCA-CA (может отсутствовать)</li> <li>– Алгоритм шифрования ответов SCEP-сервера (может отсутствовать)</li> <li>– Id технологического сертификата (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Наименование шаблона (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Обновлять технологический сертификат автоматически (может отсутствовать)</li> <li>– Статус (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Перевыпуск технологического сертификата SCEP-профиля	RAENV1410	INFO	<p>Краткое описание: Перевыпуск технологического сертификата SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля</li> <li>– Id технологического сертификата</li> <li>– Id шаблона</li> <li>– Наименование шаблона</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> </ul>
Ошибка перевыпуска технологического сертификата SCEP-профиля	RAENV1411	ERROR	<p>Краткое описание: Ошибка перевыпуска технологического сертификата SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля (может отсутствовать)</li> <li>– Id технологического сертификата (может отсутствовать)</li> <li>– Id шаблона (может отсутствовать)</li> <li>– Наименование шаблона (может отсутствовать)</li> <li>– Алгоритм ключа (может отсутствовать)</li> <li>– Длина ключа (может отсутствовать)</li> <li>– Причина ошибки</li> </ul>
Удаление SCEP-профиля	RAENV1412	INFO	<p>Краткое описание: Удаление SCEP-профиля</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля</li> <li>– Отображаемое имя SCEP-профиля</li> <li>– Отображаемое имя Центра сертификации подключённого eCA-CA</li> </ul>

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			<ul style="list-style-type: none"> <li>– Алгоритм шифрования ответов SCEP-сервера</li> <li>– Id технологического сертификата</li> <li>– Id шаблона</li> <li>– Наименование шаблона</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> <li>– Обновлять технологический сертификат автоматически</li> <li>– Статус</li> </ul>
Ошибка удаления SCEP-профиля	RAENV1413	ERROR	<p>Краткое описание: Ошибка удаления SCEP-политики</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> <li>– Id SCEP-профиля</li> <li>– Отображаемое имя SCEP-профиля</li> <li>– Отображаемое имя Центра сертификации подключённого еСА-СА</li> <li>– Алгоритм шифрования ответов SCEP-сервера</li> <li>– Id технологического сертификата</li> <li>– Id шаблона</li> <li>– Наименование шаблона</li> <li>– Алгоритм ключа</li> <li>– Длина ключа</li> <li>– Обновлять технологический сертификат автоматически</li> <li>– Статус</li> <li>– Причина ошибки</li> </ul>



## ПРИЛОЖЕНИЕ 7. НАСТРОЙКА ВЗАИМОДЕЙСТВИЯ С КРИПТОПРОВАЙДЕРОМ СКЗИ «КРИПТОПРО CSP»

Взаимодействие eCA-RA с криптопровайдером СКЗИ «КриптоПро CSP» из состава программного средства осуществляется через модуль «КриптоПро Java CSP»<sup>1</sup>.

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с eCA-RA необходимо подготовить внешнюю гамму<sup>2</sup>.

Порядок настройки взаимодействия СКЗИ «КриптоПро CSP» с eCA-RA:

- На сервере программного средства выполнить установку криптопровайдера СКЗИ «КриптоПро CSP» в соответствии с инструкцией, описанной в разделе 2 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.

**Внимание!** Перед установкой СКЗИ «КриптоПро CSP» в ОС Альт 8 СП Сервер установите пакет `newt52` командой с правами суперпользователя `apt-get install newt52`.

**Внимание!** В приведённых ниже командах файлы `cpSSL.jar` и `sspiSSL.jar` нужно указывать только если между ЦС и ЦР нужно взаимодействие по ГОСТ TLS.

- При отсутствии создайте каталог `/opt/aecaRa/services/cryptoproviders` командой с правами суперпользователя:

```
mkdir -p /opt/aecaRa/services/cryptoproviders
```

- Переместите в каталог `/opt/aecaRa/services/cryptoproviders` файлы `ASN1P.jar`, `asn1rt.jar`, `JCP.jar`, `JCSP.jar`, `cpSSL.jar` и `sspiSSL.jar` из состава дистрибутива ПО «КриптоПро Java CSP» и «КриптоПро Java TLS» командой с правами суперпользователя:

```
cp {ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar,sspiSSL.jar}
/opt/aecaRa/services/cryptoproviders
```

- Назначьте права доступа на скопированные файлы:
  - Если выполняется первоначальная установка eCA-RA, то назначьте файлам права доступа (`chmod 777`) командой с правами суперпользователя:

```
chmod 777
/opt/aecaRa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.
jar,sspiSSL.jar} -R
```

- Если eCA-RA был установлен ранее, то назначьте владельцем данных файлов пользователя «аеса» и предоставьте ему права доступа к файлам (`chmod 700`) командами с правами суперпользователя:

```
chown aeca:aeca
/opt/aecaRa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.
jar,sspiSSL.jar} -R
chmod 700 -R
/opt/aecaRa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.
jar,sspiSSL.jar}
```

- Если используется уже заранее подготовленная внешняя гамма, то пропустите этот пункт. Иначе подготовьте внешнюю гамму с помощью утилиты `/opt/cproscsp/bin/amd64/genkpim` (утилита `genkpim` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma
/opt/cproscsp/bin/amd64/genkpim <количество ключей> 0x12345678 ~/gamma
```

<sup>1</sup> Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

<sup>2</sup> Заранее сформированный набор случайных данных, необходимых для генерирования закрытых ключей. При создании сертификатов на КН и с закрытым ключом (PKCS#12) для субъектов с использованием алгоритмов ключей, для которых в активном центре сертификации выбран криптопровайдер СКЗИ «КриптоПро CSP», Центр регистрации использует внешнюю гамму, заранее подготовленную на биологическом датчике случайных числе (БДСЧ) СКЗИ «КриптоПро CSP».

- На хосте eCA-RA поместите каталог с заранее подготовленной внешней гаммой в каталог `/opt/aecaRa/dist/` командой с правами суперпользователя:

```
cp -a ~/gamma/. /opt/aecaRa/dist/gamma
```

- В результате в каталоге `/opt/aecaRa/dist/gamma` появятся подкаталоги `db1`, `db2`, `krim`.
  - Если выполняется первоначальная установка eCA-RA, то назначьте права доступа файлам (`chmod 777`) командой с правами суперпользователя:

```
chmod -R 777 /opt/aecaRa/dist/gamma
```

- Если eCA-RA был установлен ранее, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа (`chmod 700`) командами с правами суперпользователя:

```
chown -R aeca:aeca /opt/aecaRa/dist/gamma
```

```
chmod -R 700 /opt/aecaRa/dist/gamma
```

- Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд с правами суперпользователя<sup>1</sup>:

```
./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1
/opt/aecaRa/dist/gamma/db1/kis_1
./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1
/opt/aecaRa/dist/gamma/db2/kis_1
```

- Если eCA-RA был установлен ранее, перезапустите сервис `aeca-ra.service` командой с правами суперпользователя:

```
systemctl restart aeca-ra.service
```

<sup>1</sup> Подключение осуществляется с помощью файла `cpconfig` (находится в `/opt/cprocsp/sbin/amd64`). Путь к файлу в командах приведен с учётом нахождения в каталоге `/opt/cprocsp/sbin/amd64`.

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

<b>БД</b>	- База данных
<b>ЗПС</b>	- Замкнутая программная среда
<b>ОС</b>	- Операционная система
<b>ПО</b>	- Программное обеспечение
<b>СКЗИ</b>	- Средство криптографической защиты информации
<b>СУБД</b>	- Система управления базами данных
<b>ЦР</b>	- Центр регистрации
<b>ЦС</b>	- Центр сертификации
<b>AIA</b>	- Authority Information Access
<b>API</b>	- Application Programming Interface
<b>CSV</b>	- Comma-Separated Values
<b>CRL</b>	- Certificate Revocation List
<b>HDD</b>	- Hard (magnetic) Disk Drive
<b>HTTPS</b>	- Hyper Text Transfer Protocol Secure
<b>HTTP</b>	- Hyper Text Transfer Protocol
<b>LDAP</b>	- Lightweight Directory Access Protocol
<b>PKI</b>	- Public Key Infrastructure
<b>SCEP</b>	- Simple Certificate Enrollment Protocol
<b>SPN</b>	- Service Principal Name
<b>SSD</b>	- Solid-State Drive
<b>SSL</b>	- Secure Sockets Layer
<b>TCP</b>	- Transmission Control Protocol
<b>TLS</b>	- Transport Layer Security
<b>VGA</b>	- Video Graphics Array
<b>URL</b>	- Uniform Resource Locator
<b>WSTEP</b>	- WS-Trust X.509v3 Token Enrollment Extensions

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**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.

**Заявка** - это заявление от пользователя на получение сертификата, полученное через API или веб-интерфейс, содержащее совокупность данных о пользователе (запрос на сертификат (CSR)).

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

**Корневой ЦС** - экземпляр центра сертификации в информационной системе, имеющий абсолютное доверие со стороны всех участников процесса строгой аутентификации. С точки зрения службы безопасности предприятия должен быть обеспечен максимальным уровнем защиты (отдельный ПК, отключённый от сети, с доступом ограниченного круга лиц). Корневой ЦС владеет само подписанным сертификатом, который должен распространяться доверенным способом в информационной системе.

**Лог** - это текстовый файл, куда автоматически записывается важная информация о работе сервисов программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». Полученный лог-файл - журнал событий.

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

**Подчинённый ЦС** - экземпляр центра сертификации в информационной системе, обладающий функцией управления политиками строгой аутентификации или функцией управления жизненным циклом сертификатов субъектов информационной системы. Подчинённый ЦС владеет сертификатом, выданным вышестоящим ЦС (Корневым или другим Подчинённым), который используется для проверки всей цепочки доверия сертификатов.

**Принципал (principal)** - уникальное имя для клиента (пользователя, хоста или сервиса), которому разрешается аутентификация в Kerberos.

**Расширение pgcrypto** - предоставляет криптографические функции, которые позволяют администраторам баз данных PostgreSQL хранить определённые столбцы данных в зашифрованном виде.

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

**Событие безопасности** - идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

**Список отозванных сертификатов (Certificate Revocation List - CRL)** - список аннулированных (отозванных) сертификатов, издаётся центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

**Субъект** - пользователь информационной системы или устройство (сервер, шлюз, маршрутизатор). Субъекту для строгой аутентификации в информационной системе в центре сертификации выдаётся сертификат. Синоним - конечная сущность (end entity).

**Технологический ЦС** - экземпляр центра сертификации в информационной системе, обладающий функцией первичной настройки программного комплекса «Центр сертификации Aladdin Enterprise Certificate Authority».

**Тикет (ticket)** - временные данные, выдаваемые клиенту для аутентификации на сервере, на котором располагается необходимый сервис.

**Центр регистрации** - это функциональный компонент программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», предназначенный для хранения регистрационных данных пользователей, запросов на сертификаты и сертификатов пользователей; обработки заявок пользователей на выпуск сертификата.

**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 комплекс «Центр сертификации Aladdin Enterprise Certificate Authority» является частью программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

**Kerberos** - сетевой протокол аутентификации, который обеспечивает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

**Keytab-файл** - это файл, содержащий пары Kerberos-принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля.

**Веб-интерфейс** - интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы.

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]