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	2.2.1
Листов	176
Дата	17.06.2025

Авторские права, товарные знаки, ограничения

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

Соглашения:

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

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

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

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

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

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

Требования к использованию

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

Использование ПО

Пользователь вправе:

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

- встраивать ПО любым способом в продукты и решения Пользователя;

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

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

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

Я ПРОЧИТАЛ И ПОНЯЛ НАСТОЯЩЕЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ И СОГЛАСЕН ВЫПОЛНЯТЬ ВСЕ ЕГО УСЛОВИЯ.

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

ЕСЛИ Я НЕ ПРИНИМАЮ ЭТО ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ИЛИ ХОТЯ БЫ ОДИН ИЗ ЕГО ПУНКТОВ, ТО ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ НЕ ВСТУПАЕТ В СИЛУ, И Я ОБЯЗУЮСЬ НЕ УСТАНАВЛИВАТЬ И НЕ ИСПОЛЬЗОВАТЬ ДАННОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

АННОТАЦИЯ

Настоящий документ представляет собой 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» [1] из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» [2]. 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 ознакомится с актуальными инструкциями по установке и настройке продуктов на официальных сайтах производителей.

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

Настоящий документ 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 приказам 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.

[1] Далее по документу – программа, Центр регистрации Aladdin eRA

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

Содержание

Аннотация ... 5
1 Введение ... 10
1.1 Назначение программы ... 10
1.2 Состав программы ... 10
1.3 Функции программы ... 10
1.4 Роли управления ... 11
1.5 Режимы функционирования программы ... 14
2 Условия выполнения программы ... 15
2.1 Требования к программному обеспечению ... 15
2.1.1 Требования к среде функционирования Серверной части программы ... 15
2.1.2 Требования к среде функционирования Клиентской части программы ... 16
2.2 Требования к аппаратным средствам ... 16
3 Подготовка к установке программы ... 17
3.1 Подготовка среды функционирования с ОС РЕД ОС ... 19
3.1.1 Подключение репозиториев 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 SE ... 23
3.2.1 Подключение репозиториев и установка зависимостей ... 23
3.2.2 Установка среды исполнения Java ... 25
3.2.3 Установка и настройка СУБД ... 26
3.2.4 Установка веб-сервера ... 29
3.3 Подготовка среды функционирования с Альт Сервер ... 30
3.3.1 Подключение репозиториев и установка зависимостей ... 30
3.3.2 Установка среды исполнения Java ... 30
3.3.3 Установка и настройка СУБД ... 30
3.3.4 Установка веб-сервера ... 33
3.4 Создание службы HTTP и keytab-файла ... 34
3.4.1 Получение keytab-файла в Samba DC и Альт Домен ... 34
3.4.2 Получение keytab-файла в ALD PRO ... 36
3.4.3 Получение keytab-файла в Free IPA ... 36
3.4.4 Получение keytab-файла в MS AD ... 37
3.5 Установка веб-сервера Cpnginx ... 37
3.6 Установка JC-WebClient ... 38
4 Установка программы ... 39
4.1 Распаковка инсталляционного комплекта ... 39
4.2 Настройка конфигурации программы ... 40
4.3 Создание и настройка базы данных ... 48
4.3.1 Создание и настройка базы данных в автоматическом режиме ... 48
4.3.2 Создание и настройка базы данных PostgreSQL в ручном режиме ... 49
4.3.3 Создание и настройка базы данных Jatoba в ручном режиме ... 50
4.4 Установка программы ... 51
5 Запуск и завершение программы ... 53
5.1 Проверка состояния программы ... 53
5.2 Автоматический запуск программы ... 53
5.3 Запуск программы ... 53

5.4 Завершение работы программы ... 55
6 Подключение к веб-интерфейсу ... 56
6.1 Общие сведения ... 56
6.2 Установка сертификата администратора ... 56
6.3 Подключение к веб-интерфейсу ... 59
6.4 Аутентификация с использованием сертификата ... 60
6.5 Аутентификация по логину и паролю ... 61
6.6 Аутентификация с использованием Kerberos-билета ... 62
6.7 Выход из программы ... 63
7 Функции управления программы ... 64
7.1 Верхняя панель ... 64
7.2 Боковая панель ... 64
7.3 Раздел «Центр регистрации» ... 66
7.4 Раздел «Заявки» ... 68
7.4.1 Управление экранной таблицей ... 69
7.4.2 Фильтрация заявок ... 70
7.4.3 Сортировка заявок ... 71
7.4.4 Поиск заявок ... 72
7.4.5 Карточка заявки ... 72
7.4.6 Создание заявки на основании запроса ... 77
7.4.7 Создание заявки с закрытым ключом PKCS#12 ... 78
7.4.8 Создание заявки на ключевом носителе ... 81
7.4.9 Отмена заявки ... 85
7.4.10 Обработка заявки администратором ... 86
7.4.11 Импорт сертификата на ключевой носитель ... 87
7.4.12 Отзыв сертификата ... 89
7.5 Раздел «Учётные записи» ... 90
7.5.1 Вкладка «Учётные записи eCA» ... 91
7.5.2 Вкладка «Получатели сертификатов» ... 91
7.5.3 Блокировка доменной учётной записи ... 92
7.5.4 Активация доменной учётной записи ... 93
7.6 Раздел «Журнал событий» ... 93
7.6.1 Управление экранной таблицей ... 94
7.6.2 Фильтрация событий ... 95
7.6.3 Сортировка событий ... 96
7.6.4 Поиск событий ... 97
7.6.5 Карточка события ... 97
7.6.6 Копирование события в буфер обмена ... 98
7.6.7 Экспорт журнала событий ... 98
7.6.8 Архивирование и очистка журнала событий ... 99
7.7 Раздел «Управление» ... 99
7.7.1 Вкладка «Правила выпуска» ... 99
7.7.2 Вкладка «SCEP» ... 110
7.8 Раздел «Настройки» ... 118
7.8.1 Вкладка «Веб-сервер» ... 118
7.8.2 Вкладка «Syslog» ... 121
8 Поддержка протокола SCEP ... 125
8.1 Настройка SCEP-сервера ... 125

8.2 Обработку запросов по протоколу SCEP ... 126
8.2.1 Обработка запроса клиента PKCSReq/RenewalReq ... 126
8.2.2 Обработка запроса клиента CertPoll ... 127
8.2.3 Обработка запроса клиента GetCert ... 127
8.2.4 Обработка запроса клиента GetCRL ... 127
8.2.5 Обработка запроса клиента GetCACert ... 127
8.2.6 Обработка запроса клиента GetCACaps ... 128
9 Поддержка протоколов MS-XCEP и MS-WSTEP ... 129
9.1 Обработка запроса на политики «GetPolices» ... 129
9.2 Обработка запроса на выпуск сертификата «RequestSecurityToken» ... 131
10 Офлайн выпуск сертификатов ... 133
10.1 Поддерживаемые расширения и кодировки файлов запросов ... 133
10.2 Сценарий офлайн выпуска сертификатов ... 133
10.3 Включение офлайн выпуска сертификатов ... 134
10.4 Отключение офлайн выпуска сертификатов ... 134
11 Контроль целостности исполняемых файлов программы ... 135
12 Сбор диагностической информации программы ... 136
13 Резервное копирование и восстановление данных ... 137
13.1 Резервное копирование данных ... 137
13.2 Расписание резервного копирования ... 137
13.3 Восстановление данных из резервной копии ... 138
14 Обновление программы ... 139
14.1 Назначение обновлений ... 139
14.2 Информирование потребителей о выпуске обновлений ... 139
14.3 Получение обновлений потребителем ... 139
14.4 Контроль целостности обновления ПО ... 139
14.5 Процедура установки обновлений ... 140
15 Удаление программы ... 142
16 Удаление базы данных Postgres ... 143
16.1 Удаление БД «aecaca» ... 143
16.2 Удаление пользователя БД «aeca» ... 143
17 Поиск и устранение неисправностей ... 144
Приложение 1. Разрешение конфликта при Установке СУБД PostgreSQL и СУБД Postgres Pro ... 145
Приложение 2. Настройка подключения к внешней СУБД ... 146
2.1 Настройка на хосте СУБД ... 146
2.1.1 Настройка на хосте СУБД для Astra Linux ... 146
2.1.2 Настройка на хосте СУБД для РЕД ОС и Альт Сервер ... 146
2.2 Настройка на хосте Центра регистрации Aladdin eRA ... 147
Приложение 3. Настройка TLS-соединения с СУБД ... 149
3.1 Настройка на хосте СУБД ... 149
3.2 Настройка на хосте Центра регистрации Aladdin eRA ... 150
Приложение 4. Развёртывание кластера Центра регистрации Aladdin eCA ... 151
4.1 Развёртывание кластера Центра регистрации Aladdin eRA ... 151
4.2 Настройка узла с СУБД ... 151
4.3 Настройка основного узла ... 152
4.4 Настройка резервного узла ... 152
4.5 Настройка HAProxy ... 152
4.6 Подключение дополнительных резервных узлов ... 154

4.7 Обновление Центров регистрации Aladdin eCA в кластере ... 154
Приложение 5. Настройка Kerberos в веб-браузере ... 156
5.1 Настройка веб-браузера Mozilla Firefox ... 156
5.2 Настройка веб-браузера Chromium ... 156
Приложение 6. Перечень регистрируемых событий ... 158
6.1 События запуска и остановки служб ... 158
6.2 События аутентификации пользователей ... 158
6.3 События работы с УЗ получателей сертификатов ... 159
6.4 События работы с заявками ... 160
6.5 События работы с ключевыми носителями ... 163
6.6 События экспорта ... 163
6.7 События работы с правилами выпуска ... 164
6.8 События работы с веб-сервером и издателями ... 166
6.9 События Offline-выпуска ... 167
6.10 События работы с резервными копиями ... 167
6.11 События контроля целостности ... 168
6.12 События архивации и очистки записей аудита ... 168
6.13 События работы с Syslog ... 168
Приложение 7. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP» ... 170
Перечень документации для ознакомления ... 172
Обозначения и сокращения ... 173
Термины и определения ... 174
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ ... 176

1 ВВЕДЕНИЕ

1.1 Назначение программы

Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.051 входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020, которое применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификации при управлении доступом субъектов[3] доступа к объектам[4] доступа в автоматизированной (информационной) системе.

Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» предназначен для обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов)[5], выпускаемых программным комплексом «Центр сертификации Aladdin Enterprise Certification Authority»[6] RU.АЛДЕ.03.01.038 из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

1.2 Состав программы

Центра регистрации Aladdin Enterprise Registration Authority RU.АЛДЕ.03.01.051 является клиент-серверным веб-приложением и состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра регистрации»[7] RU.АЛДЕ.03.01.052.

Программный компонент реализует функции программного средства «Центр сертификации Aladdin Enterprise Certification Authority», 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»[8] RU.АЛДЕ.03.01.053.

Программный компонент реализует интерфейс, с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации».

1.3 Функции программы

Основные функции Центра регистрации Aladdin eRA:

- 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)[9];

[3] 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.

[4] 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.

[5] Далее по документу – сертификаты.

[6] Далее по документу - Центр сертификации Aladdin eCA.

[7] Далее по документу – Серверная часть программы.

[8] Далее по документу – Клиентская часть программы.

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

- создание заявок через программный интерфейс по протоколу Simple Certificate Enrollment Protocol (SCEP)[10];
- автоматическое создание заявок на основании запросов PKCS#10 из локального или сетевого каталога в соответствии с настройками Offline-выпуска;
- загрузка файлов запросов для заявок на выпуск сертификатов по запросу;
- выгрузка файлов сертификатов, цепочки сертификатов, списка отозванных сертификатов (CRL) и цепочки сертификатов Центра сертификации Aladdin eCA, 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 подключенного Центра сертификации Aladdin eCA 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.

1.4 Роли управления

Роли определяют полномочия пользователей при работе с Центром регистрации Aladdin eRA.
Пользователями Центра регистрации Aladdin eRA являются:

- Пользователи, учетные записи и сертификаты которых были созданы в Центре сертификации Aladdin eCA, подключенном к Центру регистрации Aladdin eRA.
- Пользователи, учетные записи которых созданы в доменной службе каталогов, подключенной к Центру регистрации Aladdin eRA.

В Центре регистрации Aladdin eRA определены следующие роли:

- Администратор.

Пользователь данной ролью обладает максимальными полномочиям. Пользователь с данной ролью может управлять Центром регистрации Aladdin eRA через веб-интерфейс и программный интерфейс API [11]. Идентификация и аутентификация пользователей с данной ролью выполняется по сертификату, выпущенному в Центре сертификации Aladdin eCA.

- Оператор.

Пользователь с данной ролью может управлять Центром регистрации Aladdin eRA через веб-интерфейс и программный интерфейс API [10]. Пользователь с данной ролью имеет может подавать заявки для любых субъектов, просматривать свои заявки, просматривать и обрабатывать заявки для доступных ему субъектов[12].

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

[11] См. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Приложение 8. Описание методов REST API» RU.АЛДЕ.03.01.020 30 01-4.

[12] Доступ пользователя с ролью «Оператор» к субъектам определяется в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA.

- Получатель сертификатов.

Пользователь с данной роль 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 первом входе через клиентскую часть Центра регистрации Aladdin eRA.

Доступные действия для существующих ролей пользователей Центра регистрации Aladdin eRA приведены в Таблица 2.

Таблица 2 – Полномочия пользователей Центра регистрации Aladdin eRA

Тип действия, осуществляемого пользователем, над объектом программы	**Возможные роли пользователей**		
	Получатель сертификатов	**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	-	-	✓
Создание заявок на выпуск сертификатов для субъекта своей учётной записи	✓	✓	✓
Создание заявок на выпуск сертификатов для субъекта любой учётной записи	-	✓	✓
Скачивание файла запроса на сертификат для своих заявок на выпуск сертификата по запросу	✓	✓	✓
Скачивание файла запроса на сертификат для ограниченного набора чужих заявок на выпуск сертификата по запросу	-	✓	✓
Скачивание файла запроса на сертификат для всех заявок на выпуск сертификата по запросу	-	-	✓
Скачивание сертификата для своих заявок	✓	✓	✓
Скачивание сертификата для ограниченного набора чужих заявок	-	✓	✓
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	✓	✓	✓
Отмена своих заявок	✓	✓	✓
Обработка ограниченного набора заявок	-	✓	✓
Обработка всех заявок	-	-	✓
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	-	-	✓
Запуск и остановка SCEP-политик	-	-	✓
Создание, редактирование, просмотр, копирование URL и удаление SCEP-профилей	-	-	✓
Запуск и остановка SCEP-профилей	-	-	✓
Добавление, редактирование, просмотр и удаление Syslog-серверов	-	-	✓
Смена сертификата веб-сервера	-	-	✓
Контроль целостности исполняемых файлов программы	-	-	✓

1.5 Режимы функционирования программы

Основным режимом функционирования Центра регистрации Aladdin eCA является нормальный режим.

В нормальном режиме должны штатно функционировать программные компоненты Центра регистрации Aladdin eRA, 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»[13], с которым взаимодействует Центр регистрации Aladdin eRA.

Сетевой режим работы обеспечивает возможность кластеризации Центра регистрации Aladdin eRA с целью повышения отказоустойчивости[14].

[13] Входит в состав программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority».

[14] Порядок развёртывания кластера Центра регистрации Aladdin eRA приведен 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 Центра регистрации Aladdin eRA:

- 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, сертифицированная редакция, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
- Поддерживаемые СУБД:
  - PostgreSQL из состава сертифицированной ОС;
  - Postgres Pro;
  - Jatoba.
- Поддерживаемые среды исполнения Java:
  - Java Axiom JDK Certified 17(компонент JRE).
  - OpenJDK версии 17 и выше из состава поддерживаемых ОС.
- Поддерживаемые веб-серверы:
  - Apache2 из состава сертифицированной ОС.
  - Nginx из расширенного репозитория.
  - Cpnginx из состава средства криптографической защиты (далее – СКЗИ) «КриптоПро CSP»[15]
- Поддерживаемые ресурсные системы (доменные службы каталогов):
  - Samba DC.
  - Free IPA.
  - ALD PRO.
  - РЕД АДМ.
  - Microsoft AD.
  - Альт Домен.
- Поддерживаемый центр сертификации - программный комплекс «Центр сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.038 версии 2.2.0.

[15] СКЗИ «КриптоПро CSP» входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (см. комплектность программного средства в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).

2.1.2 Требования к среде функционирования Клиентской части программы

Среда функционирования Клиентской части Центра регистрации Aladdin eRA:

- 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, сертифицированная редакция, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
- Веб-браузер из состава ОС.
- JC-WebClient последней версии (для 64-битных систем)[16].

2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования Центра регистрации Aladdin eRA:

- Накопитель HDD или SSD – не менее 50 Гбайт.
- Оперативная память – не менее 8 Гбайт.
- Процессорные ядра с архитектурой x86, x64 – не менее 4 шт.
- VGA-совместимый видеоадаптер.
- Устройства взаимодействия с пользователем:
  - клавиатура;
  - мышь;
- USB 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей:
  - JaCarta PKI.
  - JaCarta PRO.
  - JaCarta-2 PKI/ГОСТ.
  - JaCarta-2 ГОСТ.

[16] Официальный сайт производителя JCS-WebClient.

3 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

При установке Центра регистрации Aladdin eRA 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 осуществляется путём редактирования конфигурационного файла Центра регистрации Aladdin eRA (см. раздел 4.2).

В таблице ниже (см. Таблица 3) приведен список портов, которые использует Центра регистрации Aladdin eRA. Доступ к данным портам для внешних подключений ограничивается автоматически при установке Центра регистрации Aladdin eRA с помощью утилиты «iptables» из состава ОС.

Внимание! Во избежание возникновения ошибок в работе Центра регистрации Aladdin eRA переназначение данных портов запрещено.

Таблица 3 – Таблица входящих сетевых портов

Порт	Транспорт	Протокол	Назначение
1051	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «tasks-service» (сервис заявок)
1101	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «ca-adapter-service» (адаптер для подключения к Центру сертификации Aladdin eCA)
1201	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «policies-service» (сервис правил выпуска)
1251	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «security-service» (сервис безопасности)
1301	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «routes-service» (сервис маршрутизации)
1351	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «settings-service» (сервис настройки)
1401	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (сервис журнализации)
1451	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «export-service» (сервис экспорта)
1501	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «middleware-service» (связующий сервис для взаимодействия с внутренним контуром Центра регистрации Aladdin eCA)
1551	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «kerberos-provider-service» (сервис аутентификации по kerberos)
1601	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «x509-provider-service» (сервис аутентификации по сертификату)
1651	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «external-integration-service» (сервис публичного API)
1701	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «api-gateway-service» (сервис проксирования)
1751	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «scep enrollment-service» (сервис SCEP)

Порт	Транспорт	Протокол	Назначение
1801	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «wstep-enrollment-service» (сервис WSTEP)
1851	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «storage-service» (сервис хранения файлов)

Подготовка среды функционирования для установки Центра регистрации Aladdin eRA, заключается в установке и настройке следующего ПО:

- Зависимостей и подключение репозиториев ОС.
- Среды исполнения Java.
- СУБД.
- Веб-сервера.
- JC-WebClient.

Также необходимо предварительно выполнить следующие действия:

- Включить компьютер, на котором будет выполнено установка Центра регистрации Aladdin eRA, в домен ресурсной системы (доменной службы каталогов).
- Создать службу HTTP и keytab-файл[17] на контроллере домена ресурсной системы (см. раздел 3.4).
- Создать в Центре сертификации Aladdin eCA учетную запись с правами «Администратор» для взаимодействия Центра регистрации Aladdin eRA с Центром сертификации Aladdin eCA, выпустить для нее сертификат и выгрузить контейнер PKCS#12[18].
- Создать в Центре сертификации Aladdin eCA субъект для веб-сервера Центра регистрации Aladdin eRA, выпустить для него сертификат по шаблону WEB-Server (ECA-WEB-server) и выгрузить контейнер PKCS#12.
- Перенести подготовленные контейнеры PKCS#12 на компьютер, где будет выполнено развертывание Центра регистрации Aladdin eRA.

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA Центр регистрации Aladdin eRA может взаимодействовать с криптопровайдером СКЗИ «КриптоПро CSP». В данной ситуации на Центре регистрации Aladdin eRA также необходимо применять СКЗИ «КриптоПро CSP» для:

- Организации канала взаимодействия Серверных компонентов Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA по протоколу TLS ГОСТ.
- Организации канала взаимодействия Клиентского и Серверного компонентов Центра регистрации Aladdin eRA по протоколу TLS ГОСТ.
- Обеспечения TLS-аутентификации пользователей Центра сертификации Aladdin eCA в Центре регистрации Aladdin eRA с использованием отечественных криптографических алгоритмов.
- Подписи маркеров доступа пользователей Центра сертификации Aladdin eCA по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит.

[17] Keytab-файл используется для аутентификации доменных пользователей в Центре регистрации Aladdin eRA с использованием Kerberos без ввода пароля.

[18] Порядок создания субъектов 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».

Порядок установки и настройки СКЗИ «КриптоПро CSP» представлен в Приложении 7. Установка и настройка СКЗИ «КриптоПро CSP» могут быть выполнены после установки Центра регистрации Aladdin eRA в процессе его эксплуатации.

При применении СКЗИ «КриптоПро CSP»:

- В качестве веб-сервера должен использоваться веб-сервер «cpnginx» из состава СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP». Порядок установки веб-сервера «cpnginx» приведен в разделе 3.5. 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 учетной записи для взаимодействия с Центром сертификации Aladdin eCA должны быть выпущены по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит.

В зависимости от типа операционной систему сценарии подготовки частично различаются:

- для РЕД ОС 7.3 и РЕД ОС 8 сценарий подготовки описан в разделе 3.1;
- для Astra Linux Special Edition 1.7 и Astra Linux Special Edition 1.8 – в разделе 3.2;
- для Альт Сервер 8, релиз 10 – в разделе 3.3.

3.1 Подготовка среды функционирования с ОС РЕД ОС

3.1.1 Подключение репозиториев и установка зависимостей

Для РЕД ОС 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 команды:

```
sudo dnf install tar unzip iptables
```

При ошибке следует проверить наличие интернет-соединения.

Если доступ к сети Интернет отсутствует, зависимости возможно установить с USB-носителя из комплекта поставки ОС следующим образом:

- перейдите в каталог USB-носителя;
- для установки зависимостей выполните команду:

```
sudo dnf install tar unzip iptables
```

3.1.2 Установка среды исполнения Java

Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified. В противном случае можно установить свободно распространяемое ПО, например, OpenJDK.

3.1.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified 17 воспользуйтесь инструкцией с официального сайта производителяhttps://axiomjdk.ru/pages/axiomjdk-install-guide-17.0.6/.

3.1.2.2 Установка OpenJDK

Для установки OpenJDK 17 воспользуйтесь инструкцией по установке пакета «java-17-openjdk» 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 базы данных:

- PostgreSQL из состава сертифицированной операционной системы.
- 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.

Центр регистрации Aladdin eRA может быть настроен на взаимодействие с СУБД по протоколу TLS. Программное средство 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[19]

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду:

```
sudo dnf install postgresql-server
```

- Выполните установку последней доступной версии пакета `postgresql-contrib`, выполнив команду:

```
sudo dnf install postgresql-contrib
```

- Произведите инициализацию БД, выполнив команду:

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

В случае ошибки `Data directory in '/var/lib/pgsql/data' is not empty…` следует очистить директорию командой ниже и повторить инициализацию БД:

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`[20] с правами администратора – установите число подключений `max_connections` в значение `1000`[21].

- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`[22] с правами администратора. Измените параметры для успешного локального подключения пользователя к базе данных:

`host all all 127.0.0.1/32 ident` на `host all all 127.0.0.1/32 password`

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

[19] Подробное описание приведено на официальном сайте производителя.

[20] Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

[21] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

[22] Расположение файла может отличаться, для поиска файла можно использовать команду `sudo find / -type f -name pg_hba.conf`

- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив команду:

```
sudo systemctl restart postgresql
```

3.1.3.2 Установка СУБД Postgres Pro[23]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду[24]:

```
wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт, выполнив команду с правами суперпользователя (root или sudo):

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

- Обновите список пакетов, выполнив команду с правами суперпользователя (root или sudo):

```
sudo dnf update
```

- Установите Postgres Pro, выполнив команду с правами суперпользователя (root или sudo):

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`[25] с правами администратора – установите число подключений `max_connections` в значение `1000`[26].

- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`[27] с правами администратора – измените параметры для успешного локального подключения пользователя к базе данных:

`host all all 127.0.0.1/32 ident` на `host all all 127.0.0.1/32 password`

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

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

- Выполните перезапуск СУБД Postgres Pro для вступления изменений в силу, выполнив команду:

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

3.1.3.3 Установка СУБД Jatoba[28]

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя опитческой записи напрямую. В этом случае,

[23] Подробное описание приведено на официальном сайте производителя.

[24] Команды ниже приведены для 16-ой версии Postgres Pro.

[25] Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

[26] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

[27] Расположение файла указано для 16 версии Postgre Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

[28] Подробное описание приведено на официальном сайте производителя.

пользователю не требуется копировать файлы, а вместо каталога «localrepo» на всех шагах установки указывать соответствующий путь до носителя оптической запсии и директорию репозитория СУБД на носителе оптической запсии для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
  - каталог /`packages`;
  - каталог `/repodata`;
  - файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

```
sudo 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=0
gpgkey=file:///localerepo/RPM-GPG-KEY-Jatoba
```

- Обновите описания пакетов командой:

```
sudo dnf makecache
```

- Установите основные пакеты СУБД Jatoba 4 командой:

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

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

- Перейдите в директорию расположения исполняемых файлов СУБД Jatoba посредством команды:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором – установите число подключений `max_connections` в значение `1000`[29].
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf` под администратором. Измените параметры для успешного локального подключения пользователя к базе данных:

`host all all 127.0.0.1/32 ident` на `host all all 127.0.0.1/32 password`

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

- Добавьте СУБД Jatoba в автозагрузку командой:

[29] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

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

- Выполните перезапуск СУБД Jatoba для вступления изменений в силу, выполнив команду:

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

3.1.4 Установка веб-сервера

РЕД ОС поддерживает веб-сервера Nginx и Apache, которые обеспечивают сертифицированную среду функционирования. Веб-серверы устанавливаются из основного репозитория сертифицированной ОС.

3.1.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив команду с правами суперпользователя:

```
sudo dnf install httpd
```

- Установите дополнительный модуль для использования протокола SSL, выполнив:

```
sudo dnf install mod_ssl
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable httpd
```

3.1.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет из официального репозитория ОС, выполнив команду:

```
sudo dnf install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

3.2 Подготовка среды функционирования с ОС Astra Linux SE

3.2.1 Подключение репозиториев и установка зависимостей

3.2.1.1 Подключение репозиториев и установка зависимостей Astra Linux Special Edition 1.7[30]

Порядок подключения репозиториев и зависимостей:

- Для обновления посредством сети Интернет перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториев[31], отредактировав файл `/etc/apt/sources.list`, выполнив команду:

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

- Укажите ссылки на следующие репозитории[32]:

[30] Подробнее см. на официальном сайте производителя.

[31] Ссылки на репозитории приведены для Astra Linux SE версии 1.7.6

[32] При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозиториев в соответствии с инструкцией по подготовке и присоединению хоста к домену ALD Pro.

```
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-main/
1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-update/
1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-base/
1.7_x86-64 main contrib non-free
```

- Укажите нижеприведённый репозиторий для развёртывания веб-сервера Nginx, если не требуется обеспечение сертифицированной среды[33]:

```
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-extended/
1.7_x86-64 main contrib non-free
```

- Для установки необходимых компонентов в офлайн режиме предварительно необходимо настроить использование установочных дисков в качестве репозиториев, отредактировав файл `/etc/apt/sources.list` и зарегистрировать физический компакт-диск, вставленный в привод компакт-дисков, выполнив команду:

```
apt-cdrom add
```

Возможно, потребуется указать имя для регистрируемого компакт-диска, в таком случае можно указать произвольное понятное вам имя (например, MAIN для инсталляционного диска и DEVEL для диска со средствами разработки). Процедуру регистрации следует выполнить для всех дисков, на которых поставляется обновление (поочерёдно смонтировать образы или выполнить регистрацию для всех точек монтирования или поочерёдно установить диски в привод для физических дисков).

- Выполните обновление пакетов для операционной системы из указанных репозиториев, выполнив команду:

```
sudo apt update
```

- Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

```
sudo 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 Подключение репозиториев и установка зависимостей Astra Linux Special Edition 1.8[34]

Порядок подключения репозиториев и зависимостей:

- Для обновления посредством сети Интернет перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториев[35], отредактировав файл `/etc/apt/sources.list`, выполнив команду:

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

- Укажите ссылки на следующие репозитории[36]:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/main-repository/
1.8_x86-64 main contrib non-free
```

[33] В Astra Linux SE для обеспечения сертифицированной среды Центр регистрации Aladdin eCA необходимо развёртывать с использованием веб-сервера Apache.

[34] Подробнее см. на официальном сайте производителя.

[35] Ссылки на репозитории приведены для Astra Linux SE 1.8.1

[36] При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозиториев в соответствии с инструкцией по подготовке и присоединению хоста к домену ALD Pro.

- Укажите нижеприведённый репозиторий для развёртывания веб-сервера Nginx, если не требуется обеспечение сертифицированной среды[37]:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/extended-repository/
1.8_x86-64 main contrib non-free
```

- Для установки необходимых компонентов в офлайн режиме предварительно необходимо настроить использование установочных дисков в качестве репозиториев, отредактировав файл `/etc/apt/sources.list` и зарегистрировать физический компакт-диск, вставленный в привод компакт-дисков, выполнив команду:

```
apt-cdrom add
```

Возможно, потребуется указать имя для регистрируемого компакт-диска, в таком случае можно указать произвольное понятное вам имя (например, MAIN для инсталляционного диска и DEVEL для диска со средствами разработки). Процедуру регистрации следует выполнить для всех дисков, на которых поставляется обновление (поочерёдно смонтировать образы или выполнить регистрацию для всех точек монтирования или поочерёдно установить диски в привод для физических дисков).

- Выполните обновление пакетов для операционной системы из указанных репозиториев, выполнив команду:

```
sudo apt update
```

- Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

```
sudo 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»).

3.2.1.3 Поддержка активного режима замкнутой программной среды

Центр регистрации Aladdin eRA обеспечивает работу ОС Astra Linux Special Edition 1.7 и Astra Linux Special Edition 1.8 в активном режиме замкнутой программной среды (далее – ЗПС). Для этого в состав установочных пакетов программного комплекса включен публичный открытый ключ АО «Аладдин Р.Д.» - `aladdin_pub.key`. После распаковки установочного пакета ключ находится в каталоге `/opt/aecaRa/digsig/keys/aladdin_pub.key`.

Для обеспечения режима ЗПС открытый ключ необходимо переместить в каталог `/etc/digsig/keys/`.

3.2.2 Установка среды исполнения Java

Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified. В противном случае можно установить свободно распространяемое ПО, например, OpenJDK.

3.2.2.1 Установка Axiom JDK

Для установки Axiom JDK Certified 17 воспользуйтесь инструкцией с официального сайта производителя.

3.2.2.2 Установка OpenJDK

Для установки OpenJDK 17 воспользуйтесь инструкцией по установке пакета «java-17-openjdk» с официального сайта Astra Linux:

- инструкция для Astra Linux SE 1.7 (в инструкции описана установка Open JDK 11, установка Open JDK 17 аналогична).

[37] В Astra Linux SE для обеспечения сертифицированной среды Центра регистрации Aladdin eRA необходимо развёртывать с использованием веб-сервера Apache

- ;
- инструкция для Astra Linux SE 1.8

3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых базы данных:

- PostgreSQL из состава сертифицированной 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.

Программное средство может быть настроено на взаимодействие с СУБД по протоколу TLS. Программное средство не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведен в Приложении 3.

3.2.3.1 Установка СУБД PostgreSQL[38]

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду:

```
sudo apt install postgresql
```

- Выполните установку последней доступной версии пакета `postgresql-contrib`, выполнив команду:

```
sudo apt install postgresql-contrib
```

- Установите пакет `postgresql-client`, выполнив команду:

```
sudo apt install postgresql-client
```

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- При наличии мандатных политик[39]:
  - выдайте полномочия пользователю `postgres`, выполнить команду:

```
sudo pdpl-user -l 0:0 -i 63 postgres
```

  - предоставьте служебному пользователю `postgres` право на чтение файла, содержащего классификационную метку пользователя, поочерёдно выполнив команды:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
```

[38] Подробное описание приведено на официальном сайте производителя.

[39] Подробная информация по аутентификации в СУБД PostgreSQL приведена на официальном сайте производителя.

- Отредактируйте файл `/etc/postgresql/11/main/postgresql.conf`[40] с правами администратора – установите число подключений `max_connections` в значение `1000`[41].
- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив команду:

```
sudo systemctl restart postgresql
```

3.2.3.2 Установка СУБД Postgres Pro[42]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду[43]:

```
wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт, выполнив команду с правами суперпользователя (root или sudo):

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

- Обновите список пакетов, выполнив команду с правами суперпользователя (root или sudo):

```
sudo apt update
```

- Установите Postgres Pro, выполнив команду с правами суперпользователя (root или sudo):

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

- При наличии мандатных политик[44]:
  - выдайте полномочия пользователю `postgres`, выполнить команду:

```
sudo pdpl-user -l 0:0 -i 63 postgres
```

  - предоставьте служебному пользователю `postgres` право на чтение файла, содержащего классификационную метку пользователя, поочерёдно выполнив команды:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`[45] с правами администратора – установите число подключений `max_connections` в значение `1000`[46].
- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

- Выполните перезапуск СУБД Postgres Pro для вступления изменений в силу, выполнив команду:

---

[40] Расположение файла может отличаться. В инструкции расположение указано для PostgreSQL версии 11. Для поиска файла можно использовать команду `sudo find / -type f -name postgresql.conf`

[41] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

[42] Подробное описание приведено на официальном сайте производителя.

[43] Команды ниже приведены для Postgres Pro версии 16.

[44] Подробная информация по аутентификации в СУБД PostgreSQL приведена на официальном сайте производителя.

[45] Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

[46] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

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

3.2.3.3 Установка СУБД Jatoba[47]

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя опитческой записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «localrepo» на всех шагах установки указывать соответствующий путь до носителя оптической запсии и директорию репозитория СУБД на носителе оптической запсии для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
  - каталог `/pool`;
  - каталог `/dists`;
  - файл ключа `DEB-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

```
sudo rpm --import /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-freename
```

- Обновите описания пакетов командой:

```
sudo apt update
```

- Установите основные пакеты СУБД Jatoba командой:

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

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

- При наличии мандатных политик[48]:
  - выдайте полномочия пользователю `postgres`, выполнить команду:

```
sudo pdpl-user -l 0:0 -i 63 postgres
```

  - предоставьте служебному пользователю `postgres` право на чтение файла, содержащего классификационную метку пользователя, поочередно выполнив команды:

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
```

[47] Подробное описание приведено на официальном сайте производителя.

[48] Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148

```
sudo setfacl -R -m u:postgres:r /etc/parsec/macdb
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
```

- Перейдите в директорию расположения исполняемых файлов СУБД Jatoba посредством команды:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором – установите число подключений `max_connections` в значение `1000`[49].

- Добавьте СУБД Jatoba в автозагрузку командой:

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

- Выполните перезапуск СУБД Jatoba для вступления изменений в силу, выполнив команду:

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

3.2.4 Установка веб-сервера

Для обеспечения сертифицированной среды функционирования необходимо установить веб-сервер Apache из основного репозитория сертифицированной ОС. В противном случае можно установить веб-сервер Nginx.

3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив команду:

```
sudo apt install apache2
```

- Активируйте модули, выполнив поочерёдно команды:

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

- Перезагрузите веб-сервер, выполнив команду:

```
sudo systemctl restart apache2
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable apache2
```

- Для проверки корректности запуска модулей выполните команду:

```
sudo 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:

[49] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

Внимание! При выборе веб-сервера Nginx требуется расширить репозиторий операционной системы, что приведёт к потере сертифицированной среды функционирования.

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

```
sudo apt install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

3.3 Подготовка среды функционирования с Альт Сервер

3.3.1 Подключение репозиториев и установка зависимостей

Для развёртывания Центра регистрации Aladdin eRA с использованием веб-сервера Apache[50] перед началом установки компонента необходимо установить путь нахождения необходимого репозитория, отредактировав файл `/etc/apt/sources.list`, выполнив команду:

```
sudo nano /etc/apt/sources.list.d/aptsp.list
```

Укажите 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 команду:

```
sudo apt-get update
```

3.3.2 Установка среды исполнения Java

Для обеспечения сертифицированной среды функционирования необходимо установить Axiom JDK Certified. В противном случае можно установить свободно распространяемое ПО, например, OpenJDK.

3.3.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified 17 воспользуйтесь инструкцией с официального сайта производителя.

3.3.2.2 Установка OpenJDK

Для установки OpenJDK 17 воспользуйтесь инструкцией по установке пакета «java-17-openjdk» с официального сайта Альт Сервер.

3.3.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых базы данных:

- PostgreSQL из состава сертифицированной 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.

[50] Для обеспечения сертифицированной среды Центра регистрации Aladdin eRA необходимо развёртывать с использованием веб-сервера Nginx в операционной системе Альт Сервер 8, релиз 10

Программное средство может быть настроено на взаимодействие с СУБД по протоколу TLS. Программное средство не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведен в Приложении 3.

3.3.3.1 Установка СУБД PostgreSQL[51]

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду[52]:

```
sudo apt-get install postgresql15-server
```

- Выполните установку последней доступной версии пакета `postgresql-contrib`, выполнив команду:

```
sudo apt-get install postgresql15-contrib
```

- Установите пакет `postgresql`, выполнив команду:

```
sudo apt-get install postgresql15
```

- Произведите инициализацию БД, выполнив команду:

```
sudo /etc/init.d/postgresql initdb
```

В случае ошибки `Data directory in '/var/lib/pgsql/data' is not empty…` следует очистить директорию командой ниже и повторить инициализацию БД.

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/15/data/postgresql.conf`[53] с правами администратора – установите число подключений `max_connections` в значение `1000`[54].

- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив команду:

```
sudo systemctl restart postgresql
```

3.3.3.2 Установка СУБД Postgres Pro[55]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду[56]:

```
wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh
```

- Запустите скрипт, выполнив команду с правами суперпользователя (root или sudo):

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

---

[51] Подробное описание приведено на официальном сайте производителя.

[52] Команды ниже приведены для версии PostgreSQL версии 15.

[53] Расположение файла может отличаться. В инструкции расположение указано для 15 версии PostgreSQL. Для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

[54] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

[55] Подробное описание приведено на официальном сайте производителя.

[56] Команды ниже приведены для Postgres Pro версии 16.

- Обновите список пакетов, выполнив команду с правами суперпользователя (root или sudo):

```
sudo apt-get update
```

- Установите Postgres Pro, выполнив команду с правами суперпользователя (root или sudo):

```
sudo apt-get install postgrespro-16-std
```

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`[57] с правами администратора – установите число подключений `max_connections` в значение `1000`[58].

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

- Выполните перезапуск СУБД Postgres Pro для вступления изменений в силу, выполнив команду:

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

3.3.3.3 Установка СУБД Jatoba[59]

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя опитической записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «localrepo» на всех шагах установки указывать соответствующий путь до носителя оптической запсии и директорию репозитория СУБД на носителе оптической запсии для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
  - каталог `/base`;
  - каталог `/RPMS.classic`;
  - файл ключа `RPM-GPG-KEY-Jatoba`.

- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

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

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

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

- Обновите описания пакетов командой:

```
sudo apt-get update
```

---

[57] Расположение файла указано для Postgres Pro версии 16, для поиска файла можно использовать команду `sudo find / -type f -name postgresql.conf`

[58] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

[59] Подробное описание приведено на официальном сайте производителя.

- Установите основные пакеты СУБД Jatoba 4 командой:

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

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

- Перейдите в директорию расположения исполняемых файлов СУБД Jatoba посредством команды:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором – установите число подключений `max_connections` в значение `1000`[60].

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf` под администратором. Измените параметры для успешного локального подключения пользователя к базе данных:

`host all all 127.0.0.1/32 ident`	на	`host all all 127.0.0.1/32 password`
`host all all ::1/128 ident`	на	`host all all ::1/128 password`

- Добавьте СУБД Jatoba в автозагрузку командой:

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

- Выполните перезапуск СУБД Jatoba для вступления изменений в силу, выполнив команду:

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

3.3.4 Установка веб-сервера

Для обеспечения сертифицированной среды функционирования необходимо установить веб-сервер Nginx из основного репозитория сертифицированной ОС. В противном случае можно установить веб-сервер Nginx.

3.3.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

Внимание! Использование веб-сервера Apache приведёт к потере сертифицированной среды функционирования.

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

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

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

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

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

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

  - Внесите следующий текст в созданный файл:

[60] Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

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

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

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

– Внесите следующий текст в созданный файл:

```
# mod_http2 doesn't work with mpm_prefork
<IfModule !mpm_prefork>
    Protocols h2 h2c http/1.1
</IfModule>
```

- Активируйте модули, выполнив поочерёдно команды:

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

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

```
sudo a2enport https
```

3.3.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

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

- Запустите установленный веб-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

3.4 Создание службы HTTP и keytab-файла

Предварительно на Центре регистрации Aladdin eRA должен быть настроен Kerberos (должен быть настроен файл `krb5.conf`, рекомендумое расположение `/etc/krb5.conf`).

При изменении http-службы или при подключении Центре регистрации Aladdin eRA к другому домену необходимо заменять keytab-файл.

3.4.1 Получение keytab-файла в Samba DC и Альт Домен

- Подключитесь к контроллеру домена Samba DC (Альт Домен), например, по ssh, выполнив команду:

```
ssh <username>@<ip_adress>
```

где `<username>` – логин пользователя, на котором развёрнут контроллер домена, `<ip-adress>` – IP-адрес контроллера домена.

Если на контроллере домена используется нестандартный порт SSH, команда изменится:

```
ssh username@ip_adress -p 22
```

где `22` – порт, по которому будет произведено подключение по SSH.

После ввода команды система запросит подтверждение подключения (необходимо ввести `yes` и нажать Enter) и пароль пользователя. После ввода нажмите клавишу Enter — откроется SSH-соединение.

- Перейдите в режим суперпользователя, выполнив команду:

```
su
```

- Создайте пользователя-службу, который будет использоваться для авторизации в LDAP, выполнив команду[61]:

```
samba-tool user create --random-password <имя пользователя-службы>
```

- Разблокируйте созданного пользователя, выполнив команду:

```
samba-tool user setexpiry <имя пользователя-службы> --noexpiry
```

- Получите Kerberos-билет для администратора домена, выполнив команду:

```
kinit <имя администратора домена>@<домен в верхнем регистре>
```

- Расширьте для созданного пользователя-службы доступные поддерживаемые алгоритмы шифрования, выполнив команду[62]:

```
net ads enctypes set <имя пользователя-службы> 28 -U administrator
```

- Привяжите к пользователю-службе SPN HTTP-службы, выполнив команду:

```
samba-tool spn add HTTP/<имя настраиваемого клиента>.<домен> <имя
пользователя-службы>
```

где `<имя настраиваемого клиента>` – имя хоста, на котором производится установка Центра регистрации Aladdin eRA.

- Измените UPN пользователя-службы, выполнив команду:

```
samba-tool user rename <имя пользователя-службы> --upn=HTTP/<имя настраиваемого
клиента>.<домен>@<ДОМЕН>
```

где `<имя настраиваемого клиента>` – имя компьютера, на котором производится установка Центра регистрации Aladdin eRA.

- Экспортируйте Kerberos-билет пользователя-службы в `http.keytab` (можно экспортировать в любое удобное расположение):

```
samba-tool domain exportkeytab <расположение
keytab-файла>/http.keytab --principal=HTTP/<имя настраиваемого клиента>.<домен>
```

где `<имя настраиваемого клиента>` – имя хоста, на котором производится установка Центра регистрации Aladdin eRA.

- Скопируйте созданный на предыдущем шаге `keytab`-файл на настраиваемый клиент по пути `/etc/http.keytab` (рекомендованный путь расположения `keytab`-файла), выполнив команду:

```
scp <путь к файлу> <имя пользователя>@<имя хоста(ip-адрес)>:<путь к файлу>
```

где

– `<путь к файлу>` – путь к созданному `http.keytab`-файлу;

[61] При подключении нескольких Центров регистрации Aladdin eRA к одному контроллеру домена рекомендуется создать пользователя-службу для каждого Центра регистрации Aladdin eRA.

[62] В команде ниже `administrator` – это пользователь с правами администратора.

- `<имя пользователя>` – имя пользователя хоста, на котором производится установка Центра регистрации Aladdin eRA;
- `<имя сервера(ip-адрес)>` – укажите имя или IP-адрес хоста, на котором производится установка Центра регистрации Aladdin eRA;
- `<путь к файлу>` – укажите каталог хоста Центра регистрации Aladdin eRA, в который требуется скопировать `http.keytab-файл.`

Пример:

```
scp /home/user/http.keytab admin@172.22.5.23:/etc
```

- Измените права на полученный keytab-файл, выполнив команду:

```
sudo chmod 666 /etc/http.keytab
```

3.4.2 Получение keytab-файла в ALD PRO

- На контроллере домена авторизуйтесь в UI-интерфейсе ALD PRO, выполнив ввод в адресную строку браузера:

```
https://<имя контроллера домена>/ad/ui/#/
```

- Перейдите в раздел «Управление доменом» -> «Службы и параметры Kerberos», выбрав соответствующие кнопки на экранной форме, или выполните ввод в адресную строку браузера:

```
https://<имя контроллера домена>/ad/ui/#/domainmgmt/kerberos/services
```

- Создайте новую службу, нажав кнопку <+Новая служба>, выбрав класс службы – HTTP, имя компьютера - настраиваемый клиент, на который производится установка Центра регистрации Aladdin eRA. Сохраните изменения, нажав кнопку <Да> всплывающего окна.

- Получите Kerberos-билет администратора домена, выполнив команду:

```
kinit <имя администратора домена>
```

- Экспортируйте Kerberos-билет HTTP-службы на настраиваемый клиент по рекомендованному пути `/etc/http.keytab`, выполнив команду:

```
sudo ipa-getkeytab -s <имя контроллера домена>.<домен> -p HTTP/<имя настраиваемого клиента>.<домен>@<ДОМЕН> -k /etc/http.keytab
```

- Измените права на созданный `keytab`-файл (доступ на чтение и перезапись для всех), выполнив команду:

```
sudo chmod 666 /etc/http.keytab
```

где `/etc/http.keytab` – путь размещения `http.keytab`-файла.

3.4.3 Получение keytab-файла в Free IPA

- На контроллере домена авторизуйтесь в UI-интерфейсе Free IPA, выполнив ввод в адресную строку браузера:

```
https://<имя контроллера домена>/ipa/ui/#/
```

- Перейдите в раздел «Идентификация»->«Службы», выбрав соответствующие кнопки на экранной форме, или выполните ввод в адресную строку браузера:

```
https://<имя контроллера домена>/ipa/ui/#/e/service/search
```

- Создайте новую службу, нажав кнопку <+Добавить>, выбрав класс службы – HTTP, имя узла – настраиваемый клиент, на который производится установка Центра регистрации Aladdin eRA. Сохраните изменения, нажав кнопку <Да> всплывающего окна.

- Получите Kerberos-билет администратора домена, выполнив команду:

```
sudo kinit <имя администратора домена>
```

- Экспортируйте Kerberos-билет HTTP-службы на настраиваемый клиент (хост, подготавливаемый для установки Центра регистрации Aladdin eRA) по рекомендованному пути `/etc/http.keytab`, выполнив команду:

```
sudo ipa-getkeytab -s <имя контроллера домена>.<домен> -p HTTP/<имя настраиваемого клиента>.<домен>@<ДОМЕН> -k /etc/http.keytab
```

- Изменить права на созданный `keytab`-файл (доступ на чтение и перезапись для всех), выполнив команду:

```
sudo chmod 666 /etc/http.keytab
```

3.4.4 Получение keytab-файла в MS AD

- На контроллере домена MS AD запустите консоль управления «Active Directory Users and Computers» (ADUC).

- Создайте пользователя-службу, который будет использоваться для валидации Kerberos-билетов, например в организационном юните «Users».

- После создания пользователя-службы включите для него на вкладке «Свойства» - «Учётная запись» в поле «Параметры учётной записи» следующие параметры (остальные параметры должны быть отключены):
  - запретить смену пароля пользователем;
  - срок действия пароля не ограничен;
  - данная учётная запись поддерживает 128-разрядное...;
  - данная учётная запись поддерживает 256-разрядное...

- Привяжите SPN создаваемой HTTP-службы к созданному пользователю и хосту, с одновременным созданием keytab-файла (можно экспортировать в любое удобное расположение, например в `http.keytab`). Для этого выполните команду из командной строки PowerShell:

```
ktpass -princ HTTP/<имя настраиваемого клиента>.<домен>@<ДОМЕН> -mapuser <имя пользователя-службы> -pass <пароль пользователя-службы> -ptype KRB5_NT_PRINCIPAL -out <расположение keytab-файла>/http.keytab -crypto all
```

где `<имя настраиваемого клиента>` – имя хоста, на котором производится установка Центра регистрации Aladdin eRA.

3.5 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`:

- распакуете архив с дистрибутивом СКЗИ «КриптоПро CSP» командой:

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

- установите следующие пакеты:
  - для ОС Astra Linux SE командой `sudo dpkg -i <наименование пакета>.deb`:
    - `cprocsp-nginx-64_5.0.13000-7_amd64.deb`;
    - `lsb-cprocsp-rcrypt-64_5.0.13300-7_amd64.deb`;
    - `cprocsp-pki-plugin-64_2.0.15000-1_amd64.deb`.
  - для ОС РЕД ОС командой `sudo dnf install <наименование пакета>.rpm`:

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

– для ОС Альт Сервер командой `sudo apt-get install <наименование пакета>.rpm`:

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

- установите на СКЗИ «КриптоПро CSP» соответствующую лицензию (TLS-сервер) командой:

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

- выполните проверку активации лицензии командой:

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

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start cpnginx.service
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable cpnginx.service
```

3.6 Установка JC-WebClient[63]

- Программное обеспечение JC-WebClient необходимо установить на компьютер, с которого будет выполняется управление Серверной частью Центра регистрации Aladdin eRA через веб-интерфейс. JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях).
- При установке и использовании JC-WebClient сертифицированная среда функционирования не обеспечивается.
- Скачайте дистрибутив JC-WebClient с веб-сайта производителя.
- Установите зависимости.
- Установите JC-WebClient, выполнив команду:

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

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

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

- Произведите запуск ПО JC-WebClient, выполнив команду:

```
sudo sh jcmon start
```

[63] Официальный сайт производителя.

4 УСТАНОВКА ПРОГРАММЫ

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

4.1 Распаковка инсталляционного комплекта

Распакуйте инсталляционный rpm/deb-пакет, находясь в папке, где расположен пакет, выполнив команду с правами суперпользователя:

РЕД ОС	`sudo dnf install <наименование пакета>.rpm`
Astra Linux	`sudo dpkg -i <наименование пакета>.deb`
Альт Сервер	`sudo apt-get install <наименование пакета>.rpm`

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

Структура распакованного инсталляционного rpm/deb-пакета приведена в таблице ниже (Таблица 4).

Таблица 4 – Структура установочного комплекта Центра регистрации Aladdin eRA

Структурный элемент	Назначение элемента
`/opt/aecaRa`	Установочный комплект Центра регистрации Aladdin eRA, а также используемые дополнительные инструменты.
`/opt/aecaRa/dist`	Путь развертывания продукта, который содержит создаваемые временные файлы.
`..dist/backup/`	Созданные резервные копии Центра регистрации Aladdin eRA.
`..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 Центром регистрации Aladdin eRA.
`/opt/aecaRa/scripts`	Содержит скрипты управления Центром регистрации Aladdin eRA.
`../scripts/internal`	Скрипты для внутреннего использования программы.
`../scripts/backup.sh`	Скрипт резервного копирования конфигурации Центра регистрации Aladdin eRA

Структурный элемент	Назначение элемента
../scripts/config.sh	Конфигурационный файл Центра регистрации Aladdin eRA.
../scripts/database_create.sh	Скрипт создания базы данных Центра регистрации Aladdin eRA.
../scripts/diagnostics.sh	Скрипт сбора диагностической информации Центра регистрации Aladdin eRA.
../scripts/install.sh	Скрипт установки и обновления текущей версии Центра регистрации Aladdin eRA.
../scripts/restore.sh	Скрипт восстановления из резервной копии конфигурации Центра регистрации Aladdin eRA.
../scripts/uninstall.sh	Скрипт удаления Центра регистрации Aladdin eRA.
/opt/aecaRa/services	Сервисы Серверной части Центра регистрации Aladdin eRA.
/opt/aecaRa/scripts/jc_checksum	Файл с эталонами контрольных сумм исполняемых файлов Центра регистрации Aladdin eRA.
/opt/aecaRa/static	Артефакты Клиентской части Центра регистрации Aladdin eRA.
../opt/aecaRa/bin/jcverify	Каталог утилиты контроля целостности «jcverify».
../opt/aecaRa/bin/jcverify/jcverify	Утилита контроля целостности «jcverify».
../opt/aecaRa/bin/jcverify/jcverify.txt	Вспомогательный файл для работы утилиты целостности «jcverify».
/opt/aecaRa/digsig/keys/aladdin_pub.key	Публичный открытый ключ производителя для обеспечения ЗПС ОС Astra Linux SE.

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

4.2 Настройка конфигурации программы

Перед установкой программного комплекса требуется определить значения следующих параметров:

- `Webserver` – укажите используемый веб-сервер (`nginx`, `apache` или `cpnginx`). Также значение параметра можно будет ввести после запуска инсталлятора установки, в интерактивном режиме выбрав веб-сервер;
- `webserver_path` – укажите папку 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 A.yecpache располагается для Astra Linux SE по пути `/etc/apache2`, для RedOS – по пути `/etc/httpd`, для Альт Сервер по пути `/etc/httpd2;`
  - конфигурация cpnginx располагается по пути `/etc/opt/cprocsp/cpnginx`;

- `database_password` – укажите пароль создаваемой базы данных (имя базы данных по умолчанию - aecara). После обновления с версии 2.0 до версии 2.2, а также после создания и настройки базы данных (см. раздел 4.3) пароль пользователя базы данных отображается в конфигурационном файле в шифрованном виде (алгоритм шифрования AES-256 с использованием сгенерированного в файле `/opt/aecaRa/scripts/key` ключа шифрования). Пароль не должен содержать специальные символы «|» и «\»;
- `aeca_ca_host` – укажите адрес (IP-адрес или доменное имя) Центра сертификации Aladdin eCA, к которому будет подключён Центр регистрации Aladdin eRA (пример, `172.22.5.21`);
- `aeca_ca_auth_password` – укажите пароль от контейнера закрытого ключа учётной записи администратора, используемой для взаимодействия Центр регистрации Aladdin eRA с Центром сертификации Aladdin eCA;
- `kerberos_service_principal` – укажите принципал HTTP-службы, используемой для валидации Kerberos-билетов (состоит из `HTTP/<доменное имя стенда>.<домен>`, пример значения: `HTTP/ra01.presale.aeca`);
- `kerberos_keytab_location` укажите расположение keytab-файла для принципала HTTP-службы для валидации Kerberos-билетов. Рекомендуется располагать данный файл по пути `/etc/http.keytab` (пример значения `/etc/http.keytab`);
- `kerberos_krb5_location` – укажите расположение `krb5.conf` файла (по умолчанию располагается по пути `/etc/krb5.conf`, не рекомендуется изменять без веской причины);
- `kerberos_ad_domain` – укажите имя домена службы каталог в верхнем регистре (пример значения параметра: `PRESALE.AECA`);
- `kerberos_ad_server` – укажите LDAP-адрес для подключения к домену. Обычно, состоит из `ldap://<имя контроллера домена>.<домен>` (пример `ldap://dc1.presale.aeca`);
- `resource_type` – укажите тип подключаемой ресурсной системы (доступные значения: FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN);
- `resource_base_dn` – укажите точку подключения к ресурсной системе (пример значения `dc=presale,dc=aeca`);
- `certificate_raw_server_password` – укажите пароль от контейнера закрытого ключа веб-сервера;
- `root_cert_path` – укажите 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` – укажите полное имя компьютера, на котором будет развёрнут Центра регистрации Aladdin eRA.

При использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программы должен быть организован по протоколу TLS ГОСТ, должна обеспечиваться TLS-аутентификация пользователей в программном средстве с использованием отечественных криптографических алгоритмов, а маркеров доступа пользователей Центра сертификации Aladdin eCA 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 ниже (Таблица 5).

Таблица 5 – Параметры для настройки TLS ГОСТ

Параметр	Значение
webserver	'cpnginx'
webserver_path	'/etc/opt/cprocsp/cpnginx'
sign_provider	'CRYPTO_PRO'
sign_key_algorithm	'GOST_R_34_10_2012'
sign_key_length	'256' или '512
sign_hash_algorithm	'GOST_R_34_11_2012'

Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, выполнив команду:

```
sudo 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 offline-выпуска сертификатов;
- параметры сертификата веб-сервера центра регистрации;
- расписание синхронизации ресурсных систем;
- расписание синхронизации разрешённых издателей;
- расписание архивации журнала событий;
- конфигурацию базы данных;
- конфигурация памяти.

Полный перечень и описание параметров конфигурации приведено в Таблица 6.

Таблица 6 – Описание параметров конфигурации

Параметр	Значение параметра по умолчанию	Описание
Конфигурация развертывания		
webserver	#CHANGEIT	Используемый веб-сервер (nginx,apache, cpnginx)
webserver_path	#CHANGEIT	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 RedOS конфигурация apache располагается по пути /etc/httpd, конфигурация cpnginx располагается по пути /etc/opt/cprocsp/cpnginx)
aeca_path	'/opt/aecaRa/dist'	Папка с файлами для развёртывания Центра регистрации Aladdin eRA
environment_path	'/opt/aecaRa/dist/environment'	Папка с переменными окружения для сервисов
webserver_config_path	'/opt/aecaRa/dist/webserver'	Расположение конфигурации Центра регистрации Aladdin eRA для веб-сервера

Параметр	Значение параметра по умолчанию	Описание
encryption_key_path	'/opt/aecaVa/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 разработчиками. 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 разработчиками. Редактировать не следует.
proxy_read_timeout	'720'	Время ожидания чтения ответа от прокси-сервера после получения успешного запроса. Если ответ не получен в течение этого времени, запрос считается неудачным. Только для Nginx. Настраивается разработчиками. Редактировать не следует.
ssl_protocols	'TLSv1.2 TLSv1.3'	Поддерживаемые версии протокола TLS. Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обоих версий протокола необходимо указывать их через пробел).
ssl_ciphers	По умолчанию не задано.	Поддерживаемые наборы шифров для TLS-соединения. Данный параметр позволяет ограничить наборы шифров (cipher suites), которые могут использоваться при TLS-соединении. Разделитель между наборами – «:». Если клиент не поддерживает ни один из указанных в данном параметре наборов, TLS-соединение не будет установлено. По умолчанию значение в данном параметре не задано, что означает отсутствие управления со стороны Центра регистрации перечнем допустимых наборов шифров (ciphersuites) TLS-соединения для веб-сервера. В данном параметре могут быть указаны любые наборы шифров, поддерживаемые используемой на сервере Центра регистрации версией Openssl для TLS версии 1.2. Получить список поддерживаемых используемым Openssl наборов шифров для TLS версии 1.2 можно с помощью команды: `openssl ciphers -tls1_2 -s` Данный параметр учитывается только при использовании Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cpnginx осуществляется с

Параметр	Значение параметра по умолчанию	Описание
		помощью утилиты «cpconfig» из состава СКЗИ «КриптоПро CSP»[64].
Путь хранения резервных копий		
backup_path	'/opt/aecaRa/dist/backup'	Папка, в которую сохраняются резервные копии Центра регистрации Aladdin eRA
Путь хранения лог-файлов		
logs_base	'/opt/aecaRa/dist/logs'	Папка, в которой хранятся лог-файлы
archive_path	'/opt/aecaRa/dist/archive'	Папка, в которую сохраняется архив журнала событий, сформированный в результате автоматической архивации по заданным параметрам
Путь хранения контейнера сертификата и ключа веб-сервера, а также цепочек сертификатов разрешённых издателей		
certificates_ssl_path	'/opt/aecaRa/dist/certificates/ssl'	Папка, содержащая сертификат веб-сервера и цепочки сертификатов разрешённых издателей
certificates_aeca_ca_path	'/opt/aecaRa/dist/certificates/aeca-ca'	Путь хранения контейнера сертификата для авторизации в Центре сертификации Aladdin eCA
Конфигурация пользователя		
aeca_user	'aeca'	Имя пользователя Центра регистрации Aladdin eRA, используемое для работы программы
aeca_group	'aeca'	Группа, в которой состоит пользователь Центра регистрации Aladdin eRA
Конфигурация памяти		
memory	6144	Максимальный лимит оперативной памяти
enable_gc_diagnostic	'false'	Флаг сбора диагностической информации о памяти
Конфигурация базы данных		
use_tls	false	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false
max_db_pool_size	'50'	Максимальный размер пула подключений к СУБД. Настраивается разработчиками. Редактировать не следует.
database_username	'aeca'	Имя пользователя базы данных, используемое для работы Центра регистрации Aladdin eRA
database_password	#CHANGEIT	Пароль пользователя базы данных, используемый для работы Центра регистрации Aladdin eRA. Пароль не должен содержать специальные символы «|» и «\»
database_host	'localhost'	Сетевой адрес базы данных
database_port	'5432'	Порт, используемый для подключения к базе данных
database_name	'aecara'	Имя базы данных, используемой Центром регистрации Aladdin eRA

[64] Инструкция по установке и настройке cpnginx - https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/440/0/nginx-gost-binary-packages. Описание порядка конфигурирования наборов шифров представлено в разделе 6.

Параметр	Значение параметра по умолчанию	Описание
root_cert_path	#CHANGEIT	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД
Конфигурация Центра регистрации		
http_port	'80'	Порт для подключения к программному комплексу по протоколу http
https_port	'443'	Порт для подключения к программному комплексу по протоколу https
hostname	'localhost'	Имя сервера, на котором развёртывается Центр регистрации.
hostname_no_mtls	По умолчанию не задано.	Параметр используется только в конфигурации с CPNGINX. Имя хоста (должно отличаться от значения hostname), используемое для доступа к интерфейсу без использования mTLS.
number_of_services	'16'	Количество активных сервисов в системе. Настраивается разработчиками, редактировать не следует.
logs_file_max_size	'10MB'	Максимальный размер лог-файла (файла с диагностической информацией) сервиса перед его архивацией. При достижении данного значения текущий лог-файл (access.log или service.log) будет заархивирован. Файл будет сохранен в текущем каталоге хранения лог-файлов данного сервиса с именем {access или service}-{дата в формате YYYY-MM-DD}.{индекс лога}.log.
logs_max_history	'10'	Максимальный срок хранения архивов с лог-файлами в днях. Архивы, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться.
logs_total_size_cap	'100MB'	Максимальный общий объем лог-файлов, включая архивы, каждого типа (access или service) для каждого сервиса. При достижении данного объема наиболее старые архивы данного типа будут удаляться.
Переменные окружения, используемые всеми сервисами		
logging_response	false	Флаг для сбора и регистрации ответов сервисов
logging_sql	false	Флаг для сбора и регистрации информации о подключениях и запросах к базе данных PostgreSQL
Ключ для внутренней аутентификации		
api_key	'2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810'	Значение ключа для внутренней аутентификации. Для служебного пользования
Переменные окружения, используемые сервисом ca-adapter-service		
aeca_ca_host	#CHANGEIT	IP-адрес Центра сертификации, к которому происходит подключение

Параметр	Значение параметра по умолчанию	Описание
aeca_ca_auth_filename	AUTH_CA_PATH	Имя файла контейнера сертификата, используемого для авторизации в Центре сертификации
aeca_ca_auth_password	#CHANGEIT	Пароль от контейнера сертификата, используемого для авторизации в Центре сертификации
Переменные окружения, используемые сервисом kerberos-provider-service		
kerberos_service_principal	#CHANGEIT	Уникальное имя для клиента, которому разрешается аутентификация в Kerberos, используемое для авторизации
kerberos_keytab_location	#CHANGEIT	Расположение keytab-файла, содержащего Kerberos-билет принципала, используемого для авторизации
kerberos_krb5_location	#CHANGEIT	Расположение файла конфигурации krb5.conf
kerberos_ad_domain	#CHANGEIT	Имя подключаемого домена
kerberos_ad_server	#CHANGEIT	Адрес сервера AD (ldap)
Переменные окружения, используемые сервисом ldap-service		
resource_type	#CHANGEIT	Тип ресурсной системы (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN)
resource_base_dn	#CHANGEIT	Точка подключения ресурса
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
Переменные окружения, используемые сервисом settings-service		
certificate_server_name	server	Имя файла сертификата веб-сервера
certificate_raw_server_password	#CHANGEIT	Пароль от контейнера сертификата веб-сервера
issuers_name	issuers	Имя файла разрешённых издателей, получаемого от Центра сертификации Aladdin eCA
issuers_sync	'0 */30 * * * *'	CRON-выражение, по которому выполняется синхронизация разрешённых издателей
offline_enrollment_enabled	false	Флаг включения offline-выпуска сертификатов. Возможные значения: true/false
offline_enrollment_cron	'0 * * * * *'	CRON выражение, по которому будет запускаться offline-выпуск сертификатов
offline_enrollment_template_id	#CHANGEIT	Идентификатор шаблона, который будет использоваться для offline-выпуска[65]
offline_enrollment_request_path	#CHANGEIT	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.

[65] Указан идентификатор шаблона «Smartcard Logon»

Параметр	Значение параметра по умолчанию	Описание
offline_enrollment_certificate_path	#CHANGEIT	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	#CHANGEIT	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 сервисом security-service		
session_max_count	"-1"	Максимальное число одновременных сессий аккаунта в виде натурального числа. При указании значения «-1» ограничение на количество одновременных сессий пользователя будет отсутствовать.
token_expire	‘18000’	Время жизни JWT-токена (маркера доступа), мс.
refresh_token_expire	‘86400000’	Время жизни JWT-токена обновления, мс.
sign_provider	'EMBEDDED'	Провайдер подписи маркера доступа (выбирается между стандартным - 'EMBEDDED' и КриптоПро - 'CRYPTO_PRO')
sign_key_algorithm	'RSA'	Алгоритм ключа подписи маркера доступа. 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 маркера доступа
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи маркера доступа, 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'

Параметр	Значение параметра по умолчанию	Описание
Переменные окружения, используемые сервисом logs-service		
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'	Период архивации (мс) (архивировать записи старше…)
Использования HTTP взаимодействия с SCEP		
allow_scep_http	true	Флаг использования протокола HTTP при взаимодействии с ним по протоколу SCEP. Если установлено значение «false», то программа отключает от веб-сервера HTTP-конфигурацию для SCEP-сервиса
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.

4.3 Создание и настройка базы данных

Перед установкой Центра регистрации Aladdin eRA необходимо создать и настроить базу данных Центра регистрации Aladdin eRA. Это может быть выполнено одним следующих из способов:

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

После создания и настройки базы данных пароль пользователя базы данных, заданный в конфигурационном файле `/opt/aecaRa/scripts/config.sh` в параметре `database_password`, отображается в зашифрованном виде. Шифрование пароля выполняется по алгоритму AES-256 с использованием автоматически сгенерированного в файле `/opt/aecaRa/scripts/key` ключа шифрования. Пароль не должен содержать специальные символы «|» и «\».

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

- об учётных записях;
- о заявках;
- о правилах выдачи сертификатов;
- журнала событий;
- о ролях пользователей;
- о правах, определённых для ролей пользователей.

4.3.1 Создание и настройка базы данных в автоматическом режиме

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

Для создания и настройки базы данных запустите скрипт, выполнив команду от имени суперпользователя[66]:

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

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

4.3.2 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 базы данных, используемой программой в процессе работы;
- назначение созданному пользователю полных прав доступа к созданной базе данных.

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Зайдите под пользователем «postgres» в PostgreSQL, выполнив команду:

```
sudo –u postgres psql
```

- Создайте пользователя базы данных, выполнив команды:

```
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).

- Задайте пароль пользователю, выполнив команды:

```
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
```

[66] Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).

- Перезапустите СУБД PostgreSQL, выполнив команду:

```
sudo systemctl restart postgresql
```

- Установите расширение pgcrypto в БД PostgreSQL, выполнив команду от имени пользователя «postgres» (с правами root):

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

где `aecara` – имя созданной базы данных.

4.3.3 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 базы данных, используемой Программой в процессе работы;
- назначение созданному пользователю полных прав доступа к созданной базе данных.

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите Jatoba, выполнив команду:

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

Добавьте запуск Jatoba в автозагрузку, выполнив команду:

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

- Зайдите под пользователем `«postgres»` в Jatoba, выполнив команду:

РЕД ОС	`sudo -u postgres psql`
Astra Linux SE	`sudo -u postgres psql`

Альт Сервер	`sudo – postgres -s /bin/bash`
	`-bash-4.4$ /usr/jatoba-[версия]/bin/psql`
	`psql`

- Создайте пользователя базы данных, выполнив команды:

```
CREATE USER aeca;
```

где `aeca` – задаваемое имя пользователя.

- Задайте пароль пользователю, выполнив команды:

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

где `'aeca'` – задаваемый пароль пользователя.

Внимание! Пароль не должен содержать специальные символы «|» и «\».

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecara;
```

где `aecara` – задаваемое имя базы данных.

- 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 Jatoba, выполнив команду:

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

- Установите расширение pgcrypto в БД Jatoba, выполнив команду от имени пользователя «postgres» (с правами root):

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

где `aecara` – имя созданной базы данных.

4.4 Установка программы

Для инициализации процесса установки Центра регистрации Aladdin eRA необходимо запустить скрипт с правами суперпользователя[67]:

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

- В случае запуска от имени пользователя, не имеющего соответствующих привилегий, будет выведено сообщение, после которого работа инсталлятора завершится:

```
"This script must be run as root!"
```

- При использовании Astra Linux Special Edition и наличии мандатных политик[68] может быть выведено сообщение:

```
ВАЖНО: error obtaining MAC configuration for user "aeca"
```

В данном случае явно назначьте классификационную метку пользователю `aeca`, выполнив команду:

```
sudo pdpl-user -l 0:0 aeca
```

И повторно запустите скрипт установки.

После инициализации процесса установки интерактивный инсталлятор запущен и пользователю будет предложено (в случае, если ранее Центр регистрации Aladdin eRA 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:

---

[67] Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).

[68] Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148

- apache;
- nginx;
- cpnginx;

Подтвердите выбор действия вводом цифры «1», «2» или «3».

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 авторизации в Центре сертификации Aladdin eCA;
- контейнера сертификата PCS#12 веб-сервера.

В процессе установки осуществляется:

- создание системного пользователя и соответствующей группы, от имени которых функционирует Центр регистрации Aladdin eRA;
- установка прав для создаваемого пользователя Центра регистрации Aladdin eRA;
- установка контейнера сертификата, используемого для авторизации в Центре сертификации Aladdin eCA;
- установка контейнера сертификата веб-сервера Центра регистрации Aladdin eRA;
- подготовка, установка параметров и служебных сервисов;
- запуск служебных сервисов;
- запись номера сборки Центра регистрации Aladdin eRA в базу данных[69].

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 команду:

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

[69] Значение номера сборки записывается в таблицу «build_info» схемы «aeca_ra_info».

5 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

5.1 Проверка состояния программы

Для проверки состояния сервера, на котором развёрнут Центр регистрации Aladdin eRA, в терминале выполните команду с правами суперпользователя:

```
sudo 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.

5.2 Автоматический запуск программы

Центр регистрации Aladdin eRA запускается автоматически с запуском ОС.

Для проверки автозагрузки программы выполните команду с правами суперпользователя:

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

Для добавления программы в автозагрузку выполните команду с правами суперпользователя:

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

5.3 Запуск программы

Для запуска программы выполните команду с правами суперпользователя:

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

При запуске Центра регистрации Aladdin eRA выполняется ряд проверок.

- Проверка возможности подключения к базе данных[70]. Если не удаётся подключится к базе данных, то программа не запускается.
- Проверка соответствия номера своей сборки и значения номера сборки, указанной в базе данных[70]:
  - 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 Центра регистрации Aladdin eRA запускаются поочерёдно в порядке, приведенном в таблице ниже (Таблица 7).

Таблица 7 – 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

[70] Значение номера сборки указано в таблице «build_info» схемы «aeca_ra_info».

Порядок запуска	Исполняемый файл	Наименование	Назначение
2	tasks-service.jar	Модуль заявок	Обеспечивает управление заявками на сертификаты
3	ca-adapter-service.jar	Адаптер для подключения к Центру сертификации Aladdin eCA	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
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 Центра регистрации Aladdin eCA
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 Центром регистрации Aladdin eCA
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

5.4 Завершение работы программы

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

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

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

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 Центра регистрации Aladdin eRA и предназначен для управления серверным компонентом Центра регистрации Aladdin eRA (выполнения доступных пользователю в рамках его полномочий действий).

Подключение к веб-интерфейсу Центра регистрации Aladdin eRA 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 и шифрованием передаваемых данных. Идентификация и аутентификация пользователей 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.

При использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента Центра регистрации Aladdin eRA 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 учетной записи администратора для взаимодействия с Центром сертификации Aladdin eCA 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 приведен 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 сертифицированной ОС. Данный веб-браузер входит в состав базовых репозиториев ОС Astra Linux SE, Альт Сервер и РЕД ОС.

6.2 Установка сертификата администратора

Для первичной настройки программного комплекса необходимо установить сертификат учётной записи администратора Центра сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, в доверенное хранилище сертификатов веб-браузера[71].

Процесс установки сертификата рассмотрим на примере браузера Firefox:

[71] 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».

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

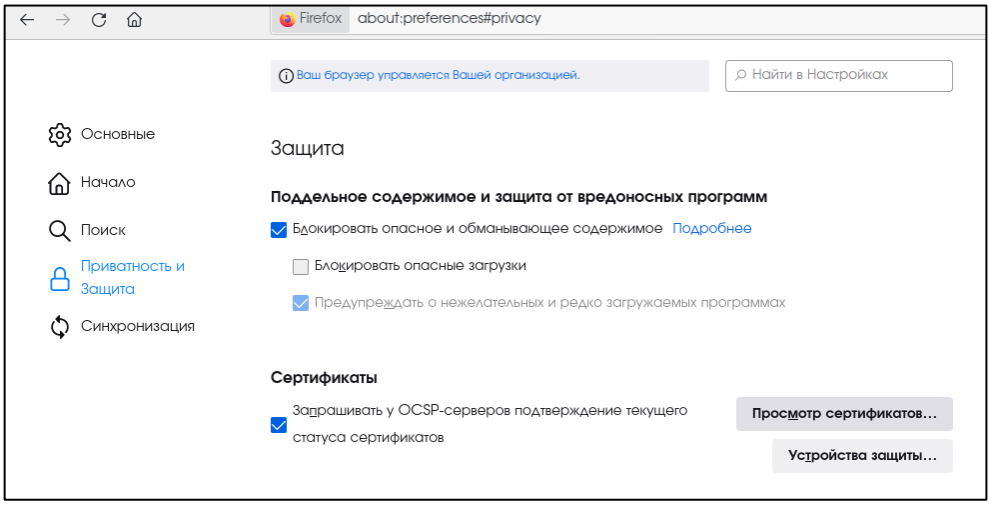


Рисунок 1 – Окно настроек браузера

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

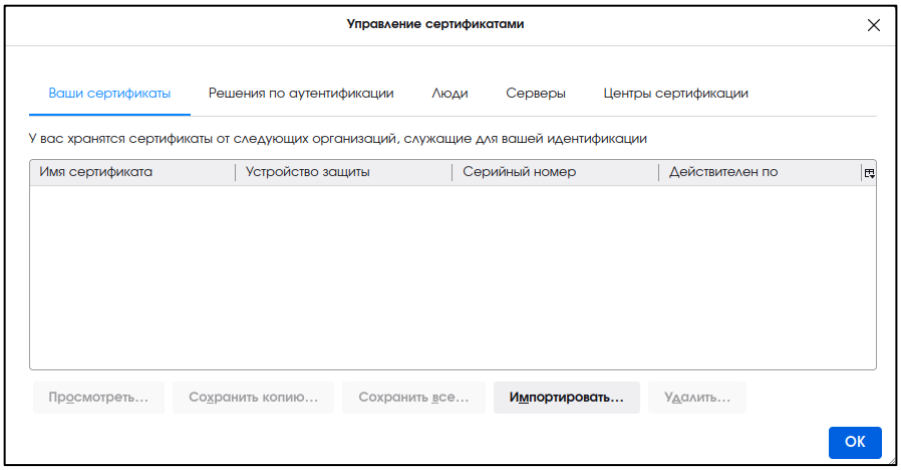


Рисунок 2 – Окно управления сертификатами

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

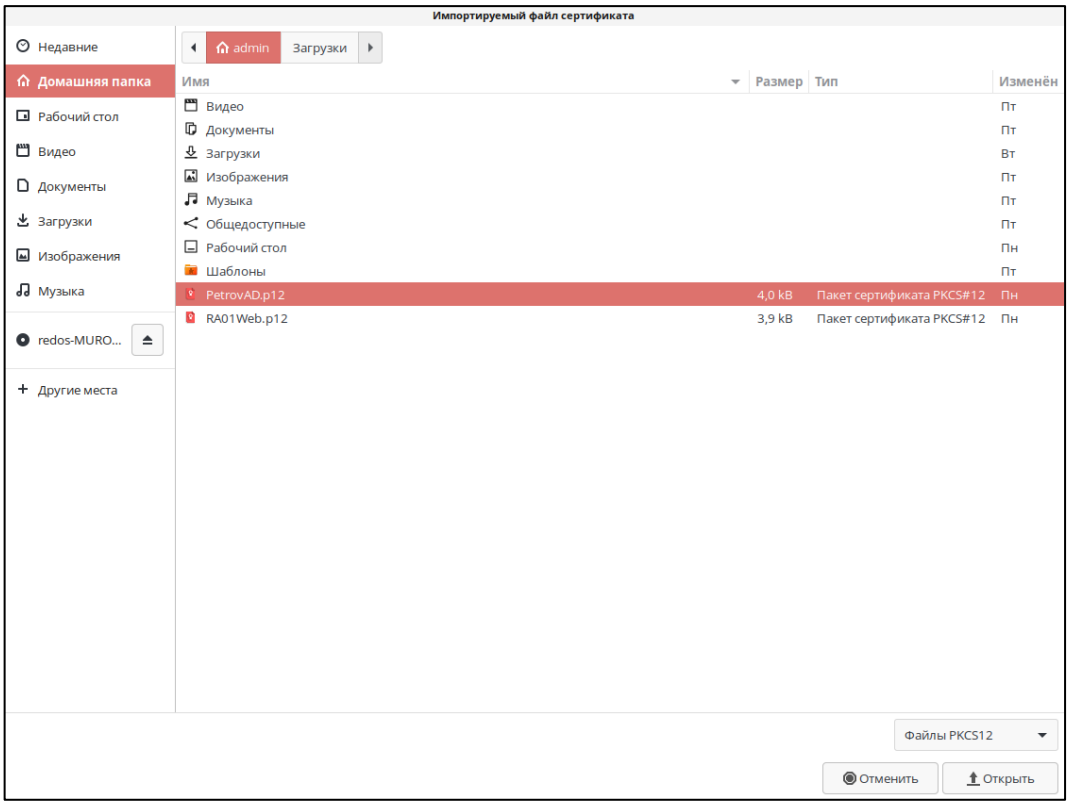


Рисунок 3 – Окно выбора импортируемого файла сертификата

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

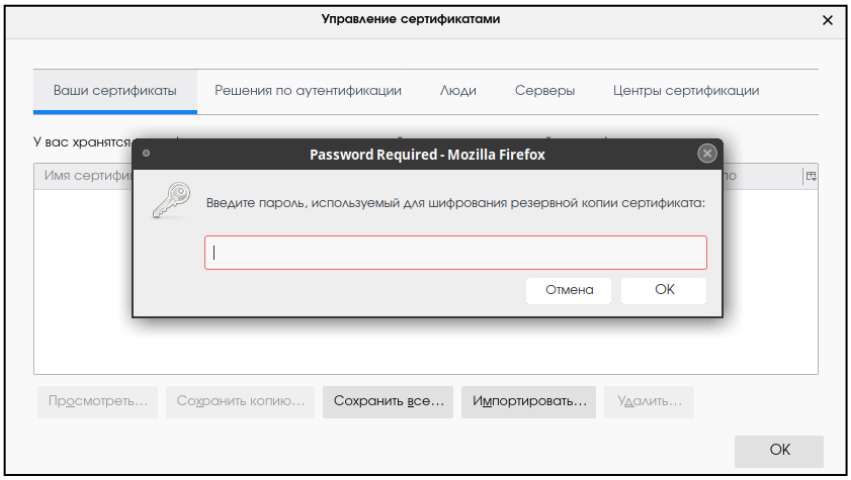


Рисунок 4 – Окно ввода PIN-кода сертификата

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

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

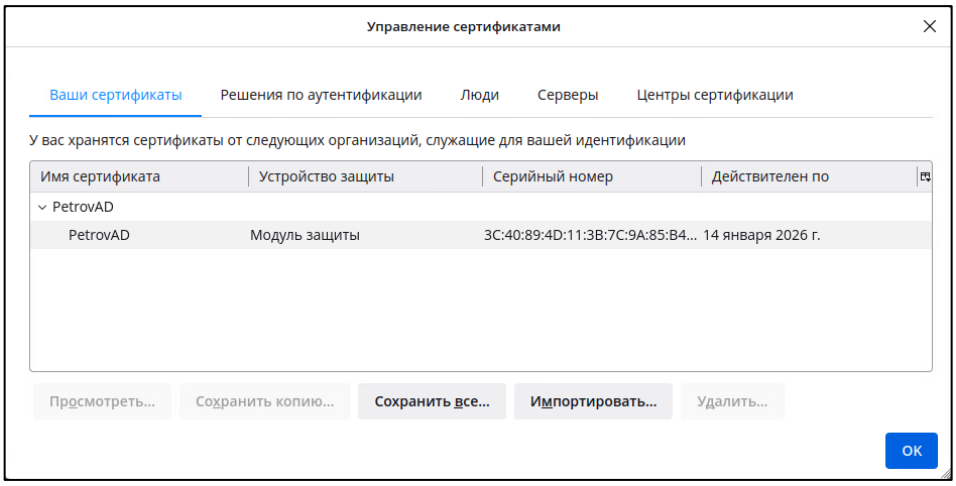


Рисунок 5 – Окно «Управление сертификатами»

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 Центр регистрации Aladdin eRA (например, `https://172.22.5.21`).
- В открывшемся окне выберите сертификат администратора (см. Рисунок 6) и нажмите кнопку <OK>.

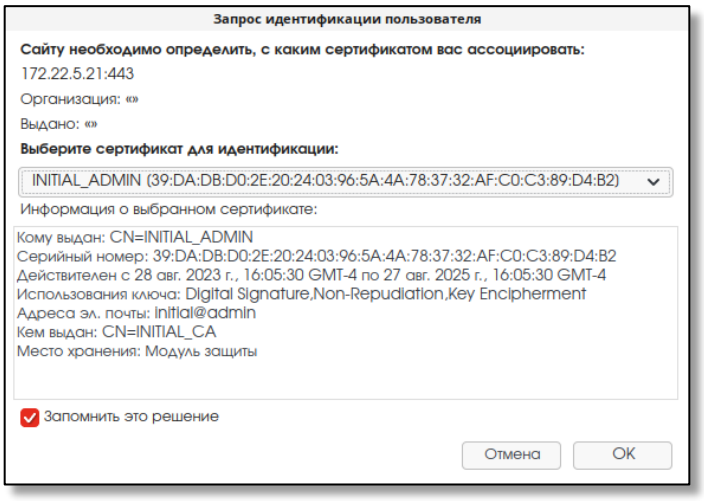


Рисунок 6 – Выбор сертификата для установки двустороннего TLS-соединения

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.

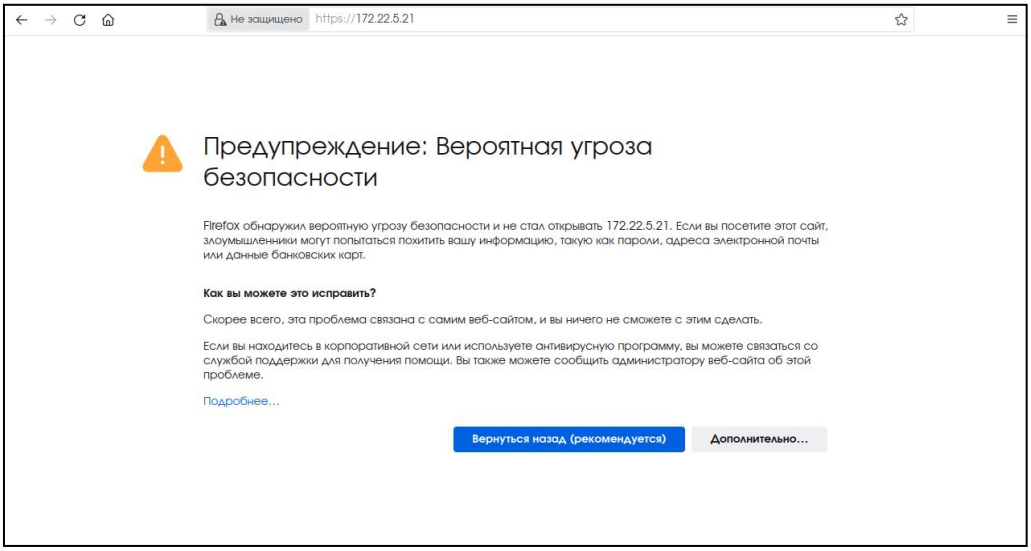


Рисунок 7 – Страница с предупреждением системы безопасности

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

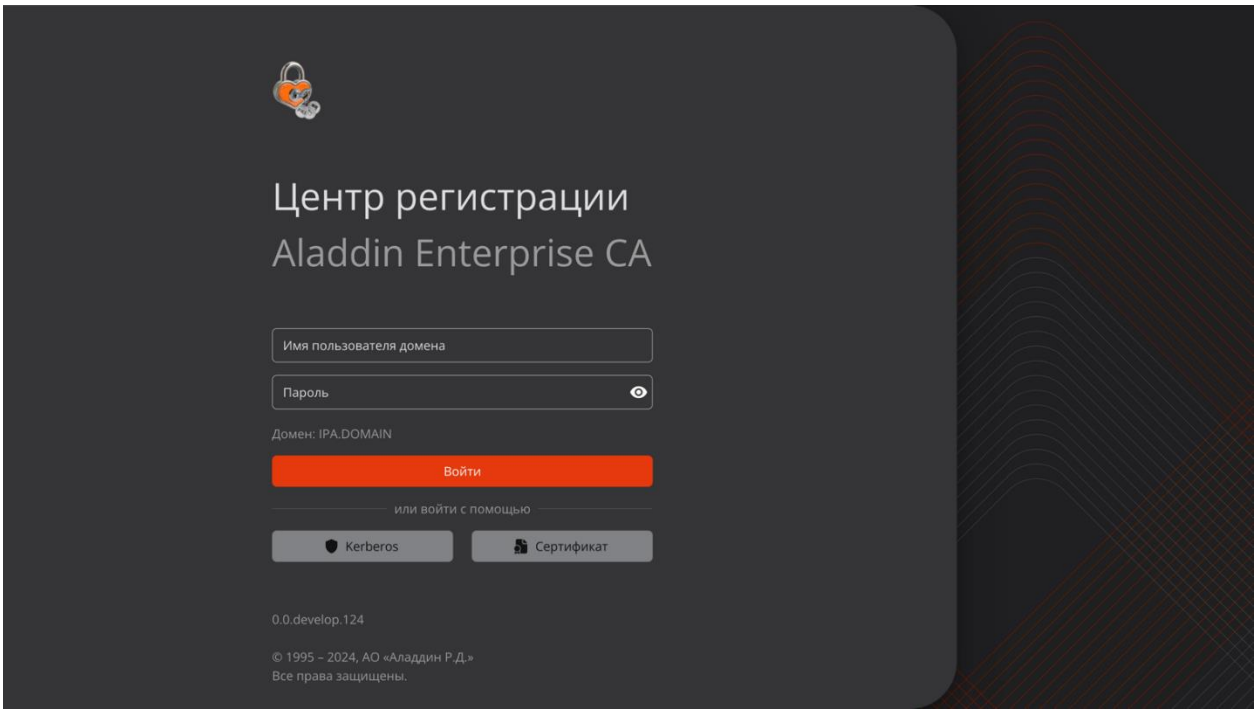


Рисунок 8 – Окно авторизации

Центр регистрации Aladdin eRA поддерживает следующие способы аутентификации:

- С использованием сертификата (см. раздел 6.4).
- С использованием Kerberos-билета (см. раздел 6.6);
- По логину и паролю (см. раздел 6.5).

6.4 Аутентификация с использованием сертификата

Пользователи Центра регистрации Aladdin eRA могут аутентифицироваться в Центре регистрации Aladdin eRA по своим сертификатам доступа. При этом роль учётной записи в Центр регистрации Aladdin eRA соответствует роли в Центре сертификации Aladdin eCA (администратор или оператор).

Для аутентификации по сертификату следует выполнить следующие шаги:

- Откройте пользовательский интерфейс Центра регистрации Aladdin eRA.
- В появившемся окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) выберите установленный ранее сертификат учётной записи. Нажмите кнопку <OK> для подтверждения.
- В появившемся окне авторизации Центра регистрации Aladdin eCA (см. Рисунок 8) нажмите на кнопку <Сертификат>.

В результате будет выполнена аутентификация по сертификату. В ходе аутентификации по сертификату могут возникать следующие ошибки (Таблица 8):

Таблица 8 – 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 Центром сертификации Aladdin eCA, не входящим в список разрешённых издателей сертификатов доступа, к которому подключён Центр регистрации Aladdin eRA
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи (параметр `session_max_count` в конфигурационном файле)

6.5 Аутентификация по логину и паролю

Для аутентификации с помощью логина и пароля, предварительно нужно зарегистрировать в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, 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[72] могут аутентифицироваться в Центре регистрации Aladdin eRA по комбинации доменного имени и пароля. Информация о домене отображена в окне авторизации в поле «Домен».

Для аутентификации по комбинации доменного имени и пароля следует выполнить следующие шаги:

- Откройте пользовательский интерфейс Центра регистрации Aladdin eRA.

  Пропустите шаг с выбором сертификата в появившемся окне «выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6).

- В появившемся окне авторизации Центра регистрации Aladdin eRA (см. Рисунок 8) введите доменное имя, пароль и нажмите на кнопку <Войти>.

[72] Учётные записи, находящиеся в домене, к которому подключён Центр регистрации Aladdin eCA (адрес сервера AD задан в параметре `kerberos_ad_server` в файле `/opt/aecaRa/scripts/config.sh`)

- При успешной доменной аутентификации по введённому доменному имени и паролю, пользователю будет предоставлен доступ к Центру регистрации Aladdin eRA.

  Если у пользователя отсутствовала[73] учётная запись в Центре регистрации Aladdin eRA, то она будет автоматически создана с ролью «Получатель сертификатов».

При аутентификации по доменному имени и паролю могут возникать следующие ошибки (Таблица 9).

Таблица 9 – 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 Центре регистрации Aladdin eRA. (Параметр `session_max_count` в файле `/opt/aecaRa/scripts/config.sh`)

6.6 Аутентификация с использованием Kerberos-билета

Для аутентификации с использованием Kerberos-билета, предварительно нужно зарегистрировать в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, 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[74] могут аутентифицироваться в Центре регистрации Aladdin eRA по Kerberos-билету. Информация о домене отображена в окне авторизации в поле «Домен».

Предварительно на клиенте должен быть настроен браузер для работы с Kerberos[75], а также должен быть получен Kerberos-биллет.

Для аутентификации по Kerberos-билету следует выполнить следующие шаги:

- Откройте пользовательский интерфейс Центра регистрации Aladdin eRA.

  Пропустите шаг с выбором сертификата в появившемся окне «выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6).

- В появившемся окне авторизации Центра регистрации Aladdin eRA (см. Рисунок 8) нажмите на кнопку «Kerberos».

- При успешной доменной аутентификации по введённому доменному имени и паролю, пользователю будет предоставлен доступ к Центру регистрации.

  Если у пользователя отсутствовала[76] учётная запись в Центре регистрации Aladdin eRA, то она будет автоматически создана с ролью «Получатель сертификатов».

При аутентификации по Kerberos-билету могут возникать следующие ошибки (Таблица 10).

[73] Проверка связи осуществляется путём сравнения идентификатора учётной записи в домене с идентификаторами учётных записей в базе данных.

[74] Учётные записи, находящиеся в домене, к которому подключён Центр регистрации Aladdin eCA (адрес сервера AD задан в параметре `kerberos_ad_server` в файле `/opt/aecaRa/scripts/config.sh`)

[75] Инструкцию по настройке Kerberos-аутентификации в браузерах см. в «Настройка Kerberos в веб-браузере»

[76] Проверка связи осуществляется путём сравнения идентификатора учётной записи в домене с идентификаторами учётных записей в базе данных.

Таблица 10 – 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 браузера[77]
«Срок действия Kerberos-билета истек»	Срок действия Kerberos-билета истек – необходимо получить новый билет с помощью команды `kinit`
«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 `session_max_count` в файле `/opt/aecaRa/scripts/config.sh`)

6.7 Выход из программы

Выход из программы доступен для аутентифицированных пользователей. Для выхода следует выполнить следующие шаги:

- На верхней панели (см. Рисунок 9) веб-интерфейса Центра регистрации нажмите на имя учётной записи пользователя.
- В появившемся меню нажмите на кнопку <Выйти>.

После этого будет произведен выход и отобразится окно авторизации Центра регистрации Aladdin eRA (см. Рисунок 8).

Если выход был выполнен после аутентификации по сертификату, то для входа по другому сертификату необходимо перезагрузить веб-браузер.

[77] Инструкцию по настройке Kerberos-аутентификации в браузерах см. в «Настройка Kerberos в веб-браузере»

7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

Данный раздел описывает функции управления Центра регистрации Aladdin eCA, доступные учётной записи с ролью Администратор.

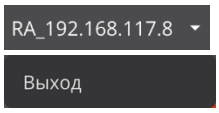
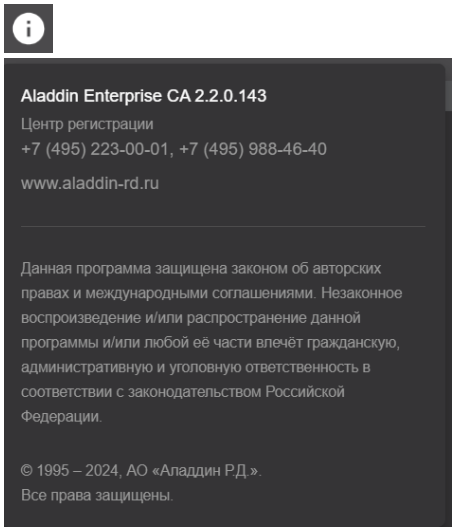
7.1 Верхняя панель

Верхняя панель (см. Рисунок 9) Центра регистрации фиксирована и отображается на любом шаге или переходе между разделами.

Рисунок 9 – Верхняя панель окна «Центра регистрации»

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

Верхняя панель содержит следующие элементы:

• 	- текущая авторизация учётной записи пользователя, при нажатии неё отображается меню с кнопкой <Выход>[78];
• 	- сведения о текущей версии программы, контактная информация разработчика, права на программное обеспечение.

7.2 Боковая панель

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

Полный вид боковой панели показан на рисунке ниже (Рисунок 10). Компактный вид боковой панели приведён на рисунке ниже (Рисунок 11). Выбор вида боковой панели происходит по нажатию кнопки  , расположенной внизу данной панели.

[78] Подробнее про выход из Центра регистрации Aladdin eRA см. подраздел 6.7

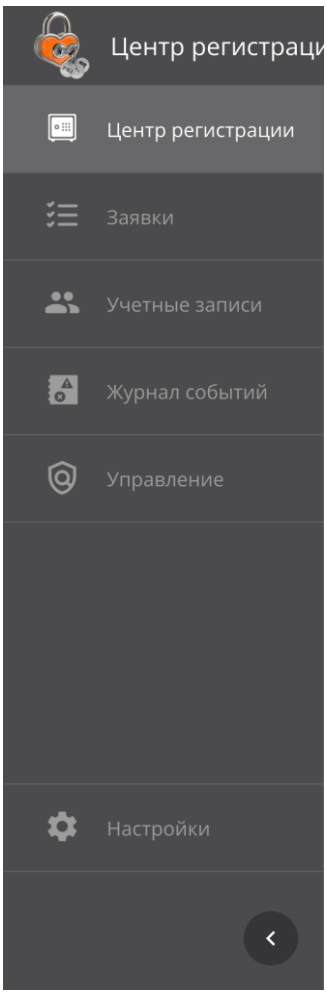


Рисунок 10 – Полный вид боковой панели

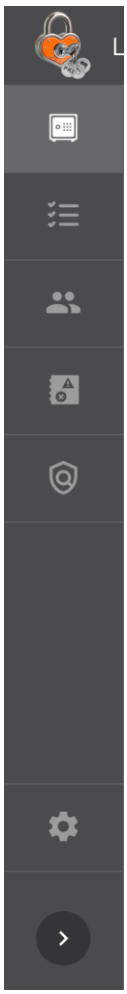


Рисунок 11 – Компактный вид боковой панели

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

- 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.
- Раздел «Настройки» – в данном разделе возможно:
  - просмотреть информацию о сертификате веб-сервера;
  - сменить текущий сертификат веб-сервера;
  - просмотреть список разрешённых издателей

Доступность разделов в зависимости от ролей представлена в таблице ниже (Таблица 11).

Таблица 11 – Доступность раздела в зависимости от роли учётной записи

Раздел	Получатель сертификатов	Оператор	Администратор
Центр регистрации	–	–	✓
Заявки	✓	✓	✓
Учётные записи	–	–	✓
Журнал событий	–	✓	✓
Управление	–	–	✓
Настройки	–	–	✓

7.3 Раздел «Центр регистрации»

Переход на экран раздела «Центр регистрации» осуществляется по выбору раздела «Центр регистрации» бокового меню, расположенного слева на главном экране (см. Рисунок 10).

Данный раздел доступен только для администратора.

На экране раздела «Центр регистрации» отображены (см. Рисунок 12):

- информация о Центре сертификации, с котором установлено подключение и который получает запросы от настоящего Центра регистрации:

- Подключённый Центр сертификации Aladdin eCA (CN) – Common name Центра сертификации;
- Подключённый Центр сертификации Aladdin eCA (HostName) – IP-адрес или Hostname Центра сертификации;
- Сертификат доступа к ЦС – расположение сертификата для доступа к Центра сертификации Aladdin eCA.

- информация об общем количестве созданных заявок:
  - Создано заявок (всего) – общее количество заявок на сертификаты, созданных с момента регистрации Центра регистрации Aladdin eRA.
- информация о заявках на сертификаты:
  - Блок «Ожидает подтверждения» – количество заявок на сертификаты, ожидающих рассмотрения. В блоке отображаются:
    - общее количество созданных заявок на сертификаты цифрами синего цвета;
    - количество созданных заявок на сертификаты за последнюю неделю.
  - Блок «Выполнена» – количество сертификатов доступа, выпущенных Центром сертификации по согласованным заявкам на сертификаты. В блоке отображаются:
    - общее количество выпущенных сертификатов цифрами зелёного цвета;
    - количество выпущенных сертификатов доступа Центром сертификации по согласованным заявкам на сертификаты за последнюю неделю.
  - Блок «Заявка отклонена» – количество отклонённых заявок. В блоке отображаются:
    - общее количество отклонённых заявок цифрами оранжевого цвета;
    - количество отклонённых заявок за последнюю неделю.
  - Блок «Ошибка выпуска» – количество заявок, при обработке которых произошла ошибка. В блоке отображаются:
    - общее количество заявок с ошибками цифрами красного цвета;
    - количество заявок с ошибками за последнюю неделю.

Раздел «Центр регистрации» является информационным и не предоставляет каких-либо действий.

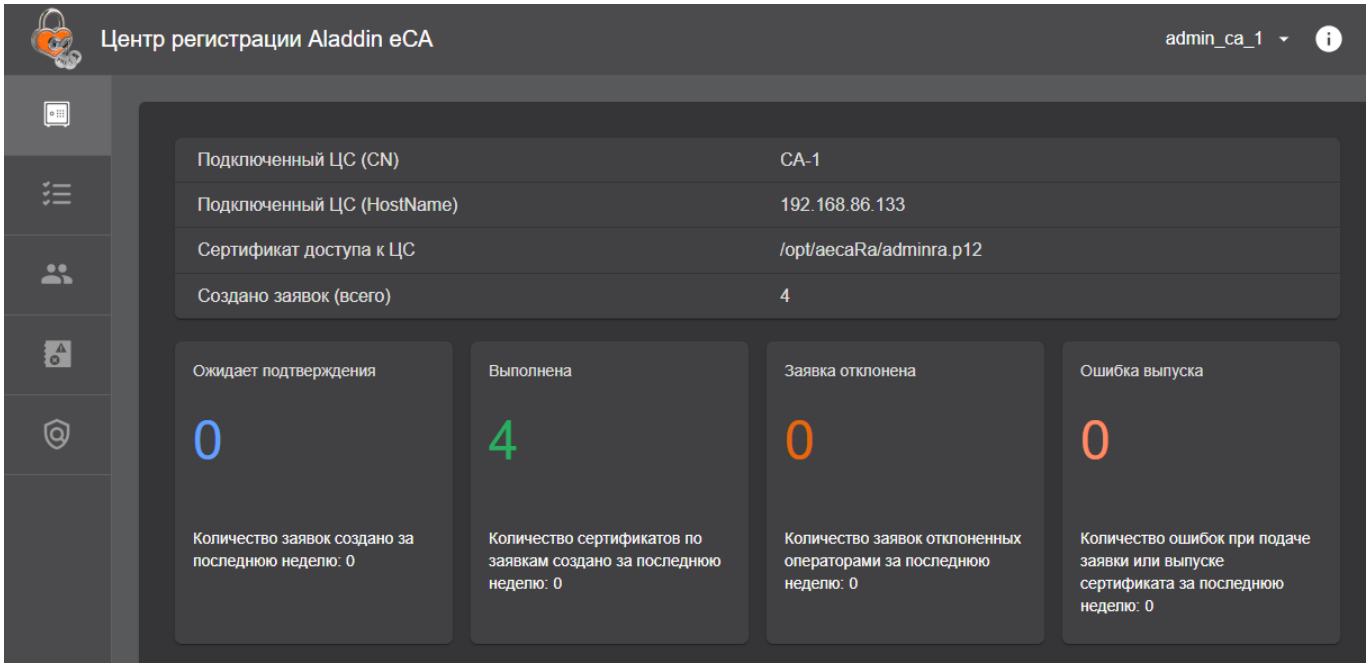


Рисунок 12 – Экран раздела «Центр регистрации»

7.4 Раздел «Заявки»

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.

Переход на экран раздела «Заявки» (см. Рисунок 13) осуществляется по выбору раздела «Заявки» бокового меню, расположенного слева на главном экране (см. Рисунок 10).

Данный раздел доступен для всех учётных записей:

- для пользователя с ролью «Администратор» на данном экране отображаются все созданные в Центре регистрации Aladdin eRA 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 13);
- пользователь с ролью «Оператор» может просматривать созданные им заявки, просматривать и обрабатывать заявки для доступных ему субъектов[79], создавать заявки для любых субъектов Центре сертификации Aladdin eCA, к которому подключён Центре регистрации Aladdin eRA, скачивать и отзывать сертификаты, выпущенные по заявкам доступным ему субъектов;
- пользователь с ролью «Получатель сертификатов» может просматривать только свои заявки, создавать новые заявки, получать выпущенные по своим заявкам сертификаты, а также отзывать их.

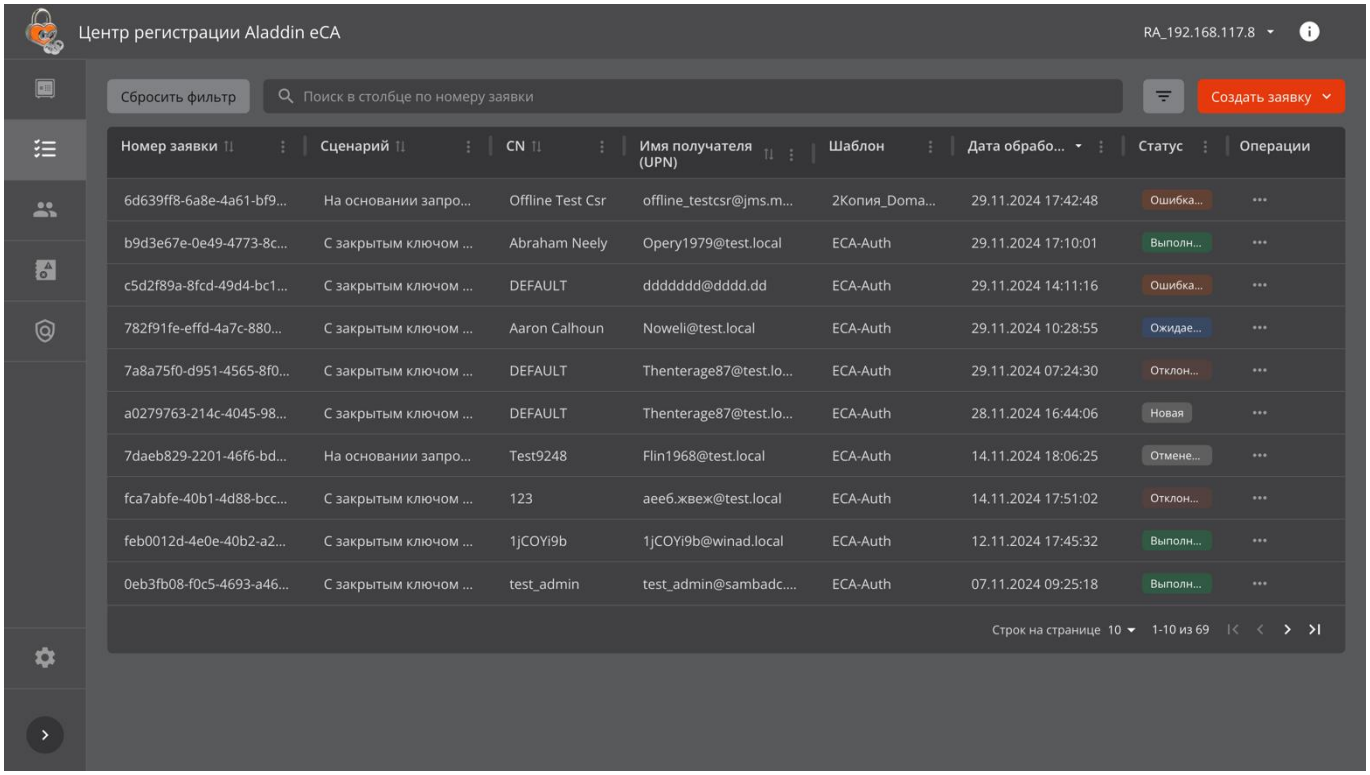


Рисунок 13 – Экран раздела «Заявки». Вид для администратора

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

- Номер заявки – содержит номер заявки;

[79] То есть заявки, у которых получателем сертификата является субъект, доступный данному оператору в соответствии с правилами доступа Центра сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA

- Сценарий – содержит сценарий, по которому была создана заявка («На основании запроса (PKCS#10)», «С закрытым ключом (PKCS#12)», «На ключевом носителе», «SCEP» [80] или «WSTEP» [81]);
- CN – содержит CN, указанный в заявке на сертификате;
- Имя получателя (UPN) – содержит UPN отправителя заявки;
- 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»[82], «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. Таблица 12.):
  - 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 14, Рисунок 15 и Рисунок 16), 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;

[80] Заявки с типом «SCEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов клиентов по протоколу SCEP, подробнее см. раздел 8.

[81] Заявки с типом «WSTEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов клиентов по протоколу MS-WSTEP, подробнее см. раздел 9.

[82] Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.

- 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.

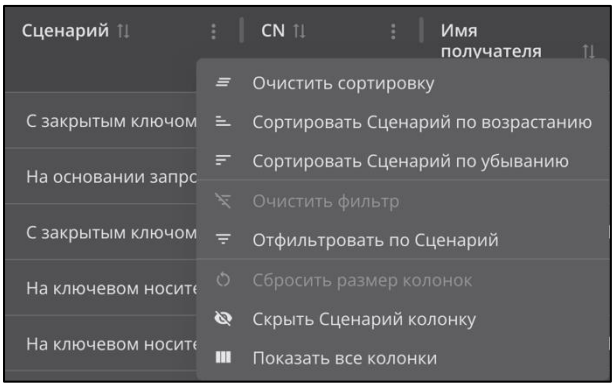


Рисунок 14 – Кнопка <Действия в колонке> в колонке «Сценарий»

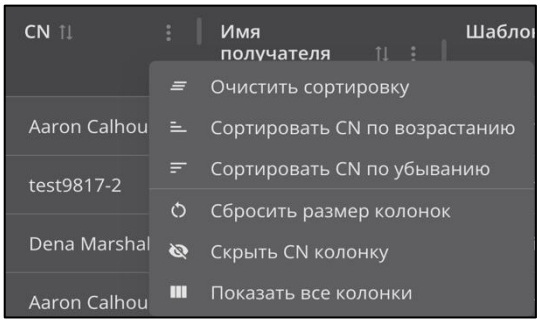


Рисунок 15 – Кнопка <Действия в колонке> в колонке «CN»

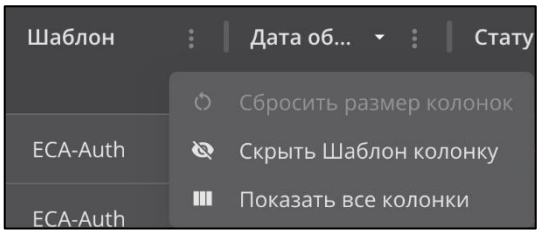


Рисунок 16 – Кнопка <Действия в колонке> в колонке «Шаблон»

Для сброса применённых фильтров следует нажать кнопку <Сбросить фильтр>  в результате чего в экранной таблице раздела «Заявки» будут отображены все произошедшие события (см. Рисунок 17).

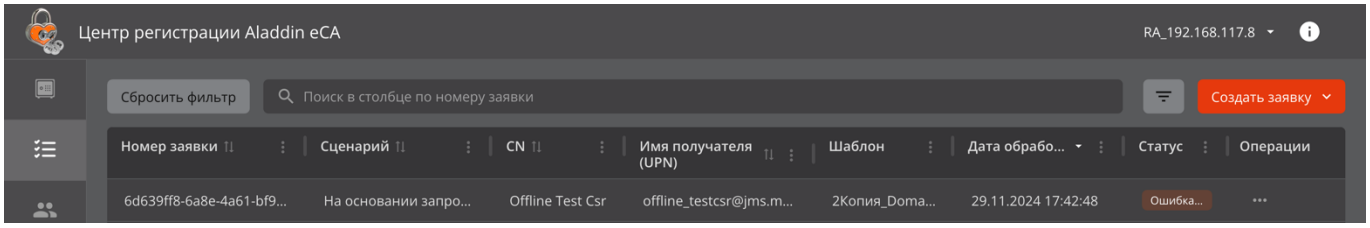


Рисунок 17 – Кнопка <Сбросить фильтр>

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 18):

- сценарий. Выберите сценарий выпуска сертификата (На основании запроса (PKCS#10), С закрытым ключом (PKCS#12), На ключевом носителе).
- дата обработки. Выберите период, в которой должна попадать дата обработки заявки. Введите дату с помощью клавиатуры или выберите в развернувшемся календаре;
- статус. Выберите статус заявки («Ошибка выпуска», «Отклонена», «Ожидает подтверждения», «Выполнена», «Отменена»[83], «Ожидает импорта на КН»).

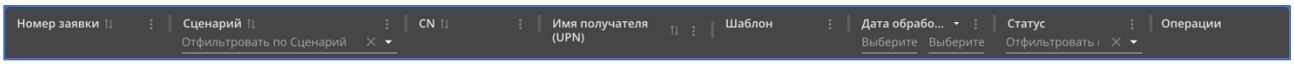


Рисунок 18 – Поля фильтра заголовков экранной таблицы

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

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

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

Для очистки применённых фильтров для каждого заголовка колонки нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 14)

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 19):

- 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 19 – 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 14, Рисунок 15).

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 14, Рисунок 15);
- или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

[83] Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.

7.4.4 Поиск заявок

Строка поиска (см. Рисунок 20) 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 20 – 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» осуществляется при нажатии на строку заявки главного экрана разделе «Заявки» (см. Рисунок 13).

Администратор может просматривать карточки заявок всех учётных записей Центра регистрации. Вид экрана «Карточка заявки» представлен на Рисунок 21.

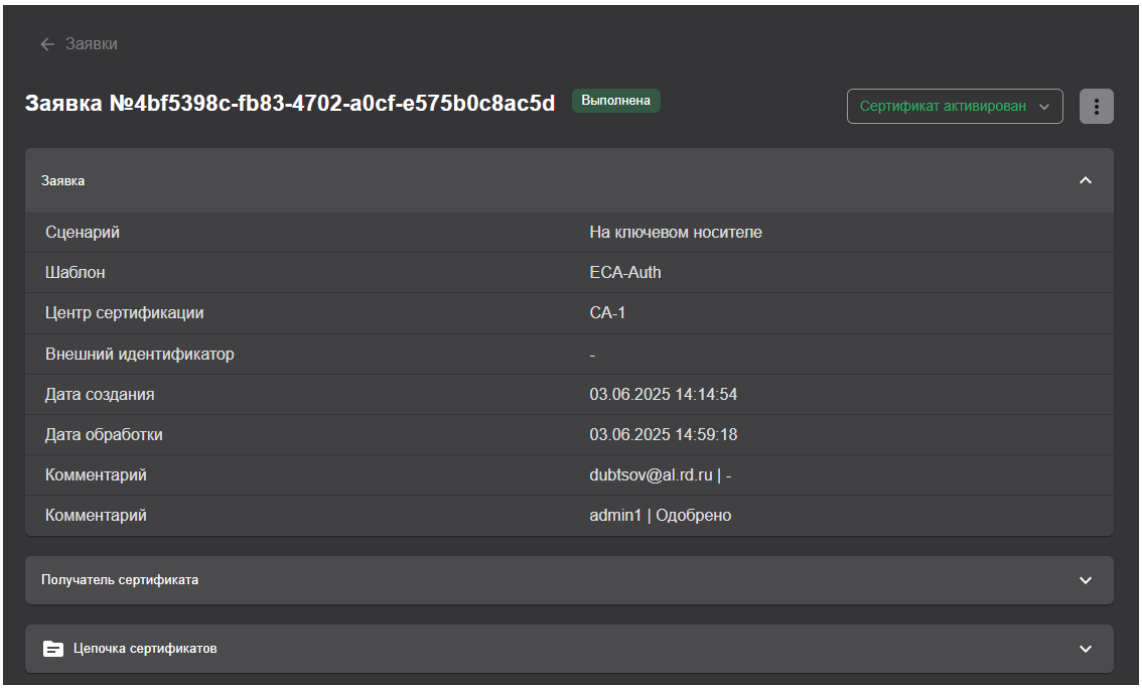


Рисунок 21 – Экран «Карточка заявки». Вид для администратора

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»[84], «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.

[84] Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска сертификата.

- Кнопка  с контекстным меню действий (состав действий (Таблица 12), контекстное меню см. Рисунок 22, Рисунок 23 и Рисунок 24).

Таблица 12 – 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
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

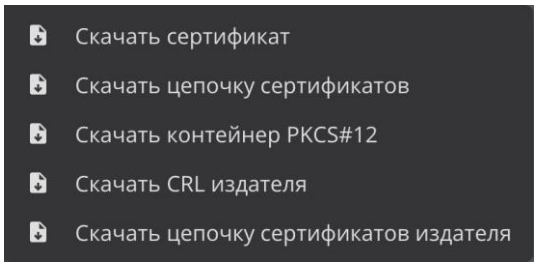


Рисунок 22 – Меню действий в карточке заявки. Вид для администратора. Выполненная заявка со сценарием «С закрытым ключом (PKCS#12)»

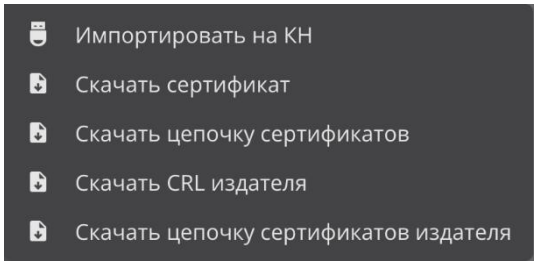


Рисунок 23 – Меню действий для заявки. Вид для администратора. Выполненная заявка со сценарием «На основании запроса (PKCS#10)»

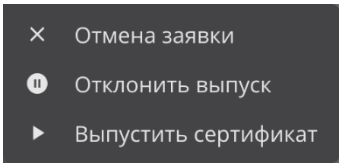


Рисунок 24 – Меню действий для заявки. Вид для администратора. Заявка в статусе Ожидает подтверждения, создателем данной заявки является текущая учётная запись

- Блок «Заявка», содержащий следующие строки в формате «ключ – значение» (см. Рисунок 25):
  - 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.

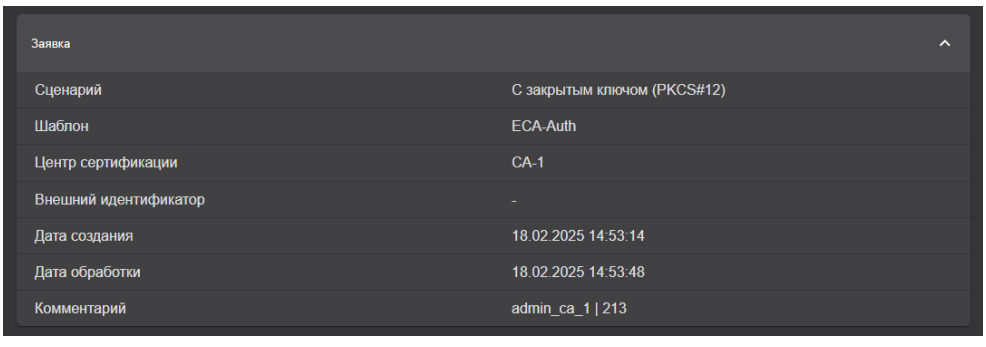


Рисунок 25 – Экран «Карточка заявки». Вид для администратора. Блок «Заявка»

- Блок «Получатель сертификата», содержащий следующие строки в формате «ключ – значение» (см. Рисунок 26):
  - 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.

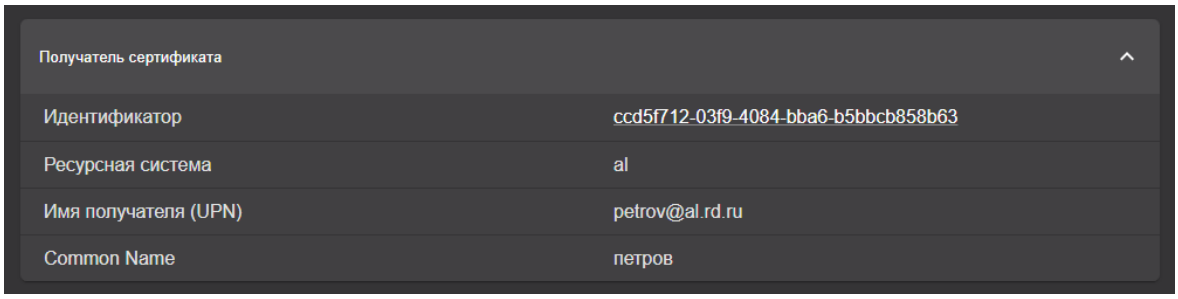


Рисунок 26 – Экран «Карточка заявки». Вид для администратора. Блок «Получатель сертификата»

- Блок «Информация о сертификате», содержащий (см. Рисунок 27):
  - 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.

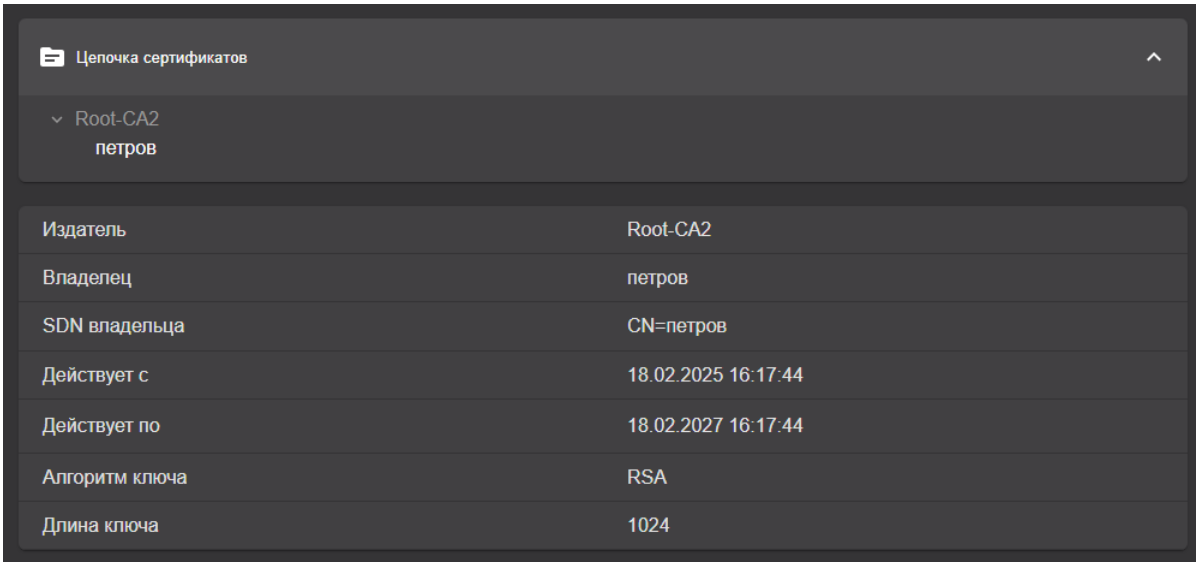


Рисунок 27 – Экран «Карточка заявки». Вид для администратора. Блок «Информация о сертификате»

- Блок «Состав сертификата», содержащий следующую информацию о сертификате (см. Рисунок 28):
  - Серийный номер – поле «Serial Number» сертификата;

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

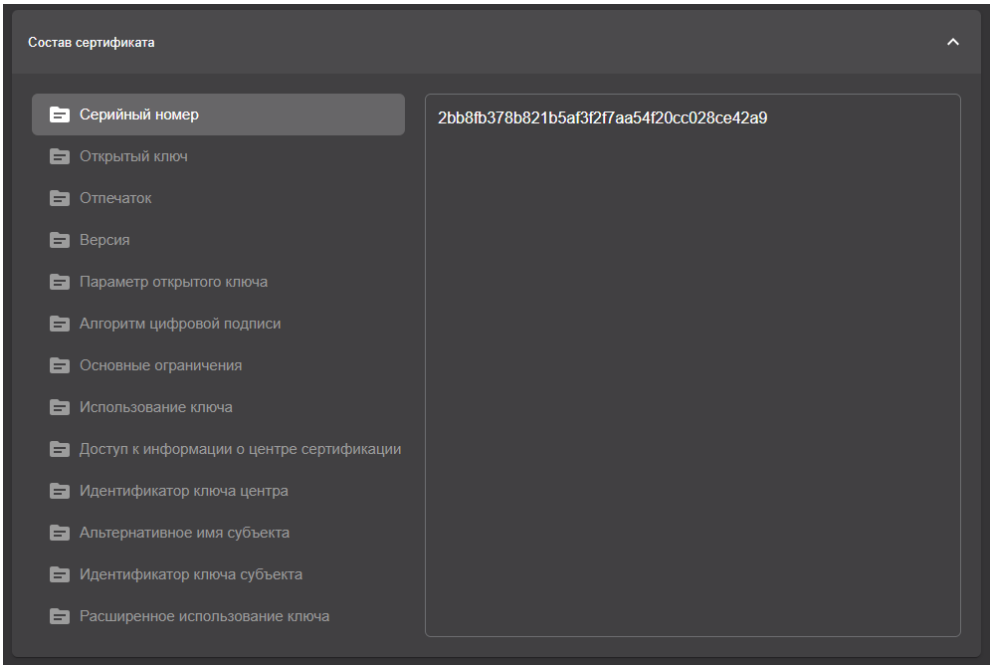


Рисунок 28 – Экран «Карточка заявки». Вид для администратора. Блок «Состав сертификата»

- Блок «История изменения заявки», содержащий историю изменений заявки в табличном виде (см. Рисунок 29). 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.

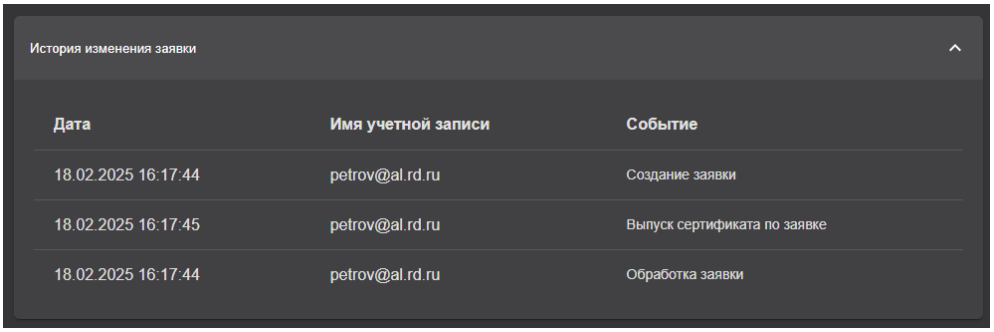


Рисунок 29 – Экран «Карточка заявки». Вид для администратора. Блок «История изменения заявки»

7.4.6 Создание заявки на основании запроса

Для создания заявки на основании запроса выполните следующие шаги:

- Нажмите кнопку <Создать +> на главном экране раздела «Заявки» (см. Рисунок 13).
- В открывшемся контекстном меню выберите сценарий выпуска сертификата «На основании запроса» (см. Рисунок 30).

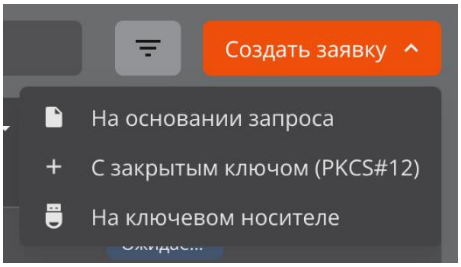


Рисунок 30 – Контекстное меню создания заявки

- В открывшемся окне «Создание заявки» на шаге 1 выберите субъект, для которого выпускается сертификат (см. Рисунок 31):
  - 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 31).
  - в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному
  - полю атрибуте у субъекта отсутствуют значения;
  - выберите субъект и нажмите кнопку <Продолжить> для перехода к следующему шагу.

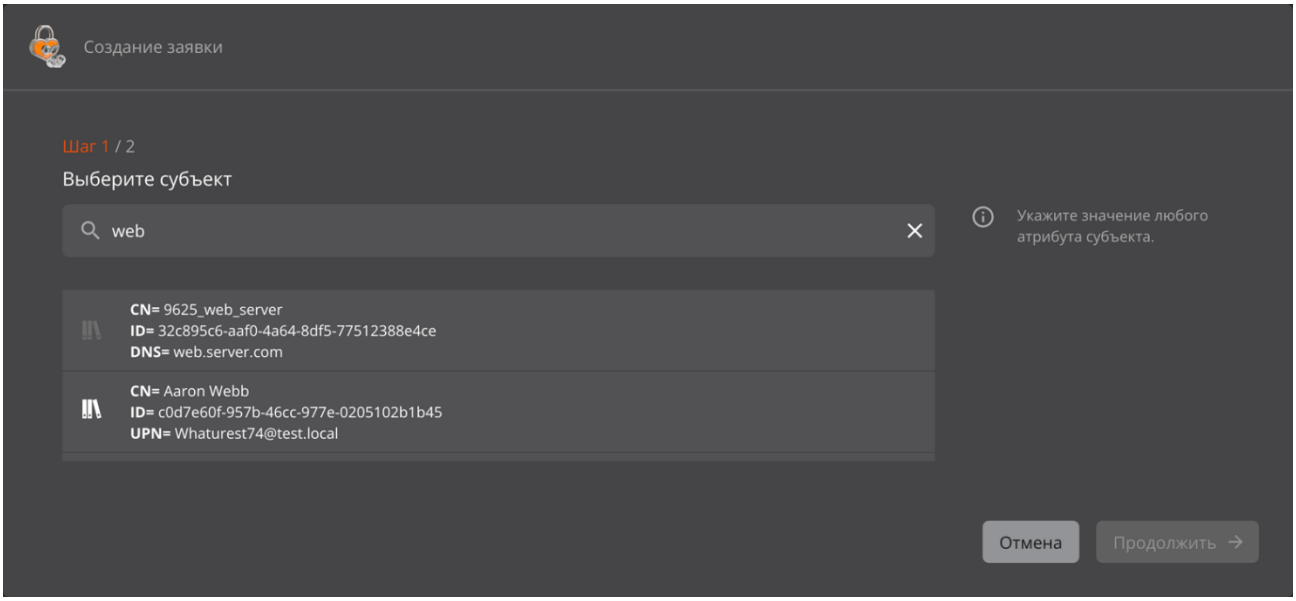


Рисунок 31 – Создание заявки на основании запроса. Шаг 1

- На втором шаге (см. Рисунок 32):
  - выберите файл-запрос (загружается по кнопке <Выбрать файл> с возможностью перевыбора 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[85].

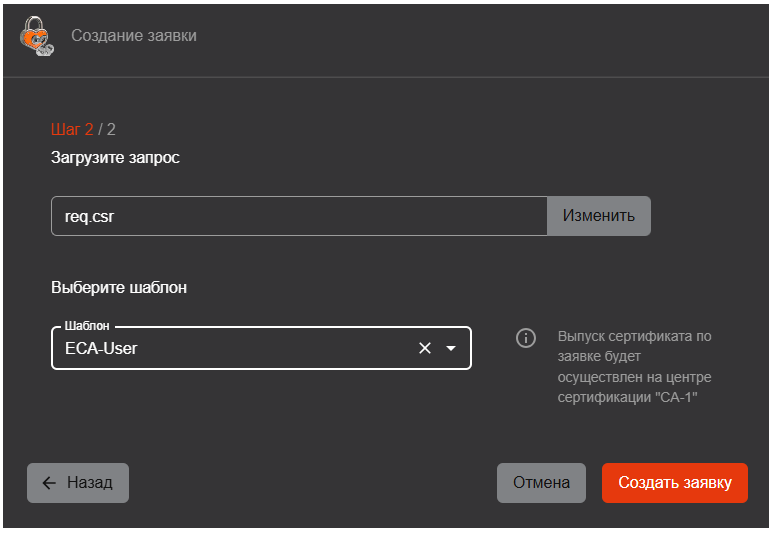


Рисунок 32 – Создание заявки на основании запроса. Шаг 2

- 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 13).
- В открывшемся контекстном меню выберите сценарий выпуска сертификата «С закрытым ключом (PKCS#12)» (см. Рисунок 33).

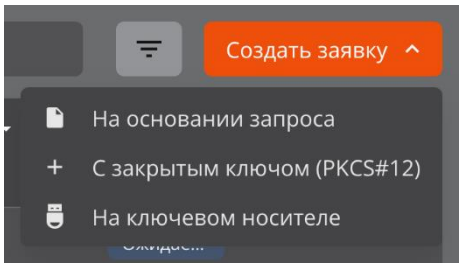


Рисунок 33 – Контекстное меню создания заявки

- В открывшемся окне «Создание заявки» на первом шаге выберите субъект, для которого выпускается сертификат (см. Рисунок 31):
  - 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:

[85] Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

- «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 полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;

– в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному

– полю атрибуте у субъекта отсутствуют значения.

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

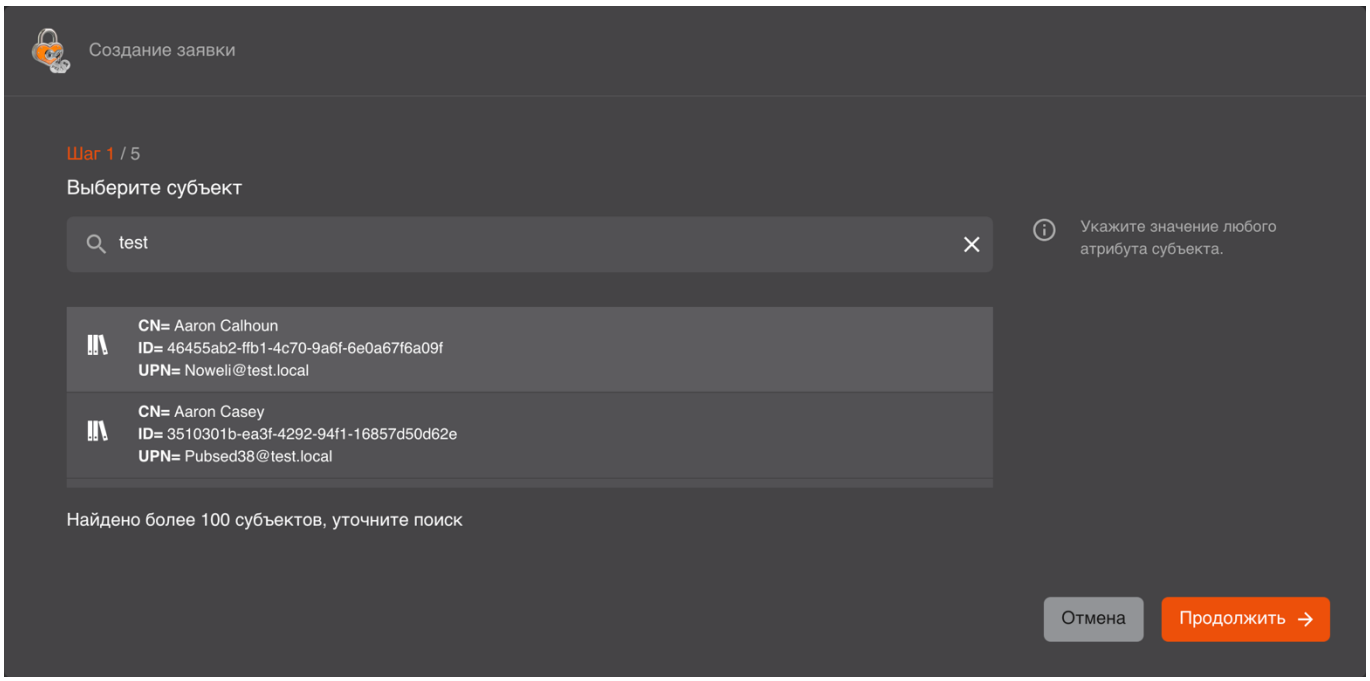


Рисунок 34 – Создание заявки с закрытым ключом PKCS#12. Шаг 1

- 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[86].

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

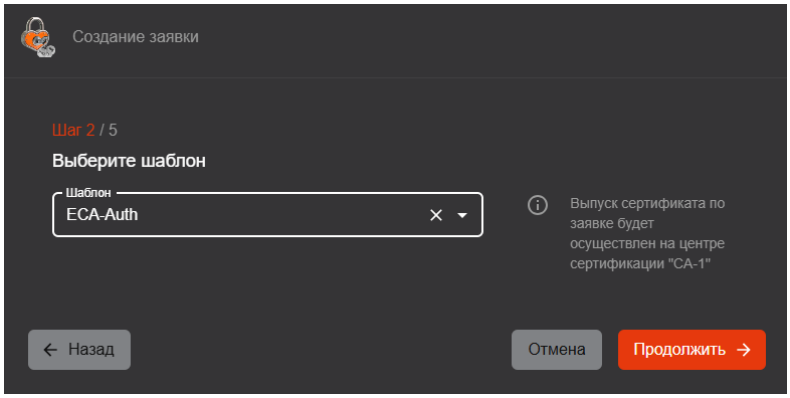


Рисунок 35 – Создание заявки с закрытым ключом PKCS#12. Шаг 2

[86] Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

- На третьем шаге указаны атрибуты в соответствии с шаблоном сертификата (см. Рисунок 36). 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.

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

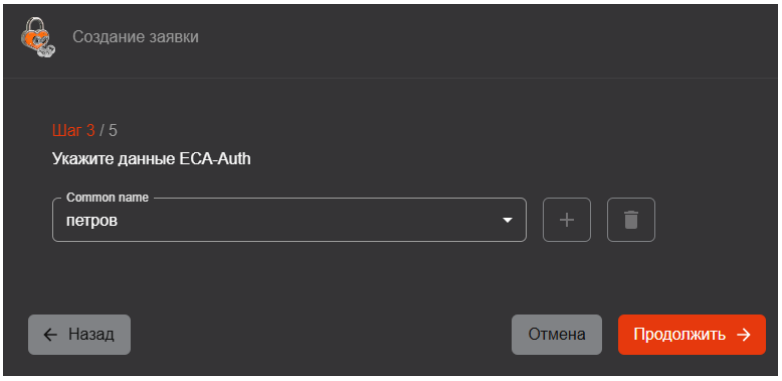


Рисунок 36 – Создание заявки с закрытым ключом PKCS#12. Шаг 3

- На четвёртом шаге задайте пароль для ключевого контейнера PKCS#12 (см. Рисунок 37):
  - 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.

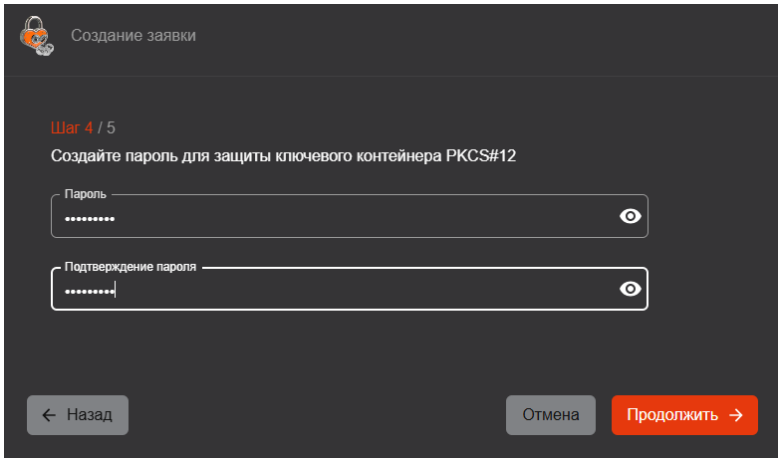


Рисунок 37 – Создание заявки с закрытым ключом PKCS#12. Шаг 4

- На пятом шаге укажите параметры криптографии (см. Рисунок 38):
  - выберите алгоритм генерации ключевой пары. Список алгоритмов определяется выбранным шаблоном;
  - выберите длину ключа. Минимальная доступная для выбора длина ключа определяется выбранным шаблоном.

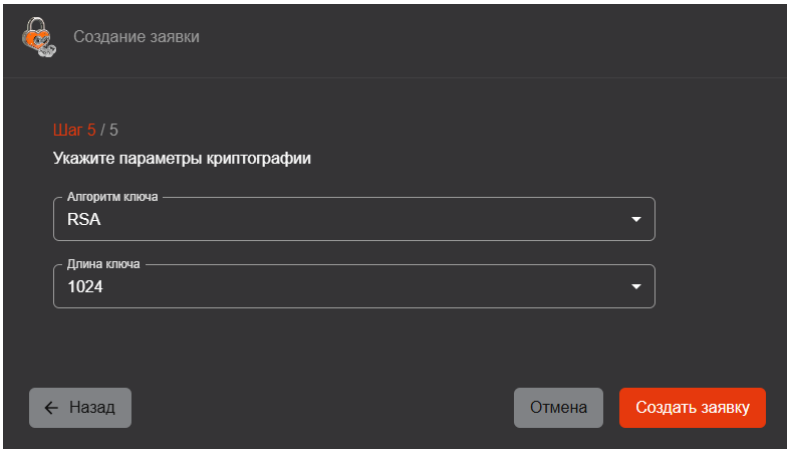


Рисунок 38 – Создание заявки с закрытым ключом PKCS#12. Шаг 5

- 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

На хосте, с которого выполняется сценарий, должно быть установлено ПО JC-WebClient. Также должен быть подключён ключевой носитель, поддерживаемый ПО JC-WebClient.

Для создания заявки на ключевом носителе выполните следующие шаги:

- Нажмите кнопку <Создать +> на главном экране раздела «Заявки» (см. Рисунок 39).
- В открывшемся контекстном меню выберите сценарий выпуска сертификата «На ключевом носителе» (см. Рисунок 40).

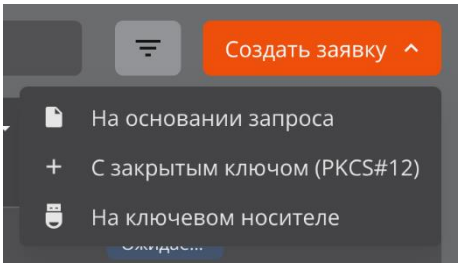


Рисунок 39 – Контекстное меню создания заявки

- При отсутствии установленного ПО JC-WebClient на хосте, с которого выполняется сценарий, отобразится окно с сообщением об ошибке (см. Рисунок 40).

  В данном случае необходимо установить на хост ПО JC-WebClient и повторить процесс создания заявки.

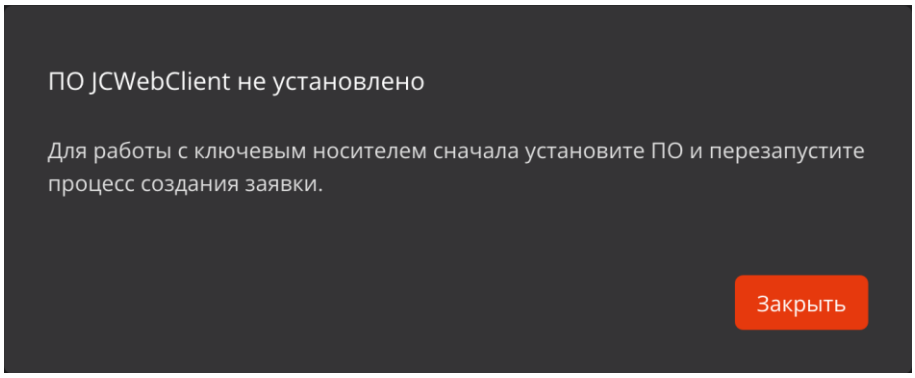


Рисунок 40 – Ошибка «ПО JS-WebClient не установлено»

- При наличии установленного ПО JC-WebClient и отсутствии подключённого ключевого носителя отобразится окно с сообщением об ошибке (см. Рисунок 41).

  В данном случае необходимо подключить ключевой носитель, поддерживаемый ПО JC-WebClient, и повторить процесс создания заявки.

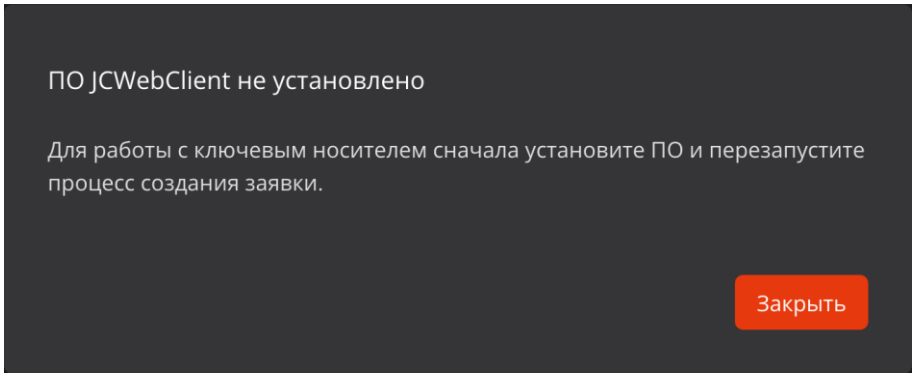


Рисунок 41 – Ошибка «Нет доступных устройств»

- При наличии установленного ПО JC-WebClient и подключённого ключевого носителя, поддерживаемого ПО JC-WebClient, отобразится окно «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 42).
  – в результате поиска в полях «CN», «UPN» и «DNS» отображаются все значения соответствующего полю атрибута субъекта, разделитель значений в поле – запятая с пробелом;
  – в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному
  – полю атрибуте у субъекта отсутствуют значения.

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

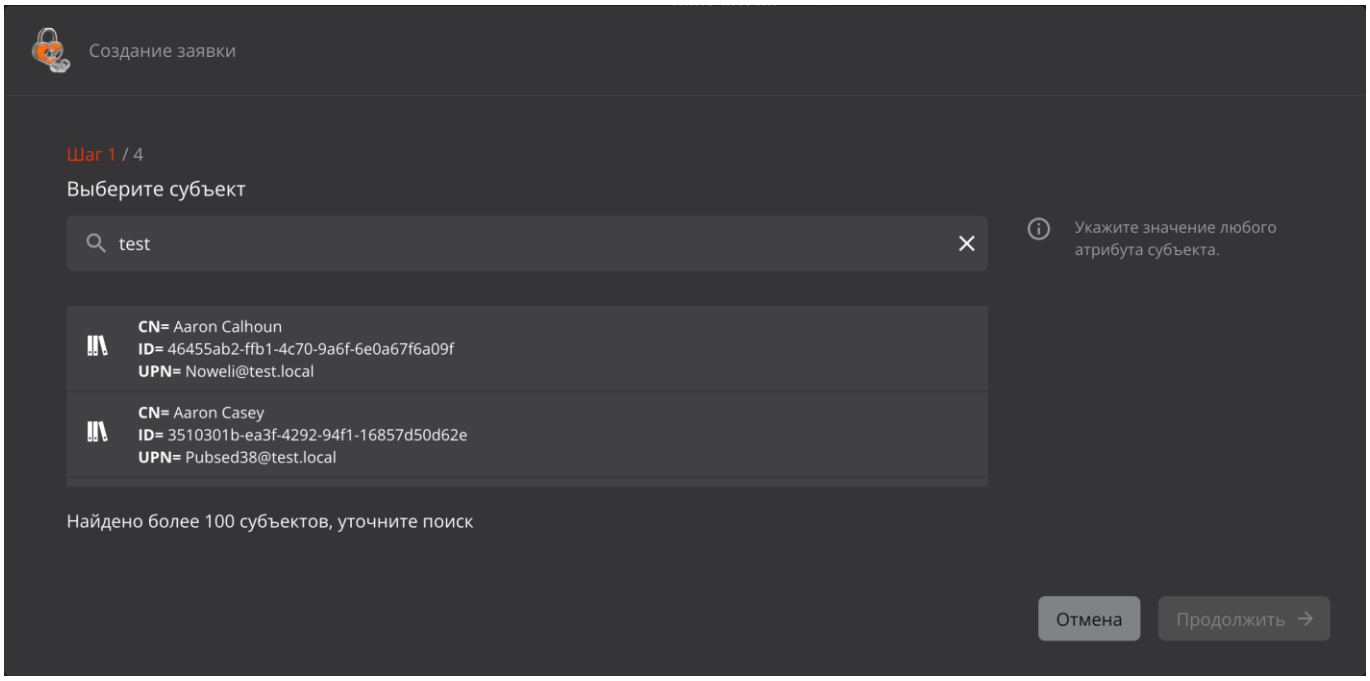


Рисунок 42 – Создание заявки на ключевом носителе. Шаг 1

- На втором шаге (см. Рисунок 43):
  - выберите ключевой носитель;
  - введите PIN-код от ключевого носителя;
  - 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[87].

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

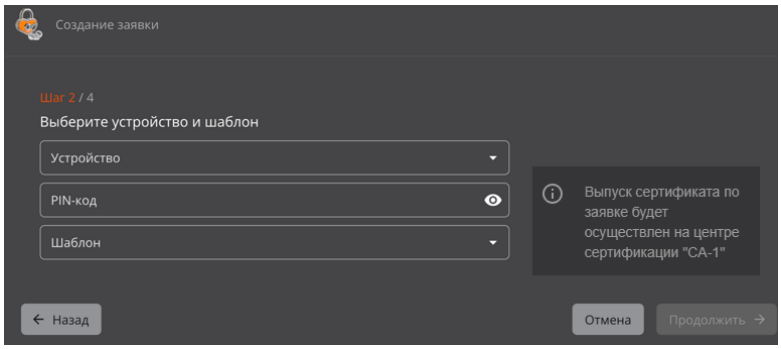


Рисунок 43 – Создание заявки на ключевом носителе. Шаг 2

- На третьем шаге указаны атрибуты в соответствии с шаблоном сертификата (см. Рисунок 44). Значения атрибутов заполняются автоматически в соответствии с данными из субъекта Центра сертификации Aladdin eCA, 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.

[87] Субъект может быть указан в правилах выпуска как напрямую, так и косвенно через группу безопасности.

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.

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

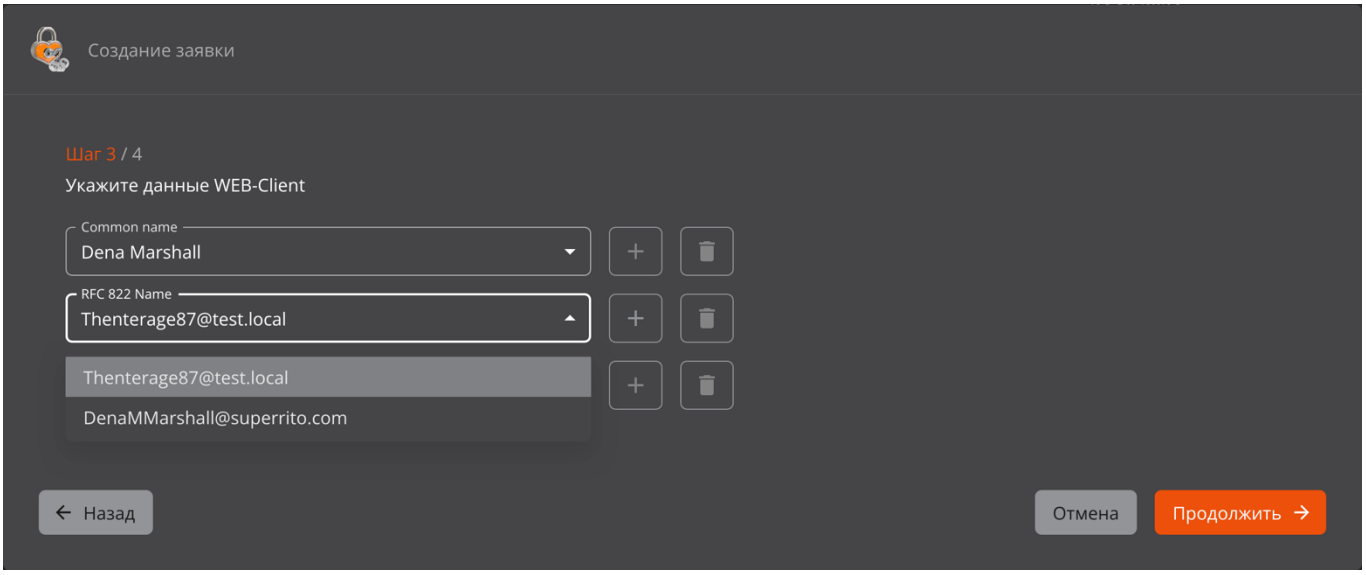


Рисунок 44 – Создание заявки на ключевом носителе. Шаг 3

- На четвёртом шаге укажите параметры криптографии (см. Рисунок 45):
  - выберите алгоритм генерации ключевой пары. Список алгоритмов определяется выбранным шаблоном;
  - выберите длину ключа. Минимальная доступная для выбора длина ключа определяется выбранным шаблоном.

  Нажмите на кнопку <Создать заявку> для перехода к завершающему шагу.

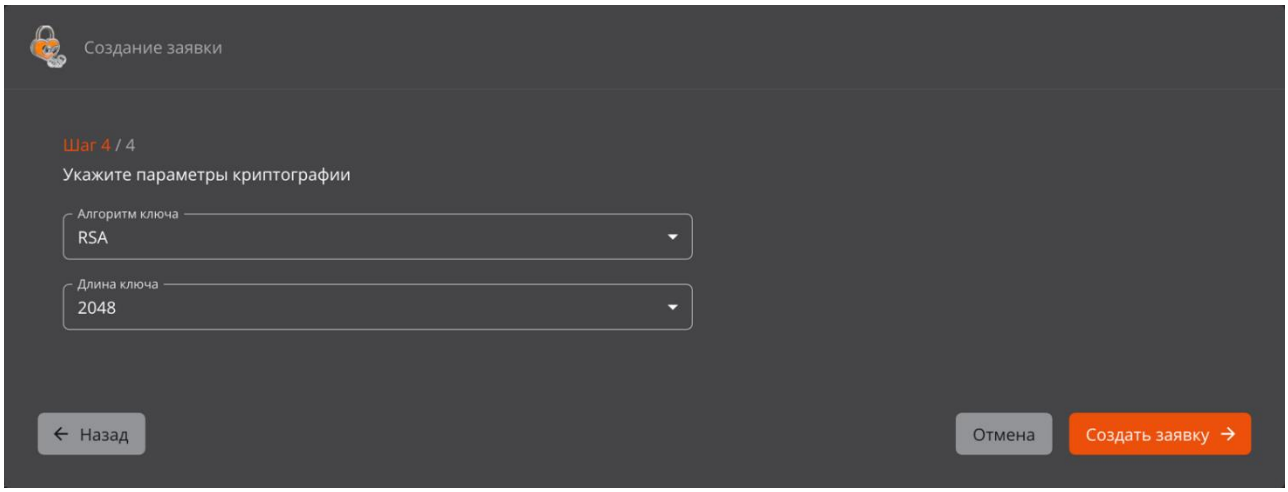


Рисунок 45 – Создание заявки на ключевом носителе. Шаг 4

- На завершающем шаге отображаются следующие стадии выполнения (см. Рисунок 46):
  - стадия «Генерация ключевой пары»;
  - стадия «Генерация запроса»;
  - стадия «Создание заявки».

В случае успешного завершения процесса (в соответствии с Рисунок 46) будет отображено успешное прохождение вышеуказанных стадий (отображение флажка в чек-боксе с положительной (зелёной) индикацией чек-бокса), а также сообщение об успешном создании заявки и текстовая подсказка о возможности импорта сертификата на КН при переходе заявки в статус «Ожидает импорта на КН».

Если во время выполнения стадий создания заявки будут выявлены ошибки, то информация об этом будет отражена под соответствующей стадией.

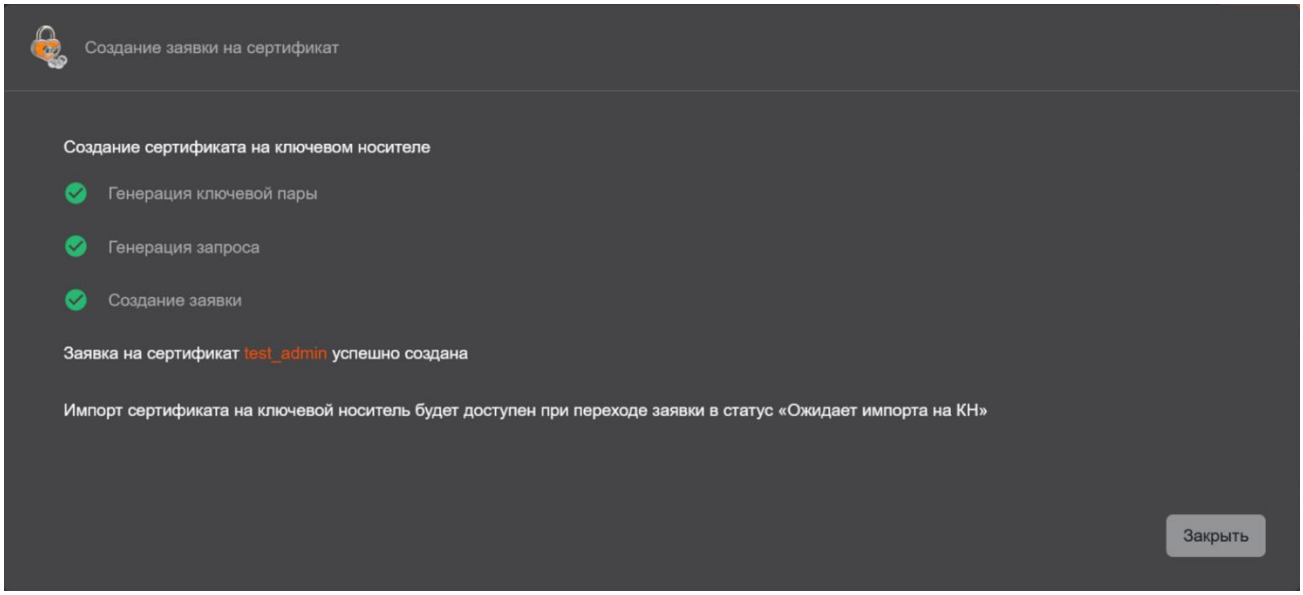


Рисунок 46 – Создание заявки на ключевом носителе. Завершающий шаг

- Для закрытия окна нажмите на кнопку <Закрыть>.

  Импорт сертификата на ключевой носитель будет доступен при переходе заявки в статус «Ожидает импорта на КН» (см. раздел 7.4.11).

7.4.9 Отмена заявки

Статус заявки, учатсвующей 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 находится 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 47) выберите действие «Отмена заявки».

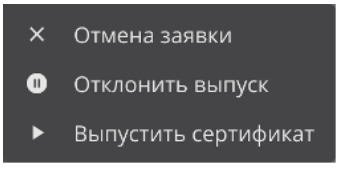


Рисунок 47 – Меню действий для заявки. Вид для администратора. Заявка в статусе Ожидает подтверждения, создателем данной заявки является текущая учётная запись

- В появившемся окне введите комментарий к отмене заявки (см. Рисунок 48).

  Нажмите на кнопку <Отменить> для подтверждения действия.

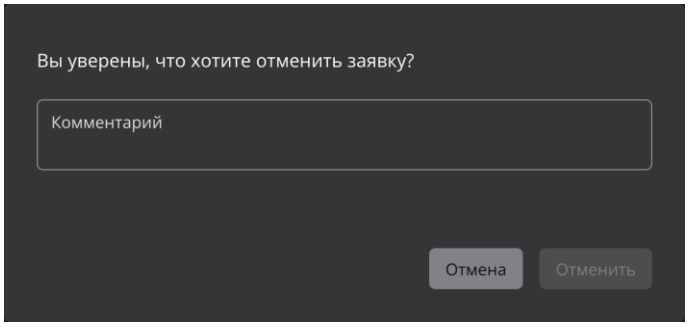


Рисунок 48 – Окно комментария к отмене заявки

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

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

7.4.10 Обработка заявки администратором

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 находится 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 49) выберите действие из перечня:

  – Отклонить выпуск;

  – Выпустить сертификат.

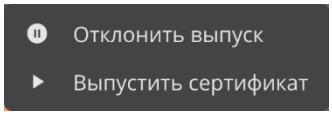


Рисунок 49 – Меню действий для заявки. Вид для администратора. Заявка в статусе Ожидает

- В появившемся окне введите комментарий к действию (см. Рисунок 50 и Рисунок 51).

  Нажмите на кнопку <Выпустить> или <Отклонить> для подтверждения действия.

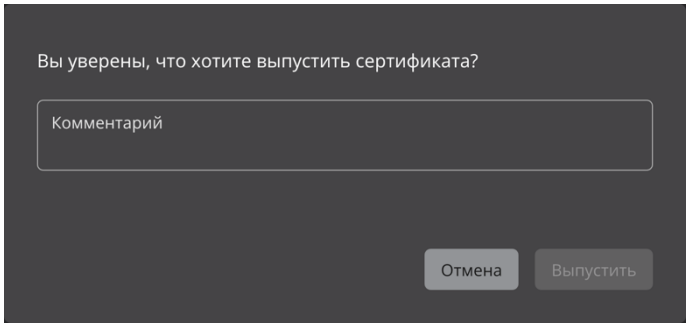


Рисунок 50 – Окно комментария к подтверждению выпуска сертификата

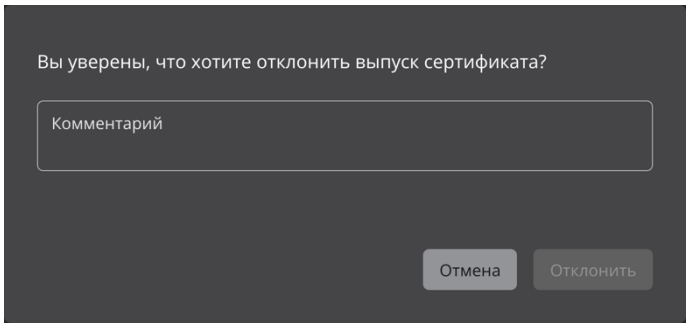


Рисунок 51 – Окно комментария к отклонению выпуска сертификата

- 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

На хосте, с которого выполняется сценарий, должно быть установлено ПО JC-WebClient. Также должен быть подключён ключевой носитель, поддерживаемый ПО JC-WebClient. Статус заявки, участвующей в сценарии, должен быть «Ожидает импорта на КН».

Для импорта сертификата на ключевой носитель выполните следующие шаги:

- На главном экране раздела «Заявки» найдите заявку, сертификат которой необходимо импортировать на КН. При этом заявка должна находится в статусе «Ожидает импорта на КН».

Далее в строке заявки нажмите на кнопку <Операции> и в контекстном меню (см. Рисунок 23) выберите действие <Импортировать на КН>. Также контекстное меню (см. Рисунок 23) можно открыть из карточки заявки, нажав на кнопку .

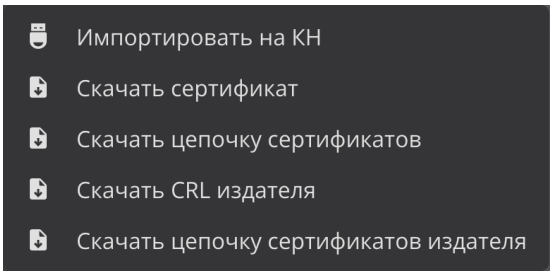


Рисунок 52 – Меню действий для заявки. Вид для администратора. Выполненная заявка со сценарием «На основании запроса (PKCS#10)»

- При отсутствии установленного ПО JC-WebClient на хосте, с которого выполняется сценарий, отобразится окно с сообщением об ошибке (см. Рисунок 53).

В данном случае необходимо установить на хост ПО JC-WebClient и повторить процесс создания заявки.

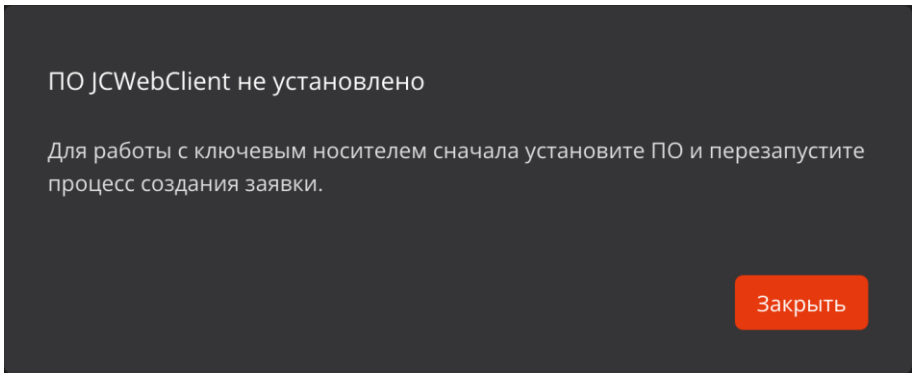


Рисунок 53 – Ошибка «ПО JS-WebClient не установлено»

- При наличии установленного ПО JC-WebClient и отсутствии подключённого ключевого носителя отобразится окно с сообщением об ошибке (см. Рисунок 54).

  В данном случае необходимо подключить ключевой носитель, поддерживаемый ПО JC-WebClient, и повторить процесс создания заявки.

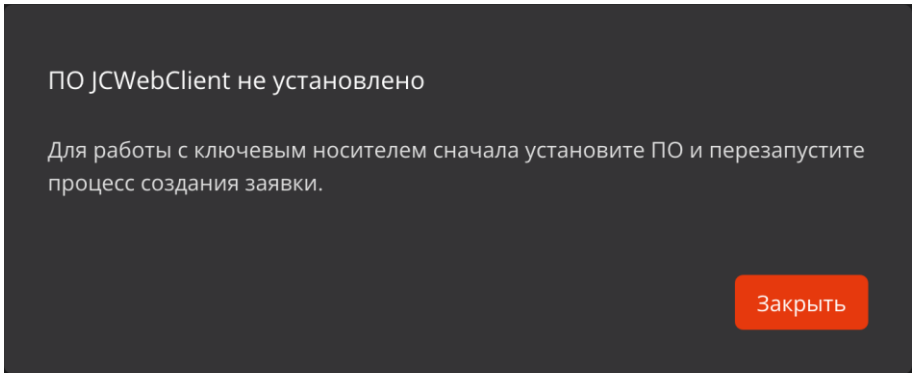


Рисунок 54 – Ошибка «Нет доступных устройств»

- При наличии установленного ПО JC-WebClient и подключённого ключевого носителя, поддерживаемого ПО JC-WebClient, отобразится окно «Импорт сертификата на ключевой носитель».

  В появившемся окне выберите ключевой носитель и введите PIN-код от него (см. Рисунок 55).

  Для продолжения нажмите на кнопку <Импортировать>.

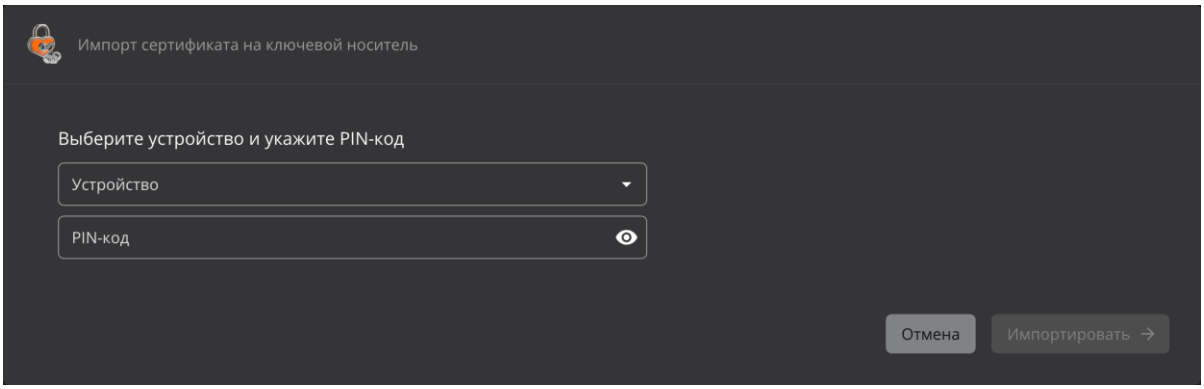


Рисунок 55 – Импорт сертификата на ключевой носитель

- После нажатия на кнопку «Импортировать» возникающие ошибки отображаются во всплывающем сообщении. Могут возникать следующие ошибки:

  – «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата» – возникает при попытке импорта сертификата на КН, который не содержит закрытый ключ, соответствующий открытому ключу импортируемого сертификата;

– Ошибки, получаемые от ПО JC-WebClient, за исключением ошибок при создании контейнера на КН[88].

При отсутствии ошибок импорта сертификата в окне «Импорт сертификата на ключевой носитель» будет отображено сообщение об успешном импорте сертификата на ключевой носитель, а также информационный элемент, содержащий имя издателя, имя субъекта и срок действия импортированного сертификата (см. Рисунок 41) . При этом заявка, сертификат которой был успешно импортирован на КН, перейдёт в статус «Выполнена».

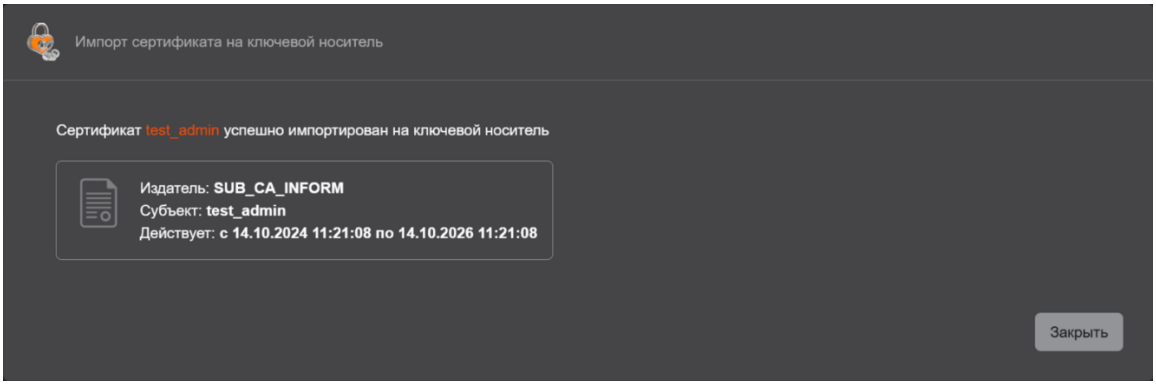


Рисунок 56 – Импорт сертификата на ключевой носитель

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 Центре сертификации Aladdin eCA, к которому подключен Центр регистрации Aladdin eRA. 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 57);

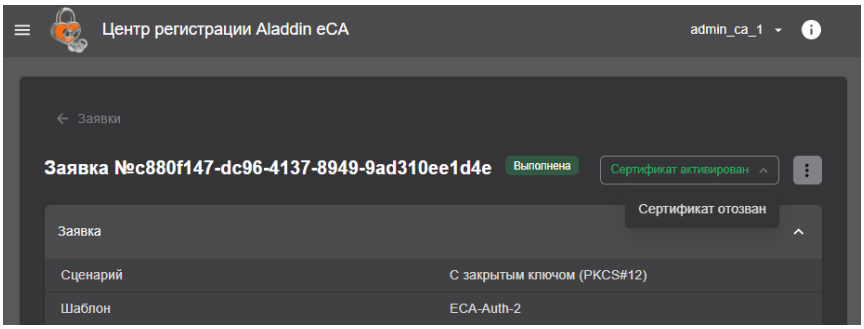


Рисунок 57 – Отзыв сертификата

[88] ПО Центра регистрации Aladdin eRA последовательно проходит по списку ключевых пар на используемом КН. Все неуспешные попытки создания контейнера завершаются ошибкой, возвращаемой ПО JC-WebClient. При этом ПО Центра регистрации Aladdin eRA не отображает ошибку для каждой ключевой пары, генерируемую ПО JC-WebClient, а выводит общую ошибку «Ключевой носитель не содержит закрытый ключ, соответствующий открытому ключу из сертификата», если КН не содержит подходящую ключевую пару.

- в открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в соответствующем поле и нажмите кнопку <Отозвать> (см. Рисунок 58);

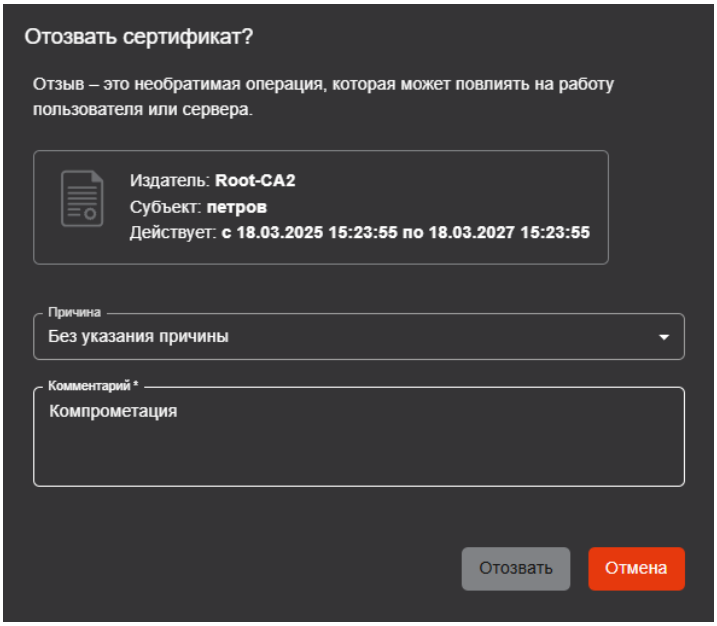


Рисунок 58 – Указание причины отзыва сертификата

- В результате сертификат будет отозван.

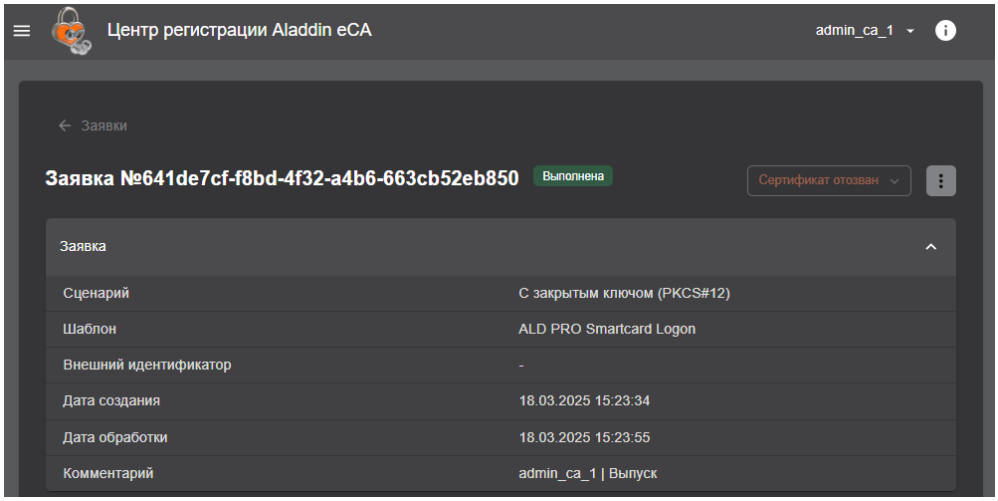


Рисунок 59 – Сертификат отозван

7.5 Раздел «Учётные записи»

Раздел «Учётные записи» предоставляет информацию об учётных записях Центра регистрации Aladdin eRA, а также обеспечивает возможность блокировать и активировать учётные записи.

Переход в раздел «Учётные записи» (см. Рисунок 60) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 10).

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

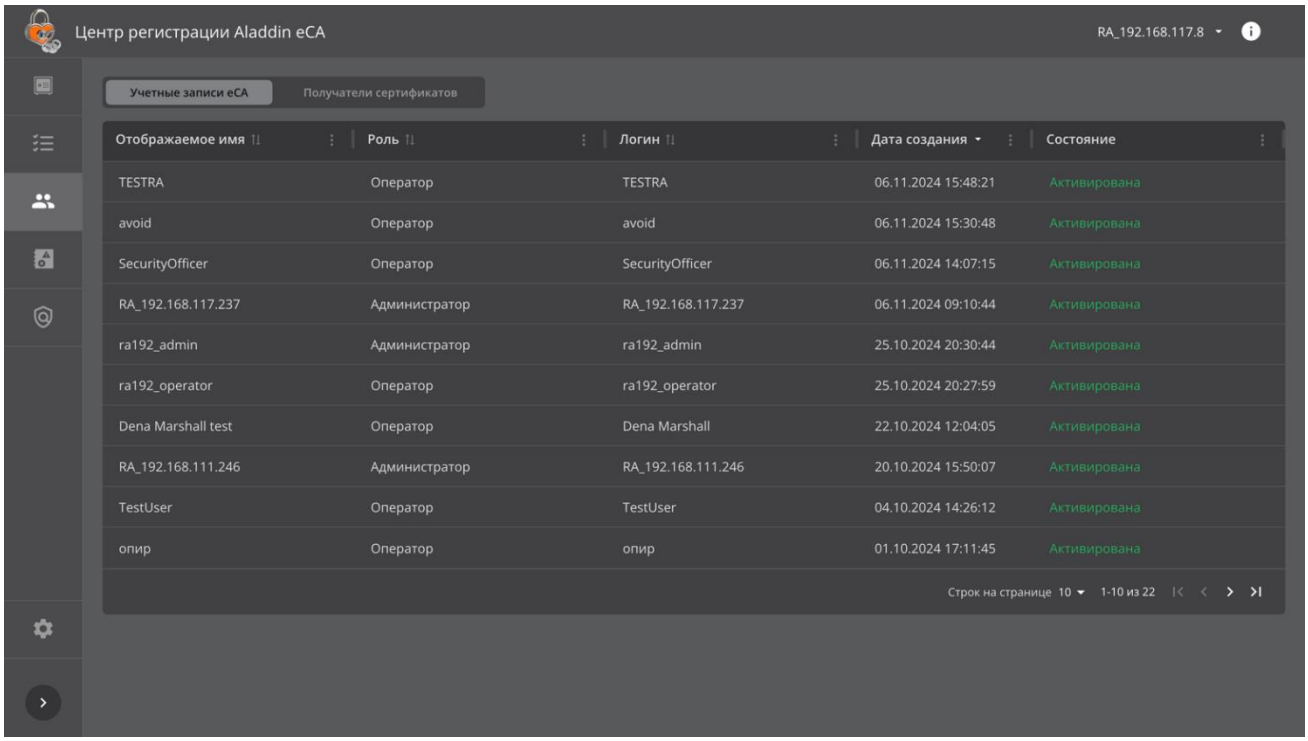


Рисунок 60 – Экран раздела «Учётные записи». Вкладка «Учётные записи eCA»

На экране раздела «Учётные записи» отображаются следующие вкладки:

- Учётные записи Центра сертификации 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 Центр регистрации Aladdin eRA (см. Рисунок 60):

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

Действия над учётными записями Центра сертификации Aladdin eCA производятся в Центре сертификации Aladdin eCA (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 61):

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

На вкладке «Получатели сертификатов» доступны следующие действия:

- блокировка активированных учётных записей;
- активация заблокированных учётных записей.

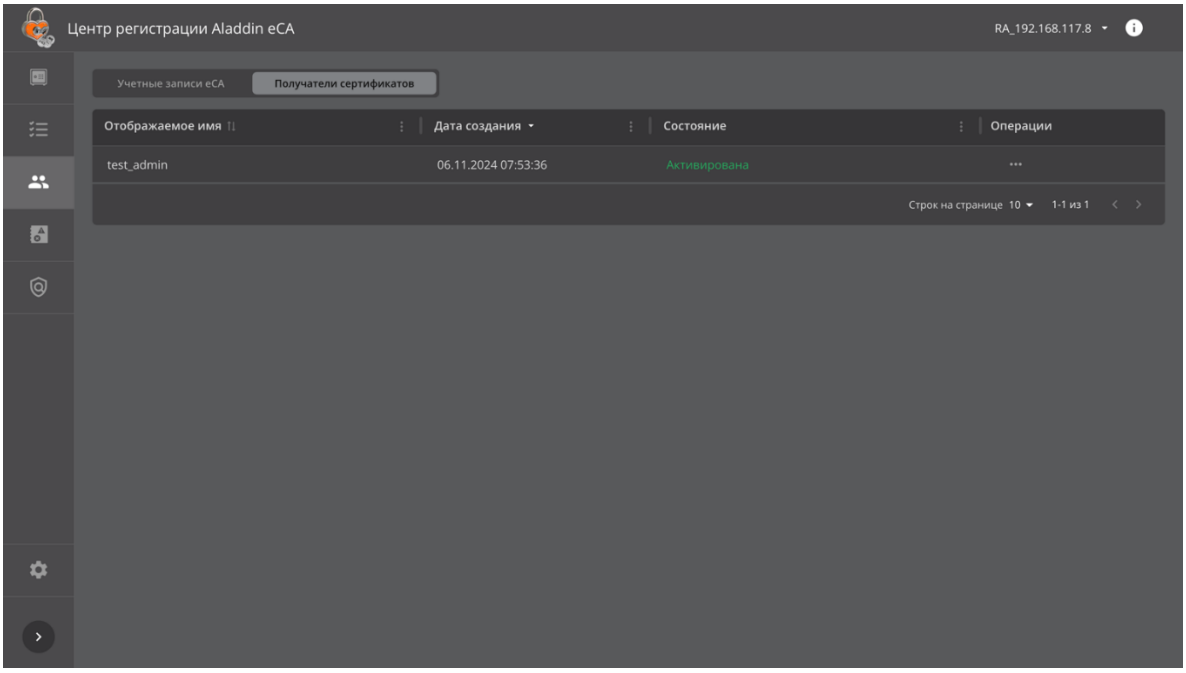


Рисунок 61 – Экран раздела «Учётные записи». Вкладка «Получатели сертификатов»

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 62).

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».

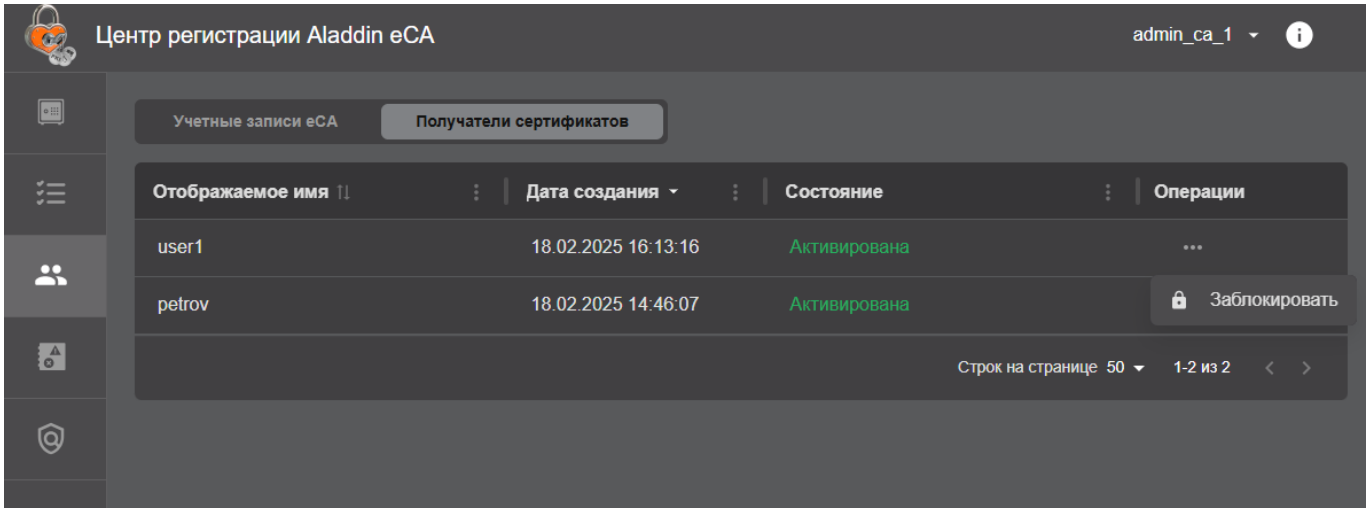


Рисунок 62 – Экран раздела «Учётные записи». Блокировка доменной учётной записи

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 63).

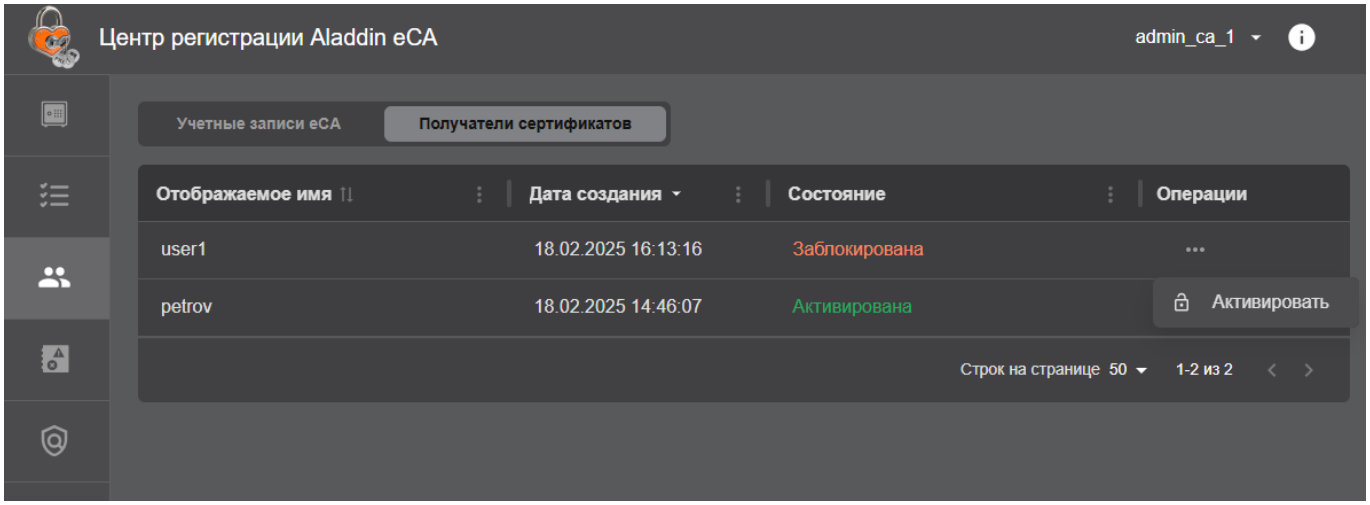


Рисунок 63 – Экран раздела «Учётные записи». Активация доменной учётной записи

7.6 Раздел «Журнал событий»

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

Переход в раздел «Журнал событий» (см. Рисунок 64) осуществляется через боковое меню, расположенное слева на главном экране (см. Рисунок 10).

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 Центр регистрации Aladdin eRA.

Центр регистрации оснащён функцией сбора диагностической информации, которая получает и аккумулирует записи о событиях для последующего анализа в базе данных (конфигурация базы данных указана в файле `/opt/aecaRa/scripts/config.sh`).

В процессе работы Центра регистрации системные службы и компоненты приложения записывают все производимые действия. Произошедшие события записываются в файлы регистрации событий с расширением .log, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaRa/dist/logs/'имя сервиса'`. Файлы технических логов, создаваемые в подкаталогах `/opt/aecaRa/dist/logs/`, имеют права доступа 640 (rw-r-----). Срок хранения файлов регистрации событий составляет 10 дней с ограничением размера в 50 Мб.

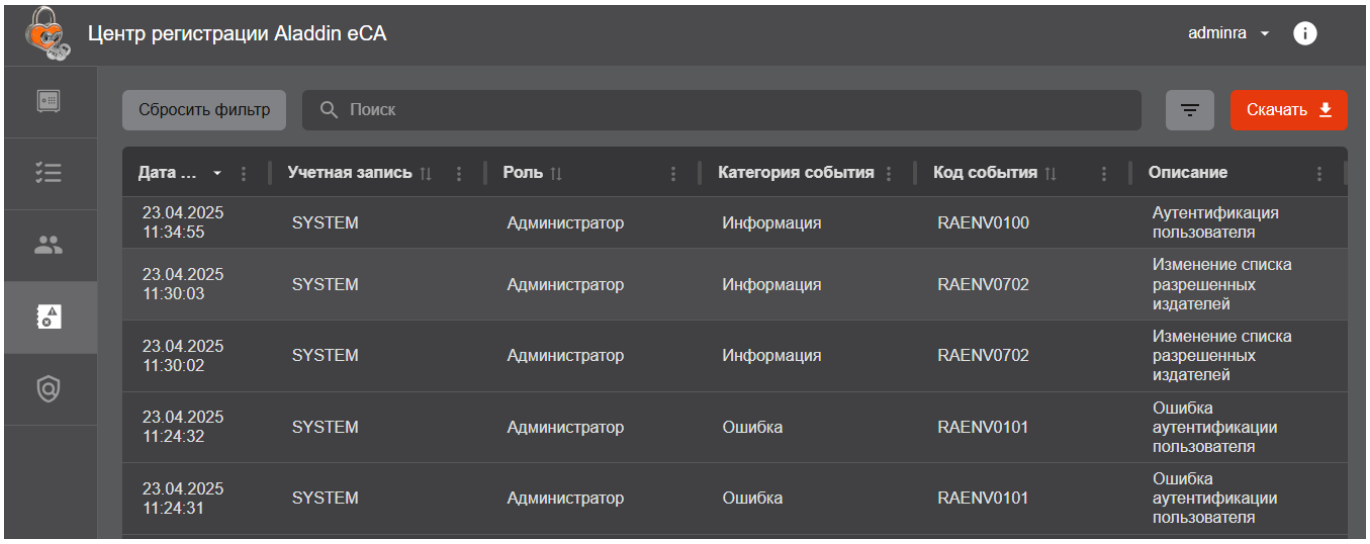


Рисунок 64 – Экран раздела «Журнал событий»

В разделе «Журнал событий» в табличной форме отображена следующая информация о событиях[89]:

- дата регистрации события;
- учётная запись – имя учётной записи, действия которой повлекли событие;
- роль (администратор, оператор);
- категория события (информация или ошибка);
- код события;
- описание.

В разделе «Журнал событий» доступны следующие действия:

- просмотр подробного описания события в его карточке;
- копирование события в буфер обмена;
- экспорт журнала событий в формате .csv файла (полный или с применением фильтров);
- полный или выборочный просмотр журнала событий.

7.6.1 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 65), в котором возможно (в зависимости от применённых ранее действий – фильтр, сортировка, изменение ширины, скрытие колонки):

- очистить сортировку, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
- сортировать по возрастанию/убыванию значений в колонке;
- очистить фильтр, если ранее было применено данное действие, и вернуться к отображению всех событий в колонке;
- отфильтровать, отобразив поле для выбора критерия фильтрации;
- сбросить размер колонок, сбросив ширину колонок к значению «по умолчанию»;

[89] Возможные сообщения журнала событий приведены в Приложении 6.

- скрыть колонку из отображаемых на экране;
- показать все колонки, отобразив на экране ранее скрытые колонки.

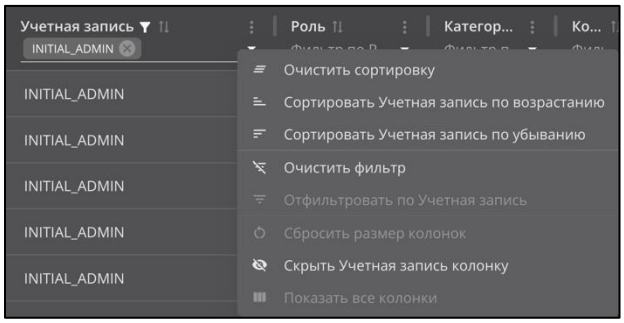


Рисунок 65 – Кнопка <Действия в колонке>

Для сброса применённых фильтров нажмите кнопку <Сбросить фильтр> 

. В результате в экранной таблице раздела «Журнал событий» будут отображены записи о всех зарегистрированных событиях.

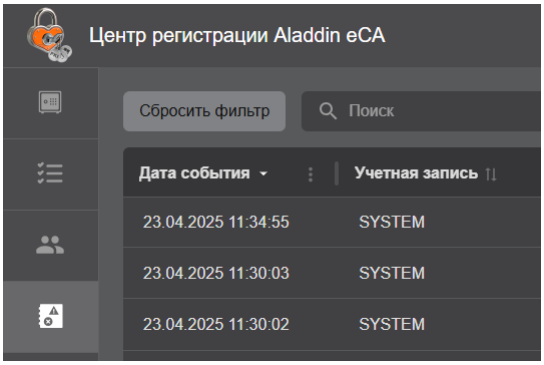


Рисунок 66 – Кнопка <Сбросить фильтр>

7.6.2 Фильтрация событий

Для выборочного просмотра событий в разделе «Журнал событий» возможно применение фильтров. Для отображения параметров фильтрации для всех колонок таблицы нажмите кнопку  <Фильтр>, заголовки колонок экранной таблицы будут дополнены полями фильтров для каждой колонки (см. Рисунок 67):

- Дата события. Выберите за какой период отразить события на экране, введите дату с помощью клавиатуры или выберите в развернувшемся календаре.
- Учётная запись. Выберите учётные записи, чьи действия повлекли события.
- Роль. Выберите роли пользователей, чьи действия повлекли события.
- Категории событий. Выберите категории событий для отображения (ошибка, информация).
- Коды событий. Выберите коды событий для отображения.

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

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

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

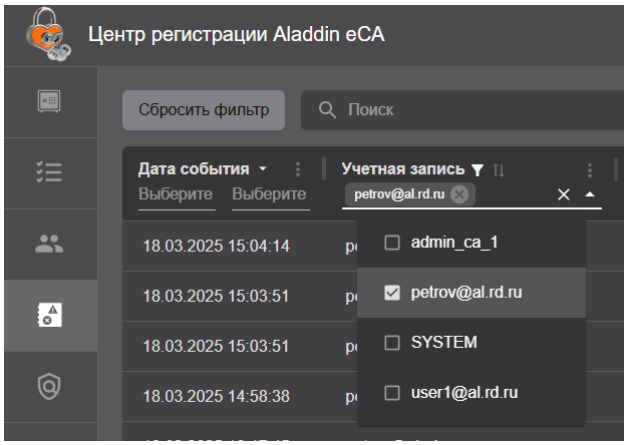


Рисунок 67 – Поля фильтров заголовков экранной таблицы

Для очистки применённых фильтров для каждого заголовка колонки нажмите кнопку  <Действия в колонке> и в раскрывшемся окне выберите пункт «Очистить фильтр» (см. Рисунок 65).

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

7.6.3 Сортировка событий

Средства сортировки событий в разделе «Журнал событий» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 68):

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

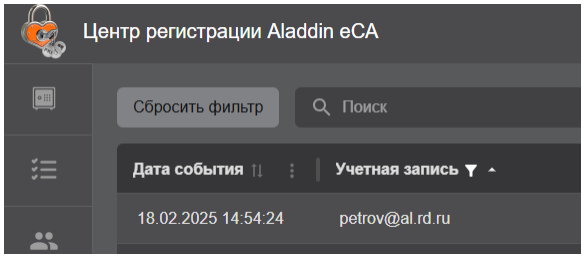


Рисунок 68 – Поля сортировки содержимого экрана раздела «Журнал событий»

Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки> (см. Рисунок 65).

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» (см. Рисунок 65);
- или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

7.6.4 Поиск событий

Строка поиска (см. Рисунок 69) предназначена для поиска записей событий в журнале по содержимому поля «Описание» и полям подраздела «Подробности» карточки события. Поиск запускается автоматически при вводе искомого значения в строку поиска, результат поиска будет отражён на экранной таблице.

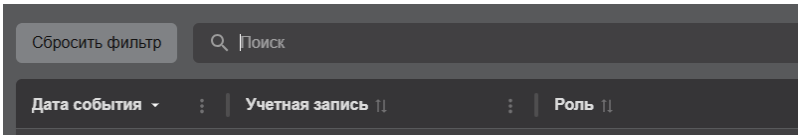


Рисунок 69 – Поисковая строка в разделе «Журнал событий»

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

7.6.5 Карточка события

- Просмотр подробного описания события возможен посредством окна «Свойства события» (карточка события);
- Переход к окну «Свойства события» (см. Рисунок 70) осуществляется при нажатии на строку события в разделе «Журнал событий» (см. Рисунок 64).

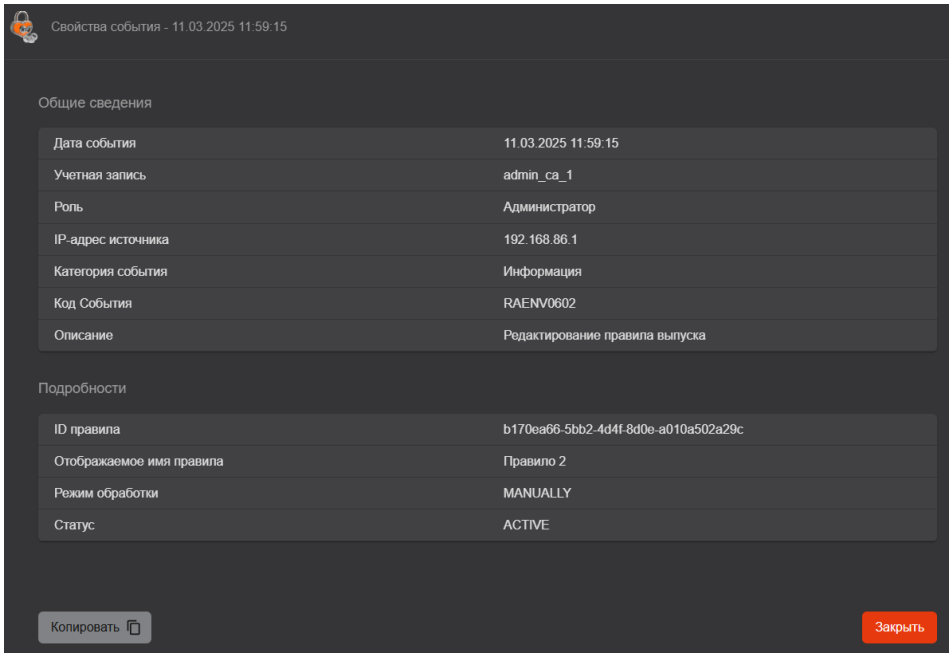


Рисунок 70 – Окно «Свойство события»

- Карточка события включает в себя следующую информацию:
  - подраздел «Общие сведения», содержащий следующие поля:
    - «Дата события» – содержит дату и время события;
    - «Учетная запись» – содержит логин учетной записи инициатора события;
    - «Роль» – содержит роль учетной записи инициатора события;
    - «IP-адрес источника» - IP-адрес узла, с которого была выполнена аутентификация пользователя (инициатора события);
    - «Категория события» – содержит категорию события (Информация или Ошибка);
    - «Код события», содержащее код события (список кодов событий см. в Приложении 6);
    - «Описание».

- подраздел «Подробности», содержащий поля расширенного описания события. Состав полей см. в Приложении 6.

- Доступные действия в карточке события:
  - копирование информации о событии в буфер обмена (см. 7.6.6);
  - закрытие окна с помощью нажатия на кнопку <Закрыть>.

7.6.6 Копирование события в буфер обмена

Для копирования события в буфер обмена выполните следующие шаги:

- откройте карточку события (см. Рисунок 70);
- в карточке события нажмите на кнопку <Копировать>. При этом происходит копирование содержимого полей карточки события в буфер обмена в формате «Название поля: значение в поле»;

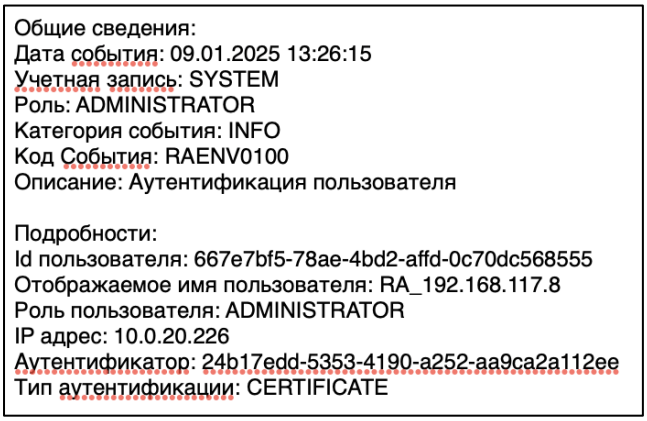
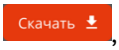


Рисунок 71 – Пример копирования события в текстовый файл

7.6.7 Экспорт журнала событий

- В разделе «Журнал событий» при необходимости воспользуйтесь фильтрами и строкой поиска для задания критериев отбора экспортируемых событий.

  Если их не задать, то будет произведено скачивание всех записей журнала событий.

- Нажмите на кнопку <Скачать> 

, расположенную на верхней панели экрана раздела «Журнал событий».

- После этого будет произведена подготовка файла с записями журнала событий, в соответствии с критериями фильтров и поиска. Кнопка меняет своё состояние в зависимости от статуса процесса скачивания:
  - скачать 

– система готова к новому формированию и скачиванию журнала событий;
  - скачивание выполняется 

– начинается подготовка файла, содержащего записи журнала событий. Нажатие на кнопку в текущем состоянии не повлечёт никаких действий;
  - скачать (готово) 

– файл журнала событий готов для скачивания. Нажатие на кнопку запускает скачивание файла журнала событий по указанному пути (в соответствии с настройками браузера). После завершения скачивания файла, статус кнопки возвращается в состояние «Скачать».

- Выгруженный файл имеет формат .csv, содержимое файла представлено в кодировке UTF-8 с разделителем полей “;” и доступно для открытия любым текстовым редактором (рекомендуемая программа просмотра записей журнала событий – MS Excel).

7.6.8 Архивирование и очистка журнала событий

Центр регистрации обеспечивает настраиваемое архивирование событий аудита с одновременной очисткой журнала событий в части заархивированных событий.

Для настройки параметров архивации и очистки отредактируйте в конфигурационном файле `/opt/aecaRa/scripts/config.sh` следующие переменные окружения:

- `archive_enabled` – флаг включения режима архивации (по умолчанию архивация включена – значение «true», для выключения режима установите значение «false»);
- `archive_millis_ago` – время хранения событий (по умолчанию 180 дней) в миллисекундах. Записи со сроком давности большим или равным времени хранения будут заархивированы;
- `archive_cron` – периодичность запуска архивации (значение указывается в формате CRON-выражения, значение по умолчанию – '0 0 0 1 * *'). По умолчанию процесс архивации будет запущен при наступлении первого числа каждого месяца;
- `archive_path` – путь расположения сформированного архива.

Архив в формате .zip, содержащий .csv файл, с именем `logs-<дата и время создания архива>.zip` будет сохранён в папке (по умолчанию) `/opt/aecaRa/dist/archive`.

7.7 Раздел «Управление»

Переход на экран раздела «Управление» (см. Рисунок 72) осуществляется по выбору раздела «Управление» бокового меню, расположенного слева на главном экране (см. Рисунок 10).

Раздел «Управление» содержит вкладки «Правила выпуска» и «SCEP».

Данный раздел доступен только для администратора.

7.7.1 Вкладка «Правила выпуска»

Вкладка «Правила выпуска» (см. Рисунок 72) раздела «Управление» обеспечивает возможности создания, изменения, удаления правил выпуска сертификатов, также управления статусами правил выпуска.

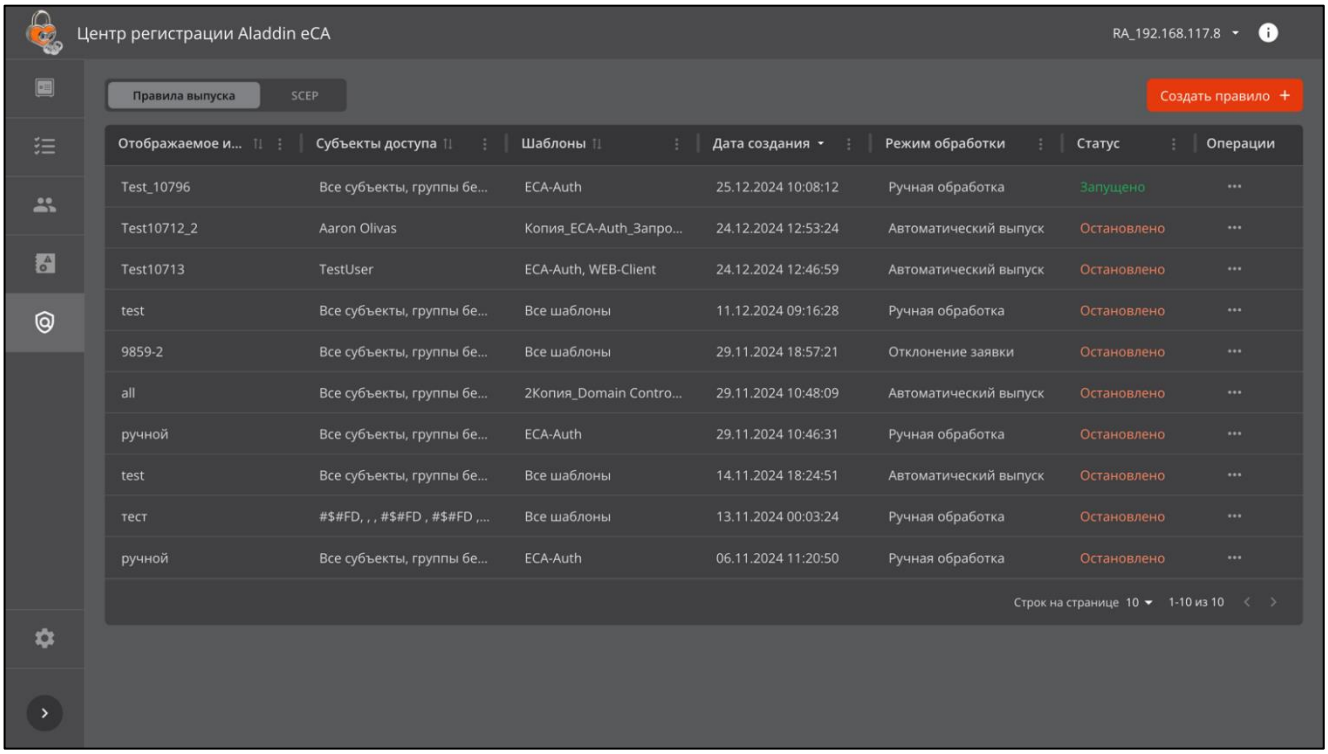


Рисунок 72 – Экран раздела «Управление». Вкладка «Правила выпуска»

Во вкладке «Правила выпуска» раздела «Управление» в табличной форме отображена следующая информация о существующих правилах выпуска (см. Таблица 13):

Таблица 13 – 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 Центра сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, 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»

Внимание! После обновления ПО до версии 2.2 правила выпуска с субъектами доступа, являющимися подразделениями, удаляются.

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 Создание правила выпуска

Для создания правила выпуска выполните следующие шаги:

- Нажмите кнопку <Создать правило +> на главном экране раздела «Управление» (см. Рисунок 72).
- В открывшемся окне укажите отображаемое имя для создаваемого правила выпуска (см. Рисунок 73).

Далее нажмите кнопку <Продолжить> для перехода к следующему шагу.

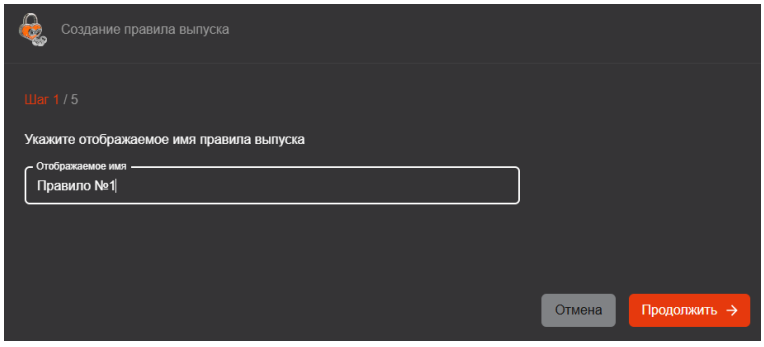


Рисунок 73 – Окно создания правила выпуска. Шаг 1. Отображаемое имя

- На втором шаге выберите субъекты доступа для создаваемого правила. Допустимые варианты выбора субъектов доступа:
  - «Все субъекты» (см. Рисунок 74). При выборе данного значения субъектами доступа будут являться все субъекты и группы безопасности ресурсных систем Центра сертификации Aladdin eCA, к которому подключён Центра регистрации Aladdin eRA, включая локальную ресурсную систему. При выборе данного значения указание отдельных субъектов или групп безопасности на данном шаге будет недоступно;

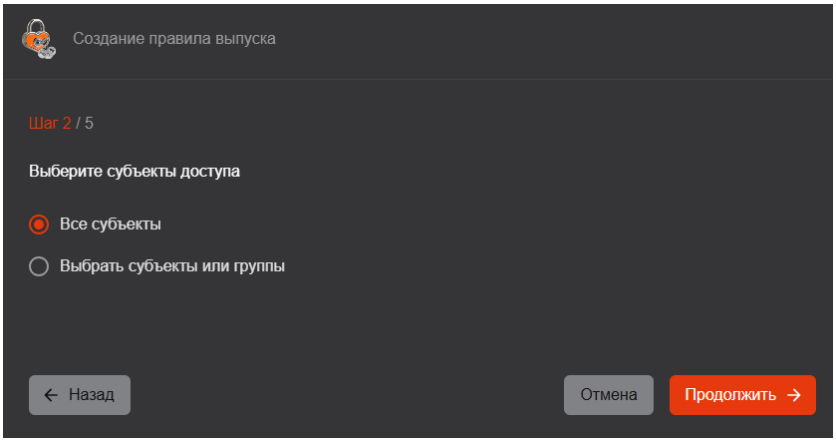


Рисунок 74 – Окно создания правила выпуска. Шаг 2. Выбор субъектов – Все субъекты

«Выбрать субъекты или группы» (см. Рисунок 75). 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.

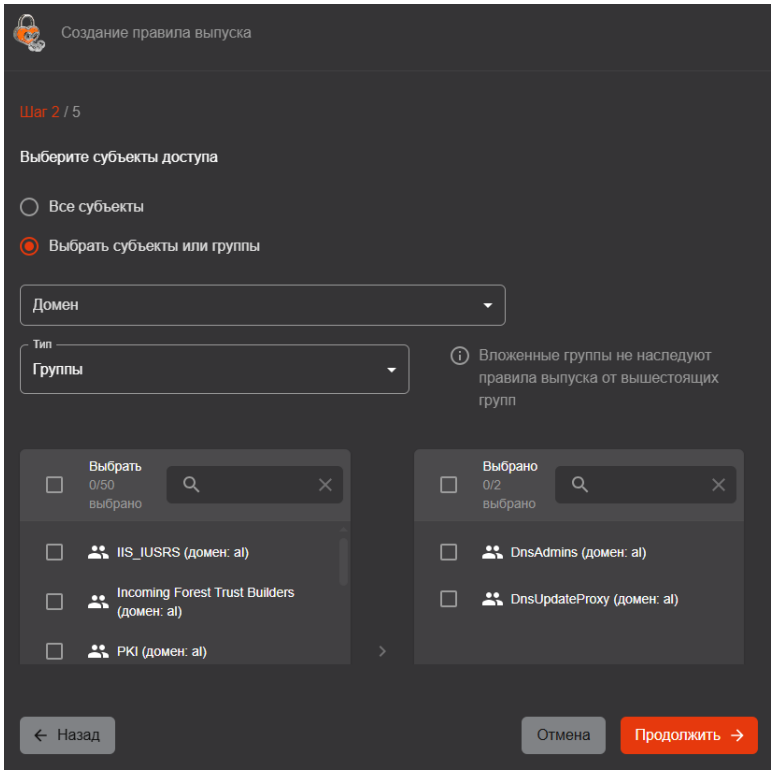


Рисунок 75 – Окно создания правила выпуска. Шаг 2. Выбор субъектов – Выбрать субъекты

- 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 76). При выборе данного значения объектами доступа будут являться все шаблоны (в том числе те, которые будут созданы в Центра сертификации Aladdin eCA позднее). При выборе данного значения указание отдельных шаблонов на данном шаге будет недоступно.

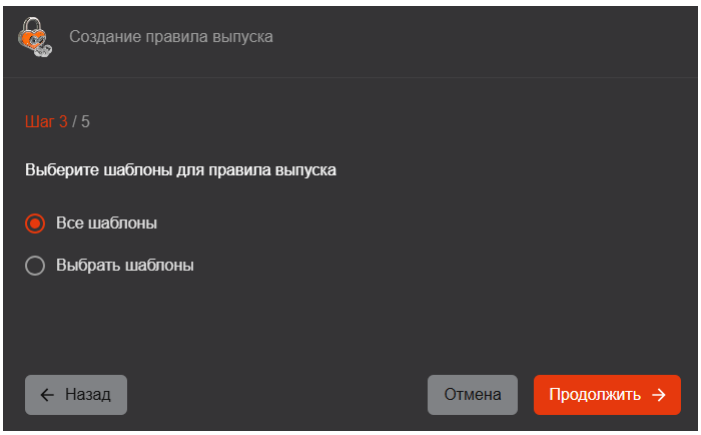


Рисунок 76 – Окно создания правила выпуска. Шаг 3. Выбор шаблонов – Все шаблоны

  - «Выбрать шаблоны» (см. Рисунок 77). 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.

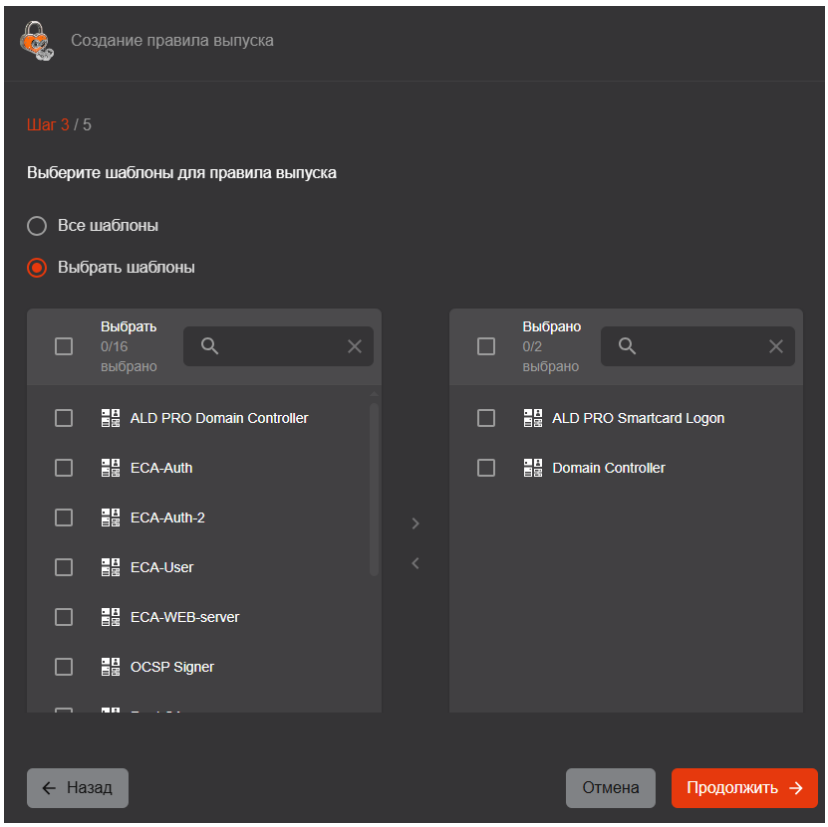


Рисунок 77 – Окно создания правила выпуска. Шаг 3. Выбор шаблонов – Выбрать шаблоны

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

- На четвёртом шаге выберите режим обработки заявок для создаваемого правила выпуска (см. Рисунок 77). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка», «Отклонение заявки».

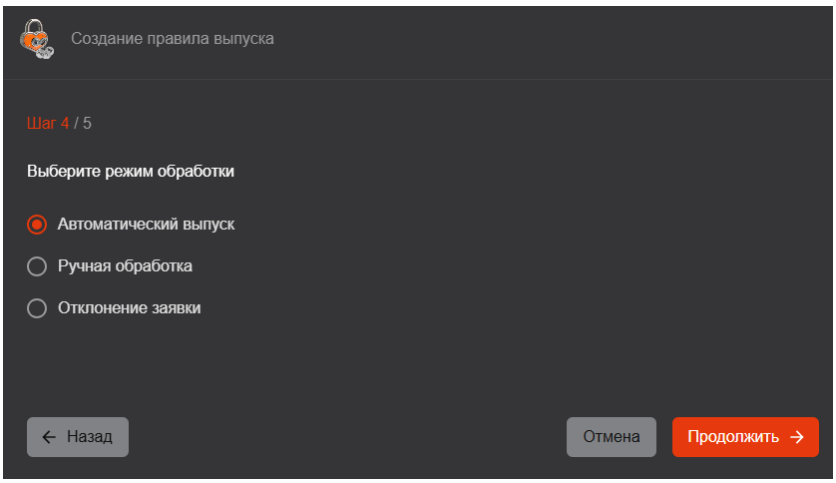


Рисунок 78 – Окно создания правила выпуска. Шаг 4. Выбор режима обработки

- 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 79).

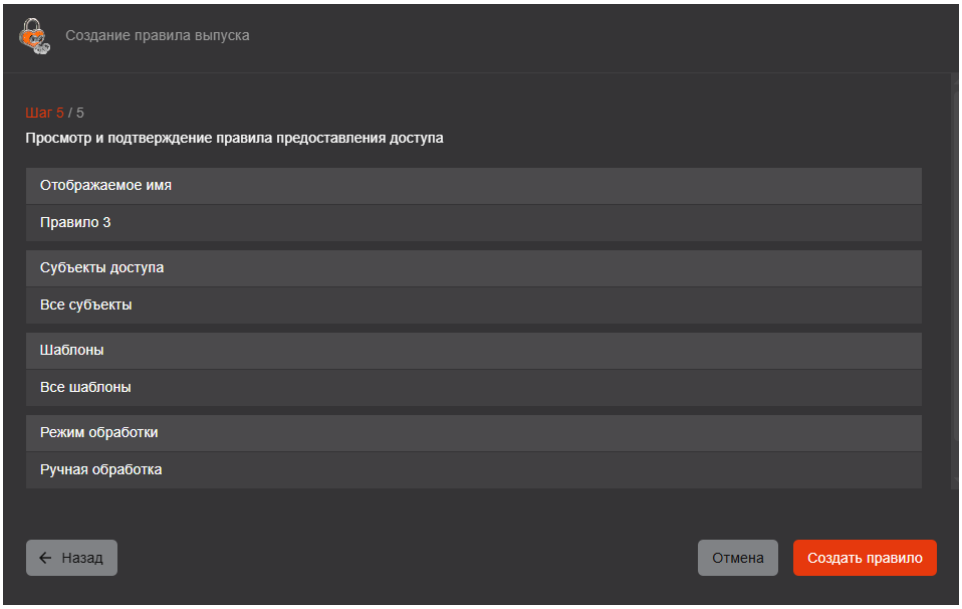


Рисунок 79 – Окно создания правила выпуска. Шаг 5. Подтверждение перед созданием

- 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».

7.7.1.2 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 80).

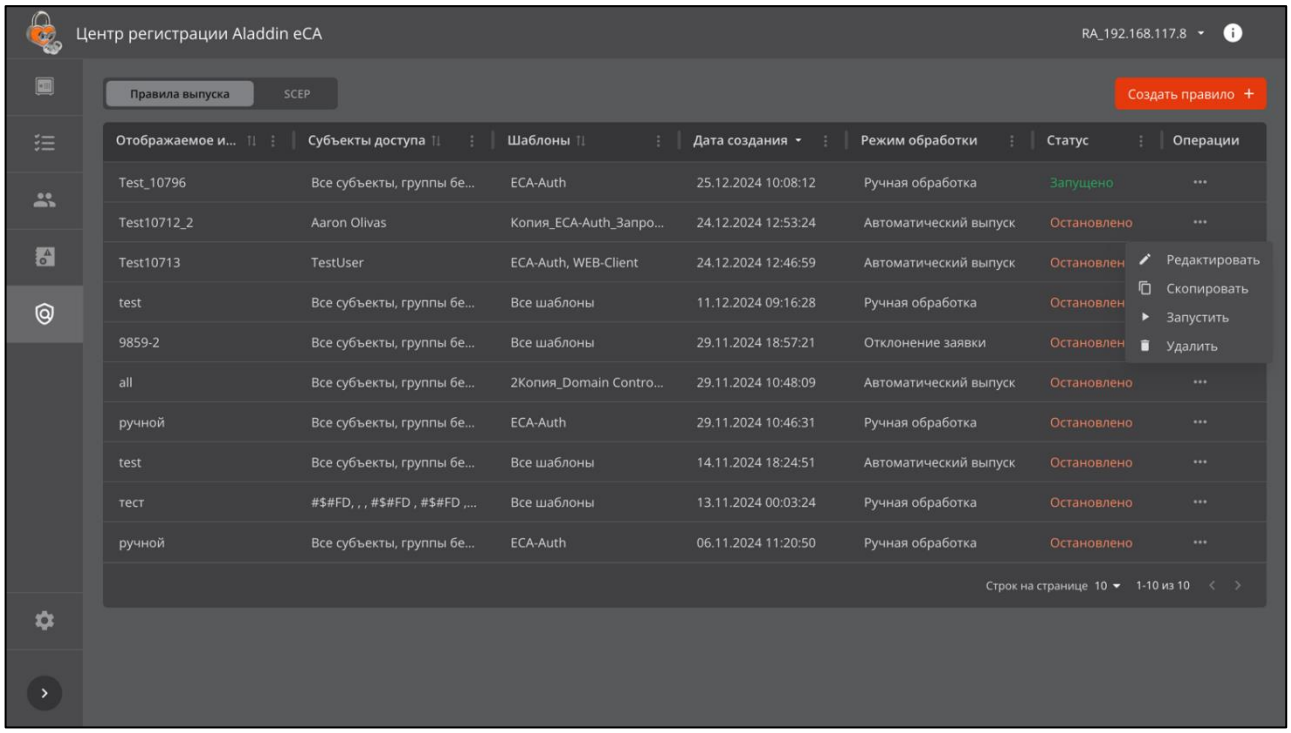


Рисунок 80 – Экран раздела «Управление». Вкладка «Правила выпуска». Редактирование правила выпуска

- В открывшемся окне «Редактирование правила выпуска» на первом шаге осуществляется редактирование отображаемого имени правила выпуска (см. Рисунок 81).

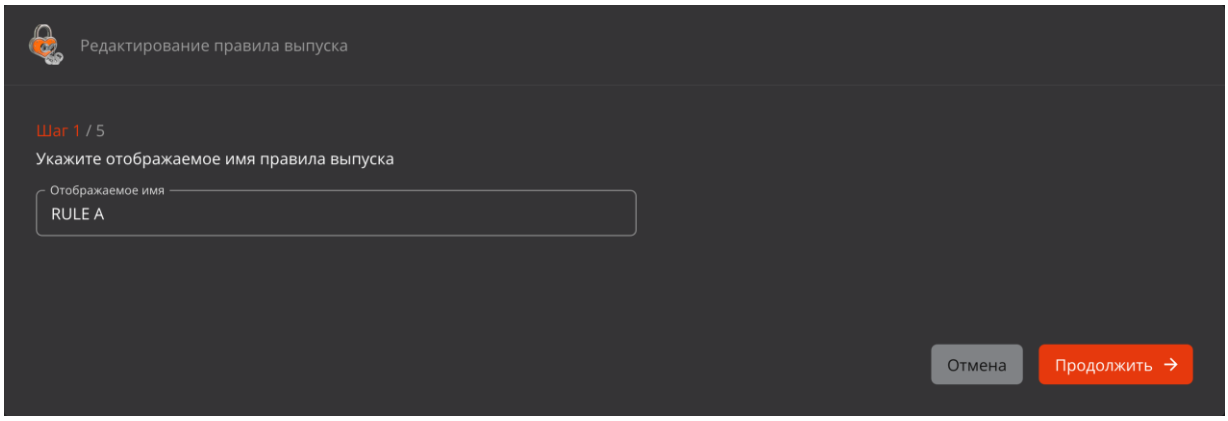


Рисунок 81 – Окно редактирования правила выпуска. Шаг 1. Отображаемое имя

- 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 82 и Рисунок 83). Редактирование субъектов доступа для правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.1). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

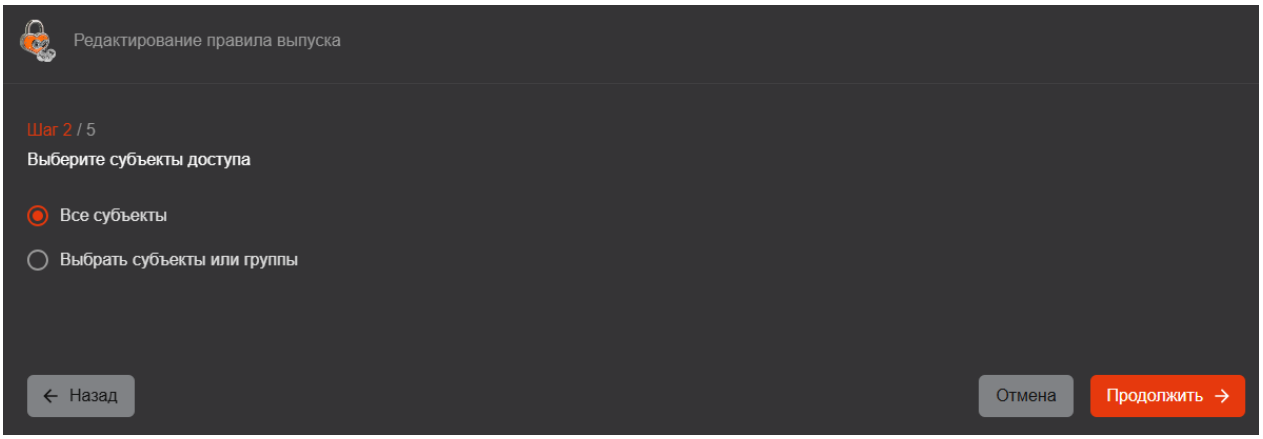


Рисунок 82 – Окно редактирования правила выпуска. Шаг 2. Выбор субъектов – Все субъекты

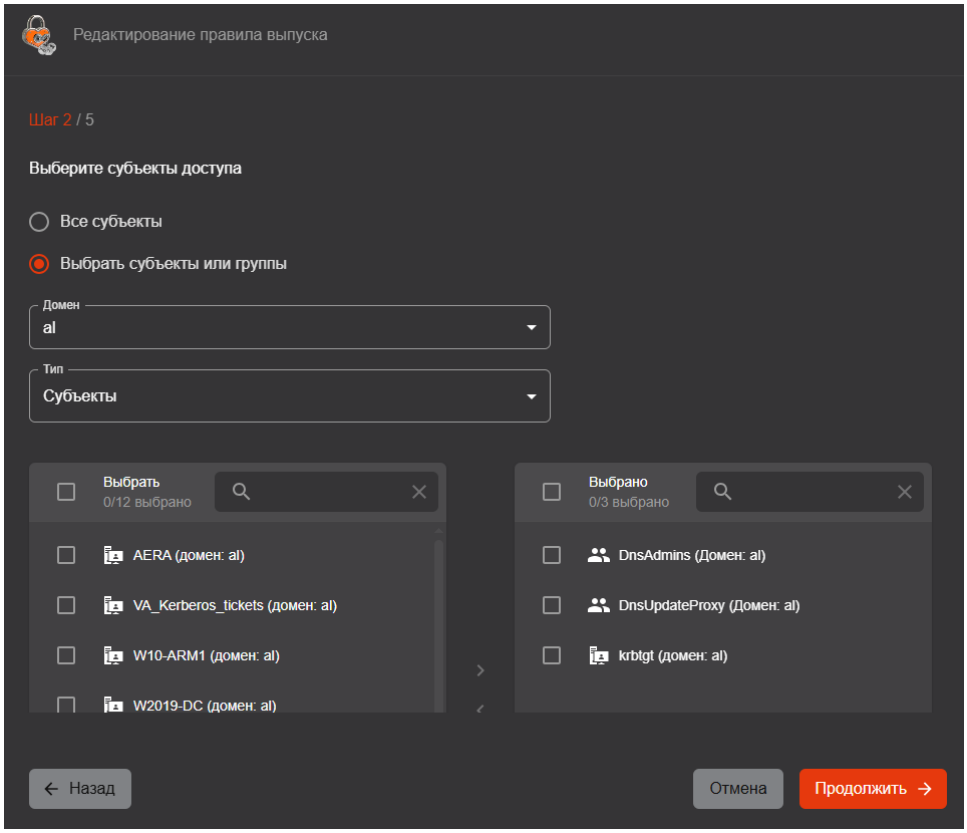


Рисунок 83 – Окно редактирования правила выпуска. Шаг 2. Выбор субъектов – Выбрать субъекты

- На шаге 3 окна «Редактирование правила выпуска» осуществляется редактирование шаблонов для правила выпуска (см Рисунок 84 и Рисунок 86). Редактирование перечня шаблонов правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.1). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

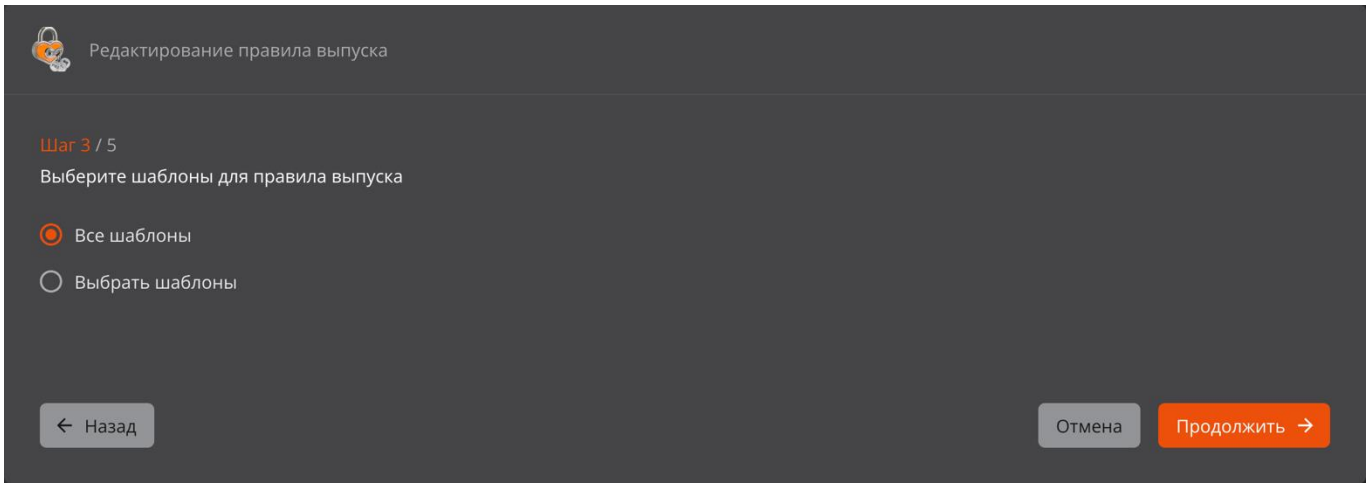


Рисунок 84 – Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов – Все шаблоны

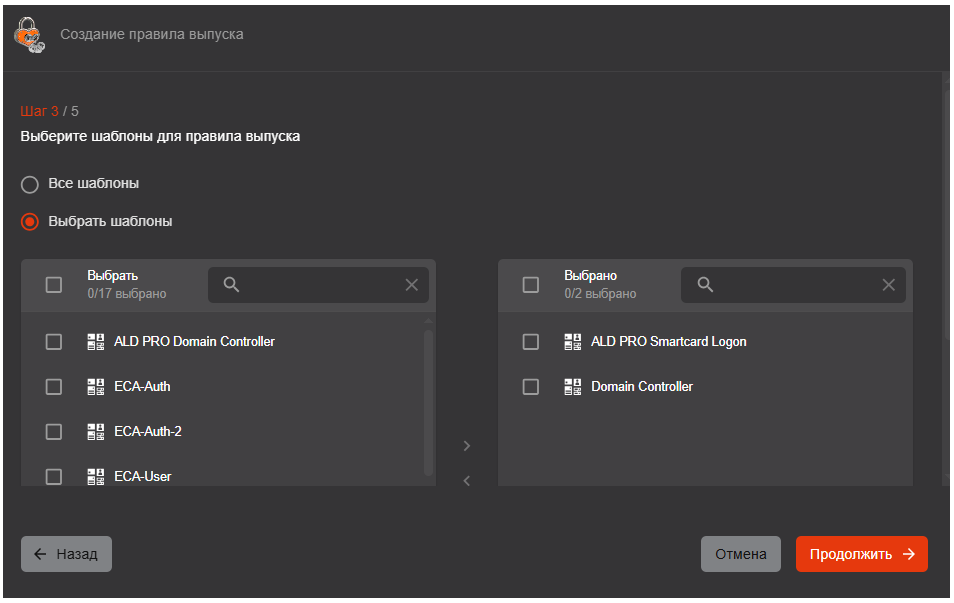


Рисунок 85 – Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов – Выбрать шаблоны

- На шаге 4 окна «Редактирование правила выпуска» осуществляется редактирование режима обработки заявок для правила выпуска (см. Рисунок 86). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка» и «Отклонение заявки».

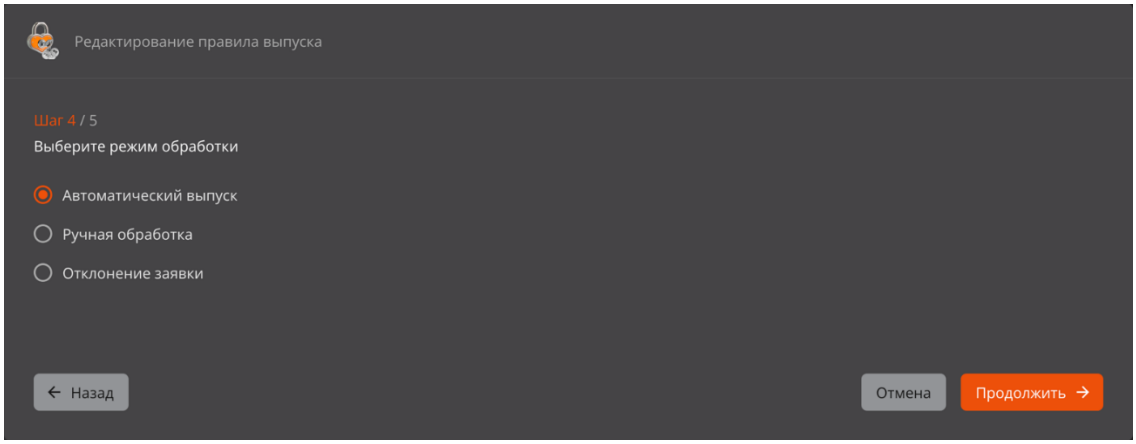


Рисунок 86 – Окно редактирования правила выпуска. Шаг 4. Выбор режима обработки

- 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 87).

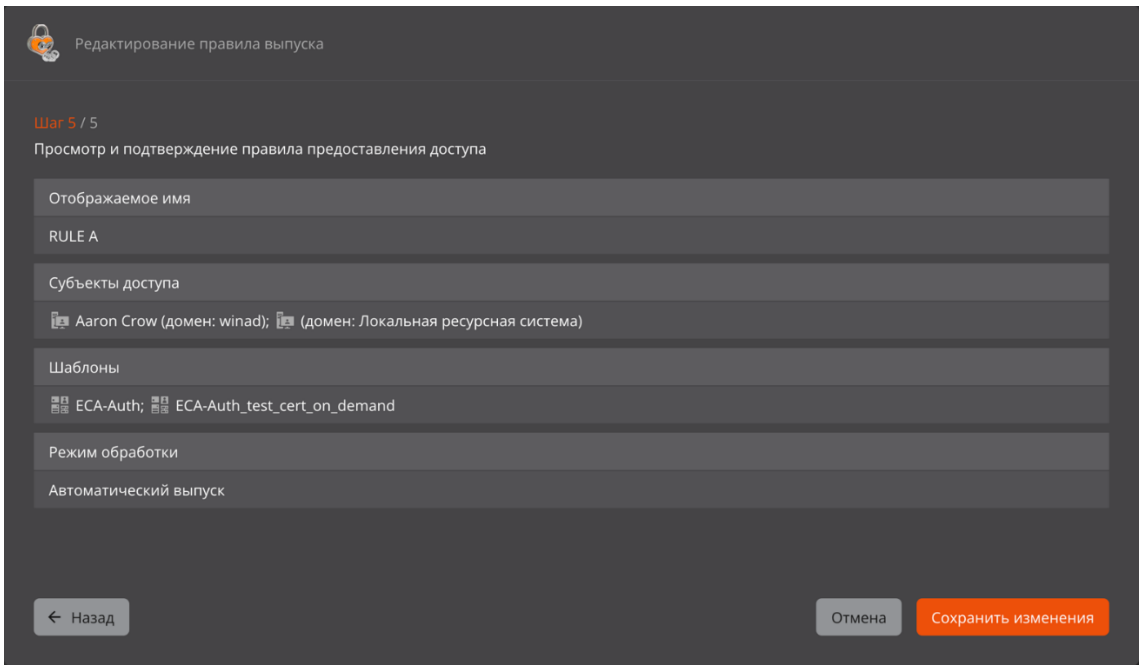


Рисунок 87 – Окно редактирования правила выпуска. Шаг 5. Подтверждение

- После нажатия на кнопку «Сохранить изменения» отредактированное правило выпуска будет обновлено.

7.7.1.3 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 88).

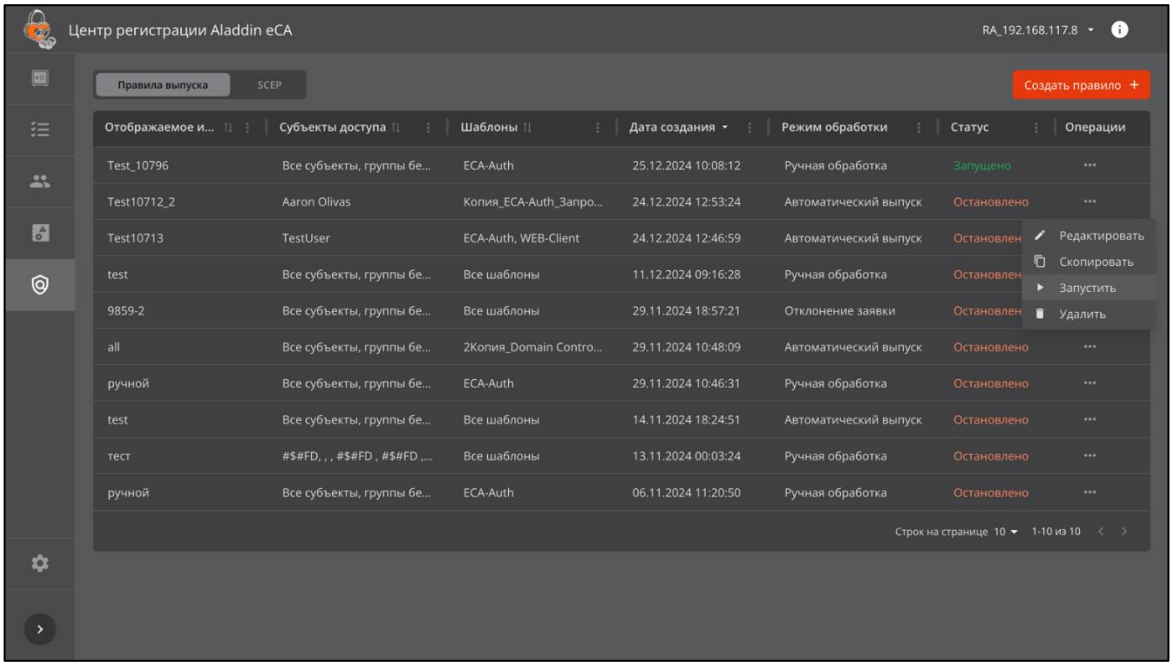


Рисунок 88 – Экран раздела «Управление». Вкладка «Правила выпуска». Запуск правила выпуска

- В появившемся окне подтверждения операции запуска (см. Рисунок 89) нажмите на кнопку <Запустить>.

После нажатия на неё правило выпуска будет запущено и будет использоваться при обработке заявок.

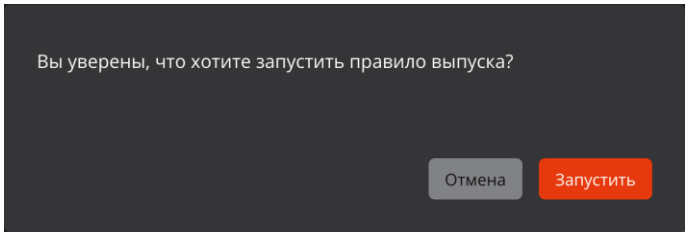


Рисунок 89 – Окно подтверждения запуска правила выпуска

7.7.1.4 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 90).

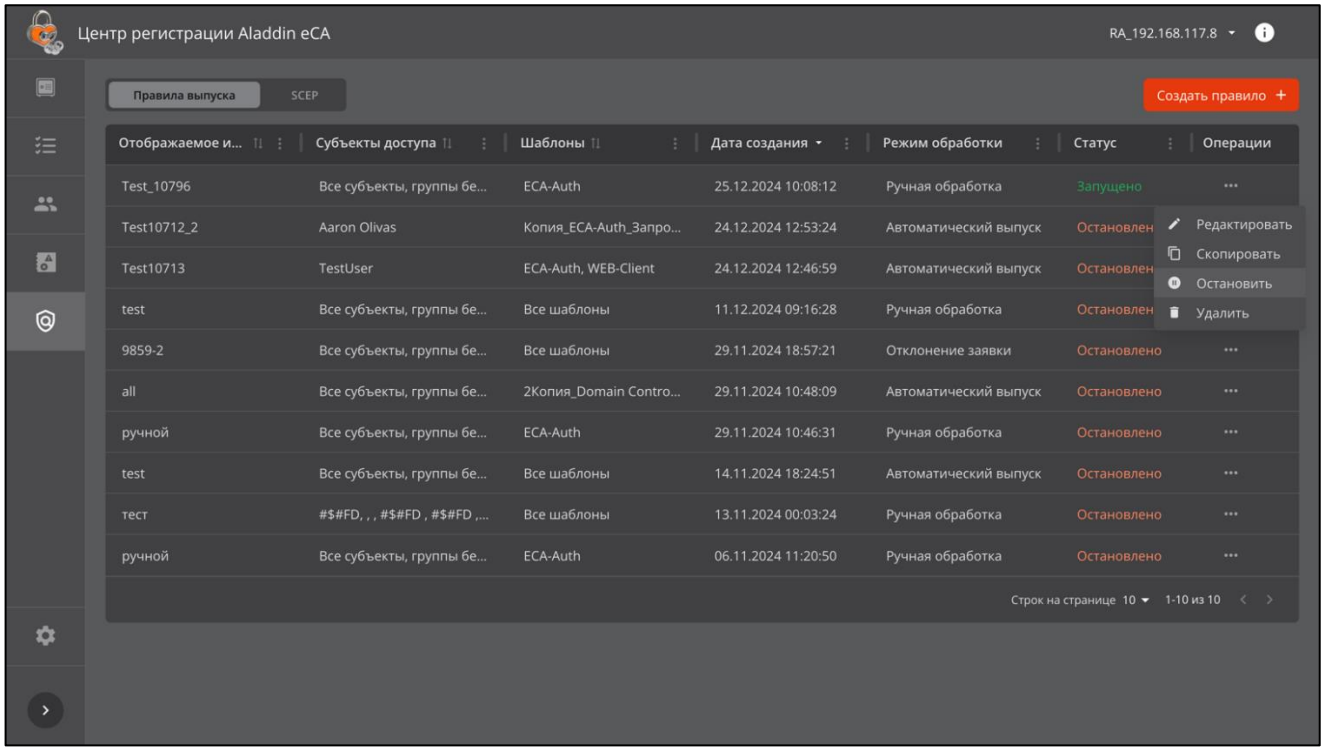


Рисунок 90 – Экран раздела «Управление». Вкладка «Правила выпуска». Остановка правила выпуска

- В появившемся окне подтверждения операции остановки (см. Рисунок 91) нажмите на кнопку <Остановить>.

После нажатия на неё правило выпуска будет остановлено и не будет использоваться при обработке заявок.

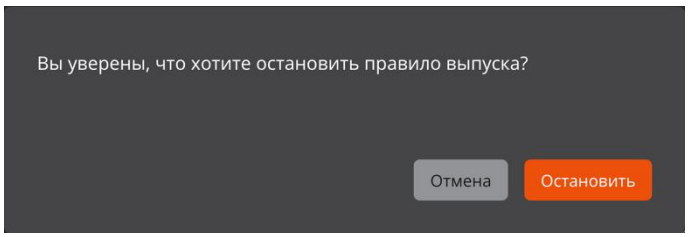


Рисунок 91 – Окно подтверждения остановки правила выпуска

7.7.1.5 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 92).

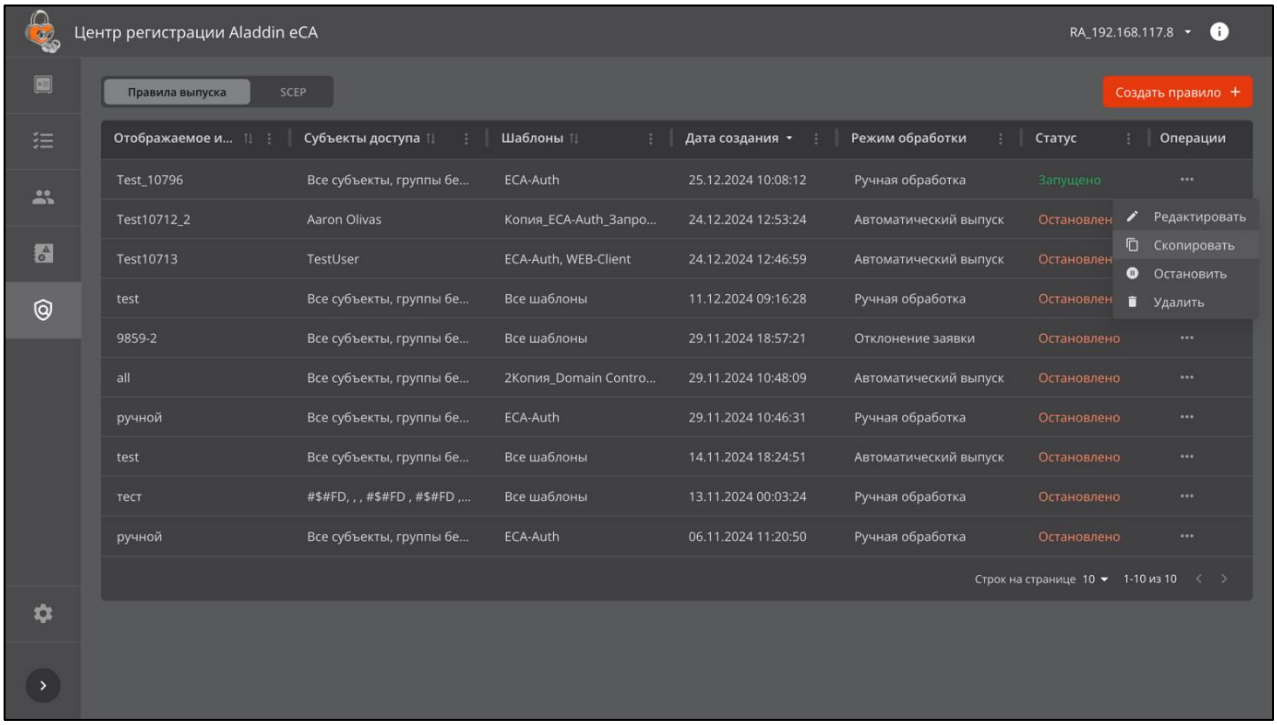


Рисунок 92 – Экран раздела «Управление». Вкладка «Правила выпуска». Копирование правила выпуска

- В появившемся окне подтверждения операции копирования (см. Рисунок 93) нажмите на кнопку <Скопировать>. После нажатия на неё правило выпуска будет скопировано, при этом созданное правило выпуска будет находится в статусе «Запущено».

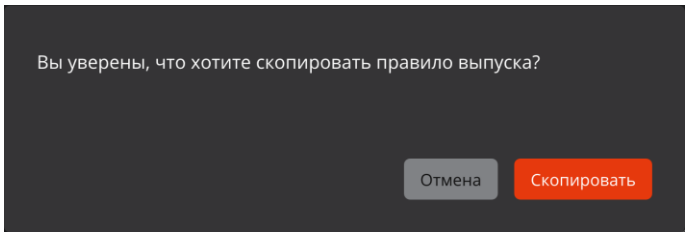


Рисунок 93 – Окно подтверждения копирования правила выпуска

7.7.1.6 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 94).

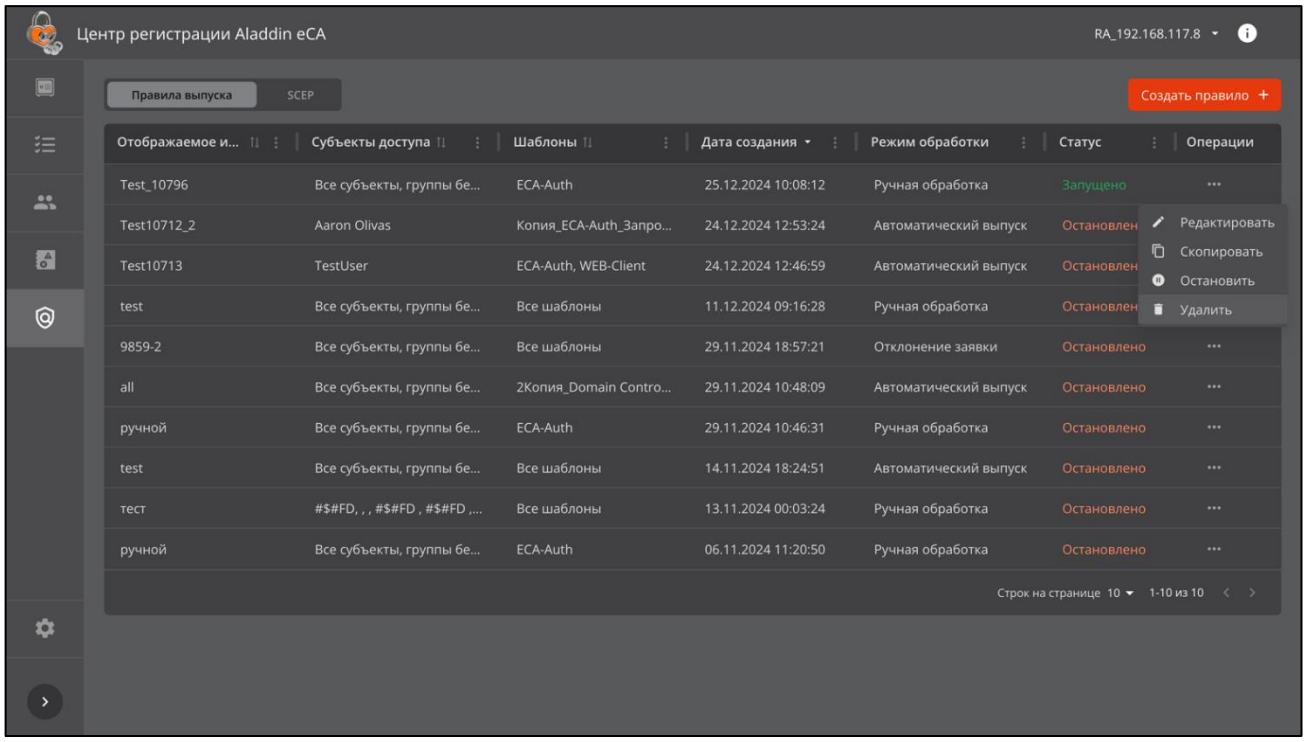


Рисунок 94 – Экран раздела «Управление». Вкладка «Правила выпуска». Удаление правила выпуска

- В появившемся окне подтверждения операции удаления (см. Рисунок 95) нажмите на кнопку <Удалить>.

После нажатия на неё правило выпуска будет удалено.

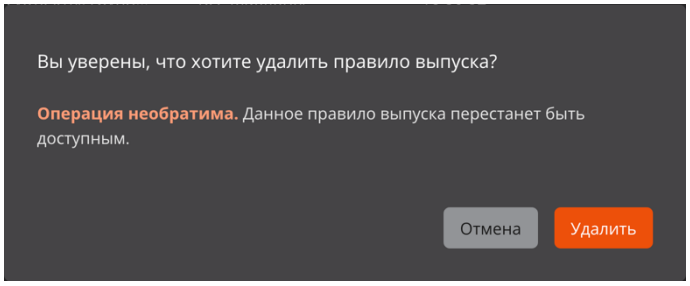


Рисунок 95 – Окно подтверждения удаления правила выпуска

7.7.2 Вкладка «SCEP»

Вкладка «SCEP» (см. Рисунок 96) раздела «Управление» обеспечивает следующие возможности:

- Создания, изменения и удаления SCEP-политик, а также управления статусами SCEP-политик.
- Создания, остановка, запуск и удаления SCEP-профилей.

Во вкладке «SCEP» раздела «Управление» отображена следующая информация:

- информация о существующих SCEP-политиках в табличной форме с полями:
  - «ChallengePassword» – содержит ChallengePassword SCEP-политики;
  - «Шаблон» – содержит шаблон, который используется при создании заявки по SCEP-политике;
  - «Статус» – содержит статус SCEP-политики. Допустимые значения в поле: «Активирована», «Остановлена».

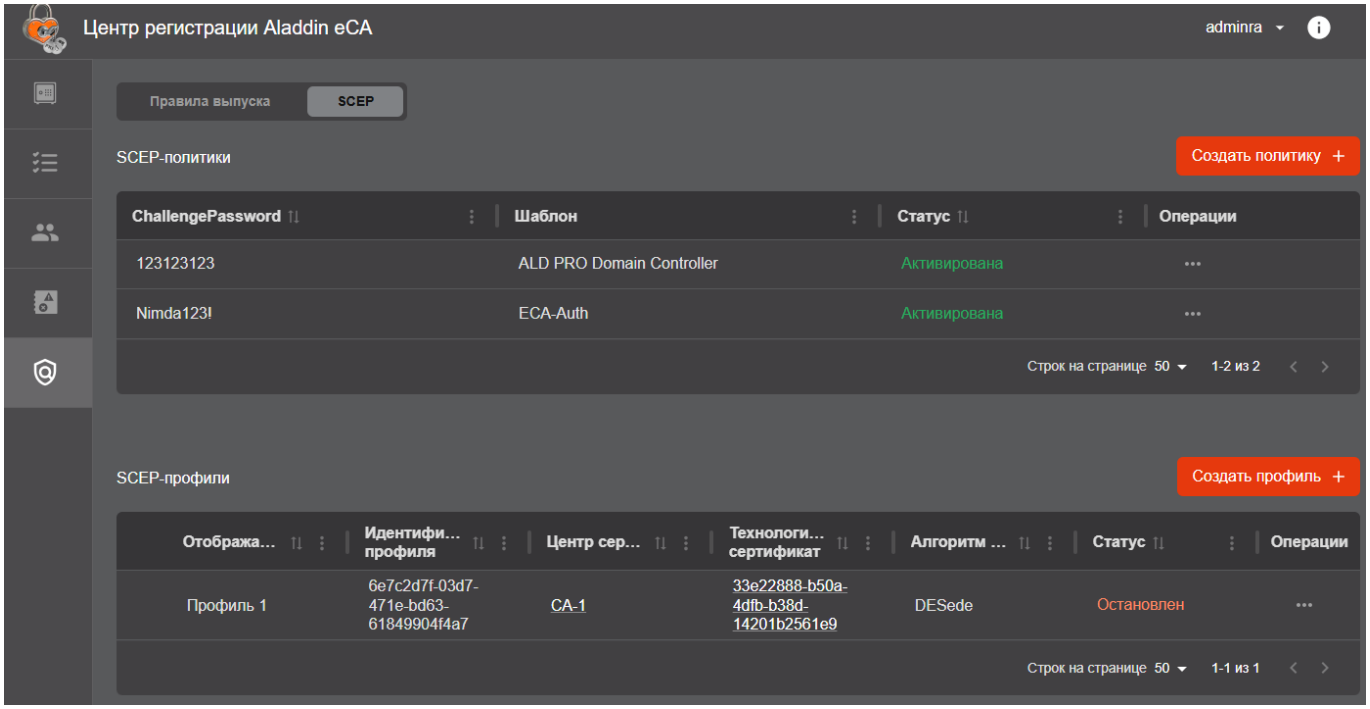


Рисунок 96 – Экран раздела «Управление». Вкладка «SCEP»

- информация о существующих SCEP-профилях в табличной форме с полями:
  - индикатор «Оранжевый треугольник с восклицательным знаком» – отображается только при неработоспособности SCEP-профиля. При наведении курсора на него отображается всплывающее сообщение «SCEP-профиль неработоспособен»;
  - «Отображаемое имя» – содержит отображаемое имя SCEP-профиля;
  - «Идентификатор профиля» – содержит идентификатор SCEP-профиля;
  - «Центр сертификации» – содержит отображаемое имя Центра сертификации подключенного Центра сертификации Aladdin eCA, с которым ассоциирован данный профиль. Значение в данном поле является гиперссылкой на карточку данного Центра сертификации в Центре сертификации Aladdin eCA;
  - «Технологический сертификат» – содержит идентификатор технологического сертификата данного SCEP-профиля. Значение в данном поле является гиперссылкой на карточку данного сертификата в Центре сертификации Aladdin eCA;
  - «Алгоритм шифрования» – содержит название алгоритма, по которому будут шифроваться ответы данного SCEP-сервера на запросы клиентов. Допустимые значения в поле: «DES», «AES», «AES_192», «AES_256», «DESede»;
  - «Статус» – статус SCEP-профиля. Допустимые значения в поле: «Активирован», «Остановлен».

Во вкладке «Правила выпуска» раздела «Управление» доступны следующие действия:

- 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. 7.7.2.8);
- Удаление SCEP-профиля (см. 7.7.2.9).

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 отрывшемся окне «Создание SCEP-политики» (см. Рисунок 97) 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».

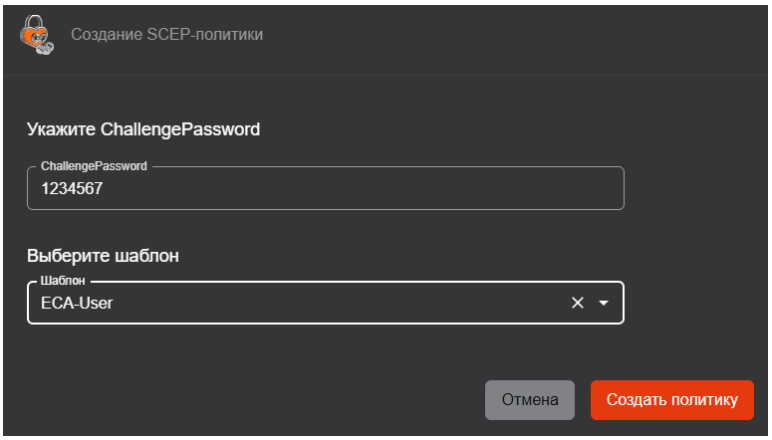


Рисунок 97 – Окно «Создание SCEP-политики»

- Далее нажмите на кнопку <Создать политику>.
- При успешном создании созданная SCEP-политика будет отображаться в списке SCEP-политик на вкладке «SCEP» в разделе «Управление».

В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском интерфейсе Центра регистрации Aladdin eRA 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 98).

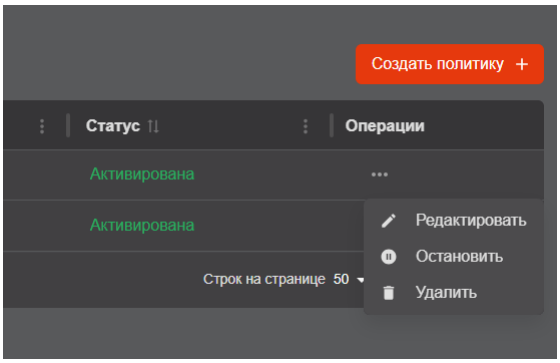


Рисунок 98 – Экран раздела «Управление». Вкладка «SCEP». Редактирование SCEP-политики

- В отрывшемся окне «Редактирование SCEP-политики» (см. Рисунок 99) 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».

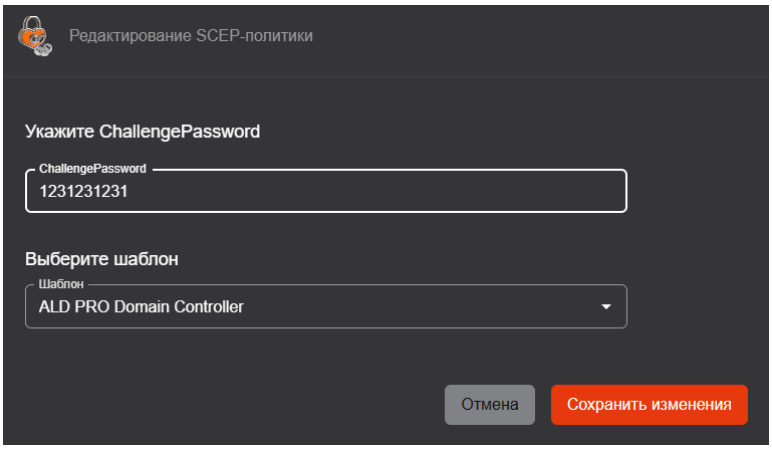


Рисунок 99 – Окно «Редактирование SCEP-политики»

- После нажатия на кнопку «Сохранить изменения» отредактированная SCEP-политика будет обновлена.

В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском интерфейсе Центра регистрации Aladdin eCA 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 100).

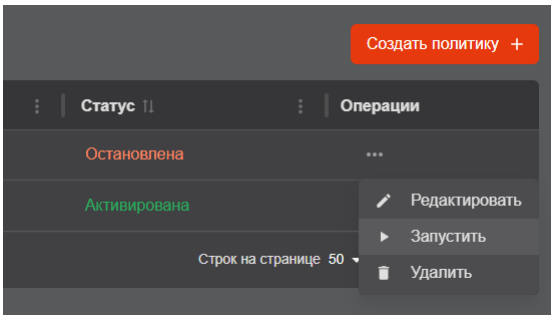


Рисунок 100 – Экран раздела «Управление». Вкладка «SCEP». Запуск SCEP-политики

- В открывшемся окне подтверждения операции запуска (см. Рисунок 101) нажмите на кнопку <Запустить>. После нажатия на неё SCEP-политика будет запущена.

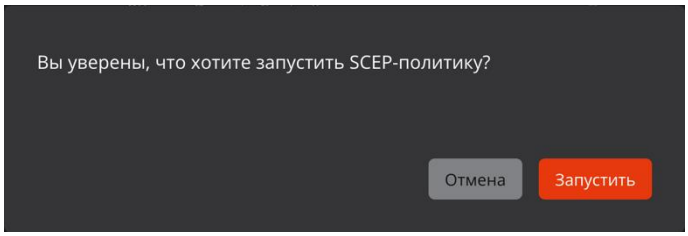


Рисунок 101 – Окно подтверждения запуска SCEP-политики

7.7.2.4 Остановка SCEP-политики

Остановка может быть выполнен 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 102).

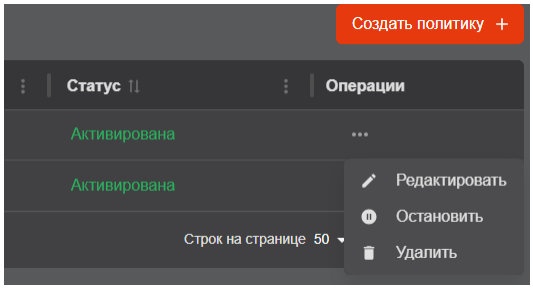


Рисунок 102 – Экран раздела «Управление». Вкладка «SCEP». Остановка SCEP-политики

- В появившемся окне подтверждения операции остановки (см. Рисунок 103) нажмите на кнопку <Остановить>. После нажатия на неё SCEP-политика будет остановлена.

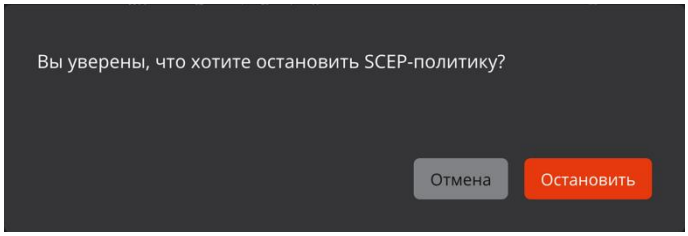


Рисунок 103 – Окно подтверждения остановки SCEP-политики

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 104).

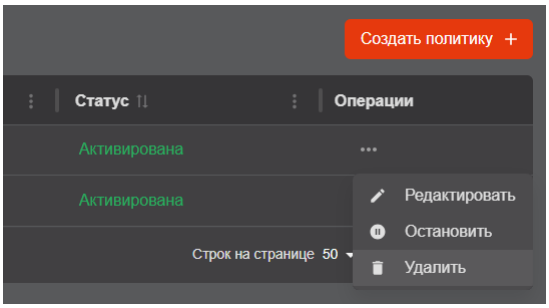


Рисунок 104 – Экран раздела «Управление». Вкладка «SCEP». Удаление SCEP-политики

- В появившемся окне подтверждения операции удаления (см. Рисунок 105) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-политика будет удалена.

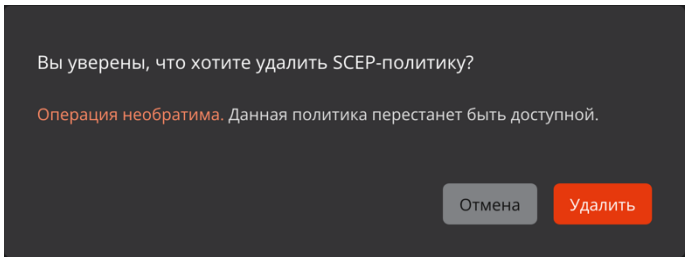
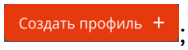


Рисунок 105 – Окно подтверждения удаления SCEP-политики

7.7.2.6 Создание SCEP-профиля

Для создания SCEP-профиля выполните следующие шаги:

- В разделе «Управление» во вкладке «SCEP» нажмите на кнопку <Создать профиль>  ;
- В отрывшемся окне «Создание SCEP- профиля» (см. Рисунок 97) заполните следующие поля:
  - отображаемое имя для создаваемого SCEP-профиля;
  - Центр сертификации подключенного Центра сертификации Aladdin eCA, для которого необходимо создать SCEP-профиль. В списке доступных для выбора Центров сертификации отсутствуют те Центры сертификации, для которых в Центре регистрации Aladdin eRA уже существует SCEP-профиль;
  - алгоритм шифрования ответов SCEP-сервера.

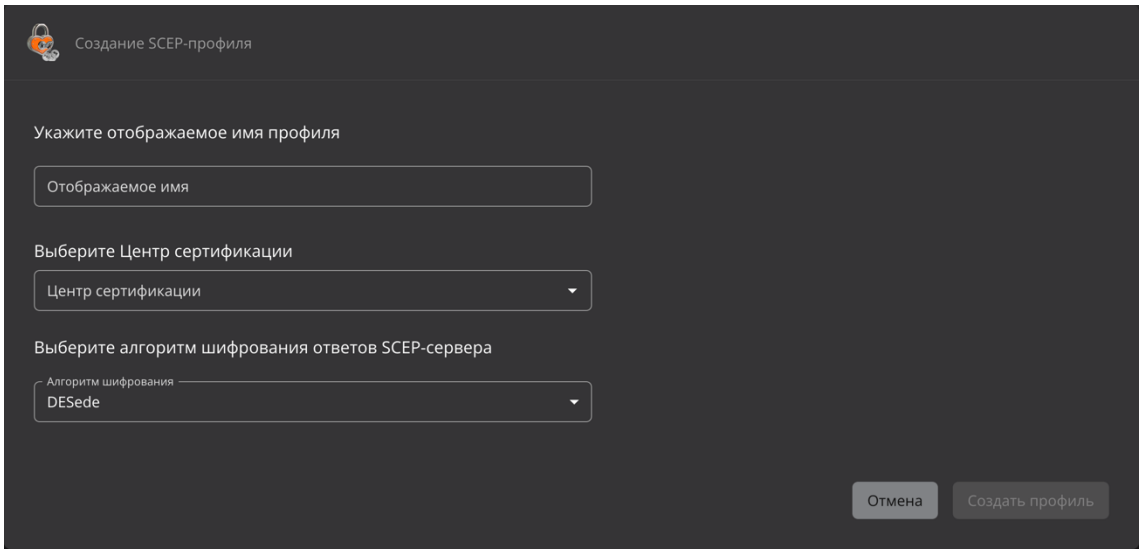


Рисунок 106 – Окно «Создание SCEP-профиля»

- Далее нажмите на кнопку <Создать профиль>.
- При успешном создании созданный SCEP-профиль будет отображаться в списке SCEP-профилей на вкладке «SCEP» в разделе «Управление».

> **Работа со SCEP-профилями Центров сертификации подключенного Центра сертификации Aladdin eCA, у которых криптопровайдером алгоритма ключа является СКЗИ «КриптоПро CSP», недоступна.**
>
> **Для такого SCEP-профиля сразу после его создания в пользовательском интерфейсе Центра регистрации Aladdin eRA будет отображаться индикация его неработоспособности**

7.7.2.7 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 107).

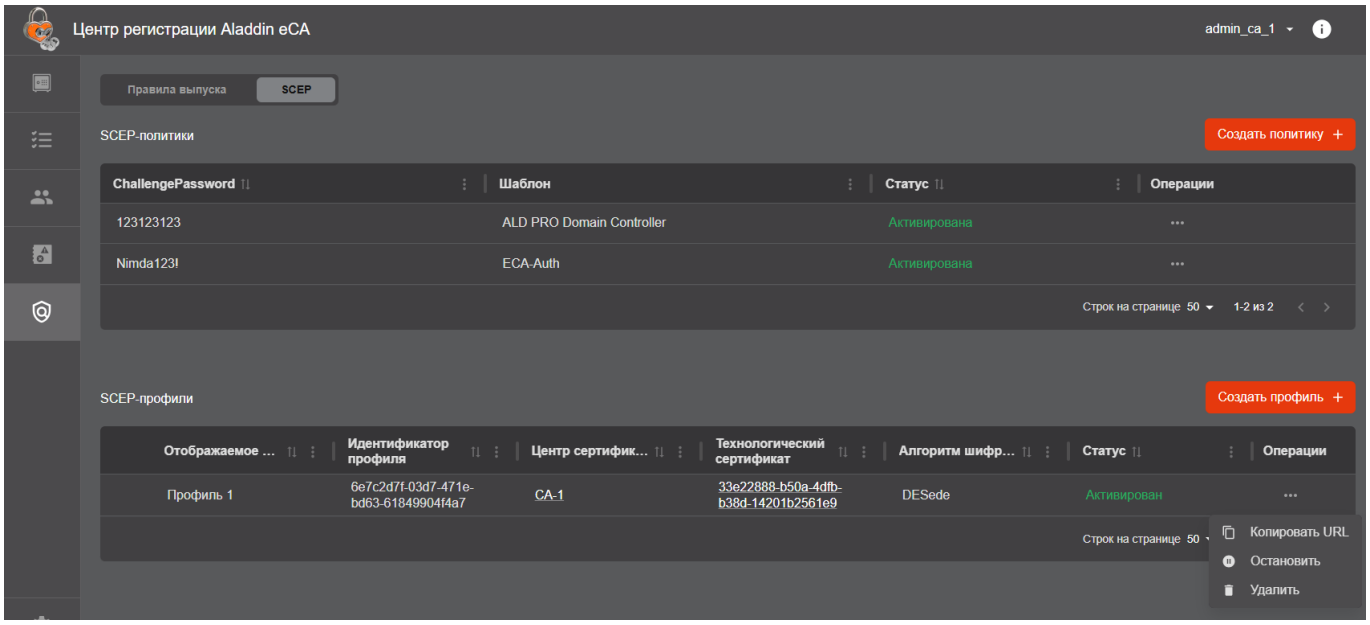


Рисунок 107 – Экран раздела «Управление». Вкладка «SCEP». Копирование URL

После этого буфер обмена будет содержать URL адреса SCEP-сервера выбранного SCEP-профиля (см. Рисунок 108).

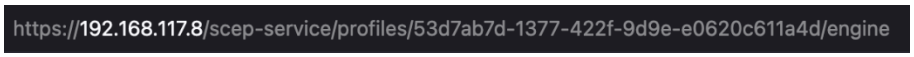


Рисунок 108 – Пример URL адреса SCEP-сервера

7.7.2.8 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).

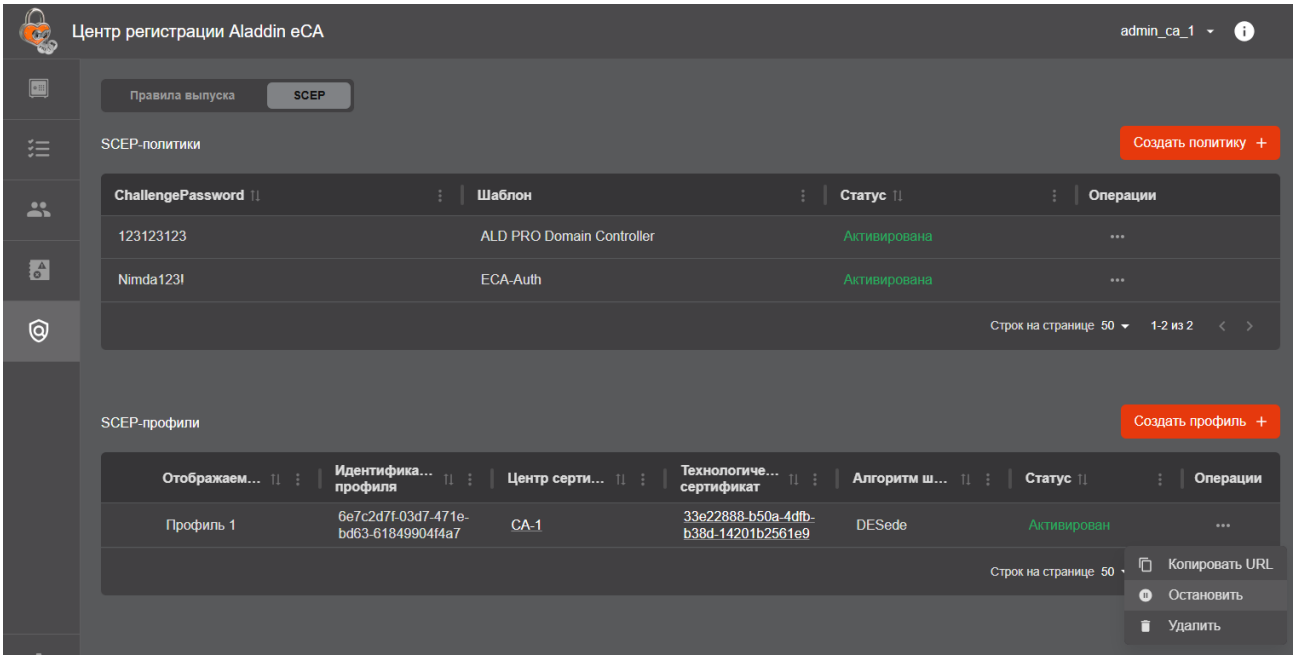


Рисунок 109 – Экран раздела «Управление». Вкладка «SCEP». Остановка SCEP-профиля

- В появившемся окне подтверждения операции (см. Рисунок 112) нажмите на кнопку <Остановить>.

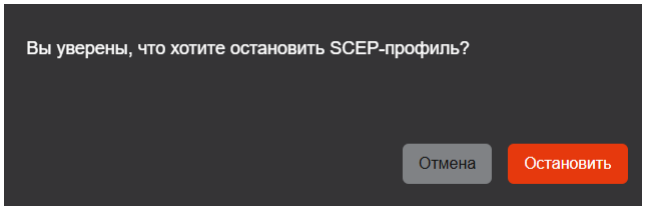


Рисунок 110 – Окно подтверждения удаления SCEP-профиля

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>.

7.7.2.9 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).

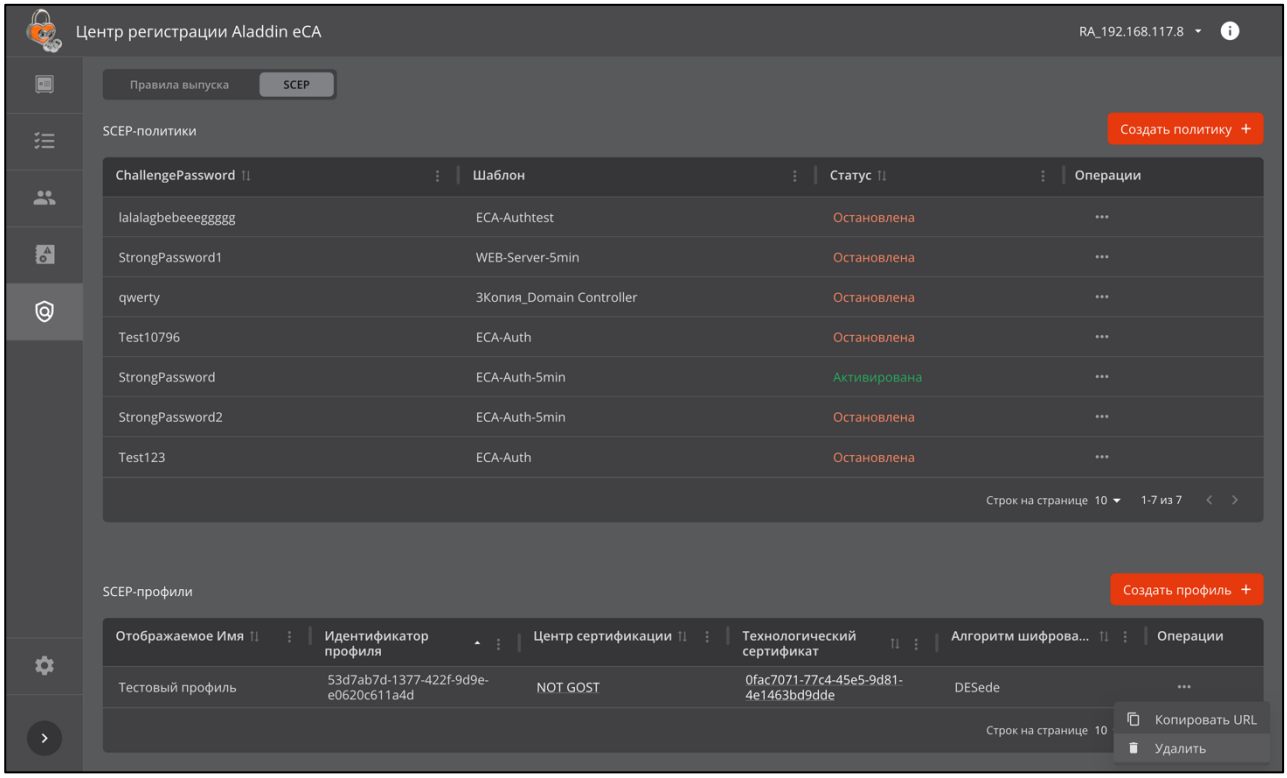


Рисунок 111 – Экран раздела «Управление». Вкладка «SCEP». Удаление SCEP-профиля

- В появившемся окне подтверждения операции удаления (см. Рисунок 112) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-профиль будет удален.

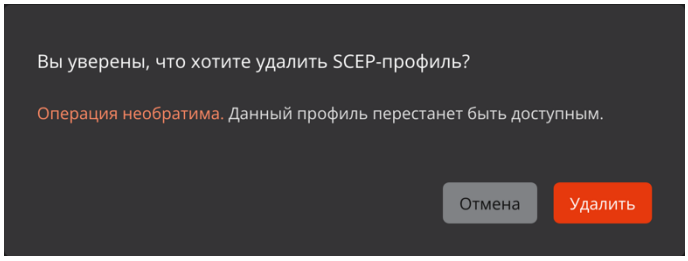


Рисунок 112 – Окно подтверждения удаления SCEP-профиля

7.8 Раздел «Настройки»

Раздел «Настройки» предоставляет информацию о текущем сертификате веб-сервера, о разрешённых издателях, обеспечивает возможность замены сертификата веб-сервера и управления Syslog-серверами для отправки сообщении с событиями аудита.

Переход на экран раздела «Настройки» (см. Рисунок 113) осуществляется по выбору раздела «Настройки» бокового меню, расположенного слева на главном экране (см. Рисунок 10).

Раздел «Настройки» содержит вкладки «Веб-сервер» и «Syslog».

Данный раздел доступен только для администратора.

7.8.1 Вкладка «Веб-сервер»

Вкладка «Веб-сервер» предназначена для:

- просмотра данных текущего сертификата веб-сервера;
- изменения текущего сертификата веб-сервера;
- просмотра списка разрешенных издателей сертификатов.

Вкладка «Веб-сервер» включает в себя следующие подразделы:

- Сертификат;
- Разрешённые издатели.

В подразделе «Сертификат» в табличной форме отображена следующая информация о текущем сертификате веб-сервера:

- в поле «Имя» – CN, указанный в сертификате;
- в поле «Издатель» – SDN издателя сертификата;
- в поле «Действителен до» – дата окончания действия сертификата.

В подразделе «Разрешённые издатели» в табличной форме отображается следующая информация об издателях сертификатов:

- в поле «Отображаемое имя» - отображаемое имя центра сертификации;
- в поле «Издатель» – CN, указанный в сертификате центра сертификации;
- в поле «Действителен до» – дата окончания действия сертификата центра сертификации;
- в поле «Разрешенный издатель» – индикатор, отражающий вхождение издателя в список разрешённых.

Рисунок 113 – Экран раздела «Настройки»

7.8.1.1 Смена сертификата веб-сервера

Предварительно на подключённом Центре сертификации Aladdin eCA необходимо выпустить сертификат для субъекта, соответствующего Центра регистрации Aladdin eRA, 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 cpnginx, 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 cpnginx установка сертификата с алгоритмом ключа, отличным от ГОСТ Р 34.10-2012, недоступна».

Для смены ключей веб-сервера выполните следующие шаги:

- Наведите курсор на строку с сертификатом веб-сервер и нажмите на появившуюся кнопку ;
- В появившемся окне (см. Рисунок 114) выберите файл сертификата и введите пароль файла контейнера, заданный при выпуске сертификата веб-сервера.
- Нажмите активировавшуюся кнопку <Сменить ключи>.

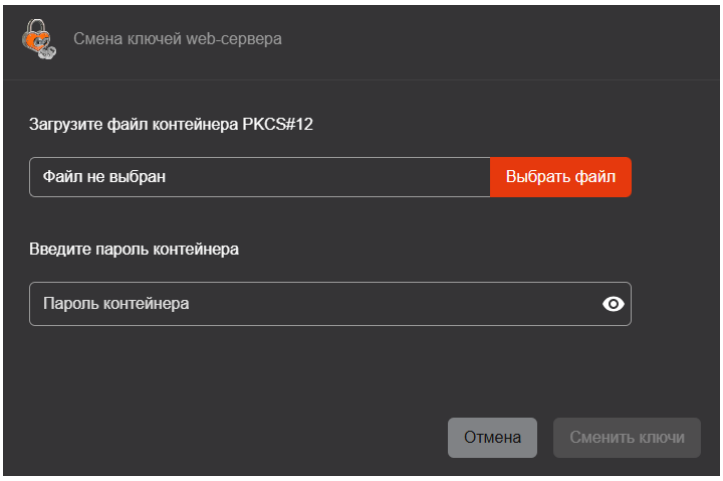


Рисунок 114 – Окно смены ключей веб-сервера

- После смены сертификата веб-сервера появится сообщение «Сертификат изменён» (см. Рисунок 115). И в результате успешной установки сертификата веб-сервера в «Журнал событий» будет записано событие с кодом RAENV035.

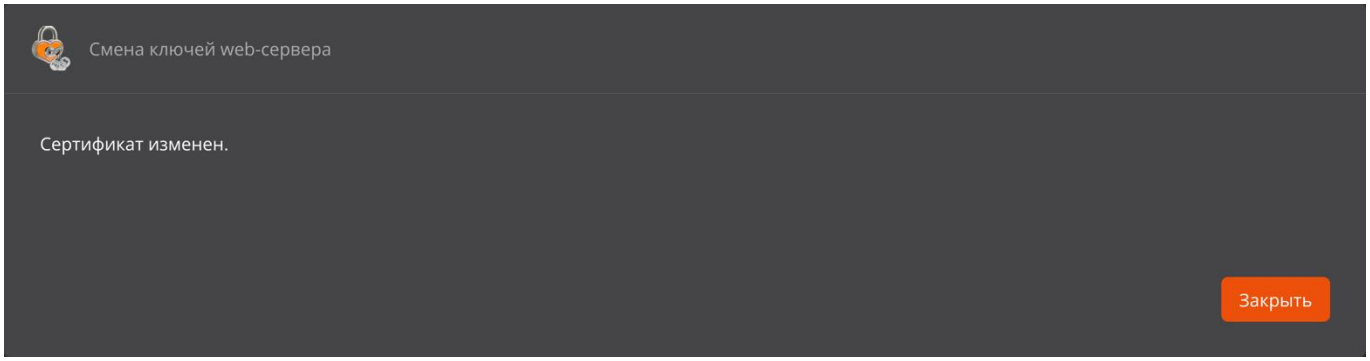


Рисунок 115 – Окно уведомления об успешной смене ключей веб-сервера

- Далее для установки безопасного соединения с серверной частью Центра регистрации (после установки нового сертификата веб-сервера) запустите браузер и выполните подключение к Центру регистрации.
- После этого откроется страница с предупреждением системы безопасности (см. Рисунок 116).

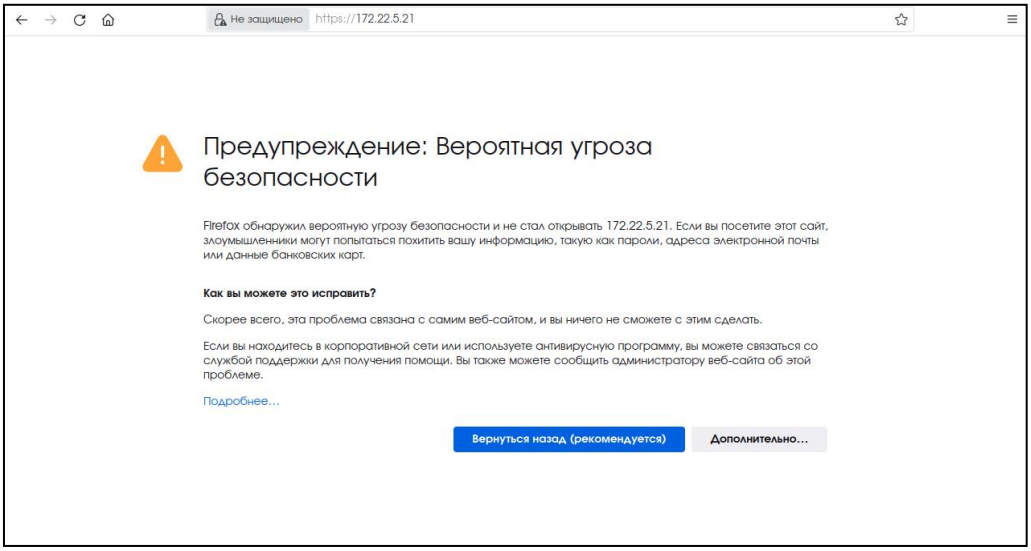


Рисунок 116 – Страница с предупреждением системы безопасности

- Нажмите кнопку <Дополнительно – произойдёт переход на страницу ошибки распознавания сертификата (см. Рисунок 117). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

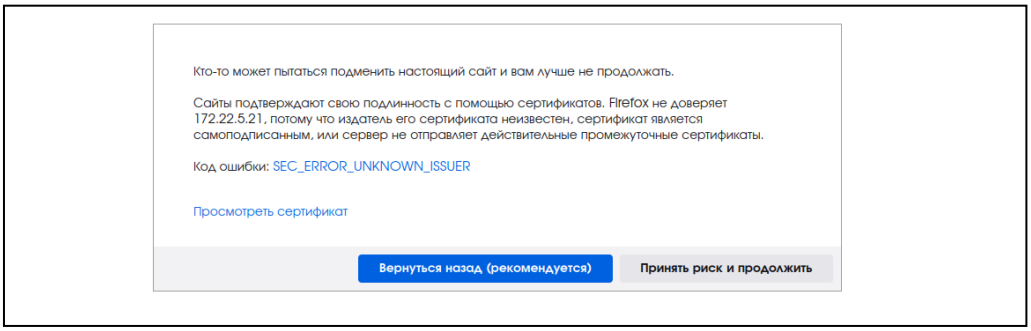


Рисунок 117 – Страница ошибки распознавания сертификата

- Установка ключей веб-сервера завершена.

7.8.2 Вкладка «Syslog»

В Центре регистрации Aladdin eRA реализована возможности автоматической отправки во внешние системы информации о регистрируемых событиях аудита по протоколу Syslog (в соответствии с рекомендацией RFC5424). Отправка Syslog-сообщений на Syslog-серверы возможна по протоколу UDP или TCP. Максимально возможно добавить 10 Syslog-серверов.

Значения полей отправляемых сообщений о зарегистрированных событиях представлено в таблице ниже (Таблица 14).

Таблица 14 – Значения полей отправляемых сообщений

Поле Syslog-сообщения	**Описание**	**Значение**
PRIVAL	Priority Value – значение, вычисляемое на основе категории и важности события	Для информационных событий – 14, для ошибок – 11
VERSION	Версия используемого стандарта Syslog	1
TIMESTAMP	Временная метка в соответствии с RFC3339	Текущее время на хосте Центра регистрации в формате ISO 8601: YYYY-MM-DDThh:mm:ss[.SSS]
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста Центра регистрации
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	[aeca-ra actionCode=''actionCode'' category=''category'' id=''id'' serviceName=''serviceName'' system=''system'' username=''username'' role=''role'' ipAddress=''ipAddress'' attributes=''attributes''] где: – ''actionCode'' – код события; – ''category'' – категория события; – ''id'' – идентификатор типа события; – ''serviceName'' – имя сервиса, в котором произошло событие; – ''system'' – флаг системного события; – ''username'' – логин учетной записи инициатора события; – ''role'' – роль инициатора события; – ''ipAddress'' – IP-адрес инициатора события; – ''attributes'' – расширенное описание события. Состав полей расширенного описания события соответствует составу полей описания события, указанному в Приложении 6.
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»).

Вкладка «Syslog» предназначена для:

- просмотра списка и параметров Syslog-серверов;
- добавления Syslog-серверов в список;
- редактирования параметров Syslog-серверов из списка, включая управление (включение/выключение) отправкой сообщений на данный Syslog-сервер;
- удаления Syslog-серверов из списка.

На вкладке «Syslog» (см. Рисунок 118) в табличной форме отображается следующая информация о добавленных Syslog-серверах:

- поле «Адрес хоста» - адрес хоста Syslog-сервера (IP-адрес или доменное имя);
- поле «Порт» - порт Syslog-сервера;
- поле «Протокол» - протокол, по которому выполняется отправка сообщение на Syslog-сервер;
- поле «Отправка сообщений» - содержит переключатель, позволяющий включить или выключить отправку сообщение на данный Syslog-сервер.

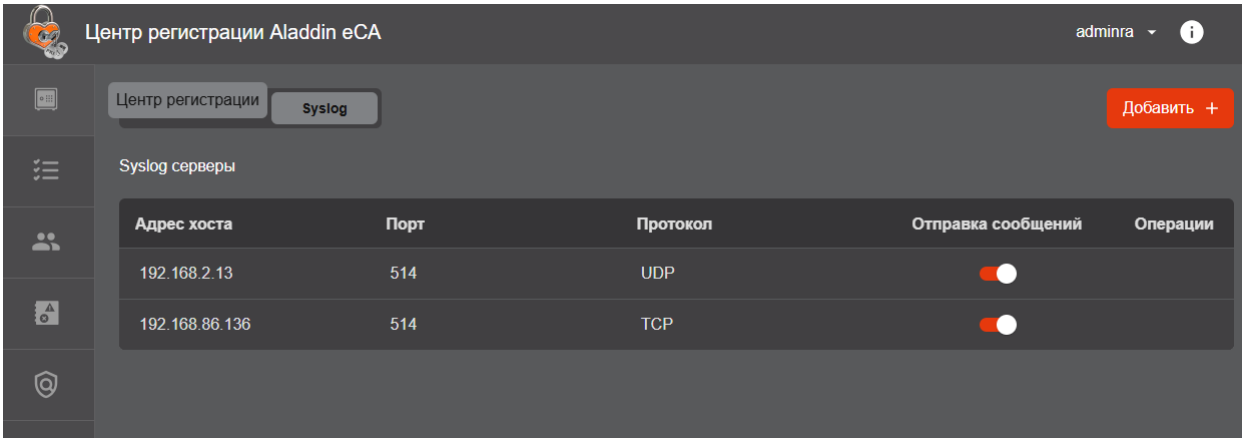


Рисунок 118 –Раздел «Настройки». Вкладка «Syslog»

7.8.2.1 Добавление Syslog-сервера

Чтобы добавить Syslog-сервер, выполните следующие действия:

- Перейдите в раздел «Настройки» на вкладку «Syslog» и нажмите кнопку «Добавить».
- В открывшемся окне (Рисунок 119) укажите параметры добавляемого Syslog-сервера:
  - в поле «Адрес хоста» укажите адрес хоста Syslog-сервера (IP-адрес или DNS-имя);
  - в поле «Порт» - укажите порт Syslog-сервера (число в диапазоне от 0 до 65535);
  - в списке «Протокол» выберите протокол взаимодействия с Syslog-сервером UDP (указан по умолчанию) или TCP.
- Нажмите кнопку «Добавить».

После добавления Syslog-сервера отправка оповещений на него по умолчанию будет включена. Выключение отправки сообщений на выбранный Syslog-сервер выполняется с помощью переключателя «Отправка сообщений».

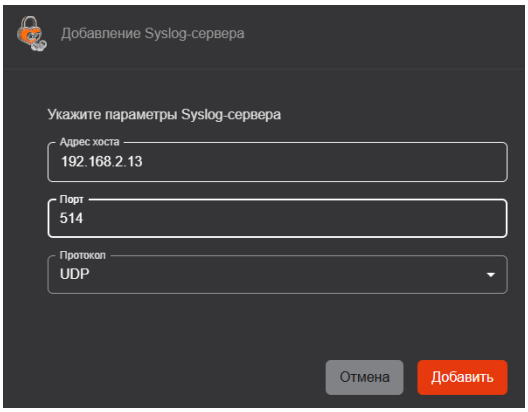


Рисунок 119 –Добавление Syslog-сервера

7.8.2.2 Редактирование параметров Syslog-сервера

Чтобы выполнить редактирование параметров Syslog-сервера, выполните следующие действия:

- Перейдите в раздел «Настройки» на вкладку «Syslog».
- В строке выбранного Syslog-сервера нажмите кнопку «Редактировать».
- В открывшемся окне (Рисунок 120) измените параметры Syslog-сервера (адрес хоста, порт, протокол передачи данных) и нажмите кнопку «Сохранить изменения».

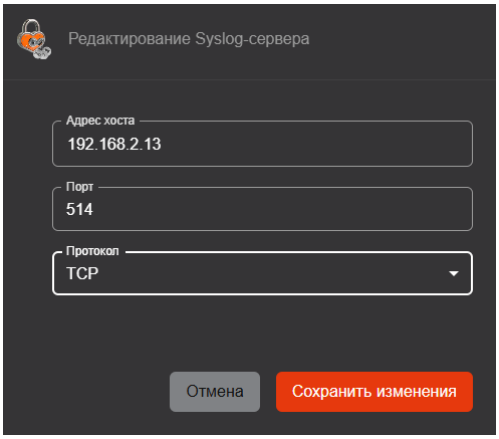


Рисунок 120 –Редактирование параметров Syslog-сервера

7.8.2.3 Удаление Syslog-сервера

Чтобы удалить Syslog-сервер, выполните следующие действия:

- Перейдите в раздел «Настройки» на вкладку «Syslog».
- В строке выбранного Syslog-сервер нажмите кнопку «Удалить».
- В открывшемся окне подтверждения удаления Syslog-сервера (Рисунок 121) нажмите кнопку «Удалить».

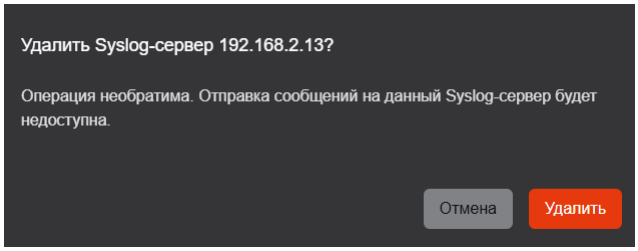


Рисунок 121 – Диалоговое окно подтверждения удаления Syslog-сервера

В результате Syslog-сервер будет удален из списка.

8 ПОДДЕРЖКА ПРОТОКОЛА SCEP

Центр регистрации Aladdin eCA реализует серверный компонент по протоколу SCEP[90] (далее SCEP-сервер Центра регистрации Aladdin eRA). SCEP-сервер Центра регистрации Aladdin eRA поддерживает возможность подключения к нему клиентов по протоколам HTTP и HTTPS.

Доступ клиентов к SCEP-серверу Центра регистрации Aladdin eRA осуществляется в контексте SCEP-профилей Центров сертификации подключенного Центра сертификации Aladdin eCA (см. раздел 7.7.2). Чтобы Центр сертификации подключенного Центра сертификации Aladdin eCA, мог быть использован в качестве издателя сертификатов по протоколу SCEP, необходимо для него создать SCEP-профиль.

При создании SCEP-профиля Центра регистрации Aladdin eRA 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 Центр регистрации Aladdin eRA и записывает его в свою базу данных в зашифрованном виде.
- экспортирует созданный контейнер закрытого ключа и сохранять 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 Центра регистрации Aladdin eRA 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 подключенного Центра сертификации Aladdin eCA 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 Центра регистрации Aladdin eRA см. раздел 7.7.2.7), где:

- «PROTOCOL» – протокол, по которому осуществляется подключение («http» или «https»);
- «HOSTNAME» – адрес хоста Центра регистрации Aladdin eRA;
- «profileId» – идентификатор существующего SCEP-профиля.

[90] Протокол SCEP описан в RFC8894, см.: https://datatracker.ietf.org/doc/html/rfc8894

- 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[91] для добавления SCEP-сервера[92]:

```
getcert add-scep-ca -c CA_Name -u SCEP_URL
```

Для проверки следует использовать команду:

```
sudo getcert list-cas -c Name
```

8.2 Обработку запросов по протоколу SCEP

Центр регистрации Aladdin eRA реализовывает обработку следующих запросов клиента по протоколу SCEP[93]:

- PKCSReq;
- CertPoll;
- RenewalReq;
- GetCert;
- GetCRL;
- GetCACert;
- GetCACaps.

8.2.1 Обработка запроса клиента PKCSReq/RenewalReq

Центр регистрации Aladdin eRA 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, Центр регистрации Aladdin eRA 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 eCA, ассоциированном с используемым пользователем SCEP-профилем.
  - Если по созданной заявке успешно выпущен сертификат, Центр регистрации Aladdin eRA в ответном сообщении возвращает клиенту выпущенный сертификат (SUCCES).
  - Если созданная заявка ожидает подтверждения или по ней произошла ошибка выпуска, Центр регистрации Aladdin eRA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
  - Если заявка не была создана или созданная заявка отклонена, Центр регистрации Aladdin eRA возвращает клиенту сообщение об отклонении запроса (FAILURE).
- Если выполненная заявка на данный сертификат клиента не найдена, Центр регистрации Aladdin eRA 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

[91] Certmonger — это служба, которая управляет сертификатами и их жизненным циклом в системах Linux.

[92] Для выполнения команд ниже необходимо, чтобы был установлен пакет `certmonger`.

[93] Запрос «GetNextCACert» на данный момент не поддерживается SCEP-сервером Центра регистрации Aladdin eRA.

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, Центр регистрации Aladdin eRA возвращает клиенту сообщение об отклонении запроса (FAILURE).
- Если по созданной заявке успешно выпущен сертификат, Центр регистрации Aladdin eRA в ответном сообщении возвращает клиенту выпущенный сертификат (SUCCES).
- Если созданная заявка ожидает подтверждения или по ней произошла ошибка выпуска, Центр регистрации Aladdin eRA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
- Если заявка не была создана или созданная заявка отклонена, Центр регистрации Aladdin eRA возвращает клиенту сообщение об отклонении запроса (FAILURE).

Центр регистрации Aladdin eRA записывает в свою базу данных «TransactionId» для каждой заявки, созданной в ходе обработки запросов «PKCSReq/RenewalReq».

8.2.2 Обработка запроса клиента CertPoll

Центр регистрации Aladdin eRA осуществляет поиск в свой базе данных заявки, у которой «TransactionId» соответствует указанному в сообщении, и определять ее статус.

- Если по найденной заявке успешно выпущен сертификат, Центр регистрации Aladdin eRA в ответном сообщении возвращает клиенту выпущенный сертификат по данной заявке (SUCCES).
- Если данная заявка ожидает подтверждения или по ней произошла ошибка выпуска, Центр регистрации Aladdin eRA возвращает клиенту сообщение о том, что заявка находится в обработке (PENDING).
- Если данная заявка отклонена или не была найдена, Центр регистрации Aladdin eRA должен возвращать клиенту сообщение об ошибке (FAILURE).

8.2.3 Обработка запроса клиента GetCert

Центр регистрации Aladdin eRA осуществляет поиск в свой 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 Центром сертификации Aladdin eCA, SCEP-профиль которого используется клиентом.

Если такая заявка найдена, Центр регистрации Aladdin eRA в ответном сообщении возвращает клиенту выпущенный по данной заявке сертификат (SUCCES), иначе – сообщение об ошибке (FAILURE).

8.2.4 Обработка запроса клиента GetCRL

Центр регистрации Aladdin eRA в ответном сообщении возвращает CRL Центра сертификации Aladdin eCA, SCEP-профиль которого используется клиентом.

8.2.5 Обработка запроса клиента GetCACert

Центр регистрации Aladdin eRA в ответном сообщении возвращает цепочку сертификатов технологического сертификата SCEP-профиля, используемого клиентом.

8.2.6 Обработка запроса клиента GetCACaps

Центр регистрации Aladdin eRA возвращает клиенту сообщение формата «CA Capabilities Response» в соответствии с RFC8894, перечисляющее следующие возможности SCEP-сервера, реализуемого Центра регистрации Aladdin eRA:

- AES;
- DES3;
- POSTPKIOperation;
- Renewal;
- SHA-1;
- SHA-256;
- SHA-512;
- SCEPStandart.

9 ПОДДЕРЖКА ПРОТОКОЛОВ MS-XCEP И MS-WSTEP

Центр регистрации Aladdin eRA реализует серверные компоненты по протоколам MS-XCEP[94] и MS-WSTEP[95]. 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 Центром регистрации Aladdin eRA в соответствии с протоколами MS-XCEP и MS-WSTEP, доступны по URL «`https://HOSTNAME/wstep-service/engine`», где «HOSTNAME» – адрес хоста Центра регистрации Aladdin eRA.

Центр регистрации Aladdin eRA в рамках реализации функций CEP-сервера (при получении запроса на политики «GetPolices») 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 политики «GetPolices»

Центр регистрации Aladdin eRA при получении запроса «GetPolices» 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 (см. Таблица 15).

Таблица 15 – Общие параметры возвращаемой политики

Параметр политики	Значение	Примечание
policyID	5817949c-a7cd-46ec-90ef-7782cd200b15	Уникальный идентификатор политики
policyFriendlyName	eCA 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 подключенного Центра сертификации Aladdin eCA, преобразованные в шаблоны по протоколу MS-XCEP (далее – шаблоны CEP).

При этом в шаблоны CEP преобразовываются только шаблоны Центра сертификации Aladdin eCA одновременно удовлетворяющие следующим условиям:

[94] Описание протокола MS-XCEP доступно по ссылке: https://winprotocoldoc.z19.web.core.windows.net/MS-XCEP/%5bMS-XCEP%5d.pdf

[95] Описание протокола MS-WSTEP доступно по ссылке: https://winprotocoldoc.z19.web.core.windows.net/MS-WSTEP/%5bMS-WSTEP%5d.pdf

- которые присутствуют в правилах выпуска Центра регистрации Aladdin eRA для данного пользователя с режимом обработки «Автоматический выпуск»;
- у которых включен алгоритм генерации ключевой пары RSA.

В атрибуты возвращаемых шаблонов CEP записываются значения в соответствии с таблицей ниже (см. Таблица 16):

Таблица 16 – Значения атрибутов шаблонов в сообщении «GetPoliciesResponse»

Атрибут шаблона в сообщении «GetPoliciesResponse»	**Примечание**
commonName	Имя шаблона Центра сертификации Aladdin eCA
policySchema	3
validityPeriodSeconds	Период действия сертификата по шаблону Центра сертификации Aladdin eCA в секундах
renewalPeriodSeconds	10 % от периода действия сертификата по шаблону в секундах
enroll	true
autoEnroll	true[96]
minimalKeyLength	Минимальная длина ключа для алгоритма RSA по шаблону Центра сертификации Aladdin eCA
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[97]
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

[96] Указанное значение обозначает, что шаблон может использоваться при автоэнроллменте.

[97] Указанное значение обозначает, что от пользователя при создании запроса на сертификат не должно требоваться указание значений для SDN и SAN.

Атрибут шаблона в сообщении «GetPoliciesResponse»	Примечание
keyArchivalAttributes	NULL
extensions	Строка вида «Имя_шаблона@ID_шаблона»[98]

Параметры издателя сертификатов в возвращаемой политике (блок «cAs») соответствуют таблице ниже (см. Таблица 17).

Таблица 17 – 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.
	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 Центром регистрации Aladdin eRA, совпадают.
priority	1	Приоритет издателя. Прочие значения не применимы для политики, формируемой Центром регистрации Aladdin eRA.
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 Центра сертификации Aladdin eCA	Сертификат в Base64.
enrollPermission	True	Значение указывает, что пользователь может выполнять запросы к данному издателю.

9.2 Обработка запроса на выпуск сертификата «RequestSecurityToken»

Центр регистрации Aladdin eRA 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.

[98] Данное значение будет записываться в расширения создаваемого на клиенте запроса на сертификат и будет использоваться в рамках реализации функций CES-севера.

Для заявок, создаваемых в ходе обработки запроса «RequestSecurityToken», указан сценарий «WSTEP».

При создании заявки и последующем выпуске сертификата в Центре сертификации Aladdin eCA атрибуты запроса на сертификат автоматически переопределяются атрибутами субъекта из Центра сертификации Aladdin eCA, требуемыми по шаблону.

Для поля, требуемого по шаблону, используются все имеющиеся у субъекта в соответствующем атрибуте значения.

В случае ошибки создания заявки Центра регистрации Aladdin eRA возвращает сообщение об ошибке с кодом «RequestFailed»;

- в случае успешного выпуска сертификата по созданной заявке Центр регистрации Aladdin eRA 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 выпушен, Центр регистрации Aladdin eCA возвращает сообщение об ошибке с кодом «RequestFailed».

- Центр регистрации Aladdin eRA поддерживает перевыпуск сертификатов с новым ключом и с тем же ключом, на котором был выпущен текущий сертификат.

10 ОФЛАЙН ВЫПУСК СЕРТИФИКАТОВ

Центр регистрации Aladdin eCA обладает возможностью офлайн выпуска сертификатов. Данная возможность заключается в том, что Центр регистрации Aladdin eRA 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 Центр регистрации Aladdin eRA 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

Центр регистрации Aladdin eCA поддерживает следующие расширения и кодировки файлов запросов на выпуск сертификатов:

- «.p10» (кодировки DER и PEM);
- «.cmc» (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 запускается по расписанию, которое задается с помощью CRON-выражения в параметре конфигурации `offline_enroll_cron`. Сценарий включает следующие шаги:

- Центр регистрации Aladdin eRA обрабатывает каждый файл запроса (запрос) из каталога запросов (параметр конфигурации `offline_enroll_req_path`);
- если в каталоге сертификатов (параметр конфигурации `offline_enroll_cert_path`) присутствует сертификат, выпущенный по данному запросу, то запрос пропускается;
- если в каталоге ошибок (параметр конфигурации `offline_enroll_error_path`) содержится данный запрос, то запрос пропускается;
- если по запросу была создана ранее заявка, то Центр регистрации Aladdin eRA анализирует её статус:
  - если заявка в статусе «Отклонена», то Центр регистрации Aladdin eRA копирует запрос в каталог ошибок;
  - если заявка в статусе «Ожидает подтверждения» или «Ошибка выпуска», то Центр регистрации Aladdin eRA пропускает запрос (при следующем выполнении сценария Центр регистрации Aladdin eRA снова проанализирует статус данной заявки);
  - если заявка в статусе «Выполнена», то Центр регистрации Aladdin eRA записывает выпущенный по заявке сертификат в каталог сертификатов. Сертификат записывается с расширением «.pem», кодировкой PEM и именем, аналогичным имени файла запроса, на основании которого был выпущен сертификат.

- если заявки не было, то Центр регистрации Aladdin eRA пытается создать заявку на основании запроса с использованием шаблона из указанного в параметре `offline_enroll_template_id` с использованием системной учётной записи (SYSTEM). При этом, если создание заявки завершается с ошибкой, то Центр регистрации Aladdin eRA копирует запрос в каталог ошибок.

10.3 Включение офлайн выпуска сертификатов

Для включения офлайн выпуска сертификатов следует выполнить следующие шаги:

- На хосте Центра регистрации Aladdin eRA создайте следующие каталоги[99]:
  - `` `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`, выполнив команду:

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

Задайте 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 следует брать из карточки шаблона в разделе «Шаблоны» у Центра сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA;
- `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, выполнив команду `sudo bash /opt/aecaRa/scripts/install.sh` с выбором действия «[Update]».

10.4 Отключение офлайн выпуска сертификатов

Для отключения офлайн выпуска сертификатов следует выполнить следующие шаги:

- Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, выполнив команду:

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

- Укажите в параметре `offline_enroll_enabled` значение `'false'`;
- Примените изменения конфигурационного файла, выполнив команду `sudo bash /opt/aecaRa/scripts/install.sh` с выбором действия «[Update]».

[99] Также можно примонтировать соответствующие сетевые каталоги к хосту Центра регистрации Aladdin eRA

11 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПРОГРАММЫ

Контроль целостности исполняемых файлов Центра регистрации Aladdin eRA 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 подкаталогах;
- все файлы в каталоге «`/opt/aecaRa/static`» и его подкаталогах;
- все файлы в каталоге «`/opt/aecaRa/bin`» и его подкаталогах;
- все файлы в каталоге `/opt/aecaRa/digsig` и его подкаталогах.

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`[100].

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 (от имени пользователя root, либо с использованием sudo):

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

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.

При успешной проверке целостности будет выведено сообщение: «Успешная проверка контрольных сумм». При этом в журнале событий будет зафиксировано событие с кодом RAENV1000 (событие «Успешная проверка контрольных сумм»).

При ошибке проверки целостности будет выведено сообщение «Неуспешная проверка контрольных сумм», а также сообщение об ошибке, генерируемое утилитой «`jcverify`». При этом в журнале событий будет зафиксировано событие с кодом RAENV1001 (событие «Неуспешная проверка контрольных сумм»).

[100] Данная утилита включена в состав Центра регистрации (каталог «`/opt/aecaRa/bin/jcverify`»).

12 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ ПРОГРАММЫ

Сбор диагностической информации компонентов необходим для предоставления в службу поддержки. пользователей информации о проблемах в работе программы.

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 18 – Данные системных логов

Системный лог	РЕД ОС	Astra Linux SE	Alt Сервер
/var/log/audit/	+	+	+
/var/log/samba/	+	+	+
/var/log/httpd/	+	-	-
/var/log/messages/	+	+	+
/var/log/secure/	+	-	-
/var/log/cron/	+	+	-
/var/log/auth/	-	+	-
/var/log/syslog/	-	+	+
/var/log/httpd2/	-	-	+
/var/log/ahttpd/	-	-	+

При включенном флаге сбора диагностической информации о памяти (параметр `enable_gc_diagnostic` конфигурационного файла `/opt/aecaCa/scripts/config.sh` архив диагностических данных дополнительно содержит:

- лог сборщика мусора;
- дампы памяти для упавших приложений Центра сертификации Aladdin eCA .

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`
```

Для сбора диагностической информации запустите скрипт от имени суперпользователя:

```
sudo 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

Создание резервных копий является неотъемлемой частью работы администратора Центра регистрации Aladdin eRA.

Перед выполнением каких-либо настроек, изменений и обновлений программы следует в обязательном порядке выполнить резервное копирование.

Резервные копии создаются для:

- содержимого каталога, содержащего сертификаты и ключи веб-сервера, разрешённых издателей, путь к которому определён значением параметра «`certificates_ssl_path`» конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `/opt/aecaRa/dist/certificates/ssl`);
- базы данных, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `aecara`);
- конфигурационного файла `/opt/aecaRa/scripts/config.sh`;

Резервное копирование осуществляется на локальный диск в папку, путь к которой определён значением параметра «`backup_path`» конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `/opt/aecaRa/dist/backup/`) с указанием даты и времени создания резервной копии в имени архива. Каталог хранения архивов выбран исходя из того, что необходимо хранить резервные копии временно и не увеличивать размер занятого пространства жёсткого диска. Для постоянного хранения требуется создать механизм переноса файлов.

Для постоянного хранения резервных копий следует:

- определить каталог для хранения резервных копий;
- составить сценарий для создания резервной копии;
- настроить расписание вызова сценариев.

Создание резервной копии Центра регистрации Aladdin eCA выполняется запуском скрипта с правами суперпользователя (root):

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

После запуска скрипта резервного копирования создаётся каталог `/opt/aecaRa/dist/backup`, где будет размещён архив, содержащий в имени дату и время создания полной резервной копии.

13.2 Расписание 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:

```
sudo 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.

Выход и сохранение из редактора расписания осуществляется командой:

```
:wq!
```

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 выполняется из папки, путь к которой определён значением параметра `backup_path` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `/opt/aecaRa/dist/backup/`).

Для восстановления данных выполните команду:

```
sudo bash /opt/aecaRa/scripts/restore.sh `путь к папке сохранения резервной копии`/архив резервной копии.tar
```

где `путь к папке сохранения резервной копии` определён значением параметра «`backup_path`» конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `/opt/aecaRa/dist/backup/`)

Если восстановление происходит после переустановки ОС и повторной установки программы, создайте каталог хранения резервных копий, путь к которому определён значением параметра «`backup_path`» конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `/opt/aecaRa/dist/backup/`), выполнив команду:

```
sudo mkdir -p /opt/aecaRa/dist/backup
```

Скопируйте в созданный каталог файл с резервной копией и выполните команду:

```
sudo bash /opt/aecaRa/scripts/restore.sh /opt/aecaRa/dist/backup/архив резервной копии.tar
```

14 ОБНОВЛЕНИЕ ПРОГРАММЫ

14.1 Назначение обновлений

Обновление базы данных и модулей Центра регистрации Aladdin eCA обеспечивает актуальность версии ПО. Выполняемые обновлениями задачи:

- исправление обнаруженных за время существования ПО недочётов и ошибок;
- устранение выявленных уязвимостей;
- изменение или улучшение работы существующих функций;
- добавление новых функций и возможностей.

14.2 Информирование потребителей о выпуске обновлений

Компания ведёт учёт покупателей «Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». Выполняется регистрация следующей информации:

- наименование организации;
- адрес организации;
- контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).

Уведомление пользователей о выпуске обновлений «Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» выполняется путём публикации информации на официальном сайте Компании и (или) с использованием рассылки электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счёт применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлом обновлений может предоставляться обновлённая документация для использования программы.

14.3 Получение обновлений потребителем

Получение файлов обновлений программного средства и соответствующих им контрольных сумм возможно:

- использованием электронной почты;
- путём загрузки с веб-сайта изготовителя (производителя).

Проверка квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений 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.

14.4 Контроль целостности обновления ПО

Контроль целостности обновления программы выполняется путём расчёта контрольной суммы полученного дистрибутива, с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0», и её сравнением со значением контрольной суммы для этого обновления.

14.5 Процедура установки обновлений

Внимание! На случай, если во время обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию программы и базы данных (см. раздел 8 настоящего документа), из которой можно будет восстановить данные.

Для обновления продукта:

- рекомендуется произвести очистку кэша используемого браузера;
- перенесите дистрибутив с обновлённой версией программы на компьютер с установленным Центром регистрации Aladdin eCA любым удобным способом;
- проверьте целостность дистрибутива путём подсчёта контрольной суммы;
- выполните распаковку инсталляционного комплекта:

РЕД ОС	`sudo dnf install aeca-*.rpm`
Astra Linux	`sudo dpkg -i aeca-*.deb`
Альт Сервер	`sudo apt-get install aeca-*.rpm`

- запустите установку продукта в режиме обновления, выполнив команду[101]:

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

- установщик обнаружит установленную версию программы 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 выбора продолжения процесса обновления, введите цифру «2»;
- при обновлении программа проверяет соответствие номера своей сборки и значения номера сборки, указанной в базе данных[102], имя которой указано в значении параметра `database_name` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `aecara`):
  - если на момент обновления в базе данных отсутствует номер сборки, то программа записывает в базе данных номер устанавливаемой сборки;
  - если на момент обновления в базе данных присутствует номер сборки, и он меньше номера устанавливаемой сборки, то программа перезаписывает номер сборки в базе данных, заменив его номером устанавливаемой сборки;
  - если на момент обновления в базе данных присутствует номер сборки, и он равен номеру устанавливаемой сборки, программа не изменяет его;
  - если на момент обновления в базе данных присутствует номер сборки, и он больше номера устанавливаемой сборки, то программа завершает обновление 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, указанный в базе данных, а «Y.Y.Y.Y» – номер устанавливаемой сборки программы.

[101] Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`)..

[102] Значение номера сборки указано в таблице «build_info» схемы «aeca_ra_info».

- после установки обновления запустите веб-браузер, удалите файлы cookie и данные сайтов, очистите кэш-память;
- запустите обновлённый Центр регистрации Aladdin eCA;
- проверьте версию обновлённого Центрf регистрации Aladdin eCA в окне «О программе».

После обновления программного средства с версии 2.0 до версии 2.2 пароль пользователя базы данных, заданный в конфигурационном файле `/opt/aecaRa/scripts/config.sh` в параметре `database_password`, отображается в зашифрованном виде. Шифрование пароля выполняется по алгоритму AES-256 с использованием автоматически сгенерированного в файле `/opt/aecaRa/scripts/key` ключа шифрования.

15 УДАЛЕНИЕ ПРОГРАММЫ

Для инициализации процесса удаления необходимо выполнить команду с правами суперпользователя:

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

В результате выполнения данного действия будут полностью уничтожены:

- все добавленные при установке программы системные службы;
- все добавленные при установке программы пользователи и группы;
- все добавленные при установке программы файлы и структура каталогов.

Все внесённые изменения будут выведены в консоль.

Процесс удаления производится вне зависимости от наличия соединения с базой данных, имя которой указано в значении параметра `database_name` конфигурационного файла `/opt/aecaRa/scripts/config.sh` (по умолчанию – `aecara`).

Удаление пакета повлечёт за собой удаление установочного комплекта в каталоге `/opt/aecaRa/`. Для удаления установочного комплекта выполните команду:

РЕД ОС	`sudo dnf remove aeca-*.rpm`
Astra Linux	`sudo apt remove aeca-*.deb`
Альт Сервер	`sudo dnf install aeca-*.rpm`

16 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

16.1 Удаление БД «aecaga»

Для удаления ранее созданной базы данных «aecaga» необходимо выполнить команды с правами суперпользователя (root или sudo):

- Зайдите под пользователем «postgres» в Postgres, выполнив команду:

```
sudo -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();
```

- Удаляем базу данных, выполнив команду:

```
DROP DATABASE aecara;
```

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

```
exit
```

16.2 Удаление пользователя БД «aeca»

Для удаления ранее созданного пользователя базы данных «aeca» необходимо выполнить команды с правами суперпользователя (root или sudo):

- Зайдите под пользователем «postgres» в Postgres, выполнив команду:

```
sudo -i -u postgres
```

- Удалите пользователя «aeca» в Postgres, выполнив команду:

```
dropuser aeca -i
```

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

```
exit
```

- Перезапустите СУБД Postgres, выполнив команду:

```
sudo systemctl restart postgresql
```

17 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ид.	Проблема	Возможная причина	Способы решения

П001	Ошибка при запуске скрипта установки `install.sh` «error obtaining MAC configuration for user «аеса»»	У пользователя postgres нет прав на чтение БД атрибутов конфиденциальности	Для предоставление дополнительных прав пользователю postgres выполните команды:
			`sudo usermod -a -G shadow postgres`
			`sudo setfacl -d -m u:postgres:r /etc/parsec/macdb`
			`sudo setfacl -R -m u:postgres:r /etc/parsec/macdb`
			`sudo setfacl -m u:postgres:rx /etc/parsec/macdb`

П002	Ошибка запуска сервисов после запуска скрипта `install.sh` для установки ЦР Aladdin eCA	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 `install.sh` для установки ЦР Aladdin eCA: «[ERROR] Не удалось запустить сервис aeca-ra-ca-adapter...»	Отсутствуют права на директории, которые указаны в файле `krb5.conf` в командах `includedir`. Пример: В файле `krb5.conf` используется команда `includedir /etc/krb5.conf.d/`, внутри этой директории есть файл `enable_ssd.conf_dir`, внутри которого есть команда `includedir /var/lib/sss/pubconf/krb5.include.d`, Соответственно должны быть права на: ▪ `krb5.conf`; ▪ `/etc/krb5.conf.d/`, а также все файлы и директории внутри, включая файл `enable_ssd.conf_dir`; ▪ `/var/lib/sss/pubconf/krb5.include.d/`, а также все файлы и директории внутри.	Выдать права на все файлы и директории, используемые в `krb5.conf`: `sudo chmod 666 путь_к_файлу` Где «путь_к_файлу» – путь к файлу или директории.
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

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 (root или sudo) 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 команду с правами суперпользователя (root или sudo):

```
/opt/pgpro/std-16/bin/pg-setup service start
```

ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

Для подключения Центра регистрации Aladdin eCA к внешней СУБД необходимо:

- выполнить настройку на хосте СУБД в соответствии с разделом 2.1, представленным ниже;
- выполнить настройку на хосте Центра регистрации Aladdin eRA в соответствии с разделом 2,2, представленным ниже.

2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД (установка СУБД описана в разделах 0, 0 и 3.3.3 настоящего руководства) 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, необходимо разрешить подключение по протоколу TCP для порта СУБД, выполнив в терминале на данном хосте следующую команду:

```
sudo 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:

```
sudo iptables -A INPUT -s IP -p tcp --destination-port post -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 `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

- Затем на хосте СУБД необходимо выполнить создание и настройку базы данных в соответствии с разделом 0. 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 и Альт Сервер

- Если в качестве ОС на хосте с СУБД используется РЕД ОС или Альт Сервер, необходимо отредактировать файл `/var/lib/pgsql/15/data/pg_hba.conf` (или `var/lib/jatoba/4/data/pg_hba.conf`, если используется СУБД Jatoba)[103], приведя его к следующему виду:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

# "local" is for Unix domain socket connections only
local   all             all                                     trust
# IPv4 local connections:
host    all             all             0.0.0.0/0               password
# IPv6 local connections:
```

[103] Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

```
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
```

Кроме того, необходимо отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)[104], 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 команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

- Затем на хосте СУБД необходимо выполнить создание и настройку базы данных. Действия по созданию и настройке базы данных в зависимости от ОС описаны в разделах: 0 для РЕД ОС, 3.3.3 для Альт Сервер. В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

2.2 Настройка на хосте Центра регистрации Aladdin eRA

На хосте Центра регистрации Aladdin eRA предварительно должна быть выполнена установка СУБД. При этом не нужно настраивать СУБД, установленную на хосте Центра регистрации Aladdin eRA.

На хосте Центра регистрации Aladdin eRA необходимо отредактировать конфигурационный файл `/opt/aecaRa/scripts/config.sh`, указав в нём значения следующих параметров:

Параметр	Значение по умолчанию	Описание
use_tls	false	Флаг обязательного использования TLS для подключения к СУБД[105]. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя базы данных, используемое для работы Центра регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
database_password	#CHANGEIT	Пароль пользователя базы данных, используемый для работы Центра регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
database_host	'localhost'	Сетевой адрес хоста СУБД
database_port	'5432'	Порт, используемый для подключения к базе данных

[104] Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

[105] Подробная информация о параметре `use_tls` приведена в Настройка TLS-соединения с СУБД

Параметр	Значение по умолчанию	Описание
database_name	'aecara'	Имя базы данных, используемой Центром регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
root_cert_path	#CHANGEIT	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД[106]

- Затем на хосте Центра регистрации Aladdin eRA необходимо применить изменения конфигурационного файла путём запуска команды `sudo bash /opt/aecaRa/scripts/install.sh` и дальнейшего выбора действия «[Update]». В случае, если Центр регистрации Aladdin eRA не был установлен ранее, выбор действия не потребуется, и будет выполнена установка с указанными в конфигурационном файле параметрами.

[106] 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 Центре сертификации Aladdin Enterprise Certification Authority 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)[107], так как Центр регистрации Aladdin eRA 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 Центре Сертификации Aladdin eCA, указав ему необходимые атрибуты CN и DNS Name).

Во избежание ошибок в работе Центра Регистрации Aladdin eRA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу Центра Регистрации Aladdin eRA путём выполнения команды `sudo systemctl stop aeca-ra.service`.

Для настройки TLS-соединения Центра Регистрации Aladdin eRA с СУБД необходимо:

- выполнить настройку СУБД в соответствии с разделом 3.1 настоящего приложения, представленным ниже;
- выполнить настройку Центра Регистрации Aladdin eRA в соответствии с разделом 3.2 настоящего приложения, представленным ниже.

3.1 Настройка на хосте СУБД

1) 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)[108], указав:

- в параметре «ssl» значение «on»;
- в параметре «ssl_cert_file» абсолютный путь к файлу сертификата сервера СУБД[109];
- в параметре «ssl_key_file» абсолютный путь к файлу закрытого ключа сервера СУБД[110];
- в параметре «ssl_ca_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД[111].

[107] Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database_host» конфигурационного файла Центра регистрации Aladdin eRA.

[108] Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

[109] Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса Центра сертификации Aladdin eCA. Например, в карточке локального субъекта сервера СУБД.

[110] 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.

[111] Файл цепочки сертификатов издателя сертификата СУБД может быть скачан в карточке ЦС, выпустившего сертификат сервера СУБД.

При этом указанные выше файлы должны иметь метку доступа «600», установить которую можно с помощью команды `sudo chmod 600 путь_к_файлу` для каждого файла. Владельцем всех указанных выше файлов необходимо назначить пользователя «postgres», выполнив команду `sudo 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 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`:

```
# - SSL -
ssl = on
ssl_cert_file = '/tmp/cert.pem'
ssl_key_file = '/tmp/key.key'
ssl_ca_file = '/tmp/chain.pem'
```

2) На хосте СУБД перезапустить СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

3.2 Настройка на хосте Центра регистрации Aladdin eRA

1) На хосте Центра регистрации Aladdin eRA 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[112].

При этом указанный выше файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен иметь метку доступа «600», установить которую можно с помощью команды `sudo chmod 600 путь_к_файлу`. Владельцем файла сертификата корневого издателя из цепочки сертификатов сервера СУБД необходимо назначить пользователя «aeca», выполнив команду `sudo 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 на хосте Центра регистрации Aladdin eRA 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 на хосте Центра регистрации Aladdin eRA необходимо дополнительно выполнить команду `restorecon -Rv "путь к файлу сертификата корневого издателя из цепочки сертификатов сервера СУБД"`.

2) На хосте Центра регистрации Aladdin eRA применить изменения конфигурационного файла путём запуска команды `sudo bash /opt/aecaRa/scripts/install.sh` и дальнейшего выбора действия «[Update]».

По завершению выполнения указанной команды дальнейший обмен данными Центра Регистрации Aladdin eRA с СУБД будет осуществляться только по протоколу TLS. Если в СУБД, к которой выполняется подключение, отключён TLS, то Центр Регистрации Aladdin eRA не будет выполнять обмен данными с такой СУБД. При этом Центр Регистрации Aladdin eRA сможет установить соединение с СУБД только в случае, если её сертификат издан издателем, путь к сертификату которого указан в конфигурационном файле Центра Регистрации Aladdin eRA и только в случае, если имя хоста сервера СУБД соответствует указанному в сертификате.

[112] Если сертификат сервера СУБД выпущен подчинённым ЦС, необходимо указать путь до сертификата корневого ЦС.

ПРИЛОЖЕНИЕ 4. РАЗВЁРТЫВАНИЕ КЛАСТЕРА ЦЕНТРА РЕГИСТРАЦИИ ALADDIN ECA

Центр регистрации Aladdin eCA обеспечивает возможность кластеризации с использованием внешнего средства балансирования нагрузки.

В кластере Центра регистрации Aladdin eRA работает аутентификация по сертификату, а также по доменному логину и паролю.

Аутентификация с использованием Kerberos-билета не работает.

4.1 Развёртывание кластера Центра регистрации Aladdin eRA

Кластер конфигурируется по схеме «Active-Passive Failover», куда входят следующие узлы:

- хост с установленным Центром регистрации Aladdin eRA (ВМ1) – основной узел кластера;
- хост с установленным Центром регистрации Aladdin eRA (ВМ2) – резервный узел кластера;
- хост с установленной и настроенной СУБД (ВМ3);
- хост с установленным и настроенным средством балансирования нагрузки HAProxy (ВМ4).

На всех указанных выше хостах допускается использование только следующих операционных систем:

- 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 «Орел»;
- 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 «Орел»;
- РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;
- РЕД ОС версия 8, конфигурация «Сервер»;
- ОС Альт 8 СП, релиз 10, вариант исполнения Сервер.

Кроме кластерных компонентов также присутствуют следующие компоненты:

- Центр сертификации Aladdin eCA – к нему подключаются узлы Центра регистрации Aladdin eRA (основной и резервный);
- РС – к ней подключаются узлы Центра регистрации Aladdin eRA (основной и резервный). Также РС должна быть подключена к Центру сертификации Aladdin eCA.

4.2 Настройка узла с СУБД

1) На ВМ3 выполнить установку одной из нижеприведённых систем управления базами данных[113]:
   - PostgreSQL из состава операционной системы;
   - Jatoba 4.

[113] Информация по установке и настройке СУБД приведена в разделах 0 для РЕД ОС, 0 для Astra Linux и 3.3.3 для Альт Сервер.

2) На ВМ3 увеличить максимальное количество подключений к СУБД, отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)[114], указав для параметра `max_connections` значение 2000[115]:

```
max_connections = 2000
```

3) На ВМ3 перезапустить используемую СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

4.3 Настройка основного узла

1) На ВМ1 выполнить подготовку к установке Центра Регистрации Aladdin eRA в соответствии с разделом 3 настоящего руководства, при этом подготовка осуществляется с учётом использования внешней СУБД.

2) На ВМ1 выполнить установку Центра Регистрации Aladdin eRA в соответствии с разделом 4 настоящего руководства, при этом подключив к Центру Регистрации Aladdin eRA внешнюю СУБД, установленную на ВМ3, в соответствии с «Приложение 2. Настройка подключения к внешней СУБД» настоящего руководства.

3) Выполнить первичную настройку Центра Регистрации Aladdin eRA.

4) При использовании офлайн выпуска сертификатов необходимо выполнить инструкцию по включению данной функции из раздела 10.3 на ВМ1.

4.4 Настройка резервного узла

1) Средствами используемого гипервизора клонировать ВМ1 (клон ВМ1 далее по тексту – «ВМ2»)[116].

2) Изменить доменное имя для ВМ2.

3) Запустить ВМ2 и ожидать завершения запуска `aeca-ra.service` на ВМ2.

4) Внести изменения в конфигурацию Центра регистрации Aladdin eRA на ВМ2 (файл `/opt/aecaRa/scripts/config.sh`):

- Отключить офлайн выпуск – на резервных узлах он должен быть всегда выключен:

```
offline_enrollment_enabled='false'
```

- Применить изменения конфигурационного файла путём запуска команды `sudo bash /opt/aecaRa/scripts/install.sh` с выбором действия «[Update]».

4.5 Настройка HAProxy

1) На ВМ4 выполнить установку средства балансирования нагрузки HAProxy:

РЕД ОС[117]	`sudo dnf install haproxy`
Astra Linux SE	`sudo apt install haproxy`
Альт Сервер	`sudo apt-get install haproxy`

[114] Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

[115] Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра Центра регистрации Aladdin eRA, взаимодействующего с СУБД

[116] Вместо клонирования ВМ1 можно произвести развёртывание Центра регистрации Aladdin eRA, выполнив инструкцию из п 0 данного приложения для резервного узла.

[117] При установке HAProxy на РЕД ОС необходимо выполнить отключение SELinux в соответствии с официальной документацией ОС:

- для РЕО ОС 7.3 см. https://redos.red-soft.ru/base/redos-7_3/7_3-network/7_3-sett-proxy/7_3-haproxy/;
- для РЕО ОС 8 см. https://redos.red-soft.ru/base/redos-8_0/8_0-network/8_0-sett-proxy/8_0-haproxy/.

2) На ВМ4 отредактировать файл `/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
    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

- вместо `DOMAINNAME_HOST1` необходимо указать доменное имя ВМ1,
- вместо `DOMAINNAME_HOST2` – доменное имя ВМ2,
- вместо `admin:password` указать логин и пароль, разделенные двоеточием, которые будут использоваться для доступа к панели мониторинга HAProxy.

3) На ВМ4 перезапустить HAProxy путем запуска команды:

```
sudo systemctl restart haproxy.service
```

В результате приведенной настройки кластера все запросы, направляемые к Центру регистрации Aladdin eRA через средство балансирования нагрузки HAProxy, будут перенаправляться на основной узел кластера (ВМ1). В случае недоступности основного узла кластера все запросы, направляемые к Центру регистрации Aladdin eRA через средство балансирования нагрузки HAProxy, будут перенаправляться на резервный узел кластера (ВМ2). Для мониторинга состояния узлов кластера может быть использована панель мониторинга, доступная по адресу `http://IP_HOST4:8404/stats`, где `IP_HOST4` – IP-адрес ВМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на ВМ4).

4.6 Подключение дополнительных резервных узлов

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла необходимо выполнить действия, аналогичные действиям по подключения резервного узла «ВМ2».

1) Развернуть Центр регистрации Aladdin eRA на ВМР (дополнительный резервный узел) – см. инструкцию в разделе 0 данного приложения.

2) На ВМ4 отредактировать файл `/etc/haproxy/haproxy.cfg` – внести в него доменное имя ВМР в секцию `backend bk_app` под строкой, соответствующей последнему резервному узлу. Если последний резервный узел – это ВМ2, то это под строкой: `server clone DOMAINNAME_HOST2:443 check backup`. Таким образом должна получиться секция вида:

```
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` – это доменное имя ВМР.

3) На ВМ4 перезапустить HAProxy путем запуска команды:

```
sudo systemctl restart haproxy.service
```

В результате в кластере появится дополнительный резервный узел. Все описанные выше рекомендации и уточнения по работе с узлом ВМ2, также относятся и к узлу ВМР.

4.7 Обновление Центров регистрации Aladdin eCA в кластере

Обновление кластера Центра Регистрации Aladdin eRA включает в себя предварительную приемку Центра Регистрации Aladdin eRA, который будет устанавливаться на узлы кластера, остановку работающих Центров Регистрации Aladdin eRA кластера и выполнение последовательного обновления Центров Регистрации Aladdin eRA на каждом узле кластера.

Обновление производится для кластера Центра Регистрации Aladdin eRA, сконфигурированного по схеме выше в разделе 0 данного приложения.

В кластер Центра Регистрации Aladdin eRA входят следующие узлы:

- хост с установленным Центром Регистрации Aladdin eRA (ВМ1) – основной узел кластера;
- хосты с установленным Центром Регистрации Aladdin eRA (ВМ2-узлы) – резервные узлы кластера;
- хост с установленной и настроенной СУБД (ВМ3);
- хост с установленным и настроенным средством балансирования нагрузки HAProxy (ВМ4).

Обновления Центров Регистрации Aladdin eRA узлов кластера включает в себя:

- обновление Центра Регистрации Aladdin eRA на основном узле кластера (ВМ1);
- обновление Центров Регистрации Aladdin eRA на резервных узлах кластера (ВМ2-узлах).

Номер сборки устанавливаемых Центров Регистрации Aladdin eRA должен быть одинаковым для основного и резервных узлов кластера.

Иначе Центры Регистрации Aladdin eRA на узлах кластера не могут быть запущены[118].

Процесс обновления кластера Центра Регистрации Aladdin eRA:

1) Предварительно произвести действия по приёмке Центра Регистрации Aladdin eRA;

2) На основном узле произвести резервное копирование данных в соответствии с разделом 14 настоящего документа для возможности восстановления данных в случае неисправности;

3) На резервных узлах произвести резервное копирование данных в соответствии с разделом 14 настоящего документа для возможности восстановить данные в случае неисправности;

4) На резервных узлах произвести остановку Центра Регистрации Aladdin eRA путем выполнения команды `sudo systemctl stop aeca-ra.service`;

Это действие необходимо для избежания ошибок и вызвано тем, что Центр Регистрации Aladdin eRA на основном узле и Центры Регистрации Aladdin eRA на резервных узлах работают с одной схемой базы данных. И при обновлении Центра Регистрации Aladdin eRA на одном узле происходит обновление схемы базы данных до новой версии, с которой Центры Регистрации Aladdin eRA на других узлах могут работать некорректно.

5) На основном узле произвести обновление Центра Регистрации Aladdin eRA в соответствии с разделом 14 настоящего руководства;

6) На каждом резервном узле произвести обновление Центра Регистрации Aladdin eRA в соответствии с разделом 14 настоящего руководства.

Критерием правильности установки обновления кластера является отображение информации о новой версии программы в окне «О программе» и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга, доступной по адресу `http://IP_HOST4:8404/stats`, где `IP_HOST4` – IP-адрес ВМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на ВМ4).

[118] Описание проверок при запуске, осуществляемых Центром регистрации Aladdin eRA, см в разделе 5.3.

ПРИЛОЖЕНИЕ 5. НАСТРОЙКА KERBEROS В ВЕБ-БРАУЗЕРЕ

Предварительно на клиенте должен быть настроен Kerberos, клиент должен быть подключён к домену и клиент должен использовать бразуер с поддержкой Kerberos.

Для того, чтобы в браузере клиента при работе с Центром регистрации Aladdin eRA была доступна аутентификация по Kerberos необходимо внести доменное имя Центра регистрации Aladdin eRA в список доверенных URI, для которых используется аутентификация Kerberos в соответствии с инструкциями ниже.

5.1 Настройка веб-браузера Mozilla Firefox

Далее в примере:

- `ra246.sambadc.host` – доменное имя Центра регистрации Aladdin eRA;
- `sambadc.host` – домен, (`SAMBADC.HOST` – realm в Kerberos);
- Версия браузера: 78.12.0esr (64-bit).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация Kerberos выполните следующие шаги:

1. Запустите Mozilla Firefox.
2. В адресной строке введите `about:config` и нажмите Enter.
3. Нажмите на кнопку **Принять риск и продолжить**.
4. В поле "Поиск" (Filter) введите `negotiate`, чтобы ограничить список опций.
5. Выполните двойное нажатие мышью на строке с параметром `network.negotiate-auth.trusted-uris`.
6. В диалоговом окне введите:
   - Чтобы разрешить SPNEGO аутентификацию только по конкретной ссылке, введите полностью домен из ссылки (например, `ra246.sambadc.host`);
   - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.sambadc.host`);
   - Чтобы разрешить SPNEGO аутентификацию для нескольких доменов, введите их через запятую (например, `ra247.sambadc.host,ra246.sambadc.host`).
     После запятой можно ставить пробел.
7. Продублируйте введённое значение параметра `network.negotiate-auth.trusted-uris` в параметр `network.negotiate-auth.delegation-uris`.
8. При необходимости удалите cookie, связанные с доменом Центра регистрации Aladdin eRA.

5.2 Настройка веб-браузера Chromium

Далее в примере:

- `ra246.sambadc.host` – доменное имя Центра регистрации Aladdin eRA;
- `sambadc.host` – домен, (`SAMBADC.HOST` – Realm в Kerberos);
- Версия браузера: Version 130.0.6723.69 (Official Build) (64-bit).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация Kerberos выполните следующие шаги:

1. Кликните правой кнопкой мыши на ярлыке "Chromium".
2. Выберите "Свойства".
3. В поле "Объект" к строке запуска браузера допишите
   - Чтобы разрешить SPNEGO аутентификацию только по конкретной ссылке, введите полностью домен из ссылки:

`--args --auth-server-whitelist="ra246.sambadc.host"`;

- Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена со звёздочкой и точкой в начале:
  `--args --auth-server-whitelist="*.sambadc.host"`;
- Чтобы разрешить SPNEGO аутентификацию для нескольких доменов, введите их через запятую:
  `--args --auth-server-whitelist="ra246.sambadc.host,ra247.sambadc.host "`.

4. При необходимости удалите cookie, связанные с доменом Центра регистрации Aladdin eRA.

Пример консольной команды:

```
chromium --args --auth-server-whitelist="ra246.sambadc.host"
```

ПРИЛОЖЕНИЕ 6. ПЕРЕЧЕНЬ РЕГИСТРИРУЕМЫХ СОБЫТИЙ

6.1 События запуска и остановки служб

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

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 – Описание 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) – Описание 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) – Описание 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) – Описание ошибки

6.4 События работы с заявками

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание заявки	RAENV0300	INFO	Краткое описание: Создание заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать)
Ошибка создания заявки	RAENV0301	ERROR	Краткое описание: Ошибка создания заявки Атрибуты: – Сценарий (может отсутствовать) – CN в заявке (может отсутствовать) – Id шаблона (может отсутствовать) – Имя шаблона (может отсутствовать) – Id получателя сертификата (может отсутствовать) – Имя получателя сертификата (может отсутствовать) – Внешний ключ (может отсутствовать) – Описание ошибки
Обработка заявки	RAENV0302	INFO	Краткое описание: Обработка заявки Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Режим обработки – Id правил
Выпуск сертификата по заявке	RAENV0303	INFO	Краткое описание: Выпуск сертификата по заявке Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата

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

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

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка отзыва заявки	RAENV0312	ERROR	Краткое описание: Ошибка отзыва сертификата Атрибуты: – Id заявки – Сценарий – CN в заявке – Id шаблона – Имя шаблона – Id получателя сертификата – Имя получателя сертификата – Статус – Внешний ключ (может отсутствовать) – Id сертификата (может отсутствовать) – Описание ошибки

6.5 События работы с ключевыми носителями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Подключение ключевого носителя	RAENV0400	INFO	Краткое описание: Подключение ключевого носителя Атрибуты: – Свойства носителя
Ошибка подключения ключевого носителя	RAENV0401	ERROR	Краткое описание: Ошибка подключения ключевого носителя Атрибуты: – Свойства носителя – Описание 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») – Описание ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
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 – Описание 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) – Описание ошибки
Редактирование правила выпуска	RAENV0602	INFO	Краткое описание: Редактирование правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка редактирования правила выпуска	RAENV0603	ERROR	Краткое описание: Ошибка редактирования правила выпуска Атрибуты: – ID правила – Отображаемое имя правила (может отсутствовать) – Режим обработки (может отсутствовать) – Статус (может отсутствовать) – Субъекты доступа (может отсутствовать) – Объекты доступа (может отсутствовать) – Описание ошибки
Запуск правила выпуска	RAENV0604	INFO	Краткое описание: Запуск правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа
Ошибка запуска правила выпуска	RAENV0605	ERROR	Краткое описание: Ошибка запуска правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа – Описание ошибки
Остановка правила выпуска	RAENV0606	INFO	Краткое описание: Остановка правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа
Ошибка остановки правила выпуска	RAENV0607	ERROR	Краткое описание: Ошибка остановки правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа – Описание ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Удаление правила выпуска	RAENV0608	INFO	Краткое описание: Удаление правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа
Ошибка удаления правила выпуска	RAENV0609	ERROR	Краткое описание: Ошибка удаления правила выпуска Атрибуты: – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа – Описание ошибки

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	Краткое описание: Изменение сертификата веб-сервера Атрибуты: – Серийный номер – Отпечаток – CN в сертификате – SDN издателя – Действует с – Действует по
Ошибка изменения сертификата веб-сервера	RAENV0701	ERROR	Краткое описание: Ошибка изменения сертификата веб-сервера Атрибуты: – Серийный номер (может отсутствовать) – Отпечаток (может отсутствовать) – CN в сертификате (может отсутствовать) – Действует с (может отсутствовать) – Действует по (может отсутствовать) – Описание ошибки
Изменение списка разрешённых издателей	RAENV0702	INFO	Краткое описание: Изменение списка разрешённых издателей Атрибуты: – Обновлённый список разрешённых издателей

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка изменения списка разрешённых издателей	RAENV0703	ERROR	Краткое описание: Ошибка изменения списка разрешённых издателей Атрибуты: – Обновлённый список разрешённых издателей (может отсутствовать) – Описание ошибки

6.9 События Offline-выпуска

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Запуск Offline-выпуска	RAENV0800	INFO	Краткое описание: Запуск Offline-выпуска Атрибуты: – Каталог запросов – Каталог сертификатов – Каталог ошибок – Id шаблона
Завершение Offline-выпуска	RAENV0801	INFO	Краткое описание: Завершение Offline-выпуска Атрибуты: – Список Id заявок, созданных в результате Offline-выпуска – 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
Ошибка создания резервной копии	RAENV0901	ERROR	Краткое описание: Ошибка создания резервной копии Атрибуты: – Абсолютное имя файла резервной копии (может отсутствовать) – Описание ошибки
Успешное восстановление из резервной копии	RAENV0902	INFO	Краткое описание: Успешное восстановление из резервной копии Атрибуты: – Абсолютное имя файла резервной копии
Ошибка восстановления из резервной копии	RAENV0903	ERROR	Краткое описание: Ошибка восстановления из резервной копии Атрибуты: – Абсолютное имя файла резервной копии (может отсутствовать) – Описание 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: Описание 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: Описание 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 Атрибуты: Описание 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: – Адрес хоста – Порт – Протокол – Флаг отправки сообщений
Ошибка добавления Syslog-сервера	RAENV1201	ERROR	Краткое описание: Ошибка добавления Syslog-сервера Атрибуты: – Адрес хоста (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщений (может отсутствовать) – Описание ошибки

Причина, вызвавшая запись в журнал	**Код события**	**Категория события**	**Описание в журнале**
Изменение параметров Syslog-сервера	RAENV1202	INFO	Краткое описание: Изменение параметров Syslog-сервера – Атрибуты: – Адрес хоста – Порт – Протокол – Флаг отправки сообщений
Ошибка изменения параметров Syslog-сервера	RAENV1203	ERROR	Краткое описание: Ошибка изменения параметров Syslog-сервера Атрибуты: – Адрес хоста (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщений (может отсутствовать) – Описание ошибки
Удаление Syslog-сервера	RAENV1204	INFO	Краткое описание: Удаление Syslog-сервера Атрибуты: – Адрес хоста – Порт – Протокол – Флаг отправки сообщений
Ошибка удаления Syslog-сервера	RAENV1205	ERROR	Краткое описание: Ошибка удаления Syslog-сервера Атрибуты: – Адрес хоста – Порт – Протокол – Флаг отправки сообщений Описание ошибки

ПРИЛОЖЕНИЕ 7. НАСТРОЙКА ВЗАИМОДЕЙСТВИЯ С КРИПТОПРОВАЙДЕРОМ СКЗИ «КРИПТОПРО CSP»

Взаимодействие Центра регистрации Aladdin eRA с криптопровайдером СКЗИ «КриптоПро CSP» из состава программного средства осуществляется через модуль «КриптоПро Java CSP»[119].

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром регистрации Aladdin eRA необходимо подготовить внешнюю гамму[120].

Порядок настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром регистрации Aladdin eRA:

- 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 `sudo apt-get install newt52`.**

- При отсутствии создайте каталог `/opt/aecaRa/services/cryptoproviders` командой:

```
sudo 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:

```
sudo 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 Центра регистрации Aladdin eRA, то назначьте файлам права доступа (chmod 777) командой:

```
sudo chmod 777 /opt/aecaRa/services/cryptoproviders/
{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar, cpSSL.jar, sspiSSL.jar}
```

  - Если Центр регистрации Aladdin eCA был установлен ранее, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа к файлам (chmod 700) командами:

```
sudo chown aeca:aeca
/opt/aecaRa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,
cpSSL.jar, sspiSSL.jar}
sudo chmod 700
/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/cprocsp/bin/amd64/genkpim` (утилита `genkpim` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma
/opt/cprocsp/bin/amd64/genkpim <количество ключей> 0x12345678 ~/gamma
```

[119] Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

[120] 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 Центра регистрации Aaddin eRA поместите каталог с заранее подготовленной внешней гаммой в каталог `/opt/aecaRa/dist/` командой:

```
sudo cp -a ~/gamma/. /opt/aecaRa/dist/gamma
```

- В результате в каталоге `/opt/aecaRa/dist/gamma` появятся подкаталоги `db1, db2, kpim`.
  - Если выполняется первоначальная установка Центра регистрации Aladdin eRA, то назначьте права доступа файлам (chmod 777) командой:

```
sudo chmod -R 777 /opt/aecaRa/dist/gamma
```

  - Если Центр регистрации Aladdin eRA был установлен ранее, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа (chmod 700) командами:

```
sudo chown -R aeca:aeca /opt/aecaRa/dist/gamma
sudo chmod -R 700 /opt/aecaRa/dist/gamma
```

- Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд[121]:

```
sudo ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
sudo ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1
/opt/aecaRa/dist/gamma/db1/kis_1
sudo ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1
/opt/aecaRa/dist/gamma/db2/kis_1
```

- Если Центр регистрации Aladdin eRA был установлен ранее, перезапустите сервис `aeca-ra.service` командой:

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

[121] 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`.

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

Перед началом работы следует ознакомиться со следующей документацией, относящейся к программному обеспечению:

- официальная документация РЕД ОС 7.1
- (адрес: https://redos.red-soft.ru/base/manual/?ysclid=l5gg69co40129982631);
- официальная документация Astra Linux Special Edition 1.7
- (адрес: https://wiki.astralinux.ru/pages/viewpage.action?pageId=137563555&ysclid=l5gg3t48tj885563182);
- официальная документация Альт Сервер 8, релиз 10
- (адрес: https://www.basealt.ru/alt-server/docs);
- официальная документация Postgres
- (адрес: http://www.postgresql.org/docs/12/index.html);
- официальная документация Jatoba 4
- (адрес: https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy);
- официальная документация JC-Web Client 4.3.5 Руководство пользователя
- (адрес: https://www.aladdin-rd.ru/support/downloads/jc-webclient/).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	–	Операционная система
ПО	–	Программное обеспечение
СУБД	–	Система управления базами данных
УЦ	–	Удостоверяющий центр
ЦР	–	Центр регистрации
ЦС	–	Центр сертификации
AeCA CE	–	Центр сертификатов Aladdin Enterprise Certificate Authority Certified Edition
AeCA VA	–	Aladdin Enterprise Certificate Authority Validation Authority
AeCA RA	–	Aladdin Enterprise Certificate Authority Registration Authority
CRL	–	Certificate Revocation List
AIA	–	Authority Information Access
URL	–	Uniform Resource Locator

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 токену, программному или аппаратному модулю безопасности Hardware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

Контрольный список – это текстовый файл, в котором содержатся контрольные суммы всех файлов, входящих в дистрибутив ПО «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition, записанный на компакт-диск с размещённым на нём дистрибутивом программы и комплектом документации.

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.

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

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.

UI-интерфейс (user interface) – интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводи-тельного документа и дата	Подпись	Дата
	изме-ненных	заменен-ных	новых	аннулиро-ванных					