



Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition KG

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

Изделие	33714370.03.01.001
Документ	33714370.03.01.001 32 01-5
Версия	2.3.0
Листов	181
Дата	30.05.2025

АННОТАЦИЯ

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

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 KG»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 KG. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority».

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

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

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.....	2
1 Введение	7
1.1 Назначение программы	7
1.2 Состав программы.....	7
1.3 Функции программы	7
1.4 Роли управления.....	8
1.5 Режимы функционирования программы	11
2 Условия выполнения программы	12
2.1 Требования к программному обеспечению	12
2.1.1 Требования к среде функционирования Серверной части программы.....	12
2.1.2 Требования к среде функционирования Клиентской части программы	13
2.2 Требования к аппаратным средствам.....	13
3 Подготовка к установке программы	15
3.1 Подготовка среды функционирования с ОС РЕД ОС.....	17
3.1.1 Подключение репозитория и установка зависимостей.....	17
3.1.2 Установка среды исполнения Java	18
3.1.3 Установка и настройка СУБД.....	18
3.1.4 Установка веб-сервера	21
3.2 Подготовка среды функционирования с ОС Astra Linux SE.....	22
3.2.1 Подключение репозитория и установка зависимостей.....	22
3.2.2 Установка среды исполнения Java	24
3.2.3 Установка и настройка СУБД.....	24
3.2.4 Установка веб-сервера	27
3.3 Подготовка среды функционирования с Альт Сервер	28
3.3.1 Подключение репозитория и установка зависимостей.....	28
3.3.2 Установка среды исполнения Java	28
3.3.3 Установка и настройка СУБД.....	29
3.3.4 Установка веб-сервера	32
3.4 Подготовка среды функционирования с Platform V SberLinux OS Server	33
3.4.1 Установка среды исполнения Java	33
3.4.2 Установка и настройка СУБД.....	33
3.4.3 Установка веб-сервера	36
3.5 Создание службы HTTP и keytab-файла	36
3.5.1 Получение keytab-файла в Samba DC и Альт Домен.....	37
3.5.2 Получение keytab-файла в ALD PRO.....	38
3.5.3 Получение keytab-файла в Free IPA	38
3.5.4 Получение keytab-файла в MS AD	39
3.6 Установка веб-сервера Cppnginx.....	39
3.7 Установка JC-WebClient.....	40
3.8 Установка Рутокен плагина и его расширения	41
3.9 Установка программного средства «Криптографический модуль Aladdin JCP».....	41
4 Установка программы.....	42
4.1 Распаковка инсталляционного комплекта	42
4.2 Настройка конфигурации программы	43
4.3 Создание и настройка базы данных.....	50
4.3.1 Создание и настройка базы данных в автоматическом режиме.....	50
4.3.2 Создание и настройка базы данных PostgreSQL в ручном режиме	51
4.3.3 Создание и настройка базы данных Jatoba в ручном режиме.....	52

4.4 Установка программы.....	53
4.1 Порядок совместной установки программы с другими компонентами Центра сертификатов доступа на одном сервере.....	54
5 Запуск и завершение программы.....	55
6 Подключение к веб-интерфейсу.....	57
6.1 Общие сведения	57
6.2 Установка сертификата администратора.....	58
6.3 Подключение к веб-интерфейсу.....	60
6.4 Аутентификация с использованием сертификата	61
6.5 Аутентификация по имени и паролю учетной записи.....	62
6.6 Аутентификация с использованием Kerberos-билета.....	63
6.7 Завершение рабочей сессии пользователя.....	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».....	67
7.4.1 Управление экранной таблицей	69
7.4.2 Фильтрация заявок.....	70
7.4.3 Сортировка заявок	70
7.4.4 Поиск заявок.....	71
7.4.5 Карточка заявки	71
7.4.6 Создание заявки на основании запроса	76
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».....	91
7.5.1 Вкладка «Учётные записи еСА».....	91
7.5.2 Вкладка «Получатели сертификатов».....	91
7.5.3 Блокировка доменной учётной записи.....	92
7.5.4 Активация доменной учётной записи.....	92
7.6 Раздел «Журнал событий».....	93
7.6.1 О журнале событий	93
7.6.2 Просмотр записей журнала событий.....	94
7.6.3 Просмотр карточки события.....	97
7.6.4 Экспорт записей журнала событий.....	98
7.6.5 Передача информации о событиях в сторонние системы по протоколу Syslog	98
7.7 Раздел «Управление»	101
7.7.1 Вкладка «Правила выпуска».....	101
7.7.2 Вкладка «SCEP».....	112
7.8 Смена сертификата веб-сервера	119
7.9 Просмотр информации о разрешённых издателях.....	121
8 Поддержка протокола SCEP.....	122
8.1 Настройка SCEP-сервера.....	122
8.2 Обработка запросов по протоколу SCEP	123
8.2.1 Обработка запроса клиента PKCSReq/RenewalReq.....	123
8.2.2 Обработка запроса клиента CertPoll.....	124

8.2.3 Обработка запроса клиента GetCert	124
8.2.4 Обработка запроса клиента GetCRL.....	124
8.2.5 Обработка запроса клиента GetCACert.....	124
8.2.6 Обработка запроса клиента GetCACaps.....	124
9 Поддержка протоколов MS-XCER и MS-WSTEP	125
9.1 Обработка запроса на политики «GetPolicies».....	125
9.2 Обработка запроса на выпуск сертификата «RequestSecurityToken»	127
9.3 Создания политики регистрации сертификатов	128
9.4 Запрос нового сертификата	130
9.5 Перевыпуск сертификатов.....	131
10 Офлайн выпуск сертификатов	132
10.1 Поддерживаемые расширения и кодировки файлов запросов	132
10.2 Сценарий офлайн выпуска сертификатов	132
10.3 Включение офлайн выпуска сертификатов.....	133
10.4 Отключение офлайн выпуска сертификатов	133
11 Контроль целостности исполняемых файлов программы	134
12 Сбор диагностической информации	135
13 Резервное копирование и восстановление данных.....	137
13.1 Резервное копирование данных	137
13.2 Настройка расписания резервного копирования.....	137
13.3 Восстановление данных из резервной копии.....	138
14 Обновление программы.....	139
15 Удаление программы	141
16 Удаление базы данных Postgres.....	142
16.1 Удаление базы данных.....	142
16.2 Удаление пользователя базы данных	142
17 Поиск и устранение неисправностей	143
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, SberLinux OS Server 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	151
4.1 Развертывание кластера в виртуальной среде с холодным резервированием «active-passive»	151
4.2 Развертывание кластера с холодным резервированием «active-passive».....	153
4.3 Развертывания кластера в виртуальной среде с горячим резервированием «active-active»	156
4.4 Развертывание кластера с горячим резервированием «active-active»	158
4.3 Обновление ПО узлов кластера	161
Приложение 5. Настройка Kerberos в веб-браузере	162
5.1 Настройка веб-браузера Firefox	162
5.2 Настройка веб-браузера Chromium.....	163
Приложение 6. Перечень регистрируемых событий	164
6.1 События запуска и остановки служб	164
6.2 События аутентификации пользователей.....	164
6.3 События работы с УЗ получателей сертификатов.....	165
6.4 События работы с заявками.....	166

6.5 События работы с ключевыми носителями	169
6.6 События экспорта	169
6.7 События работы с правилами выпуска.....	170
6.8 События работы с веб-сервером и издателями.....	171
6.9 События Offline-выпуска	172
6.10 События работы с резервными копиями	172
6.11 События контроля целостности.....	173
6.12 События архивации и очистки записей аудита	173
6.13 События работы с Syslog	173
Приложение 7. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP»	175
Перечень документации для ознакомления	177
Обозначения и сокращения.....	178
Термины и определения	179
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ	181

1 ВВЕДЕНИЕ

1.1 Назначение программы

Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» 33714370.03.01.009 входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG» 33714370.03.01.001, которое применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификацию при управлении доступом субъектов¹ доступа к объектам² доступа в автоматизированной (информационной) системе.

Центр регистрации Aladdin eRA предназначен для обработки заявок на выпуск сертификатов безопасности (цифровых сертификатов)³, выпускаемых программным комплексом «Центр сертификации Aladdin Enterprise Certification Authority»⁴ 33714370.03.01.003 из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG».

1.2 Состав программы

Центра регистрации Aladdin eRA является клиент-серверным веб-приложением и состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра регистрации»⁵ 33714370.03.01.010.

Программный компонент реализует функции Центра регистрации Aladdin eRA, 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»⁶ 33714370.03.01.011.

Программный компонент реализует интерфейс, с помощью 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)⁷.
 - Создание заявок через программный интерфейс по протоколу Simple Certificate Enrollment Protocol (SCEP)⁸.

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

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

³ Далее по документу - сертификаты.

⁴ Далее по документу - Центр сертификации Aladdin eCA.

⁵ Далее по документу - Серверная часть программы.

⁶ Далее по документу - Клиентская часть программы.

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

⁸ В соответствии с документом «RFC 8894. Simple Certificate Enrollment Protocol».

- 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.
- Регистрация, хранение, просмотр и хранение записей аудита, а также их публикация по протоколу Syslog.
- Управление профилями³ и политиками SCEP, в том числе:
 - Создание, изменение и удаление SCEP-политик, а также управления их статусами.
 - Создание, остановка, запуск и удаление SCEP-профилей.

1.4 Роли управления

Роли определяют полномочия пользователей при работе с 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 и Центру сертификации Aladdin eCA.

В Центре регистрации Aladdin eRA определены следующие роли:

- Администратор.

Пользователь с данной ролью обладает максимальными полномочиями. Пользователь с данной ролью может взаимодействовать с Центром регистрации Aladdin eRA через веб-интерфейс и программный интерфейс API¹. Идентификация и аутентификация пользователей с данной ролью выполняется по сертификату, выпущенному в Центре сертификации Aladdin eCA.

- Оператор.

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

Пользователь с данной ролью может взаимодействовать с Центром регистрации Aladdin eRA через веб-интерфейс и программный интерфейс API ¹. Пользователь с данной ролью имеет может подавать заявки для любых субъектов, просматривать свои заявки, просматривать и обрабатывать заявки для доступных ему субъектов². Идентификация и аутентификация пользователей с данной ролью выполняется по сертификату, выпущенному в Центре сертификации Aladdin eCA.

- Получатель сертификатов.

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

- Аноним (анонимный субъект доступа).

Пользователь с данной ролью может управлять Центром регистрации Aladdin eRA через программный интерфейс по протоколу SCEP, а также путем размещения заявок на выпуск сертификатов в удаленном сетевом каталоге (офлайн выпуск сертификатов). Идентификация пользователей с данной ролью выполняется по атрибуту «ChallengePassword» SCEP-запроса на регистрацию при подключении через программный интерфейс по протоколу SCEP и по атрибуту «Common Name», содержащемуся в запросе на выпуск сертификата, при офлайн выпуске сертификатов. Аноним (анонимный субъект доступа) процедуру аутентификации не проходит.

Доступные действия для существующих ролей пользователей Центра регистрации Aladdin eRA приведены в таблице 1.

Таблица 1 - Полномочия пользователей Центра регистрации Aladdin eRA

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей			
	Аноним	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	-	-	-	✓
Получение статуса своих заявок по протоколу SCEP	✓	-	-	-
Создание заявок на выпуск сертификатов для субъекта своей учётной записи	-	✓	✓	✓
Создание заявок на выпуск сертификатов для субъекта любой учётной записи	-	-	✓	✓

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

² Доступ пользователя с ролью «Оператор» к субъектам определяется в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA.

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей			
	Аноним	Получатель сертификатов	Оператор	Администратор
Создание заявок на выпуск сертификатов по протоколу SCEP (PKCS#7)	✓	-	-	-
Скачивание файла запроса на сертификат для своих заявок на выпуск сертификата по запросу	-	✓	✓	✓
Скачивание файла запроса на сертификат для ограниченного набора чужих заявок на выпуск сертификата по запросу	-	-	✓	✓
Скачивание файла запроса на сертификат для всех заявок на выпуск сертификата по запросу	-	-	-	✓
Скачивание сертификата для своих заявок	-	✓	✓	✓
Скачивание сертификата для своих заявок по протоколу SCEP	✓	-	-	-
Скачивание сертификата для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание сертификата для всех заявок	-	-	-	✓
Отзыв сертификатов для своих заявок	-	✓	✓	✓
Отзыв сертификатов для ограниченного набора чужих заявок	-	-	✓	✓
Отзыв сертификатов для всех заявок	-	-	-	✓
Скачивание цепочки сертификатов для своих заявок	-	✓	✓	✓
Скачивание цепочки сертификатов для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание цепочки сертификатов для всех заявок	-	-	-	✓
Скачивание контейнера закрытого ключа PKCS#12 для своих заявок	-	✓	✓	✓
Скачивание контейнера закрытого ключа PKCS#12 для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание контейнера закрытого ключа PKCS#12 для всех заявок	-	-	-	✓
Импорт сертификата на ключевой носитель для своих заявок	-	✓	✓	✓
Импорт сертификата на ключевой носитель для ограниченного набора чужих заявок	-	-	✓	✓
Импорт сертификата на ключевой носитель для всех заявок	-	-	-	✓
Скачивание цепочки сертификатов издателя для своих заявок	-	✓	✓	✓
Скачивание цепочки сертификатов издателя для ограниченного набора чужих заявок	-	-	✓	✓
Скачивание цепочки сертификатов издателя для всех заявок	-	-	-	✓
Скачивание списка отозванных сертификатов	-	✓	✓	✓
Скачивание списка отозванных сертификатов по протоколу SCEP	✓	-	-	-
Отмена своих заявок	-	✓	✓	✓
Обработка ограниченного набора заявок	-	-	✓	✓
Обработка всех заявок	-	-	-	✓
Настройка офлайн выпуска сертификатов по запросам	-	-	-	✓
Офлайн выпуск сертификатов по запросам	✓	-	-	✓
Просмотр учётных записей	-	-	-	✓

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

1.5 Режимы функционирования программы

Основным режимом функционирования Центра регистрации Aladdin eRA 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»¹, с которым взаимодействует Центр регистрации Aladdin eRA.

Сетевой режим работы обеспечивает возможность кластеризации Центра регистрации Aladdin eRA с целью повышения отказоустойчивости².

¹ Входит в состав программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority».

² 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, конфигурация «Сервер».
 - РЕД ОС версия 8, конфигурация «Сервер».
 - Альт 8 СП, релиз 10, вариант исполнения Сервер.
 - Platform V SberLinux OS Server.
- Поддерживаемые СУБД:
 - PostgreSQL из состава ОС.
 - Postgres Pro.
 - Jatoba.
- Поддерживаемые среды исполнения Java:
 - Java Axiom JDK Certified (компонент JRE).
 - OpenJDK версии 17 и выше из состава поддерживаемых ОС.
- Поддерживаемые веб-серверы:
 - Apache2 из состава ОС.
 - Nginx из расширенного репозитория.
 - Cpnginx ¹
- Поддерживаемые ресурсные системы (доменные службы каталогов):
 - Samba DC.
 - Free IPA.
 - ALD PRO.
 - РЕД АДМ.
 - Microsoft AD.
 - Альт Домен.
- Поддерживаемый Центр сертификации Aladdin eCA версии 2.3.0 ².
- Поддерживаемые криптопровайдеры, обеспечивающие формирование электронной подписи ответов службы OCSP по алгоритму ГОСТ Р 34.10-2012:

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

² Входит в состав программного средства.

- Программное средство «Криптографический модуль Aladdin JCP» ¹.
- СКЗИ «КриптоПро CSP» ²
- средство криптографической защиты информации «КриптоПро CSP».

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, конфигурация «Сервер».
 - РЕД ОС версия 8, конфигурация «Сервер».
 - Альт 8 СП, релиз 10, вариант исполнения Сервер.
 - Platform V SberLinux OS Server.
- Веб-браузер из состава ОС.
- JC-WebClient последней версии (для 64-битных систем) ³.
- ПО «Рутокен Плагин» и браузерное расширение «Адаптер Рутокен Плагин»⁴.

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 и мышь.
- USB 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей:
 - JaCarta:
 - JaCarta PKI.
 - JaCarta PRO.
 - JaCarta-2 PKI/ГОСТ.
 - JaCarta-2 ГОСТ.

¹ Входит в состав программного средства.

² СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в состав и комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно. Порядок настройки взаимодействия Центра валидации Aladdin eVA с СКЗИ «КриптоПро CSP» описан в приложении 5 настоящего руководства.

³ JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) JaCarta. Официальный сайт производителя [JC-WebClient](#).

⁴ ПО «Рутокен Плагин» через браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) Рутокен. Официальный [сайт производителя](#).

- JaCarta-3.
- Рутокен ¹:
 - Рутокен ЭЦП 3.0.
 - Рутокен ЭЦП 2.0.
 - Рутокен ЭЦП 2.0 Flash.
 - Рутокен ЭЦП PKI.

¹ Возможность использования ключевых носителей Рутокен может быть ограничена лицензией.

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 выполняется путём редактирования конфигурационного файла Центра регистрации Aladdin eRA (см. раздел 4.2).

В таблице ниже (Таблица 2) приведён список портов, которые должны быть открыты в Центре регистрации Aladdin eRA и взаимодействующих компонентах.

Таблица 2 - Таблица сетевого взаимодействия

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

В таблице ниже (Таблица 3) приведен список портов, которые используются в Центре 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 внутренних 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 «sa-adapter-service» (адаптер для подключения к программе)
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)

Порт	Транспорт	Протокол	Назначение
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 программы)
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)
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 Центра регистрации Aladdin eRA заключается в установке и настройке следующего ПО:

- Зависимостей и подключение репозитория ОС.
- Среды исполнения Java.
- СУБД.
- Веб-сервера.
- JC-WebClient (при необходимости работы с электронными ключами JaCarta).
- ПО «Рутокен Плагин» и браузерное расширение «Адаптер Рутокен Плагин» (при необходимости работы с электронными ключами Рутокен).
- Программного средства «Криптографический модуль Aladdin JCP» (при необходимости подписи маркеров доступа пользователей Центра сертификации Aladdin eCA по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит).

Предварительно необходимо выполнить следующие действия:

- Ввести компьютер, на котором будет выполнена установка Центра регистрации Aladdin eRA, в домен ресурсной системы (доменной службы каталогов).
- Создать службу HTTP и keytab-файл ¹ на контроллере домена ресурсной системы (см. раздел 3.5).

¹ Keytab-файл используется для аутентификации доменных пользователей в Центре регистрации Aladdin eRA с использованием Kerberos-билетов без ввода пароля.

- Создать в Центре сертификации Aladdin eCA технологическую учетную запись с правами «Администратор» для взаимодействия Центра регистрации Aladdin eRA с Центром сертификации Aladdin eCA, выпустить для нее сертификат по шаблону «User» и выгрузить контейнер PKCS#12 ¹.
- Создать в Центре сертификации Aladdin eCA субъект для веб-сервера Центра регистрации Aladdin eRA, выпустить для него сертификат по шаблону «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». При этом в Центре регистрации Aladdin eRA необходимо применять СКЗИ «КриптоПро CSP» для:

- Организации канала взаимодействия Серверных частей Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA по протоколу TLS ГОСТ.
- Организации канала взаимодействия Клиентской и Серверной части 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.

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 3.6. После установки веб-сервера необходимо установить на СКЗИ «КриптоПро CSP» серверную лицензию, обеспечивающую возможность использования СКЗИ «КриптоПро CSP» в качестве TLS-сервера.
- Сертификаты для веб-сервера и учетной записи с ролью «Администратор» для взаимодействия с Центром сертификации Aladdin eCA должны быть выпущены по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 Бит.

3.1 Подготовка среды функционирования с ОС РЕД ОС

3.1.1 Подключение репозитория и установка зависимостей

Для РЕД ОС репозитории настроены по умолчанию для загрузки зависимостей из сети Интернет. Установите необходимые пакеты из состава ОС, выполнив следующую команду с правами суперпользователя:

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

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

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

¹ Порядок создания субъектов, учетных записей и выпуска сертификатов приведен в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».

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

3.1.2 Установка среды исполнения Java

3.1.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified 17 воспользуйтесь [инструкцией с официального сайта производителя](#).

Внимание! В РЕД ОС Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

3.1.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС:

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

Внимание! В РЕД ОС OpenJDK определенных версий работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена для OpenJDK версий 17.0.15.0.6 и 21.0.7.0.6.

3.1.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в Приложении 1.

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

Центр регистрации Aladdin eRA может быть настроен на взаимодействие с СУБД по протоколу TLS.

Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведен в Приложении 3.

3.1.3.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

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

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

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

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

- Произведите инициализацию БД, выполнив следующую команду с правами суперпользователя:

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

В случае ошибки `Data directory in '/var/lib/pgsql/data' is not empty...` следует очистить каталог командой с правами суперпользователя `sudo rm -rf /var/lib/pgsql/data` и повторить инициализацию БД.

- Запустите PostgreSQL, выполнив следующую команду с правами суперпользователя:

¹ Подробное описание приведено на [официальном сайте производителя](#).

```
sudo systemctl start postgresql
```

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

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`¹, установив число подключений `max_connections` в значение `1000`².
- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`³, изменив следующие параметры для успешного локального подключения пользователя к БД:

```
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
```

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

```
sudo systemctl restart postgresql
```

3.1.3.2 Установка СУБД Postgres Pro⁴

Порядок установки СУБД Postgres Pro:

Загрузите скрипт для добавления репозитория, выполнив следующую команду⁵:

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

- Запустите скрипт, выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов, выполнив следующую команду с правами суперпользователя:

```
sudo dnf update
```

- Установите Postgres Pro, выполнив следующую команду с правами суперпользователя:

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`⁶, установите число подключений `max_connections` в значение `1000`⁷.
- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`⁸, изменив следующие параметры для успешного локального подключения пользователя к БД:

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

¹ Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

² Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

³ Расположение файла может отличаться, для поиска файла можно использовать команду `sudo find / -type f -name pg_hba.conf`

⁴ Подробное описание приведено на [официальном сайте производителя](#).

⁵ Команды ниже приведены для Postgres Pro версии 16.

⁶ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁷ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁸ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

```
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 следующие команды с правами суперпользователя:

```
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 следующую команду с правами суперпользователя:

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

3.1.3.3 Установка СУБД Jatoba ¹

Порядок установки СУБД Jatoba:

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

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

- Дистрибутив СУБД Jatoba содержит:
 - Каталог `/packages`.
 - Каталог `/repopdata`.
 - 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, выполнив следующую команду с правами суперпользователя:

```
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:///localrepo/RPM-GPG-KEY-Jatoba
```

- Обновите описания пакетов, выполнив следующую команду с правами суперпользователя:

```
sudo dnf makecache
```

¹ Подробное описание приведено на [официальном сайте производителя](#).

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf`, установив число подключений `max_connections` в значение `1000`¹.
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf`, изменив параметры для успешного локального подключения пользователя к БД:

```
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, следующую команду с правами суперпользователя:

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

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

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

3.1.4 Установка веб-сервера

3.1.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив следующую команду с правами суперпользователя:

```
sudo dnf install httpd
```

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

```
sudo dnf install mod_ssl
```

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

```
sudo systemctl enable httpd
```

3.1.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

¹ Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

```
sudo dnf install nginx
```

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

```
sudo systemctl start nginx
```

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

```
sudo systemctl enable nginx
```

3.2 Подготовка среды функционирования с ОС Astra Linux SE

3.2.1 Подключение репозитория и установка зависимостей

3.2.1.1 Подключение репозитория и установка зависимостей Astra Linux Special Edition 1.7 ¹

Порядок подключения репозитория и зависимостей:

- Для установки зависимостей через сеть Интернет перед началом установки компонентов необходимо установить пути нахождения необходимых репозиториях², отредактировав файл `/etc/apt/sources.list`, выполнив следующую команду с правами суперпользователя:

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

- Укажите ссылки на следующие репозитории ³:

```
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:

```
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 оптических дисков в качестве репозитория, отредактировав файл `/etc/apt/sources.list`. Пример:

```
deb cdrom:[OS Astra Linux 1.7.6 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib main non-free
```

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

```
apt-cdrom add
```

- Выполните обновление пакетов для ОС из указанных репозиториях, выполнив следующую команду с правами суперпользователя:

```
sudo apt update
```

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

```
sudo apt install tar unzip iptables
```

¹ Подробнее см. на [официальном сайте производителя](#).

² Ссылки на репозитории приведены для Astra Linux SE версии 1.7.6

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

В процессе установки в офлайн режиме может потребоваться замена оптических дисков с нужным репозиторием («диск 1», «диск 2», «develop»).

3.2.1.2 Подключение репозитория и установка зависимостей Astra Linux Special Edition 1.8¹

Порядок подключения репозитория и зависимостей:

- Для обновления посредством сети Интернет перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториях², отредактировав файл `/etc/apt/sources.list`, выполнив следующую команду с правами суперпользователя:

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

- Укажите ссылки на следующие репозитории:

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

- Укажите нижеприведённый репозиторий для развёртывания веб-сервера Nginx:

```
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 репозитория, отредактировав файл `/etc/apt/sources.list`. Пример:

```
deb cdrom:[OS Astra Linux 1.7.6 1.7_x86-64 DVD ]/ 1.7_x86-64 contrib main non-free
```

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

```
apt-cdrom add
```

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

```
sudo apt update
```

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

```
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 в [активном режиме замкнутой программной среды \(далее - ЗПС\)](#). Для этого в состав установочных пакетов программного комплекса включен публичный открытый ключ ОсОО «Аладдин КГ» - `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 переместить³ в каталог `/etc/digsig/keys/`.

¹ Подробнее см. на [официальном сайте производителя](#).

² Ссылки на репозитории приведены для Astra Linux SE 1.8.1

³ Данное действие необходимо выполнять после распаковки установочных пакетов Центра сертификации Aladdin eCA.

3.2.2 Установка среды исполнения Java

3.2.2.1 Установка Axiom JDK

Для установки Axiom JDK Certified воспользуйтесь [инструкцией с официального сайта производителя](#).

Внимание! В Astra Linux Special Edition Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

3.2.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС:

- [Инструкция для Astra Linux SE 1.7](#) (в инструкции описана установка Open JDK 11, установка Open JDK 17 и 21 аналогична).
- [Инструкция для Astra Linux SE 1.8](#) (в инструкции описана установка Open JDK 17, установка Open JDK 21 аналогична).

3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в Приложении 1.

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

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

3.2.3.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

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

```
sudo apt install postgresql
```

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

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

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

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

- Запустите PostgreSQL, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl start postgresql
```

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

```
sudo systemctl enable postgresql
```

¹ Подробное описание приведено на [официальном сайте производителя](#).

- При наличии мандатных политик¹:
 - выдайте полномочия пользователю `postgres`, выполнить следующую команду с правами суперпользователя:

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

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

```
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 `/etc/postgresql/11/main/postgresql.conf`², установите число подключений `max_connections` в значение `1000`³.
- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl restart postgresql
```

3.2.3.2 Установка СУБД Postgres Pro⁴

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив следующую команду⁵:

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

- Запустите скрипт, выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов, выполнив следующую команду с правами суперпользователя:

```
sudo dnf update
```

- Установите Postgres Pro, выполнив следующую команду с правами суперпользователя:

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

- При наличии мандатных политик⁶:
 - 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 следующие команды с правами суперпользователя:

```
sudo usermod -a -G shadow postgres
```

¹ Подробная информация по аутентификации в СУБД PostgreSQL приведена на [официальном сайте производителя](#).

² 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`

³ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁴ Подробное описание приведено на [официальном сайте производителя](#).

⁵ Команды ниже приведены для Postgres Pro версии 16.

⁶ Подробная информация по аутентификации в СУБД PostgreSQL приведена на [официальном сайте производителя](#).

```
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`¹, установив число подключений `max_connections` в значение `1000`².
- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив следующие команды с правами суперпользователя:

```
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 следующую команду с правами суперпользователя:

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

3.2.3.3 Установка СУБД Jatoba³

Порядок установки СУБД Jatoba:

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

```
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 оптической записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «`localrepo`» на всех шагах установки указывать соответствующий путь до носителя оптической записи и директорию репозитория СУБД на носителе оптической записи 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, выполнив следующую команду с правами суперпользователя:

```
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, выполнив следующую команду с правами суперпользователя:

```
sudo apt update
```

¹ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

² Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

³ Подробное описание приведено на [официальном сайте производителя](#).

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

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

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

- При наличии мандатных политик ¹:
 - выдайте полномочия пользователю `postgres`, выполнить следующую команду с правами суперпользователя:

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

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

```
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
```

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf`, установив число подключений `max_connections` в значение `1000`².
- Добавьте СУБД Jatoba в автозагрузку, выполнив следующую команду с правами суперпользователя:

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

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

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

3.2.4 Установка веб-сервера

3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив следующую команду с правами суперпользователя:

```
sudo apt install apache2
```

- Активируйте модули, выполнив поочередно следующие команды с правами суперпользователя:

```
sudo a2enmod ssl
sudo a2enmod proxy
```

¹ Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена на [официальном сайте производителя](#).

² Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

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

- Перезагрузите веб-сервер, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl restart apache2
```

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

```
sudo systemctl enable apache2
```

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

```
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:

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

```
sudo apt install nginx
```

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

```
sudo systemctl start nginx
```

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

```
sudo systemctl enable nginx
```

3.3 Подготовка среды функционирования с Альт Сервер

3.3.1 Подключение репозитория и установка зависимостей

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

```
sudo nano /etc/apt/sources.list.d/aptsr.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 следующую команду с правами суперпользователя:

```
sudo apt-get update
```

3.3.2 Установка среды исполнения Java

3.3.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified 17 воспользуйтесь [инструкцией с официального сайта производителя](#).

Для установки Axiom JDK Certified 21 воспользуйтесь [инструкцией с официального сайта производителя](#).

3.3.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с [официального сайта производителя ОС](#).

3.3.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в Приложении 1.

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

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

3.3.3.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив следующую команду с правами суперпользователя²:

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

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

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

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

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

- Произведите инициализацию БД, выполнив следующую команду с правами суперпользователя:

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

В случае ошибки `Data directory in '/var/lib/pgsql/data' is not empty...` следует очистить каталог командой с правами суперпользователя `sudo rm -rf /var/lib/pgsql/data` и повторить инициализацию БД.

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

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

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/15/data/postgresql.conf`³, установив число подключений `max_connections` в значение `1000`⁴.

¹ Подробное описание приведено на [официальном сайте производителя](#).

² Команды ниже приведены для версии PostgreSQL версии 15.

³ Расположение файла может отличаться. В инструкции расположение указано для 15 версии PostgreSQL. Для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁴ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

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

```
sudo systemctl restart postgresql
```

3.3.3.2 Установка СУБД Postgres Pro¹

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду ²:

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

- Запустите скрипт, выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов, выполнив следующую команду с правами суперпользователя:

```
sudo apt-get update
```

- Установите Postgres Pro, выполнив следующую команду с правами суперпользователя:

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`³ с правами администратора - установите число подключений `max_connections` в значение `1000`⁴.
- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив следующие команды с правами суперпользователя:

```
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 следующую команду с правами суперпользователя:

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

3.3.3.3 Установка СУБД Jatoba⁵

Порядок установки СУБД Jatoba:

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

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

- Дистрибутив СУБД Jatoba содержит:

- Каталог `/base`.

¹ Подробное описание приведено на [официальном сайте производителя](#).

² Команды ниже приведены для Postgres Pro версии 16.

³ Расположение файла указано для Postgres Pro версии 16, для поиска файла можно использовать команду `sudo find / -type f -name postgresql.conf`

⁴ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁵ Подробное описание приведено на [официальном сайте производителя](#).

- 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, выполнив следующую команду с правами суперпользователя:

```
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, выполнив следующую команду с правами суперпользователя:

```
sudo apt-get update
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf`, установив число подключений `max_connections` в значение `1000`¹.
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf`, изменив параметры для успешного локального подключения пользователя к БД:

```
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, выполнив следующую команду с правами суперпользователя:

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

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

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

¹ Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

3.3.4 Установка веб-сервера

3.3.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив следующую команду с правами суперпользователя:

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

- Установите модуль SSL, выполнив следующую команду с правами суперпользователя:

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

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

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

- Внесите следующий текст в созданный файл:

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

- Создайте следующий файл `/etc/httpd2/conf/mods-available/http2.conf` выполнив следующую 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 следующие команды с правами суперпользователя:

```
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 следующую 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 следующую команду с правами суперпользователя:

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

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

```
sudo systemctl start nginx
```

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

```
sudo systemctl enable nginx
```


3.4 Подготовка среды функционирования с Platform V SberLinux OS Server

3.4.1 Установка среды исполнения Java

3.4.1.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь [инструкцией с официального сайта производителя](#).

Внимание! В Platform V SberLinux OS Server Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

3.4.1.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией по установке пакета [с официального сайта Platform V SberLinux OS Server](#).

Внимание! В ОС «Platform V SberLinux OS Server» OpenJDK определенных версий работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена для OpenJDK версий 17.0.15.0.6 и 21.0.7.0.6.

3.4.2 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в Приложении 1.

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

Центр сертификации Aladdin eCA может быть настроено на взаимодействие с СУБД по протоколу TLS.

Программа не будет функционировать, если ему не удалось установить TLS-соединение с СУБД. Порядок настройки TLS-соединения с СУБД приведен в Приложении 3.

3.4.2.1 Установка СУБД PostgreSQL¹

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 каталог командой ниже и повторить инициализацию БД.

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

¹ Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>.

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`¹ под администратором - установите число подключений `max_connections` в значение `1000`².
- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`³ 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
```

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

```
sudo systemctl restart postgresql
```

3.4.2.2 Установка СУБД Postgres Pro⁴

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду⁵:

```
wget --user [ключ] --password='' https://repo.postgrespro.ru/std/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`⁶ под администратором - установите число подключений `max_connections` в значение `1000`⁷.
- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`⁸ 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
```

¹ Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

² Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

³ Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

⁴ Подробное описание приведено в официальной документации на Postgres Pro, размещённой по адресу <https://postgrespro.ru/docs>

⁵ Команды ниже приведена для Postgres Pro версии 16.

⁶ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁷ Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁸ Расположение файла указано для 16 версии Postgre Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

- 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
```

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

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

3.4.2.3 Установка СУБД Jatoba¹

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

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

- Дистрибутив СУБД Jatoba содержит:
 - каталог `/packages`;
 - каталог `/repdata`;
 - 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:///localrepo/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
```

Внимание! 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:

¹ Подробное описание приведено в официальной документации на [Jatoba](#).

```
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`¹.
- 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]
```

3.4.3 Установка веб-сервера

3.4.3.1 Установка веб-сервера Apache

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

```
sudo dnf install httpd
```

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

```
sudo dnf install mod_ssl
```

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

```
sudo systemctl enable httpd
```

3.4.3.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
sudo dnf install nginx
```

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

```
sudo systemctl start nginx
```

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

```
sudo systemctl enable nginx
```

3.5 Создание службы HTTP и keytab-файла

Внимание! В Центре регистрации Aladdin eRA предварительно должен быть настроен Kerberos - файл `krb5.conf` (рекомендуется располагать файл в каталоге `/etc`). При

¹ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

изменении HTTP-службы или при подключении Центра регистрации Aladdin eRA к другому домену необходимо заменять keytab-файл.

3.5.1 Получение keytab-файла в Samba DC и Альт Домен

Порядок создания HTTP-службы и получения keytab-файла:

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

```
ssh <username>@<ip_address> -p <порт>
```

где **<username>** - логин пользователя контроллера домена, **<ip-address>** - IP-адрес контроллера домена, **<порт>** - порт подключения по SSH (по умолчанию 22).

- Перейдите в режим суперпользователя, выполнив команду: **su**
- Создайте пользователя-службу, который будет использоваться для авторизации в LDAP, выполнив команду ¹: **samba-tool user create <UPN пользователя-службы> --random-password**
- Разблокируйте созданного пользователя, выполнив команду:

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

Имя учетной записи пользователя-службы необходимо указывать в формате RFC822Name.

- С сервера, на котором выполняется установка Центра регистрации Aladdin eRA, 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 ²:

```
net ads enttypes set <имя пользователя-службы> 28 -U <имя администратора>
```

- 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 сервера, на котором выполняется 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 сервера, на котором выполняется 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 сервера, на котором выполняется 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:

¹ При подключении нескольких Центров регистрации Aladdin eRA к одному контроллеру домена рекомендуется создать пользователя-службу для каждого Центра регистрации Aladdin eRA.

² В команде ниже **administrator** - это пользователь с правами администратора.

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

где:

- <путь к файлу> - путь к созданному http.keytab-файлу;
- <имя пользователя> - имя пользователя сервера, на котором выполняется установка Центра регистрации Aladdin eRA;
- <имя сервера (ip-адрес)> - укажите полное имя или IP-адрес сервера, на котором выполняется 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 следующую команду с правами суперпользователя:

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

3.5.2 Получение keytab-файла в ALD PRO

Порядок создания HTTP-службы и получения keytab-файла:

- На контроллере домена авторизуйтесь в веб-интерфейсе ALD PRO. Для этого введите в адресной строке веб-браузера: `https://<адрес контроллера домена>/ad/ui/#/`
- Перейдите в раздел «Управление доменом» -> «Службы и параметры Kerberos» в веб-интерфейсе или введите в адресной строке веб-браузера:

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

- Нажмите кнопку «Новая служба», в списке «Класс службы» выберите «HTTP», в списке «Имя компьютера» выберите доменное имя сервера, на котором выполняется установка Центра регистрации Aladdin eRA. Сохраните изменения, нажав кнопку «Да».
- С сервера, на котором выполняется установка Центра регистрации Aladdin eRA, получите Kerberos-билет администратора домена, выполнив команду:

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

- Экпортируйте Kerberos-билет HTTP-службы на настраиваемый сервер по рекомендованному пути `/etc/http.keytab`, выполнив следующую команду с правами суперпользователя:

```
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`

3.5.3 Получение keytab-файла в Free IPA

Порядок создания HTTP-службы и получения keytab-файла:

- На контроллере домена авторизуйтесь в веб-интерфейсе Free IPA. Для этого введите в адресной строке веб-браузера: `https://<имя контроллера домена>/ipa/ui/#/`
- Перейдите в веб-интерфейсе в раздел «Идентификация» -> «Службы» или введите в адресной строке веб-браузера: `https://<имя контроллера домена>/ipa/ui/#/e/service/search`
- Нажмите кнопку «Добавить», в списке «Служба» выберите «HTTP», в списке «Имя узла» выберите доменное имя сервера, на котором выполняется установка Центра регистрации Aladdin eRA. Сохраните изменения, нажав кнопку «Добавить».

- С сервера, на котором выполняется установка Центра регистрации Aladdin eRA, получите Kerberos-билет администратора домена, выполнив команду:

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

- Экпортируйте Kerberos-билет HTTP-службы на настраиваемый сервер по рекомендованному пути `/etc/http.keytab`, выполнив следующую команду с правами суперпользователя:

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

- Измените права на созданный keytab-файл (доступ на чтение и перезапись для всех), выполнив следующую команду с правами суперпользователя: `sudo chmod 666 /etc/http.keytab`

3.5.4 Получение keytab-файла в MS AD

Порядок создания HTTP-службы и получения keytab-файла:

- На контроллере домена MS AD запустите консоль управления «Active Directory Users and Computers».
- 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 шифрование;
 - данная учётная запись поддерживает 256-разрядное шифрование.
- 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 <UPN пользователя-службы> -pass <пароль пользователя-службы> -ptype KRB5_NT_PRINCIPAL -out <расположение keytab-файла>/http.keytab -crypto all
```

где `<имя настраиваемого клиента>` - имя сервера, на котором выполняется установка Центра регистрации Aladdin eRA.

- Переместите keytab-файл на сервер, где будет установлен Центр регистрации Aladdin eRA (например, в каталог `/etc`).
- Измените права на полученный keytab-файл, выполнив следующую команду с правами суперпользователя:

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

3.6 Установка веб-сервера Cppnginx

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

Порядок установки веб-сервера `cppnginx`:

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

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

- Установите следующие пакеты:

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

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

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

- для ОС РЕД ОС и SberLinux OS Server, выполнив следующую команду с правами суперпользователя:

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

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

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

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

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

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

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

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

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

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

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

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

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

3.7 Установка JC-WebClient

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

Скачайте дистрибутив JC-WebClient [с веб-сайта производителя](#) и установите зависимости.

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

РЕД ОС и SberLinux OS Server

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

Astra Linux SE

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

Альт Сервер

```
sudo apt-get install JC-WebClient-x64-x.x.x.xxxx.rpm
```

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

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

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

```
sudo sh jcmon start
```


3.8 Установка Рутокен плагина и его расширения

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

Скачайте дистрибутив ПО «Рутокен Плагин» с [официального сайта производителя](#).

Установите ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен» по инструкции с [официального сайта производителя](#).

3.9 Установка программного средства «Криптографический модуль Aladdin JCP»

Порядок установки криптопровайдера «Aladdin JCP»:

- Получите от ОсОО «Аладдин КГ» набор файлов «Aladdin JCP».
- При отсутствии создайте каталог `/opt/aecaRa/services/cryptoproviders` командой:

```
sudo mkdir -p /opt/aecaCa/services/cryptoproviders
```

- Переместите в каталог `/opt/aecaRa/services/cryptoproviders` все файлы криптопровайдера «Aladdin JCP».
- Назначьте права доступа на скопированные файлы:
 - Если выполняется первоначальная установка Центра регистрации Aladdin eRA, то назначьте файлам права доступа (`chmod 777`).
 - Если Центр регистрации Aladdin eRA был ранее установлен, то назначьте владельцем данных файлов пользователя «аеса» и предоставьте ему права доступа к файлам (`chmod 700`).
- Выполните установку программы (см. раздел 4), если Центр регистрации Aladdin eRA не был ранее установлен.
- Если Центр регистрации Aladdin eRA был ранее установлен необходимо запустить скрипт с правами суперпользователя в режиме обновления программы:

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

4 УСТАНОВКА ПРОГРАММЫ

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

4.1 Распаковка инсталляционного комплекта

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

РЕД ОС и SberLinux OS Server

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

Astra Linux

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

Альт Сервер

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

Инсталляционный 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.
../scripts/config.sh	Конфигурационный файл Центра регистрации Aladdin eRA.
../scripts/database_create.sh	Скрипт создания базы данных Центра регистрации Aladdin eRA.

Структурный элемент	Назначение элемента
../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

Конфигурация Центра регистрации Aladdin eRA задается с помощью параметров конфигурационного файла `/opt/aecaRa/scripts/config.sh`.

Перед установкой программы требуется определить значения следующих параметров:

- `webserver` - укажите используемый веб-сервер (`nginx`, `apache` или `cprnginx`). Также значение параметра можно будет ввести после запуска инсталлятора установки, в интерактивном режиме выбрав веб-сервер.
- `webserver_path` - 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 Apache располагается для Astra Linux SE по пути `/etc/apache2`, для РЕД ОС и SberLinux OS Server - по пути `/etc/httpd`, для Альт Сервер по пути `/etc/httpd2`;
 - конфигурация Cprnginx располагается по пути `/etc/opt/cproscsp/cprnginx`.
- `database_password` - укажите пароль создаваемой базы данных (имя базы данных по умолчанию - aecaRa). После обновления с версии 2.0 до версии 2.3, а также после создания и настройки базы данных (см. раздел 4.3) пароль пользователя базы данных отображается в конфигурационном файле в зашифрованном 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 Центра регистрации Aladdin eRA с Центром сертификации Aladdin eCA.
- `kerberos_service_principal` - укажите принципал HTTP-службы, используемой для валидации Kerberos-билетов в формате `HTTP/<доменное имя стенда>.<домен>` (например, `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`.
- `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 (например, `PRESALE.AECA`).
- `kerberos_ad_server` - укажите LDAP-адрес для подключения к домену в формате `ldap://<имя контроллера домена>.<домен>` (например, `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 (например, `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 доменное 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 программе 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
<code>webserver</code>	<code>'cpnginx'</code>
<code>webserver_path</code>	<code>'/etc/opt/cprosp/cpnginx'</code>
<code>sign_provider</code>	<code>'CRYPTO_PRO'</code>
<code>sign_key_algorithm</code>	<code>'GOST_R_34_10_2012'</code>
<code>sign_key_length</code>	<code>'256' или '512'</code>
<code>sign_hash_algorithm</code>	<code>'GOST_R_34_11_2012'</code>

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

```
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 офлайн-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 таблице ниже (Таблица 6).

Таблица 6 - Описание параметров конфигурации

Параметр	Значение параметра по умолчанию	Описание
Конфигурация развёртывания		
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 РЕД ОС и SberLinux OS Server конфигурация apache располагается по пути /etc/httpd, конфигурация cpnginx располагается по пути /etc/opt/cprosp/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
encryption_key_path	'/opt/aecaRa/scripts/key'	Ключ для шифрования конфигурационного файла
proxy_connect_timeout	'320'	Время ожидания подключения к прокси-серверу перед тем, как будет выдано сообщение об ошибке. Только для Nginx. Настраивается 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.

Параметр	Значение параметра по умолчанию	Описание
ssl_protocols	'TLSv1.2 TLSv1.3'	Поддерживаемые версии протокола TLS. Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обеих версий протокола необходимо указывать их через пробел).
ssl_ciphers	По умолчанию не задано.	<p>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.</p> <p>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.</p> <p>В данном параметре могут быть указаны любые наборы шифров, поддерживаемые используемой на сервере Центра регистрации версией Openssl для TLS версии 1.2.</p> <p>Получить список поддерживаемых используемым Openssl наборов шифров для TLS версии 1.2 можно с помощью команды:</p> <pre>openssl ciphers -tls1_2 -s</pre> <p>Данный параметр учитывается только при использовании Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cprnginx осуществляется с помощью утилиты «cprconfig» из состава СКЗИ «КриптоПро CSP»¹</p>
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

¹ [Инструкция по установке и настройке cprnginx](#). Описание конфигурирования наборов шифров представлено в разделе 6.

Параметр	Значение параметра по умолчанию	Описание
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
root_cert_path	#CHANGEIT	Абсолютный путь к сертификату корневого Центра сертификации из цепочки сертификатов сервера СУБД
Конфигурация Центра регистрации		
http_port	'80'	Порт для подключения к программе 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

Параметр	Значение параметра по умолчанию	Описание
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
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 ¹
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.

¹ 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		
		Максимальное число одновременных сессий аккаунта в виде натурального числа. При указании значения «-1» ограничение на количество одновременных сессий пользователя будет отсутствовать.
session_max_count	"-1"	
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', СКЗИ «КриптоПро CSP» - 'CRYPTO_PRO' и 'ALADDIN_JCP' для киптопровайдера Aladdin JCP)
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'. Для провайдера Aladdin JCP доступен алгоритм '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): <ul style="list-style-type: none">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): <ul style="list-style-type: none">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' 3) Для провайдера Aladdin JCP (ALADDIN_JCP) для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012'
Переменные окружения, используемые сервисом logs-service		
archive_cron	'0 0 0 1 * *'	CRON-выражение, по которому запускается архивация журнала событий

Параметр	Значение параметра по умолчанию	Описание
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 БД. Это может быть выполнено одним следующих из способов:

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

После создания и настройки БД 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 БД (имя базы данных по умолчанию `aecara`) предназначена для хранения информации:

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

4.3.1 Создание и настройка базы данных в автоматическом режиме

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

Для создания и настройки БД запустите скрипт, выполнив следующую команду с правами суперпользователя ¹:

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

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

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

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 БД, используемой программой в процессе работы.
- Назначение созданному пользователю полных прав доступа к созданной БД.

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите PostgreSQL, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

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

```
sudo -u postgres psql
```

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

```
CREATE USER aeca
```

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

- Задайте пароль пользователю, выполнив команду:

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

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

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecara;
```

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

- Назначьте владельцем созданной базы данных созданного пользователя, выполнив команду:

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

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

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

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

```
exit
```

- Перезапустите СУБД PostgreSQL, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl restart postgresql
```

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

```
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 БД, используемой программой в процессе работы.
- Назначение созданному пользователю полных прав доступа к созданной БД.

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите Jatoba, выполнив следующую команду с правами суперпользователя:

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

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

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

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

РЕД ОС и SberLinux OS Server `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 БД, выполнив команду:

```
CREATE USER aeca;
```

где `aeca` - задаваемое имя пользователя.

- Задайте пароль пользователю, выполнив команду:

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

где `'aeca'` - задаваемый пароль пользователя.

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

- Создайте БД, выполнив команду:

```
CREATE DATABASE aecara;
```

где `aecara` - задаваемое имя БД.

- Назначьте владельцем созданной БД созданного пользователя, выполнив команду:

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

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

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

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

```
exit
```

- Перезапустите СУБД Jatoba, выполнив следующую команду с правами суперпользователя:

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

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

```
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 запустите скрипт с правами суперпользователя ¹:

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

При использовании Astra Linux Special Edition и наличии мандатных политик² может быть выведено сообщение:

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

В данном случае явно назначьте классификационную метку пользователю `aeca`, выполнив следующую команду с правами суперпользователя и повторно запустите скрипт установки:

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

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:

- Apache.
- Nginx.
- Cpnginx.

Выберите веб-сервер вводом соответствующей цифры.

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

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

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

В процессе установки выполняется:

- Создание системного пользователя и соответствующей группы, от имени которых функционирует Центр регистрации Aladdin eRA.

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

² Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена на [официальном сайте производителя](#).

- 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 БД ¹.

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
```

4.1 Порядок совместной установки программы с другими компонентами Центра сертификатов доступа на одном сервере

В Центре сертификатов доступа поддерживается совместная работа Центра сертификации Aladdin eCA, Центра регистрации Aladdin eRA и Центра валидации Aladdin eVA на одном сервере. Также поддерживается совместная работа Центра регистрации Aladdin eRA и Центра валидации Aladdin eVA, а также Центра регистрации Aladdin eRA и Центра сертификации Aladdin eCA на одном сервере.

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

¹ Значение номера сборки записывается в таблицу «build_info» схемы «aeca_ra_info».

5 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

Центр регистрации Aladdin eRA запускается автоматически:

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

Для проверки состояния Центра 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.

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
```

Для запуска программы выполните команду с правами суперпользователя:

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

Для перезапуска программы выполните команду с правами суперпользователя:

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

При запуске Центра регистрации Aladdin eRA выполняются следующие проверки:

- Проверка возможности подключения к базе данных. Если не удаётся подключиться к базе данных, то программа не запускается.
- Проверка соответствия номера своей сборки и значения номера сборки, указанной в базе данных¹:
 - 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
2	tasks-service.jar	Модуль заявок	Обеспечивает управление заявками на сертификаты

¹ Значение номера сборки указано в таблице «build_info» схемы «aeca_ra_info».

Порядок запуска	Исполняемый файл	Наименование	Назначение
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

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

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

Центр регистрации Aladdin eCA при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты ¹, используемые для доступа к Центру регистрации Aladdin eCA (определяются параметрами «http_port» и «https_port» конфигурационного файла /opt/aeceRa/scripts/config.sh), если данные порты не используются иными программами.

¹ Порты будут закрыты только в том случае, если они были открыты Центром регистрации Aladdin eCA.

6 ПОДКЛЮЧЕНИЕ К ВЕБ-ИНТЕРФЕЙСУ

6.1 Общие сведения

Веб-интерфейс представляет 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 аутентификацией¹ и шифрованием передаваемых данных.

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

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

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 ОС. Данный веб-браузер входит в состав базовых репозиториях ОС Astra Linux SE, Альт Сервер, РЕД ОС и SberLinux OS Server.

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

6.2 Установка сертификата администратора

Для первичной настройки программы необходимо установить сертификат учётной записи пользователя с ролью «Администратор» Центра сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, в доверенное хранилище сертификатов веб-браузера или ОС ¹.

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

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

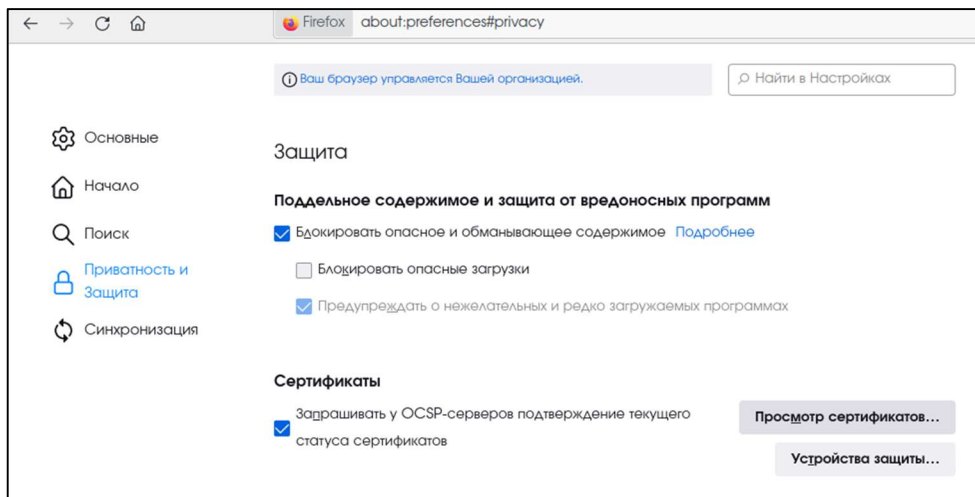


Рисунок 1 - Окно настроек браузера

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

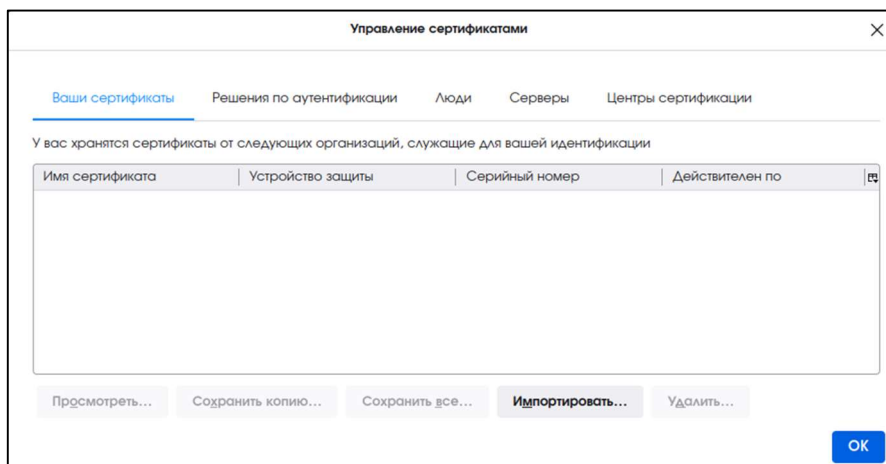


Рисунок 2 - Окно управления сертификатами

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

¹ Сертификат администратора из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, устанавливается в личное хранилище пользователя с помощью утилиты «crttools» из состава СКЗИ «КриптоПро CSP».

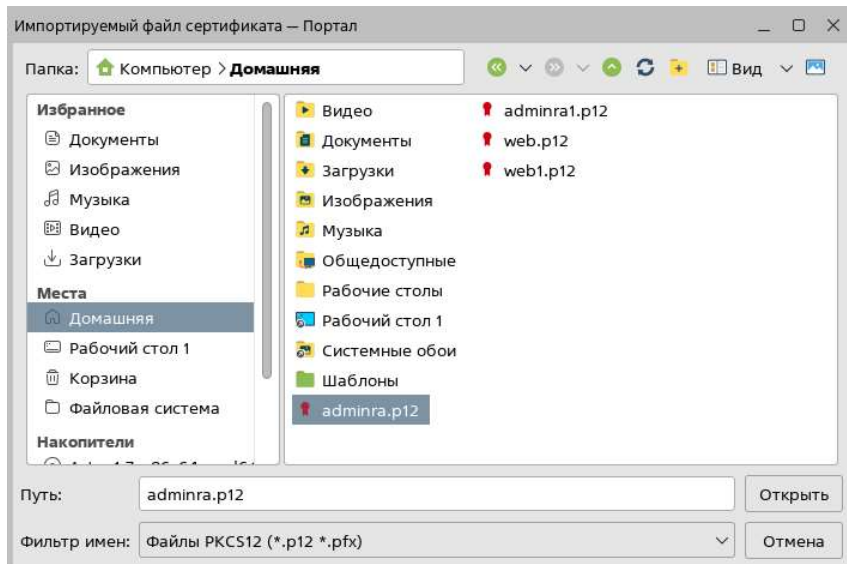


Рисунок 3 - Окно выбора импортируемого файла сертификата

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

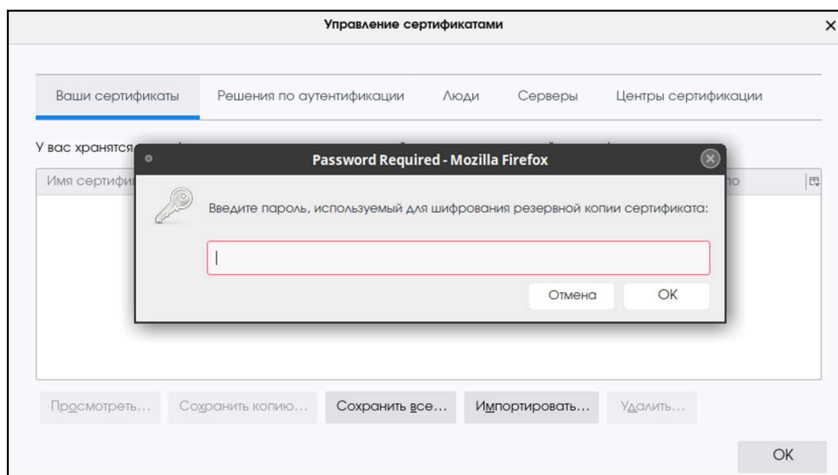


Рисунок 4 - Окно ввода PIN-кода сертификата

Внимание! Пароль устанавливается администратором Центра сертификации Aladdin eCA при выпуске сертификата доступа.

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

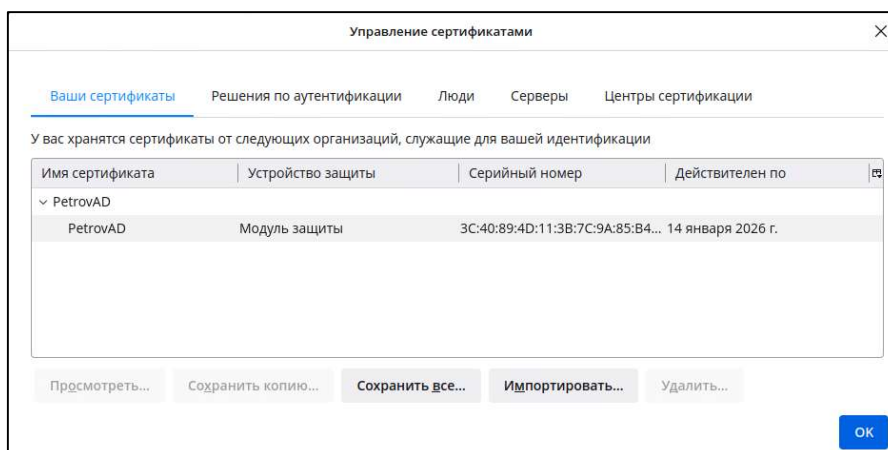


Рисунок 5 - Окно «Управление сертификатами»

6.3 Подключение к веб-интерфейсу

Порядок подключения к веб-интерфейсу:

- Запустите веб-браузер и в адресной строке введите IP-адрес или доменное имя компьютера, на котором установлен Центр регистрации Aladdin eRA (например, <https://172.22.5.21>).
- В открывшемся окне выберите сертификат администратора (см. Рисунок 6) и нажмите кнопку <OK>.

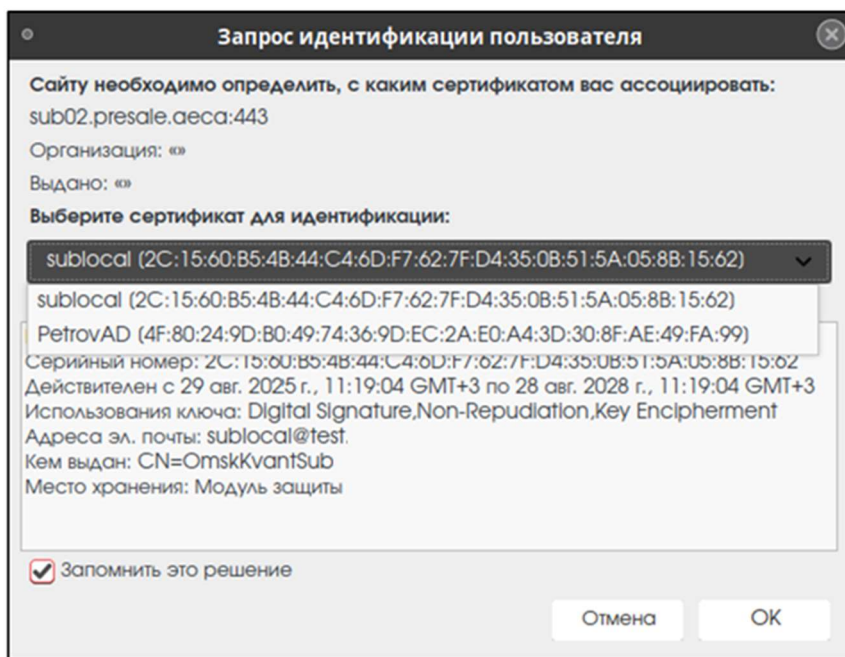


Рисунок 6 - Выбор сертификата для установки двустороннего TLS-соединения

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.

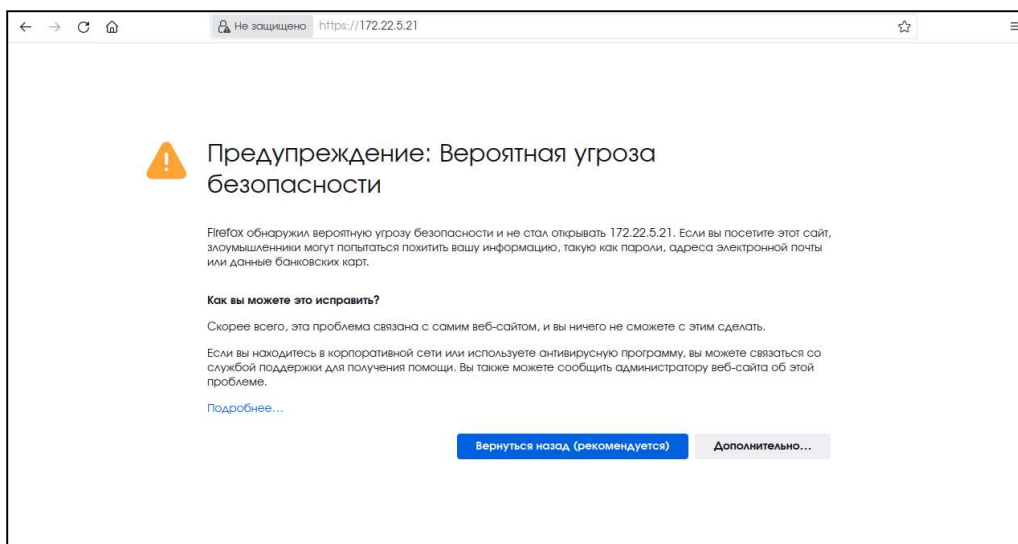


Рисунок 7 - Страница с предупреждением системы безопасности

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

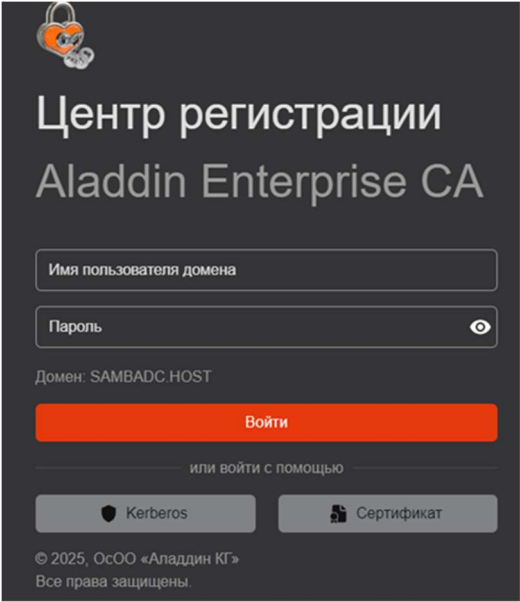


Рисунок 8 - Окно авторизации

Центр регистрации Aladdin eRA поддерживает следующие способы аутентификации:

- С использованием сертификата учетной записи пользователя Центра сертификации Aladdin eCA (см. раздел 6.4).
- С использованием Kerberos-билета пользователя ресурсной системы (см. раздел 6.6).
- По имени и паролю доменной учетной записи пользователя ресурсной системы (см. раздел 6.5).

6.4 Аутентификация с использованием сертификата

Пользователи с ролями «Администратор» и «Оператор» Центра сертификации Aladdin eCA могут аутентифицироваться в Центре регистрации Aladdin eRA по сертификатам своих учетных записей. При этом роль учётной записи в Центр регистрации Aladdin eRA соответствует роли в Центре сертификации Aladdin eCA.

Для аутентификации по сертификату следует выполнить следующие действия:

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



В результате будет выполнена авторизация пользователя в Центре регистрации Aladdin eRA. В ходе аутентификации по сертификату могут возникать ошибки, приведенные в таблице ниже (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	Описание
«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 <code>session_max_count</code> конфигурационного файла)

6.5 Аутентификация по имени и паролю учетной записи

Внимание! Для аутентификации с помощью имени и пароля доменной учетной записи необходимо 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 KG. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».

Доменные учётные записи¹ могут аутентифицироваться в Центре регистрации Aladdin eRA по имени и паролю доменной учетной записи пользователя. Информация о домене отображена в окне авторизации в поле «Домен».

Для аутентификации по имени и паролю выполните следующие действия:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA, пропустив при подключении в окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) выбор сертификата.
- В открывшемся окне авторизации Центра регистрации Aladdin eRA (см. Рисунок 8) в соответствующих полях введите имя и пароль доменной учетной записи и нажмите кнопку .

В результате будет выполнена авторизация доменного пользователя в Центре регистрации Aladdin eRA. Если у пользователя отсутствовала² 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 ошибки, приведенные в таблице ниже (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 <code>session_max_count</code> конфигурационного файла)

¹ Учётные записи, находящиеся в домене ресурсной системы, к которому подключён Центр регистрации Aladdin eCA (адрес сервера доменной службы каталогов задан в параметре `kerberos_ad_server` конфигурационного файла).

² Проверка связи осуществляется путём сравнения идентификатора учётной записи в домене с идентификаторами учётных записей в БД.

6.6 Аутентификация с использованием Kerberos-билета

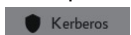
Внимание! Для аутентификации пользователя ресурсной системы с использованием Kerberos-билета необходимо зарегистрировать в Центре сертификации Aladdin eCA, к которому подключён Центр регистрации Aladdin eRA, ресурсную систему, содержащую субъект, под которым будет проходить аутентификация, в соответствии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

Доменные учётные записи ¹ могут аутентифицироваться в Центре регистрации Aladdin eRA по Kerberos-билету. Информация о домене отображена в окне авторизации в поле «Домен».

Предварительно на компьютере доменного пользователя должен быть настроен веб-браузер с поддержкой Kerberos-аутентификации ², а также должен быть получен Kerberos-билет.

Для аутентификации по Kerberos-билету выполните следующие действия:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA, пропустив при подключении в окне «Выбора сертификата для установки двустороннего TLS-соединения» (см. Рисунок 6) выбор сертификата.
- В открывшемся окне авторизации Центра регистрации Aladdin eRA (см. Рисунок 8) нажмите кнопку



В результате будет выполнена авторизация доменного пользователя в Центре регистрации Aladdin eRA. Если у пользователя отсутствовала ³ учётная запись в Центре регистрации Aladdin eRA, то она будет автоматически создана с ролью «Получатель сертификатов».

При аутентификации по Kerberos-билету могут возникать ошибки, приведенные в таблице ниже (Таблица 10).

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 веб-браузера ⁴
«Срок действия Kerberos-билета истек»	Срок действия Kerberos-билета истек - необходимо получить новый билет с помощью команды <code>kinit</code>
«Аккаунт заблокирован»	Доменная учётная запись или учётная запись в программе заблокирована
«Достигнуто предельное число сессий аккаунта»	Выполнение пользователем аутентификации при уже достигнутом предельном количестве сессий для его учётной записи в программе (параметр <code>session_max_count</code> конфигурационного файла)

6.7 Завершение рабочей сессии пользователя

Для завершения рабочей сессии пользователя на верхней панели (см. Рисунок 9) веб-интерфейса Центра регистрации Aladdin eRA нажмите на имя учётной записи пользователя и выберите в появившемся списке <Выход>. В результате рабочая сессия пользователя будет завершена - выполнен переход в окно авторизации Центра регистрации Aladdin eRA (см. Рисунок 8).

Внимание! Для аутентификации по дугому сертификату учетной записи необходимо перезагрузить веб-браузер.

¹ Учётные записи, находящиеся в домене, к которому подключён Центр регистрации Aladdin eCA (адрес сервера AD задан в параметре `kerberos_ad_server` конфигурационного файла).

² Инструкцию по настройке Kerberos-аутентификации в браузерах см. в Приложении 5 «Настройка Kerberos в веб-браузере».

³ Проверка связи осуществляется путём сравнения идентификатора учётной записи в домене с идентификаторами учётных записей в БД.

⁴ Инструкцию по настройке Kerberos-аутентификации в браузерах см. в «Настройка Kerberos в веб-браузере».

7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

В данном раздел описаны функции управления Центра регистрации Aladdin eCA, доступные пользователям с ролью «Администратор».

Функции управления Центра регистрации Aladdin eCA, доступные пользователям с ролью «Оператор», описаны в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG. Руководство оператора».

Функции управления Центра регистрации Aladdin eCA, доступные пользователям с ролью «Получатель сертификатов», описаны в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG. Руководство получателя сертификатов».

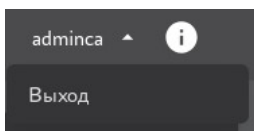
7.1 Верхняя панель

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

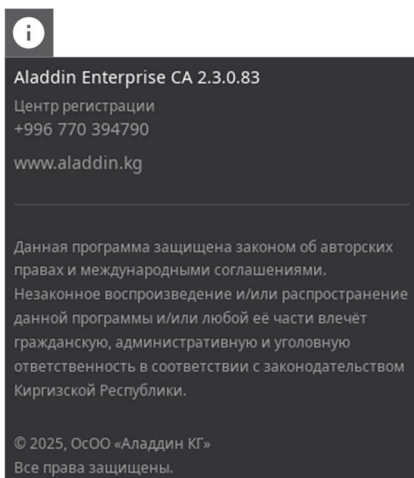


Рисунок 9 - Верхняя панель окна «Центра регистрации»

Верхняя панель содержит следующие элементы:





- имя учётной записи авторизованного пользователя.



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

7.2 Боковая панель

Боковая панель 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 (см. Рисунок 11). Выбор вида боковой панели происходит по нажатию кнопки , расположенной внизу данной панели.

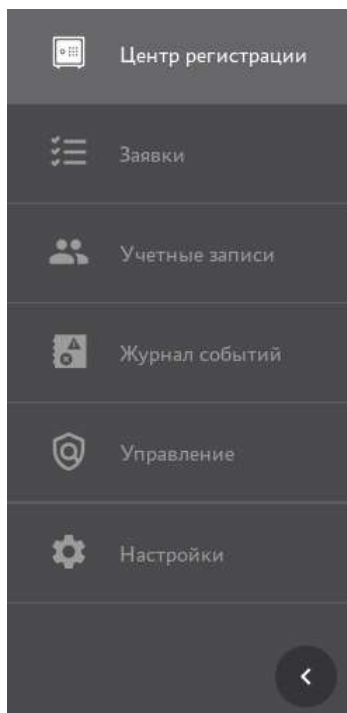


Рисунок 10 - Полный вид боковой панели

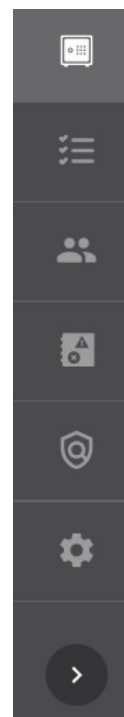


Рисунок 11 - Компактный вид боковой панели

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

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

7.3 Раздел «Центр регистрации»

В разделе «Центр регистрации» присутствует следующая информация (см. Рисунок 12):

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

- Общее количество отклоненных заявок на сертификаты и количество отклоненных заявок на сертификаты за последнюю неделю.
- Общее количество заявок на сертификаты, при обработке которых произошла ошибка, и количество заявок на сертификаты, при обработке которых произошла ошибка, за последнюю неделю.

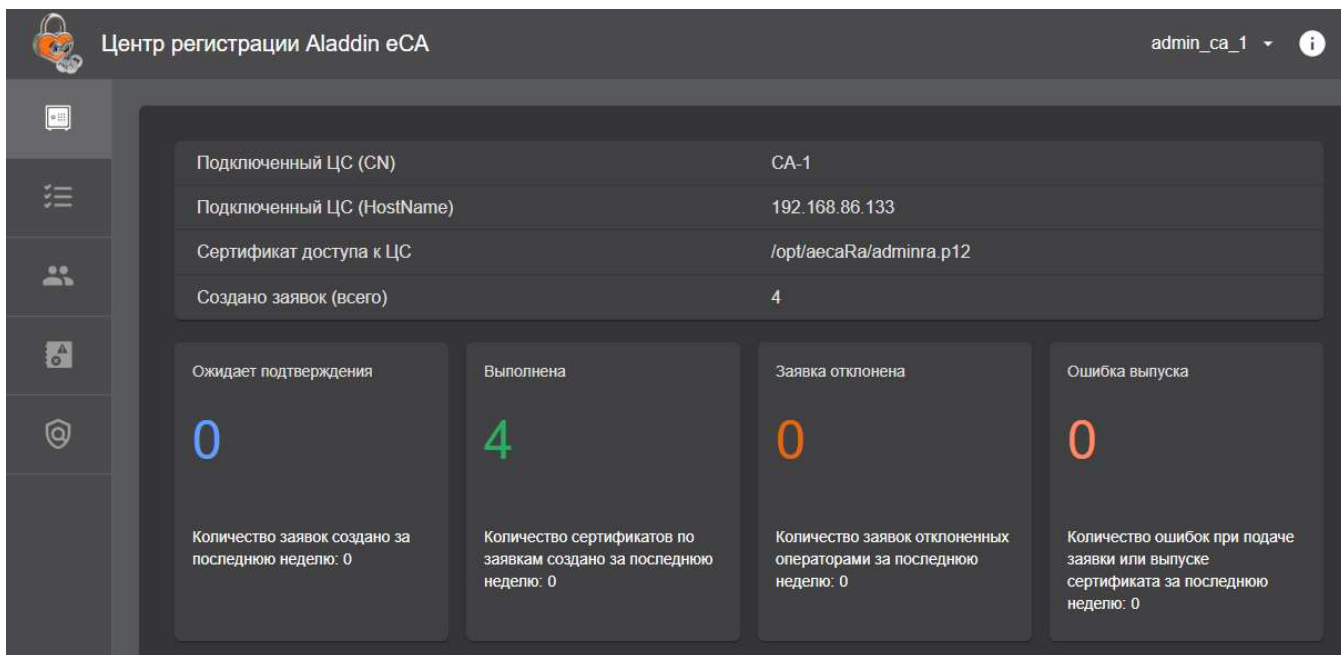


Рисунок 12 - Экран раздела «Центр регистрации»

7.4 Раздел «Заявки»

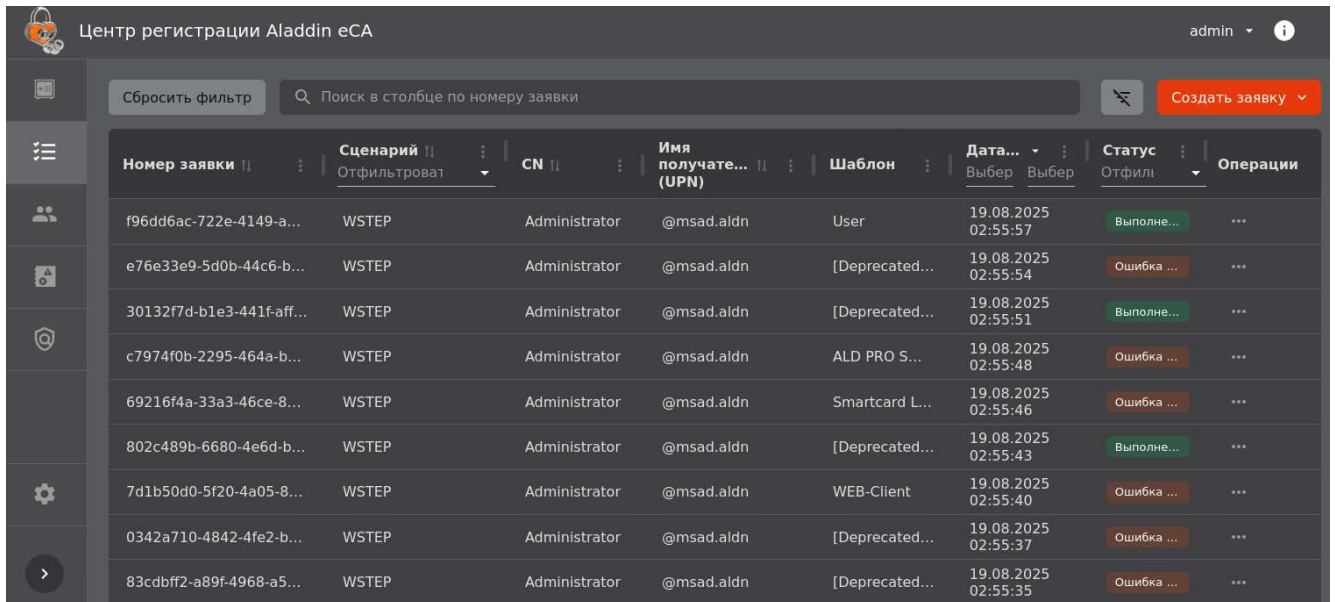
Внимание! Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

Раздел «Заявки» (см. Рисунок 13) 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.

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 субъектов¹, 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.

¹ 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



Центр регистрации Aladdin eCA

admin

Сбросить фильтр

Поиск в столбце по номеру заявки

Создать заявку

Номер заявки	Сценарий	CN	Имя получателя (UPN)	Шаблон	Дата...	Статус	Операции
	Отфильтровать				Выбер	Отфильтр	
f96dd6ac-722e-4149-a...	WSTEP	Administrator	@msad.aldn	User	19.08.2025 02:55:57	Выполне...	...
e76e33e9-5d0b-44c6-b...	WSTEP	Administrator	@msad.aldn	[Deprecated...	19.08.2025 02:55:54	Ошибка
30132f7d-b1e3-441f-aff...	WSTEP	Administrator	@msad.aldn	[Deprecated...	19.08.2025 02:55:51	Выполне...	...
c7974f0b-2295-464a-b...	WSTEP	Administrator	@msad.aldn	ALD PRO S...	19.08.2025 02:55:48	Ошибка
69216f4a-33a3-46ce-8...	WSTEP	Administrator	@msad.aldn	Smartcard L...	19.08.2025 02:55:46	Ошибка
802c489b-6680-4e6d-b...	WSTEP	Administrator	@msad.aldn	[Deprecated...	19.08.2025 02:55:43	Выполне...	...
7d1b50d0-5f20-4a05-8...	WSTEP	Administrator	@msad.aldn	WEB-Client	19.08.2025 02:55:40	Ошибка
0342a710-4842-4fe2-b...	WSTEP	Administrator	@msad.aldn	[Deprecated...	19.08.2025 02:55:37	Ошибка
83cdbff2-a89f-4968-a5...	WSTEP	Administrator	@msad.aldn	[Deprecated...	19.08.2025 02:55:35	Ошибка

Рисунок 13 - Экран раздела «Заявки»

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

- Номер заявки - содержит номер заявки;
- Сценарий - содержит сценарий, по которому была создана заявка («На основании запроса (PKCS#10)», «С закрытым ключом (PKCS#12)», «На ключевом носителе», «SCEP»¹ или «WSTEP»²);
- CN - содержит CN, указанный в заявке на сертификат;
- 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»³, «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;


¹ Заявки с типом «SCEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов клиентов по протоколу SCEP, подробнее см. раздел 8.

² Заявки с типом «WSTEP» создаются в Центре регистрации Aladdin eRA автоматически в результате обработки запросов клиентов по протоколу MS-WSTEP, подробнее см. раздел 9.

³ Статус «Отмена» подразумевает, заявка была отменена её создателем. Статус «Отклонена» подразумевает, что пользователь, обрабатывавший заявку, отклонил процесс выпуска 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;
- 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.

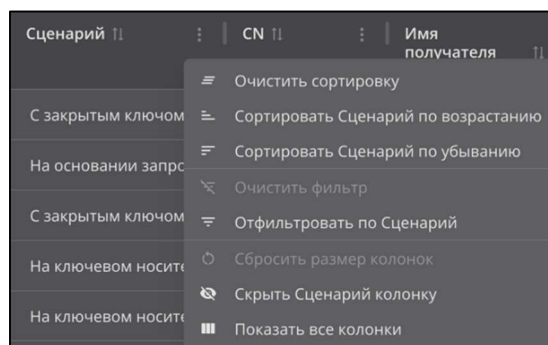


Рисунок 14 - Кнопка <Действия в колонке> в колонке «Сценарий»

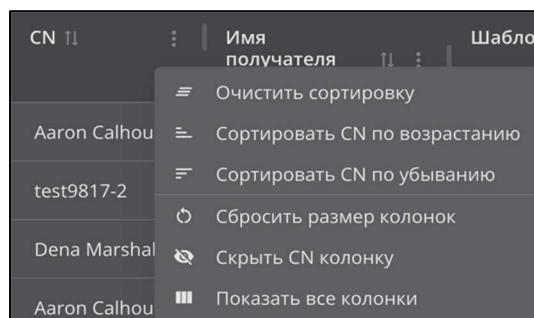


Рисунок 15 - Кнопка <Действия в колонке> в колонке «CN»

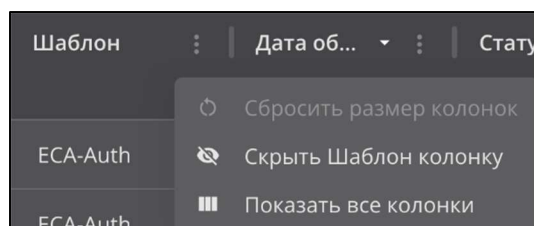



Рисунок 16 - Кнопка <Действия в колонке> в колонке «Шаблон»

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).

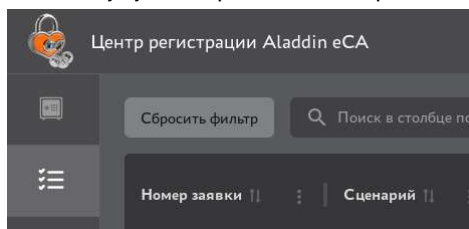



Рисунок 17 - Кнопка <Сбросить фильтр>

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», «SCEP», «WSTEP»).
- Дата обработки - выберите период, в которой должна попадать дата обработки заявки (введите дату с помощью клавиатуры или выберите в календаре).
- Статус - выберите статус заявки («Ошибка выпуска», «Отклонена», «Ожидает подтверждения», «Выполнена», «Отменена»¹, «Ожидает импорта на КН», «Новая»).

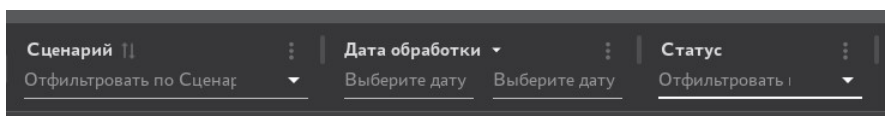





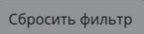
Рисунок 18 - Поля фильтра заголовков экранной таблицы

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;

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

- дата обработки - упорядочивание осуществляется от старых к новым и от новых к старым.

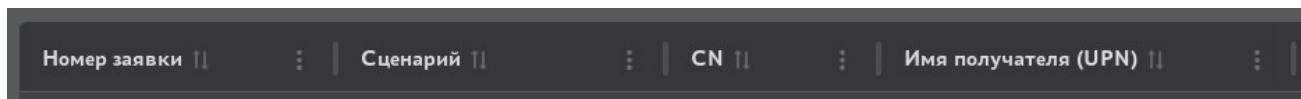




Рисунок 19 - Поля сортировки содержимого экрана раздела «Заявки»

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.

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.

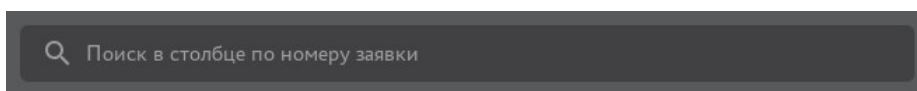


Рисунок 20 - Поисковая строка в разделе «Заявки»


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» (см. Рисунок 21) осуществляется при нажатии на строку заявки главного экрана разделе «Заявки» (см. Рисунок 13).

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»¹, «Ожидает импорта на КН»;
- Кнопка <Сертификат активирован>, отражающая текущий статус сертификата и предназначенная для отзыва сертификата, выпущенного по данной заявке. После отзыва сертификата кнопка меняет свое наименование на «Сертификат отозван» и становится неактивной.
- Кнопка  с контекстным меню действий (состав действий (Таблица 12), контекстное меню см. Рисунок 22, Рисунок 23 и Рисунок 24).

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

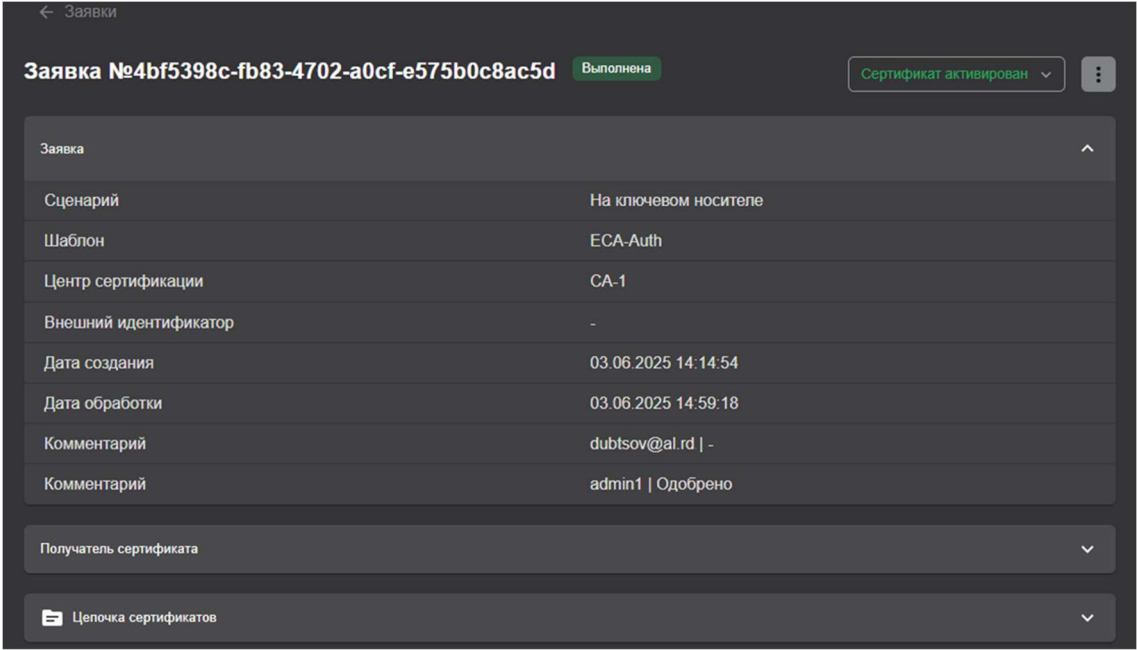


Рисунок 21 - Экран «Карточка заявки»

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

Действия	Условие отображения действия	Выполнение
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

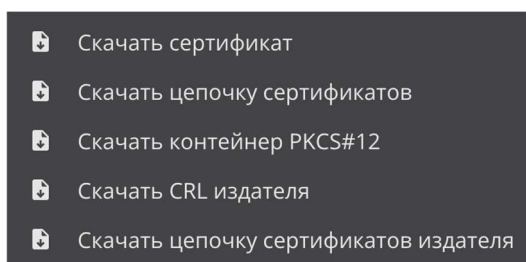


Рисунок 22 - Меню действий в карточке заявки

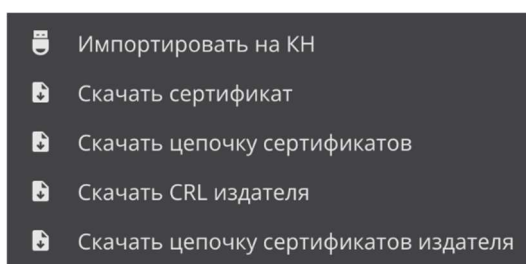


Рисунок 23 - Меню действий для заявки

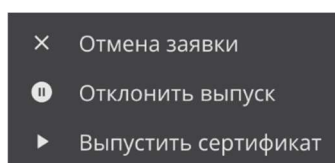


Рисунок 24 - Меню действий для заявки. Заявка в статусе «Ожидает подтверждения»

- 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.

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

Рисунок 25 - Экран «Карточка заявки». 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.

Получатель сертификата	
Идентификатор	ccd5f712-03f9-4084-bba6-b5bbcb858b63
Ресурсная система	al
Имя получателя (UPN)	petrov@al.rd
Common Name	петров

Рисунок 26 - Экран «Карточка заявки». 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.

Цепочка сертификатов	
<ul style="list-style-type: none"> Root-CA2 петров 	
Издатель	Root-CA2
Владелец	петров
SDN владельца	CN=петров
Действует с	18.02.2025 16:17:44
Действует по	18.02.2027 16:17:44
Алгоритм ключа	RSA
Длина ключа	1024

Рисунок 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.

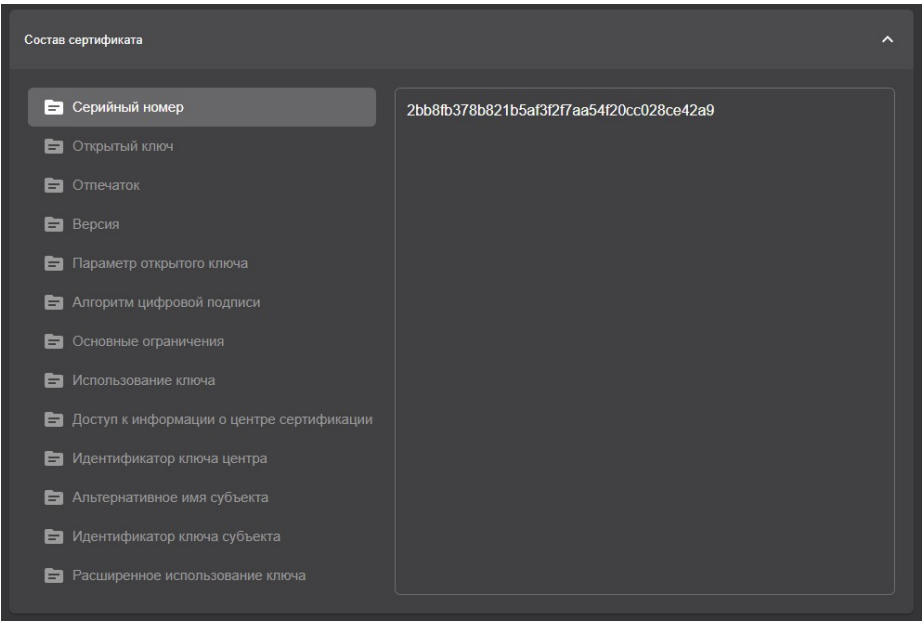


Рисунок 28 - Экран «Карточка заявки». Блок «Состав сертификата»

- 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.

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

Рисунок 29 - Экран «Карточка заявки». Блок «История изменения заявки»

7.4.6 Создание заявки на основании запроса

Для создания заявки на основании запроса выполните следующие шаги:

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

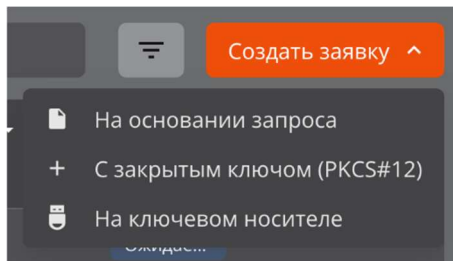



Рисунок 30 - Контекстное меню создания заявки

- 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 поля атрибута субъекта, разделитель значений в поле - запятая с пробелом;
 - в результате поиска поля «CN», «UPN» и «DNS» не отображаются, если в соответствующем данному полю атрибуте у субъекта отсутствуют значения;
 - выберите субъект и нажмите кнопку «Продолжить» для перехода к следующему шагу.

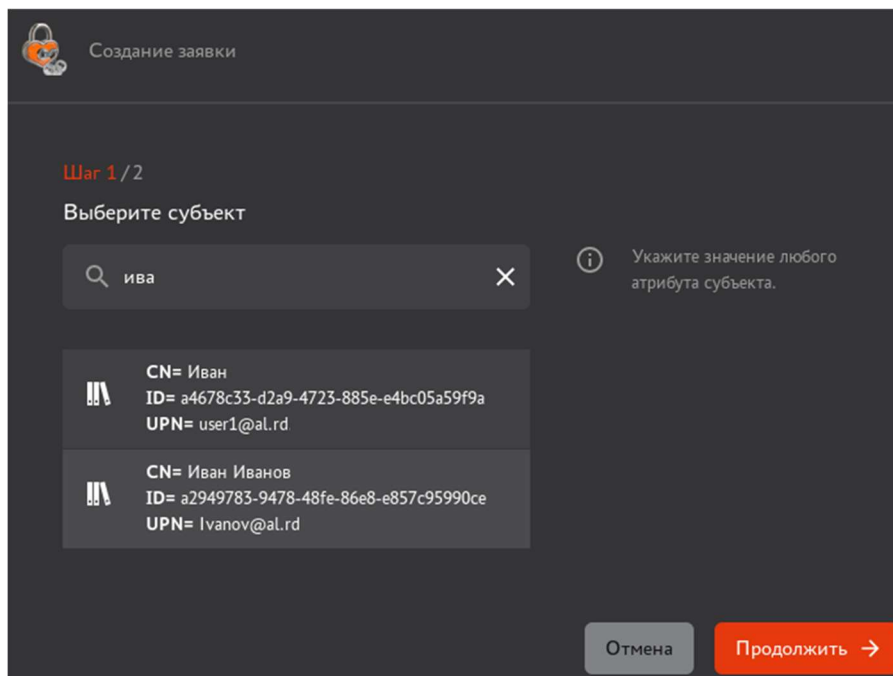


Рисунок 31 - Создание заявки на основании запроса. Шаг 1

- На втором шаге (см. Рисунок 32):
 - выберите файл-запрос (загружается по кнопке «Выбрать файл» с возможностью повторного выбора по кнопке «Изменить»);

- выберите шаблон, на основании которого будет создан сертификат. В списке шаблонов присутствуют шаблоны, которые указаны в правилах выпуска с режимом обработки «Автоматический выпуск» или «Ручная обработка» для выбранного на шаге 1 субъекта¹.

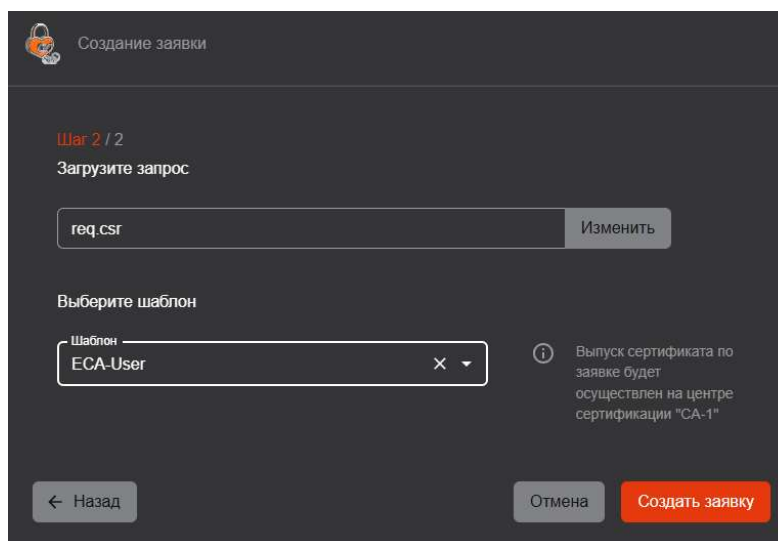


Рисунок 32 - Создание заявки на основании запроса. Шаг 2

- 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).

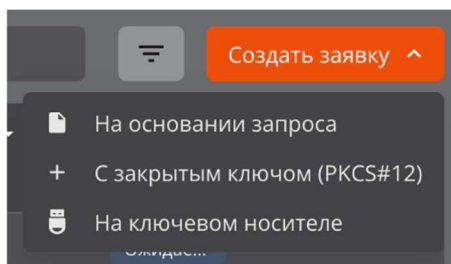



Рисунок 33 - Контекстное меню создания заявки

- 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:
 - «CN» - значение атрибута «Common Name» субъекта;
 - «ID» - идентификатор субъекта;
 - «UPN» - значение атрибута «MS UPN, User Principal Name» субъекта;
 - «DNS» - значение атрибута «DNS Name» субъекта;

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

- 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.

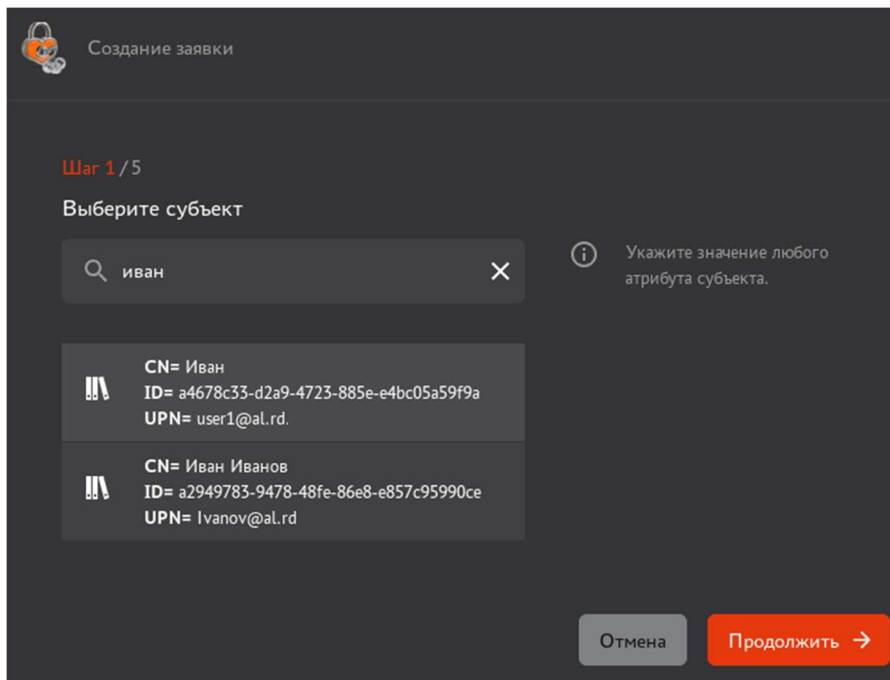


Рисунок 34 - Создание заявки с закрытым ключом PKCS#12. Шаг 1

- 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 субъекта¹.

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

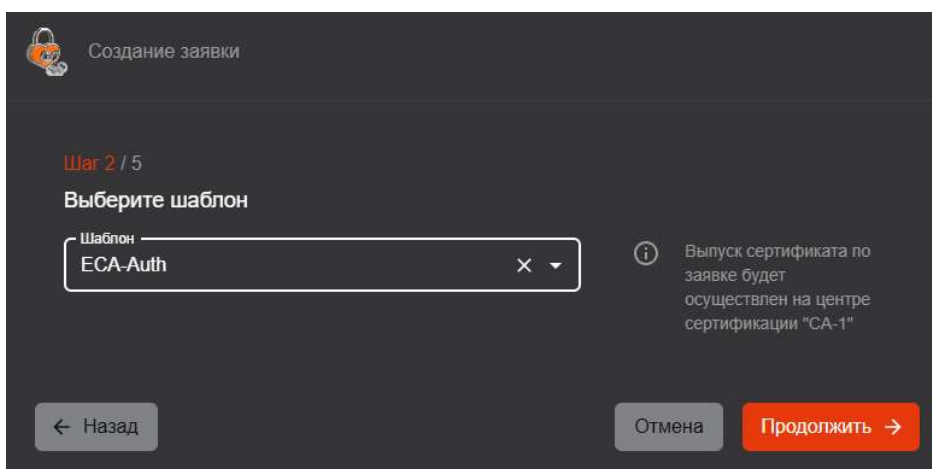




Рисунок 35 - Создание заявки с закрытым ключом PKCS#12. Шаг 2

¹ 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.

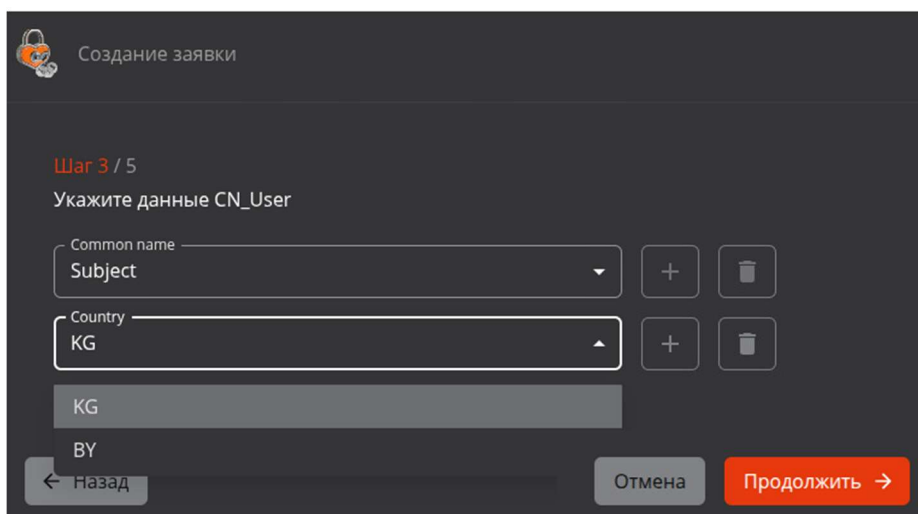



Рисунок 36 - Создание заявки с закрытым ключом PKCS#12. Шаг 3

- 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.

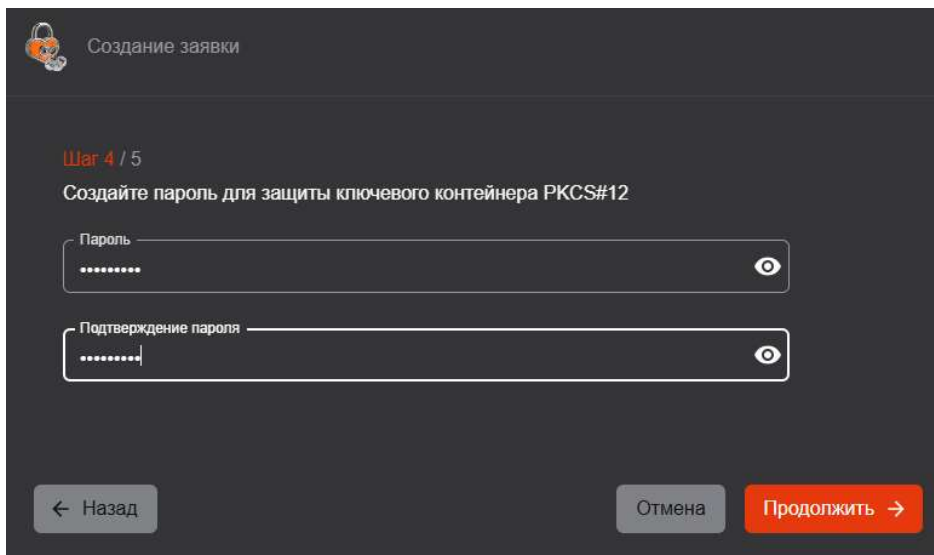


Рисунок 37 - Создание заявки с закрытым ключом PKCS#12. Шаг 4

- 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.

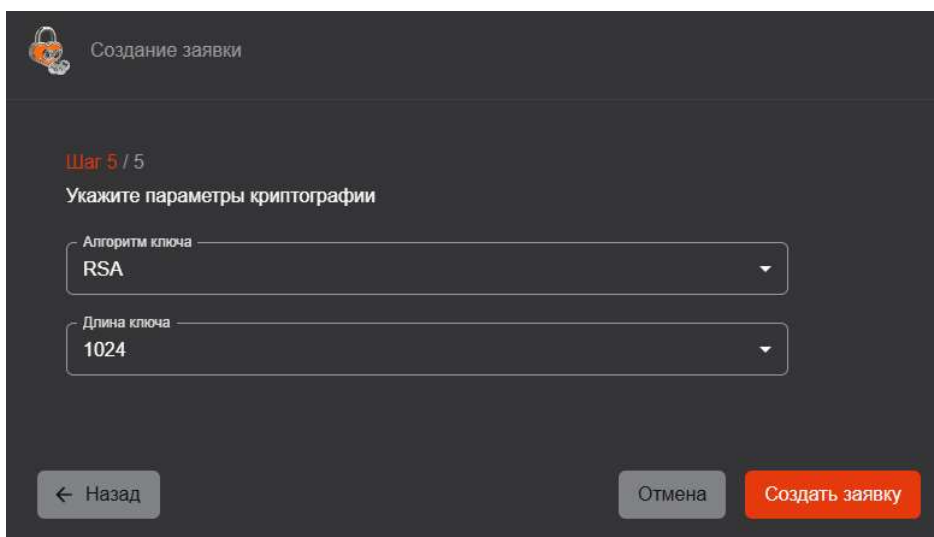


Рисунок 38 - Создание заявки с закрытым ключом PKCS#12. Шаг 5

- 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



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

Внимание! Ограничения по возможностям генерации для ключевых носителей Рутокен приведены на [официальном сайте производителя](#).

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

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

Для создания заявки на ключевом носителе выполните следующие действия:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- На панели инструментов нажмите кнопку  и выберите в открывшемся списке сценарий создания заявки **<На ключевом носителе>** (см. Рисунок 39).

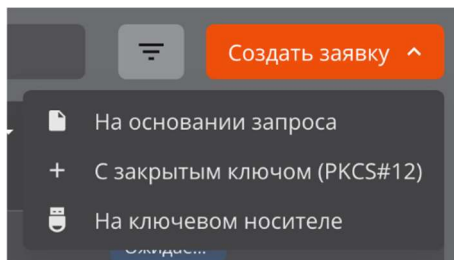


Рисунок 39 - Контекстное меню создания заявки

Внимание! Если JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 40) или к компьютеру не подключен ключевой носитель (см. Рисунок 41), создать заявку невозможно.

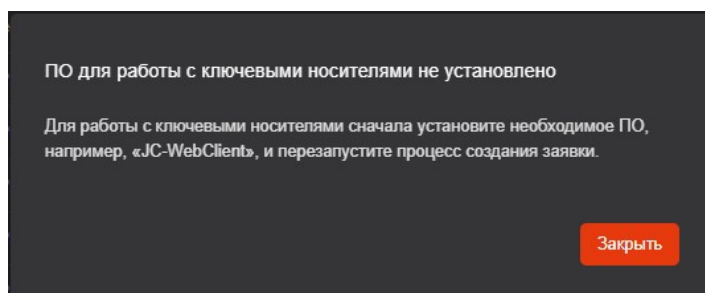


Рисунок 40 - ПО для работы с ключевыми носителями не установлено

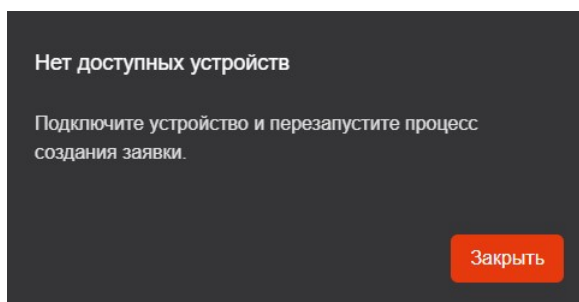





Рисунок 41 - Подключенные ключевые носители отсутствуют

- В открывшемся окне «Создание заявки на сертификат» (см. Рисунок 34) выберите субъекта и нажмите кнопку .

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

- «CN» - значение атрибута «Common Name» субъекта.
- «ID» - идентификатор субъекта.
- «UPN» - значение атрибута «MS UPN, User Principal Name» субъекта.
- «DNS» - значение атрибута «DNS Name» субъекта

-  - признак подключения к ресурсной системе.
- В открывшемся окне «Создание заявки на сертификат» (шаг 1 сценария) (см. Рисунок 42):
 - В списке «Устройство» выберите подключенный ключевой носитель.
 - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
 - В списке «Шаблон» выберите доступный шаблон, по которому будет выпущен сертификат ¹.
В списке шаблонов присутствуют шаблоны, которые указаны в правилах выпуска с режимом обработки «Автоматический выпуск» или «Ручная обработка» для выбранного на шаге 1 субъекта².
 - Нажмите кнопку .

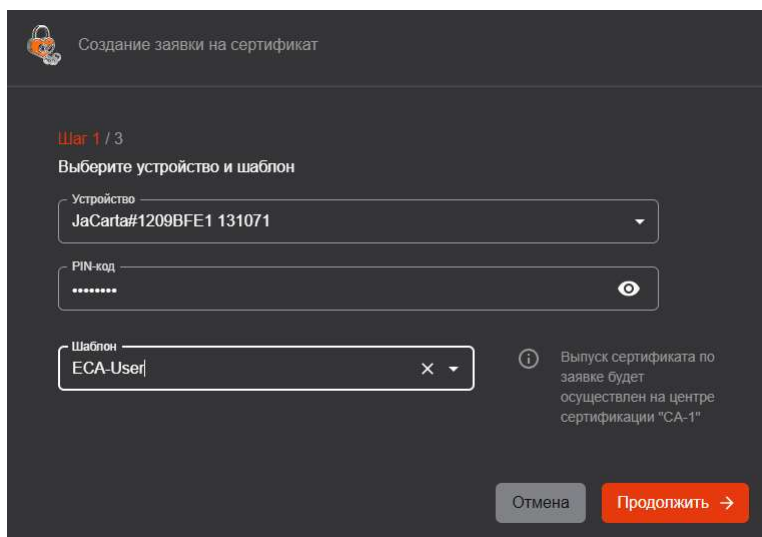



Рисунок 42 - Выбор ключевого носителя и шаблона для выпуска сертификата

- В открывшемся окне «Создание заявки на сертификат» (шаг 2 сценария) (см. Рисунок 43) укажите атрибуты получателя сертификатов (субъекта PC) и нажмите кнопку .


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


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

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

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

Рисунок 43 - Создание заявки на ключевом носителе. Шаг 3

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

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

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

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



- В открывшемся окне «Создание заявки на сертификат» (шаг сценария 3)(см. Рисунок 44):
 - В списке «Алгоритм ключа» выберите алгоритм генерации ключевой пары (список алгоритмов определяется выбранным шаблоном).
 - В списке «Длина ключа» выберите длину ключа (минимальная доступная для выбора длина ключа определяется выбранным шаблоном).
 - Нажмите кнопку .

Рисунок 44 - Создание заявки на ключевом носителе. Шаг 4

- В открывшемся окне «Создание заявки на сертификат» (процесс формирования заявки и его результат) (см. Рисунок 45) отображаются следующие процессы:
 - Генерации ключевой пары.
 - Генерации запроса.
 - Создания заявки.

Успешное завершения каждого процесса помечается значком .

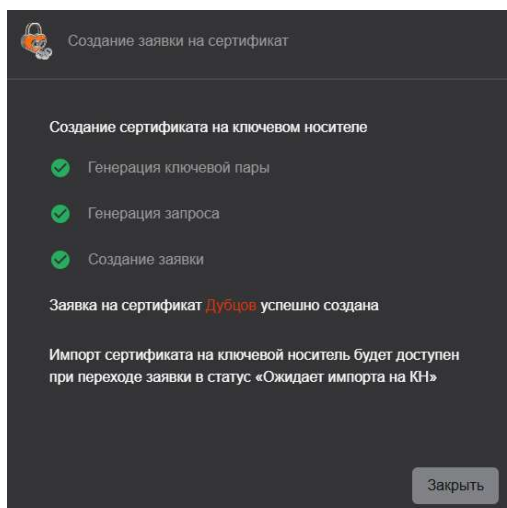


Рисунок 45 - Заявка на выпуск сертификата на ключевом носителе заведена успешно

Внимание! Некоторые типы ключевых носителей поддерживают определенный набор алгоритмов выработки ключевых пар (например, в приведенном ниже примере при создании заявки на выпуск сертификата на электронном ключе JaCarta-2 ГОСТ был выбран неподдерживаемый алгоритм RSA) (см. Рисунок 46).

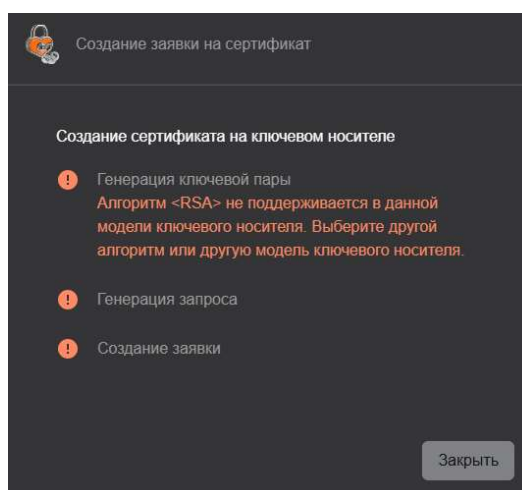



Рисунок 46 - Выбранный алгоритм не поддерживается в используемом ключевом носителе

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

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

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

7.4.9 Отмена заявки



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

Отмена заявки может быть выполнена только учётной записью, создавшей данную заявку.

Для отмены заявки выполните следующие шаги:

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

Далее необходимо нажать на кнопку выбора действий для заявки:

- в строке заявки нажмите на кнопку «Операции» ;
- либо в карточке заявки нажмите на кнопку .
- В появившемся контекстном меню (см. Рисунок 47) выберите действие «Отмена заявки».

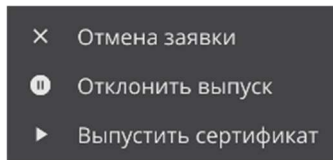


Рисунок 47 - Меню действий для заявки. Заявка в статусе «Ожидает подтверждения», создателем данной заявки является текущая учётная запись

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

Нажмите на кнопку «Отменить» для подтверждения действия.

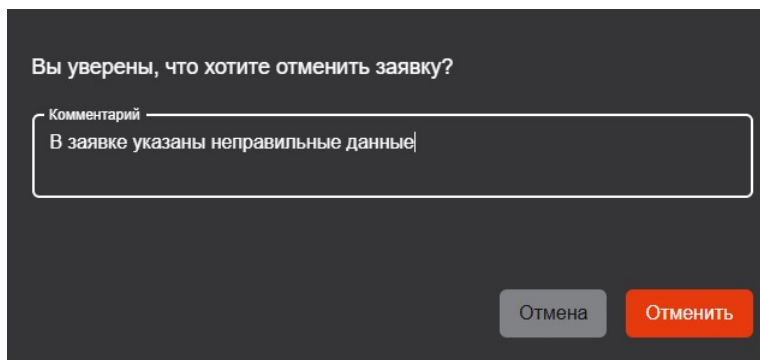


Рисунок 48 - Окно комментария к отмене заявки

- 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

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

Для обработки заявки выполните следующие шаги:

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

Далее необходимо нажать на кнопку выбора действий для заявки:

- в строке заявки нажмите на кнопку «Операции» ;
- либо в карточке заявки нажмите на кнопку .
- В появившемся контекстном меню (см. Рисунок 49) выберите действие из перечня:
 - Отклонить выпуск.
 - Выпустить сертификат.

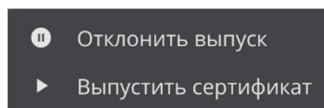


Рисунок 49 - Меню действий для заявки. Вид для администратора. Заявка в статусе Ожидает

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

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

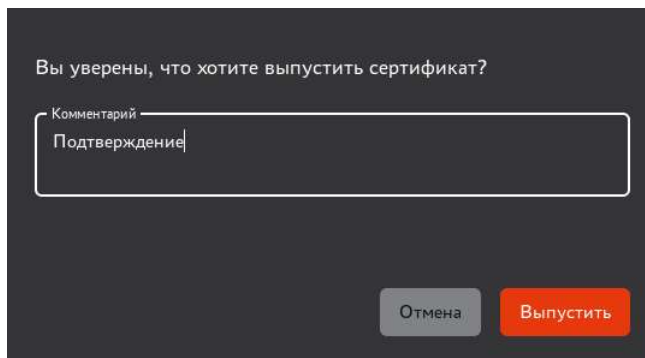


Рисунок 50 - Окно комментария к подтверждению выпуска сертификата

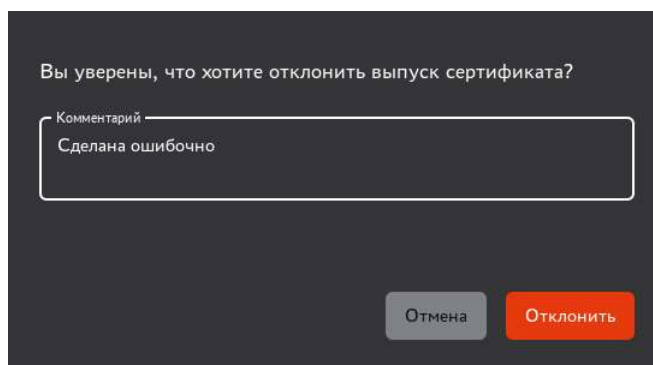


Рисунок 51 - Окно комментария к отклонению выпуска сертификата

- 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

Предварительные условия для импорта сертификата на ключевой носитель:

- На компьютере, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должно быть установлено приложение JC-WebClient или ПО «Рутокен Плагин».
- К компьютеру, с которого выполняется подключение к веб-интерфейсу Центра регистрации Aladdin eRA, должен быть подключен поддерживаемый ключевой носитель (электронный ключ).
- Заявка, по которой был выпущен сертификат для последующего импорта на ключевой носитель, должна иметь статус «Ожидает импорта на КН».

Порядок импорта сертификата на ключевой носитель:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Заявки**.
- Иницилируйте процесс импорта сертификата на ключевой носитель одним из следующих способов:

- Найдите заявку в списке, щелкните в колонке **[Операции]** значок  **<Операции строки>** и выберите в открывшемся списке  **<Импортировать на КН>**.

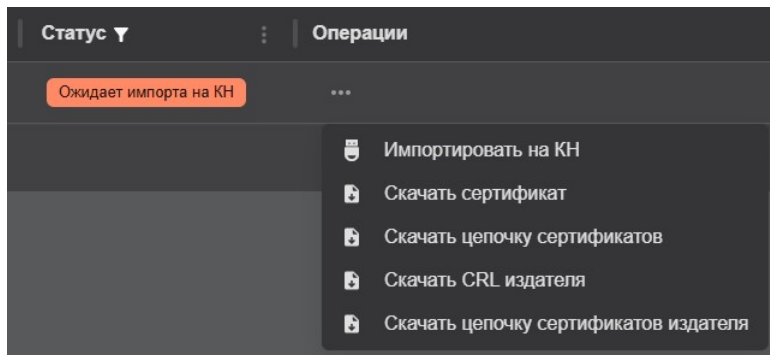



Рисунок 52 - Инициализация процесса импорта сертификата на ключевой носитель из списка

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

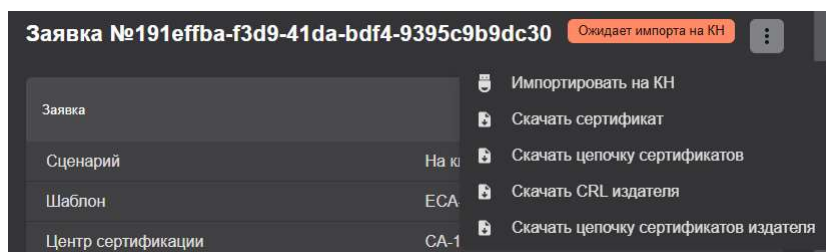



Рисунок 53 - Инициализация процесса импорта сертификата на ключевой носитель из карточки заявки

Внимание! Если JC-WebClient или ПО «Рутокен Плагин» не установлено (см. Рисунок 40) или к компьютеру не подключен ключевой носитель (см. Рисунок 41), создать заявку невозможно.

- В открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 54):
 - В списке «Устройство» выберите подключенный ключевой носитель.
 - В поле «PIN-код» введите PIN-код доступа к ключевому носителю.
 - Нажмите кнопку .

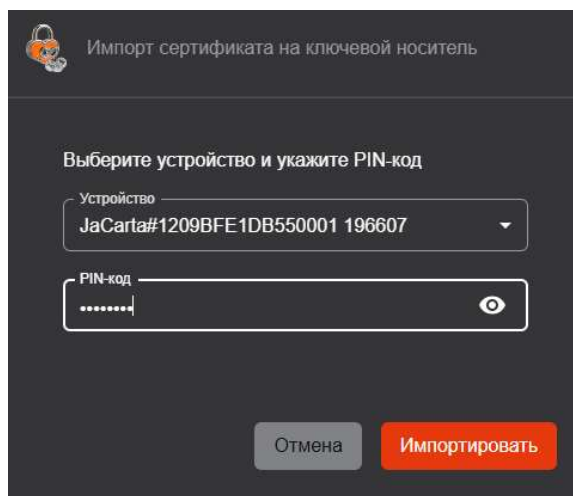



Рисунок 54 - Импорт сертификата на ключевой носитель

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

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

- В случае успешного импорта сертификата на ключевой носитель в открывшемся окне «Импорт сертификата на ключевой носитель» (см. Рисунок 55) проверьте данные сертификата и нажмите кнопку .

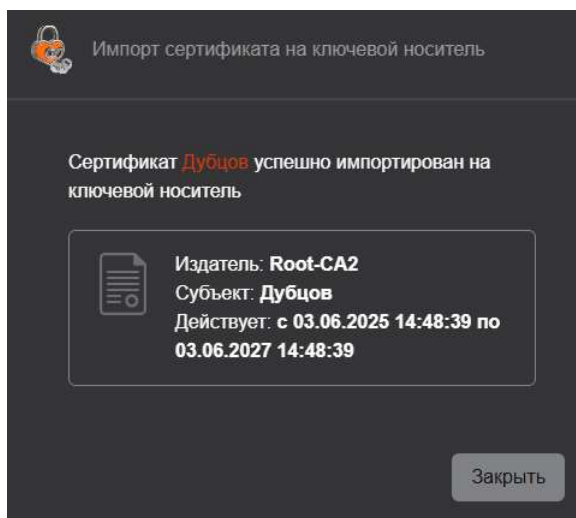


Рисунок 55 - Импорт сертификата на ключевой носитель успешно выполнен

7.4.12 Отзыв сертификата

Чтобы отозвать сертификат, заявка по которой он был выпущен должна быть в статусе «Выполнена», а статус сертификата «Активирован». Отзыв сертификата является необратимой операцией, которая может повлиять на работу пользователя или устройства.

Для пользователя с ролью «Получатель сертификатов» доступен отзыв сертификатов, выпущенных только по собственным заявкам. Пользователю с ролью «Оператор» доступен отзыв сертификатов из заявок для субъектов, доступ к которым ему предоставлен в соответствии с правилами доступа, назначенными в 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 56);

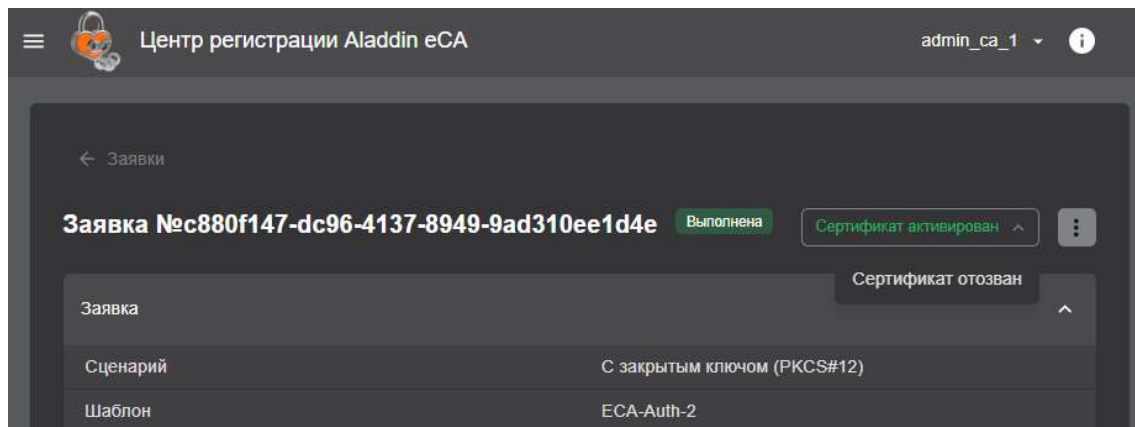


Рисунок 56 - Отзыв сертификата

- в открывшемся окне выберите в списке «Причина» причину отзыва сертификата, оставьте обязательный комментарий в соответствующем поле и нажмите кнопку <Отозвать> (см. Рисунок 57);

Отозвать сертификат?

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

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

Причина
 Без указания причины

Комментарий *
 Компрометация

Отозвать Отмена

Рисунок 57 - Указание причины отзыва сертификата

- В результате сертификат будет отозван.

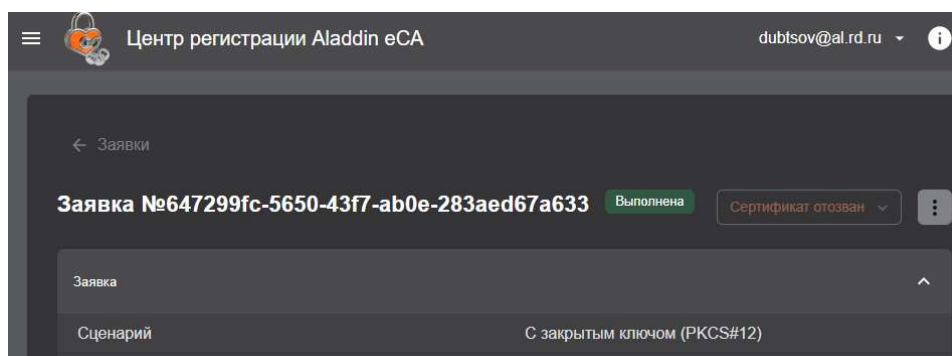
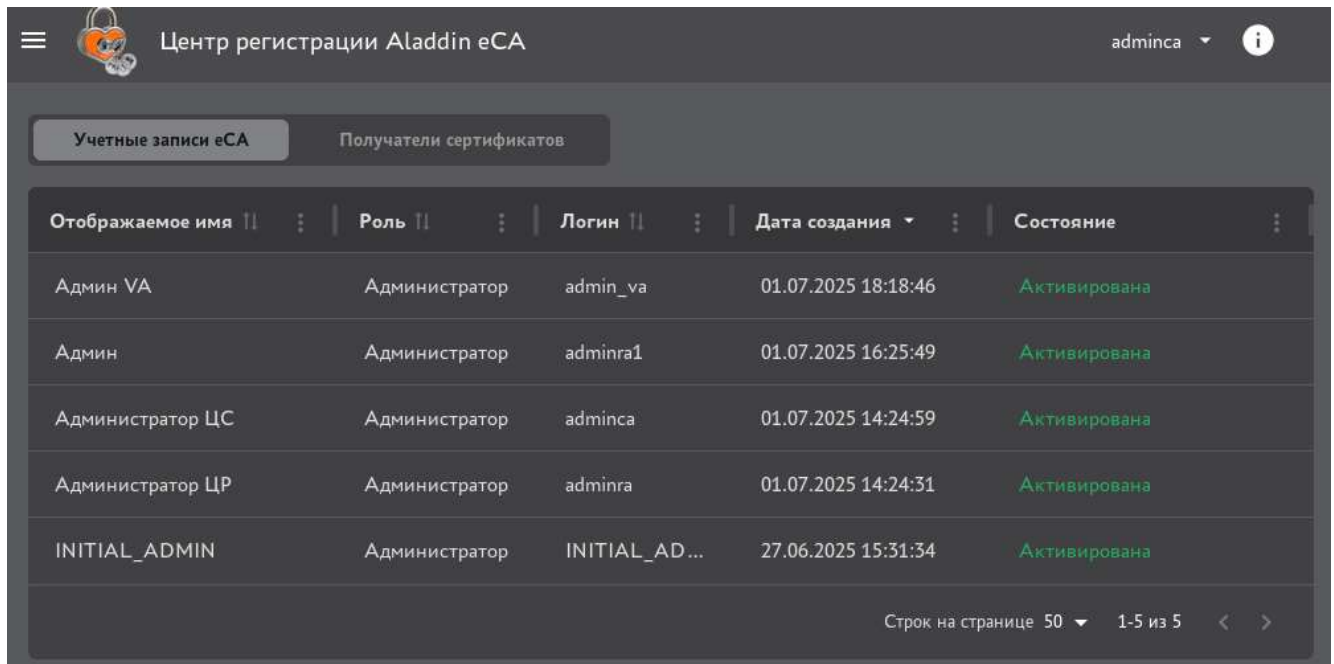


Рисунок 58 - Сертификат отозван

7.5 Раздел «Учётные записи»

Раздел «Учётные записи» (см. Рисунок 59) предоставляет информацию об учётных записях Центра регистрации Aladdin eRA, а также обеспечивает возможность блокировать и активировать учётные записи.



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

Рисунок 59 - 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 59):

- 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 KG. 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 60):

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

На вкладке «Получатели сертификатов» доступны следующие действия:

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

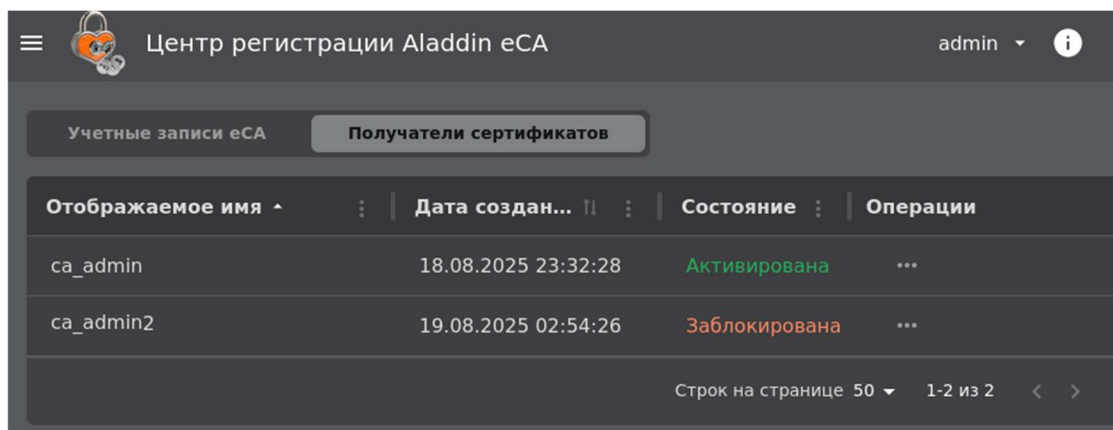


Рисунок 60 - Экран раздела «Учётные записи». Вкладка «Получатели сертификатов»

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 61).

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».

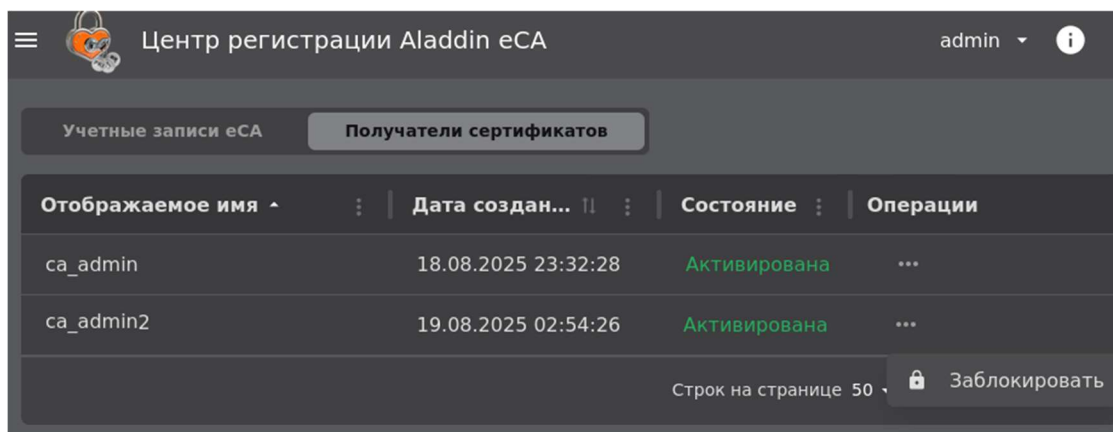


Рисунок 61 - Экран раздела «Учётные записи». Блокировка доменной учётной записи

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 62).

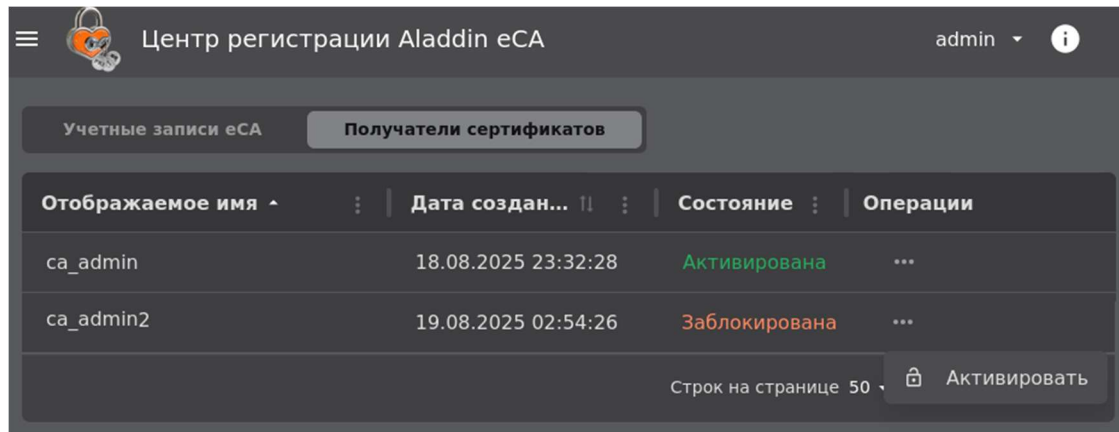


Рисунок 62 - Экран раздела «Учётные записи». Активация доменной учётной записи

7.6 Раздел «Журнал событий»

7.6.1 О журнале событий

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

Каждая запись в журнале событий содержит следующую информацию:

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

Перечень событий с их кодами, категориями и подробным описанием приведен в Приложении 6.

Время хранения записей в журнале событий по умолчанию составлять 180 дней с момента регистрации. Время хранения регулируется с помощью параметра `archive_millis_ago` конфигурационного файла. Записи со сроком давности большим или равным времени хранения архивируются и удаляются из журнала событий. Режим архивации событий по умолчанию включен (параметр `archive_enabled` - флаг управления режимом архивации).


Периодичность запуска архивации регулируется параметром `archive_cron` конфигурационного файла. Значение указывается в формате CRON-выражения (значение по умолчанию - '0 0 0 1 * *'). По умолчанию процесс архивации запускается при наступлении первого числа каждого месяца.

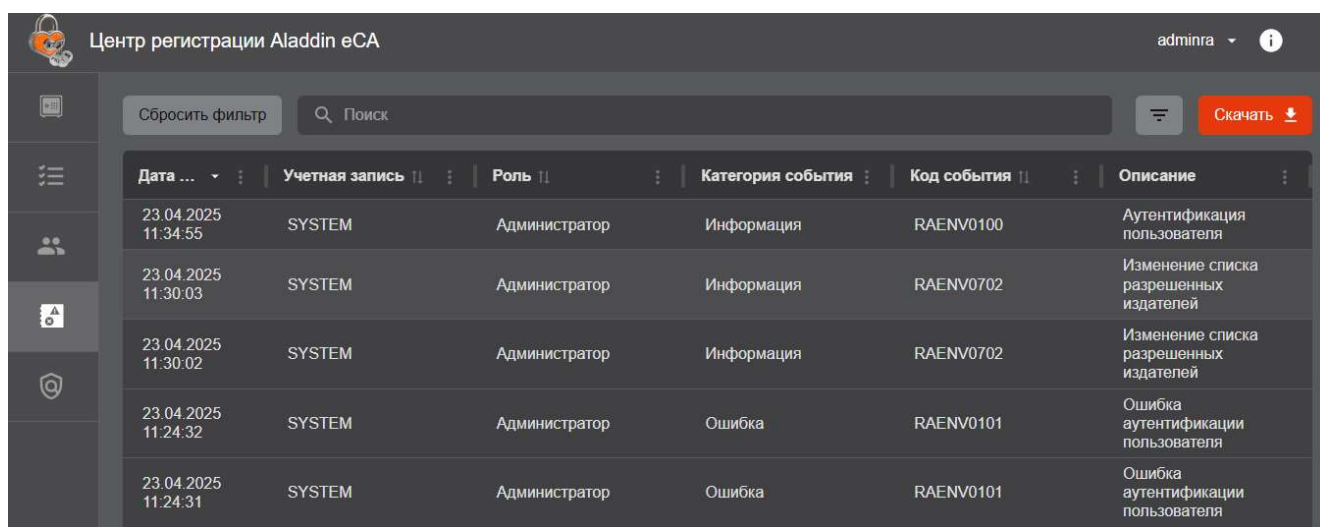
Архив в формате `.zip`, содержащий `.csv` файл, с именем `logs-<дата создания архива>.zip` будет сохранён в каталог, указанный в параметре `archive_path` конфигурационного файла (по умолчанию `/opt/aecaRa/dist/archive`).

7.6.2 Просмотр записей журнала событий

Данный раздел доступен для пользователей с ролями «Администратор» и «Оператор»:

- Для пользователя с ролью «Администратор» доступен просмотр всех событий журнала.
- Для пользователя с ролью «Оператор» доступен просмотр только следующих событий журнала:
 - события, для которых он является инициатором;
 - события по заявкам, которые были созданы данным пользователем;
 - события по заявкам, у которых получателем сертификата является субъект, доступный данному пользователю в соответствии с правилами доступа Центра сертификации, к которому подключён Центр регистрации Aladdin eRA.

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



Дата ...	Учетная запись	Роль	Категория события	Код события	Описание
23.04.2025 11:34:55	SYSTEM	Администратор	Информация	RAENV0100	Аутентификация пользователя
23.04.2025 11:30:03	SYSTEM	Администратор	Информация	RAENV0702	Изменение списка разрешенных издателей
23.04.2025 11:30:02	SYSTEM	Администратор	Информация	RAENV0702	Изменение списка разрешенных издателей
23.04.2025 11:24:32	SYSTEM	Администратор	Ошибка	RAENV0101	Ошибка аутентификации пользователя
23.04.2025 11:24:31	SYSTEM	Администратор	Ошибка	RAENV0101	Ошибка аутентификации пользователя

Рисунок 63 - Просмотр записей журнала событий

Записи о событиях отображаются списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты событий:




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





Записи о событиях выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 64).



Рисунок 64 - Инструменты навигации

Описание инструментов навигации:

-  — переход на следующую страницу списка.
-  — переход на предыдущую страницу списка.
-  — выбор количества записей, отображаемых на одной странице списка.

Для удобства анализа записей в списке вы можете управлять видимостью колонок таблицы. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок  **<Действие колонки>** и в открывшемся списке ¹ выберите  **<Скрыть [название колонки] колонку>** (см. Рисунок 65). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок  **<Действие колонки>** и в открывшемся списке выберите  **<Показать все колонки>** (см. Рисунок 65).

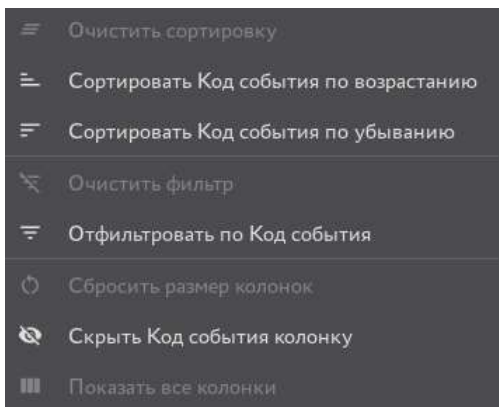



Рисунок 65 - Список действий с колонкой **[Код события]**



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

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




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



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

Чтобы выполнить сортировку записей о событиях по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся списке ² (см. Рисунок 65) выберите:

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

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками ³:

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

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

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

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




² Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.


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

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

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

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку

 **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок  **<Действие колонки>** и в открывшемся списке выберите  **<Отфильтровать по [название колонки]>** (см. Рисунок 65).

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

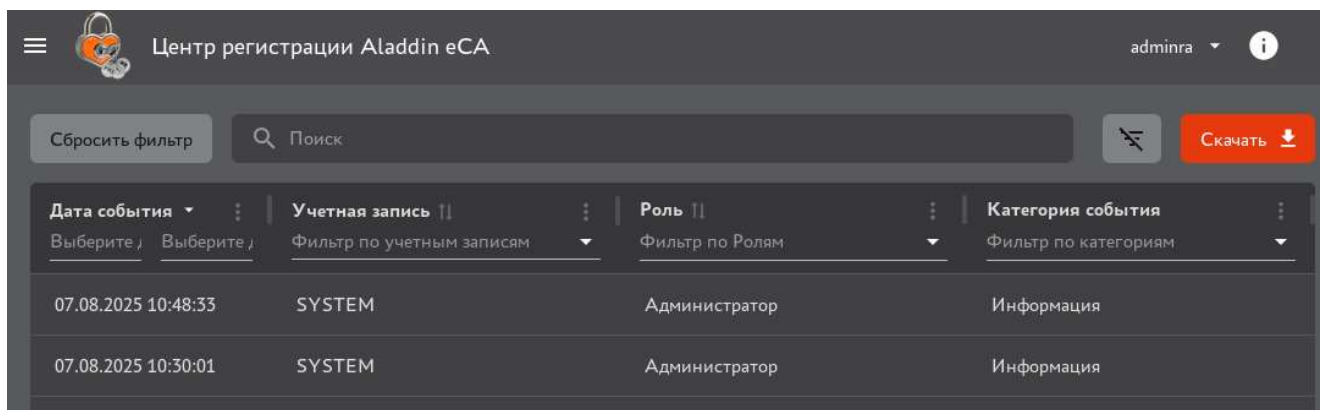






Рисунок 66 - Отображение фильтров в заголовках колонок включено


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

Фильтры по атрибутам событий, представленный в колонках **[Учетная запись]** (см. Рисунок 67а), **[Роль]** (см. Рисунок 67б), **[Категория события]** (см. Рисунок 67в) и **[Код события]** (см. Рисунок 67г) обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов. Фильтр по атрибуту события, представленном в колонке **[Дата события]** (см. Рисунок 67д), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок. Признаком применения фильтра является значок  в заголовке соответствующей колонки (см. Рисунок 67д).

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

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

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

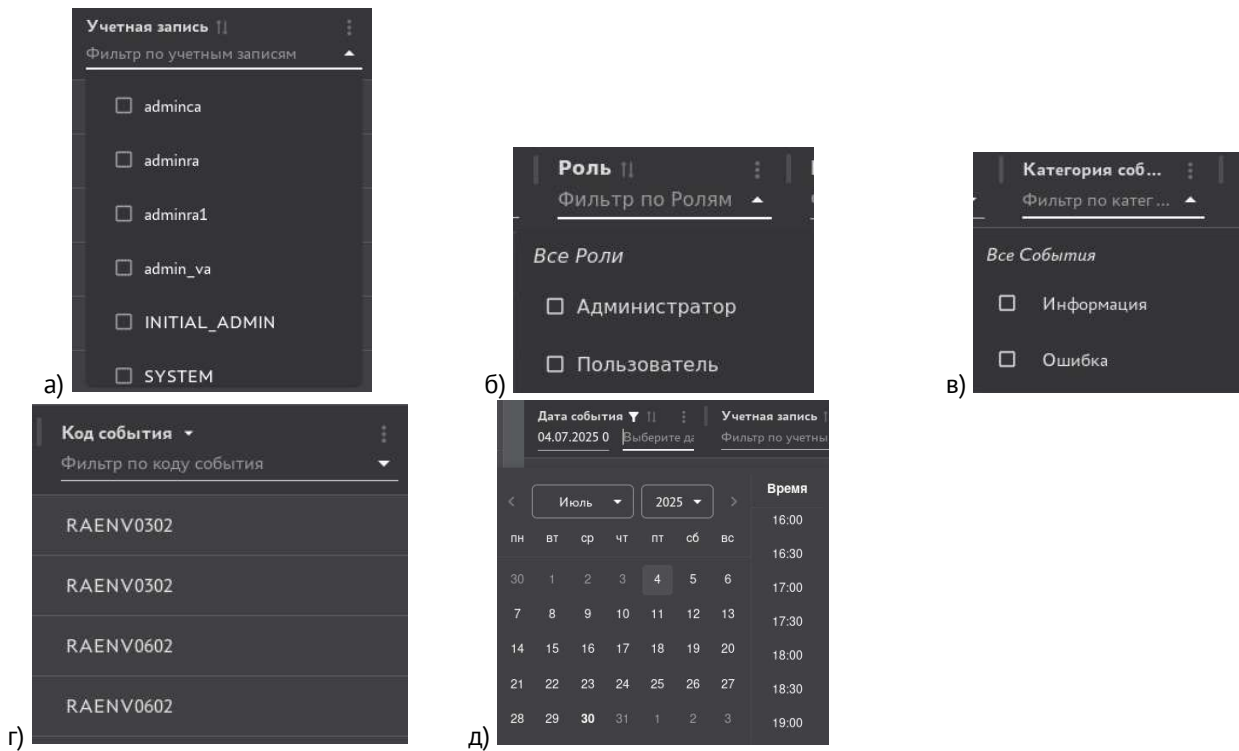



Рисунок 67 - Указание критериев выборки в фильтрах

7.6.3 Просмотр карточки события

Карточка события содержит представленную в удобном для анализа виде подробную информацию о событии (описание атрибутов события см. в разделе 7.6.1).

Чтобы открыть карточку события:

- Подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Журнал событий**.
- Найдите нужное событие и щелкните запись о нем в списке (см. Рисунок 68).

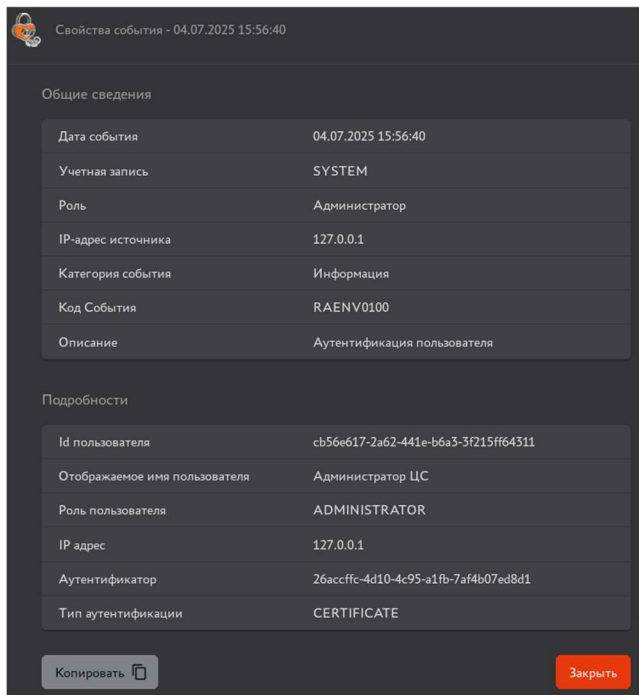
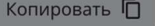


Рисунок 68 - Окно «Свойства события» (карточка события)

Для копирования информации о событии в буфер обмена нажмите кнопку . Содержимое события из буфера обмена можно вставить, например, в текстовый файл (см. Рисунок 69).

```
Общие сведения:
Дата события: 09.06.2025 13:26:15
Учетная запись: SYSTEM
Роль: ADMINISTRATOR
Категория события: INFO
Код События: RAENV0100
Описание: Аутентификация пользователя





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

Рисунок 69 - Пример копирования события в текстовый файл

7.6.4 Экспорт записей журнала событий

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

Порядок экспорта журнала событий:

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

7.6.5 Передача информации о событиях в сторонние системы по протоколу Syslog


Мониторинг событий аудита может выполняться в сторонних SIEM-системах. Передача информации о событиях на принимающие серверы SIEM-систем выполняется по протоколу Syslog (в соответствии с рекомендацией RFC5424). В качестве транспортного протокола для передачи данных может использоваться UDP или TCP. Использование протокола UDP не гарантирует доставку данных принимающей стороне. Максимально возможно добавить и отправлять сообщения на 10 Syslog-серверов.

Значения полей отправляемых Syslog-сообщений о зарегистрированных событиях представлено в таблице ниже.

Таблица 13 - Значения полей отправляемых Syslog-сообщений

Поле сообщения	Syslog-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 Aladdin eRA в формате ISO 8601: YYYY-MM-DDThh:mm:ss[.SSS]
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста Центра регистрации

Поле сообщения	Syslog-описание	Значение
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	<p>[aeca-ra actionCode="actionCode" category="category" id="id" serviceName="serviceName" system="system" username="username" role="role" ipAddress="ipAddress" attributes="attributes"]</p> <p>где:</p> <ul style="list-style-type: none"> – "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. <p>Для категории события «ERROR» (ошибка) также должно передаваться значение поля "description" (причина ошибки) данных события в API.</p>
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»).

Чтобы просмотреть созданные в Центре регистрации Aladdin eRA Syslog-серверы, подключитесь к веб-интерфейсу Центра регистрации Aladdin eRA и перейдите в раздел  **Настройка > Syslog**.

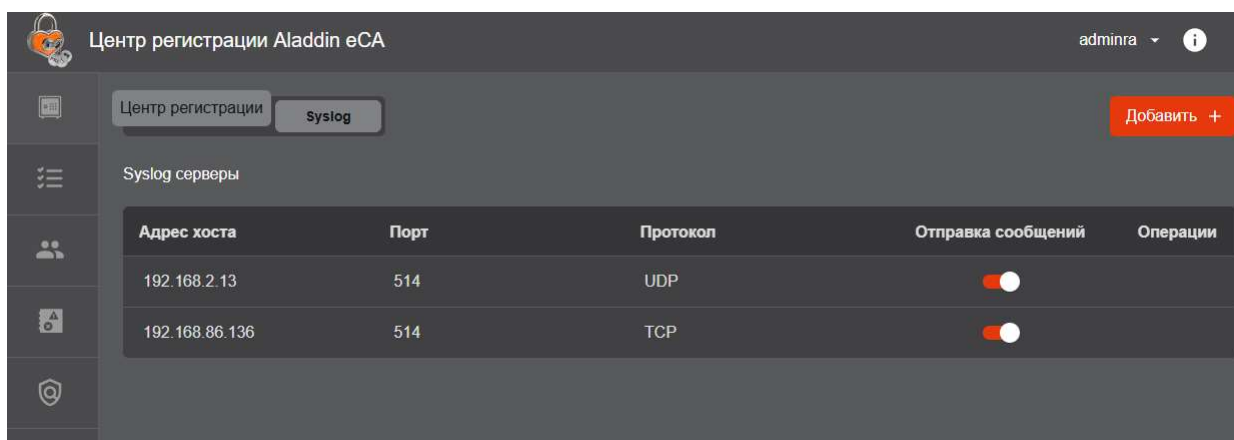




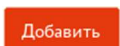
Рисунок 70 - Просмотр списка Syslog-серверов

Записи о Syslog-серверах отображаются списком в табличном виде. По умолчанию в колонках таблицы отображаются следующие атрибуты Syslog-серверов:

- Адрес хоста - IP-адрес или доменное имя Syslog-сервера.
- Входящий порт Syslog-сервера, на который отправляются сообщения (число в диапазоне от 0 до 65535).
- Транспортный протокол, по которому выполняется передача данных.

После добавления нового Syslog-сервера отправка сообщений на него по умолчанию включена. Чтобы управлять передачей данных на выбранный Syslog-сервер, используйте переключатель  в колонке **[Отправка сообщений]**.

Порядок добавления Syslog-сервера:

- На панели инструментов нажмите кнопку .
- В открывшемся окне (см. Рисунок 71) выполните следующие действия:
 - В поле «Адрес хоста» укажите IP-адрес или доменное имя Syslog-сервера.
 - В поле «Порт» укажите входящий порт Syslog-сервера, на который будут отправляться сообщения (число в диапазоне от 0 до 65535).
 - В списке «Протокол» выберите транспортный протокол, по которому будет выполняться передача данных.
 - Нажмите кнопку .

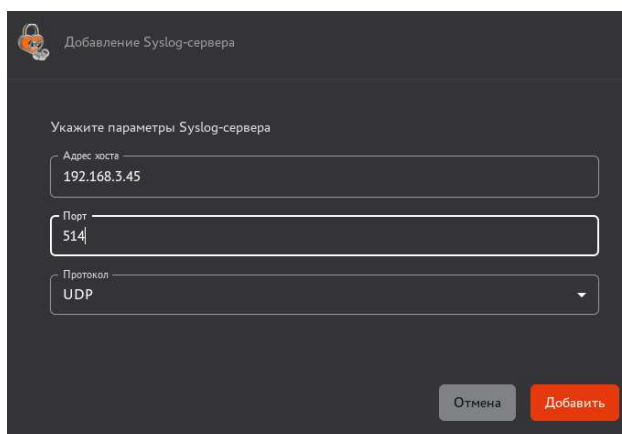






Рисунок 71 - Добавление Syslog-сервера

Чтобы изменить настройки Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Редактировать>** (Рисунок 72) и в открывшемся окне измените параметры Syslog-сервера.

Чтобы удалить Syslog-сервера в строке с записью о выбранном Syslog-сервере щелкните значок  **<Выбрать действие>**, выберите в списке  **<Удалить>** (Рисунок 72) и в открывшемся окне подтвердите удаление Syslog-сервера.

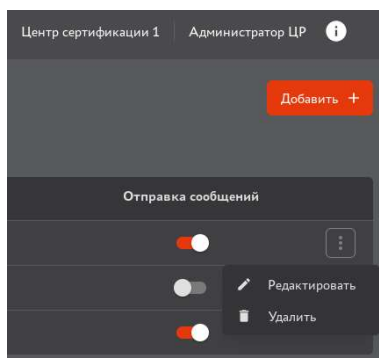


Рисунок 72 - Выбор действия с Syslog-сервером

7.7 Раздел «Управление»

Раздел «Управление» содержит вкладки «Правила выпуска» и «SCEP» (см. Рисунок 73).
 Данный раздел доступен только для администратора.

7.7.1 Вкладка «Правила выпуска»

Вкладка «Правила выпуска» (см. Рисунок 73) раздела «Управление» обеспечивает возможности создания, изменения, удаления правил выпуска сертификатов, также управления статусами правил выпуска.

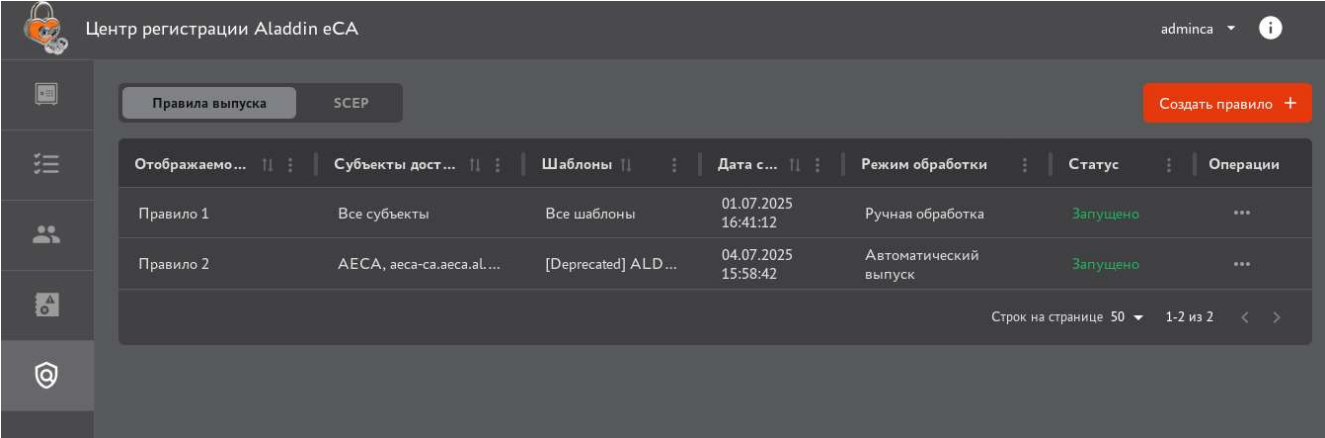


Рисунок 73 - Экран раздела «Управление». Вкладка «Правила выпуска»

Во вкладке «Правила выпуска» раздела «Управление» в табличной форме отображена информация о существующих правилах выпуска, представленная в таблице ниже (Таблица 14).


Таблица 14 - 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»

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

- Создание нового правила выпуска;
- Редактирование правила выпуска;
- Запуск и остановка правила выпуска;
- Копирование правила выпуска;
- Удаление правила выпуска.

7.7.1.1 Управление экранной таблицей

Для каждой колонки экранной таблицы (справа от названия заголовка) доступна кнопка управления действиями  <Действия в колонке>. По нажатию данной кнопки разворачивается меню (см. Рисунок 74), в котором возможно (в зависимости от применённых ранее действий - фильтр, сортировка, изменение ширины, скрытие колонки):

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

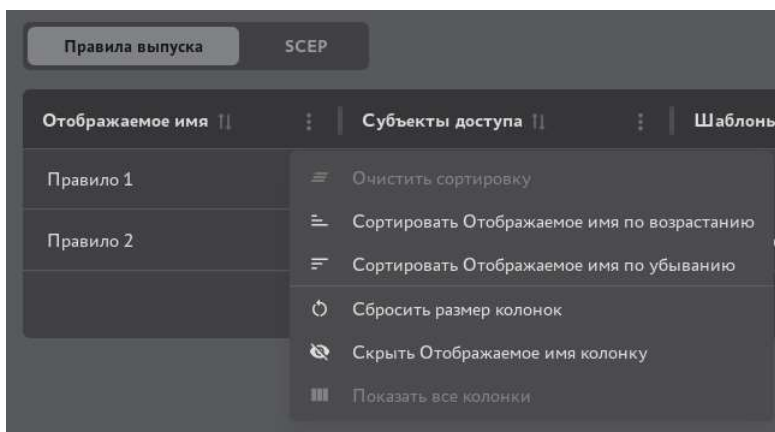


Рисунок 74 - Кнопка <Действия в колонке>

7.7.1.2 Сортировка событий

Средства сортировки событий в разделе «Правила выпуска» представлены элементами выбора направления сортировки в заголовке таблицы экранной формы (см. Рисунок 75)

- Отображаемое имя - упорядочивание осуществляется в алфавитном порядке.
- Субъекты доступа - упорядочивание осуществляется в алфавитном порядке.
- Шаблоны - упорядочивание осуществляется в алфавитном порядке.
- Дата создания - упорядочивание выполняется по дате и времени создания правила в порядке убывания или возрастания временных меток.

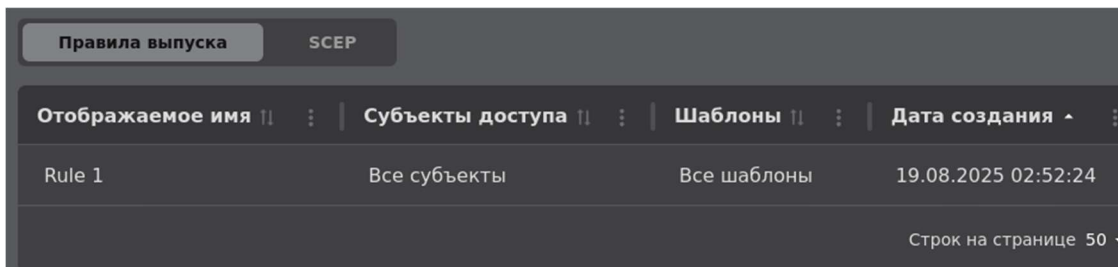




Рисунок 75 - Поля сортировки содержимого экрана раздела «Правила выпуска»

Для выполнения сортировки по выбранной колонке таблицы нажмите на заголовок выбранной колонки или используйте кнопку <Действие колонки>.

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

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

Для сброса сортировки в каждой колонке:

- нажмите кнопку  <Действия в колонке> и в раскрывшемся списке выберите пункт «Очистить сортировку»;
- или несколько раз нажмите на заголовке колонки, для которой применена сортировка.

7.7.1.3 Создание правила выпуска

Для создания правила выпуска выполните следующие шаги:

- Нажмите кнопку <Создать правило +> на главном экране раздела «Управление» (см. Рисунок 73).
- В открывшемся окне укажите отображаемое имя для создаваемого правила выпуска (см. Рисунок 76). Далее нажмите кнопку <Продолжить> для перехода к следующему шагу.

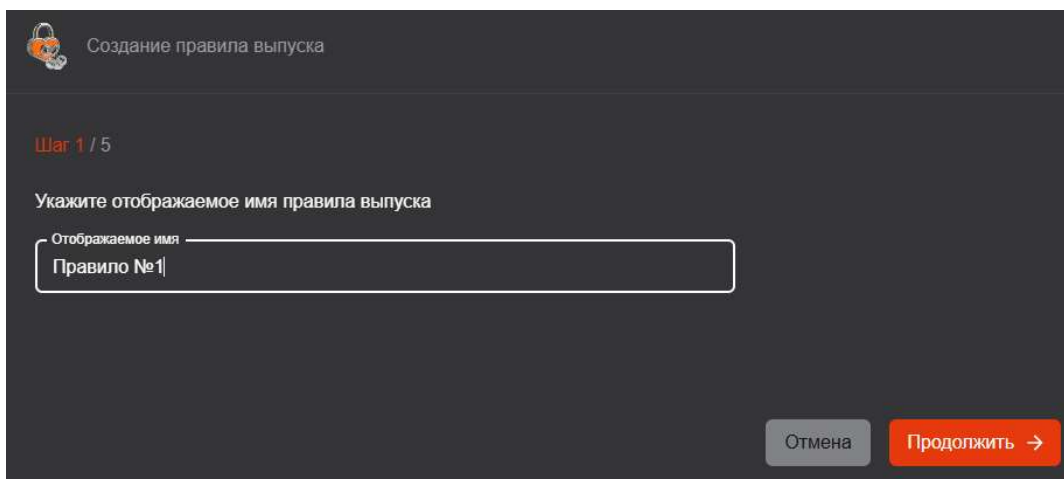


Рисунок 76 - Окно создания правила выпуска. Шаг 1. Отображаемое имя

- На втором шаге выберите субъекты доступа для создаваемого правила. Допустимые варианты выбора субъектов доступа:
 - «Все субъекты» (см. Рисунок 77). 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;

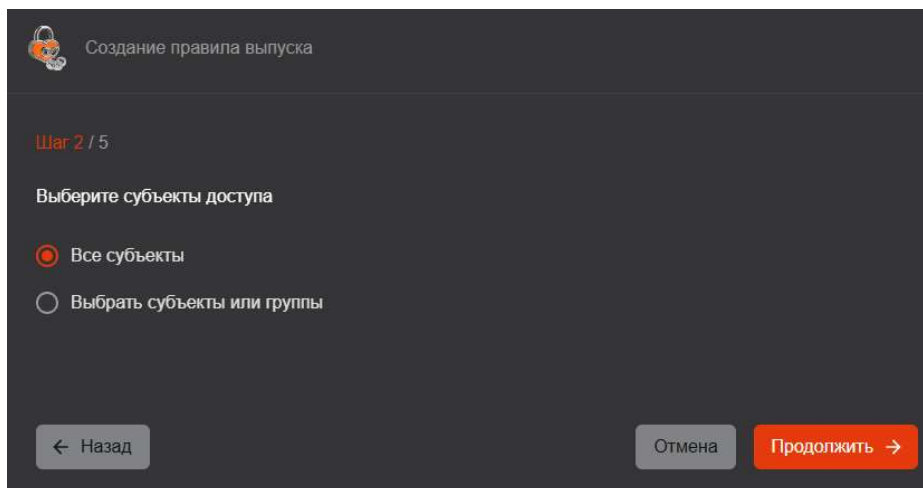


Рисунок 77 - Окно создания правила выпуска. Шаг 2. Выбор субъектов - Все субъекты

«Выбрать субъекты или группы» (см. Рисунок 78). 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.

Создание правила выпуска

Шаг 2 / 5

Выберите субъекты доступа

☐ Все субъекты

☒ Выбрать субъекты или группы

Домен

Тип

Группы

Вложенные группы не наследуют правила выпуска от вышестоящих групп

Выбрать 0/50 выбрано

- ☐ IIS_IUSRS (домен: al)
- ☐ Incoming Forest Trust Builders (домен: al)
- ☐ PKI (домен: al)

Выбрано 0/2 выбрано

- ☐ DnsAdmins (домен: al)
- ☐ DnsUpdateProxy (домен: al)

Назад Отмена Продолжить

Рисунок 78 - 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 79). 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.

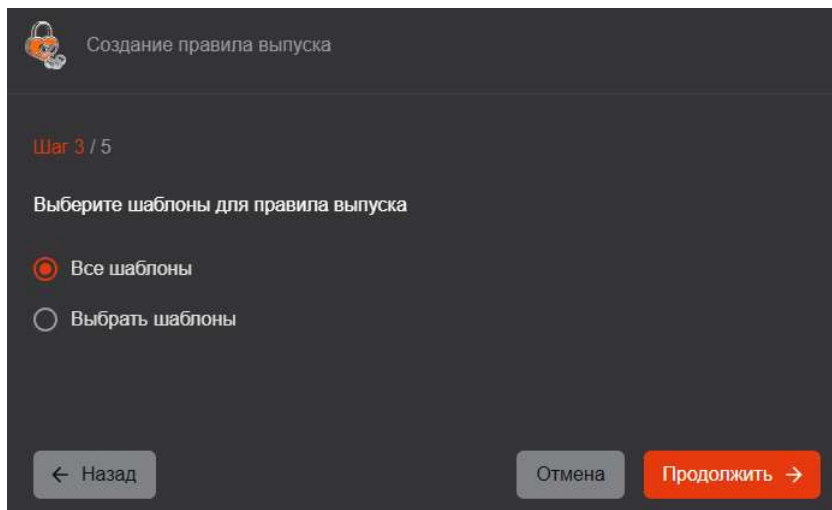


Рисунок 79 - Окно создания правила выпуска. Шаг 3. Выбор шаблонов - Все шаблоны

- «Выбрать шаблоны» (см. Рисунок 80). 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.

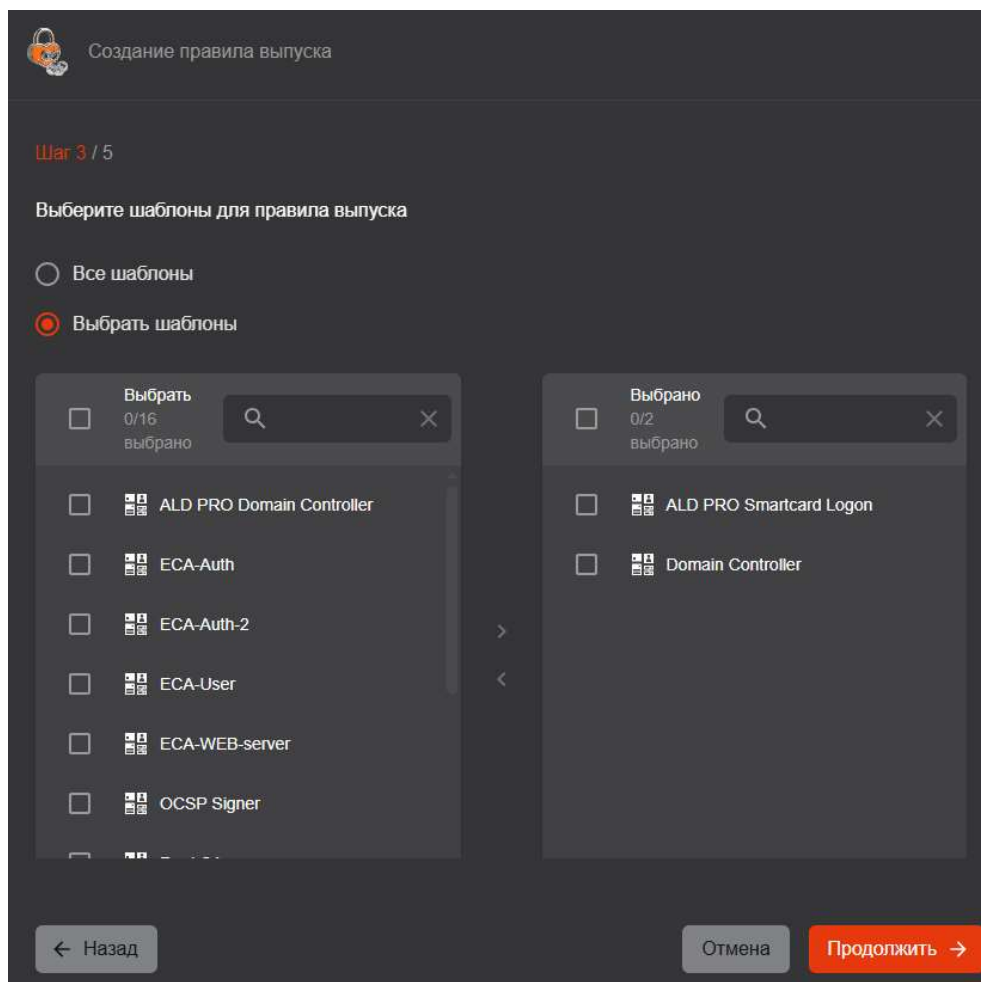


Рисунок 80 - Окно создания правила выпуска. Шаг 3. Выбор шаблонов - Выбрать шаблоны

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

- На четвертом шаге выберите режим обработки заявок для создаваемого правила выпуска (см. Рисунок 80). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка», «Отклонение заявки».

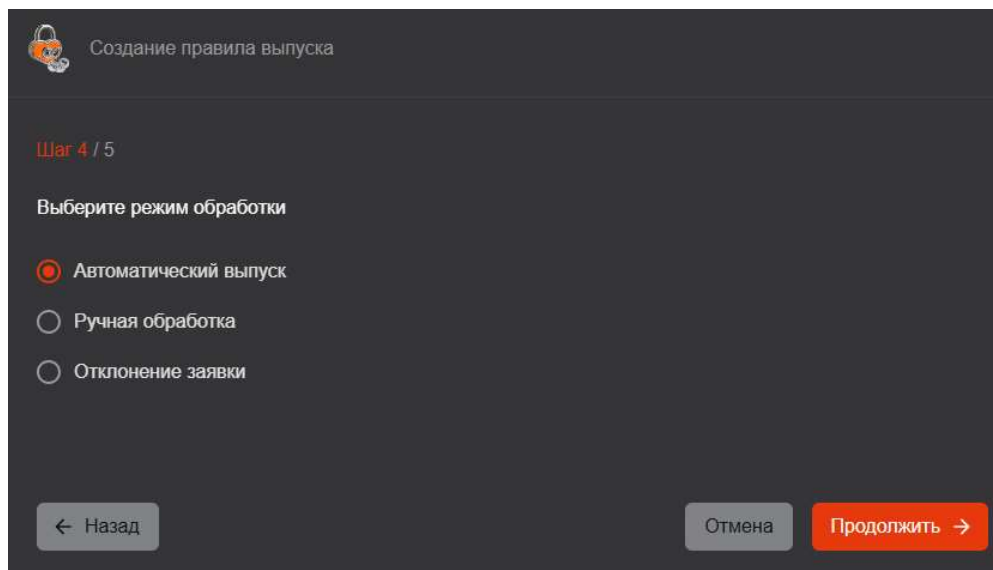


Рисунок 81 - Окно создания правила выпуска. Шаг 4. Выбор режима обработки

- 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 82).

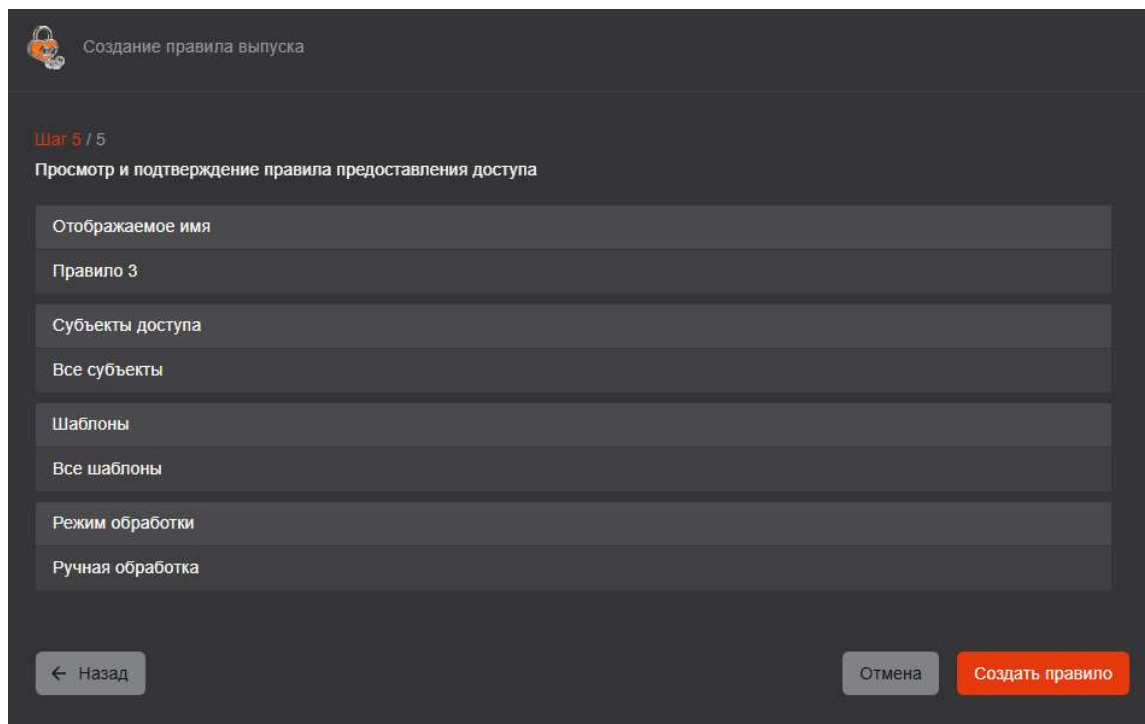


Рисунок 82 - Окно создания правила выпуска. Шаг 5. Подтверждение перед созданием

- Для создания правила выпуска нажмите на кнопку <Создать правило>. После этого окно создания закроется, и созданное правило выпуска появится в списке правил выпуска в разделе «Управление».

7.7.1.4 Редактирование правила выпуска

Для редактирования правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо отредактировать, нажмите на кнопку <Операции> и выберите опцию <Редактировать> (см. Рисунок 83).

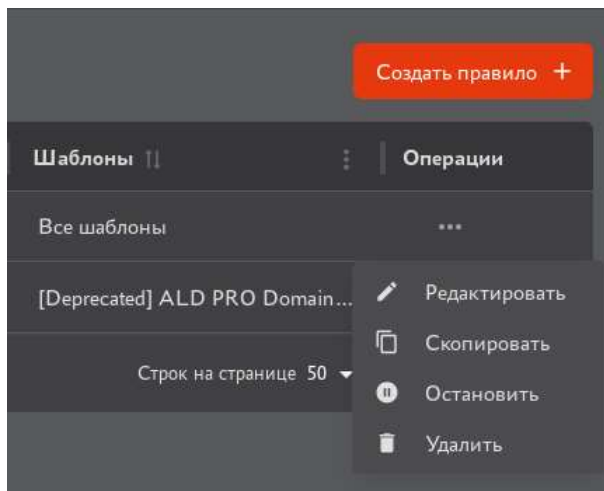


Рисунок 83 - Экран раздела «Управление». Вкладка «Правила выпуска». Редактирование правила выпуска

- В открывшемся окне «Редактирование правила выпуска» на первом шаге осуществляется редактирование отображаемого имени правила выпуска (см. Рисунок 84).

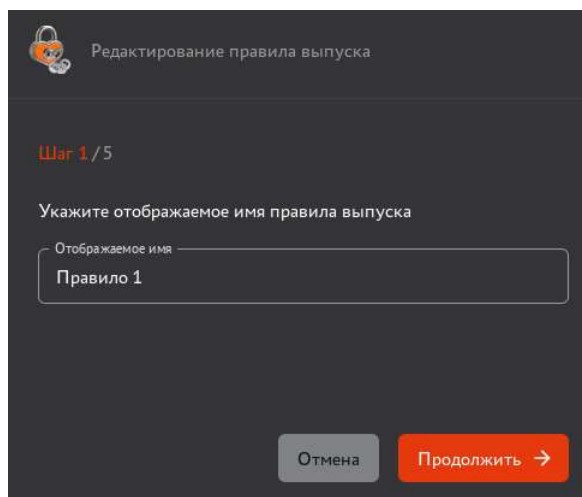


Рисунок 84 - Окно редактирования правила выпуска. Шаг 1. Отображаемое имя

- 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 85 и Рисунок 86). Редактирование субъектов доступа для правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.3). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

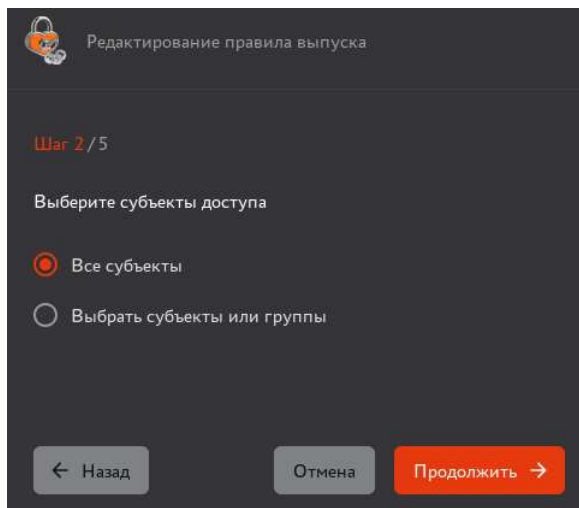


Рисунок 85 - Окно редактирования правила выпуска. Шаг 2. Выбор субъектов - Все субъекты

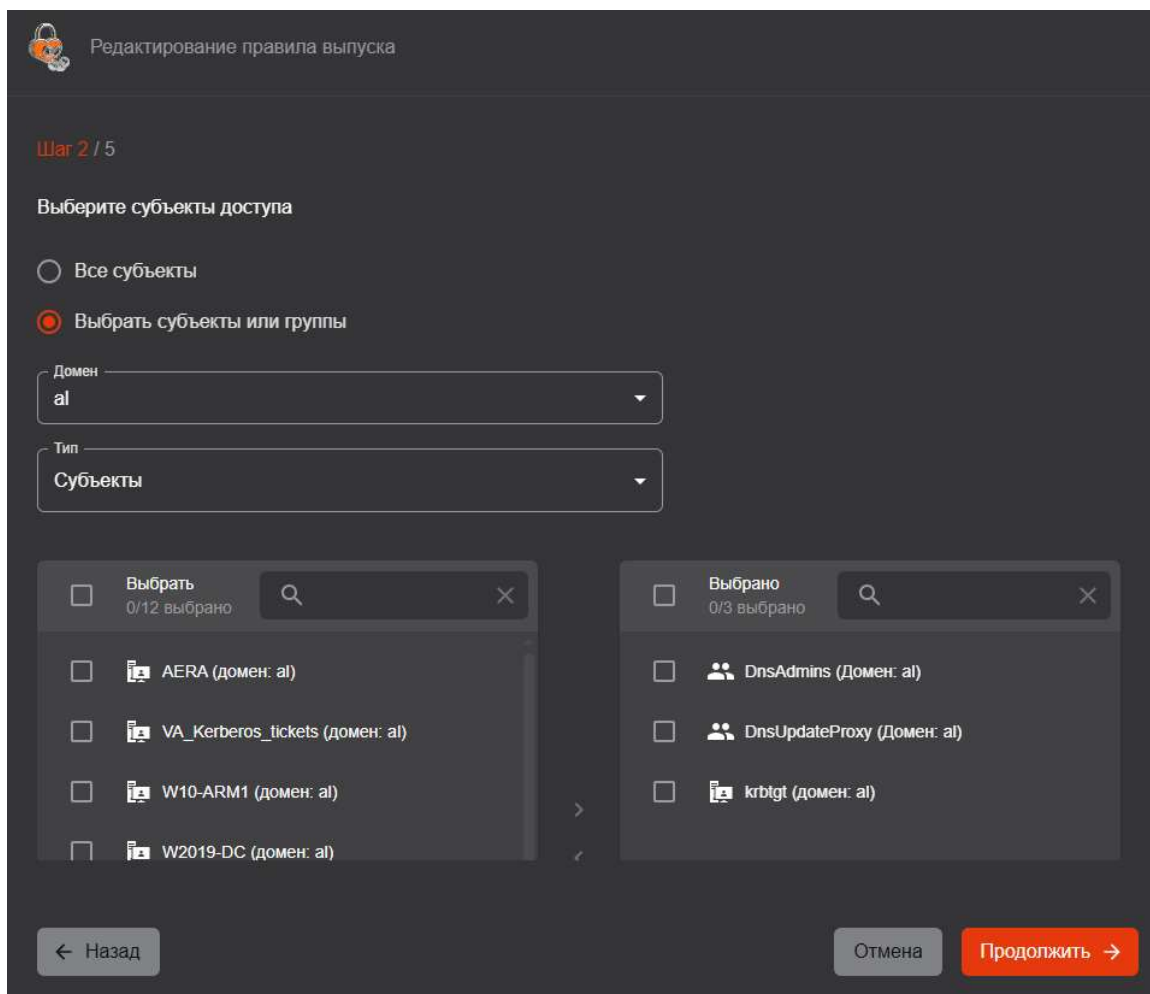


Рисунок 86 - Окно редактирования правила выпуска. Шаг 2. Выбор субъектов - Выбрать субъекты

- На шаге 3 окна «Редактирование правила выпуска» осуществляется редактирование шаблонов для правила выпуска (см Рисунок 87 и Рисунок 89). Редактирование перечня шаблонов правила выпуска осуществляется аналогично их выбору при создании правила выпуска (см. раздел 7.7.1.3). В случае, если из правого столбца («Выбрано») исключены все элементы, переход на следующий шаг недоступен.

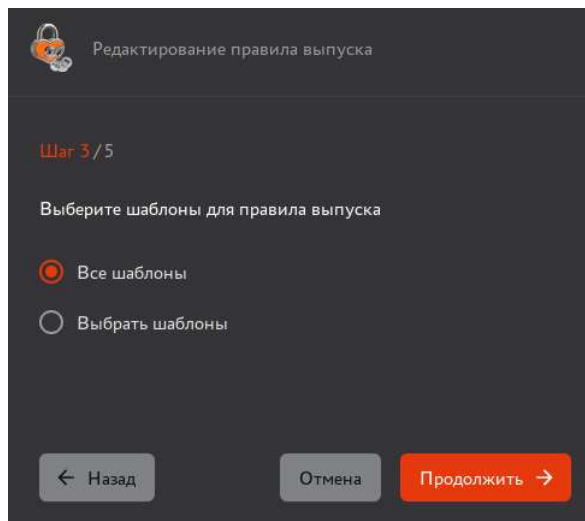


Рисунок 87 - Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов - Все шаблоны

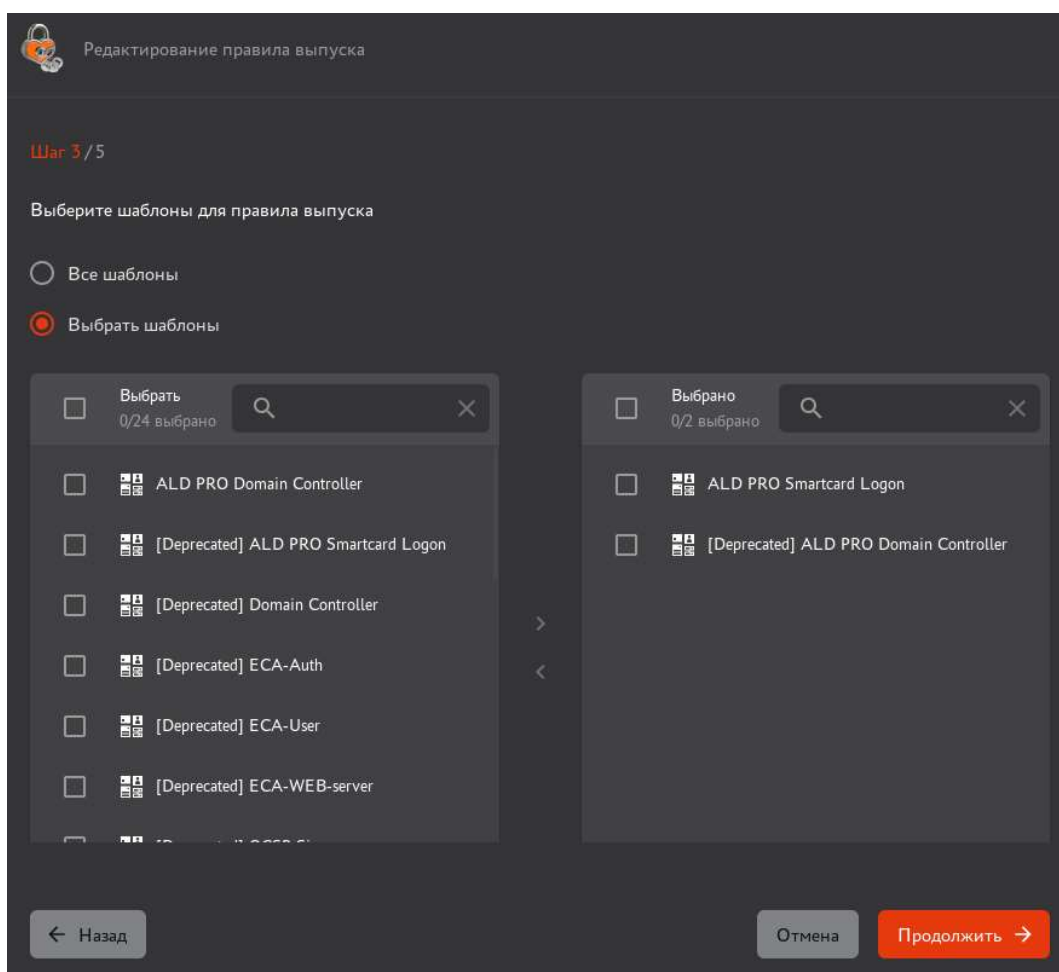


Рисунок 88 - Окно редактирования правила выпуска. Шаг 3. Выбор шаблонов - Выбрать шаблоны

- На шаге 4 окна «Редактирование правила выпуска» осуществляется редактирование режима обработки заявок для правила выпуска (см. Рисунок 89). Режим обработки выбирается из следующих вариантов: «Автоматический выпуск», «Ручная обработка» и «Отклонение заявки».

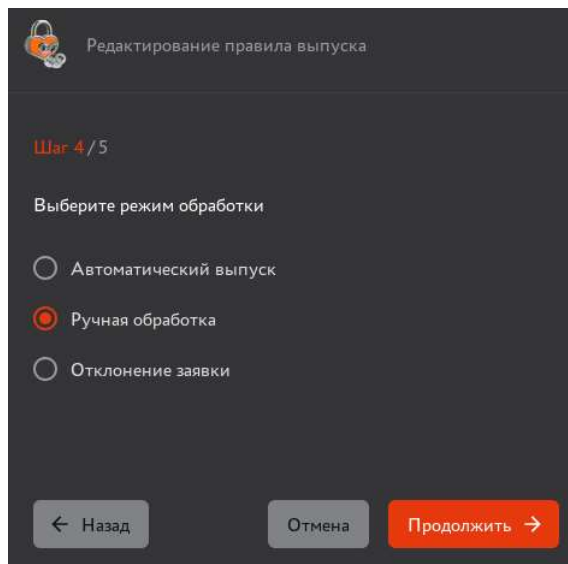


Рисунок 89 - Окно редактирования правила выпуска. Шаг 4. Выбор режима обработки

- 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 90).

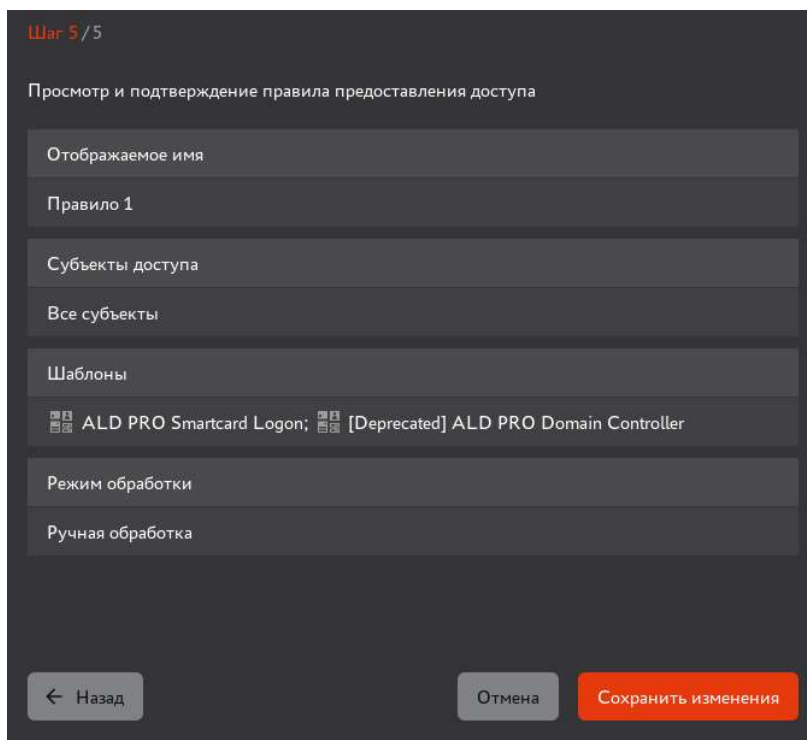



Рисунок 90 - Окно редактирования правила выпуска. Шаг 5. Подтверждение

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

7.7.1.5 Запуск правила выпуска

Запуск может быть выполнен только для правил выпуска в статусе «Остановлено».

Для запуска правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо запустить, нажмите на кнопку «Операции»  и выберите опцию «Запустить» (см. Рисунок 91).

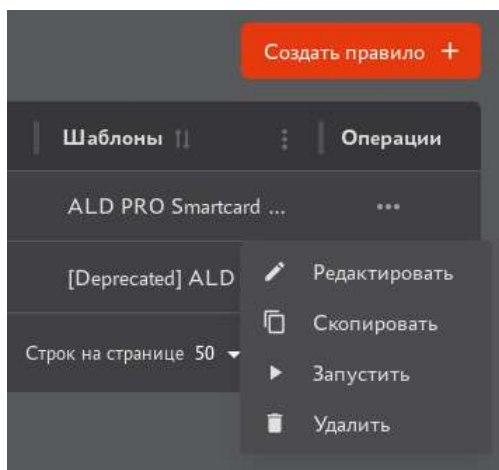


Рисунок 91 - Экран раздела «Управление». Вкладка «Правила выпуска». Запуск правила выпуска

- В появившемся окне подтверждения операции запуска (см. Рисунок 92) нажмите на кнопку <Запустить>. После нажатия на неё правило выпуска будет запущено и будет использоваться при обработке заявок.

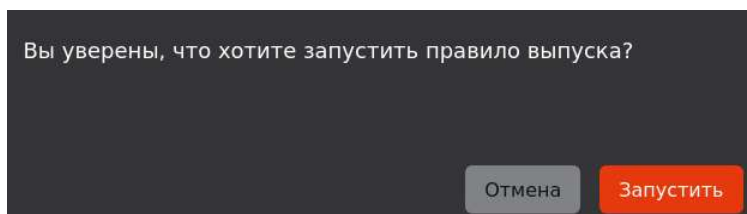



Рисунок 92 - Окно подтверждения запуска правила выпуска

7.7.1.6 Остановка правила выпуска

Остановка может быть выполнена только для правил выпуска в статусе «Запущено».

Для остановки правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо остановить, нажмите на кнопку <Операции>  и выберите опцию <Остановить> (см. Рисунок 93).

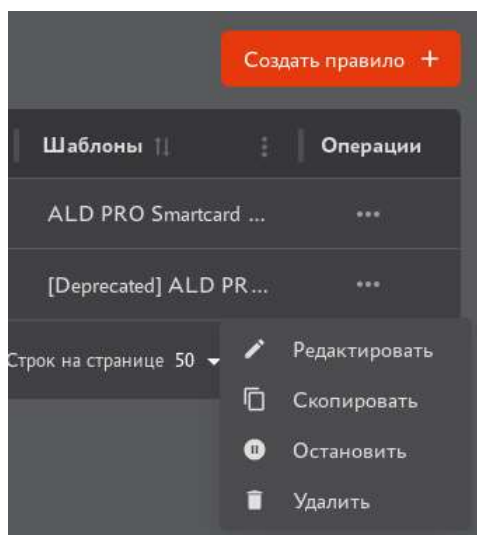


Рисунок 93 - Экран раздела «Управление». Вкладка «Правила выпуска». Остановка правила выпуска

- В появившемся окне подтверждения операции остановки (см. Рисунок 94) нажмите на кнопку <Остановить>. После нажатия на неё правило выпуска будет остановлено и не будет использоваться при обработке заявок.

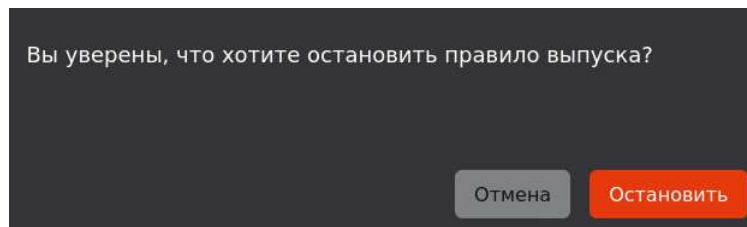



Рисунок 94 - Окно подтверждения остановки правила выпуска

7.7.1.7 Копирование правила выпуска

Для копирования правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо скопировать, нажмите на кнопку <Операции>  и выберите опцию <Скопировать> (см. Рисунок 93).
- В появившемся окне подтверждения операции копирования (см. Рисунок 95) нажмите на кнопку <Скопировать>. После нажатия на неё правило выпуска будет скопировано, при этом созданное правило выпуска будет находиться в статусе «Запущено».

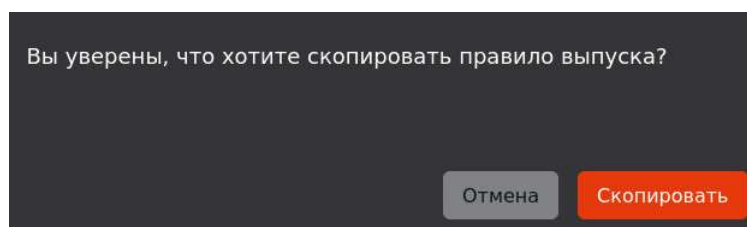



Рисунок 95 - Окно подтверждения копирования правила выпуска

7.7.1.8 Удаление правила выпуска

Для удаления правила выпуска выполните следующие шаги:

- Найдите правило выпуска, которое необходимо удалить, нажмите на кнопку <Операции>  и выберите опцию <Удалить> (см. Рисунок 93).
- В появившемся окне подтверждения операции удаления (см. Рисунок 96) нажмите на кнопку <Удалить>. После нажатия на неё правило выпуска будет удалено.

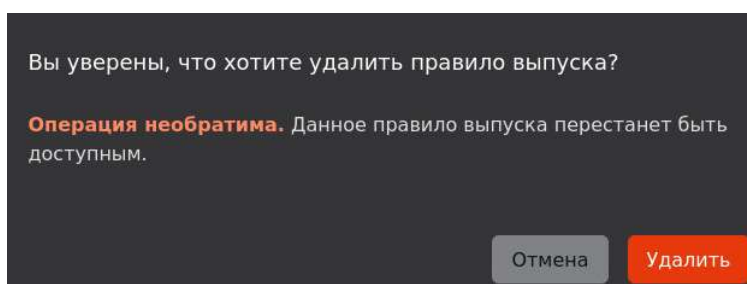


Рисунок 96 - Окно подтверждения удаления правила выпуска

7.7.2 Вкладка «SCEP»

Вкладка «SCEP» (см. Рисунок 97) 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».

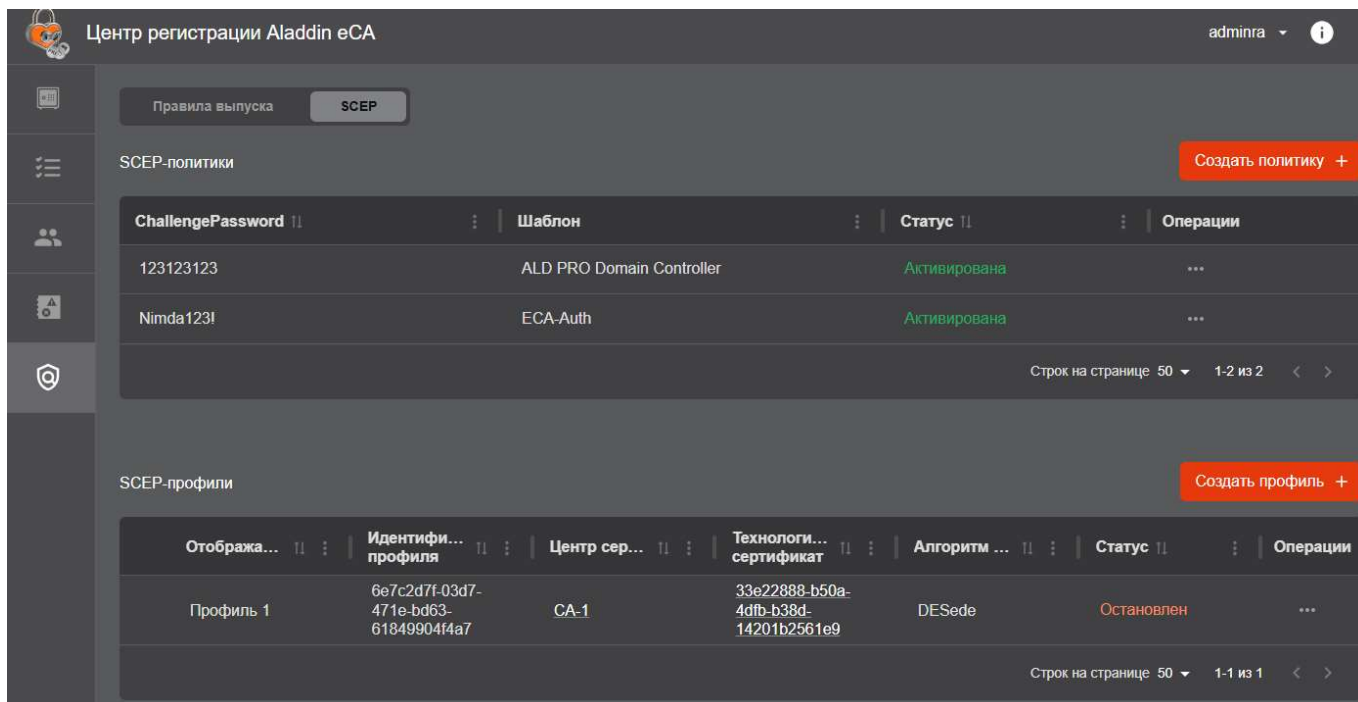


Рисунок 97 - Экран раздела «Управление». Вкладка «SCEP»

- 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 открывшемся окне «Создание SCEP-политики» (см. Рисунок 98) 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 98 - Окно «Создание SCEP-политики»

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

Внимание! В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском интерфейсе 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 99).

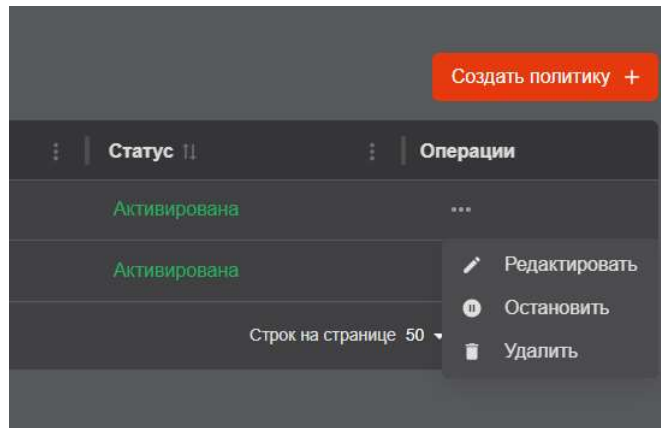


Рисунок 99 - Экран раздела «Управление». Вкладка «SCEP». Редактирование SCEP-политики

- В отрывшемся окне «Редактирование SCEP-политики» (см. Рисунок 100) 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».

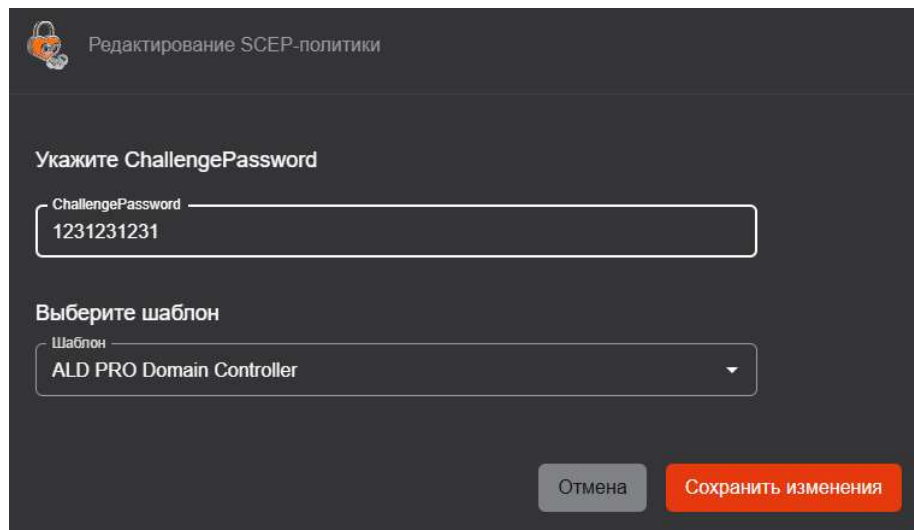


Рисунок 100 - Окно «Редактирование SCEP-политики»

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

Внимание! В случае, если указанный ChallengePassword уже используется в существующей SCEP-политике, после нажатия на кнопку «Создать политику» в пользовательском интерфейсе 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 101).

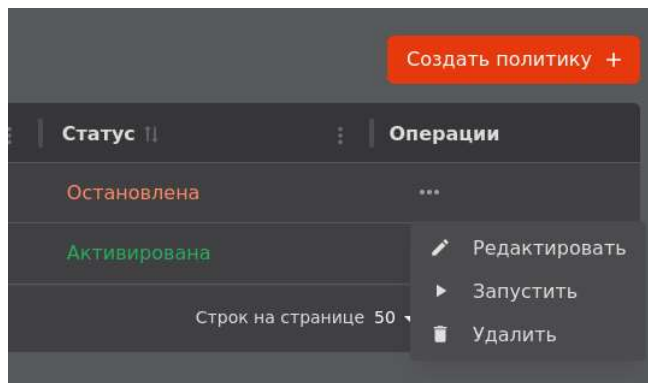


Рисунок 101 - Экран раздела «Управление». Вкладка «SCEP». Запуск SCEP-политики

- В открывшемся окне подтверждения операции запуска (см. Рисунок 102) нажмите на кнопку <Запустить>. После нажатия на неё SCEP-политика будет запущена.

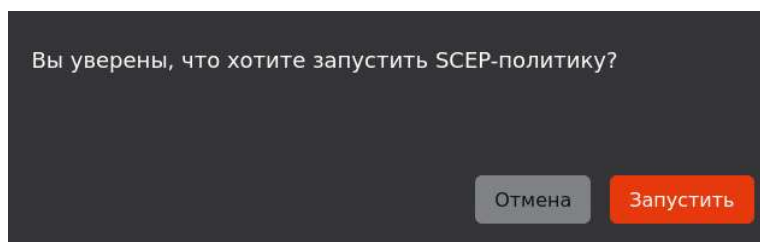


Рисунок 102 - Окно подтверждения запуска SCEP-политики

7.7.2.4 Остановка SCEP-политики

Остановка может быть выполнена только для SCEP-политик в статусе «Активирована». Для остановки SCEP-политики выполните следующие шаги:

- Найдите SCEP-политику, которую необходимо остановить, нажмите на кнопку <Операции> и выберите опцию <Остановить> (см. Рисунок 103).

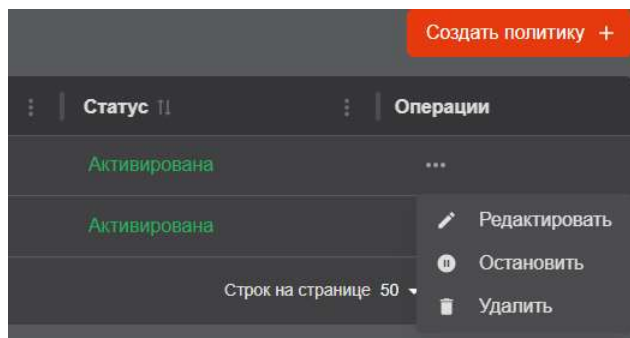


Рисунок 103 - Экран раздела «Управление». Вкладка «SCEP». Остановка SCEP-политики

- В появившемся окне подтверждения операции остановки (см. Рисунок 104) нажмите на кнопку <Остановить>. После нажатия на неё SCEP-политика будет остановлена.

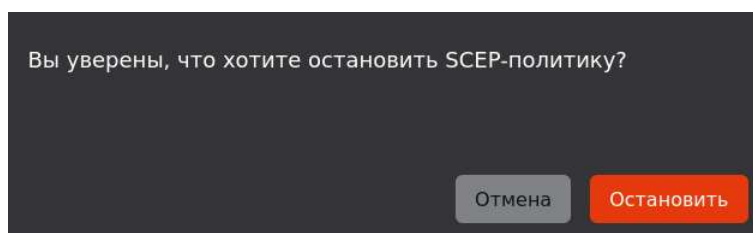



Рисунок 104 - Окно подтверждения остановки SCEP-политики

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 105).

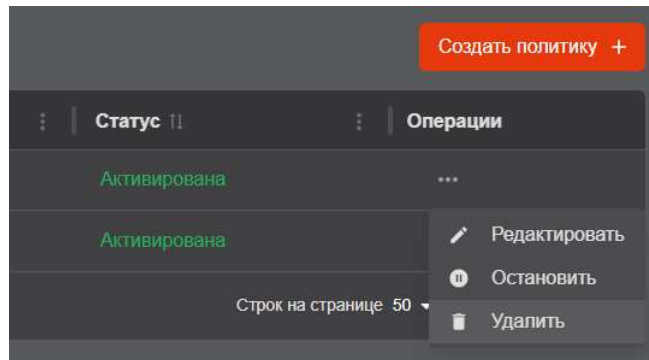


Рисунок 105 - Экран раздела «Управление». Вкладка «SCEP». Удаление SCEP-политики

- В появившемся окне подтверждения операции удаления (см. Рисунок 106) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-политика будет удалена.

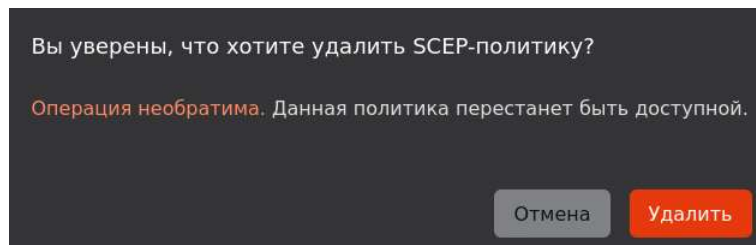



Рисунок 106 - Окно подтверждения удаления SCEP-политики

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 98) 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.
- Далее нажмите на кнопку <Создать профиль>.
- При успешном создании созданный SCEP-профиль будет отображаться в списке SCEP-профилей на вкладке «SCEP» в разделе «Управление».

Внимание! Работа со SCEP-профилями Центров сертификации 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 о его неработоспособности.

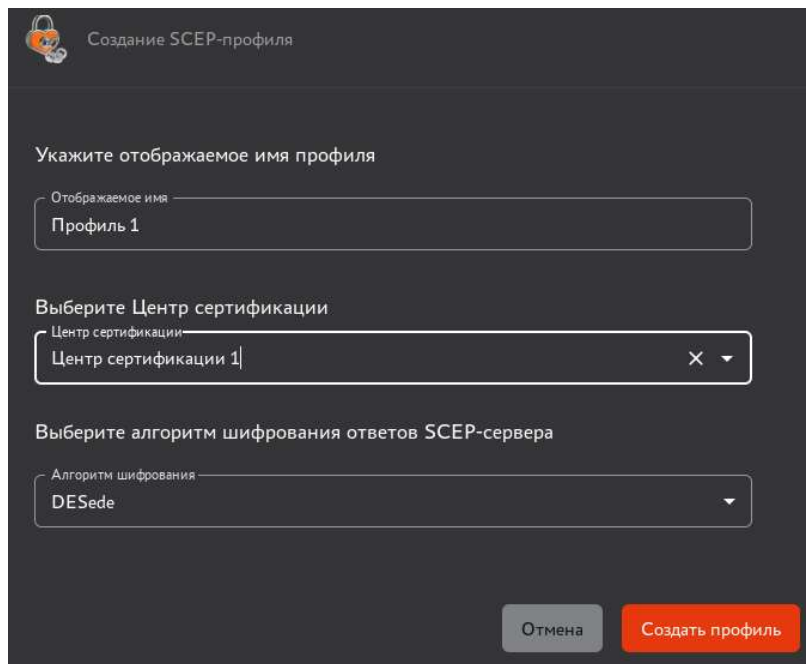


Рисунок 107 - Окно «Создание SCEP-профиля»

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 108).

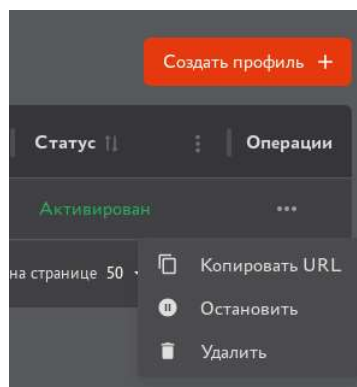


Рисунок 108 - Экран раздела «Управление». Вкладка «SCEP». Копирование URL

После этого буфер обмена будет содержать URL адреса SCEP-сервера выбранного SCEP-профиля (см. Рисунок 109).

`https://rasberos8.msad.aldn/scep-service/profiles/419d9801-e7a8-4ca6-82ab-f9570a55b704/engine`

Рисунок 109 - 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 108).
- В появившемся окне подтверждения операции (см. Рисунок 112) нажмите на кнопку <Остановить>.

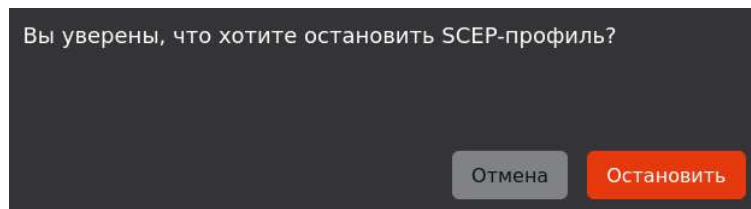



Рисунок 110 - Окно подтверждения остановки SCEP-профиля

В результате SCEP-профиль будет остановлен (статус «Остановлен»)

Чтобы активировать (запустить) SCEP-профиль найдите его в списке, нажмите на кнопку <Операции>  и выберите в списке <Запустить>. В открывшемся окне подтвердите запуск профиля, нажав кнопку <Запустить>.

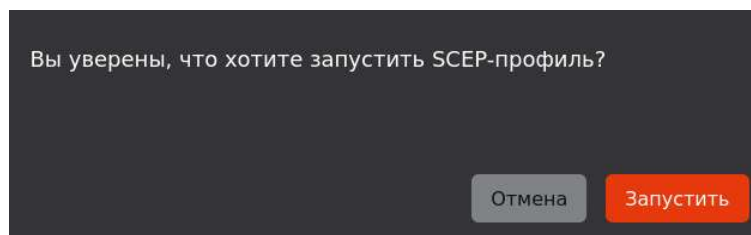



Рисунок 111 - Окно подтверждения запуска SCEP-профиля

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 108).
- В появившемся окне подтверждения операции удаления (см. Рисунок 112) нажмите на кнопку <Удалить>. После нажатия на неё SCEP-профиль будет удален.

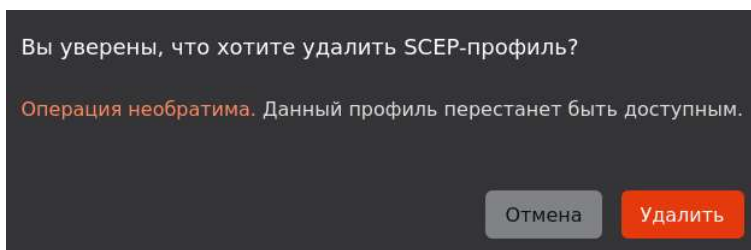


Рисунок 112 - Окно подтверждения удаления SCEP-профиля

7.8 Смена сертификата веб-сервера

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

Для смены сертификата веб-сервера выполните следующие действия:

- Подключитесь к веб-интерфейсу Центра валидации Aladdin eVA и перейдите в раздел  **Настройка > Веб-сервер** (Рисунок 113).

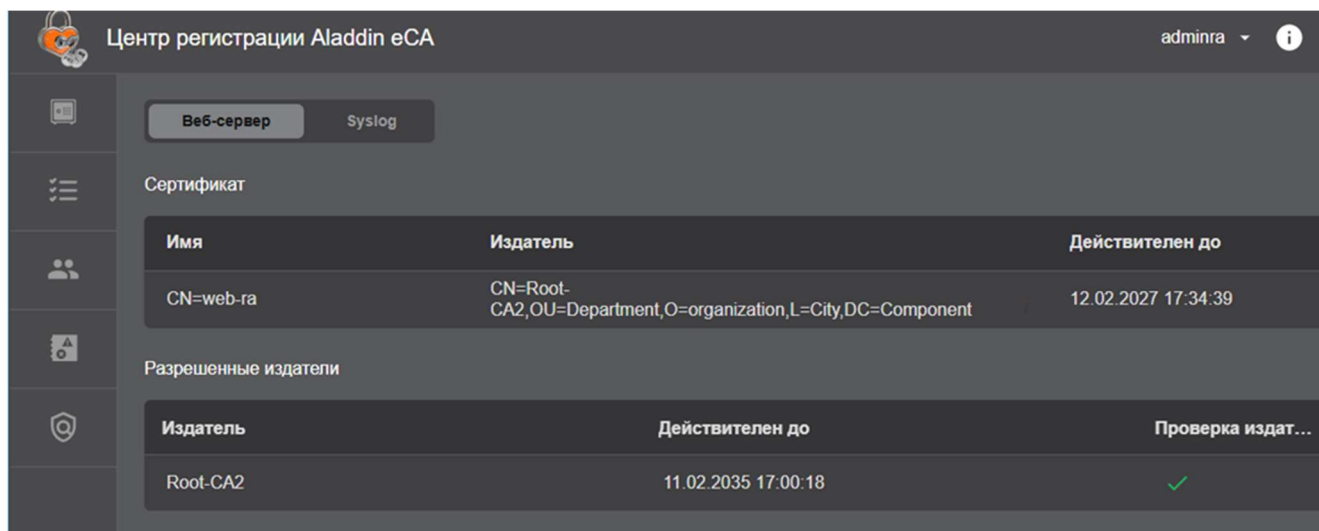




Рисунок 113 - Смена сертификата веб-сервера

Информация об установленном сертификате отображается в разделе «Сертификат» в табличном виде и содержит:

- «Имя» - CN, указанный в сертификате.
- «Издатель» - SDN издателя сертификата.
- «Действителен до» - дата окончания действия сертификата.
- Наведите на запись о веб-сервере и нажмите появившуюся кнопку .
- В появившемся окне (см. Рисунок 114) выберите файл сертификата и введите пароль от контейнера.
- Нажмите кнопку  **Сменить ключи**.

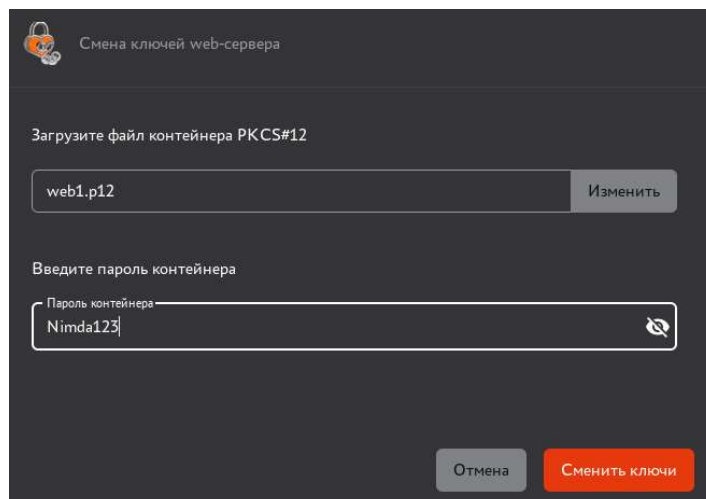




Рисунок 114 - Окно смены ключей веб-сервера

- В открывшемся окне с сообщением об успешной смене ключей нажмите кнопку .


В результате будет выполнена автоматическая перезагрузка веб-сервера. В результате перезагрузки веб-сервера в журнале событий будет зарегистрировано событие с кодом RAENV0700 в случае успешной перезагрузки веб-сервера или событие с кодом RAENV0701 в случае ошибки в процессе перезагрузки веб-сервера.

7.9 Просмотр информации о разрешённых издателях

Для доступа пользователей с ролями «Администратор» и «Оператор» к текущему веб-серверу необходимо, чтобы для издателя (Центра сертификации) сертификата учётной записи была включена проверка (издатель включен в список разрешенных). С сертификатом, выпущенным исключённым из списка разрешенных издателем, аутентификация пользователя будет невозможна.

Для просмотра списка разрешенных издателей подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA и перейдите в раздел  **Настройка > Веб-сервер**.

Информация о разрешенных издателях отображается в разделе «Разрешенные издатели» (Рисунок 113) списком в табличном виде и содержит:

- «Издатель» - CN, указанный в сертификате Центра сертификации.
- «Действителен до» - дата окончания действия сертификата Центра сертификации.
- «Проверка издателя» - статус издателя (разрешенные издатели помечены значком ).

8 ПОДДЕРЖКА ПРОТОКОЛА SCEP

Центр регистрации Aladdin eCA реализует серверный компонент по протоколу SCEP¹ (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 сохраняет его в своей базе данных.

В дальнейшем технологический сертификат SCEP-профиля используется в обработке запросов по протоколу SCEP (см. раздел 8.2).

8.1 Настройка SCEP-сервера

Для настройки SCEP-сервера 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 сервера Центра регистрации Aladdin eRA;
- «profileId» - идентификатор существующего SCEP-профиля.
- Далее URL созданного SCEP-профиля следует использовать при добавлении конфигурации SCEP-сервера. Получить URL можно с помощью функции копирования URL адреса SCEP-профиля - см. раздел 7.7.2.7. Пример команды certmonger² для добавления SCEP-сервера³:

¹ Протокол SCEP описан в RFC8894, см.: <https://datatracker.ietf.org/doc/html/rfc8894>

² Certmonger — это служба, которая управляет сертификатами и их жизненным циклом в системах Linux.

³ Для выполнения команд ниже необходимо, чтобы был установлен пакет `certmonger`.

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

Для проверки следует использовать команду:

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

8.2 Обработка запросов по протоколу SCEP

Центр регистрации Aladdin eRA реализовывает обработку следующих запросов клиента по протоколу SCEP¹:

- 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 (SUCCESS).
 - 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 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 (SUCCESS).

¹ Запрос «GetNextCACert» на данный момент не поддерживается SCEP-сервером Центра регистрации Aladdin eRA.

- 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 своей 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 своей базе данных заявки, по которой выпущенный сертификат имеет серийный номер, соответствующий указанному в сообщении серийному номеру. Поиск осуществляется только среди заявок, сертификат по которым выпущен 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:

- 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-XCEP¹ и MS-WSTEP². 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 «GetPolicies») и функций CES-сервера (при получении запроса на выпуск сертификата «RequestSecurityToken») обеспечивает следующие способы аутентификации пользователей домена, к которому он подключен:

- по имени пользователя и паролю;
- по Kerberos-билету.

9.1 Обработка запроса на политики «GetPolicies»

Центр регистрации Aladdin eRA при получении запроса «GetPolicies» в случае успешной аутентификации пользователя, от имени которого был выполнен запрос, возвращает в ответе «GetPoliciesResponse» политику выпуска сертификатов.

Общие параметры возвращаемой политики соответствуют таблице ниже (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:

¹ Описание протокола MS-XCEP доступно по ссылке: <https://winprotocoldoc.z19.web.core.windows.net/MS-XCEP/%5bMS-XCEP%5d.pdf>

² 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 CER записываются значения в соответствии с таблицей ниже (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 ¹
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 ²
enrollmentFlags	0
generalFlags	0 - для типа субъекта шаблона «Пользователь», 64 - для типа субъекта шаблона «Устройство», 128 - для типа субъекта шаблона «Корневой ЦС», 2048 - для типа субъекта шаблона «Подчиненный ЦС»
hashAlgorithmOIDReference	NULL
rARequirements	NULL
keyArchivalAttributes	NULL
extensions	Строка вида «Имя_шаблона@ID_шаблона» ³

¹ Указанное значение обозначает, что шаблон может использоваться при автоэнроллменте.

² Указанное значение обозначает, что от пользователя при создании запроса на сертификат не должно требоваться указание значений для SDN и SAN.

³ Данное значение будет записываться в расширения создаваемого на клиенте запроса на сертификат и будет использоваться в рамках реализации функций CES-севера.

Параметры издателя сертификатов в возвращаемой политике (блок «сAs») 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 СЕР-сервере по Kerberos-билету.
	4	Данное значение указывается, если пользователь аутентифицируется на СЕР-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 СЕР- 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.

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 выпущен, 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.

9.3 Создания политики регистрации сертификатов

Порядок создания политики регистрации сертификатов в ОС Windows:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Вызовите контекстное меню и выберите Все задачи > Дополнительные операции > Управление политиками регистрации сертификатов (см. Рисунок 115).

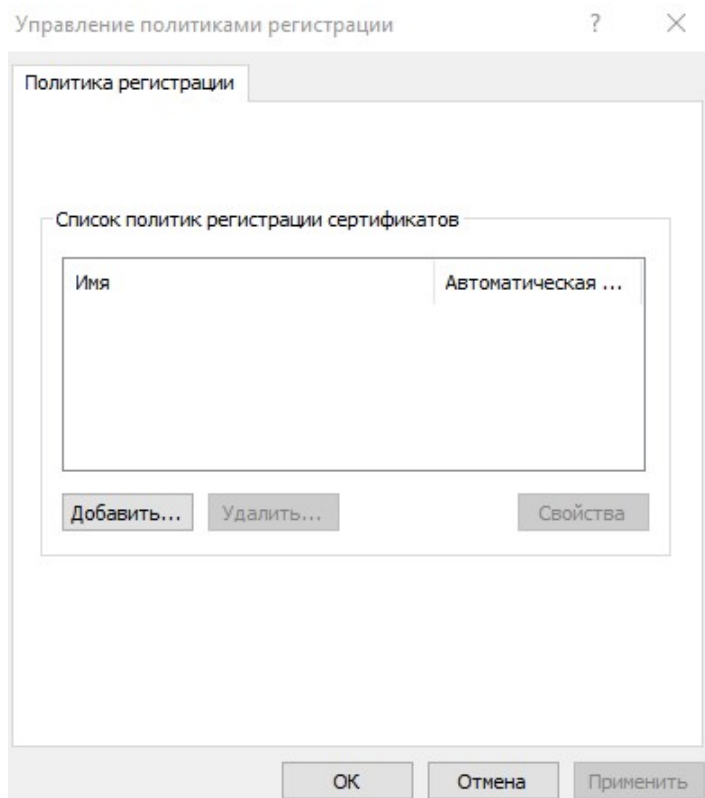


Рисунок 115 - Управление политиками регистрации сертификатов

- В открывшемся окне «Управление политикам и регистрации» нажмите кнопку **<Добавить...>**.

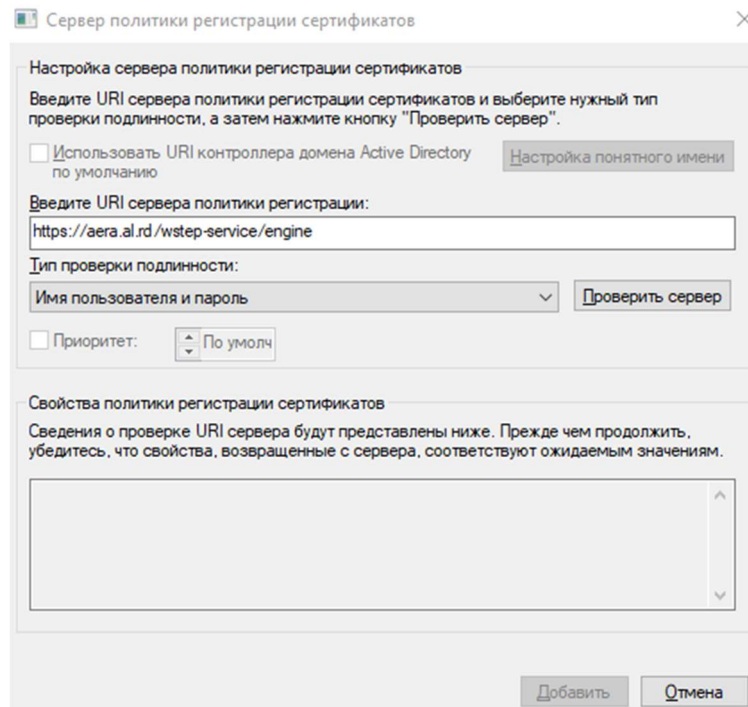


Рисунок 116 - Управление политиками регистрации сертификатов

- В открывшемся окне «Сервер политики регистрации сертификатов» выполните следующие действия:
 - В соответствующем поле введите URL сервера политик выпуска сертификатов Центра регистрации Aladdin eRA.
 - В списке «Тип проверки подлинности» выберите:
 - «Имя пользователя и пароль» для аутентификации по имени и паролю вашей доменной учетной записи.
 - «Встроенная проверка подлинности Windows» для аутентификации по Kerberos-билету.
 - Нажмите кнопку **<Проверить сервер>**.

При выбранном способе аутентификации по имени и паролю укажите их в соответствующих поля открывшегося окна и нажмите кнопку **<ОК>**.

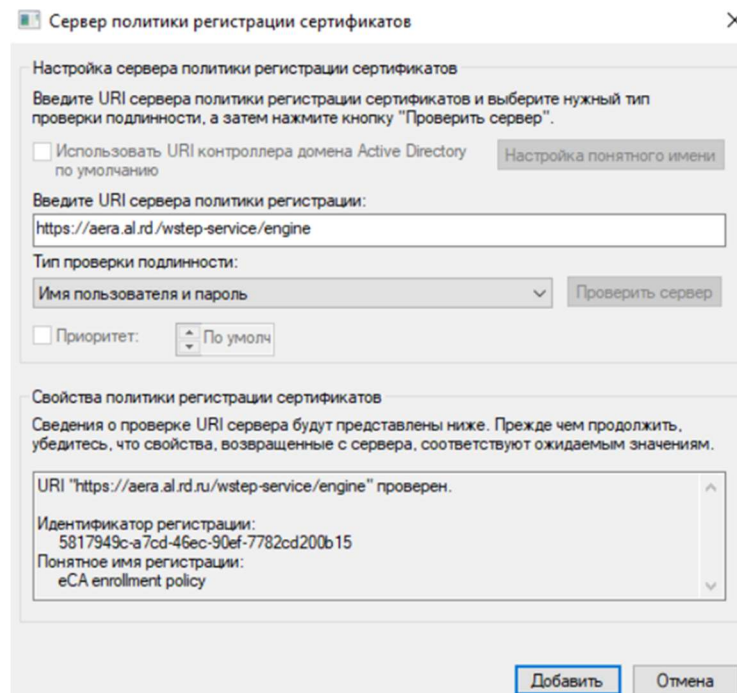


Рисунок 117 - Проверка сервера выполнена успешно

- В случае успешной проверки сервера нажмите кнопку **<Добавить>**.
- В окне «Управление политикам и регистрации» нажмите кнопку **<Применить>**, а затем **<ОК>**.

9.4 Запрос нового сертификата

Порядок запроса сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Для запроса нового сертификата вызовите контекстное меню каталога «Сертификаты» и выберите **Все задачи > Запросить новый сертификат**.
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

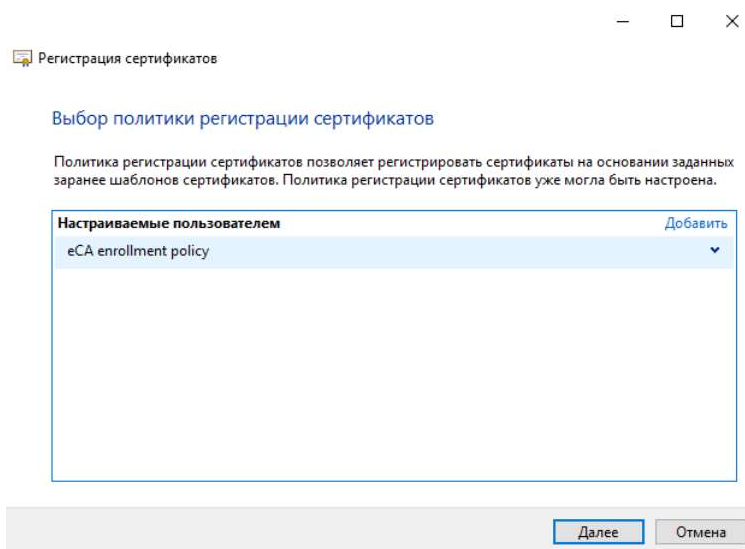


Рисунок 118 - Выбор политики регистрации сертификатов

- На 2 шаге мастера регистрации сертификатов выберите политику **eCA enrollment policy** и нажмите кнопку **<Далее>**.

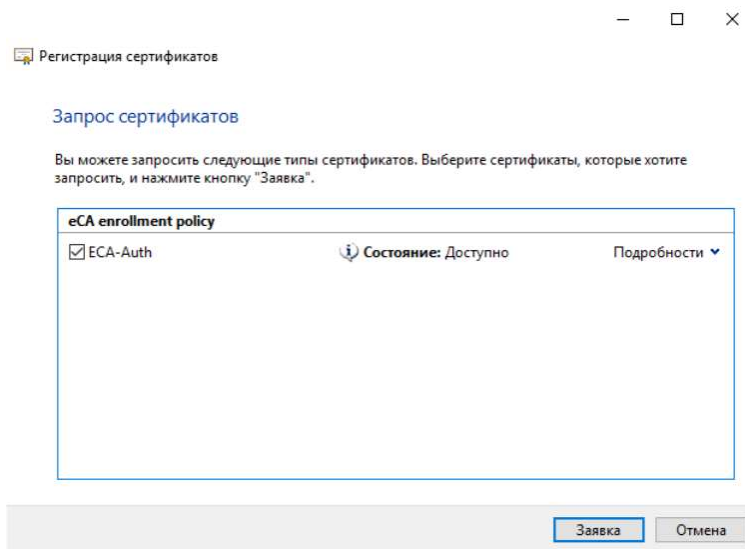


Рисунок 119 - Выбор шаблона для выпуска сертификата

- На 3 шаге мастера регистрации сертификатов выберите шаблоны, по которым необходимо выпустить сертификаты, и нажмите кнопку **<Заявка>**.

- На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 120).

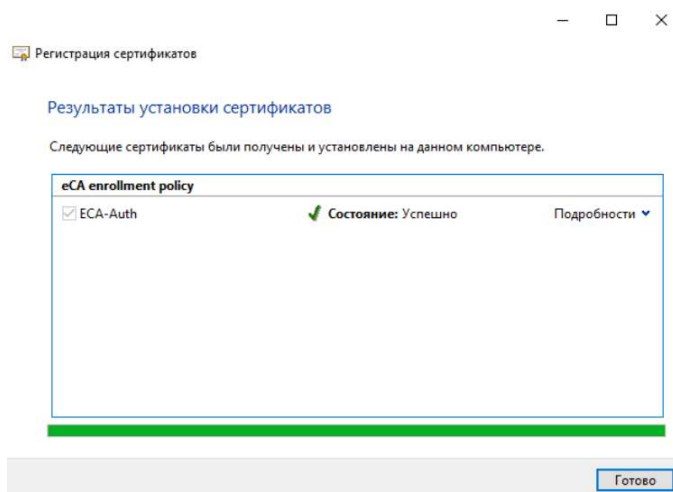


Рисунок 120 - Сертификат получен и успешно установлен в хранилище

9.5 Перевыпуск сертификатов

Центр регистрации Aladdin eRA поддерживает перевыпуск сертификатов с новым ключом и с тем же ключом, на котором был выпущен текущий сертификат.

Порядок перевыпуска сертификата:

- Запустите оснастку «Сертификаты».
- Перейдите в каталог Сертификаты - текущий пользователь > Личное > Сертификаты.
- Для запроса нового сертификата вызовите контекстное меню выбранного сертификата и выберите необходимый сценарий перевыпуска или выпуска нового сертификата:
 - **Все задачи > Обновить сертификат с новым ключом.**
 - **Все задачи > Запросить сертификат с новым ключом.**
 - **Все задачи > Дополнительные операции > Обновить сертификат с тем же ключом.**
 - **Все задачи > Дополнительные операции > Запросить новый сертификат с тем же ключом.**
- В открывшемся окне мастера регистрации сертификатов на 1 шаге нажмите кнопку **<Далее>**.

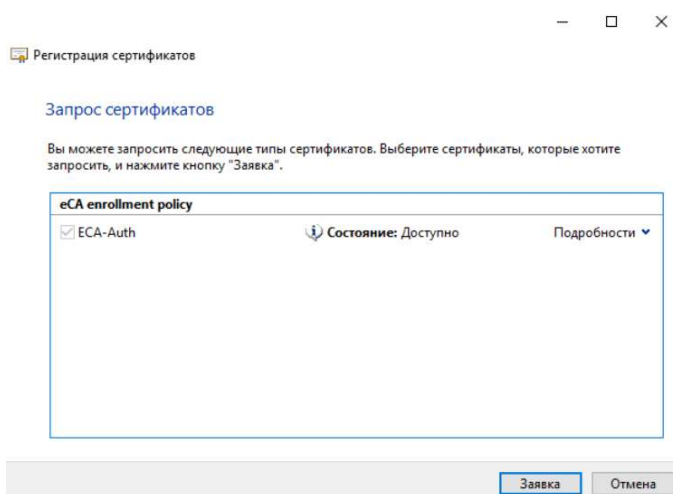


Рисунок 121 - Отправка заявки для выпуска сертификата

- На 2 шаге мастера регистрации сертификатов нажмите кнопку **<Заявка>**.
На последнем шаге мастера регистрации сертификатов убедитесь, что сертификат получен и успешно установлен в хранилище и нажмите кнопку **<Готово>** (см. Рисунок 120).

10 ОФЛАЙН ВЫПУСК СЕРТИФИКАТОВ

Центр регистрации Aladdin eRA 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 eRA поддерживает следующие расширения и кодировки файлов запросов на выпуск сертификатов:

- «.p10» (кодировки DER и PEM);
- «.cms» (кодировка PEM);
- «.req» (кодировки DER и PEM);
- «.pem» (кодировка PEM);
- «.der» (кодировка DER);
- «.dat» (кодировка PEM);
- «.csr» (кодировка PEM).

10.2 Сценарий офлайн выпуска сертификатов

Сценарий офлайн выпуска сертификатов запускается по расписанию, которое задается с помощью CRON-выражения в параметре «offline_enroll_cron» конфигурационного файла. Сценарий офлайн выпуска сертификатов заключается в обработке каждого файла с запросом (запрос) из каталога, указанного в параметре «offline_enroll_req_path» конфигурационного файла.

Если в каталоге сертификатов, заданном в параметре «offline_enroll_cert_path» конфигурационного файла, присутствует сертификат, выпущенный по данному запросу, а в каталоге ошибок, заданном в параметре «offline_enroll_error_path» конфигурационного файла, содержится данный запрос, то запрос пропускается.

Если по запросу ранее была создана заявка, то выполняется анализ её статуса:

- Если заявка в статусе «Отклонена», то запрос копируется в каталог ошибок.
- Если заявка в статусе «Ожидает подтверждения» или «Ошибка выпуска», то запрос пропускается. Статус данной заявки будет проанализирован при следующем выполнении сценария.
- Если заявка в статусе «Выполнена», то выпущенный по заявке сертификат записывается в каталог сертификатов.

Если заявки не было, то выполняется попытка создать заявку на основании запроса с использованием шаблона, указанного в параметре «offline_enroll_template_id» конфигурационного файла, с использованием системной учётной записи (SYSTEM). При этом, если создание заявки завершается с ошибкой, то запрос копируется в каталог ошибок.

10.3 Включение офлайн выпуска сертификатов

Для включения выполнения сценария офлайн выпуска сертификатов выполните следующие действия:

- На сервере, где функционирует Центр регистрации Aladdin eRA, создайте следующие каталоги¹:
 - ``requests`` - каталог, в который будут размещаться файлы запросов на выпуск сертификатов, обрабатываемые при офлайн выпуске;
 - ``certs`` - каталог, в который будут записываться выпущенные сертификаты;
 - ``errors`` - каталог, в который будут записываться файлы запросов, по которым выпуск был отклонен или завершён с ошибкой.
- Выдайте права пользователю `aeca` на запись и чтение для указанных выше каталогов;
- Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, задав следующие значения параметрам:
 - `«offline_enroll_enabled»` - укажите значение `'true'` для активации возможности офлайн выпуска;
 - `«offline_enroll_cron»` - укажите значение cron-выражения, в соответствии с которым будет запускаться офлайн выпуск;
 - `«offline_enroll_template_id»` - укажите значение идентификатора шаблона сертификата, который будет использован для выпуска сертификата. Идентификатор шаблона указан в карточке шаблона в Центре 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 выполните следующие действия:

- Отредактируйте конфигурационный файл `/opt/aecaRa/scripts/config.sh`, задав параметру `«offline_enroll_enabled»` значение `'false'`.
- Примените изменения конфигурационного файла, выполнив команду `sudo bash /opt/aecaRa/scripts/install.sh` с выбором действия «[Update]».

¹ 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 подкаталогов;
- все файлы в каталоге «/opt/aecaRa/static» и его подкаталогов;
- все файлы в каталоге «/opt/aecaRa/bin» и его подкаталогов;
- все файлы в каталоге /opt/aecaRa/digsig и его подкаталогов.

Контроль целостности осуществляется с помощью скрипта «integrity_check.sh», находящегося в каталоге скриптов «/opt/aecaRa/scripts». Скрипт «integrity_check.sh» осуществляет проверку целостности исполняемых файлов программного средства средствами утилиты «Утилита контроля целостности 2.0» - `jcverify`¹.

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»).

¹ Данная утилита включена в состав Центра регистрации (каталог «/opt/aecaRa/bin/jcverify»).

12 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ

Сбор диагностической информации компонентов необходим для предоставления в службу поддержки. пользователей информации о проблемах в работе программы.

Центр регистрации Aladdin eRA 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 Aladdin eRA системные службы и компоненты приложения записывают все производимые действия. Произошедшие события записываются в файлы регистрации событий¹ с расширением `.log`, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaRa/dist/logs/` (определяется параметром `logs_base` конфигурационного файла). Максимальный размер лог-файла каждого сервиса перед его архивацией составляет 10 Мбайт (определяется параметром `logs_file_max_size` конфигурационного файла). Срок хранения архивов составляет 10 дней (определяется параметром `logs_max_history` конфигурационного файла). Максимальный общий объем файлов регистрации событий, включая архивы, каждого типа (`access.log` или `service.log`) для каждого сервиса составляет 100 Мбайт (определяется параметром `logs_total_size_cap` конфигурационного файла)

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- О работе сервисов программы (файлы в формате `.log`).
- Конфигурационный файл `/opt/aecaRa/scripts/config.sh`.
- О работе веб-сервера Nginx/Apache (в формате `.log` и `.gz`).
- О работе системы управления базой данных PostgreSQL.
- О работе системы управления базой данных Jatoba.
- О работе ОС (системная).
- Данные системных логов, представленные в таблице 18.

Таблица 18 - Данные системных логов

Системный лог	РЕД ОС	Astra Linux SE	Alt Сервер	SberLinux OS Server
<code>/var/log/audit/</code>	+	+	+	+
<code>/var/log/samba/</code>	+	+	+	+
<code>/var/log/httpd/</code>	+	-	-	+
<code>/var/log/messages/</code>	+	+	+	+
<code>/var/log/secure/</code>	+	-	-	+
<code>/var/log/cron/</code>	+	+	-	+
<code>/var/log/auth/</code>	-	+	-	-
<code>/var/log/syslog/</code>	-	+	+	-
<code>/var/log/httpd2/</code>	-	-	+	-
<code>/var/log/ahttpd/</code>	-	-	+	-

При включенном флаге сбора диагностической информации о памяти (параметр `enable_gc_diagnostic` конфигурационного файла `/opt/aecaRa/scripts/config.sh`) архив диагностических данных дополнительно содержит:

¹ Файлы регистрации событий, создаваемые в подкаталогах `/opt/aecaRa/dist/logs/`, имеют права доступа 640 (rw-r-----).

- Лог сборщика мусора.
- Дампы памяти для завершивших работу с ошибкой модулей Центра регистрации Aladdin eRA.

Предварительно выполните переход в каталог, где будет сохранён архив с диагностической информацией в формате `tar.gz`, выполнив команду:

```
cd /`палка размещения архива собранной диагностической информации`
```

Для сбора диагностической информации запустите скрипт от имени суперпользователя командой:

```
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 данных выполняется 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: `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 Настройка расписания резервного копирования

Для снижения потерь данных во время сбоя выполните настройку автоматического резервного копирования, настроив системный планировщик расписания `crontab`.

Выполните переход в режим редактирования `crontab`, выполнив команду:

```
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.

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 с правами суперпользователя:

```
sudo bash /opt/aecaRa/scripts/restore.sh `путь к папке с резервной копией`/архив
резервной копии.tar
```

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

Обновление базы данных и модулей Центра регистрации Aladdin eRA обеспечивает актуальность версии программного обеспечения.

При обновлении программы решаются следующие задачи:

- Исправление обнаруженных за время существования программы недочетов и ошибок.
- Устранение выявленных уязвимостей.
- Изменение или улучшение функций программы.
- Добавление новых функций и возможностей.

Компания ведет учет покупателей Центра сертификатов доступа. Выполняется регистрация следующей информации:

- Наименование организации.
- Адрес организации.
- Контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).

Уведомление пользователей о выпуске новой версии Центра сертификатов доступа выполняется путем публикации информации на [официальном сайте Компании](#) и (или) рассылкой электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счет применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлами новой версии программного средства может предоставляться обновленная документация для использования программы.

Получение файлов для обновления программного средства и соответствующих им контрольных сумм возможно:

- С использованием электронной почты.
- Путем загрузки с [веб-сайта изготовителя \(производителя\)](#).

Проверка квалифицированной электронной подписи изготовителя (производителя) файлов для обновления программного средства и файлов соответствующих им контрольных сумм выполняется любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления.

Контроль целостности файлов для обновления программного средства выполняется путем расчета КС полученных установочных пакетов (дистрибутивов) с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0», и её сравнением со значением контрольной суммы для этого обновления.

Внимание! На случай, если во время процесса обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию данных программы (см. раздел 13 настоящего руководства).

Порядок обновления программы:

- Перенесите дистрибутив с новой версией программы на компьютер с установленным Центром регистрации Aladdin eRA.
- Выполните распаковку установочного пакета:
 - для РЕД ОС и SberLinux OS Server командой: `sudo dnf install aeca-*.rpm`;
 - для ОС Astra Linux SE командой: `sudo dpkg -i aeca-*.deb`;
 - для Альт Сервер командой: `sudo apt-get install aeca-*.rpm`.

- Запустите процесс установки программы в режиме обновления, выполнив команду:

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

Установщик обнаружит текущую версию Центра регистрации Aladdin eRA и предложит выбрать необходимое действие в интерактивном режиме:

- Удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программы.
- Выполнить обновление установленной версии до актуальной версии программы.
- Прервать процесс установки.

Для продолжения процесса обновления введите в терминале цифру «2».

При обновлении программа проверяет соответствие номера сборки и значения номера сборки, указанной в БД¹, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaRa/scripts/config.sh`:

- Если на момент обновления в БД отсутствует номер сборки, то программа записывает в БД номер устанавливаемой сборки.
- Если на момент обновления в базе данных присутствует номер сборки, и он меньше номера устанавливаемой сборки, то Центр регистрации Aladdin eRA перезаписывает номер сборки в БД, заменив его номером устанавливаемой сборки.
- Если на момент обновления в БД записан номер сборки, и он равен номеру устанавливаемой сборки, программа не изменяет его.
- Если на момент обновления в БД записан номер сборки, и он больше номера устанавливаемой сборки, то программа завершает процесс обновления с ошибкой «Текущая версия схемы базы данных не позволяет выполнить установку или обновление службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где X.X.X.X - номер сборки, записанный в БД, а Y.Y.Y.Y - номер устанавливаемой сборки программы. Номер сборки в БД при этом не меняется.

После обновления программы запустите веб-браузер и очистите его данные.

Запустите обновленный Центр регистрации Aladdin eRA, подключитесь к веб-интерфейсу и проверьте версию программы в окне «О программе».

¹ Значение номера сборки указано в таблице «`build_info`» схемы «`aeca_info`».

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 компонента системные службы.
- Все добавленные при установке компонента пользователи и группы.
- Все добавленные при установке компонента файлы и структура каталогов.
- Процесс удаления выполняется вне зависимости от наличия соединения с БД, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaRa/scripts/config.sh`.

16 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

16.1 Удаление базы данных

Для удаления ранее созданной базы данных (по умолчанию «aecara») необходимо выполнить команды с правами суперпользователя:

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

```
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();
```

- Для удаления базы данных выполните команду:

```
DROP DATABASE aecara;
```

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

```
exit
```

16.2 Удаление пользователя базы данных

Для удаления ранее созданного пользователя базы данных (по умолчанию «aeca») необходимо выполнить команды с правами суперпользователя:

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

```
sudo -i -u postgres
```

- Удалите пользователя базы данных в Postgres, выполнив команду:

```
dropuser aeca -i
```

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

```
exit
```

- Перезапустите СУБД Postgres, выполнив команду:

```
sudo systemctl restart postgresql
```

17 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Ид.	Проблема	Возможная причина	Способы решения
П001	Ошибка при запуске скрипта установки <code>install.sh</code> «error obtaining MAC configuration for user «аеса»»	У пользователя postgres нет прав на чтение БД атрибутов конфиденциальности	<p>Для предоставления дополнительных прав пользователю postgres выполните команды:</p> <pre>sudo usermod -a -G shadow postgres sudo setfacl -d -m u:postgres:r /etc/parsec/macd b sudo setfacl -R -m u:postgres:r /etc/parsec/macd b sudo setfacl -m u:postgres:rx /etc/parsec/macd b</pre>
П002	Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для установки ЦР Aladdin eCA	Нехватка аппаратных ресурсов	<p>Проверьте показатель загруженности оперативной памяти. Для корректной работы программы требуется не менее 8 Гб свободной оперативной памяти</p>
П003	Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для установки ЦР Aladdin eCA: «[ERROR] Не удалось запустить сервис аеса-га-са-adapter...»	<p>Отсутствуют права на директории, которые указаны в файле <code>krb5.conf</code> в командах <code>includedir</code>.</p> <p>Пример: В файле <code>krb5.conf</code> используется команда <code>includedir /etc/krb5.conf.d/</code>, внутри этой директории есть файл <code>enable_ssd.conf_dir</code>, внутри которого есть команда <code>includedir /var/lib/sss/pubconf/krb5.include.d</code>, Соответственно должны быть права на:</p> <ul style="list-style-type: none"> ▪ <code>krb5.conf</code>; ▪ <code>/etc/krb5.conf.d/</code>, а также все файлы и директории внутри, включая файл <code>enable_ssd.conf_dir</code>; ▪ <code>/var/lib/sss/pubconf/krb5.include.d/</code>, а также все файлы и директории внутри. 	<p>Выдать права на все файлы и директории, используемые в <code>krb5.conf</code>:</p> <pre>sudo chmod 666 путь_к_файлу</pre> <p>Где «путь_к_файлу» - путь к файлу или директории.</p>

П004	Вход в интерфейс Центра регистрации невозможен в браузере Firefox. Ошибка SEC_ERROR_BAD_SIGNATURE	<p>Проблема возникает при наличии в хранилище сертификатов ОС сертификата ЦС с аналогичным SDN издателю сертификата веб-сервера.</p> <p>Она связана с алгоритмом проверки сертификата веб-сервера браузером Firefox для решения уязвимости, связанной с подлогом серверного сертификата:</p> <ol style="list-style-type: none"> 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 	<ol style="list-style-type: none"> 1. Проверьте состав сертификатов доверенных ЦС в хранилище ОС 2. В случае несоответствия установите сертификат издателя сертификата веб-сервера
П005	Вход в интерфейс ЦС невозможен. Ошибка 400. The SSL certificate error	<p>Вход в интерфейс выполнялся в момент синхронизации разрешенных издателей. В параметре «issuers_sync» конфигурационного файла установлено слишком маленькое значение. Синхронизация выполняется слишком часто.</p>	<ol style="list-style-type: none"> 1. Увеличьте интервал синхронизации разрешенных издателей (по умолчанию - каждые 30 минут). 2. Обновите страницу веб-браузера.

ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА ПРИ УСТАНОВКЕ СУБД POSTGRESQL И СУБД POSTGRES PRO

В случае, если другой продукт Postgres уже установлен, то для разрешения конфликта необходимо выполнить команды:

- Создайте начальную базу данных, запустив вспомогательный скрипт `pg-setup` с правами суперпользователя и ключом `initdb`:

```
/opt/pgpro/std-16/bin/pg-setup initdb [--tune=конфигурация] [параметры_initdb]
```

- где
 - аргумент `tune` выбирает вариант конфигурации базы данных;
 - `параметры_initdb` – обычные параметры `initdb`.
- Для настройки автозапуска сервера запустите скрипт `pg-setup` со следующими параметрами:

```
/opt/pgpro/std-16/bin/pg-setup service enable
```

- Запустите сервер с помощью `pg-setup`, выполнив следующую команду с правами суперпользователя):

```
/opt/pgpro/std-16/bin/pg-setup service start
```

ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

Для подключения Центра регистрации Aladdin eCA к внешней СУБД необходимо:

- выполнить настройку на хосте СУБД в соответствии с разделом 2.1 настоящего приложения;
- выполнить настройку на хосте Центра регистрации Aladdin eRA в соответствии с разделом 2.2 настоящего приложения.

2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД (установка СУБД описана в разделах 3.1.3, 3.2.3 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 port -j ACCEPT
```

где `IP` - IP-адрес, доступ с которого необходимо разрешить; `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432).

- Затем на хосте СУБД необходимо перезапустить используемую СУБД, выполнив команду `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, SberLinux OS Server 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/[версия]/data/pg_hba.conf`, если используется СУБД Jatoba)¹, приведя его к следующему виду:

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		all		peer
# IPv4 local connections:					
host	all		all	0.0.0.0/0	password
# IPv6 local connections:					
host	all		all	:::1/128	password

¹ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

```
# 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)¹, 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.

2.2 Настройка на хосте Центра регистрации Aladdin eRA

Внимание! 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
<code>use_tls</code>	<code>false</code>	Флаг обязательного использования TLS для подключения к СУБД ² . Допустимые значения: <code>true</code> , <code>false</code>
<code>database_username</code>	<code>'aeca'</code>	Имя пользователя базы данных, используемое для работы Центра регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>database_password</code>	<code>#CHANGEIT</code>	Пароль пользователя базы данных, используемый для работы Центра регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>database_host</code>	<code>'localhost'</code>	Сетевой адрес хоста СУБД
<code>database_port</code>	<code>'5432'</code>	Порт, используемый для подключения к базе данных
<code>database_name</code>	<code>'aecara'</code>	Имя базы данных, используемой Центром регистрации Aladdin eRA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
<code>root_cert_path</code>	<code>#CHANGEIT</code>	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД ³

¹ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

² Подробная информация о параметре `use_tls` приведена в Настройка TLS-соединения с СУБД

³ Подробная информация о параметре `root_cert_path` приведена в Настройка TLS-соединения с СУБД

- 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.

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 eCA 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)¹, 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)², указав:

- в параметре «ssl» значение «on»;
- в параметре «ssl_cert_file» абсолютный путь к файлу сертификата сервера СУБД³;
- в параметре «ssl_key_file» абсолютный путь к файлу закрытого ключа сервера СУБД⁴;
- в параметре «ssl_ca_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД⁵.

¹ Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database_host» конфигурационного файла Центра регистрации Aladdin eRA.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса Центра сертификации Aladdin eCA. Например, в карточке локального субъекта сервера СУБД.

⁴ 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.

⁵ 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. Владелец 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 и SberLinux OS Server на хосте СУБД указанные выше файлы должны располагаться в каталоге /var/lib/pgsql (или /var/lib/jatoba, если используется СУБД Jatoba). При этом указанные выше файлы должны быть скопированы в нужный каталог, а не перемещены.

Пример значений отредактированных параметров конфигурационного файла СУБД postgresql.conf:

```
# - 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 СУБД¹.

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`. Владелец 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 и SberLinux OS Server 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 и SberLinux OS Server 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.

¹ Если сертификат сервера СУБД выпущен подчинённым ЦС, необходимо указать путь до сертификата корневого ЦС.

ПРИЛОЖЕНИЕ 4. РАЗВЕРТЫВАНИЕ КЛАСТЕРА

Программное средство обеспечивает объединение нескольких Центров регистрации Aladdin eRA в кластер. Кластеризация обеспечивается в отказоустойчивом режиме с использованием внешнего средства балансировки нагрузки HAProxy¹. Отказоустойчивый режим кластеризации обеспечивает как холодное «active-passive»², так и горячее «active-active»³ резервирование. Горячее «active-active» резервирование возможно только при «source»⁴ балансировке.

Внимание! В кластере Центра регистрации Aladdin eRA работает аутентификация по сертификату, а также по доменному логину и паролю. Аутентификация с использованием Kerberos-билета не поддерживается.

Развертывание кластера Центра регистрации Aladdin eRA возможно в следующих вариантах:

- В виртуальной инфраструктуре путем клонирования виртуальной машины.
- С помощью переноса контейнера закрытого ключа.

4.1 Развертывание кластера в виртуальной среде с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Виртуальная машина с установленным Центром регистрации Aladdin eRA (далее - BM1) - основной узел кластера.
- Клон BM1, созданный сразу установки на BM1 Центра регистрации Aladdin eRA (далее - BM2) - резервный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - BM3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - BM4).
- Клон BM1, созданный при необходимости при эксплуатации кластера (далее - BMP) – дополнительный резервный узел кластера.

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации BM3 и BM4.

Порядок развертывания кластера:

- Выполните следующие действия на BM3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000⁵ в файле ⁶:

¹ Серверное программное обеспечение для обеспечения высокой доступности и балансировки нагрузки для TCP- и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов

² Это конфигурация отказоустойчивых кластеров, в которой одни узлы назначаются активными, а другие — резервными, готовыми взять на себя работу в случае отказа активного узла.

³ Это архитектурный подход построения кластера, при котором оба или все узлы активны и работают одновременно, обрабатывая запросы и трафик.

⁴ Это режим, при котором балансировщик выбирает узел кластера на основе хэш-суммы источника IP-адреса, с которого клиенты отправляют запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера.

⁵ Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра Центра регистрации Aladdin eRA, взаимодействующего с СУБД.

⁶ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
- Перезапустите используемую СУБД, выполнив команду с правами суперпользователя:
 - `sudo systemctl restart postgresql` для СУБД PostgreSQL.
 - `sudo systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на ВМ1 установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. Приложение 2 настоящего руководства).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-ra.service`.
- Выполните следующие действия на ВМ4:
 - Установите средство балансировки нагрузки HAProxy, выполнив следующую команду с правами суперпользователя:
 - `sudo dnf install haproxy` - для РЕД ОС и SberLinux OS Server.
 - `sudo apt install haproxy` - для ОС Astra Linux SE.
 - `sudo apt-get install haproxy` - для ОС Альт Сервер.
 - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup

listen stats
```



```
bind *:8404
stats enable
stats uri /stats
stats auth admin:password
```

где:

- DOMAINNAME_HOST1 – доменное имя VM1.
- DOMAINNAME_HOST2 – доменное имя VM2.
- admin:password – имя и пароль учетной записи, которые будут использоваться для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy, выполнив следующую команду с правами суперпользователя `sudo systemctl restart haproxy.service`.

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла необходимо выполнить действия, аналогичные действиям по подключению узла VM2:

- Средствами используемого гипервизора клонируйте VM1, тем самым создав BMP.
- Запустите BMP и дождитесь запуска службы `aeca-ra.service`.
- Выполните на VM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об доменном имени BMP в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
```

где DOMAINNAME_HOSTR – доменное имя BMP.

- Перезапустить HAProxy на VM4, выполнив следующую команду с правами суперпользователя: `sudo systemctl restart haproxy.service`.

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки кластера все запросы, направляемые к Центру регистрации Aladdin eRA через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера VM1. При недоступности основного узла кластера все запросы будут перенаправляться на резервный узел кластера VM2. При недоступности VM2 все запросы будут перенаправляться на дополнительный резервный узел кластера BMP. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats`, где IP_VM4 - IP-адрес VM4. Пройдите идентификацию и аутентификацию с помощью имени и пароля учетной записи администратора, указанных при настройке конфигурационного файла.

4.2 Развертывание кластера с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Сервер с установленным Центром регистрации Aladdin eRA (далее - APM1) - основной узел кластера.
- Сервер с установленным Центром регистрации Aladdin eRA (далее - APM2) - резервный узел кластера.
- Сервер с установленным Центром регистрации Aladdin eRA (далее - APMP) – дополнительный резервный узел кластера.

- Сервер с установленной и настроенной СУБД (далее - АРМ3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - АРМ4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1.1.

Допускается использование одного сервера для реализации АРМ3 и АРМ4.

Порядок развертывания кластера:

- Выполните следующие действия на АРМ3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле ²:
 - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
 - Перезапустите используемую СУБД, выполнив команду с правами суперпользователя:
 - `sudo systemctl restart postgresql` для СУБД PostgreSQL.
 - `sudo systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на АРМ1 установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на АРМ3 (см. Приложение 2 настоящего руководства).
- Выполните на АРМ2 установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД ³, установленной на АРМ3 (см. Приложение 2 настоящего руководства).
- Выполните следующие действия на ВМ4:
 - На АРМ4 выполните установку средства балансировки нагрузки HAProxy, выполнив следующую команду с правами суперпользователя:
 - `sudo dnf install haproxy`- для РЕД ОС и SberLinux OS Server.
 - `sudo apt install haproxy`- для ОС Astra Linux SE.
 - `sudo apt-get install haproxy`- для ОС Альт Сервер.
 - На АРМ4 выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon
```

¹ Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра Центра регистрации Aladdin eRA, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ В конфигурационном файле Центра регистрации Aladdin eRA на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным СУБД АРМ1.

```
defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- DOMAINNAME_HOST1 – доменное имя APM1.
- DOMAINNAME_HOST2 – доменное имя APM2.
- admin:password – имя и пароль учетной записи, которые будут использоваться для доступа к панели мониторинга HAProxy.
- На APM4 перезапустите HAProxy, выполнив следующую команду с правами суперпользователя:
`sudo systemctl restart haproxy.service`

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла (далее - APMР) необходимо выполнить действия, аналогичные действиям по подключению узла APM2:

- Выполните для APMР действия, производимые для APM2 данного раздела (при их выполнении вместо APM2 использовать APMР).
- Выполните на APM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени APMР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
```

где DOMAINNAME_HOSTR – доменное имя APMР.

- На APM4 перезапустите HAProxy, выполнив следующую команду с правами суперпользователя:
`sudo systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел. Все описанные выше рекомендации и уточнения по работе с узлом APM2, также относятся и к узлу APMР.

В результате приведенной настройки кластера все запросы, направляемые к Центру регистрации Aladdin eRA через средство балансирования нагрузки HAProxy, будут перенаправляться на основной узел кластера APM1. 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 APM2. Для мониторинга состояния узлов кластера может быть использована панель мониторинга, доступная по адресу `http://IP_ARM4:8404/stats`, где IP_ARM4 - IP-адрес APM4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на APM4).

4.3 Развертывания кластера в виртуальной среде с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Виртуальная машина с установленным Центром регистрации Aladdin eRA (далее - BM1) - первый узел кластера.
- Клон BM1, созданный сразу после завершения установки на BM1 Центра регистрации Aladdin eRA (далее - BM2) - второй узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - BM3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - BM4).
- Клон BM1, созданный при необходимости при эксплуатации кластера (далее - BMP) - дополнительный узел кластера.

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1.1 настоящего руководства.

Допускается использование одной виртуальной машины для реализации BM3 и BM4.

Порядок развертывания кластера:

- Выполните следующие действия на BM3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле ²:
 - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
 - Перезапустите используемую СУБД, выполнив команду с правами суперпользователя:
 - `sudo systemctl restart postgresql` для СУБД PostgreSQL.
 - `sudo systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на BM1 установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на BM3 (см. Приложение 2 настоящего руководства).
- Средствами используемого гипервизора клонируйте BM1, тем самым создав BM2.

¹ Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра Центра регистрации Aladdin eRA, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- Запустите VM2 и дождитесь завершения запуска службы `aeca-ra.service`.
- Выполните следующие действия на VM4:
 - Установите средство балансировки нагрузки HAProxy, выполнив следующую команду с правами суперпользователя:
 - `sudo dnf install haproxy` - для РЕД ОС и SberLinux OS Server.
 - `sudo apt install haproxy` - для ОС Astra Linux SE.
 - `sudo apt-get install haproxy` - для ОС Альт Сервер.
 - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- `DOMAINNAME_HOST1` – доменное имя VM1.
- `DOMAINNAME_HOST2` – доменное имя VM2.

- `admin:password` – имя и пароль учетной записи, которые будут использоваться для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy, выполнив следующую команду с правами суперпользователя:
`sudo systemctl restart haproxy.service.`

В кластер можно подключать дополнительные узлы. Для подключения нового узла необходимо выполнить действия, аналогичные действиям по подключению узла VM2:

- Средствами используемого гипервизора клонируйте VM1, тем самым создав BMP.
- Запустите BMP и дождитесь запуска службы `aeca-ra.service`.
- Выполните на VM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`,

добавив в секцию `backend bk_app` информацию о доменном имени BMP в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где `DOMAINNAME_HOSTR` - это доменное имя BMP.

- Перезапустить HAProxy на VM4, выполнив следующую команду с правами суперпользователя:
`sudo systemctl restart haproxy.service.`

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это будет гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats`, где `IP_VM4` - IP-адрес VM4. Пройдите идентификацию и аутентификацию с помощью имени и пароля учетной записи администратора, указанных при настройке конфигурационного файла.

4.4 Развертывание кластера с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Сервер с установленным Центром регистрации Aladdin eRA (далее - APM1) – первый узел кластера.
- Сервер с установленным Центром регистрации Aladdin eRA (далее - APM2) – второй узел кластера.
- Сервер с установленным Центром регистрации Aladdin eRA (далее - APMР) – дополнительный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - APM3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - APM4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1.1.

Допускается использование одного сервера для реализации APM3 и APM4.

Порядок развертывания кластера:

- Выполните следующие действия на APM3:

- Выполнить установку одной из нижеприведённых СУБД:
 - o PostgreSQL из состава ОС
 - o Jatoba.
- Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле²:
 - o `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - o `var/lib/jatoba/[версия]/data/postgresql.conf` для СУБД Jatoba.
- Перезапустите используемую СУБД, выполнив команду с правами суперпользователя:
 - o `sudo systemctl restart postgresql` для СУБД PostgreSQL.
 - o `sudo systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните на АРМ1 установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на АРМ3 (см. Приложение 2 настоящего руководства).
- На АРМ2 выполните установку Центра регистрации Aladdin eRA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД³, установленной на АРМ3 (см. Приложение 2 настоящего руководства).
- На АРМ4 выполните установку средства балансировки нагрузки HAProxy, выполнив следующую команду с правами суперпользователя:
 - `sudo dnf install haproxy`- для РЕД ОС и SberLinux OS Server.
 - `sudo apt install haproxy`- для ОС Astra Linux SE.
 - `sudo apt-get install haproxy`- для ОС Альт Сервер.
- На АРМ4 выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000
```

¹ Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра Центра сертификации Aladdin eCA, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ В конфигурационном файле Aladdin eCA на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным СУБД АРМ1.

```
frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- DOMAINNAME_HOST1 – доменное имя APM1.
- DOMAINNAME_HOST2 – доменное имя APM2.
- admin:password – имя и пароль учетной записи, которые будут использоваться для доступа к панели мониторинга HAProxy.

- На APM4 перезапустите HAProxy, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl restart haproxy.service
```

В кластер можно подключать дополнительные узлы. Для подключения нового узла (далее - APMР) необходимо выполнить действия, аналогичные действиям по подключения узла APM2:

- Выполните для APMР действия, производимые для APM2 данного раздела (при их выполнении вместо APM2 использовать APMР).
- Выполните на APM4 редактирование конфигурационного файла /etc/haproxy/haproxy.cfg, добавив в секцию backend bk_app информацию о доменном имени APMР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где DOMAINNAME_HOSTR - это доменное APMР.

- На APM4 перезапустите HAProxy, выполнив следующую команду с правами суперпользователя:

```
sudo systemctl restart haproxy.service
```

В результате в кластере появится дополнительный узел. Все описанные выше рекомендации и уточнения по работе с узлом APM2, также относятся и к узлу APMР.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это будет гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов

кластера может быть использована панель мониторинга, доступная по адресу `http://IP_ARM4:8404/stats`, где `IP_ARM4` - IP-адрес АРМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на АРМ4).

4.3 Обновление ПО узлов кластера

Процесс обновления кластера Центра сертификации Aladdin eCA:

- Выполните резервное копирование данных на всех узлах кластера (см. раздел 13 настоящего руководства).
- Для кластера по схеме «active-passive» на всех резервных узлах выполните остановку службы Центра регистрации Aladdin eRA, выполнив следующую команду с правами суперпользователя:
`sudo systemctl stop aeca-ra.service.`
- Для кластера по схеме «active-active» на всех узлах кроме первого, выполните остановку службы Центра регистрации Aladdin eRA, выполнив следующую команду с правами суперпользователя:
`sudo systemctl stop aeca-ra.service.`
- Для кластера по схеме «active-passive» выполнить обновление ПО Центра регистрации Aladdin eRA на основном узле (см. раздел 14 настоящего руководства).
- Для кластера по схеме «active-active» выполнить обновление ПО Центра регистрации Aladdin eRA на первом узле кластера (см. раздел 14 настоящего руководства).
- Вне зависимости от схемы кластера выполните обновление ПО Центра регистрации Aladdin eRA на всех остальных узлах кластера (см. раздел 14 настоящего руководства).

Критерием правильности установки обновления ПО кластера является отображение информации о новой версии в окне «О программе» веб-интерфейса и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга HAроху, доступной по адресу `http://IP_ARM4:8404/stats`, где `IP_ARM4` - IP-адрес АРМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg`).

ПРИЛОЖЕНИЕ 5. НАСТРОЙКА KERBEROS В ВЕБ-БРАУЗЕРЕ

Внимание! Предварительно на клиенте должен быть настроен Kerberos, клиент должен быть подключён к домену и клиент должен использовать браузер с поддержкой Kerberos.

Для того, чтобы в браузере клиента при работе с 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 Firefox

Далее в примере:

- `aeca.al.rd.kg`, `aeca1.al.rd.kg` - доменные имена Центров регистрации Aladdin eRA
- `al.rd.kg` - домен, (`AL.RD.KG` - realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Запустите веб-браузер Mozilla Firefox.
- В адресной строке введите `about:config`.
- Нажмите на кнопку <Принять риск и продолжить>.
- В поле поиска введите `negotiate`, чтобы ограничить список отображаемых параметров.
- Установите параметру `network.negotiate-auth.trusted-uris` одно из следующих значений (см. Рисунок 122):
 - Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, введите полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.rd.kg`).
 - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.al.rd.kg`).
 - Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, введите их полные доменные имена через запятую (например, `aeca.al.rd.kg, aeca1.al.rd.kg`).
- Продублируйте введённое значение параметра `network.negotiate-auth.trusted-uris` в параметре `network.negotiate-auth.delegation-uris`.

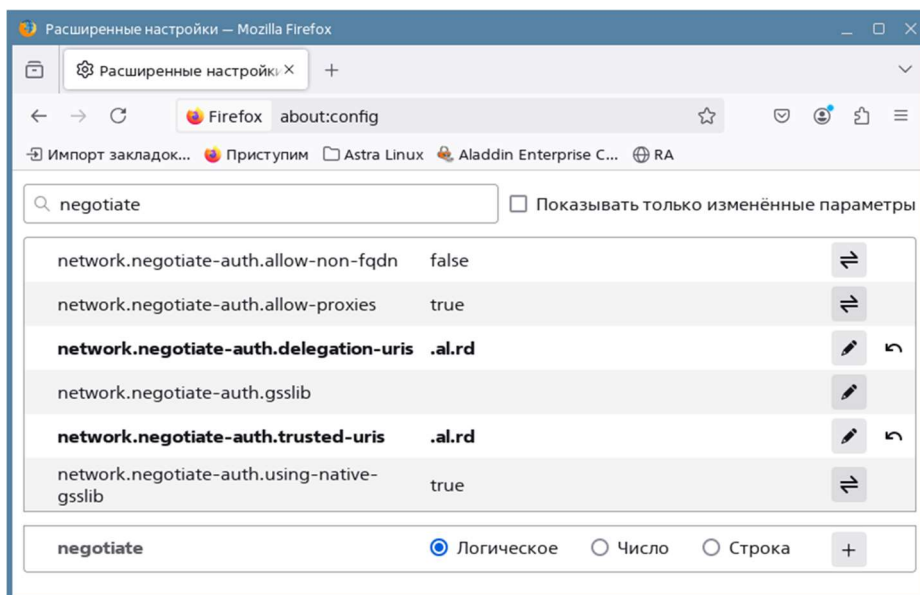


Рисунок 122 - Настройка Kerberos-аутентификации в веб-браузере Firefox

5.2 Настройка веб-браузера Chromium

Далее в примере:

- `aeca.al.rd.kg`, `aecal.al.rd.kg` - доменные имена Центров регистрации Aladdin eRA
- `al.rd.kg` - домен, (`AL.RD.KG` - realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Создайте в каталоге `/etc/chromium/policies/managed` файл `policies.json`, выполнив следующую команду с правами суперпользователя:

```
sudo touch /etc/chromium/policies/managed/policies.json
```

- Откройте файл для редактирования, выполнив следующую команду с правами суперпользователя:

```
sudo nano /etc/chromium/policies/managed/policies.json
```

- В файле `policies.json` укажите следующие политики в формате JSON:

```
{
  "AuthServerAllowlist": "*.al.rd.kg",
  "AuthSchemes": "ntlm,negotiate"
}
```

Примечания:

- Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, укажите для политики «AuthServerAllowlist» полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.rd.kg`).
- Чтобы разрешить SPNEGO аутентификацию для целого домена, укажите для политики «AuthServerAllowlist» имя домена (например, `*.al.rd.kg`).
- Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, укажите для политики «AuthServerAllowlist» их полные доменные имена через запятую (например, `aeca.al.rd.kg, aecal.al.rd.kg`).
- Запустите веб-браузер Chromium и введите в адресной строке `chrome://policy`.
- Убедитесь, что политики были применены (см. Рисунок 123).

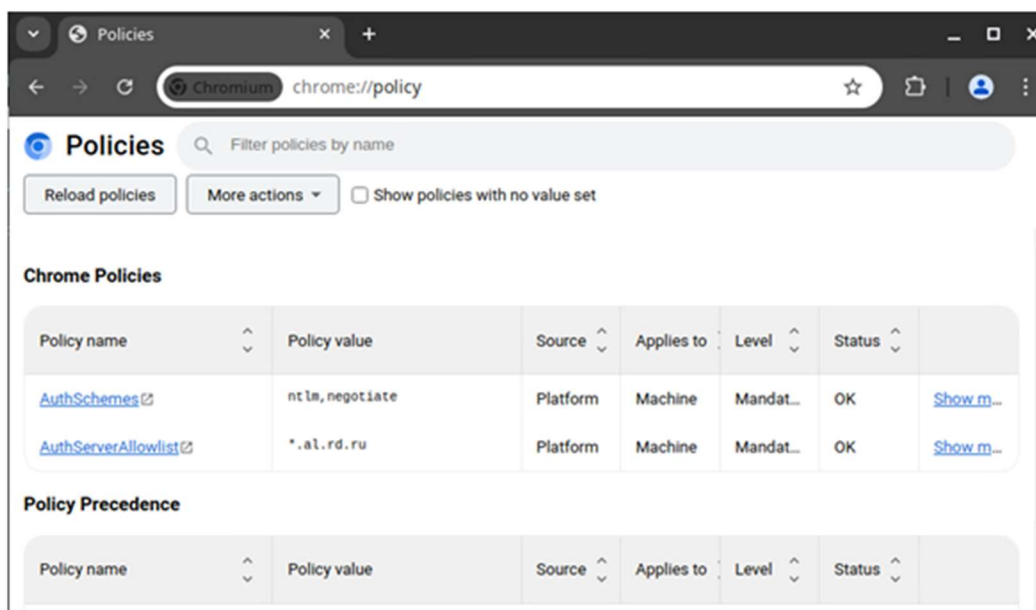


Рисунок 123 - Настройка Kerberos-аутентификации в веб-браузере Chromium

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	<p>Краткое описание: Создание заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка создания заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Обработка заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Выпуск сертификата по заявке</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка выпуска сертификата по заявке</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Отмена заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка отмены заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Отклонение заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка отклонения заявки</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Импорт сертификата на носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка импорта сертификата на носитель</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Отзыв сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка отзыва сертификата</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Подключение ключевого носителя</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – Свойства носителя
Ошибка подключения ключевого носителя	RAENV0401	ERROR	<p>Краткое описание: Ошибка подключения ключевого носителя</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – Свойства носителя – Описание ошибки

6.6 События экспорта

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Экспорт файла	RAENV0500	INFO	<p>Краткое описание: Экспорт файла</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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	<p>Краткое описание: Ошибка экспорта файла</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID заявки – Тип файла (возможные значения: «PKCS#10», «Сертификат», «Цепочка сертификатов», «PKCS#12», «Сертификат издателя», «Цепочка сертификатов издателя», «CRL издателя») – Описание ошибки
Экспорт журнала событий	RAENV0502	INFO	<p>Краткое описание: Экспорт журнала событий</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – Параметры фильтрации
Ошибка экспорта журнала событий	RAENV0503	ERROR	<p>Краткое описание: Ошибка экспорта журнала событий</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа
Ошибка редактирования правила выпуска	RAENV0603	ERROR	Краткое описание: Ошибка редактирования правила выпуска Атрибуты: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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
Остановка правила выпуска	RAENV0606	INFO	Краткое описание: Остановка правила выпуска Атрибуты: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – ID правила – Отображаемое имя правила – Режим обработки – Статус – Субъекты доступа – Объекты доступа – Описание ошибки
Удаление правила выпуска	RAENV0608	INFO	Краткое описание: Удаление правила выпуска Атрибуты: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – Серийный номер (может отсутствовать) – Отпечаток (может отсутствовать) – CN в сертификате (может отсутствовать) – Действует с (может отсутствовать) – Действует по (может отсутствовать) – Описание ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Изменение списка разрешённых издателей	RAENV0702	INFO	Краткое описание: Изменение списка разрешённых издателей Атрибуты: – Обновлённый список разрешённых издателей
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: <ul style="list-style-type: none"> – Адрес хоста – Порт – Протокол – Флаг отправки сообщений
Ошибка добавления Syslog-сервера	RAENV1201	ERROR	Краткое описание: Ошибка добавления Syslog-сервера Атрибуты: <ul style="list-style-type: none"> – Адрес хоста (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщений (может отсутствовать) – Описание ошибки
Изменение параметров Syslog-сервера	RAENV1202	INFO	Краткое описание: Изменение параметров Syslog-сервера Атрибуты: <ul style="list-style-type: none"> – Адрес хоста – Порт – Протокол – Флаг отправки сообщений

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка изменения параметров Syslog-сервера	RAENV1203	ERROR	<p>Краткое описание: Ошибка изменения параметров Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – Адрес хоста (может отсутствовать) – Порт (может отсутствовать) – Протокол (может отсутствовать) – Флаг отправки сообщений (может отсутствовать) – Описание ошибки
Удаление Syslog-сервера	RAENV1204	INFO	<p>Краткое описание: Удаление Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – Адрес хоста – Порт – Протокол – Флаг отправки сообщений
Ошибка удаления Syslog-сервера	RAENV1205	ERROR	<p>Краткое описание: Ошибка удаления Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – 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»¹.

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром регистрации Aladdin eRA необходимо подготовить внешнюю гамму².

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} -R
```

- 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} -R
sudo chmod 700 -R
/opt/aecaRa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.
jar,sspiSSL.jar}
```

- Если используется уже заранее подготовленная внешняя гамма, то пропустите этот пункт. Иначе подготовьте внешнюю гамму с помощью утилиты `/opt/cproscsp/bin/amd64/genkpim` (утилита `genkpim` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma
/opt/cproscsp/bin/amd64/genkpim <количество ключей> 0x12345678 ~/gamma
```

¹ Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

² 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 чисел (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`, `krim`.
 - 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 «аеса» 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 команд¹:

```
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
```

¹ Подключение осуществляется с помощью файла `cpconfig` (находится в `/opt/cproscsp/sbin/amd64`). Путь к файлу в командах приведен с учётом нахождения в каталоге `/opt/cproscsp/sbin/amd64`.

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

Перед началом работы следует ознакомиться со следующей документацией, относящейся к программному обеспечению:

- [официальная документация РЕД ОС 7.1;](#)
- [официальная документация Astra Linux Special Edition 1.7;](#)
- [официальная документация Альт Сервер 8, релиз 10;](#)
- [официальная документация Postgres;](#)
- [официальная документация Jatoba 4;](#)
- [официальная документация JC-Web Client 4.3.5 Руководство пользователя.](#)

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

БД	- База данных
ЗПС	- Замкнутая программная среда
ОС	- Операционная система
ПО	- Программное обеспечение
СКЗИ	- Средство криптографической защиты информации
СУБД	- Система управления базами данных
ЦР	- Центр регистрации
ЦС	- Центр сертификации
AIA	- Authority Information Access
API	- Application Programming Interface
CSV	- Comma-Separated Values
CRL	- Certificate Revocation List
HDD	- Hard (magnetic) Disk Drive
HTTPS	- Hyper Text Transfer Protocol Secure
HTTP	- Hyper Text Transfer Protocol
LDAP	- Lightweight Directory Access Protocol
PKI	- Public Key Infrastructure
SCEP	- Simple Certificate Enrollment Protocol
SPN	- Service Principal Name
SSD	- Solid-State Drive
SSL	- Secure Sockets Layer
TCP	- Transmission Control Protocol
TLS	- Transport Layer Security
VGA	- Video Graphics Array
URL	- Uniform Resource Locator
WSTEP	- WS-Trust X.509v3 Token Enrollment Extensions

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Заявка - это заявление от пользователя на получение сертификата, полученное через API или веб-интерфейс, содержащее совокупность данных о пользователе (запрос на сертификат (CSR)).

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

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 KG, 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 KG». 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 KG», 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 KG».

Kerberos - сетевой протокол аутентификации, который обеспечивает механизм взаимной аутентификации клиента и сервера перед установлением связи между ними.

Keytab-файл - это файл, содержащий пары Kerberos-принципалов и их ключей (полученных с использованием Kerberos пароля). Эти файлы используются для аутентификации в системах, использующих Kerberos, без ввода пароля.

Веб-интерфейс - интерфейс, обеспечивающий передачу информации между пользователем-человеком и программно-аппаратными компонентами компьютерной системы.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]