



Центр сертификатов доступа

# Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition

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

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-1
Версия	2.2.0
Листов	102
Дата	23.05.2025

## Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является АО «Аладдин Р.Д.».

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

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

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

### Ограничение ответственности

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

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

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

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

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

### Государственное регулирование и экспортный контроль

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

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

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

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

© АО «Аладдин Р.Д.», 1995–2025. Все права защищены

## Лицензионное соглашение

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

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

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

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

### Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ.

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

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

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

### Лицензия

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

### Соглашения:

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

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

- не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;
- не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;
- не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;
- не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому-либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

### Требования к использованию

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

### Использование ПО

Пользователь вправе:

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

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

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

- дизайна (графики, расположения элементов оформления и т.п.);
- всех иных элементов, в том числе изображений, фонограмм, текстов.

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

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

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

## Обслуживание и поддержка

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

## Ограниченная гарантия

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

## Отказ от гарантии

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

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

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

## Ограничение возмещения

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

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

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

## Исключение косвенных убытков

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

## Ограничение ответственности

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

## Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

## Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

## Разное

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

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

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

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

## Аннотация

Настоящий документ представляет собой первую часть руководства администратора программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»<sup>1</sup>.

Документ предназначен для администраторов программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», регламентирующих права доступа субъектов к объектам и введение ограничений на действия пользователей, а также на изменение условий эксплуатации, состава и конфигурации программных и программно-аппаратных средств.

Руководство определяет порядок подготовки и установки программного средства «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». Перед эксплуатацией программного средства рекомендуется внимательно ознакомиться с настоящим руководством.

Инструкции по установке стороннего программного обеспечения приведены в ознакомительных целях, для получения более точной информации рекомендуем ознакомиться с актуальной инструкцией по установке и настройке продуктов на официальных сайтах производителей.

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

Настоящий документ ориентирован на администраторов безопасности, ответственных за установку, настройку и сопровождение систем безопасности организации.

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

Таблица 1 – Соответствие документации требованиям доверия

Требования доверия (16.1 Руководство администратора должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
действий по приёмке поставленного средства	часть 1, раздел 3 «Действия по приёмке программного компонента “Центр сертификации Aladdin Enterprise Certification Authority”»
действий по безопасной установке и настройке средства	часть 1, раздел 1, подраздел 1.8 «Действия по безопасной установке и настройке программы»
действий по реализации функций безопасности среды функционирования средства	часть 1, раздел 1, подраздел 1.9 «Действия по реализации функций безопасности среды функционирования программы»

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

<sup>1</sup> Далее по документу – программа, программное средство, Aladdin eCA CE

## Содержание

1 Введение .....	9
1.1 Область применения .....	9
1.2 Состав программного средства .....	9
1.3 Функции Центра сертификатов доступа .....	10
1.4 Комплект поставки .....	11
1.5 Имя пакета компонентов поставки .....	11
1.6 Доступные роли .....	12
1.7 Режимы функционирования программы .....	14
1.8 Действия по безопасной установке и настройке программы .....	15
1.9 Действия по реализации функций безопасности среды функционирования программы .....	15
2 Условия выполнения программного средства .....	16
2.1 Требования к программному обеспечению .....	16
2.1.1 Требования к среде функционирования серверной части центра сертификации .....	16
2.1.2 Требования к среде функционирования клиентской части центра сертификации .....	16
2.2 Требования к аппаратным средствам .....	17
3 Действия по приёму программного средства .....	19
3.1 Проверка комплектности .....	19
3.2 Контроль целостности установочных пакетов .....	19
4 Подготовка к установке программного средства .....	21
4.1 Таблица сетевого взаимодействия .....	21
4.2 Подготовка сервера .....	22
4.3 Подготовка сервера с операционной системой РЕД ОС .....	23
4.3.1 Подключение репозитория и установка зависимостей .....	23
4.3.2 Установка среды исполнения Java .....	23
4.3.3 Установка и настройка СУБД .....	23
4.3.4 Установка веб-сервера .....	26
4.4 Подготовка сервера с операционной системой Astra Linux Special Edition .....	27
4.4.1 Подключение репозитория и установка зависимостей .....	27
4.4.2 Установка среды исполнения Java .....	29
4.4.3 Установка и настройка СУБД .....	29
4.4.4 Установка веб-сервера .....	33
4.5 Подготовка сервера с операционной системой Альт Сервер .....	34
4.5.1 Подключение репозитория и установка зависимостей .....	34
4.5.2 Установка среды исполнения Java .....	34
4.5.3 Установка и настройка СУБД .....	34
4.5.4 Установка веб-сервера .....	37

4.6 Установка веб-сервера Cppnginx .....	38
4.7 Установка JC-WebClient .....	39
5 Установка программного средства .....	40
5.1 Распаковка инсталляционного комплекта программного средства .....	40
5.2 Настройка параметров конфигурации программного средства .....	42
5.3 Подключение Центра валидации .....	54
5.4 Создание и настройка базы данных .....	54
5.4.1 Создание и настройка базы данных в автоматическом режиме .....	55
5.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме .....	55
5.4.3 Создание и настройка базы данных Jatoba в ручном режиме .....	57
5.5 Установка программного средства .....	58
6 Запуск и остановка программного средства .....	60
6.1 Запуск программного средства .....	60
6.2 Остановка программного средства .....	61
7 Подключение к веб-интерфейсу .....	62
7.1 Общие сведения .....	62
7.2 Установка сертификата администратора инициализации .....	63
7.3 Подключение к веб-интерфейсу .....	65
8 Контроль целостности исполняемых файлов программного средства .....	67
9 Сбор диагностической информации .....	68
10 Резервное копирование и восстановление данных программного средства .....	69
10.1 Создание резервной копии .....	69
10.2 Расписание резервного копирования .....	69
10.3 Восстановление данных из резервной копии .....	70
11 Восстановление доступа к Центру Сертификации .....	71
12 Обновление программного средства .....	72
12.1 Назначение обновлений .....	72
12.2 Информирование потребителей о выпуске обновлений .....	72
12.3 Получение обновлений потребителем .....	72
12.4 Контроль целостности обновления ПО .....	72
12.5 Процедура установки обновлений .....	72
12.6 Критерий успешности установки обновления .....	74
13 Удаление программного средства .....	75
13.1 Инициализация процесса удаления .....	75
14 Удаление базы данных Postgres .....	76
14.1 Удаление БД «аесаса» .....	76
14.2 Удаление пользователя БД «аеса» .....	76

15 Поиск и устранение неисправностей .....	77
Приложение 1. Разрешение конфликта «при установке СУБД Postgres и PostgresPro.....	78
Приложение 2. Настройка подключения к внешней СУБД .....	79
2.1 Настройка на хосте СУБД.....	79
2.2 Настройка на хосте Aladdin eCA .....	80
Приложение 3. Настройка TLS-соединения с СУБД.....	82
3.1 Настройка СУБД .....	82
3.2 Настройка программного компонента Aladdin eCA .....	83
Приложение 4. Развертывание кластера Aladdin eCA .....	84
4.1 Развертывание кластера Aladdin eCA в виртуальной инфраструктуре .....	84
4.2 Развертывание кластера Aladdin eCA с помощью переноса контейнеров закрытого ключа основного узла..	88
4.3 Обновление программных компонент Aladdin eCA узлов кластера Aladdin eCA .....	92
Приложение 5. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP» .....	94
5.1 Настройка взаимодействия с СКЗИ «КриптоПро CSP» .....	95
5.2 Индикация об отсутствии связи с СКЗИ «КриптоПро CSP» .....	96
Лист регистрации изменений.....	102
Перечень документации для ознакомления .....	98
Обозначения и сокращения .....	99
Термины и определения .....	100



# 1 ВВЕДЕНИЕ

## 1.1 Область применения

Программное средство «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020 (далее – Центр сертификатов доступа) применяется как элемент систем защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации при идентификации и строгой аутентификации субъектов<sup>2</sup> и объектов доступа<sup>3</sup> в автоматизированной (информационной) системе.

## 1.2 Состав программного средства

Центр сертификатов доступа включает:

- программное средство «Центр сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.038 (далее – программное средство или Центр сертификации Aladdin eCA), состоящее из:
  - программный компонент «Серверная часть Центра сертификации» RU.АЛДЕ.03.01.040. Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения;
  - программный компонент «Клиентская часть центра сертификации» RU.АЛДЕ.03.01.041. Программный компонент реализует интерфейс, с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра сертификации»;
- программное средство «Центр регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.051 (далее – Центр регистрации Aladdin eRA), состоящее из:
  - программный компонент «Серверная часть Центра регистрации» RU.АЛДЕ.03.01.052. Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения;
  - программный компонент «Клиентская часть Центра регистрации» RU.АЛДЕ.03.01.053. Программный компонент реализует интерфейс, с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации»;
- программное средство «Утилита контроля целостности 2.0»<sup>4</sup> RU.АЛДЕ.02.13.002-09. Программа предназначена для контроля целостности исполняемых файлов и дистрибутивов Центра сертификатов доступа;
- средство криптографической защиты информации «КриптоПро CSP»<sup>5</sup> версии 5.0 R3 KC1 (исполнение 1-Base) ЖТЯИ.00101-03 или версии 5.0 R3 KC2 (исполнение 2-Base) ЖТЯИ.00102-03<sup>6</sup>. Средство криптографической защиты информации (далее – СКЗИ) предназначено для создания, хранения и удаления ключевых пар (открытый и закрытый ключи) центров сертификации инфраструктуры открытых ключей, создания ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств), генерации и проверки цифровой подписи, а также для идентификации, аутентификации, шифрования и имитозащиты TLS-соединений;

<sup>2</sup> Субъектами доступа могут являться как физические лица (пользователи), так и ресурсы автоматизированной информационной системы, а также вычислительные процессы, инициирующие получение и получающие доступ от имени пользователей, программ, средств вычислительной техники и других программно-аппаратных устройств информационно-телекоммуникационной инфраструктуры.

<sup>3</sup> Объект доступа представляет собой одну из сторон информационного взаимодействия, предоставляющую доступ.

<sup>4</sup> Алгоритм расчета контрольных сумм по ГОСТ Р 34.11-2012, 256 бит.

<sup>5</sup> Изделия не входят в комплект поставки Центра сертификатов доступа и приобретаются заказчиком самостоятельно.

<sup>6</sup> Настройка взаимодействия Центра сертификации с СКЗИ «КриптоПро CSP» описана в Приложении 5.

- программно-аппаратный криптографический модуль «КриптоПро HSM» версии 2.0 ЖТЯИ.00096-01 (исполнение 1К, комплектация 1 или 2). Программно-аппаратный криптографический модуль (далее – ПАКМ) предназначен для создания, хранения и удаления ключевых пар (открытый и закрытый ключи) центров сертификации инфраструктуры открытых ключей, создания ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств), а также генерации и проверки цифровой подписи.

### 1.3 Функции Центра сертификатов доступа

Программное средство «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» реализует следующие функции, для выполнения которых оно предназначено в заданных условиях применения:

- формирование идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств) на основе данных, полученных при первичной идентификации непосредственно от пользователей и средств вычислительной техники (устройств) через заявку на выпуск сертификатов безопасности (цифровых сертификатов), либо полученных от доменной службы каталогов или уполномоченных пользователей;
- выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
  - создание ключевых пар (открытый и закрытый ключи) пользователей и средств вычислительной техники (устройств);
  - формирование сертификатов безопасности (цифровых сертификатов) для пользователей и средств вычислительной техники (устройств);
  - формирование заявок на выпуск сертификатов безопасности (цифровых сертификатов) для пользователей и средств вычислительной техники (устройств);
  - выдача сертификатов безопасности (цифровых сертификатов) для их использования владельцами;
  - централизованное автоматическое (автоматизированное) отслеживание актуальности (с уведомлением владельцев о сроках действия) сертификатов безопасности (цифровых сертификатов);
- выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) центров сертификации инфраструктуры открытых ключей, в том числе:
  - создание, экспорт, импорт и удаление ключевой пары (открытый и закрытый ключи) центра сертификации (корневого и/или подчиненного);
  - создание, импорт, просмотр, экспорт и удаление корневого (самоподписанного) сертификата центра сертификации;
  - создание, просмотр, экспорт и удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации;
  - создание на основании запроса, импорт, просмотр, экспорт, удаление и отзыв сертификата для подчиненного центра сертификации;
- приостановка и/или возобновление действия сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
  - блокирование, возобновление действия, отзыв и перевыпуск сертификатов безопасности (цифровых сертификатов);
  - формирование, экспорт и публикация списка отозванных сертификатов безопасности (цифровых сертификатов);

## 1.4 Комплект поставки

Комплект поставки Центра сертификатов доступа включает в себя:

- Программное средство «Центр сертификации Aladdin Enterprise Certification Authority» на носителе оптической записи (rpm-пакет для установки на ОС РЕД ОС или Альт 8 СП, релиз 10, deb-пакет для установки на Astra Linux Special Edition).
- Программное средство «Центр регистрации Aladdin Enterprise Registration Authority» на носителе оптической записи (rpm-пакет для установки на ОС РЕД ОС или Альт 8 СП, релиз 10, deb-пакет для установки на Astra Linux Special Edition).
- Контрольные суммы (далее – КС) установочных пакетов (дистрибутивов) (rpm- и deb-пакеты) и исполняемых файлов Центра сертификации Aladdin eCA на носителе оптической записи;
- КС установочных пакетов (дистрибутивов) (rpm- и deb-пакеты) и исполняемых файлов Центра регистрации Aladdin eRA на носителе оптической записи;
- Программное средство «Утилита контроля целостности 2.0»;
- КС исполняемого файла программного средства «Утилита контроля целостности 2.0»;
- Эксплуатационная документация:
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Часть 1. Общие сведения»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Часть 2. Свидетельства о приёмке, упаковке и маркировке»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Приложение 3. Описание методов REST API»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство оператора»;
  - «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр регистрации Aladdin Enterprise Registration Authority»;

## 1.5 Имя пакета компонентов поставки

Имя пакета компонентов поставки представлено в формате:

• <name>	– название компонента;
• <major_version>	– мажорная версия компонента;
• <minor_version>	– минорная версия компонента;
• <release>	– номер релиза компонента;
• <build_number>	– номер сборки;
• <arch>	– целевая архитектура.

## 1.6 Доступные роли

В Центра сертификации Aladdin eCA определены следующие роли пользователей:

- Оператор

Пользователь с ролью «Оператор» должен обладать правами на работу с субъектами группы, над которой он может осуществлять свои ролевые права, и принадлежащими им сертификатами (выпуск, отзыв, приостановка и возобновление сертификата), иметь полномочия запуска обновления списка субъектов из ресурсной системы. Для конкретного «Оператора» можно определить перечень субъектов, над которыми он может осуществлять свои ролевые права, а также перечень групп субъектов, над элементами которых он может осуществлять свои ролевые права.

- Администратор

Пользователь с ролью «Администратор» должен иметь неограниченные права доступа к ОС и серверу, на котором развёрнут Центр сертификации Aladdin eCA, а также доступ через веб-интерфейс или программный интерфейс API к функциональным задачам и к функциям управления учетными записями. Все учётные записи могут быть созданы, отредактированы, удалены или заблокированы только пользователем с ролью «Администратор».

Доступные действия пользователей в соответствии с назначенными ролями приведены в таблице ниже (Таблица 2).

Таблица 2 – Полномочия пользователей в соответствии с назначенной ролью

Тип действия, осуществляемого пользователем, над объектом программы	Возможные роли пользователей	
	Оператор	Администратор
Установка или обновление программы	-	+
Установка лицензии на программу	-	+
Внесение изменений в конфигурационную информацию лицензии на программу	-	+
Просмотр информации о лицензии на ПО	-	+
Инициализация центра сертификации	-	+
Чтение конфигурационной информации о планах архивации в автоматическом режиме из базы данных	-	+
Внесение изменений в конфигурационную информацию о планах архивации в автоматическом режиме из базы данных	-	+
Чтение конфигурационной информации о уведомлениях об истечении срока действия сертификата	-	+
Внесение изменений в конфигурационную информацию о уведомлениях об истечении срока действия сертификата	-	+
Просмотр журнала событий	-	+
Архивация журнала событий	-	+
Экспорт журнала событий	-	+
Просмотр списка сертификатов центра сертификации (свои и подчинённые)	-	+
Импорт и экспорт закрытого ключа центра сертификации	-	+
Удаление сертификата центра сертификации	-	+

Тип действия, осуществляемого пользователем, над объектом	Возможные роли пользователей	
Просмотр цепочки сертификатов центра сертификации	-	+
Скачивание цепочки сертификатов центра сертификации	-	+
Скачивание сертификата центра сертификации	-	+
Скачивание сертификата центра сертификации в контейнере #pkcs12	-	+
Подписание запроса на сертификат подчинённого центра сертификации	-	+
Импортирование сертификата центра сертификации (активация центра сертификации)	-	+
Создание сертификатов доступа для полного набора субъектов ресурсных систем	-	+
Создание сертификатов доступа для ограниченного набора субъектов ресурсных систем	-	+
Просмотр списка сертификатов доступа для полного набора субъектов ресурсных систем	-	+
Просмотр списка сертификатов доступа для ограниченного набора субъектов ресурсных систем	+	+
Экспорт списка выпущенных сертификатов для полного набора субъектов ресурсных систем	-	+
Экспорт списка выпущенных сертификатов для ограниченного набора субъектов ресурсных систем	+	+
Скачивание сертификата доступа для полного набора субъектов ресурсных систем	-	+
Скачивание сертификата доступа для ограниченного набора доступных субъектов ресурсных систем	+	+
Скачивание сертификата доступа субъекта в контейнере #pkcs12 для полного набора субъектов ресурсных систем	-	+
Скачивание сертификата доступа субъекта в контейнере #pkcs12 для ограниченного набора субъектов ресурсных систем	+	+
Скачивание цепочки сертификатов для полного набора субъектов ресурсных систем	-	+
Скачивание цепочки сертификатов для ограниченного набора субъектов ресурсных систем	+	+
Управление статусом сертификата доступа субъекта для полного набора субъектов ресурсных систем	-	+
Управление статусом сертификата доступа субъекта для ограниченного набора субъектов ресурсных систем	+	+
Создание учётной записи с определением роли для субъектов ресурсных систем	-	+
Управление учётными записями субъектов ресурсных систем	-	+
Просмотр учётных записей субъектов ресурсных систем	-	+
Просмотр ограниченного списка субъектов ресурсных систем	+	+

Тип действия, осуществляемого пользователем, над объектом	Возможные роли пользователей	
Просмотр полного списка субъектов ресурсных систем	-	+
Просмотр списка полного набора зарегистрированных ресурсных систем	-	+
Просмотр списка ограниченного набора зарегистрированных ресурсных систем	+	+
Регистрация ресурсных систем	-	+
Обновление полного набора субъектов ресурсных систем	-	+
Обновление ограниченного набора субъектов ресурсных систем	+	+
Просмотр списка зарегистрированных центров валидации	-	+
Управление настройкой обновления списков отозванных сертификатов	-	+
Экспорт списка отозванных сертификатов	-	+
Моментальная публикация списка отозванных сертификатов	-	+
Регистрация центра валидации	-	+
Просмотр шаблонов сертификатов	-	+
Создание нового шаблона сертификата	-	+
Импорт шаблонов сертификатов	-	+
Редактирование созданных шаблонов сертификатов	-	+
Удаление созданных шаблонов сертификатов	-	+
Просмотр идентификаторов расширенного использования ключа	-	+
Просмотр ограниченного набора идентификаторов расширенного использования ключа	+	+
Создание пользовательских идентификаторов расширенного использования ключа	-	+
Удаление пользовательских идентификаторов расширенного использования ключа	-	+
Просмотр списка разрешённых издателей	-	+
Управление проверкой издателя	-	+
Перезагрузка веб-сервера	-	+
Контроль целостности исполняемых файлов программы	-	+

## 1.7 Режимы функционирования программы

Основным режимом функционирования Центра сертификации Aladdin eCA является нормальный режим.

В нормальном режиме должны исправно функционировать клиентская и серверная части программы, обеспечивая возможность круглосуточного функционирования, с перерывами на обслуживание (обновление программы).

Функционирование корневого и/или подчинённого Центра сертификации Aladdin eCA предусматривает автономный режим (Stand alone operation) или сетевой режим работы.

Сетевой режим работы Центра сертификации Aladdin eCA обеспечивает возможность кластеризации с целью отказоустойчивости<sup>7</sup>.

### **1.8 Действия по безопасной установке и настройке программы**

Установка программного средства производится только с диска, получаемого от разработчика, после выполнения действий по приёмке поставленного средства.

Установка (изменение) программного обеспечения компьютеров и локальной вычислительной сети должна осуществляться только в присутствии и под контролем администратора информационной безопасности того технологического участка, в котором эксплуатируется данное программное средство.

Настройка программного средства должна проводится привилегированным пользователем с ролью «Администратор», допускаемым к установке и настройке Центра сертификации Aladdin eCA.

### **1.9 Действия по реализации функций безопасности среды функционирования программы**

Для безопасной работы программного средства в среде ОС должно обеспечиваться:

- предотвращение несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администратора);
- разделение полномочий (ролей) пользователей;
- порядок обработки, хранения и передачи аутентификационной информации пользователей, созданной программным средством;
- срок хранения информации о зарегистрированных событиях безопасности не менее трех месяцев;
- синхронизация внутренних системных часов информационной системы для регистрации всех событий безопасности в журнале событий;
- защита аппаратного обеспечения с функционирующим программным средством от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

---

<sup>7</sup> Справочная информация по развертыванию кластера Центра сертификации Aladdin eCA приведена в «Приложение 4. Развертывание кластера Aladdin eCA» настоящего руководства

## 2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО СРЕДСТВА

### 2.1 Требования к программному обеспечению

#### 2.1.1 Требования к среде функционирования серверной части центра сертификации

Среда функционирования серверной части Центра сертификации Aladdin eCA :

- 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 «Орел»;
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск»;
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж»;
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Орел»;
  - РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;
  - РЕД ОС версия 8, конфигурация «Сервер»;
  - ОС Альт 8 СП, релиз 10, вариант исполнения Сервер.
- поддерживаемые СУБД:
  - PostgreSQL из состава ОС;
  - Postgres Pro;
  - Jatoba.
- поддерживаемая среда исполнения Java:
  - Java Axiom JDK Certified (компонент JRE);
  - Open JDK версии 17 и выше из состава поддерживаемых ОС.
- поддерживаемые веб-серверы:
  - Apache2 из состава ОС;
  - Nginx из состава ОС;
  - Cprnginx из состава СКЗИ «Крипто Про CSP».
- поддерживаемые ресурсные системы:
  - Samba DC;
  - Free IPA;
  - ALD PRO;
  - РЕД АДМ;
  - Microsoft AD;
  - Альт Домен.

#### 2.1.2 Требования к среде функционирования клиентской части центра сертификации

Среда функционирования клиентской части Центра сертификации Aladdin eCA:

- 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 «Орел»;
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск»;



- Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Орел»;
- РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;
- РЕД ОС версия 8, конфигурация «Сервер»;
- ОС Альт 8 СП, релиз 10, вариант исполнения Рабочая станция.
- веб-браузер из состава ОС;
- JC-WebClient 4.3.3 (для 64-битных систем)<sup>8</sup>.

## 2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования Центра сертификации Aladdin eCA:

- системные требования, предъявляемые к конфигурации серверного оборудования, зависят от количества выпускаемых сертификатов и количества одновременных обращений к серверу Центра сертификации Aladdin eCA приведены ниже (Таблица 3).

Таблица 3 – Системные требования, предъявляемые к серверу Центра сертификации Aladdin eCA

Приложение	Системные требования	Тип внедрения		
		Малое внедрение (до 1000 сертификатов и 5 одновременных соединений)	Среднее внедрение (до 20000 сертификатов и 15 одновременных соединений)	Крупное внедрение (до 100000 сертификатов и 50 одновременных соединений)
СУБД	ОЗУ, GB	2	3	4
	CPU, (core)	2	4	4
	HDD, GB	6	12	18
Центр сертификации Aladdin eCA	ОЗУ, GB	6	8	16
	CPU, (core)	2	4	6
	HDD, GB	40	60	300
ОС	ОЗУ, GB	4	4	4
	CPU, (core)	2	2	2
	HDD, GB	20	20	20
Итого	ОЗУ, GB	<b>12</b>	<b>15</b>	<b>24</b>
	CPU, (core)	<b>6</b>	<b>10</b>	<b>12</b>
	HDD, GB	<b>66</b>	<b>92</b>	<b>338</b>

- монитор с поддерживаемым разрешением экрана:
  - 1920x1080 16:9 HD 1080;
  - 1366x768 HD;
  - 1536x864;
  - 1440x900 8:5 WSXGA;

<sup>8</sup> При установке дополнительного программного обеспечения изделие обеспечивает возможность работы с ключевыми носителями (электронными ключами), при этом класс защиты не обеспечивается.

- 2560x1440;
- 1280x720 16:9 HD 720;
- 1600x900 16:9 HD+ 900p;
- 1680x1050 8:5 WSXGA+;
- 1280x1024 5:4 SXGA;
- 1280x800 8:5 WXGA;
- 1920x1200 8:5 WUXGA;
- устройства взаимодействия с пользователем:
  - клавиатура;
  - мышь;
- USB 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей:
  - JaCarta PKI;
  - JaCarta PRO;
  - JaCarta-2 PKI/ГОСТ;
  - JaCarta-2 ГОСТ.

## 3 ДЕЙСТВИЯ ПО ПРИЁМКЕ ПРОГРАММНОГО СРЕДСТВА

Приёмка Центра сертификатов доступа предусматривает проверку комплектности и контроль целостности установочных пакетов (дистрибутивов) Центра сертификации Aladdin eCA и Центра регистрации Aladdin eRA.

### 3.1 Проверка комплектности

Проверку комплектности программного средства выполняют путём сверки комплектности поставленного программного средства с комплектностью, указанной в разделе 3 документа «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Часть 1. Общие сведения» RU.АЛДЕ.03.01.020 30 01-1 (далее – Формуляр).

### 3.2 Контроль целостности установочных пакетов

Расчет КС установочных пакетов (дистрибутивов) программного средства, расположенных на носителе оптической записи из комплекта поставки, выполняется по алгоритму ГОСТ 34.11-2012, 256 бит.

Эталонные КС установочных пакетов (дистрибутивов) программного средства приведены в таблице 2 Формуляра, а также содержатся в следующих файлах на носителе оптической записи из комплекта поставки:

- `aeca-ca_[версия]_[номер сбоки].deb.txt` – для deb-пакета;
- `aeca-ca_[версия]_[номер сбоки].rpm.txt` – для rpm-пакета.
- `aeca-ra_[версия]_[номер сбоки].deb.txt` – для deb-пакета;
- `aeca-ra_[версия]_[номер сбоки].rpm.txt` – для rpm-пакета.

Допускается выполнять расчет контрольных сумм одним из следующих программных средств:

- «Утилита контроля целостности 2.0». Утилита входит в комплект поставки Центра сертификатов доступа.
- «ФИКС-Unix 1.0» (сертификат соответствия ФСТЭК № 680 от 30.10.2002 г.). Программное средство «ФИКС-UNIX 1.0» не входит в комплект поставки Центра сертификатов доступа.

Порядок расчета КС с помощью программного средства «Утилита контроля целостности 2.0»:

- установите оптический диск с установочными пакетами (дистрибутивами) в оптический привод;
- выполните монтирование оптического диска, выполнив в командной строке команду:

```
sudo mount /media/cdrom -o nojoliet,norock
```

- скопируйте с оптического диска в выбранный каталог файловой системы:
  - исполняемый файл утилиты «jcverify» и файл с его КС «jcverify.txt»;
  - установочный deb- или rpm-пакет (в зависимости от выбранной для среды функционирования программного средства ОС);
  - файл с КС соответствующего установочного пакета;
- проверьте КС исполняемого файла программного средства «Утилита контроля целостности 2.0», выполнив в командной строке команду:

```
sudo ./jcverify
```

- выполните анализ информации, отображаемой в терминале:
  - в случае успешной проверки отображается сообщение вида:

```
Checksums in the file jcverify.txt verified
```

- при нарушении целостности отображается сообщение вида:

```
An error occurred while processing!
```

```
Error: Hashes of the file jcverify.txt are not equal.
Actual: [рассчитанная КС]
Expected: [эталонная КС]
Exit code: 1
```

**При нарушении целостности исполняемого файла программного средства «Утилита контроля целостности 2.0» дальнейшая проверка КС установочного пакета запрещена.**

- проверьте КС установочного пакета, выполнив в командной строке команду:

```
sudo ./jcverify [имя файла с КС установочного пакета]
```

- выполните анализ информации, отображаемой в терминале:
  - в случае успешной проверки отображается сообщение вида:

```
Checksums in the file [имя файла с КС установочного пакета] verified
```

- при нарушении целостности отображается сообщение вида:

```
An error occurred while processing!
Error: Hashes of the file [имя файла с КС установочного пакета] are not equal.
Actual: [рассчитанная КС]
Expected: [эталонная КС]
Exit code: 1
```

Порядок расчета КС с помощью программного средства «ФИКС-UNIX 1.0»:

- установите оптический диск с установочными пакетами (дистрибутивами) программного средства в оптический привод и выполните его монтирование командой:

```
sudo mount /media/cdrom -o nojoliet,norock
```

- скопируйте в выбранный каталог файловой системы исполняемый файл программного средства «ФИКС-UNIX 1.0» `ufix_rus` и перейдите в этот каталог;
- выполните в командной строке следующие команды:

```
./ufix_eng -jR /media/cdrom/ > /tmp/contr_summ t.txt
./ufix_eng -e --alg s256 -E /tmp/contr_summ.txt /tmp/contr_summ.prj
./ufix_eng -h -E /tmp/contr_summ.prj /tmp/contr_summ.html
```

- откройте в веб-браузере сформированный отчет, выполнив в командной строке команду:

```
firefox /tmp/contr_summ.html
```

- выполните размонтирование оптического диска командой:

```
sudo umount /media/cdrom
```

- сравните рассчитанную КС (в html-отчете) установочного пакета с эталонной КС, приведенной в таблице 2 Формуляра на программное средство.

**При нарушении целостности установочного пакета (дистрибутива) дальнейшая установка Центра сертификации Aladdin eCA запрещена.**

## 4 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММНОГО СРЕДСТВА

Подготовка к установке Центра сертификации Aladdin eCA должна быть проведена на каждом компьютере, где предполагается его развертывание.

В зависимости от типа операционной системы действия по подготовке сервера различаются.

### 4.1 Таблица сетевого взаимодействия

При установке Центра сертификации Aladdin eCA осуществляется конфигурирование установленного в среде функционирования веб-сервера, в результате чего для внешнего доступа открывается порт сервера, используемый для подключения по протоколу HTTPS (по умолчанию 443). Изменение порта веб-сервера для подключения к нему по протоколу HTTPS осуществляется путем редактирования конфигурационного файла программного средства (см. раздел 5.2 настоящего руководства).

Ниже приведён список портов (Таблица 4), которые открывает для локальной передачи данных внутри сервера и использует Центр сертификации Aladdin eCA. Доступ к данным портам для внешних подключений ограничивается автоматически при установке программного средства с помощью утилиты «iptables» из состава ОС сервера. Во избежание возникновения ошибок в работе программного средства переназначение данных портов запрещено.

Таблица 4 – Таблица входящих сетевых портов

Порт	Транспорт	Протокол	Назначение
1100	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «certificate-authority-service» (Сервис сертификатов)
1150	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «storage-service» (Сервис хранения)
1200	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «templates-service» (Сервис шаблонов)
1250	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «security-service» (Сервис безопасности)
1300	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «licenses-service» (Сервис лицензирования)
1350	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «routes-service» (Сервис маршрутизации)
1400	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «external-integration-service» (Сервис внешних интеграций)
1450	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «validation-authority-service» (Сервис валидации)
1500	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «publisher-service» (Сервис публикации)
1550	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «subjects-service» (Сервис субъектов)
1600	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «ldap-service» (Сервис синхронизации по LDAP)

Порт	Транспорт	Протокол	Назначение
1650	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (Сервис журнализации)
1700	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «export-service» (Сервис экспорта)
1750	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «event-delivery-service» (Сервис доставки событий)
1800	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «settings-service» (Сервис настройки)
1850	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «x509-provider-service» (Сервис аутентификации по сертификату)
1900	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «api-gateway-service» (Сервис проксирования)

## 4.2 Подготовка сервера

Подготовка сервера Центра сертификации Aladdin eCA заключается в установке и настройке следующих программных компонентов:

- Зависимостей и подключение репозитория ОС.
- Среды исполнения Java.
- СУБД.
- Веб-сервера.
- СКЗИ «КриптоПро CSP» (для использования алгоритмов ГОСТ Р 34.10-2012 и RSA). Порядок установки и настройки СКЗИ «КриптоПро CSP» представлен в Приложении 5. Установка и настройка СКЗИ «КриптоПро CSP» могут быть выполнены после установки Центра сертификации Aladdin eCA в процессе его эксплуатации.

При использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программного средства должен быть организован по протоколу TLS ГОСТ, а также должна обеспечиваться TLS-аутентификация пользователей в программном средстве с использованием отечественных криптографических алгоритмов. Для этого 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** из состава СКЗИ «КриптоПро CSP» приведен в подразделе 4.6. После установки веб-сервера необходимо установить на СКЗИ «КриптоПро CSP» серверную лицензию, обеспечивающую возможность использования СКЗИ «КриптоПро CSP» в качестве TLS-сервера.

В зависимости от ОС сценарии подготовки различаются:

- для РЕД ОС 7.3 и РЕД ОС 8 сценарий подготовки описан в разделе 4.3;
- для Astra Linux Special Edition 1.7 и Astra Linux Special Edition 1.8 – в разделе 4.4;
- для Альт Сервер 8, релиз 10 – в разделе 4.5.

## 4.3 Подготовка сервера с операционной системой РЕД ОС

Далее приведена инструкция по подготовке сервера под управлением РЕД ОС 7.3 и РЕД ОС 8.

### 4.3.1 Подключение репозитория и установка зависимостей

- Для РЕД ОС репозитории настроены по умолчанию для скачивания из сети Интернет. Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

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

При ошибке следует проверить наличие доступа к сети Интернет.

- Если доступ к сети Интернет отсутствует, зависимости возможно установить с USB-носителя из комплекта поставки ОС следующим образом:
  - установите USB-носитель в соответствующий порт сервера;
  - перейдите в каталог USB-носителя;
  - для установки зависимостей выполните команду:

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

### 4.3.2 Установка среды исполнения Java

- Для обеспечения сертифицированной среды функционирования на сервере необходимо установить Axiom JDK Certified (см. подраздел 4.3.2.1).
- В случае, если обеспечение сертифицированной среды функционирования не требуется, возможно использовать программное обеспечение OpenJDK (см. подраздел 4.3.2.2).

#### 4.3.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified 17 воспользуйтесь [инструкцией с официального сайта производителя](https://axiomjdk.ru/pages/axiomjdk-install-guide-17.0.6/) <https://axiomjdk.ru/pages/axiomjdk-install-guide-17.0.6/>.

#### 4.3.2.2 Установка OpenJDK

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

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

### 4.3.3 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.

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

#### 4.3.3.1 Установка СУБД PostgreSQL<sup>9</sup>

- 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
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`<sup>10</sup> под администратором – установите число подключений `max_connections` в значение `1000`<sup>11</sup>.

- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`<sup>12</sup> 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
```

#### 4.3.3.2 Установка СУБД Postgres Pro<sup>13</sup>

- Загрузите скрипт для добавления репозитория, выполнив команду<sup>14</sup>:

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

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

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

<sup>9</sup> Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>

<sup>10</sup> Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>11</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>12</sup> Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

<sup>13</sup> Подробное описание приведено в официальной документации на Postgres Pro, размещённой по адресу <https://postgrespro.ru/docs>

<sup>14</sup> Команды ниже приведены для Postgres Pro версии 16.



- 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`<sup>15</sup> под администратором – установите число подключений `max_connections` в значение `1000`<sup>16</sup>.
- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`<sup>17</sup> 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
```

- 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
```

#### 4.3.3.3 Установка СУБД Jatoba<sup>18</sup>

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

**Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с CD/DVD носителя 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 `/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 командой:

<sup>15</sup> Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>16</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>17</sup> Расположение файла указано для 16 версии Postgre Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

<sup>18</sup> Подробное описание приведено в официальной документации на Jatoba, размещённой по адресу <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>

```
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
```

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

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

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором – установите число подключений `max_connections` в значение `1000`<sup>19</sup>.

- 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]
```

#### 4.3.4 Установка веб-сервера

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

<sup>19</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

#### 4.3.4.1 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 в apache, 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
```

#### 4.3.4.2 Установка веб-сервера Nginx

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

```
sudo dnf install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

### 4.4 Подготовка сервера с операционной системой Astra Linux Special Edition

Далее приведена инструкция по подготовке сервера под управлением Astra Linux Special Edition 1.7 («Смоленск», «Воронеж», «Орел») и Astra Linux Special Edition 1.8 («Смоленск», «Воронеж», «Орел»).

#### 4.4.1 Подключение репозитория и установка зависимостей

##### 4.4.1.1 Подключение репозитория и установка зависимостей Astra Linux Special Edition 1.7<sup>20</sup>

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

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

- Укажите ссылки на следующие репозитории:

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

- Укажите нижеприведённый репозиторий для развёртывания веб-сервера Nginx, если не требуется обеспечение сертифицированной среды<sup>21</sup>:

<sup>20</sup> Подробнее о репозиториях Astra Linux SE 1.7 см. в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=158598882>

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

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

```
apt-cdrom add
```

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

- Выполните обновление пакетов для ОС из указанных репозиториях, выполнив команду:

```
sudo apt update
```

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

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

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

#### 4.4.1.2 Подключение репозитория и установка зависимостей Astra Linux Special Edition 1.8<sup>22</sup>

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

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

- Укажите ссылки на следующие репозитории:

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

- Укажите нижеприведённый репозиторий для развёртывания веб-сервера Nginx, если не требуется обеспечение сертифицированной среды<sup>23</sup>:

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

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

```
apt-cdrom add
```

<sup>21</sup> Для обеспечения сертифицированной среды программный компонент «Центр сертификации Aladdin Enterprise Certification Authority» необходимо развёртывать с использованием веб-сервера Apache в ОС Astra Linux Special Edition 1.7

<sup>22</sup> Подробнее о репозиториях Astra Linux SE 1.8 см. в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043111>

<sup>23</sup> В Astra Linux для обеспечения сертифицированной среды программный компонент «Центр регистрации Aladdin eCA» необходимо развёртывать с использованием веб-сервера Apache

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

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

```
sudo apt update
```

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

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

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

#### 4.4.1.3 Поддержка активного режима замкнутой программной среды

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

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

#### 4.4.2 Установка среды исполнения Java

- Для обеспечения сертифицированной среды функционирования на сервере необходимо установить Axiom JDK Certified.
- В случае, если обеспечение сертифицированной среды функционирования не требуется, возможно использовать программное обеспечение OpenJDK.

##### 4.4.2.1 Установка Axiom JDK Certified

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

##### 4.4.2.2 Установка OpenJDK

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

- [инструкция для Astra Linux SE 1.7](#);
- [инструкция для Astra Linux SE 1.8](#)

#### 4.4.3 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.

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

#### 4.4.3.1 Установка СУБД PostgreSQL<sup>24</sup>

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду:

```
sudo apt install postgresql
```

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

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

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

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- При наличии мандатных политик<sup>25</sup>:

- выдайте полномочия пользователю `postgres`, выполнив команду:

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

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

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
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`<sup>26</sup> – установите число подключений `max_connections` в значение `1000`<sup>27</sup>.

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

```
sudo systemctl restart postgresql
```

#### 4.4.3.2 Установка СУБД Postgres Pro<sup>28</sup>

- Загрузите скрипт для добавления репозитория, выполнив команду<sup>29</sup>:

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

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

<sup>24</sup> Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>

<sup>25</sup> Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148>

<sup>26</sup> Расположение файла может отличаться. В инструкции расположение указано для 11 версии PostgreSQL. Для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>27</sup> Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>28</sup> Подробное описание приведено в официальной документации на Postgres Pro, размещённой по адресу <https://postgrespro.ru/docs>

<sup>29</sup> Команды ниже приведены для 16-ой версии Postgres Pro.

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

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

```
sudo apt update
```

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

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

- При наличии мандатных политик<sup>30</sup>:
  - выдайте полномочия пользователю `postgres`, выполнив команду:

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

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

```
sudo usermod -a -G shadow postgres
sudo setfacl -d -m u:postgres:r /etc/parsec/macdb
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`<sup>31</sup> с правами администратора – установите число подключений `max_connections` в значение `1000`<sup>32</sup>.
- 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
```

#### 4.4.3.3 Установка СУБД Jatoba<sup>33</sup>

- Создайте каталог `/localrepo`, выполнив команду:

```
mkdir /localrepo
```

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

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

- Дистрибутив СУБД Jatoba содержит:
  - каталог `/pool`;

<sup>30</sup> Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148>

<sup>31</sup> Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>32</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>33</sup> Подробное описание приведено в официальной документации на Jatoba, размещённой по адресу <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>

- каталог `/dists`;
- файл ключа `DEB-GPG-KEY-Jatoba`.

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

```
ls -l
```

- Установите открытый ключ репозитория командой:

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

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

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

- Обновите описания пакетов командой:

```
sudo apt update
```

- Установите основные пакеты СУБД Jatoba командой:

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

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

- При наличии мандатных политик<sup>34</sup>:

- выдайте полномочия пользователю `postgres`, выполнив команду:

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

• Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами администратора – установите число подключений `max_connections` в значение `1000`<sup>35</sup>.

- Добавьте СУБД Jatoba в автозагрузку командой:

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

<sup>34</sup> Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pagelId=238751148>

<sup>35</sup> Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.



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

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

В случае возникновения ошибки запуска следует обратиться к внутренним логам:

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

#### 4.4.4 Установка веб-сервера

ОС Astra Linux SE поддерживает веб-сервер Apache, которые обеспечивают сертифицированную среду функционирования. Веб-сервер Apache устанавливается из основного репозитория сертифицированной ОС.

Также в качестве веб-сервера можно использовать Nginx, но он устанавливается из расширенного репозитория. Использование веб-сервера Nginx приведёт к потере сертифицированной среды функционирования.

##### 4.4.4.1 Установка веб-сервера Apache

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

```
sudo apt install apache2
```

- Активируйте модули, выполнив поочередно команды:

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

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

```
sudo systemctl restart apache2.service
```

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

```
sudo systemctl enable apache2
```

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

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

##### 4.4.4.2 Установка веб-сервера Nginx

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

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

```
sudo apt install nginx
```

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

## 4.5 Подготовка сервера с операционной системой Альт Сервер

Далее приведена инструкция по подготовке сервера под управлением Альт Сервер 8, релиз 10.

### 4.5.1 Подключение репозитория и установка зависимостей

- Для развёртывания Центра сертификации Aladdin eCA с использованием веб-сервера Apache<sup>36</sup> перед началом установки компонента необходимо установить путь нахождения необходимого репозитория, отредактировав файл `/etc/apt/sources.list`, выполнив команду:

```
sudo nano /etc/apt/sources.list.d/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 команду:

```
sudo apt-get update
```

### 4.5.2 Установка среды исполнения Java

- Для обеспечения сертифицированной среды функционирования на сервере необходимо установить Axiom JDK Certified.
- В случае, если обеспечение сертифицированной среды функционирования не требуется, возможно использовать программное обеспечение OpenJDK.

#### 4.5.2.1 Установка Axiom JDK Certified

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

#### 4.5.2.2 Установка OpenJDK

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

### 4.5.3 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.

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

<sup>36</sup> Для обеспечения сертифицированной среды программный компонент «Центр сертификации Aladdin Enterprise Certification Authority» необходимо развёртывать с использованием web-сервера Nginx в ОС Альт Сервер 8, релиз 10

#### 4.5.3.1 Установка СУБД PostgreSQL<sup>37</sup>

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду<sup>38</sup>:

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

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

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

- Установите пакет `postgresql`, выполнив команду:

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

- Произведите инициализацию БД, выполнив команду:

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

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

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/15/data/postgresql.conf`<sup>39</sup> – установите число подключений `max_connections` в значение `1000`<sup>40</sup>.

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

```
sudo systemctl restart postgresql
```

#### 4.5.3.2 Установка СУБД Postgres Pro<sup>41</sup>

- Загрузите скрипт для добавления репозитория, выполнив команду<sup>42</sup>:

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

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

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

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

```
sudo apt-get update
```

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

<sup>37</sup> Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>

<sup>38</sup> Команды ниже приведены для установки 15-ой версии PostgreSQL.

<sup>39</sup> Расположение файла может отличаться. В инструкции расположение указано для 15 версии PostgreSQL. Для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>40</sup> Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>41</sup> Подробное описание приведено в официальной документации на Postgres Pro, размещённой по адресу <https://postgrespro.ru/docs>

<sup>42</sup> Команды ниже приведены для 16-ой версии Postgres Pro.

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`<sup>43</sup> с правами администратора – установите число подключений `max_connections` в значение `1000`<sup>44</sup>.
- 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
```

#### 4.5.3.3 Установка СУБД Jatoba<sup>45</sup>

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

**Требуется скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с CD/DVD носителя 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 `/base`;
  - каталог `/RPMS.classic`;
  - файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

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

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

- Обновите описания пакетов командой:

```
sudo apt-get update
```

- Установите основные пакеты СУБД Jatoba командой:

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

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

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

<sup>43</sup> Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

<sup>44</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

<sup>45</sup> Подробное описание приведено в официальной документации на Jatoba, размещённой по адресу <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>

```
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`<sup>46</sup>.

- 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]
```

#### 4.5.4 Установка веб-сервера

ОС Альт Сервер поддерживает веб-сервер Nginx, который обеспечивает сертифицированную среду функционирования. Веб-сервер Nginx устанавливается из основного репозитория сертифицированной ОС.

Также в качестве веб-сервера можно использовать Apache, но он устанавливается из расширенного репозитория. Использование веб-сервера Apache приведёт к потере сертифицированной среды функционирования.

##### 4.5.4.1 Установка веб-сервера Apache

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

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

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

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

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

- Создайте файлы:

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

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

Внесите следующий текст в созданный файл:

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

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

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

Внесите следующий текст в созданный файл:

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

<sup>46</sup> Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

```
</IfModule>
```

- Активируйте модули, выполнив поочередно команды:

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

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

```
sudo a2enport https
```

#### 4.5.4.2 Установка веб-сервера Nginx

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

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

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start nginx
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable nginx
```

#### 4.6 Установка веб-сервера Cpnnginx

Пакеты веб-сервера `cpnnginx` расположены в дистрибутиве СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP» (см. Приложение 5).

Порядок установки веб-сервера `cpnnginx`:

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

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

- установите следующие пакеты:

- для ОС Astra Linux SE командой `sudo dpkg -i <наименование пакета>.deb`:
  - o `cproscsp-nginx-64_5.0.13000-7_amd64.deb`;
  - o `lsb-cproscsp-rcrypt-64_5.0.13300-7_amd64.deb`;
  - o `cproscsp-pki-plugin-64_2.0.15000-1_amd64.deb`.
- для ОС РЕД ОС командой `sudo dnf install <наименование пакета>.rpm`:
  - o `cproscsp-nginx-64-5.0.13000-7.x86_64.rpm`;
  - o `lsb-cproscsp-rcrypt-64-5.0.13000-7.x86_64.rpm`.
- для ОС Альт Сервер командой `sudo apt-get install <наименование пакета>.rpm`:
  - o `cproscsp-nginx-64-5.0.13000-7.x86_64.rpm`;
  - o `lsb-cproscsp-rcrypt-64-5.0.13000-7.x86_64.rpm`.

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

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

- выполните проверку активации лицензии командой:

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

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start cpnnginx.service
```

- Добавьте веб-сервер в автозагрузку, выполнив команду:

```
sudo systemctl enable cpnnginx.service
```

## 4.7 Установка JC-WebClient

• Программное обеспечение JC-WebClient необходимо установить на компьютер, с которого будет выполняться управление серверной частью Центра сертификации Aladdin eCA через веб-интерфейс. JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях).

• При установке дополнительного программного обеспечения программное средство обеспечивает возможность работы с ключевыми носителями (электронными ключами). При этом класс защиты программного средства не обеспечивается.

- Скачайте дистрибутив JC-WebClient [с веб-сайта производителя](#).
- Установите зависимости.
- Установите JC-WebClient, выполнив команду:

РЕД ОС

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

Astra Linux SE

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

Альт Сервер

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

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

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

- Произведите запуск ПО JC-WebClient, выполнив команду:

```
sudo sh jcmon start
```

## 5 УСТАНОВКА ПРОГРАММНОГО СРЕДСТВА

Перед установкой Центр сертификации Aladdin eCA необходимо выполнить подготовку сервера, где предполагается развертывание программного средства, в соответствии с разделом 5 настоящего руководства.

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

### 5.1 Распаковка инсталляционного комплекта программного средства

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

РЕД ОС

sudo dnf install <наименование пакета>.rpm

Astra Linux SE

sudo dpkg -i <наименование пакета>.deb

Альт Сервер

sudo apt-get install <наименование пакета>.rpm

- Инсталляционный rpm/deb-пакет будет автоматически распакован в директорию /opt/aecaCa.
- Структура распакованного инсталляционного rpm/deb-пакета приведена в таблице ниже (Таблица 5).

Таблица 5 – Структура установочного комплекта Центра сертификации Aladdin eCA

Структурный элемент	Назначение элемента
../opt/aecaCa	установочный комплект программного средства, а также используемые дополнительные инструменты
/opt/aecaCa/digsig/keys/aladdin_pub.key	публичный открытый ключ производителя для обеспечения ЗПС ОС Astra Linux SE
../opt/aecaCa/bin	каталог с дополнительными утилитами
../opt/aecaCa/bin/jcverify	каталог утилиты контроля целостности «jcverify»
../opt/aecaCa/bin/jcverify/jcverify	утилита контроля целостности «jcverify»
../opt/aecaCa/bin/jcverify/jcverify.txt	вспомогательный файл для работы утилиты целостности «jcverify»
../opt/aecaCa/dist	путь развертывания продукта, содержит создаваемые временные файлы
..dist/archive/	архивы, сформированные в результате очистки журнала событий
..dist/backup/	созданные резервные копии Центра сертификации
..dist/certificates/account	расположение pkcs#12 контейнера сертификата администратора инициализации
..dist/certificates/ssl	расположение сертификатов для управления ssl-соединением
..dist/cryptotoken/	расположение pkcs#12 контейнеров, содержащих открытый и закрытый ключи Центров сертификации



Структурный элемент	Назначение элемента
../dist/environment/	расположение переменных окружения сервисов
../dist/logs/	расположения технических журналов сервисов
../opt/aecaCa/eula	файл лицензионного соглашения
../opt/aecaCa/samples	содержит шаблоны файлов конфигурации для внутреннего использования программным средством
../opt/aecaCa/scripts	содержит скрипты управления Центра сертификации Aladdin eCA
../scripts/external	содержит скрипт для экспорта шаблонов MSCS
../scripts/internal	скрипты для внутреннего использования программы, запускаемые автоматически при выполнении скриптов из каталога /opt/aecaCa/scripts
/opt/aecaCa/scripts/internal/aeca/selinux	политики, подключаемые к selinux, необходимые для функционирования Центра сертификации Aladdin eCA
../scripts/backup.sh	скрипт резервного копирования конфигурации Центра сертификации Aladdin eCA
../scripts/config.sh	bash-скрипт конфигурации Центра сертификации Aladdin eCA (развертывание продукта, настройка подключения к БД, управление конфигурацией сервисов)
../scripts/database_create.sh	скрипт создания базы данных на разворачиваемом сервере Центра сертификации с предустановленными параметрами по умолчанию (именем пользователя, наименованием базы данных и т.д.)
../scripts/diagnostics.sh	скрипт сбора диагностических данных
../scripts/email_config.sh	bash-скрипт управления шаблонами email-рассылки
../scripts/install.sh	скрипт установки и обновления текущей версии Центра сертификации Aladdin eCA
../scripts/integrity_check.sh	скрипт контроля целостности исполняемых файлов
../scripts/restore.sh	скрипт восстановления из резервной копии конфигурации Центра сертификации Aladdin eCA
../scripts/restore_access.sh	скрипт резервного восстановления доступа к Центру сертификации Aladdin eCA
../scripts/export-ca-data.sh	скрипт экспорта файлов CRL, Delta CRL, AIA из Центра сертификации Aladdin eCA
../scripts/uninstall.sh	скрипт удаления Центра сертификации Aladdin eCA
../opt/aecaCa/services	сервисы Серверной части Центра сертификации

Структурный элемент	Назначение элемента
<code>../opt/aecaCa/services/cryptoproviders</code>	каталог файлов для взаимодействия со сторонним криптопровайдером
<code>../services/checksum.md5</code>	файл эталонных хэш-сумм сервисов и список сервисов, подвергаемых контролю целостности
<code>../services/internal.md5</code>	файл эталонных хэш-сумм сервисов и список сервисов, подвергаемых контролю целостности (для внутреннего использования)
<code>../opt/aecaCa/static</code>	артефакты Клиентской части Центра сертификации

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

## 5.2 Настройка параметров конфигурации программного средства

- Конфигурация Центра сертификации Aladdin eCA задается с помощью параметров конфигурационного файла `/opt/aecaCa/scripts/config.sh`.

- Перед установкой программного компонента определите значения следующих параметров:
  - `webserver` – укажите используемый веб-сервер (nginx, apache или cprnginx). О выборе веб-сервера смотри в подразделе 5.4. Также значение параметра можно будет ввести при запуске инсталлятора в интерактивном режиме;
  - `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 по пути `/etc/apache2`, для РЕД ОС по пути `/etc/httpd`; для Alt Linux конфигурация `apache` располагается по пути `/etc/httpd2/conf`; конфигурация cprnginx располагается по пути `/etc/opt/cprosp/cprnginx`);
  - `database_password` – укажите пароль пользователя базы данных. После обновления с версии 2.1 до версии 2.2 (см. раздел 12), а также после создания и настройки базы данных (см. подраздел 5.4) пароль пользователя базы данных отображается в конфигурационном файле в зашифрованном виде (алгоритм шифрования AES-256 с использованием сгенерированного в файле `/opt/aecaCa/scripts/key` ключа шифрования);

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

- `root_cert_path` – абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД. Значение параметра необходимо заполнить только при включенном флаге обязательного использования TLS для подключения к СУБД (при значении параметра `use_tls=true`). Иначе (при `use_tls=false`) следует оставить параметр незаполненным;
- `hostname` – укажите полное имя сервера Центра сертификации Aladdin eCA. Установленное значение заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых при развёртывании локального субъекта веб-сервера и сертификата для него.

- Для соответствия Центра сертификатов доступа 4 уровню доверия, установленному документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждённым приказом ФСТЭК России от 2 июня 2020 г. № 76) при использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программного средства должен быть организован по протоколу TLS ГОСТ, а также должна обеспечиваться TLS-аутентификация пользователей в программном средстве с использованием отечественных криптографических алгоритмов. Для этого настройте конфигурационный файл в соответствии с таблицей ниже (Таблица 6).

Таблица 6 – Параметры для настройки TLS ГОСТ

Параметр	Значение
webserver	'cpnginx'
webserver_path	'/etc/opt/cproscsp/cpnginx'
initial_cryptography_provider	'CRYPTO_PRO'
initial_cryptography_key_algorithm	'GOST_R_34_10_2012'
initial_cryptography_key_bits	'256' или '512'
initial_cryptography_hash_algorithm	'GOST_R_34_11_2012'
initial_ca_common_name	пример значения: 'INITIAL_CA_GOST'
initial_admin_principal	пример значения: 'INITIAL_ADMIN_GOST'
sign_provider	'CRYPTO_PRO'
sign_key_algorithm	'GOST_R_34_10_2012'
sign_key_length	'256' или '512'
sign_hash_algorithm	'GOST_R_34_11_2012'

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

```
sudo nano /opt/aecaCa/scripts/config.sh
```

- Настраиваемые параметры конфигурационного файла позволяют задавать:
  - параметры конфигурации развёртывания сервисов центра сертификации;
  - параметры e-mail уведомлений пользователям об истечении срока действия выданного сертификата;
  - параметры конфигурации центра валидации;
  - параметры конфигурации технического центра сертификации, создаваемого по умолчанию в процессе развёртывания сервера центра сертификации;
  - параметры сертификата технического центра сертификации;
  - параметры сертификата учётной записи администратора инициализации;
  - параметры сертификата веб-сервера технологического центра сертификации;
  - расписание синхронизации ресурсных систем;
  - расписание публикации списка отозванных сертификатов;

- расписание проверки срока действия сертификатов центров сертификации и выпущенных сертификатов субъектов;
- расписание архивации журнала событий;
- конфигурацию базы данных.
- Полный перечень и описание параметров конфигурации приведено в Таблица 7.

Таблица 7 – Описание параметров конфигурации

Параметр	Значение параметра по умолчанию	Описание
<b>Конфигурация развертывания</b>		
webserver	'#CHANGEIT'	Используемый веб-сервер (nginx, apache или cprnginx)
webserver_path	'#CHANGEIT'	Папка с файлами для развёртывания сервиса (конфигурация nginx располагается по пути <code>etc/nginx</code> ; конфигурация apache располагается: для Astra Linux по пути <code>/etc/apache2</code> , для РЕД ОС по пути <code>/etc/httpd</code> ; для AltLinux конфигурация apache располагается по пути <code>/etc/httpd2/conf</code> ; конфигурация cprnginx располагается по пути <code>/etc/opt/cproscsp/cprnginx</code> )
aeca_path	'/opt/aecaCa/dist'	Папка с файлами для развёртывания Центра сертификации Aladdin eCA
environment_path	'/opt/aecaCa/dist/environment'	Папка с переменными окружения для сервисов
cryptotoken_path	'/opt/aecaCa/dist/cryptotoken'	Папка, содержащая открытый и закрытый ключи для доступа (аутентификации) к центру сертификации
webserver_config_path	'/opt/aecaCa/dist/webserver'	Расположение конфигурации Центра сертификации Aladdin eCA для веб-сервера

Параметр	Значение параметра по умолчанию	Описание
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 сертификации 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 сертификации 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 веб-серверов Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cpnginx осуществляется с помощью утилиты «срconfig» из состава СКЗИ «КриптоПро CSP»<sup>47</sup>.</p>
<b>Параметры проксирования nginx</b>		
		Время ожидания подключения к прокси-серверу перед тем, как будет выдано сообщение об ошибке.
proxy_connect_timeout	'320'	Только для nginx.
		Настраивается разработчиком Центра сертификации Aladdin eCA, редактировать не следует.
		Время ожидания ответа от прокси-сервера после отправки запроса. Если ответ не получен в течение этого времени, запрос считается неудачным.
proxy_send_timeout	'320'	Только для nginx.
		Настраивается разработчиком Центра сертификации Aladdin eCA, редактировать не следует.

<sup>47</sup> Инструкция по установке и настройке cpnginx - <https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/440/0/nginx-gost-binary-packages>. Описание порядка конфигурирования наборов шифров представлено в разделе 6.

Параметр	Значение параметра по умолчанию	Описание
		Время ожидания чтения ответа от прокси-сервера после получения успешного запроса. Если ответ не получен в течение этого времени, запрос считается неудачным.
proxy_read_timeout	'720'	Только для nginx.
		Настраивается разработчиком Центра сертификации Aladdin eCA, редактировать не следует.
<b>Путь до резервных копий</b>		
		Папка, в которую сохраняются резервные копии Центра сертификации Aladdin eCA
backup_path	'/opt/aecaCa/dist/backup'	
<b>Путь хранения архива журнала событий</b>		
		Папка, в которую сохраняется журнал событий (лог-файлы)
logs_base	'/opt/aecaCa/dist/logs'	
		Папка, в которую сохраняется архив журнала событий, сформированный в результате автоматической архивации по заданным параметрам
archive_path	'/opt/aecaCa/dist/archive'	
		Максимальный размер лог-файла (файла с диагностической информацией) сервиса перед его архивацией.
logs_file_max_size	'10MB'	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.
		Максимальный срок хранения архивов с лог-файлами в днях.
logs_max_history	'10'	Архивы, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться.
		Максимальный общий объем лог-файлов, включая архивы, каждого типа (access или service) для каждого сервиса.
logs_total_size_cap	'100MB'	При достижении данного объема наиболее старые архивы данного типа будут удаляться.
<b>Путь хранения контейнера сертификата и ключа веб-сервера, а также цепочек сертификатов разрешенных издателей</b>		
		Папка, содержащая сертификат веб-сервера и цепочки сертификатов разрешённых издателей
certificates_ssl_path	'/opt/aecaCa/dist/certificates/ssl'	

Параметр	Значение параметра по умолчанию	Описание
certificates_account_path	'/opt/aecaCa/dist/certificates/account'	Папка, содержащая сертификат администратора инициализации в контейнере .p12
<b>Конфигурация пользователя</b>		
aeca_user	'aeca'	Имя пользователя Центра сертификации Aladdin eCA, используемое для работы программы.
aeca_group	'aeca'	Группа, в которой состоит пользователь Центра сертификации Aladdin eCA
<b>Конфигурация памяти</b>		
memory	'8192'	<p>Лимит оперативной памяти для программы. Значение в Мб.</p> <p>ЦС при запуске резервирует указанное в данном параметре количество оперативной памяти для своих сервисов.</p> <p>При значении параметра менее 8 Гб ЦС не запустится – будет выдано сообщение об ошибке.</p> <p>При значении параметра, превышающем количество оперативной памяти хоста, будет использована вся доступная оперативной памяти хоста.</p> <p>Необходимо изменять при крупном внедрении.</p>
enable_gc_diagnostic	'false'	<p>Флаг сбора диагностической информации о памяти</p> <p>При включении данного флага и выполнении скрипта сбора диагностических данных в архиве диагностических данных<sup>48</sup> будет содержаться лог сборщика мусора и дампы памяти для упавших приложений ЦС.</p>
<b>Конфигурация базы данных</b>		
max_db_pool_size	'200'	<p>Максимальный размер пула подключений к СУБД.</p> <p>Настраивается разработчиком Центра сертификации Aladdin eCA, редактировать не следует.</p>

<sup>48</sup> Размещение скрипта сбора диагностических данных – /opt/aecaCa/scripts/diagnostics.sh

Параметр	Значение параметра по умолчанию	Описание
use_tls	false	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя базы данных, используемое для работы Центра сертификации Aladdin eCA
database_password	'#CHANGEIT'	Пароль пользователя базы данных, используемый для работы Центра сертификации Aladdin eCA. 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	'aecaca'	Имя базы данных, используемой Центром сертификации Aladdin eCA
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД
<b>Конфигурация аеса-са</b>		
http_port	'80'	Порт для подключения к программному компоненту «Центр Сертификации» по протоколу http
https_port	'443'	Порт для подключения к программному компоненту «Центр Сертификации» по протоколу https
number_of_services	'17'	Количество активных сервисов в системе. Настраивается разработчиком Центра сертификации Aladdin eCA, редактировать не следует.
hostname	'localhost'	Имя сервера, на котором развёртывается Центр сертификации. Также заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых (при развёртывании ЦС) сертификата веб-сервера и локального субъекта. Должно совпадать с hostname сервера.
<b>Переменные окружения, используемые всеми сервисами</b>		
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
internal_http_read_timeout	'240'	Максимальный таймаут ожидания ответа методов сервисов при внутреннем взаимодействии. Единица измерения – секунды.
internal_http_connection_timeout	'60'	Максимальный таймаут ожидания подключения к сервисам при внутреннем взаимодействии. Единица измерения – секунды.
<b>Ключ для внутренней аутентификации</b>		
api_key	'2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810'	Значение ключа для внутренней аутентификации. Для служебного пользования, доступ к учётной записи Системного администратора ограничен, установку программы выполняет ответственный специалист
<b>Переменные окружения, используемые certificate-authority-service</b>		
pkcs12_key_protection_algorithm	'PBEWithHmacSHA256AndAES_256'	Алгоритм хеширования для ключа контейнера PKCS12 Допустимые значения: PBEWithHmacSHA256AndAES_256 - рекомендуется; PBEWithSHA1AndDESede - устаревший
pkcs12_mac_protection_algorithm	'HmacPBESHA256'	Алгоритм хеширования MAC контейнера PKCS12 Допустимые значения: HmacPBESHA256 - рекомендуется; HmacPBESHA1 - устаревший
pkcs12_certificate_protection_algorithm	'PBEWithHmacSHA256AndAES_256'	Алгоритм хеширования для сертификата контейнера PKCS12 Допустимые значения: PBEWithHmacSHA256AndAES_256 - рекомендуется; PBEWithSHA1AndRC2_40 - устаревший
<b>Переменные окружения, используемые ldap-service</b>		
ldap_sync_connection_point	'0 */30 * * * *'	CRON выражение, по которому запускается частичная синхронизация зарегистрированных точек подключения (значение по умолчанию: '0 */30 * * * *' - запуск каждые полчаса)
ldap_sync_resource	'0 0 0 * * *'	CRON выражение, по которому запускается полная синхронизация ресурсных систем (значение по умолчанию: '0 0 0 * * *' - запуск каждую полночь)
ldap_partition_size	'1000'	Максимальное количество объектов, получаемых из ресурсных систем при каждом запросе.

Параметр	Значение параметра по умолчанию	Описание
<b>Переменные окружения, используемые publisher-service</b>		
crl_scheduler	'0 */1 * * * *'	CRON выражение, по которому запускается служба выпуска CRL
<b>Переменные окружения, используемые event-delivery-service</b>		
email_host	'127.0.0.1'	Хост почтового сервера
email_port	'25'	Порт почтового сервера
email_login	'aeca'	Логин пользователя
email_password	'aeca'	Пароль пользователя
email_from	'no_reply@aeca.ru'	Почтовый адрес, с которого отправлено сообщение. Может не работать. Google предоставляет логин
email_schedule	'0 0 12 * * *'	CRON для запуска метода отправки почтовых уведомлений
email_enabled	'true'	Флаг отправки почтовых уведомлений, если выкл. то сообщения не отправляются, но помечаются, как отправленные
email_protocol	'smtp'	Протокол подключения к почтовому серверу
email_smtp_auth	'false'	Флаг: использование SMTP-авторизации
email_start_tls	'false'	Флаг: использование директивы start tls при подключении к почтовому серверу
<b>Переменные окружения, используемые validation-service</b>		
aeca_va_port	'8888'	Порт, на котором запущен Центр валидации
aeca_cdp_port	'8080'	Порт, на котором запущен Центр валидации – CDP (точка распространения)
aeca_crl_publish_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/publish-crl/{2}'	Шаблон URL точки публикации CRL
aeca_crl_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/get-crl/{2}'	Шаблон URL точки распространения CRL
aeca_delta_crl_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/get-delta-crl/{2}'	Шаблон URL точки распространения Delta CRL
aeca_aia_publish_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/aia/publish-aia/{2}'	Шаблон URL точки публикации AIA

Параметр	Значение параметра по умолчанию	Описание
aeca_aia_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/aia/get-aia/{2}'	Шаблон URL точки распространения AIA
aeca_ocsp_pattern	'http://{0}:{1}/aeca-va/ocsp'	Шаблон URL сервиса OCSP
<b>Переменные окружения, используемые settings-service</b>		
initial_cryptography_provider	'EMBEDDED'	Криптопровайдер (используется для технологического ЦС и сертификатов веб-сервера и администратора инициализации) Доступные для выбора значения: 'EMBEDDED' и 'CRYPTO_PRO'
initial_cryptography_key_algorithm	'RSA'	Алгоритм ключа (используется для технологического ЦС и сертификатов веб-сервера и администратора инициализации) Доступные для выбора значения алгоритмов ключа: <ul style="list-style-type: none"> <li>для стандартного провайдера (EMBEDDED) - 'RSA' и 'ECDSA'</li> <li>для провайдера КриптоПро (CRYPTO_PRO) - 'RSA' и 'GOST_R_34_10_2012'</li> </ul>
initial_cryptography_key_bits	'2048'	Длина ключа (используется для технологического ЦС и сертификатов веб-сервера и администратора инициализации)
initial_cryptography_hash_algorithm	'SHA256'	Хеш алгоритм (используется для технологического ЦС) Доступные для выбора значения алгоритмов хэширования: Для стандартного провайдера (EMBEDDED): <ul style="list-style-type: none"> <li>для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'</li> <li>для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'</li> </ul> Для провайдера КриптоПро (CRYPTO_PRO): <ul style="list-style-type: none"> <li>для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012'</li> <li>для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'</li> </ul>
initial_ca_common_name	'INITIAL_CA'	Subject DN сертификата технологического ЦС

Параметр	Значение параметра по умолчанию	Описание
initial_ca_hash_algorithm	'SHA256'	Хеш алгоритм сертификата технологического ЦС
initial_ca_key_algorithm	'RSA'	Алгоритм ключа сертификата технологического ЦС
initial_ca_key_bits	'2048'	Длина ключа сертификата технологического ЦС
initial_admin_principal	'INITIAL_ADMIN'	Имя учетной записи администратора инициализации
initial_client_key_algorithm	'RSA'	Алгоритм ключа сертификата администратора инициализации
initial_client_key_bits	'2048'	Длина ключа сертификата администратора инициализации
initial_client_password	'INITIAL'	Пароль от pkcs12 контейнера сертификата администратора инициализации
initial_server_key_algorithm	'RSA'	Алгоритм ключа сертификата веб-сервера
initial_server_key_bits	'2048'	Длина ключа сертификата веб-сервера
initial_server_password	'INITIAL'	Пароль от pkcs12 контейнера сертификата веб-сервера
certificate_server_name	'server'	Шаблон имени файлов сертификата и закрытого ключа сертификата Веб-сервера
issuers_name	'issuers'	Шаблон имени файла активных издателей
<b>Переменные окружения, используемые logs-service</b>		
archive_cron	'0 0 0 1 * *'	CRON выражение, по которому запускается архивация журнала событий
archive_enabled	'true'	Флаг: включена архивация. Возможные значения: true,false
archive_millis_ago	'15778800000'	Период архивации (мс) (архивировать записи старше...)
<b>Переменные окружения, используемые security-service</b>		
session_max_count	'100'	Максимальное число одновременных сессий аккаунта в виде натурального числа. При указании значения «-1» ограничение на количество одновременных сессий пользователя будет отсутствовать.
token_expire	'18000'	Время жизни JWT-токена (маркера доступа), мс.

Параметр	Значение параметра по умолчанию	Описание
refresh_expire	'86400000'	Время жизни JWT-токена обновления, мс.
sign_provider	'EMBEDDED'	Провайдер подписи маркера доступа (выбирается между стандартным - 'EMBEDDED' и КриптоПро - 'CRYPTO_PRO')
sign_key_algorithm	'RSA'	Алгоритм ключа подписи маркера доступа. Для стандартного провайдера доступны алгоритмы 'RSA' и 'ECDSA'. Для провайдера КриптоПро доступны алгоритмы 'RSA' и 'GOST_R_34_10_2012'.
sign_key_length	'2048'	Длина ключа подписи маркера доступа
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи Доступные для выбора значения алгоритмов хэширования: 1) для стандартного провайдера (EMBEDDED): <ul style="list-style-type: none"> <li>для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384'</li> <li>для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384'</li> </ul> 2) для провайдера КриптоПро (CRYPTO_PRO): <ul style="list-style-type: none"> <li>для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012'</li> <li>для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384'</li> </ul>
block_inactive_account_delay	'0'	Период неактивности в миллисекундах, после которого учетные записи операторов блокируются. Значение по умолчанию – 0, обозначающее отсутствие ограничения на неактивность учетных записей операторов. Операциями, обновляющими дату и время последней активности пользователя, являются: <ul style="list-style-type: none"> <li>успешная аутентификация, включая аутентификацию в Центре сертификации и Центре регистрации;</li> <li>успешное обновление маркера доступа, включая его обновление в Центре сертификации и Центре регистрации.</li> </ul>

Параметр	Значение параметра по умолчанию	Описание
block_inactive_account_cron	'0 0 0 * * *'	CRON-выражение, определяющее расписание запуска блокировки учетных записей операторов, период неактивности которых равен или превышает указанное в параметре «block_inactive_account_delay» значение. Значение по умолчанию – запуск каждую полночь.
<b>Переменные окружения, используемые api-gateway-service</b>		
		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 Центра сертификации Aladdin eCA, редактировать не следует.
max_requests_count	'30'	
<b>Переменные окружения, используемые subjects-service</b>		
ldap_automatically_certificates_publication_enable	'true'	Флаг: включена автоматическая публикация сертификатов, требующих публикации Возможные значения: true/false
ldap_automatically_certificates_publication_cron	'0 0 * * * *'	CRON выражение, по которому запускается автоматическая публикация сертификатов, требующих публикации. Значение по умолчанию – '0 0 * * * *', обозначающее запуск публикации сертификатов, ожидающих её, каждый час.

### 5.3 Подключение Центра валидации

- Если порт подключения к точке распространения Центра валидации имеет отличное от заданного по умолчанию (8080) значение, то необходимо привести в соответствие значение параметра `aeca_cdp_port` конфигурационного файла `/opt/aecaCa/scripts/config.sh`.

### 5.4 Создание и настройка базы данных

Перед установкой Центра сертификации Aladdin eCA необходимо создать и настроить базу данных одним из следующих способов:

- В автоматическом режиме посредством запуска скрипта (в результате будет создана база данных с параметрами, указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh`). Порядок создания и настройки базы данных в автоматическом режиме приведен в подразделе 5.4.1.
- В ручном режиме (в результате будет создана база данных с параметрами, указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh`). Порядок создания и настройки базы данных в ручном режиме для PostgreSQL приведен в подразделе 5.4.2, а для Jatoba – в 5.4.3.

После создания и настройки базы данных пароль пользователя базы данных, заданный в конфигурационном файле `/opt/aecaCa/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/aecaCa/scripts/key` ключа шифрования.

База данных предназначена для хранения информации:

- об учетных записях;
- о сертификатах;
- сведений о субъектах;
- сведений о ресурсных системах;
- о шаблонах;
- журнала событий;
- сведений о лицензии;
- профили сертификатов;
- профили конечных сущностей;
- центры сертификатов;
- настройки оповещения пользователей по e-mail об истечении срока действия сертификата;
- о ролях пользователей;
- о группах субъектов;
- о дискретных правах, определенных для ролей пользователей;
- Security Groups.

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

- Предварительно необходимо:
  - распаковать инсталляционный пакет программного компонента в соответствии с подразделом 5.1 настоящего документа;
  - указать параметры создаваемой базы данных в конфигурационном файле `/opt/aecaCa/scripts/config.sh` (см. подраздел 5.2 настоящего руководства).
- Запустите скрипт создания и настройки базы данных с параметрами по умолчанию, выполнив команду от имени суперпользователя (с правами `sudo` или `root`)<sup>49</sup>:



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

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

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

Требования к настройке предварительно установленной СУБД PostgreSQL:

- создание пользователя, от имени которого будет осуществляться взаимодействие с СУБД;
- создание базы данных, используемой программным компонентом в процессе работы;
- назначение созданному пользователю полных прав доступа к созданной базе данных.

<sup>49</sup> Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std-jatoba4-client`). Установка и настройка СУБД описана в подразделах ,  или 4.5.2 в зависимости ОС.

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

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

```
sudo -u postgres psql
```

- Создайте пользователя базы данных, выполнив команду:

```
CREATE USER aeca;
```

где **aeca** – задаваемое имя пользователя по умолчанию, в случае указания отличного имени пользователя, требуется соответственно отредактировать конфигурационный файл (см. подраздел 5.2).

- Задайте пароль пользователю, выполнив команды:

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

где **'aeca'** – задаваемый пароль пользователя по умолчанию. В случае указания отличного пароля, требуется соответственно отредактировать конфигурационный файл (см. подраздел 5.2).

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

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecaca;
```

где **aecaca** – задаваемое имя базы данных по умолчанию, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационный файл (см. подраздел 5.2).

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

```
ALTER DATABASE aecaca OWNER TO aeca;
```

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

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

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

```
exit
```

- Перезапустите СУБД PostgreSQL, выполнив команду:

```
sudo systemctl restart postgresql
```

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

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

где **aecaca** – имя созданной базы данных.



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

Требования к настройке предварительно установленной СУБД Jatoba:

- создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД;
- создание базы данных, используемой Программой в процессе работы;
- назначение созданному пользователю полных прав доступа к созданной базе данных.

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите Jatoba, выполнив команду:

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

Добавьте запуск Jatoba в автозагрузку, выполнив команду:

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

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

РЕД ОС

```
sudo -u postgres psql
```

Astra Linux SE

```
sudo -u postgres psql
```

Альт Сервер

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

- Создайте пользователя базы данных, выполнив команды:

```
CREATE USER aeca;
```

где **aeca** – задаваемое имя пользователя.

- Задайте пароль пользователю, выполнив команды:

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

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

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

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecasa;
```

где **aecasa** – задаваемое имя базы данных.

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

```
ALTER DATABASE aecasa OWNER TO aeca;
```

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

```
GRANT ALL PRIVILEGES ON DATABASE aecasa TO aeca;
```

```
\q
```

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

```
exit
```

- Перезапустите СУБД Jatoba, выполнив команду:

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

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

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

где **aecaca** – имя созданной базы данных.

## 5.5 Установка программного средства

- Для инициализации процесса установки Центра сертификации Aladdin eCA необходимо запустить скрипт с правами суперпользователя (от имени пользователя root, либо с использованием sudo)<sup>50</sup>:

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

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

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

- При использовании Astra Linux Special Edition и наличии мандатных политик<sup>51</sup> может быть выведено сообщение:

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

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

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

Повторно запустите скрипт установки. После инициализации процесса установки интерактивный инсталлятор будет запущен и пользователю будет предложено (в случае, если ранее на сервере был установлен Центр сертификации Aladdin eCA):

- установить Центр сертификации Aladdin eCA ;
- установить обновление Центра сертификации Aladdin eCA ;
- завершить работу инсталлятора.

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

- В случае, если в конфигурационном файле **/opt/aecaCa/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.

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

<sup>50</sup> Выполнение скрипта требует наличия утилиты **psql** из пакета СУБД (**postgresql**, **postgresql-client**, **postgrespro-std**, **jatoba4-client**). Установка и настройка СУБД описана в подразделах **❑**, **❑** или 4.5.2 в зависимости ОС.

<sup>51</sup> Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148>

При выборе веб-сервера apache, nginx или cpanginx требуется предварительно выполнить установку пакета, описанную в подразделах 4.3.4 (для РЕД ОС), 4.4.4 (для Astra Linux), 4.5.4 (для Альт Сервер) настоящего руководства.

- В случае, если в конфигурационном файле `/opt/aecaCa/scripts/config.sh` не определено расположение конфигурации выбранного веб-сервера (параметр `webserver_path`), то в процессе установки пользователю будет предложено ввести расположение (конфигурация nginx располагается по пути `etc/nginx`; конфигурация apache располагается: для Astra Linux по пути `/etc/apache2`, для РЕД ОС по пути `/etc/httpd`; для AltLinux конфигурация `apache` располагается по пути `/etc/httpd2/conf`; конфигурация `cpanginx` располагается по пути `/etc/opt/cproccsp/cpanginx`).

- В процессе установки осуществляется:

- создание системного пользователя и соответствующей группы, от имени которых функционирует продукт;
- установка прав для создаваемого пользователя продукта;
- подготовка, установка параметров и служебных сервисов;
- запуск служебных сервисов;
- запись номера сборки Центра сертификации Aladdin eCA в базу данных<sup>52</sup>;
- создание и выпуск сертификата технологического центра сертификации;
- выпуск сертификата веб-сервера технологического центра сертификации;
- создание учётной записи и выпуск сертификата администратора инициализации.

- Ход установки программного компонента отображен в виде горизонтальной шкалы с указанием процентов выполнения установки.

В результате успешной установки программного средства:

- В каталоге `/opt/aecaCa/dist/certificates/account` (значение по умолчанию параметра `certificates_account_path` конфигурационного файла `config.sh`) будет выпущен сертификат администратора инициализации (с использованием выбранного алгоритма – RSA, ECDSA или ГОСТ<sup>53</sup>) – контейнер закрытого ключа `INITIAL_ADMIN.p12` (`INITIAL_ADMIN_GOST.p12`) (имя контейнера задано в параметре `initial_admin_principal` конфигурационного файла).

- Выпущен технологический сертификат веб-сервера (с использованием выбранного алгоритма - RSA, ECDSA или ГОСТ) и применён в качестве сертификата веб-сервера технологического Центра сертификации;

- Создан технологический центр сертификации `INITIAL_CA` (`INITIAL_CA_GOST`) (значение задано в параметре `initial_ca_common_name` конфигурационного файла).

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
```

В случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

<sup>52</sup> Значение номера сборки записывается в таблицу «build\_info» схемы «aeca\_info».

<sup>53</sup> Маркеры доступа будут подписаны по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256 Бит.

## 6 ЗАПУСК И ОСТАНОВКА ПРОГРАММНОГО СРЕДСТВА

### 6.1 Запуск программного средства

Запуск Центра сертификации Aladdin eCA происходит:

- автоматически в случае выполнения успешной установки (см. подраздел 5.5);
- автоматически в случае выполнения успешного обновления (см. подраздел 12);
- автоматически после запуска ОС (при этом Центр сертификации Aladdin eCA должен был быть ранее установлен);
- после выполнения команды `sudo systemctl start aeca-ca.service`, если сервис `aeca-ca.service` был остановлен;
- после выполнения команды `sudo systemctl restart aeca-ca.service`.

При запуске программное средство выполняет ряд проверок.

- Проверяет возможность подключения к базе данных<sup>54</sup> имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`):
  - если не удастся осуществить подключение к СУБД, то Центр сертификации Aladdin eCA не будет запущен;
  - иначе Центр сертификации Aladdin eCA продолжает сценарий запуска.
- Проверяет соответствия номера своей сборки и значения номера сборки, указанной в базе данных<sup>54</sup>, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`):
  - если в базе данных отсутствует номер сборки, то Центр сертификации Aladdin eCA не будет запущен;
  - если в базе данных присутствует номер сборки и он не равен номеру сборки Центра сертификации Aladdin eCA, то Центр сертификации Aladdin eCA 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 запускаемого Центра сертификации Aladdin eCA;
  - если в базе данных присутствует номер сборки и он равен номеру сборки Центра сертификации Aladdin eCA, то Центр сертификации Aladdin eCA оставляет его без изменений и запускается.
- Выполняет проверку целостности контейнеров закрытого ключа всех центров сертификации, существующих в программном компоненте. Результат проверки целостности для каждого контейнера закрытого ключа записывается в журнал событий: событие с кодом CAENV076 – при успешной проверке целостности и событие CAENV077 – при неуспешной проверке целостности.

<sup>54</sup> Значение номера сборки указано в таблице «`build_info`» схемы «`aeca_info`».

## 6.2 Остановка программного средства

Остановка Центра сертификации Aladdin eCA выполняется с помощью команды: `sudo systemctl stop aeca-ca.service`.

Программное средство при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты, используемые для доступа к программному средству (определяются параметрами «`http_port`» и «`https_port`» конфигурационного файла `/opt/aecaCa/scripts/config.sh`), если данные порты не используются иными программами.

## 7 ПОДКЛЮЧЕНИЕ К ВЕБ-ИНТЕРФЕЙСУ

### 7.1 Общие сведения

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

Подключение к веб-интерфейсу Центра сертификации Aladdin eCA выполняется из веб-браузера удаленно по сети передачи данных с выделенного компьютера, на котором развернута среда функционирования.

Канал управления является защищенным – организован по протоколу HTTPS/TLS с двусторонней аутентификацией и шифрованием передаваемых данных. Идентификация и аутентификация пользователей выполняется по предъявленному сертификату, который должен быть предварительно установлен в хранилище веб-браузера или хранилище сертификатов используемой ОС. Пример установки сертификата администратора инициализации из контейнера закрытого ключа PKCS#12 (по умолчанию `INITIAL_ADMIN.p12`) приведен в подразделе 7.2.

Для соответствия Центра сертификатов доступа 4 уровню доверия, установленному документом «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утверждённым приказом ФСТЭК России от 2 июня 2020 г. № 76) при использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программного средства 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 администратора инициализации из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ при установке программного средства (по умолчанию `INITIAL_ADMIN_GOST.p12`), 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 подразделе 2.6.5 документа «СКЗИ «КриптоПро CSP». Инструкция по использованию графического приложения Инструменты КриптоПро (cptools)» ЖТЯИ.00101-03 92 06.
- Установлен веб-браузер Chromium с поддержкой TLS ГОСТ из состава используемой сертифицированной ОС. Данный веб-браузер входит в состав базовых репозиториях ОС Astra Linux SE, Альт Сервер и РЕД ОС.

## 7.2 Установка сертификата администратора инициализации

После установки Центра сертификации Aladdin eCA сформирован контейнер закрытого ключа PKCS12, содержащий сертификат администратора инициализации технологического центра сертификации. По умолчанию контейнер расположен в каталоге `/opt/aecaCa/dist/certificates/account/` (каталог определен параметром `certificates_account_path` конфигурационного файла). Пароль от контейнера с сертификатом определен в параметре `initial_client_password` конфигурационного файла (по умолчанию – «INITIAL»).

Установите сертификат администратора инициализации `INITIAL_ADMIN.p12` (имя контейнера по умолчанию) в доверенное хранилище сертификатов веб-браузера<sup>55</sup>.

Порядок установки сертификата администратора инициализации в хранилище веб-браузера Firefox:

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

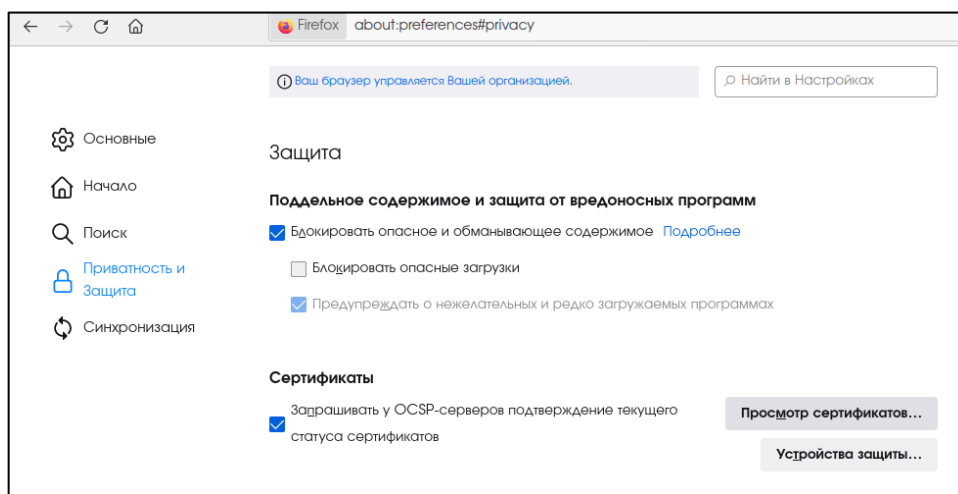


Рисунок 1 – Окно настроек браузера

- На вкладке «Ваши сертификаты» нажмите кнопку <Импортировать> (см. Рисунок 2).

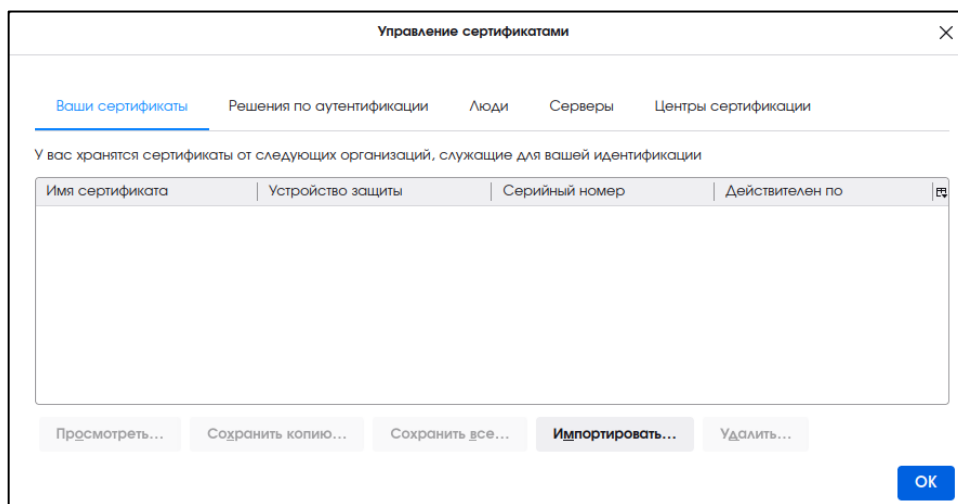


Рисунок 2 – Окно управления сертификатами

- Укажите путь к контейнеру с сертификатом администратора инициализации и нажмите кнопку <Открыть> (см. Рисунок 3).

<sup>55</sup> Сертификат администратора инициализации 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» (см. раздел 6.1).

**ВНИМАНИЕ!** Запрещается каким-либо образом удалять сертификат технологического центра сертификации «INITIAL\_CA», созданного при развёртывании Центра сертификации.

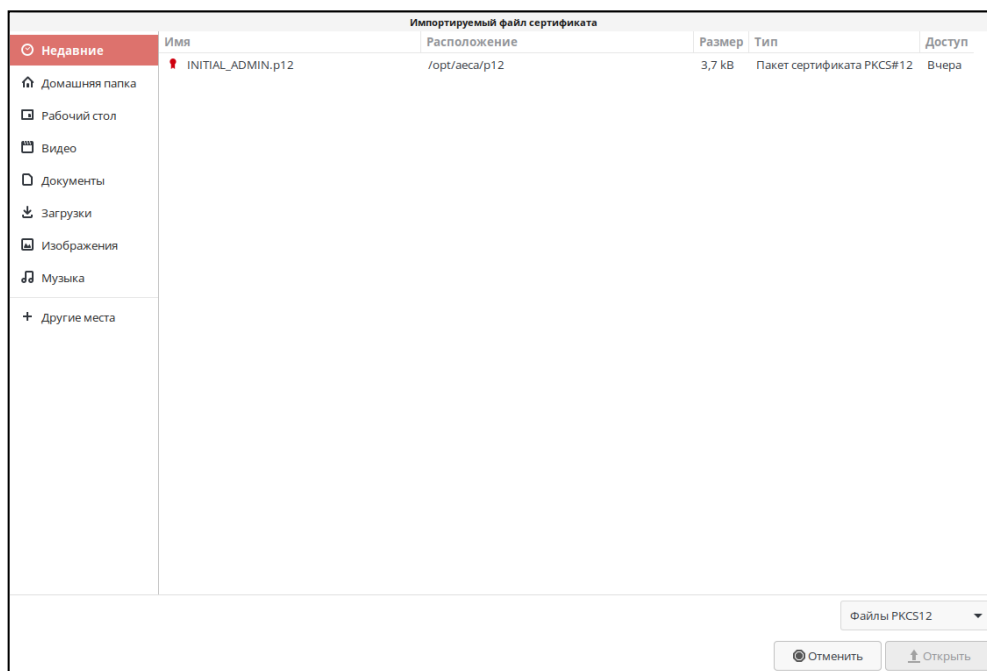


Рисунок 3 – Окно выбора импортируемого файла сертификата

- В открывшемся окне введите пароль от контейнера и нажмите кнопку <Ок> (см. Рисунок 4).

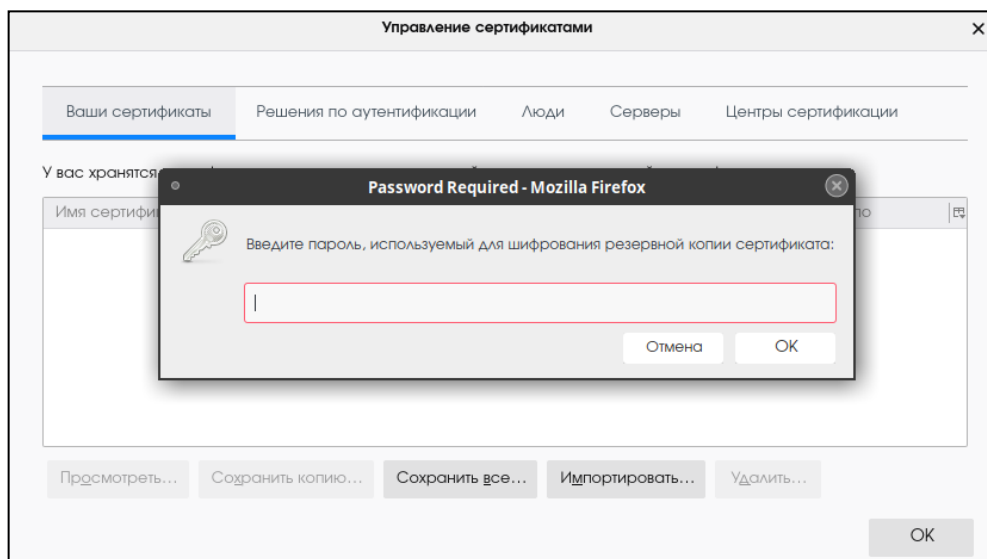


Рисунок 4 – Окно ввода пароля от контейнера

- В результате в окне «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 5). Завершите установку сертификата, нажав кнопку <ОК>.



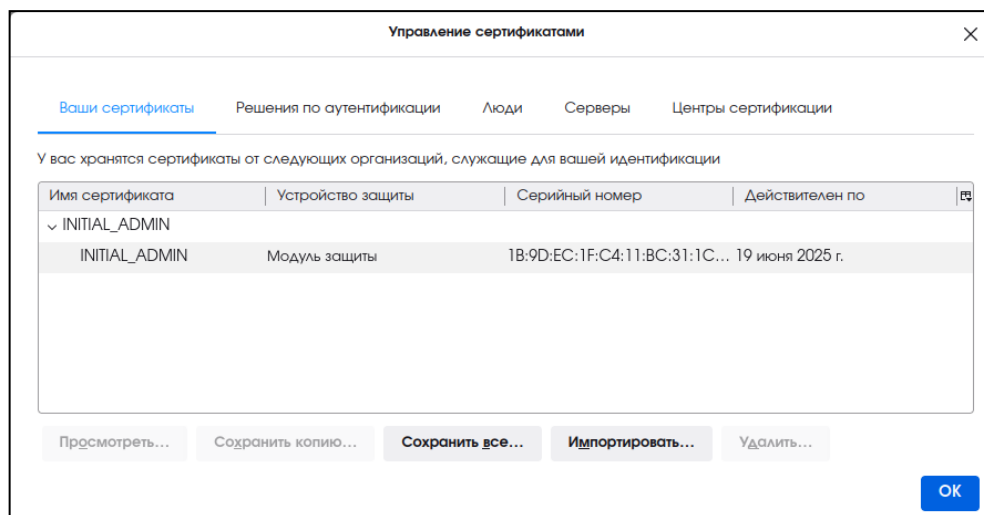


Рисунок 5 – Окно «Управление сертификатами»

### 7.3 Подключение к веб-интерфейсу

Порядок подключения к веб-интерфейсу:

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

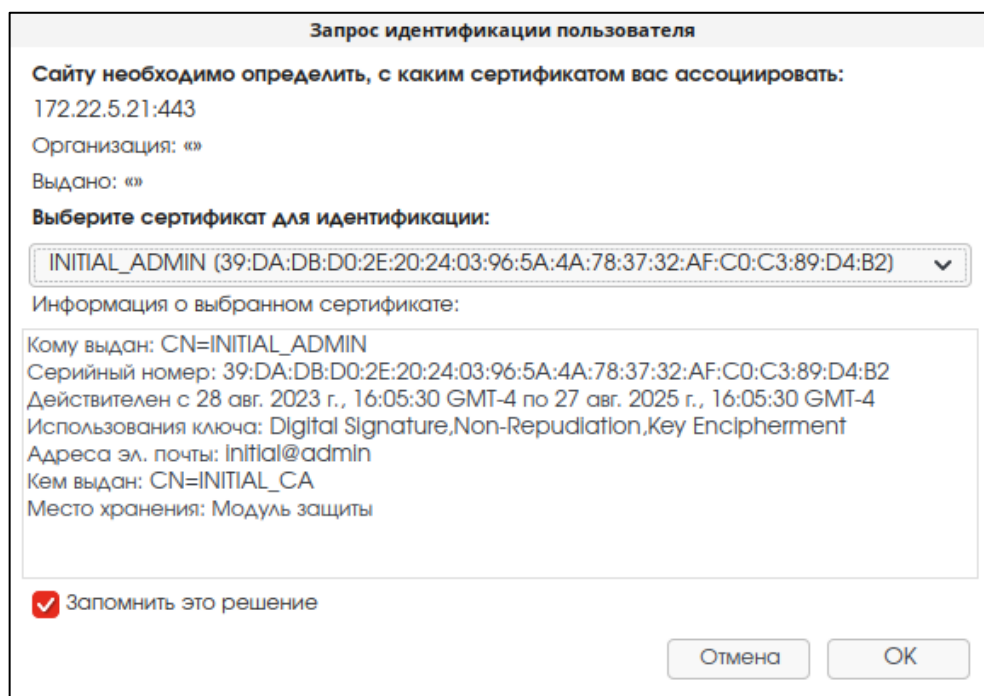


Рисунок 6 – Окно выбора сертификата

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

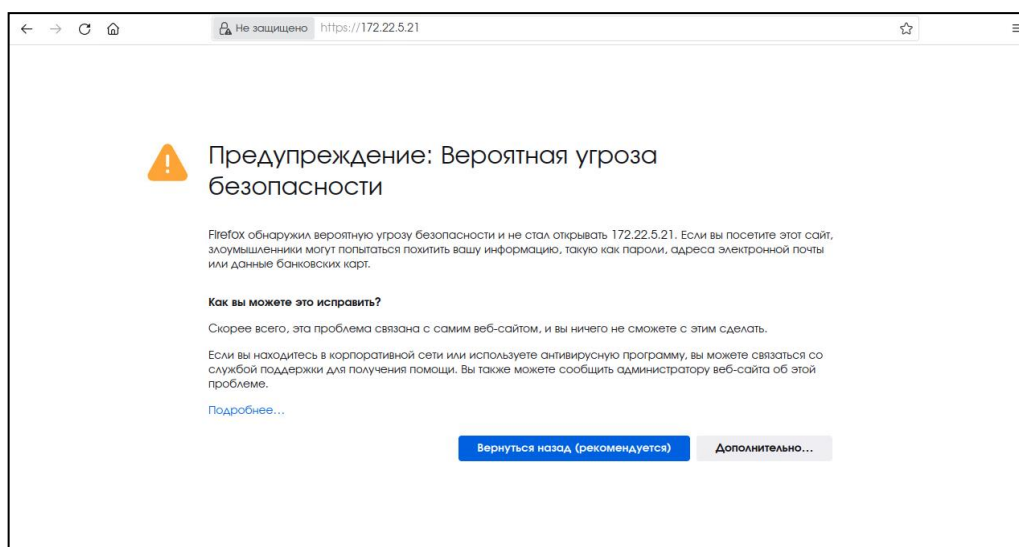


Рисунок 7 – Страница с предупреждением системы безопасности

- В результате вы подключитесь к веб-интерфейсу Центра сертификации Aladdin eCA, где запущен Мастер инициализации (первый шаг - установка лицензии) (см. часть 2 настоящего руководства администратора).

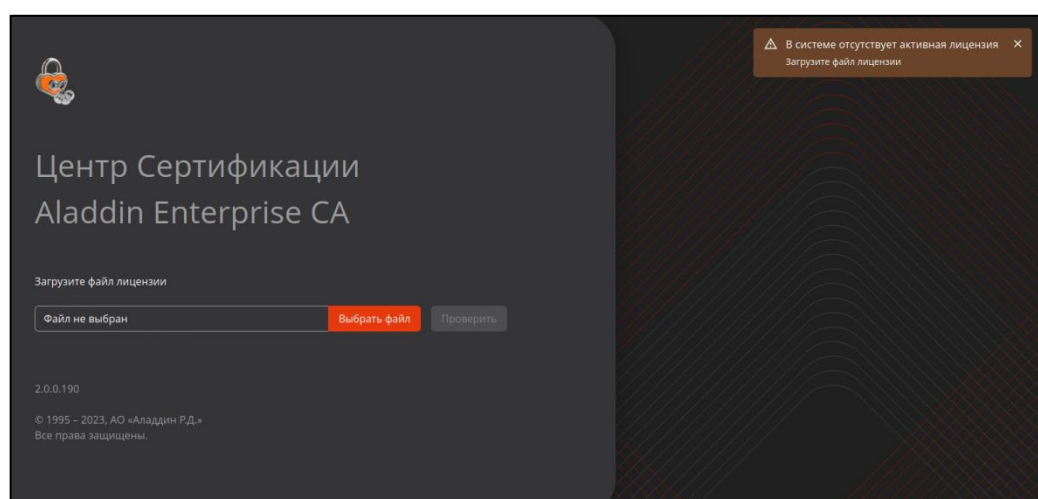


Рисунок 8 – Окно инициализации Центра сертификации. Шаг 1 – выбор лицензии

## 8 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПРОГРАММНОГО СРЕДСТВА

Контроль целостности исполняемых файлов Центра сертификации Aladdin eCA необходим для отслеживания неизменности и контроля состояния файлов, перечень которых приведён ниже:

- все файлы из каталога `/opt/aecaCa/samples` и его подкаталогов;
- все файлы из каталога `/opt/aecaCa/scripts` и его подкаталогов, кроме файлов `config.sh` и `jc_checksum`;
- все `.jar` файлы в каталоге `/opt/aecaCa/services` и его подкаталогах;
- все файлы в каталоге `/opt/aecaCa/static` и его подкаталогах;
- все файлы в каталоге `/opt/aecaCa/bin` и его подкаталогах;
- все файлы в каталоге `/opt/aecaCa/digsig` и его подкаталогах.

Контроль целостности осуществляется с помощью скрипта `integrity_check.sh`, находящегося в каталоге скриптов `/opt/aecaCa/scripts`. Скрипт `integrity_check.sh` осуществляет проверку целостности исполняемых файлов программного средства средствами утилиты «Утилита контроля целостности 2.0» - `jcverify`<sup>56</sup>.

Скрипт `integrity_check.sh` принимает в качестве опционального входного параметра путь к файлу с контрольными суммами, на основании которого должна выполняться проверка. В случае, если путь к файлу не указан, то по умолчанию будет использоваться файл `/opt/aecaCa/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/aecaCa/scripts/integrity_check.sh
```

В данном случае будет использован файл с эталонами контрольных сумм по умолчанию – `/opt/aecaCa/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 CAENV074 (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 CAENV075 (событие «Неуспешная проверка контрольных сумм»).

<sup>56</sup> Данная утилита включена в состав Центра сертификации (каталог `/opt/aecaCa/bin/jcverify`).

## 9 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ

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

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- о работе сервисов программы (файлы в формате .log);
- конфигурационный файл `/opt/aecaCa/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 10.

Таблица 8 – Данные системных логов

Системный лог	РЕД ОС	Astra Linux SE	Alt Сервер
<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/aecaCa/scripts/config.sh` архив диагностических данных дополнительно содержит:

- лог сборщика мусора;
- дампы памяти для упавших приложений Центра сертификации Aladdin eCA .

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

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

Для выполнения сбора диагностической информации запустите скрипт от имени суперпользователя:

```
sudo bash /opt/aecaCa/scripts/diagnostics.sh
```

Сформированный архив в формате .tar.gz с диагностической информацией будет сохранён в текущую рабочую директорию, из которой вы вызываете команды в терминале.

Для вывода текущей рабочей директории используйте команду: `pwd`

## 10 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ ПРОГРАММНОГО СРЕДСТВА

Создание резервных копий является неотъемлемой частью работы администратора Центра сертификации Aladdin eCA.

Перед выполнением каких-либо настроек, изменений и обновлений программного компонента 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/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aecaCa/dist/certificates/ssl`);
- закрытого и открытого ключей центра сертификации из каталога, путь к которому определён значением параметра «`cryptotoken_path`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aecaCa/dist/cryptotoken`);
- базы данных, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`);
- конфигурационного файла `/opt/aecaCa/scripts/config.sh`;

Резервное копирование осуществляется на локальный диск в папку, путь к которой определён значением параметра «`backup_path`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aecaCa/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 жесткого 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.

### 10.1 Создание резервной копии

Создание резервной копии программного средства осуществляется запуском скрипта с правами суперпользователя (root):

```
bash /opt/aecaCa/scripts/backup.sh
```

После запуска скрипта резервного копирования создаётся каталог `/opt/aecaCa/dist/backup`, где будет размещён архив, содержащий в имени дату и время создания полной резервной копии.

При успешном создании резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV086». В случае ошибки создания резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV087».

### 10.2 Расписание резервного копирования

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

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

```
sudo nano /etc/crontab
```

- Укажите время и период запуска сценариев создания резервных копий:

0	0	1	*	*	/opt/aecaCa/scripts/backup.sh
0	0	1	12	*	/opt/aecaCa/scripts/backup.sh

где:

- первая строка описывает запуск резервного копирования один раз в месяц,
- вторая строка описывает запуск резервного копирования один раз в год.

Примечание:

Выход и сохранение из редактора расписания осуществляется командой:

```
:wq!
```

Для просмотра настроенного расписания используется команда:

```
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**

### 10.3 Восстановление данных из резервной копии

Восстановление данных производится из папки, путь к которой определен значением параметра «backup\_path» конфигурационного файла /opt/aecaCa/scripts/config.sh (по умолчанию – /opt/aecaCa/dist/backup/), на сервере программного средства.

Если восстановление происходит на том же сервере, для которого ранее создана резервная копия, и путь к папке не изменен (значение по умолчанию), выполните команду:

```
sudo bash /opt/aecaCa/scripts/restore.sh `путь к папке сохранения резервной копии`/архив резервной копии.tar
```

где `путь к папке сохранения резервной копии` определен значением параметра «backup\_path» конфигурационного файла /opt/aecaCa/scripts/config.sh (по умолчанию – /opt/aecaca/dist/backup/).

- Если восстановление происходит после переустановки ОС, выполните:
  - подготовку к установке программного компонента в соответствии с разделом 4 настоящего документа;
  - установку программного компонента в соответствии с разделом 5 настоящего документа;
  - создание каталога хранения резервных копий, путь к которому определен значением параметра «backup\_path» конфигурационного файла /opt/aecaCa/scripts/config.sh (по умолчанию – /opt/aecaCa/dist/backup/), выполнив команду:

```
sudo mkdir -p /opt/aecaCa/dist/backup
```

- копирование в созданный каталог файла резервной копии;
- восстановление данных из резервной копии, выполнив команду:

```
sudo bash /opt/aecaCa/scripts/restore.sh /opt/aecaCa/dist/backup/архив резервной копии.tar
```

При успешном восстановлении из резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV088». В случае ошибки восстановления из резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV089».

## 11 ВОССТАНОВЛЕНИЕ ДОСТУПА К ЦЕНТРУ СЕРТИФИКАЦИИ

Восстановление доступа к Центру сертификации Aladdin eCA необходимо выполнить в случае отсутствия ранее созданной резервной копии и блокировки доступа к программному средству, возникшей в результате некорректного удаления технологических составляющих или истечения срока действия сертификата Центра сертификации или сертификата администратора.

Для выполнения восстановления доступа к Центра сертификации Aladdin eCA запустите скрипт от имени суперпользователя (с правами root или sudo):

```
sudo bash /opt/aecaCa/scripts/restore_access.sh
```

По результату выполнения скрипта восстановления доступа к программному средству:

- создан и выпущен:
  - технологический Центр сертификации «INITIAL\_CA» (по умолчанию статус «активирован»);
  - сертификат технологического Центра сертификации «INITIAL\_CA»;
- заменена:
  - учётная запись администратора «INITIAL\_ADMIN»;
- выпущены и заменены:
  - сертификат учётной записи администратора «INITIAL\_ADMIN»;
  - сертификат технологического веб-сервера.

Для дальнейшего доступа к Центру сертификации выполните аутентификацию по выпущенному сертификату учётной записи «INITIAL\_ADMIN» (см. раздел 7 настоящего документа).

## 12 ОБНОВЛЕНИЕ ПРОГРАММНОГО СРЕДСТВА

### 12.1 Назначение обновлений

Обновление базы данных и модулей Центра сертификации Aladdin eCA обеспечивает актуальность версии программного средства.

Выполняемые обновлениями задачи:

- исправление обнаруженных за время существования ПО недочетов и ошибок;
- устранение выявленных уязвимостей;
- изменение или улучшение работы существующих функций;
- добавление новых функций и возможностей.

### 12.2 Информирование потребителей о выпуске обновлений

• 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 новых версий компонентов Центра сертификатов доступа выполняется путем публикации информации на [официальном сайте Компании](#) и (или) с использованием рассылки электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счет применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлом обновлений может предоставляться обновленная документация для использования программы.

### 12.3 Получение обновлений потребителем

• Получение файлов обновлений 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) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм выполняется любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления.

### 12.4 Контроль целостности обновления ПО

Контроль целостности обновления программы выполняется путем расчета КС полученного установочного пакета (дистрибутива), с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0», и её сравнением со значением контрольной суммы для этого обновления (см. раздел 3 настоящего документа).

### 12.5 Процедура установки обновлений

**На случай, если во время обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию программы и базы данных (см. раздел 9 настоящего документа), из которой можно будет восстановить данные.**

Для обновления продукта:



- рекомендуется произвести очистку кэша используемого веб-браузера;
- перенесите дистрибутив с обновленной версией программного средства на сервер с установленным Центром сертификации Aladdin eCA;
- проверьте целостность дистрибутива путем подсчёта КС (см. подраздел 3.2 настоящего документа);
- выполните распаковку установочного пакета:

РЕД ОС

```
sudo dnf install aeca-*.rpm
```

Astra Linux SE

```
sudo dpkg -i aeca-*.deb
```

Альт Сервер

```
sudo apt-get install aeca-*.rpm
```

- запустите установку продукта в режиме обновления, выполнив команду<sup>57</sup>:

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

- установщик обнаружит установленную версию программного средства и предложит выбрать необходимое действие в интерактивном режиме:

- удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программного средства;
- выполнить обновление установленной версии до актуальной версии программного средства;
- прервать процесс установки;

- для выбора продолжения процесса обновления введите в терминале цифру «2»;

- при обновлении программного средства проверяет соответствия номера своей сборки и значения номера сборки, указанной в базе данных<sup>58</sup>, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`):

- если на момент обновления в базе данных отсутствует номер сборки, то Центр сертификации Aladdin eCA записывает в базе данных номер устанавливаемой сборки;
- если на момент обновления в базе данных присутствует номер сборки, и он меньше номера устанавливаемой сборки, то Центр сертификации Aladdin eCA перезаписывает номер сборки в базе данных, заменив его номером устанавливаемой сборки;
- если на момент обновления в базе данных присутствует номер сборки, и он равен номеру устанавливаемой сборки, Центр сертификации Aladdin eCA не изменяет его;
- если на момент обновления в базе данных присутствует номер сборки, и он больше номера устанавливаемой сборки, то Центр сертификации Aladdin eCA завершает обновление с ошибкой «Текущая версия схемы базы данных не позволяет выполнить установку или обновление службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где «X.X.X.X» – номер сборки, указанный в базе данных, а «Y.Y.Y.Y» – номер устанавливаемой сборки Центра сертификации Aladdin eCA. Номер сборки в базе данных при этом не меняется.

- после установки обновления запустите браузер, удалите файлы cookie и данные сайтов, очистите кэш-память браузера;

<sup>57</sup> Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std-jatoba4-client`). Установка и настройка СУБД описана в подразделах [3.2](#), [3.3](#) или 4.5.2 в зависимости ОС.

<sup>58</sup> Значение номера сборки указано в таблице «`build_info`» схемы «`aeca_info`».

- запустите обновленный Центр сертификации Aladdin eCA<sup>59</sup>;
- проверьте версию обновленного компонента в окне Центра сертификации «О программе».

После обновления программного средства с версии 2.1 до версии 2.2 пароль пользователя базы данных, заданный в конфигурационном файле `/opt/aecaCa/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/aecaCa/scripts/key` ключа шифрования.

## 12.6 Критерий успешности установки обновления

Критерием правильности установки обновления продукта является отображение информации о новой версии компонента изделия в окне «О программе».

---

<sup>59</sup> Описание проверок при запуске, выполняемых программным компонентом Aladdin eCA, см. в подразделе 6.1 настоящего руководства

## 13 УДАЛЕНИЕ ПРОГРАММНОГО СРЕДСТВА

### 13.1 Инициализация процесса удаления

Для инициализации процесса удаления необходимо выполнить команду с правами суперпользователя (root или sudo):

```
sudo bash /opt/aecaCa/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.

**Все внесённые изменения будут выведены в консоль.**

Процесс удаления производится вне зависимости от наличия соединения с базой данных, имя которой указано в значении параметра «database\_name» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`).

## 14 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

### 14.1 Удаление БД «аесаса»

Для удаления ранее созданной базы данных «аесаса» необходимо выполнить команды с правами суперпользователя (root или sudo):

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

```
sudo -u postgres psql
```

- Для предотвращения возможности новых подключений выполните команду:

```
UPDATE pg_database SET datallowconn = 'false' WHERE datname = 'aecaca';
```

- Для закрытия всех текущих сессий выполните команду:

```
SELECT pg_terminate_backend(pg_stat_activity.pid)
FROM pg_stat_activity
WHERE pg_stat_activity.datname = 'aecaca' AND pid <> pg_backend_pid();
```

- Удаляем базу данных, выполнив команду:

```
DROP DATABASE aecaca;
```

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

```
exit
```

### 14.2 Удаление пользователя БД «аеса»

Для удаления ранее созданного пользователя базы данных «аеса» необходимо выполнить команды с правами суперпользователя (root или sudo):

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

```
sudo -i -u postgres
```

- Удалите пользователя «аеса» 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
```

## 15 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения
Ошибка при запуске скрипта установки <code>install.sh</code> «error obtaining MAC configuration for user «aeca»»	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/macdb sudo setfacl -R -m u:postgres:r /etc/parsec/macdb sudo setfacl -m u:postgres:rx /etc/parsec/macdb</pre>
Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для программного компонента «Центр сертификации Aladdin eCA»	<p>На сервере была установлена и удалена более ранняя версия Программы</p> <p>Не хватка аппаратных ресурсов</p>	<p>Очистите конфигурацию nginx, выполнив команды:</p> <pre>sudo rm -rfv /etc/nginx/general-configs sudo rm -rfv /etc/nginx/conf.d/default.conf</pre> <p>Проверьте показатель загруженности оперативной памяти. Для корректной работы программы требуется не менее 6 Гб свободной оперативной памяти</p>
Ошибка при запуске скрипта установки <code>install.sh</code> «Минимальное количество оперативной памяти для развертывания системы составляет 8192 мегабайта!»	Значение параметра <code>memory</code> в файле конфигурации меньше 8192 или не задано	<p>В файле <code>/opt/aecaCa/scripts/config.sh</code> для параметра <code>memory</code> указать значение 8192:</p> <pre>memory='8192'</pre>
Ошибка при запуске скрипта установки <code>install.sh</code> «psql: FATAL: remaining connection slots are reserved for non-replication superuser connections»	Недостаточное число соединений к БД	В файле <code>postgresql.conf</code> необходимо установить в <code>max_connections</code> значение 1000 и более <sup>60</sup> .

<sup>60</sup> Параметр `max_connections` задается в инструкциях из разделов про установке и настройке СУБД: 4.3.3, 4.4.3 и 4.5.3.

## ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА «ПРИ УСТАНОВКЕ СУБД POSTGRES И POSTGRES PRO<sup>61</sup>

В случае, если другой продукт Postgres установлен, то для разрешения конфликта необходимо выполнить команды:

- Создайте начальную базу данных, запустив вспомогательный скрипт `pg-setup` с правами суперпользователя (root или sudo) и ключом `initdb`:

```
/opt/pgpro/std-16/bin/pg-setup initdb [--tune=конфигурация] [параметры_initdb]
```

где аргумент `tune` выбирает вариант конфигурации базы данных; параметры `_initdb` – обычные параметры `initdb`.

- Для настройки автозапуска сервера запустите скрипт `pg-setup` со следующими параметрами:

```
/opt/pgpro/std-16/bin/pg-setup service enable
```

- Запустите сервер с помощью `pg-setup`, выполнив команду с правами суперпользователя (root или sudo):

```
/opt/pgpro/std-16/bin/pg-setup service start
```

---

<sup>61</sup> Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>

## ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

Для подключения программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» к внешней СУБД необходимо:

- выполнить настройку на хосте СУБД в соответствии с разделом 2.1, представленным ниже;
- выполнить настройку на хосте Aladdin еСА в соответствии с разделом 2.2, представленным ниже.

### 2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД (установка СУБД описана в подразделах 4.3.4 для РЕД ОС, 4.4.4 для Astra Linux, 4.5.4 для Альт Сервер настоящего руководства) в зависимости от используемой на нем ОС необходимо выполнить следующие настройки:

- Если в качестве ОС на хосте СУБД используется Astra Linux Special Edition 1.7, 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 определенного 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, а `port` – порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432).

- Если в качестве ОС на хосте с СУБД используется РЕД ОС или ОС Альт 8 СП, необходимо отредактировать файл `/var/lib/pgsql/15/data/pg_hba.conf` (или `var/lib/jatoba/4/data/pg_hba.conf`, если используется СУБД Jatoba)<sup>62</sup>, приведя его к следующему виду:

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		all		trust
# IPv4 local connections:					
host	all		all	0.0.0.0/0	password
# IPv6 local connections:					
host	all		all	:::1/128	password
# Allow replication connections from localhost, by a user with the					
# replication privilege.					
local	replication		all		peer
host	replication		all	127.0.0.1/32	ident
host	replication		all	:::1/128	ident

<sup>62</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

Кроме того, необходимо отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)<sup>63</sup>, указав для параметра `listen_addresses` значение `*`:

```
listen_addresses = '*'
```

Значение `*` позволит подключаться к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к СУБД, предоставив его только для определенного IP-адреса, необходимо указать данный IP-адрес в параметре `listen_addresses`, например:

```
listen_addresses = '192.168.111.100'
```

- Затем на хосте СУБД необходимо перезапустить используемую СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).
- Затем на хосте СУБД необходимо выполнить создание и настройку базы данных. Действия по созданию и настройке базы данных описаны в подразделах 4.3.4 (для РЕД ОС), 4.4.4 (для Astra Linux), 4.5.4 (для Альт Сервер) . В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

## 2.2 Настройка на хосте Aladdin eCA

**На хосте Aladdin eCA предварительно должна быть выполнена установка СУБД (установка СУБД описана в разделах подразделах 4.3.4 для РЕД ОС, 4.4.4 для Astra Linux, 4.5.4 для Альт Сервер настоящего руководства.**

**При этом не нужно настраивать СУБД, установленную на хосте Aladdin eCA.**

На хосте Aladdin eCA необходимо отредактировать конфигурационный файл `/opt/aecaCa/scripts/config.sh`, указав в нем значения следующих параметров:

Параметр	Значение по умолчанию	Описание
<code>use_tls</code>	<code>false</code>	Флаг обязательного использования TLS для подключения к СУБД <sup>64</sup> . Допустимые значения: <code>true</code> , <code>false</code>
<code>database_username</code>	<code>'aeca'</code>	Имя пользователя базы данных, используемое для работы Центра сертификации Aladdin eCA. 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 сертификации Aladdin eCA. 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>'aecasca'</code>	Имя базы данных, используемой Центром сертификации Aladdin eCA. Необходимо внести значение, указанное при создании и

<sup>63</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

<sup>64</sup> Подробная информация о параметре `use_tls` приведена в «Приложение 3. Настройка TLS-соединения с СУБД»



Параметр	Значение по умолчанию	Описание
		настройке базы данных на хосте СУБД
root_cert_path	#CHANGEIT	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД <sup>65</sup>

- Затем на хосте Aladdin eCA необходимо применить изменения конфигурационного файла путем запуска команды `sudo bash /opt/aecaCa/scripts/install.sh` и дальнейшего выбора действия «[Update]». В случае, Aladdin eCA не был установлен ранее, выбор действия не потребуется, и будет выполнена установка с указанными в конфигурационном файле параметрами.

---

<sup>65</sup> Подробная информация о параметре `root_cert_path` приведена в «Приложение 3. Настройка TLS-соединения с СУБД»

## ПРИЛОЖЕНИЕ 3. НАСТРОЙКА TLS-СОЕДИНЕНИЯ С СУБД

Для настройки TLS-соединения программного компонента «Центр сертификации Aladdin Enterprise Certification Authority» с СУБД необходимо в предварительно развернутом и инициализированном программном компоненте «Центр сертификации Aladdin Enterprise Certification Authority» создать сертификат с закрытым ключом (PKCS#12) для сервера СУБД. При этом в сертификате сервера СУБД в атрибуте Common Name или в атрибуте Subject Alternative Name типа dNSName обязательно должно быть указано доменное сервера СУБД (или IP-адрес)<sup>66</sup>, так как программный компонент Aladdin eCA 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 программном компоненте Aladdin eCA, указав ему необходимые атрибуты CN и DNS Name).

Во избежание ошибок в работе программного компонента Aladdin eCA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу программного компонента Aladdin eCA путем выполнения команды `sudo systemctl stop aeca-ca.service`.

Для настройки TLS-соединения программного компонента Aladdin eCA с СУБД необходимо:

- выполнить настройку СУБД в соответствии с разделом 3.1, представленным ниже;
- выполнить настройку программного компонента Aladdin eCA в соответствии с разделом 3.2, представленным ниже.

### 3.1 Настройка 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)<sup>67</sup>, указав:

- в параметре «ssl» значение «on»;
- в параметре «ssl\_cert\_file» абсолютный путь к файлу сертификата сервера СУБД<sup>68</sup>;
- в параметре «ssl\_key\_file» абсолютный путь к файлу закрытого ключа сервера СУБД<sup>69</sup>;
- в параметре «ssl\_ca\_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД<sup>70</sup>.

<sup>66</sup> Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database\_host» конфигурационного файла программного компонента Aladdin eCA.

<sup>67</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

<sup>68</sup> Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса программного компонента Aladdin eCA. Например, в карточке локального субъекта сервера СУБД.

<sup>69</sup> Файл закрытого ключа сервера СУБД может быть получен из контейнера закрытого ключа сервера СУБД путем выполнения команды `openssl pkcs12 -in container.p12 -out key.key -nocerts -nodes`, где `container.p12` - путь к контейнеру закрытого ключа сервера СУБД, а «key.key» - путь к файлу для сохранения закрытого ключа.

<sup>70</sup> 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 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 программного компонента Aladdin eCA

1) На хосте Aladdin eCA отредактировать конфигурационный файл `/opt/aecaCa/scripts/config.sh`, указав в нем в параметре конфигурации БД `use_tls` значение `true`, а в параметре `root_cert_path` абсолютный путь к файлу сертификата корневого издателя из цепочки сертификатов сервера СУБД<sup>71</sup>.

При этом указанный выше файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен иметь метку доступа «600», установить которую можно с помощью команды `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 ОС РЕД ОС на хосте Aladdin eCA файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен располагаться в каталоге `/opt/aecaCa` (или в его подкаталогах). Кроме того, в случае использования ОС РЕД ОС на хосте Aladdin eCA необходимо дополнительно выполнить команду `restorecon -Rv "путь к файлу сертификата корневого издателя из цепочки сертификатов сервера СУБД"`.

2) На хосте Aladdin eCA применить изменения конфигурационного файла путем запуска команды `sudo bash /opt/aecaCa/scripts/install.sh` и дальнейшего выбора действия «[Update]».

По завершению выполнения указанной команды дальнейший обмен данными программного компонента Aladdin eCA с СУБД будет осуществляться только по протоколу TLS. Если в СУБД, к которой выполняется подключение, отключен TLS, то программный компонент Aladdin eCA не будет выполнять обмен данными с такой СУБД. При этом программный компонент Aladdin eCA сможет установить соединение с СУБД только в случае, если ее сертификат издан издателем, путь к сертификату которого указан в конфигурационном файле программного компонента Aladdin eCA и только в случае, если имя хоста сервера СУБД соответствует указанному в сертификате.

<sup>71</sup> Если сертификат сервера СУБД выпущен подчиненным ЦС, необходимо указать путь до сертификата корневого ЦС.

## ПРИЛОЖЕНИЕ 4. РАЗВЕРТЫВАНИЕ КЛАСТЕРА ALADDIN eCA

Программное обеспечение «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» обеспечивает возможность кластеризации с использованием внешнего средства балансирования нагрузки.

Доступны следующие варианты развертывания кластера Aladdin eCA:

- развертывание кластера в виртуальной инфраструктуре, порядок которого представлен в разделе 4.1 ниже;
- развертывание кластера с помощью переноса контейнеров закрытого ключа основного узла, порядок которого представлен в разделе 4.2 ниже.

### 4.1 Развертывание кластера Aladdin eCA в виртуальной инфраструктуре

Кластер конфигурируется по схеме «Active-Passive Failover», куда входят следующие узлы:

- виртуальная машина с установленным и инициализированным программным обеспечением «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (BM1) – основной узел кластера;
- клон виртуальной машины BM1, созданный сразу после завершения инициализации на BM1 программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (BM2) – резервный узел кластера<sup>72</sup>;
- виртуальная машина с установленной и настроенной СУБД (BM3);
- виртуальная машина с установленным и настроенным средством балансирования нагрузки HAProxy (BM4).

На всех указанных выше виртуальных машинах допускается использование только следующих 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 «Орел»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Орел»;
- РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;
- РЕД ОС версия 8, конфигурация «Сервер»;
- ОС Альт 8 СП, релиз 10, вариант исполнения Сервер.

Допускается использование единой виртуальной машины для реализации BM3 и BM4.

1) На BM3 выполнить установку одной из нижеприведённых систем управления базами данных<sup>73</sup>:

- PostgreSQL из состава ОС;
- Jatoba 4.

2) На BM3 увеличить максимальное количество подключений к СУБД, отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)<sup>74</sup>, указав для параметра `max_connections` значение 2000<sup>75</sup>:

<sup>72</sup> BM2 создается в ходе развертывания кластера Aladdin eCA в виртуальной инфраструктуре путем клонирования BM1 на шаге 8

<sup>73</sup> Справочная информация по установке и настройке СУБД приведена в разделах **✕** для РЕД ОС, **✕** для Astra Linux и 4.5.2 для Альт Сервер настоящего руководства

```
max_connections = 2000
```

- 3) На ВМ3 перезапустить используемую СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).
  - 4) На ВМ1 выполнить установку программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» в соответствии с разделом 5 настоящего руководства, при этом подключив к Aladdin еСА внешнюю СУБД, установленную на ВМ3, в соответствии с «Приложение 2. Настройка подключения к внешней СУБД» настоящего руководства.
  - 5) На ВМ1 выполнить первичную настройку программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» в соответствии разделом 6 настоящего документа.
  - 6) На ВМ1 выполнить первичное лицензирование в соответствии с разделом 2.1 эксплуатационного документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01-2.
  - 7) На ВМ1 выполнить создание центра сертификации в соответствии с разделом 3.1 эксплуатационного документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01-2.
  - 8) Средствами используемого гипервизора клонировать ВМ1 (клон ВМ1 далее по тексту обозначены «ВМ2»).
  - 9) Запустить ВМ2 и ожидать завершения запуска `aeca-ca.service` на ВМ2.
- В случае создания на ВМ1 Центра сертификации, закрытый ключ которого хранится на КриптоПро HSM, необходимо после запуска ВМ2 восстановить ее подключение к КриптоПро HSM и перезапустить `aeca-ca.service`.**
- 10) На ВМ4 выполнить установку средства балансирования нагрузки HAProxy:

РЕД ОС <sup>76</sup>	<code>sudo dnf install haproxy</code>
Astra Linux SE	<code>sudo apt install haproxy</code>
Альт Сервер	<code>sudo apt-get install haproxy</code>

<sup>74</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

<sup>75</sup> Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», взаимодействующего с СУБД

<sup>76</sup> При установке HAProxy на РЕД ОС необходимо выполнить отключение SELinux в соответствии с официальной документацией ОС:

- для РЕО ОС 7.3 см. [https://redos.red-soft.ru/base/redos-7\\_3/7\\_3-network/7\\_3-sett-proxy/7\\_3-haproxy/](https://redos.red-soft.ru/base/redos-7_3/7_3-network/7_3-sett-proxy/7_3-haproxy/);
- для РЕО ОС 8 см. [https://redos.red-soft.ru/base/redos-8\\_0/8\\_0-network/8\\_0-sett-proxy/8\\_0-haproxy/](https://redos.red-soft.ru/base/redos-8_0/8_0-network/8_0-sett-proxy/8_0-haproxy/).

11) На ВМ4 отредактировать файл `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
    timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main IP_VM1:443 check
    server clone IP_VM2:443 check backup

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где вместо `IP_VM1` необходимо указать IP-адрес ВМ1, вместо `IP_VM2` – IP-адрес ВМ2, а вместо `admin:password` указать логин и пароль, разделенные двоеточием, которые будут использоваться для доступа к панели мониторинга HAProxy.

12) На ВМ4 перезапустить HAProxy путем запуска команды `sudo systemctl restart haproxy.service`

В результате приведенной настройки кластера все запросы, направляемые к Aladdin eCA через средство балансирования нагрузки HAProxy, будут перенаправляться на основной узел кластера (BM1). В случае недоступности основного узла кластера все запросы, направляемые к Aladdin eCA через средство балансирования нагрузки HAProxy, будут перенаправляться на резервный узел кластера (BM2). Для мониторинга состояния узлов кластера может быть использована панель мониторинга, доступная по адресу `http://IP_VM4:8404/stats`, где `IP_VM4` – IP-адрес BM4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на BM4).

**В случае дальнейшего создания Центров сертификации в развернутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище КриптоПро HDIMAGE на BM1 и BM2. Например, если активным узлом кластера в момент создания Центра сертификации являлся BM2, необходимо скопировать созданные закрытые ключи Центров сертификации с BM2 на BM1, затем перезапустить `aeca-ca.service` на BM1.**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «Локально», хранятся в каталоге `/opt/aecaCa/dist/cryptotoken`. При копировании файлов необходимо назначать владельцем данных файлов на конечной ВМ пользователя «aeca».**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге `/var/opt/cproscsp/keys/aeca`. Имена файлов контейнеров закрытых ключей в данном каталоге соответствуют первым 8 символам идентификатора Центра сертификации. При копировании файлов необходимо назначать владельцем данных файлов на конечной ВМ пользователя «aeca», затем перезапускать на данной ВМ КриптоПро CSP.**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «КриптоПро HSM», не требуют копирования. Для поддержки работы с такими ключами необходимо сохранять подключение всех узлов кластера к одному КриптоПро HSM.**

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла необходимо выполнить действия, аналогичные действиям по подключению узла BM2:

- 1) Средствами используемого гипервизора клонировать BM1 (клон далее по тексту «BMP»).
- 2) Запустить BMP и дождаться запуска `aeca-ca.service` на ней.

3) На BM4 отредактировать файл `/etc/haproxy/haproxy.cfg` – внести в него IP-адрес BMP в секцию `backend bk_app` под строкой, соответствующей последнему резервному узлу. Если последний резервный узел – это BM2, то это под строкой: `server clone IP_VM2:443 check backup`). Таким образом должна получиться секция вида:

```
backend bk_app
    mode tcp
    server main IP_VM1:443 check
    server clone IP_VM2:443 check backup
    server clone IP_VMR:443 check backup
```

где `IP_VMR` – это IP-адрес BMP.

4) На BM4 перезапустить HAProxy путем запуска команды `sudo systemctl restart haproxy.service`.

В результате в кластере появится дополнительный резервный узел. Все описанные выше рекомендации и уточнения по работе с узлом BM2, также относятся и к узлу BMP.

## 4.2 Развертывание кластера Aladdin eCA с помощью переноса контейнеров закрытого ключа основного узла

Кластер конфигурируется по схеме «Active-Passive Failover», куда входят следующие узлы:

- сервер с установленным и инициализированным программным обеспечением «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (APM1) – основной узел кластера;
- сервер с установленным и инициализированным программным обеспечением «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», для которого будет выполнен перенос контейнеров закрытого ключа (APM2) – резервный узел кластера;
- сервер с установленной и настроенной СУБД (APM3);
- сервер с установленным и настроенным средством балансирования нагрузки HAProxy (APM4).

На всех указанных выше серверах допускается использование только следующих 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 «Орел»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж»;
- Astra Linux Special Edition версия 1.8, уровень защищённости «Орел»;
- РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;
- РЕД ОС версия 8, конфигурация «Сервер»;
- ОС Альт 8 СП, релиз 10, вариант исполнения Сервер.

Допускается использование одного сервера для реализации APM3 и APM4.

1) На APM3 выполнить установку одной из нижеприведённых систем управления базами данных<sup>77</sup>:

- PostgreSQL из состава ОС;
- Jatoba 4.

2) На APM3 увеличить максимальное количество подключений к СУБД, отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)<sup>78</sup>, указав для параметра `max_connections` значение 2000<sup>79</sup>:

```
max_connections = 2000
```

3) На APM3 перезапустить используемую СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

4) На APM1 выполнить установку программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» в соответствии с разделом 5

<sup>77</sup> Справочная информация по установке и настройке СУБД приведена в разделах ☒ для РЕД ОС, ☒ для Astra Linux и 4.5.2 для Альт Сервер настоящего руководства

<sup>78</sup> Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

<sup>79</sup> Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», взаимодействующего с СУБД



настоящего руководства, при этом подключив к Aladdin eCA внешнюю СУБД, установленную на АРМ3, в соответствии с «Приложение 2. Настройка подключения к внешней СУБД» настоящего руководства.

5) На АРМ1 выполнить первичную настройку программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» в соответствии разделом 6 настоящего документа.

6) На АРМ1 выполнить первичное лицензирование в соответствии с разделом 2.1 эксплуатационного документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01-2.

7) На АРМ1 выполнить создание центра сертификации в соответствии с разделом 3.1 эксплуатационного документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01-2.

8) На АРМ2 выполнить установку программного обеспечения «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» в соответствии с разделом 5 настоящего руководства, при этом подключив<sup>80</sup> к Aladdin eCA внешнюю СУБД, установленную на АРМ3, в соответствии с «Приложение 2. Настройка подключения к внешней СУБД» настоящего руководства.

**В случае, если на АРМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является КриптоПро CSP, на АРМ2 необходимо выполнить аналогичную АРМ1 установку КриптоПро CSP и подключение внешней гаммы.**

**В случае, если на АРМ1 был создан Центр сертификации, местом хранения закрытого ключа которого является КриптоПро HSM, необходимо выполнить на АРМ2 подключение КриптоПро CSP к тому же ПАКМ КриптоПро HSM.**

9) Если на АРМ1 был создан Центр сертификации, для которого было выбрано место хранения закрытого ключа «Локально», необходимо с АРМ1 скопировать содержимое каталога `/opt/aecaCa/dist/cryptotoken` и заменить им содержимое каталога `/opt/aecaCa/dist/cryptotoken` на АРМ2.

Если на АРМ1 был создан Центр сертификации, для которого было выбрано место хранения закрытого ключа «Жесткий диск (HDIMAGE)», необходимо с АРМ1 скопировать контейнер Центра сертификации (имя файла будет соответствовать первым 8 символам идентификатора Центра сертификации) из каталога `/var/opt/cproscsp/keys/aeca` и вставить его в каталог `/var/opt/cproscsp/keys/aeca` на АРМ2. При этом необходимо назначить владельцем данного файла на АРМ2 пользователя «аеса» и перезапустить на АРМ2 КриптоПро CSP.

10) На АРМ1 скопировать содержимое каталога `/opt/aecaCa/dist/certificates` и заменить им содержимое каталога `/opt/aecaCa/dist/certificates` на АРМ2.

<sup>80</sup> В конфигурационном файле Aladdin eCA на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным на шаге 5

11) В случае, если в качестве ОС на АРМ2 используется «РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер» или «РЕД ОС версия 8, конфигурация «Сервер», необходимо выполнить следующие команды в терминале на АРМ2:

```
sudo restorecon -Rv /opt/aecaCa/dist/cryptotoken
sudo restorecon -Rv /opt/aecaCa/dist/certificates
```

12) Произвести на АРМ2 перезапуск сервиса для обеспечения работы ЦС с перенесенными контейнерами. Перезапуск производится посредством команды

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

13) На АРМ4 выполнить установку средства балансирования нагрузки HAProxy:

РЕД ОС<sup>81</sup>

```
sudo dnf install haproxy
```

Astra Linux SE

```
sudo apt install haproxy
```

Альт Сервер

```
sudo apt-get install haproxy
```

14) На АРМ4 отредактировать файл `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon

defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client 50000
```

<sup>81</sup> При установке HAProxy на РЕД ОС необходимо выполнить отключение SELinux в соответствии с официальной документацией ОС:

- для РЕД ОС 7.3 см. [https://redos.red-soft.ru/base/redos-7\\_3/7\\_3-network/7\\_3-sett-proxy/7\\_3-haproxy/](https://redos.red-soft.ru/base/redos-7_3/7_3-network/7_3-sett-proxy/7_3-haproxy/);
- для РЕД ОС 8 см. [https://redos.red-soft.ru/base/redos-8\\_0/8\\_0-network/8\\_0-sett-proxy/8\\_0-haproxy/](https://redos.red-soft.ru/base/redos-8_0/8_0-network/8_0-sett-proxy/8_0-haproxy/).

```

timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main IP_ARM1:443 check
    server clone IP_ARM2:443 check backup

listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
    
```

где вместо `IP_ARM1` необходимо указать IP-адрес АРМ1, вместо `IP_ARM2` – IP-адрес АРМ2, а вместо `admin:password` указать логин и пароль, разделенные двоеточием, которые будут использоваться для доступа к панели мониторинга HAProxy.

15) На АРМ4 перезапустить HAProxy путем запуска команды `sudo systemctl restart haproxy.service`

В результате приведенной настройки кластера все запросы, направляемые к Aladdin eCA через средство балансирования нагрузки HAProxy, будут перенаправляться на основной узел кластера (АРМ1). В случае недоступности основного узла кластера все запросы, направляемые к Aladdin eCA через средство балансирования нагрузки HAProxy, будут перенаправляться на резервный узел кластера (АРМ2). 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).

**В случае дальнейшего создания Центров сертификации в развернутом кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище КриптоПро HDIMAGE на АРМ1 и АРМ2. Например, если активным узлом кластера в момент создания Центра сертификации являлся АРМ2, необходимо скопировать созданные закрытые ключи Центров сертификации с АРМ2 на АРМ1, затем перезапустить `aeca-ca.service` на АРМ1.**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «Локально», хранятся в каталоге `/opt/aecaCa/dist/cryptotoken`. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «aeca».**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге `/var/opt/cprosp/keys/aeca`. Имена файлов контейнеров закрытых ключей в данном каталоге соответствуют первым 8 символам идентификатора Центра сертификации. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «aeca», затем перезапускать на данном АРМ КриптоПро CSP.**

**Закрытые ключи центров сертификации, для которых при создании Центра сертификации было выбрано место хранения «КриптоПро HSM», не требуют копирования. Для поддержки работы с такими ключами необходимо сохранять подключение всех узлов кластера к одному КриптоПро HSM.**

В кластер можно подключать дополнительные резервные узлы. Для подключения нового резервного узла (APMP) необходимо выполнить действия, аналогичные действиям по подключения узла APM2:

1) Выполнить для APMP действия, производимые для APM2 в пунктах 8, 9, 10, 11, 12 выше данного раздела (при их выполнении вместо APM2 использовать APMP).

2) На APM4 отредактировать файл `/etc/haproxy/haproxy.cfg` – внести в него IP-адрес APMP в секцию `backend bk_app` под строкой, соответствующей последнему резервному узлу. Если последний резервный узел – это APM2, то это под строкой: `server clone IP_ARM2:443 check backup`). Таким образом должна получиться секция вида:

```
backend bk_app
    mode tcp
    server main IP_ARM1:443 check
    server clone IP_ARM2:443 check backup
    server clone IP_ARMR:443 check backup
```

где `IP_ARMR` – это IP-адрес APMP.

3) На APM4 перезапустить HAProxy путем запуска команды: `sudo systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел. Все описанные выше рекомендации и уточнения по работе с узлом APM2, также относятся и к узлу APMP.

### 4.3 Обновление программных компонент Aladdin eCA узлов кластера Aladdin eCA

Обновление кластера Aladdin eCA включает в себя предварительную приемку программного компонента Aladdin eCA, который будет устанавливаться на узлы кластера, остановку работающих программных компонент Aladdin eCA на узлах кластера и выполнение последовательного обновления программных компонент Aladdin eCA на каждом узле кластера.

Обновление производится для кластера Aladdin eCA, сконфигурированного по схемам, описанных в подразделах 4.1 и 4.2 настоящего Приложения.

В кластер Aladdin eCA входят следующие узлы:

- сервер с установленным и инициализированным программным обеспечением «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (APM1) – основной узел кластера;
- сервера с установленным и инициализированным программным обеспечением «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (APM2-узлы) – резервные узлы кластера:
  - это либо клоны сервера APM1, созданные сразу после завершения инициализации на APM1 (подраздел 4.1 настоящего Приложения);
  - либо сервера, для которого выполнен перенос контейнеров закрытого ключа с APM1 (подраздел 4.2 настоящего приложения).
- сервер с установленной и настроенной СУБД (APM3);

- сервер с установленным и настроенным средством балансирования нагрузки HAProxy (APM4).

Обновления программных компонент Aladdin eCA узлов кластера Aladdin eCA включает в себя:

- обновление программного компонента Aladdin eCA на основном узле кластера (APM1);
- обновление программного компонента Aladdin eCA на резервных узлах кластера (APM2-узлах).

**Номер сборки устанавливаемых программных компонент Aladdin eCA должен быть одинаковым для основного и резервных узлов кластера.**

**Иначе программные компоненты Aladdin eCA на узлах кластера не могут быть запущены<sup>82</sup>.**

Процесс обновления кластера Aladdin eCA:

- 1) Предварительно произвести действия по приёме программного компонента Aladdin eCA в соответствии с разделом 3 настоящего руководства;
- 2) На APM1-узле произвести резервное копирование данных программного компонента Aladdin eCA в соответствии с разделом 10 настоящего документа для возможности восстановить данные в случае неисправности;
- 3) На APM2-узлах произвести резервное копирование данных программного компонента Aladdin eCA в соответствии с разделом 10 настоящего документа для возможности восстановить данные в случае неисправности;
- 4) На APM2-узлах произвести остановку программного компонента Aladdin eCA путем выполнения команды `sudo systemctl stop aeca-ca.service`;

**Это действие необходимо для избежания ошибок и вызвано тем, что программный компонент Aladdin eCA на основном узле (APM1) и программные компоненты Aladdin eCA на резервных узлах (APM2-узлах) работают с одной схемой базы данных (APM3). И при обновлении программного компонента Aladdin eCA на одном узле происходит обновление схемы базы данных до новой версии, с которой программные компоненты Aladdin eCA на других узлах могут работать некорректно.**

- 5) На APM1 произвести обновление программного компонента Aladdin eCA в соответствии с разделом 12 настоящего руководства;
- 6) На каждом APM2-узле произвести обновление программного компонента Aladdin eCA в соответствии с разделом 12 настоящего руководства.

Критерием правильности установки обновления кластера является отображение информации о новой версии компонента изделия в окне «О программе» и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга, доступной 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).

<sup>82</sup> Описание проверок при запуске, осуществляемых программным компонентом Aladdin eCA, см в разделе 6.

## ПРИЛОЖЕНИЕ 5. НАСТРОЙКА ВЗАИМОДЕЙСТВИЯ С КРИПТОПРОВАЙДЕРОМ СКЗИ «КРИПТОПРО CSP»

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA Центр сертификации Alladin eCA может взаимодействовать со средством криптографической защиты информации (СКЗИ) - криптопровайдером СКЗИ «КриптоПро CSP» из состава программного средства с целью реализации следующих возможностей:

- создание ключевой пары (открытый и закрытый ключи) Центра сертификации (корневого или подчиненного);
- подписание сертификата Центра сертификации (самоподписанный сертификат);
- создание контейнеров закрытого ключа Центра сертификации с возможностью указания места хранения;
- подписание запроса на сертификат Центра сертификации в вышестоящем центре сертификации;
- создание ключевой пары (открытый и закрытый ключи) для субъектов (пользователей или технических средств);
- подписание сертификатов доступа для субъектов (пользователей или технических средств – владельцев сертификатов доступа);
- создание контейнеров закрытого ключа субъектов (пользователей или технических средств);
- подписание списка отозванных сертификатов.

Взаимодействие Центра сертификации с криптопровайдером СКЗИ «КриптоПро CSP» из состава программного средства осуществляется через модуль «КриптоПро Java CSP»<sup>83</sup>. При каждом запуске Центр сертификации автоматически определяется наличие на его хосте активного криптопровайдера СКЗИ «КриптоПро CSP».

Также Центр сертификации может интегрироваться с программно-аппаратным криптографическим модулем (ПАКМ) «КриптоПро HSM»<sup>84</sup> для обеспечения возможности генерации и хранения в последнем закрытых ключей Центров Сертификации. Взаимодействие программного средства с ПАКМ «КриптоПро HSM» осуществляется посредством криптопровайдера СКЗИ «КриптоПро CSP». При каждом запуске Центр сертификации автоматически определяется наличие подключения криптопровайдера СКЗИ «КриптоПро CSP» к ПАКМ «КриптоПро HSM», при наличии подключения будет доступен выбор ПАКМ «КриптоПро HSM» в качестве места хранения закрытых ключей создаваемых Центров Сертификации.

Установка и настройка ПАКМ «КриптоПро HSM» выполняется в соответствии с документом «ПАКМ «КриптоПро HSM». Инструкция по использованию» ЖТЯИ.00096-01 90 01.

Настройка СКЗИ «КриптоПро CSP» в качестве клиентского приложения ПАКМ «КриптоПро HSM» выполняется в соответствии с документом «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.

---

<sup>83</sup> Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

<sup>84</sup> Сетевое устройство, подключаемое либо непосредственно к серверу (хосту), использующему криптографические сервисы ПАКМ «КриптоПро HSM», либо в сегмент локальной сети через стандартные сетевые устройства (коммутаторы, маршрутизаторы, концентраторы) для обслуживания групп серверов и компьютеров пользователей сети.

## 5.1 Настройка взаимодействия с СКЗИ «КриптоПро CSP»

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром сертификации Aladdin eCA необходимо подготовить внешнюю гамму<sup>85</sup>. Подключение внешней гаммы необходимо для генерации ключевых пар центров сертификации, субъектов и пользователей по алгоритмам, криптопровайдером которых является СКЗИ «КриптоПро CSP». При этом, внешняя гамма не используется для генерации ключевой пары центра сертификации, если при его создании в качестве места хранения закрытого ключа выбран ПАКМ «КриптоПро HSM»<sup>86</sup>.

**При развертывании нескольких экземпляров Центра сертификации Aladdin eCA под одним средством балансирования нагрузки необходимо для каждого экземпляра программного средства подготовить уникальную внешнюю гамму, чтобы исключить совпадения ключевых пар.**

Порядок настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром сертификации Aladdin eCA:

- 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/aecaCa/services/cryptoproviders` командой:

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

- Переместите в каталог `/opt/aecaCa/services/cryptoproviders` файлы `ASN1P.jar`, `asn1rt.jar`, `JCP.jar` и `JCSP.jar` из состава дистрибутива ПО «КриптоПро Java CSP» командой:

```
sudo cp {ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar} /opt/aecaCa/services/cryptoproviders
```

- Назначьте права доступа на скопированные файлы:
  - Если выполняется первоначальная установка Центра сертификации Aladdin eCA, то назначьте файлам права доступа (`chmod 777`) командой:

```
sudo chmod 777 /opt/aecaCa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar}
```

- Если Центр сертификации Aladdin eCA был ранее установлен, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа к файлам (`chmod 700`) командами:

```
sudo chown aeca:aeca /opt/aecaCa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar}
sudo chmod 700 /opt/aecaCa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar}
```

<sup>85</sup> Заранее сформированный набор случайных данных, необходимых для генерирования закрытых ключей. При создании сертификатов на КН и с закрытым ключом (PKCS#12) для субъектов с использованием алгоритмов ключей, для которых в активном центре сертификации выбран криптопровайдер СКЗИ «КриптоПро CSP», Центр сертификации использует внешнюю гамму, заранее подготовленную на биологическом датчике случайных чисел (БДСЧ) криптопровайдера «КриптоПро CSP».

<sup>86</sup> Выбор места хранения осуществляется в разделе 3.1.3 эксплуатационного документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центром сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01-2.

- 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
```

- На хосте Центра сертификации Aladdin eCA поместите каталог с заранее подготовленной внешней гаммой в каталог `/opt/aecaCa/dist/` командой:

```
sudo cp -a ~/gamma/. /opt/aecaCa/dist/gamma
```

- В результате в каталоге `/opt/aecaCa/dist/gamma` появятся подкаталоги `db1`, `db2`, `kpim`.
  - Если выполняется первоначальная установка Центра сертификации Aladdin eCA, то назначьте права доступа файлам (`chmod 777`) командой:

```
sudo chmod -R 777 /opt/aecaCa/dist/gamma
```

- Если Центр сертификации Aladdin eCA был ранее установлен, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа (`chmod 700`) командами:

```
sudo chown -R aeca:aeca /opt/aecaCa/dist/gamma
sudo chmod -R 700 /opt/aecaCa/dist/gamma
```

- Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд<sup>87</sup>:

```
sudo ./cpconfig -hardware rndm -add cpsd -name 'cpsd rng' -level 3
sudo ./cpconfig -hardware rndm -configure cpsd -add string /db1/kis_1
/opt/aecaCa/dist/gamma/db1/kis_1
sudo ./cpconfig -hardware rndm -configure cpsd -add string /db2/kis_1
/opt/aecaCa/dist/gamma/db2/kis_1
```

- Если Центр сертификации Aladdin eCA был ранее установлен, перезапустите сервис `aeca-ca.service` командой:

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

Если в дальнейшем к СКЗИ «КриптоПро CSP» будет подключен ПАКМ «КриптоПро HSM», для обнаружения Центром сертификации Aladdin eCA наличия такого подключения необходимо перезапустить сервис `aeca-ca.service`.

## 5.2 Индикация об отсутствии связи с СКЗИ «КриптоПро CSP»

При отсутствии на хосте Центра сертификации Aladdin eCA активного криптопровайдера «КриптоПро CSP» для центров сертификации, закрытый ключ которых создан с его помощью, в пользовательском интерфейсе будет отображаться следующая индикация:

- В разделе «Центр сертификации» в списках для центров сертификации в соответствующих строках слева от имени отображаемого центра сертификации будет присутствовать индикация вида «треугольник с восклицательным знаком», при наведении на которую курсора будет отображаться всплывающее сообщение «Закрытый ключ центра сертификации недоступен».

<sup>87</sup> 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`.



- При переходе на карточку центра сертификации справа от индикации состояния центра сертификации будет присутствовать индикация «треугольник с восклицательным знаком», при наведении на которую курсора будет отображаться всплывающее сообщение «Закрытый ключ центра сертификации недоступен».
- В карточке центра сертификации в подразделе «Криптопровайдеры» справа от названия криптопровайдера СКЗИ «КриптоПро CSP» в полях алгоритмов, для которых он был выбран в качестве криптопровайдера при создании центра сертификации, будет присутствовать индикация «треугольник с восклицательным знаком», при наведении курсора на которую будет отображаться всплывающее сообщение «Криптопровайдер недоступен».

## ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

Перед началом работы следует ознакомиться со следующей документацией, относящейся к программному обеспечению:

- официальная документация РЕД ОС 7.1  
(адрес: <https://redos.red-soft.ru/base/manual/?ysclid=l5gg69co40129982631>);
- официальная документация Astra Linux Special Edition 1.7  
(адрес: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=137563555&ysclid=l5gg3t48tj885563182>);
- официальная документация Astra Linux Special Edition 1.8  
(адрес: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=302043140>);
- официальная документация Альт Сервер 8, релиз 10  
(адрес: <https://www.basealt.ru/alt-server/docs>);
- официальная документация Postgres  
(адрес: <http://www.postgresql.org/docs/12/index.html>);
- официальная документация Jatoba 4  
(адрес: <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>);
- официальная документация JC-Web Client 4.3.2 Руководство пользователя  
(адрес: [https://www.aladdin-rd.ru/upload/downloads/jc-webclient/JC-WebClient\\_4.3.2\\_Manual.pdf](https://www.aladdin-rd.ru/upload/downloads/jc-webclient/JC-WebClient_4.3.2_Manual.pdf)).

## ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**Администратор инициализации** – сотрудник (специалист), ответственный за приёмку и ввод в эксплуатацию изделия, которому доступны все функции роли «Администратор» в центре сертификации.

**Артефакт** – объект, применяемый или создаваемый в процессе разработки программного обеспечения.

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

**Ключевой носитель** – это сущность в центре сертификации, соответствующая физическому 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 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition, записанный на компакт-диск с размещённым на нём дистрибутивом программы и комплектом документации.

**Корневой ЦС** – экземпляр центра сертификации в информационной системе, имеющий абсолютное доверие со стороны всех участников процесса строгой аутентификации. С точки зрения службы безопасности предприятия должен быть обеспечен максимальным уровнем защиты (отдельный ПК, отключённый от сети, с доступом ограниченного круга лиц). Корневой ЦС владеет само подписанным сертификатом, который должен распространяться доверенным способом в информационной системе.

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

**Подчиненный ЦС** – экземпляр центра сертификации в информационной системе, обладающий функцией управления политиками строгой аутентификации или функцией управления жизненным циклом сертификатов субъектов информационной системы. Подчиненный ЦС владеет сертификатом, выданным вышестоящим ЦС (Корневым или другим Подчиненным), который используется для проверки всей цепочки доверия сертификатов.

**Расширение pgcrypto** – предоставляет криптографические функции, которые позволяют администраторам баз данных PostgreSQL хранить определенные 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, издается центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

**Субъект** – пользователь информационной системы или устройство (сервер, шлюз, маршрутизатор). Субъекту для строгой аутентификации в информационной системе в центре сертификации выдается сертификат. Синоним – конечная сущность (end entity).

**Технологический ЦС** – экземпляр центра сертификации в информационной системе, обладающий функцией первичной настройки программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

**Центр сертификации** – комплекс средств, задача которых заключается в обеспечении жизненного цикла сертификатов пользователей и устройств информационной системы, а также в создании инфраструктуры для обеспечения процессов идентификации и строгой аутентификации в информационной системе. Программный

компонент «Центр сертификации» является частью Центра сертификатов Aladdin Enterprise Certificate Authority Certified Edition.

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

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]