



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.03.01.02032 01-1
Версия	2.4
Листов	120
Дата	28.05.2026

Авторские права, товарные знаки, ограничения

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

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

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

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

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

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

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

Лицензионное соглашение

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

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

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

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

Права и собственность

ДАННОЕ СОГЛАШЕНИЕ НЕ ЯВЛЯЕТСЯ СОГЛАШЕНИЕМ О ПРОДАЖЕ.

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

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

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

Лицензия

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

Соглашения:

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

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

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

Требования к использованию

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

Использование ПО

Пользователь вправе:

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

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

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

АННОТАЦИЯ

Настоящий документ представляет собой первую часть руководства администратора программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020 (далее по тексту – программное средство или Центр сертификатов доступа).

Документ содержит сведения об области применения, составе, основных функциях, комплектности, действиях по приёмке, безопасной установке и настройке программного средства.

Документ предназначен для администраторов программного средства, 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 также определяет порядок подготовки и установки программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority» из состава программного средства. Перед эксплуатацией программы 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 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	Подраздел 1.5 «Действия по приёмке программного средства»
Действий по безопасной установке и настройке средства	Подраздел 1.6 «Действия по безопасной установке и настройке программы»
Действий по реализации функций безопасности среды функционирования средства	Подраздел 1.7 «Действия по реализации функций безопасности среды функционирования программы»

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

СОДЕРЖАНИЕ

Аннотация	5
Содержание.....	6
1 Основные сведения о программном средстве	9
1.1 Область применения.....	9
1.2 Состав программного средства	9
1.3 Основные функции программного средства	10
1.4 Комплект поставки программного средства	14
1.5 Действия по приёму программного средства	16
1.5.1 Проверка комплектности.....	16
1.5.2 Контроль целостности установочных пакетов.....	16
1.6 Действия по безопасной установке и настройке программного средства.....	18
1.7 Действия по реализации функций безопасности среды функционирования программного средства	18
2 Условия выполнения программы.....	20
2.1 Требования к программному обеспечению	20
2.1.1 Требования к среде функционирования серверной части центра сертификации	20
2.1.2 Требования к среде функционирования клиентской части центра сертификации	21
2.2 Требования к аппаратным средствам	21
3 Подготовка к установке программы.....	23
3.1 Подготовка среды функционирования программы	24
3.2 Подготовка среды функционирования с ОС РЕД ОС и РОСА «ХРОМ» 12 Сервер	24
3.2.1 Подключение репозитория и установка зависимостей	24
3.2.2 Установка среды исполнения Java	24
3.2.3 Установка и настройка СУБД.....	25
3.2.4 Установка веб-сервера.....	28
3.3 Подготовка среды функционирования с ОС Astra Linux Special Edition 1.8.....	29
3.3.1 Подключение репозитория и установка зависимостей	29
3.3.2 Поддержка активного режима замкнутой программной среды.....	30
3.3.3 Установка среды исполнения Java	30
3.3.4 Установка и настройка СУБД.....	30
3.3.5 Установка веб-сервера.....	33
3.4 Подготовка среды функционирования с ОС Альт 8 СП релиз 10 вариант исполнения Сервер и ОС «Альт Сервер» 11.....	34
3.4.1 Подключение репозитория и установка зависимостей в ОС Альт 8 СП релиз 10 вариант исполнения Сервер	34
3.4.2 Установка среды исполнения Java	34
3.4.3 Установка и настройка СУБД.....	35
3.4.4 Установка веб-сервера.....	38
3.5 Подготовка среды функционирования с ОС «Platform V SberLinux OS Server».....	39
3.5.1 Установка среды исполнения Java	39
3.5.2 Установка и настройка СУБД.....	39

3.5.3 Установка веб-сервера.....	43
3.6 Создание службы HTTP и keytab-файла	43
3.6.1 Получение keytab-файла в Samba DC и Альт Домен.....	43
3.6.2 Получение keytab-файла в ALD PRO.....	44
3.6.3 Получение keytab-файла в Free IPA.....	45
3.6.4 Получение keytab-файла в Dynamic Directory	45
3.6.5 Получение keytab-файла в MS AD.....	45
3.7 Установка веб-сервера Cprnginx.....	46
3.8 Установка JC-WebClient	47
3.9 Установка ПО «Рутокен Плагин» и его расширения	47
4 Установка программы	48
4.1 Распаковка инсталляционного комплекта программы	48
4.2 Настройка параметров конфигурации программы	49
4.3 Настройка веб-сервера при ограничении доступа к его файлам.....	63
4.4 Создание и настройка базы данных	63
4.4.1 Создание и настройка базы данных в автоматическом режиме.....	64
4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме	65
4.4.3 Создание и настройка базы данных Jatoba в ручном режиме	66
4.5 Установка программы	68
4.6 Порядок совместной установки компонентов программного средства на одном сервере	70
5 Запуск и остановка программы.....	73
6 Подключение к веб-интерфейсу	75
6.1 Общие сведения.....	75
6.2 Установка сертификата администратора инициализации	75
6.3 Настройка подключения к веб-интерфейсу.....	78
7 Контроль целостности исполняемых файлов программы	80
8 Сбор диагностической информации.....	81
9 Резервное копирование и восстановление данных программы.....	83
9.1 Резервное копирование данных	83
9.2 Расписание резервного копирования	84
9.3 Восстановление данных из резервной копии	84
10 Восстановление доступа к программе.....	86
11 Обновление программы.....	87
12 Удаление программы	90
13 Удаление базы данных Postgres.....	91
13.1 Удаление базы данных	91
13.2 Удаление пользователя базы данных	91
14 Поиск и устранение неисправностей.....	92
Приложение 1. Разрешение конфликта при установке СУБД Postgres и PostgresPro.....	93
Приложение 2. Настройка подключения к внешней СУБД	94
2.1 Настройка на хосте СУБД	94
2.2 Настройка на хосте eCA-CA.....	95
Приложение 3. Настройка TLS-соединения с СУБД.....	96

3.1 Настройка СУБД.....	96
3.2 Настройка eCA-CA	97
Приложение 4. Развёртывание кластера.....	98
4.1 Развёртывание кластера в виртуальной среде с холодным резервированием «active-passive».....	98
4.2 Развёртывание кластера с холодным резервированием «active-passive» путём переноса контейнера закрытого ключа основного узла.....	102
4.3 Развёртывания кластера в виртуальной среде с горячим резервированием «active-active».....	105
4.4 Развёртывание кластера с горячим резервированием «active-active» путём переноса контейнера закрытого ключа первого узла	109
4.3 Обновление ПО узлов кластера eCA-CA.....	113
Приложение 5. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP».....	114
5.1 Настройка взаимодействия с СКЗИ «КриптоПро CSP».....	115
5.2 Индикация об отсутствии связи с СКЗИ «КриптоПро CSP»	116
Обозначения и сокращения.....	118
Термины и определения.....	119
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	120

1 ОСНОВНЫЕ СВЕДЕНИЯ О ПРОГРАММНОМ СРЕДСТВЕ

1.1 Область применения

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020 применяется как элемент систем защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации при идентификации и строгой аутентификации субъектов¹ и объектов доступа² в автоматизированной (информационной) системе.

1.2 Состав программного средства

Центр сертификатов доступа включает:

- Программный комплекс «Центр сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.038 (далее – программа или eCA-CA), состоящий из следующих программных компонентов:

- 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, в части формирования идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) (далее – сертификаты), выпуска и обслуживания сертификатов, приостановки и/или возобновления действия сертификатов, предоставления информации о сертификатах и их статусах.
- Программный компонент «Клиентская часть Центра сертификации» RU.АЛДЕ.03.01.041.
Программный компонент реализует интерфейс (веб–интерфейс), с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра сертификации» RU.АЛДЕ.03.01.040.

- Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority» RU.АЛДЕ.03.01.039 (далее – eCA-VA), состоящий из следующих программных компонентов:

- Программный компонент «Серверная часть Центра валидации» RU.АЛДЕ.03.01.042.
Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части предоставления информации о сертификатах и их статусах.
- Программный компонент «Клиентская часть Центра валидации» RU.АЛДЕ.03.01.043.
Программный компонент реализует интерфейс (веб–интерфейс), с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра валидации» RU.АЛДЕ.03.01.042.

- Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.051 (далее – eCA-RA), состоящий из следующих программных компонентов:

- 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, в части формирования идентификационной информации, необходимой для выпуска сертификатов, выпуска и обслуживания сертификатов.
- Программный компонент «Клиентская часть Центра регистрации» RU.АЛДЕ.03.01.053.

¹ 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.

² Объект доступа представляет собой одну из сторон информационного взаимодействия, предоставляющую доступ.

Программный компонент реализует интерфейс (веб–интерфейс), с помощью которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра регистрации» RU.АЛДЕ.03.01.052.

- Программное средство «Утилита контроля целостности 2.0» RU.АЛДЕ.02.13.002–09.

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

- Средство криптографической защиты информации «КриптоПро CSP» версии 5.0 R3 KC1 (исполнение 1–Base) ЖТЯИ.00101–03 или версии 5.0 R3 KC2 (исполнение 2–Base) ЖТЯИ.00102–03 ¹.

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.

- Программно–аппаратный криптографический модуль (далее — ПАКМ) «КриптоПро HSM» версии 2.0 R3 ЖТЯИ.00096–01 (исполнение 1К, комплектация 1 или 2)². Поддерживается кластерная конфигурация ПАКМ «КриптоПро HSM».

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 Основные функции программного средства

Центр сертификатов доступа реализует следующие функции:

- Формирование идентификационной информации, необходимой для выпуска сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств) (далее по тексту - СВТ) на основе данных, полученных при первичной идентификации непосредственно от пользователей и СВТ через заявку на выпуск сертификатов, либо полученных от доменной службы каталогов или уполномоченных пользователей. Первичная идентификация пользователей и СВТ в программном средстве завершается созданием для них субъектов. Идентификационная информация, необходимая для выпуска сертификатов, представляет собой атрибуты субъекта, значения которых записываются в поля сертификатов, создаваемых для данного субъекта.
- Выпуск и обслуживание сертификатов безопасности (цифровых сертификатов) пользователей и средств вычислительной техники (устройств), в том числе:
 - Создание ключевых пар (открытый и закрытый ключи) пользователей и СВТ.
Создание ключевых пар для пользователей и средств вычислительной техники (устройств) выполняется при формировании для них сертификатов с закрытым ключом (PKCS#12) ³.

¹ СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки Центра сертификатов доступа и при необходимости приобретается заказчиком самостоятельно. Порядок настройки взаимодействия eCA–CA с СКЗИ «КриптоПро CSP» описан в приложении 5 настоящего документа. Порядок настройки взаимодействия eCA–RA с СКЗИ «КриптоПро CSP» описан в приложении 7 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 5. Центр регистрации Aladdin Enterprise Registration Authority». Порядок настройки взаимодействия eCA–VA с СКЗИ «КриптоПро CSP» описан в приложении 4 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority».

² ПАКМ «КриптоПро HSM» не является обязательным программным средством, не входит в комплект поставки программного средства и при необходимости приобретается заказчиком самостоятельно.

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

- Формирование сертификатов для пользователей и СВТ.

В программном средстве реализовано формирование сертификатов для пользователей и СВТ:

- С закрытым ключом (PKCS#12).
- На основании запроса PKCS#10 ¹.

- Формирование заявок на выпуск сертификатов для пользователей и СВТ.

В программном средстве реализовано:

- Создание заявок пользователями с ролями «Администратор» и «Оператор» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации»
- Создание заявок пользователем с ролью «Получатель сертификата» через программный компонент «Клиентская часть Центра регистрации» и программный интерфейс программного компонента «Серверная часть Центра регистрации», включая заявки, создаваемые через программный интерфейс по протоколу WS-Trust X.509v3 Token Enrollment Extensions (WSTEP) ².
- Создание заявок через программный интерфейс программного компонента «Серверная часть Центра регистрации» по протоколу Simple Certificate Enrollment Protocol (SCEP) ³.
- Автоматическое создание заявок на основании запросов PKCS#10 из локального или сетевого каталога в соответствии с настройками Offline-выпуска.

- Выдача сертификатов для их использования владельцами.

Выдача сертификатов для их использования владельцами доступна:

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

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

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

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

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

¹ В соответствии с документом «RFC 2986. PKCS #10: Certification Request Syntax Specification Version 1.7».

² В соответствии с документом «OASIS WS-Trust 1.3. WS-Trust X.509 Token Profile (WSTEP)».

³ В соответствии с документом «RFC 8894. Simple Certificate Enrolment Protocol».

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

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

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

- Создание, просмотр, экспорт и удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации.

Создание запроса на сертификат центра сертификации в вышестоящий центр сертификации выполняется при создании в программном средстве подчинённого центра сертификации. Запрос на сертификат центра сертификации в вышестоящий центр сертификации доступен для просмотра средствами из состава операционной системы (среды функционирования) (далее - ОС). Запрос на сертификат центра сертификации в вышестоящий центр сертификации доступен для экспорта за пределы программного средства. Удаление запроса на сертификат центра сертификации в вышестоящий центр сертификации выполняется при удалении в программном средстве данного подчинённого центра сертификации.

- Создание на основании запроса, импорт, просмотр, экспорт, удаление и отзыв сертификата для подчинённого центра сертификации.

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

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

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

- Формирование, экспорт и публикация списка отозванных сертификатов.

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

- Предоставление информации о сертификатах центров сертификации, пользователей и СБТ, а также информации об их статусах, в том числе:

- Формирование и экспорт реестра сертификатов.

В программном средстве реализовано формирование реестра сертификатов, содержащего значения полей всех созданных сертификатов. При экспорте реестра сертификатов доступен выбор критериев, которым должны соответствовать сертификаты в экспортируемом реестре.

- Проверка статусов сертификатов на основании данных, опубликованных в точке распространения.

Программное средство позволяет экспортировать опубликованные списки отозванных сертификатов и сертификаты центров сертификации из точек распространения, реализованных программным средством.

- Проверка статусов сертификатов в режиме реального времени.

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

Центр сертификатов доступа выпускает сертификаты в следующих форматах:

- Формат сертификата открытого ключа X.509v3 ².

Сертификат включает в себя следующие данные:

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

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

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

- Альтернативное имя субъекта.
- Альтернативное имя издателя сертификата.
- Базовые ограничения.
- Точки распространения списков отзыва.
- Доступ к информации о центрах сертификации.
- Идентификаторы расширенного использования ключа.
- Подпись сертификата.
- Формат списка отозванных сертификатов безопасности (CRL) ¹.
Список отозванных сертификатов включает в себя следующие данные:
 - Версия CRL.
 - Отличительное имя издателя CRL.
 - Дата и время издания текущего CRL.
 - Дата и время издания следующего CRL.
 - Расширения CRL, включая следующие возможные поля:
 - Идентификатор ключа издателя CRL.
 - Номер CRL.
 - Перечень отозванных сертификатов, где для каждого сертификата указаны:
 - Серийный номер.
 - Дата и время отзыва.
 - Причина отзыва (может отсутствовать).
 - Алгоритм подписи CRL.
 - Подпись CRL.
- Формат контейнера закрытого ключа PKCS #12 ².
Контейнеры закрытого ключа включают в себя следующие данные:
 - Цепочка сертификатов владельца закрытого ключа.
 - Закрытый ключ.

Центр сертификатов доступа реализовывает следующие криптографические алгоритмы:

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

1.4 Комплект поставки программного средства

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» RU.АЛДЕ.03.01.020 поставляется в следующей комплектации:

- Программный комплекс «Центр сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.038.

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

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

Установочные пакеты (дистрибутивы) на носителе оптической записи в формате:

- `аеса-са_[версия]-[номер сборки].deb`
- `аеса-са_[версия]-[номер сборки].rpm`

- Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority» RU.АЛДЕ.03.01.039.

Установочные пакеты (дистрибутивы) на носителе оптической записи в формате:

- `аеса-ва_[версия]-[номер сборки].deb`
- `аеса-ва_[версия]-[номер сборки].rpm`

- Программный комплекс «Центр регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.051 на носителе оптической записи (rpm-пакет и deb-пакет).

Установочные пакеты (дистрибутивы) на носителе оптической записи в формате:

- `аеса-ра_[версия]-[номер сборки].deb`
- `аеса-ра_[версия]-[номер сборки].rpm`

- Контрольная сумма установочного rpm-пакета (дистрибутива) программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма установочного deb-пакета (дистрибутива) программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма исполняемых файлов программного комплекса «Центр сертификации Aladdin Enterprise Certification Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма установочного rpm-пакета (дистрибутива) программного комплекса «Центр валидации Aladdin Enterprise Validation Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма установочного deb-пакета (дистрибутива) программного комплекса «Центр валидации Aladdin Enterprise Validation Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма исполняемых файлов программного комплекса «Центр валидации Aladdin Enterprise Validation Authority» на носителе оптической записи (файл в формате TXT на носителе оптической записи).

- Контрольная сумма установочного rpm-пакета (дистрибутива) программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма установочного deb-пакета (дистрибутива) программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority» (файл в формате TXT на носителе оптической записи).

- Контрольная сумма исполняемых файлов программного комплекса «Центр регистрации Aladdin Enterprise Registration Authority» (файл в формате TXT на носителе оптической записи).

- Программное средство «Утилита контроля целостности 2.0» RU.АЛДЕ.02.13.002-09 (исполняемый файл `jcverify` на носителе оптической записи).

- Контрольная сумма исполняемого файла программного средства «Утилита контроля целостности 2.0» (текстовый файл `jcverify.txt` на носителе оптической записи).

- Эксплуатационная документация в составе:

- «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Часть 1. Общие сведения» RU.АЛДЕ.03.01.020 30 01-1.
- «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Часть 2. Свидетельства о приёмке, упаковке и маркировке» RU.АЛДЕ.03.01.020 30 01-2.

- «Центр сертификатов доступа Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Описание применения» RU.АЛДЕ.03.01.020 31 01.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01–1.
 - «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.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 3. Описание REST API Центра сертификации Aladdin Enterprise Certification Authority» RU.АЛДЕ.03.01.020 32 01–3.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority» RU.АЛДЕ.03.01.020 32 01–4.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 5. Центр регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.020 32 01–5.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 6. Описание методов REST API Центра регистрации Aladdin Enterprise Registration Authority» RU.АЛДЕ.03.01.020 32 01–6.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора безопасности» RU.АЛДЕ.03.01.020 32 02.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство оператора» RU.АЛДЕ.03.01.020 34 01.
 - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство получателя сертификатов» RU.АЛДЕ.03.01.020 34 02.
- Потребительская упаковка.

1.5 Действия по приёме программного средства

Приёмка Центра сертификатов доступа предусматривает проверку комплектности и контроль целостности установочных пакетов (дистрибутивов) eCA-CA, eCA-RA и eCA-VA

1.5.1 Проверка комплектности

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

1.5.2 Контроль целостности установочных пакетов

Расчет контрольных сумм (далее – 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;
- aeca-ca_[версия]_[номер сбоки].rpm.txt.
- aeca-ra_[версия]_[номер сбоки].deb.txt;
- aeca-ra_[версия]_[номер сбоки].rpm.txt;
- aeca-va_[версия]_[номер сбоки].deb.txt;
- aeca-va_[версия]_[номер сбоки].rpm.txt.

Допускается выполнять расчет КС одним из следующих программных средств:

- «Утилита контроля целостности 2.0» из состава программного средства.
- «ФИКС–Unix 1.0»¹ (сертификат соответствия ФСТЭК № 680 от 30.10.2002 г.).

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

- Установите носитель оптической записи из комплекта поставки с установочными пакетами (дистрибутивами) в оптический привод.
- Выполните монтирование носителя оптической записи выполнив следующую команду с правами суперпользователя:

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

- Скопируйте с носителя оптической записи в выбранный каталог файловой системы:
 - Исполняемый файл утилиты «jcverify» и файл с его КС `jcverify.txt`.
 - Установочные пакеты (дистрибутивы) (в зависимости от состава программного средства и выбранной для среды функционирования программного средства ОС).
 - Текстовые файлы с КС для скопированных ранее установочных пакетов (дистрибутивов).
- Проверьте КС исполняемого файла программного средства «Утилита контроля целостности 2.0» выполнив следующую команду с правами суперпользователя:

```
./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
```

Внимание! При нарушении целостности исполняемого файла программного средства «Утилита контроля целостности 2.0» дальнейшая проверка КС установочных пакетов (дистрибутивов) запрещена.

- Рассчитайте последовательно КС установочных пакетов (дистрибутивов) выполнив следующую команду с правами суперпользователя:

```
./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]
```

¹ Программное средство «ФИКС–UNIX 1.0» не входит в комплект поставки программного средства.

Expected: [эталонная КС]

Exit code: 1

Внимание! При нарушении целостности установочных пакетов (дистрибутивов) дальнейшая установка программного средства запрещена.

Порядок расчёта КС с помощью программного средства «ФИКС–UNIX 1.0»:

- Установите носитель оптической записи из комплекта поставки с установочными пакетами (дистрибутивами) в оптический привод.
- Выполните монтирование носителя оптической записи выполнив следующую команду с правами суперпользователя:

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

- Скопируйте в выбранный каталог файловой системы исполняемый файл `ufix_rus` программного средства «ФИКС–UNIX 1.0» и выполните 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 отчёт, выполнив следующую команду:

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

- Размонтируйте носитель оптической записи выполнив следующую команду с правами суперпользователя:

```
umount /media/cdrom
```

- Сравните рассчитанные КС установочных пакетов (дистрибутивов) в HTML-отчёте с эталонными КС, приведёнными в таблице 2 Формуляра программного средства.

Внимание! При нарушении целостности установочных пакетов (дистрибутивов) дальнейшая установка программного средства запрещена.

1.6 Действия по безопасной установке и настройке программного средства

Установка компонентов Центра сертификатов доступа производится только с диска, получаемого от разработчика, после выполнения действий по приёмке поставленных компонентов Центра сертификатов доступа.

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 Центр сертификатов доступа.

Настройка Центра сертификатов доступа должна проводиться привилегированным пользователем с ролью «Администратор», допускаемым к установке и настройке Центра сертификатов доступа.

1.7 Действия по реализации функций безопасности среды функционирования программного средства

Для безопасной работы Центра сертификатов доступа 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 Центра сертификатов доступа.
- 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 функционирующими компонентами Центра сертификатов доступа от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов).

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

2.1 Требования к программному обеспечению

2.1.1 Требования к среде функционирования серверной части центра сертификации

Среда функционирования серверной части eCA-CA:

- 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.
 - ОС «Альт Сервер» 11.
 - ОС Platform V SberLinux OS Server.
 - РОСА «ХРОМ» 12 Сервер.
- Поддерживаемые СУБД:¹
 - PostgreSQL из состава ОС.
 - Postgres Pro.
 - Jatoba.
- Поддерживаемая среда исполнения Java:
 - Java Axiom JDK Certified.
 - Open JDK версии 17 и выше из состава поддерживаемых ОС.
- Поддерживаемые веб-серверы:
 - Apache2 из состава ОС.
 - Nginx из состава ОС.
 - Cpnginx ².
- Поддерживаемые ресурсные системы:
 - Samba DC.
 - FreeIPA.
 - ALD PRO.
 - РЕД АДМ.
 - Microsoft AD.
 - Альт Домен.
 - Dynamic Directory.
- СКЗИ «КриптоПро CSP»³ - криптопровайдер, обеспечивающий поддержку алгоритмов ГОСТ Р 34.10-2012.

¹ Поддерживаются кластерные конфигурации СУБД.

² Из состава средства криптографической защиты (далее - СКЗИ) «КриптоПро CSP». СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно.

³ СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки Центра сертификатов доступа и при необходимости приобретается заказчиком самостоятельно. Порядок настройки взаимодействия eCA-CA с СКЗИ «КриптоПро CSP» описан в приложении 5 настоящего руководства.

2.1.2 Требования к среде функционирования клиентской части центра сертификации

Среда функционирования клиентской части eCA-CA:

- 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.
 - ОС «Альт Сервер» 11.
 - ОС Platform V SberLinux OS Server.
 - РОСА «ХРОМ» 12 Сервер.
- Веб-браузер из состава ОС.
- JC-WebClient (для 64-битных систем) ¹.
- ПО «Рутокен Плагин» и веб-браузерное расширение «Адаптер Рутокен Плагин» ².

2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования eCA-CA:

- Системные требования, предъявляемые к конфигурации серверного оборудования, зависят от количества выпускаемых сертификатов и количества одновременных обращений к серверу eCA-CA приведены в таблице 2:
 - 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.

Таблица 2 - Системные требования, предъявляемые к серверу eCA-CA

Приложение	Системные требования	Тип внедрения		
		Малое внедрение	Среднее внедрение	Крупное внедрение
СУБД	ОЗУ, Гбайт	2	3	4
	Количество ядер процессора, шт.	2	4	4
	Накопитель HDD, Гбайт	6	12	18
eCA-CA	ОЗУ, Гбайт	6	8	16
	Количество ядер процессора, шт.	2	4	6
	Накопитель HDD, Гбайт	50	60	120
ОС	ОЗУ, Гбайт	4	4	4
	Количество ядер процессора, шт.	2	2	2
	Накопитель HDD, Гбайт	20	20	20

¹ JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) JaCarta (официальный сайт производителя [производителя](#)).

² ПО «Рутокен Плагин» через браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) Рутокен (официальный [сайт производителя](#)).

Приложение	Системные требования	Тип внедрения		
		Малое внедрение	Среднее внедрение	Крупное внедрение
Итого:	ОЗУ, Гбайт	12	15	24
	Количество ядер процессора, шт.	6	10	12
	Накопитель HDD, Гбайт	66	92	158

- Устройства взаимодействия с пользователем: клавиатура и мышь.
- USB 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей (ключевых носителей):
 - JaCarta:
 - JaCarta PKI.
 - JaCarta PRO.
 - JaCarta-2 PKI/ГОСТ.
 - JaCarta-2 ГОСТ.
 - JaCarta-3.
 - Рутокен ¹:
 - Рутокен ЭЦП 3.0.
 - Рутокен ЭЦП 2.0.
 - Рутокен ЭЦП 2.0 Flash.
 - Рутокен ЭЦП PKI.

¹ Возможность использования ключевых носителей Рутокен может быть ограничена лицензией.

3 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

При установке eCA-CA 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 путём редактирования конфигурационного файла eCA-CA (см. подраздел 4.2).

В таблице 3 приведён список портов, которые должны быть открыты в eCA-CA.

Таблица 3 — Таблица сетевого взаимодействия

Порт	Транспорт	Протокол	Назначение	Возможность изменения
443	TCP	TLS/HTTPS	Порт для подключения к веб-интерфейсу eCA-CA, а также для взаимодействия с eCA-RA и eCA-VA.	Да
80	TCP	HTTP	С данного порта выполняется переадресация пакетов на порт 443.	Да
88, 464	TCP	Kerberos	Порты для взаимодействия со службой аутентификации Kerberos ресурсной системы.	Нет
389	TCP	LDAP	Порт для взаимодействия с доменной службой каталогов (ресурсной системой) по протоколу LDAP.	Нет
5432	TCP	TCP	Порт для подключения к СУБД.	Да
	TCP	TLS		
514	UDP/TCP	Syslog	Порт для отправки сообщений на Syslog-серверы (порт 514, как правило, используется по умолчанию).	Да
25	TCP	SMTP	Порт для подключения к почтовому серверу (значение 25 задано по умолчанию).	Да

В таблице 4 приведён список портов, которые открывает для локальной передачи данных внутри сервера и использует eCA-CA. Доступ к данным портам для внешних подключений ограничивается автоматически при установке eCA-CA с помощью утилиты «iptables» из состава ОС сервера. Во избежание возникновения ошибок в работе eCA-CA 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 «discovery-service» (Сервис обнаружения)
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)
1400	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «external-integration-service» (Сервис внешних интеграций)
1650	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (Сервис журнализации)
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)

Порт	Транспорт	Протокол	Назначение
1900	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «api-gateway-service» (Сервис проксирования)

3.1 Подготовка среды функционирования программы

Порядок подготовки среды функционирования eCA-CA:

- Установка ОС (выполняется в соответствии с документацией производителя).
- Подключение репозитория и установка зависимостей ОС.
- Развёртывание среды исполнения Java.
- Установка СУБД.
- Установка веб-сервера.
- Установка СКЗИ «КриптоПро CSP» (для использования алгоритмов ГОСТ Р 34.10-2012 и RSA). Порядок установки и настройки СКЗИ «КриптоПро CSP» представлен в приложении 5 настоящего руководства. Установка и настройка СКЗИ «КриптоПро CSP» могут быть выполнены после установки eCA-CA в процессе его эксплуатации.

Для обеспечения корректности встраивания СКЗИ «КриптоПро CSP» канал взаимодействия клиентской и серверной части eCA-CA должен быть организован по протоколу TLS ГОСТ, а также должна обеспечиваться TLS-аутентификация пользователей в eCA-CA 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» приведён в подразделе 3.6. После установки веб-сервера необходимо установить на СКЗИ «КриптоПро CSP» серверную лицензию, обеспечивающую возможность использования СКЗИ «КриптоПро CSP» в качестве TLS-сервера.

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

3.2.1 Подключение репозитория и установка зависимостей

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

```
dnf install tar unzip iptables
```

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

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

```
dnf install tar unzip iptables
```

3.2.2 Установка среды исполнения Java

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

3.2.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.2.2.2 Установка OpenJDK

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

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

3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

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

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

3.2.3.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

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

```
dnf install postgresql-server
```

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

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

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

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

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

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

¹ Подробное описание приведено на официальном сайте производителя.

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

³ Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

Примеры изменений:

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

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

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

```
systemctl restart postgresql
```

3.2.3.2 Установка СУБД Postgres Pro ¹

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив следующую команду ²:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

Примеры изменений:

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

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

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

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

¹ Подробное описание приведено на официальном сайте производителя.

² Команды ниже приведены для СУБД Postgres Pro версии 16.

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

⁴ Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

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

3.2.3.3 Установка СУБД Jatoba ¹

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

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

```
ls -l
```

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

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

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

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

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

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

¹ Подробное описание приведено на официальном сайте производителя.

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`¹.
- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/jatoba/[версия]/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например, `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке DATABASE указано значение `replication`.

Примеры изменений:

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

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

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

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

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

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

3.2.4 Установка веб-сервера

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

3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install httpd
```

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

```
dnf install mod_ssl
```

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

```
systemctl enable httpd
```

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

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

```
dnf install apache-mod_ssl
```

¹ Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

```
urpmi apache-mod_proxy
```

- Установите модуль поддержку разделяемой памяти (shared memory) на основе слотов выполнив команду с правами суперпользователя:

```
dnf install apache-mod_slotmem_shm
```

3.2.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

3.3 Подготовка среды функционирования с ОС Astra Linux Special Edition 1.8

3.3.1 Подключение репозитория и установка зависимостей¹

Порядок подключения репозитория и зависимостей:

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

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

- Укажите ссылки на следующие репозитории³:

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

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

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

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

Пример:

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

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

```
apt-cdrom add
```

¹ Подробнее см. на официальном сайте производителя.

² Ссылки на репозитории приведены для Astra Linux SE 1.8.5

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

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

```
apt update
```

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

```
apt install tar unzip iptables
```

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

3.3.2 Поддержка активного режима замкнутой программной среды

еСА-CA обеспечивает работу ОС Astra Linux Special Edition версий 1.8 в активном режиме замкнутой программной среды (далее — ЗПС). Для этого в состав установочных пакетов еСА-CA включён публичный открытый ключ АО «Аладдин Р.Д.» - `aladdin_pub.key`.

После распаковки установочного пакета ключ находится по пути:

```
/opt/aecaCa/digsig/keys/aladdin_pub.key.
```

Для обеспечения режима ЗПС открытый ключ необходимо скопировать ¹ в каталог:

```
/etc/digsig/keys/.
```

3.3.3 Установка среды исполнения Java

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

3.3.3.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.3.3.2 Установка OpenJDK

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

3.3.4 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

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

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

3.3.4.1 Установка СУБД PostgreSQL²

Порядок установки СУБД PostgreSQL:

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

```
apt install postgresql
```

¹ Данное действие необходимо выполнять после распаковки установочных пакетов еСА-CA.

² Подробное описание приведено на официальном сайте производителя.

- Выполните установку последней доступной версии пакета `postgresql-contrib`¹ выполнив следующую команду с правами суперпользователя:

```
apt install postgresql-contrib
```

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

```
apt install postgresql-client
```

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

```
systemctl enable postgresql
```

- Отредактируйте файл `/etc/postgresql/15/main/postgresql.conf`² с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`³.

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

Примеры изменений:

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

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

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

```
systemctl restart postgresql
```

3.3.4.2 Установка СУБД Postgres Pro⁴

Порядок установки СУБД PostgreSQL Pro:

- Загрузите скрипт для добавления репозитория, выполнив следующую команду⁵:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

- Установите СУБД, выполнив следующую команду с правами суперпользователя:

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`⁶ с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`⁷.

¹ Для некоторых минорных версий ОС данный пакет может отсутствовать.

² Расположение файла может отличаться. Расположение файла указано для СУБД PostgreSQL версии 15. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

³ Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

⁴ Подробное описание приведено на официальном сайте производителя.

⁵ Команды ниже приведены для СУБД Postgres Pro версии 16.

⁶ Расположение файла указано для СУБД Postgres Pro версии 16. Для поиска файла используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

⁷ Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

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

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

Примеры изменений:

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

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

- Перезапустите СУБД выполнив команду с правами суперпользователя:

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

3.3.4.3 Установка СУБД Jatoba ¹

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

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

```
ls -l
```

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

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

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

¹ Подробное описание приведено на официальном сайте производителя.

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

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

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

Примеры изменений:

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

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

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

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

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

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

3.3.5 Установка веб-сервера

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

3.3.5.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
apt install apache2
```

¹ Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

- Активируйте модули выполнив следующую команду с правами суперпользователя:

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

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

```
systemctl restart apache2.service
```

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

```
systemctl enable apache2
```

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

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

3.3.5.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
apt install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

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

3.4.1 Подключение репозитория и установка зависимостей в ОС Альт 8 СП релиз 10 вариант исполнения Сервер

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

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

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

- Укажите в файле ссылку на следующий репозиторий:

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

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

```
apt-get update
```

3.4.2 Установка среды исполнения Java

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

3.4.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.4.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС.

3.4.3 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 приведён в приложении 1.

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

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

3.4.3.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

1. Установите последнюю доступную версию СУБД PostgreSQL выполнив команду:

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

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

```
apt-get install postgresql-contrib
```

3. Произведите инициализацию СУБД:

- 3.1. Выполните команду с правами суперпользователя:

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

- 3.2. Если выполнить команду шаге 3.1 не удалось, то выполните команду с правами суперпользователя:

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

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

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

5. Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

6. Добавьте СУБД в автозагрузку выполнив следующую команду с правами суперпользователя:

```
systemctl enable postgresql
```

7. Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`² с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`³.
8. Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgsql/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

¹ Подробное описание приведено на официальном сайте производителя.

² Расположение файла может отличаться, для поиска используйте с правами суперпользователя команду `find / -type f -name postgresql.conf`

³ Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

Примеры изменений:

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

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

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

```
systemctl restart postgresql
```

3.4.3.2 Установка СУБД Postgres Pro¹

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив следующую команду²:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

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

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

Примеры изменений:

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

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

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

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

¹ Подробное описание приведено на официальном сайте производителя.

² Команды ниже приведены для СУБД Postgres Pro версии 16.

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

⁴ Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

3.4.3.3 Установка СУБД Jatoba¹

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

- Дистрибутив СУБД содержит:

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

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

```
ls -l
```

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`².

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

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

¹ Подробное описание приведено в официальной документации на Jatoba.

² Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

Примеры изменений:

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

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

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

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

3.4.4 Установка веб-сервера

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

3.4.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

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

- Установите модуль ssl выполнив следующую команду с правами суперпользователя:

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

- Создайте следующие файлы:

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

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

Внесите следующий текст в созданный файл:

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

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

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

Внесите следующий текст в созданный файл:

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

- Активируйте модули выполнив поочерёдно следующие команды с правами суперпользователя:

```
a2enmod ssl
a2enmod proxy
a2enmod proxy_http
a2enmod headers
a2enmod cgi
```

```
a2enmod rewrite
a2enmod http2
```

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

```
a2enport https
```

3.4.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
apt-get install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

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

3.5.1 Установка среды исполнения Java

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

3.5.1.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.5.1.2 Установка OpenJDK

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

3.5.2 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

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

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

3.5.2.1 Установка СУБД PostgreSQL¹

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL выполнив команду:

```
dnf install postgresql-server
```

¹ Подробное описание приведено на официальном сайте производителя.

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

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду:

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

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

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

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

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

Примеры изменений:

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

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

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

```
systemctl restart postgresql
```

3.5.2.2 Установка СУБД Postgres Pro³

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив следующую команду⁴:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

¹ Расположение файла может отличаться. Для поиска файла используйте команду с правами суперпользователя `find / -type f -name postgresql.conf`

² Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

³ Подробное описание приведено на официальном сайте производителя.

⁴ Команды ниже приведены для СУБД Postgres Pro версии 16.

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`¹ с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`².
- Убедитесь, что для сетевых подключений к СУБД по протоколам IPv4 и IPv6 используется защищённый метод парольной аутентификации `scram-sha-256`. Для этого проанализируйте содержимое конфигурационного файла `/var/lib/pgpro/std-16/data/pg_hba.conf`. Если для записей типа `host` указан метод, отличный от `scram-sha-256` (например: `password`, `md5` или `ident`), замените его на `scram-sha-256`, за исключением тех строк, где в колонке `DATABASE` указано значение `replication`.

Примеры изменений:

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

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

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

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

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

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

3.5.2.3 Установка СУБД Jatoba³

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

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

```
ls -l
```

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

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

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

² Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

³ Подробное описание приведено на официальном сайте производителя.

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

Примеры изменений:

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

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

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

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

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

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

¹ Значение `max_connections` равно `1000` является рекомендуемым. При необходимости увеличьте данное значение.

3.5.3 Установка веб-сервера

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

3.5.3.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install httpd
```

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

```
dnf install mod_ssl
```

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

```
systemctl enable httpd
```

3.5.3.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

3.6 Создание службы HTTP и keytab-файла

Внимание! Предварительно eCA-CA должен быть настроен Kerberos (должен быть настроен файл `krb5.conf`, рекомендуемое расположение `/etc/krb5.conf`).

При изменении http-службы или при подключении eCA-CA к другому домену необходимо заменять keytab-файл.

3.6.1 Получение keytab-файла в Samba DC и Альт Домен

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

```
ssh <username>@<ip_address>
```

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

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

```
ssh username@ip_address -p 22
```

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

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

- Перейдите в режим суперпользователя выполнив команду:

```
su
```

- Создайте пользователя-службу, который будет использоваться для авторизации в LDAP, выполнив команду¹:

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

- Разблокируйте созданного пользователя выполнив команду:

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

- Получите Kerberos-билет для администратора домена выполнив команду:

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

- Расширьте для созданного пользователя-службы доступные поддерживаемые алгоритмы шифрования, выполнив команду²:

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

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

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

где <имя настраиваемого клиента> - имя хоста, на котором производится установка eCA-CA.

- Измените UPN пользователя-службы выполнив команду:

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

где <имя настраиваемого клиента> - имя компьютера, на котором производится установка eCA-CA.

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

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

где <имя настраиваемого клиента> - имя хоста, на котором производится установка eCA-CA.

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

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

3.6.2 Получение keytab-файла в ALD PRO

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

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

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

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

¹ При подключении нескольких eCA-CA к одному контроллеру домена рекомендуется создать пользователя-службу для каждого eCA-CA.

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

- Создайте новую службу, нажав кнопку <+Новая служба>, выбрав класс службы - HTTP, имя компьютера - настраиваемый клиент, на который производится установка еСА-СА. Сохраните изменения, нажав кнопку <Да> всплывающего окна.
- Получите Kerberos-билет администратора домена выполнив команду:

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

- Экспортируйте Kerberos-билет HTTP-службы на настраиваемый клиент по рекомендованному пути `/etc/http.keytab`. Для этого с сервера, на котором выполняется установка еСА-СА, выполните команду:

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

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

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

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

3.6.3 Получение keytab-файла в Free IPA

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

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

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

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

- Создайте новую службу, нажав кнопку <+Добавить>, выбрав класс службы - HTTP, имя узла - настраиваемый клиент, на который производится установка еСА-СА. Сохраните изменения, нажав кнопку <Да> всплывающего окна.
- Получите Kerberos-билет администратора домена выполнив команду:

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

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

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

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

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

3.6.4 Получение keytab-файла в Dynamic Directory

Получение keytab-файла в Dynamic Director выполняется аналогично получению keytab-файла в Free IPA (см. 3.6.3).

3.6.5 Получение keytab-файла в MS AD

- На контроллере домена MS AD запустите консоль управления «Active Directory Users and Computers» (ADUC).
- Создайте пользователя-службу, который будет использоваться для валидации Kerberos-билетов, например в организационном юните «Users».

- После создания пользователя-службы включите для него на вкладке «Свойства» - «Учётная запись» в поле «Параметры учётной записи» следующие параметры (остальные параметры должны быть отключены):
 - «Запретить смену пароля пользователем»;
 - «Срок действия пароля не ограничен»;
 - «Данная учётная запись поддерживает 128-разрядное шифрование»;
 - «Данная учётная запись поддерживает 256-разрядное шифрование».
- Привяжите SPN создаваемой HTTP-службы к созданному пользователю и хосту, с одновременным созданием keytab-файла (можно экспортировать в любое удобное расположение, например в `http.keytab`). Для этого выполните команду из командной строки PowerShell:

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

где `<имя настраиваемого клиента>` - имя хоста, на котором производится установка eCA-CA.

3.7 Установка веб-сервера Cppnginx

Пакеты веб-сервера Cppnginx расположены в дистрибутиве СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP» (см. приложение 5 настоящего руководства).

Порядок установки веб-сервера Cppnginx:

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

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

- Установите следующие пакеты:
 - Для ОС Astra Linux SE выполните следующую команду с правами суперпользователя `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, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server выполните следующую команду с правами суперпользователя `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 выполните следующую команду с правами суперпользователя `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) выполнив следующую команду с правами суперпользователя:

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

- Проверьте активацию лицензии выполнив следующую команду с правами суперпользователя командой:

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

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

```
systemctl start cpnginx.service
```

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

```
systemctl enable cpnginx.service
```

3.8 Установка JC-WebClient

JC-WebClient необходимо установить на компьютер, с которого будет выполняется управление серверной частью еСА-СА через веб-интерфейс. JC-WebClient обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях).

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

Скачайте дистрибутив JC-WebClient с веб-сайта АО «Аладдин Р.Д» и установите зависимости. Установите JC-WebClient выполнив следующую команду с правами суперпользователя:

РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	<code>dnf install JC-WebClient-x64-x.x.x.xxxx.rpm</code>
Astra Linux SE	<code>apt install -f JC-WebClient-x64-x.x.x.xxxx.deb</code>
Альт Сервер	<code>apt-get install JC-WebClient-x64-x.x.x.xxxx.rpm</code>

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

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

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

```
sh jcmon start
```

3.9 Установка ПО «Рутокен Плагин» и его расширения

ПО «Рутокен Плагин» и его веб-браузерное расширение «Адаптер Рутокен Плагин» обеспечивает выпуск сертификатов на электронных ключах (ключевых носителях) Рутокен. ПО «Рутокен Плагин» и его браузерное расширение «Адаптер Рутокен Плагин» необходимо установить на компьютер, с которого будет выполняется подключение к Клиентской части еСА-СА.

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

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

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

4 УСТАНОВКА ПРОГРАММЫ

4.1 Распаковка инсталляционного комплекта программы

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

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

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

Astra Linux SE

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

Альт Сервер

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

Инсталляционный rpm/deb-пакет будет автоматически распакован в каталог `/opt/aecaCa`.

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

Таблица 5 - Структура распакованного инсталляционного rpm/deb-пакета eCA-CA

Структурный элемент	Описание
/opt/aecaCa	Установочный комплект eCA-CA, а также используемые дополнительные инструменты
/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 развёртывания продукта; содержит создаваемые временные файлы
/opt/aecaCa/dist/archive/	Архивы, сформированные в результате очистки журнала событий
/opt/aecaCa/dist/backup/	Созданные резервные копии eCA-CA
/opt/aecaCa/dist/certificates/account	Расположение pkcs#12 контейнера сертификата администратора инициализации и пароля от этого контейнера
/opt/aecaCa/dist/certificates/ssl	Расположение сертификатов для управления ssl-соединением
/opt/aecaCa/dist/cryptotoken/	Расположение pkcs#12 контейнеров, содержащих открытый и закрытый ключи центров сертификации
/opt/aecaCa/dist/environment/	Расположение переменных окружения сервисов
/opt/aecaCa/dist/logs/	Расположения технических журналов сервисов
/opt/aecaCa/dist/webserver/	Конфигурации, подключаемые к Web-серверу
/opt/aecaCa/eula	Каталог с файлом лицензионного соглашения (EULA)
/opt/aecaCa/samples	Содержит шаблоны файлов конфигурации для внутреннего использования программным средством
/opt/aecaCa/scripts	Содержит скрипты управления программным средством eCA-CA
/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

Структурный элемент	Описание
/opt/aecaCa/scripts/external/export-ca-data.sh	Скрипт экспорта файлов CRL, Delta CRL, AIA из eCA-CA
/opt/aecaCa/scripts/internal/aeca/selinux	Политики, подключаемые к selinux, необходимые для функционирования eCA-CA
/opt/aecaCa/scripts/backup.sh	Скрипт резервного копирования конфигурации eCA-CA
/opt/aecaCa/scripts/config.sh	Bash-скрипт конфигурации eCA-CA (развёртывание продукта, настройка подключения к БД, управление конфигурацией сервисов)
/opt/aecaCa/scripts/database_create.sh	Скрипт создания базы данных на разворачиваемом сервере eCA-CA с предустановленными параметрами по умолчанию (именем пользователя, наименованием базы данных и т.д.)
/opt/aecaCa/scripts/diagnostics.sh	Скрипт сбора диагностических данных
/opt/aecaCa/scripts/install.sh	Скрипт установки и обновления текущей версии eCA-CA
/opt/aecaCa/scripts/integrity_check.sh	Скрипт контроля целостности исполняемых файлов
/opt/aecaCa/scripts/restore.sh	Скрипт восстановления из резервной копии конфигурации eCA-CA
/opt/aecaCa/scripts/restore_access.sh	Скрипт резервного восстановления доступа к eCA-CA
/opt/aecaCa/scripts/uninstall.sh	Скрипт удаления eCA-CA
/opt/aecaCa/scripts/jc_checksum	Файл с эталонами контрольных сумм исполняемых файлов eCA-CA
/opt/aecaCa/scripts/key	Файл, содержащий ключ шифрования пароля пользователя СУБД в конфигурационном файле
/opt/aecaCa/services	Сервисы Серверной части eCA-CA
/opt/aecaCa/services/cryptoproviders	Каталог файлов для взаимодействия со сторонним криптопровайдером
/opt/aecaCa/static	Артефакты Клиентской части eCA-CA
/opt/aecaCa/digsig/keys/aladdin_pub.key	Открытый ключ АО «Аладдин Р.Д.», используемый для проверки подписи исполняемых файлов и библиотек eCA-CA в режиме замкнутой программной среды (ЗПС) на Astra Linux Special Edition.

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

4.2 Настройка параметров конфигурации программы

- Конфигурация eCA-CA задаётся с помощью параметров конфигурационного файла `/opt/aecaCa/scripts/config.sh`.
- Перед установкой программного компонента определите значения следующих параметров:
 - `webserver` — используемый веб-сервер (nginx, apache или cprnginx). 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, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server по пути `/etc/httpd`; для Альт Сервера конфигурация `apache` располагается по пути `/etc/httpd2/conf`; конфигурация `cpnginx` располагается по пути `/etc/opt/cprosp/cpnginx`);
- `use_credentials_from_config` — значение флага использования имени и пароля пользователя СУБД из конфигурационного файла.
- Если параметр `use_credentials_from_config` установлен в значение `true` (значение по умолчанию), то укажите значения параметра `database_password` — пароль создаваемой базы данных.¹
- `root_cert_path` — абсолютный путь к сертификату корневого Центра сертификации 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` — полное имя сервера eCA-CA. Установленное значение заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых при развёртывании локального субъекта веб-сервера и сертификата для него.

• Для обеспечения корректности встраивания СКЗИ «КриптоПро CSP» канал взаимодействия клиентской и серверной части eCA-CA должен быть организован по протоколу TLS ГОСТ, а также должна обеспечиваться TLS-аутентификация пользователей в eCA-CA с использованием отечественных криптографических алгоритмов. Для этого настройте конфигурационный файл в соответствии с таблицей 6.

Таблица 6 - Параметры для настройки TLS ГОСТ

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

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

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

¹ Если параметр `use_credentials_from_config` имеет значение `true`, то после установки или обновления eCA-VA параметр `database_password` отображается в конфигурационном файле в зашифрованном виде (алгоритм шифрования AES-256 с использованием хранимого в файле `/opt/aecaRa/scripts/key` ключа шифрования).

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.

Описание параметров конфигурационного файла приведено в таблице 7.

Таблица 7 — Описание параметров конфигурации

Параметр	Значение по умолчанию	Описание
Конфигурация развёртывания		
webserver	'#CHANGEIT'	Используемый web-сервер. Допустимые значения: "apache", "nginx", "cprnginx". '#CHANGEIT' означает, что параметр не задан. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
webserver_path	'#CHANGEIT'	Расположение конфигурации веб-сервера. '#CHANGEIT' означает, что параметр не задан. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
aeca_path	'/opt/aecaCa/dist'	Каталог установки eCA-CA
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 eCA-CA
webserver_config_path	'/opt/aecaCa/dist/webserver'	Расположение конфигурации eCA-CA для веб-сервера
encryption_key_path	'/opt/aecaCa/scripts/key'	Ключ для шифрования конфигурационного файла
proxy_connect_timeout	'320'	Время ожидания подключения к прокси-серверу перед тем, как будет выдано сообщение об ошибке

Параметр	Значение по умолчанию	Описание
		Только для nginx Настраивается разработчиком eCA-CA, редактировать не следует
proxy_send_timeout	'320'	Время ожидания ответа от прокси-сервера после отправки запроса. Если ответ не получен в течение этого времени, запрос считается неудачным. Только для nginx Настраивается разработчиком eCA-CA, редактировать не следует
proxy_read_timeout	'720'	Время ожидания чтения ответа от прокси-сервера после получения успешного запроса. Если ответ не получен в течение этого времени, запрос считается неудачным. Только для nginx Настраивается разработчиком eCA-CA, редактировать не следует
ssl_ciphers	' '	Поддерживаемые наборы шифров для TLS-соединения Данный параметр позволяет ограничить наборы шифров (cipher suites), которые могут использоваться при TLS-соединении. Разделитель между наборами – двоеточие (:). Если клиент не поддерживает ни один из указанных в данном параметре наборов, TLS-соединение не будет установлено. По умолчанию значением данного параметра является пустая строка, что означает отсутствие управления со стороны eCA-CA перечнем допустимых наборов шифров (ciphersuites) TLS-соединения для веб-сервера. (Исходный набор шифров веб-сервера не переопределяется). В данном параметре могут быть указаны любые наборы шифров, поддерживаемые используемой на сервере eCA-CA версией Openssl для TLS v1.2. Получить список поддерживаемых используемым Openssl наборов шифров для TLS v1.2 можно с помощью команды «openssl ciphers -tls1_2 -s». Данный параметр учитывается только при использовании Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cprnginx осуществляется с помощью утилиты «cprconfig» из состава «КриптоПро CSP».1
ssl_protocols	'TLSv1.2 TLSv1.3'	Поддерживаемые версии протокола TLS

¹ Инструкция по установке и настройке cprnginx - <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 по умолчанию	Описание
		Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обеих версий необходимо указывать их через пробел).
backup_path	'/opt/aecaCa/dist/backup'	Путь до места хранения резервных копий
logs_base	'/opt/aecaCa/dist/logs'	Путь хранения лог-файлов
archive_path	'/opt/aecaCa/dist/archive'	Путь до архивированных файлов. Можно менять. Только абсолютные пути. Права на каталог должны быть предоставлены пользователю/группе аеса:аеса.
certificates_ssl_path	'/opt/aecaCa/dist/certificates/ssl'	Путь хранения контейнера, сертификата и ключа web-сервера, а также цепочек сертификатов разрешенных издателей
certificates_account_path	'/opt/aecaCa/dist/certificates/account'	Путь хранения контейнера администратора инициализации
Конфигурация пользователя		
aeca_user	'aeca'	Имя пользователя
aeca_group	'aeca'	Наименование группы, в которую входит пользователь
Конфигурация памяти		
memory	'6144'	Значение в МБ. еСА-СА при запуске резервирует указанное в данном параметре количество RAM для своих сервисов. При значении параметра менее 6 ГБ еСА-СА не запустится – будет выдано сообщение об ошибке.
enable_gc_diagnostic	'false'	Флаг сбора диагностической информации о памяти. При включении данного флага и выполнении скрипта сбора диагностических данных в архиве диагностических данных будет содержаться лог сборщика мусора и дампы памяти для упавших приложений ЦС
enable_heap_dump	'false'	Флаг сбора дампов памяти для «упавших» приложений ЦС
Конфигурация БД		
max_db_pool_size	'200'	Максимальный размер пула подключений к СУБД. Настраивается разработчиком еСА-СА, редактировать не следует
use_tls	'false'	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false

Параметр	Значение по умолчанию	Описание
database_username	'aeca'	Имя пользователя СУБД
database_password	'#CHANGEIT'	Пароль пользователя СУБД. '#CHANGEIT' означает, что параметр не задан. Пароль пользователя СУБД. Администратор инициализации при установке должен сменить значение '#CHANGEIT' на необходимое
database_host	'localhost'	Имя хоста СУБД
database_port	'5432'	Порт для доступа к СУБД
database_name	'aecaca'	Имя БД
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД. '#CHANGEIT' означает, что параметр не задан
Конфигурация eCA-CA		
http_port	'80'	Порт для подключения к программному компоненту eCA-CA по протоколу HTTP
https_port	'433'	Порт для подключения к eCA-CA по протоколу HTTPS
hostname	'localhost'	Имя сервера, на котором разворачивается eCA-CA. Также заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых (при развёртывании eCA-CA) сертификата веб-сервера и локального субъекта. Должно совпадать с hostname сервера
number_of_services	'10'	Количество активных сервисов в системе Настраивается разработчиком eCA-CA, редактировать не следует
logging_response	'false'	—
logging_sql	'false'	—
Переменные окружения для logback		
logs_file_max_size	'10MB'	Максимальный размер файла лога сервиса перед его архивацией. При достижении данного значения текущий лог-файл (access.log или service.log) будет архивироваться – файл будет сохранен в текущем каталоге логов данного сервиса с именем {access или service}-{дата в формате YYYY-MM-DD}.{индекс лога}.log.
logs_max_history	'10'	Максимальный срок хранения архивов логов в днях. Архивы логов, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться.

Параметр	Значение по умолчанию	Описание
logs_total_size_cap	'100MB'	Максимальный общий объем логов, включая архивы, каждого типа (access или service) для каждого сервиса При достижении данного объема наиболее старые архивы логов данного типа будут удаляться.
Тайм-ауты		
internal_http_read_timeout	'240'	Максимальный тайм-аут ожидания ответа методов сервисов при внутреннем взаимодействии. Единица измерения – секунды.
internal_http_connection_timeout	'60'	Максимальный тайм-аут ожидания подключения к сервисам при внутреннем взаимодействии. Единица измерения – секунды.
Переменные окружения, используемые certificate-authority-service		
pkcs12_key_protection_algorithm	PBEWithHmacSHA256AndAES_256	Алгоритм хеширования для ключа контейнера PKCS12 Допустимые значения: – PBEWithHmacSHA256AndAES_256; – PBEWithSHA1AndDESede. Рекомендуется использовать алгоритм PBEWithHmacSHA256AndAES_256; Устаревший алгоритм PBEWithSHA1AndDESede
crl_scheduler	'0 */1 * * * *'	CRON выражение, по которому запускается служба выпуска CRL
crl_clean_queues	'0 */30 * * * *'	CRON выражение, по которому очищаются очереди службы выпуска CRL
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 ее, каждый час.
ldap_sync_connection_point	'0 */30 * * * *'	CRON выражение, по которому запускается синхронизация точек подключения ресурсных систем (частичная синхронизация) Значение по умолчанию - '0 */30 * * * *', обозначающее запуск частичной синхронизации каждые 30 минут.
ldap_sync_resource	'0 0 0 * * *'	CRON выражение, по которому запускается синхронизация ресурсных систем (полная синхронизация) Значение по умолчанию - '0 0 0 * * *', обозначающее запуск полной синхронизации каждую полночь.

Параметр	Значение по умолчанию	Описание
ldap_clean_queues	'0 */30 * * * *'	CRON выражение, по которому запускается очистка необработанных элементов очередей на синхронизацию
ldap_partition_size	'1000'	Максимальное количество объектов, получаемых из ресурсных систем при каждом запросе.
pkcs12_mac_protection_algorithm	HmacPBESHA256	Алгоритм хеширования MAC контейнера PKCS12 Допустимые значения: HmacPBESHA256 HmacPBESHA1 Рекомендуется использовать алгоритм HmacPBESHA256; Устаревший алгоритм HmacPBESHA1
pkcs12_certificate_protection_algorithm	PBEWithHmacSHA256AndAES_256	Алгоритм хеширования для сертификата контейнера PKCS12 Допустимые значения: PBEWithHmacSHA256AndAES_256 PBEWithSHA1AndRC2_40 Рекомендуется использовать алгоритм PBEWithHmacSHA256AndAES_256; Устаревший алгоритм PBEWithSHA1AndRC2_40
Переменные окружения, используемые event-delivery-service		
email_schedule	'0 0 12 * * *'	CRON выражение, для запуска метода отправки почтовых уведомлений
Переменные окружения, используемые settings-service		
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: для стандартного провайдера (EMBEDDED) - 'RSA' и 'ECDSA' для провайдера КриптоПро (CRYPTO_PRO) - 'RSA' и 'GOST_R_34_10_2012'
initial_cryptography_key_bits	'4096'	Длина ключа (используется для технологического ЦС и сертификатов веб-сервера и администратора инициализации)
initial_cryptography_hash_algorithm	'SHA512'	Алгоритм хэширования (используется для технологического ЦС) Доступные для выбора значения алгоритмов хэширования: Для стандартного провайдера (EMBEDDED): для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'

Параметр	Значение по умолчанию	Описание
		для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'. Для провайдера КриптоПро (CRYPTO_PRO): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012' для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA384', 'SHA512'
initial_ca_common_name	'INITIAL_CA'	Subject DN сертификата технологического ЦС
initial_admin_principal	'INITIAL_ADMIN'	Имя учётной записи администратора инициализации
certificate_server_name	'server'	Шаблон имени файлов сертификата и закрытого ключа сертификата Web-сервера
issuers_name	'issuers'	Шаблон имени файла активных издателей
Переменные окружения, используемые logs-service		
archive_cron	'0 0 0 1 * *'	CRON выражение, по которому запускается архивация журнала событий
archive_enabled	'true'	Флаг: включена архивация. Возможные значения: true/false
archive_millis_ago	'15778800000'	Архивировать записи старше (значение в мс)
Переменные окружения, используемые security-service		
kerberos_enabled	'false'	Активация возможности аутентификации по kerberos-билету
session_max_count	'100'	Максимальное число сессий аккаунта (-1 - ограничение отключено) Значение по умолчанию: 100. Допустимые варианты указания предельного количества сессий для учетных записей: 1) натуральное число, представленное в десятичной системе счисления; 2) число «0»; 3) число «-1» (для выключения ограничения на количество сессий).
kerberos_service_principal	'#CHANGEIT'	Имя принципа, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_keytab_location	'#CHANGEIT'	Расположение keytab файла, содержащего тикет принципа, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_krb5_location	'#CHANGEIT'	Расположение файла конфигурации krb5.conf '#CHANGEIT' означает, что параметр не задан

Параметр	Значение по умолчанию	Описание
kerberos_ad_domain	'#CHANGEIT'	Имя подключаемого домена. '#CHANGEIT' означает, что параметр не задан
kerberos_ad_server	'#CHANGEIT'	Адрес сервера. Доступно указание сервера в формате ldap://<имя контроллера домена>.<домен> (для подключения по протоколу LDAP) и ldaps:// <имя контроллера домена>.<домен> (для подключения по протоколу LDAPS). По умолчанию еСА-СА в рамках работы с ресурсной системой по протоколу LDAPS будет доверять любому сертификату, предоставленному контроллером домена. '#CHANGEIT' означает, что параметр не задан
resource_type	'#CHANGEIT'	Тип PC (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN). При подключении к ресурсной системе Dynamic Directory указывать значение 'FREE_IPA'. '#CHANGEIT' означает, что параметр не задан
resource_base_dn	'#CHANGEIT'	Точка подключения ресурса. '#CHANGEIT' означает, что параметр не задан
ldap_enabled	'false'	Активация возможности аутентификации по логину/паролю пользователя ldap
ldap_sign_in_failure_max_count	'5'	Максимальное количество неудачных попыток аутентификации через LDAP
ldap_sign_in_failure_delay_millis	'3600000'	Время задержки после последней неудачной попытки аутентификации через LDAP
ldap_accounts_status_sync_enabled	'false'	Флаг автоматического управления статусами учетных записей, связанных с подключенными доменными субъектами, на основании их статуса в домене. Если параметр «ldap_accounts_status_sync_enabled» имеет значение «true», еСА-СА будет: 1) Блокировать активную УЗ в еСА-СА, если при синхронизации определено, что связанный с ней подключенный субъект заблокирован в PC. 2) Активировать заблокированную УЗ в еСА-СА, если при синхронизации определено, что связанный с ней подключенный субъект активен в PC. 3) Блокировать активную УЗ в еСА-СА, если при синхронизации определено, что связанный с ней субъект удален из PC (будет выполняться только при полной синхронизации). 4) Запрещать создавать УЗ в еСА-СА для заблокированного в PC субъекта.

Параметр	Значение по умолчанию	Описание
		5) Запрещать изменять вручную статус у УЗ, связанных с подключенными субъектами, в еСА-СА. Допустимые значения: true, false.
Дополнительные настройки для подключения к домену с усиленными требованиями по безопасности аутентификации		
channel_binding_enabled	'false'	Включает поддержку привязки к TLS-каналу (Channel Bindings). Только для подключения к домену по протоколу LDAPS. Флаг будет проигнорирован, если подключение осуществляется по протоколу LDAP. Включение данного флага требуется для удовлетворения требования домена к наличию токенов привязки канала при аутентификации по Kerberos.
ldap_starttls_enabled	'false'	Включает TLS-шифрование (директива STARTTLS) при подключении к домену по протоколу LDAP для аутентификации. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS. Включение данного флага требуется для возможности аутентификации доменных пользователей по логинам и паролям, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию
kerberos_qop_enabled	'false'	Включает механизмы QOP (Quality of Protection) для защиты данных внутри протокола Kerberos при подключении к домену по протоколу LDAP. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS. Включение данного флага требуется для возможности аутентификации доменных пользователей по Kerberos-билетам, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию
token_expire	'180000'	Время жизни JWT токена доступа в миллисекундах
refresh_expire	'86400000'	Время жизни JWT токена обновления в миллисекундах
sign_provider	'EMBEDDED'	Провайдер подписи (выбирается между стандартным - 'EMBEDDED', КриптоПро - 'CRYPTO_PRO' и Aladdin JCP - 'ALADDIN_JCP')
sign_key_algorithm	'RSA'	Алгоритм подписи ключа

Параметр	Значение по умолчанию	Описание
		Для стандартного провайдера доступны алгоритмы 'RSA' и 'ECDSA'. Для провайдера КриптоПро доступны алгоритмы 'RSA' и 'GOST_R_34_10_2012'. Для провайдера Aladdin JCP доступен алгоритм 'GOST_R_34_10_2012'.
sign_key_length	'2048'	Длина ключа подписи
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи Доступные для выбора значения алгоритмов хэширования: 1) для стандартного провайдера (EMBEDDED): для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' 2) для провайдера КриптоПро (CRYPTO_PRO): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012' для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' 3) для провайдера Aladdin JCP (ALADDIN_JCP): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012'
block_inactive_account_delay	'0'	Период неактивности в миллисекундах, после которого УЗ операторов Центра сертификации Aladdin eCA блокируются. Значение по умолчанию – 0, обозначающее отсутствие ограничения на неактивность учетных записей операторов. Операциями, обновляющими дату и время последней активности пользователя, являются: успешная аутентификация, включая аутентификацию в eCA-RA и eCA-VA; успешное обновление маркера доступа, включая его обновление в eCA-RA и eCA-VA.
block_inactive_account cron	'0 0 0 * * *'	Расписание запуска блокировки учетных записей операторов, период неактивности которых равен или превышает указанное в «block_inactive_account_delay» значение. Значение по умолчанию – '0 0 0 * * *' - запуск каждую полночь.
Параметры автоматического создания УЗ для субъекта РС		
ldap_automatic_accounts_enable	'false'	Поддержка автоматических учётных записей. Автоматические УЗ создаются на основе субъектов ресурсной системы, подключённой к eCA-SA на синхронизацию данных, при их успешной аутентификации через компоненты

Параметр	Значение по умолчанию	Описание
		еСА по доменному логину и паролю или по Kerberos-билету при условии вхождения данных субъектов в группу, GUID которой указан в параметрах <code>ldap_automatic_accounts_administrators_group_guid</code> или <code>ldap_automatic_accounts_operators_group_guid</code> . При включении флага требуется указание значения как минимум для одного из двух параметров: <code>ldap_automatic_accounts_administrators_group_guid</code> и <code>ldap_automatic_accounts_operators_group_guid</code> .
<code>ldap_automatic_accounts_administrators_group_guid</code>	'#CHANGEIT'	GUID группы домена, для членов которой их автоматические УЗ будут иметь роль «Администратор». '#CHANGEIT' означает, что параметр не задан
<code>ldap_automatic_accounts_operators_group_guid</code>	'#CHANGEIT'	GUID группы домена, для членов которой их автоматические УЗ будут иметь роль «Оператор». '#CHANGEIT' означает, что параметр не задан
Переменные окружения, используемые api-gateway-service		
<code>max_requests_count</code>	'30'	Максимальное число параллельных HTTP запросов. При превышении числа запросов в систему данного значения, для последующих запросов будет возвращаться HTTP код ошибки 429 (Слишком много запросов). Настраивается разработчиком еСА-СА, редактировать не следует
<code>actuator_authenticate</code>	'false'	Флаг доступности без аутентификации методов Spring Boot Actuator (используются для получения информации о сервисах еСА-СА) и метода GET <code>api/version</code> сервиса внешних интеграций (<code>external-integration-service</code>). При включении данного флага методы Spring Boot Actuator и GET <code>api/version</code> будут недоступны без аутентификации пользователя. Для аутентифицированного пользователя в любой роли (администратора и оператора) останутся доступными.
Параметры выполнения контроля целостности при запуске еСА-СА		
<code>integrity_check_startup_enabled</code>	'true'	Флаг контроля целостности при запуске еСА-СА. Допустимые значения: <code>true</code> , <code>false</code>
<code>integrity_check_fail_block_startup</code>	'true'	Флаг блокировки запуска служб еСА-СА при неуспешной проверке контроля целостности. Допустимые значения: <code>true</code> , <code>false</code>

Параметр	Значение по умолчанию	Описание
Данные продукта, отображаемые в окне авторизации		
login_window_product_name	'Aladdin Enterprise CA'	Название продукта, отображаемое в окне авторизации
login_window_component_name	'Центр сертификации'	Название компонента, отображаемое в окне авторизации
tab_title	'Aladdin Enterprise Certificate Authority'	Текст, отображаемый в заголовке вкладок браузера
Конфигурация БД		
use_credentials_from_config	'true'	<p>Флаг использования имени и пароля пользователя СУБД, указанных в параметрах <code>database_username</code> и <code>database_password</code> соответственно.</p> <p>Допустимые значения: <code>true</code>, <code>false</code>.</p> <p>Если данный параметр имеет значение <code>false</code>, еСА-СА будет требовать указывать имя и пароль пользователя СУБД при выполнении следующих скриптов:</p> <ul style="list-style-type: none"> - <code>install.sh</code>; - <code>uninstall.sh</code>; - <code>integrity_check.sh</code>; - <code>database_create.sh</code>; - <code>backup.sh</code>; - <code>restore.sh</code>. <p>Данные скрипты поддерживают следующие способы передачи в них имени и пароля пользователя СУБД:</p> <ul style="list-style-type: none"> - в параметрах запуска <code>--dbuser</code> или <code>-U</code> (имя пользователя СУБД) и <code>--dbpass</code> или <code>-P</code> (пароль пользователя СУБД); - в диалоговом режиме. Если не был указан какой-либо из параметров запуска, приведённых выше, скрипты при их запуске запросят ввод имени и/или пароля пользователя СУБД («Укажите имя пользователя СУБД» и/или «Укажите пароль пользователя СУБД») <p>Если параметр <code>use_credentials_from_config</code> имеет значение <code>true</code>, при работе скриптов в качестве имени и пароля пользователя СУБД будут использоваться значения параметров <code>database_username</code> и <code>database_password</code> конфигурационного файла. При этом скрипты будут игнорировать параметры запуска <code>--dbuser</code> (<code>-U</code>) и/или <code>--dbpass</code> (<code>-P</code>), уведомляя пользователя сообщением в терминале: «[WARN] Параметр запуска "название параметра" проигнорирован, так как включено использование имени и пароля пользователя СУБД из конфигурационного файла»</p>
Конфигурация еСА-СА		
strong_permissions_to_exclusion_files	'false'	Флаг установки прав доступа 640 на файлы-исключения.

Параметр	Значение по умолчанию	Описание
		<p>По умолчанию еСА-СА устанавливает права доступа 640 на все свои файлы, кроме исключений (см. список ниже) и утилиты «jsverify». Утилита «jsverify» имеет права 740 (-rwxr-----) для возможности ее запуска при выполнении КЦ.</p> <p>Исключения:</p> <ul style="list-style-type: none"> • файлы в каталоге «/opt/aecaCa/static» и его подкаталогах. Они представляют собой файлы клиентского компонента, доступ к ним необходим для Web-сервера. • файлы в каталоге «/opt/aecaCa/dist/webserver» и его подкаталогах. Данные файлы представляют собой конфигурации, подключаемые к Web-серверу. • файлы в каталоге «/opt/aecaCa/dist/certificates/ssl». В данном каталоге располагается сертификат Web-сервера, его закрытый ключ, а также файл с разрешенными издателями. <p>Если в данном параметре указано значение «true», права доступа 640 будут установлены на указанные выше файлы-исключения.</p> <p>Для обеспечения сертифицированной среды функционирования присвойте параметру значение 'true'</p>

4.3 Настройка веб-сервера при ограничении доступа к его файлам

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

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

4.4 Создание и настройка базы данных

Перед установкой еСА-СА 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 4.4.1.
- 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 4.4.2, а для Jatoba - в 4.4.3.

База данных предназначена для хранения информации:

- об учётных 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.

4.4.1 Создание и настройка базы данных в автоматическом режиме

- Предварительно необходимо:
 - распаковать инсталляционный пакет программного компонента в соответствии с подразделом 4.1 настоящего документа;
 - указать параметры создаваемой базы данных в конфигурационном файле `/opt/aecaCa/scripts/config.sh` (см. подраздел 4.2 настоящего руководства).

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

- Запустите скрипт создания и настройки базы данных с параметрами по умолчанию выполнив следующую команду с правами суперпользователя²:

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

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

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

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

² Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).

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

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

4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме

Требования к настройке предварительно установленной СУБД PostgreSQL:

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

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите PostgreSQL выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

```
-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 4.2).

Внимание! Если в качестве операционной системы в среде функционирования eCA-CA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД¹, при использовании локальной СУБД имя пользователя СУБД должно отличаться от имени пользователя ОС, указанного в параметре `aeca_user` конфигурационного файла `/opt/aecaCa/scripts/config.sh`, (см. подраздел 4.2 настоящего руководства).

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

- Задайте пароль пользователю выполнив команду:

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

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

- 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 4.2).

- 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
```

- Перезапустите СУБД PostgreSQL выполнив команду с правами суперпользователя:

```
systemctl restart postgresql
```

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

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

где aecaca - имя созданной базы данных.

• Если в качестве операционной системы в среде функционирования eCA-CA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД¹, при использовании локальной СУБД дополнительно необходимо:

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

4.4.3 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.

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

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите Jatoba выполнив команду:

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

Добавьте запуск Jatoba в автозагрузку выполнив команду:

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

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

РЕД ОС и РОСА «ХРОМ» 12
Сервер

```
-u postgres psql
```

SberLinux OS Server

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

Astra Linux SE

```
-u postgres psql
```

Альт Сервер

```
- 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.

Внимание! Если в качестве операционной системы в среде функционирования eCA-CA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД¹, при использовании локальной СУБД имя пользователя СУБД должно отличаться от имени пользователя ОС, указанного в параметре **aeca_user** конфигурационного файла **/opt/aecaCa/scripts/config.sh**, (см. подраздел 4.2 настоящего руководства).

- Задайте пароль пользователю, выполнив команды:

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

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

- Создайте базу данных выполнив команду:

```
CREATE DATABASE aecaca;
```

где **aecaca** - задаваемое имя базы данных.

- 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
```

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

- Перезапустите СУБД Jatoba выполнив команду с правами суперпользователя:

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

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

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

где `aecaca` - имя созданной базы данных.

- Если в качестве операционной системы в среде функционирования еСА-СА используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД¹, при использовании локальной СУБД дополнительно необходимо:

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

4.5 Установка программы

Для инициализации процесса установки еСА-СА необходимо запустить скрипт с правами суперпользователя²:

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

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

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!"
```

После инициализации процесса установки интерактивный инсталлятор будет запущен и пользователю будет предложено (в случае, если ранее на сервере был установлен еСА-СА):

- Установить еСА-СА.
- Установить обновление еСА-СА.
- 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`;
- `срnginx`.

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

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

² Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).

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, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server по пути `/etc/httpd`; для Альт Сервера конфигурация `apache` располагается по пути `/etc/httpd2/conf`; конфигурация `срnginx` располагается по пути `/etc/opt/cprocp/cpnginx`).

В процессе установки программы 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 еСА-СА в базу данных¹;
- 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 программы:

- 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 ГОСТ²) - 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).

Внимание! Технологический Центр сертификации использовать для выпуска сертификатов запрещено.

После первичной установки еСА-СА 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 с правами суперпользователя:

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

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

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

² Маркеры доступа будут подписаны по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256 бит.

4.6 Порядок совместной установки компонентов программного средства на одном сервере

В Центре сертификатов доступа поддерживается совместная работа eCA-CA, eCA-RA и eCA-VA (далее в разделе - компоненты программного средства) на одном хосте. Также поддерживается совместная работа двух выбранных компонентов программного средства на одном хосте.

Порядок совместной установки всех компонентов программного средства на одном хосте ¹:

- Выполните подготовку среды функционирования компонентов программного средства на хосте (см. раздел 3 настоящего руководства).
- Введите хост в домен ресурсной системы в соответствии с документацией производителя используемой ОС.
- Определите имя хоста (hostname) для каждого компонента программного средства. Имя хоста компонента формируется путём добавления к реальному сетевому имени хоста, на котором выполняется совместная установка компонентов программного средства, префикса, идентифицирующего данный компонент. Например, имя хоста `ra.eca-host` для eCA-RA, в котором `ra` это префикс, а `eca-host` это реальное имя хоста (hostname), на котором выполняется совместная установка компонентов программного средства.
- Отредактируйте файл `etc/hosts`, сопоставив в нем имена хостов компонентов программного средства, включая доменную часть, IP-адресу `127.0.0.1`.

В указанном ниже примере содержания файла `etc/hosts` префикс `ca` идентифицирует eCA-CA, `va` - eCA-VA, `ra` - eCA-RA, а `eca-host.ad.local` - это полное доменное имя хоста (FQDN), на котором выполняется совместная установка компонентов программного средства.

```
127.0.0.1 ca.eca-host.ad.local
127.0.0.1 va.eca-host.ad.local
127.0.0.1 ra.eca-host.ad.local
```

При совместной установке компонентов программного средства в среде ОС Astra Linux Special Edition и взаимодействии с доменной службой каталогов Samba DC, Альт Домен или MS AD заполнение файла `etc/hosts` не выполняется. При этом на в DNS-сервисе домена ресурсной системы необходимо добавить DNS-записи, сопоставив выбранные имена хостов компонентов программного средства IP-адресу хоста, на котором выполняется совместная установка компонентов программного средства.

Формат команды для добавления DNS-записи на контроллере домена. Команду надо выполнять с правами суперпользователя:

```
samba-tool dns add [IP-адрес контроллера домена] [Домен] [Имя хоста компонента] A [IP-адрес хоста] -U [Имя учётной записи администратора домена]
```

Пример команды:

```
sudo samba-tool dns add 192.168.86.129 ad.local ca.eca-host A 192.168.86.138 -U admin_dc
```

- Установите eCA-CA, указав в конфигурационном файле в параметре `hostname` выбранное для eCA-CA имя хоста, включая доменную часть (см. разделы 4.1-4.5 настоящего руководства) (например, `ca.eca-host.ad.local`).
- Установите сертификат администратора инициализации технологического Центра сертификации (см. раздел 6 настоящего руководства):
 - Контейнер закрытого ключа `INITIAL_ADMIN.p12` в хранилище сертификатов веб-браузера, если сертификат был выпущен с использованием алгоритмов RSA или ECDSA.

¹ Аналогичным образом выполняется совместная установка двух выбранных компонентов на одном сервере.

- Контейнер закрытого ключа `INITIAL_ADMIN_GOST.p12` в личное хранилище пользователя с помощью утилиты `cptools` из состава СКЗИ «КриптоПро CSP, если сертификат был выпущен с использованием алгоритмов ГОСТ.

- Подключитесь к веб-интерфейсу еСА-СА (см. раздел 6 настоящего руководства) и пройдите аутентификацию с помощью сертификата администратора инициализации. В качестве адреса еСА-СА необходимо указать имя хоста компонента, включая доменную часть (например, `https://ca.eca-host.ad.local`).

- Установите лицензию и выполните инициализацию еСА-СА (документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority» (далее в разделе - часть 2 руководства администратора)).

- Выполните подключение ресурсной системы к еСА-СА (см. часть 2 руководства администратора).

- Создайте учетную запись пользователя локального ресурса (см. часть 2 руководства администратора) или субъекта ресурсной системы (см. часть 2 руководства администратора) с ролью «Администратор» для управления компонентами программного средства и выпустите для нее сертификат с закрытым ключом по шаблону «User» (см. часть 2 руководства администратора).

- Создайте субъект локальной ресурсной системы для веб-сервера центра сертификации, указав в атрибутах «Common Name» и «DNS Name» имя хоста компонента, выбранное для еСА-СА, включая доменную часть (см. часть 2 руководства администратора), выпустите для созданного субъекта сертификат с закрытым ключом по шаблону «WEB-Server» и установите данный сертификат в качестве сертификата веб-сервера еСА-СА (см. часть 2 руководства администратора).

- Создайте субъект локальной ресурсной системы для веб-сервера еСА-РА, указав в атрибутах «Common Name» и «DNS Name» имя хоста компонента, выбранное для еСА-РА, включая доменную часть (см. часть 2 руководства администратора) и выпустите для созданного субъекта сертификат с закрытым ключом по шаблону «WEB-Server» (см. часть 2 руководства администратора).

- Создайте для еСА-РА учетную запись пользователя с ролью «Администратор» и выпустите для нее сертификат с закрытым ключом по шаблону «User» (см. часть 2 руководства администратора).

- Создайте субъект локальной ресурсной системы для веб-сервера еСА-ВА, указав в атрибутах «Common Name» и «DNS Name» имя хоста компонента, выбранное для еСА-ВА, включая доменную часть (см. часть 2 руководства администратора) и выпустите для созданного субъекта сертификат с закрытым ключом по шаблону «WEB-Server» (см. часть 2 руководства администратора).

- Создайте для еСА-ВА учетную запись пользователя с ролью «Администратор» и выпустите для нее сертификат с закрытым ключом по шаблону «User» (см. часть 2 руководства администратора). Данный сертификат будет использоваться в дальнейшем для подключения к еСА-СА.

- Создайте пользователя-службу HTTP и keytab-файл¹ на контроллере домена ресурсной системы:

- Для еСА-РА (см. документ «Руководство администратора. Часть 5. Центр регистрации Aladdin Enterprise Registration Authority» (далее в разделе - часть 5 руководства администратора).
- Для еСА-ВА (см. документ «Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority» (далее в разделе - часть 4 руководства администратора).

При совместной установке компонентов в среде ОС Astra Linux Special Edition и взаимодействии с доменной службой каталогов Samba DC, Альт Домен или MS AD создайте только один keytab-файл. При создании keytab-файла в соответствующей для доменной службы каталогов команде укажите полное доменное имя хоста (FQDN), на котором выполняется совместная установка компонентов программного средства (например, `eca-host.ad.local`).

¹ Keytab-файл используется для аутентификации доменных пользователей в еСА-РА с использованием Kerberos без ввода пароля.

Настройку HTTP-службы в доменной службе каталогов ALD PRO необходимо выполнять через интерфейс FreeIPA.

- При совместной установке для eCA-CA и eCA-RA в среде ОС Astra Linux Special Edition 1.7 убедитесь, что в ОС имеется учётная запись пользователя с именем, совпадающим с именем пользователя СУБД (см. значение параметра `database_username` в конфигурационном файле eCA-CA). Если такой учётной записи нет, то создайте её.

- Установите eCA-RA (см. часть 5 руководства администратора), указав в конфигурационном файле:

- В параметре `hostname` выбранное для eCA-RA имя хоста.
- В параметре `aeca_ca_host` выбранное для eCA-CA имя хоста.
- Значения параметров `aeca_user`, `aeca_group` и `database_username` должны отличаться от значений этих же параметров в конфигурационном файле eCA-CA.

Остальные параметры конфигурационного файла указываются в соответствии с частью 5 руководства администратора.

- Установите eCA-VA (см. часть 4 руководства администратора), указав в конфигурационном файле:

- В параметре `hostname` выбранное для eCA-VA имя хоста.
- Значения параметров `aeca_user`, `aeca_group` и `database_username` должны отличаться от значений этих же параметров в конфигурационных файлах eCA-CA и eCA-RA.

Остальные параметры конфигурационного файла указываются в соответствии с частью 4 руководства администратора.

5 ЗАПУСК И ОСТАНОВКА ПРОГРАММЫ

еСА-СА запускается автоматически:

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

Для проверки состояния еСА-СА в терминале выполните команду с правами суперпользователя:

```
systemctl status aeca-ca.service
```

Возможные варианты ответа:

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

Для проверки автозагрузки программы выполните команду с правами суперпользователя:

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

Для добавления программы в автозагрузку выполните команду с правами суперпользователя:

```
systemctl enable aeca-ca.service
```

Для запуска программы выполните команду с правами суперпользователя:

```
systemctl start aeca-ca.service
```

Для перезапуска программы выполните команду с правами суперпользователя:

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

При запуске еСА-СА выполняются следующие проверки:

- Проверка возможности подключения к базе данных. Если не удаётся подключиться к базе данных, то программа не запускается.
- Проверка соответствия номера своей сборки и значения номера сборки, указанной в базе данных:
 - Если в базе данных отсутствует номер сборки, то программа не запускается.
 - Если номер сборки не равен номеру сборки программы, то программа завершает запуск с ошибкой «Текущая версия схемы базы данных не позволяет выполнить запуск службы. Текущая версия схемы базы данных: X.X.X.X. Необходимая версия схемы базы данных: Y.Y.Y.Y.», где «X.X.X.X» - номер сборки указанный в базе данных, а «Y.Y.Y.Y» - номер сборки запускаемой программы.
- Контроль целостности контейнеров закрытого ключа всех Центров сертификации программы.
- Контроль целостности следующих файлов:
 - /opt/aecaCa/samples/*;
 - /opt/aecaCa/scripts/* (кроме "config.sh" и "jc_checksum");
 - /opt/aecaCa/services/* (все .jar файлы во всех подкаталогах);
 - /opt/aecaCa/static/*;
 - /opt/aecaCa/bin/*.

еСА-СА блокирует дальнейший запуск служб в случае неуспешной проверки контроля целостности. Настройка параметров выполнения контроля целостности осуществляется в конфигурационном файле.

Модули еСА-СА запускаются поочерёдно в порядке, приведённом в таблице 8 ниже.

Таблица 8 — Модули программы

Порядок запуска	Исполняемый файл	Наименование	Назначение
1	discovery-service.jar	Модуль обнаружения	Выполняет роль реестра сервисов, содержит такую информацию как IP-адреса и порты сервисов
2	logs-service.jar	Модуль журнала событий	Обеспечивает фиксацию событий в журнале и получение событий из журнала, просмотр и поиск записей журнала, экспорт и архивацию записей журнала
3	storage-service.jar	Модуль хранения данных	Обеспечивает хранение и управление файлами сертификатов
4	event-delivery-service.jar	Модуль оповещения пользователей	Предназначен для оповещения посредством рассылки уведомлений по адресам электронной почты владельцев сертификатов
5	certificate-authority-service.jar	Модуль сертификатов	Обеспечивает создание сертификата, подпись сертификата (включая цепочки сертификатов), генерацию CRL, валидацию сертификата, взаимодействие уполномоченного пользователя с контейнерами и точками распространения.
6	license-service.jar	Модуль лицензирования	Обеспечивает управление лицензиями программы
7	external-integration-service.jar	Модуль внешних интеграций	Предназначен для предоставления пользователям или внешним системам доступа к программным интерфейсам, реализуемым другими модулями. (Публичный API)
8	security-service.jar	Модуль безопасности	Предназначен для идентификации и аутентификации пользователей программы, управления учётными записями пользователей программы, предоставления информации о пользователях программы
9	settings-service.jar	Модуль настроек	Обеспечивает управление жизненным циклом программы, её состоянием и параметрами (данные о продукте, конфигурация серверного сертификата SSL, разрешённые издатели сертификатов)
10	api-gateway-service.jar	Модуль проксирования	Предназначен для перенаправления поступающих в программу запросов в нужный сервис (на основании данных, указанных в URL запроса), а также для перенаправления запросов к модулю безопасности с целью аутентификации пользователя

Для завершения работы еСА-СА выполните команду с правами суперпользователя:

```
systemctl stop aeca-ca.service
```

еСА-СА при остановке отключает от веб-сервера свою конфигурацию. В результате отключения от веб-сервера конфигурации закрываются порты¹, используемые для доступа к программе (определяются параметрами «`http_port`» и «`https_port`» конфигурационного файла `/opt/aecaCa/scripts/config.sh`), если данные порты не используются иными программами.

¹ Порты будут закрыты только в том случае, если они были открыты еСА-СА.

6 ПОДКЛЮЧЕНИЕ К ВЕБ-ИНТЕРФЕЙСУ

6.1 Общие сведения

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

Подключение к веб-интерфейсу «eCA-SA 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 6.2.

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 программы (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 репозиторий ОС Astra Linux SE, Альт Сервер, РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.

6.2 Установка сертификата администратора инициализации

После установки eCA-SA 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 указан в файле `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.txt`.

Установите сертификат администратора инициализации `INITIAL_ADMIN.p12` (имя контейнера по умолчанию) в доверенное хранилище сертификатов веб-браузера¹.

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

¹ Сертификат администратора инициализации из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, устанавливается в личное хранилище пользователя с помощью утилиты `cptools` из состава СКЗИ «КриптоПро CSP» (см. подраздел 6.1).

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

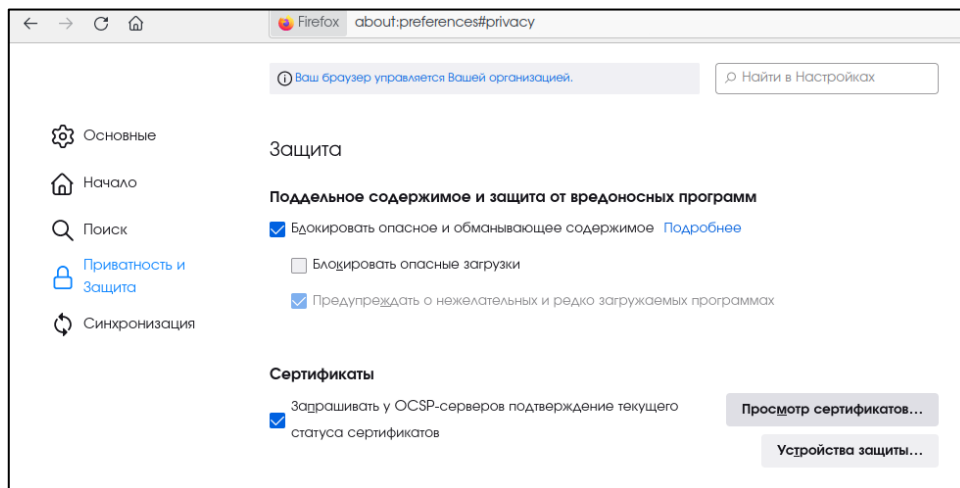


Рисунок 1 - Окно настроек браузера

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

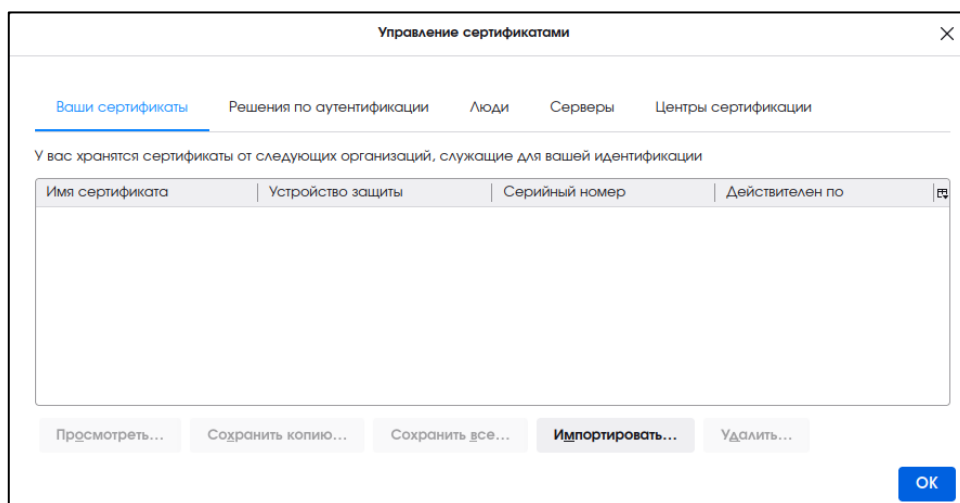


Рисунок 2 - Окно управления сертификатами

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

Внимание! Запрещается каким-либо образом удалять сертификат технологического центра сертификации «INITIAL_CA», созданного при развёртывании Центра сертификации.

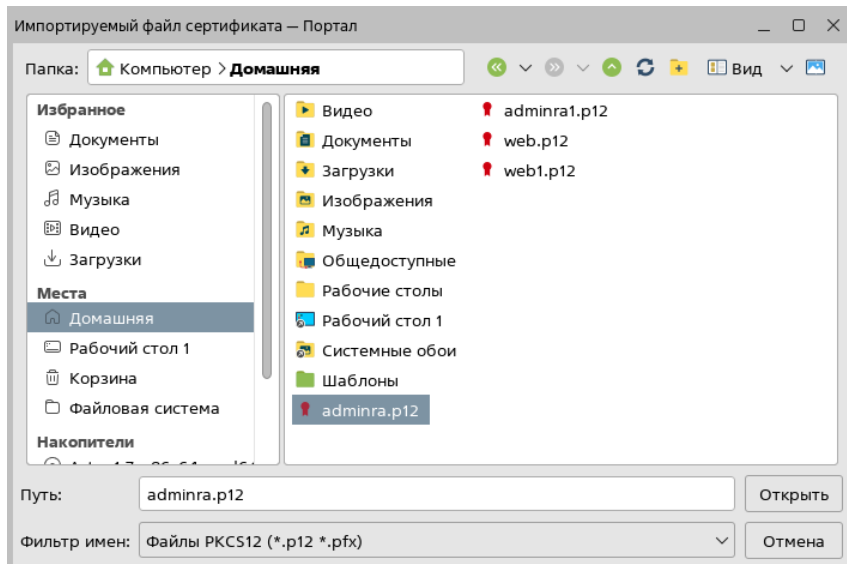


Рисунок 3 - Окно выбора импортируемого файла сертификата

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

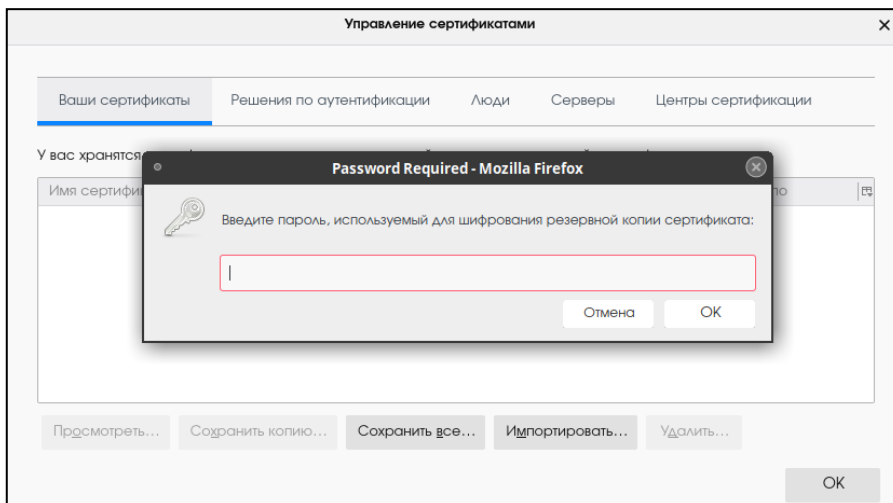


Рисунок 4 - Окно ввода пароля от контейнера

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

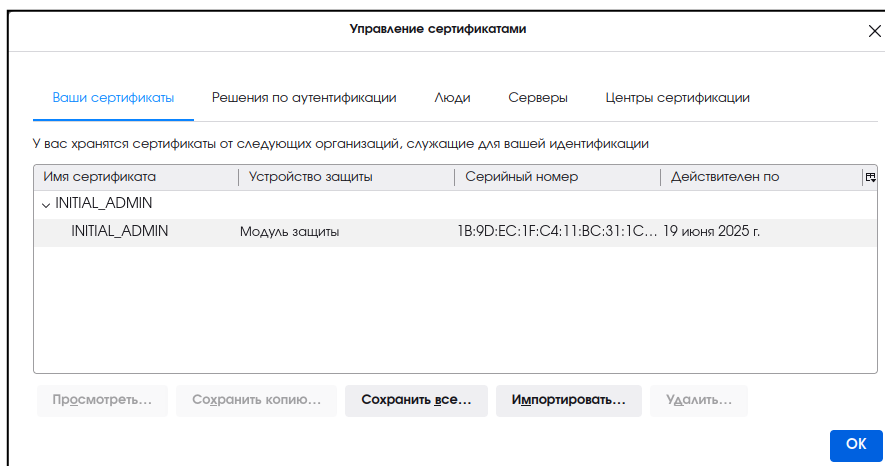


Рисунок 5 - Окно «Управление сертификатами»

6.3 Настройка подключения к веб-интерфейсу

Порядок подключения к веб-интерфейсу:

- Если параметр `strong_permissions_to_exception_files` конфигурационного файла имеет значение `true` запускать веб-браузер с правами суперпользователя или пользователя аеса.
- Если параметр `strong_permissions_to_exception_files` конфигурационного файла имеет значение `false` запустите веб-браузер с обычными правами.
- В адресной строке введите IP-адрес или доменное имя сервера, на котором установлен еСА-СА. Например, `https://172.22.5.21`.
- В открывшемся окне выберите сертификат администратора инициализации (см. Рисунок 6) и нажмите кнопку <ОК>.

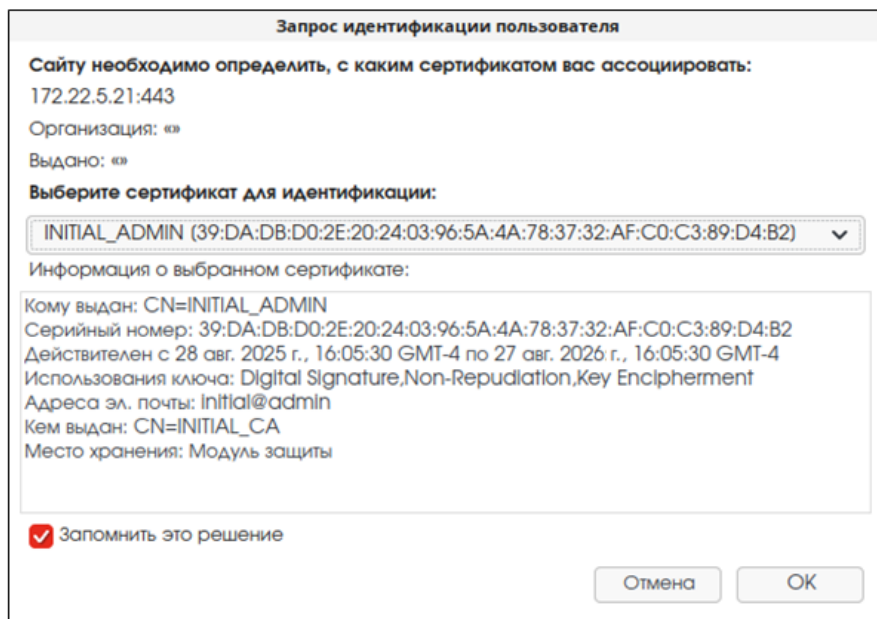


Рисунок 6 — Окно выбора сертификата

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

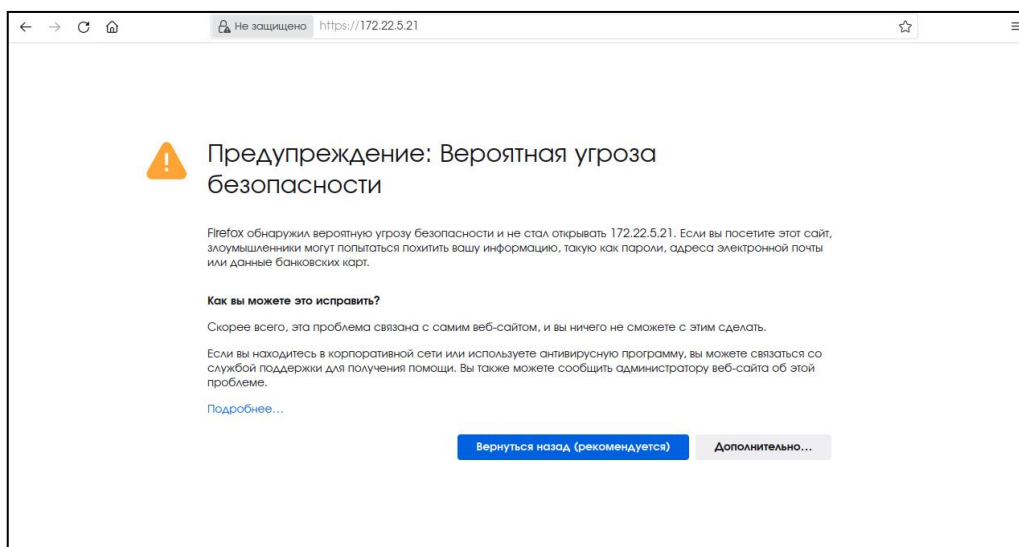


Рисунок 7 - Страница с предупреждением системы безопасности

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

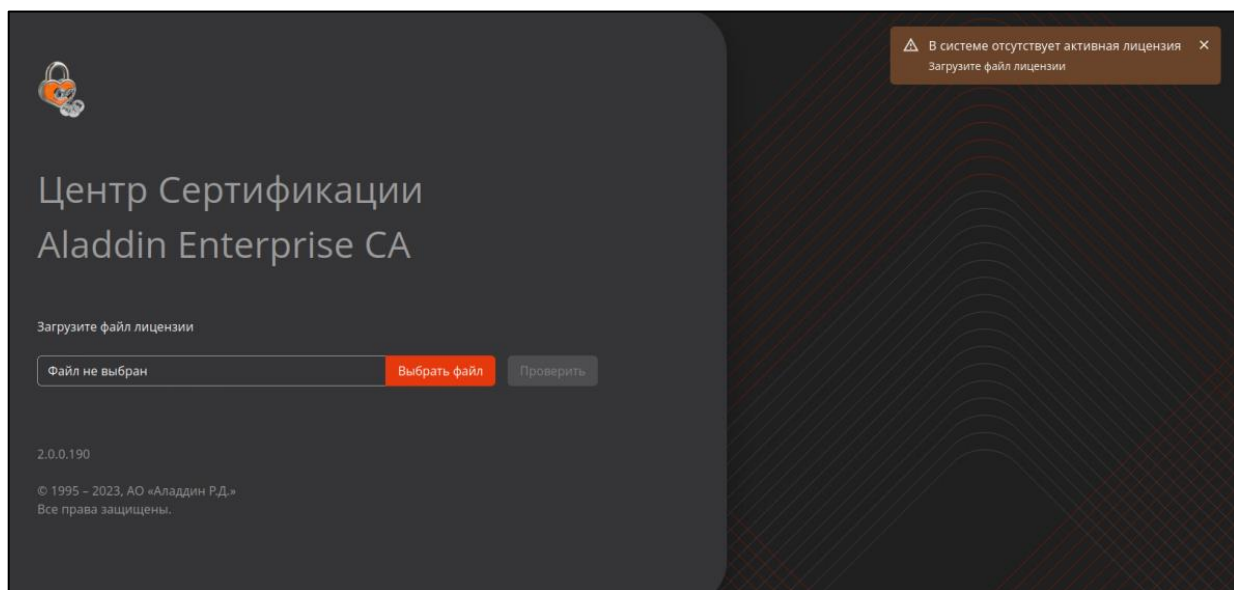


Рисунок 8 — Окно инициализации Центра сертификации. Шаг 1 - выбор лицензии

7 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПРОГРАММЫ

Контроль целостности исполняемых файлов еСА-СА необходим для отслеживания неизменности и контроля состояния файлов, перечень которых приведен 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 подкаталогов;
- все файлы в каталоге «`/opt/aecaCa/static`» и его подкаталогов;
- все файлы в каталоге «`/opt/aecaCa/bin`» и его подкаталогов;
- все файлы в каталоге «`/opt/aecaCa/digsig`» и его подкаталогов.

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 еСА-СА средствами утилиты «Утилита контроля целостности 2.0» - `jcverify`¹.

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

Файл с эталонами контрольными суммами `jc_checksum` формируется при сборке программы с помощью утилиты контроля целостности `jcverify`.

Для выполнения контроля целостности исполняемых файлов запустите скрипт `integrity_check.sh` с правами суперпользователя:

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

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

В данном случае будет использован файл с эталонами контрольных сумм по умолчанию - `/opt/aecaCa/scripts/jc_checksum`.

После завершения работы скрипта необходимо проанализировать полученные данные.

При успешной проверке целостности будет выведено сообщение: «Успешная проверка контрольных сумм».

При ошибке проверки целостности будет выведено сообщение «Неуспешная проверка контрольных сумм», а также сообщение об ошибке, генерируемое утилитой `jcverify`.

¹ Данная утилита включена в состав Центра сертификации (каталог «`/opt/aecaCa/bin/jcverify`»).

8 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ

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

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

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- О работе сервисов программы (файлы в формате `.log`).
- Конфигурационный файл `/opt/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 9.

Таблица 9 - Данные системных логов

Системный лог	РЕД ОС, РОСА «ХПОМ» 12 Сервер и SberLinux OS Server	Astra Linux SE	Альт 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/httpd/</code>	-	-	+

При включённом 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 еСА-СА.

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

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

```
cd /`папка размещения архива`
```

Для выполнения сбора диагностической информации запустите скрипт от имени суперпользователя:

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

Сформированный архив в формате `tar.gz` с диагностической информацией будет сохранён в каталог, из которого запускался скрипт.

Для вывода текущей рабочей директории используйте команду: `pwd`

9 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ ПРОГРАММЫ

9.1 Резервное копирование данных

Резервное копирование данных eCA-CA выполняется при помощи скрипта `/opt/aecaCa/scripts/backup.sh`.

Резервная копия включает:

- обязательно:
 - сертификаты и ключи веб-сервера, а также для файл, содержащий сертификаты разрешённых издателей, из каталога, указанного в параметре `certificates_ssl_path` конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию: `/opt/aeca/dist/certificates/ssl`);
 - контейнеры закрытых ключей центров сертификации из каталога, указанного в параметре `cryptotoken_path` конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию `/opt/aeca/dist/cryptotoken`);
 - ключи для шифрования пароля пользователя СУБД в конфигурационном файле (файл `/opt/aecaCa/scripts/key`);
 - конфигурационный файл программы `/opt/aecaCa/scripts/config.sh`;
- опционально: базу данных программы, указанную в параметре `database_name` конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию `aecaca`).

Содержимое каталога, указанного в параметре `certificates_account_path` конфигурационного файла, в том числе контейнер закрытого ключа администратора инициализации и пароль от него, не будет включено в состав резервной копии. При восстановлении из резервной копии текущее содержимое данного каталога не будет изменено. Для резервного копирования контейнера закрытого ключа администратора инициализации и пароля от него используйте организационно-технические меры, например, сохраните на резервном носителе контейнер и пароль от него после их формирования (в результате чистой установки или восстановления доступа с помощью скрипта `restore_access`).

Путь к каталогу, в котором создаются резервные копии, определяется значением, указанным в параметре `backup_path` конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aecaCa/dist/backup/`).

Имена файлов резервных копий имеют следующий формат:

- `aeca-ca-backup-«дата-время-создания».tar` — для резервных копий, содержащих базу данных;
- `aeca-ca-backup-«дата-время-создания»-nodb.tar` — для резервных копий, не содержащих базу данных.

Параметры запуска скрипта `/opt/aecaCa/scripts/backup.sh` представлены в таблице 10.

Таблица 10 — Параметры запуска скрипта `/opt/aecaCa/scripts/backup.sh`

Параметр	Описание
<code>-nodb</code>	При указании параметра скрипт не вносит базу данных в создаваемую резервную копию
<code>--dbuser имя_пользователя_СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-U имя_пользователя_СУБД</code>	То же, что <code>--dbuser имя_пользователя_СУБД</code>
<code>--dbpass пароль_пользователя_СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-P пароль_пользователя_СУБД</code>	То же, что <code>--dbpass пароль_пользователя_СУБД</code>

Для создания резервной копии:

- Запустите скрипт `/opt/aecaCa/scripts/backup.sh` с правами суперпользователя и необходимыми параметрами (см. таблицу 10).
- При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.
- Дождитесь завершения создания резервной копии. В случае успешного создания резервной копии будет выведено сообщение «[BACKUP] Резервное копирование завершено», иначе — сообщение об ошибке.

Пример запуска скрипта `backup.sh` без параметров с правами суперпользователя:

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

9.2 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 с правами суперпользователя:

```
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.

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`

9.3 Восстановление данных из резервной копии

Восстановление данных eCA-CA из резервной копии выполняется при помощи скрипта `/opt/aecaCa/scripts/restore.sh`.

Скрипт `/opt/aecaCa/scripts/restore.sh` поддерживает следующие способы передачи в него пути к файлу с резервной копией:

- в параметре запуска `--backup` или `-B`;
- в диалоговом режиме. Если не указан параметр запуска `--backup` или `-B`, скрипт при запуске запросит ввод пути к резервной копии («Укажите путь до резервной копии»).

Параметры запуска скрипта `/opt/aecaCa/scripts/restore.sh` представлены в таблице 11.

Таблица 11 — Параметры запуска скрипта `/opt/aecaCa/scripts/restore.sh`

Параметр	Описание
<code>--backup</code> путь_к_файлу_резервной_копии	Параметр позволяет передать путь к резервной копии при запуске скрипта
<code>-B</code> путь_к_файлу_резервной_копии	Параметр позволяет передать путь к резервной копии при запуске скрипта. Параметр <code>-B</code> аналогичен параметру <code>--backup</code>

Параметр	Описание
<code>-nodb</code>	При указании параметра скрипт не восстанавливает базу данных из резервной копии
<code>--dbuser имя_пользователя_СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-U имя_пользователя_СУБД</code>	То же, что <code>--dbuser имя_пользователя_СУБД</code>
<code>--dbpass пароль_пользователя_СУБД</code>	см. описание параметра <code>use_credentials_from_config</code> в 4.2
<code>-P пароль_пользователя_СУБД</code>	То же, что <code>--dbpass пароль_пользователя_СУБД</code>

Для восстановления данных из резервной копии:

- Запустите скрипт `/opt/aecaCa/scripts/restore.sh`, с правами суперпользователя и необходимыми параметрами (см. таблицу 11).
- При необходимости укажите в диалоге:
 - имя и пароль пользователя СУБД (см. описание параметра `use_credentials_from_config` в 4.2).
 - путь к резервной копии.
- Дождитесь завершения восстановления из резервной копии. В случае успешного восстановления будет выведено сообщение «[RESTORE] Восстановление из резервной копии завершено», иначе — сообщение об ошибке.

Пример запуска скрипта `/opt/aecaCa/scripts/restore.sh` без параметров с правами суперпользователя:

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

Возобновления доступа после восстановления из резервной копии выполняется одним из двух способов:

При помощи соответствующих резервной копии контейнера закрытого ключа администратора инициализации и пароля от него.

При помощи скрипта `restore_access`. Данный скрипт пересоздаст УЗ администратора инициализации и контейнер закрытого ключа для неё. Старая УЗ и её сертификат для доступа в результате выполнения скрипта станут не валидными.

10 ВОССТАНОВЛЕНИЕ ДОСТУПА К ПРОГРАММЕ

Восстановление доступа к eCA-CA необходимо выполнить в случае отсутствия ранее созданной резервной копии и блокировки доступа к eCA-CA, возникшей в результате:

- Некорректного удаления технологических составляющих.
- Истечения срока действия сертификата Центра сертификации.
- Истечения срока действия сертификата администратора.
- Удаления Корневого Центра сертификации с автоматическим удалением активного Подчинённого Центра сертификации.

Для восстановления доступа к eCA-CA запустите скрипт от имени суперпользователя:

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

В результате выполнения скрипта восстановления доступа к программе будут созданы:

4. Технологический корневой центр сертификации с параметрами, полученными из конфигурационного файла:
 - криптопровайдер алгоритма ключа и хэш-алгоритма ЦС (параметр «initial_cryptography_provider»);
 - CN в сертификате технологического ЦС (параметр «initial_ca_common_name»);
 - хэш-алгоритм сертификата технологического ЦС (параметр «initial_cryptography_hash_algorithm»);
 - алгоритм ключа сертификата технологического ЦС (параметр «initial_cryptography_key_algorithm»);
 - длина ключа сертификата технологического ЦС (параметр «initial_cryptography_key_bits»).

Сертификат технологического корневого центра сертификации будет выпущен по шаблону «Root CA».

После создания технологический корневой центр сертификации будет активирован.

5. Учётная запись администратора инициализации с логином, указанным в параметре «initial_admin_principal» конфигурационного файла eCA-CA, при её отсутствии (определение наличия существующей учётной записи администратора инициализации выполняется путём поиска учётной записи с логином, аналогичным указанному в параметре «initial_admin_principal» конфигурационного файла eCA-CA). Если учётная запись администратора инициализации уже существует на момент запуска скрипта «restore_access.sh» и данная учётная запись заблокирована, в результате работы скрипта учётная запись администратора инициализации будет активирована.
6. Контейнер закрытого ключа для администратора инициализации с параметрами, полученными из конфигурационного файла:
 - CN в сертификате администратора инициализации (параметр «initial_admin_principal»);
 - алгоритм ключа сертификата администратора инициализации (параметр «initial_cryptography_key_algorithm»);
 - длина ключа сертификата администратора инициализации (параметр «initial_cryptography_key_bits»).

Контейнер будет создан в каталоге, указанном в параметре «certificates_account_path».

Пароль от созданного контейнера сертификата администратора инициализации будет записан в каталог, указанный в параметре «certificates_account_path», в текстовый файл с названием формата «initial_admin_principal.txt», где «initial_admin_principal» — значение соответствующего параметра конфигурационного файла.

Сертификат администратора инициализации будет выпущен по шаблону «User» на технологическом корневом центре сертификации (см. пункт 4).

7. Технологический сертификат Web-сервера с параметрами, полученными из конфигурационного файла:
 - алгоритм ключа сертификата Web-сервера (параметр «initial_cryptography_key_algorithm»);
 - длина ключа сертификата Web-сервера (параметр «initial_cryptography_key_bits»).

Технологический сертификат будет установлен. Технологический сертификат Web-сервера будет выпущен по шаблону «WEB-Server» на технологическом корневом центре сертификации (см. пункт 4).

Для дальнейшего доступа к Центру сертификации выполните аутентификацию по выпущенному сертификату администратора инициализации.

11 ОБНОВЛЕНИЕ ПРОГРАММЫ

Обновление базы данных и модулей еСА-СА обеспечивает актуальность версии программного обеспечения.

При обновлении программы решаются следующие задачи:

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

Компания ведёт учёт покупателей Центра сертификатов доступа. Выполняется регистрация следующей информации:

- наименование организации;
- адрес организации;
- контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).

Уведомление пользователей о выпуске новой версии Центра сертификатов доступа выполняется путём публикации информации на официальном сайте АО «Аладдин Р.Д.» и (или) рассылкой электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счёт применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлами новой версии программного средства может предоставляться обновлённая документация для использования программы.

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

- С использованием электронной почты.
- Путём загрузки с веб-сайта АО «Аладдин Р.Д.».

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

Контроль целостности файлов для обновления программы выполняется путём расчёта КС полученных установочных пакетов (дистрибутивов) с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0» или программного средства «Утилита контроля целостности 2.0» из состава программного средства, и её сравнением со значением контрольной суммы для этого обновления (см. подраздел 1.5.2 настоящего документа).

Внимание! На случай, если во время процесса обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию данных программы (см. раздел 9 настоящего руководства).

Схема обновления программного средства представлена на рисунке ниже.

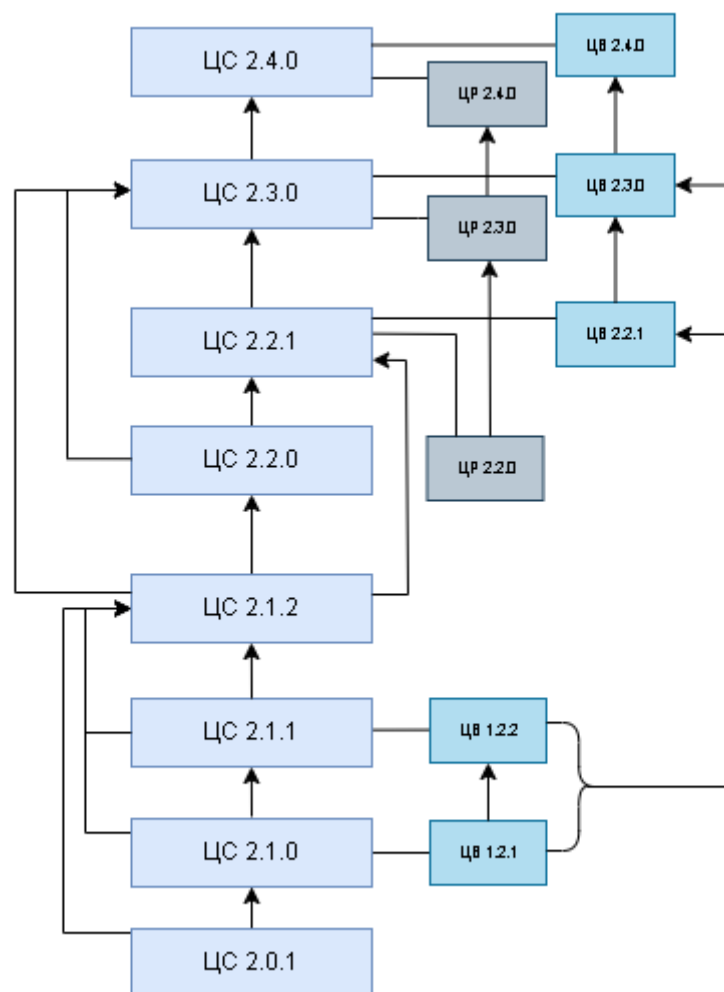


Рисунок 9 — Схема обновления программы

Порядок обновления программы:

- Перенесите дистрибутив с новой версией программы на компьютер с установленным eCA-CA.
- Проверьте целостность дистрибутива путём подсчёта КС (см. подраздел 1.5.2 настоящего документа);
- Выполните распаковку установочного пакета:
 - для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server командой с правами суперпользователя: `dnf install aeca-*.rpm`;
 - для ОС Astra Linux SE командой с правами суперпользователя: `dpkg -i aeca-*.deb`;
 - для Альт Сервер командой с правами суперпользователя: `apt-get install aeca-*.rpm`.
- Запустите процесс установки продукта в режиме обновления выполнив команду с правами суперпользователя:

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

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

Установщик обнаружит текущую версию eCA-CA и предложит выбрать необходимое действие в интерактивном режиме:

- Удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программы.

- Выполнить обновление установленной версии до актуальной версии программы.
- Прервать процесс установки.

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

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

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

В результате обновления еСА-СА на версию 2.4:

- имеющиеся на момент обновления в конфигурационном файле программы параметры подключения к почтовому серверу для отправки уведомлений на электронную почту будут преобразованы в запись о почтовом сервере в базе данных.
- имеющиеся в программе на момент запуска обновления шаблоны рассылки получают значение «Все субъекты» в качестве объектов, о сертификатах которых должны рассылаться уведомления, и будут иметь владельцев сертификатов в качестве получателей уведомлений с опцией «по атрибуту «RFC 822 Name» или «MS UPN» (если «RFC 822 Name» не задан)».
- в имеющихся на момент запуска обновления шаблонов, включая шаблоны по умолчанию, опция (чекбокс) «Короткоживущий (short-lived, throwaway) сертификат» будет переведена выключенное состояние.
- для всех имеющихся на момент запуска обновления шаблонов, включая шаблоны по умолчанию, опция (чекбокс) «Выпуск сертификатов с закрытым ключом (PKCS#12)» перейдёт во включённое состояние, а регулярное выражение валидации паролей от контейнеров закрытого ключа в шаблонах примет значение по умолчанию.

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

Запустите обновлённый еСА-СА², подключитесь к веб-интерфейсу и проверьте версию программы в окне «О программе».

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

² Описание проверок при запуске, выполняемых еСА-СА, см. в разделе 6 настоящего руководства.

12 УДАЛЕНИЕ ПРОГРАММЫ

Для инициализации процесса удаления программы выполните команду с правами суперпользователя:

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

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

В результате выполнения скрипта `uninstall.sh` будут полностью уничтожены:

- Все добавленные при установке программы системные службы.
- Все добавленные при установке программы пользователи и группы.
- Все добавленные при установке программы файлы и структура каталогов.

Процесс удаления выполняется вне зависимости от наличия соединения с БД, имя которой указано в значении параметра `database_name` конфигурационного файла `/opt/aecaCa/scripts/config.sh`.

13 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

13.1 Удаление базы данных

Для удаления ранее созданной базы данных «аесаса» (по умолчанию) необходимо выполнить команды с правами суперпользователя:

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

```
-u postgres psql
```

- Для предотвращения возможности новых подключений выполните команду:

```
UPDATE pg_database SET datallowconn = 'false' WHERE datname = '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();
```

- Удалите базу данных выполнив команду:

```
DROP DATABASE aecaca;
```

13.2 Удаление пользователя базы данных

Для удаления ранее созданного пользователя базы данных «аеса» (по умолчанию) необходимо выполнить команды с правами суперпользователя:

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

```
-i -u postgres
```

- Удалите пользователя «аеса» в Postgres выполнив команду:

```
dropuser aeca -i
```

- Перезапустите СУБД Postgres выполнив команду с правами суперпользователя:

```
systemctl restart postgresql
```

14 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения
Ошибка при запуске скрипта установки <code>install.sh</code> «error obtaining MAC configuration for user «имя пользователя СУБД»» в ОС Astra Linux Special Edition 1.8	Не выполнена дополнительная настройка пользователя СУБД для поддержки работы с активным механизмом МРД	Выполнить настройку пользователя СУБД для поддержки работы с активным механизмом МРД в соответствии с инструкциями пунктов 4.4.1, 4.4.2 или 4.4.3 (в зависимости от использованного способа создания пользователя СУБД) и перезапустить скрипт установки <code>install.sh</code> .
Ошибка запуска сервисов после запуска скрипта <code>install.sh</code> для установки программы	На сервере была установлена и удалена более ранняя версия программы	Очистите конфигурацию <code>nginx</code> выполнив команды с правами суперпользователя: <pre>rm -rfv /etc/nginx/general-configs rm -rfv /etc/nginx/conf.d/default.conf</pre>
	Не хватка аппаратных ресурсов	Проверьте показатель загруженности оперативной памяти. Для корректной работы программы требуется не менее 6 Гб свободной оперативной памяти
Ошибка при запуске скрипта установки <code>install.sh</code> «Минимальное количество оперативной памяти для развёртывания системы составляет 6144 мегабайта!»	Значение параметра <code>memory</code> в файле конфигурации меньше 6144 или не задано	В файле <code>/opt/aecaCa/scripts/config.sh</code> для параметра <code>memory</code> указать значение 6144: <pre>memory='6144'</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 ¹ .

¹ Параметр `max_connections` задаётся в инструкциях из разделов по установке и настройке СУБД.

ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА ПРИ УСТАНОВКЕ СУБД POSTGRES И POSTGRES PRO

В случае, если другой продукт Postgres¹ установлен, то для разрешения конфликта необходимо выполнить следующие команды:

- Создайте начальную базу данных, запустив вспомогательный скрипт `pg-setup` с правами суперпользователя и ключом `initdb`:

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

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

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

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

- Запустите сервер с помощью скрипта `pg-setup`, выполнив команду с правами суперпользователя:

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

¹ Подробное описание приведено в официальной документации на PostgreSQL.

ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

Для подключения еСА-СА к внешней СУБД необходимо:

- выполнить настройку на хосте СУБД в соответствии с подразделом 2.1 настоящего приложения.
- выполнить настройку на хосте еСА-СА в соответствии с подразделом 2.2 настоящего приложения.

2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД) 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 с правами суперпользователя:

```
iptables -A INPUT -p tcp --destination-port port -j ACCEPT
```

где **port** - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432). Данная команда разрешит подключение к СУБД с любого IP-адреса.

- Если необходимо ограничить доступ к порту СУБД, предоставив его только для определенного IP-адреса, то необходимо использовать следующую команду с правами суперпользователя:

```
iptables -A INPUT -s IP -p tcp --destination-port port -j ACCEPT
```

где **IP** - IP-адрес, доступ с которого необходимо разрешить, 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, РОСА «ХРОМ» 12 Сервер, SberLinux OS Server и ОС Альт 8 СП, необходимо отредактировать файл `/var/lib/pgsql/15/data/pg_hba.conf` или `var/lib/jatoba/[версия]/data/pg_hba.conf`, если используется СУБД Jatoba)¹, приведя его к следующему виду:

#	TYPE	DATABASE	USER	ADDRESS	METHOD
# "local" is for Unix domain socket connections only					
local	all		all		peer
# IPv4 local connections:					
host	all		all	0.0.0.0/0	password
# IPv6 local connections:					
host	all		all	:::1/128	password
# 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

¹ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

Кроме того, необходимо отредактировать файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)¹, указав для параметра `listen_addresses` значение `''`:

```
listen_addresses = ''
```

Значение `''` позволит подключаться к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к СУБД, предоставив его только для 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 с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-[версия]`, если используется СУБД Jatoba).
- Затем на хосте СУБД необходимо создать и настроить базу данных. В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

2.2 Настройка на хосте eCA-CA

Внимание! На хосте eCA-CA предварительно должна быть установлена СУБД. При этом не нужно настраивать СУБД, установленную на хосте eCA-CA.

На хосте eCA-CA 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 ² . Допустимые значения: <code>true</code> , <code>false</code> .
<code>database_username</code>	<code>'aeca'</code>	Имя пользователя базы данных, используемое для работы «eCA-CA». Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД.
<code>database_password</code>	<code>#CHANGEIT</code>	Пароль пользователя базы данных, используемый для работы eCA-CA. 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>'aecaca'</code>	Имя базы данных, используемой eCA-CA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД.
<code>root_cert_path</code>	<code>#CHANGEIT</code>	Абсолютный путь к сертификату корневого Центра сертификации из цепочки сертификатов сервера СУБД ³ .

- Затем на хосте eCA-CA необходимо применить изменения конфигурационного файла путём выполнения с правами суперпользователя команды `bash /opt/aecaCa/scripts/install.sh` и дальнейшего выбора действия «[Update]». Если eCA-CA не был установлен ранее, выбор действия не потребуется, и будет выполнена установка с указанными в конфигурационном файле параметрами.

¹ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

² Подробная информация о параметре `use_tls` приведена в приложении 3.

³ Подробная информация о параметре `root_cert_path` приведена в приложении 3.

ПРИЛОЖЕНИЕ 3. НАСТРОЙКА TLS-СОЕДИНЕНИЯ С СУБД

Внимание! Для настройки TLS-соединения еCA-CA с СУБД необходимо в предварительно развёрнутом и инициализированном еCA-CA создать сертификат с закрытым ключом (PKCS#12) для сервера СУБД. При этом в сертификате сервера СУБД в атрибуте «Common Name» или в атрибуте «Subject Alternative Name» типа «dNSName» обязательно должно быть указано доменное сервера СУБД (или IP-адрес)¹, так как программный компонент еCA-CA 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, указав ему необходимые атрибуты «Common Name» и «DNS Name»).

Во избежание ошибок в работе еCA-CA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу программы путём выполнения с правами суперпользователя команды `systemctl stop aeca-ca.service`.

Для настройки TLS-соединения еCA-CA с СУБД необходимо:

- Выполнить настройку СУБД в соответствии с подразделом 3.1 настоящего приложения;
- Выполнить настройку еCA-CA в соответствии с подразделом 3.2 настоящего приложения.

3.1 Настройка СУБД

На хосте с установленной и настроенной СУБД отредактировать файл `/var/lib/pgsql/15/data/postgresql.conf` (или `/var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)², указав:

- в параметре «ssl» значение «on»;
- в параметре «ssl_cert_file» абсолютный путь к файлу сертификата сервера СУБД³;
- в параметре «ssl_key_file» абсолютный путь к файлу закрытого ключа сервера СУБД⁴;
- в параметре «ssl_ca_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД⁵.

При этом указанные выше файлы должны иметь метку доступа «600», установить которую можно с правами суперпользователя с помощью команды `chmod 600 путь_к_файлу` для каждого файла. Владелец всех указанных выше файлов необходимо назначить пользователя «postgres» выполнив с правами суперпользователя команду `chown postgres:postgres путь_к_файлу` для всех перечисленных файлов. Указанные файлы должны располагаться в каталоге, к которому имеет доступ пользователь postgres (например, `/tmp`). В случае использования ОС РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server на хосте СУБД указанные выше файлы должны располагаться в каталоге `/var/lib/pgsql` (или `/var/lib/jatoba`, если используется СУБД Jatoba). При этом указанные выше файлы должны быть скопированы в нужный каталог, а не перемещены.

¹ Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database_host» конфигурационного файла еCA-CA.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса еCA-CA. Например, в карточке локального субъекта сервера СУБД.

⁴ 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.

⁵ Файл цепочки сертификатов издателя сертификата СУБД может быть скачан в карточке Центра сертификации, выпустившего сертификат сервера СУБД.

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'
```

На хосте СУБД перезапустить СУБД выполнив с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-[версия]`, если используется СУБД Jatoba).

3.2 Настройка eCA-CA

На хосте eCA-CA 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 СУБД¹.

При этом указанный выше файл сертификата корневого издателя из цепочки сертификатов сервера СУБД должен иметь метку доступа «600», установить которую можно с правами суперпользователя с помощью команды `chmod 600 путь_к_файлу`. Владелец файла сертификата корневого издателя из цепочки сертификатов сервера СУБД необходимо назначить пользователя «aeca» выполнив с правами суперпользователя команду `chown aeca:aeca путь_к_файлу`. Указанный файл должен располагаться в каталоге, к которому имеет доступ пользователь `aeca` (например, `/tmp`). В случае использования ОС РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server на хосте eCA-CA 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, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server на хосте eCA-CA необходимо дополнительно выполнить команду `restorecon -Rv "путь_к_файлу_сертификата_корневого_издателя_из_цепочки_сертификатов_сервера_СУБД"`.

На хосте eCA-CA применить изменения конфигурационного файла путём выполнения с правами суперпользователя команды `bash /opt/aecaCa/scripts/install.sh` и дальнейшего выбора действия «[Update]».

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

¹ Если сертификат сервера СУБД выпущен подчиненным Центром сертификации, необходимо указать путь до сертификата корневого Центра сертификации.

ПРИЛОЖЕНИЕ 4. РАЗВЁРТЫВАНИЕ КЛАСТЕРА

Программное средство обеспечивает объединение нескольких eCA-CA в кластер. Кластеризация обеспечивается в отказоустойчивом режиме с использованием внешнего средства балансировки нагрузки HAProxy¹. Отказоустойчивый режим кластеризации обеспечивает как холодное «active-passive»², так и горячее «active-active»³ резервирование. Горячее «active-active» резервирование возможно только при «source»⁴ балансировке.

Развёртывания кластера eCA-CA возможно в следующих вариантах:

- В виртуальной инфраструктуре путём клонирования виртуальной машины основного узла.
- С помощью переноса контейнеров закрытого ключа основного узла.

4.1 Развёртывание кластера в виртуальной среде с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Виртуальная машина с установленным и инициализированным eCA-CA (далее - VM1) - основной узел кластера.
- Клон VM1, созданный сразу после завершения инициализации на VM1 eCA-CA (далее - VM2) - резервный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - VM3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - VM4).
- Клон VM1, созданный при необходимости при эксплуатации кластера (далее - VMP) – дополнительный резервный узел кластера.

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в подразделе 2.1.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации VM3 и VM4.

Порядок развёртывания кластера:

- Выполните следующие действия на VM3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000⁵ в файле⁶:
 - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
 - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
 - `systemctl restart postgresql` для СУБД PostgreSQL.
 - `systemctl restart jatoba-[версия]` для СУБД Jatoba.

¹ Серверное программное обеспечение для обеспечения высокой доступности и балансировки нагрузки для TCP- и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов

² Это конфигурация отказоустойчивых кластеров, в которой одни узлы назначаются активными, а другие — резервными, готовыми взять на себя работу в случае отказа активного узла.

³ Это архитектурный подход построения кластера, при котором оба или все узлы активны и работают одновременно, обрабатывая запросы и трафик.

⁴ Это режим, при котором балансировщик выбирает узел кластера на основе хэш-суммы источника IP-адреса, с которого клиенты отправляют запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера.

⁵ Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-CA, взаимодействующего с СУБД.

⁶ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- Выполните следующие действия на ВМ1:
 - Выполните установку еСА-СА (см. 4) с подключением внешней СУБД, установленной на ВМ3 (см. приложение 2 настоящего руководства).
 - Подключитесь к веб-интерфейсу еСА-СА под учётной записью администратора инициализации технологического центра сертификации.
 - Выполните первичное лицензирование еСА-СА (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
 - Выполните инициализацию Центра сертификации (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-ca.service`.

Внимание! В случае, если на ВМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на ВМ2 необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните следующие действия на ВМ4:
 - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
 - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
 - `apt install haproxy`- для ОС Astra Linux SE.
 - `apt-get install haproxy`- для ОС Альт Сервер.
 - Выполните редактирование конфигурационного файла `/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:

- IP_VM1 – IP-адрес ВМ1.
- IP_VM2 – IP-адрес ВМ2.
- admin:password – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя `systemctl restart haproxy.service`.

В кластер можно подключать дополнительные резервные узлы ВМР. Для подключения нового резервного узла ВМР необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР.
- Запустите ВМР и дождитесь запуска службы `aeca-ca.service`.

Внимание! В случае, если на ВМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на ВМР необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните следующие действия на ВМ4:
 - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об IP-адреса ВМР в соответствии с примером, представленном ниже:

```
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 ВМР.

- Перезапустите HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки кластера все запросы, направляемые к еСА-СА через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера ВМ1. При недоступности основного узла кластера все запросы будут перенаправляться на резервный узел кластера ВМ2. При недоступности ВМ2 все запросы будут перенаправляться на дополнительный резервный узел кластера ВМР. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где `IP_VM4` - IP-адрес ВМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

Внимание! В случае дальнейшего создания Центров сертификации в развёрнутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» на ВМ1, ВМ2 и всех дополнительных резервных узлах. Например, если активным узлом кластера в момент создания Центра сертификации являлся ВМ2, скопируйте созданный закрытый ключ Центра сертификации с ВМ2 на ВМ1, а затем перезапустите сервис `aeca-ca.service` на ВМ1.

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` (по умолчанию).

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` (по умолчанию), затем перезапускать на данной ВМ СКЗИ «КриптоПро CSP».

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

4.2 Развёртывание кластера с холодным резервированием «active-passive» путём переноса контейнера закрытого ключа основного узла

Кластер включает следующие узлы:

- Сервер с установленным и инициализированным eCA-CA (далее - APM1) - основной узел кластера.
- Сервер с установленным и инициализированным eCA-CA, на который будет выполнен перенос контейнера закрытого ключа (далее - APM2) - резервный узел кластера.
- Сервер с установленным и инициализированным eCA-CA, на который будет выполнен перенос контейнера закрытого ключа (далее - APMР) – дополнительный резервный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - APM3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - APM4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в подразделе 2.1.1. Допускается использование одного сервера для реализации APM3 и APM4.

Порядок развёртывания кластера:

- Выполните следующие действия на APM3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле ²:
 - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
 - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
 - `systemctl restart postgresql` для СУБД PostgreSQL.
 - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните следующие действия на APM1:
 - Выполните установку eCA-CA (см. 4) с подключением внешней СУБД, установленной на APM3 (см. приложение 2 настоящего руководства).
 - Подключитесь к веб-интерфейсу eCA-CA под учётной записью администратора инициализации технологического центра сертификации.
 - Выполните первичное лицензирование eCA-CA (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
 - Выполните инициализацию Центра сертификации (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
- На APM2 выполните установку eCA-CA с подключением внешней СУБД ³, установленной на APM3 (см. приложение 2 настоящего руководства).

Внимание! В случае, если на APM1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на APM2

¹ Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-CA, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ В конфигурационном файле eCA-CA на APM2 необходимо указывать параметры СУБД, аналогичные указанным СУБД APM1.

необходимо выполнить аналогичную APM1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на APM1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на APM2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Если на APM1 был создан Центр сертификации, закрытый ключ которого хранится локально, скопируйте с APM1 содержимое каталога `/opt/aecaCa/dist/cryptotoken` в каталог `/opt/aecaCa/dist/cryptotoken` APM2.

- Если на APM1 был создан Центр сертификации, закрытый ключ которого расположен в хранилище HDIMAGE СКЗИ «КриптоПро CSP», скопируйте с APM1 контейнер Центра сертификации (имя файла будет соответствовать первым 8 символам идентификатора Центра сертификации) из каталога `/var/opt/cproscsp/keys/aeca` в каталог `/var/opt/cproscsp/keys/aeca` APM2. При этом необходимо назначить владельцем данного файла на APM2 пользователя «aeca», и перезапустить на APM2 СКЗИ «КриптоПро CSP».

- Скопируйте с APM1 содержимое каталога `/opt/aecaCa/dist/certificates` в каталог `/opt/aecaCa/dist/certificates` APM2.

- Если на APM2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, то выполните с правами суперпользователя следующие команды в терминале на APM2:

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

- Выполните на APM2 перезапуск `aeca-ca.service` для обеспечения работы Центра сертификации с перенесёнными контейнерами выполнив с правами суперпользователя следующую команду:

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

- Выполните следующие действия на ВМ4:

- Выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
 - o `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
 - o `apt install haproxy`- для ОС Astra Linux SE.
 - o `apt-get install haproxy`- для ОС Альт Сервер.
- Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

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

defaults
    log global
    mode http
    option httplog
```

```
option dontlognull
timeout connect 5000
timeout client 50000
timeout server 50000

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    server main 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:

- IP_ARM1 – IP-адрес АРМ1.
- IP_ARM2 – IP-адрес АРМ2.
- admin:password – имя и пароль учётной записи администратора для доступа к панели мониторинга HAProxy.
- На АРМ4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

В кластер можно подключать дополнительные резервные узлы АРМР. Для подключения нового резервного узла АРМР необходимо выполнить действия, аналогичные действиям по подключению узла АРМ2.

Внимание! В случае, если на АРМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на АРМР необходимо выполнить аналогичную АРМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

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

Выполните на АРМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об IP-адреса АРМР в соответствии с примером, представленном ниже:

```
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 АРМР.

На АРМ4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел. В результате приведённой настройки кластера все запросы, направляемые к еСА-СА через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера APM1. В случае недоступности основного узла кластера все запросы, направляемые к еСА-СА через средство балансирования нагрузки HAProxy, будут перенаправляться на резервный узел кластера APM2. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_ARM4:8404/stats` (где IP_ARM4 - IP-адрес APM4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

Внимание! В случае дальнейшего создания Центров сертификации в развёрнутом кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище КриптоПро HDIMAGE на APM1, APM2 и дополнительных узлах. Например, если активным узлом кластера в момент создания Центра сертификации являлся APM2, необходимо скопировать созданные закрытые ключи Центров сертификации с APM2 на APM1, затем перезапустить службу `aeca-ca.service` на APM1.

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 APM пользователя `aeca` (по умолчанию).

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 APM пользователя `aeca` (по умолчанию), затем перезапускать на данной APM СКЗИ «КриптоПро CSP».

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

4.3 Развёртывания кластера в виртуальной среде с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Виртуальная машина с установленным и инициализированным еСА-СА (далее - BM1) - первый узел кластера.
- Клон BM1, созданный сразу после завершения инициализации на BM1 еСА-СА (далее - BM2) - второй узел кластера.
- Клон BM1, созданный при необходимости при эксплуатации кластера (далее - BMP) - дополнительный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - BM3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - BM4).

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в подразделе 2.1.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации BM3 и BM4.

Порядок развёртывания кластера:

- Выполните следующие действия на ВМ3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.
 - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле ²:
 - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
 - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
 - `systemctl restart postgresql` для СУБД PostgreSQL.
 - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните следующие действия на ВМ1:
 - Выполните установку еСА-СА (см. 4) с подключением внешней СУБД, установленной на ВМ3 (см. приложение 2 настоящего руководства).
 - Подключитесь к веб-интерфейсу еСА-СА под учётной записью администратора инициализации технологического центра сертификации.
 - Выполните первичное лицензирование еСА-СА (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
 - Выполните инициализацию Центра сертификации (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-ca.service`.

Внимание! В случае, если на ВМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на ВМ2 необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните следующие действия на ВМ4:
 - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
 - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
 - `apt install haproxy`- для ОС Astra Linux SE.
 - `apt-get install haproxy`- для ОС Альт Сервер.

¹ Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра еСА-СА, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

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

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

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main IP_VM1:443 check
    server clone IP_VM2:443 check

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

где:

- o `IP_VM1` – IP-адрес ВМ1.
- o `IP_VM2` – IP-адрес ВМ2.
- o `admin:password` – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.
- Перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

В кластер можно подключать дополнительные узлы. Для подключения нового резервного узла необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР.
- Запустите ВМР и дождитесь запуска службы `aeca-ca.service`.

Внимание! В случае, если на ВМ1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP, на ВМР необходимо выполнить аналогичную ВМ1 установку КЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните на ВМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об IP-адреса ВМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main IP_VM1:443 check
    server clone IP_VM2:443 check
    server clone IP_VMR:443 check
```

где `IP_VMR` - это IP-адрес ВМР.

- Перезапустите HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где `IP_VM4` - IP-адрес ВМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла HAProxy.

Внимание! В случае дальнейшего создания Центров сертификации в развёрнутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» на VM1, VM2 и всех дополнительных резервных узлах. Например, если активным узлом кластера в момент создания Центра сертификации являлся VM2, скопируйте созданный закрытый ключ Центра сертификации с VM2 на VM1, а затем перезапустите сервис `aeca-ca.service` на VM1.

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 VM пользователя `aeca` (по умолчанию).

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 VM пользователя `aeca` (по умолчанию), затем перезапускать на данной VM СКЗИ «КриптоПро CSP».

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

4.4 Развёртывание кластера с горячим резервированием «active-active» путём переноса контейнера закрытого ключа первого узла

Кластер включает следующие узлы:

- Сервер с установленным и инициализированным eCA-CA (далее - APM1) – первый узел кластера.
- Сервер с установленным и инициализированным eCA-CA, для которого будет выполнен перенос контейнеров закрытого ключа (далее - APM2) – второй узел кластера.
- Сервер с установленным и инициализированным eCA-CA, для которого будет выполнен перенос контейнеров закрытого ключа (далее - APMР) – дополнительный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - APM3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - APM4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в подразделе 2.1.1. Допускается использование одного сервера для реализации APM3 и APM4.

Порядок развёртывания кластера:

- Выполните следующие действия на APM3:
 - Выполнить установку одной из нижеприведённых СУБД:
 - PostgreSQL из состава ОС
 - Jatoba.

- Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000¹ в файле²:
 - o `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
 - o `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
- Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
 - o `systemctl restart postgresql` для СУБД PostgreSQL.
 - o `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните следующие действия на APM1:
 - Выполните установку еСА-СА (см. 4) с подключением внешней СУБД, установленной на APM3 (см. приложение 2 настоящего руководства).
 - Подключитесь к веб-интерфейсу еСА-СА под учётной записью администратора инициализации технологического центра сертификации.
 - Выполните первичное лицензирование еСА-СА (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
 - Выполните инициализацию Центра сертификации (см. документ «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
- На APM2 выполните установку еСА-СА (см. 4) с подключением внешней СУБД³, установленной на APM3 (см. приложение 2 настоящего руководства).

Внимание! В случае, если на APM1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на APM2 необходимо выполнить аналогичную APM1 установку программного средства СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на APM1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на APM2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Если на APM1 был создан Центр сертификации, закрытый ключ которого хранится локально, скопируйте с APM1 содержимое каталога `/opt/aecaCa/dist/cryptotoken` в каталог `/opt/aecaCa/dist/cryptotoken` APM2.
- Если на APM1 был создан Центр сертификации, закрытый ключ которого расположен в хранилище HDIMAGE СКЗИ «КриптоПро CSP», скопируйте с APM1 контейнер Центра сертификации (имя файла будет соответствовать первым 8 символам идентификатора Центра сертификации) из каталога `/var/opt/cproscsp/keys/aeca` в каталог `/var/opt/cproscsp/keys/aeca` APM2. При этом необходимо назначить владельцем данного файла на APM2 пользователя «aeca», и перезапустить на APM2 СКЗИ «КриптоПро CSP».
- Скопируйте с APM1 содержимое каталога `/opt/aecaCa/dist/certificates` в каталог `/opt/aecaCa/dist/certificates` APM2.

¹ Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра еСА-СА, взаимодействующего с СУБД.

² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

³ В конфигурационном файле еСА-СА на APM2 необходимо указывать параметры СУБД, аналогичные указанным СУБД APM1.

- Если на APM2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, то выполните с правами суперпользователя следующие команды в терминале на APM2:

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

- Выполните на APM2 перезапуск `aeca-ca.service` для обеспечения работы Центра сертификации с перенесенными контейнерами выполнив с правами суперпользователя следующую команду:

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

- Выполните следующие действия на APM4:
 - Выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
 - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
 - `apt install haproxy`- для ОС Astra Linux SE.
 - `apt-get install haproxy`- для ОС Альт Сервер.
 - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

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

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

frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app

backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main IP_VM1:443 check
    server clone IP_VM2:443 check
```

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

где:

- IP_ARM1 – IP-адрес APM1.
- IP_ARM2 – IP-адрес APM2.
- admin:password – имя и пароль учётной записи для доступа к панели мониторинга HAProxy.

- На APM4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

В кластер можно подключать дополнительные резервные узлы APMР. Для подключения нового резервного узла APMР необходимо выполнить действия, аналогичные действиям по подключению узла APM2.

Внимание! В случае, если на APM1 был создан Центр сертификации, у которого криптопровайдером какого-либо алгоритма является СКЗИ «КриптоПро CSP», на APMР необходимо выполнить аналогичную APM1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на APM1 был создан Центр сертификации, местом хранения закрытого ключа которого является ПАКМ «КриптоПро HSM», необходимо выполнить на APMР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

Выполните на APM4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию об IP-адреса APMР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main IP_ARM1:443 check
    server clone IP_ARM2:443 check
    server clone IP_ARMR:443 check
```

где IP_ARMR - это IP-адрес APMР.

На APM4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_ARM4:8404/stats` (где IP_ARM4 - IP-адрес APM4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройка конфигурационного файла HAProxy.

Внимание! В случае дальнейшего создания Центров сертификации в развёрнутом кластере необходимо сохранять соответствие перечня закрытых ключей, хранимых локально и в хранилище КриптоПро HDIMAGE на АРМ1, АРМ2 и дополнительных узлах. 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 службу `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 конечной АРМ пользователя `aeca` (по умолчанию).

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 конечной АРМ пользователя `aeca` (по умолчанию), затем перезапускать на данной АРМ СКЗИ «КриптоПро CSP».

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

4.3 Обновление ПО узлов кластера eCA-CA

Процесс обновления кластера eCA-CA:

- Выполните резервное копирование данных на всех узлах кластера (см. раздел 9 настоящего руководства).
- Для кластера по схеме «active-passive» на всех резервных узлах произведите остановку службы eCA-CA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-ca.service`.
- Для кластера по схеме «active-active» на всех узлах, на которые был перенесён закрытый ключ, произведите остановку службы eCA-CA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-ca.service`.
- Для кластера по схеме «active-passive» выполнить обновление ПО eCA-CA на основном узле (см. раздел 11 настоящего руководства).
- Для кластера по схеме «active-active» выполнить обновление ПО eCA-CA на узле, на котором был создан закрытый ключ (см. раздел 11 настоящего руководства).
- Вне зависимости от схемы кластера выполните обновление ПО eCA-CA на всех остальных узлах кластера (см. раздел 11 настоящего руководства).

Критерием правильности установки обновления ПО кластера является отображение информации о новой версии в окне «О программе» веб-интерфейса и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга НАргоху. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_Haproxy:8404/stats` (где `IP_Haproxy` - IP-адрес ВМ4 или АРМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учётной записи, указанных при настройке конфигурационного файла НАРгоху.

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

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA eCA-CA 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 подчинённого);
- 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»¹. 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»² 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.

¹ Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

² 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 еСА-СА необходимо подготовить внешнюю гамму¹. Внешняя гамма представляет собой каталог `gamma`, содержащий каталоги `db1`, `db2` и файл `krim`. В каталоге `db1` хранится файл гаммы `kis_1`. Каталог `db2` дублирует каталог `db1` для надёжности. `krim` — служебный файл с параметрами гаммы. 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»².

Внимание! При развёртывании нескольких экземпляров еСА-СА 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 еСА-СА:

1. На сервере еСА-СА 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` с правами суперпользователя командой `apt-get install newt52`.

2. При отсутствии создайте каталог `/opt/aecaCa/services/cryptoproviders` командой с правами суперпользователя:

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

3. 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 с правами суперпользователя:

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

4. Назначьте права доступа на скопированные файлы:
 - Если выполняется первоначальная установка еСА-СА, то назначьте файлам права доступа (`chmod 777`) командой с правами суперпользователя:

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

- Если еСА-СА был ранее установлен, то назначьте владельцем данных файлов пользователя «аеса» и предоставьте ему права доступа к файлам (`chmod 700`) командами с правами суперпользователя:

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

¹ 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».

² Выбор места хранения осуществляется в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центром сертификации Aladdin Enterprise Certification Authority».

5. Если Вы собираетесь использовать заранее подготовленный каталог `gamma` с внешней гаммой, то пропустите этот пункт. Иначе подготовьте каталог `gamma` с внешней гаммой с помощью утилиты `/opt/cproscsp/bin/amd64/genkpm` (утилита `genkpm` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma /opt/cproscsp/bin/amd64/genkpm <количество ключей> 0x12345678
~/gamma
```

6. На хосте Центра сертификации Aaddin eCA поместите каталог `gamma` в каталог `/opt/aecaCa/dist/` командой с правами суперпользователя:

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

7. В результате в каталоге `/opt/aecaCa/dist/gamma` появятся подкаталоги `db1`, `db2`, `kpm`.
 - Если выполняется первоначальная установка eCA-CA, то назначьте права доступа файлам (`chmod 777`) командой с правами суперпользователя:

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

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

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

8. Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд¹ с правами суперпользователя:

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

9. Правильность настройки гаммы можно выполнив команду с правами суперпользователя:

```
/opt/cproscsp/bin/amd64/csptest -keyset -newkeyset -cont '\\.\HDIMAGE\1'
```

Если после выполнения команды произошёл запрос пароля, гамма настроена правильно.

10. Если eCA-CA был ранее установлен, перезапустите сервис `aeca-ca.service` командой с правами суперпользователя:

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

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

5.2 Индикация об отсутствии связи с СКЗИ «КриптоПро CSP»

При отсутствии на хосте eCA-CA 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».

¹ Подключение осуществляется с помощью файла `cpconfig` (находится в `/opt/cproscsp/sbin/amd64`). Путь к файлу в командах приведен с учётом нахождения в каталоге `/opt/cproscsp/sbin/amd64`.

- 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».

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

БД	- База данных
ЗПС	- Замкнутая программная среда
КС	- Контрольная сумма
ОС	- Операционная система
ПАКМ	- Программно-аппаратный криптографический модуль
ПО	- Программное обеспечение
СВТ	- Средство вычислительной техники
СКЗИ	- Средство криптографической защиты информации
СУБД	- Система управления базами данных
ЦС	- Центр сертификатов
CSP	- Cryptography Service Provider
HTTP	- Hypertext Transfer Protocol
HTTPS	- Hyper Text Transfer Protocol Secure
LDAP	- Lightweight Directory Access Protocol
API	- Application Programming Interface
CRL	- Certificate Revocation List
AIA	- Authority Information Access
URL	- Uniform Resource Locator
TCP	- Transmission Control Protocol
TLS	- Transport Layer Security
VGA	- Video Graphics Array
WSTEP	- WS-Trust X.509v3 Token Enrollment Extensions
SCEP	- Simple Certificate Enrollment Protocol
HDD	- Hard (magnetic) Disk Drive
SMTP	- Simple Mail Transfer Protocol
OCSP	- Online Certificate Status Protocol

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.

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 самоподписанным 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.

Подчинённый ЦС - экземпляр центра сертификации в информационной системе, который получает доверие от корневого ЦС и выполняет функции по выдаче сертификатов конечным пользователям, компьютерам и сервисам в рамках определенной инфраструктуры открытых ключей. Подчинённый ЦС - это следующая ступень иерархии центров сертификации. Доверие к подчинённому ЦС определяется цепочкой сертификатов. Корневой центр сертификации, подчинённые центры сертификации, получившие сертификаты от корневого центра, и подчинённые центры сертификации, получившие сертификаты от других подчинённых центров вместе образуют иерархию сертификации.

Сертификат - выпущенный центром сертификации цифровой документ в форматах x509v3 или другом поддерживаемом формате (например, PGP (OpenPGP) или S/MIME), 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 (CRL) - список аннулированных (отозванных) сертификатов, издаётся центром сертификации по запросу или с заданной периодичностью, либо при изменении статуса сертификата на отозванный, приостановленный или активированный (из статуса приостановленного). Список отозванных сертификатов применяется для идентификации и признания недействительными сертификатов до истечения их срока действия

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, обладающий функцией первичной настройки программного компонента eCA-CA.

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.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

[illegible]