



ЦЕНТР ВАЛИДАЦИИ

Aladdin Enterprise Certificate Authority

Руководство администратора. Установка и обслуживание

Изделие	RU.ALDE.03.01.039-01
Документ	32 01-1
Листов	43
Дата	07.12.2023

Авторские права, товарные знаки, ограничения

Данный документ, включая подбор и расположение иллюстраций и материалов в нём, является субъектом 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 ВСПЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

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

Права и собственность

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

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

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

Лицензия

Компания настоящим предоставляет Вам, а Вы получаете индивидуальное, неисключительное и отзываемое ограниченное право на использование данного ПО только в форме исполняемого кода, как

описано в прилагаемой к ПО технической/эксплуатационной документации, и только в соответствии с условиями данного Соглашения: Вы можете установить ПО и использовать его на компьютерах, расположенных в пределах Вашего предприятия, как описано в соответствующей технической/эксплуатационной документации ПО и в настоящем соглашении.

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

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

Требования к использованию

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

Использование ПО

Пользователь вправе:

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

При использовании и распространении ПО Пользователь обязан руководствоваться действующим законодательством Российской Федерации и международным законодательством, учитывая ограничения и дополнительные требования, которые могут возникнуть 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 возникнуть 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: - дизайны (графики, расположения элементов оформления и т.п.);

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

- возместить стоимость, выплаченную Вами за ПО.

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

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

Ограничение ответственности

В случае если, несмотря на условия данного соглашения, компания признана ответственной за убытки на основании каких-либо дефектов или несоответствия программного обеспечения Вашим ожиданиям, полная ответственность за каждый экземпляр дефектного программного

обеспечения не будет превышать суммы, выплаченной вами АО «Аладдин Р.Д.» за это ПО.

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

АННОТАЦИЯ

Настоящий документ представляет собой первую часть руководства администратора программного средства «Центр валидации Aladdin Enterprise Certificate Authority»¹.

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

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

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

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

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

¹ Далее по документу – функциональный компонент, Центр валидации, Центр валидации Aladdin eCA

Содержание

Авторские права, товарные знаки, ограничения.....	2
Лицензионное соглашение.....	2
Аннотация.....	4
1 Введение	7
1.1 Назначение компонента.....	7
1.2 Функции компонента.....	7
1.3 Комплект поставки.....	7
1.4 Имя пакета компонента поставки.....	7
1.5 Исполняемые файлы компонента.....	8
1.6 Действия по безопасной установке и настройке компонента	8
2 Условия выполнения	9
2.1.1 Требования к программному обеспечению	9
2.1.2 Требования к аппаратным средствам	9
3 Подготовка к установке	10
3.1 Таблица сетевого взаимодействия.....	10
3.2 Подготовка сервера к установке компонента	10
3.2.1 Подключение репозитория и установка зависимостей.....	10
3.2.2 Установка набора инструментов Java	10
3.2.3 Установка и настройка СУБД	10
4 Установка.....	12
4.1 Распаковка инсталляционного комплекта компонента	12
4.2 Настройка параметров компонента	13
4.2.1 Настройка config.sh	13
4.2.2 Настройка cdp.env	14
4.3 Смена порта доступа	15
4.4 Установка компонента.....	16
4.4.1 Дополнительные возможные действия при установке	18
5 Подготовка сервера и совместная установка функциональных компонентов «Центр сертификации Aladdin eCA» и «Центра валидации Aladdin eCA»	19
5.1 Вариант (1) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»	19
5.2 Вариант (2) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»	20
5.3 Вариант (3) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»	21
6 Резервное копирование и восстановление данных	22
6.1 Создание полной резервной копии.....	22
6.2 Расписание резервного копирования	22
6.3 Восстановление данных из резервной копии	23
7 Обновление	25
7.1 Назначение обновлений	25
7.2 Информирование потребителей о выпуске обновлений.....	25
7.3 Получение обновлений потребителем	25

7.4	Контроль целостности обновления ПО	25
7.5	Процедура установки обновлений	25
7.6	Критерий успешности установки обновления	26
8	Удаление программы	27
8.1	Инициализация процесса удаления	27
8.2	Удаление установочного пакета	27
9	Удаление базы данных Postgres	28
9.1	Удаление БД «aecatst»	28
9.2	Удаление пользователя БД «aesa»	28
10	Поиск и устранение неисправностей	29
Приложение А. Установка репозитория		30
A.1	Установка репозитория и подключение зависимостей для сервера под управлением ОС РЕД ОС 7.3	30
A.2	Установка репозитория и подключение зависимостей для сервера под управлением ОС Astra Linux Special Edition 1.7	30
A.3	Установка репозитория и подключение зависимостей для сервера под управлением ОС Альт Сервер 10	30
Приложение Б. Установка Open JDK		31
Приложение В. Установка и настройка СУБД PostgreSQL		32
V.1	Установка СУБД PostgreSQL	32
V.2	Создание и настройка СУБД PostgreSQL	33
Приложение Г. Установка и настройка СУБД Jatoba		35
G.1	Установка СУБД Jatoba из локального репозитория	35
G.2	Создание и настройка СУБД Jatoba 4	38
Перечень документации для ознакомления		40
Обозначения и сокращения		41
Термины и определения		42

1 ВВЕДЕНИЕ

1.1 Назначение компонента

Центр валидации Aladdin Enterprise Certificate Authority является функциональным компонентом программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority»², которое предназначено для защиты информации автоматизированных (информационных) систем и используется совместно с другими средствами защиты информации для организации процессов идентификации и строгой аутентификации пользователей, защиты серверной инфраструктуры и устройств сертификатами.

Центр валидации Aladdin Enterprise Certificate Authority предназначен для поддержки функционала проверки статуса сертификатов, выпускаемых программным средством «Центр сертификации Aladdin Enterprise Certificate Authority».

1.2 Функции компонента

Функциональный компонент «Центр валидации Aladdin Enterprise Certificate Authority» реализует следующие основные функции:

- проверка статуса сертификата, выпущенного программным средством Aladdin eCA;
- проверка издателя сертификата, выпущенного программным средством Aladdin eCA;
- предоставление возможности получения (распространения) цепочки сертификатов Центра сертификации;
- предоставление возможности получения (распространения) списка отозванных сертификатов (CRL).

1.3 Комплект поставки

Комплект поставки включает в себя:

- Функциональный компонент «Центр валидации Aladdin Enterprise Certificate Authority» на носителе оптической записи (rpm-пакет для установки на ОС РЕД ОС 7.3 или Альт Сервер 10, deb-пакет для установки на Astra Linux Special Edition 1.7 Смоленск);
- Эксплуатационная документация:
 - «Центр валидации Aladdin Enterprise Certificate Authority. Руководство администратора. Часть 1. Установка и обслуживание»;
 - «Центр валидации Aladdin Enterprise Certificate Authority. Руководство администратора. Часть 2. Функции управления»;

1.4 Имя пакета компонента поставки

Имя пакета компонентов поставки представлено в формате:

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

² Далее по тексту – программное средство Aladdin eCA, программное средство

1.5 Исполняемые файлы компонента

Список исполняемых файлов функционального компонента компонент «Центр валидации Aladdin Enterprise Certificate Authority», выполняющих код при запуске, приведён в Таблице 1.

Таблица 1 – Список исполняемых файлов Центра валидации Aladdin Enterprise Certificate Authority

Наименование исполняемого файла	Описание	Назначение
ejbca.ear	Главный контейнер	Система с компонентом Центра валидации с интеграцией EJBСA, обеспечивающая выполнение целевых функций продукта
aeca-cdp-1.0.0.0.war	Модуль по работе с точками распространения CRL или AIA	Обеспечивает взаимодействия с точками распространения списков отзыва и сертификатов ЦС

1.6 Действия по безопасной установке и настройке компонента

Установка программного компонента производится только с диска, получаемого от разработчика.

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 данный программный компонент.

Настройка программного компонента должна проводится привилегированным пользователем с правами администратора, допускаемым к установке и настройке функционального компонента «Центр валидации Aladdin Enterprise Certificate Authority».

2 УСЛОВИЯ ВЫПОЛНЕНИЯ

2.1.1 Требования к программному обеспечению

Среда функционирования функционального компонента компонент «Центр валидации Aladdin Enterprise Certificate Authority»:

- Операционная системы:
 - Astra Linux Special Edition 1.7 Смоленск в конфигурации «Минимальный сервер» с опцией SSH-сервер и уровнем безопасности «Базовая защита»;
или
 - РЕД ОС 7.3;
или
 - ОС Альт Сервер 10 ("Альт СП Сервер" 10/Альт СП (релиз 10));
- поддерживаемые СУБД:
 - PostgreSQL из состава операционной системы;
или
 - Postgres Pro;
или
 - JatoBa 4;
- поддерживаемая среда исполнения Java:
 - Java Axiom JDK 11 x86_64;
или
 - Open JDK версии 11.
- браузер из состава операционной системы (Firefox Browser v. 75.18.0esr (64-битный) и выше, Google Chrome, Яндекс.Браузер, Спутник, Edge).

2.1.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования компонента «Центр валидации Aladdin Enterprise Certificate Authority»:

- свободное дисковое пространство – не менее 40 Гб;
- доступная оперативная память – не менее 8 Гб.
- 4 процессора с архитектурой x86, x64;
- VGA-совместимый видеоадаптер;
- монитор с поддерживаемым разрешением экрана:
 - 1920x1080 16:9 HD 1080;
 - 1366x768 HD;
 - 1536x864;
 - 1440x900 8:5 WSXGA;
 - 2560x1440;
 - 1280x720 16:9 HD 720;
 - 1600x900 16:9 HD+ 900p;
 - 1680x1050 8:5 WSXGA+;
 - 1280x1024 5:4 SXGA;
 - 1280x800 8:5 WXGA;
 - 1920x1200 8:5 WUXGA;
- устройства взаимодействия с пользователем:
 - клавиатура;
 - мышь.

3 ПОДГОТОВКА К УСТАНОВКЕ

Подготовка к установке функционального компонента «Центр валидации Aladdin Enterprise Certificate Authority» должна быть проведена на каждом сервере, где предполагается развертывание сервера Центра валидации.

3.1 Таблица сетевого взаимодействия

Ниже приведён список портов (см. Таблица 2), которые необходимо открыть для полноценной работы программного средства «Центр валидации Aladdin Enterprise Certificate Authority».

Чтобы узнать, как открыть порты, обратитесь к документации вашей ОС, сетевого оборудования, или к системному администратору вашей организации.

Таблица 2 – Таблица входящих сетевых портов

Порт	Транспорт	Протокол	Назначение	Можно ли переназначить
5432	TCP	TCP	Для подключения к базе данных	Да
587	TCP	SMTP	Для подключения почтового сервера	Да
8888	TCP	HTTPS	Для подключения к функциональному компоненту Центр валидации	Да
8080	TCP	HTTPS	Для подключения к точке распространения Центра валидации	Да
8888	TCP	HTTPS	Для подключения к внутреннему сервису «cdp-service» (Сервис точек распространения)	Да

3.2 Подготовка сервера к установке компонента

Произведите подготовку сервера для дальнейшей установки компонента программного средства «Центр валидации Aladdin Enterprise Certificate Authority», выполнив установку и настройку следующих элементов, в зависимости от того, под управлением какой ОС находится сервер:

- зависимостей и подключение репозитория ОС;
- Java v.11;
- СУБД.

3.2.1 Подключение репозитория и установка зависимостей

Перед началом установки функционального компонента «Центр валидации Aladdin Enterprise Certificate Authority» установите пути нахождения всех необходимых репозитория с использованием сети Интернет или без доступа к сети³.

3.2.2 Установка набора инструментов Java

Произведите установку Java версии 11 одного из пакетов:

- выполните установку программного обеспечения, например, OpenJDK⁴.

3.2.3 Установка и настройка СУБД

- Выполните установку и настройку одной из нижеприведённых базы данных:
 - PostgreSQL⁵ из состава операционной системы;

³ Справочная информация по процедуре подключения репозитория приведена в Приложении А настоящего руководства

⁴ Справочная информация по установке OpenJDK приведена в Приложении Б настоящего руководства

⁵ Справочная информация по установке и настройке СУБД PostgreSQL приведена в Приложении В настоящего руководства

ИЛИ

– Jatoba 4⁶.

- В результате действий должна быть создана база данных с параметрами по умолчанию (имя пользователя - `aeca`, пароль - `aeca`, имя базы данных - `aecatetest`) или выбранными параметрами (имя пользователя, пароль, имя базы данных), указанными в конфигурационных файлах `/opt/aecaVa/scripts/config.sh` и `/opt/aecaVa/env/cdp.env`.
- Созданная СУБД `aecatetest` (имя базы данных по умолчанию) предназначена для хранения служебной информации.

⁶ Справочная информация по установке и настройке СУБД Jatoba приведена в Приложении Г настоящего руководства

4 УСТАНОВКА

Перед установкой функционального компонента «Центр валидации Aladdin Enterprise Certificate Authority» необходимо выполнить подготовку сервера.

4.1 Распаковка инсталляционного комплекта компонента

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

РЕД ОС 7.3

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

Astra Linux SE 1.7

```
sudo apt install ./<наименование пакета>.deb
```

Альт Сервер 10

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

- Инсталляционный rpm/deb-пакет будет автоматически распакован в директорию `/opt/aecaVa`.
- Структура распакованного инсталляционного rpm/deb-пакета приведена в Таблица 3.

Таблица 3 – Структура установочного комплекта Aladdin eCA

Структурный элемент	Назначение элемента
../dist	установочный комплект Изделия, а также используемых дополнительных инструментов
../dist/aeca_plugins.tar.gz	архив, содержащий плагин центра валидации Aladdin eCA
../dist/db_connectors.tar.gz	архив, содержащий набор драйверов, необходимых для работы WildFly с различными СУБД
../dist/sql	автоматически выполняемые при установке наборы SQL-запросов для подготовки БД
../dist/wildfly	автоматически развёртываемые при установке файлы конфигурации WildFly
../dist/ejbca_ce_7_4_3_2.tar.gz	архив, содержащий оригинальный установочный комплект EJBCA 7.4.3.2
../dist/wildfly-18.0.0.Final.tar.gz	архив, содержащий оригинальный установочный комплект WildFly 18
../env/email.env	первичные настройки рассылки уведомлений пользователям об истечении срока действия сертификата
../env/subjects.env	конфигурационный файл сервиса работы с субъектами
../properties	шаблоны файлов настроек
../scripts	установочные скрипты, которые необходимо выполнить пользователю при установке Изделия
../scripts/auxiliary_aeca_setup.sh	скрипт установки «Центра валидации Aladdin eCA»
../scripts/auxiliary_default_properties_setup.sh	скрипт первичной настройки АЕСА для установки

Структурный элемент	Назначение элемента
<code>../scripts/auxiliary_ejbca_database_setup.sh</code>	скрипт подготовки структуры БД для EJBCA
<code>../scripts/auxiliary_database_cleanup.sh</code>	скрипт очистки структуры БД для AeCA перед повторной установкой
<code>../scripts/auxiliary_ejbca_setup.sh</code>	скрипт установки EJBCA
<code>../scripts/auxiliary_wildfly_setup.sh</code>	скрипт установки Wildfly
<code>../scripts/config.sh</code>	скрипт установки параметров
<code>../scripts/install.sh</code>	скрипт установки «Центра валидации Aladdin eCA»
<code>../scripts/uninstall.sh</code>	скрипт удаления «Центра валидации Aladdin eCA»
<code>../scripts/update.sh</code>	скрипт обновления текущей версии ПО «Центра валидации Aladdin eCA»

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

4.2 Настройка параметров компонента

Внимание! При внесении изменений параметров СУБД в конфигурационный файл `/opt/aecaVa/scripts/config.sh` следует внести соответствующие изменения в файл `/opt/aecaVa/env/cdp.env` для синхронизации изменений.

4.2.1 Настройка config.sh

Обязательно необходимо задать значение параметра `aeca_https_server_hostname`.

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

- параметры конфигурации развёртывания сервисов центра валидации;
- параметры конфигурации центра валидации;
- параметры конфигурации сертификата технического Центра сертификации и сертификата пользователя (администратора) Центра валидации, создаваемого по умолчанию в процессе развёртывания сервера центра валидации;
- конфигурацию базы данных.

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

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

В Таблица 4 приводится описание параметров конфигурации.

Таблица 4 – Описание параметров конфигурации `config.sh`

Параметр	Значение параметра по умолчанию	Описание
<code>aeca_https_server_hostname</code>	"localhost"	Сетевое имя ПК, на которое производится установка Центра валидации

Параметр	Значение параметра по умолчанию	Описание
		В случае, если БД установлена на другое ПК, то следует изменить значение на «host»
aeca_install_directory	"/opt/aeca"	Директория, в которую будет осуществляться установка Центра валидации
aeca_user	"aeca"	Имя пользователя, от имени которого будет функционировать Центр валидации (пользователь будет создан в процессе установки)
aeca_database_type	"postgres "	Тип используемой СУБД
aeca_database_username	"ejbca"	Имя пользователя СУБД, используемого для работы Изделия
aeca_database_password	"ejbca"	Пароль пользователя СУБД используемого для работы Изделия
aeca_database_host	"localhost"	Сетевой адрес СУБД
aeca_database_port	"5432"	Порт, используемый для подключения к базе данных
aeca_database_name	"ejbctest"	Имя используемой Изделием базы данных в указанной СУБД
aeca_BASE_DN	"O=Aladdin test AECA CA, C=RU"	Базовое назначаемое имя в сертификате суперадминистратора, где: O=наименование организационной единицы C=страна
aeca_superadmin_cn	"InitialAdmin"	Наименование первоначально создаваемого администратора инициализации - суперадминистратора
aeca_ca_name	"ManagementTestCA"	Наименование первоначально создаваемого центра сертификации – служебного ЦС

4.2.2 Настройка cdp.env

Пропустите данный шаг, если имя пользователя базы данных, пароль пользователя базы данных, название базы данных совпадают с заданными по умолчанию «aeca», «aeca», «aecatest» соответственно.

- В другом случае отредактируйте конфигурационный файл /opt/aecaVa/env/cdp.env, выполнив команду:

```
sudo nano /opt/aecaVa/env/cdp.env
```

В листинге файла отредактируйте в соответствии с заданными при создании базы данных и параметрами файла /opt/aecaVa/scripts/config.sh следующие параметры:

Таблица 5 – Описание параметров конфигурации cdp.env

Параметр	Значение параметра по умолчанию	Описание
SERVER_ADDRESS	"0.0.0.0"	ip-адрес сетевого интерфейса cdp-service
SERVER_PORT	"8080"	Порт, назначенный для подключения к точке распространения Центра валидации

Параметр	Значение параметра по умолчанию	Описание
DB_URL	"jdbc:postgresql://localhost:5432/aecatest"	Путь подключения к СУБД, с указанием адреса сервера, где расположена СУБД и указания имени подключаемой СУБД
DB_USER	"aeca"	Имя пользователя, от имени которого будет функционировать Изделие (пользователь будет создан в процессе установки)
DB_PASSWORD	"aeca"	Пароль пользователя для входа в СУБД

4.3 Смена порта доступа

• Пропустите данный шаг, если используемый порт доступа 8888 (определённый по умолчанию) не требует изменения значения на произвольный из числа свободных.

Изменение порта доступа возможно только при выполнении первоначальной установки компонента «Центр валидации Aladdin eCA»! Не применимо в случае наличия предыдущей версии ПО, как активной, так и удаленной с сервера, на который производилась установка.

• Для изменения порта доступа выполните изменения в следующих файлах, указав выбранный порт доступа для нижеописанных переменных:

- /opt/aecaVa/env/subjects.env;
- /opt/aecaVa/env/validation.env;
- /opt/aecaVa/properties/web.properties.env;
- /opt/aecaVa/scripts/auxiliary_wildfly_setup.sh.env.

• Откройте файл /opt/aecaVa/env/subjects.env для редактирования, выполнив команду:

```
sudo nano /opt/aecaVa/env/subjects.env
```

Измените значение порта доступа по умолчанию (8888) на выбранное в следующих переменных:

- SERVER_PORT;
- AECA_CA_URL;
- AECA_LOGS_URL;
- AECA_VA_URL – для данной переменной используйте значение порта, которое используется на удалённом сервере, где развёрнут Центр валидации Aladdin eCA, если данный компонент отсутствует, то значение порта доступа оставляем по умолчанию (8888).

После изменения значения портов доступа в переменных вид содержимого файла subjects.env должен иметь следующий вид:

```
SERVER_PORT="значение порта доступа";
AECA_CA_URL="https://127.0.0.1:значение порта доступа/aeca";
AECA_VA_URL="https://127.0.0.1:значение порта доступа Центра валидации/aeca-ca";
AECA_LOGS_URL="https://127.0.0.1:значение порта доступа/aecaLogs";
```

Сохраните изменения.

• Откройте файл /opt/aecaVa/env/validation.env для редактирования, выполнив команду:

```
sudo nano /opt/aecaVa/env/validation.env
```

Измените значение порта доступа по умолчанию (8888) на выбранное в следующих переменных:

- AECA_SUBJECTS_URL;

- `AECA_VA_URL` – для данной переменной используйте значение порта, которое используется на удалённом сервере, где развёрнут Центр валидации Aladdin eCA, если данный компонент отсутствует, то значение порта доступа оставляем по умолчанию (8888).

После изменения значения портов доступа в переменных вид содержимого файла `validation.env` должен иметь следующий вид:

```
AECA_SUBJECTS_URL="https://127.0.0.1:значение порта доступа/aecaSubjects"
AECA_VA_PORT="значение порта доступа Центра валидации"
```

Сохраните изменения.

- Откройте файл `/opt/aecaVa/scripts/auxiliary_wildfly_setup.sh` для редактирования, выполнив команду:

```
sudo nano /opt/aecaVa/scripts/auxiliary_wildfly_setup.sh
```

Измените значение порта по умолчанию (8888) на выбранное в строке:

```
"wildfly_add "/socket-binding-group=standard-sockets/socket-
binding=aecahttps:add(port="\8888", interface="\aecahttps"
```

Сохраните изменения.

- Откройте файл `/opt/aecaVa/properties/web.properties` для редактирования, выполнив команду:

```
sudo nano -l /opt/aecaVa/properties/web.properties
```

Измените значение порта по умолчанию (8888) на выбранное в следующей переменной:

- `aecaserver.https.`

Сохраните изменения.

- После всех правок откройте доступ к выбранному порту, значение которого было прописаны на предыдущих шагах.
- После изменения порта доступа продолжите установку компонента «Центр валидации Aladdin eCA» в соответствии с настоящим документом.

4.4 Установка компонента

- Для инициализации процесса установки Центра валидации Aladdin eCA необходимо запустить скрипт с правами суперпользователя (от имени пользователя `root`, либо с использованием `sudo`):

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

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

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

- После инициализации процесса установки интерактивный инсталлятор запущен и пользователю будет предложено (в случае, если ранее на сервере был установлен Центр валидации Aladdin eCA):
 - установить обновление Aladdin eCA;
 - установить Aladdin eCA;
 - завершить работу инсталлятора.

Подтвердите выбор действия, вводом цифры 2 и процесс установки продукта будет запущен.

ВНИМАНИЕ! В процессе установки все действия подтверждаются выбором пункта ([Yes], [No] или [Cancel]) посредством нажатия соответствующей цифры (1, 2 или 3 соответственно).

После инициализации процесса установки интерактивный инсталлятор запущен автоматически выполняются действия, описанные ниже.

- Создание системного пользователя (если не существует) и соответствующей группы, от имени которых будет функционировать Изделие. Будет создана systemd-служба `aeca.service`, функционирующая от имени заданного пользователя.

- Пользователю будет предложено сформировать файлы конфигурации пакета ПО центра сертификации EJBCA из шаблонов в `/opt/aecaVa/properties` на основе значений, заданных при редактировании файла в `/opt/aecaVa/scripts/config.sh`.

- Для более тонкой настройки EJBCA возможно ручное редактирование данных файлов в соответствии с руководствами по эксплуатации EJBCA. Автоматически будут заменены только параметры со значением CHANGEIT:

- при выборе пункта [Yes] будет осуществлена замена CHANGEIT на значения из конфигурационного файла `/opt/aecaVa/scripts/config.sh`;
- при выборе пункта [No] будут использоваться файлы конфигурации в неизменном виде;

ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеются корректно сформированные `.properties` файлы конфигурации EJBCA, которые должны быть скопированы в каталог `/opt/aecaVa/properties` с заменой существующих файлов.

- при выборе пункта [Cancel] установка будет прекращена.

- Пользователю будет предложено установить сервер приложений Java EE:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки сервера приложений Java EE Wildfly-18.0.0.Final с подробным выводом процесса установки и конфигурирования сервера приложений в консоль пользователя;
- при выборе пункта [No] установка сервера приложений Java EE будет пропущена;

ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный сервер приложений, функционирующий по пути, указанному в параметре `aeca_appserver_home` скрипта конфигурации `/opt/aecaVa/scripts/config.sh`

- при выборе пункта [Cancel] установка будет прекращена.

- Пользователю будет предложено установить пакет ПО центра сертификации EJBCA CE 7.4.3.2:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки пакета ПО EJBCA CE 7.4.3.2 с подробным выводом процесса установки и конфигурирования в консоль пользователя;
- при выборе пункта [No] установка EJBCA будет пропущена;

ВНИМАНИЕ! Только для опытных пользователей! Данный сценарий рекомендуется только в том случае, когда уже имеется корректно настроенный EJBCA CE 7.4.3.2, функционирующий по пути, указанному в параметре `aeca_ejbca_home` скрипта конфигурации `/opt/aecaVa/scripts/config.sh`

- при выборе пункта [Cancel] установка будет прекращена.

- Пользователю будет предложено установить Центр валидации Aladdin eCA соответствующей версии:

- при выборе пункта [Yes] будет осуществлена автоматическая установка и конфигурирование входящего в комплект поставки Aladdin eCA;
- при выборе пункта [No] установка Aladdin eCA будет пропущена;
- при выборе пункта [Cancel] установка будет прекращена.

- После завершения установки в директории, выбранной в качестве пути для установки, будут содержаться:

- файл `generated_passwords.txt` (по умолчанию, расположен по пути `/opt/aeca/generated_passwords.txt`), содержащий все созданные и используемые пароли;
 - каталог «p12» (по умолчанию, расположен по пути `/opt/aeca/p12/superadmin.p12`), содержащий сертификат «Администратора Инициализации», необходимый для дальнейшей аутентификации через Web.
- В процессе установки в случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

4.4.1 Дополнительные возможные действия при установке

- Так как предусмотрен модульный процесс установки, возможны различные варианты установки:
 - возможно использование заранее подготовленных файлов настроек пакета ПО центра сертификации EJBCA;
 - если в каталоге «properties» уже находятся файлы конфигурации, необходимые пользователю, то при установке возможно пропустить шаг их формирования, ответив отрицательно за запрос инсталлятора;
 - возможно использование заранее подготовленного и корректно настроенного существующего сервера приложений WildFly. Для этого путь, по которому он размещён, должен соответствовать пути, описанному в `config.sh`. При установке возможно пропустить данный шаг, ответив отрицательно на запрос инсталлятора;
 - возможно использование заранее подготовленного и корректно настроенного установленного пакета ПО EJBCA, если путь, по которому он размещён, соответствует пути, описанному в `config.sh`. При установке возможно пропустить данный шаг, ответив отрицательно за запрос инсталлятора.
 - каждый шаг установки можно выполнить отдельно или повторно, запустив соответствующий скрипт, выполнив команду:

```
auxiliary<наименование_действия>.sh
```

- В случае отсутствия `config.sh` или наличие ошибок в `config.sh` каждый скрипт установки содержит определённые по умолчанию значения, достаточные для его автономной работы.

5 ПОДГОТОВКА СЕРВЕРА И СОВМЕСТНАЯ УСТАНОВКА ФУНКЦИОНАЛЬНЫХ КОМПОНЕНТОВ «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ECA» И «ЦЕНТРА ВАЛИДАЦИИ ALADDIN ECA»

При развёртывании Центра валидации и Центра сертификации на одном сервере рекомендовано соблюдать следующую очередность установки компонентов:

- 1) установка компонента «Центр валидации Aladdin Enterprise Certificate Authority»;
- 2) установка «Центра сертификации Aladdin Enterprise Certificate Authority».

5.1 Вариант (1) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»

Далее будет рассмотрен случай первоочерёдной установки в соответствии с рекомендацией, приведённой выше.

Порядок действий по установке компонента «Центр валидации Aladdin Enterprise Certificate Authority» приведён для первоочерёдной установки в соответствии с рекомендацией выше.

- Выполните подготовку сервера к установке компонента «Центр валидации Aladdin Enterprise Certificate Authority»:
 - выполните подключение репозитория в соответствии с разделом 3.2.1 настоящего руководства;
 - выполните установку набора инструментов Java, в соответствии с разделом 3.2.2 настоящего руководства;
 - выполните установку и настройку СУБД, в соответствии с разделом 3.2.3 настоящего руководства;

Важно: для каждого функционального компонента Aladdin eCA должна быть создана база данных с уникальным именем (по умолчанию: «aecatst» - для Центра валидации Aladdin eCA, «aecas» - для Центра сертификации Aladdin eCA). Одному пользователю (по умолчанию «aeca») должны быть назначены права на базу данных Центра валидации и базу данных Центра сертификации.

- Выполните установку компонента «Центр валидации Aladdin Enterprise Certificate Authority»:
 - распакуйте инсталляционный комплект Центра валидации Aladdin Enterprise Certificate Authority в соответствии с разделом 4.1 настоящего руководства;
 - получите путь до установленного пакета JDK-11, выполнив команду:

```
dirname $(dirname $(readlink -f $(which javac)))
```

- отредактируйте конфигурационный файл сервиса wildfly, выполнив команду:

```
sudo nano /opt/aecaVa/dist/wildfly/standalone.conf
```

- добавьте новую запись для переменной `JAVA_HOME`, установив значением путь до установленного пакета JDK-11, полученный на предыдущем шаге. Пример добавленной записи переменной `JAVA_HOME` в конфигурационном файле `standalone.conf` сервиса wildfly:

```
JAVA_HOME=/usr/lib/jvm/java-11-openjdk-11.0.17.0.8-3.e17.x86_64
```

- выполните настройку параметров компонента в соответствии с разделом 4.2 настоящего руководства;

- выполните установку компонента в соответствии с разделом 4.4 настоящего документа.

5.2 Вариант (2) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»

Далее будет рассмотрен случай установки компонента «Центр валидации Aladdin Enterprise Certificate Authority» на сервер, с предустановленным компонентом «Центр сертификации Aladdin Enterprise Certificate Authority» версии 2.0 или 2.1

- Выполните подготовку сервера к установке компонента «Центр валидации Aladdin Enterprise Certificate Authority»:

- выполните подключение репозитория в соответствии с разделом 3.2.1 настоящего руководства;
- выполните установку набора инструментов Java, в соответствии с разделом 3.2.2 настоящего руководства;
- выполните установку и настройку СУБД, в соответствии с разделом 3.2.3 настоящего руководства;

Важно: для каждого функционального компонента Aladdin eCA должна быть создана база данных с уникальным именем (по умолчанию: «aecatst» - для Центра валидации Aladdin eCA, «aecasа» - для Центра сертификации Aladdin eCA). Одному пользователю (по умолчанию «aеса») должны быть назначены права на базу данных Центра валидации и базу данных Центра сертификации.

- Выполните установку компонента «Центр валидации Aladdin Enterprise Certificate Authority»:
- распакуйте инсталляционный комплект Центра валидации Aladdin Enterprise Certificate Authority в соответствии с разделом 4.1 настоящего руководства;
- получите путь до установленного пакета JDK-11, выполнив команду:

```
dirname $(dirname $(readlink -f $(which javac)))
```

- отредактируйте конфигурационный файл сервиса wildfly, выполнив команду:

```
sudo nano /opt/aecaVa/dist/wildfly/standalone.conf
```

- добавьте новую запись для переменной `JAVA_HOME`, установив значением путь до установленного пакета JDK-11, полученный на предыдущем шаге. Пример добавленной записи переменной `JAVA_HOME` в конфигурационном файле `standalone.conf` сервиса wildfly:

```
JAVA_HOME=/usr/lib/jvm/java-11-openjdk-11.0.17.0.8-3.e17.x86_64
```

- для ранее установленного программного компонента «Центр сертификации Aladdin eCA» необходимо назначить обращения к компонентам JDK-17, определив в системе символические ссылки, выполнив команды и выбрав версию java 17 вводом соответствующей цифрой:

```
sudo update-alternatives --config java
sudo update-alternatives --config javac
sudo update-alternatives --config javap
```

- выполните настройку параметров компонента в соответствии с разделом 4.2 настоящего руководства;
- выполните установку компонента в соответствии с разделом 4.4 настоящего документа.

5.3 Вариант (3) установки компонента «Центр валидации Aladdin Enterprise Certificate Authority»

Установка компонента «Центр валидации Aladdin Enterprise Certificate Authority» и компонента «Центр сертификации Aladdin Enterprise Certificate Authority» версии 1.2 НЕ возможна.

6 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

- Создание резервных копий является неотъемлемой частью работы администратора Центров валидации.
 - Перед выполнением каких-либо настроек, изменений и обновлений функционального компонента следует в обязательном порядке выполнить резервное копирование.
 - Резервные копии создаются для:
 - содержимого каталога `/opt/aeca`;
 - базы данных `aecatest5`;
 - файла `/usr/bin/wildfly_pass`.
 - Резервное копирование осуществляется на локальный диск в папку `/opt/backup/` с указанием даты и времени создания резервной копии в имени архива. Каталог хранения архивов выбран исходя из того, что необходимо хранить резервные копии временно и не увеличивать размер занятого пространства жесткого диска. Для постоянного хранения требуется создать механизм переноса файлов.
 - Для постоянного хранения резервных копий следует:
 - создать каталог для хранения резервных копий;
 - составить сценарий для создания резервной копии;
 - настроить расписание вызова сценариев.

6.1 Создание полной резервной копии

- Создание полной резервной копии Центра валидации Aladdin Enterprise Certificate Authority осуществляется запуском скрипта с правами суперпользователя (root):

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

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

6.2 Расписание резервного копирования

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

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

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

- Укажите время и период запуска сценариев создания резервных копий:

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

где:

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

Примечание:

Выход и сохранение из редактора расписания осуществляется командой:

```
:wq!
```

Для просмотра настроенного расписания используется команда:

```
crontab -l
```

Внимание! В случаях, когда изменений между резервными копиями обнаружено не было, возможно отображение сообщения о некорректном срабатывании функции `stat` следующего вида: `tar: /tmp/1/inc/copia_*: Функция stat завершилась с ошибкой: No such file or directory`

6.3 Восстановление данных из резервной копии

Восстановление данных производится из папки `/opt/aecaCa/backup` на машине, где развернут функциональный компонент «Центр валидации Aladdin Enterprise Certificate Authority».

- Если восстановление происходит после переустановки ОС выполните:
 - создание каталога `/opt/aeca/backup`, выполнив команду:

```
sudo mkdir -p /opt/aeca/backup
```

- копирование в созданный каталог файла полной резервной копии;
- переход в каталог, выполнив команду:

```
cd /opt/aeca/backup/
```

- Выполните распаковку архива выбранной резервной копии во временную папку:
 - создайте временную папку, выполнив команду:

```
sudo mkdir -p /tmp/1/full
```

- скопируйте выбранный архив резервной копии во временную папку, выполнив команду:

```
sudo cp /opt/aeca/backup/<имя_файла>.zip /tmp/1/full
```

- перейдите в созданную папку с архивом резервной копии, выполнив команду:

```
cd /tmp/1/full
```

- распакуйте zip-архив, выполнив команду:

```
sudo unzip <имя_файла>.zip
```

В результате в текущем каталог должен быть получен файл `aeca.tar`.

- Распакуйте полученные архивы, выполнив команду:

```
sudo tar xfv aeca.tar
```

- Скопируйте полученные файлы, выполнив команды:

```
sudo mv /tmp/1/full/wildfly_pass /usr/bin
```

```
sudo cp -rf /tmp/1/full/opt/aeca /opt/
```

• Если восстановление резервной копии производится на ПК, где уже развёрнут Центр валидации, то необходимо предварительно удалить базу данных, выполнив команду:

```
sudo -u postgres dropdb "aecatest"
```

- Создайте базу данных (см. раздел 3 настоящего руководства), выполнив команды:

```
sudo -u postgres psql -c 'create database aecatest;'
```

```
sudo -u postgres psql -c 'create role aeca with superuser;'
```

```
sudo -u postgres psql -c 'alter database aecatest owner to aeca;'
```

```
sudo -u postgres psql -c 'grant all privileges on database aecatest to aeca;'
```

- Восстановите базу данных, выполнив команду:

```
sudo psql -U aeca -W aecatest < aecatest.sql
```

Внимание! База данных aecatest должна быть создана предварительно.

- После ввода команды восстановления базы данных необходимо ввести пароль пользователя «аеса».
- Перезапустите службу Центра валидации Aladdin eCA, выполнив команду:

```
sudo systemctl restart aeca.service
```

Внимание! В ОС RedOS запуск/перезапуск сервиса может быть заблокирован подсистемой selinux. Для отключения подсистемы selinux необходимо отредактировать её конфигурационный файл `sudo nano /etc/selinux/config`, где строку `SELINUX=permissive` заменить на `SELINUX=disabled`

- Для проверки состояния службы выполнить:

```
sudo systemctl status aeca.service
```

Если служба работает корректно, то должно быть указано состояние `active (running)`.

- Задайте права на объекты файловой системы программного компонента «Центр валидации Aladdin eCA», выполнив команды:

```
sudo chmod 777 /usr/bin/wildfly_pass
sudo chown aeca /usr/bin/wildfly_pass
sudo chown aeca -R /opt/aec
```


7 ОБНОВЛЕНИЕ

7.1 Назначение обновлений

Обновление базы данных и модулей функционального компонента «Центр валидации Aladdin Enterprise Certificate Authority» обеспечивает актуальность версии ПО.

Выполняемые обновлениями задачи:

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

7.2 Информирование потребителей о выпуске обновлений

- Компания ведет учет покупателей компонента «Центр валидации Aladdin Enterprise Certificate Authority».
- Выполняется регистрация следующей информации:
 - наименование организации;
 - адрес организации;
 - контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).
- Уведомление пользователей о выпуске обновлений «Центра валидации Aladdin Enterprise Certificate Authority Certified Edition» выполняется путем публикации информации на официальном сайте Компании (<https://www.aladdin-rd.ru/company/pressroom/news>) и (или) с использованием рассылки электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счет применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлом обновлений может предоставляться обновленная документация для использования программы.

7.3 Получение обновлений потребителем

- Получение файлов обновлений программного средства и соответствующих им контрольных сумм возможно:
 - с использованием электронной почты;
 - путем загрузки с Web-сайта изготовителя (производителя) по адресу <https://aladdin-rd.ru/support>;
- Проверка квалифицированной электронной подписи изготовителя (производителя) для файлов обновлений программного средства и файлов соответствующих им контрольных сумм выполняется любым доступным способом, если сведения о наличии обновления не предписывают иной порядок проверки подлинности и целостности обновления.

7.4 Контроль целостности обновления ПО

Контроль целостности обновления программы выполняется путем расчета контрольной суммы полученного дистрибутива, с использованием алгоритма MD5, с помощью утилиты md5sum, и её сравнением со значением контрольной суммы для этого обновления .

7.5 Процедура установки обновлений

На случай, если во время обновления произойдет сбой, рекомендуем предварительно сделать резервную копию программы и базы данных (см. раздел 6 настоящего документа), из которой можно будет восстановить данные.

Для обновления продукта:

- перенесите дистрибутив с обновленной версией компонента на сервер с установленным «Центром валидации Aladdin Enterprise Certificate Authority» любым удобным способом;
- проверьте целостность дистрибутива путем подсчёта контрольной суммы;
- выполните распаковку инсталляционного комплекта:

РЕД ОС 7.3 `sudo dnf install aeca-*.rpm`

Astra Linux SE
1.7 `sudo dpkg -i ./aeca-*.deb`

Альт Сервер 10 `sudo dnf install aeca-*.rpm`

- запустите установку продукта в режиме обновления, выполнив команду:

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

- установщик обнаружит установленную версию функционального компонента и предложит выбрать необходимое действие в интерактивном режиме:
 - o удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программного компонента;
 - o выполнить обновление установленной версии до актуальной версии программного компонента;
 - o прервать процесс установки;
- для выбора продолжения процесса обновления, введите в терминале цифру «2»;
- после установки обновления запустите браузер, удалите файлы cookie и данные сайтов, очистите кэш-память браузера;
- запустите обновленный компонент «Центр валидации Aladdin Enterprise Certificate Authority»;
- проверьте версию обновленного компонента в окне Центра валидации «О программе».

7.6 Критерий успешности установки обновления

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

8 УДАЛЕНИЕ ПРОГРАММЫ

8.1 Инициализация процесса удаления

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

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

В результате выполнения данного действия будут полностью уничтожены:

- все добавленные при установке компонента системные службы;
- все добавленные при установке компонента пользователи и группы;
- все добавленные при установке компонента файлы и структура каталогов.

Все внесённые изменения будут выведены в консоль.

8.2 Удаление установочного пакета

Удаление пакета повлечёт за собой удаление установочного комплекта в каталоге `/opt/aecaCa/`.

- Для удаления необходимо выполнить следующую команду:

РЕД ОС 7.3

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

Astra Linux SE 1.7

```
sudo apt remove aeca-*.deb
```

Альт Сервер 10

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

9 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

9.1 Удаление БД «aecatetest»

Для удаления ранее созданной базы данных «aecatetest» (имя БД, заданное по умолчанию) необходимо выполнить команды с правами суперпользователя (root или sudo):

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

```
sudo -i -u postgres  
  
psql;
```

- Для предотвращения возможности новых подключений выполните команду:

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

- Для закрытия всех текущих сессий выполните команду:

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

- Удаляем базу данных, выполнив команду:

```
DROP DATABASE aecatetest;
```

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

```
exit
```

9.2 Удаление пользователя БД «aeca»

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

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

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

- Удалите пользователя «aeca» в Postgres, выполнив команду:

```
dropuser aeca -i
```

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

```
exit
```

- Перезапустите СУБД Postgres, выполнив команду:

```
sudo systemctl restart postgresql
```

10 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения
<p>Ошибка при запуске скрипта установки install.sh «error obtaining MAC configuration for user «aeca»»</p>	<p>У пользователя postgres нет прав на чтение БД атрибутов конфиденциальности</p>	<p>Для предоставление дополнительных прав пользователю postgres выполните команды:</p> <pre>sudo usermod -a -G shadow postgres sudo setfacl -d -m u:postgres:r /etc/parsec/macdb sudo setfacl -R -m u:postgres:r /etc/parsec/macdb sudo setfacl -m u:postgres:rx /etc/parsec/macdb</pre>

ПРИЛОЖЕНИЕ А. УСТАНОВКА РЕПОЗИТОРИЕВ

А.1 Установка репозитория и подключение зависимостей для сервера под управлением ОС РЕД ОС 7.3

Перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториях.

- Для ОС РЕД ОС 7.3 репозитории настроены по умолчанию для скачивания из сети Интернет. Для проверки доступности и готовности к дальнейшим командам следует установить необходимые пакеты из состава ОС, выполнив команды:

```
sudo yum install -y git wget ant psmisc bc patch  
sudo yum install tar unzip
```

При ошибке следует проверить наличие интернет-соединения.

- Также эти зависимости возможно установить с носителя, на котором находится комплект поставки целевой ОС в случае, если подключение к сети Интернет отсутствует. Для этого:

- вставьте USB-носитель в компьютере без Интернета;
- перейдите в каталог носителя, содержащий два файла;
- для обновления репозитория выполните команду:

```
sudo apt-offline install
```

- для установки зависимостей выполните команду:

```
sudo yum install tar unzip
```

А.2 Установка репозитория и подключение зависимостей для сервера под управлением ОС Astra Linux Special Edition 1.7

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

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

- Укажите ссылки на следующие репозитории:

```
sudo apt install -y git wget ant psmisc bc patch  
sudo apt install tar unzip
```

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

А.3 Установка репозитория и подключение зависимостей для сервера под управлением ОС Альт Сервер 10

Для ОС Альт Сервер 10 не требуется производить установку дополнительных репозиториях и подключение зависимостей.

ПРИЛОЖЕНИЕ Б. УСТАНОВКА OPEN JDK

- Для корректной работы ПО АеСА требуется установить OpenJDK версии 11, выполнив команды (под учетной записью root или sudo):

РЕД ОС 7.3

```
sudo dnf install java-11-openjdk
sudo dnf install java-11-openjdk-devel
```

Astra Linux SE 1.7

```
sudo apt install openjdk-11-jdk
```

Альт Сервер 10

```
sudo apt-get ./install java-11-openjdk-devel
```

- После установки новой версии по умолчанию будет использоваться именно она. Проверить используемую версию можно следующей командой:

```
java -version
```

- Проверьте, что все компоненты java (java, javac, javap) на соответствие выбранной версии 11:

РЕД ОС 7.3

Astra Linux SE 1.7

```
sudo update-alternatives --config java
sudo update-alternatives --config javac
sudo update-alternatives --config javap
```

Альт Сервер 10

-

- Получите путь до установленного пакета JDK-11, выполнив команду:

```
dirname $(dirname $(readlink -f $(which javac)))
```

- Установите полученный на предыдущем шаге путь в значение переменной `JAVA_HOME`, выполнив команду:

```
sudo nano /etc/java/java.conf
```

ПРИЛОЖЕНИЕ В. УСТАНОВКА И НАСТРОЙКА СУБД POSTGRESQL⁷

В.1 Установка СУБД PostgreSQL

- Установите СУБД PostgreSQL, выполнив команду:

РЕД ОС 7.3

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

Astra Linux SE 1.7

```
sudo apt install postgresql-11
```

Альт Сервер 10

```
sudo apt-get install ./postgresql-server
```

- Выполните установку пакета `postgresql-contrib`:

РЕД ОС 7.3

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

Astra Linux SE 1.7

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

Альт Сервер 10

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

- Произведите инициализацию БД, выполнив команду:

РЕД ОС 7.3

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

Astra Linux SE 1.7

```
-
```

Альт Сервер 10

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

- Запустите PostgreSQL, выполнив команду:

```
sudo service postgresql start
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

• Для ОС РЕД ОС 7.3 и Альт Сервер 10 отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf` и измените параметры для успешного локального подключения пользователя к базе данных:

```
sudo nano /var/lib/pgsql/data/pg_hba.conf
```

- в открывшемся файле `pg_hba.conf` сделайте замены согласно Таблица 6.

⁷ Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <http://www.postgresql.org/docs/9.2/static/index.html>

Таблица 6 – Выдержка из файла `pg_hba.conf` для редактирования

<code>local all all peer</code>	на	<code>local all all trust</code>
<code>host all all 127.0.0.1/32 ident</code>	на	<code>host all all 127.0.0.1/32 password</code>
<code>host all all ::1/128 ident</code>	на	<code>host all all ::1/128 password</code>

После вышеуказанных изменений строки должны иметь следующий вид:

<code>local</code>	<code>all</code>	<code>all</code>		<code>trust</code>
<code>#IPv4 local connection:</code>				
<code>host</code>	<code>all</code>	<code>all</code>	<code>127.0.0.1/32</code>	<code>password</code>
<code>#IPv6 local connection:</code>				
<code>host</code>	<code>all</code>	<code>all</code>	<code>::1/128</code>	<code>password</code>

- сохраните изменения.

- Для ОС Astra Linux SE 1.7 откройте файл `/etc/parsec/mswitch.conf` и измените параметр для создания пользователя СУБД PostgreSQL, который не назначен в ОС Astra Linux Special Edition 1.7:

<code>zero_if_notfound: no</code>	на	<code>zero_if_notfound: yes</code>
-----------------------------------	----	------------------------------------

После вышеуказанных изменений строки должны иметь следующий вид:

<code>zero_if_notfound: yes</code>

Перезапустите СУБД PostgreSQL для вступления изменений в силу, выполнив последовательно команды:

<code>sudo systemctl start postgresql</code>
--

Отредактируйте файл `/etc/postgresql/11/main/pg_hba.conf` и измените параметры для успешного локального подключения пользователя к базе данных:

<code>local all all peer</code>	на	<code>local all all trust</code>
---------------------------------	----	----------------------------------

- Сохраните изменения и выполните перезапуск СУБД PostgreSQL для вступления изменений в силу, выполнив команду:

<code>sudo systemctl restart postgresql</code>
--

В.2 Создание и настройка СУБД PostgreSQL

Требования к настройке предварительно установленной СУБД PostgreSQL:

- создание пользователя, от имени которого будет осуществляться всё 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 команду:

<code>sudo systemctl start postgresql</code>
--

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

<code>sudo systemctl enable postgresql</code>

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

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

- Создайте пользователя базы данных, выполнив команды:

```
psql  
CREATE USER aeca;
```

где `aeca` – задаваемое имя пользователя по умолчанию, в случае указания отличного имени пользователя, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

- Задайте пароль пользователю, выполнив команды:

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

где `'aeca'` – задаваемый пароль пользователя по умолчанию. В случае указания отличного пароля, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecatest;
```

где `aecatest` – задаваемое имя базы данных по умолчанию, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

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

```
ALTER DATABASE aecatest OWNER TO aeca;
```

• Наделите созданного пользователя полными правами доступа к созданной базе данных, выполнив команду:

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

- Назначьте созданного пользователя суперпользователем и завершите действия, выполнив команды:

```
ALTER USER aeca SUPERUSER;
```

```
\q
```

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

```
exit
```

- Перезапустите СУБД PostgreSQL, выполнив команду:

```
sudo systemctl restart postgresql
```

ПРИЛОЖЕНИЕ Г. УСТАНОВКА И НАСТРОЙКА СУБД JATOBA⁸

Г.1 Установка СУБД JatoBa из локального репозитория

- Создайте каталог `/localrepo`, выполнив команду:

```
mkdir /localrepo
```

- В каталог `/localrepo` скопируйте необходимые файлы для установки СУБД JatoBa 4.

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

- Дистрибутив СУБД JatoBa 4 содержит:

РЕД ОС 7.3	<ul style="list-style-type: none"> каталог <code>/packages</code>; каталог <code>/repodata</code>; файл ключа <code>RPM-GPG-KEY-Jatoba</code>
Astra Linux SE 1.7	<ul style="list-style-type: none"> каталог <code>/pool</code>; каталог <code>/dists</code>; файл ключа <code>DEB-GPG-KEY-Jatoba</code>.
Альт Сервер 10	<ul style="list-style-type: none"> каталог <code>/base</code>; каталог <code>/RPMS.classic</code>; файл ключа <code>RPM-GPG-KEY-Jatoba</code>.

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

```
ls -l
```

- Установите открытый ключ репозитория командой:

РЕД ОС 7.3	<code>sudo rpm --import /localrepo/RPM-GPG-KEY-Jatoba</code>
------------	--

Astra Linux SE 1.7	<code>sudo apt-key add /localrepo/DEB-GPG-KEY-Jatoba</code>
--------------------	---

Альт Сервер 10	-
----------------	---

- Создайте файл с описанием локального репозитория в системе, в котором разместите следующее описание:

РЕД ОС 7.3	<code>jatoba-4]</code>	файл с описанием репозитория <code>/etc/yum.repos.d/jatoba-4.repo</code>
------------	------------------------	---

⁸ Подробное описание приведено в официальной документации на JatoBa, размещённой по адресу <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>

```
name=Jatoba 4 Official Repository
baseurl=file:///localrepo
enabled=1
gpgcheck=0
gpgkey=file:///localrepo/RPM-GPG-KEY-
Jatoba
```

Astra Linux SE 1.7

```
deb file:///localrepo stable non-
freename=Jatoba 4 Official Repository
```

файл с описанием репозитория
/etc/apt/sources.list.d/jatoba-4.list

Альт Сервер 10

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

файл с описанием репозитория
/etc/apt/sources.list.d/jatoba-4.list

- Обновите описания пакетов командой:

РЕД ОС 7.3

```
sudo dnf makecache
```

Astra Linux SE 1.7

```
sudo apt-get update
```

Альт Сервер 10

```
sudo apt-get update
```

- Установите основные пакеты СУБД Jatoba 4 командой:

РЕД ОС 7.3

```
sudo dnf install jatoba4-client jatoba4-contrib jatoba4-libs jatoba4-
server
```

Astra Linux SE 1.7

```
sudo apt-get install jatoba4-client jatoba4-contrib jatoba4-libs
jatoba4-server
```

Альт Сервер 10

```
sudo apt-get install jatoba4-client jatoba4-contrib jatoba4-libs
jatoba4-server
```

Пакеты `jatoba4-client`, `jatoba4-contrib`, `jatoba4-libs` и `jatoba4-server` являются обязательными для установки СУБД.

- Перейдите в директорию расположения исполняемых файлов СУБД Jatoba» 4 посредством команды:

```
cd /usr/jatoba-4/bin/
```

- Инициализируйте каталог данных СУБД Jatoba 4 при помощи команды:

```
./jatoba-setup initdb jatoba-4
```

- Пройдите процедуру активации. Активатор находится в каталоге `/usr/jatoba-4/bin`.

Активация возможна онлайн и офлайн. Онлайн-активация означает, что запрос на активацию, формирование и сохранение лицензии будет выполнено непосредственно с этого компьютера (Для проведения онлайн-активации требуется подключение к сети Internet.). Офлайн-активация означает, что на данном компьютере будет выполнен только запрос активации (сгенерирован специальный файл запроса). Саму активацию необходимо будет выполнить на компьютере, имеющем доступ в сеть Internet. Ниже приведены действия для онлайн-активации.

- Перейдите в каталог `/usr/jatoba-4/bin` и запустите активатор:

```
./jactivator
```

- введите лицензионный ключ;
- введите адрес электронной почты администратора СУБД;
- на запрос способа активации укажите «1»;
- при первоначальной установке СУБД Jatoba 4 выберете режим активации «Обычная активация», введя значение «1» (при окончании срока действия лицензии следует выбрать режим активации «Реактивация», введя значение «2». Дальнейший порядок установки при реактивации лицензии идентичен нижеописанному);
- введите ключ активации СУБД, полученный из письма, пришедшего на электронную почту администратора СУБД;
- укажите директорию сохранения файла лицензии по пути `/usr/jatoba-4/bin`;
- после получения сообщения «Лицензия выпущена. Файл лицензии успешно сохранен» онлайн-активация лицензии является завершенной;
- разместите файл лицензии в каталоге `/usr/jatoba-4/bin`;
- установите лицензию в каталог данных командой:

```
cp jatoba.cer /usr/jatoba-4/bin/
chown postgres.postgres /usr/jatoba-4/bin/jatoba.cer
```

- Для пользовательского контроля необходимо проверить права на файл лицензии, который должен быть доступен на чтение системному пользователю `postgres`, выполнив команду:

```
ls -l jatoba.cer
```

- Если права некорректны, необходимо выполнить команду:

```
chown postgres.postgres jatoba.cer
```

- Перед запуском СУБД в конце конфигурационного файла `/var/lib/jatoba/4/data/postgresql.conf`, в разделе «LICENSER OPTION AND PARAMETERS» проверьте наличие параметров и, в случае их отсутствия, внесите следующие данные, как указано в Таблица 7.

Таблица 7 – Задаваемые параметры в конфигурационном файле `postgresql.conf`

Наименование параметра	Наименование параметра (англ.)	Значение
Продукт	lic_product_name	jatoba
Файл сертификата	lic_file_path	/usr/jatoba-4/bin/jatoba.cer
Сервер лицензирования	lic_server_addr	https://license.gaz-is.ru

- сохраните изменения.

- Отредактируйте файл `var/lib/jatoba/4/data/pg_hba.conf` и измените параметры для успешного локального подключения пользователя к базе данных:

```
sudo nano var/lib/jatoba/4/data/pg_hba.conf
```

- в открывшемся файле `pg_hba.conf` сделайте замены согласно указанному в Таблица 8.

Таблица 8 – Выдержка из файла `pg_hba.conf` для редактирования

<code>local all all peer</code>	на	<code>local all all trust</code>
<code>host all all 127.0.0.1/32 ident</code>	на	<code>host all all 127.0.0.1/32 password</code>
<code>host all all ::1/128 ident</code>	на	<code>host all all ::1/128 password</code>

После вышеуказанных изменений строки должны иметь следующий вид:

<code>local</code>	<code>all</code>	<code>all</code>		<code>trust</code>
<code>#IPv4 local connection:</code>				
<code>host</code>	<code>all</code>	<code>all</code>	<code>127.0.0.1/32</code>	<code>password</code>
<code>#IPv6 local connection:</code>				
<code>host</code>	<code>all</code>	<code>all</code>	<code>::1/128</code>	<code>password</code>

- Сохраните изменения и выполните перезапуск СУБД Jatoba 4 для вступления изменений в силу, выполнив команду:

```
sudo systemctl restart jatoba-4
```

Г.2 Создание и настройка СУБД Jatoba 4

Требования к настройке предварительно установленной СУБД Jatoba 4:

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

Возможно использование локальной СУБД или удаленной, доступной для подключений.

- Запустите Jatoba 4, выполнив команду:

```
sudo systemctl start jatoba-4
```

Добавьте запуск Jatoba-4 в автозагрузку, выполнив команду:

```
sudo systemctl enable jatoba-4
```

- Зайдите под пользователем `postgres` в Jatoba 4, выполнив команду:

РЕД ОС 7.3

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

Astra Linux SE 1.7

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

Альт Сервер 10

```
sudo -postgres -s /bin/bash
-bash-4.4$ /usr/jatoba-4/bin/psql
psql
```

- Создайте пользователя базы данных, выполнив команды:

```
psql
CREATE USER aeca;
```

где `aeca` – задаваемое имя пользователя, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

- Задайте пароль пользователю, выполнив команды:

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

где `'aeca'` – задаваемый пароль пользователя, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecatest;
```

где `aecatest` – задаваемое имя базы данных, в случае указания отличного имени базы данных, требуется соответственно отредактировать конфигурационные файлы (см. подраздел 4.2).

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

```
ALTER DATABASE aecatest OWNER TO aeca;
```

• Наделите созданного пользователя полными правами доступа к созданной базе данных, выполнив команду:

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

- Назначьте созданного пользователя суперпользователем и завершите действия, выполнив команды:

```
ALTER USER aeca SUPERUSER;
```

```
\q
```

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

```
exit
```

- Перезапустите СУБД Jatoba 4, выполнив команду:

```
sudo systemctl restart jatoba-4
```

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

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

где `aecatest` – имя созданной базы данных.

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

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

- официальная документация РЕД ОС 7.1
(адрес: <https://redos.red-soft.ru/base/manual/?ysclid=I5gg69co40129982631>);
- официальная документация Astra Linux Special Edition 1.7
(адрес: <https://wiki.astralinux.ru/pages/viewpage.action?pageId=137563555&ysclid=I5gg3t48tj885563182>);
- официальная документация Альт Сервер 10
(адрес: <https://www.basealt.ru/alt-server/docs>);
- официальная документация Postgres
(адрес: <http://www.postgresql.org/docs/12/index.html>);
- официальная документация Jatoba 4
(адрес: <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>);

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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 токену, программному или аппаратному модулю безопасности Hardware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

Сервис валидации – служба, составная часть Центра сертификации, отвечающая за предоставление информации о действительности сертификатов. Предоставляет сервисы CRL DP, OCSP.

Сертификат – выпущенный центром сертификации цифровой документ в форматах x509v3 или другом поддерживаемом формате, подтверждающий принадлежность владельцу закрытого ключа или каких-либо атрибутов и предназначенный для аутентификации в информационной системе.

Список отозванных сертификатов (Certificate Revocation List – **CRL**) – список аннулированных (отозванных) сертификатов, издается центром сертификации по запросу или с заданной периодичностью на основании запросов об отзыве сертификатов.

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

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

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

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

