ЦЕНТР СЕРТИФИКАТОВ ДОСТУПА

Aladdin Enterprise Certificate Authority Certified Edition

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

Изделие	RU.АЛДЕ.03.01.020-01
Документ	32 01-1
Версия	2.0.1.406
Автор	Липатова Ю.А.
Листов	74
Дата	14.05.2024

1.1. 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 ВСЛЕДСТВИЕ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И/ИЛИ ЛЮБОГО КОМПОНЕНТА ОПИСАННОГО ПРОДУКТА, ДАЖЕ ЕСЛИ АО «Аладдин Р.Д.» БЫЛО ПИСЬМЕННО УВЕДОМЛЕНО О ВОЗМОЖНОСТИ ПОДОБНЫХ УБЫТКОВ.

1.2. 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.

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.

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

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

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.

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

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 использоваться каким-либо противоречащим закону и условиям настоящего соглашения образом. ПО является предметом дополнительного экспортного контроля, относящегося к Вам или Вашей юрисдикции. Вы гарантируете, что будете соблюдать накладываемые ограничения на экспорт и реэкспорт ПО.

Разное

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

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

АННОТАЦИЯ

Настоящий документ представляет собой первую часть руководства администратора программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»[1].

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

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

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

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

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

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

Таблица 1 – Соответствие документации требованиям доверия – раздел 16 «Требования к разработке эксплуатационной документации»

Требования доверия (16.1 Руководство администратора должно содержать описание)	Раздел настоящего документа, в котором представлено свидетельство
действий по приёмке поставленного средства	часть 1, раздел 3 «Действия по приёмке»
действий по безопасной установке и настройке средства	часть 1, раздел 1, подраздел 1.7 «Действия по безопасной установке и настройке программы»
действий по реализации функций безопасности среды функционирования средства	часть 1, раздел 1, подраздел 1.8 «Действия по реализации функций безопасности среды функционирования программы»

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

[1] Далее по документу – программа, программное средство, Aladdin eCA CE

Содержание

1 ВВЕДЕНИЕ

1.1 Назначение программы

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» 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.

1.2 Функции программы

Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» (далее - Aladdin eCA) реализует следующие основные функции:

- выпуск сертификатов Центра сертификации;
- выпуск сертификатов для субъектов доступа;
- экспорт открытого ключа сертификата, сертификата в контейнере #pkcs12 (с закрытым ключом), цепочки сертификатов центра сертификации на ключевой носитель;
- управление статусом сертификата доступа (отозвать или приостановить действие выпущенного сертификата субъекта, активировать);
- формирование списка всех выпущенных сертификатов в файл формата, удобного для просмотра;
- управление учетными записями пользователей (создание, назначение роли, удаление, редактирование, назначение доступа к субъектам ресурсных систем);
- управление ресурсными системами (подключение, обновление списка групп и субъектов);
- управление списком отозванных сертификатов (настройка периодов формирования и действия CRL, публикация CRL в ручном режиме);
- регистрация Центров валидации;
- управление журналом событий (архивация, очистка, экспорт журнала событий по выбранным критериям);
- разграничение доступа к интерфейсу и функционалу программы (на основании ролей).

1.3 Основные компоненты

«Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» является клиент-серверным web-приложением и включает программный компонент:

- RU.АЛДЕ.03.01.038 Центр сертификации Aladdin Enterprise Certificate Authority[2], состоящий из:
  - RU.АЛДЕ.03.01.040 Серверная часть центра сертификации. Серверная часть центра сертификации реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения.
  - RU.АЛДЕ.03.01.041 Клиентская часть центра сертификации. Клиентская часть центра сертификации реализует интерфейс, с помощь которого обеспечивается взаимодействие пользователя и программного компонента «RU.АЛДЕ.03.01.040 Серверная часть Центра сертификации».

[2] Далее по тексту – программный компонент, компонент, Aladdin eCA, AeCA

1.4 Комплект поставки

Комплект поставки включает в себя:

- Программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» на носителе оптической записи (rpm-пакет для установки на ОС РЕД ОС 7.3 или Альт 8 СП, релиз 10, deb-пакет для установки на Astra Linux Special Edition 1.7 Смоленск);
- Копия сертификата соответствия системы сертификации средств защиты информации по требованиям безопасности информации (рег. № РОСС RU.0001.01БИ00) в цифровом или бумажном виде;
- Контрольные суммы дистрибутивов программы (rpm и и deb-пакеты) и исполняемых файлов (см. Таблица 8) программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» на носителе оптической записи;
- Эксплуатационная документация:
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр. Приложение. Свидетельства о приёмке, упаковке и маркировке»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Описание применения»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certificate Authority»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certificate Authority»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Приложение Б. Описание REST-API»;
  - «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство пользователя».

1.5 Имя пакета компонентов поставки

Имя пакета компонентов поставки представлено в формате:

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

1.6 Доступные роли

Управление центрами сертификации осуществляют сотрудники организации, обладающие правами администратора и оператора, в соответствии с назначенными правами.

Для безопасной и успешной эксплуатации ПО «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition определяются следующие роли:

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

- администратор. Пользователь с ролью «Администратор» должен иметь неограниченные права доступа к операционной системе и серверу, на котором развёрнуто программное средство «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», а также доступ через web-интерфейс или программный интерфейс API к функциональным задачам, к функциям управления учетными записями Центра сертификации. Все учётные записи могут быть созданы, отредактированы, удалены или заблокированы администратором.

Доступные действия для существующих ролей пользователей программного средства приведены в Таблица 2.

Таблица 2 – Полномочия пользователей программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»

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

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

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

1.7 Режимы функционирования программы

Основным режимом функционирования программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» является нормальный режим.

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

Функционирование Корневого и/или Подчинённого Центра сертификации предусматривает автономный режим (Stand alone operation) или сетевой режим работы.

1.8 Действия по безопасной установке и настройке программы

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

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

Настройка программного средства должна проводится привилегированным пользователем с правами администратора, допускаемым к установке и настройке программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

1.9 Действия по реализации функций безопасности среды функционирования программы

Для безопасной работы программного средства в среде операционной системы должно обеспечиваться:

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

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

2.1 Требования к программному обеспечению

2.1.1 Требования к среде функционирования серверной части центра сертификации

Среда функционирования серверной части центра сертификации:

- Операционная системы:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск»;

    или
  - РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;

    или
  - ОС Альт 8 СП, релиз 10, вариант исполнения Сервер;
- поддерживаемые СУБД:
  - PostgreSQL из состава сертифицированной операционной системы;

    или
  - Postgres Pro;

    или
  - Jatoba 4;
- поддерживаемая среда исполнения Java:
  - Java Axiom JDK Certified (компонент JRE);
- поддерживаемые web-серверы:
  - Apache2 из состава сертифицированной операционной системы;

    или
  - Nginx из состава сертифицированной операционной системы;
- поддерживаемые ресурсные системы:
  - Samba DC;
  - Free IPA;
  - ALD PRO;
  - РЕД АДМ;
  - Microsoft AD.

2.1.2 Требования к среде функционирования клиентской части центра сертификации

Среда функционирования клиентской части центра сертификации:

- Операционная система:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск»;

    или
  - РЕД ОС версия 7.3, сертифицированная редакция, конфигурация «Сервер»;

    или
  - ОС Альт 8 СП, релиз 10, вариант исполнения Рабочая станция;

- браузер из состава сертифицированной операционной системы;
- JC-WebClient 4.3.3 (для 64-битных систем)[3].

2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования ПО «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition»:

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

Таблица 3 – Системные требования, предъявляемые к Центру сертификации Aladdin Enterprise Certificate Authority Certified Edition

Приложение	Системные требования	Тип внедрения		
		Малое внедрение (до 1000 сертификатов и 5 одновременных соединений)	Среднее внедрение (до 20000 сертификатов и 15 одновременных соединений)	Крупное внедрение (до 100000 сертификатов и 50 одновременных соединений)
СУБД	ОЗУ, GB	2	3	4
	CPU, (core)	2	4	4
	HDD, GB	6	12	18
Приложение АЕСА	ОЗУ, GB	6	8	16
	CPU, (core)	2	4	6
	HDD, GB	40	60	300
ОС	ОЗУ, GB	4	4	4
	CPU, (core)	2	2	2
	HDD, GB	20	20	20
Итого	ОЗУ, GB	**12**	**15**	**24**
	CPU, (core)	**6**	**10**	**12**
	HDD, GB	**58**	**92**	**328**

- VGA-совместимый видеоадаптер;
- монитор с поддерживаемым разрешением экрана:
  - 1920x1080 16:9 HD 1080;

[3] При установке дополнительного программного обеспечения изделие обеспечивает возможность работы с ключевыми носителями (электронными ключами), при этом класс защиты не обеспечивается.

  - 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;
- usb 2.0 тип A или совместимые.
- Поддерживаемые модели электронных ключей:
  - JaCarta PKI;
  - JaCarta PRO.

3 ДЕЙСТВИЯ ПО ПРИЁМКЕ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

Приёмка программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» предусматривает:

- проверку комплектности программного средства;
- оценку результата подсчёта контрольной суммы для контроля целостности по контрольному списку или по указанным значениям контрольных сумм в «RU.АЛДЕ.03.01.020-01 30 01-1 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр».

3.1 Проверка комплектности

Проверку комплектности программного продукта производят путём сверки комплектности поставленного программного продукта с комплектностью, указанной в разделе 3 «RU.АЛДЕ.03.01.020-01 30 01-1 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр».

3.2 Подсчёт контрольной суммы

Подсчёт контрольной суммы необходимо произвести с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0», алгоритм «ГОСТ 34.11-2012», 256 бит, пользователем с правами администратора на рабочей станции, оборудованной устройством чтения CD/DVD-дисков, под управлением программного средства в следующей последовательности:

- установить компакт-диск с дистрибутивом в устройство чтения CD/DVD-дисков;
- выполнить в командной строке:

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

- перейти в директорию, содержащую исполняемый модуль программы «ФИКС-UNIX 1.0» (ufix), и выполнить 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
```

- открыть в браузере полученный файл выполнить в командной строке:

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

- выполнить команду:

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

3.3 Сравнение контрольной суммы

Сравнить значение контрольной суммы в строке «ВСЕГО», выданное на экран в результате подсчёта контрольных сумм программой «ФИКС-Unix 1.0», со значением, указанными в таблице 2 «RU.АЛДЕ.03.01.020-01 30 01-1 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр».

Контрольные суммы DVD-диска продукта, рассчитанные с использованием программы подсчета контрольных сумм «ФИКС-Unix 1.0» должны соответствовать значениям, приведенным в таблице 2 «RU.АЛДЕ.03.01.020-01 30 01-1 Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Формуляр».

4 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

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

В зависимости от установленной на сервере типа операционной системы проведите подготовку сервера согласно пункту 5.1 или 5.2 настоящего руководства.

4.1 Таблица сетевого взаимодействия

Ниже приведён список портов (см. Таблица 4), которые необходимо открыть для полноценной работы программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

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

Таблица 4 – 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
443	TCP	HTTPS	Для подключения к программному компоненту «Центр Сертификации»	Да
1100	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «certificate-service» (Сервис сертификатов)	Нет
1150	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «store-service» (Сервис хранения)	Нет
1200	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «templates-service» (Сервис шаблонов)	Нет
1250	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «security-service» (Сервис безопасности)	Нет
1300	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «licenses-service» (Сервис лицензирования)	Нет
1350	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «routes-service» (Сервис маршрутизации)	Нет
1400	TCP	HTTP	Внутренний интерфейс для подключения к	Нет

Порт	Транспорт	Протокол	Назначение	Можно ли переназначить
			внутреннему сервису «backward-compatibility-service» (Сервис совместимости)	
1450	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «validation-service» (Сервис валидации)	Нет
1500	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «publisher-service» (Сервис публикации)	Нет
1550	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «subjects-service» (Сервис субъектов)	Нет
1600	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «ldap-service» (Сервис синхронизации по LDAP)	Нет
1650	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (Сервис журнализации)	Нет
1700	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «export-service» (Сервис экспорта)	Нет
1750	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «event-delivery-service» (Сервис доставки событий)	Нет
1800	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «settings-service» (Сервис настройки)	Нет

4.2 Подготовка сервера

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

- зависимостей и подключение репозиториев ОС;
- Java v.17;
- СУБД;
- JC-WebClient.

4.2.1 Подключение репозиториев и установка зависимостей

Перед началом установки компонентов программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» установите пути нахождения всех необходимых репозиториев с использованием сети Интернет или без доступа к сети[4].

4.2.2 Установка набора инструментов Java

Произведите установку Java версии 17 одного из пакетов:

- Для обеспечения сертифицированной среды функционирования выполните установку Axiom JDK Certified[5].
- В случае, если обеспечение сертифицированной среды функционирования не требуется, возможно использовать свободно распространяемое программное обеспечение, например, OpenJDK[6].

4.2.3 Установка и настройка СУБД

- Выполните установку и настройку одной из нижеприведённых базы данных:
  - PostgreSQL[7] из состава сертифицированной операционной системы;
    ИЛИ
  - Jatoba 4[8].
- Создание и настройка базы данных может быть выполнена одним из способов:
  - в ручном режиме, в результате выполнения действий, приведённых в Приложении 4, будет создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных), указанными в конфигурационном файле `/opt/aecaCa/scripts/config.sh` (см. Приложение 4.5, 5.3);
  - в автоматическом режиме посредством запуска скрипта, в результате будет создана база данных с предустановленными параметрами (имя пользователя «аеса», пароль «аеса», имя базы данных «аесаса») (см. Приложение 4.4, 5.2).
- Созданная СУБД `aecaca` (имя базы данных по умолчанию) предназначена для хранения информации:
  - об учетных записях;
  - о сертификатах;
  - сведений о субъектах;
  - сведений о ресурсных системах;
  - о шаблонах;
  - журнала событий;
  - сведений о лицензии;
  - профили сертификатов;
  - профили конечных сущностей;
  - центры сертификатов;

[4] Справочная информация по процедуре подключения репозиториев приведена в Приложении 1 настоящего руководства

[5] Справочная информация по установке Axiom JDK Certified приведена в Приложении 2 настоящего руководства

[6] Справочная информация по установке OpenJDK приведена в Приложении 3 настоящего руководства

[7] Справочная информация по установке и настройке СУБД PostgreSQL приведена в Приложении 4 настоящего руководства

[8] Справочная информация по установке и настройке СУБД Jatoba приведена в Приложении 5 настоящего руководства

- 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.

4.2.4 Установка JC-WebClient 4.3.2

Программное обеспечение JC-WebClient[9] необходимо установить на сервер, где предполагается развернуть Центры Сертификации для выпуска сертификата на электронном ключе.

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

[9] Справочная информация по установке JC-WebClient приведена в Приложении 6 настоящего руководства

5 УСТАНОВКА ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

Перед установкой компонента «Центр сертификации Aladdin Enterprise Certificate Authority» необходимо выполнить подготовку сервера, где предполагается развертывание Центра сертификации, в соответствии с разделом 5 настоящего руководства.

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

5.1 Распаковка инсталляционного комплекта компонента «Центр сертификации Aladdin Enterprise Certificate Authority»

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

РЕД ОС 7.3	`sudo dnf install <наименование пакета>.rpm`
Astra Linux SE 1.7	`sudo apt install <наименование пакета>.deb`
Альт Сервер 8	`sudo apt-get install <наименование пакета>.rpm`

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

Таблица 5 – Структура установочного комплекта Aladdin eCA

Структурный элемент	Назначение элемента
`../opt/aecaCa`	установочный комплект Aladdin eCA, а также используемые дополнительные инструменты
`../opt/aecaCa/dist`	путь развертывания продукта; содержит создаваемые временные файлы
`..dist/archive/`	архивы, сформированные в результате очистки журнала событий
`..dist/backup/`	созданные резервные копии Центра сертификации
`..dist/certificates/account`	расположение pkcs#12 контейнера сертификата администратора инициализации
`..dist/certificates/ssl`	расположение сертификатов для управления ssl-соединением
`..dist/cryptotoken/`	расположение pkcs#12 контейнеров, содержащих открытый и закрытый ключи Центров сертификации
`..dist/environment/`	расположение переменных окружения сервисов
`..dist/logs/`	расположения технических журналов сервисов

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

Структурный элемент	Назначение элемента
../services/checksum.md5	файл эталонных хэш-сумм сервисов и список сервисов, подвергаемых контролю целостности
../services/internal.md5	файл эталонных хэш-сумм сервисов и список сервисов, подвергаемых контролю целостности (для внутреннего использования)
../opt/aecaCa/static	артефакты Клиентской части Центра сертификации

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

5.2 Настройка параметров конфигурации программного компонента

- Перед установкой программного компонента требуется определить значения следующих параметров:
  - `webserver` – укажите используемый web-сервер (`nginx` или `apache`). О выборе web-сервера смотри п. 5.4. Также значение параметра можно будет ввести при запуске инсталлятора, в интерактивном режиме выбрав web-сервер;
  - `webserver_path` – укажите папку с файлами для развёртывания web-сервера. Также значение параметра можно будет ввести при запуске инсталлятора, в интерактивном режиме указав путь к файлам web-сервера (конфигурация nginx располагается по пути `etc/nginx`; конфигурация apache располагается: для AstraLinux по пути `/etc/apache2`, для RedOS по пути `/etc/httpd`);
  - `database_password` – укажите пароль созданной базы данных `aecaca` (имя базы данных по умолчанию, созданной в п. 4.2.3);
  - `hostname` – укажите полное имя сервера (hostname), на котором происходит развёртывание Центра сертификации. Установленное значение заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых (при развёртывании ЦС) локального субъекта web-сервера и сертификата для него.
- Отредактируйте конфигурационный файл `/opt/aecaCa/scripts/config.sh`**,** выполнив команду:

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

- Настраиваемые параметры конфигурационного файла `/opt/aecaCa/scripts/config.sh` 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 web-сервера технологического центра сертификации;
  - расписание синхронизации ресурсных систем;
  - расписание публикации списка отозванных сертификатов;
  - расписание проверки срока действия сертификатов центров сертификации и выпущенных сертификатов субъектов;

- расписание архивации журнала событий;
- конфигурацию базы данных.

- Полный перечень и описание параметров конфигурации приведено в Таблица 6.

Таблица 6 – Описание параметров конфигурации

Параметр	Значение параметра по умолчанию	Описание
Конфигурация развертывания		
webserver	`#CHANGEIT`	Используемый веб-сервер (nginx или apache)
webserver_path	`#CHANGEIT`	Папка с файлами для развёртывания сервиса (по умолчанию: конфигурация nginx располагается по пути /etc/nginx, для AstraLinux конфигурация apache располагается по пути /etc/apache2, для RedOS конфигурация apache располагается по пути /etc/httpd)
aeca_path	"/opt/aeca/dist"	Папка с файлами для развёртывания Центра сертификации Aladdin eCA
environment_path	"${aeca_path}/environment"	Папка с переменными окружения для сервисов
cryptotoken_path	"${aeca_path}/cryptotoken"	Папка, содержащая открытый и закрытый ключи для доступа (аутентификации) к центру сертификации
Путь до резервных копий		
backup_path	"${aeca_path}/backup"	Папка, в которую сохраняются резервные копии Центра сертификации Aladdin eCA
Путь хранения архива журнала событий		
logs_base	"${aeca_path}/logs"	Папка, в которую сохраняется журнал событий (лог-файлы)
archive_path	"${aeca_path}/archive"	Папка, в которую сохраняется архив журнала событий, сформированный в результате автоматической архивации по заданным параметрам
Путь хранения контейнера сертификата и ключа web-сервера, а также цепочек сертификатов разрешенных издателей		
certificates_ssl_path	"${aeca_path}/certificates/ssl"	Папка, содержащая сертификат веб-сервера и цепочки сертификатов разрешённых издателей
certificates_account_path	"${aeca_path}/certificates/account"	Папка, содержащая сертификат администратора инициализации в контейнере .p12
Конфигурация пользователя		
aeca_user	aeca	Имя пользователя Центра сертификации Aladdin eCA, используемое для работы программы
aeca_group	aeca	Группа, в которой состоит пользователь Центра сертификации Aladdin eCA
Конфигурация памяти		

Параметр	Значение параметра по умолчанию	Описание
memory	6144	Лимит оперативной памяти для программы. Значение в Мб
Конфигурация базы данных		
database_username	"aeca"	Имя пользователя базы данных, используемое для работы Центра сертификации Aladdin eCA
database_password	#CHANGEIT	Пароль пользователя базы данных, используемый для работы Центра сертификации Aladdin eCA
database_host	"localhost"	Сетевой адрес базы данных
database_port	"5432"	Порт, используемый для подключения к базе данных
database_name	"aecaca"	Имя базы данных, используемой Центром сертификации Aladdin eCA
Конфигурация aeca-ca		
http_port	"80"	Порт для подключения к программному компоненту «Центр Сертификации» по протоколу http
https_port	"443"	Порт для подключения к программному компоненту «Центр Сертификации» по протоколу https
hostname	'localhost'	Имя сервера, на котором развёртывается Центр сертификации. Также заносится в атрибуты «Common name» и «DNS Name» автоматически создаваемых (при развёртывании ЦС) сертификата web-сервера и локального субъекта. Должно совпадать с hostname сервера.
Переменные окружения, используемые всеми сервисами		
logging_response	false	Флаг для сбора и регистрации ответов сервисов
logging_sql	false	Флаг для сбора и регистрации информации о подключениях и запросах к базе данных PostgreSQL
Ключ для внутренней аутентификации		
api_key	"2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810"	Значение ключа для внутренней аутентификации. Для служебного пользования, доступ к учётной записи Системного администратора ограничен, установку программы выполняет ответственный специалист
Переменные окружения, используемые certificate-authority-service		
pkcs12_key_protection_algorithm	PBEWithHmacSHA256AndAES_256	Алгоритм хеширования для ключа контейнера PKCS12 (Допустимые значения: PBEWithHmacSHA256AndAES_256 - рекомендуется; PBEWithSHA1AndDESede - устаревший)
pkcs12_mac_protection_algorithm	HmacPBESHA256	Алгоритм хеширования MAC контейнера PKCS12 Допустимые значения: HmacPBESHA256 - рекомендуется; HmacPBESHA1 - устаревший

Параметр	Значение параметра по умолчанию	Описание
Переменные окружения, используемые ldap-service		
ldap_sync_connection_point	'0 */30 * * * *'	CRON выражение, по которому запускается частичная синхронизация зарегистрированных точек подключения (значение по умолчанию: '0 */30 * * * *' - запуск каждые полчаса)
ldap_sync_resource	'0 0 0 * * *'	CRON выражение, по которому запускается полная синхронизация ресурсных систем (значение по умолчанию: '0 0 0 * * *' - запуск каждую полночь)
Переменные окружения, используемые publisher-service		
crl_scheduler	'0 */1 * * * *'	CRON выражение, по которому запускается служба выпуска CRL
Переменные окружения, используемые store-service		
certificate_expired_scheduler	'0 */1 * * * *'	CRON выражение, по которому запускается служба проверки сертификатов на предмет истечения срока действия
Переменные окружения, используемые event-delivery-service		
email_host	'127.0.0.1'	Хост почтового сервера
email_port	'25'	Порт почтового сервера
email_login	'aeca'	Логин пользователя
email_password	'aeca'	Пароль пользователя
email_from	'no_reply@aeca.ru'	Почтовый адрес, с которого отправлено сообщение. Может не работать. Google проставляет логин
email_schedule	'0 0 12 * * *'	CRON для запуска метода отправки почтовых уведомлений
email_enabled	'true'	Флаг отправки почтовых уведомлений, если выкл. то сообщения не отправляются, но помечаются, как отправленные
email_protocol	'smtp'	Протокол подключения к почтовому серверу
email_smtp_auth	'false'	Флаг: использование SMTP-авторизации
email_start_tls	'false'	Флаг: использование директивы start tls при подключении к почтовому серверу
Переменные окружения, используемые validation-service		
aeca_va_port	'8888'	Порт, на котором запущен Центр валидации
aeca_cdp_port	'8080'	Порт, на котором запущен Центр валидации – CDP (точка распространения)
aeca_crl_publish_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/publish-crl/{2}'	Шаблон URL точки публикации CRL
aeca_crl_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/get-crl/{2}'	Шаблон URL точки распространения CRL

Параметр	Значение параметра по умолчанию	Описание
aeca_delta_crl_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/crl/get-delta-crl/{2}'	Шаблон URL точки распространения Delta CRL
aeca_aia_publish_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/aia/publish-aia/{2}'	Шаблон URL точки публикации AIA
aeca_aia_distribution_point_pattern	'http://{0}:{1}/aecaCdp/api/v2/aia/get-aia/{2}'	Шаблон URL точки распространения AIA
aeca_ocsp_pattern	'http://{0}:{1}/aeca-va/ocsp'	Шаблон URL сервиса OCSP
Переменные окружения, используемые settings-service		
initial_ca_common_name	"INITIAL_CA"	Subject DN сертификата технологического ЦС
initial_ca_hash_algorithm	'SHA256'	Хеш алгоритм сертификата технологического ЦС
initial_ca_key_algorithm	'RSA'	Алгоритм ключа сертификата технологического ЦС
initial_ca_key_bits	'2048'	Длина ключа сертификата технологического ЦС
initial_admin_principal	'INITIAL_ADMIN'	Имя учетной записи администратора инициализации
initial_client_key_algorithm	'RSA'	Алгоритм ключа сертификата администратора инициализации
initial_client_key_bits	'2048'	Длина ключа сертификата администратора инициализации
initial_client_password	'INITIAL'	Пароль от pkcs12 контейнера сертификата администратора инициализации
initial_server_key_algorithm	'RSA'	Алгоритм ключа сертификата Web-сервера
initial_server_key_bits	'2048'	Длина ключа сертификата Web-сервера
initial_server_password	'INITIAL'	Пароль от pkcs12 контейнера сертификата Web-сервера
certificate_server_name	server	Шаблон имени файлов сертификата и закрытого ключа сертификата Web-сервера
certificate_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	Период архивации (мс) (архивировать записи старше...)
Переменные окружения, используемые security-service		
session_max_count	100	Максимальное число одновременных сессий аккаунта в виде натурального числа. При указании

Параметр	Значение параметра по умолчанию	Описание
		значения «-1» ограничение на количество одновременных сессий пользователя будет отсутствовать.

5.3 Подключение Центра валидации

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

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

5.4 Установка web-сервера

При принятии решения о выборе web-сервера необходимо учитывать требования к среде функционирования, в частности см. Таблица 7.

Таблица 7 – Поддержка web-серверов сертифицированными ОС

Операционная система	**Web-сервер**	**Поддержка сертифицированной среды функционирования**	**Примечание**
РЕД ОС 7.3	Nginx	Обеспечивает	установка компонента производится из основного репозитория сертифицированной ОС
	Apache	Обеспечивает	установка компонента производится из основного репозитория сертифицированной ОС
Astra Linux SE 1.7	Nginx	Не обеспечивает	требуется установка компонента из доп. репозитория
	Apache	Обеспечивает	установка компонента производится из основного репозитория сертифицированной ОС
Альт Сервер 8, релиз 10	Nginx	Обеспечивает	установка компонента производится из основного репозитория сертифицированной ОС
	Apache	Не обеспечивает	требуется установка компонента из доп. репозитория

5.4.1 Установка web-сервера Apache

- Если выбран web-сервер Apache (значение параметра `webserver` конфигурационного файла `/opt/aecaCa/scripts/config.sh`), то выполните установку пакета и необходимых модулей из официального репозитория ОС.

- для ОС **РЕД ОС 7.3**:
  - Установите пакет, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo dnf install httpd
```

– Установите дополнительный модуль для использования протокола ssl в apache, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo dnf install mod_ssl
```

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

```
sudo systemctl is-enabled httpd
```

- для ОС **Astra Linux SE 1.7**:

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

```
sudo apt install apache2
```

– Активируйте модули, выполнив команды:

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

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

```
sudo systemctl is-enabled apache2
```

- для ОС **Альт Сервер 8, релиз 10**:

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

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

– Создайте файлы:

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

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

Внесите следующий текст в созданный файл:

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

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

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

Внесите следующий текст в созданный файл:

```
/etc/httpd2/conf/mods-available/http2.conf
# mod_http2 doesn't work with mpm_prefork
<IfModule !mpm_prefork>
    Protocols h2 h2c http/1.1

    # # HTTP/2 push configuration
    #
```

```
    # H2Push          on
    #
    # # Default Priority Rule
    #
    # H2PushPriority * After 16
    #
    # # More complex ruleset:
    #
    # H2PushPriority  *                       after
    # H2PushPriority  text/css                before
    # H2PushPriority  image/jpeg              after   32
    # H2PushPriority  image/png               after   32
    # H2PushPriority  application/javascript  interleaved
    #
    # # Configure some stylesheet and script to be pushed by the webserver
    #
    # <FilesMatch "\.html$">
    #     Header add Link "</style.css>; rel=preload; as=style"
    #     Header add Link "</script.js>; rel=preload; as=script"
    # </FilesMatch>
    # Since mod_http2 doesn't support the mod_logio module (which provide the %O
format),
    # you may want to change your LogFormat directive as follow:
    #
    # LogFormat "%v:%p %h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
vhost_combined
    # LogFormat "%h %l %u %t \"%r\" %>s %B \"%{Referer}i\" \"%{User-Agent}i\""
combined
    # LogFormat "%h %l %u %t \"%r\" %>s %B" common
</IfModule>
```

– Активируйте модули, выполнив команды:

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

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

```
sudo a2enport https
```

5.4.2 Установка web-сервера Nginx

- Если выбран web-сервер Nginx (значение параметра `webserver` конфигурационного файла `/opt/aecaCa/scripts/config.sh`), то установите пакет из официального репозитория ОС (для РЕД ОС и Альт Сервер 8, релиз 10) или расширенного репозитория (для Astra Linux SE 1.7), выполнив команду с правами суперпользователя:

РЕД ОС 7.3

```
sudo dnf install nginx
```

Astra Linux SE 1.7	`sudo apt install nginx`
Альт Сервер 8	`sudo apt-get install nginx`

Для ОС Astra Linux SE 1.7 требуется расширить репозиторий операционной системы при выборе web-сервера Nginx (см. Приложение 1. Установка репозиториев), что приведёт к потере сертифицированной среды функционирования.

- Запустите установленный web-сервер, выполнив команду:

```
systemctl start nginx
```

- Добавьте web-сервер в автозагрузку, выполнив команду:

```
systemctl is-enabled nginx
```

5.5 Установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority»

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

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

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

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

- После инициализации процесса установки интерактивный инсталлятор запущен и пользователю будет предложено (в случае, если ранее на сервере было установлено программное средство Aladdin eCA):
  - установить Aladdin eCA;
  - установить обновление Aladdin eCA;
  - завершить работу инсталлятора.

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

- В случае, если в конфигурационном файле `/opt/aecaCa/scripts/config.sh` не определён используемый web-сервер или введено неверное значение параметра `webserver`, то в процессе установки пользователю будет предложено выбрать используемый web-сервер:
  - apache
  - nginx.

Подтвердите выбор действия, вводом цифры 1 или 2.

При выборе web-сервера apache или nginx требуется предварительно выполнить установку пакета, описанную в пункте 5.4 настоящего руководства.

- В случае, если в конфигурационном файле `/opt/aecaCa/scripts/config.sh` не определено расположение конфигурации выбранного web-сервера (параметр `webserver_path`), то в процессе установки пользователю будет предложено ввести расположение конфигурации. По умолчанию конфигурация `nginx` располагается по пути `/etc/nginx`, для AstraLinux конфигурация `apache` располагается по пути `/etc/apache2`, для RedOS конфигурация `apache` располагается по пути `/etc/httpd`, для AltLinux конфигурация `apache` располагается по пути `/etc/httpd2/conf`.

- В процессе установки осуществляется:

- создание системного пользователя и соответствующей группы, от имени которых функционирует продукт;
- установка прав для создаваемого пользователя продукта;
- подготовка, установка параметров и служебных сервисов;
- запуск служебных сервисов;
- создание и выпуск сертификата технологического центра сертификации;
- выпуск сертификата web-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.

- После завершения установки в директории, выбранной в качестве пути для установки, будет содержаться:
  - каталог «`account`» (по умолчанию, расположен по пути `/opt/aecaCa/dist/certificates/account` – установленное значение параметра `certificates_account_path` конфигурационного файла `config.sh`), содержащий сертификат администратора технологического ЦС `INITIAL_ADMIN.p12`, необходимый для дальнейшей аутентификации на web-сервере. Более подробно шаги по аутентификации на web-сервере описаны в разделе 6 «Первичная настройка компонента «Центр сертификации Aladdin Enterprise Certificate Authority»» настоящего руководства.

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

6 ПЕРВИЧНАЯ НАСТРОЙКА ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

В результате успешной установки программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» в установочном каталоге будет сформирован сертификат доступа администратора инициализации `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.p12` (установленное значение параметра `certificates_account_path` конфигурационного файла `config.sh`), PIN-код сертификата указан в параметре `initial_server_password` конфигурационного файла `/opt/aecaCa/scripts/config.sh` , по умолчанию – «**INITIAL**».

Для первичной настройки программного компонента необходимо установить сертификат в доверенное хранилище сертификатов вашего браузера.

Процесс установки сертификата рассмотрим на примере браузера Firefox:

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

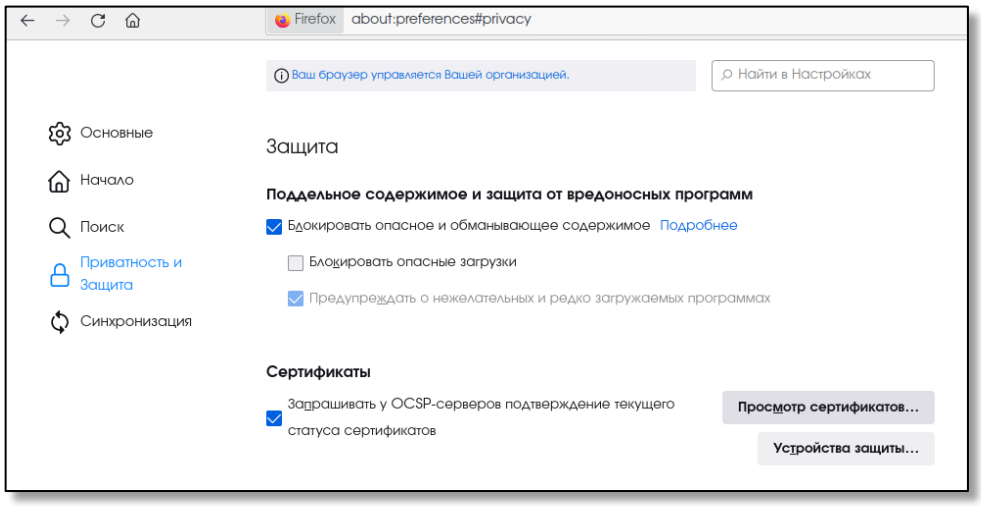

Рисунок 1 – Окно настроек браузера

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

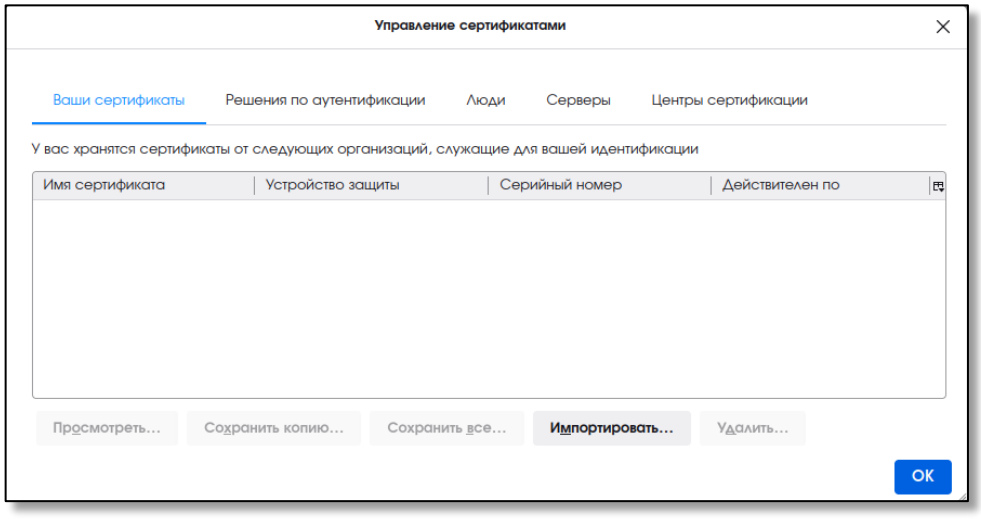

Рисунок 2 – Окно управления сертификатами

- Выберите файл сертификата `/opt/aecaCa/dist/certificates/account/INITIAL_ADMIN.p12`, подписанный технологическим ЦС «INITIAL_CA» и созданный на этапе установки компонента Aladdin eCA. Нажмите кнопку <Открыть> (см. Рисунок 3).

ВНИМАНИЕ! Запрещается каким-либо образом удалять сертификат технологического центра сертификации «INITIAL_CA», созданного при развёртывании Aladdin eCA.

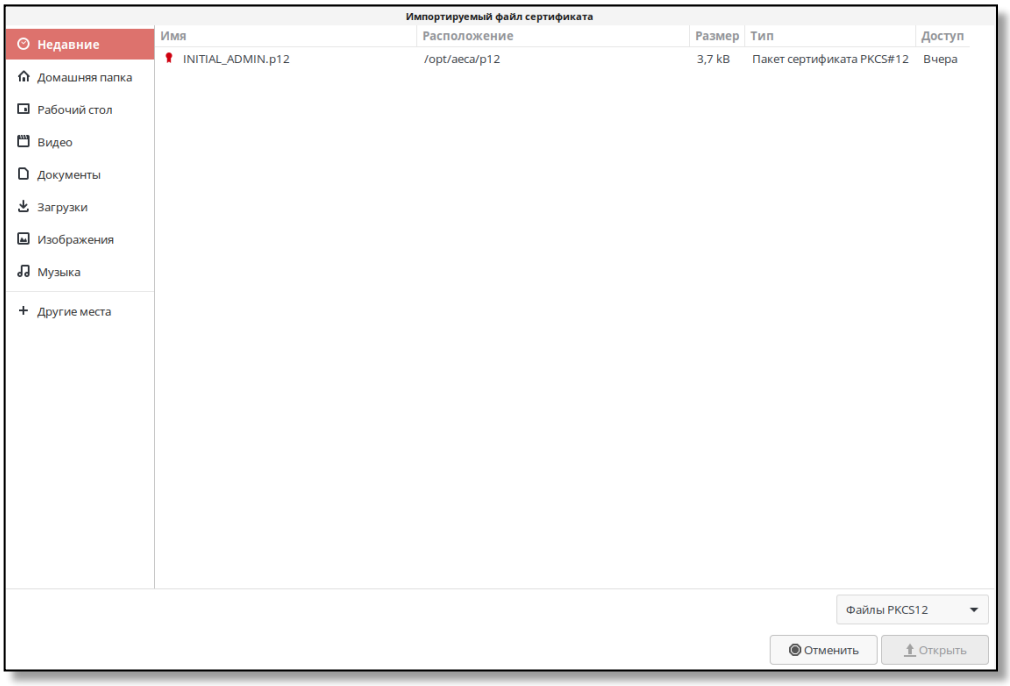

Рисунок 3 – Окно выбора импортируемого файла сертификата

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

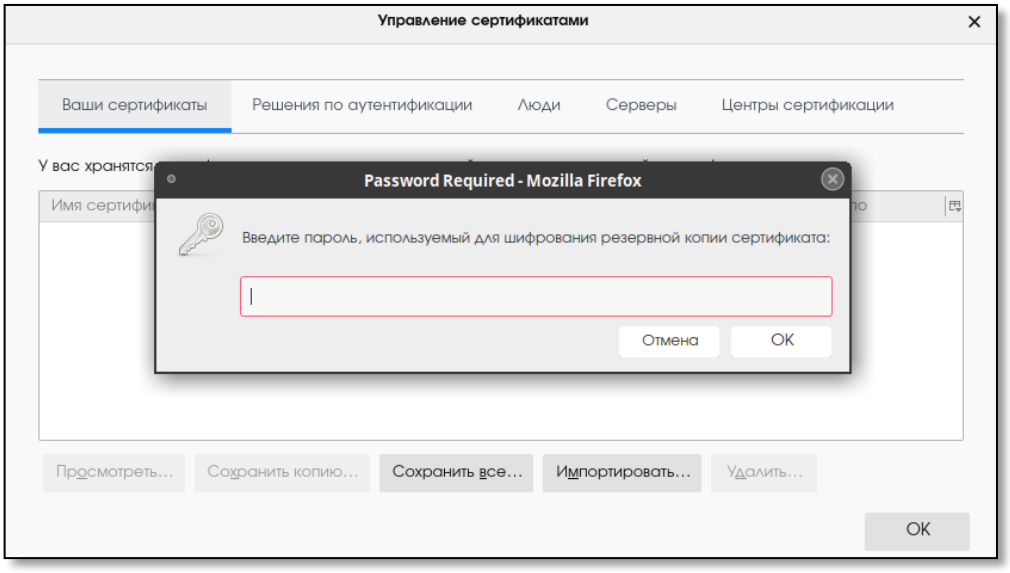

Рисунок 4 – Окно ввода PIN-кода сертификата

PIN-код сертификата доступен в директории установленного приложения `/opt/aecaCa/scripts/`, из файла `config.sh`, данные параметра `initial_client_password` (см. Рисунок 5).

```
#Пароль от pkcs12 контейнера сертификата администратора инициализации
initial_client_password=INITIAL
```

Рисунок 5 – Окно файла `config.sh`

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. Рисунок 6). Нажать кнопку <OK>.

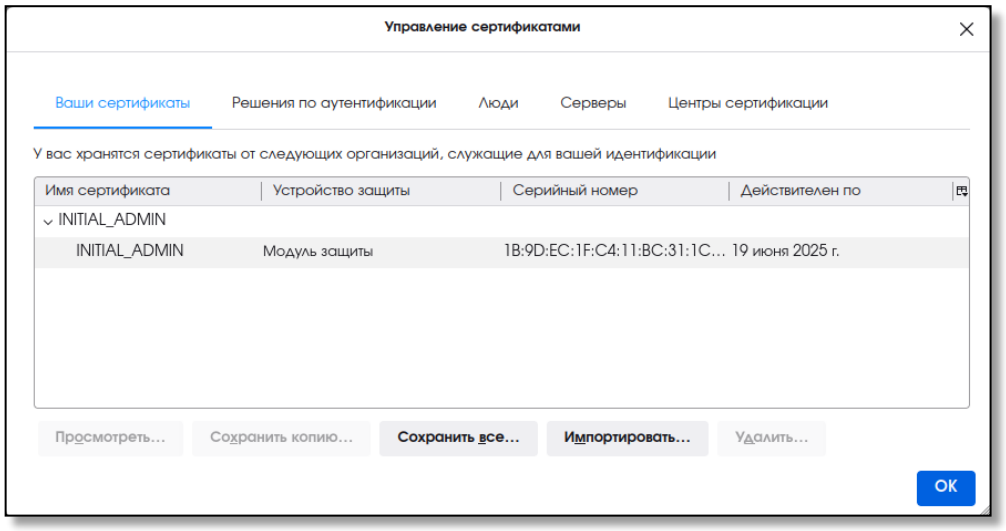

Рисунок 6 – Окно «Управление сертификатами»

- В адресную строку браузера ввести ip-адрес или полное доменное имя сервера, на котором произведена установка программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority».

Например:

```
https://172.22.5.21
```

- В открывшемся окне выберите импортированный сертификат для аутентификации `INITIAL_ADMIN` (см. Рисунок 6). Нажмите кнопку <OK>.

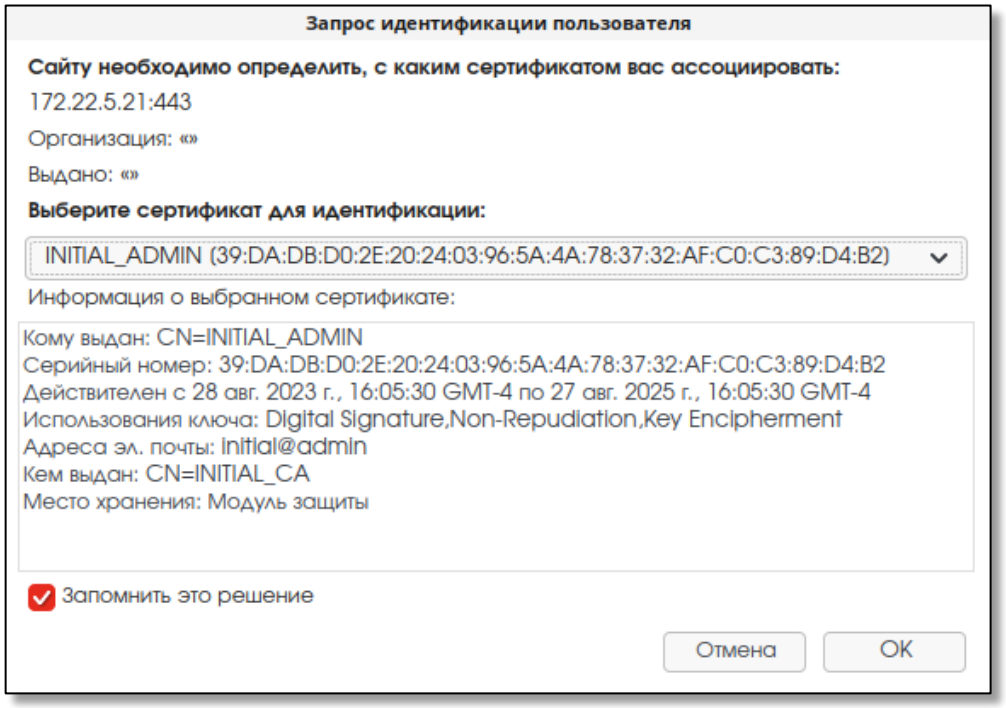

Рисунок 7 – Окно выбора сертификата

- Далее откроется страница с предупреждением системы безопасности (см. Рисунок 8). Нажмите кнопку <Дополнительно>.

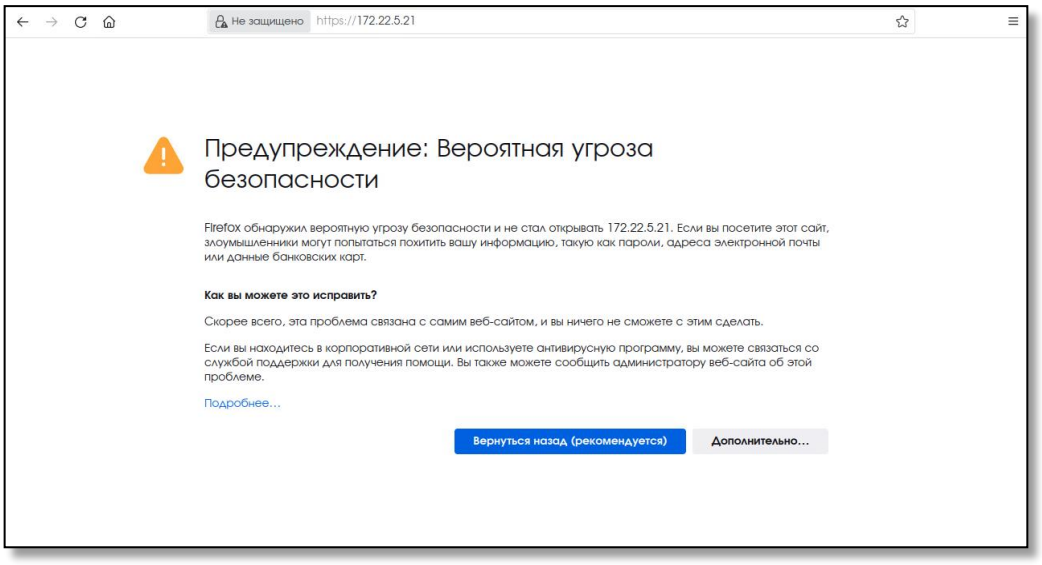

Рисунок 8 – Страница с предупреждением системы безопасности

- По нажатию кнопки <Дополнительно> на странице предупреждения системы безопасности (см. Рисунок 8) осуществляется переход на страницу ошибки распознавания сертификата (см. Рисунок 9). Нужно принять риски, нажав кнопку <Принять риск и продолжить> на текущей странице.

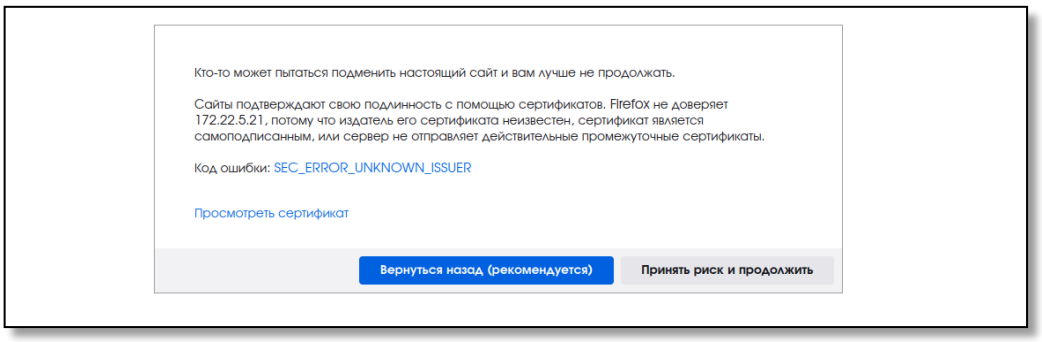

Рисунок 9 – Страница ошибки распознавания сертификата

- Установка и предварительный ввод в эксплуатацию Aladdin eCA завершены, далее следует установить лицензию для компонента «Центр Сертификации Aladdin Enterprise Certificate Authority» с помощью Мастера инициализации (см. часть 2 настоящего руководства администратора).

- Первичная авторизация в открывшемся интерфейсе установленного программного компонента «Центр Сертификации Aladdin Enterprise Certificate Authority» по умолчанию выполняется под учетной записью «INITIAL_ADMIN» с правами администратора.

- Порт, используемый для защищённой связи программы с веб-браузером, 443.

- Для работы программного компонента «Центр Сертификации Aladdin Enterprise Certificate Authority» подключение к глобальной сети Интернет не требуется.

7 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

7.1 Назначение контроля целостности

Контроль целостности кода исполняемых файлов программного обеспечения «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» необходим для отслеживания неизменности и контроля состояния объектов файловой системы (исполняемых фалов), перечень которых приведён в Таблица 8, сопровождающихся поиском и обнаружением искажений выполняемого кода загрузочных модулей, в результате различных сбоев.

Таблица 8 – Исполняемые файлы, проверяемые на целостность

Исполняемый файл (сервис)	**Наименование**	**Назначение**	**Возможные результаты проверки**
certificate-service.jar	Модуль сертификатов	Обеспечивает создание сертификата, подпись сертификата (включая цепочки сертификатов), генерацию CRL, валидацию сертификата, взаимодействие уполномоченного пользователя с контейнерами и точками распространения.	ЦЕЛ ПОВРЕЖДЁН
event-delivery-service.jar	Модуль оповещения пользователей	Предназначен для оповещения посредством рассылки уведомлений по адресам электронной почты владельцев сертификатов	ЦЕЛ ПОВРЕЖДЁН
export-service.jar	Модуль экспорта данных	Обеспечивает управление экспортом файлов программы	ЦЕЛ ПОВРЕЖДЁН
internal.md5	Файл контрольных сумм	Для внутреннего использования программой	ЦЕЛ ПОВРЕЖДЁН
ldap-service.jar	Модуль работы с LDAP	Обеспечивает взаимодействие с ресурсными системами и обеспечивает публикацию сертификатов в ресурсную систему, а также получение данных из ресурсной системы	ЦЕЛ ПОВРЕЖДЁН
licenses-service.jar	Модуль лицензирования	Обеспечивает управление лицензиями программы	ЦЕЛ ПОВРЕЖДЁН
logs-service.jar	Модуль журнала событий	Обеспечивает фиксацию событий в журнале и получение событий из журнала, просмотра и поиск записей журнала событий, экспорт и архивацию записей журнала событий	ЦЕЛ ПОВРЕЖДЁН
publisher-service.jar	Модуль публикации сертификатов	Обеспечивает обслуживание точек публикации CRL, Delta CRL и AIA	ЦЕЛ ПОВРЕЖДЁН
routes-service.jar	Модуль управления	Предоставляет пользовательские веб-интерфейсы, обеспечивает разграничение доступа на основе ролей пользователей	ЦЕЛ ПОВРЕЖДЁН
security-service.jar	Модуль безопасности	Обеспечивает управление учётными записями пользователей	ЦЕЛ ПОВРЕЖДЁН
settings-service.jar	Модуль настроек	Обеспечивает управление жизненным циклом программы, её состоянием и параметрами (данные о продукте,	ЦЕЛ ПОВРЕЖДЁН

Исполняемый файл (сервис)	Наименование	Назначение	Возможные результаты проверки
		конфигурация серверного сертификата SSL, разрешенные издатели сертификатов)	
backward-compatibility-service.jar	Модуль обратной совместимости	Предназначен для обеспечения обратной совместимости с API Центра сертификатов доступа Aladdin eCA CE версии 1.2.0.	ЦЕЛ ПОВРЕЖДЁН
store-service.jar	Модуль хранения сертификатов	Обеспечивает хранение и управление файлами сертификатов	ЦЕЛ ПОВРЕЖДЁН
subjects-service.jar	Модуль работы с субъектами	Обеспечивает взаимодействие с группами безопасности и субъектами	ЦЕЛ ПОВРЕЖДЁН
templates-service.jar	Модуль шаблонов	Обеспечивает просмотр, создание, редактирование и удаление шаблонов сертификатов	ЦЕЛ ПОВРЕЖДЁН
validation-service.jar	Модуль валидации сертификатов	Обеспечивает взаимодействия с точками распространения, а также для валидации сертификатов	ЦЕЛ ПОВРЕЖДЁН

7.2 Описание выполнения контроля целостности

Для определения факта неизменности объектов файловой системы программы необходимо произвести проверку посредством формирования значений хеш-сумм контролируемых исполняемых файлов (перечень файлов приведён в Таблица 8), расположенных в папке `opt/aecaCa/services/`, вычисленных по алгоритму MD5, и последующую проверку их подлинности путём сравнения с эталонными значениями хэш-сумм этих файлов. Перечень контролируемых исполняемых файлов и соответствующих хеш-сумм хранится в специальной базе эталонов, в ранее определённом и сформированном файле `/opt/aecaCa/services/checksum.md5`.

7.3 Выполнение контроля целостности

- Для выполнения контроля целостности исполняемых файлов запустите скрипт `integrity_check.sh` с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

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

- После завершения проверки необходимо проанализировать полученные данные.

7.4 Результаты выполнение контроля целостности

Результаты выполнения контроля целостности исполняемых файлов являются: выведение в консоли с построчным указанием наименования проверяемых модулей и результатами их проверки. Возможные результаты проверки: «ЦЕЛ» - информирует администратора о том, что файл успешно прошёл контроль целостности и хеш-сумма соответствует эталонному значению; «ПОВРЕЖДЕН» - информирует администратора о том, что код исполняемого файла был каким-либо образом модифицирован и хеш-сумма не соответствует эталонному значению;

- запись сообщения в журнал событий в соответствии с результатами выполнения контроля целостности:
  - информационного сообщения с кодом события CAENV074 об успешной проверке контрольных сумм;
  - сообщения об ошибке с кодом CAENV075 о неуспешной проверке контрольных сумм, с указанием исполняемых файлов, целостность которых нарушена или доступ, к которым не предоставлен.

8 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ

8.1 Назначение сбора диагностической информации

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

8.2 Описание сбора диагностической информации

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- о работе сервисов программы (файлы в формате .log);
- конфигурация программы (`/opt/aecaCa/scripts/config.sh`);
- о работе сервиса 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).

8.3 Выполнение сбора диагностической информации

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

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

- Для выполнения сбора диагностической информации запустите скрипт от имени суперпользователя (с правами root):

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

8.4 Результат сбора диагностической информации

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

Для вывода текущей рабочей директории используйте команду:

```
pwd
```

9 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

- Создание резервных копий является неотъемлемой частью работы администратора Центров сертификации.
- Перед выполнением каких-либо настроек, изменений и обновлений программного компонента следует в обязательном порядке выполнить резервное копирование.
- Резервные копии создаются для:
  - содержимого каталога, содержащего сертификаты и ключи web-сервера, разрешённых издателей, путь к которому определён значением параметра «`certificates_ssl_path`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aeca/dist/certificates/ssl`);
  - закрытого и открытого ключей Центра сертификации из каталога, путь к которому определён значением параметра «`cryptotoken_path`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/aeca/dist/cryptotoken`);
  - базы данных, имя которой указано в значении параметра «`database_name`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `aecaca`);
  - конфигурационного файла `/opt/aecaCa/scripts/config.sh`;
- Резервное копирование осуществляется на локальный диск в папку, путь к которой определён значением параметра «`backup_path`» конфигурационного файла `/opt/aecaCa/scripts/config.sh` (по умолчанию – `/opt/dist/backup/`) с указанием даты и времени создания резервной копии в имени архива. Каталог хранения архивов выбран исходя из того, что необходимо хранить резервные копии временно и не увеличивать размер занятого пространства жесткого диска. Для постоянного хранения требуется создать механизм переноса файлов.
- Для постоянного хранения резервных копий следует:
  - определить каталог для хранения резервных копий;
  - составить сценарий для создания резервной копии;
  - настроить расписание вызова сценариев.

9.1 Создание резервной копии

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

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

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:

```
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

9.3 Восстановление данных из резервной копии

Восстановление данных производится из папки, путь к которой определён значением параметра «backup_path» конфигурационного файла /opt/aecaCa/scripts/config.sh (по умолчанию – /opt/dist/backup/), на машине, где развернут программный компонент «Центр сертификации Aladdin Enterprise Certificate Authority».

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

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

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

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

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

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

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

9.4 Регистрация событий в журнале событий

- При успешном создании резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV086». В случае ошибки создания резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV087».
- При успешном восстановлении из резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV088». В случае ошибки восстановления из резервной копии в журнале событий продукта должно регистрироваться событие с кодом «CAENV089».
- Полный перечень событий с описанием приведён в части 2 настоящего руководства, раздел 7.10.

10 ВОССТАНОВЛЕНИЕ ДОСТУПА К ЦЕНТРУ СЕРТИФИКАЦИИ

10.1 Назначение

Восстановление доступа к Центру сертификации необходимо выполнить в случае отсутствия ранее созданной резервной копии и блокировки доступа к программному компоненту «Центр сертификации Aladdin Enterprise Certificate Authority», возникшей в результате некорректного удаления технологических составляющих или истечения срока действия сертификата ЦС или сертификата администратора.

10.2 Выполнение восстановления доступа к ЦС

- Для выполнения восстановления доступа к ЦС запустите скрипт от имени суперпользователя (с правами root):

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

10.3 Результат восстановления доступа к ЦС

По результату выполнения скрипта восстановления доступа к ЦС:

- создан и выпущен:
  - технологический Центр сертификации «INITIAL_CA» (по умолчанию статус «активирован»);
  - сертификат технологического Центра сертификации «INITIAL_CA»;
- заменена:
  - учётная запись администратора «INITIAL_ADMIN»;
- выпущены и заменены:
  - сертификат учётной записи администратора «INITIAL_ADMIN»;
  - сертификат технологического Web-сервера.

Для дальнейшего доступа к Центру сертификации выполните аутентификацию по выпущенному сертификату учётной записи «INITIAL_ADMIN» (см. раздел 6 настоящего Руководства администратора).

11 ОБНОВЛЕНИЕ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

11.1 Назначение обновлений

Обновление базы данных и модулей программного компонента «Центр сертификации 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.

11.2 Информирование потребителей о выпуске обновлений

- Компания ведет учет покупателей «Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition». Выполняется регистрация следующей информации:
  - наименование организации;
  - адрес организации;
  - контактная информация (содержит электронный почтовый адрес лица, обеспечивающего администрирование программы).
- Уведомление пользователей о выпуске обновлений «Центра сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» выполняется 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.

11.3 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.

11.4 Контроль целостности обновления ПО

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

11.5 Процедура установки обновлений

На случай, если во время обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию программы и базы данных (см. раздел 8 настоящего документа), из которой можно будет восстановить данные.

Для обновления продукта:

- рекомендуется произвести очистку кэша используемого браузера;
- перенесите дистрибутив с обновленной версией программного компонента на сервер с установленным «Центром сертификации Aladdin Enterprise Certificate Authority» любым удобным способом;
- проверьте целостность дистрибутива путем подсчёта контрольной суммы (см. подраздел 3.2 настоящего документа);
- 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 8	`sudo apt-get install aeca-*.rpm`

- запустите установку продукта в режиме обновления, выполнив команду:

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

- установщик обнаружит установленную версию программного компонента и предложит выбрать необходимое действие в интерактивном режиме:
  - удалить установленную версию со всеми данными и выполнить чистую установку актуальной версии программного компонента;
  - выполнить обновление установленной версии до актуальной версии программного компонента;
  - 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 сертификации Aladdin Enterprise Certificate Authority»;
- проверьте версию обновленного компонента в окне Центра сертификации «О программе».

11.6 Критерий успешности установки обновления

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

12 УДАЛЕНИЕ ПРОГРАММНОГО КОМПОНЕНТА «ЦЕНТР СЕРТИФИКАЦИИ ALADDIN ENTERPRISE CERTIFICATE AUTHORITY»

12.1 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.

13 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

13.1 Удаление БД «aecaca»

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

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

```
sudo psql -U postgres
```

- Для предотвращения возможности новых подключений выполните команду:

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

- Для закрытия всех текущих сессий выполните команду:

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

- Удаляем базу данных, выполнив команду:

```
DROP DATABASE aecaca;
```

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

```
exit
```

13.2 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
```

14 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения

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

Ошибка запуска сервисов после запуска скрипта install.sh для установки программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority»	На сервере была установлена и удалена более ранняя версия Программы	Очистите конфигурацию nginx, выполнив команды:
		`sudo rm -rfv /etc/nginx/general-configs`
		`sudo rm -rfv /etc/nginx/conf.d/default.conf`

	Не хватка аппаратных ресурсов	Проверьте показатель загруженности оперативной памяти. Для корректной работы программы требуется не менее 6 Гб свободной оперативной памяти

ПРИЛОЖЕНИЕ 1. УСТАНОВКА РЕПОЗИТОРИЕВ

1.1 Установка репозиториев и подключение зависимостей для сервера под управлением ОС РЕД ОС 7.3

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

- 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 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 репозиториев выполните команду:

```
sudo apt-offline install
```

  - для установки зависимостей выполните команду:

```
sudo yum install tar unzip
```

1.2 Установка репозиториев 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 репозиториев, отредактировав файл `/etc/apt/sources.list`, выполнив команду:

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

- Укажите ссылки на следующие репозитории:

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

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

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

- Укажите нижеприведённый репозиторий для развёртывания web-сервера Nginx, если не требуется обеспечение сертифицированной среды[10]:

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

[10] для обеспечения сертифицированной среды программный компонент «Центр сертификации Aladdin Enterprise Certificate Authority» необходимо развёртывать с использованием web-сервера Apache в операционной системе Astra Linux Special Edition 1.7

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

```
apt-cdrom add
```

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

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

```
sudo apt update
```

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

```
sudo apt install tar unzip
```

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

1.3 Установка репозиториев и подключение зависимостей для сервера под управлением ОС Альт Сервер 8, релиз 10

- Для развёртывания программного компонента «Центр сертификации Aladdin Enterprise Certificate Authority» с использованием web-сервера Apache[11] перед началом установки компонента необходимо установить путь нахождения необходимого репозитория, отредактировав файл `/etc/apt/sources.list`, выполнив команду:

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

Укажите ссылку на следующий репозиторий:

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

[11] для обеспечения сертифицированной среды программный компонент «Центр сертификации Aladdin Enterprise Certificate Authority» необходимо развёртывать с использованием web-сервера Nginx в операционной системе Альт Сервер 8, релиз 10

ПРИЛОЖЕНИЕ 2. УСТАНОВКА AXIOM JDK[12]

2.1 Установка Axiom JDK для сервера под управлением ОС РЕД ОС 7.3, Альт Сервер 8, релиз 10

- Скачайте пакет и установите его, выполнив команду от имени суперпользователя (root или sudo):

```
sudo rpm --install axiomjdk-jdk-pro17.0.5+8-linux-amd64.rpm
```

2.2 Установка Axiom JDK для сервера под управлением ОС Astra Linux Special Edition 1.7

- Чтобы установить Axiom JDK, скачайте пакет .deb и запустите apt от имени суперпользователя (root или sudo):

```
sudo apt install axiomjdk-jdk-pro17.0.5+8-linux-amd64.deb
```

Эта команда установит пакет axiomjdk-java17-pro, включая AxiomFX.

- Чтобы использовать Axiom JRE, просто запустите команду

```
java -jar $your_app
```

Эта команда автоматически выберет зависимости AxiomFX или DeviceIO в случае наличия их в используемом JDK.

[12] Подробное описание приведено в официальной документации на Axiom JDK, размещённой по адресу https://axiomjdk.ru/pages/axiomjdk-install-guide-17.0.5/

ПРИЛОЖЕНИЕ 3. УСТАНОВКА OPEN JDK

3.1 Установка Open JDK на сервер под управлением ОС РЕД ОС 7.3

- Установите зависимости, выполнив команду:

```
sudo yum update
```

- Произведите установку вручную, предварительно загрузив дистрибутив с https://download.java.net/java/GA, выполнив команду:

```
sudo rm -rf jdk*
curl -s
https://download.java.net/java/GA/jdk17.0.2/dfd4a8d0985749f896bed50d7138ee7f/8/GPL/openjdk-17.0.2_linux-x64_bin.tar.gz | tar -zx
[ ! -d jdk-17.0.2/bin ] && exit 1
```

- Подготовьте папку для установки пакета, выполнив команду:

```
sudo mkdir -p /usr/java
[ -d /usr/java/jdk-17.0.2 ] && sudo rm -rf /usr/java/jdk-17.0.2
```

- Перенесите загруженный дистрибутив в созданную папку, выполнив команду:

```
sudo mv -f jdk-17.0.2 /usr/java
[ ! -d /usr/java/jdk-17.0.2/bin ] && exit 1
```

- Очистите папку `/usr/java/default` и сделайте символическую ссылку на папку установки, чтобы системные оболочки Java могли найти этот JDK, выполнив команду:

```
sudo rm -f /usr/java/default
sudo ln -sf /usr/java/jdk-17.0.2 /usr/java/default
```

- Сделайте необходимые символические ссылки, выполнив команды:

```
sudo update-alternatives --install "/usr/bin/java" "java" "/usr/java/jdk-17.0.2/bin/java" 1
sudo update-alternatives --install "/usr/bin/jstack" "jstack" "/usr/java/jdk-17.0.2/bin/jstack" 1
sudo update-alternatives --install "/usr/bin/jcmd" "jcmd" "/usr/java/jdk-17.0.2/bin/jcmd" 1
sudo update-alternatives --install "/usr/bin/jmap" "jmap" "/usr/java/jdk-17.0.2/bin/jmap" 1
sudo update-alternatives --set "java" "/usr/java/jdk-17.0.2/bin/java"
sudo update-alternatives --set "jstack" "/usr/java/jdk-17.0.2/bin/jstack"
sudo update-alternatives --set "jcmd" "/usr/java/jdk-17.0.2/bin/jcmd"
sudo update-alternatives --set "jmap" "/usr/java/jdk-17.0.2/bin/jmap"
```

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

```
java -version
```

- Проверьте все компоненты java (java, javac, javap) на соответствие выбранной версии 17:

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

- Получите путь до установленного пакета JDK-17, выполнив команду:

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

или

```
sudo update-alternatives --config javac
```

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

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

3.2 Установка Open JDK на сервер под управлением ОС Astra Linux Special Edition 1.7

- Установите зависимости, выполнив команды:

```
sudo apt-get update
sudo apt-get install wget curl
```

- Произведите установку вручную, предварительно загрузив дистрибутив с https://download.java.net/java/GA, выполнив команду:

```
sudo rm -rf jdk*
curl -s
https://download.java.net/java/GA/jdk17.0.2/dfd4a8d0985749f896bed50d7138ee7f/8/GPL/openjdk-17.0.2_linux-x64_bin.tar.gz | tar -zx
[ ! -d jdk-17.0.2/bin ] && exit 1
```

- Подготовьте папку для установки пакета, выполнив команду:

```
sudo mkdir -p /usr/java
[ -d /usr/java/jdk-17.0.2 ] && sudo rm -rf /usr/java/jdk-17.0.2
```

- Перенесите загруженный дистрибутив в созданную папку, выполнив команду:

```
sudo mv -f jdk-17.0.2 /usr/java
[ ! -d /usr/java/jdk-17.0.2/bin ] && exit 1
```

- Очистите папку `/usr/java/default` и сделайте символическую ссылку на папку установки, чтобы системные оболочки Java могли найти этот JDK, выполнив команду:

```
sudo rm -f /usr/java/default
sudo ln -sf /usr/java/jdk-17.0.2 /usr/java/default
```

- Сделайте необходимые символические ссылки, выполнив команды:

```
sudo update-alternatives --install "/usr/bin/java" "java" "/usr/java/jdk-17.0.2/bin/java" 1
sudo update-alternatives --install "/usr/bin/jstack" "jstack" "/usr/java/jdk-17.0.2/bin/jstack" 1
sudo update-alternatives --install "/usr/bin/jcmd" "jcmd" "/usr/java/jdk-17.0.2/bin/jcmd" 1
```

```
sudo update-alternatives --install "/usr/bin/jmap" "jmap" "/usr/java/jdk-17.0.2/bin/jmap" 1
sudo update-alternatives --set "java" "/usr/java/jdk-17.0.2/bin/java"
sudo update-alternatives --set "jstack" "/usr/java/jdk-17.0.2/bin/jstack"
sudo update-alternatives --set "jcmd" "/usr/java/jdk-17.0.2/bin/jcmd"
sudo update-alternatives --set "jmap" "/usr/java/jdk-17.0.2/bin/jmap"
```

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

```
java -version
```

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

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

3.3 Установка Open JDK на сервер под управлением ОС Альт Сервер 8, релиз 10

- Установите зависимости, выполнив команды:

```
sudo apt-get update
sudo apt-get install wget nano fontconfig libGL fonts-ttf-ms fonts-ttf-PTAstra fonts-ttf-paratype-pt-* fonts-ttf-ubuntu-font-family
fc-cache -f -v
sudo fc-cache -f -v
```

- Добавьте пользователя `root` в `/etc/sudoers`, выполнив команду:

```
sudo nano /etc/sudoers
```

Необходимо раскомментировать следующую строку в файле:

```
root ALL=(ALL:ALL) ALL
```

- Установите JDK (в репозиториях доступны только JRE). Загрузите дистрибутив и разархивируйте его, выполнив команды:

```
wget https://download.java.net/java/GA/jdk15.0.2/0d1cfde4252546c6931946de8db48ee2/7/GPL/openjdk-15.0.2_linux-x64_bin.tar.gz
gzip -d openjdk-15.0.2_linux-x64_bin.tar.gz
tar -xf openjdk-15.0.2_linux-x64_bin.tar
```

- Подготовьте папку для установки пакета, выполнив команду:

```
sudo mkdir -p /usr/java
[ -d /usr/java/jdk-15.0.2 ] && sudo rm -rf /usr/java/jdk-15.0.2
```

- Перенесите загруженный дистрибутив в созданную папку, выполнив команду:

```
sudo mv -f jdk-15.0.2 /usr/java
[ ! -d /usr/java/jdk-15.0.2/bin ] && exit 1
```

- Очистите папку `/usr/java/default` и сделайте символическую ссылку на папку установки, чтобы системные оболочки Java могли найти этот JDK, выполнив команду:

```
sudo rm -f /usr/java/default
sudo ln -sf /usr/java/jdk-15.0.2 /usr/java/default
```

- Сделайте необходимые символические ссылки, выполнив команды:

```
sudo ln -sf /usr/java/jdk-15.0.2/bin/java /usr/bin/java
sudo ln -sf /usr/java/jdk-15.0.2/bin/jstack /usr/bin/jstack
sudo ln -sf /usr/java/jdk-15.0.2/bin/jcmd /usr/bin/jcmd
sudo ln -sf /usr/java/jdk-15.0.2/bin/jmap /usr/bin/jmap
```

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

```
java -version
```

ПРИЛОЖЕНИЕ 4. УСТАНОВКА И НАСТРОЙКА СУБД POSTGRES[13]

4.1 Установка СУБД PostgreSQL

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду:

РЕД ОС 7.3	`sudo dnf install postgresql-server`
Astra Linux SE 1.7	`sudo apt install postgresq`
Альт Сервер 8	`sudo apt-get install postgresql-server`

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

РЕД ОС 7.3	`sudo dnf install postgresql-contrib`
Astra Linux SE 1.7	`sudo apt install postgresql-contrib`
Альт Сервер 8	`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 8	`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 8, релиз 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 9.

[13] Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу https://postgrespro.ru/docs

Таблица 9 – Выдержка из файла `pg_hba.conf` для редактирования

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

После вышеуказанных изменений строки должны иметь следующий вид:

`local`	`all`	`all`		`trust`
`#IPv4 local connection:`				
`host`	`all`	`all`	`127.0.0.1/32`	`password`
`#IPv6 local connection:`				
`host`	`all`	`all`	`::1/128`	`password`

– 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:

`zero_if_notfound: no`	на	`zero_if_notfound: yes`

После вышеуказанных изменений строки должны иметь следующий вид:

```
zero_if_notfound: yes
```

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

```
sudo systemctl start postgresql
```

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

`local all all peer`	на	`local all all trust`

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

```
sudo systemctl restart postgresql
```

4.2 Установка СУБД Postgres Pro

- Загрузите скрипт для добавления репозитория, выполнив команду:

РЕД ОС 7.3	`wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh`
Astra Linux SE 1.7	`wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh`
Альт Сервер 8	`wget https://repo.postgrespro.ru/std-16/keys/pgpro-repo-add.sh`

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

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

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

РЕД ОС 7.3	`sudo dnf update`
Astra Linux SE 1.7	`sudo apt update`
Альт Сервер 8	`sudo apt-get update`

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

РЕД ОС 7.3	`dnf install postgrespro-16-std`
Astra Linux SE 1.7	`sudo apt install postgrespro-std-16`
Альт Сервер 8	`sudo apt-get install postgrespro-16-std`

4.3 Установка СУБД PostgreSQL и СУБД Postgres Pro

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

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

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

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

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

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

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

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

4.4 Создание и настройка СУБД PostgreSQL в автоматическом режиме

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

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

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

4.5 Создание и настройка СУБД PostgreSQL в ручном режиме

Требования к настройке предварительно установленной СУБД PostgreSQL:

- создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД;
- создание базы данных, используемой 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:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

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

```
sudo psql –U postgres
```

- Создайте пользователя базы данных, выполнив команды:

```
CREATE USER aeca;
```

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

- Задайте пароль пользователю, выполнив команды:

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

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

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE aecaca;
```

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

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

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

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

```
GRANT ALL PRIVILEGES ON DATABASE aecaca 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
```

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

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

где `aecaca` – имя созданной базы данных.

ПРИЛОЖЕНИЕ 5. УСТАНОВКА И НАСТРОЙКА СУБД JATOBA[14]

5.1 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	– каталог /`packages`; – каталог `/repodata`; – файл ключа `RPM-GPG-KEY-Jatoba`
Astra Linux SE 1.7	– каталог /`pool`; – каталог `/dists`; – файл ключа `DEB-GPG-KEY-Jatoba`.
Альт Сервер 8	– каталог `/base`; – каталог `/RPMS.classic`; – файл ключа `RPM-GPG-KEY-Jatoba`.

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

```
ls -l
```

- Установите открытый ключ репозитория командой:

РЕД ОС 7.3	`sudo rpm --import /localrepo/RPM-GPG-KEY-Jatoba`
Astra Linux SE 1.7	`sudo apt-key add /localrepo/DEB-GPG-KEY-Jatoba`
Альт Сервер 8	-

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

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

РЕД ОС 7.3	`[jatoba-4]`
	`name=Jatoba 4 Official Repository`
	`baseurl=file:///localrepo`
	`enabled=1`
	`gpgcheck=0`
	`gpgkey=file:///localerepo/RPM-GPG-KEY-Jatoba`
		файл с описанием репозитория
		`/etc/yum.repos.d/jatoba-4.repo`

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 8	`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 8	`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 8	`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 завершённой;
  – 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:

```
crown postgres.postgres jatoba.cer
```

  – перед запуском СУБД в конце конфигурационного файла `/var/lib/jatoba/4/data/postgresql.conf`, в разделе `«LICENSER OPTION AND PARAMETRS»` проверьте наличие параметров и, в случае их отсутствия, внесите следующие данные, как указано в Таблица 10.

Таблица 10 – 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 11.

Таблица 11 – Выдержка из файла pg_hba.conf для редактирования

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

После вышеуказанных изменений строки должны иметь следующий вид:

`local`	`all`	`all`		`trust`
`#IPv4 local connection:`				
`host`	`all`	`all`	`127.0.0.1/32`	`password`
`#IPv6 local connection:`				
`host`	`all`	`all`	`::1/128`	`password`

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

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

5.2 Создание и настройка СУБД Jatoba 4 в автоматическом режиме

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

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

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

5.3 Создание и настройка СУБД Jatoba 4 в ручном режиме

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 psql -U postgres`
Astra Linux SE 1.7	`sudo psql -U postgres`

Альт Сервер 8	`sudo – postgres -s /bin/bash`
	`-bash-4.4$ /usr/jatoba-4/bin/psql`
	`psql`

- Создайте пользователя базы данных, выполнив команды:

```
CREATE USER aeca;
```

где aeca – задаваемое имя пользователя.

- Задайте пароль пользователю, выполнив команды:

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

где 'aeca' – задаваемый пароль пользователя.

- 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, выполнив команду:

```
GRANT ALL PRIVILEGES ON DATABASE aecaca 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 БДJatoba, выполнив команду от имени пользователя «postgres» (с правами root):

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

где `aecaca` – имя созданной базы данных.

ПРИЛОЖЕНИЕ 6. УСТАНОВКА JC-WEBCLIENT 4.3.2[15]

- Скачайте дистрибутив JC-WebClient. Дистрибутив для скачивания находится по адресу https://www.aladdin-rd.ru/support/downloads/jc-webclient.
- Установите зависимости
- Установите JC-WebClient, выполнив команду:

РЕД ОС 7.3	`sudo dnf install JC-WebClient-x64-x.x.x.xxxx.rpm`
Astra Linux SE 1.7	`sudo apt install -f JC-WebClient-x64-x.x.x.xxxx.deb`
Альт Сервер 8	`sudo apt-get install JC-WebClient-x64-x.x.x.xxxx.rpm`

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

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

- Произведите запуск ПО JC-WebClient, выполнив команду:

```
sh jcmon start
```

[15] При установке дополнительного программного обеспечения изделие обеспечивает возможность работы с ключевыми носителями (электронными ключами), при этом класс защиты не обеспечивается.

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

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

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

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

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

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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

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

Ключевой носитель – это сущность в центре сертификации, соответствующая физическому токену, программному или аппаратному модулю безопасности Hardware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

Контрольный список – это текстовый файл, в котором содержатся контрольные суммы всех файлов, входящих в дистрибутив ПО «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition, записанный на компакт-диск с размещённым на нём дистрибутивом программы и комплектом документации.

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

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

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

Расширение pgcrypto – предоставляет криптографические функции, которые позволяют администраторам баз данных PostgreSQL хранить определенные столбцы данных в зашифрованном виде.

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

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

Событие безопасности – идентифицированное возникновение состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или сбой средств контроля, или ранее неизвестную ситуацию, которая может быть значимой для безопасности.

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

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

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

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

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

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изм.	Номера листов (страниц)				Всего листов (страниц) в документе	Номер документа	Входящий номер сопроводительного документа и дата	Подпись	Дата
	измененных	замененных	новых	аннулированных					