Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition

Руководство администратора. Часть 4. Центр валидации Aladdin Enterprise Validation Authority

Изделие	RU.АЛДЕ.03.01.020
Документ	RU.АЛДЕ.03.01.020 32 01-4
Версия	2.4
Листов	176
Дата	28.05.2026

Авторские права, товарные знаки, ограничения

Ограничение ответственности

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

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

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

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

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

Государственное регулирование и экспортный контроль

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

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

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

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

Лицензионное соглашение

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

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

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

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

Права и собственность

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

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

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

Лицензия

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

Соглашения:

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

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

– не использовать, не модифицировать и не выдавать сублицензии на данное Программное обеспечение и любое другое ПО Компании, за исключением явных разрешений в данном Соглашении;

– не модифицировать, не демонтировать, не декомпилировать, не реконструировать, не видоизменять и не расширять данное Программное обеспечение и не пытаться раскрыть (получить) исходные коды данного Программного обеспечения;

– не помещать данное Программное обеспечение на сервер с возможностью доступа к нему третьих лиц через открытую сеть;

– не использовать какие бы то ни было резервные или архивные копии данного Программного обеспечения (или позволять кому–либо ещё использовать такие копии) с любой иной целью, кроме замены его оригинального экземпляра в случае его разрушения или наличия дефектов.

Требования к использованию

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

Использование ПО

Пользователь вправе:

– воспроизводить ПО путём записи его в память электронно–вычислительных машин Пользователя, ограниченное правом инсталляции, копирования и запуска программ для ЭВМ;

– встраивать ПО любым способом в продукты и решения Пользователя;

– распространять ПО любым способом исключительно в составе продуктов и решений Пользователя.

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

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

– дизайна (графики, расположения элементов оформления и т.п.);

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

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

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

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

Обслуживание и поддержка

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

Ограниченная гарантия

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

Отказ от гарантии

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

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

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

Ограничение возмещения

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

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

– возместить стоимость, выплаченную Вами за ПО.

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

Исключение косвенных убытков

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

Ограничение ответственности

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

Прекращение действия соглашения

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

После прекращения действия данного Лицензионного соглашения:

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

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

Применимое законодательство

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

Государственное регулирование и экспортный контроль

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

Разное

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

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

Я ПРИНИМАЮ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ ЦЕЛИКОМ.

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

АННОТАЦИЯ

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

Документ определяет порядок установки и эксплуатации программного комплекса eCA-VA из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

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

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

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

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

Требования доверия (16.1 Руководство администратора должно содержать описание)	**Раздел документа, в котором представлено свидетельство**
Действий по приёмке поставленного средства	Подраздел 1.5 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»
Действий по безопасной установке и настройке средства	Подраздел 1.6 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»
Действий по реализации функций безопасности среды функционирования средства	Подраздел 1.7 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»

СОДЕРЖАНИЕ

1 ВВЕДЕНИЕ

1.1 Назначение программы

Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority» (далее — eCA-VA) входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», которое применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификации при управлении доступом субъектов[1] доступа к объектам[2] доступа в автоматизированной (информационной) системе.

eCA-VA предназначен для проверки статуса сертификатов, выпускаемых программным комплексом «Центр сертификации Aladdin Enterprise Certification Authority» (далее — eCA-CA) из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

1.2 Состав программы

eCA-VA состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра валидации».

  Программный компонент реализует функции программного средства, для выполнения которых оно предназначено в заданных условиях применения, в части предоставления информации о сертификатах и их статусах.

- Программный компонент «Клиентская часть Центра валидации».

  Программный компонент реализует интерфейс (веб-интерфейс), с помощь которого обеспечивается взаимодействие пользователя и программного компонента «Серверная часть Центра валидации».

1.3 Функции программы

eCA-VA предоставляет информацию о сертификатах центров сертификации, пользователей и устройств, а также информацию об их статусах, в том числе:

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

Программа позволяет экспортировать опубликованные списки отозванных сертификатов (CRL) и сертификаты центров сертификации из точек распространения, реализованных программой.

- Проверку статусов сертификатов в режиме реального времени.

Программа позволяет выполнять проверку статусов сертификатов в режиме реального времени по протоколу Online Certificate Status Protocol (OCSP) [3].

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

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

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

1.4 Роли управления

В eCA-VA определены следующие роли: «Администратор», «Администратор инициализации» и «Аноним».

Пользователю с ролью «Администратор» доступны функции, сгруппированные в следующих разделах главного окна eCA-VA (см. 7.1):

- «Центры валидации» (см. 7.2);
- «Настройки» (см. 7.3);
- «Журнал событий» (см. 7.4).

Пользователю с ролью «Администратор инициализации» доступны функции, сгруппированные в следующих разделах главного окна eCA-VA (см. 7.1):

- «Настройки»;
- «Журнал событий».

Субъекту доступа с ролью «Аноним» не проходит аутентификацию в eCA-VA, ему недоступен пользовательский интерфейс eCA-VA, однако доступно взаимодействие с eCA-VA по его программным интерфейсам получения данных из точек распространения AIA и CRL (CDP) и выполнения OCSP-запросов. В зависимости от значения параметра actuator_authenticate конфигурационного файла «Анониму» могут быть доступны методы получения информации о сервисах.

Таблица 2 - Полномочия субъектов доступа

Тип действия, осуществляемого над объектом программы	**Возможные роли**		
	Администратор инициализации	**Администратор**	**Аноним**
Функции, сгруппированные в разделе «Центры валидации»			
Создание Центра валидации	-	✓	-
Создание службы OCSP созданного Центра валидации	-	✓	-
Ручное обновление сертификата службы OCSP	-	✓	-
Настройка параметров службы OCSP	-	✓	-
Удаление службы OCSP из Центра валидации	-	✓	-
Удаление Центра валидации	-	✓	-
Функции, сгруппированные в разделе «Настройки»			
Просмотр краткой информации о сертификате веб-сервера	✓	✓	-
Смена сертификата веб-сервера	✓	-	-
Просмотр списка разрешённых издателей подключённых eCA-CA	✓	✓	-
Просмотр параметров Syslog-серверов	✓	✓	-
Добавление Syslog-сервера	✓	-	-
Редактирование параметров Syslog-сервера	✓	-	-
Удаление Syslog-сервера	✓	-	-
Добавление подключения к eCA-CA	✓	-	-

Тип действия, осуществляемого над объектом программы	Возможные роли		
	Администратор инициализации	Администратор	Аноним
Удаление подключения к eCA-CA	✓	-	-
Функции, сгруппированные в разделе «Журнал событий»			
Просмотр всех существующих в программе событий журнала	✓	-	-
Просмотр событий журнала, ассоциированных с подключением к eCA-CA, которому принадлежит данный «Администратор»	✓	✓	-
Операции с сертификатами при помощи запросов к CDP, AIA и OCSP			
Экспорт сертификата центра сертификации из точки распространения AIA	-	-	✓
Экспорт списка отозванных сертификатов из точки распространения CRL или Delta CRL (при наличии)	-	-	✓
Получение статуса сертификата безопасности через запрос к службе OCSP	-	-	✓
Экспорт сертификата службы OCSP через запрос к службе OCSP (при включённой опции «Включать сертификат подписи в ответ» у службы OCSP)	-	-	✓
Экспорт цепочки сертификатов службы OCSP через запрос к службе OCSP (при включённой опции «Включать цепочку сертификатов в ответ» у службы OCSP)	-	-	✓

2 УСЛОВИЯ ВЫПОЛНЕНИЯ ПРОГРАММЫ

Для корректной работы Центру валидации Aladdin eVA необходима сетевая связанность с eCA-CA.

2.1 Требования к программному обеспечению

2.1.1 Требования к среде функционирования Серверной части программы

Среда функционирования Серверной части eCA-VA:

- Поддерживаемые ОС:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск».
  - Platform V SberLinux OS Server.
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
  - ОС «Альт Сервер» 11.
  - РЕД ОС версия 7.3, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - РОСА «ХРОМ» 12 Сервер.
- Поддерживаемые СУБД:
  - PostgreSQL из состава ОС.
  - Postgres Pro.
  - Jatoba.
- Поддерживаемые среды исполнения Java:
  - Java Axiom JDK Certified (компонент JRE).
  - OpenJDK версии 17 и выше из состава поддерживаемых ОС.
- Поддерживаемые веб-серверы:
  - Apache2 из состава ОС.
  - Nginx из состава ОС.
  - Cpnginx [1].
- Поддерживаемые ресурсные системы (доменные службы каталогов):
  - Samba DC.
  - Dynamic Directory.
  - Free IPA.
  - ALD PRO.
  - РЕД АДМ.
  - Microsoft AD.
  - Альт Домен.
- Поддерживаемый eCA-CA версии 2.4 [2].

[1] Из состава средства криптографической защиты (далее - СКЗИ) «КриптоПро CSP». СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» и при необходимости приобретается заказчиком самостоятельно.

[2] Входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition».

- СКЗИ «КриптоПро CSP»[1] - криптопровайдер, обеспечивающий формирование электронной подписи ответов службы OCSP по алгоритму ГОСТ Р 34.10-2012.

2.1.2 Требования к среде функционирования Клиентской части программы

Среда функционирования Клиентской части eCA-VA:

- Поддерживаемые ОС:
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Орёл».
  - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск».
  - Platform V SberLinux OS Server.
  - Альт 8 СП, релиз 10, вариант исполнения Сервер.
  - ОС «Альт Сервер» 11.
  - РЕД ОС версия 7.3, конфигурация «Сервер».
  - РЕД ОС версия 8, конфигурация «Сервер».
  - РОСА «ХРОМ» 12 Сервер.
- Веб-браузер из состава ОС.

2.2 Требования к аппаратным средствам

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

- Накопитель HDD или SSD - не менее 20 Гбайт.
- Оперативная память - не менее 4 Гбайт.
- Процессорные ядра с архитектурой x86, x64 - не менее 4 шт.
- VGA-совместимый видеоадаптер.
- Устройства взаимодействия с пользователем: клавиатура и мышь.
- USB 2.0 тип A или совместимые.

[1] СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в комплект поставки программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition» и при необходимости приобретается заказчиком самостоятельно. Порядок настройки взаимодействия eCA-VA с СКЗИ «КриптоПро CSP» описан в Приложении 4 настоящего руководства.

3 ПОДГОТОВКА К УСТАНОВКЕ ПРОГРАММЫ

При установке Центра валидации выполняется конфигурирование установленного в среде функционирования веб-сервера, в результате чего для внешнего доступа открывается порт, используемый для подключения по протоколу HTTPS (по умолчанию 443). Изменение порта веб-сервера для подключения к нему по протоколу HTTPS осуществляется путём редактирования конфигурационного файла Центра валидации.

В таблице ниже (Таблица 3) приведён список портов, которые должны быть открыты в eCA-VA и взаимодействующих компонентах.

Таблица 3 — Таблица сетевого взаимодействия

Порт	Транспорт	Протокол	Назначение	Возможность изменения
443	TCP	TLS/HTTPS	Порт для подключения к веб-интерфейсу eCA-VA (в версии 1.2 использовался порт 8888), а также для взаимодействия с eCA-CA.	Да
80	TCP	HTTP	Порт предоставляет доступ к точкам распространения CRL, DELTA CRL и AIA, а также к службе OCSP (в версии 1.2 использовался порт 8080).	Да
389	TCP	LDAP	Порт для взаимодействия с доменной службой каталогов (ресурсной системой) по протоколу LDAP.	Нет
88, 464	TCP	Kerberos	Порты для взаимодействия со службой аутентификации Kerberos ресурсной системы.	Нет
5432	TCP	TCP	Порт для подключения к СУБД.	Да
	TCP	TLS		
514	UDP	Syslog	Порт для отправки сообщений на Syslog-серверы (порт 514, как правило, используется по умолчанию).	Да
	TCP			

В таблице ниже (см. таблицу 4) приведён список портов, которые использует Центра валидации. Доступ к данным портам для внешних подключений ограничивается автоматически при установке Центра валидации с помощью утилиты «iptables» из состава ОС.

> **Внимание! Во избежание возникновения ошибок в работе Центра валидации переназначение данных портов запрещено.**

Таблица 4 - Входящие сетевые порты

Порт	Транспорт	Протокол	Назначение
1051	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «tasks-service» (сервис заявок)
1101	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «ca-adapter-service» (адаптер для подключения к Центру сертификации)
1201	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «policies-service» (сервис правил выпуска)
1251	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «security-service» (сервис безопасности)
1301	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «routes-service» (сервис маршрутизации)
1351	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «settings-service» (сервис настройки)
1401	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (сервис журнализации)

Порт	Транспорт	Протокол	Назначение
1451	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «export-service» (сервис экспорта)
1501	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «middleware-service» (связующий сервис для взаимодействия с внутренним контуром Центра валидации)
1551	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «kerberos-provider-service» (сервис аутентификации по kerberos)
1601	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «x509-provider-service» (сервис аутентификации по сертификату)
1651	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «external-integration-service» (сервис публичного API)
1701	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «api-gateway-service» (сервис проксирования)
1751	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «scep-enrollment-service» (сервис SCEP)
1801	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «wstep-enrollment-service» (сервис WSTEP)
1851	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «storage-service» (сервис хранения файлов)

Подготовка среды функционирования для установки Центра валидации, заключается в установке и настройке следующего ПО:

- Зависимостей и подключение репозиториев ОС.
- Среды исполнения Java.
- СУБД.
- Веб-сервера.

Также необходимо предварительно выполнить следующие действия:

- Если будет необходима аутентификация по доменным имени и паролю или билету Kerberos:
  - включить компьютер, на котором будет выполнено установка eCA-VA, в домен ресурсной системы (доменной службы каталогов);
  - создать службу HTTP и keytab-файл[1] на контроллере домена ресурсной системы (см. раздел 3.5).
- Создать в Центре сертификации учётную запись с правами «Администратор» для взаимодействия Центра валидации с Центром сертификации, выпустить для неё сертификат и выгрузить контейнер PKCS#12[2].
- Создать в Центре сертификации локальный субъект [8] для веб-сервера Центра валидации, выпустить для него сертификат и выгрузить контейнер PKCS#12.
- Перенести подготовленные контейнеры PKCS#12 на компьютер, где будет выполнено развёртывание Центра валидации.

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA Центр валидации может взаимодействовать с криптопровайдером СКЗИ «КриптоПро CSP». В данной ситуации в Центре валидации также необходимо применять СКЗИ «КриптоПро CSP» для:

[1] Keytab-файл используется для аутентификации доменных пользователей в eCA-VA с использованием Kerberos без ввода пароля.

[2] Порядок создания субъектов, учётных записей и выпуска сертификатов приведён в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority».

- Организации канала взаимодействия Серверных компонентов Центра сертификации и Центра валидации по протоколу TLS ГОСТ.
- Организации канала взаимодействия Клиентского и Серверного компонентов Центра валидации по протоколу TLS ГОСТ.
- Обеспечения TLS-аутентификации пользователей Центра сертификации в Центре валидации с использованием отечественных криптографических алгоритмов.
- Подписи маркеров доступа пользователей Центра сертификации по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 бит.
- Хранения закрытого ключа службы OCSP в «КриптоПро CSP (HDIMAGE)» или «КриптоПро HSM».

Порядок установки и настройки СКЗИ «КриптоПро CSP» представлен в приложении 4. Установка и настройка СКЗИ «КриптоПро CSP» могут быть выполнены после установки Центра валидации в процессе его эксплуатации.

При применении СКЗИ «КриптоПро CSP»:

- В качестве веб-сервера должен использоваться веб-сервер cpnginx из состава СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP». Порядок установки веб-сервера «cpnginx» приведён в разделе 3.6. После установки веб-сервера необходимо установить на СКЗИ «КриптоПро CSP» серверную лицензию, обеспечивающую возможность использования СКЗИ «КриптоПро CSP» в качестве TLS-сервера.
- Сертификаты для веб-сервера и учётной записи для взаимодействия с Центром сертификации должны быть выпущены по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 бит.

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

3.1.1 Подключение репозиториев и установка зависимостей

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

```
dnf install tar unzip iptables
```

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

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

```
dnf install tar unzip iptables
```

3.1.2 Установка среды исполнения Java

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

3.1.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.1.2.2 Установка OpenJDK

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

- Инструкция для РЕД ОС 7.3.
- Инструкция для РЕД ОС 8.

3.1.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в Приложении 1.

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

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

3.1.3.1 Установка СУБД PostgreSQL [1]

Порядок установки СУБД PostgreSQL:

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

```
dnf install postgresql-server
```

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

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду:

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

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

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

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

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

Примеры изменений:

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

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

[1] Подробное описание приведено на официальном сайте производителя.

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

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

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

```
systemctl restart postgresql
```

3.1.3.2 Установка СУБД Postgres Pro [1]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду [2]:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

Примеры изменений:

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

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

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

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

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

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

3.1.3.3 Установка СУБД Jatoba [5]

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

---

[1] Подробное описание приведено на официальном сайте производителя.

[2] Команды ниже приведена для СУБД Postgres Pro версии 16.

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

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

[5] Подробное описание приведено на официальном сайте производителя.

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

- Дистрибутив СУБД содержит:
  - Каталог /`packages`.
  - Каталог `/repodata.`
  - Файл ключа `RPM-GPG-KEY-Jatoba`.

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

```
ls -l
```

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

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

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

[1] Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

Примеры изменений:

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

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

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

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

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

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

3.1.4 Установка веб-сервера

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

3.1.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache для РЕД ОС:

- Установите пакет выполнив с правами суперпользователя следующую команду:

```
dnf install httpd
```

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

```
dnf install mod_ssl
```

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

```
systemctl enable httpd
```

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

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

```
dnf install apache-mod_ssl
```

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

```
urpmi apache-mod_proxy
```

- Установите модуль поддержку разделяемой памяти (shared memory) на основе слотов при помощи команды с правами суперпользователя:

```
dnf install apache-mod_slotmem_shm
```

3.1.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

3.2 Подготовка среды функционирования с ОС Astra Linux Special Edition 1.8

3.2.1 Подключение репозиториев и установка зависимостей

Порядок подключения репозиториев и зависимостей:

- Для обновления посредством сети Интернет перед началом установки компонентов необходимо установить пути нахождения всех необходимых репозиториев [1] отредактировав с правами суперпользователя файл `/etc/apt/sources.list`:
- Укажите ссылки на следующие репозитории [2]:

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

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

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

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

Пример:

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

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

```
apt-cdrom add
```

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

```
apt update
```

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

```
apt install tar unzip iptables
```

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

3.2.1.1 Поддержка активного режима замкнутой программной среды

eCA-VA обеспечивает работу ОС Astra Linux Special Edition 1.8 в активном режиме замкнутой программной среды (далее — ЗПС). Для этого в состав установочных пакетов eCA-VA включён публичный открытый ключ АО «Аладдин Р.Д.» — `aladdin_pub.key`. После распаковки установочного пакета ключ находится в каталоге `/opt/aecaVa/digsig/keys/aladdin_pub.key`.

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

[1] Ссылки на репозитории приведены для Astra Linux SE 1.8.5

[2] При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозиториев в соответствии с инструкцией по подготовке и присоединению хоста к домену ALD Pro.

3.2.2 Установка среды исполнения Java

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

3.2.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.2.2.2 Установка OpenJDK

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

3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

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

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

3.2.3.1 Установка СУБД PostgreSQL [1]

Порядок установки СУБД PostgreSQL:

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

```
apt install postgresql
```

- Выполните установку последней доступной версии пакета `postgresql-contrib`[2] выполнив следующую команду с правами суперпользователя:

```
apt install postgresql-contrib
```

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

```
apt install postgresql-client
```

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

```
systemctl enable postgresql
```

- Отредактируйте файл `/etc/postgresql/15/main/postgresql.conf`[3] с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`[4].

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

Примеры изменений:

---

[1] Подробное описание приведено на официальном сайте производителя.

[2] Для некоторых минорных версий ОС данный пакет может отсутствовать.

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

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

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

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

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

```
systemctl restart postgresql
```

3.2.3.2 Установка СУБД Postgres Pro [1]

Порядок установки СУБД PostgreSQL Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду [2]:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

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

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

Примеры изменений:

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

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

- Перезапустите СУБД выполнив команду с правами суперпользователя:

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

[1] Подробное описание приведено на официальном сайте производителя.

[2] Команды ниже приведены для СУБД Postgres Pro версии 16.

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

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

3.2.3.3 Установка СУБД Jatoba [1]

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

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

```
ls -l
```

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

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

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt update
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

[1] Подробное описание приведено на официальном сайте производителя.

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

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

Примеры изменений:

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

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

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

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

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

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

3.2.4 Установка веб-сервера

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

3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив команду с правами суперпользователя:

```
apt install apache2
```

- Активируйте модули выполнив команду с правами суперпользователя:

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

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

```
systemctl restart apache2.service
```

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

```
systemctl enable apache2
```

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

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

3.2.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
apt install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

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

3.3.1 Подключение репозиториев и установка зависимостей Альт 8 СП релиз 10 вариант исполнения Сервер

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

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

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

- Укажите в файле ссылку на следующий репозиторий:

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

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

```
apt-get update
```

3.3.2 Установка среды исполнения Java

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

3.3.2.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.3.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС.

3.3.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

- PostgreSQL.
- Postgres Pro.
- Jatoba.

Порядок разрешения конфликтов между СУБД PostgreSQL приведен в приложении 1.

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

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

3.3.3.1 Установка СУБД PostgreSQL [1]

Порядок установки СУБД PostgreSQL:

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

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

[1] Подробное описание приведено на официальном сайте производителя.

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

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

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

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

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

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

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

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

Примеры изменений:

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

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

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

```
systemctl restart postgresql
```

3.3.3.2 Установка СУБД Postgres Pro[3]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду [4]:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

[3] Подробное описание приведено на официальном сайте производителя.

[4] Команды ниже приведена для СУБД Postgres Pro версии 16.

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`[1] с правами суперпользователя, установив для числа подключений `max_connections` значение `1000`[2].

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

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

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

Примеры изменений:

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

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

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

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

3.3.3.3 Установка СУБД Jatoba [3]

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

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

- Дистрибутив СУБД содержит:
  - Каталог /`packages`.
  - Каталог `/repodata.`
  - Файл ключа `RPM-GPG-KEY-Jatoba`.

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

```
ls -l
```

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
apt-get update
```

---

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

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

[3] Подробное описание приведено в официальной документации на Jatoba.

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

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

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

Примеры изменений:

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

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

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

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

3.3.4 Установка веб-сервера

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

3.3.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

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

- Установите модуль ssl выполнив следующую команду с правами суперпользователя:

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

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

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

    Внесите следующий текст в созданный файл:

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

[1] Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

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

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

Внесите следующий текст в созданный файл:

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

- Активируйте модули выполнив поочерёдно следующие команды с правами суперпользователя:

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

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

```
a2enport https
```

3.3.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

```
apt-get install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

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

3.4.1 Установка среды исполнения Java

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

3.4.1.1 Установка Axiom JDK Certified

Для установки Axiom JDK Certified воспользуйтесь инструкцией из комплекта поставки.

3.4.1.2 Установка OpenJDK

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

3.4.2 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых СУБД:

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

Порядок разрешения конфликтов между СУБД PostgreSQL приведён в приложении 1.

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

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

3.4.2.1 Установка СУБД PostgreSQL [1]

Порядок установки СУБД PostgreSQL:

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

```
dnf install postgresql-server
```

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

```
dnf install postgresql-contrib
```

- Произведите инициализацию СУБД выполнив команду с правами суперпользователя:

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

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

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

- Запустите СУБД выполнив следующую команду с правами суперпользователя:

```
systemctl start postgresql
```

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

```
systemctl enable postgresql
```

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

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

Примеры изменений:

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

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

[1] Подробное описание приведено на официальном сайте производителя.

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

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

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

```
systemctl restart postgresql
```

3.4.2.2 Установка СУБД Postgres Pro [1]

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория выполнив следующую команду [2]:

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

- Запустите скрипт выполнив следующую команду с правами суперпользователя:

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

- Обновите список пакетов выполнив следующую команду с правами суперпользователя:

```
dnf update
```

- Установите СУБД выполнив следующую команду с правами суперпользователя:

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

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

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

Примеры изменений:

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

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

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

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

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

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

3.4.2.3 Установка СУБД Jatoba [5]

Порядок установки СУБД Jatoba:

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

```
mkdir /localrepo
```

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

---

[1] Подробное описание приведено на официальном сайте производителя.

[2] Команды ниже приведена для СУБД Postgres Pro версии 16.

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

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

[5] Подробное описание приведено на официальном сайте производителя.

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

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

```
ls -l
```

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

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

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

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

- Обновите описания пакетов выполнив следующую команду с правами суперпользователя:

```
dnf makecache
```

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

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

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

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

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

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

[1] Значение `max_connections` равное `1000` является рекомендуемым. При необходимости увеличьте данное значение.

Примеры изменений:

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

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

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

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

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

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

3.4.3 Установка веб-сервера

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

3.4.3.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install httpd
```

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

```
dnf install mod_ssl
```

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

```
systemctl enable httpd
```

3.4.3.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

- Установите пакет выполнив следующую команду с правами суперпользователя:

```
dnf install nginx
```

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

```
systemctl start nginx
```

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

```
systemctl enable nginx
```

3.5 Создание службы HTTP и keytab-файла

Создание службы HTTP и keytab-файла для eCA-VA выполняется аналогично созданию службы HTTP и keytab-файла для eCA-CA.

3.6 Установка веб-сервера cpnginx

Пакеты веб-сервера `cpnginx` расположены в дистрибутиве СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP» (см. приложение 4).

Порядок установки веб-сервера `cpnginx`:

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

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

- установите следующие пакеты:
  - для ОС Astra Linux SE командой с правами суперпользователя `dpkg -i <наименование пакета>.deb`:
  - `cprocsp-nginx-64_5.0.13000-7_amd64.deb`;
  - `lsb-cprocsp-rcrypt-64_5.0.13300-7_amd64.deb`;
  - `cprocsp-pki-plugin-64_2.0.15000-1_amd64.deb`.
  - для ОС РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server командой с правами суперпользователя `dnf install <наименование пакета>.rpm`:
  - `cprocsp-nginx-64-5.0.13000-7.x86_64.rpm`;
  - `lsb-cprocsp-rcrypt-64-5.0.13000-7.x86_64.rpm`.
  - для ОС Альт Сервер командой с правами суперпользователя `apt-get install <наименование пакета>.rpm`:
  - `cprocsp-nginx-64-5.0.13000-7.x86_64.rpm`;
  - `lsb-cprocsp-rcrypt-64-5.0.13000-7.x86_64.rpm`.
- установите на СКЗИ «КриптоПро CSP» соответствующую лицензию (TLS-сервер) командой с правами суперпользователя:

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

- выполните проверку активации лицензии командой с правами суперпользователя:

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

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

```
systemctl start cpnginx.service
```

- Включите автоматический запуск веб-сервера при загрузке выполнив команду с правами суперпользователя:

```
systemctl enable cpnginx.service
```

4 УСТАНОВКА ПРОГРАММЫ

4.1 Установка инсталляционного пакета eCA-VA

Установите инсталляционный rpm/deb-пакет eCA-VA штатными средствами ОС.
Инсталляционный rpm/deb-пакет автоматически распакуется в директорию `/opt/aecaVa`.
Структура инсталляционного rpm/deb-пакета eCA-VA приведена в таблице 5.

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

Структурный элемент	**Назначение элемента**
/opt/aecaVa	Установочный комплект eCA-VA, а также используемые дополнительные инструменты
/opt/aecaVa/bin	Каталог с дополнительными утилитами
/opt/aecaVa/bin/jcverify	Каталог утилиты контроля целостности «jcverify»
/opt/aecaVa/bin/jcverify/jcverify	Утилита контроля целостности «jcverify»
/opt/aecaVa/bin/jcverify/jcverify.txt	Вспомогательный файл для работы утилиты целостности «jcverify»
/opt/aecaVa/dist	Путь развёртывания продукта; содержит создаваемые временные файлы
/opt/aecaVa/dist/archive/	Архивы, сформированные в результате очистки журнала событий (путь по умолчанию, может быть изменён)
/opt/aecaVa/dist/backup/	Созданные резервные копии eCA-VA
/opt/aecaVa/dist/certificates/ssl	Расположение сертификатов для управления ssl-соединением
/opt/aecaVa/dist/environment/	Расположение переменных окружения сервисов
/opt/aecaVa/dist/sign-in/initial_admin.txt	Файл, содержащий логин и пароль администратора инициализации, создаваемого при чистой установке eCA-VA
/opt/aecaVa/dist/logs/	Расположения технических логов сервисов
/opt/aecaVa/eula	Каталог с файлом лицензионного соглашения (EULA). Название и содержимое файла лицензионного соглашения различаться в зависимости от редакции eCA-VA: в оригинальной редакции файл имеет название «LicenAgr_ПО_v1_2015.rtf»
/opt/aecaVa/samples	Содержит шаблоны файлов конфигурации для внутреннего использования программным средством
/opt/aecaVa/scripts	Содержит скрипты управления eCA-VA
/opt/aecaVa/scripts/internal	Скрипты для внутреннего использования программы, запускаемые автоматически при выполнении скриптов из каталога /opt/aecaVa/scripts
/opt/aecaVa/scripts/backup.sh	Скрипт резервного копирования eCA-VA
/opt/aecaVa/scripts/config.sh	Файл конфигурации eCA-VA
/opt/aecaVa/scripts/database_create.sh	Скрипт создания базы данных и её пользователя на сервере eCA-VA с указанными в конфигурационном файле параметрами
/opt/aecaVa/scripts/diagnostics.sh	Скрипт сбора диагностической информации eCA-VA
/opt/aecaVa/scripts/install.sh	Скрипт установки и обновления eCA-VA
/opt/aecaVa/scripts/integrity_check.sh	Скрипт контроля целостности исполняемых файлов
/opt/aecaVa/scripts/restore_access.sh	Скрипт восстановления данных для входа администратора инициализации
/opt/aecaVa/scripts/restore.sh	Скрипт восстановления из резервной копии eCA-VA
/opt/aecaVa/scripts/uninstall.sh	Скрипт удаления eCA-VA
/opt/aecaVa/scripts/jc_checksum	Файл с эталонами контрольных сумм исполняемых файлов eCA-VA
/opt/aecaVa/scripts/key	Файл, содержащий симметричный ключ шифрования паролей в конфигурационном файле eCA-VA
/opt/aecaVa/services	Сервисы eCA-VA
/opt/aecaVa/static	Артефакты клиентского компонента eCA-VA

Структурный элемент	Назначение элемента
/opt/aecaVa/digsig/keys/aladdin_pub.key	Открытый ключ АО «Аладдин Р.Д.», используемый для проверки подписи исполняемых файлов и библиотек eCA-VA на Astra Linux Special Edition в режиме замкнутой программной среды (ЗПС).

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

4.2 Настройка конфигурации программы

Настройка конфигурации программы выполняется путём редактирования конфигурационного файла `/opt/aecaVa/scripts/config.sh`.

Параметры конфигурации, содержащиеся в конфигурационном файле, приведены в таблице 6.

Таблица 6 — Параметры конфигурации

Ключ	Значение по умолчанию	Описание
Конфигурация развёртывания		
webserver	'#CHANGEIT'	Используемый web-сервер Допустимые значения: "nginx", "apache", "cpnginx" '#CHANGEIT' означает, что параметр не задан
webserver_path	'#CHANGEIT'	Расположение конфигурации веб-сервера. '#CHANGEIT' означает, что параметр не задан
aeca_path	'/opt/aecaVa/dist'	Каталог установки eCA-VA
environment_path	'/opt/aecaVa/dist/environment'	Конфигурация развёртывания
cryptotoken_path	'/opt/aecaVa/dist/cryptotoken'	Каталог хранения контейнеров служб OCSP
webserver_config_path	'/opt/aecaVa/dist/webserver'	Расположение конфигурации eCA-VA для веб-сервера
encryption_key_path	'/opt/aecaVa/scripts/key'	Ключ для шифрования конфигурационного файла
proxy_connect_timeout	'320'	Время ожидания подключения к прокси-серверу перед тем, как будет выдано сообщение об ошибке Только для nginx Настраивается разработчиком eCA-VA, редактировать не следует.
proxy_send_timeout	'320'	Время ожидания ответа от прокси-сервера после отправки запроса. Если ответ не получен в

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

Ключ	Значение по умолчанию	Описание
		помощью утилиты «cpconfig» из состава «КриптоПро CSP» 1
ssl_protocols	'TLSv1.2 TLSv1.3'	Поддерживаемые версии протокола TLS Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обоих версий необходимо указывать их через пробел).
backup_path	'/opt/aecaVa/dist/backup'	Путь до места хранения резервных копий
logs_base	'/opt/aecaVa/dist/logs'	Путь хранения лог-файлов
archive_path	'/opt/aecaVa/dist/archive'	Путь до архивированных файлов. Можно менять. Только абсолютные пути. Права на каталог должны быть предоставлены пользователю/группе aeca:aeca.
certificates_ssl_path	'/opt/aecaVa/dist/certificates/ssl'	Путь хранения контейнера, сертификата и ключа web-сервера, а также цепочек сертификатов разрешенных издателей
Конфигурация пользователя		
aeca_user	'aeca'	Имя локального пользователя, создаваемого при установке eCA-VA
aeca_group	'aeca'	Наименование группы, создаваемой при установке eCA-VA, в которую входит пользователь, создаваемый по параметру «aeca_user»
Конфигурация памяти		
memory	'4096'	Конфигурация памяти (значение в МБ)
enable_gc_diagnostic	'false'	Флаг сбора диагностической информации о памяти
enable_heap_dump	'false'	Флаг сбора дампов памяти для упавших сервисов eCA-VA
Конфигурация БД		
max_db_pool_size	'200'	Максимальный размер пула подключений к СУБД

[1] Инструкция по установке и настройке cpnginx - https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/440/0/nginx-gost-binary-packages.

Ключ	Значение по умолчанию	Описание
		Настраивается разработчиком eCA-VA, редактировать не следует
use_tls	'false'	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя СУБД
database_password	По умолчанию не задано. Указывается администратором инициализации при установке	Пароль пользователя СУБД
database_host	'localhost'	Имя хоста СУБД. Указано значение по умолчанию.
database_port	'5432'	Порт для доступа к СУБД. Указано значение по умолчанию.
database_name	'aecava'	Имя БД. Указано значение по умолчанию.
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД. '#CHANGEIT' означает, что параметр не задан
Конфигурация eCA-VA		
http_port	'80'	Порт для подключения к eCA-VA по протоколу http
https_port	'433'	Порт для подключения к eCA-VA по протоколу https
hostname	'localhost'	Имя сервера eCA-VA
hostname_no_mtls	'#CHANGEIT'	Параметр используется только в конфигурации с CPNGINX Имя хоста (должно отличаться от значения hostname), используемое для доступа к интерфейсу без использования mTLS '#CHANGEIT' означает, что параметр не задан
Переменные окружения, используемые всеми сервисами		
number_of_services	'9'	Количество активных сервисов
logging_response	'false'	Переменные окружения, используемые всеми сервисами
logging_sql	'false'	Переменные окружения, используемые всеми сервисами

Ключ	Значение по умолчанию	Описание
Переменные окружения для logback		
logs_file_max_size	'10MB'	Максимальный размер файла лога сервиса перед его архивацией. При достижении данного значения текущий лог-файл (access.log или service.log) будет архивироваться – файл будет сохранен в текущем каталоге логов данного сервиса с именем {access или service}-{дата в формате YYYY-MM-DD}.{индекс лога}.log.
logs_max_history	'10'	Максимальный срок хранения архивов логов в днях. Архивы логов, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться.
logs_total_size_cap	'100MB'	Максимальный общий объем логов, включая архивы, каждого типа (access или service) для каждого сервиса При достижении данного объема наиболее старые архивы логов данного типа будут удаляться.
api_key	'2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810'	Ключ для внутренней аутентификации
Переменные окружения, используемые settings-service		
certificate_server_name	'#CHANGEIT'	Имя файла сертификата web-сервера. '#CHANGEIT' означает, что параметр не задан
certificate_raw_server_password	'#CHANGEIT'	Пароль от контейнера сертификата web-сервера. '#CHANGEIT' означает, что параметр не задан
issuers_name	'issuers'	Имя файла разрешённых издателей
issuers_sync	'0 */30 * * * *'	CRON-выражение, по которому выполняется синхронизация разрешённых издателей
refresh__token_expire	'86400000'	Время жизни JWT токена обновления в миллисекундах Значение по умолчанию: 86400000 мс (1 сутки). В течение данного срока маркер обновления можно использовать для получения нового маркера доступа и маркера обновления.

Ключ	Значение по умолчанию	Описание
		По истечению данного срока маркер обновления нельзя использовать для этого. И для получения нового маркера доступа и обновления потребуется повторная аутентификация.
token_expire	'180000'	Время жизни JWT токена доступа в миллисекундах Значение по умолчанию: 180000 мс (3 минуты).
Переменные окружения, используемые security-service		
kerberos_enabled	'false'	Активация kerberos
session_max_count	'100'	Максимальное число сессий аккаунта (-1 - ограничение отключено) Значение по умолчанию: 100. Допустимые варианты указания предельного количества сессий для учетных записей: 1) натуральное число, представленное в десятичной системе счисления; 2) число «0»; 3) число «-1» (для выключения ограничения на количество сессий).
kerberos_service_principal	'#CHANGEIT'	Имя принципала, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_keytab_location	'#CHANGEIT'	Расположение keytab файла, содержащего тикет принципала, используемого для авторизации. '#CHANGEIT' означает, что параметр не задан
kerberos_krb5_location	'#CHANGEIT'	Расположение файла конфигурации krb5.conf '#CHANGEIT' означает, что параметр не задан
kerberos_ad_domain	'#CHANGEIT'	Имя подключаемого домена. '#CHANGEIT' означает, что параметр не задан
kerberos_ad_server	'#CHANGEIT'	Адрес сервера контроллера домена Доступно указание сервера в формате ldap://<адрес контроллера домена> (для подключения по протоколу LDAP) и ldaps://<адрес контроллера домена> (для подключения по протоколу LDAPS).

Ключ	Значение по умолчанию	Описание
		По умолчанию eCA-VA при подключении к домену по протоколу LDAPS будет доверять любому сертификату, предоставленному контроллером домена. '#CHANGEIT' означает, что параметр не задан
resource_type	'#CHANGEIT'	Тип РС (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN). При подключении к ресурсной системе Dynamic Directory необходимо указывать значение 'FREE_IPA' '#CHANGEIT' означает, что параметр не задан
resource_base_dn	'#CHANGEIT'	Точка подключения ресурса. '#CHANGEIT' означает, что параметр не задан
ldap_enabled	'false'	Активация ldap
ldap_sign_in_failure_max_count	'5'	Максимальное количество неудачных попыток аутентификации через LDAP
ldap_sign_in_failure_delay_millis	'3600000'	Время задержки после последней неудачной попытки аутентификации через LDAP
Дополнительные настройки для подключения к домену с усиленными требованиями по безопасности аутентификации		
channel_binding_enabled	'false'	Включает поддержку привязки к TLS-каналу (Channel Bindings). Только для подключения к домену по протоколу LDAPS. Флаг будет проигнорирован, если подключение осуществляется по протоколу LDAP. Включение данного флага требуется для удовлетворения требования домена к наличию токенов привязки канала при аутентификации по Kerberos.
ldap_starttls_enabled	'false'	Включает TLS-шифрование (директива STARTTLS) при подключении к домену по протоколу LDAP для аутентификации. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS.

Ключ	Значение по умолчанию	Описание
		Включение данного флага требуется для возможности аутентификации доменных пользователей по логинам и паролям, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию.
kerberos_qop_enabled	'false'	Включает механизмы QOP (Quality of Protection) для защиты данных внутри протокола Kerberos при подключении к домену по протоколу LDAP. Только для подключения к домену по протоколу LDAP. Флаг будет проигнорирован, если подключение осуществляется по LDAPS. Включение данного флага требуется для возможности аутентификации доменных пользователей по Kerberos-билетам, если используется протокол LDAP (а не LDAPS) и сервер домена требует строгую аутентификацию.
sign_provider	'EMBEDDED'	Провайдер подписи (выбирается между стандартным - 'EMBEDDED', КриптоПро - 'CRYPTO_PRO' и Aladdin JCP – 'ALADDIN_JCP')
sign_key_algorithm	'RSA'	Алгоритм подписи ключа Для стандартного провайдера подписи доступны алгоритмы 'RSA' и 'ECDSA'. Для провайдера подписи КриптоПро доступны алгоритмы 'RSA' и 'GOST_R_34_10_2012'. Для провайдера Aladdin JCP доступен алгоритм 'GOST_R_34_10_2012'.
sign_key_length	'2048'	Длина ключа подписи
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи Доступные для выбора значения алгоритмов хэширования: 1) для стандартного провайдера (EMBEDDED): для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования

Ключ	Значение по умолчанию	Описание
		'SHA1', 'SHA256', 'SHA512', 'SHA384' 2) для провайдера КриптоПро (CRYPTO_PRO): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012' для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' 3) для провайдера Aladdin JCP (ALADDIN_JCP): для алгоритма ключа 'GOST_R_34_10_2012' доступен алгоритм хэширования 'GOST_R_34_11_2012'
Переменные окружения, используемые logs-service		
archive_cron	'0 0 0 1 * *'	CRON выражение, по которому запускается архивация журнала событий.
archive_enabled	'true'	Флаг: включена архивация. Возможные значения: true/false
archive_millis_ago	'15778800000'	Архивировать записи старше
Переменные окружения, используемые validation-authority-service		
ocsp_certificate_renewal_threshold	'90'	Пороговое значение для проверки сертификатов
ocsp_certificate_renewal_cron	'0 0 0 * * *'	CRON-выражение, по которому выполняется синхронизация сертификатов
validation_authority_status_cron	'0 0/5 * * * *'	CRON-выражение, по которому выполняется проверка подключения центров валидации к центрам сертификации eCA-CA
Переменные окружения, используемые api-gateway-service		
max_requests_count	'30'	Максимальное число параллельных HTTP запросов
actuator_authenticate	'false'	Флаг доступности без аутентификации методов Spring Boot Actuator (используются для получения информации о сервисах eCA-VA) и метода GET api/version сервиса внешних интеграций (external-integration-service). При включении данного флага методы Spring Boot Actuator и GET api/version будут недоступны без

Ключ	Значение по умолчанию	Описание
		аутентификации пользователя. Для аутентифицированного пользователя в любой роли (администратора, администратора инициализации) останутся доступными.
integrity_check_startup_enabled	'true'	Флаг выполнения контроля целостности при запуске eCA-VA Допустимые значения: true, false
integrity_check_fail_block_startup	'true'	Флаг блокировки запуска служб eCA-VA при неуспешной проверке целостности Допустимые значения: true, false
Данные eCA-VA, отображаемые в окне авторизации		
login_window_product_name	'Aladdin Enterprise CA'	Название программы, отображаемое в окне авторизации
login_window_component_name	'Центр валидации'	Название компонента, отображаемое в окне авторизации
tab_title	'Aladdin Enterprise Validation Authority'	Текст, отображаемый в заголовке вкладок браузера
use_credentials_from_config	'true'	Флаг использования имени и пароля пользователя СУБД, указанных в параметрах `database_username` и `database_password` соответственно. Допустимые значения: `true`, `false`. Если данный параметр имеет значение `false`, eCA-VA будет требовать указывать имя и пароль пользователя СУБД при выполнении следующих скриптов: – `install.sh`; – `uninstall.sh`; – `integrity_check.sh`; – `database_create.sh`; – `backup.sh`; – `restore.sh`. Данные скрипты поддерживают следующие способы передачи в них имени и пароля пользователя СУБД: – в параметрах запуска `--dbuser` или `-U` (имя пользователя СУБД) и

Ключ	Значение по умолчанию	Описание
		`--dbpass` или `-P` (пароль пользователя СУБД); – в диалоговом режиме. Если не был указан какой-либо из параметров запуска, приведённых выше, скрипты при их запуске запросят ввод имени и/или пароля пользователя СУБД («Укажите имя пользователя СУБД» и/или «Укажите пароль пользователя СУБД») Если параметр `use_credentials_from_config` имеет значение `true`, то при работе скриптов в качестве имени и пароля пользователя СУБД будут использоваться значения параметров `database_username` и `database_password` конфигурационного файла. При этом скрипты будут игнорировать параметры запуска `--dbuser` (`-U`) и/или `--dbpass` (`-P`), уведомляя пользователя сообщением в терминале: «[WARN] Параметр запуска "название параметра" проигнорирован, так как включено использование имени и пароля пользователя СУБД из конфигурационного файла»
strong_permissions_to_exception_files	'false'	Флаг установки прав доступа 640 на файлы-исключения. По умолчанию eCA-VA устанавливает права доступа 640 на все свои файлы, кроме исключений (см. список ниже) и утилиты «jcverify». Утилита «jcverify» имеет права 740 (-rwxr-----) для возможности ее запуска при выполнении КЦ. Исключения (файлы по умолчанию имеют права 775): • файлы в каталоге «/opt/aecaVa/static» и его подкаталогах. Они представляют собой файлы клиентского компонента, доступ к ним необходим для Web-сервера. • файлы в каталоге «/opt/aecaVa/dist/webserver» и его подкаталогах. Данные файлы представляют собой конфигурации, подключаемые к Web-серверу. • файлы в каталоге «/opt/aecaVa/dist/certificates/ssl». В

Ключ	Значение по умолчанию	Описание
		данном каталоге располагается сертификат Web-сервера, его закрытый ключ, а также файл с разрешенными издателями. При включении данного флага права доступа 640 будут установлены на указанные выше файлы-исключения. Для обеспечения сертифицированной среды функционирования присвойте параметру значение 'true'

Необходимо определить значения следующих параметров:

- `webserver` — используемый веб-сервер (`nginx`, `apache` или `cpnginx`). Также значение параметра можно будет ввести после запуска инсталлятора установки, в интерактивном режиме выбрав веб-сервер;
- `webserver_path` — папка с файлами для развёртывания веб-сервера. Также значение параметра можно будет ввести при запуске инсталлятора, в интерактивном режиме указав путь к файлам веб-сервера:
  - `/etc/nginx` для nginx;
  - `/etc/apache2` для apache на Astra Linux SE;
  - `/etc/httpd` для apache на RedOS и SberLinux OS Server;
  - `/etc/httpd2` для apache на Альт Сервер;
  - `/etc/opt/cprocsp/cpnginx` для cpnginx;
- `use_credentials_from_config` — значение флага использования имени и пароля пользователя СУБД из конфигурационного файла.
- Если параметр `use_credentials_from_config` установлен в значение `true` (значение по умолчанию), то укажите значения параметра `database_password` — пароль создаваемой базы данных.[1]
- `certificate_raw_server_password` — пароль от контейнера закрытого ключа веб-сервера.
- `root_cert_path` — абсолютный путь к сертификату корневого центра сертификации из цепочки сертификатов сервера СУБД. Значение параметра необходимо заполнить только при включённом флаге обязательного использования TLS для подключения к СУБД (при значении параметра `use_tls=true`).
- `hostname` — полное доменное имя компьютера, на котором будет развёрнут eCA-VA.

Для обеспечения корректности встраивания СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента программы должен быть организован по протоколу TLS ГОСТ, должна обеспечиваться TLS-аутентификация пользователей в программном средстве с использованием отечественных криптографических алгоритмов, а маркеров доступа пользователей eCA-CA должен быть подписан по алгоритму ГОСТ Р 34.11-2012/34.10-2012 256/512 бит. Для этого настройте конфигурационный файл в соответствии с таблицей 7.

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

Таблица 7 - Параметры для настройки TLS ГОСТ

Параметр	Значение
webserver	'cpnginx'
webserver_path	'/etc/opt/cprocsp/cpnginx'
sign_provider	'CRYPTO_PRO'
sign_key_algorithm	'GOST_R_34_10_2012'
sign_key_length	'256' или '512
sign_hash_algorithm	'GOST_R_34_11_2012'

Для обеспечения аутентификации в eCA-VA субъектов домена, к которому подключён eCA-VA и eCA-CA, укажите необходимые значения следующих параметров в конфигурационном файле:

- `kerberos_enabled` - для активации аутентификации по билету Kerberos, параметр должен иметь значение true. Пример: `kerberos_enabled='true'`.
- `session_max_count` - предельное количества сессий для учётных записей ресурсной системы. Пример: `session_max_count='100'`.
- `kerberos_service_principal` - имя принципала, для которого выпущен файл http.keytab; должно совпадать с именем хоста компьютера, на котором запускается eCA-VA; создаётся в ресурсной системе; формат имени принципала: `HTTP/<имя хоста>@<имя домена>`. Пример: `kerberos_service_principal='HTTP/va-22.ms.ad.aldn@MS.AD.ALDN'`.
- `kerberos_keytab_location` - место размещения файла http.keytab для имени принципала хоста, на котором размещается eCA-VA.

Пример: `kerberos_keytab_location='/opt/va-22/pki_admin_http.keytab'`.

- `kerberos_krb5_location` - путь к файлу krb5.conf хоста, на котором размещается eCA-VA. Пример: `kerberos_krb5_location='/etc/krb5.conf'`.
- `kerberos_ad_domain` - имя домена заглавными буквами.

Пример: `kerberos_ad_domain='MS.AD.ALDN'`.

- `kerberos_ad_server` — имя сервера контроллера домена в формате: `ldap://<имя контроллера домена>.<имя домена>` или `ldaps://<имя контроллера домена>.<имя домена>`

Пример: `kerberos_ad_server='ldap://dc1.ms.ad.aldn'`.

- `resource_type` - тип ресурсной системы (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN). Пример: `resource_type='MS_AD'`.
- `resource_base_dn` - должен указывать на каталог в ресурсной системе, либо на контейнер в нем, ограничивая аутентификацию субъектами данной ресурсной системы. Пример: `resource_base_dn='dc=ms,dc=ad,dc=aldn'`.
- `ldap_enabled` - для активации аутентификации по доменным логину и паролю, параметр должен иметь значение true. Пример: `ldap_enabled='true'`.

4.3 Настройка веб-сервера при ограничении доступа к его файлам

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

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

4.4 Создание и настройка базы данных

База данных eCA-VA (имя базы данных по умолчанию `aecava`) предназначена для хранения информации:

- об учётных записях;
- о заявках;
- о правилах выдачи сертификатов;
- журнала событий;
- о ролях пользователей;
- о правах, определённых для ролей пользователей.

Базу данных eCA-VA необходимо создать и настроить перед установкой eCA-VA. Это может быть выполнено одним следующих из способов:

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

4.4.1 Создание и настройка базы данных в автоматическом режиме

Перед созданием базы данных в конфигурационном файле `/opt/aecaVa/scripts/config.sh` должны быть заданы параметры создаваемой базы данных в (см. 4.2).

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

Для создания и настройки базы данных:

1. Запустите скрипт[2] командой с правами суперпользователя:

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

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

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

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

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

- Если в качестве операционной системы в среде функционирования eCA-VA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным МРД, то при использовании локальной СУБД необходимо:
  - создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путём выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя_СУБД`.
  - назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя_СУБД`;
  - предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме

Требования к настройке предварительно установленной СУБД PostgreSQL:

- создание пользователя, от имени которого будет осуществляться 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 удалённой, доступной для подключений.

- Запустите PostgreSQL выполнив с правами суперпользователя команду:

```
systemctl start postgresql
```

- Включите автоматический запуск PostgreSQL при загрузке выполнив с правами суперпользователя команду:

```
systemctl enable postgresql
```

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

```
-u postgres psql
```

- 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. 4.2).

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

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

- Задайте пароль пользователю выполнив команду:

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

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

- Создайте базу данных выполнив команду:

```
CREATE DATABASE aecava;
```

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

- Назначьте владельцем созданной базы данных созданного пользователя выполнив команду:

```
ALTER DATABASE aecava OWNER TO aeca;
```

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

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

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

```
exit
```

- Перезапустите СУБД PostgreSQL выполнив с правами суперпользователя команду:

```
systemctl restart postgresql
```

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

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

где `aecava` - имя созданной базы данных.

- Если в качестве операционной системы в среде функционирования eCA-VA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД[1], при использовании локальной СУБД дополнительно необходимо:
  - создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путем выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя_СУБД`.
  - назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя_СУБД`;
  - предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

4.4.3 Создание и настройка базы данных Jatoba в ручном режиме

Требования к настройке предварительно установленной СУБД Jatoba:

- создание пользователя, от имени которого будет осуществляться всё взаимодействие с СУБД;
- создание базы данных, используемой Программой в процессе работы;

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

- назначение созданному пользователю полных прав доступа к созданной базе данных.

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите Jatoba командой с правами суперпользователя:

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

- Включите автоматический запуск Jatoba при загрузке выполнив с правами суперпользователя команду:

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

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

РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	`-u postgres psql`
Astra Linux SE	`-u postgres psql`

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

- Создайте пользователя базы данных выполнив команды:

```
CREATE USER aeca;
```

где `aeca` - задаваемое имя пользователя.

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

- Задайте пароль пользователю выполнив команды:

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

где `'aeca'` - задаваемый пароль пользователя.

- Создайте базу данных выполнив команду:

```
CREATE DATABASE aecava;
```

где `aecava` - задаваемое имя базы данных.

- Назначьте владельцем созданной базы данных созданного пользователя выполнив команду:

```
ALTER DATABASE aecava OWNER TO aeca;
```

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

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

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

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

```
exit
```

- Перезапустите СУБД Jatoba выполнив с правами суперпользователя команду:

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

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

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

где `aecava` - имя созданной базы данных.

- Если в качестве операционной системы в среде функционирования eCA-VA используется ОС Astra Linux Special Edition 1.8 с уровнем защищённости «Смоленск» и активным механизмом МРД[1], при использовании локальной СУБД дополнительно необходимо:
  - создать пользователя ОС с именем, соответствующим имени созданного пользователя СУБД, путём выполнения в терминале с правами суперпользователя команды `useradd имя_пользователя_СУБД`.
  - назначить классификационную метку созданному пользователю ОС путём выполнения в терминале с правами суперпользователя команды `pdpl-user -l 0:0 имя_пользователя_СУБД`;
  - предоставить служебному пользователю `postgres` права на чтение файлов с классификационными метками выполнив в терминале с правами суперпользователя команду `setfacl -Rm u:postgres:rx /etc/parsec/macdb`.

4.5 Установка программы

В процессе установки осуществляется:

- создание системного пользователя и соответствующей группы, от имени которых функционирует eCA-VA;
- установка прав для создаваемого пользователя eCA-VA;
- установка контейнера сертификата веб-сервера eCA-VA;
- подготовка, установка параметров и служебных сервисов;
- запуск служебных сервисов;
- запись номера сборки eCA-VA в базу данных[2].

Ход установки программы отображён в виде горизонтальной шкалы с указанием процентов выполнения установки. В случае возникновения ошибки установка будет прекращена, сообщение об ошибке будет выведено в консоль пользователя.

Установка выполняется при помощи скрипта install.sh. Необходимые для работы переменные могут быть переданы при запуске скрипта (см. таблицу 8) или введены в диалоге.

Таблица 8 — Параметры запуска скрипта `/opt/aecaVa/scripts/install.sh`

Параметр	**Описание**
`--webp12 путь_к_контейнеру`	Параметр предназначен для передачи в скрипт пути к контейнеру закрытого ключа для веб-сервера
`-W путь_к_контейнеру`	То же, что `--webp12 путь_к_контейнеру`
`--dbuser имя_пользователя_СУБД`	См. описание параметра use_credentials_from_config в 4.2

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

[2] Значение номера сборки записывается в таблицу «build_info» схемы «aeca_ra_info».

Параметр	Описание
`-U имя_пользователя_СУБД`	То же, что `--dbuser имя_пользователя_СУБД`
`--dbpass пароль_пользователя_СУБД`	см. описание параметра use_credentials_from_config в 4.2
`-P пароль_пользователя_СУБД`	То же, что `--dbpass пароль_пользователя_СУБД`

Для установки программы:

1. Запустите скрипт[1] командой с правами суперпользователя:

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

2. При необходимости введите в диалоге путь к контейнеру закрытого ключа для веб-сервера, имя и пароль пользователя СУБД. В случае запуска от имени пользователя, не имеющего соответствующих привилегий, будет выведено сообщение, после которого работа инсталлятора завершится:

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

3. Если ранее eCA-VA уже был установлен будет предложено:
   - установить ПО;
   - обновить ПО;
   - завершить работу инсталлятора.

   Подтвердите выбор действия, вводом цифры «1».
4. Если в конфигурационном файле `/opt/aecaVa/scripts/config.sh` не определён используемый веб-сервер или введено неверное значение параметра `webserver`, то в процессе установки пользователю будет предложено выбрать используемый веб-сервер:
   - apache;
   - nginx;
   - cpnginx;

   Подтвердите выбор действия вводом цифры «1», «2» или «3».
5. Если в конфигурационном файле `/opt/aecaVa/scripts/config.sh` не определено расположение конфигурации выбранного веб-сервера (параметр `webserver_path`), то в процессе установки пользователю будет предложено ввести расположение конфигурации.
6. Введите полный путь до ранее подготовленного и скопированного на жёсткий диск файла контейнера сертификата PCS#12 веб-сервера.

После завершения установки создайте полную резервную копию (запустите `backup.sh` без параметров) eCA-VA (см. 10).

После первичной установки программного средства системному пользователю `aeca` будет назначена командная оболочка `/sbin/nologin`, которая запрещает интерактивный вход в ОС. При обновлении ПО командная оболочка не меняется. Чтобы сменить командную оболочку выполните с правами суперпользователя команду:

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

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

В Центре сертификатов доступа поддерживается совместная работа eCA-CA, eCA-RA и eCA-VA на одном сервере. Также поддерживается совместная работа eCA-RAи eCA-VA, а также eCA-VA и eCA-CA на одном сервере.

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

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

5 ПОДКЛЮЧЕНИЕ К ВЕБ-ИНТЕРФЕЙСУ

5.1 Общие сведения

Веб-интерфейс Центра валидации представляется собой графический интерфейс в виде совокупности динамических веб-страниц, отображаемых в веб-браузере. Веб-интерфейс реализован клиентским компонентом Центра валидации и предназначен для управления серверным компонентом Центра валидации.

Канал управления является защищённым — организован по протоколу HTTPS/TLS с аутентификацией и шифрованием передаваемых данных. Идентификация и аутентификация пользователей выполняется по предъявленному сертификату, который должен быть предварительно установлен в хранилище веб-браузера или хранилище сертификатов используемой ОС. Пример установки сертификата администратора из контейнера закрытого ключа PKCS#12 приведён в подразделе 5.2.

При использовании СКЗИ «КриптоПро CSP» канал взаимодействия клиентского и серверного компонента Центра валидации должен быть организован по протоколу TLS ГОСТ с использованием отечественных криптографических алгоритмов. Для этого на компьютере, предназначенном для подключения к веб-интерфейсу, должны быть выполнены следующие действия:

- Установлен криптопровайдер СКЗИ «КриптоПро CSP» в соответствии с инструкцией, описанной в разделе 2 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.
- Установлена клиентская лицензия СКЗИ «КриптоПро CSP», дающая право использовать двустороннюю аутентификацию по протоколу TLS. Порядок установки лицензии описан в разделе 4 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.
- Сертификат учётной записи администратора для взаимодействия с Центром сертификации из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, должен быть установлен в личное хранилище пользователя с помощью утилиты `cptools` из состава СКЗИ «КриптоПро CSP». Порядок установки сертификата из контейнера закрытого ключа приведён в подразделе 2.6.5 документа «СКЗИ «КриптоПро CSP». Инструкция по использованию графического приложения Инструменты КриптоПро (cptools)» ЖТЯИ.00101-03 92 06.
- Установлен веб-браузер Chromium с поддержкой TLS ГОСТ из состава ОС. Данный веб-браузер входит в состав базовых репозиториев ОС Astra Linux SE, Альт Сервер, РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.

5.2 Установка сертификата администратора

Для первичной настройки программного комплекса необходимо установить сертификат учётной записи администратора Центра сертификации, к которому подключён Центр валидации, в доверенное хранилище сертификатов веб-браузера[1].

Процесс установки сертификата рассмотрим на примере браузера Firefox:

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

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

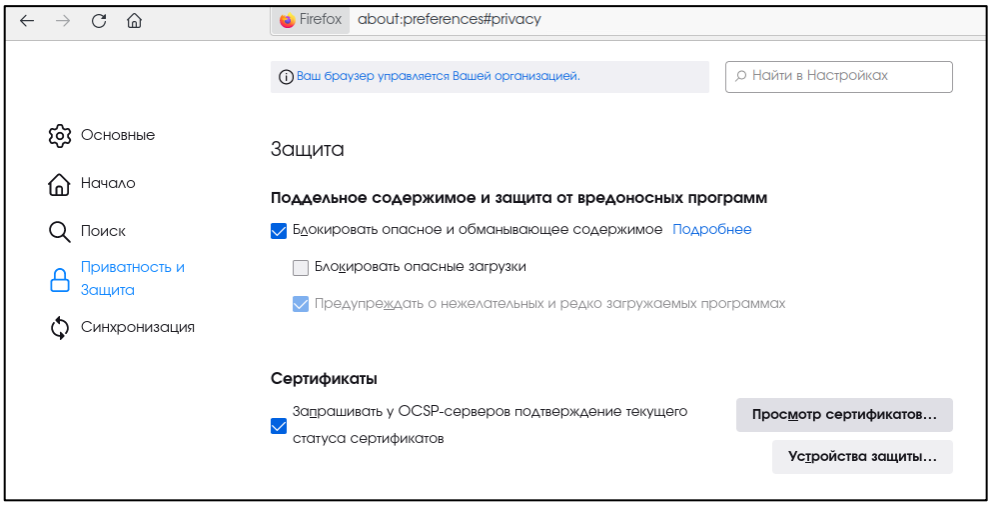


Рисунок 1 - Окно настроек браузера

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

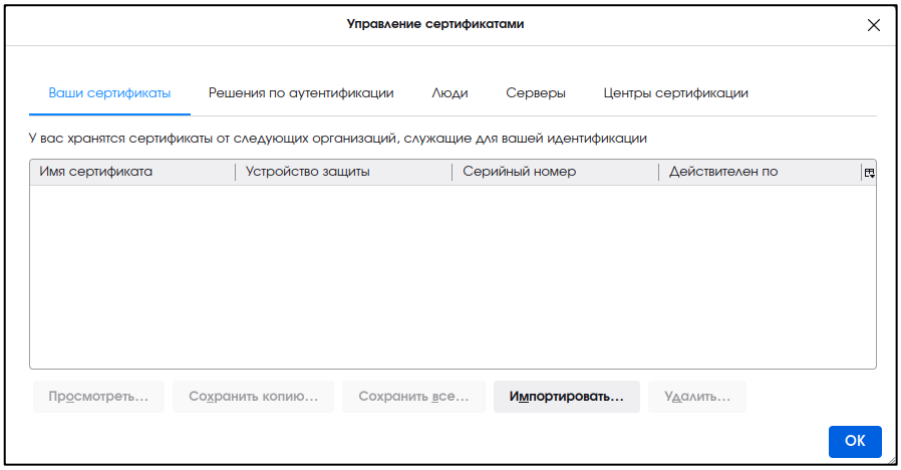


Рисунок 2 - Окно управления сертификатами

- Выберите предварительно подготовленный файл сертификата, подписанный Центром сертификации. Нажмите кнопку <Открыть> (см. рисунок 3).

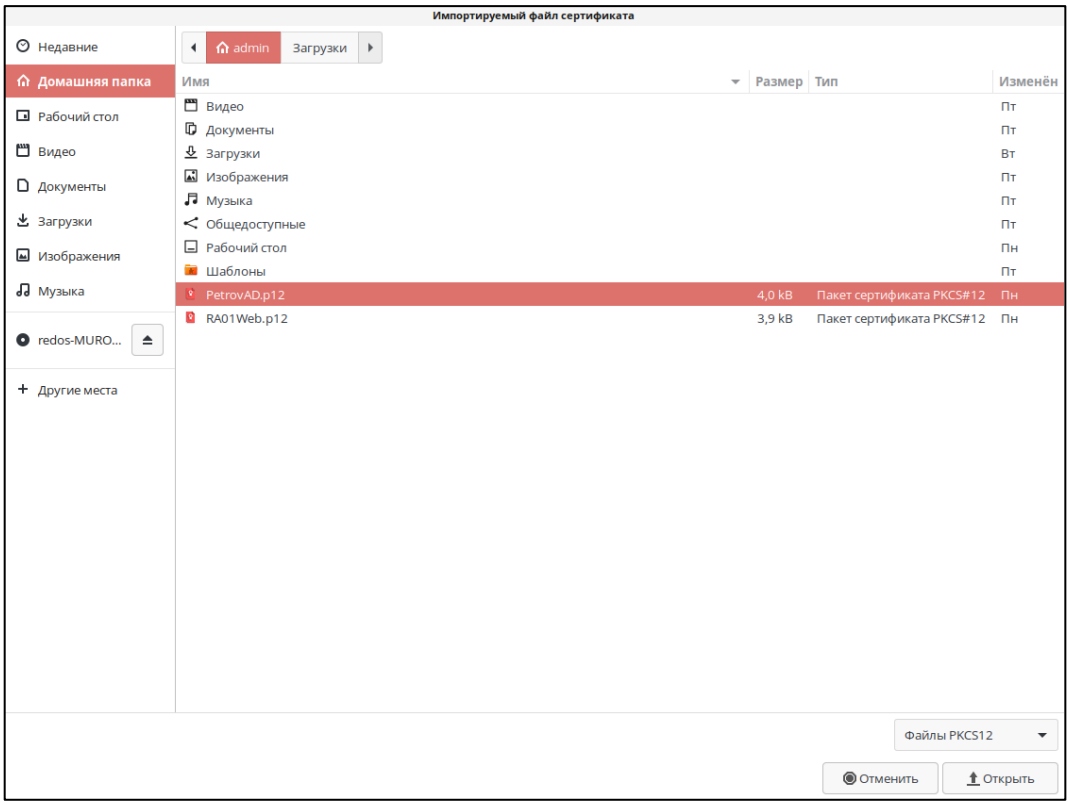


Рисунок 3 - Окно выбора импортируемого файла сертификата

- Введите пароль сертификата доступа в открывшемся окне и нажмите кнопку <OK> (см. рисунок 4).

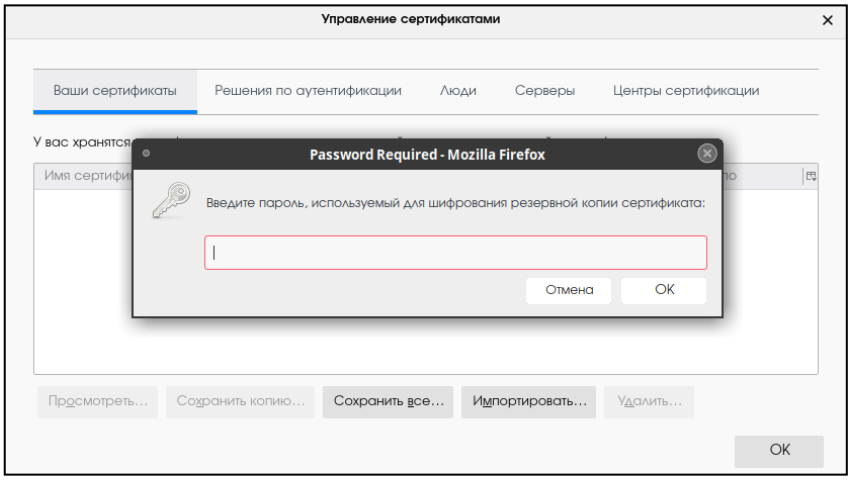


Рисунок 4 - Окно ввода PIN-кода сертификата

PIN-код сертификата устанавливается администратором Центра сертификации при выпуске сертификата доступа.

- В таблице окна «Управление сертификатами» появится запись об импортированном сертификате (см. рисунок 5). Нажать кнопку <OK>.

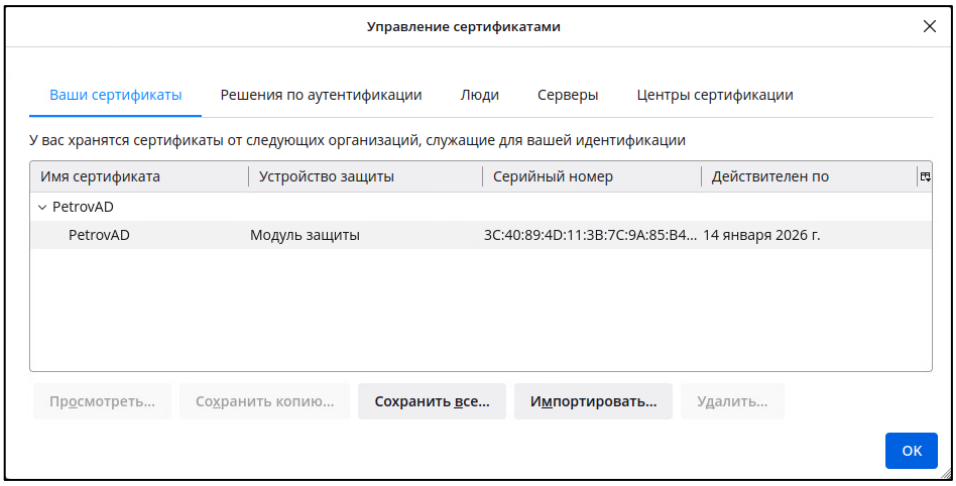


Рисунок 5 - Окно «Управление сертификатами»

5.2.1 Подключение к веб-интерфейсу

Порядок подключения к веб-интерфейсу:

- Запустите веб-браузер и в адресной строке введите IP-адрес или доменное имя компьютера, на котором установлен Центр валидации (например, `https://172.22.5.21`).
- В открывшемся окне выберите импортированный сертификат для аутентификации (см. рисунок 6). Нажмите кнопку <ОК>.

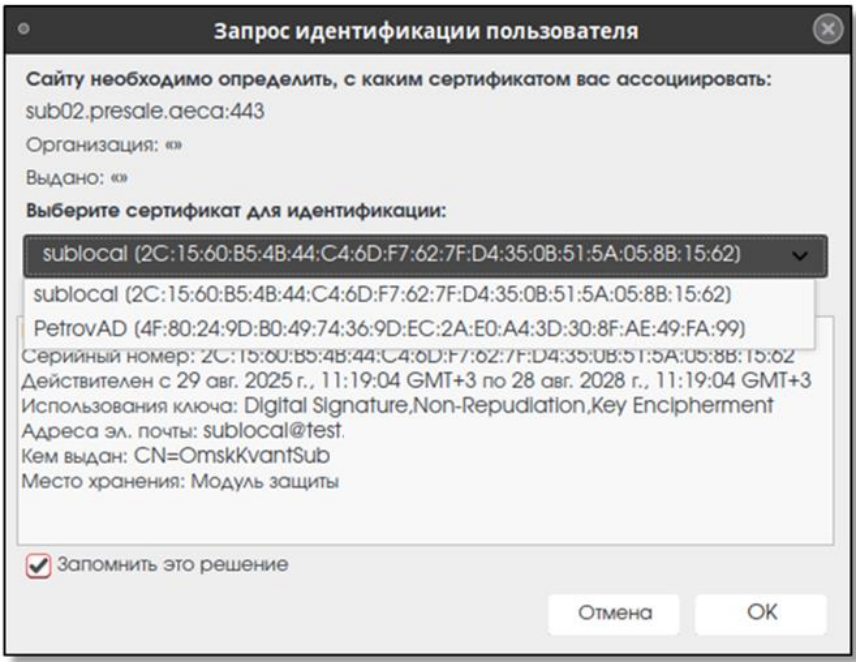


Рисунок 6 - Окно выбора сертификата

5.2.2 Доступ к программе

eCA-VA предоставляет возможность аутентификации в нем:

- администраторам подключённых eCA-CA [1];
- администратору инициализации eCA-VA.

[1] Управление подключениями к eCA-CA осуществляется администратором инициализации в разделе «Настройки».

> **Внимание! После успешной чистой установки программы создается пользователь с ролью «Администратор инициализации». Логин администратора инициализации имеет значение «INITIAL_ADMIN». Пароль администратора инициализации находится в файле «/opt/aecaVa/dist/sign-in/initial_admin.txt».**
>
> **Первое подключение необходимо сделать локально (с сервера Центра валидации), авторизоваться администратором инициализации и создать подключение к ЦС (см. 7.3.8).**

eCA-VA позволяет администраторам подключённых eCA-CA аутентифицироваться в нем по сертификатам.

Для учётных записей администраторов eCA-CA, созданных на основе субъектов ресурсных систем, к которому подключён eCA-VA и данный eCA-CA аутентификация возможна по доменным имени и паролю или по Kerberos-билету. В этом случает, если используется cpnginx, то подключение к веб-интерфейсу eCA-VA должно осуществляться по имени хоста из параметра hostname_no_mtls конфигурационного файла.

eCA-VA позволяет администратору инициализации аутентифицироваться в нем по логину и паролю[1].

При обращении к пользовательскому интерфейсу eCA-VA неаутентифицированному пользователю предлагается необязательный выбор сертификата для установки двустороннего TLS-соединения. При этом выбранный пользователем сертификат в дальнейшем автоматически используется для аутентификации в eCA-VA в случае, если пользователем будет выбрана аутентификация по сертификату. В случае, если пользователем не был выбран сертификат, с веб-сервером eCA-VA устанавливается одностороннее TLS-соединение.

В пользовательском интерфейсе eCA-VA при попытке доступа неаутентифицированного пользователя после установки TLS-соединения отображается окно авторизации.

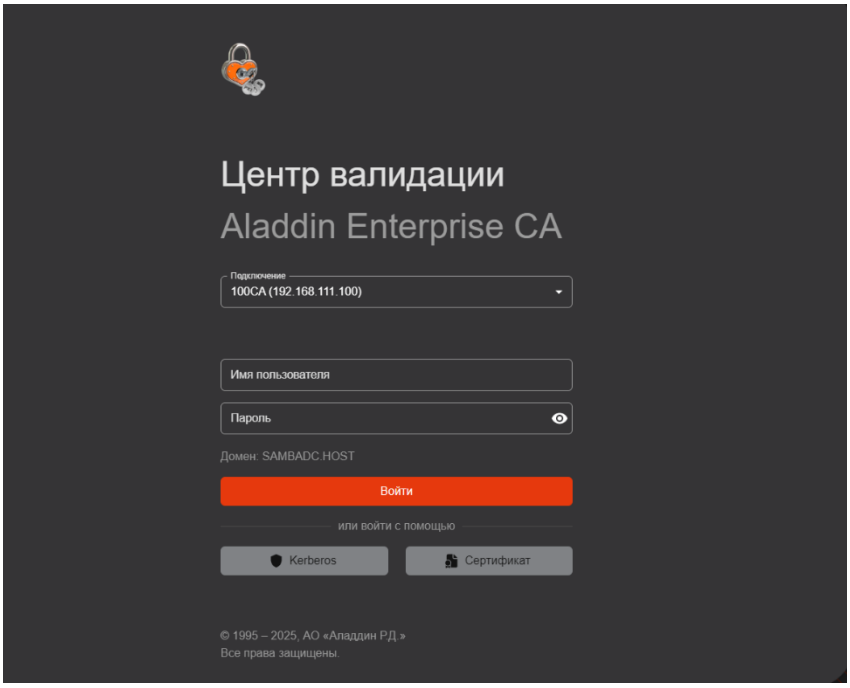


Рисунок 7 — Окно авторизации

В окне авторизации eCA-VA присутствуют:

- поле выбора подключения «Подключение». В данном поле отображаются все подключения к eCA-CA, а также вариант выбора «Локальное». Подключения к eCA-CA отображаются в списке в формате «Отображаемое имя подключения (адрес хоста подключения)», например, «Тестовое подключение (192.168.111.100)».
- поля ввода реквизитов пользователя («Имя пользователя» и «Пароль»).
- текстовый блок, содержащий имя домена, к которому подключён eCA-VA;

[1] Учётная запись администратора инициализации Центра валидации Aladdin eVA создаётся при чистой установке Центра валидации Aladdin eVA.

- кнопка «Войти» для выполнения аутентификации по введённым пользователем реквизитам.
- кнопка «Сертификат» для выполнения аутентификации пользователя по ранее выбранному для установки двустороннего TLS-соединения сертификату. Данная кнопка заблокирована, если выбрано «Локальное» подключение;
- кнопка «Kerberos» для выполнения аутентификации пользователя по Kerberos-билету. Данная кнопка заблокирована, если выбрано «Локальное» подключение.
- Для аутентификации по имени и паролю администратора инициализации в окне авторизации eCA-VA:
- Выберите «Локальное» в поле «Подключение».
- Выберите INITIAL_ADMIN «Имя пользователя».
- Введите пароль в поле «Пароль».
- Нажмите кнопку «Войти».
- В случае использования СКЗИ «КриптоПро CSP» введите пароль контейнера Crypto-Pro (см. рисунок 8).

Рисунок 8 — Окно ввода пароля контейнера Crypto-Pro

Для аутентификации по сертификату в окне авторизации eCA-VA:

- В поле «Подключение» выберите Центр сертификации, в котором был выпущен ранее выбранный для установки двустороннего TLS-соединения сертификат.
- Нажмите кнопку «Сертификат».
- При необходимости введите пароль контейнера Crypto-Pro (см. рисунок 8).

Для аутентификации по доменным имени и паролю в окне авторизации eCA-VA:

- Выберите подключение к eCA-CA в поле «Подключение».
- Введите доменное имя пользователя в поле «Имя пользователя».
- Введите доменный пароль в поле «Пароль».
- Нажмите кнопку «Войти».

Для аутентификации по Kerberos-билету[1] в окне авторизации eCA-VA:

- Выберите подключение к eCA-CA в поле «Подключение».
- Нажмите кнопку Kerberos.

- Далее на открывшейся странице с предупреждением системы безопасности (см. рисунок 9) нажмите кнопку <Дополнительно>, примите риск и продолжите подключение.

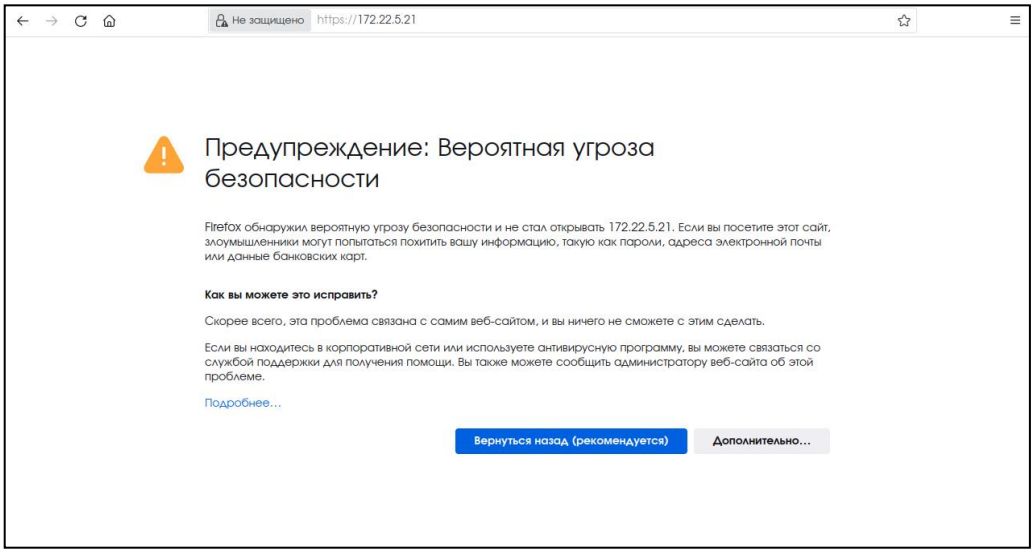


Рисунок 9 - Страница с предупреждением системы безопасности

- В результате вы подключитесь к веб-интерфейсу Центра валидации, где необходимо пройти аутентификацию.

5.3 Переопределение сведений, отображаемых в окне авторизации и в заголовке вкладки браузера

Для переопределения сведений, отображаемых в окне авторизации и в заголовке вкладки браузера (см. рисунок 10):

1. В конфигурационном файле `/opt/aecaVa/scripts/config.sh` задайте необходимые значения параметрам:
   - `login_window_product_name` (для переопределения названия продукта, отображаемого в окне авторизации);
   - `login_window_component_name` (для переопределения названия компонента, отображаемого в окне авторизации);
   - `tab_title` (для переопределения текста, отображаемого в заголовке вкладок браузера).
2. Для применения внесённых настроек запустите сценарий обновления при помощи команды с правами суперпользователя:

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

3. При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.
4. Установщик предложит выбрать необходимое действие в интерактивном режиме.
5. Введите в терминале цифру «2».
6. Дождитесь окончания выполнения сценария обновления.

[1] Для аутентификации по Kerberos-билету предварительно необходимо создать службу HTTP и получить keytab-файл (см. 3.5). На клиенте должен быть настроен браузер для работы с Kerberos. Инструкция по настройке Kerberos-аутентификации в браузерах приведена в приложении 5.

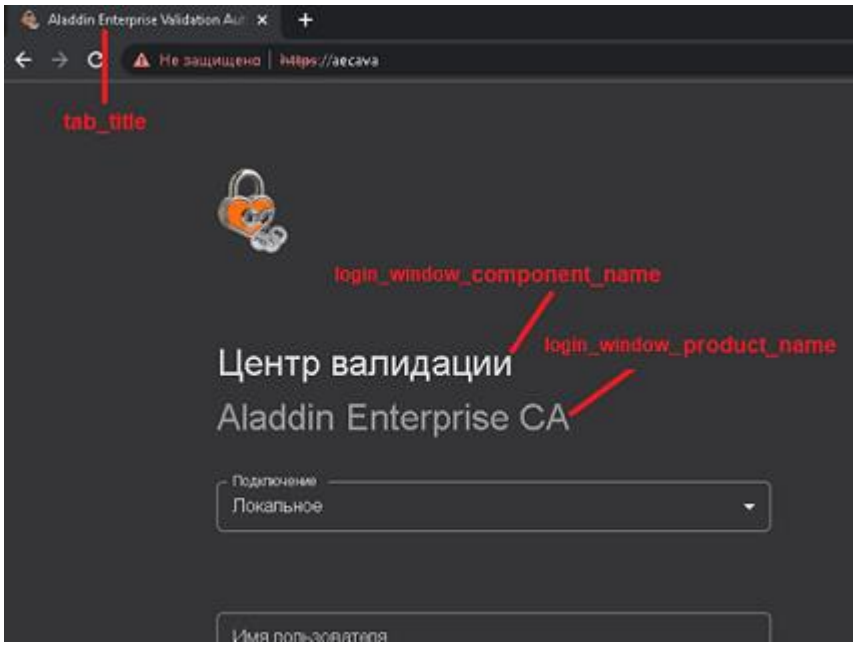


Рисунок 10 — Сведения, отображаемые в окне авторизации и в заголовке вкладки браузера

6 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

eCA-VA запускается автоматически с запуском операционной системы.

Для проверки состояния eCA-VA в терминале:

- выполните команду с правами суперпользователя:

```
systemctl status aeca-va.service
```

- ознакомьтесь с ответом.

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

Для запуска eCA-VA в терминале выполните команду с правами суперпользователя:

```
systemctl start aeca-va.service
```

Для завершения работы eCA-VA в терминале выполните команду с правами суперпользователя:

```
systemctl stop aeca-va.service
```

7 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

7.1 Главное окно eCA-VA

В главном окне eCA-VA присутствуют:

- шапка программы;
- в левой части экрана, под шапкой, следующие разделы:

– «Центры валидации»;
– «Журнал событий»;
– «Настройки».

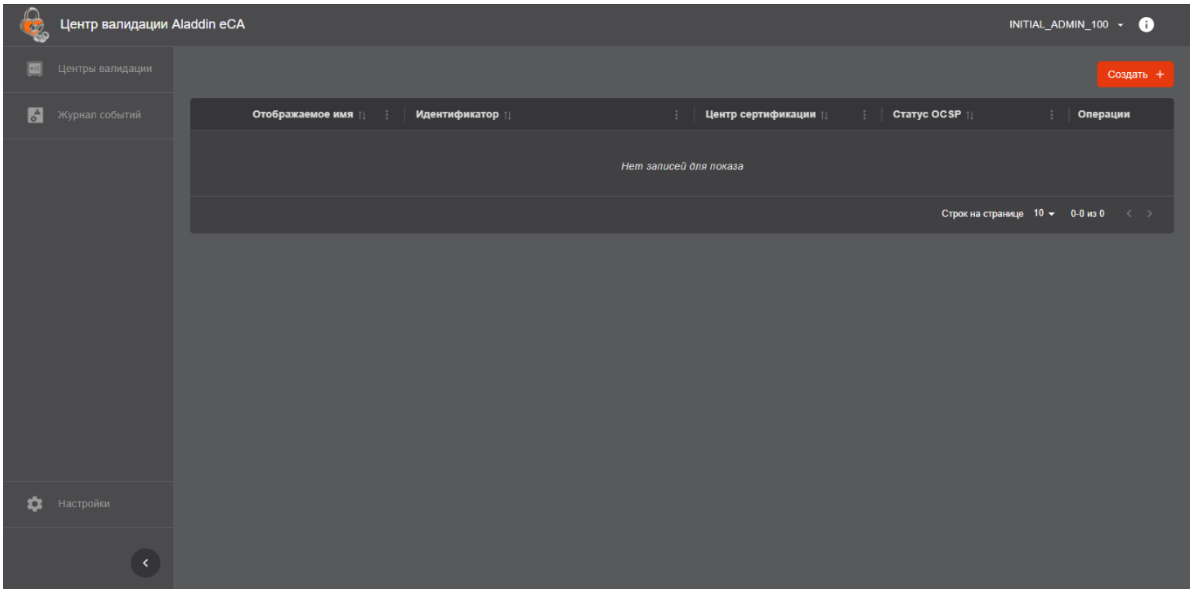


Рисунок 11 — Главное окно eCA-VA

В шапке программы отображается имя текущей учётной записи.

При нажатии на отображаемое имя текущей учётной записи в шапке главного окна появляется всплывающее меню, содержащее кнопку «Выйти», при нажатии на которую происходит завершение сессии пользователя в eCA-VA.

В окне «О программе» должны присутствуют следующие сведения:

- название программы и её версия;
- информация о разработчике программы.

7.2 Раздел «Центры валидации»

Внимание! Данный раздел доступен только пользователю с ролью «Администратор».

В разделе «Центры валидации» главного окна Центра валидации присутствуют (см. рисунок 12):

- Кнопка «Создать» для создания нового Центра валидации.
- Список существующих в программе Центров валидации. Для администратора подключённого eCA-CA в списке присутствуют только Центры валидации, обслуживающие Центры сертификации его экземпляра eCA-CA.
- Для каждого Центра валидации в списке присутствуют следующие поля:

– «Обслуживаемый центр сертификации», содержащее отображаемое имя Центра сертификации, который обслуживается данным Центром валидации. Значение в данном поле является гиперссылкой на карточку данного Центра сертификации в eCA-CA;

- «Статус CRL», содержащее текущий статус CRL, опубликованного в данный Центр валидации. Возможные значения в поле: «Действует до DD.MM.YYYY hh:mm:ss», где «DD.MM.YYYY hh:mm:ss» - дата и время окончания действия CRL (цвет текста - зелёный), «Истек срок действия» (цвет текста - красный), «Не публиковался» (цвет текста - белый);
- «Статус Delta CRL», содержащее текущий статус Detla CRL, опубликованного в данный Центр валидации. Возможные значения в поле: «Действует до DD.MM.YYYY hh:mm:ss», где «DD.MM.YYYY hh:mm:ss» - дата и время окончания действия Delta CRL (цвет текста - зелёный), «Истек срок действия» (цвет текста - красный), «Не публиковался» (цвет текста - белый);
- «Статус OCSP», содержащее текущее состояние службы OCSP. Возможные значения в поле: «Активна» (цвет текста - зелёный), «Истек сертификат» (цвет текста - красный), «Истек CRL» (цвет текста - красный), «Сертификат отсутствует» (цвет текста - красный), «Остановлена» (цвет текста - оранжевый), «Не создана» (цвет текста - белый).
- «Операции», содержащее элемент (три горизонтальных точки) для вызова контекстного меню операций с Центром валидации. В меню присутствуют следующие операции:
    - Копировать URL распространения CRL;
    - Копировать URL распространения Delta CRL. Данная кнопка отсутствует, если в Центр валидации не осуществлялась публикация Delta CRL;
    - Копировать URL распространения AIA;
    - Копировать URL службы OCSP. Данная кнопка отсутствует, если для Центра валидации не создана служба OCSP (статус службы - «Не создана»);
    - Запустить/остановить работу службы OCSP. Запуск доступен только для Центра валидации с состоянием службы OCSP «Активна»; остановка доступна только для Центра валидации с состоянием службы OCSP «Остановлена»;
    - Удалить.

- кнопки управления отображением колонок в виде трёх вертикальных точек в каждой колонке, позволяющие:

- сбросить размер колонок, если он был изменён ранее;
- скрыть выбранную колонку;
- показать все колонки, если какие-либо колонки были скрыты ранее.

- Элементы управления пагинацией списка Центров валидации. По умолчанию установлено отображение 50 элементов списка.

Слева от отображаемого имени Центра валидации присутствует индикация ошибки (пиктограмма «Треугольник с восклицательным знаком»), если подключение данного Центра валидации к eCA-CA было отключено (например, если данный Центр валидации удалён в eCA-CA). При наведении курсора на данную индикацию отображаться всплывающее сообщение «Отсутствует подключение к обслуживаемому центру сертификации».

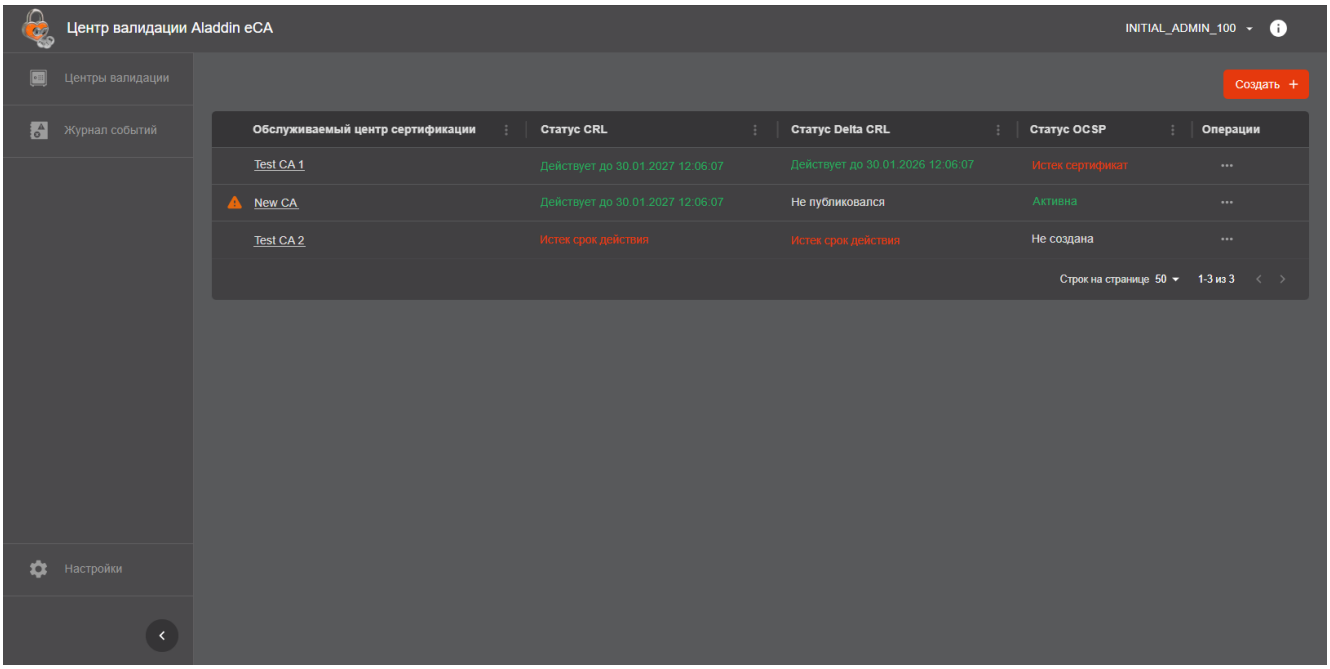


Рисунок 12 - Окно раздела «Центры валидации» eCA-VA

7.2.1 Карточка Центра валидации

Для перехода к карточке Центра валидации необходимо щёлкнуть левой кнопкой мыши на строке с записью Центра валидации в разделе «Центы валидации» (см. 7.1).

В карточке Центра валидации (см. рисунок 13) отображаются:

- кнопка «Переподключиться», для повторной регистрации данного Центра валидации в eCA-CA. Данная кнопка присутствует только для Центра валидации, у которого отсутствует подключение к обслуживаемому ЦС eCA-CA;
- кнопка «Удалить» для удаления Центра валидации;
- блок с общей информацией о Центре валидации, содержащий поля:

– «Идентификатор центра валидации»;
– «Обслуживаемый центр сертификации». В данном поле указано отображаемое имя обслуживаемого ЦС eCA-CA. Значение в данном поле является гиперссылкой на карточку данного ЦС в eCA-CA. Справа от значения в данном поле в случае потери подключения Центра валидации к ЦС eCA-CA отображается пиктограмма «Треугольник с восклицательным знаком», при наведении курсора на которую отображается всплывающее сообщение «Отсутствует подключение к обслуживаемому центру сертификации»;

- вкладки:

– CRL DP;
– AIA;
– OCSP.

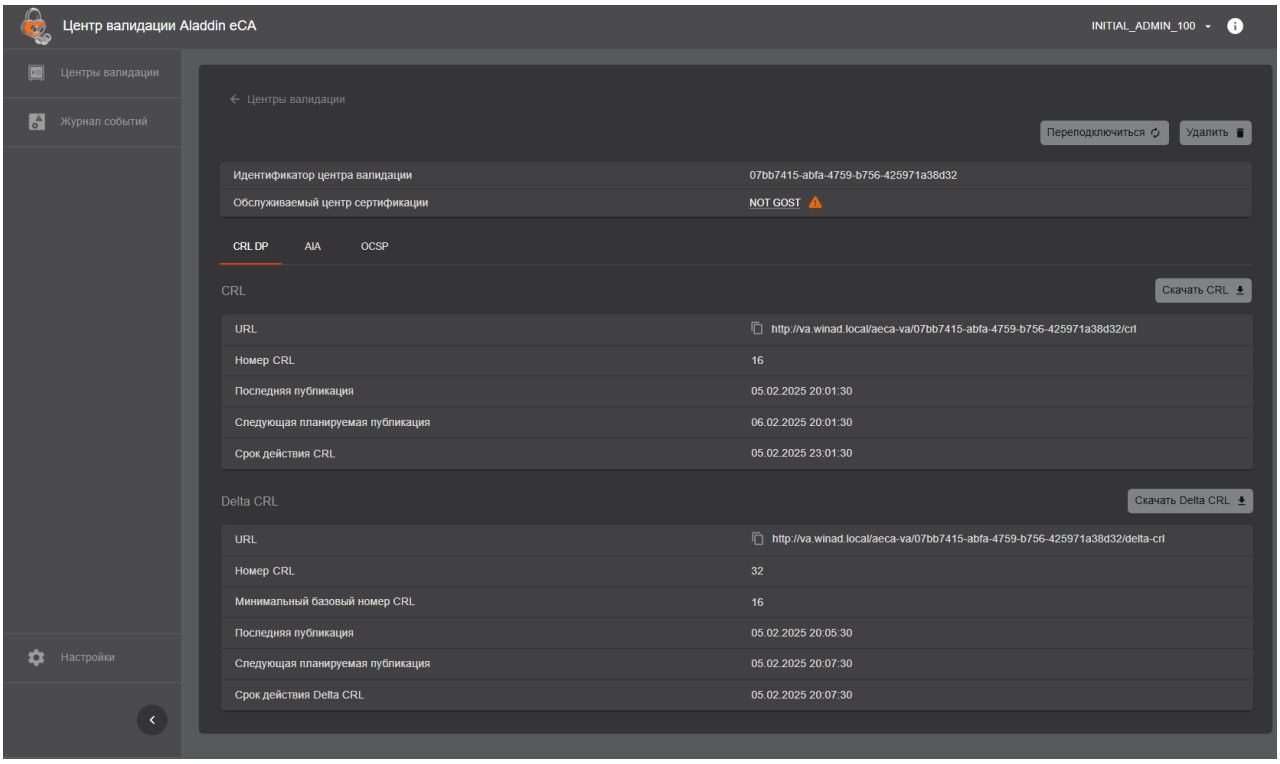


Рисунок 13 - Окно карточки Центра валидации

7.2.1.1 Вкладка «CRL DP»

На вкладке «CRL DP» присутствуют:

- Подраздел «CRL». В данном подразделе присутствует:
  - кнопка «Скачать CRL» для экспорта последнего CRL, опубликованного в CRL DP данного Центра валидации;
  - блок, содержащий следующие информационные поля:
    - «URL», содержащее URL точки распространения CRL данного Центра валидации. При нажатии на данное поле URL копируется в буфер обмена пользователя;
    - «Номер CRL», содержащее номер публикации последнего CRL, опубликованного в CRL DP данного Центра валидации;
    - «Последняя публикация», содержащее дату и время последней публикации CRL на данный Центр валидации;
    - «Следующая планируемая публикация», содержащее дату и время следующей планируемой публикации CRL на данный Центр валидации;
    - «Срок действия CRL», содержащее дату и время окончания действия последнего CRL, опубликованного в CRL DP данного Центра валидации. При истечении срока действия CRL цвет значения поля будет красным. Если до истечения срока действия CRL остается менее суток, то цвет значения поля будет оранжевым.
- Подраздел «Delta CRL». Данный подраздел присутствует только при публикации на данный Центр валидации Delta CRL. В данном подразделе присутствует:
  - кнопка «Скачать Delta CRL» для экспорта последнего Delta CRL, опубликованного в CRL DP данного Центра валидации;
  - блок, содержащий следующие информационные поля:
    - «URL», содержащее URL точки распространения Delta CRL данного Центра валидации. При нажатии на данное поле URL копируется в буфер обмена пользователя;
    - «Номер CRL», содержащее номер публикации последнего Delta CRL, опубликованного в CRL DP данного Центра валидации;
    - «Минимальный базовый номер CRL», содержащее номер базового CRL;
    - «Последняя публикация», содержащее дату и время последней публикации Delta CRL на данный Центр валидации;

- «Следующая планируемая публикация», содержащее дату и время следующей планируемой публикации Delta CRL на данный Центр валидации;
- «Срок действия Delta CRL», содержащее дату и время окончания действия последнего Delta CRL, опубликованного в CRL DP данного Центра валидации. При истечении срока действия Delta CRL цвет значения поля будет красным. Если до истечения срока действия Delta CRL остаётся менее суток, то цвет значения поля будет оранжевым.

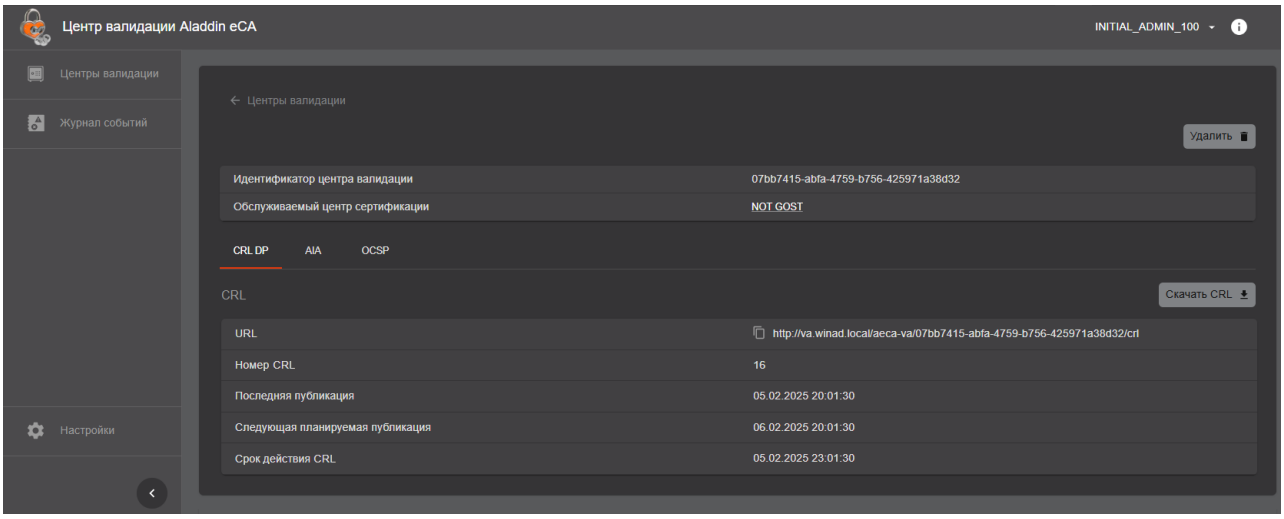


Рисунок 14 - Карточка Центра валидации. Вкладка «CRL DP». Delta CRL не публикуется в данный ЦВ

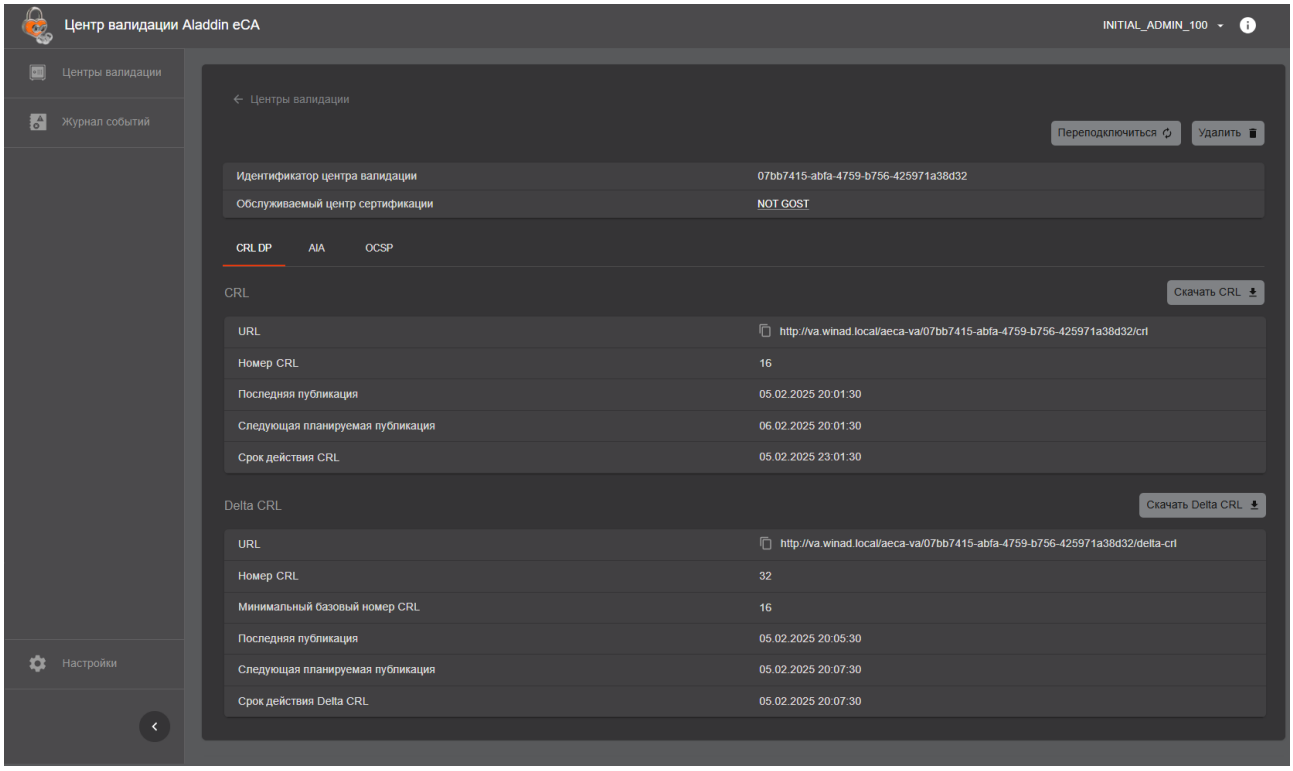


Рисунок 15 - Карточка Центра валидации. Вкладка «CRL DP». Delta CRL публикуется в данный ЦВ.

7.2.1.2 Вкладка «AIA»

На вкладке «AIA» присутствуют:

- Кнопка «Скачать сертификат» для экспорта сертификата ЦС, обслуживаемого данным Центром валидации:
- Блок, содержащий следующие информационные поля:

– «URL», содержащее URL точки распространения AIA данного Центра валидации. При нажатии на данное поле URL копируется в буфер обмена пользователя;

- «Владелец», содержащее Common Name из сертификата ЦС, обслуживаемого данным Центром валидации;
- «SDN владельца», содержащее SDN из сертификата ЦС, обслуживаемого данным Центром валидации;
- «Срок действия сертификата», содержащее дату и время окончания действия сертификата ЦС, обслуживаемого данным Центром валидации. При истечении срока действия сертификата цвет значения поля будет красным. Если до истечения срока действия сертификата остаётся менее месяца, то цвет значения поля будет оранжевый.
- «Алгоритм ключа», содержащее алгоритм ключа ЦС, обслуживаемого данным Центром валидации;
- «Длина ключа», содержащее длину ключа ЦС, обслуживаемого данным Центром валидации.

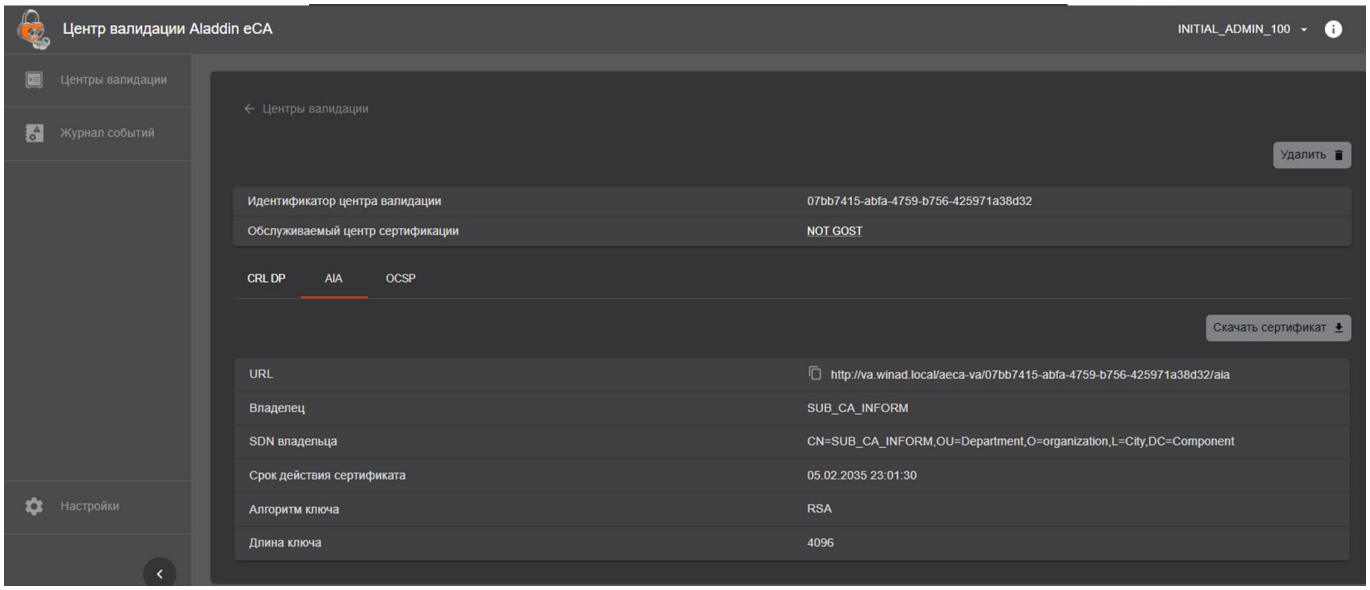


Рисунок 16 - Карточка Центра валидации. Вкладка «AIA»

7.2.1.3 Вкладка «OCSP»

На вкладке «OCSP» при отсутствии созданной для данного Центра валидации службы OCSP отображается кнопка «Создать службу OCSP» (см. рисунок 17) для запуска сценария создания службы OCSP (см. «Создание службы OCSP созданного »). При этом кнопка недоступна для нажатия, если у данного Центра валидации отсутствует подключение к обслуживаемому Центру сертификации (см. рисунок 18).

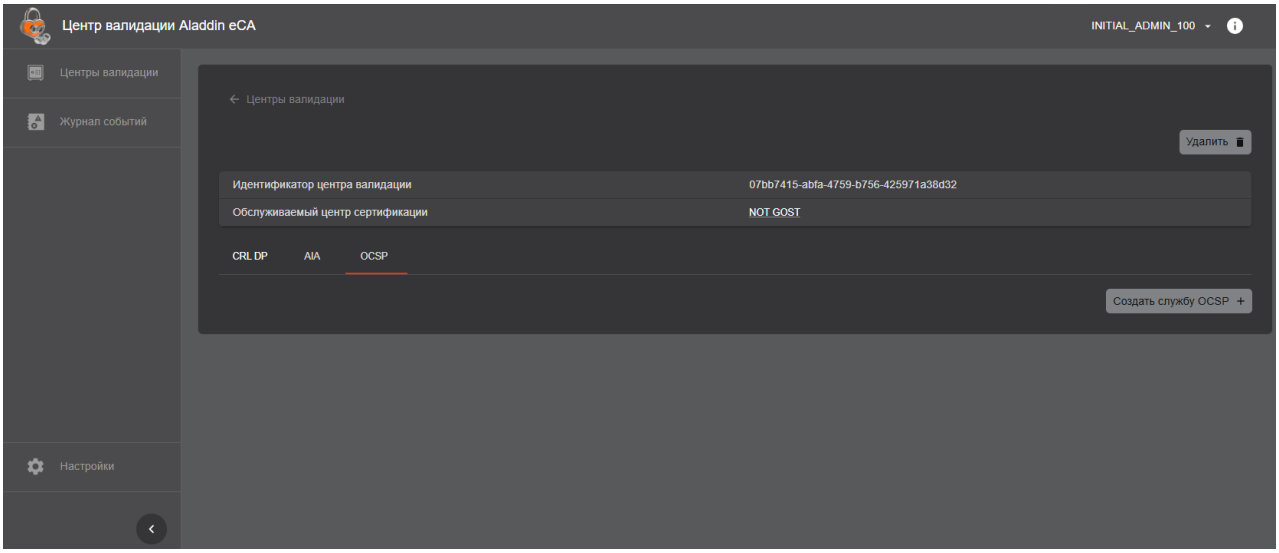


Рисунок 17 - Карточка Центра валидации, вкладка «OCSP» при отсутствии у Центра валидации созданной службы OCSP

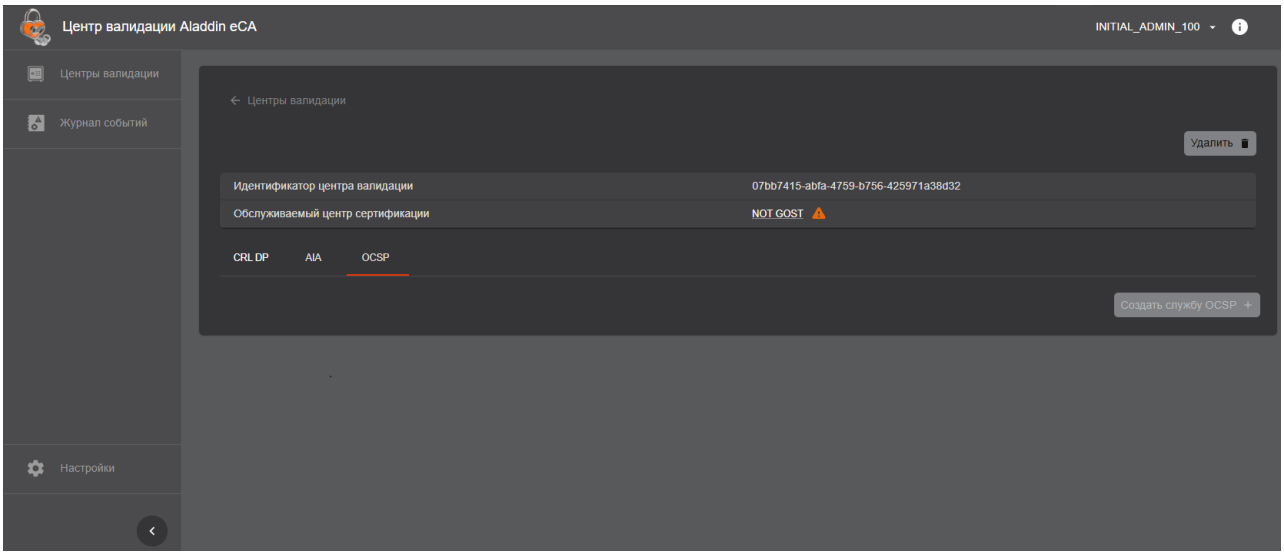


Рисунок 18 - Карточка Центра валидации, вкладка «OCSP» при отсутствии у Центра валидации созданной службы OCSP и при отсутствии подключения к обслуживаемому Центру сертификации

На вкладке «OCSP» при наличии созданной для данного Центра валидации службы OCSP (см. рисунок 19) отображаются:

- Подраздел «Параметры службы», включающий:
  - кнопку «Остановить» («Запустить»). Для запуска/остановки работы службы OCSP. Кнопка присутствует только для Центра валидации с состоянием службы OCSP «Активна» или «Остановлена»;
  - кнопку «Настроить» для настройки параметров службы OCSP (см. «Настройка параметров службы OCSP»);
  - кнопку «Удалить» для удаления службы OCSP у Центра валидации (см. «Удаление службы OCSP из Центра валидации»);
  - блок, содержащий следующие информационные поля:
    - «URL», содержащее URL службы OCSP данного Центра валидации. При нажатии на данное поле URL копируются в буфер обмена пользователя;
    - «Статус», содержащее службы OCSP данного Центра валидации. Возможные значение в поле: «Активна» (цвет текста - зелёный), «Истек сертификат» (цвет текста - красный), «Истек CRL» (цвет текста - красный), «Остановлена» (цвет текста - оранжевый);
    - «Алгоритм хэш-суммы ответа», содержащее название алгоритма вычисления хэш-функции ответа данного Центра валидации;
    - «Обновлять сертификат службы автоматически», содержащее флаг состояния опции автоматического обновления сертификата службы OCSP. Если данная опция включена, в данном поле должна отображаться пиктограмма «Галочка», иначе - прочерк;
    - «Статус неизвестных сертификатов GOOD», содержащее флаг состояния опции ответа «GOOD» по статусу неизвестных сертификатов для службы OCSP. Если данная опция включена, в данном поле отображается пиктограмма «Галочка», иначе - прочерк;
    - «Включать цепочку сертификатов в ответ», содержащее флаг состояния опции включения цепочки сертификатов в ответ службы OCSP. Если данная опция включена, в данном поле отображается пиктограмма «Галочка», иначе - прочерк;
    - «Включать сертификат подписи в ответ», содержащее флаг состояния опции включения сертификата подписи в ответ службы OCSP. Если данная опция включена, в данном поле отображается пиктограмма «Галочка», иначе - прочерк.
- Подраздел «Сертификат службы», включающий:
  - кнопку «Обновить» для ручного обновления сертификата службы OCSP (см. «Ручное обновление сертификата службы OCSP»);

- блок, содержащий следующие информационные поля:
  - «Идентификатор», содержащее идентификатор сертификата службы OCSP. Значение в данном поле является гиперссылкой на карточку данного сертификата в подключённом eCA-CA;
  - «Шаблон», содержащее шаблона сертификата службы OCSP. Значение в данном поле является гиперссылкой на карточку данного шаблона в подключённом eCA-CA;
  - «Владелец», содержащее Common Name из сертификата службы OCSP, обслуживаемого данным Центром валидации;
  - «Издатель», содержащее отображаемое имя ЦС, издавшего данный сертификат. Значение в данном поле является гиперссылкой на карточку данного ЦС в подключённом eCA-CA;
  - «Срок действия», содержащее окончания действия сертификата службы OCSP данного Центра валидации. При истечении срока действия сертификата цвет значения поля будет красным. Если до истечения срока действия сертификата остаётся менее месяца, то цвет значения поля будет оранжевым;
  - «Алгоритм ключа», содержащее алгоритм ключа службы OCSP данного Центра валидации;
  - «Длина ключа», содержащее длину ключа службы OCSP данного Центра валидации.

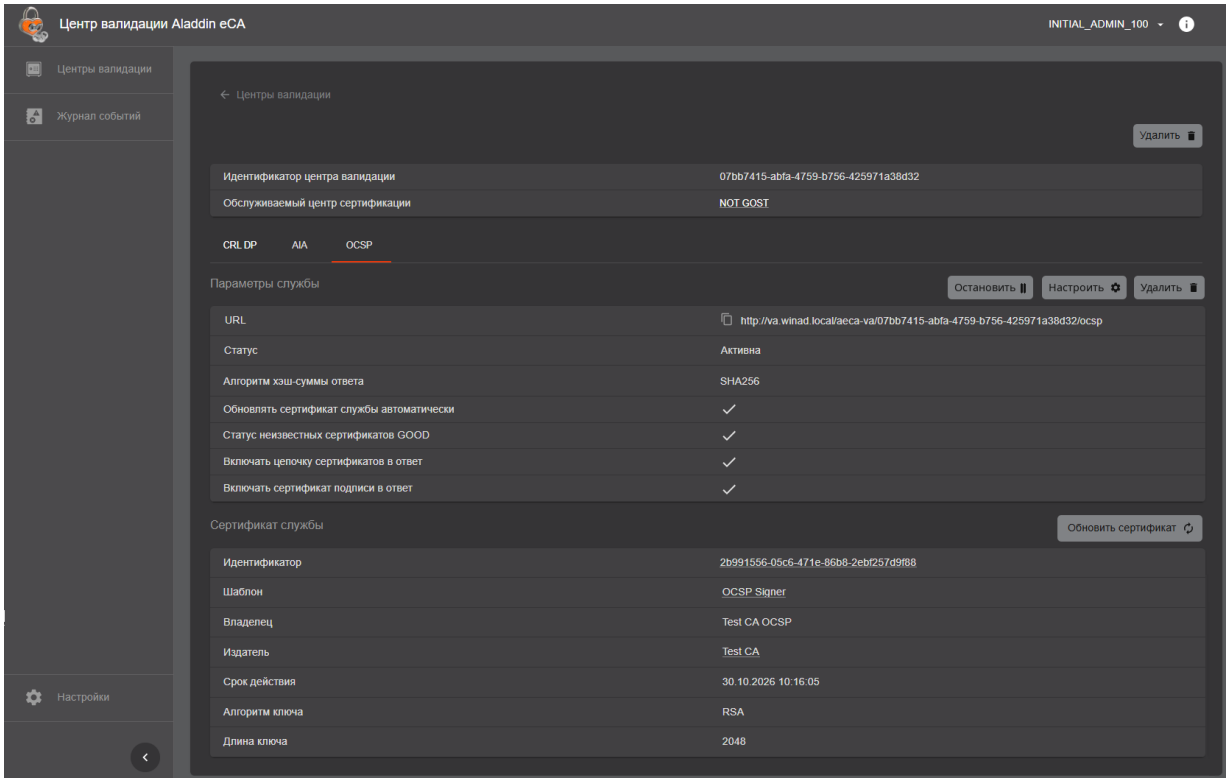


Рисунок 19 - Карточка Центра валидации, вкладка «OCSP», служба OCSP создана

7.2.2 Создание Центра валидации

Для создания Центра валидации необходимо:

- Перейти в раздел «Центры валидации».
- Нажать на кнопку «Создать».
- В открывшемся окне «Создание центра валидации» необходимо:

- выбрать из списка Центр сертификации подключённого eCA-CA;
- определиться с необходимостью автоматического создания службы OCSP для данного ЦВ в результате его создания путём управления чек-боксом «Создать службу OCSP». По умолчанию данный чекбокс включён.

- в зависимости от состояния чек-бокса «Создать службу OCSP» кнопка перехода на следующий шаге будет иметь значение «Продолжить» (если чек-бокс включён) или «Создать» (если чек-бокс выключен). При нажатии на кнопку «Создать» сценарий создания центра валидации будет завершаться.

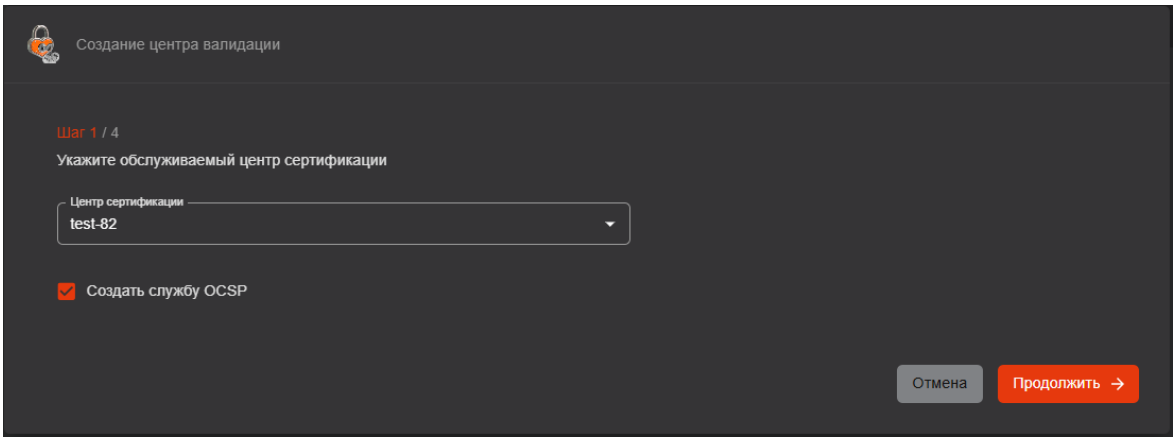


Рисунок 20 — Окно «Создание центра валидации» с включённым чек-боксом «Создать службу OCSP»

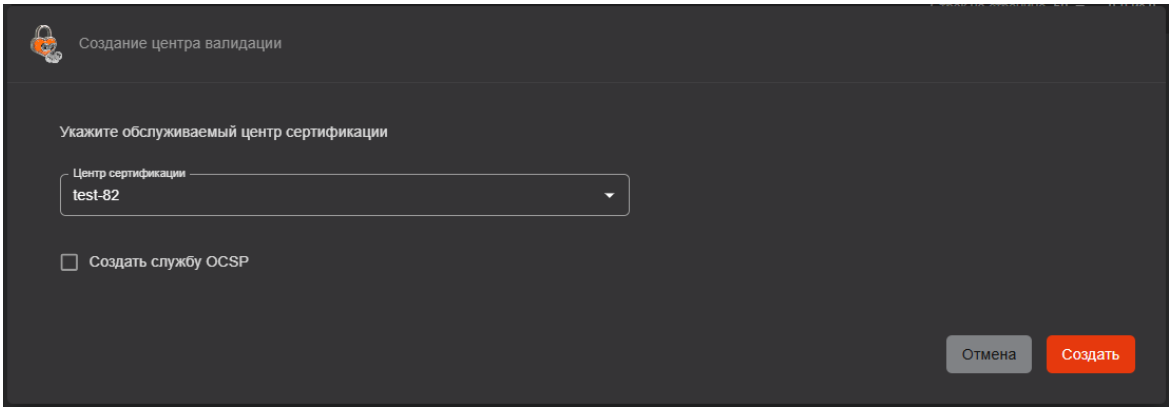


Рисунок 21 — Окно «Создание центра валидации» с выключенным чек-боксом «Создать службу OCSP»

- Если была нажата кнопка «Продолжить», на следующем шаге окна «Создание центра валидации» необходимо сделать (см. рисунок 22):

- выбор криптопровайдера службы OCSP.

  При наличии активного криптопровайдера «КриптоПро CSP» на хосте eCA-VA в поле будет доступно указание значения «КриптоПро CSP».

  По умолчанию указано значение «Стандартный»;

- выбор места хранения закрытого ключа службы OCSP.

  Значение в данном поле зависит от выбранного криптопровайдера службы OCSP.

  Если выбран стандартный криптопровайдер, для места хранения будет указано неизменяемое значение «Локальное хранилище».

  Если выбран криптопровайдер «КриптоПро CSP», для места хранения, то доступно указание значения из следующего перечня: «Локальное хранилище Aladdin eCA», «КриптоПро CSP (HDIMAGE)», «КриптоПро HSM».

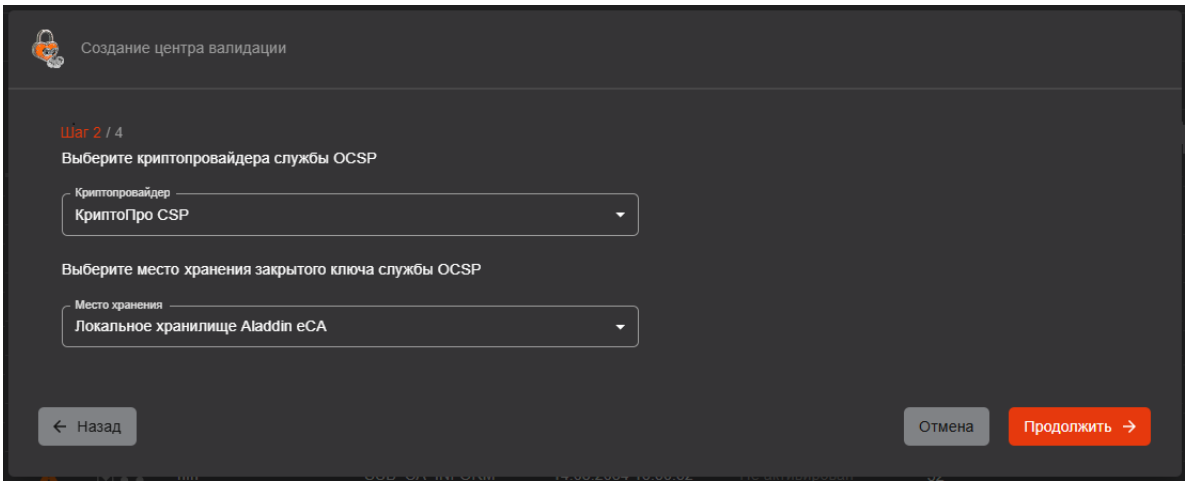


Рисунок 22 — Окно «Создание центра валидации» на шаге 2

- Нажмите кнопку «Продолжить».
- На следующем шаге необходимо сделать (см. рисунок 23):

– выбор шаблона сертификата создаваемой службы OCSP. В списке должны присутствовать шаблоны подключённого eCA-CA, имеющие EKU «OCSP Signer» и имеющие в поле «Центр сертификации» значение «Любой» или центр сертификации, для которого создаётся ЦВ;

– выбор алгоритма ключевой пары службы OSCP. Определяется шаблоном и выбранным на предыдущем шаге криптопровайдером службы OCSP;

– выбор длины ключа;

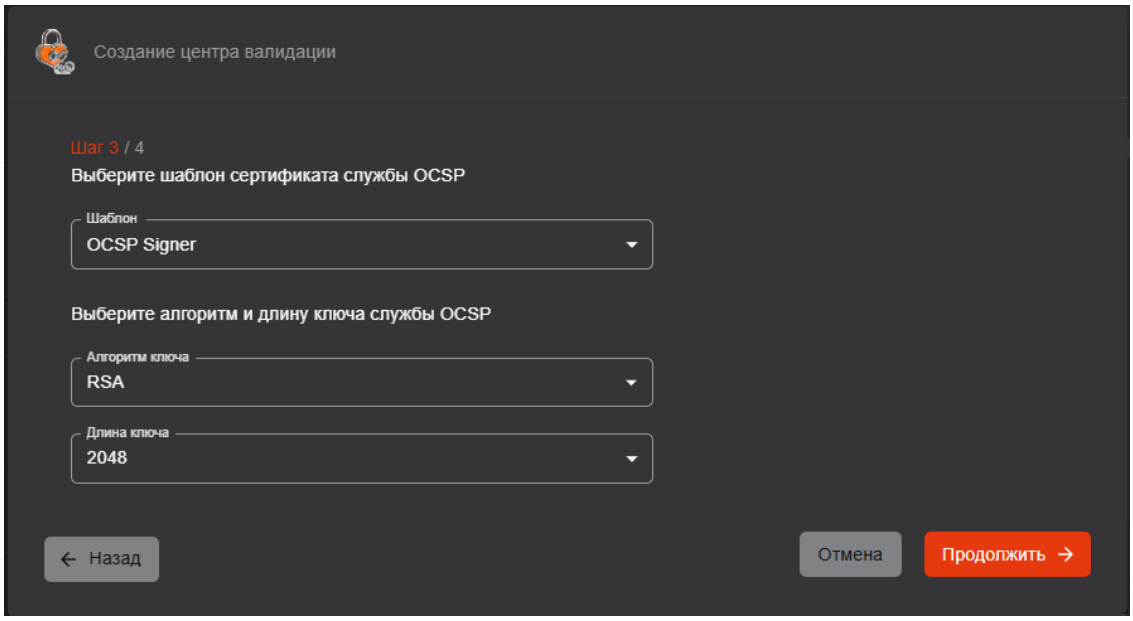


Рисунок 23 — Окно «Создание центра валидации» на шаге 3

- Нажмите кнопку «Продолжить».
- На следующем шаге необходимо сделать (см. рисунок 24):

– выбор алгоритма вычисления хэш-кода ответа.

Доступные для выбора значения в данном поле должны зависеть от выбранного на предыдущем шаге алгоритма ключа: при выборе алгоритма ключа RSA или ECDSA должны быть доступны алгоритмы SHA1, SHA256 (указан по умолчанию), SHA384 SHA512; при выборе алгоритма ключа ГОСТ Р 34.10-2012 доступен только алгоритм ГОСТ Р 34.11-2012;

– управление следующими параметрами создаваемой службы OCSP:

  - «Статус неизвестных сертификатов GOOD».

Внимание! Не рекомендуется отключать данную опцию. Если опция отключена, служба OCSP в ответе на запрос проверки статусов любых сертификатов, кроме отозванных, будет возвращать статус «Unknown».

- «Включать сертификат подписи в ответ».

Внимание! Данная опция может быть отключена только в случае, если на клиенте, обращающемся для проверки статуса сертификата, установлен сертификат издателя сертификата службы OCSP. В противном случае клиент не сможет проверить подпись ответа службы OCSP, и проверка статуса сертификата завершится ошибкой.

- «Включать цепочку сертификатов в ответ» (доступно для включения только при включённой опции «Включать сертификат подписи в ответ»).

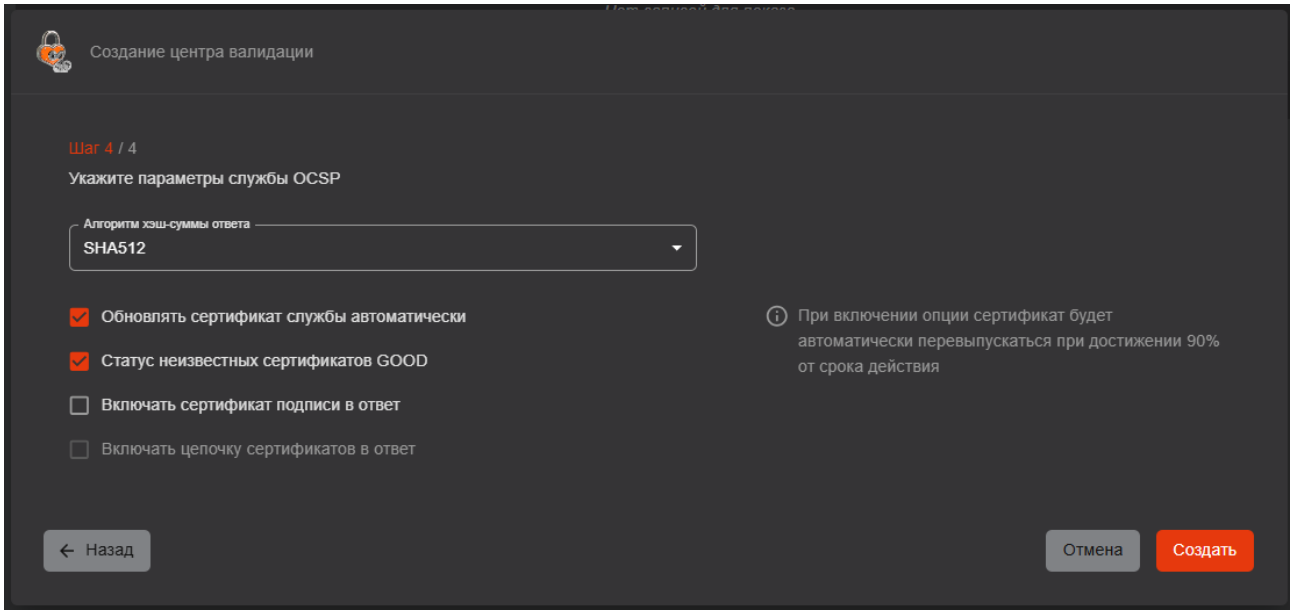


Рисунок 24 — Окно «Создание центра валидации» на шаге 4

- Нажмите кнопку «Создать».

В результате успешного создания Центра валидации будет отображено сообщение: «Успешно! Центр валидации успешно создан».

Количество Центров валидации, которые можно создать, ограничено лицензией eCA-CA.

7.2.3 Создание службы OCSP созданного eCA-VA

Для создания службы OCSP созданного eCA-VA:

- Перейдите в раздел «Центры валидации».
- Перейдите в карточку Центра валидации, для которого служба OCSP не создана (значение в поле «Статус OCSP» — «Не создана»).
- В карточке перейдите на вкладку «OCSP». Нажмите кнопку «Создать службу OCSP».
- В открывшемся окне «Создание службы OCSP» (см. рисунок 25) выберите:

– Криптопровайдера службы OCSP.

При наличии активного криптопровайдера «КриптоПро CSP» на хосте eCA-VA в поле будет доступно указание значения «КриптоПро CSP».

По умолчанию указано значение «Стандартный»;

– выбор места хранения закрытого ключа службы OCSP.

Значение в данном поле зависит от выбранного криптопровайдера службы OCSP.

Если выбран стандартный криптопровайдер, для места хранения будет указано неизменяемое значение «Локальное хранилище».

Если выбран криптопровайдер «КриптоПро CSP», для места хранения, то доступно указание значения из следующего перечня: «Локальное хранилище Aladdin eCA», «КриптоПро CSP (HDIMAGE)», «КриптоПро HSM».

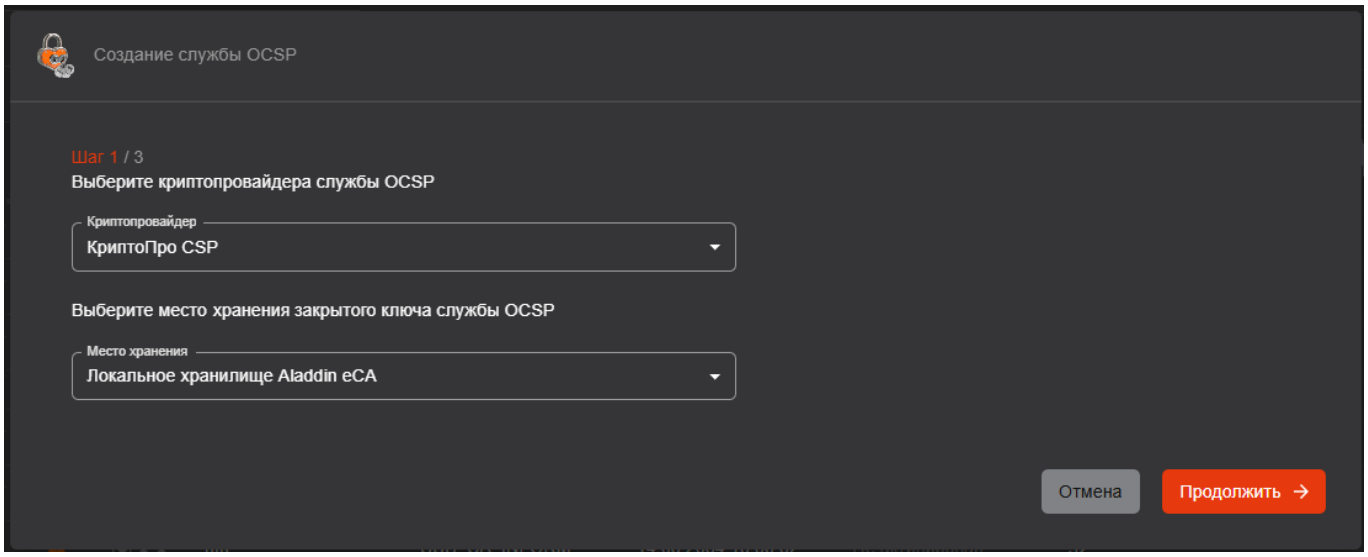


Рисунок 25 — Окно «Создание службы OCSP» на шаге 1

- Нажмите кнопку «Продолжить».
- На данном шаге (см. рисунок 26) выберите:

– шаблон сертификата создаваемой службы OCSP. В списке должны присутствовать шаблоны подключённого eCA-CA, содержащие идентификатор расширенного использования ключа — «OCSP подписант» и имеющие в поле «Центр сертификации» значение «Любой» или название Центра сертификации, для которого создаётся ЦВ.

– алгоритм ключевой пары службы OSCP. Определяется шаблоном и выбранным на предыдущем шаге криптопровайдером службы OCSP.

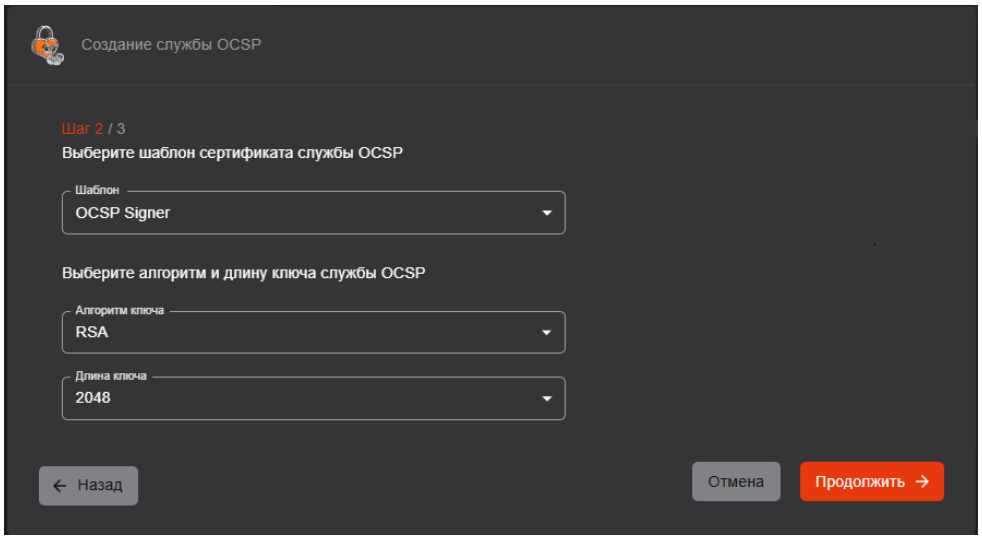


Рисунок 26 — Окно «Создание службы OCSP» на шаге 2

- Нажмите кнопку «Продолжить».

- На данном шаге (см. рисунок 27) выберите:

– алгоритм вычисления хэш-кода ответа. Доступные для выбора значения в данном поле должны зависеть от выбранного на предыдущем шаге алгоритма ключа: при выборе алгоритма ключа RSA или ECDSA должны быть доступны алгоритмы SHA1, SHA256 (указан по умолчанию), SHA384 SHA512; при выборе алгоритма ключа ГОСТ Р 34.10-2012 доступен только алгоритм ГОСТ Р 34.11—2012.

– параметры создаваемой службы OCSP:

  - «Статус неизвестных сертификатов GOOD».

Внимание! Не рекомендуется отключать данную опцию. Если опция отключена, служба OCSP в ответе на запрос проверки статусов любых сертификатов, кроме отозванных, будет возвращать статус «Unknown».

  - «Включать сертификат подписи в ответ».

Внимание! Данная опция может быть отключена только в случае, если на клиенте, обращающемся для проверки статуса сертификата, установлен сертификат издателя сертификата службы OCSP. В противном случае клиент не сможет проверить подпись ответа службы OCSP, и проверка статуса сертификата завершится ошибкой.

  - «Включать цепочку сертификатов в ответ» (доступно для включения только при включённой опции «Включать сертификат подписи в ответ».

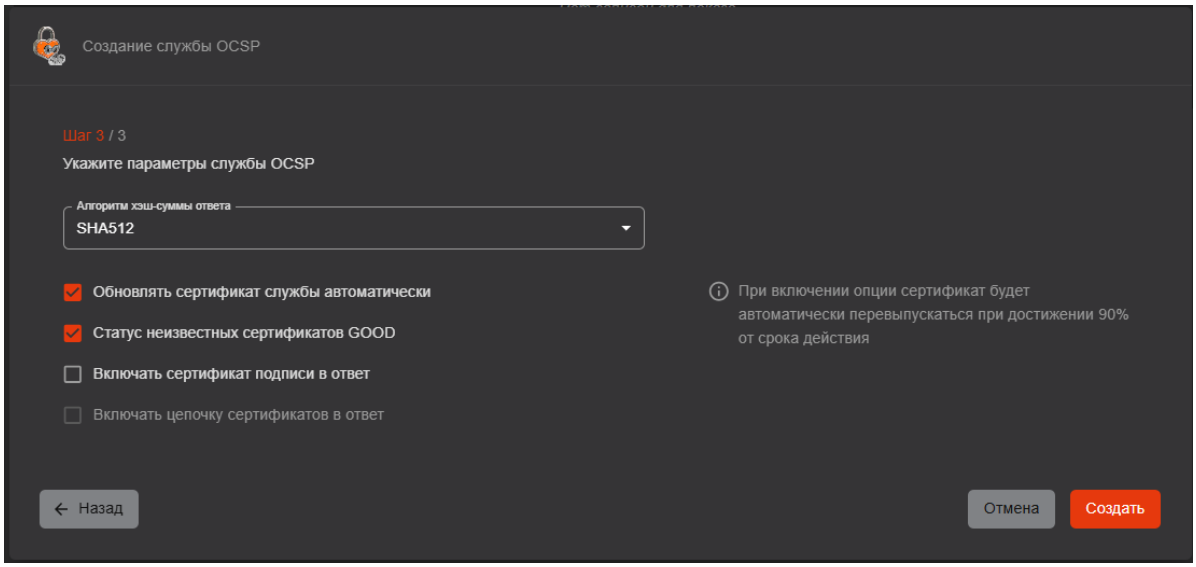


Рисунок 27 — Окно «Создание службы OCSP» на шаге 3

Результат выполнения операции создания службы OCSP будет отображён во всплывающем сообщении в карточке Центра валидации.

В результате успешного создания службы OCSP будет отображено сообщение: «Успешно! Служба OCSP успешно создан».

7.2.4 Ручное обновление сертификата службы OCSP

Для ручного обновления сертификата службы OCSP:

- Перейдите в раздел «Центры валидации».
- Перейдите в карточку Центра валидации, для которого создана служба OCSP.
- В карточке перейдите на вкладку «OCSP».
- Нажмите на кнопку «Обновить сертификат». После нажатия будет осуществлён перевыпуск сертификата службы OCSP с ранее использовавшимися параметрами выпуска (шаблон, алгоритм ключа, длина ключа) на обслуживаемом ЦС eCA-CA. При успехе выпуска сертификат службы OCSP будет заменён на вновь выпущенный.

Результат выполнения операции обновления сертификата будет отображён во всплывающем сообщении в карточке Центра валидации. В результате успешного обновления сертификата службы OCSP будет отображено сообщение: «Успешно! Сертификат службы OCSP успешно обновлён».

7.2.5 Настройка параметров службы OCSP

Для настройки параметров службы OCSP:

- Перейдите в раздел «Центры валидации».
- Перейдите в карточку Центра валидации, для которого создана служба OCSP.
- В карточке перейдите на вкладку «OCSP».
- Нажмите на кнопку «Настроить».
- В открывшемся окне «Настройка службы OCSP» (см. рисунок 28) выберите:

– алгоритм вычисления хэш-кода ответа;

– управление следующими параметрами службы OCSP:

  - «Статус неизвестных сертификатов GOOD».

Внимание! Не рекомендуется отключать данную опцию. Если опция отключена, служба OCSP в ответе на запрос проверки статусов любых сертификатов, кроме отозванных, будет возвращать статус «Unknown».

  - «Включать сертификат подписи в ответ».

Внимание! Данная опция может быть отключена только в случае, если на клиенте, обращающемся для проверки статуса сертификата, установлен сертификат издателя сертификата службы OCSP. В противном случае клиент не сможет проверить подпись ответа службы OCSP, и проверка статуса сертификата завершится ошибкой.

  - «Включать цепочку сертификатов в ответ» (доступно для включения только при включённой опции «Включать сертификат подписи в ответ»).

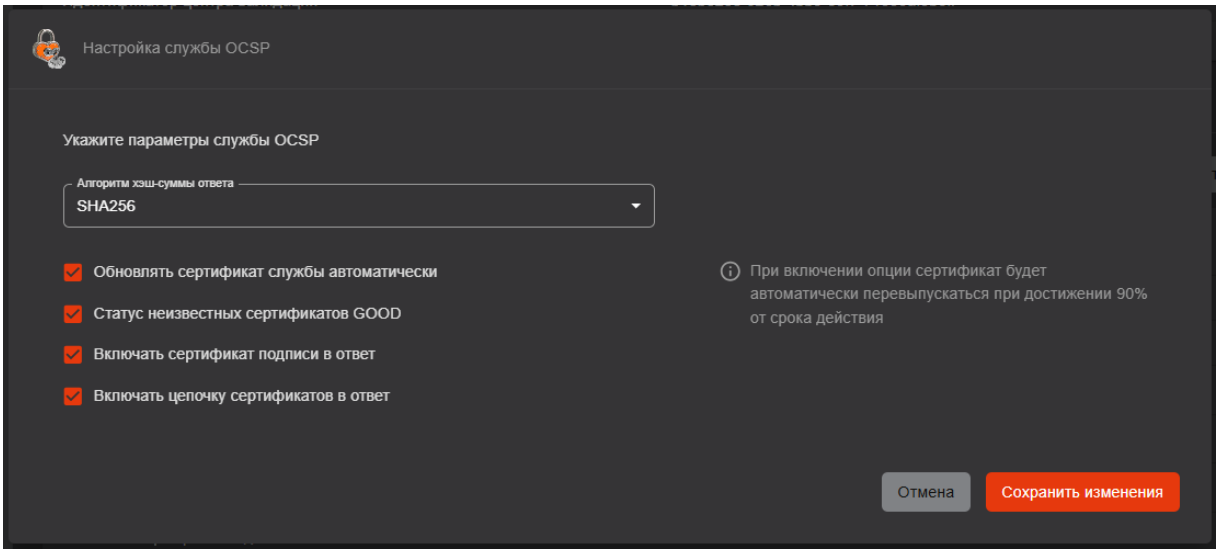


Рисунок 28 — Окно «Настройка службы OCSP»

- После изменения необходимых параметров нажмите на кнопку «Сохранить изменения».

Результат выполнения операции настройки параметров службы OCSP будет отображён во всплывающем сообщении в карточке Центра валидации. В результате успешной настройки службы OCSP будет отображено сообщение: «Успешно! Сертификат службы OCSP успешно обновлены».

7.2.6 Удаление службы OCSP из Центра валидации

Для удаления службы OCSP из Центра валидации необходимо:

- Перейти в раздел «Центры валидации».
- Перейти в карточку любого Центра валидации, для которого создана служба OCSP.
- В карточке перейти на вкладку «OCSP».
- Нажать на кнопку «Удалить».
- В открывшемся окне (см. рисунок 29) подтвердите удаление службы OCSP:

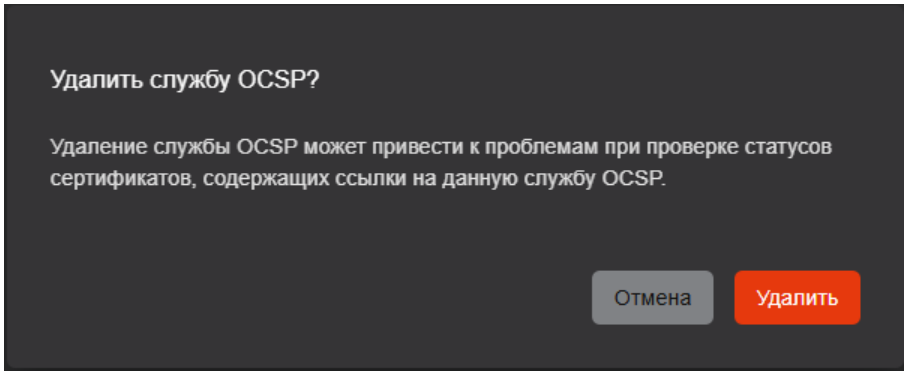


Рисунок 29 — Окно подтверждения удаления службы OCSP

Результат выполнения операции удаления службы OCSP будет отображён во всплывающем сообщении в карточке Центра валидации.

В результате успешного удаления службы OCSP будет отображено сообщение: «Успешно! Служба OCSP успешно удалена».

7.2.7 Удаление Центра валидации

Для удаления Центра валидации необходимо:

- Перейти в раздел «Центры валидации».
- В контекстном меню операций с Центром валидации или в карточке Центра валидации нажать на кнопку «Удалить».
- В карточке перейти на вкладку «OCSP».
- В отобразившемся окне (см. рисунок 30) необходимо подтвердить удаление Центра валидации:

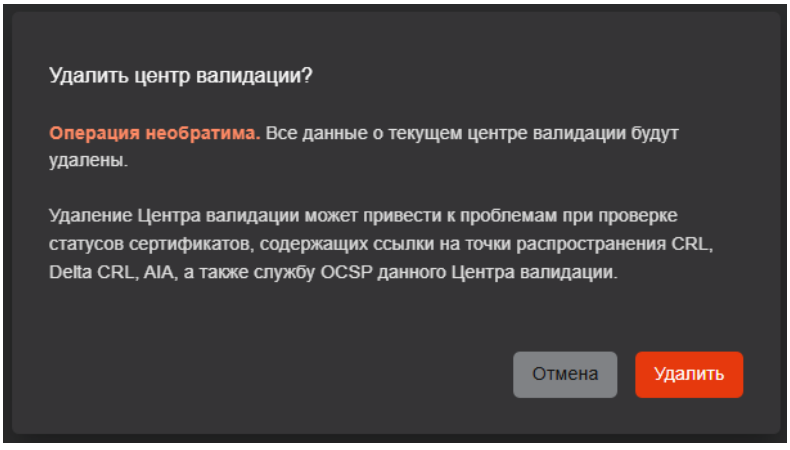


Рисунок 30 — Окно подтверждения удаления Центра валидации.

Результат выполнения операции удаления Центра валидации будет отображён во всплывающем сообщении в разделе «Центры валидации».

В результате успешного удаления Центра валидации будет отображено сообщение: «Успешно! Центр валидации успешно удалён».

7.3 Раздел «Настройки»

Для перехода в раздел «Настройки» главного окна Центра валидации необходимо щёлкнуть левой кнопкой мыши на значке  .

7.3.1 Вкладка «Веб сервер»

На вкладке «Веб-сервер» (см. рисунок 31) присутствуют следующие подразделы:

- «Сертификат»;
- «Разрешенные издатели».

В подразделе «Сертификат» в табличной форме отображается следующая информация о текущем сертификате веб-сервера:

- CN, указанный в сертификате (поле «Имя»; обозначено цифрой 1 на рисунке 31);
- SDN издателя сертификата (поле «Издатель»; обозначено цифрой 2 на рисунке 31);
- Дата окончания действия сертификата (поле «Действителен до»; обозначено цифрой 3 на рисунке 31).

В таблице с данными текущего сертификата веб-сервера присутствует кнопка «Настройка» (обозначена цифрой 4 на рисунке 31), позволяющая запустить сценарий смены сертификата веб-сервера (см. «Смена сертификата веб-сервера»). Для пользователя с ролью «Администратор» данная кнопка заблокирована.

В подразделе «Разрешенные издатели» в табличной форме отображается следующая информация об издателях сертификатов:

- Отображаемое имя центра сертификации (в поле «Отображаемое имя»; обозначено цифрой 5 на рисунке 31);
- CN, указанный в сертификате центра сертификации (в поле «Издатель»; обозначено цифрой 6 на рисунке 31);
- Дата окончания действия сертификата центра сертификации (в поле «Действителен до», обозначено цифрой 7 на рисунке 31);
- Флаг вхождения центра сертификации в список разрешённых издателей (в поле «Разрешенный издатель», обозначено цифрой 8 на рисунке 31). В данном поле отображается символ «Галочка» зелёного цвета, если центр сертификации входит в список разрешённых издателей, иначе в поле отображается прочерк.

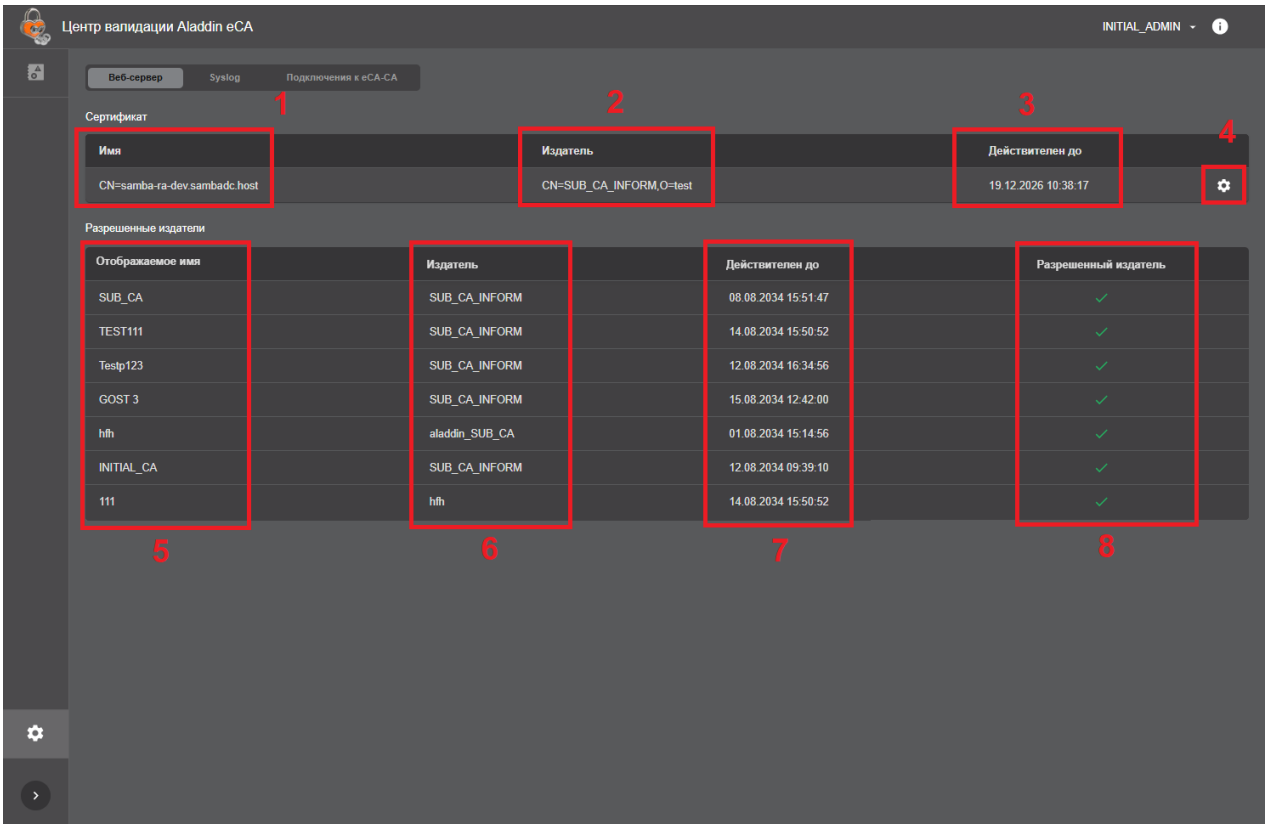


Рисунок 31 -Вкладка «Веб-сервер»

7.3.2 Вкладка «Syslog»

На вкладке «Веб-сервер» в подразделе «Syslog серверы» (см. рисунок 32) присутствуют следующие элементы:

- кнопка «Добавить» (обозначена цифрой 1 на рисунке 32), предназначенная для добавления нового Syslog-сервера в список (см. 7.3.5). Данная возможность доступна только пользователю с ролью «Администратор инициализации»;
- список Syslog-серверов в табличной форме, содержащий следующие элементы:

– поле «Адрес хоста», содержащее в себе адрес хоста Syslog-сервера (обозначено цифрой 2 на рисунке 32);
– поле «Порт», содержащее в себе порт Syslog-сервера (обозначено цифрой 3 на рисунке 32);
– поле «Протокол», содержащее в себе протокол, по которому выполняется отправка сообщение на Syslog-сервер (обозначено цифрой 4 на рисунке 32);
– поле «Отправка сообщений», содержащее в себе переключатель, позволяющий включить или выключить отправку сообщение на данный Syslog-сервер (обозначено цифрой 5 на рисунке 32). Данная возможность доступна только пользователю с ролью «Администратор инициализации»;
– кнопка «Редактировать» (обозначена цифрой 6 на рисунке 32), позволяющая изменить параметры данного Syslog-сервера (см. 7.3.6). Данная возможность доступна только пользователю с ролью «Администратор инициализации»;
– кнопка «Удалить» (обозначена цифрой 7 на рисунке 32), позволяющая удалить данный Syslog-сервер из списка (см. 7.3.7). Данная возможность доступна только пользователю с ролью «Администратор инициализации».

В списке может присутствовать не более 10 Syslog-серверов.

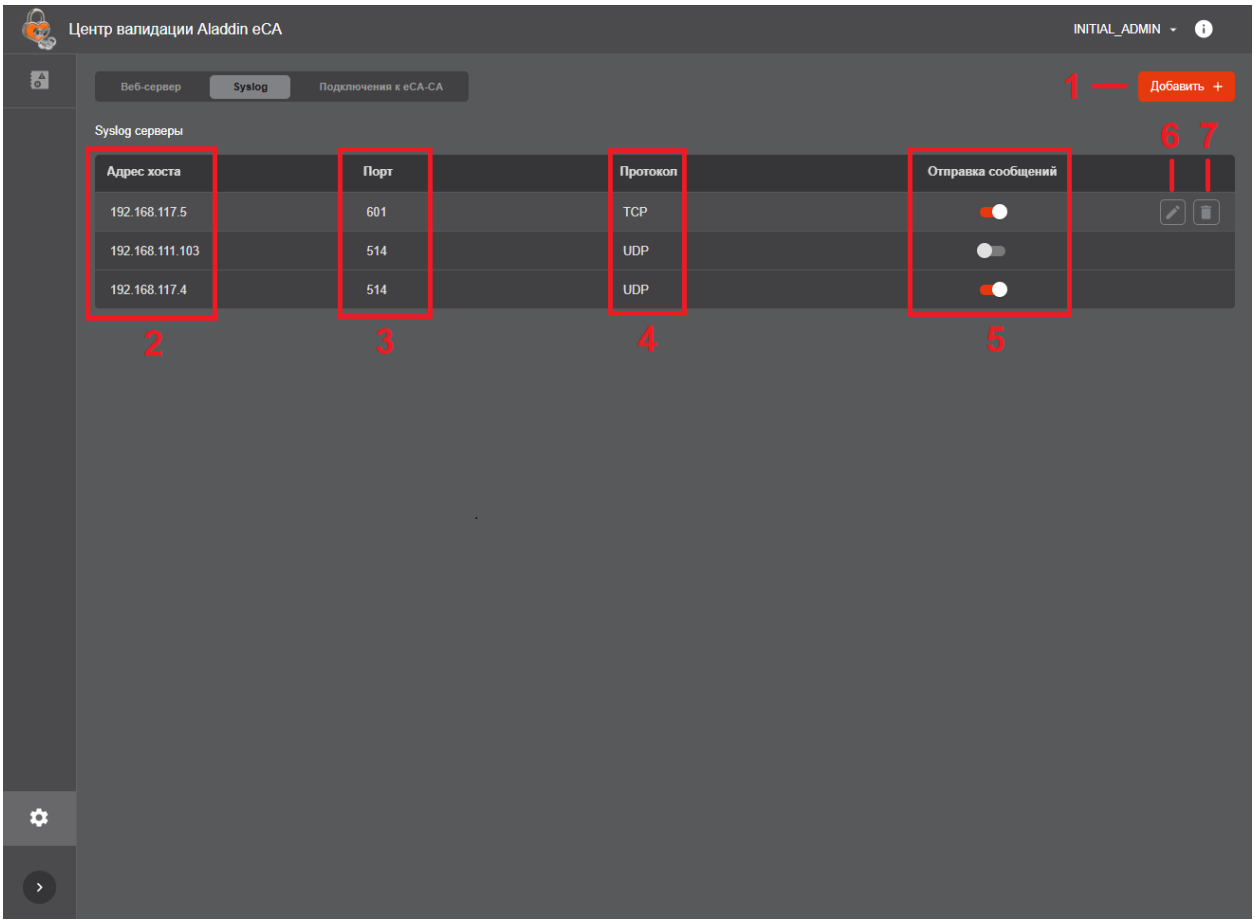


Рисунок 32 - Вкладка «Syslog»

7.3.3 Вкладка «Подключения к eCA-CA»

Внимание! Данная вкладка доступна только пользователю с ролью «Администратор инициализации».

На вкладке «Подключения к eCA-CA» (см. рисунок 33) присутствуют следующие элементы:

- кнопка «Добавить», предназначенная для добавления нового подключения к eCA-CA (см. 7.3.8);
- список подключений к eCA-CA в табличной форме, содержащий для каждого из них следующие элементы:

– поле «Отображаемое имя», содержащее в себе отображаемое имя подключения к eCA-CA;
– поле «Адрес хоста», содержащее в себе адрес хоста eCA-CA;
– поле «Порт», содержащее в себе порт, по которому осуществляется подключение к eCA-CA;
– кнопка «Удалить», позволяющая удалить подключение к eCA-CA (см. 7.3.9).

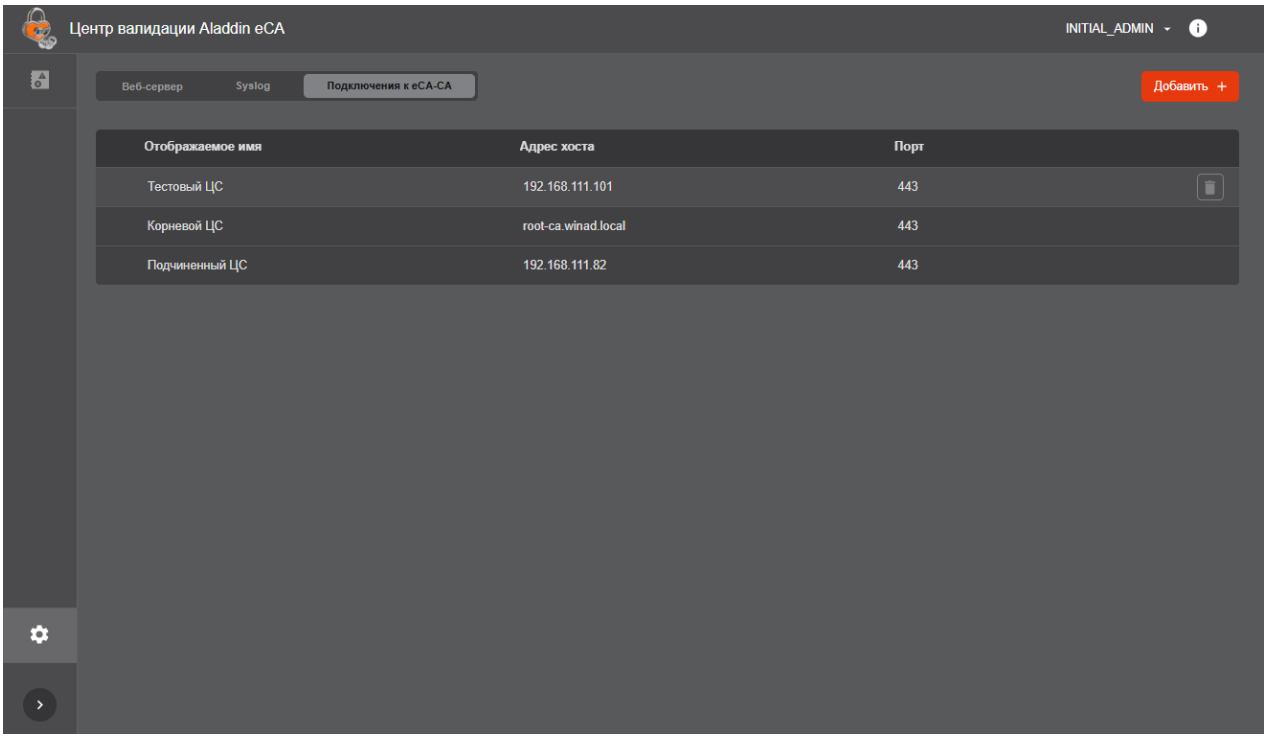


Рисунок 33 -Вкладка «Подключения к eCA-CA»

7.3.4 Смена сертификата веб-сервера

> **Внимание! Данная возможность доступна только пользователю с ролью «Администратор инициализации».**

Для смены сертификата веб-сервера:

1. В ПО eCA-VA необходимо перейти в раздел «Настройки» на вкладку «Веб-сервер». Затем в подразделе «Сертификат» в таблице с данными текущего сертификата веб-сервера нажать на кнопку «Настройки».
2. В появившемся окне (см. рисунок 34) необходимо нажать кнопку «Выбрать файл» и выбрать файл контейнера закрытого ключа, содержащий сертификат веб-сервера, затем ввести пароль от данного контейнера в полей «Пароль контейнера» и подтвердить действие нажатием по кнопке «Сменить ключи» (активируется при заполнении полей в данном окне, нажатие на кнопку «Отмена» производит возврат на вкладку «Веб-сервер» раздела «Настройки» без сохранения изменений).

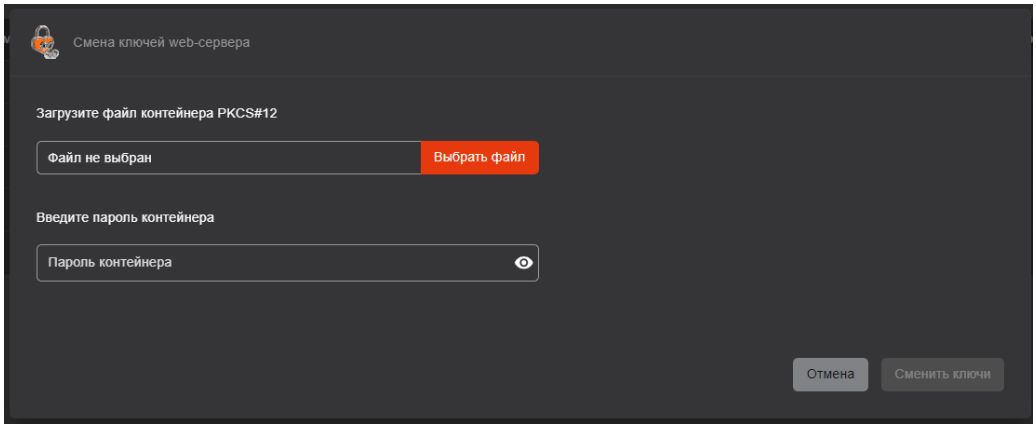


Рисунок 34 - Окно смены сертификата веб-сервера

3. При успешной смене сертификата веб-сервера будет отображено окно с сообщением «Сертификат изменен» (см. рисунок 35). По нажатию на кнопку «Закрыть» клиентский компонент программы будет перезапущен.

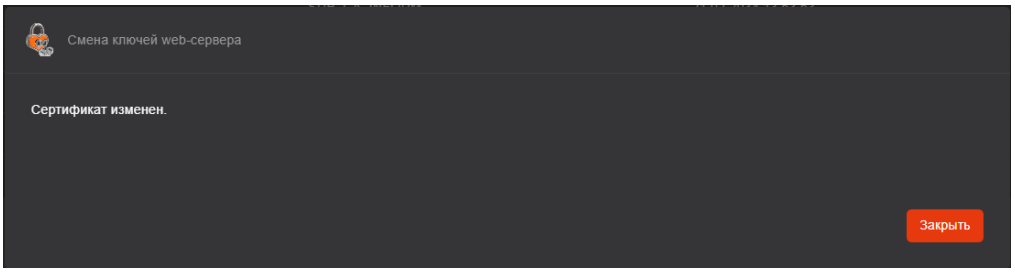


Рисунок 35 - Окно с сообщением об успешном изменении сертификата веб-сервера

В случае, если срок действия сертификата, загруженного на шаге 2 данного сценария, истёк или загружаемый сертификат не содержит идентификатор расширенного использования ключа «Аутентификация сервера» (OID 1.3.6.1.5.5.7.3.1), при нажатии на кнопку «Сменить ключи» в веб-интерфейсе будет отображено сообщение об ошибке «Не валидный сертификат веб-сервера»:

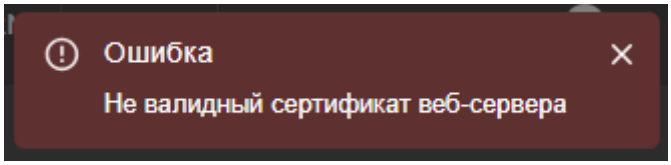


Рисунок 36 - Ошибка «Не валидный сертификат веб-сервера»

7.3.5 Добавление Syslog-сервера

Данная возможность доступна только пользователю с ролью «Администратор инициализации».

eCA-VA может выполняться автоматическая отправка сообщений о зафиксированных событиях по стандарту Syslog (в соответствии с рекомендацией RFC5424) на Syslog-серверы.

Значения полей отправляемых сообщений представлены в таблице 9.

Таблица 9 — Значения полей отправляемых сообщений

Поле Syslog-сообщения	Описание	Значение
PRIVAL	Priority Value - значение, вычисляемое на основе категории и важности события	– Для информационных событий: 14. – Для ошибок: 11
VERSION	Версия используемого стандарта Syslog	1
TIMESTAMP	Временная метка в соответствии с RFC3339	Текущее время на хосте eCA-VA в формате ISO 8601: YYYY-MM-DDThh:mm:ss[.SSS]
HOSTNAME	Имя хоста, отправляющего сообщение	FQDN хоста eCA-VA
APP-NAME	Тег, указывающий приложение или процесс, создавшего сообщение	AECA-VA
PROCID	Идентификатор процесса (PID) приложения	PID сервиса, являющегося источником события

Поле Syslog-сообщения	Описание	Значение
MSGID	Идентификатор сообщения	Код события
[STRUCTURED-DATA]	Структурированные данные	`[aeca-va eventId=''eventId'' actionCode=''actionCode'' category=''category'' id=''id'' serviceName=''serviceName'' system=''system'' username=''username'' role=''role'' ipAddress=''ipAddress'' attributes=''attributes'']` где: – `''eventId''` – идентификатор события; – `''actionCode''` - код события; – `''category''` - категория события; – `''id''` - идентификатор типа события; – `''serviceName''` - имя сервиса, в котором произошло событие; – `''system''` - флаг системного события; – `''username''` - логин учётной записи инициатора события; – `''role''` - роль инициатора события; – `''ipAddress''` - IP-адрес инициатора события; – `''attributes''` - расширенное описание события. Состав полей расширенного описания события соответствует составу полей описания события, указанному в разделе 7.4.1
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»)

Внимание! Количество Syslog-серверов, на которые eCA-VA отправляет сообщения, не может превышать 10.

Для добавления Syslog-сервера:

1. Перейдите в раздел «Настройки» на вкладку «Syslog».
2. В подразделе «Syslog серверы» нажмите кнопку «Добавить».
3. В окне «Добавление Syslog-сервера» (см. рисунок 37) укажите параметры добавляемого Syslog-сервера:
   - 3.1. «Адрес хоста». В данном поле ввода укажите адрес хоста Syslog-сервера. Формат ввода – IPv4 или FQDN [1].
   - 3.2. «Порт». В данном поле ввода необходимо указать порт Syslog-сервера. Формат ввода – число от 1 до 65535.
   - 3.3. «Протокол». Допустимые варианты выбора: UDP, TCP, TCP (TLS).
4. Нажмите кнопку «Добавить».

[1] Регулярное выражение для параметра «Адрес хоста»: ^((25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])\.){3}(25[0-5]|2[0-4][0-9]|1[0-9][0-9]|[1-9][0-9]|[0-9])$|^(?=.{1,253}$)([a-zA-Z0-9_]([a-zA-Z0-9-_]{0,61}[a-zA-Z0-9_])?\.)+[a-zA-Z]{2,}$

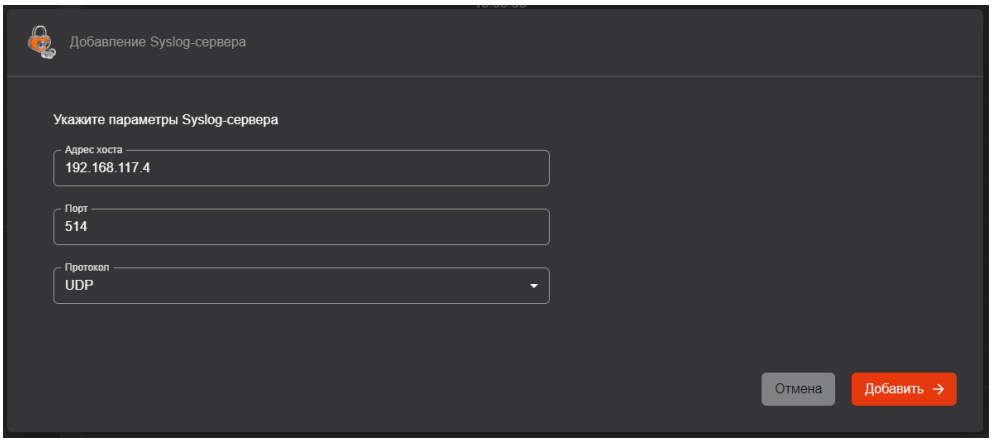


Рисунок 37 – Окно «Добавление Syslog-сервера»

Если в качестве протокола используется TCP (как с TLS, так и без него), то при добавлении Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения новый Syslog-сервер не будет добавлен.

7.3.6 Редактирование параметров Syslog-сервера

Данная возможность доступна только пользователю с ролью «Администратор инициализации».

Для редактирования параметров Syslog-сервера:

1. Перейдите в раздел «Настройки» на вкладку «Syslog».
2. В строке необходимого Syslog-сервера нажмите кнопку «Редактировать».
3. В окне «Редактирование Syslog-сервера» (см. рисунок 38) отредактируйте необходимые параметры.
4. Нажмите на кнопку «Сохранить изменения».

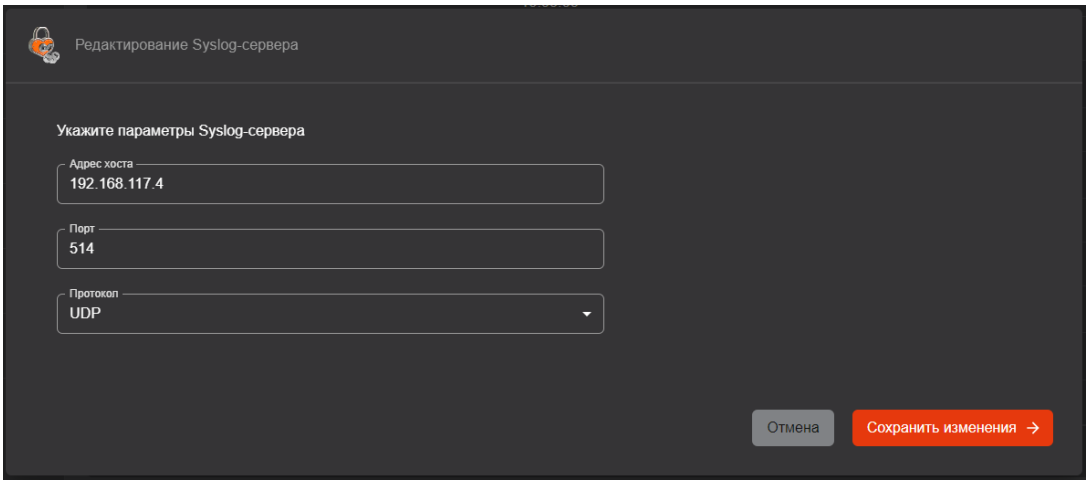


Рисунок 38 –Окно «Редактирование Syslog-сервера»

Если в качестве протокола используется TCP (как с TLS, так и без него), то при изменении параметров Syslog-сервера будет осуществляться попытка подключения к нему. При невозможности подключения параметры Syslog-сервер не будут изменены.

7.3.7 Удаление Syslog-сервера

Данная возможность доступна только пользователю с ролью «Администратор инициализации».

Для удаления Syslog-сервера:

- В ПО eCA-VA необходимо перейти в раздел «Настройки» на вкладку «Syslog».
- В строке любого из имеющихся в списке Syslog-серверов необходимо нажать на кнопку «Удалить».
- При нажатии кнопку «Удалить» будет отображаться диалоговое окно подтверждения удаления Syslog-сервера (см. рисунок 39). В данном окне в строке «Удалить Syslog-сервер?» будет содержаться адрес хоста удаляемого Syslog-сервера.

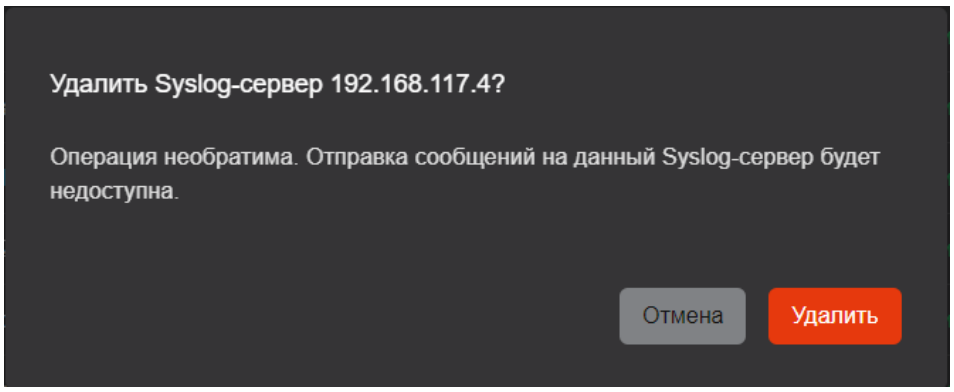


Рисунок 39 - Диалоговое окно подтверждения удаления Syslog-сервера

После нажатия на кнопку «Удалить» в диалоговом окне подтверждения удаления Syslog-сервер будет удалён из списка отображаемых на вкладке «Syslog» в разделе «Настройки». При этом будет отображаться сообщение об успешном удалении Syslog-сервера «Успешно! Syslog-сервер удален» (см. рисунок 40).

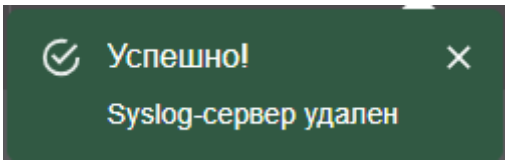


Рисунок 40 - Сообщение об успешном удалении Syslog-сервера

7.3.8 Добавление подключения к eCA-CA

Данная возможность доступна только пользователю с ролью «Администратор инициализации».

Для добавления подключения к eCA-CA:

- В веб-интерфейсе eCA-VA необходимо перейти в раздел «Настройки» на вкладку «Подключения к eCA-CA», затем нажать на кнопку «Добавить».
- В открывшемся окне «Добавление подключения к eCA-CA» (см. рисунок 41) необходимо:

– указать следующие параметры подключения к eCA-CA:

  - «Отображаемое имя». В случае, если отображаемое имя не указано, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия).
  - «Адрес хоста». В данном поле необходимо указать адрес хоста eCA-CA (доступно указание IP-адреса или DNS-имени). В случае, если адрес хоста не указан, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия). В случае, если указанный адрес хоста содержит пробел, в данном поле ввода будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Добавить» будет недоступна для нажатия).

- «Порт». В данном поле необходимо указать порт, по которому будет осуществляться подключение к eCA-CA. Формат ввода - число от 0 до 65535. В случае, если порт не указан, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Добавить» будет недоступна для нажатия). В случае, если в поле «Порт» указано значение, не соответствующее формату ввода, в данном поле будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Добавить» будет недоступна для нажатия);

– импортировать контейнер закрытого ключа (PKCS#12) администратора eCA-CA;

– указать пароль от контейнера закрытого ключа (PKCS#12) администратора eCA-CA.

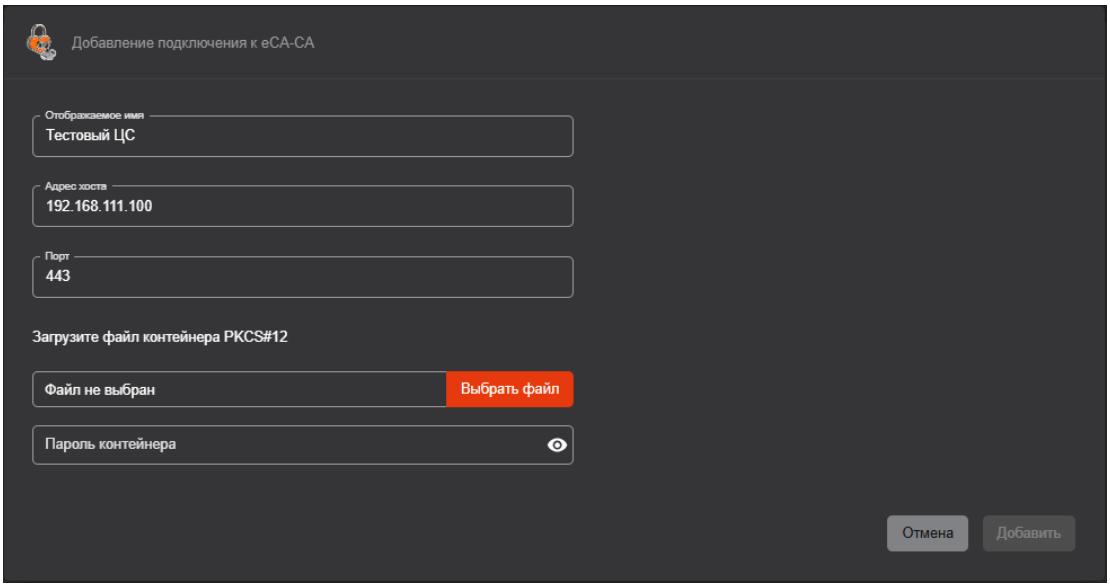


Рисунок 41 — Окно добавления подключения к eCA-CA

После нажатия на кнопку «Добавить» будет выполнено тестовое подключение к eCA-CA, параметры и контейнер которого были указаны. Если тестовое подключение было выполнено успешно, в список будет добавлено новое подключение с параметрами, указанными в окне «Добавление подключения к eCA-CA».

7.3.9 Удаление подключения к eCA-CA

Данная возможность доступна только пользователю с ролью «Администратор инициализации».

Для удаления подключения к eCA-CA:

- В ПО eCA-VA перейдите в раздел «Настройки» на вкладку «Подключения к eCA-CA».
- В строке любого из имеющихся в списке подключений к eCA-CA нажмите кнопку «Удалить».

- В окне подтверждения удаления подключения к eCA-CA (см. рисунок 42) нажмите кнопку удалить. В данном окне в строке «Удалить подключение?» содержится отображаемое имя удаляемого подключения, например, «Удалить подключение «Test»?».

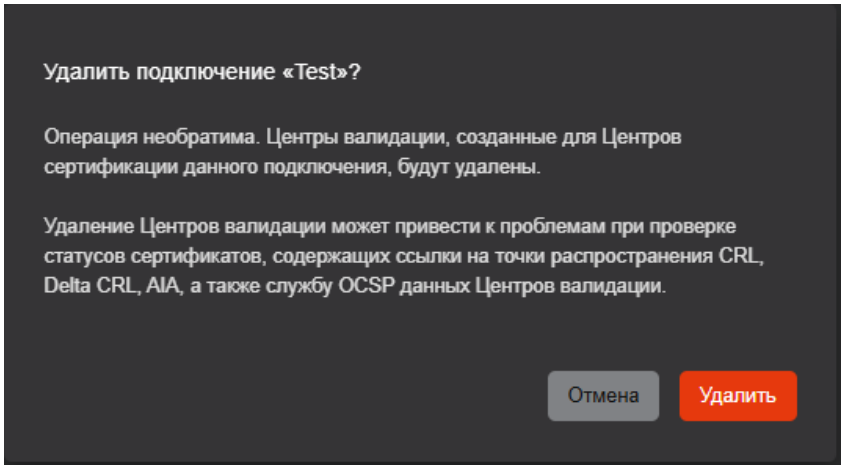


Рисунок 42 - Диалоговое окно подтверждения удаления Syslog-сервера

После нажатия на кнопку «Удалить» в диалоговом окне подтверждения подключение будет удалено из списка. При этом будет отображаться сообщение о успешном удалении подключения «Успешно! Подключение удалено» (см. рисунок 43).

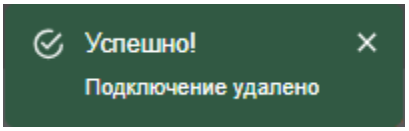


Рисунок 43 - Сообщение об успешном удалении подключения

7.4 Раздел «Журнал событий»

7.4.1 О журнале событий

Перечень событий с их кодами, категориями и подробным описанием приведён в разделе 7.4.2.

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

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

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

7.4.2 Фиксируемые события

7.4.2.1 События запуска/остановки служб и применения параметров конфигурационного файла

События запуска/остановки служб и применения параметров конфигурационного файла описаны в таблице 10.

Таблица 10 — События запуска/остановки служб и применения параметров конфигурационного файла

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Запуск службы	VAENV0000	INFO	Краткое описание: Запуск службы Атрибуты: – Название службы
Остановка службы	VAENV0001	INFO	Краткое описание: Остановка службы Атрибуты: – Название службы
Применение параметров конфигурационного файла	VAENV0002	INFO	Описание: Применение параметров конфигурационного файла Атрибуты: – Наличие изменений в конфигурационном файле; – Параметры конфигурационного файла. В данном атрибуте присутствуют все параметры и значения параметров применённого конфигурационного файла в формате «ключ=значение», кроме параметров «database_password», «aeca_ca_auth_password» и «certificate_raw_server_password»

7.4.2.2 События аутентификации пользователей

События аутентификации пользователей описаны в таблице 11.

Таблица 11 - События аутентификации пользователей

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Аутентификация пользователя	VAENV0100	INFO	Краткое описание: «Аутентификация пользователя». Атрибуты: – Id пользователя. – Отображаемое имя пользователя. – Роль пользователя. – Аутентификатор. – Тип аутентификации. – IP адрес
Ошибка аутентификации пользователя	VAENV0101	ERROR	Краткое описание: «Ошибка аутентификации пользователя». Атрибуты: – Id пользователя (может отсутствовать). – Отображаемое имя пользователя (может отсутствовать). – Роль пользователя (может отсутствовать). – Аутентификатор (может отсутствовать). – Тип аутентификации. – IP адрес. – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Выход пользователя	VAENV0102	INFO	Краткое описание: «Выход пользователя» Атрибуты: – Id пользователя. – Отображаемое имя пользователя. – Роль пользователя. – Аутентификатор. – Тип аутентификации. – IP адрес

7.4.2.3 События работы с Центрами валидации

События работы с Центрами валидации описаны в таблице 12.

Таблица 12 - События работы с Центрами валидации

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание центра валидации	VAENV0200	INFO	Краткое описание: «Создание центра валидации». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Статус CRL. – Статус Delta CRL. – Статус OCSP
Ошибка создания центра валидации	VAENV0201	ERROR	Краткое описание: «Ошибка создания центра валидации». Атрибуты: – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – Причина ошибки
Создание службы OCSP	VAENV0202	INFO	Краткое описание: «Создание службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – ID сертификата. – Алгоритм ключа. – Длина ключа. – Алгоритм хэш-суммы ответа. – Автоматическое обновление сертификата службы. – Статус неизвестных сертификатов GOOD. – Включать цепочку сертификатов в ответ. – Включать сертификат подписи в ответ

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка создания службы OCSP	VAENV0203	ERROR	Краткое описание: «Ошибка создания службы OCSP». Атрибуты: – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – ID сертификата (может отсутствовать). – Алгоритм ключа (может отсутствовать). – Длина ключа (может отсутствовать). – Алгоритм хэш-суммы ответа (может отсутствовать). – Автоматическое обновление сертификата службы (может отсутствовать). – Статус неизвестных сертификатов GOOD (может отсутствовать). – Включать цепочку сертификатов в ответ (может отсутствовать) – Включать сертификат подписи в ответ (может отсутствовать). – Причина ошибки
Запуск службы OCSP	VAENV0204	INFO	Краткое описание: «Запуск службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Статус OCSP
Ошибка запуска службы OCSP	VAENV0205	ERROR	Краткое описание: «Ошибка запуска службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Статус OCSP. – Причина ошибки
Остановка службы OCSP	VAENV0206	INFO	Краткое описание: «Остановка службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Статус OCSP
Ошибка остановки службы OCSP	VAENV0207	ERROR	Краткое описание: «Ошибка остановки службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Статус OCSP. – Причина ошибки
Изменение параметров службы OCSP	VAENV0208	INFO	Краткое описание: «Изменение параметров службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Алгоритм хэш-суммы ответа. – Автоматическое обновление сертификата службы. – Статус неизвестных сертификатов GOOD. – Включать цепочку сертификатов в ответ. – Включать сертификат подписи в ответ

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка изменения параметров службы OCSP	VAENV0209	ERROR	Краткое описание: «Ошибка изменения параметров службы OCSP». Атрибуты: – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – Алгоритм хэш-суммы ответа (может отсутствовать). – Автоматическое обновление сертификата службы (может отсутствовать). – Статус неизвестных сертификатов GOOD (может отсутствовать). – Включать цепочку сертификатов в ответ (может отсутствовать). – Включать сертификат подписи в ответ (может отсутствовать). – Причина ошибки
Обновление сертификата службы OCSP	VAENV0210	INFO	Краткое описание: «Обновление сертификата службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – ID сертификата. – Алгоритм ключа. – Длина ключа
Ошибка обновления сертификата службы OCSP	VAENV0211	ERROR	Краткое описание: «Ошибка обновления сертификата службы OCSP». Атрибуты: – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – ID сертификата (может отсутствовать). – Алгоритм ключа (может отсутствовать). – Длина ключа (может отсутствовать). – Причина ошибки
Удаление службы OCSP	VAENV0212	INFO	Краткое описание: «Удаление службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка удаления службы OCSP	VAENV0213	ERROR	Краткое описание: «Ошибка удаления службы OCSP». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки
Переподключение центра валидации	VAENV0214	INFO	Краткое описание: «Переподключение центра валидации». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка переподключения центра валидации	VAENV0215	ERROR	Краткое описание: «Ошибка переподключения центра валидации». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Удаление центра валидации	VAENV0216	INFO	Краткое описание: «Удаление центра валидации». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка удаления центра валидации	VAENV0217	ERROR	Краткое описание: «Ошибка удаления центра валидации». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки
Обновление CRL	VAENV0218	INFO	Краткое описание: «Обновление CRL». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка обновления CRL	VAENV0219	ERROR	Краткое описание: «Ошибка обновления CRL». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки
Обновление Delta CRL	VAENV0220	INFO	Краткое описание: «Обновление Delta CRL». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка обновления Delta CRL	VAENV0221	ERROR	Краткое описание: «Ошибка обновления Delta CRL». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки
Служба OCSP вернула ошибку	VAENV0222	ERROR	Краткое описание: «Служба OCSP вернула ошибку». Атрибуты: – ID центра валидации. – ID обслуживаемого центра сертификации. – Причина ошибки

7.4.2.4 События экспорта

События экспорта описаны в таблице 13.

Таблица 13 - События экспорта

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Экспорт файла	VAENV0500	INFO	Краткое описание: «Экспорт файла». Атрибуты: – ID центра валидации. – Тип файла
Ошибка экспорта файла	VAENV0501	ERROR	Краткое описание: «Ошибка экспорта файла». Атрибуты: – ID центра валидации. – Тип файла. – Причина ошибки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Экспорт журнала событий	VAENV0502	INFO	Краткое описание: «Экспорт журнала событий». Атрибут: Параметры фильтрации
Ошибка экспорта журнала событий	VAENV0503	ERROR	Краткое описание: «Ошибка экспорта журнала событий». Атрибуты: – Параметры фильтрации. – Причина ошибки

7.4.2.5 События работы с веб-сервером и издателями

События работы с веб-сервером и издателями описаны в таблице 14.

Таблица 14 - События работы с веб-сервером и издателями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Изменение сертификата веб-сервера	VAENV0700	INFO	Краткое описание: «Изменение сертификата веб-сервера». Атрибуты: – «Серийный номер». – «Отпечаток». – «CN в сертификате». – «SDN издателя». – «Действует с». – «Действует по»
Ошибка изменения сертификата веб-сервера	VAENV0701	ERROR	Краткое описание: «Ошибка изменения сертификата веб-сервера». Атрибуты: – «Серийный номер» (может отсутствовать). – «Отпечаток» (может отсутствовать). – «CN в сертификате» (может отсутствовать). – «Действует с» (может отсутствовать). – «Действует по» (может отсутствовать). – «Причина ошибки»
Изменение списка разрешённых издателей	VAENV0702	INFO	Краткое описание: «Изменение списка разрешённых издателей». Атрибут: «Обновленный список разрешенных издателей»
Ошибка изменения списка разрешённых издателей	VAENV0703	ERROR	Краткое описание: «Ошибка изменения списка разрешенных издателей». Атрибуты: – «Обновленный список разрешенных издателей» (может отсутствовать). – «Причина ошибки»

7.4.2.6 События работы с резервными копиями

События работы с резервными копиями описаны в таблице 15.

Таблица 15 - События работы с резервными копиями

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Успешное создание резервной копии	VAENV0900	INFO	Краткое описание: «Успешное создание резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии». – «Наличие БД в резервной копии»

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Ошибка создания резервной копии	VAENV0901	ERROR	Краткое описание: «Ошибка создания резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии» (может отсутствовать). – «Причина ошибки»
Успешное восстановление из резервной копии	VAENV0902	INFO	Краткое описание: «Успешное восстановление из резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии». – «Восстановление БД»
Ошибка восстановления из резервной копии	VAENV0903	ERROR	Краткое описание: «Ошибка восстановления из резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии» (может отсутствовать). – «Причина ошибки»

7.4.2.7 События контроля целостности

События контроля целостности описаны в таблице 16.

Таблица 16 - События контроля целостности

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Успешная проверка контрольных сумм	VAENV1000	INFO	Краткое описание: «Успешная проверка контрольных сумм»
Неуспешная проверка контрольных сумм	VAENV1001	ERROR	Краткое описание: «Неуспешная проверка контрольных сумм». Атрибут: «Причина ошибки» (может отсутствовать)

7.4.2.8 События архивации и очистки записей аудита

События архивации и очистки записей аудита описаны в таблице 17.

Таблица 17 - События архивации и очистки записей аудита

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Начало очистки записей аудита	VAENV1100	INFO	Краткое описание: «Начало очистки записей аудита»
Завершение очистки записей аудита	VAENV1101	ERROR	Краткое описание: «Завершение очистки записей аудита»
Ошибка очистки записей аудита	VAENV1102	INFO	Краткое описание: «Ошибка очистки записей аудита». Атрибут: «Причина ошибки»
Начало архивации записей аудита	VAENV1103	ERROR	Краткое описание: «Начало архивации записей аудита»
Завершение архивации записей аудита	VAENV1104	INFO	Краткое описание: «Завершение архивации записей аудита»
Ошибка архивации записей аудита	VAENV1105	ERROR	Краткое описание: «Ошибка архивации записей аудита».

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			Атрибут: «Причина ошибки»

7.4.2.9 События работы с Syslog

События работы с Syslog описаны в таблице 18.

Таблица 18 - События работы с Syslog

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Добавление Syslog-сервера	VAENV1200	INFO	Краткое описание: Добавление Syslog-сервера Атрибуты: – «Адрес хоста». – «Порт». – «Протокол». – «Флаг отправки сообщений»
Ошибка добавления Syslog-сервера	VAENV1201	ERROR	Краткое описание: Ошибка добавления Syslog-сервера Атрибуты: – «Адрес хоста» (может отсутствовать). – «Порт» (может отсутствовать). – «Протокол» (может отсутствовать). – «Флаг отправки сообщений» (может отсутствовать). – «Причина ошибки»
Изменение параметров Syslog-сервера	VAENV1202	INFO	Краткое описание: Изменение параметров Syslog-сервера Атрибуты: – «Адрес хоста». – «Порт». – «Протокол». – «Флаг отправки сообщений»
Ошибка изменения параметров Syslog-сервера	VAENV1203	ERROR	Краткое описание: Ошибка изменения параметров Syslog-сервера Атрибуты: – «Адрес хоста» (может отсутствовать). – «Порт» (может отсутствовать). – «Протокол» (может отсутствовать). – «Флаг отправки сообщений» (может отсутствовать). – «Причина ошибки»
Удаление Syslog-сервера	VAENV1204	INFO	Краткое описание: Удаление Syslog-сервера Атрибуты: – «Адрес хоста». – «Порт». – «Протокол». – «Флаг отправки сообщений»
Ошибка удаления Syslog-сервера	VAENV1205	ERROR	Краткое описание: Ошибка удаления Syslog-сервера Атрибуты: – «Адрес хоста». – «Порт». – «Протокол». – «Флаг отправки сообщений». – «Причина ошибки»

7.4.2.10 События работы с подключениями к eCA-CA

События работы с подключениями к eCA-CA описаны в таблице 19.

Таблица 19 — События работы с подключениями к eCA-CA

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Создание подключения к eCA-CA	VAENV1300	INFO	Краткое описание: Создание подключения к eCA-CA Атрибуты: – Отображаемое имя – Адрес хоста – Порт – Серийный номер сертификата – CN в сертификате
Ошибка создания подключения к eCA-CA	VAENV1301	ERROR	Краткое описание: Ошибка создания подключения к eCA-CA Атрибуты: – Отображаемое имя (может отсутствовать) – Адрес хоста (может отсутствовать) – Порт (может отсутствовать) – Серийный номер сертификата (может отсутствовать) – CN в сертификате (может отсутствовать) – Причина ошибки
Удаление подключения к eCA-CA	VAENV1302	INFO	Краткое описание: Удаление подключения к eCA-CA Атрибуты: – Отображаемое имя – Адрес хоста – Порт – Серийный номер сертификата – CN в сертификате
Ошибка удаления подключения к eCA-CA	VAENV1303	ERROR	Краткое описание: Ошибка удаления подключения к eCA-CA Атрибуты: – Отображаемое имя – Адрес хоста – Порт – Серийный номер сертификата – CN в сертификате – Причина ошибки

7.4.3 Просмотр записей журнала событий

Для пользователя с ролью «Администратор» в разделе «Журнал событий» для просмотра доступны только события, ассоциированные с подключением к eCA-CA, которому принадлежит данный «Администратор».

Просмотр записей журнала событий доступен пользователям с ролью «Администратор» и «Администратор инициализации». Пользователю с ролью «Администратор» доступен просмотр событий журнала, ассоциированных с подключением к eCA-CA, которому принадлежит данный пользователь.

Для просмотра записей журнала событий подключитесь к веб-интерфейсу eCA-VA и перейдите в раздел **Журнал событий.**

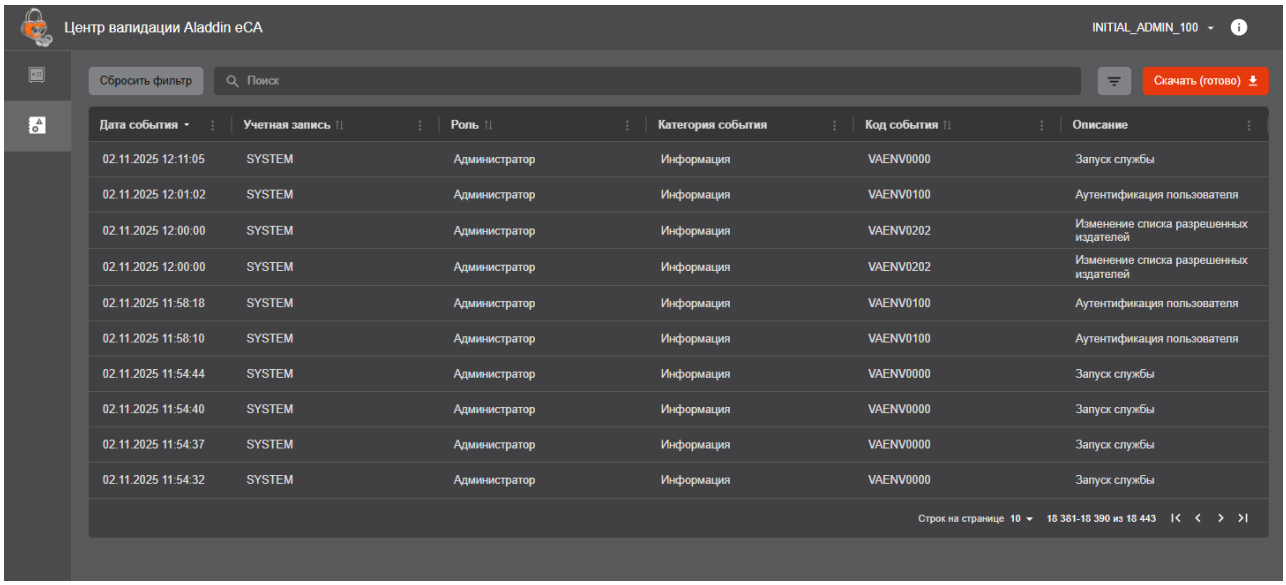


Рисунок 44 - Просмотр журнала событий

Записи о событиях выводятся постранично. Для перемещения по страницам списка используйте инструменты навигации (см. Рисунок 45).

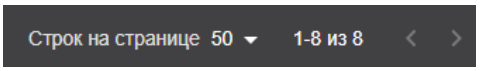


Рисунок 45 - Инструменты навигации

Описание инструментов навигации:

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

Для удобства анализа записей в списке вы можете управлять видимостью колонок таблицы. Чтобы скрыть отображение выбранной колонки, щелкните в ее заголовке значок **<Действие колонки>** и в открывшемся списке [1] выберите **<Скрыть [название колонки] колонку>** (см. Рисунок 46). Чтобы вернуть в таблице отображение скрытых колонок, щелкните в заголовке любой колонки значок **<Действие колонки>** и в открывшемся списке выберите **<Показать все колонки>** (см. Рисунок 46).

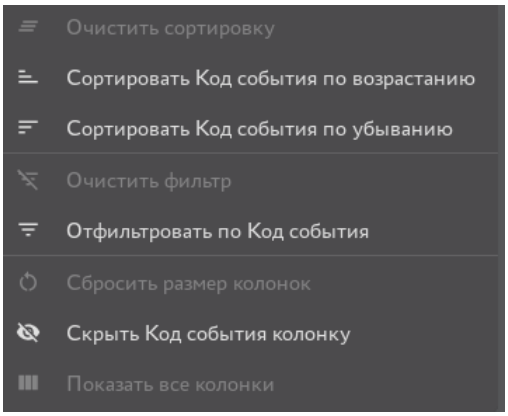


Рисунок 46 - Список действий с колонкой **[Код события]**

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

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

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

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

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

Чтобы выполнить сортировку записей о событиях по выбранному атрибуту, щелкните в заголовке сооответсвующей колонки значок **<Действие колонки>** и в открывшемя списке [1] (см. Рисунок 46) выберите:

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

Статусы выполненной сортировки отображаются в заголовках колонок следующими значками [2]:

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

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

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

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

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

По умолчанию фильтры скрыты. Чтобы использовать фильтры, нажмите на панели инструментов кнопку **<Фильтр>** или щелкните в заголовке колонок **[Сценарий]**, **[Дата обработки]** или **[Статус]** значок **<Действие колонки>** и в открывшемя списке выберите **<Отфильтровать по [название колонки]>**.

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

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

Фильтры по атрибутам событий, представленный в колонках **[Учетная запись]** (см. Рисунок 47а), **[Роль]** (см. Рисунок 47б), **[Категория события]** (см. Рисунок 47в) и **[Код события]** (см. Рисунок 47г) обеспечивают выборку информации по выбранным атрибутам. Выбор атрибутов выполняется установкой флажков для соответствующих значений атрибутов. Фильтр по атрибуту события, представленном в колонке **[Дата события]** (см. Рисунок 47д), обеспечивает выборку информации за указанный временной интервал. Начало и конец временного интервала (дата и время) задаются с помощью календарей и списков.

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

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

Заданные фильтрами критерии выборки отображаются в заголовках соответствующих колонок. Признаком применения фильтра является значок в заголовке соответствующей колонки (см. Рисунок 47).

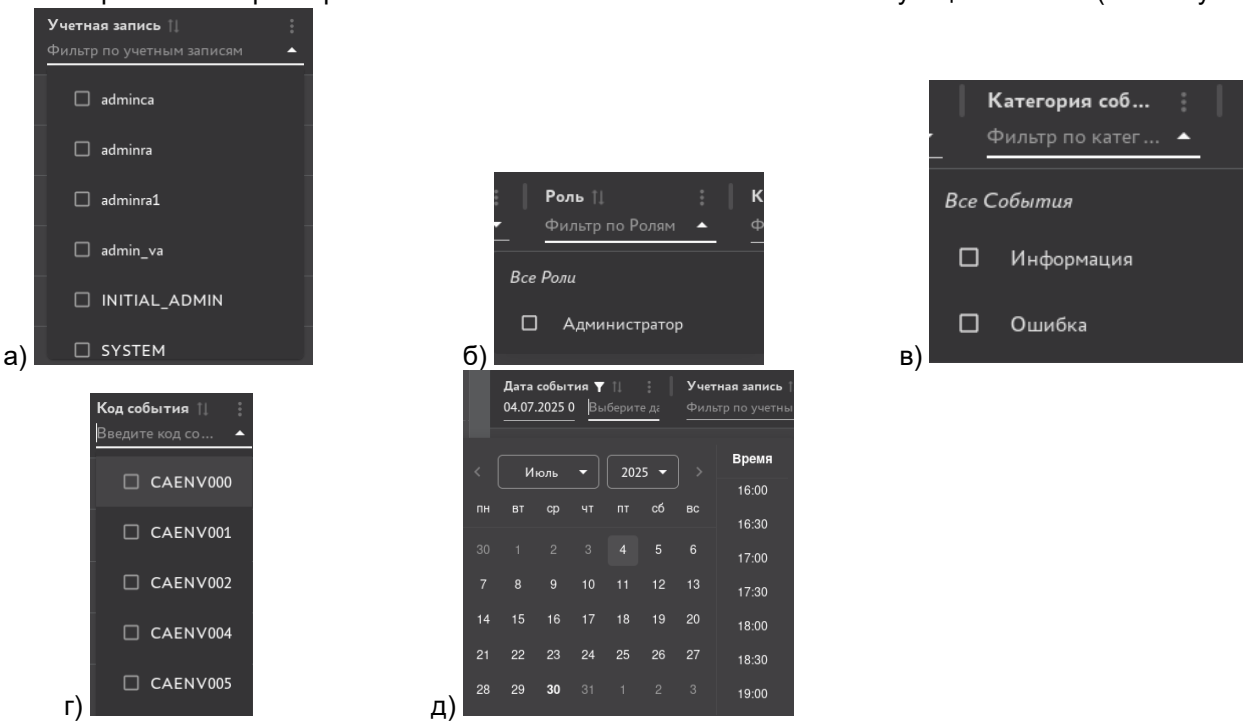


Рисунок 47 - Указание критериев выборки в фильтрах

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

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

Чтобы выполнить выборку событий по их описанию (в том числе и подробному) и причинам, введите в поисковой строке, расположенной на панели инструментов, ключевое слово, содержащееся в описании или причине события (см. Рисунок 48). Для отмены выборки щёлкните в поисковой строке значок .

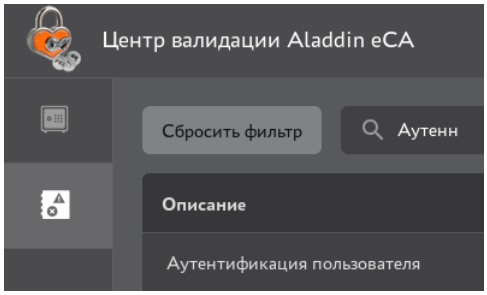


Рисунок 48 - Выборка событий по описанию с помощью поисковой строки

7.4.4 Просмотр карточки события

Карточка события содержит подробную информацию о событии:

- В полях раздела «Общие сведения»:
  - «Идентификатор события»;
  - «Дата и время события»;
  - «Учётная запись» — инициатор события, логин учётной записи, действия которой повлекли событие (имя пользователя eCA-VA или «SYSTEM» для системных событий);
  - «Роль» — роль инициатора события. Для системных событий должна быть указана роль «ADMINISTRATOR»;

- «IP-адрес источника» — IP-адрес инициатора события. Для системных событий значение в данном поле может отсутствовать;
- «Категория события» — «INFO» для информационных событий или «ERROR» для ошибок;
- «Код События» — (см. 7.4.2);
- «Описание» — описание события с атрибутами (см. 7.4.2).

- В разделе «Подробности». Состав полей раздела «Подробности» соответствует составу полей списка «Атрибуты» в столбце «Описание в журнале» таблиц, представленных в 7.4.2.

Чтобы открыть карточку события:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел **Журнал событий.**
- Найдите нужное событие и щёлкните запись о нем в списке (см. Рисунок 49).

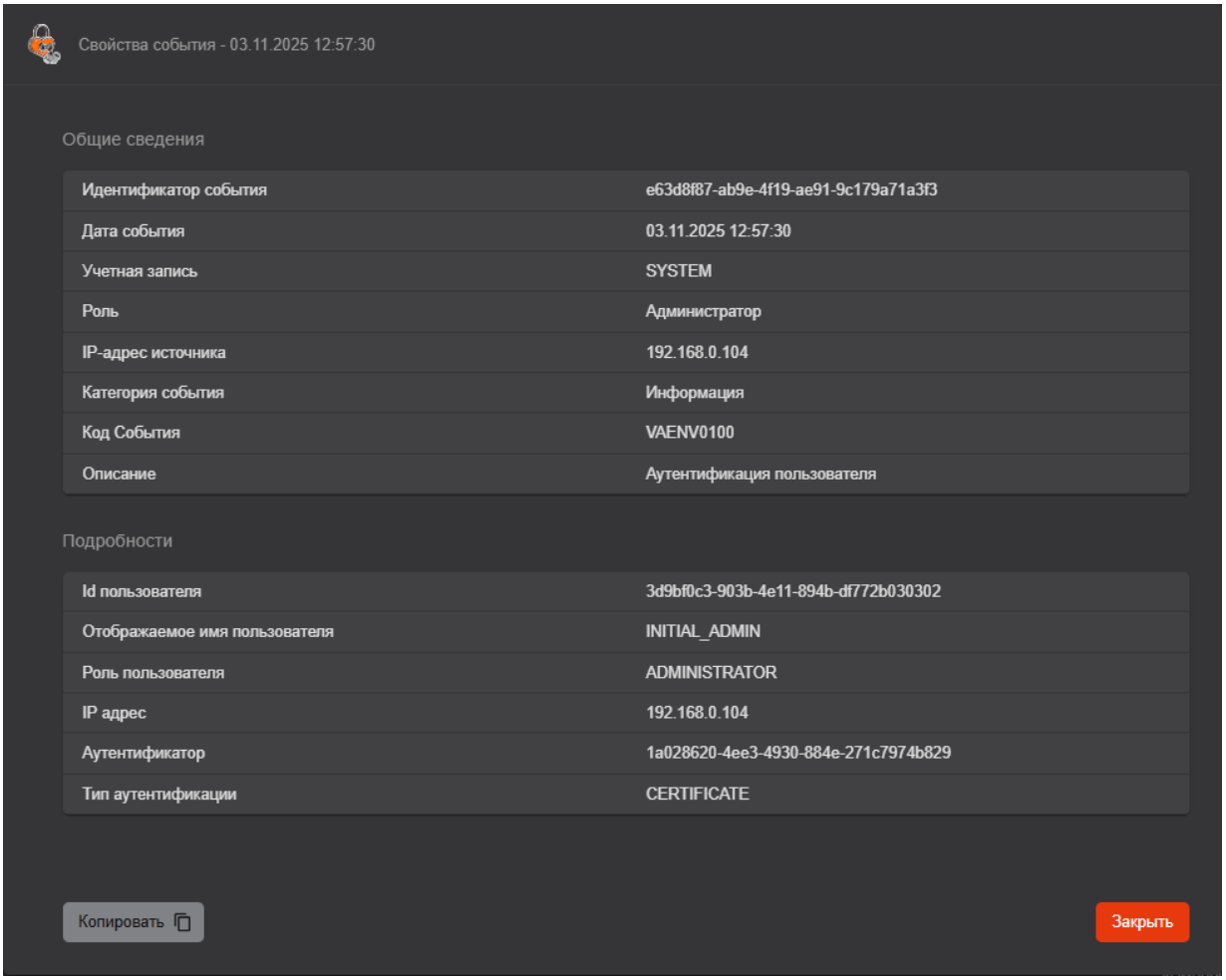


Рисунок 49 — Окно «Свойства события» (карточка события)

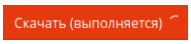
Для копирования информации о событии в буфер обмена нажмите кнопку Копировать.

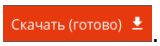
7.4.5 Экспорт записей журнала событий

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

Порядок экспорта журнала событий:

- Подключитесь к веб-интерфейсу eCA-CA и перейдите в раздел  **Журнал событий.**
- Запустите процесс подготовки файла с событиями, нажав на панели инструментов кнопку 

. В результате кнопка меняет свое состояние на 

(начинается подготовка файла, содержащего записи журнала событий).
- После подготовки файла для экспорта журнала нажмите кнопку 

.

8 КОНТРОЛЬ ЦЕЛОСТНОСТИ

8.1 Автоматический контроль целостности при запуске eCA-VA

Контроль целостности eCA-VA при запуске регулируется путём редактирования параметров `integrity_check_startup_enabled` и `integrity_check_fail_block_startup` конфигурационного файла.

Для корректировки автоматического контроля целостности eCA-VA:

1. Укажите в конфигурационном файле необходимые значения для параметров `integrity_check_startup_enabled` и `integrity_check_fail_block_startup` (см. 4.2).
2. Для применения внесённых настроек запустите сценарий обновления при помощи команды с правами суперпользователя:

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

3. При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.
4. Установщик предложит выбрать необходимое действие в интерактивном режиме.
5. Введите в терминале цифру «2».
6. Дождитесь окончания выполнения сценария обновления.

8.2 Контроль целостности исполняемых файлов программы по требованию

Контроль целостности исполняемых файлов eCA-VA необходим для отслеживания неизменности и контроля состояния файлов, перечень которых приведён ниже:

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

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

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

Файл с эталонами контрольными суммами «`jc_checksum`» формируется при сборке программного средства с помощью утилиты контроля целостности «`jcverify`».

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

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

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

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

После завершения работы скрипта необходимо проанализировать полученные данные.

[1] Данная утилита включена в состав Центра валидации Aladdin eVA (каталог «`/opt/aecaVa/bin/jcverify`»).

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

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

9 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ ПРОГРАММЫ

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

В процессе работы eCA-VA системные службы и компоненты приложения записывают все производимые действия. Произошедшие события записываются в файлы регистрации событий [1] с расширением `.log`, расположенные в папках соответствующих сервисов, которыми были инициированы события по пути `/opt/aecaVa/dist/logs/` (определяется параметром `logs_base` конфигурационного файла). Максимальный размер лог-файла каждого сервиса перед его архивацией составляет 10 Мбайт (определяется параметром `logs_file_max_size` конфигурационного файла). Срок хранения архивов составляет 10 дней (определяется параметром `logs_max_history` конфигурационного файла). Максимальный общий объем файлов регистрации событий, включая архивы, каждого типа (`access.log` или `service.log`) для каждого сервиса составляет 100 Мбайт (определяется параметром `logs_total_size_cap` конфигурационного файла)

В процессе автоматизированного сбора диагностической информации будет собрана следующая информация:

- Сведения о работе:
  - сервисов программы (файлы в формате .log);
  - веб-сервера nginx/Apache (в формате .log и .gz);
  - системы управления базой данных PostgreSQL.;
  - системы управления базой данных Jatoba;
  - ОС.
- Конфигурационный файл `/opt/aecaVa/scripts/config.sh`.
- Данные системных логов, представленные в таблице 20.

Таблица 20 — Данные системных логов

Системный лог	РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	Astra Linux SE	Alt Сервер
/var/log/audit/	+	+	+
/var/log/samba/	+	+	+
/var/log/httpd/	+	-	-
/var/log/messages/	+	+	+
/var/log/secure/	+	-	-
/var/log/cron/	+	+	-
/var/log/auth/	-	+	-
/var/log/syslog/	-	+	+
/var/log/httpd2/	-	-	+
/var/log/httpd/	-	-	+

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

- Лог сборщика мусора.
- Дампы памяти для упавших приложений eCA-VA.

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

Для сбора диагностической информации:

- Выполните переход в каталог, где будет сохранён архив с диагностической информацией в формате .tar.gz выполнив команду:

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

- Запустите скрипт от имени суперпользователя при помощи команды:

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

Сформированный архив в формате .tar.gz с диагностической информацией будет сохранён в каталоге, из которого был запущен скрипт.

Для вывода текущего каталога используйте команду:

```
pwd
```

10 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

10.1 Резервное копирование данных

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

Резервная копия включает:

- обязательно:
  - сертификат и ключ веб-сервера, а также файл, содержащий сертификаты разрешённых издателей, из каталога, указанного в параметре `certificates_ssl_path` конфигурационного файла `/opt/aecaVa/scripts/config.sh` (по умолчанию: `/opt/aecaVa/dist/certificates/ssl`);
  - контейнеры закрытого ключа служб OCSP (файлы в каталоге `/opt/aecaVa/dist/cryptotoken/`);
  - ключи для шифрования пароля пользователя СУБД в конфигурационном файле (файл `/opt/aecaVa/scripts/key`);
  - конфигурационный файл программы `/opt/aecaVa/scripts/config.sh`;
- опционально: базу данных программы, указанную в параметре `database_name` конфигурационного файла `/opt/aecaVa/scripts/config.sh` (по умолчанию `aecava`).

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

Имена файлов резервных копий имеют следующий формат:

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

Параметры запуска скрипта `/opt/aecaVa/scripts/backup.sh` представлены в таблице 21.

Таблица 21 — Параметры запуска скрипта `/opt/aecaVa/scripts/backup.sh`

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

Для создания резервной копии:

- Запустите скрипт `/opt/aecaVa/scripts/backup.sh` с необходимыми параметрами (см. таблицу 21).
- При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.

Пример запуска скрипта `/opt/aecaVa/scripts/backup.sh` без параметров:

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

10.2 Расписание резервного копирования

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

Выполните переход в режим редактирования crontab выполнив с правами суперпользователя команду:

```
nano /etc/crontab
```

Укажите время и период запуска сценариев создания резервных копий:

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

где:

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

Выход и сохранение из редактора расписания осуществляется командой:

```
:wq!
```

Для просмотра настроенного расписания используйте команду:

```
crontab -l
```

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

10.3 Восстановление данных из резервной копии

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

Параметры запуска скрипта `/opt/aecaVa/scripts/restore.sh` представлены в таблице 22.

Таблица 22 — Параметры запуска скрипта `/opt/aecaVa/scripts/restore.sh`

Параметр	Описание
`--backup путь_к_файлу_резервной копии`	Параметр позволяет передать путь к резервной копии при запуске скрипта
`-B путь_к_файлу_резервной копии`	Параметр позволяет передать путь к резервной копии при запуске скрипта. Параметр `-B` аналогичен параметру `--backup`
`-nodb`	При указании параметра скрипт не восстанавливает базу данных из резервной копии
`--dbuser имя_пользователя_СУБД`	см. описание параметра `use_credentials_from_config` в 4.2
`-U имя_пользователя_СУБД`	То же, что `--dbuser имя_пользователя_СУБД`
`--dbpass пароль_пользователя_СУБД`	см. описание параметра `use_credentials_from_config` в 4.2
`-P пароль_пользователя_СУБД`	То же, что `--dbpass пароль_пользователя_СУБД`

Для восстановления данных из резервной копии:

- Запустите скрипт `/opt/aecaVa/scripts/restore.sh` с необходимыми параметрами (см. таблицу 22).

- При необходимости укажите в диалоге:
  - имя и пароль пользователя СУБД (см. описание параметра `use_credentials_from_config` в 4.2).
  - путь к резервной копии.

  Пример запуска скрипта `/opt/aecaVa/scripts/restore.sh` без параметров:

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

11 ОБНОВЛЕНИЕ ПРОГРАММЫ

11.1 Назначение обновлений

Обновление базы данных и модулей eCA-VA 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 ведёт учёт покупателей eCA-VA.
Выполняется регистрация следующей информации:

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

Уведомление пользователей о выпуске обновлений eCA-VA выполняется путем публикации информации на официальном сайте АО «Аладдин Р.Д.» и (или) с использованием рассылки электронных почтовых сообщений на электронные адреса потребителей. Рассылка может происходить за счёт применения средств, обеспечивающих доведение уведомлений до потребителя автоматически. Вместе с файлом обновлений может предоставляться обновлённая документация для использования программы.

11.3 Получение обновлений потребителем

Получение файлов обновлений программного средства и соответствующих им контрольных сумм возможно:

- с использованием электронной почты;
- путём загрузки с веб-сайта АО «Аладдин Р.Д.».

Проверка квалифицированной электронной подписи изготовителя (производителя) 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 файлов для обновления программы выполняется путем расчета КС полученных установочных пакетов (дистрибутивов) с использованием предварительно установленного программного обеспечения «ФИКС-Unix 1.0» или программного средства «Утилита контроля целостности 2.0» из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition», и её сравнением со значением контрольной суммы для этого обновления (см. подраздел 1.5.2 документа «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).

11.5 Установка обновлений

На случай, если во время обновления произойдёт сбой, рекомендуем предварительно сделать резервную копию программы и базы данных (см. 10).

Для обновления продукта:

- перенесите дистрибутив с обновлённой версией компонента на сервер с установленным eCA-VA любым удобным способом;

- проверьте целостность дистрибутива путём подсчёта контрольной суммы;
- выполните распаковку инсталляционного комплекта командой с правами суперпользователя:

РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	`dnf install aeca-*.rpm`
Astra Linux SE	`dpkg -i aeca-*.deb`
Альт Сервер	`apt-get install aeca-*.rpm`

- запустите установку продукта в режиме обновления выполнив с правами суперпользователя команду:

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

- при необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД;
- установщик обнаружит установленную версию функционального 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 кеш-память браузера;
- запустите обновлённый eCA-VA;
- проверьте версию обновлённого eCA-VA в окне «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 ПРОГРАММЫ

Для инициализации процесса удаления:

1. Выполните с правами суперпользователя команду:

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

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

В результате выполнения данного действия будут полностью удалены:

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

База данных удалена не будет, но при повторной установке изменения в базе будут стёрты.
Все внесённые изменения будут выведены в консоль.
Удаление пакета повлечёт за собой удаление установочного комплекта в каталоге `/opt/aecaVa/`.

- Для удаления необходимо выполнить с правами суперпользователя следующую команду:

РЕД ОС РОСА «ХРОМ» 12 Сервер и SberLinux OS Server	`dnf remove aeca-*.rpm`
Astra Linux SE	`apt remove aeca-*.deb`
Альт Сервер	`apt-get remove aeca-*.rpm`

13 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

13.1 Удаление БД «aecava»

Для удаления ранее созданной базы данных «aecava» (имя БД, заданное по умолчанию) необходимо выполнить команду `drop database aecava;` с правами суперпользователя.

13.2 Удаление пользователя БД «aeca»

Для удаления ранее созданного пользователя базы данных «aeca» необходимо выполнить команды с правами суперпользователя:

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

```
-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 с правами суперпользователя команду:

```
systemctl restart postgresql
```

14 МИГРАЦИЯ С ВЕРСИИ ПРОГРАММЫ 1.2 НА ВЕРСИЮ 2.4

14.1 Начальное состояние

Установлен eCA-VA 1.2.

14.2 Цель

На том же сервере, где ранее был развернут eCA-VA версии 1.2, развернуть eCA-VA версии 2.4 и обеспечить проксирование запросов к старым URL CDP и OCSP на новые URL CDP и OCSP от eCA-VA версии 2.4.

14.3 Рекомендации

В ходе миграции eCA-VA версии 1.2 будет удалён. До полного завершения сценария миграции проверка сертификатов по указанных в них URL CRL DP и OCSP eCA-VA версии 1.2 будет недоступна. Рекомендуется выполнять миграцию во время минимальной нагрузки, а также уведомить пользователей о возможных проблемах при проверке статусов их сертификатов.

При этом, если eCA-VA версии 1.2 использовался в кластерной конфигурации, указанные выше ограничения не повлияют на проверку статусов сертификатов при выполнении миграции на узлах кластера последовательно (в соответствии планом миграции далее), так как во время выполнения сценария узлы, на которых миграция ещё не выполнялась, продолжат обрабатывать запросы по URL от eCA-VA версии 1.2.

Если миграция по какой-либо причине не будет выполнена, то при одновременном использовании eCA-VA версии 1.2 и версии 2.4 рекомендуется отключить запись точек распространения и служб OCSP от eCA-VA версии 1.2 в выпускаемые сертификаты, обеспечивая таким образом постепенный переход на eCA-VA версии 2.4. Такая возможность доступна в разделе «Центры валидации» программы. Это необходимо сделать для всех eCA-CA, которые обслуживает данный eCA-VA версии 1.2. Работоспособность eCA-VA 1.2 при отказе от миграции необходимо будет сохранить до истечения срока действия последнего выпущенного сертификата, содержащего URL точек распространения и служб OCSP от данного eCA-VA 1.2.

14.4 План миграции №1[1]

Порядок миграции eCA-VA версии 1.2 на версию 2.4:

1. Составьте список издателей (ЦС). Сохраните URL распространения CRL, Delta CRL (при наличии), AIA и служб OCSP (при наличии) ЦВ для данных ЦС. Сохраните идентификаторы ЦС.
   Примечание - Сценарий, при котором ЦС принадлежат разным экземплярам eCA-CA, не блокирует процесс миграции.
   Пример: eCA-VA версии 1.2 зарегистрирован в одном ЦС eCA-CA. Сведения о ЦВ:
   - URL распространения CRL: http://va.eca.domain.ru:8080/aecaCdp/api/v2/crl/get-crl/3
   - URL распространения Delta CRL: http://va.eca.domain.ru:8080/aecaCdp/api/v2/crl/get-delta-crl/3
   - URL AIA: http://va.eca.domain.ru:8080/aecaCdp/api/v2/aia/get-aia/3
   - URL OCSP: http://va.eca.domain.ru:8080/aeca-va/ocsp
   - Идентификатор ЦВ: 2bf441c6-52f7-4204-b6f2-338c5edba38f
2. Если eCA-VA версии 1.2 был развернут в виртуальной среде, рекомендуется при наличии возможности сделать снимок состояния виртуальной машины.
3. Обновите все экземпляры eCA-CA до версии 2.4, в ЦС которых зарегистрирован eCA-VA версии 1.2 (см. раздел 12 документа «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
4. Удалите во всех экземплярах eCA-CA ЦВ, в ЦС которых зарегистрирован eCA-VA версии 1.2 (см. раздел 7.10.4 документа «Aladdin Enterprise Certificate Authority Certified Edition.

[1] В Центре валидации Aladdin eVA версии 1.2 служба OCSP была создана только для одного Центра сертификации.

Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).

5. Удалите eCA-VA версии 1.2 (см. раздел 12 настоящего руководства администратора).
6. Выполните установку eCA-VA версии 2.4 в соответствии с настоящим руководством администратора (см. разделы 3 и 4).
7. В eCA-VA версии 2.4 создайте подключения ко всем экземплярам eCA-CA, в ЦС которых ранее был зарегистрирован eCA-VA версии 1.2 (см. раздел 7.3.8 настоящего руководства администратора).
8. В eCA-VA версии 2.4 создайте ЦВ для всех ЦС, в которых ранее был зарегистрирован eCA-VA версии 1.2 (см. раздел 7.2.2).

   Примечания:

   1 Если ЦС принадлежат к разным экземплярам eCA-CA, создавать ЦВ необходимо под учётной записью пользователя с ролью «Администратор», созданной в соответствующем экземпляре eCA-CA.

   2 В ходе создания ЦВ создайте службу OCSP, если она ранее использовалась для ЦС.
9. В конфигурационном файле используемого веб-сервера для каждого URL распространения CRL и Delta CRL (при наличии), URL AIA и службы OCSP (при наличии) ЦВ eCA-VA версии 1.2 (URL сохранены на шаге 1 настоящего сценария) укажите пути проксирования к соответствующим URL ЦВ eCA-VA версии 2.4.

   9.1. Порядок действий для веб-серверов **Nginx** и **Cpnginx**

   Создайте конфигурационный файл **proxy.conf** в любом каталоге ОС (в дальнейшем не допускается перемещение данного файла).

   Перед указанием путей проксирования необходимо указать директиву **listen 8080**, которая определяет порт, на котором веб-сервер будет принимать HTTP-запросы от клиентов (порт 8080 использовался в eCA-VA версии 1.2).

   Формат указания пути проксирования URL:

```
location [URL без доменного имени и порта]{
proxy_pass http://[доменное имя Aladdin eVA]/validation-authority-
service/api/v2/public/validation-authorities/[идентификатор ЦВ]/
[тип распространяемых данных или службы];
}
```

   Пример содержания конфигурационного файла **proxy.conf** веб-сервера (URL взяты из примера, приведенного на шаге 1 настоящего сценария):

```
listen 8080;

# Путь проксирования к URL распространения CRL
location /aecaCdp/api/v2/crl/get-crl/3 {
proxy_pass http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/cdp/crl;
}
# Путь проксирования к URL распространения DELTA CRL
```

```
location /aecaCdp/api/v2/crl/get-delta-crl/3 {
proxy_pass http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/cdp/delta-crl;
}
# Путь проксирования к URL AIA
location /aecaCdp/api/v2/aia/get-aia/3 {
proxy_pass http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/aia;
```

```
}
# Путь проксирования к URL службы OCSP
location /aeca-va/ocsp {
proxy_pass http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/ocsp/engine;
}
```

Добавьте символическую ссылку на файл **proxy.conf** в каталог **/opt/aecaVa/dist/webserver/aeca-va-configs/http** под именем **proxy** выполнив следующую команду с правами суперпользователя:

```
ln -s [путь к конфигурационному файлу]/proxy.conf
/opt/aecaVa/dist/webserver/aeca-va-configs/http/proxy
```

Перезапустите веб-сервер выполнив следующую команду с правами суперпользователя:

- systemctl restart nginx - для веб-сервера Nginx
- systemctl restart cpnginx - для веб-сервера Cpnginx

Внимание! В связи с особенностями работы веб-серверов Nginx и Cpnginx создание символической ссылки и перезапуск веб-сервера необходимо выполнять после каждого обновления конфигурации (запуска скрипта install.sh в режимах «Update» и «Upgrade»).

9.2. Порядок действий для веб-сервера **Apache**

В зависимости от ОС среды функционирования конфигурационный файл расположен по пути **/etc/apache2/apache2.conf** или **/etc/httpd/conf/httpd.conf**.

Формат указания пути проксирования URL:

```
ProxyPass [URL без доменного имени и порта]
http:// [доменное имя Aladdin eVA]/validation-authority-
service/api/v2/public/validation-authorities/[идентификатор ЦВ]/
[тип распространяемых данных или службы]
ProxyPassReverse [URL без доменного имени и порта]
http://[доменное имя Aladdin eVA]/validation-authority-
service/api/v2/public/validation-authorities/[идентификатор ЦВ]/
[тип распространяемых данных или службы]
```

Пример содержания конфигурационного файла веб-сервера (URL взяты из примера, приведенного на шаге 1 настоящего сценария):

```
IfModule mod_proxy.c>
ProxyPreserveHost On
# Путь проксирования к URL распространения CRL
ProxyPass /aecaCdp/api/v2/crl/get-crl/3
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/cdp/crl

ProxyPassReverse /aecaCdp/api/v2/crl/get-crl/3
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/cdp/crl
# Путь проксирования к URL распространения DELTA CRL
ProxyPass /aecaCdp/api/v2/crl/get-delta-crl/5
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
```

```
338c5edba38f/cdp/delta-crl

ProxyPassReverse /aecaCdp/api/v2/crl/get-delta-crl/5
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/cdp/delta-crl
# Путь проксирования к URL AIA
ProxyPass /aecaCdp/api/v2/aia/get-aia/3
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/aia

ProxyPassReverse /aecaCdp/api/v2/aia/get-aia/3
http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/aia
# Путь проксирования к URL службы OCSP
ProxyPass /aeca-va/ocsp http://va.eca.domain.ru/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/ocsp/engine

ProxyPassReverse /aeca-va/ocsp http://va.eca.domain.ru/validation-
authority-service/api/v2/public/validation-authorities/2bf441c6-52f7-
4204-b6f2-338c5edba38f/ocsp/engine
```

Перезапустите веб-сервер, в зависимости от установленной ОС выполнив одну из следующих команд с правами суперпользователя:

- `systemctl restart apache2`;
- `systemctl restart httpd`.

10. Выполните проверку результатов миграции. Убедитесь в доступности точек распространения и службы OCSP (при наличии) по URL ЦВ eCA-VA версии 1.2.

14.5 План миграции №2[1]

1. Составьте список издателей (ЦС), в которых зарегистрирован eCA-VA версии 1.2. Сохраните URL распространения CRL, Delta CRL (при наличии), AIA и служб OCSP (при наличии) ЦВ для данных ЦС. Сохраните идентификаторы ЦС. Пример сохраненных данных представлен в разделе 13.4 настоящего рукосводства.
   Примечание - Сценарий, при котором ЦС принадлежат разным экземплярам eCA-CA, не блокирует процесс миграции.
2. Если eCA-VA версии 1.2 был развернут в виртуальной среде, рекомендуется при наличии возможности сделать снимок состояния виртуальной машины.
3. Обновите все экземпляры eCA-CA до версии 2.4, в ЦС которых зарегистрирован eCA-VA версии 1.2 (см. раздел 12 документа «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
4. Удалите во всех экземплярах eCA-CA ЦВ, в ЦС которых зарегистрирован eCA-VA версии 1.2 (см. раздел 7.10.4 документа «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 2. Функции управления Центра сертификации Aladdin Enterprise Certification Authority»).
5. Удалите eCA-VA версии 1.2 (см. раздел 12 настоящего руководства администратора).

[1] Служба OCSP была создана для нескольких Центров сертификации.

6. Выполните установку eCA-VA версии 2.4 в соответствии с настоящим руководством администратора (см. разделы 3 и 4).
7. В eCA-VA версии 2.4 создайте подключения ко всем экземплярам eCA-CA, в ЦС которых ранее был зарегистрирован eCA-VA версии 1.2 (см. раздел 7.3.8 настоящего руководства администратора).
8. В eCA-VA версии 2.4 создайте ЦВ для всех ЦС, в которых ранее был зарегистрирован eCA-VA версии 1.2 (см. раздел 7.3.8).

   Примечания:

   1 Если ЦС принадлежат к разным экземплярам eCA-CA, создавать ЦВ необходимо под учётной записью пользователя с ролью «Администратор», созданной в соответствующем экземпляре eCA-CA.

   2 В ходе создания ЦВ создайте службу OCSP, если она ранее использовалась для ЦС.
9. Установите на сервер, где развернут eCA-VA, средство балансирования нагрузки HAProxy, и отредактируйте конфигурационный файл согласно примеру[1], приведенному ниже:[2]

```
global
    log /dev/log local0 debug
    tune.bufsize 32768


defaults
    mode http
    timeout connect 5s
    timeout client 30s
    timeout server 30s
    option httplog
frontend ocsp_reader
    bind *:8080
    # В строке выше указывается порт, по которому осуществлялся доступ к eCA-VA 1.2. По умолчанию использовался 8080 порт.
    log global
    option http-buffer-request
    acl is_ocsp path_beg /aeca-va/ocsp
    acl redirect_ocsp1 req.payload(0,0),hex -m sub 6471CD0F3B304DEED6E92F2CC388EDF2037924C6
    #В строке выше вместо "6471CD0F3B304DEED6E92F2CC388EDF2037924C6" нужно указать SKI (идентификатор ключа ЦС) первого ЦС (ЦС1) ОБЯЗАТЕЛЬНО в верхнем регистре
    acl redirect_ocsp2 req.payload(0,0),hex -m sub 01D6EA7DC0C57BA447627D4166C47169187C8C1C
    #В строке выше вместо "6471CD0F3B304DEED6E92F2CC388EDF2037924C6" нужно указать SKI (идентификатор ключа ЦС) второго ЦС (ЦС2) ОБЯЗАТЕЛЬНО в верхнем регистре
    acl is_crl1 path_beg /aecaCdp/api/v2/crl/get-crl/3
    #В строке выше необходимо указать путь к точке распространения CRL ЦС1 в eCA-VA 1.2
    acl is_delta_crl1 path_beg /aecaCdp/api/v2/crl/get-delta-crl/3
```

[1] В примере представлена настойка проксирования для двух служб OCSP разных Центров сертификации.

```
    #В строке выше необходимо указать путь к точке распространения DELTA CRL ЦС1 в
eCA-VA 1.2
    acl is_aia1 path_beg /aecaCdp/api/v2/aia/get-aia/3
    #В строке выше необходимо указать путь к точке распространения AIA ЦС1 в eCA-VA
1.2
    acl is_crl2 path_beg /aecaCdp/api/v2/crl/get-crl/5
    #В строке выше необходимо указать путь к точке распространения CRL ЦС2 в eCA-VA
1.2
    acl is_delta_crl2 path_beg /aecaCdp/api/v2/crl/get-delta-crl/5
    #В строке выше необходимо указать путь к точке распространения DELTA CRL ЦС2 в
eCA-VA 1.2
    acl is_aia2 path_beg /aecaCdp/api/v2/aia/get-aia/5
    #В строке выше необходимо указать путь к точке распространения AIA ЦС2 в eCA-VA
1.2
    use_backend ocsp1 if redirect_ocsp1 is_ocsp
    use_backend ocsp2 if redirect_ocsp2 is_ocsp
    use_backend crl1 if is_crl1
    use_backend deltacrl1 if is_delta_crl1
    use_backend aia1 if is_aia1
    use_backend crl2 if is_crl2
    use_backend deltacrl2 if is_delta_crl2
    use_backend aia2 if is_aia2
    option forwardfor

backend ocsp1
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/db995074-9edb-4498-84d4-7950311145a8/ocsp/engine
    #В строке выше необходимо указать URL службы OCSP, которая обслуживает ЦС1
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA 2.4
    server ocsp01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA 2.4

backend ocsp2
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/71543360-cc9b-417e-b9e7-5b18bf2e15a0/ocsp/engine
    #В строке выше необходимо указать URL службы OCSP, которая обслуживает ЦС2
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA 2.4
    server ocsp02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA 2.4

backend crl1
```

```
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/db995074-9edb-4498-84d4-7950311145a8/cdp/crl
    #В строке выше необходимо указать URL точки распространения CRL ЦС1
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA 2.4
    server crl01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA 2.4

backend deltacrl1
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/db995074-9edb-4498-84d4-7950311145a8/cdp/delta-crl
    #В строке выше необходимо указать URL точки распространения DELTA CRL ЦС1
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA 2.4
    server deltacrl01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA 2.4

backend aia1
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/db995074-9edb-4498-84d4-7950311145a8/aia
    #В строке выше необходимо указать URL точки распространения AIA ЦС1
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA2.x
    server aia01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA2.x

backend crl2
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/71543360-cc9b-417e-b9e7-5b18bf2e15a0/cdp/crl
    #В строке выше необходимо указать URL точки распространения CRL ЦС2
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA2.x
    server crl02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA2.x

backend deltacrl2
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/71543360-cc9b-417e-b9e7-5b18bf2e15a0/cdp/delta-crl
    #В строке выше необходимо указать URL точки распространения DELTA CRL ЦС2
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA2.x
    server deltacrl02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA2.x
```

```
backend aia2
    http-request set-path /validation-authority-service/api/v2/public/validation-
authorities/71543360-cc9b-417e-b9e7-5b18bf2e15a0/aia
    #В строке выше необходимо указать URL точки распространения AIA ЦС2
    http-request set-header Host aecava
    #В строке выше вместо "aecava" необходимо указать имя хоста eCA-VA2.x
    server aia02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт eCA-VA2.x
```

10. Выполните проверку результатов миграции. Убедитесь в доступности точек распространения и служб OCSP по URL ЦВ eCA-VA версии 1.2.

15 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

<table>
<tr><th>Проблема</th><th>Возможная причина</th><th>Способы решения</th></tr>
<tr><td>Ошибка при запуске скрипта установки <code>install.sh</code> «error obtaining MAC configuration for user «имя пользователя СУБД»» в ОС Astra Linux Special Edition 1.8</td><td>Не выполнена дополнительная настройка пользователя СУБД для поддержки работы с активным механизмом МРД</td><td>Выполнить настройку пользователя СУБД для поддержки работы с активным механизмом МРД в соответствии с инструкциями подраздела 4.4 (в зависимости от использованного способа создания пользователя СУБД) и перезапустить скрипт установки <code>install.sh</code>.</td></tr>
<tr><td rowspan="2">Прекращение установки ПО или обновления eCA-VA</td><td>1. Нехватка аппаратных ресурсов</td><td>Произведите оценку ресурса вашего ПК в соответствии с требованием к аппаратным ресурсам, указанным в первой части Руководства администратора</td></tr>
<tr><td colspan="2">2. Не корректная установка или отсутствие программного компонента, указанного в требовании Проверьте наличие установленного ПО согласно разделу 3 Руководство администратора.

Также проверьте и при необходимости переключите текущую версию java-компонентов выполнив с правами суперпользователя команды:

<code>update-alternatives --config java</code>
<code>update-alternatives --config javac</code>
<code>update-alternatives --config javap</code></td></tr>
<tr><td rowspan="3">Нет подключения к ресурсной системе</td><td>1. Включён протокол TLS</td><td>Измените настройку конфигурационного файла контроллера домена <code>/etc/samba/smb.conf</code>, добавив в раздел <code>[global]</code>:

<code>ldap server require strong auth = no</code></td></tr>
<tr><td>2. Проверить подключение к контроллеру домена Samba</td><td>Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:

- получение списка пользователей

<code>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=user)"</code>

- получение списка компьютеров

<code>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=computer)"</code>

- получение списка групп безопасности

<code>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC= pki-test " -H "ldap://192.168.111.148" "(objectCategory=group)"</code>

где:

<code>Administrator@pki-test.local</code> - имя администратора домена;

<code>Qwerty1234</code> - пароль администратора домена;

<code>pki-test, pki-test</code> - доменное имя;

<code>192.168.111.148</code> - ip-адрес контроллера домена.

В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.</td></tr>
<tr><td>3. Проверить подключение к контроллеру домена ALD PRO</td><td>Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:

- получение списка пользователей

<code>ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w</code></td></tr>
</table>

Проблема	Возможная причина	Способы решения

		`"Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=x-ald-user)"`
		- получение списка компьютеров
		`ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=nshost)"`
		- получение списка групп безопасности
		`ldapsearch -D "uid=admin,cn=users,cn=accounts,dc=domain,dc=local" -w "Qwerty1234" -b "dc=domain,dc=local" -H "ldap://192.168.0.10" "(objectclass=ipausergroup)"`
		где:
		`admin` - имя администратора домена;
		`users`, `accounts`
		`Qwerty1234` - пароль администратора домена;
		`domain, local` - доменное имя;
		`192.168.111.148` - ip-адрес контроллера домена.
		В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.

Вход в интерфейс eCA-VA с выпущенным сертификатом невозможен в браузере Chromium	Браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой браузер
Вход в интерфейс eCA-VA невозможен в браузере Firefox. Ошибка SEC_ERROR_BAD_SIGNATURE	Проблема возникает при наличии в хранилище сертификатов ОС сертификата ЦС с аналогичным SDN издателю сертификата веб-сервера. Она связана с алгоритмом проверки сертификата веб-сервера браузером Firefox для решения уязвимости, связанной с подлогом серверного сертификата: 1. Firefox получает сертификат веб-сервера от сервера 2. После этого выполняет поиск в хранилище сертификатов ОС сертификата ЦС по SDN издателя сертификата 3. И далее выполняет проверку цепочки по открытым ключам	1. Проверьте состав сертификатов доверенных ЦС в хранилище ОС 2. В случае несоответствия установите сертификат издателя сертификата веб-сервера
Периодическая остановка или падение службы aeca-va.service	Недостаток оперативной памяти	1. Проверьте потребление оперативной памяти на хосте с помощью команды `top`: - в `MiB Mem` значение `total` - это общий объем оперативной памяти; - в `MiB Mem` значение `free` - это свободная оперативная память; - в строке таблицы `USER=aeca` значение в колонке `RES` - это потребляемая ЦВ оперативная память. Для корректной работы ЦВ сумма `free` и `RES` должна быть не менее 8 Гб (см. 2.2). 2. Если полученное значение меньше 8 Гб, то при исчерпании свободной оперативной памяти `oom-killer` останавливает ЦВ.

Проблема	Возможная причина	Способы решения
		В данном случае рекомендуется проанализировать состав стороннего ПО на хосте и его потребление памяти, например, с помощью команд `top` или `htop`. 3. После этого следует либо добавить необходимое количество оперативной памяти, либо удалить с хоста стороннее ПО, освободив этим оперативную память. В итоге для ЦВ должно быть доступно не менее 8 Гб оперативной памяти (см. 2.2).

16 ОПИСАНИЕ МЕТОДОВ REST API

16.1 Методы получения информации о сервисах

16.1.1 Методы получения информации о сервисе безопасности (security-service)

16.1.1.1 Метод получения эндпоинтов для запроса информации о сервисе безопасности (security-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе безопасности	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – security-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/security-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/security-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/security-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/security-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/security-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.1.2 Метод получения информации о состоянии сервиса безопасности (security-service)

GET – Получение информации о состоянии сервиса безопасности	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – security-service/actuator/health	
Swagger: -	
Query –	

Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.1.3 Метод получения информации о сервисе безопасности (security-service)

GET – Получение информации о сервисе безопасности	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – security-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.1.4 Метод получения Prometheus-метрик сервиса безопасности (security-service)

GET – Получение Prometheus-метрик сервиса безопасности	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – security-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.2 Методы получения информации о сервисе журнала событий (logs-service)

16.1.2.1 Метод получения эндпоинтов для запроса информации о сервисе журнала событий (logs-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе журнала событий
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.

URL – logs-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/logs-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/logs-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/logs-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/logs-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/logs-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.2.2 Метод получения информации о состоянии сервиса журнала событий (logs-service)

GET – Получение информации о состоянии сервиса журнала событий	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – logs-service/actuator/health	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.2.3 Метод получения информации о сервисе журнала событий (logs-service)

GET – Получение информации о сервисе журнала событий
Метод по умолчанию доступен неаутентифицированному пользователю.

В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – logs-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.2.4 Метод получения Prometheus-метрик сервиса журнала событий (logs-service)

GET – Получение Prometheus-метрик сервиса журнала событий	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – logs-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.3 Методы получения информации о сервисе интеграции с центром сертификации (ca-adapter-service)

16.1.3.1 Метод получения эндпоинтов для запроса информации о сервисе интеграции с центром сертификации (ca-adapter-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе интеграции с центром сертификации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – ca-adapter-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/ca-adapter-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	

"href": "http://HOST/ca-adapter-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/ca-adapter-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/ca-adapter-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/ca-adapter-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.3.2 Метод получения информации о состоянии сервиса интеграции с центром сертификации (ca-adapter-service)

GET – Получение информации о состоянии сервиса интеграции с центром сертификации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – ca-adapter-service/actuator/health	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.3.3 Метод получения информации о сервисе интеграции с центром сертификации (ca-adapter-service)

GET – Получение информации о сервисе интеграции с центром сертификации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – ca-adapter-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса

}	
}	

16.1.3.4 Метод получения Prometheus-метрик сервиса интеграции с центром сертификации (ca-adapter-service)

GET – Получение Prometheus-метрик сервиса интеграции с центром сертификации	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – ca-adapter-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.4 Методы получения информации о сервисе валидации (validation-authority-service)

16.1.4.1 Метод получения эндпоинтов для запроса информации о сервисе валидации (validation-authority-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе валидации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – validation-authority-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/validation-authority-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/validation-authority-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/validation-authority-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/validation-authority-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	

"prometheus": {	
"href": "http://HOST/validation-authority-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.4.2 Метод получения информации о состоянии сервиса валидации (validation-authority-service)

GET – Получение информации о состоянии сервиса валидации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – validation-authority-service/actuator/health	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.4.3 Метод получения информации о сервисе валидации (validation-authority-service)

GET – Получение информации о сервисе валидации	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – validation-authority-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.4.4 Метод получения Prometheus-метрик сервиса валидации (validation-authority-service)

GET – Получение Prometheus-метрик сервиса валидации
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.
URL – validation-authority-service/actuator/prometheus
Swagger: -
Query -

Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.5 Методы получения информации о сервисе настроек (settings-service)

16.1.5.1 Метод получения эндпоинтов для запроса информации о сервисе настроек (settings-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе настроек	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – settings-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/settings-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/settings-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/settings-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/settings-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/settings-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.5.2 Метод получения информации о состоянии сервиса настроек (settings-service)

GET – Получение информации о состоянии сервиса настроек	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – settings-service/actuator/health	
Swagger: -	
Query –	

Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.5.3 Метод получения информации о сервисе настроек (settings-service)

GET – Получение информации о сервисе настроек	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – settings-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.5.4 Метод получения информации о сервисе настроек (settings-service)

GET – Получение Prometheus-метрик сервиса настроек	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – settings-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.6 Методы получения информации о сервисе хранения данных (storage-service)

16.1.6.1 Метод получения эндпоинтов для запроса информации о сервисе хранения данных (storage-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе хранения данных
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.
URL – storage-service/actuator
Swagger: -

Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/storage-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/storage-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health-path": {	
"href": "http://HOST/storage-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/storage-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/storage-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.6.2 Метод получения информации о состоянии сервиса хранения данных (storage-service)

GET – Получение информации о состоянии сервиса хранения данных	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – storage-service/actuator/health	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.6.3 Метод получения информации о сервисе хранения данных (storage-service)

GET – Получение информации о сервисе хранения данных
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.
URL – storage-service/actuator/info

Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.6.4 Метод получения Prometheus-метрик сервиса хранения данных (storage-service)

GET – Получение Prometheus-метрик сервиса хранения данных	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – storage-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

16.1.7 Методы получения информации о сервисе внешних интеграций (external-integration-service)

16.1.7.1 Метод получения эндпоинтов для запроса информации о сервисе внешних интеграций (external-integration-service)

GET – Получение списка доступных эндпоинтов для запроса информации о сервисе внешних интеграций	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – external-integration-service/actuator	
Swagger: -	
Query –	
Request –	
Response	Ответ JSON в HTTP-body
{	
"_links": {	
"self": {	
"href": "http://HOST/external-integration-service/actuator",	URL эндпоинта, который возвращает эндпоинты для запроса информации о сервисе, где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"health": {	
"href": "http://HOST/external-integration-service/actuator/health",	URL эндпоинта, который возвращает информацию о состоянии сервиса (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL

},	
"health-path": {	
"href": "http://HOST/external-integration-service/actuator/health/{*path}",	URL зарезервированного эндроинта под будущие реализации
"templated": true	Флаг наличия переменной в URL
},	
"info": {	
"href": "http://HOST/external-integration-service/actuator/info",	URL эндпоинта, который возвращает информацию о сервисе (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
},	
"prometheus": {	
"href": "http://HOST/external-integration-service/actuator/prometheus",	URL эндпоинта, который возвращает метрики сервиса в формате Prometheus (подробнее см. ниже), где HOST – адрес хоста eCA-VA
"templated": false	Флаг наличия переменной в URL
}	
}	
}	

16.1.7.2 Метод получения информации о состоянии сервиса внешних интеграций (external-integration-service)

GET – Получение информации о состоянии сервиса внешних интеграций	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – external-integration-service/actuator/health	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
status (enum: UP, DOWN, OUT_OF_SERVICE, UNKNOWN)	Статус (состояние) сервиса безопасности. Возможные значения: - UP – работает; - DOWN – не работает; - OUT_OF_SERVICE – выключен; - UNKNOWN – нет информации.
}	

16.1.7.3 Метод получения информации о сервисе внешних интеграций (external-integration-service)

GET – Получение информации о сервисе внешних интеграций	
Метод по умолчанию доступен неаутентифицированному пользователю. В конфигурационном файле имеется возможность отключения доступа неаутентифицированному пользователю.	
URL – external-integration-service/actuator/info	
Swagger: -	
Query –	
Request –	
Response {	Ответ JSON в HTTP-body
"application": {	
name (string)	Название сервиса
version (string)	Версия сервиса
}	
}	

16.1.7.4 Метод получения Prometheus-метрик сервиса внешних интеграций (external-integration-service)

GET – Получение Prometheus-метрик сервиса внешних интеграций	
Доступность метода для неаутентифицированного пользователя зависит от значения параметра «actuator_authenticate» конфигурационного файла: • если параметр имеет значение «true», доступ к методу будет разрешен только аутентифицированным пользователям; • если параметр имеет значение «false» (по умолчанию), доступ к методу будет разрешен без аутентификации.	
URL – external-integration-service/actuator/prometheus	
Swagger: -	
Query -	
Request -	
Response	
Метод возвращает метрики сервиса в формате Prometheus (text/plain)	

17 ОПИСАНИЕ PROMETHEUS-МЕТРИК СЕРВИСОВ

17.1 Базовые метрики сервиса

17.1.1 Время запуска:

- application_ready_time_seconds{main_application_class="..."} gauge. Время, за которое сервис стал готов обслуживать запросы (в секундах). Метка «main_application_class» содержит имя основного класса сервиса.
- application_started_time_seconds{main_application_class="..."} gauge. Время, затраченное на запуск сервиса (в секундах). Метка «main_application_class» содержит имя основного класса сервиса.

17.2 Метрики диска:

- disk_free_bytes{path="..."} gauge. Свободное место на диске, в котором располагается сервис (в байтах). Метка «path» указывает путь к сервису в файловой системе.
- disk_total_bytes{path="..."} gauge. Общий объем диска, в котором располагается сервис (в байтах). Метка «path» указывает путь к сервису в файловой системе.

17.3 Метрики исполнителей (Thread Pools)

17.3.1 taskExecutor (пул асинхронных задач):

- executor_active_threads{name="taskExecutor"} gauge. Количество потоков, прямо сейчас выполняющих задачи.
- executor_completed_tasks_total{name="taskExecutor"} counter. Сколько задач уже выполнено с момента запуска.
- executor_pool_core_threads{name="taskExecutor"} gauge. Минимальное количество потоков, которое пул старается поддерживать.
- executor_pool_max_threads{name="taskExecutor"} gauge. Максимальное количество потоков, которое может быть создано.
- executor_pool_size_threads{name="taskExecutor"} gauge. Сколько потоков сейчас существует в пуле.
- executor_queue_remaining_tasks{name="taskExecutor"} gauge. Количество свободных мест в очереди задач без блокировки.
- executor_queued_tasks{name="taskExecutor"} gauge. Количество задач, ожидающих в очереди на выполнение.

17.3.2 taskScheduler (пул планировщика задач):

- executor_active_threads{name="taskScheduler"} gauge. Количество потоков, прямо сейчас выполняющих запланированные задачи.
- executor_completed_tasks_total{name="taskScheduler"} counter. Общее количество уже завершенных запланированных задач.
- executor_pool_core_threads{name="taskScheduler"} gauge. Базовый (core) размер пула потоков.
- executor_pool_max_threads{name="taskScheduler"} gauge. Максимально допустимый размер пула.
- executor_pool_size_threads{name="taskScheduler"} gauge. Текущее количество потоков в пуле.
- executor_queue_remaining_tasks{name="taskScheduler"} gauge. Количество свободных мест в очереди запланированных задач.
- executor_queued_tasks{name="taskScheduler"} gauge. Количество задач, ожидающих в очереди на выполнение.

17.4 Метрики пула подключений к БД (HikariCP)

17.4.1 Основные метрики пула:

- hikaricp_connections{pool="..."} gauge. Общее количество подключений в пуле.
- hikaricp_connections_acquire_seconds_count{pool="..."} counter. Количество операций получения подключения из пула.
- hikaricp_connections_acquire_seconds_sum{pool="..."} counter. Суммарное время получения подключений (в секундах).
- hikaricp_connections_acquire_seconds_max{pool="..."} gauge. Максимальное время получения подключения (в секундах).
- hikaricp_connections_active{pool="..."} gauge. Количество активных подключений.
- hikaricp_connections_creation_seconds_count{pool="..."} counter. Количество созданных подключений.
- hikaricp_connections_creation_seconds_sum{pool="..."} counter. Суммарное время создания подключений (в секундах).
- hikaricp_connections_creation_seconds_max{pool="..."} gauge. Максимальное время создания подключения (в секундах).
- hikaricp_connections_idle{pool="..."} gauge. Количество простаивающих подключений.
- hikaricp_connections_max{pool="..."} gauge. Максимальный размер пула.
- hikaricp_connections_min{pool="..."} gauge. Минимальный размер пула.
- hikaricp_connections_pending{pool="..."} gauge. Количество потоков, ожидающих подключение.
- hikaricp_connections_timeout_total{pool="..."} counter. Количество таймаутов при получении подключения.
- hikaricp_connections_usage_seconds_count{pool="..."} counter. Количество операций использования подключений.
- hikaricp_connections_usage_seconds_sum{pool="..."} counter. Суммарное время использования подключений (в секундах).
- hikaricp_connections_usage_seconds_max{pool="..."} gauge. Максимальное время использования одного подключения (в секундах).

17.5 Метрики HTTP-клиента

17.5.1 Активные клиентские запросы:

- http_client_requests_active_seconds_count{client_name="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Количество активных исходящих запросов.
- http_client_requests_active_seconds_sum{client_name="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Суммарное время активных исходящих запросов.
- http_client_requests_active_seconds_max{client_name="...", exception="...", method="...", outcome="...", status="...", uri="..."} gauge. Максимальное время активного исходящего запроса.

17.5.2 Завершенные клиентские запросы:

- http_client_requests_seconds_count{client_name="...", error="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Количество исходящих HTTP-запросов.
- http_client_requests_seconds_sum{client_name="...", error="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Суммарное время выполнения исходящих запросов (в секундах).
- http_client_requests_seconds_max{client_name="...", error="...", exception="...", method="...", outcome="...", status="...", uri="..."} gauge. Максимальное время выполнения исходящего запроса.

17.6 Метрики HTTP-сервера

17.6.1 Активные серверные запросы:

- http_server_requests_active_seconds_count{exception="...", method="...", outcome="...", status="...", uri="..."} counter. Количество активных входящих запросов.
- http_server_requests_active_seconds_sum{exception="...", method="...", outcome="...", status="...", uri="..."} counter. Суммарное время активных запросов.
- http_server_requests_active_seconds_max{exception="...", method="...", outcome="...", status="...", uri="..."} gauge. Максимальное время активного запроса.

17.6.2 Завершенные серверные запросы:

- http_server_requests_seconds_count{error="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Количество входящих HTTP-запросов.
- http_server_requests_seconds_sum{error="...", exception="...", method="...", outcome="...", status="...", uri="..."} counter. Суммарное время обработки входящих запросов (в секундах).
- http_server_requests_seconds_max{error="...", exception="...", method="...", outcome="...", status="...", uri="..."} gauge. Максимальное время обработки входящего запроса (в секундах).

17.7 JDBC-метрики (альтернативное представление HikariCP):

- jdbc_connections_active{name="dataSource"} gauge. Количество активных подключений.
- jdbc_connections_idle{name="dataSource"} gauge. Количество простаивающих подключений.
- jdbc_connections_max{name="dataSource"} gauge. Максимальный размер пула.
- jdbc_connections_min{name="dataSource"} gauge. Минимальный размер пула.

17.8 Метрики JVM (Java Virtual Machine)

17.8.1 Общая информация:

- jvm_info{runtime="...", vendor="...", version="..."} gauge. Информация о версии JVM (значение всегда 1, метки содержат детали).

17.8.2 Буферы:

- jvm_buffer_count_buffers{id="..."} gauge. Количество буферов в пуле. Метка id указывает тип буфера (direct или mapped).
- jvm_buffer_memory_used_bytes{id="..."} gauge. Память, используемая буферами (в байтах).
- jvm_buffer_total_capacity_bytes{id="..."} gauge. Общая емкость буферов (в байтах).

17.8.3 Классы:

- jvm_classes_loaded_classes gauge. Количество загруженных классов.
- jvm_classes_unloaded_classes_total counter. Общее количество выгруженных классов.

17.8.4 Компиляция:

- jvm_compilation_time_ms_total{compiler="..."} counter. Общее время, затраченное на JIT-компиляцию (в миллисекундах).

17.8.5 Сборка мусора:

- jvm_gc_live_data_size_bytes gauge. Размер данных в long-lived heap после последней сборки мусора.
- jvm_gc_max_data_size_bytes gauge. Максимальный размер "долгоживущей" области (Old Generation) в байтах.

- jvm_gc_memory_allocated_bytes_total counter. Объем памяти, выделенной в молодом поколении после сборки мусора.
- jvm_gc_memory_promoted_bytes_total counter. Объем памяти, продвинутой из молодого поколения в старое.
- jvm_gc_overhead gauge. Процент времени CPU, затраченного на сборку мусора (значение от 0 до 1).

17.8.6 Память (выделенная):

- jvm_memory_committed_bytes{area="...", id="..."} gauge. Объем памяти, гарантированно доступный JVM (в байтах). Метка area указывает область (heap или nonheap), метка id указывает конкретный пул памяти.

17.8.7 Память (максимальная):

- jvm_memory_max_bytes{area="...", id="..."} gauge. Максимальный объем памяти, который может использовать JVM (в байтах).

17.8.8 Память (после сборки мусора):

- jvm_memory_usage_after_gc{area="heap", pool="long-lived"} gauge. Процент использования long-lived области после последней сборки мусора (значение от 0 до 1).

17.8.9 Память (используемая):

- jvm_memory_used_bytes{area="...", id="..."} gauge. Используемая память (в байтах) по областям heap и non-heap.

17.8.10 Потоки:

- jvm_threads_daemon_threads gauge. Количество потоков-демонов.
- jvm_threads_live_threads gauge. Текущее количество живых потоков.
- jvm_threads_peak_threads gauge. Пиковое количество потоков с момента запуска.
- jvm_threads_started_threads_total counter. Общее количество запущенных потоков.
- jvm_threads_states_threads{state="..."} gauge. Количество потоков в каждом состоянии (runnable, waiting, timed-waiting, blocked, new, terminated).

17.9 Метрики логирования (Logback):

- logback_events_total{level="..."} counter. Количество событий лога по уровням: debug, error, info, trace, warn.

17.10 Метрики процесса:

- process_cpu_time_ns_total counter. Процессорное время, использованное процессом JVM (в наносекундах).
- process_cpu_usage gauge. Загрузка ЦП процессом JVM (значение от 0 до 1).
- process_files_max_files gauge. Максимальное количество файловых дескрипторов.
- process_files_open_files gauge. Количество открытых файловых дескрипторов.
- process_start_time_seconds gauge. Время запуска процесса в формате Unix timestamp.
- process_uptime_seconds gauge. Время работы процесса с момента запуска (в секундах).

17.11 Метрики Spring Data Repository:

- spring_data_repository_invocations_seconds_count{exception="...", method="...", repository="...", state="..."} counter. Количество вызовов методов репозиториев.

- spring_data_repository_invocations_seconds_sum{exception="...", method="...", repository="...", state="..."} counter. Суммарное время выполнения методов репозиториев (в секундах).
- spring_data_repository_invocations_seconds_max{exception="...", method="...", repository="...", state="..."} gauge. Максимальное время выполнения метода репозитория (в секундах).

17.12 Метрики безопасности (Spring Security)

17.12.1 Активная авторизация:

- spring_security_authorizations_active_seconds_count{spring_security_authentication_type="...", spring_security_authorization_decision="...", spring_security_object="..."} counter. Количество активных проверок авторизации.
- spring_security_authorizations_active_seconds_sum{...} counter. Суммарное время активных проверок (в секундах).
- spring_security_authorizations_active_seconds_max{...} gauge. Максимальное время активной проверки.

17.12.2 Завершенная авторизация:

- spring_security_authorizations_seconds_count{error="...", spring_security_authentication_type="...", spring_security_authorization_decision="...", spring_security_object="..."} counter. Количество проверок авторизации.
- spring_security_authorizations_seconds_sum{...} counter. Суммарное время проверок авторизации (в секундах).
- spring_security_authorizations_seconds_max{...} gauge. Максимальное время проверки авторизации.

17.12.3 Счетчики прохождения фильтров безопасности (часть 1):

- spring_security_filterchains_[FilterName]_after_total{security_security_reached_filter_section="after", spring_security_filterchain_position="...", spring_security_filterchain_size="...", spring_security_reached_filter_name="none"} counter. Количество запросов, прошедших после выполнения фильтра.
- spring_security_filterchains_[FilterName]_before_total{security_security_reached_filter_section="before", spring_security_filterchain_position="...", spring_security_filterchain_size="...", spring_security_reached_filter_name="none"} counter. Количество запросов, прошедших перед выполнением фильтра.

Примечание: [FilterName] заменяется на имя конкретного фильтра (например, AecaAuthenticationExceptionFilter, ApiKeyAuthenticationFilter, UserPrincipalAuthenticationFilter и др.). Набор фильтров зависит от конфигурации безопасности конкретного сервиса.

17.12.4 Активные фильтры безопасности:

- spring_security_filterchains_active_seconds_count{security_security_reached_filter_section="...", spring_security_filterchain_position="...", spring_security_filterchain_size="...", spring_security_reached_filter_name="..."} counter. Количество активных выполнений фильтров безопасности.
- spring_security_filterchains_active_seconds_sum{...} counter. Суммарное время активных выполнений фильтров (в секундах).
- spring_security_filterchains_active_seconds_max{...} gauge. Максимальное время активного выполнения фильтра.

17.12.5 Счетчики прохождения фильтров безопасности (часть 2):

- spring_security_filterchains_authentication_anonymous_after_total{...} counter. Количество прохождений после фильтра authentication_anonymous.
- spring_security_filterchains_authentication_anonymous_before_total{...} counter. Количество прохождений перед фильтром authentication_anonymous.

- spring_security_filterchains_authorization_after_total{...} counter. Количество прохождений после фильтра authorization.
- spring_security_filterchains_authorization_before_total{...} counter. Количество прохождений перед фильтром authorization.
- spring_security_filterchains_context_async_after_total{...} counter. Количество прохождений после фильтра context_async.
- spring_security_filterchains_context_async_before_total{...} counter. Количество прохождений перед фильтром context_async.
- spring_security_filterchains_context_holder_after_total{...} counter. Количество прохождений после фильтра context_holder.
- spring_security_filterchains_context_holder_before_total{...} counter. Количество прохождений перед фильтром context_holder.
- spring_security_filterchains_context_servlet_after_total{...} counter. Количество прохождений после фильтра context_servlet.
- spring_security_filterchains_context_servlet_before_total{...} counter. Количество прохождений перед фильтром context_servlet.
- spring_security_filterchains_header_after_total{...} counter. Количество прохождений после фильтра header.
- spring_security_filterchains_header_before_total{...} counter. Количество прохождений перед фильтром header.
- spring_security_filterchains_logout_after_total{...} counter. Количество прохождений после фильтра logout.
- spring_security_filterchains_logout_before_total{...} counter. Количество прохождений перед фильтром logout.
- spring_security_filterchains_requestcache_after_total{...} counter. Количество прохождений после фильтра requestcache.
- spring_security_filterchains_requestcache_before_total{...} counter. Количество прохождений перед фильтром requestcache.

17.12.6 Время выполнения фильтров:

- spring_security_filterchains_seconds_count{error="...", security_security_reached_filter_section="...", spring_security_filterchain_position="...", spring_security_filterchain_size="...", spring_security_reached_filter_name="..."} counter. Количество выполнений фильтров безопасности.
- spring_security_filterchains_seconds_sum{...} counter. Суммарное время выполнения фильтров (в секундах).
- spring_security_filterchains_seconds_max{...} gauge. Максимальное время выполнения фильтра (в секундах).

17.12.7 Счетчики прохождения фильтров безопасности (часть 3):

- spring_security_filterchains_session_management_after_total{...} counter. Количество прохождений после фильтра session_management.
- spring_security_filterchains_session_management_before_total{...} counter. Количество прохождений перед фильтром session_management.
- spring_security_filterchains_session_urlencoding_after_total{...} counter. Количество прохождений после фильтра session_urlencoding.
- spring_security_filterchains_session_urlencoding_before_total{...} counter. Количество прохождений перед фильтром session_urlencoding.

17.12.8 Защищенные запросы:

- spring_security_http_secured_requests_active_seconds_count counter. Количество активных защищенных запросов.
- spring_security_http_secured_requests_active_seconds_sum counter. Суммарное время активных защищенных запросов (в секундах).
- spring_security_http_secured_requests_active_seconds_max gauge. Максимальное время активного защищенного запроса.
- spring_security_http_secured_requests_seconds_count{error="..."} counter. Количество защищенных HTTP-запросов.

- spring_security_http_secured_requests_seconds_sum{error="..."} counter. Суммарное время обработки защищенных запросов (в секундах).
- spring_security_http_secured_requests_seconds_max{error="..."} gauge. Максимальное время обработки защищенного запроса.

17.12.9 Незащищенные запросы:

- spring_security_http_unsecured_requests_active_seconds_count counter. Количество активных незащищенных запросов.
- spring_security_http_unsecured_requests_active_seconds_sum counter. Суммарное время активных незащищенных запросов (в секундах).
- spring_security_http_unsecured_requests_active_seconds_max gauge. Максимальное время активного незащищенного запроса.
- spring_security_http_unsecured_requests_seconds_count{error="..."} counter. Количество незащищенных HTTP-запросов.
- spring_security_http_unsecured_requests_seconds_sum{error="..."} counter. Суммарное время обработки незащищенных запросов (в секундах).
- spring_security_http_unsecured_requests_seconds_max{error="..."} gauge. Максимальное время обработки незащищенного запроса.

17.13 Системные метрики CPU:

- system_cpu_count gauge. Количество процессоров/ядер, доступных JVM.
- system_cpu_usage gauge. Общая загрузка ЦП системы (значение от 0 до 1).
- system_load_average_1m gauge. Средняя нагрузка на систему за 1 минуту.

17.14 Метрики планировщика задач

17.14.1 Активные задачи:

- tasks_scheduled_execution_active_seconds_count{code_function="...", code_namespace="...", exception="...", outcome="..."} counter. Количество активных выполнений запланированных задач.
- tasks_scheduled_execution_active_seconds_sum{...} counter. Суммарное время активных выполнений.
- tasks_scheduled_execution_active_seconds_max{...} gauge. Максимальное время активного выполнения.

17.14.2 Завершенные задачи:

- tasks_scheduled_execution_seconds_count{code_function="...", code_namespace="...", error="...", exception="...", outcome="..."} counter. Количество выполнений запланированных задач.
- tasks_scheduled_execution_seconds_sum{...} counter. Суммарное время выполнения запланированных задач (в секундах).
- tasks_scheduled_execution_seconds_max{...} gauge. Максимальное время выполнения запланированной задачи.

17.15 Метрики Tomcat-сессий:

- tomcat_sessions_active_current_sessions gauge. Текущее количество активных HTTP-сессий.
- tomcat_sessions_active_max_sessions gauge. Максимальное количество одновременных активных сессий.
- tomcat_sessions_alive_max_seconds gauge. Максимальное время жизни сессии.
- tomcat_sessions_created_sessions_total counter. Общее количество созданных сессий.
- tomcat_sessions_expired_sessions_total counter. Количество истекших сессий.
- tomcat_sessions_rejected_sessions_total counter. Количество отклоненных сессий.

ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА «ПРИ УСТАНОВКЕ СУБД POSTGRES И POSTGRESPRO[1]

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 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 автоматического запуска 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:

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

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

ПРИЛОЖЕНИЕ 2. НАСТРОЙКА ПОДКЛЮЧЕНИЯ К ВНЕШНЕЙ СУБД

2.1 Настройка на хосте СУБД

На внешнем хосте с установленной СУБД в зависимости от используемой на нем ОС необходимо выполнить следующие настройки:

- Если в качестве ОС на хосте СУБД используется Astra Linux Special Edition 1.7, то необходимо разрешить подключение по протоколу TCP для порта СУБД выполнив в терминале на данном хосте следующую команду с правами суперпользователя:

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

где `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432). Данная команда разрешит подключение к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к порту СУБД, предоставив его только для определенного IP-адреса необходимо использовать следующую команду с правами суперпользователя:

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

где `IP` - IP-адрес, доступ с которого необходимо разрешить, а `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432).

- Если в качестве ОС на хосте с СУБД используется РЕД ОС, РОСА «ХРОМ» 12 Сервер, SberLinux OS Server или ОС Альт 8 СП, необходимо отредактировать файл `/var/lib/pgsql/15/data/pg_hba.conf` (или `var/lib/jatoba/4/data/pg_hba.conf`, если используется СУБД Jatoba)[1], приведя его к следующему виду:

```
# TYPE  DATABASE        USER            ADDRESS                 METHOD

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

Кроме того, необходимо отредактировав файл `/var/lib/pgsql/15/data/postgresql.conf` (или `var/lib/jatoba/4/data/postgresql.conf`, если используется СУБД Jatoba)[2], указав для параметра `listen_addresses` значение '*':

```
listen_addresses = '*'
```

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

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

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

```
listen_addresses = '192.168.111.100'
```

- Затем на хосте СУБД необходимо перезапустить используемую СУБД выполнив с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-4` если используется СУБД Jatoba).
- Затем на хосте СУБД необходимо выполнить создание и настройку базы данных. В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

2.2 Настройка на хосте eCA-VA

На хосте eCA-VA предварительно должна быть выполнена установка СУБД.

При этом не нужно настраивать СУБД, установленную на хосте eCA-VA.

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

Параметр	Значение по умолчанию	Описание
use_tls	'false'	Флаг обязательного использования TLS для подключения к СУБД[1]. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя базы данных, используемое для работы eCA-VA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
database_password	'#CHANGEIT'	Пароль пользователя базы данных, используемый для работы eCA-VA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
database_host	'localhost'	Сетевой адрес хоста СУБД
database_port	'5432'	Порт, используемый для подключения к базе данных
database_name	'aecava'	Имя базы данных, используемой eCA-VA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД[2]

- Затем на хосте eCA-VA примените изменения конфигурационного файла:
  - Выполните с правами суперпользователя команду `bash /opt/aecaVa/scripts/install.sh`.
  - При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.

[1] Подробная информация о параметре `use_tls` приведена в приложении 3.

[2] Подробная информация о параметре `root_cert_path` приведена в приложении 3.

- Выберите действие «[Update]». В случае, если eCA-VA не был установлен ранее, выбор действия не потребуется, и будет выполнена установка с указанными в конфигурационном файле параметрами.

ПРИЛОЖЕНИЕ 3. НАСТРОЙКА TLS-СОЕДИНЕНИЯ С СУБД

Для настройки TLS-соединения eCA-VA с СУБД необходимо в предварительно развернутом и инициализированном eCA-CA создать сертификат с закрытым ключом (PKCS#12) для сервера СУБД. При этом в сертификате сервера СУБД в атрибуте Common Name или в атрибуте Subject Alternative Name типа dNSName обязательно должно быть указано доменное сервера СУБД (или IP-адрес)[1], так как eCA-VA аутентифицирует сервер СУБД в режиме «verify-full», который предполагает проверку соответствия имени узла сервера имени, записанному в сертификате. Для создания сертификата может быть использован шаблон «WEB-Server» (необходимо предварительно создать локальный субъект в eCA-VA, указав ему необходимые атрибуты CN и DNS Name).

Во избежание ошибок в работе eCA-VA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу eCA-VA путем выполнения команды с правами суперпользователя `systemctl stop aeca-va.service`.

Для настройки TLS-соединения eCA-VA с СУБД необходимо:

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

3.1 Настройка СУБД

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

- «ssl» значение «on»;
- «ssl_cert_file» абсолютный путь к файлу сертификата сервера СУБД[3];
- «ssl_key_file» абсолютный путь к файлу закрытого ключа сервера СУБД[4];
- «ssl_ca_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД[5].

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

---

[1] Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database_host» конфигурационного файла программного компонента Центра валидации Aladdin eVA.

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

[3] Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса программного компонента Центра валидации Aladdin eVA. Например, в карточке локального субъекта сервера СУБД.

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

[5] Файл цепочки сертификатов издателя сертификата СУБД может быть скачан в карточке ЦС, выпустившего сертификат сервера СУБД.

Пример значений отредактированных параметров конфигурационного файла СУБД `postgresql.conf`:

```
# - SSL -
ssl = on
ssl_cert_file = '/tmp/cert.pem'
ssl_key_file = '/tmp/key.key'
ssl_ca_file = '/tmp/chain.pem'
```

На хосте СУБД перезапустите СУБД выполнив с правами суперпользователя команду `systemctl restart postgresql` (или `systemctl restart jatoba-4`, если используется СУБД Jatoba).

3.2 Настройка eCA-VA

На хосте eCA-VA отредактируйте конфигурационный файл `/opt/aecaVa/scripts/config.sh`, указав в нем в параметре конфигурации БД `use_tls` значение `true`, а в параметре `root_cert_path` абсолютный путь к файлу сертификата корневого издателя из цепочки сертификатов сервера СУБД[1].

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

На хосте eCA-VA примените изменения конфигурационного файла:

1. Выполните с правами суперпользователя команду `bash /opt/aecaVa/scripts/install.sh`.
2. При необходимости (см. описание параметра `use_credentials_from_config` в 4.2) введите в диалоге имя и пароль пользователя СУБД.
3. Выберите «[Update]».
4. Дождитесь завершения работы скрипта.

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

[1] Если сертификат сервера СУБД выпущен подчинённым ЦС, необходимо указать путь до сертификата корневого ЦС.

ПРИЛОЖЕНИЕ 4. НАСТРОЙКА ВЗАИМОДЕЙСТВИЯ С КРИПТОПРОВАЙДЕРОМ СКЗИ «КРИПТОПРО CSP»

Для использования алгоритмов ГОСТ Р 34.10-2012 и RSA eCA-VA может взаимодействовать со средством криптографической защиты информации (СКЗИ) - криптопровайдером СКЗИ «КриптоПро CSP».

Взаимодействие eCA-VA с криптопровайдером СКЗИ «КриптоПро CSP» осуществляется через модуль «КриптоПро Java CSP»[1]. При каждом запуске eCA-VA определяется наличие на его хосте активного криптопровайдера СКЗИ «КриптоПро CSP».

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с eCA-VA необходимо подготовить внешнюю гамму[2]. Подключение внешней гаммы необходимо для генерации ключевых пар центров сертификации, субъектов и пользователей по алгоритмам, криптопровайдером которых является СКЗИ «КриптоПро CSP».

> **При развертывание нескольких экземпляров eCA-VA под одним средством балансирования нагрузки необходимо для каждого экземпляра программного средства подготовить уникальную внешнюю гамму, чтобы исключить совпадения ключевых пар.**

Порядок настройки взаимодействия СКЗИ «КриптоПро CSP» с eCA-VA:

- На сервере eCA-VA выполнить установку криптопровайдера СКЗИ «КриптоПро CSP» в соответствии с инструкцией, описанной в разделе 2 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.

> **Внимание! Перед установкой СКЗИ «КриптоПро CSP» в ОС Альт 8 СП Сервер установите пакет `newt52` командой с правами суперпользователя `apt-get install newt52`.**
>
> **Внимание! В приведённых ниже командах файлы cpSSL.jar и sspiSSL.jar нужно указывать только если между ЦС и ЦР нужно взаимодействие по ГОСТ TLS.**

- При отсутствии создайте каталог `/opt/aecaVa/services/cryptoproviders` командой с правами суперпользователя:

```
mkdir -p /opt/aecaVa/services/cryptoproviders
```

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

```
cp {ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar,sspiSSL.jar}
/opt/aecaVa/services/cryptoproviders
```

- Назначьте права доступа на скопированные файлы:

– Если выполняется первоначальная установка eCA-VA, то назначьте файлам права доступа (chmod 777) командой с правами суперпользователя:

```
chmod 777 -R
/opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar
,sspiSSL.jar}
```

[1] Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

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

– Если eCA-VA был ранее установлен, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа к файлам (chmod 700) командами с правами суперпользователя:

```
chown aeca:aeca -R
/opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar
,sspiSSL.jar}
chmod 700 -R
/opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar
,sspiSSL.jar}
```

- Если используется уже заранее подготовленная внешняя гамма, то пропустите этот пункт. Иначе подготовьте внешнюю гамму с помощью утилиты `/opt/cprocsp/bin/amd64/genkpim` (утилита `genkpim` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma
/opt/cprocsp/bin/amd64/genkpim <количество ключей> 0x12345678 ~/gamma
```

- На хосте eCA-VA поместите каталог с заранее подготовленной внешней гаммой в каталог `/opt/aecaVa/dist/` командой с правами суперпользователя:

```
cp -a ~/gamma/. /opt/aecaVa/dist/gamma
```

- В результате в каталоге `/opt/aecaVa/dist/gamma` появятся подкаталоги `db1, db2, kpim`.

– Если выполняется первоначальная установка eCA-VA, то назначьте права доступа файлам (chmod 777) командой с правами суперпользователя:

```
chmod -R 777 /opt/aecaVa/dist/gamma
```

– Если eCA-VA был ранее установлен, то назначьте владельцем данных файлов пользователя «aeca» и предоставьте ему права доступа (chmod 700) командами с правами суперпользователя:

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

- Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд с правами суперпользователя [1]:

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

- Если eCA-VA был ранее установлен, перезапустите сервис `aeca-va.service` командой с правами суперпользователя:

```
systemctl restart aeca-va.service
```

Если в дальнейшем к СКЗИ «КриптоПро CSP» будет подключён ПАКМ «КриптоПро HSM», для обнаружения eCA-VA наличия такого подключения необходимо перезапустить сервис `aeca-va.service`.

[1] Подключение осуществляется с помощью файла `cpconfig` (находится в `/opt/cprocsp/sbin/amd64`). Путь к файлу в командах приведен с учётом нахождения в каталоге `/opt/cprocsp/sbin/amd64`.

ПРИЛОЖЕНИЕ 5. НАСТРОЙКА KERBEROS В ВЕБ-БРАУЗЕРЕ

Предварительно на клиенте должен быть настроен Kerberos, клиент должен быть подключён к домену и клиент должен использовать бразуер с поддержкой Kerberos.

Для того, чтобы в браузере клиента при работе с eCA-VA была доступна аутентификация по Kerberos необходимо внести доменное имя eCA-VA в список доверенных URI, для которых используется аутентификация Kerberos в соответствии с инструкциями ниже.

5.1 Настройка веб-браузера Mozilla Firefox

Далее в примере:

- `aeca.al.rd.kg, aeca1.al.rd.kg` — доменные имена eCA-RA
- `al.rd.kg` — имя домена, (`AL.RD.KG` — realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Запустите веб-браузер Mozilla Firefox.
- В адресной строке введите `about:config`.
- Нажмите на кнопку <Принять риск и продолжить>.
- В поле поиска введите `negotiate`, чтобы ограничить список отображаемых параметров.
- Установите параметру `network.negotiate-auth.trusted-uris` (см. рисунок 50) одно из следующих значений:
  - Чтобы разрешить аутентификацию eCA-RA, введите его полное доменное имя (например, `aeca.al.rd.kg`).
  - Чтобы разрешить аутентификацию для нескольких eCA-RA, введите их полные доменные имена через запятую (например, `aeca.al.rd.kg, aeca1.al.rd.kg`).
  - Чтобы разрешить аутентификацию для всех узлов домена, введите имя данного домена с точкой в начале (например, `.al.rd.kg`).
- Продублируйте введённое значение параметра `network.negotiate-auth.trusted-uris` в параметре `network.negotiate-auth.delegation-uris`.

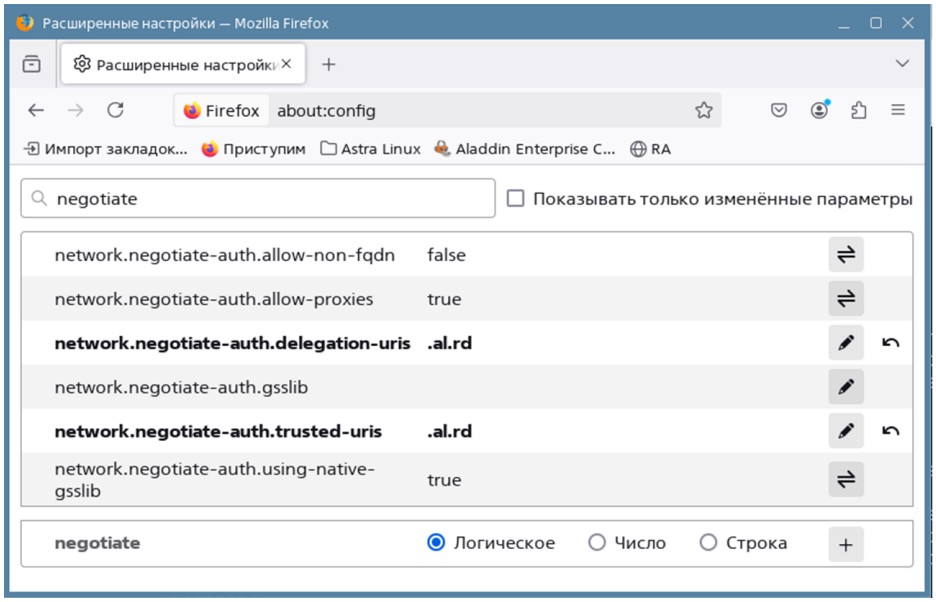


Рисунок 50 — Настройка Kerberos-аутентификации в веб-браузере Firefox

5.2 Настройка веб-браузера Chromium

Далее в примере:

- `aeca.al.rd.ru, aeca1.al.rd.ru` - доменные имена eCA-RA.
- `al.rd.ru` - домен, (`AL.RD.RU` - realm в Kerberos).

Для внесения доменного имени в список доверенных URI, для которых будет использоваться аутентификация по Kerberos-билету выполните следующие шаги:

- Создайте в каталоге `/etc/chromium/policies/managed` файл `policies.json` выполнив следующую команду с правами суперпользователя:

```
touch /etc/chromium/policies/managed/policies.json
```

- Откройте файл для редактирования выполнив следующую команду с правами суперпользователя:

```
nano /etc/chromium/policies/managed/policies.json
```

- В файле `policies.json` укажите следующие политики в формате JSON:

```
{
"AuthServerAllowlist": "*.al.rd.ru",
"AuthSchemes": "ntlm,negotiate"
}
```

Примечания:

- Чтобы разрешить аутентификацию eCA-RAукажите для политики «AuthServerAllowlist» полное доменное имя eCA-VA (например, `aeca.al.rd.ru`).
- Чтобы разрешить аутентификацию для нескольких eCA-VA, укажите для политики «AuthServerAllowlist» их полные доменные имена через запятую (например, `aeca.al.rd.ru, aeca1.al.rd.ru`).
- Чтобы разрешить аутентификацию для всех узлов домена, укажите для политики «AuthServerAllowlist» имя домена (например, `*.al.rd.ru`).

- Запустите веб-браузер Chromium и введите в адресной строке `chrome://policy`.
- Убедитесь, что политики были применены (см. Рисунок 51).

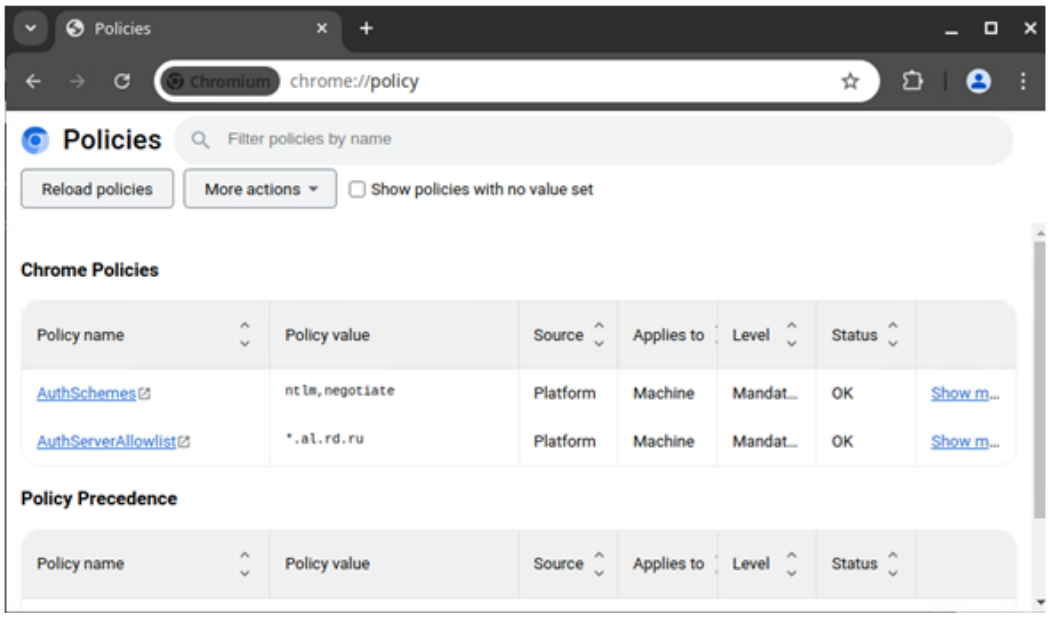


Рисунок 51 - Настройка Kerberos-аутентификации в веб-браузере Chromium

ПРИЛОЖЕНИЕ 6. РАЗВЕРТЫВАНИЕ КЛАСТЕРА

Программное средство обеспечивает объединение нескольких eCA-VA в кластер. Кластеризации обеспечивается в отказоустойчивом режиме с использованием внешнего средства балансировки нагрузки HAProxy [1]. Отказоустойчивый режим кластеризации обеспечивает как холодное «active-passive» [2], так и горячее «active-active» [3] резервирование. Горячее «active-active» резервирование возможно только при «source» [4] балансировке.

Развертывания кластера eCA-VA возможно в следующих вариантах:

- В виртуальной инфраструктуре путем клонирования виртуальной машины основного узла.
- С помощью переноса контейнера закрытого ключа службы OCSP основного узла.

6.1 Развертывание кластера в виртуальной среде с холодным резервированием «active-passive»

Кластер включает следующие узлы:

- Виртуальная машина с установленным eCA-VA (далее - ВМ1) - основной узел кластера.
- Клон ВМ1 eCA-VA (далее - ВМ2) - резервный узел кластера.
- Клон ВМ1, созданный при необходимости при эксплуатации кластера (далее - ВМР) – дополнительный резервный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - ВМ3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - ВМ4).

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации ВМ3 и ВМ4.

Порядок развертывания кластера:

- Выполните следующие действия на ВМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000[5] в файле [6]:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.
    - `systemctl restart jatoba-[версия]` для СУБД Jatoba.

[1] Серверное программное обеспечение для обеспечения высокой доступности и балансировки нагрузки для TCP- и HTTP-приложений посредством распределения входящих запросов на несколько обслуживающих серверов

[2] Это конфигурация отказоустойчивых кластеров, в которой одни узлы назначаются активными, а другие — резервными, готовыми взять на себя работу в случае отказа активного узла.

[3] Это архитектурный подход построения кластера, при котором оба или все узлы активны и работают одновременно, обрабатывая запросы и трафик.

[4] Это режим, при котором балансировщик выбирает узел кластера на основе хэш-суммы источника IP-адреса, с которого клиенты отправляют запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера.

[5] Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-VA, взаимодействующего с СУБД.

[6] Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

- Выполните следующие действия на ВМ1:
  - Выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. Приложение 2 настоящего руководства).
  - Подключитесь локально к веб-интерфейсу eCA-VA под учетной записью администратора инициализации и выполните подключение к обслуживаемым eCA-CA (см. раздел 7.3.8 настоящего руководства).
  - Подключитесь к веб-интерфейсу eCA-VA под учетной записью администратора и создайте для обслуживаемых eCA-CA Центры валидации (см. раздел 7.2.2 настоящего руководства), а при необходимости службы OCSP для них (см. раздел 7.2.3 настоящего руководства).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-va.service`.

Внимание! В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на ВМ2 необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните следующие действия на ВМ4:
  - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy`- для ОС Astra Linux SE.
    - `apt-get install haproxy`- для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon
defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000
frontend ft_app
    bind *:443
    mode tcp
```

```
    default_backend bk_app
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

- `DOMAINNAME_HOST1` – доменное имя ВМ1.
- `DOMAINNAME_HOST2` – доменное имя ВМ2.
- `admin:password` – имя и пароль учетной записи для доступа к панели мониторинга HAProxy.

– Перезапустите HAProxy выполнив следующую команду с правами суперпользователя `systemctl restart haproxy.service`.

К кластеру можно подключать дополнительные резервные узлы ВРМ. Для подключения нового резервного узла ВРМ необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР.
- Запустите ВМР и дождитесь запуска службы `aeca-va.service`.

> **Внимание! В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на ВМР необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.**
>
> **В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».**

- Выполните на ВМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени ВМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
```

где `DOMAINNAME_HOSTR` – доменное имя ВМР.

- Перезапустить HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

- создайте резервные копии (см. 10):

– полную резервную копию («backup.sh» без параметров) на основном узле кластера;

– резервную копию без БД («backup.sh» с параметром «-nodb») на резервном узле кластера. Это позволит восстанавливать резервный узел без влияния на базу данных eCA-VA и, как следствие, на работоспособность основного узла.

В результате выполненной настройки кластера все запросы, направляемые к eCA-VA через средство балансировки нагрузки HAProxy, будут перенаправляться на основной узел кластера ВМ1. При

недоступности основного узла кластера все запросы будут перенаправляться на резервный узел кластера ВМ2. При недоступности ВМ2 все запросы будут перенаправляться на дополнительный резервный узел кластера ВМР. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats` (где `IP_VM4` - IP-адрес ВМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учетной записи, указанных при настройка конфигурационного файла HAProxy.

> **Внимание! В случае дальнейшего создания Центров валидации со службами OCSP в развернутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей служб OCSP, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» и контейнеров закрытого ключа администраторов (для взаимодействия с eCA-CA) на ВМ1, ВМ2 и всех дополнительных резервных узлах. Например, если активным узлом кластера являлся ВМ2, скопируйте созданные закрытые ключи служб OCSP и администраторов с ВМ2 на ВМ1, а затем перезапустите `aeca-va.service` на ВМ1.**
>
> **Закрытые ключи служб OCSP, для которых при создании было выбрано место хранения «Локально», хранятся в каталоге `/opt/aecaVa/dist/cryptotoken`. При копировании файлов необходимо назначать владельцем данных файлов на конечной ВМ пользователя «aeca».**
>
> **Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге /`var/opt/cprocsp/keys/aeca`. При копировании файлов необходимо назначать владельцем данных файлов на конечной ВМ пользователя «aeca», затем перезапускать на данной ВМ СКЗИ «КриптоПро CSP».**
>
> **Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения ПАКМ «КриптоПро HSM», не требуют копирования. Для поддержки работы с такими ключами необходимо сохранять подключение всех узлов кластера к одному ПАКМ «КриптоПро HSM».**
>
> **Закрытые ключи администраторов для взаимодействия с eCA-CA расположены в каталоге `/opt/aecaVa/dist/certificates/account`.**

6.2 Развертывание кластера с холодным резервированием «active-passive» путем переноса контейнеров закрытого ключа служб OCSP основного узла

Кластер включает следующие узлы:

- Сервер с установленным eCA-VA (далее - ВМ1) - основной узел кластера.
- Сервер с установленным eCA-VA, на который будет выполнен перенос контейнеров закрытого ключа служб OCSP Центров валидации (далее - АРМ2) - резервный узел кластера.
- Сервер с установленным eCA-VA (далее - ВМ1), а который будет выполнен перенос контейнеров закрытого ключа служб OCSP Центров валидации (далее - АРМР) – дополнительный резервный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - АРМ3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - АРМ4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1 настоящего руководства. Допускается использование одного сервера для реализации АРМ3 и АРМ4.

Порядок развертывания кластера:

- Выполните следующие действия на АРМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.

- Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000 [1] в файле [2]:
  - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
  - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
- Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
  - `systemctl restart postgresql` для СУБД PostgreSQL.
  - `systemctl restart jatoba-[версия]` для СУБД Jatoba.

- Выполните следующие действия на АРМ1:
  - Выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. Приложение 2 настоящего руководства).
  - Подключитесь локально к веб-интерфейсу eCA-VA под учетной записью администратора инициализации и выполните подключение к обслуживаемым eCA-CA (см. раздел 7.3.8 настоящего руководства).
  - Подключитесь к веб-интерфейсу eCA-VA под учетной записью администратора и создайте для обслуживаемых eCA-CA Центры валидации (см. раздел 7.2.2 настоящего руководства), а при необходимости службы OCSP для них (см. раздел 7.2.3 настоящего руководства).

- На АРМ2 выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД [3], установленной на АРМ3 (см. Приложение 2 настоящего руководства).

> **Внимание! В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на АРМ2 необходимо выполнить аналогичную АРМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.**
>
> **В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на АРМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».**

- Если на АРМ1 была создана служба OCSP, закрытый ключ которой хранится локально, скопируйте с АРМ1 содержимое каталога `/opt/aecaVa/dist/cryptotoken` в каталог `/opt/aecaa/dist/cryptotoken` АРМ2.

- Если на АРМ1 была создана служба OCSP, закрытый ключ которой расположен в хранилище HDIMAGE СКЗИ «КриптоПро CSP», скопируйте с АРМ1 контейнер закрытого ключа из каталога `/var/opt/cprocsp/keys/aeca` в каталог `/var/opt/cprocsp/keys/aeca` АРМ2. При этом необходимо назначить владельцем данного файла на АРМ2 пользователя `aeca` (по умолчанию), и перезапустить на АРМ2 СКЗИ «КриптоПро CSP».

- Скопируйте с АРМ1 содержимое каталога `/opt/aecaVa/dist/certificates` в каталог `/opt/aecaVa/dist/certificates` АРМ2.

- Если на АРМ2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, то выполните с правами суперпользователя следующие команды в терминале на АРМ2:
  - `restorecon -Rv /opt/aecaVa/dist/cryptotoken`
  - `restorecon -Rv /opt/aecaVa/dist/certificates`

- Перезапустите на АРМ2 службу `aeca-va.service` выполнив с правами суперпользователя следующую команду:

```
systemctl restart aeca-va.service
```

[1] Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-VA, взаимодействующего с СУБД.

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

[3] В конфигурационном файле на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным СУБД АРМ1.

- Выполните следующие действия на ВМ4:
  - Выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy`- для ОС Astra Linux SE.
    - `apt-get install haproxy`- для ОС Альт Сервер.
  - На АРМ4 выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon
defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000
frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

    где:
    - `DOMAINNAME_HOST1` – доменное имя АРМ1.
    - `DOMAINNAME_HOST2` – доменное имя АРМ2.
    - `admin:password` – имя и пароль учетной записи для доступа к панели мониторинга HAProxy.

- На АРМ4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

К кластеру можно подключать дополнительные резервные узлы АРМР. Для подключения нового резервного узла АРМР необходимо выполнить действия, аналогичные действиям по подключению узла АРМ2.

> **Внимание! В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на АРМР необходимо выполнить аналогичную АРМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.**
>
> **В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на АРМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».**

Выполните на АРМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени АРМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check backup
    server clone DOMAINNAME_HOSTR:443 check backup
```

где `DOMAINNAME_HOSTR` – доменное имя АРМР.

Перезапустите на АРМ4 HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел. Все описанные выше рекомендации и уточнения по работе с узлом АРМ2, также относятся и к узлу АРМР.

В результате приведенной настройки кластера все запросы, направляемые к eCA-VA через средство балансирования нагрузки HAProxy, будут перенаправляться на основной узел кластера АРМ1. В случае недоступности основного узла кластера все запросы, направляемые к eCA-VA через средство балансирования нагрузки HAProxy, будут перенаправляться на резервный узел кластера АРМ2. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_ARM4:8404/stats` (где `IP_ARM4` - IP-адрес АРМ4) и пройдите идентификацию и аутентификацию с помощью имени и пароля учетной записи, указанных при настройка конфигурационного файла HAProxy.

> **Внимание! В случае дальнейшего создания Центров валидации со службами OCSP в развернутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей служб OCSP, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» и контейнеров закрытого ключа администраторов (для взаимодействия с eCA-CA) на АРМ1, АРМ2 и всех дополнительных резервных узлах. Например, если активным узлом кластера являлся АРМ2, скопируйте созданные закрытые ключи служб OCSP с АРМ2 на АРМ1, а затем перезапустите `aeca-ca.service` на АРМ1.**
>
> **Закрытые ключи служб OCSP, для которых при создании было выбрано место хранения «Локально», хранятся в каталоге `/opt/aecaVa/dist/cryptotoken`. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «аеса».**
>
> **Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге `/var/opt/cprocsp/keys/aeca`. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «аеса», затем перезапускать на данном АРМ СКЗИ «КриптоПро CSP».**

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

Закрытые ключи администраторов для взаимодействия с eCA-CA расположены в каталоге `/opt/aecaVa/dist/certificates/account`.

6.3 Развертывания кластера в виртуальной среде с горячим резервированием «active-active»

Кластер включает следующие узлы:

- Виртуальная машина с установленным eCA-VA (далее - ВМ1) - основной узел кластера.
- Клон ВМ1 eCA-VA (далее - ВМ2) - резервный узел кластера.
- Клон ВМ1, созданный при необходимости при эксплуатации кластера (далее - ВМР) – дополнительный резервный узел кластера.
- Виртуальная машина с установленной и настроенной СУБД (далее - ВМ3).
- Виртуальная машина с установленным и настроенным средством балансировки нагрузки HAProxy (далее - ВМ4).

На всех указанных выше виртуальных машинах допускается использование только ОС, определенных требованиями в разделе 2.1 настоящего руководства. Допускается использование одной виртуальной машины для реализации ВМ3 и ВМ4.

Порядок развертывания кластера:

- Выполните следующие действия на ВМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000[1] в файле [2]:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.
  - Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
    - `systemctl restart postgresql` для СУБД PostgreSQL.
    - `systemctl restart jatoba-[версия]` для СУБД Jatoba.
- Выполните следующие действия на ВМ1:
  - Выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. Приложение 2 настоящего руководства).
  - Подключитесь локально к веб-интерфейсу eCA-VA под учетной записью администратора инициализации и выполните подключение к обслуживаемым eCA-CA (см. раздел 7.3.8 настоящего руководства).
  - Подключитесь к веб-интерфейсу eCA-VA под учетной записью администратора и создайте для обслуживаемых eCA-CA Центры валидации (см. раздел 7.2.2 настоящего руководства), а при необходимости службы OCSP для них (см. раздел 7.2.3 настоящего руководства).
- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМ2.
- Запустите ВМ2 и дождитесь завершения запуска службы `aeca-va.service`.

Внимание! В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на ВМ2 необходимо

[1] Значение 2000 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-VA, взаимодействующего с СУБД.

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

выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Выполните следующие действия на ВМ4:
  - Установите средство балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
    - `dnf install haproxy` — для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
    - `apt install haproxy` — для ОС Astra Linux SE.
    - `apt-get install haproxy` — для ОС Альт Сервер.
  - Выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon
defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000
frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
listen stats
    bind *:8404
    stats enable
```

```
    stats uri /stats
    stats auth admin:password
```

- `DOMAINNAME_HOST1` – доменное имя ВМ1.
- `DOMAINNAME_HOST2` – доменное имя ВМ2.
- `admin:password` – имя и пароль учетной записи для доступа к панели мониторинга HAProxy.

– Перезапустите HAProxy выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

К кластеру можно подключать дополнительные узлы ВМР. Для подключения нового резервного узла ВМР необходимо выполнить действия, аналогичные действиям по подключению узла ВМ2:

- Средствами используемого гипервизора клонируйте ВМ1, тем самым создав ВМР.
- Запустите ВМР и дождитесь запуска службы `aeca-va.service`.

> **Внимание! В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на ВМР необходимо выполнить аналогичную ВМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.**
>
> **В случае, если на ВМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на ВМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».**

- Выполните на ВМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени ВМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где `IP_VMR` - это IP-адрес ВМР.

- Перезапустить HAProxy на ВМ4 выполнив следующую команду с правами суперпользователя: `systemctl restart haproxy.service`.

В результате в кластер будет добавлен дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера используйте панель мониторинга HAProxy. Для подключения к панели мониторинга введите в адресной строке веб-браузера `http://IP_VM4:8404/stats`, где `IP_VM4` - IP-адрес ВМ4. Пройдите идентификацию и аутентификацию с помощью имени и пароля учетной записи администратора, указанных при настройка конфигурационного файла.

Внимание! В случае дальнейшего создания Центров валидации со службами OCSP в развернутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей служб OCSP, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» и контейнеров закрытого ключа администраторов (для взаимодействия с eCA-CA) на ВМ1, ВМ2 и всех дополнительных резервных узлах. Например, если активным узлом кластера являлся ВМ2, скопируйте созданные закрытые ключи служб OCSP и администраторов с ВМ2 на ВМ1, а затем перезапустите `aeca-va.service` на ВМ1.

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

Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге /`var/opt/cprocsp/keys/aeca`. При копировании файлов необходимо назначать владельцем данных файлов на конечной ВМ пользователя «aeca», затем перезапускать на данной ВМ СКЗИ «КриптоПро CSP».

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

Закрытые ключи администраторов для взаимодействия с eCA-CA расположены в каталоге `/opt/aecaVa/dist/certificates/account`.

6.4 Развертывание кластера с горячим резервированием «active-active» путем переноса контейнеров закрытого ключа служб OCSP спервого узла

Кластер включает следующие узлы:

- Сервер с установленным eCA-VA (далее - АРМ1) – первый узел кластера.
- Сервер с установленным eCA-VA, на который будет выполнен перенос контейнеров закрытого ключа служб OCSP Центров валидации (далее - АРМ2) – второй узел кластера.
- Сервер с установленным eCA-VA, на который будет выполнен перенос контейнеров закрытого ключа служб OCSP Центров валидации (далее - АРМР) – дополнительный узел кластера.
- Сервер с установленной и настроенной СУБД (далее - АРМ3).
- Сервер с установленным и настроенным средством балансировки нагрузки HAProxy (далее - АРМ4).

На всех указанных выше серверах допускается использование только следующих ОС, определенных требованиями в разделе 2.1 настоящего руководства. Допускается использование одного сервера для реализации АРМ3 и АРМ4.

Порядок развёртывания кластера:

- Выполните следующие действия на АРМ3:
  - Выполнить установку одной из нижеприведённых СУБД:
    - PostgreSQL из состава ОС
    - Jatoba.
  - Увеличьте максимальное количество подключений к СУБД, указав в параметре `max_connections` значение 2000 [1] в файле [2]:
    - `/var/lib/pgsql/15/data/postgresql.conf` для СУБД PostgreSQL.
    - `var/lib/jatoba/[версия]/data/ostgresql.conf` для СУБД Jatoba.

[1] Значение 200 указано из необходимости наличия 1000 подключений для каждого экземпляра eCA-VA, взаимодействующего с СУБД.

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

- Перезапустите используемую СУБД выполнив команду с правами суперпользователя:
  - `systemctl restart postgresql` для СУБД PostgreSQL.
  - `systemctl restart jatoba-[версия]` для СУБД Jatoba.

- Выполните следующие действия на АРМ1:
  - Выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД, установленной на ВМ3 (см. Приложение 2 настоящего руководства).
  - Подключитесь локально к веб-интерфейсу eCA-VA под учетной записью администратора инициализации и выполните подключение к обслуживаемым eCA-CA (см. раздел 7.3.8 настоящего руководства).
  - Подключитесь к веб-интерфейсу eCA-VA под учетной записью администратора и создайте для обслуживаемых eCA-CA Центры валидации (см. раздел 7.2.2 настоящего руководства), а при необходимости службы OCSP для них (см. раздел 7.2.3 настоящего руководства).

- На АРМ2 выполните установку eCA-VA (см. разделы 3 - 4 настоящего руководства) с подключением внешней СУБД [1], установленной на АРМ3 (см. Приложение 2 настоящего руководства).

Внимание! В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на АРМ2 необходимо выполнить аналогичную АРМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.

В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на АРМ2 подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».

- Если на АРМ1 была создана служба OCSP, закрытый ключ которой хранится локально, скопируйте с АРМ1 содержимое каталога `/opt/aecaVa/dist/cryptotoken` в каталог `/opt/aecaa/dist/cryptotoken` АРМ2.

- Если на АРМ1 была создана служба OCSP, закрытый ключ которой расположен в хранилище HDIMAGE СКЗИ «КриптоПро CSP», скопируйте с АРМ1 контейнер закрытого ключа из каталога `/var/opt/cprocsp/keys/aeca` в каталог `/var/opt/cprocsp/keys/aeca` АРМ2. При этом необходимо назначить владельцем данного файла на АРМ2 пользователя «aeca», и перезапустить на АРМ2 СКЗИ «КриптоПро CSP».

- Скопируйте с АРМ1 содержимое каталога `/opt/aecaVa/dist/certificates` в каталог `/opt/aecaVa/dist/certificates` АРМ2.

- Если на АРМ2 установлена РЕД ОС, РОСА «ХРОМ» 12 Сервер или SberLinux OS Server, то выполните с правами суперпользователя следующие команды в терминале на АРМ2:
  - `restorecon -Rv /opt/aecaVa/dist/cryptotoken`
  - `restorecon -Rv /opt/aecaVa/dist/certificates`

- Выполните на АРМ2 перезапуск `aeca-Va.service` с перенесёнными контейнерами при помощи команды с правами суперпользователя:

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

- На АРМ4 выполните установку средства балансировки нагрузки HAProxy выполнив следующую команду с правами суперпользователя:
  - `dnf install haproxy`- для РЕД ОС, РОСА «ХРОМ» 12 Сервер и SberLinux OS Server.
  - `apt install haproxy`- для ОС Astra Linux SE.
  - `apt-get install haproxy`- для ОС Альт Сервер.

[1] В конфигурационном файле на АРМ2 необходимо указывать параметры СУБД, аналогичные указанным СУБД АРМ1.

- На АРМ4 выполните редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, приведя его к следующему виду:

```
global
    log /var/log/haproxy/log local0
    log /var/log/haproxy/log local1 notice
    chroot /var/lib/haproxy
    stats socket /run/haproxy/admin.sock mode 660 level admin
    stats timeout 30s
    user haproxy
    group haproxy
    daemon
defaults
    log global
    mode http
    option httplog
    option dontlognull
    timeout connect 5000
    timeout client  50000
    timeout server  50000
frontend ft_app
    bind *:443
    mode tcp
    default_backend bk_app
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
listen stats
    bind *:8404
    stats enable
    stats uri /stats
    stats auth admin:password
```

где:

  - `DOMAINNAME_HOST1` – доменное имя АРМ1.
  - `DOMAINNAME_HOST2` – доменное имя АРМ2.
  - `admin:password` – имя и пароль учетной записи, которые будут использоваться для доступа к панели мониторинга HAProxy.

- На АРМ4 перезапустите HAProxy выполнив следующую команду с правами суперпользователя:

```
systemctl restart haproxy.service
```

В кластер можно подключать дополнительные резервные узлы АРМР. Для подключения нового резервного узла АРМР необходимо выполнить действия, аналогичные действиям по подключения узла АРМ2:

> **Внимание! В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, у которых криптопровайдером является СКЗИ «КриптоПро CSP», на АРМР необходимо выполнить аналогичную АРМ1 установку СКЗИ «КриптоПро CSP» и подключение внешней гаммы.**
>
> **В случае, если на АРМ1 для каких-либо Центров валидации были созданы службы OCSP, местом хранения закрытого ключа которых является ПАКМ «КриптоПро HSM», необходимо выполнить на АРМР подключение СКЗИ «КриптоПро CSP» к тому же ПАКМ «КриптоПро HSM».**

Выполните на АРМ4 редактирование конфигурационного файла `/etc/haproxy/haproxy.cfg`, добавив в секцию `backend bk_app` информацию о доменном имени АРМР в соответствии с примером, представленном ниже:

```
backend bk_app
    mode tcp
    balance source
    hash-type consistent
    server main DOMAINNAME_HOST1:443 check
    server clone DOMAINNAME_HOST2:443 check
    server clone DOMAINNAME_HOSTR:443 check
```

где `DOMAINNAME_HOSTR` - это доменное АРМР.

Перезапустите на АРМ4 HAProxy выполнив следующую команду с правами суперпользователя:
`systemctl restart haproxy.service`

В результате в кластере появится дополнительный резервный узел.

В результате выполненной настройки средство балансировки нагрузки HAProxy будет выбирать узел кластера на основе хэш-суммы источника IP-адреса и перенаправлять на него запросы. Это гарантирует, что одни и те же пользователи используют один и тот же узел кластера. Для мониторинга состояния узлов кластера может быть использована панель мониторинга, доступная по адресу `http://IP_ARM4:8404/stats`, где `IP_ARM4` - IP-адрес АРМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg` на АРМ4).

> **Внимание! В случае дальнейшего создания Центров валидации со службами OCSP в развернутом в виртуальной инфраструктуре кластере необходимо сохранять соответствие перечня закрытых ключей служб OCSP, хранимых локально и в хранилище HDIMAGE СКЗИ «КриптоПро CSP» и контейнеров закрытого ключа администраторов (для взаимодействия с eCA-CA) на АРМ1, АРМ2 и всех дополнительных резервных узлах. Например, если активным узлом кластера являлся АРМ2, скопируйте созданные закрытые ключи служб OCSP с АРМ2 на АРМ1, а затем перезапустите `aeca-ca.service` на АРМ1.**
>
> **Закрытые ключи служб OCSP, для которых при создании было выбрано место хранения «Локально», хранятся в каталоге `/opt/aecaVa/dist/cryptotoken`. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «аеса».**
>
> **Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения «Жесткий диск (HDIMAGE)», по умолчанию хранятся в каталоге `/var/opt/cprocsp/keys/aeca`. При копировании файлов необходимо назначать владельцем данных файлов на конечном АРМ пользователя «аеса», затем перезапускать на данном АРМ СКЗИ «КриптоПро CSP».**
>
> **Закрытые ключи служб OCSP, для которых при их создании было выбрано место хранения ПАКМ «КриптоПро HSM», не требуют копирования. Для поддержки работы с такими ключами необходимо сохранять подключение всех узлов кластера к одному ПАКМ «КриптоПро HSM».**
>
> **Закрытые ключи администраторов для взаимодействия с eCA-CA расположены в каталоге `/opt/aecaVa/dist/certificates/account`.**

6.3 Обновление ПО узлов кластера

Процесс обновления кластера eCA-VA:

- Выполните резервное копирование данных на всех узлах кластера (см. 10).
- Для кластера по схеме «active-passive» на всех резервных узлах выполните остановку службы eCA-VA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-va.service`.
- Для кластера по схеме «active-active» на всех узлах, на которые были перенесены закрытые ключи служб OCSP и администраторов, выполните остановку службы eCA-VA выполнив следующую команду с правами суперпользователя: `systemctl stop aeca-va.service`.
- Для кластера по схеме «active-passive» выполнить обновление ПО eCA-VA на основном узле (см. раздел 0 настоящего руководства).
- Для кластера по схеме «active-active» выполнить обновление ПО eCA-VA на узле, на котором расположены закрытые ключи служб OCSP и администраторов (см. раздел 0 настоящего руководства).
- Вне зависимости от схемы кластера выполните обновление ПО eCA-VA на всех остальных узлах кластера (см. раздел 0 настоящего руководства).

Критерием правильности установки обновления ПО кластера является отображение информации о новой версии в окне «О программе» веб-интерфейса и работоспособность всех узлов кластера. Работоспособность узлов можно посмотреть в панели мониторинга HAproxy, доступной по адресу `http://IP_ARM4:8404/stats`, где `IP_ARM4` - IP-адрес АРМ4 (для входа в панель мониторинга потребуется ввод логина и пароля, указанных в файле `/etc/haproxy/haproxy.cfg`).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ОС	-	Операционная система
ПО	-	Программное обеспечение
СУБД	-	Система управления базами данных
УЦ	-	Удостоверяющий центр
ЦС	-	Центр сертификатов
AIA	-	Authority Information Access
CRL	-	Certificate Revocation List
OCSP	-	Online Certificate Status Protocol
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 eCA-VA.

Анонимный субъект доступа (аноним) - неаутентифицированный в программе субъект доступа среды функционирования.

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 eCA-VA, 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 eCA-VA, отвечающая за управление жизненным циклом сертификатов субъектов.

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

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

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

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

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

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

Технологический ЦС - экземпляр центра сертификации в информационной системе, обладающий функцией первичной настройки eCA-CA.

Центр валидации — сервис (служба), предоставляющая обслуживаемому им Центру сертификации услуги распространения CRL, Delta CRL и AIA, а также услуги службы OCSP. Каждый Центр валидации представлен отдельной записью в разделе «Центры валидации».

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

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

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					