



Центр сертификатов доступа

Aladdin Enterprise Certificate Authority Certified Edition KG

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

Изделие	33714370.03.01.001
Документ	33714370.03.01.001 32 01-4
Версия	2.3.0
Листов	135
Дата	30.05.2025

АННОТАЦИЯ

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

Документ определяет порядок установки и эксплуатации программного комплекса «Центр валидации Aladdin Enterprise Validation Authority» из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG».

Инструкции по установке стороннего программного обеспечения приведены в ознакомительных целях, для получения более точной информации рекомендуем ознакомиться 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.

СОДЕРЖАНИЕ

Аннотация.....	2
Содержание	3
1 Введение	6
1.1 Назначение программы	6
1.2 Состав программы.....	6
1.3 Функции программы	6
1.4 Роли управления.....	7
2 Условия выполнения программы.....	9
2.1 Требования к программному обеспечению	9
2.1.1 Требования к среде функционирования Серверной части программы.....	9
2.1.2 Требования к среде функционирования Клиентской части программы	10
2.2 Требования к аппаратным средствам.....	10
3 Подготовка к установке программы	11
3.1 Подготовка среды функционирования с ОС РЕД ОС.....	13
3.1.1 Установка пакетов tar unzip и iptables.....	13
3.1.2 Установка среды исполнения Java	13
3.1.3 Установка и настройка СУБД.....	14
3.1.4 Установка веб-сервера	17
3.2 Подготовка среды функционирования с ОС Astra Linux SE.....	18
3.2.1 Подключение репозитория и установка пакетов	18
3.2.2 Установка среды исполнения Java	19
3.2.3 Установка и настройка СУБД.....	20
3.2.4 Установка веб-сервера	23
3.3 Подготовка среды функционирования с Альт Сервер	24
3.3.1 Подключение репозитория и установка зависимостей.....	24
3.3.2 Установка среды исполнения Java	24
3.3.3 Установка и настройка СУБД.....	24
3.3.4 Установка веб-сервера	27
3.4 Подготовка среды функционирования с ОС «Platform V SberLinux OS Server»	28
3.4.1 Установка среды исполнения Java	28
3.4.2 Установка и настройка СУБД.....	28
3.4.3 Установка веб-сервера	31
3.5 Создание службы HTTP и keytab-файла	32
3.5.1 Получение keytab-файла в Samba DC и Альт Домен.....	32
3.5.2 Получение keytab-файла в ALD PRO.....	33
3.5.3 Получение keytab-файла в Free IPA	34
3.5.4 Получение keytab-файла в MS AD	34
3.6 Установка веб-сервера сnginx	35
3.7 Установка программного средства «Криптографический модуль Aladdin JCP»	35
4 Установка программы.....	37
4.1 Установка инсталляционного пакета Центра валидации Aladdin eVA	37
4.2 Поддержка активного режима замкнутой программной среды в ОС Astra Linux Special Edition	39
4.3 Настройка конфигурации программы	39
4.4 Создание и настройка базы данных.....	48
4.4.1 Создание и настройка базы данных в автоматическом режиме.....	48
4.4.2 Создание и настройка базы данных PostgreSQL в ручном режиме	48

4.4.3 Создание и настройка базы данных Jatoba в ручном режиме.....	49
4.5 Установка программы.....	50
4.1 Порядок совместной установки программы с другими компонентами Центра сертификатов доступа на одном сервере	52
4.2 Подключение к веб-интерфейсу	52
4.2.1 Общие сведения.....	52
4.2.2 Установка сертификата администратора	53
4.2.3 Подключение к веб-интерфейсу.....	55
4.2.4 Доступ к программе.....	55
5 Запуск и завершение программы.....	60
5.1 Проверка состояния программы.....	60
5.2 Запуск программы в ручном режиме.....	60
5.3 Завершение работы программы	60
6 Функции управления программы	61
6.1 Главное окно Центра валидации Aladdin eVA.....	61
6.2 Раздел «Центры валидации»	61
6.2.1 Карточка Центра валидации	63
6.2.2 Создание Центра валидации.....	69
6.2.3 Создание службы OCSP созданного Центра валидации Aladdin eVA.....	72
6.2.4 Ручное обновление сертификата службы OCSP.....	74
6.2.5 Настройка параметров службы OCSP.....	75
6.2.6 Удаление службы OCSP из Центра валидации	75
6.2.7 Удаление Центра валидации.....	76
6.3 Раздел «Настройки»	77
6.3.1 Вкладка «Веб сервер».....	77
6.3.2 Вкладка «Syslog».....	78
6.3.3 Вкладка «Подключения к eCA-CA».....	79
6.3.4 Смена сертификата веб-сервера.....	80
6.3.5 Добавление Syslog-сервера	81
6.3.6 Редактирование параметров Syslog-сервера	83
6.3.7 Удаление Syslog-сервера	84
6.3.8 Добавление подключения к Центру сертификации Aladdin eCA.....	85
6.3.9 Удаление подключения к Центру сертификации Aladdin eCA	86
6.4 Раздел «Журнал событий»	87
6.4.1 О журнале событий	87
6.4.2 Просмотр записей журнала событий.....	88
6.4.3 Просмотр карточки события.....	91
6.4.4 Экспорт записей журнала событий.....	92
6.4.5 События, отслеживаемые Центром валидации Aladdin eVA.....	93
7 Контроль целостности исполняемых файлов программы.....	102
8 Сбор диагностической информации программы	103
9 Резервное копирование и восстановление данных	104
9.1 Резервное копирование данных.....	104
9.2 Расписание резервного копирования.....	105
9.3 Восстановление данных из резервной копии	105
10 Обновление программы.....	106
10.1 Назначение обновлений.....	106
10.2 Информирование потребителей о выпуске обновлений	106

10.3	Получение обновлений потребителем	106
10.4	Контроль целостности обновления ПО	106
10.5	Процедура установки обновлений	106
10.6	Критерий успешности установки обновления	107
11	Удаление программы	108
11.1	Инициализация процесса удаления	108
11.2	Удаление установочного пакета	108
12	Удаление базы данных Postgres	109
12.1	Удаление БД «aesava»	109
12.2	Удаление пользователя БД «aesava»	109
13	Миграция с версии программы 1.2 на версию 2.3.0	110
13.1	Начальное состояние	110
13.2	Цель	110
13.3	Рекомендации	110
13.4	План миграции №1	110
13.5	План миграции №2	114
14	Поиск и устранение неисправностей	118
	Приложение 1. Разрешение конфликта «при установке СУБД Postgres и PostgresPro	122
	Приложение 2. Настройка подключения к внешней СУБД	123
	2.1 Настройка на хосте СУБД	123
	2.2 Настройка на хосте Центра валидации Aladdin eVA	124
	Приложение 3. Настройка TLS-соединения с СУБД	125
	3.1 Настройка СУБД	125
	3.2 Настройка Центра валидации Aladdin eVA	126
	Приложение 4. Настройка взаимодействия с криптопровайдером СКЗИ «КриптоПро CSP»	127
	Приложение 5. Настройка Kerberos в веб-браузере	129
	5.1 Настройка веб-браузера Mozilla Firefox	129
	5.2 Настройка веб-браузера Chromium	129
	Перечень документации для ознакомления	131
	Обозначения и сокращения	131
	Термины и определения	133

1 ВВЕДЕНИЕ

1.1 Назначение программы

Программный комплекс «Центр валидации Aladdin Enterprise Validation Authority» 33714370.03.01.006 (далее – программа или Центр валидации Aladdin eVA) входит в состав программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG» 33714370.03.01.001, которое применяется как элемент систем защиты автоматизированных (информационных) систем, используется совместно с другими средствами защиты информации и обеспечивает идентификацию и строгую аутентификацию при управлении доступом субъектов¹ доступа к объектам² доступа в автоматизированной (информационной) системе.

Центр валидации Aladdin eVA предназначен для проверки статуса сертификатов, выпускаемых программным комплексом «Центр сертификации Aladdin Enterprise Certification Authority» 33714370.03.01.003 (далее – Центр сертификации Aladdin eCA) из состава программного средства «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG».

1.2 Состав программы

Центр валидации Aladdin eVA состоит из следующих программных компонентов:

- Программный компонент «Серверная часть Центра валидации» 33714370.03.01.007.

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» 33714370.03.01.008.

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

1.3 Функции программы

Центр валидации Aladdin eVA 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 Центре валидации Aladdin eVA определены следующие роли: «Администратор», «Администратор инициализации» и «Аноним».

Пользователю с ролью «Администратор» доступны функции, сгруппированные в следующих разделах главного окна Центра валидации Aladdin eVA (см. 6.1):

- «Центры валидации» (см. 6.2);
- «Настройки» (см. 6.3);
- «Журнал событий» (см. 6.4).

Пользователю с ролью «Администратор инициализации» доступны функции, сгруппированные в следующих разделах главного окна Центра валидации Aladdin eVA (см. 6.1):

- «Настройки»;
- «Журнал событий».

Субъекту доступа с ролью «Аноним» не проходит аутентификацию в Центре валидации Aladdin eVA, ему недоступен пользовательский интерфейс Центра валидации Aladdin eVA, однако доступно взаимодействие с Центром валидации Aladdin eVA по его программным интерфейсам получения данных из точек распространения AIA и CRL (CDP) и выполнения OCSP-запросов.

Таблица 1 - 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 Центров сертификации Aladdin eCA	✓	✓	-
Просмотр параметров Syslog-серверов	✓	✓	-
Добавление Syslog-сервера	✓	-	-
Редактирование параметров Syslog-сервера	✓	-	-

Тип действия, осуществляемого над объектом программы	Возможные роли		
	Администратор инициализации	Администратор	Аноним
Удаление Syslog-сервера	✓	-	-
Добавление подключения к Центру сертификации Aladdin eCA	✓	-	-
Удаление подключения к Центру сертификации Aladdin eCA	✓	-	-
Функции, сгруппированные в разделе «Журнал событий»			
Просмотр всех существующих в программе событий журнала	✓	-	-
Просмотр событий журнала, ассоциированных с подключением к Центру сертификации Aladdin eCA, 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 Центром сертификации Aladdin eCA.

2.1 Требования к программному обеспечению

2.1.1 Требования к среде функционирования Серверной части программы

Среда функционирования Серверной части Центра валидации Aladdin eVA:

- Поддерживаемые ОС:
 - Astra Linux Special Edition версия 1.7, уровень защищённости «Смоленск».
 - Astra Linux Special Edition версия 1.7, уровень защищённости «Воронеж».
 - Astra Linux Special Edition версия 1.7, уровень защищённости «Орёл».
 - Astra Linux Special Edition версия 1.8, уровень защищённости «Смоленск».
 - Astra Linux Special Edition версия 1.8, уровень защищённости «Воронеж».
 - Astra Linux Special Edition версия 1.8, уровень защищённости «Орёл».
 - РЕД ОС версия 7.3, конфигурация «Сервер».
 - РЕД ОС версия 8, конфигурация «Сервер».
 - Альт 8 СП, релиз 10, вариант исполнения Сервер.
 - Platform V SberLinux OS Server.
- 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 расширенного репозитория.
 - Cpnginx ⁴.
- Поддерживаемые ресурсные системы (доменные службы каталогов):
 - Samba DC.
 - Free IPA.
 - ALD PRO.
 - РЕД АДМ.
 - Microsoft AD.
 - Альт Домен.

⁴ Из состава средства криптографической защиты (далее - СКЗИ) «КриптоПро CSP». СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в состав и комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно.

- Поддерживаемый Центр сертификации Aladdin eCA версии 2.3.0 ⁵.
- Поддерживаемые криптопровайдеры, обеспечивающие формирование электронной подписи ответов службы OCSP по алгоритму ГОСТ Р 34.10-2012:
 - Программное средство «Криптографический модуль Aladdin JCP» ⁶.
 - СКЗИ «КриптоПро CSP» ⁷.

2.1.2 Требования к среде функционирования Клиентской части программы

Среда функционирования Клиентской части Центра валидации Aladdin eVA:

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

2.2 Требования к аппаратным средствам

Минимальные аппаратные требования, необходимые для стабильного функционирования Центра валидации Aladdin eVA:

- 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.

⁵ Входит в состав программного средства.

⁶ Входит в состав программного средства.

⁷ СКЗИ «КриптоПро CSP» не является обязательным программным средством, не входит в состав и комплект поставки Центра сертификатов доступа и, при необходимости, приобретается заказчиком самостоятельно. Порядок настройки взаимодействия Центра валидации Aladdin eVA 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 2) приведён список портов, которые должны быть открыты в Центре валидации Aladdin eVA и взаимодействующих компонентах.

Таблица 2 - Таблица сетевого взаимодействия

Порт	Транспорт	Протокол	Назначение	Возможность изменения
443	TCP	TLS/HTTPS	Порт для подключения к веб-интерфейсу Центра валидации Aladdin eVA (в версии 1.2 использовался порт 8888), а также для взаимодействия с Центром сертификации Aladdin eCA.	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 3) 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 3 - 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 «sa-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)

Порт	Транспорт	Протокол	Назначение
1401	TCP	HTTP	Внутренний интерфейс для подключения к внутреннему сервису «logs-service» (сервис журнализации)
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 репозитория ОС.
- Среда исполнения Java.
- СУБД.
- Веб-сервера.
- Программного средства «Криптографический модуль Aladdin JCP» (при необходимости формирования электронной подписи ответов службы OSCP по алгоритму ГОСТ Р 34.10-2012).

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 Центра валидации Aladdin eVA, в домен ресурсной системы (доменной службы каталогов);
 - создать службу HTTP и keytab-файл⁸ 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#12⁹.

⁸ Keytab-файл используется для аутентификации доменных пользователей в Центре валидации Aladdin eVA с использованием Kerberos без ввода пароля.

⁹ Порядок создания субъектов, учётных записей и выпуска сертификатов приведён в документе «Центр сертификатов доступа Aladdin Enterprise Certificate Authority Certified Edition KG. Руководство администратора. Часть 2. Функции управления Центром сертификации Aladdin Enterprise Certification Authority».

- Создать в Центре сертификации локальный субъект ⁹ 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 на Центре валидации также необходимо применять СКЗИ «КриптоПро CSP» для:

- 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.

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 «српнгінх» из состава СКЗИ «КриптоПро CSP». Установка веб-сервера выполняется после установки СКЗИ «КриптоПро CSP». Порядок установки веб-сервера «српнгінх» приведён в разделе 3.5. 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

3.1.1 Установка пакетов tar unzip и iptables

Для установки пакетов tar unzip и iptables из сети Интернет выполните команду:

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

Если доступ к сети Интернет отсутствует, пакеты tar unzip и iptables возможно установить с USB-носителя из комплекта поставки ОС следующим образом:

- перейдите в каталог USB-носителя;
- выполните команду:

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

3.1.2 Установка среды исполнения Java

3.1.2.1 Установка Axiom JDK Certified

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

Внимание! В РЕД ОС Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

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.](#)

Внимание! В РЕД ОС OpenJDK определенных версий работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена для OpenJDK версий 17.0.15.0.6 и 21.0.7.0.6.

3.1.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых базы данных:

- 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.

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

3.1.3.1 Установка СУБД PostgreSQL¹⁰

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL командой:

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

- Установите последнюю доступную версию пакета `postgresql-contrib` командой:

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

- Произведите инициализацию БД командой:

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

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

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

- Запустите PostgreSQL командой:

```
sudo systemctl start postgresql
```

- Включите автоматический запуск PostgreSQL при загрузке, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf11` с правами администратора - установите число подключений `max_connections` в значение `100012`.

¹⁰ Подробное описание приведено на [официальном сайте производителя](#).

¹¹ Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

¹² Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`¹³ с правами администратора. Измените параметры для успешного локального подключения пользователя к базе данных:

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

- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу командой:

```
sudo systemctl restart postgresql
```

3.1.3.2 Установка СУБД Postgres Pro¹⁴

Порядок установки СУБД Postgres Pro:

- Получите ключ доступа Postgres PRO.
- Загрузите скрипт для добавления репозитория, выполнив команду¹⁵:

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

где <ключ> – ключ доступа Postgres PRO.

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

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

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

```
sudo dnf update
```

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

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`¹⁶ с правами администратора - установите число подключений `max_connections` в значение `1000`¹⁷.
- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`¹⁸ с правами администратора - измените параметры для успешного локального подключения пользователя к базе данных:

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

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

¹³ Расположение файла может отличаться, для поиска файла можно использовать команду `sudo find / -type f -name pg_hba.conf`

¹⁴ Подробное описание приведено на [официальном сайте производителя](#).

¹⁵ Команды ниже приведены для 16-ой версии Postgres Pro.

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

¹⁷ Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

¹⁸ Расположение файла указано для 16 версии Postgre Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

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

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

3.1.3.3 Установка СУБД Jatoba¹⁹

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя оптической записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «`localrepo`» на всех шагах установки указывать соответствующий путь до носителя оптической записи и директорию репозитория СУБД на носителе оптической записи для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
 - каталог `/packages`;
 - каталог `/repodata`;
 - файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

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

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

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

- Обновите описания пакетов командой:

```
sudo dnf makecache
```

- Установите основные пакеты СУБД Jatoba 4 командой:

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

¹⁹ Подробное описание приведено на [официальном сайте производителя](#).

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором - установите число подключений `max_connections` в значение `1000`²⁰.
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf` под администратором. Измените параметры для успешного локального подключения пользователя к базе данных:

```
host all all 127.0.0.1/32 ident на host all all 127.0.0.1/32 password
```

```
host all all ::1/128 ident на host all all ::1/128 password
```

- Включите автоматический запуск Jatoba при загрузке, выполнив команду:

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

- Выполните перезапуск СУБД Jatoba для вступления изменений в силу командой:

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

3.1.4 Установка веб-сервера

3.1.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет, выполнив команду с правами суперпользователя:

```
sudo dnf install httpd
```

- Установите дополнительный модуль для использования протокола SSL, выполнив команду:

```
sudo dnf install mod_ssl
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable httpd
```

3.1.4.2 Установка веб-сервера nginx

Порядок установки веб-сервера nginx:

- Установите пакет из официального репозитория ОС командой:

```
sudo dnf install nginx
```

- Запустите установленный веб-сервер командой:

```
sudo systemctl start nginx
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable nginx
```

²⁰ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

3.2 Подготовка среды функционирования с ОС Astra Linux SE

3.2.1 Подключение репозитория и установка пакетов

3.2.1.1 Подключение репозитория и установка пакетов Astra Linux Special Edition 1.7²¹

Для подключения репозитория в сети Интернет установите пути нахождения репозитория²², отредактировав файл `/etc/apt/sources.list`:²³

- Укажите ссылки на репозитории base, main и update в поддереве frozen:

```
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-main/
1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-update/
1.7_x86-64 main contrib non-free
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-base/
1.7_x86-64 main contrib non-free
```

- Укажите ссылку на репозиторий extended в поддереве frozen для развёртывания веб-сервера nginx:

```
deb https://dl.astralinux.ru/astra/frozen/1.7_x86-64/1.7.6/repository-extended/
1.7_x86-64 main contrib non-free
```

Для установки необходимых компонентов в офлайн режиме:

- Настройте использование установочных дисков в качестве репозитория, отредактировав файл `/etc/apt/sources.list`.
- Зарегистрируйте физический компакт-диск, вставленный в привод компакт-дисков, выполнив команду:

```
apt-cdrom add
```

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

Выполните обновление списка пакетов из указанных репозиториях при помощи команды:

```
sudo apt update
```

Установите пакеты tar, unzip и iptables при помощи команды:

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

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

3.2.1.2 Подключение репозитория и установка пакетов Astra Linux Special Edition 1.8²⁴

Для подключения репозитория в сети Интернет установите пути нахождения репозитория²⁵, отредактировав файл `/etc/apt/sources.list`:

²¹ Подробнее см. на [официальном сайте производителя](#).

²² При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозитория в соответствии с [инструкцией по подготовке и присоединению хоста к домену ALD Pro](#).

²³ Ссылки на репозитории приведены для Astra Linux SE версии 1.7.6

²⁴ Подробнее см. на [официальном сайте производителя](#).

²⁵ Ссылки на репозитории приведены для Astra Linux SE 1.8.1

- Укажите ссылку на репозиторий main в поддереве frozen²⁶:

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/main-repository/ 1.8_x86-64 main contrib non-free
```

- Укажите ссылку на репозиторий extended в поддереве frozen для развёртывания веб-сервера Nginx.

```
deb https://dl.astralinux.ru/astra/frozen/1.8_x86-64/1.8.1/extended-repository/ 1.8_x86-64 main contrib non-free
```

Для установки необходимых компонентов в офлайн режиме:

- Настройте использование установочных дисков в качестве репозитория, отредактировав файл `/etc/apt/sources.list`
- Зарегистрируйте физический компакт-диск, вставленный в привод компакт-дисков, выполнив команду:

```
apt-cdrom add
```

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

Выполните обновление списка пакетов из указанных репозиториях при помощи команды:

```
sudo apt update
```

Установите пакеты tar, unzip и iptables командой:

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

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

3.2.2 Установка среды исполнения Java

3.2.2.1 Установка Axiom JDK

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

Внимание! В Astra Linux Special Edition Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

3.2.2.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией с официального сайта производителя ОС:

- [Инструкция для Astra Linux SE 1.7](#) (в инструкции описана установка Open JDK 11, установка Open JDK 17 и 21 аналогична).
- [Инструкция для Astra Linux SE 1.8](#) (в инструкции описана установка Open JDK 17, установка Open JDK 21 аналогична).

²⁶ При использовании доменной службы каталогов ALD Pro необходимо указывать адреса репозитория в соответствии с [инструкцией по подготовке и присоединению хоста к домену ALD Pro](#).

3.2.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых баз данных:

- 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.

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

3.2.3.1 Установка СУБД PostgreSQL²⁷

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL командой:

```
sudo apt install postgresql
```

- Установите последнюю доступную версию пакета `postgresql-contrib` командой:

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

- Установите пакет `postgresql-client` командой:

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

- Запустите PostgreSQL командой:

```
sudo systemctl start postgresql
```

- Включите автоматический запуск PostgreSQL при загрузке, выполнив команду:

```
sudo systemctl enable postgresql
```

- При наличии мандатных политик²⁸:

- выдайте полномочия пользователю `postgres` командой:

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

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

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

- Отредактируйте файл `/etc/postgresql/11/main/postgresql.conf`²⁹ с правами администратора - установите число подключений `max_connections` в значение `1000`³⁰.
- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу командой:

²⁷ Подробное описание приведено на [официальном сайте производителя](#).

²⁸ Подробная информация по аутентификации в СУБД PostgreSQL приведена на [официальном сайте производителя](#).

²⁹ Расположение файла может отличаться. В инструкции расположение указано для PostgreSQL версии 11. Для поиска файла можно использовать команду `sudo find / -type f -name postgresql.conf`

³⁰ Значение `max_connections` равное `1000` является рекомендуемым, при необходимости можно установить и большее значение.

```
sudo systemctl restart postgresql
```

3.2.3.2 Установка СУБД Postgres Pro³¹

Порядок установки СУБД Postgres Pro:

- Получите ключ доступа Postgres PRO.
- Загрузите скрипт для добавления репозитория, выполнив команду³²:

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

где <ключ> – ключ доступа Postgres PRO.

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

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

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

```
sudo apt update
```

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

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

- При наличии мандатных политик³³:
 - выдайте полномочия пользователю postgres командой:

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

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

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

- Отредактируйте файл /var/lib/pgpro/std-16/data/postgresql.conf³⁴ с правами администратора - установите число подключений max_connections в значение 1000³⁵.
- При отсутствии создайте символические ссылки на утилиты psql и pg_dump, выполнив команды с правами суперпользователя (root или sudo):

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

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

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

³¹ Подробное описание приведено на [официальном сайте производителя](#).

³² Команды ниже приведены для 16-ой версии Postgres Pro.

³³ Подробная информация по аутентификации в СУБД PostgreSQL приведена на [официальном сайте производителя](#).

³⁴ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

³⁵ Значение max_connections равно 1000 является рекомендуемым, при необходимости можно установить и большее значение.

3.2.3.3 Установка СУБД Jatoba³⁶

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя оптической записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «`localrepo`» на всех шагах установки указывать соответствующий путь до носителя оптической записи и директорию репозитория СУБД на носителе оптической записи для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
 - каталог `/pool`;
 - каталог `/dists`;
 - файл ключа `DEB-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

```
sudo rpm --import /localrepo/DEB-GPG-KEY-Jatoba
```

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

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

- Обновите описания пакетов командой:

```
sudo apt update
```

- Установите основные пакеты СУБД Jatoba командой:

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

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

- При наличии мандатных политик³⁷:
 - выдайте полномочия пользователю `postgres`, выполнив команду:

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

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

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

³⁶ Подробное описание приведено на [официальном сайте производителя](#).

³⁷ Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148>

```
sudo setfacl -m u:postgres:rx /etc/parsec/macdb
```

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

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором - установите число подключений `max_connections` в значение `1000`³⁸.
- Включите автоматический запуск СУБД Jatoba при загрузке, выполнив команду:

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

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

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

3.2.4 Установка веб-сервера

3.2.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

- Установите пакет `apache2` командой:

```
sudo apt install apache2
```

- Активируйте модули `ssl`, `proxy`, `proxy_http`, `headers`, `cgi`, `rewrite` и `http2` при помощи команд:

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

- Перезагрузите веб-сервер командой:

```
sudo systemctl restart apache2
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable apache2
```

- Для проверки корректности запуска модулей выполните команду:

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

Если модуль активирован успешно, то в выводе команды будет присутствовать имя модуля с пометкой `shared`.

3.2.4.2 Установка веб-сервера nginx

Порядок установки веб-сервера nginx:

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

```
sudo apt install nginx
```

³⁸ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

- Запустите установленный веб-сервер командой:

```
sudo systemctl start nginx
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable nginx
```

3.3 Подготовка среды функционирования с Альт Сервер

3.3.1 Подключение репозитория и установка зависимостей

Для развёртывания Центра валидации с использованием веб-сервера Apache в файле `/etc/apt/sources.list` укажите ссылку на следующий репозиторий:

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

После этого обновите список доступных пакетов командой:

```
sudo apt-get update
```

3.3.2 Установка среды исполнения Java

3.3.3 Установка и настройка СУБД

Выполните установку и настройку одной из нижеприведённых базы данных:

- 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.

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

3.3.3.1 Установка СУБД PostgreSQL³⁹

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL командой⁴⁰:

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

- Установите последнюю доступную версию пакета `postgresql-contrib` командой:

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

- Установите пакет `postgresql` командой:

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

- Произведите инициализацию БД командой:

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

³⁹ Подробное описание приведено на [официальном сайте производителя](#).

⁴⁰ Команды ниже приведены для версии PostgreSQL версии 15.

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

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

- Запустите PostgreSQL командой:

```
sudo systemctl start postgresql
```

- Включите автоматический запуск PostgreSQL при загрузке, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/15/data/postgresql.conf`⁴¹ с правами администратора - установите число подключений `max_connections` в значение `1000`⁴².
- Выполните перезапуск СУБД PostgreSQL для вступления изменений в силу командой:

```
sudo systemctl restart postgresql
```

3.3.3.2 Установка СУБД Postgres Pro⁴³

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду⁴⁴:

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

где *<ключ>* – ключ доступа Postgres PRO.

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

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

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

```
sudo apt-get update
```

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

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`⁴⁵ с правами администратора - установите число подключений `max_connections` в значение `1000`⁴⁶.
- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

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

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

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

⁴¹ Расположение файла может отличаться. В инструкции расположение указано для 15 версии PostgreSQL. Для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁴² Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁴³ Подробное описание приведено на [официальном сайте производителя](#).

⁴⁴ Команды ниже приведены для Postgres Pro версии 16.

⁴⁵ Расположение файла указано для Postgres Pro версии 16, для поиска файла можно использовать команду `sudo find / -type f -name postgresql.conf`

⁴⁶ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

3.3.3.3 Установка СУБД Jatoba⁴⁷

Порядок установки СУБД Jatoba:

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo mkdir /localrepo
```

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

Внимание! Необходимо скопировать полную структуру файлов и каталогов из дистрибутива. Также допускается установка с носителя оптической записи напрямую. В этом случае, пользователю не требуется копировать файлы, а вместо каталога «localrepo» на всех шагах установки указывать соответствующий путь до носителя оптической записи и директорию репозитория СУБД на носителе оптической записи для соответствующей ОС.

- Дистрибутив СУБД Jatoba содержит:
 - каталог `/base`;
 - каталог `/RPMS.classic`;
 - файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

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

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

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

- Обновите описания пакетов командой:

```
sudo apt-get update
```

- Установите основные пакеты СУБД Jatoba 4 командой:

```
sudo 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 директорию расположения исполняемых файлов СУБД Jatoba посредством команды:

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором - установите число подключений `max_connections` в значение `1000`⁴⁸.
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf` под администратором. Измените параметры для успешного локального подключения пользователя к базе данных:

```
host all all 127.0.0.1/32 ident      на host all all 127.0.0.1/32 password
```

⁴⁷ Подробное описание приведено на [официальном сайте производителя](#).

⁴⁸ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

```
host all all ::1/128 ident
```

на

```
host all all ::1/128 password
```

- Включите автоматический запуск СУБД Jatoba при загрузке, выполнив команду:

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

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

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

3.3.4 Установка веб-сервера

3.3.4.1 Установка веб-сервера Apache

Порядок установки веб-сервера Apache:

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

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

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

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

- Создайте файлы:

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

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

- Внесите следующий текст в созданный файл:

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

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

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

- Внесите следующий текст в созданный файл:

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

- Активируйте модули, выполнив поочерёдно команды:

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

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

```
sudo a2enport https
```

3.3.4.2 Установка веб-сервера Nginx

Порядок установки веб-сервера Nginx:

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

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

- Запустите установленный веб-сервер, выполнив команду:

```
systemctl start nginx
```

- Включите автоматический запуск веб-сервер при загрузке, выполнив команду:

```
sudo systemctl enable nginx
```

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

3.4.1 Установка среды исполнения Java

3.4.1.1 Установка Axiom JDK Certified

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

Внимание! В Platform V SberLinux OS Server Axiom JDK Certified версии 21 работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена в Axiom JDK Certified версии 21.0.4+10.

3.4.1.2 Установка OpenJDK

Для установки OpenJDK воспользуйтесь инструкцией по установке пакета [с официального сайта ОС «Platform V SberLinux OS Server»](#).

Внимание! В Platform V SberLinux OS Server OpenJDK определенных версий работает некорректно. В результате установка Центра сертификации Aladdin eCA прерывается. Проблема была выявлена для OpenJDK версий 17.0.15.0.6 и 21.0.7.0.6.

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 приведен в Приложении 1.

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

Центр сертификации Aladdin eCA может быть настроено 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.

3.4.2.1 Установка СУБД PostgreSQL⁴⁹

Порядок установки СУБД PostgreSQL:

- Установите последнюю доступную версию СУБД PostgreSQL, выполнив команду:

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

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

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

⁴⁹ Подробное описание приведено в официальной документации на PostgreSQL, размещённой по адресу <https://postgrespro.ru/docs>.

- Произведите инициализацию БД, выполнив команду:

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

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

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

- Запустите PostgreSQL, выполнив команду:

```
sudo systemctl start postgresql
```

- Добавьте запуск PostgreSQL в автозагрузку, выполнив команду:

```
sudo systemctl enable postgresql
```

- Отредактируйте файл `/var/lib/pgsql/data/postgresql.conf`⁵⁰ под администратором - установите число подключений `max_connections` в значение `1000`⁵¹.
- Отредактируйте файл `/var/lib/pgsql/data/pg_hba.conf`⁵² под администратором - измените параметры для успешного локального подключения пользователя к базе данных:

```
host all all 127.0.0.1/32 ident на host all all 127.0.0.1/32 password
```

```
host all all ::1/128 ident на host all all ::1/128 password
```

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

```
sudo systemctl restart postgresql
```

3.4.2.2 Установка СУБД Postgres Pro⁵³

Порядок установки СУБД Postgres Pro:

- Загрузите скрипт для добавления репозитория, выполнив команду⁵⁴:

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

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

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

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

```
sudo dnf update
```

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

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

- Отредактируйте файл `/var/lib/pgpro/std-16/data/postgresql.conf`⁵⁵ под администратором - установите число подключений `max_connections` в значение `1000`⁵⁶.

⁵⁰ Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁵¹ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

⁵² Расположение файла может отличаться, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

⁵³ Подробное описание приведено в официальной документации на Postgres Pro, размещённой по адресу <https://postgrespro.ru/docs>

⁵⁴ Команды ниже приведены для Postgres Pro версии 16.

⁵⁵ Расположение файла указано для 16 версии Postgres Pro, для поиска можно использовать команду `sudo find / -type f -name postgresql.conf`

⁵⁶ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

- Отредактируйте файл `/var/lib/pgpro/std-16/data/pg_hba.conf`⁵⁷ под администратором - измените параметры для успешного локального подключения пользователя к базе данных:

```
host all all 127.0.0.1/32 ident на host all all 127.0.0.1/32 password
```

```
host all all ::1/128 ident на host all all ::1/128 password
```

- При отсутствии создайте символические ссылки на утилиты `psql` и `pg_dump`, выполнив команды с правами суперпользователя (root или sudo):

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

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

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

3.4.2.3 Установка СУБД Jatoba⁵⁸

- Создайте каталог `/localrepo`, выполнив команду:

```
sudo 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 `/packages`;
 - каталог `/repopdata`;
 - файл ключа `RPM-GPG-KEY-Jatoba`.
- Проверьте результат копирования всех файлов дистрибутива, перейдя в каталог `/localrepo` и выполнив команду:

```
ls -l
```

- Установите открытый ключ репозитория командой:

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

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

```
[jatoba-[версия]]
name=Jatoba [версия] Official Repository
baseurl=file:///localrepo
enabled=1
gpgcheck=0
```

⁵⁷ Расположение файла указано для 16 версии Postgre Pro, для поиска можно использовать команду `sudo find / -type f -name pg_hba.conf`

⁵⁸ Подробное описание приведено в официальной документации на Jatoba, размещённой по адресу <https://www.gaz-is.ru/produkty/inform-sistemy/subd-jatoba.html#materialy>

```
gpgkey=file:///localrepo/RPM-GPG-KEY-Jatoba
```

- Обновите описания пакетов командой:

```
sudo dnf makecache
```

- Установите основные пакеты СУБД Jatoba 4 командой:

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

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

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

```
cd /usr/jatoba-[версия]/bin/
```

- Инициализируйте каталог данных СУБД Jatoba при помощи команды:

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

- Отредактируйте файл `/var/lib/jatoba/[версия]/data/postgresql.conf` под администратором - установите число подключений `max_connections` в значение `1000`⁵⁹.
- Отредактируйте файл `/var/lib/jatoba/[версия]/data/pg_hba.conf` под администратором - измените параметры для успешного локального подключения пользователя к базе данных:

```
host all all 127.0.0.1/32 ident      на host all all 127.0.0.1/32 password
```

```
host all all ::1/128 ident          на host all all ::1/128 password
```

- Добавьте СУБД Jatoba в автозагрузку командой:

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

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

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

3.4.3 Установка веб-сервера

3.4.3.1 Установка веб-сервера Apache

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

```
sudo dnf install httpd
```

- Установите дополнительный модуль для использования протокола SSL, выполнив команду с правами суперпользователя (от имени пользователя root, либо с использованием sudo):

```
sudo dnf install mod_ssl
```

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

```
sudo systemctl enable httpd
```

3.4.3.2 Установка веб-сервера Nginx

Порядок установки веб-сервера nginx:

- Установите пакет из официального репозитория ОС командой:

⁵⁹ Значение `max_connections` равно `1000` является рекомендуемым, при необходимости можно установить и большее значение.

```
sudo dnf install nginx
```

- Запустите установленный веб-сервер командой:

```
sudo systemctl start nginx
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable nginx
```

3.5 Создание службы HTTP и keytab-файла

Предварительно на Центре валидации Aladdin eVA должен быть настроен Kerberos⁶⁰ (должен быть настроен файл `krb5.conf`, рекомендуемое расположение `/etc/krb5.conf`).

При изменении http-службы или при подключении Центра валидации Aladdin eVA к другому домену необходимо заменять keytab-файл.

3.5.1 Получение keytab-файла в Samba DC и Альт Домен

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

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

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

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

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

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

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

- Перейдите в режим суперпользователя, выполнив команду:

```
su
```

- Создайте пользователя-службу, который будет использоваться для авторизации в LDAP, выполнив команду⁶¹:

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

- Разблокируйте созданного пользователя, выполнив команду:

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

- Получите Kerberos-билет для администратора домена, выполнив команду:

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

- Расширьте для созданного пользователя-службы доступные поддерживаемые алгоритмы шифрования, выполнив команду⁶²:

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

⁶⁰ Справочная информация об особенностях настройки Центра регистрации и Центра валидации Aladdin eVA для обеспечения возможности Kerberos-аутентификации в них при их совместной работе на одном хосте приведена в подразделе 5.5 «Руководства администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority».

⁶¹ При подключении нескольких Центров регистрации Aladdin eRA к одному контроллеру домена рекомендуется создать пользователя-службу для каждого Центра регистрации Aladdin eRA.

⁶² В команде ниже `administrator` - это пользователь с правами администратора.

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

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

где <имя настраиваемого клиента> - имя хоста, на котором производится установка Центра валидации Aladdin eVA.

- Измените UPN пользователя-службы, выполнив команду:

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

где <имя настраиваемого клиента> - имя компьютера, на котором производится установка Центра валидации Aladdin eVA.

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

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

где <имя настраиваемого клиента> - имя хоста, на котором производится установка Центра валидации Aladdin eVA.

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

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

3.5.2 Получение keytab-файла в ALD PRO

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

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

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

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

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

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

- Экспортируйте Kerberos-билет HTTP-службы на настраиваемый клиент по рекомендованному пути `/etc/http.keytab`, выполнив команду:

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

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

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

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

3.5.3 Получение keytab-файла в Free IPA

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

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

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

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

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

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

- Экпортируйте Kerberos-билет HTTP-службы на настраиваемый клиент (хост, подготавливаемый для установки Центра валидации Aladdin eVA) по рекомендованному пути `/etc/http.keytab`, выполнив команду:

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

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

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

3.5.4 Получение keytab-файла в MS AD

- На контроллере домена MS AD запустите консоль управления «Active Directory Users and Computers» (ADUC).
- Создайте пользователя-службу, который будет использоваться для валидации Kerberos-билетов, например в организационном юните «Users».
- После создания пользователя-службы включите для него на вкладке «Свойства» - «Учётная запись» в поле «Параметры учётной записи» следующие параметры (остальные параметры должны быть отключены):
 - «Запретить смену пароля пользователем»;
 - «Срок действия пароля не ограничен»;
 - «Данная учётная запись поддерживает 128-разрядное шифрование»;
 - «Данная учётная запись поддерживает 256-разрядное шифрование».
- Привяжите SPN создаваемой HTTP-службы к созданному пользователю и хосту, с одновременным созданием `keytab`-файла (можно экспортировать в любое удобное расположение, например в `http.keytab`). Для этого выполните команду из командной строки PowerShell:

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

где `<имя настраиваемого клиента>` - имя хоста, на котором производится установка Центра валидации Aladdin eVA.

3.6 Установка веб-сервера cnginx

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

- установите следующие пакеты:

- для ОС Astra Linux SE командой `sudo 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 и SberLinux OS Server командой `sudo 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 `sudo 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:

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

- выполните проверку активации лицензии командой:

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

- Запустите установленный веб-сервер, выполнив команду:

```
sudo systemctl start cpnginx.service
```

- Включите автоматический запуск веб-сервера при загрузке, выполнив команду:

```
sudo systemctl enable cpnginx.service
```

3.7 Установка программного средства «Криптографический модуль Aladdin JCP»

Порядок установки криптопровайдера «Aladdin JCP»:

- Получите от ОсОО «Аладдин КГ» набор файлов «Aladdin JCP».
- При отсутствии создайте каталог `/opt/aecaVa/services/cryptoproviders` командой:

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

- Переместите в каталог `/opt/aecaVa/services/cryptoproviders` все файлы криптопровайдера «Aladdin JCP».
- Назначьте права доступа на скопированные файлы:
 - Если выполняется первоначальная установка Центра валидации Aladdin eVA, то назначьте файлам права доступа (`chmod 777`).
 - Если Центр валидации Aladdin eVA был ранее установлен, то назначьте владельцем данных файлов пользователя «аеса» и предоставьте ему права доступа к файлам (`chmod 700`).

- Выполните установку программы (см. раздел 4), если Центр валидации Aladdin eVA не был ранее установлен.
- Если Центр валидации Aladdin eVA был ранее установлен необходимо запустить скрипт с правами суперпользователя в режиме обновления программы:

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

4 УСТАНОВКА ПРОГРАММЫ

Перед установкой Центра валидации Aladdin eVA необходимо выполнить подготовку сервера, где предполагается развёртывание Центра валидации Aladdin eVA, в соответствии с разделом **4** настоящего руководства.

4.1 Установка инсталляционного пакета Центра валидации Aladdin eVA

Установите инсталляционный rpm/deb-пакет Центра валидации Aladdin eVA штатными средствами ОС. Инсталляционный rpm/deb-пакет автоматически распакуется в директорию `/opt/aecaVa`.

Структура инсталляционного rpm/deb-пакета Центра валидации Aladdin eVA приведена в таблице 4.

Таблица 4 - Структура распакованного инсталляционного rpm/deb-пакета Центра валидации Aladdin eVA

Структурный элемент	Назначение элемента
<code>/opt/aecaVa</code>	Установочный комплект Центра валидации Aladdin eVA, а также используемые дополнительные инструменты
<code>/opt/aecaVa/bin</code>	Каталог с дополнительными утилитами
<code>/opt/aecaVa/bin/jcverify</code>	Каталог утилиты контроля целостности «jcverify»
<code>/opt/aecaVa/bin/jcverify/jcverify</code>	Утилита контроля целостности «jcverify»
<code>/opt/aecaVa/bin/jcverify/jcverify.txt</code>	Вспомогательный файл для работы утилиты целостности «jcverify»
<code>/opt/aecaVa/dist</code>	Путь развёртывания продукта; содержит создаваемые временные файлы
<code>/opt/aecaVa/dist/archive/</code>	Архивы, сформированные в результате очистки журнала событий (путь по умолчанию, может быть изменён)
<code>/opt/aecaVa/dist/backup/</code>	Созданные резервные копии Центра валидации Aladdin eVA
<code>/opt/aecaVa/dist/certificates/ssl</code>	Расположение сертификатов для управления ssl-соединением
<code>/opt/aecaVa/dist/environment/</code>	Расположение переменных окружения сервисов
<code>/opt/aecaVa/dist/sign-in/initial_admin.txt</code>	Файл, содержащий логин и пароль администратора инициализации, создаваемого при чистой установке Центра валидации Aladdin eVA
<code>/opt/aecaVa/dist/logs/</code>	Расположения технических логов сервисов
<code>/opt/aecaVa/eula</code>	Файл лицензионного соглашения
<code>/opt/aecaVa/samples</code>	Содержит шаблоны файлов конфигурации для внутреннего использования программным средством

Структурный элемент	Назначение элемента
/opt/aecaVa/scripts	Содержит скрипты управления Центра валидации Aladdin eVA
/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 Центра валидации Aladdin eVA
/opt/aecaVa/scripts/config.sh	Файл конфигурации Центра валидации Aladdin eVA
/opt/aecaVa/scripts/database_create.sh	Скрипт создания базы данных и её пользователя на сервере Центра валидации Aladdin eVA с указанными в конфигурационном файле параметрами
/opt/aecaVa/scripts/diagnostics.sh	Скрипт сбора диагностической информации Центра валидации Aladdin eVA
/opt/aecaVa/scripts/install.sh	Скрипт установки и обновления Центра валидации Aladdin eVA
/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 Центра валидации Aladdin eVA
/opt/aecaVa/scripts/uninstall.sh	Скрипт удаления Центра валидации Aladdin eVA
/opt/aecaVa/scripts/jc_checksum	Файл с эталонами контрольных сумм исполняемых файлов Центра валидации Aladdin eVA
/opt/aecaVa/scripts/key	Файл, содержащий симметричный ключ шифрования паролей в конфигурационном файле Центра валидации Aladdin eVA
/opt/aecaVa/services	Сервисы Центра валидации Aladdin eVA
/opt/aecaVa/static	Артефакты клиентского компонента Центра валидации Aladdin eVA
/opt/aecaVa/digsig/keys/aladdin_pub.key	Открытый ключ, используемый для проверки подписи исполняемых файлов и библиотек Центра валидации Aladdin eVA 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 Поддержка активного режима замкнутой программной среды в ОС Astra Linux Special Edition

Центр валидации Aladdin eVA обеспечивает работу ОС Astra Linux Special Edition 1.7 и Astra Linux Special Edition 1.8 в [активном режиме замкнутой программной среды \(далее - ЗПС\)](#). Для этого в состав установочных пакетов Центра валидации Aladdin eVA включён публичный открытый ключ ОсОО «Аладдин КГ» – `aladdin_pub.key`. После распаковки установочного пакета ключ находится в каталоге `/opt/aecaVa/digisig/keys/aladdin_pub.key`.

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

4.3 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 5.

Таблица 5 - Параметры конфигурации

Ключ	Значение по умолчанию	Описание
webserver	'#CHANGEIT'	Используемый web-сервер. Допустимые значения: "nginx", "apache", "cprnginx"
webserver_path	'#CHANGEIT'	Папка с файлами для развёртывания сервиса (по умолчанию: конфигурация nginx располагается по пути <code>/etc/nginx</code> , для Astra Linux конфигурация apache располагается по пути <code>/etc/apache2</code> , для РЕД ОС и SberLinux OS Server конфигурация apache располагается по пути <code>/etc/httpd</code> , конфигурация cprnginx располагается по пути <code>/etc/opt/cproscsp/cprnginx</code>)
aeca_path	'/opt/aecaVa/dist'	Папка с файлами для развёртывания Центра валидации
environment_path	'/opt/aecaVa/dist/environment'	Папка с переменными окружения для сервисов
cryptotoken_path	'/opt/aecaVa/dist/cryptotoken'	Каталог хранения контейнеров служб OCSP
webserver_config_path	'/opt/aecaVa/dist/webserver'	Расположение конфигурации Центра валидации 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 разработчиками. Редактировать не следует
proxy_send_timeout	'320'	Время ожидания ответа от прокси-сервера после отправки запроса. Если ответ не получен в течение этого времени, запрос считается неудачным. Только для nginx.

Ключ	Значение по умолчанию	Описание
		Настраивается разработчиками. 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 разработчиками. Редактировать не следует
ssl_protocols	'TLSv1.2 TLSv1.3'	Поддерживаемые версии протокола TLS. Доступно использование только TLSv1.2 и/или TLSv1.3 (при использовании обеих версий протокола необходимо указывать их через пробел)
ssl_ciphers	'#CHANGEIT'	<p>Поддерживаемые наборы шифров для TLS-соединения. Данный параметр позволяет ограничить наборы шифров (cipher suites), которые могут использоваться при TLS-соединении. Разделитель между наборами - «;». Если клиент не поддерживает ни один из указанных в данном параметре наборов, TLS-соединение не будет установлено.</p> <p>По умолчанию значение в данном параметре не задано, что означает отсутствие управления со стороны Центра валидации перечнем допустимых наборов шифров (ciphersuites) TLS-соединения для веб-сервера.</p> <p>В данном параметре могут быть указаны любые наборы шифров, поддерживаемые используемой на сервере Центра валидации версией Openssl для TLS версии 1.2.</p> <p>Получить список поддерживаемых используемым Openssl наборов шифров для TLS версии 1.2 можно с помощью команды:</p> <pre>openssl ciphers -tls1_2 -s</pre> <p>Данный параметр учитывается только при использовании Nginx или Apache. Конфигурирование наборов шифров TLS-соединения для Cppnginx осуществляется с помощью утилиты «срconfig» из состава СКЗИ «КриптоПро CSP».⁶³</p>
backup_path	'/opt/aecaVa/dist/backup'	Папка, в которую сохраняются резервные копии Центра валидации
logs_base	'/opt/aecaVa/dist/logs'	Папка, в которой хранятся лог-файлы

⁶³ Инструкция по установке и настройке cрnginx - <https://support.cryptopro.ru/index.php?Knowledgebase/Article/View/440/0/nginx-gost-binary-packages>. Описание порядка конфигурирования наборов шифров представлено в разделе 6 данной инструкции.

Ключ	Значение по умолчанию	Описание
archive_path	'/opt/aecaVa/dist/archive'	Папка, в которую сохраняется архив журнала событий, сформированный в результате автоматической архивации по заданным параметрам
certificates_ssl_path	'/opt/aecaVa/dist/certificates/ssl'	Папка, содержащая сертификат веб-сервера и цепочки сертификатов разрешённых издателей
aeca_user	'aeca'	Имя пользователя Центра валидации, используемое для работы программы
aeca_group	'aeca'	Группа, в которой состоит пользователь Центра валидации
memory	'4096'	Максимальный лимит оперативной памяти (МБ)
enable_gc_diagnostic	'false'	Флаг сбора диагностической информации о памяти
enable_heap_dump	'false'	Флаг сбора дампов памяти для завершившихся аварийно сервисов Центра валидации
Конфигурация БД		
max_db_pool_size	'50'	Максимальный размер пула подключений к СУБД. Настраивается разработчиками. Редактировать не следует
use_tls	'false'	Флаг обязательного использования TLS для подключения к СУБД. Допустимые значения: true, false
database_username	'aeca'	Имя пользователя базы данных, используемое для работы Центра валидации
database_password	'#CHANGEIT'	Указывается администратором инициализации при установке. Пароль пользователя базы данных, используемый для работы Центра валидации. Пароль не должен содержать специальные символы « » и «\»
database_host	'localhost'	Сетевой адрес базы данных
database_port	'5432'	Порт, используемый для подключения к базе данных
database_name	'aecava'	Имя базы данных, используемой Центром валидации
root_cert_path	'#CHANGEIT'	Абсолютный путь к сертификату корневого ЦС из цепочки сертификатов сервера СУБД.
Конфигурация Центра валидации Aladdin eVA		

Ключ	Значение по умолчанию	Описание
http_port	'80'	Порт для подключения к программному комплексу по протоколу http
https_port	'433'	Порт для подключения к программному комплексу по протоколу https
hostname	'localhost'	Имя сервера, на котором развёртывается Центр валидации Aladdin eVA
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
number_of_services	'9'	Количество активных сервисов в системе. Настраивается разработчиками, редактировать не следует
logging_response	'false'	Флаг для сбора и регистрации ответов сервисов
logging_sql	'false'	Флаг для сбора и регистрации информации о подключениях и запросах к базе данных PostgreSQL
Переменные окружения для logback		
logs_file_max_size	'10MB'	Максимальный размер лог-файла (файла с диагностической информацией) сервиса перед его архивацией. При достижении данного значения текущий лог-файл (access.log или service.log) будет заархивирован. Файл будет сохранен в текущем каталоге хранения лог-файлов данного сервиса с именем {access или service}-{дата в формате YYYY-MM-DD}.{индекс лога}.log.
logs_max_history	'10'	Максимальный срок хранения архивов с лог-файлами в днях. Архивы, срок хранения которых превышает указанное в данном параметре значение, будут автоматически удаляться
logs_total_size_cap	'100MB'	Максимальный общий объем лог-файлов, включая архивы, каждого типа (access или service) для каждого сервиса. При достижении данного объема наиболее старые архивы данного типа будут удаляться
api_key	'2d2ec9b4-ad3d-4ed0-8961-d2a4ab99d810'	Значение ключа для внутренней аутентификации. Для служебного пользования
Переменные окружения, используемые settings-service		
certificate_server_name	'#CHANGEIT'	Имя файла сертификата web-сервера

Ключ	Значение по умолчанию	Описание
certificate_raw_server_password	'#CHANGEIT'	Пароль от контейнера сертификата web-сервера
issuers_name	'issuers'	Имя файла разрешённых издателей, получаемого от Центра сертификации
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. По истечению данного срока маркер обновления нельзя использовать для этого. И для получения нового маркера доступа и обновления потребуются повторная аутентификация.
token_expire	'180000'	Время жизни JWT-токена (маркера доступа), мс
Переменные окружения, используемые security-service		
kerberos_enabled	'false'	Активация kerberos
session_max_count	'100'	Максимальное число одновременных сессий аккаунта в виде натурального числа. При указании значения «-1» ограничение на количество одновременных сессий пользователя будет отсутствовать
kerberos_service_principal	'#CHANGEIT'	Имя принципала, используемого для авторизации
kerberos_keytab_location	'#CHANGEIT'	Расположение keytab файла, содержащего тикет принципала, используемого для авторизации
kerberos_krb5_location	'#CHANGEIT'	Расположение файла конфигурации krb5.conf
kerberos_ad_domain	'#CHANGEIT'	Имя подключаемого домена
kerberos_ad_server	'#CHANGEIT'	Адрес сервера AD (ldap)
resource_type	'#CHANGEIT'	Тип ресурсной системы (FREE_IPA, ALD_PRO, SAMBA_DC, MS_AD, RED_ADM, ALT_DOMAIN)
resource_base_dn	'#CHANGEIT'	Точка подключения ресурса
ldap_enabled	'false'	Активация ldap

Ключ	Значение по умолчанию	Описание
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
sign_provider	'EMBEDDED'	Провайдер подписи маркера доступа (выбирается между стандартным - 'EMBEDDED', СКЗИ «КриптоПро CSP» - 'CRYPTO_PRO' и 'ALADDIN_JCP' для китопровайдера Aladdin JCP))
sign_key_algorithm	'RSA'	Алгоритм ключа подписи маркера доступа. Для стандартного провайдера доступны алгоритмы 'RSA' и 'ECDSA'. Для провайдера КриптоПро доступны алгоритмы 'RSA' и 'GOST_R_34_10_2012'. Для провайдера Aladdin JCP доступен алгоритм 'GOST_R_34_10_2012'.
sign_key_length	'2048'	Длина ключа подписи маркера доступа
sign_hash_algorithm	'SHA512'	Алгоритм хэширования подписи маркера доступа, Доступные для выбора значения алгоритмов хэширования: 1) для стандартного провайдера (EMBEDDED): <ul style="list-style-type: none"> для алгоритма ключа 'RSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' для алгоритма ключа 'ECDSA' доступны алгоритмы хэширования 'SHA1', 'SHA256', 'SHA512', 'SHA384' 2) для провайдера КриптоПро (CRYPTO_PRO): <ul style="list-style-type: none"> 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

Ключ	Значение по умолчанию	Описание
archive_millis_ago	'15778800000'	Период архивации (мс) (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 Aladdin eCA
Переменные окружения, используемые api-gateway-service		
max_requests_count	'30'	Максимальное число параллельных HTTP запросов. При превышении числа запросов в систему данного значения, для последующих запросов будет возвращаться HTTP код ошибки 429 (Слишком много запросов). Настраивается разработчиком, редактировать не следует

Необходимо определить значения следующих параметров:

- `webserver` - используемый веб-сервер ('nginx', 'apache' или 'cprnginx'). 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/cprosp/cprnginx` для cprnginx;
- `database_password` – пароль создаваемой базы данных (имя базы данных по умолчанию - aecava). Пароль не должен содержать символы «|» и «\». После создания и настройки базы данных (см. раздел 4.4) пароль пользователя базы данных будет отображаться в конфигурационном файле в зашифрованном виде (алгоритм шифрования AES-256 с использованием сгенерированного в файле `/opt/aecaVa/scripts/key` ключа шифрования).
- `certificate_raw_server_password` - укажите пароль от контейнера закрытого ключа веб-сервера.
- `root_cert_path` - укажите 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` - укажите полное доменное имя компьютера, на котором будет развёрнут Центра регистрации Aladdin eVA.

При использовании 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 Центра сертификации Aladdin eCA 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 6.

Таблица 6 - Параметры для настройки TLS ГОСТ

Параметр	Значение
webserver	'cpnginx'
webserver_path	'/etc/opt/cproscsp/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 Центре валидации Aladdin eVA субъектов домена, к которому подключён Центр валидации Aladdin eVA и Центр сертификации Aladdin eCA, 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 Центр валидации Aladdin eVA; 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 Центр валидации Aladdin eVA.
Пример: `kerberos_keytab_location='/opt/va-22/pki_admin_http.keytab'`.
- `kerberos_krb5_location` - путь к файлу krb5.conf хоста, на котором размещается Центр валидации Aladdin eVA. 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>`.
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'`.

4.4 Создание и настройка базы данных

База данных Центра валидации Aladdin eVA (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 Центра валидации Aladdin eVA необходимо создать и настроить перед установкой Центра валидации Aladdin eVA. Это может быть выполнено одним из следующих способов:

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

После создания и настройки базы данных пароль пользователя базы данных, заданный в конфигурационном файле `/opt/aecaVa/scripts/config.sh` в параметре `database_password`, будет отображаться в зашифрованном виде. Шифрование пароля выполняется по алгоритму AES-256 с использованием автоматически сгенерированного в файле `/opt/aecaVa/scripts/key` ключа шифрования. Пароль не должен содержать символы «|» и «\».

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 (см. 4.3).

Для создания и настройки базы данных запустите скрипт⁶⁴ командой:

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

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).

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 команду:

```
sudo systemctl start postgresql
```

- Включите автоматический запуск PostgreSQL при загрузке, выполнив команду:

```
sudo systemctl enable postgresql
```

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

⁶⁴ Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).


```
sudo -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. 4.3).

- Задайте пароль пользователю, выполнив команды:

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

где `'aeca'` - задаваемый пароль пользователя по умолчанию. В случае указания отличного пароля, требуется соответственно отредактировать конфигурационный файл (см. 4.3).

- 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. 4.3).

- 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 команду:

```
sudo systemctl restart postgresql
```

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

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

где `aecava` - имя созданной базы данных.

4.4.3 Создание и настройка базы данных Jatoba в ручном режиме

Требования к настройке предварительно установленной СУБД Jatoba:

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

Возможно использование локальной СУБД или удалённой, доступной для подключений.

- Запустите Jatoba командой:

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

- Включите автоматический запуск Jatoba при загрузке, выполнив команду:

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

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

РЕД ОС и SberLinux OS Server `sudo -u postgres psql`

Astra Linux SE `sudo -u postgres psql`

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

- Создайте пользователя базы данных, выполнив команды:

```
CREATE USER aeca;
```

где `aeca` - задаваемое имя пользователя.

- Задайте пароль пользователю, выполнив команды:

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

где `'aeca'` - задаваемый пароль пользователя.

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

- Создайте базу данных, выполнив команду:

```
CREATE DATABASE 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:

```
exit
```

- Перезапустите СУБД Jatoba, выполнив команду:

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

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

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

где `aecava` - имя созданной базы данных.

4.5 Установка программы

В процессе установки осуществляется:

- создание системного пользователя и соответствующей группы, от имени которых функционирует Центр валидации Aladdin eVA;
- установка прав для создаваемого пользователя Центра валидации Aladdin eVA;

- установка контейнера сертификата, используемого для авторизации в Центре сертификации Aladdin eCA;
- установка контейнера сертификата веб-сервера Центра валидации Aladdin eVA;
- подготовка, установка параметров и служебных сервисов;
- запуск служебных сервисов;
- запись номера сборки Центра валидации Aladdin eVA в базу данных⁶⁵.

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.

Для установки программы:

1. Запустите скрипт⁶⁶ командой:

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

2. 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 при использовании Astra Linux Special Edition и наличии мандатных политик⁶⁷ выведено сообщение:

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

- 3.1. Явно назначьте классификационную метку пользователю `aeca` командой:

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

- 3.2. Перейдите к шагу 1.

4. Если ранее Центр валидации Aladdin eVA уже был установлен будет предложено:

- установить ПО;
- обновить ПО;
- завершить работу инсталлятора.

Подтвердите выбор действия, вводом цифры «1».

5. 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».

6. 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.
7. Введите полный путь до ранее подготовленного и скопированного на жёсткий диск файла контейнера сертификата PCS#12 веб-сервера.

⁶⁵ Значение номера сборки записывается в таблицу «build_info» схемы «aeca_ra_info».

⁶⁶ Выполнение скрипта требует наличия утилиты `psql` из пакета СУБД (`postgresql`, `postgresql-client`, `postgrespro-std`, `jatoba4-client`).

⁶⁷ Подробная информация по аутентификации в СУБД PostgreSQL для Astra Linux Special Edition приведена в <https://wiki.astralinux.ru/pages/viewpage.action?pageId=238751148>

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

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

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

В Центре сертификатов доступа поддерживается совместная работа Центра сертификации Aladdin eCA, Центра регистрации Aladdin eRA и Центра валидации Aladdin eVA на одном сервере. Также поддерживается совместная работа Центра регистрации Aladdin eRA и Центра валидации Aladdin eVA, а также Центра валидации Aladdin eVA и Центра сертификации Aladdin eCA на одном сервере.

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

4.2 Подключение к веб-интерфейсу

4.2.1 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 4.2.2.

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 `cpptools` 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 (cpptools)» ЖТЯИ.00101-03 92 06.

- Установлен веб-браузер Chromium с поддержкой TLS ГОСТ из состава ОС. Данный веб-браузер входит в состав базовых репозиториях ОС Astra Linux SE, Альт Сервер, РЕД ОС и SberLinux OS Server.

4.2.2 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-браузера⁶⁸.

Процесс установки сертификата рассмотрим на примере браузера Firefox:

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

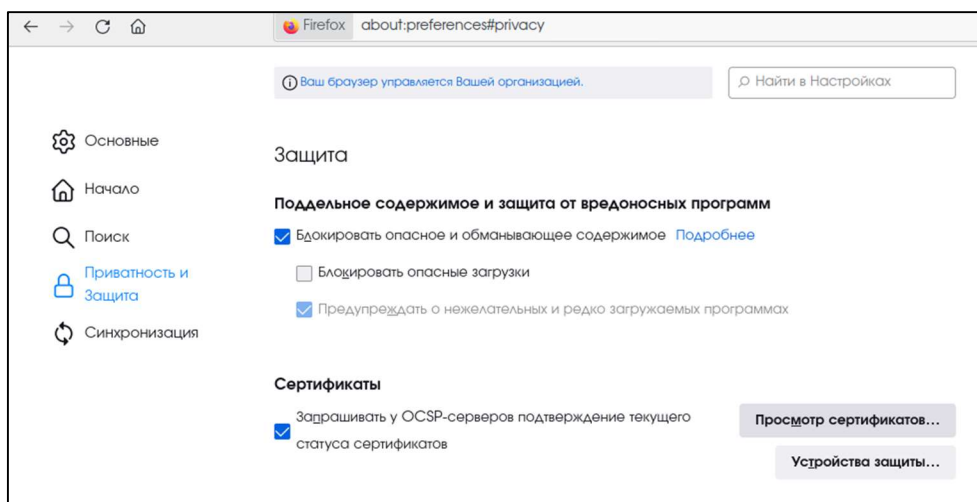


Рисунок 1 - Окно настроек браузера

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

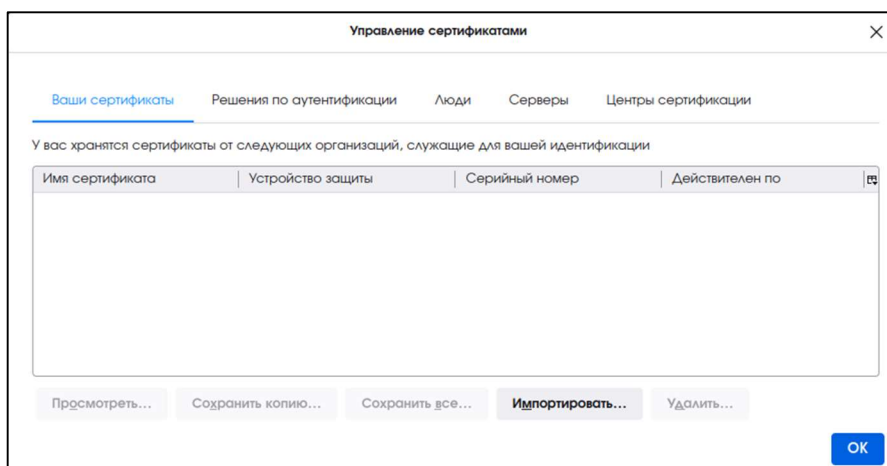


Рисунок 2 - Окно управления сертификатами

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

⁶⁸ Сертификат администратора из контейнера закрытого ключа PKCS#12, выпущенного с использованием алгоритмов ГОСТ, устанавливается в личное хранилище пользователя с помощью утилиты crtools из состава СКЗИ «КриптоПро CSP».

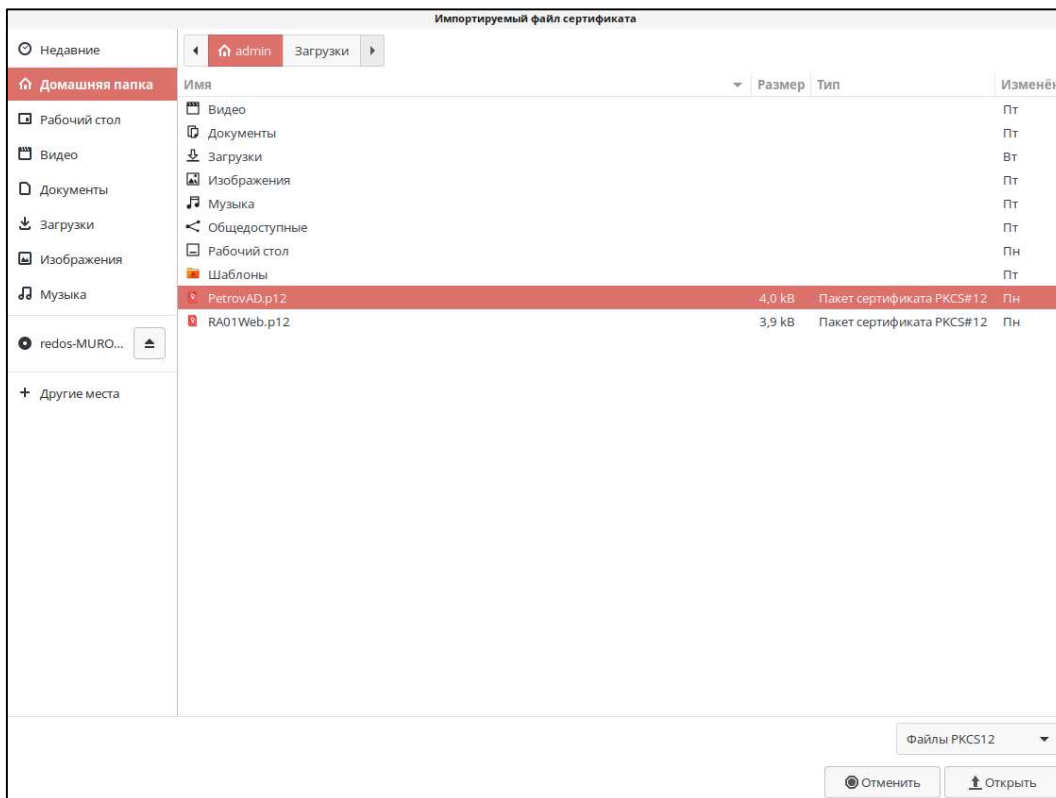


Рисунок 3 - Окно выбора импортируемого файла сертификата

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

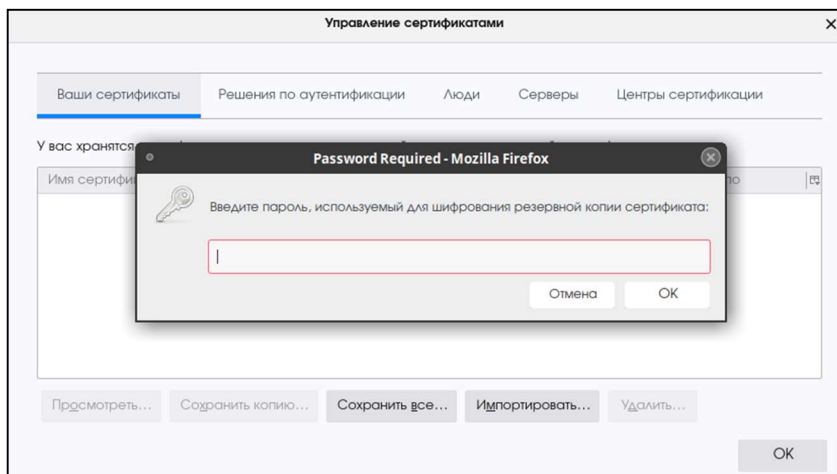


Рисунок 4 - Окно ввода PIN-кода сертификата

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>.

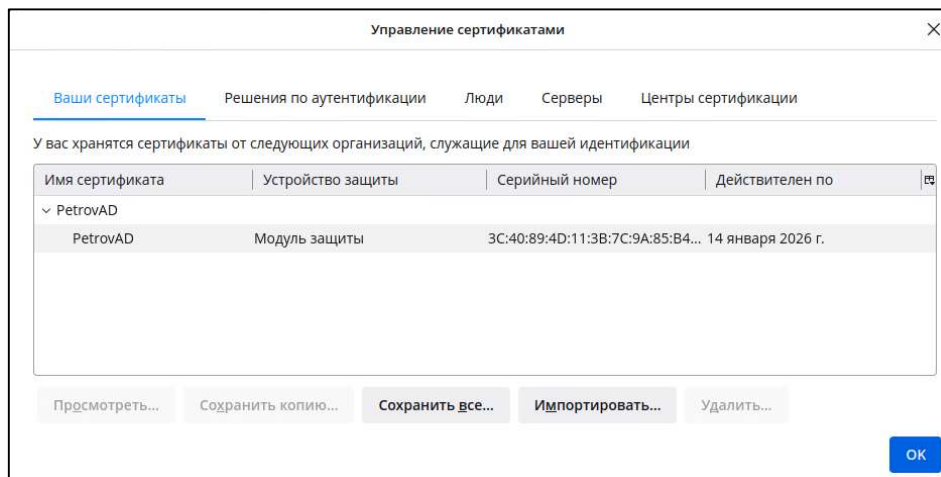


Рисунок 5 - Окно «Управление сертификатами»

4.2.3 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 <OK>.

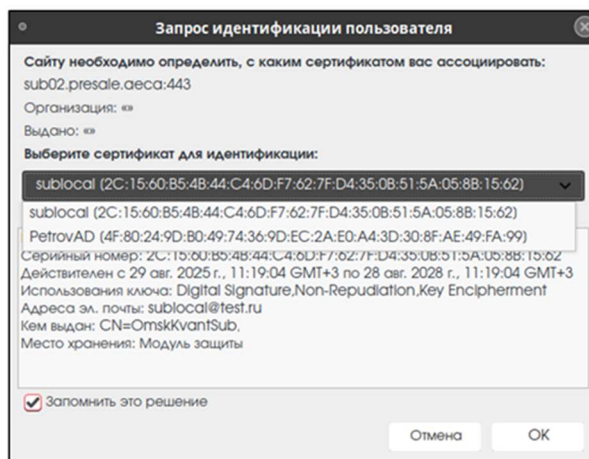


Рисунок 6 - Окно выбора сертификата

4.2.4 Доступ к программе

Центр валидации Aladdin eVA предоставляет возможность аутентификации в нем:

- администраторам подключённых Центров сертификации Aladdin eCA⁶⁹;
- администратору инициализации Центра валидации Aladdin eVA.

⁶⁹ Управление подключениями к Центру сертификации Aladdin eCA осуществляется администратором инициализации в разделе «Настройки».

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. 6.3.8).

Центр валидации Aladdin eVA позволяет администраторам подключённых Центров сертификации Aladdin eCA аутентифицироваться в нем по сертификатам.

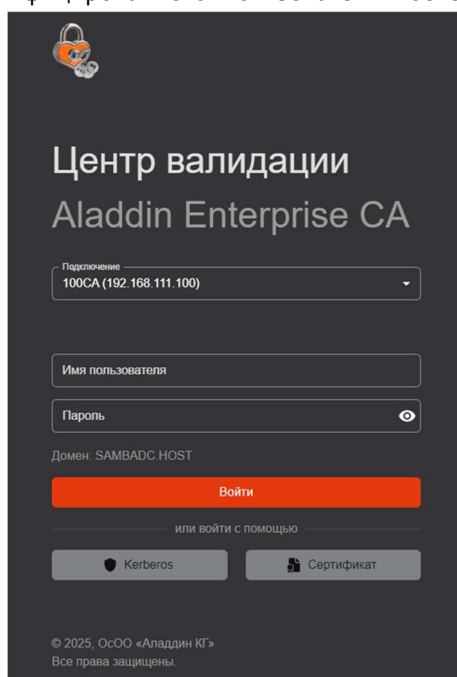
Для учётных записей администраторов Центров сертификации Aladdin eCA, созданных на основе субъектов ресурсных систем, к которому подключён Центр валидации Aladdin eVA и данный Центр сертификации Aladdin eCA аутентификация возможна:

- по имени и паролю доменного пользователя, на основе которого создана учётная запись;
- по Kerberos-билету доменного пользователя, на основе которого создана учётная запись.

Центр валидации Aladdin eVA позволяет администратору инициализации аутентифицироваться в нем по логину и паролю⁷⁰.

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

В пользовательском интерфейсе Центра валидации Aladdin eVA при попытке доступа неаутентифицированного пользователя после установки TLS-соединения отображается окно авторизации (см.



рисунок

Рисунок 7).

⁷⁰ Учётная запись администратора инициализации Центра валидации Aladdin eVA создаётся при чистой установке Центра валидации Aladdin eVA.

Рисунок 7 – Окно авторизации

В окне авторизации Центра валидации Aladdin eVA присутствуют:

- поле выбора подключения «Подключение». В данном поле отображаются все подключения к Центру сертификации Aladdin eCA, а также вариант выбора «Локальное». Подключения к Центру сертификации Aladdin eCA 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 Центр 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 Центра валидации Aladdin eVA:
 - 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 Центра валидации Aladdin eVA:

- 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 Центра валидации Aladdin eVA:

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

Для аутентификации по Kerberos-билету⁷¹ в окне авторизации Центра валидации Aladdin eVA:

- Выберите подключение к Центру сертификации Aladdin eCA 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.

⁷¹ 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.

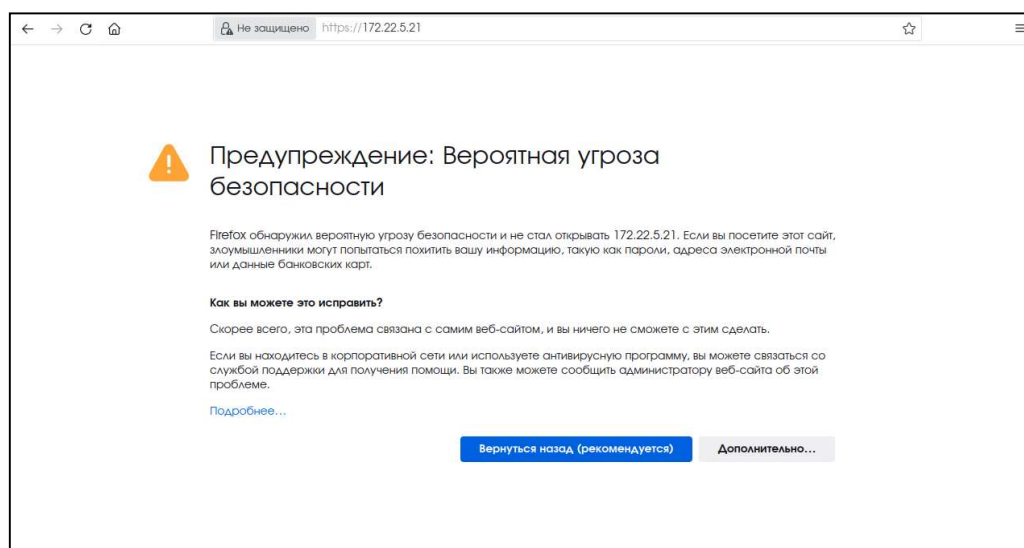


Рисунок 9 - Страница с предупреждением системы безопасности

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

5 ЗАПУСК И ЗАВЕРШЕНИЕ ПРОГРАММЫ

Центр валидации Aladdin eVA запускается автоматически с запуском операционной системы.

5.1 Проверка состояния программы

Для проверки состояния Центра валидации Aladdin eVA в терминале:

- выполните команду с правами суперпользователя (root или sudo):

```
sudo 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.

5.2 Запуск программы в ручном режиме

Для запуска Центра валидации Aladdin eVA в терминале выполните команду с правами суперпользователя (root или sudo):

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

5.3 Завершение работы программы

Для завершения работы Центра валидации Aladdin eVA в терминале выполните команду с правами суперпользователя (root или sudo):

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

6 ФУНКЦИИ УПРАВЛЕНИЯ ПРОГРАММЫ

6.1 Главное окно Центра валидации Aladdin eVA

В главном окне Центра валидации Aladdin eVA присутствуют:

- шапка программы;
- в левой части экрана, под шапкой, следующие разделы:
 - «Центры валидации»;
 - «Журнал событий»;
 - «Настройки».

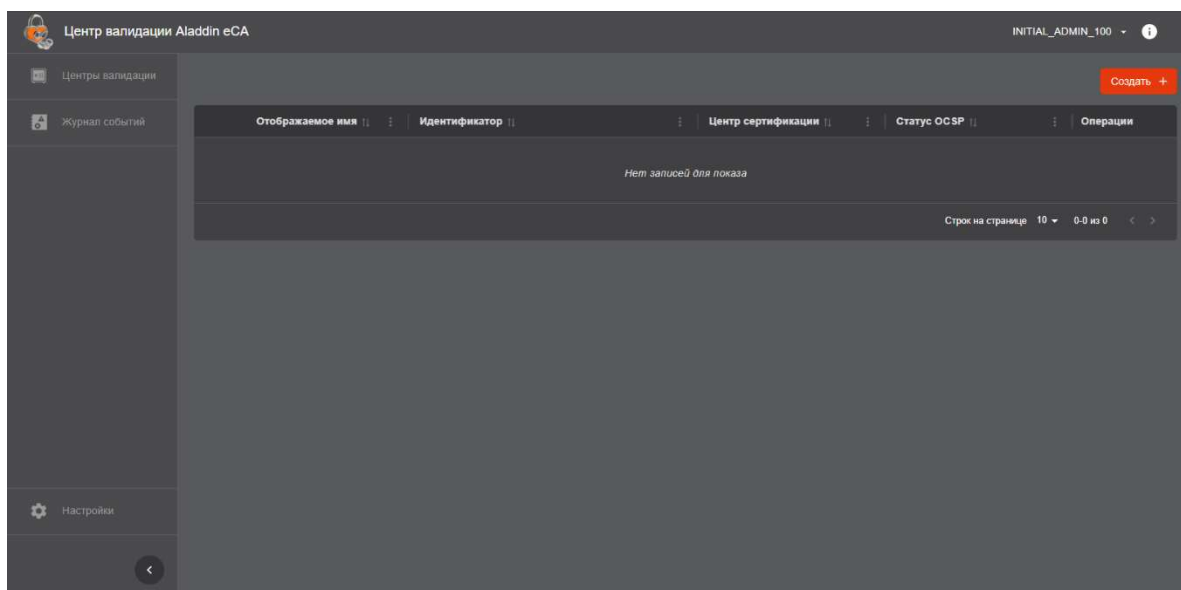


Рисунок 10 — Главное окно Центра валидации Aladdin eVA

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 Центре валидации Aladdin eVA.

В окне «О программе» должны присутствовать следующие сведения:

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

6.2 Раздел «Центры валидации»

Данный раздел доступен только пользователю с ролью «Администратор».

В разделе «Центры валидации» главного окна Центра валидации присутствуют (см. рисунок 11):

- Кнопка «Создать» для создания нового Центра валидации.
- Список существующих в программе Центров валидации. Для администратора подключённого Центра сертификации Aladdin eCA в списке присутствуют только Центры валидации, обслуживающие Центры сертификации его экземпляра Центра сертификации Aladdin eCA.
- 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 Центре сертификации Aladdin eCA;

- «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 Delta 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 Центру сертификации Aladdin eCA было отключено (например, если данный Центр валидации удалён в Центре сертификации Aladdin eCA). При наведении курсора на данную индикацию отображаться всплывающее сообщение «Отсутствует подключение к обслуживаемому центру сертификации».

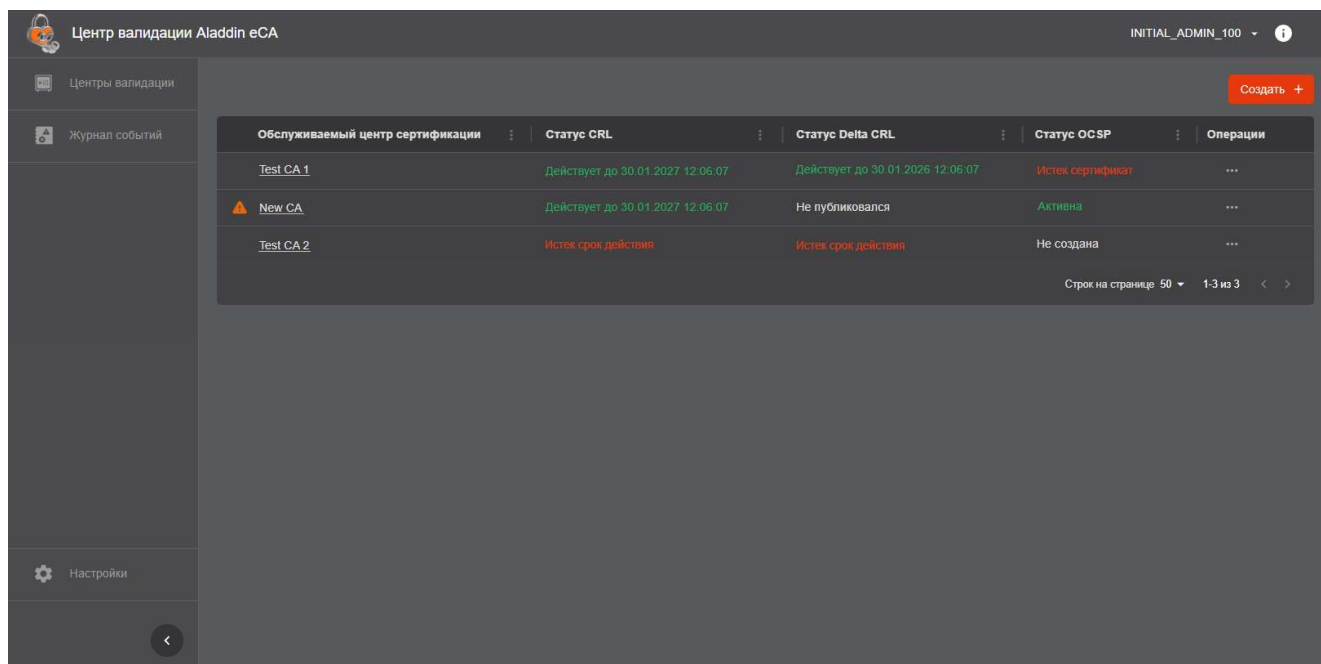


Рисунок 11 - Окно раздела «Центры валидации» Центра валидации Aladdin eVA

6.2.1 Карточка Центра валидации

Для перехода к карточке Центра валидации необходимо щёлкнуть левой кнопкой мыши на строке с записью Центра валидации в разделе «Центры валидации» (см. 6.1).

В карточке Центра валидации (см. рисунок 12) отображаются:

- кнопка «Переподключиться», для повторной регистрации данного Центра валидации в Центре сертификации Aladdin eCA. Данная кнопка присутствует только для Центра валидации, у которого отсутствует подключение к обслуживаемому ЦС Центра сертификации Aladdin eCA;
- 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 Центра сертификации Aladdin eCA. Значение в данном поле является гиперссылкой на карточку данного ЦС в Центре сертификации Aladdin eCA. Справа от значения в данном поле в случае потери подключения Центра валидации к ЦС Центра сертификации Aladdin eCA 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.

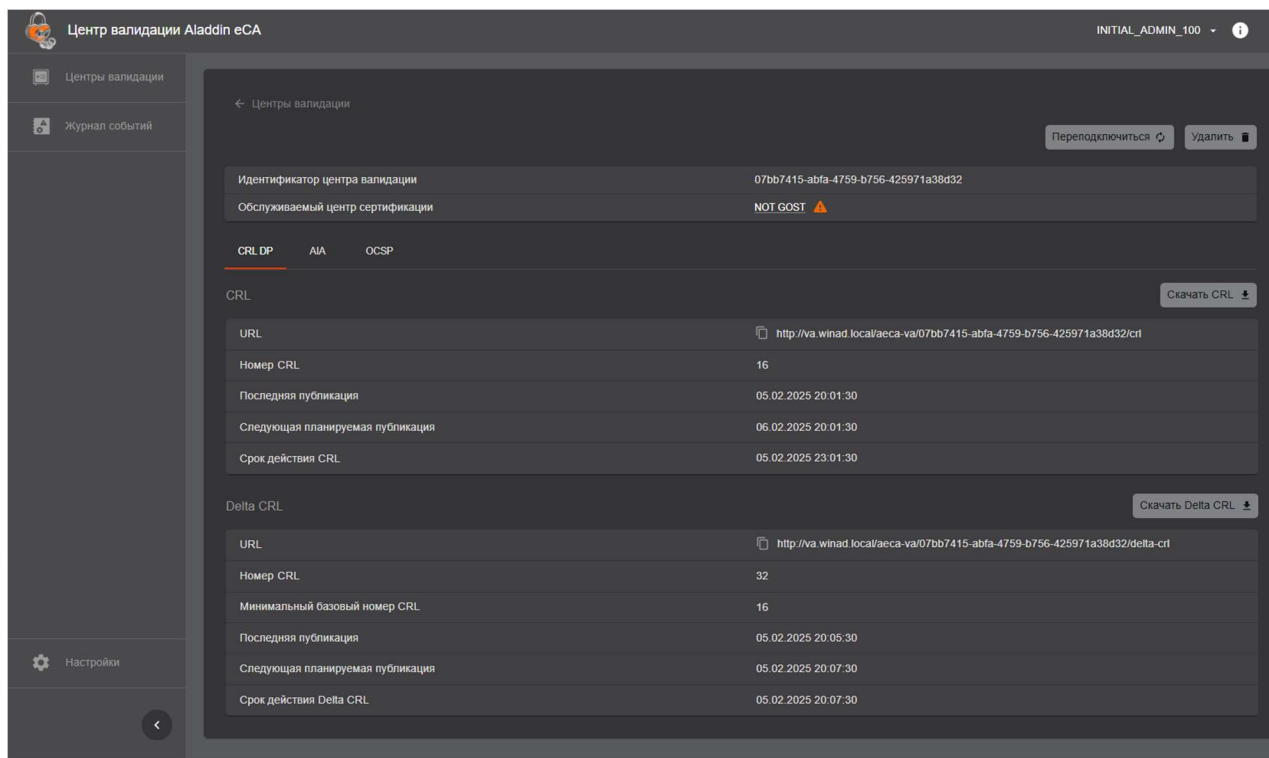


Рисунок 12 - Окно карточки Центра валидации

6.2.1.1 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.

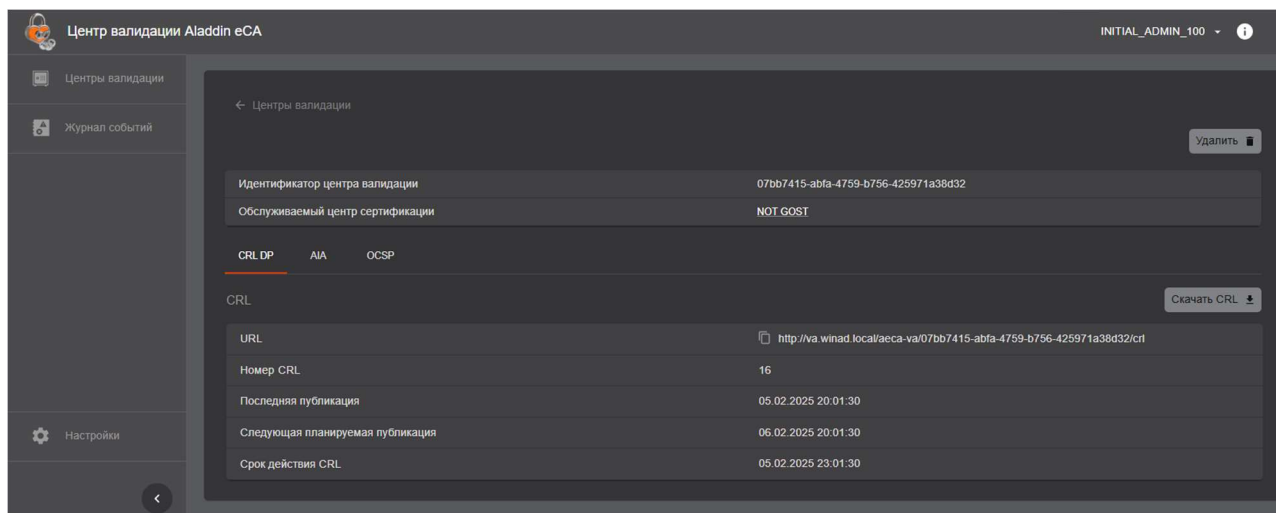


Рисунок 13 - Карточка Центра валидации. Вкладка «CRL DP». Delta CRL не публикуется в данный ЦВ

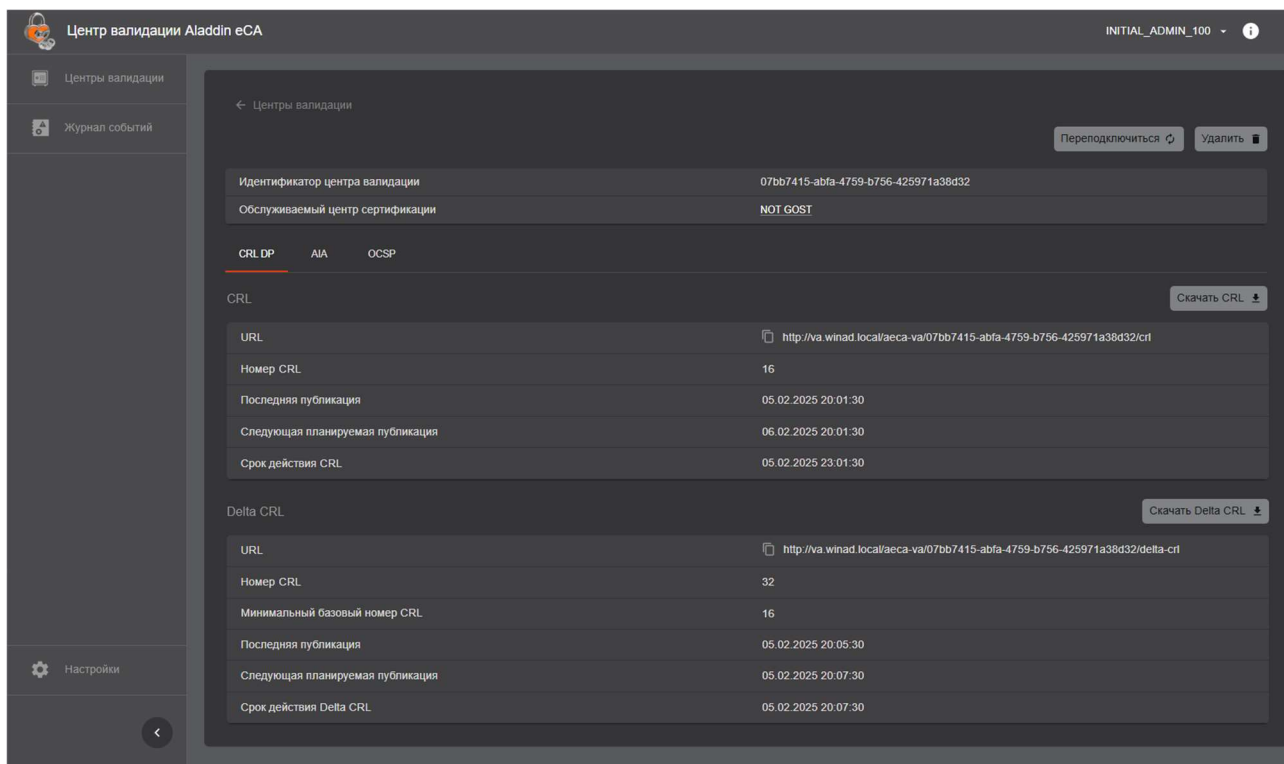


Рисунок 14 - Карточка Центра валидации. Вкладка «CRL DP». Delta CRL публикуется в данный ЦВ.

6.2.1.2 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.

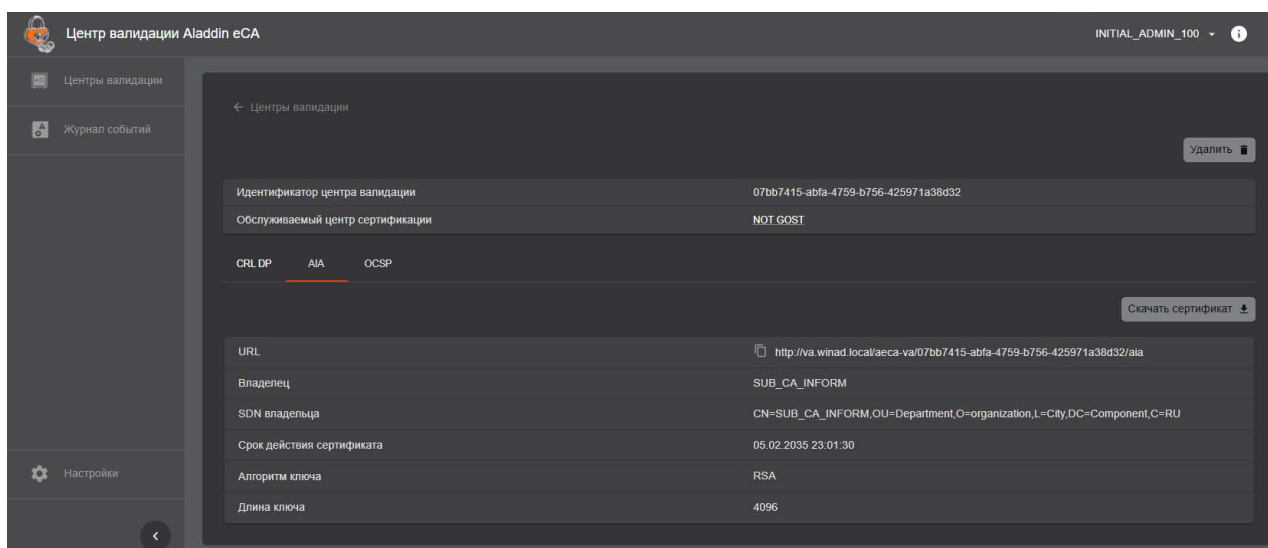


Рисунок 15 - Карточка Центра валидации. Вкладка «AIA»

6.2.1.3 Вкладка «OCSP»

На вкладке «OCSP» при отсутствии созданной для данного Центра валидации службы OCSP отображается кнопка «Создать службу OCSP» (см. рисунок 16) для запуска сценария создания службы OCSP (см. «Создание службы OCSP созданного Центра валидации»). При этом кнопка недоступна для нажатия, если у данного Центра валидации отсутствует подключение к обслуживаемому Центру сертификации (см. рисунок 17).

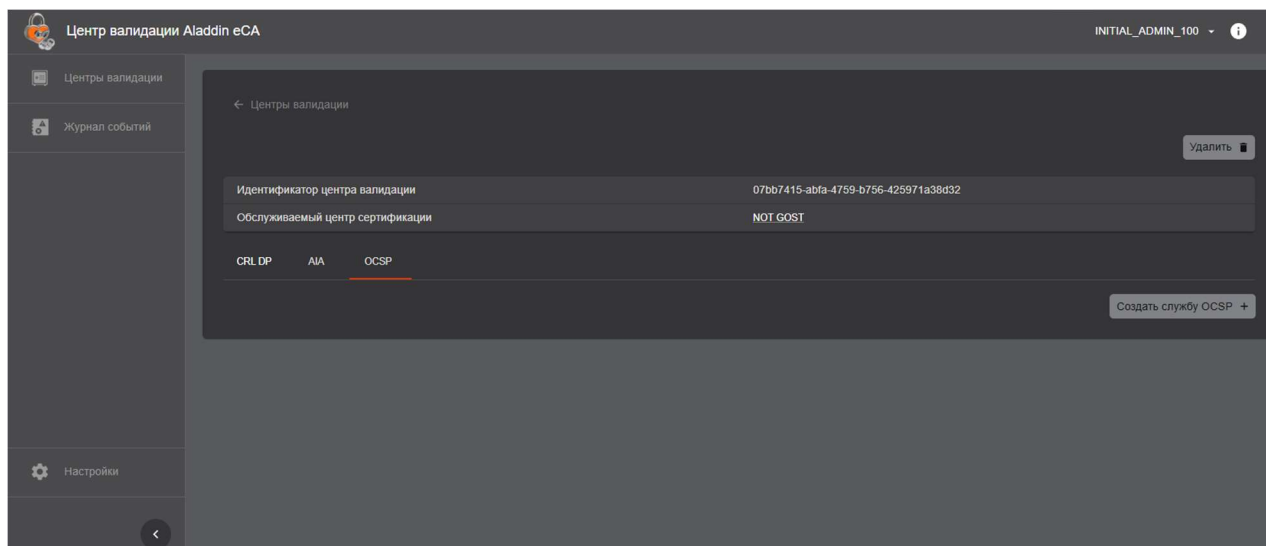


Рисунок 16 - Карточка Центра валидации, вкладка «OCSP» при отсутствии у Центра валидации созданной службы OCSP

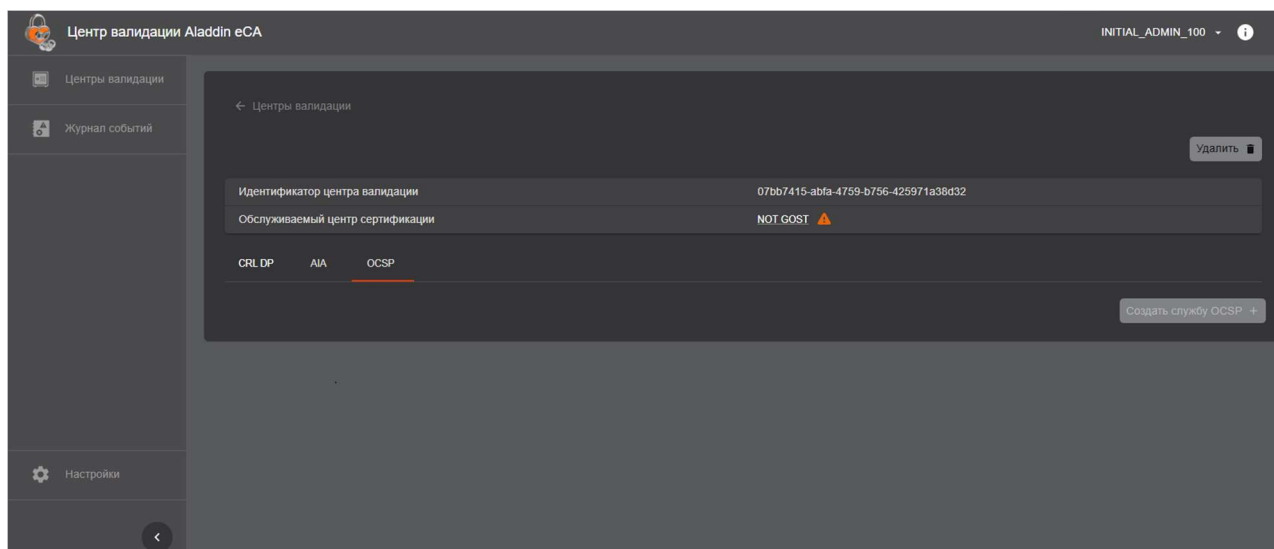


Рисунок 17 - Карточка Центра валидации, вкладка «OCSP» при отсутствии у Центра валидации созданной службы OCSP и при отсутствии подключения к обслуживаемому Центру сертификации

На вкладке «OCSP» при наличии созданной для данного Центра валидации службы OCSP (см. рисунок 18) 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 значения 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 Центре сертификации Aladdin eCA;
 - «Шаблон», содержащее шаблона сертификата службы OCSP. Значение в данном поле является гиперссылкой на карточку данного шаблона в подключённом Центре сертификации Aladdin eCA;
 - «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 Центре сертификации Aladdin eCA;
 - «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.

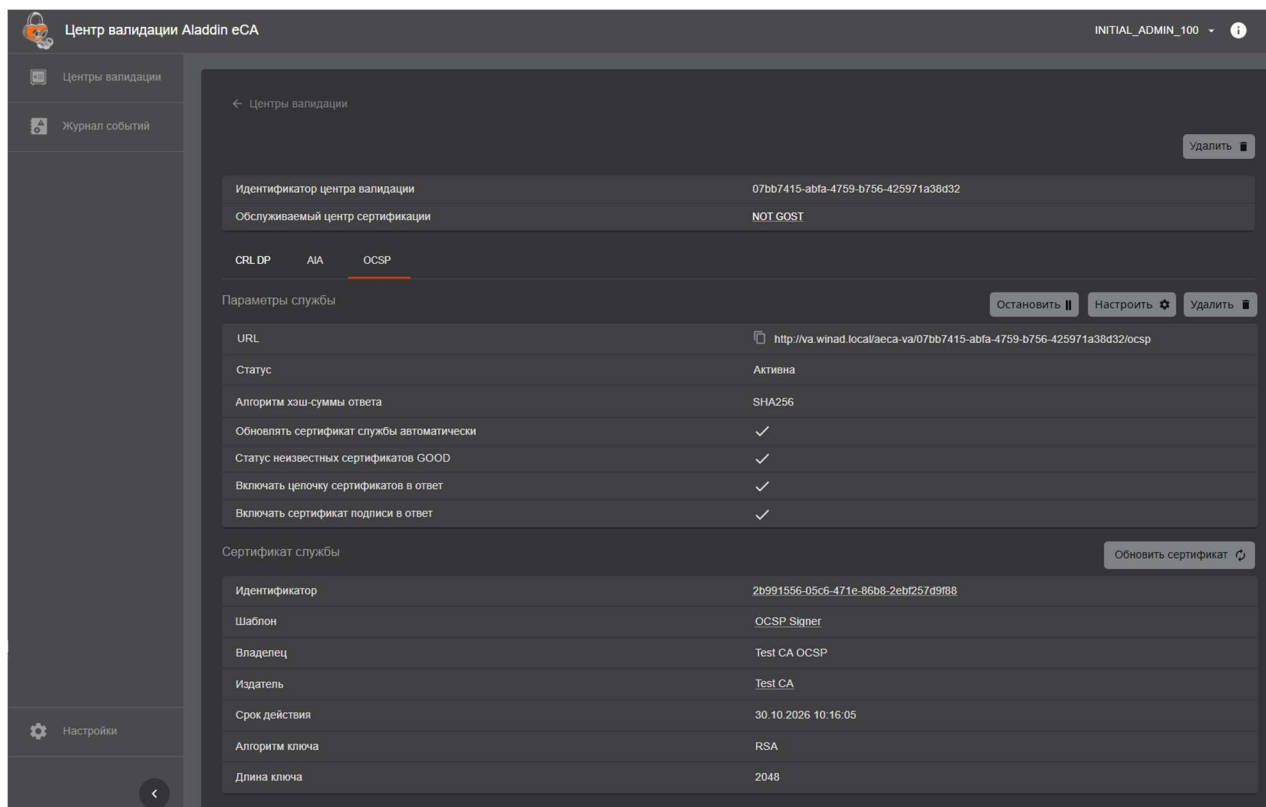


Рисунок 18 - Карточка Центра валидации, вкладка «OCSP», служба OCSP создана

6.2.2 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 Центра сертификации Aladdin eCA;
 - определиться с необходимостью автоматического создания службы OCSP для данного ЦВ в результате его создания путём управления чек-боксом «Создать службу OCSP». По умолчанию данный чек-бокс включён.

в зависимости от состояния чек-бокса «Создать службу OCSP» кнопка перехода на следующий шаг будет иметь значение «Продолжить» или «Создать» (если чек-бокс выключен, см. рисунок 20). При нажатии на кнопку «Создать» сценарий создания центра валидации будет завершаться.

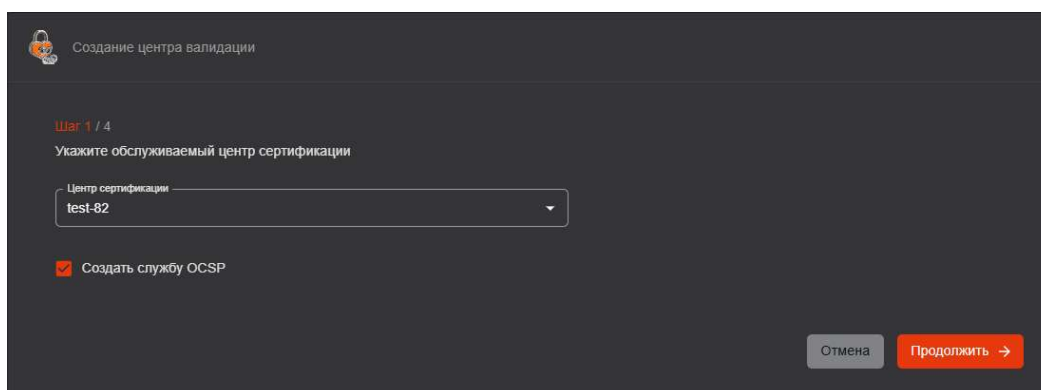


Рисунок 19 — Окно «Создание центра валидации» с включённым чек-боксом «Создать службу OCSP»

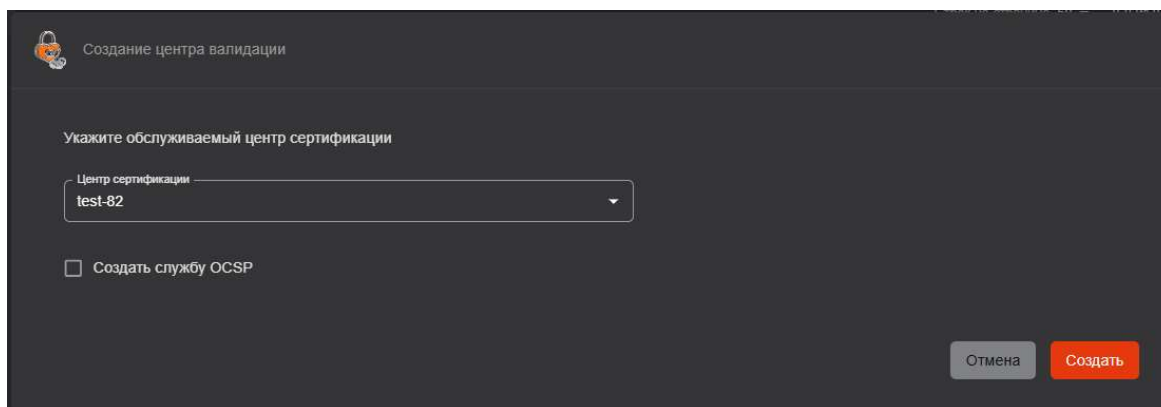


Рисунок 20 — Окно «Создание центра валидации» с выключенным чек-боксом «Создать службу OCSP»

- Если была нажата кнопка «Продолжить», на следующем шаге окна «Создание центра валидации» необходимо сделать (см. рисунок 21):

- выбор криптопровайдера службы OCSP.

При наличии активного криптопровайдера «КриптоПро CSP» на хосте Центра валидации Aladdin eVA в поле будет доступно указание значения «КриптоПро CSP».

При наличии активного криптопровайдера «Aladdin JCP» на хосте Центра валидации Aladdin eVA в поле будет доступно указание значения «Aladdin JCP».

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 или «Aladdin JCP», 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».

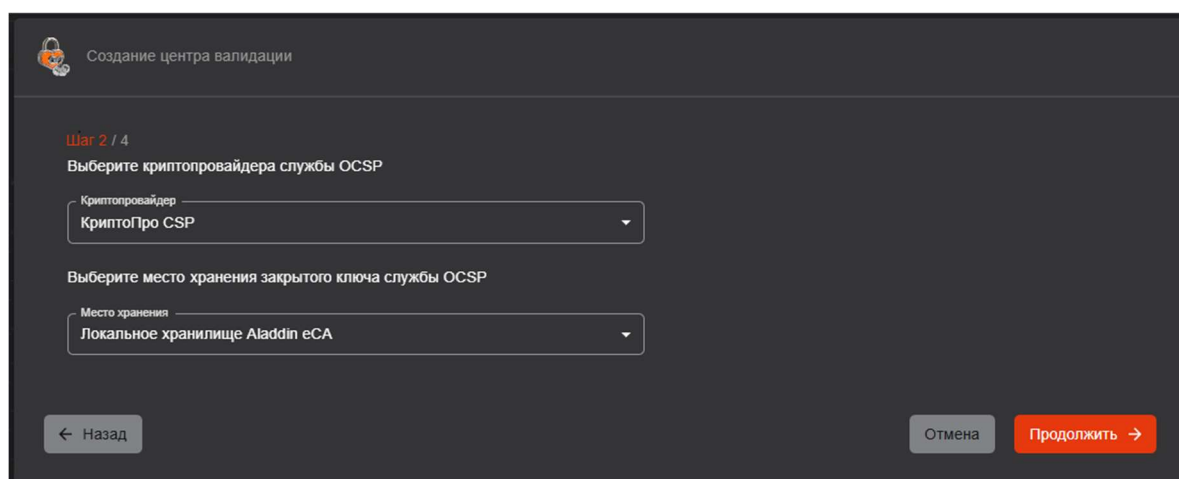


Рисунок 21 — Окно «Создание центра валидации» на шаге 2

- Нажмите кнопку «Продолжить».
- На следующем шаге необходимо сделать (см. рисунок 22):

- выбор шаблона сертификата создаваемой службы OSCP. В списке должны присутствовать шаблоны подключённого Центра сертификации Aladdin eCA, имеющие ECU «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 OSCP;
- выбор длины ключа;

Рисунок 22 — Окно «Создание центра валидации» на шаге 3

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

- 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 OSCP:
 - «Статус неизвестных сертификатов GOOD».

Внимание! Не рекомендуется отключать данную опцию. Если опция отключена, служба OSCP 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 OSCP. В противном случае клиент не сможет проверить подпись ответа службы OSCP, и проверка статуса сертификата завершится ошибкой.

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

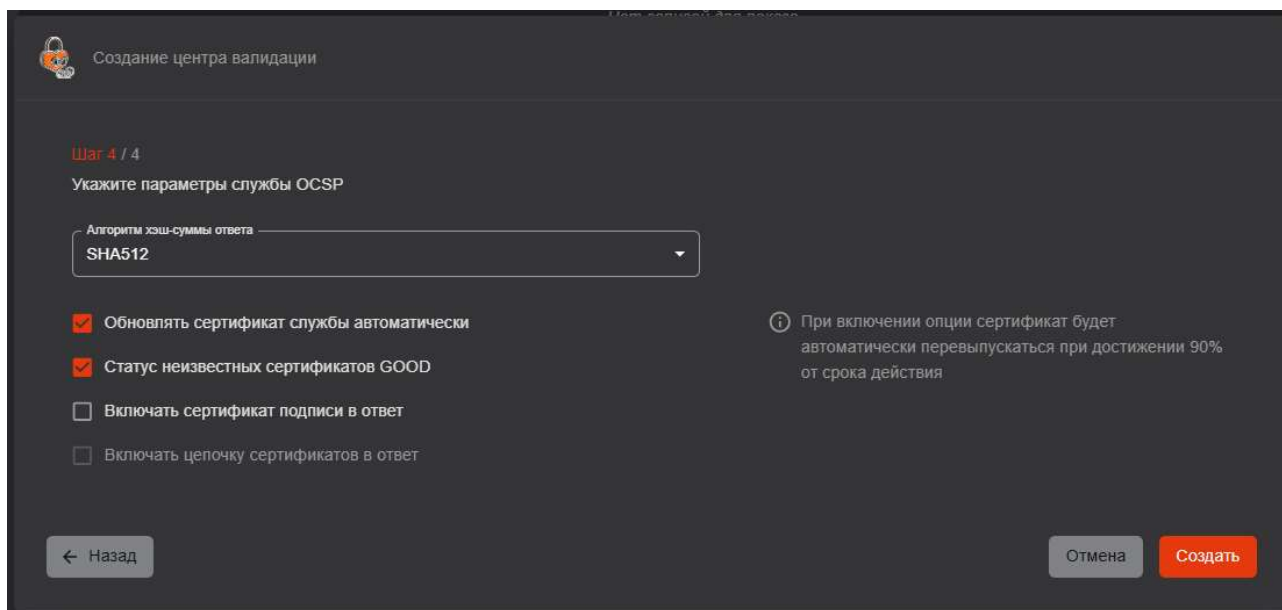


Рисунок 23 — Окно «Создание центра валидации» на шаге 4

- 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 Центра сертификации Aladdin eCA.

6.2.3 Создание службы OCSP созданного Центра валидации Aladdin eVA

Для создания службы OCSP созданного Центра валидации Aladdin eVA:

- 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 24) выберите:
 - Криптопровайдера службы OCSP.

При наличии активного криптопровайдера «КриптоПро CSP» на хосте Центра валидации Aladdin eVA в поле будет доступно указание значения «КриптоПро CSP».

При наличии активного криптопровайдера «Aladdin JCP» на хосте Центра валидации Aladdin eVA в поле будет доступно указание значения «Aladdin JCP».

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 или «Aladdin JCP», 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 24 — Окно «Создание службы OSCP» на шаге 1

- Нажмите кнопку «Продолжить».
- На данном шаге (см. рисунок 25) выберите:
 - шаблон сертификата создаваемой службы OSCP. В списке должны присутствовать шаблоны подключённого Центра сертификации Aladdin eCA, 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 OSCP.

Рисунок 25 — Окно «Создание службы OSCP» на шаге 2

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

6.2.4 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 Центра сертификации Aladdin eCA. 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».

6.2.5 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 27) 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»).

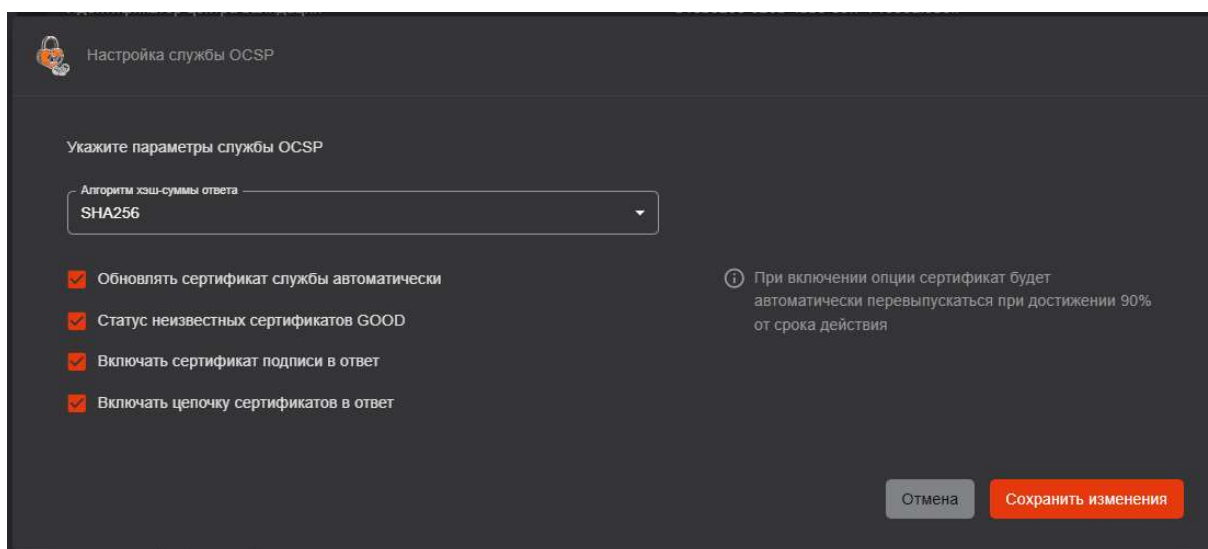


Рисунок 27 — Окно «Настройка службы OCSP»

- 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».

6.2.6 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 28) подтвердите удаление службы OCSP:

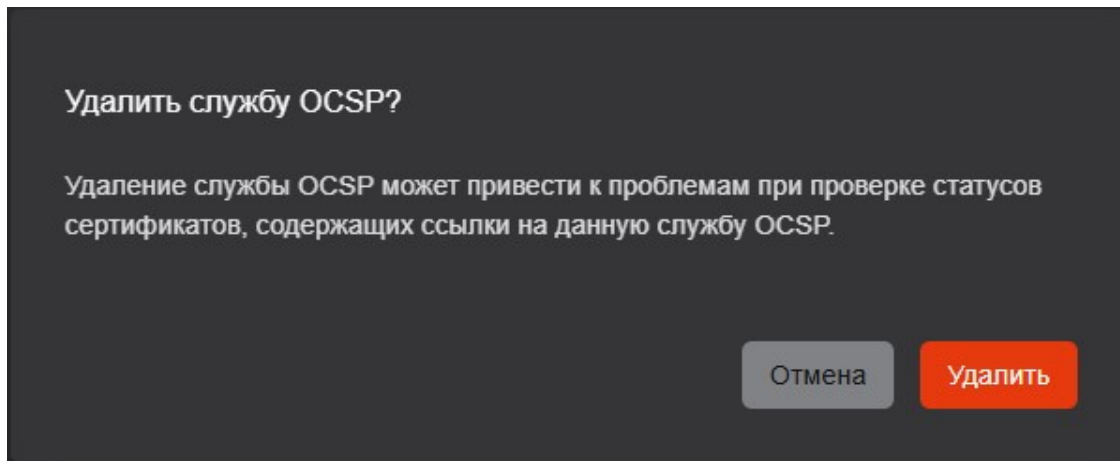


Рисунок 28 — Окно подтверждения удаления службы OCSP

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».

6.2.7 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 29) необходимо подтвердить удаление Центра валидации:

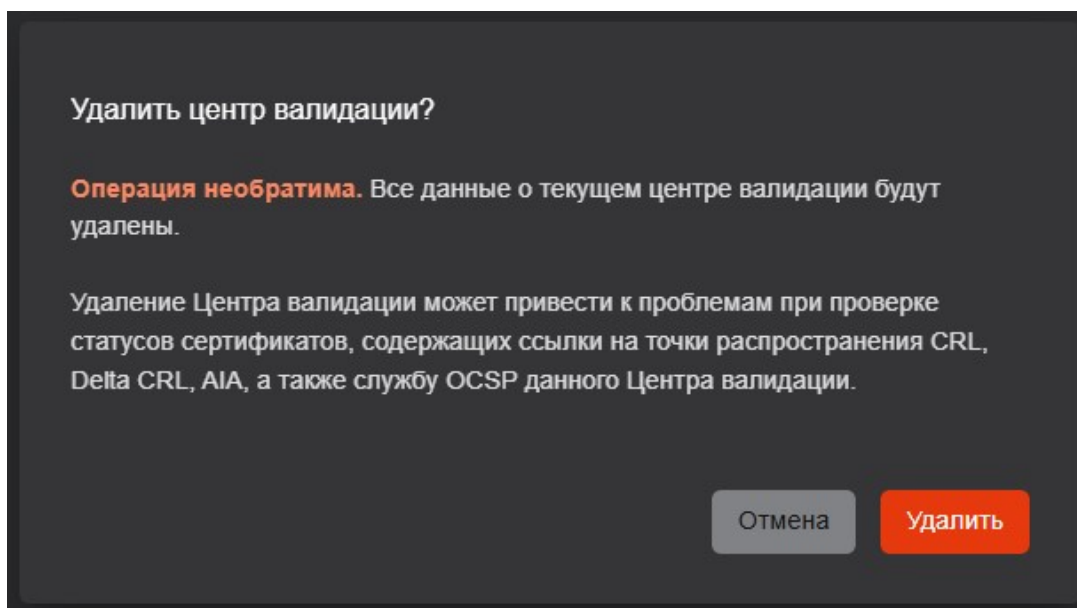



Рисунок 29 — Окно подтверждения удаления Центра валидации.

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».

6.3 Раздел «Настройки»

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

6.3.1 Вкладка «Веб сервер»

На вкладке «Веб-сервер» (см. рисунок 30) 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 30);
- SDN издателя сертификата (поле «Издатель»; обозначено цифрой 2 на рисунке 30);
- Дата окончания действия сертификата (поле «Действителен до»; обозначено цифрой 3 на рисунке 30).

В таблице с данными текущего сертификата веб-сервера присутствует кнопка «Настройка» (обозначена цифрой 4 на рисунке 30), 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 30);
- CN, указанный в сертификате центра сертификации (в поле «Издатель»; обозначено цифрой 6 на рисунке 30);
- Дата окончания действия сертификата центра сертификации (в поле «Действителен до», обозначено цифрой 7 на рисунке 30);
- Флаг вхождения центра сертификации в список разрешённых издателей (в поле «Разрешенный издатель», обозначено цифрой 8 на рисунке 30). В данном поле отображается символ «Галочка» зелёного цвета, если центр сертификации входит в список разрешённых издателей, иначе в поле отображается прочерк.

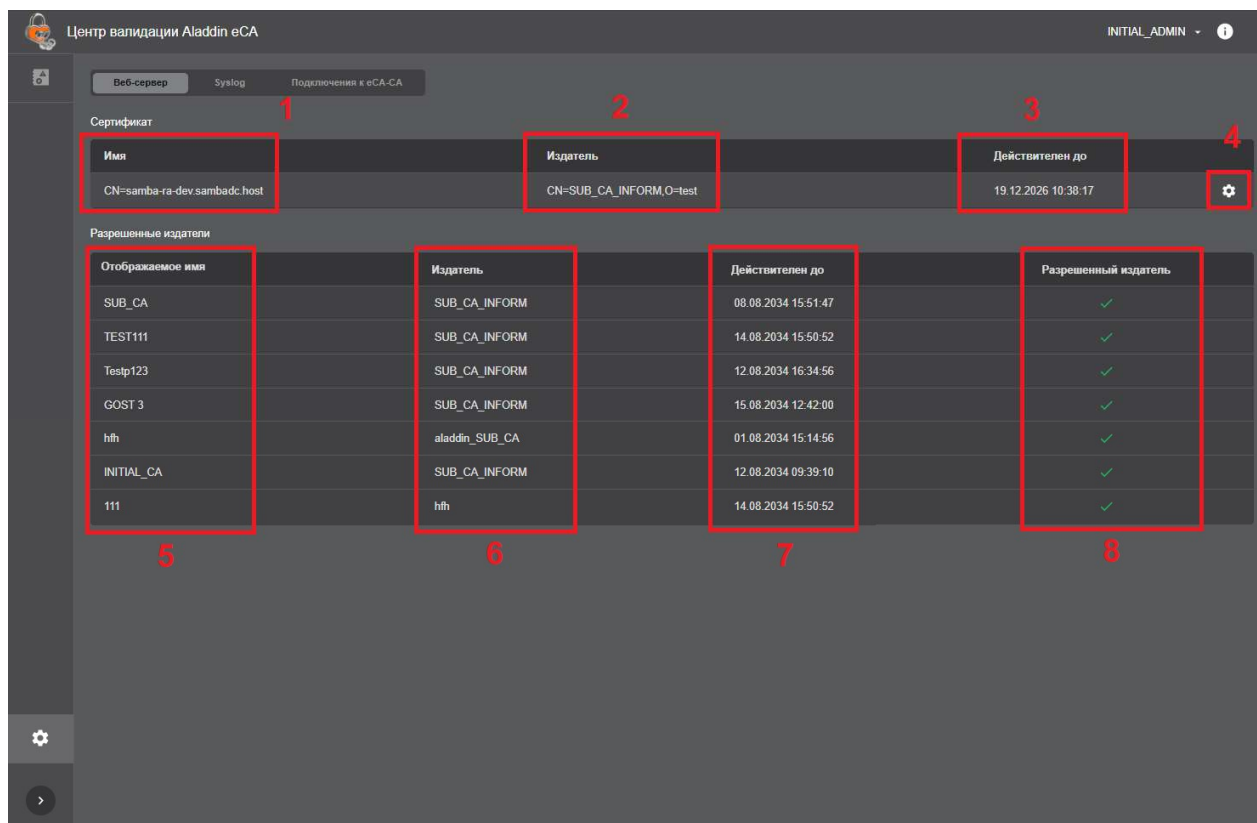


Рисунок 30 -Вкладка «Веб-сервер»

6.3.2 Вкладка «Syslog»

На вкладке «Веб-сервер» в подразделе «Syslog серверы» (см. рисунок 31) присутствуют следующие элементы:

- кнопка «Добавить» (обозначена цифрой 1 на рисунке 2), предназначенная для добавления нового Syslog-сервера в список (см. 6.3.5). Для пользователя с ролью «Администратор» данная кнопка отсутствует;
- список Syslog-серверов в табличной форме, содержащий следующие элементы:
 - поле «Адрес хоста», содержащее в себе адрес хоста Syslog-сервера (обозначено цифрой 2 на рисунке 31);
 - поле «Порт», содержащее в себе порт Syslog-сервера (обозначено цифрой 3 на рисунке 31);
 - поле «Протокол», содержащее в себе протокол, по которому выполняется отправка сообщение на Syslog-сервер (обозначено цифрой 4 на рисунке 31);
 - поле «Отправка сообщений», содержащее в себе переключатель, позволяющий включить или выключить отправки сообщения на данный Syslog-сервер (обозначено цифрой 5 на рисунке 31). Для пользователя с ролью «Администратор» данный переключатель заблокирован от изменений;
 - кнопка «Редактировать» (обозначена цифрой 6 на рисунке 31), позволяющая изменить параметры данного Syslog-сервера (см. 6.3.6). Для пользователя с ролью «Администратор» данная кнопка заблокирована;
 - кнопка «Удалить» (обозначена цифрой 7 на рисунке 31), позволяющая удалить данный Syslog-сервер из списка (см. 6.3.7). Для пользователя с ролью «Администратор» данная кнопка заблокирована.

В списке может присутствовать не более 10 Syslog-серверов.

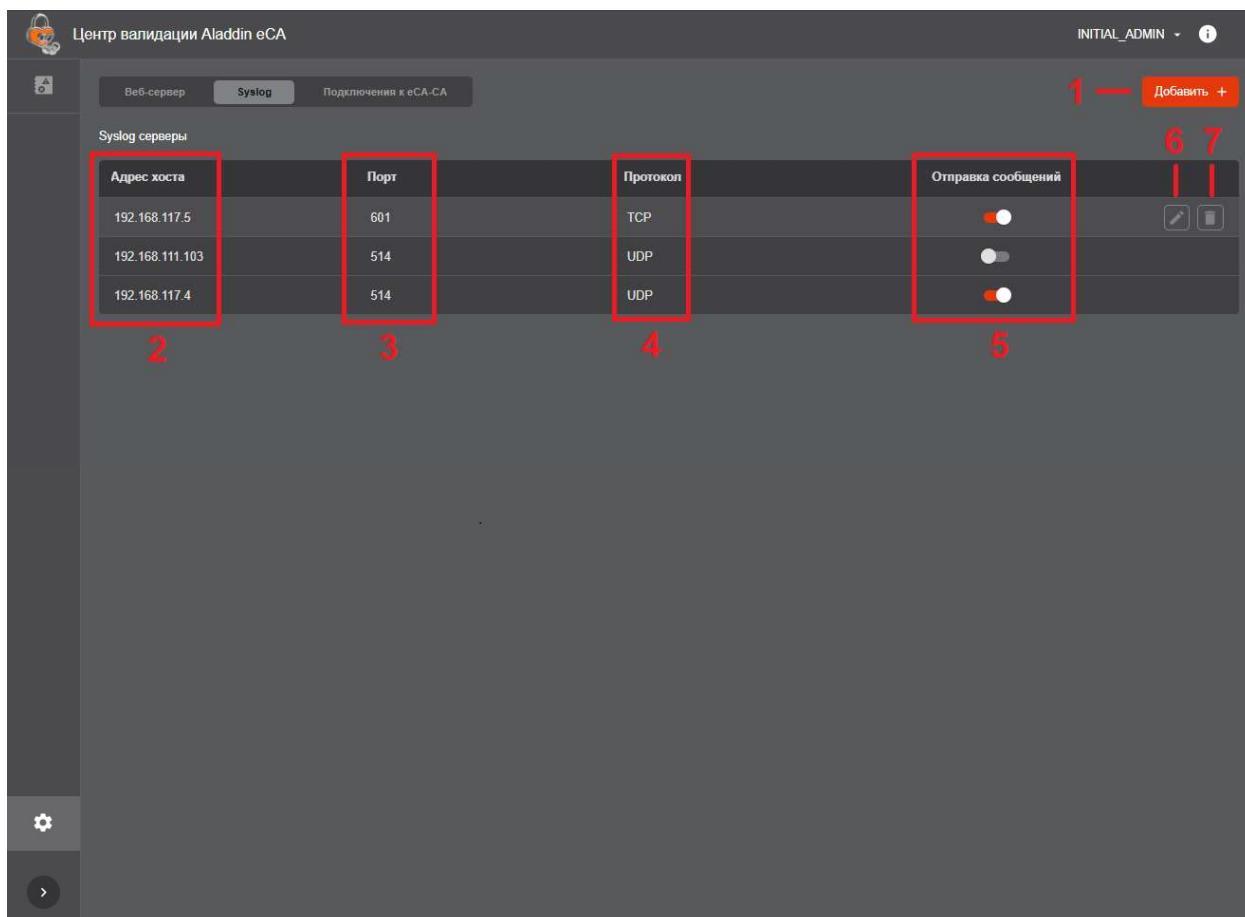


Рисунок 31 - Вкладка «Syslog»

6.3.3 Вкладка «Подключения к еСА-СА»

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

Вкладка «Подключения к еСА-СА» для пользователя с ролью «Администратор» отсутствует.

На вкладке «Подключения к еСА-СА» (см. рисунок 32) присутствуют следующие элементы:

- кнопка «Добавить», предназначенная для добавления нового подключения к Центру сертификации Aladdin eCA (см. 6.3.8);
- список подключений к Центру сертификации Aladdin eCA в табличной форме, содержащий для каждого из них следующие элементы:
 - поле «Отображаемое имя», содержащее в себе отображаемое имя подключения к Центру сертификации Aladdin eCA;
 - поле «Адрес хоста», содержащее в себе адрес хоста Центра сертификации Aladdin eCA;
 - поле «Порт», содержащее в себе порт, по которому осуществляется подключение к Центру сертификации Aladdin eCA;
 - кнопка «Удалить», позволяющая удалить подключение к Центру сертификации Aladdin eCA (см. 6.3.9).

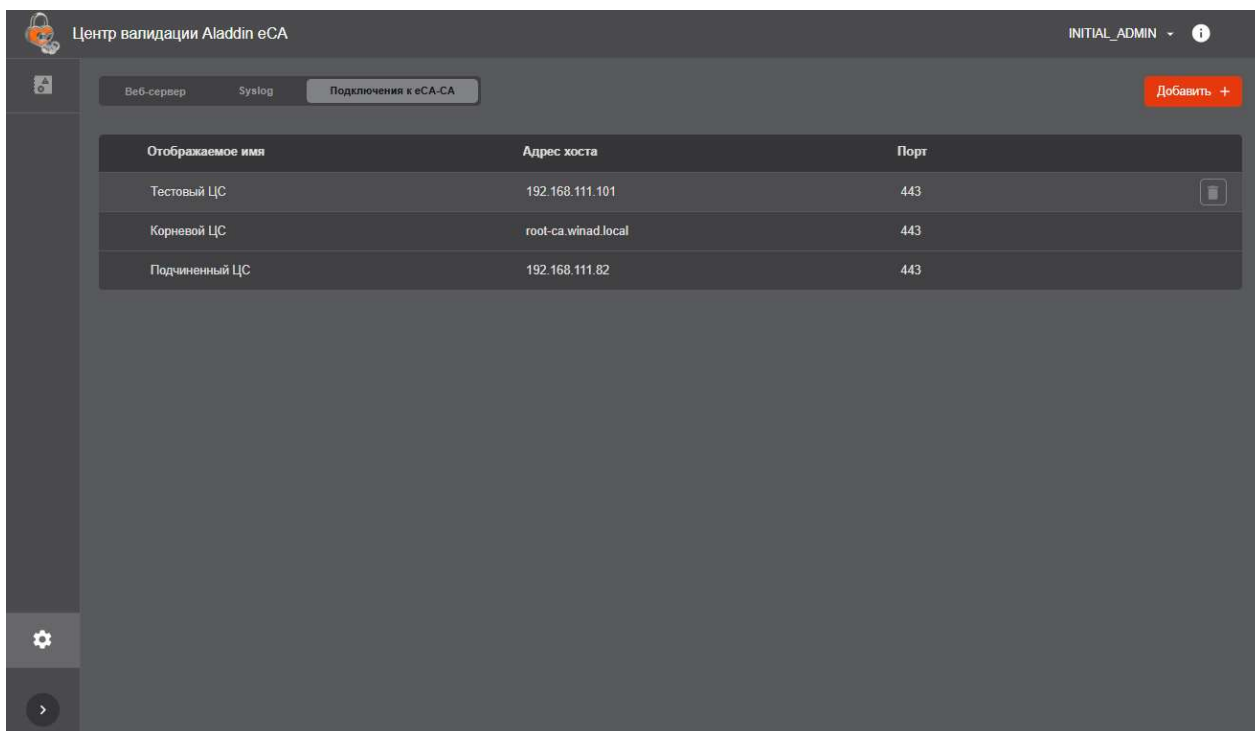


Рисунок 32 -Вкладка «Подключения к eCA-CA»

6.3.4 Смена сертификата веб-сервера

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

Для смены сертификата веб-сервера:

1. В ПО Центра валидации Aladdin eVA 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 33) необходимо нажать кнопку «Выбрать файл» и выбрать файл контейнера закрытого ключа, содержащий сертификат веб-сервера, затем ввести пароль от данного контейнера в поле «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).

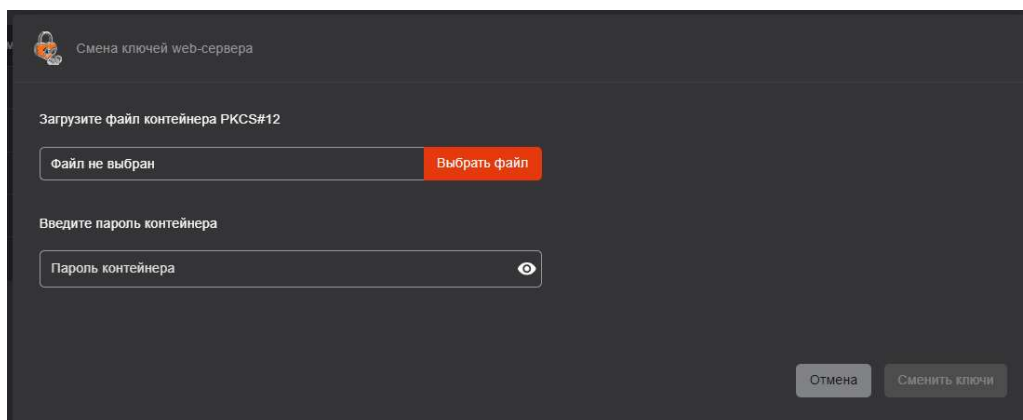


Рисунок 33 - Окно смены сертификата веб-сервера

3. При успешной смене сертификата веб-сервера будет отображено окно с сообщением «Сертификат изменен» (см. рисунок 34). По нажатию на кнопку «Закрыть» клиентский компонент программы будет перезапущен.



Рисунок 34 - 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»:

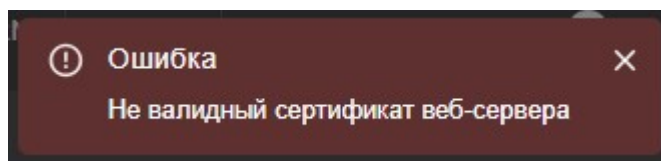


Рисунок 35 - Ошибка «Не валидный сертификат веб-сервера»

6.3.5 Добавление Syslog-сервера

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

Центром валидации Aladdin eVA выполняются автоматическая отправка сообщений о зафиксированных событиях по стандарту Syslog (в соответствии с рекомендацией RFC5424) на Syslog-серверы.

Значения полей отправляемых сообщений представлены в таблице 7.

Таблица 7 — Значения полей отправляемых сообщений

Поле Syslog-сообщения	Описание	Значение
PRIVAL	Priority Value - значение, вычисляемое на основе категории и важности события	<ul style="list-style-type: none"> 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

Поле Syslog-сообщения	Описание	Значение
PROCID	Идентификатор процесса (PID) приложения	PID сервиса, являющегося источником события
MSGID	Идентификатор сообщения	Код события
[STRUCTURED-DATA]	Структурированные данные	<pre>[aeca-va actionCode='actionCode' category='category' id='id' serviceName='serviceName' system='system' username='username' role='role' ipAddress='ipAddress' attributes='attributes']</pre> <p>где:</p> <ul style="list-style-type: none"> '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.
MESSAGE	Строка, содержащая краткую информацию о событии	Краткое описание события (аналогично описанию события, отображаемому в списке событий в разделе «Журнал событий»)

Для добавления Syslog-сервера:

- В ПО Центра валидации Aladdin eVA необходимо перейти в раздел «Настройки» на вкладку «Syslog». Затем в подразделе «Syslog серверы» нажать на кнопку «Добавить».
- В отобразившемся окне «Добавление Syslog-сервера» (см. рисунок 36) необходимо указать параметры добавляемого Syslog-сервера:
 - В поле «Адрес хоста» необходимо указать адрес хоста Syslog-сервера (доступно указание IP-адреса или DNS-имени). В случае, если адрес хоста Syslog-сервера 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 Syslog-сервера содержит пробел, в данном поле ввода будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Добавить» будет недоступна для нажатия).

- В поле «Порт» необходимо указать порт Syslog-сервера. 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).
- В поле «Протокол» необходимо указать допустимые варианты выбора: UDP (должен быть указан по умолчанию) или TCP.

Рисунок 36 - Окно добавления Syslog-сервера

После нажатия на кнопку «Добавить» в список Syslog-серверов будет добавлен новый Syslog-сервер с параметрами, указанными в окне «Добавление Syslog-сервера». При этом переключатель «Отправка сообщений» у добавленного Syslog-сервера по умолчанию будет во включённом состоянии. Если в списке уже присутствуют 10 Syslog-серверов, после нажатия на кнопку «Добавить» будет отображаться сообщение об ошибке «Ошибка. Максимальное количество Syslog-серверов - 10» (см. рисунок 37). При этом новый Syslog-сервер не будет добавлен в список.

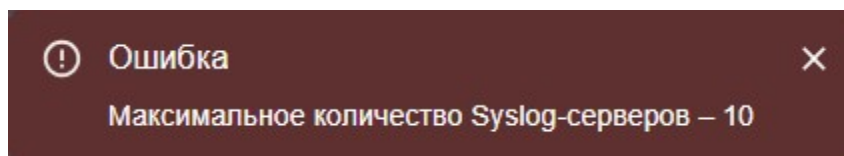


Рисунок 37 - Ошибка при превышении максимального количества Syslog-серверов

6.3.6 Редактирование параметров Syslog-сервера

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

Для редактирования параметров Syslog-сервера:

- В ПО Центра валидации Aladdin eVA необходимо перейти в раздел «Настройки» на вкладку «Syslog».
- В строке любого из имеющихся в списке Syslog-серверов необходимо нажать на кнопку «Редактировать».
- В отобразившемся окне «Редактирование Syslog-сервера» (см. рисунок 38) допустимо редактирование следующих параметров Syslog-сервера:

- «Адрес хоста». В случае, если адрес хоста Syslog-сервера не указан, в данном поле ввода будет отображаться сообщение об ошибке «Обязательно к заполнению» (кнопка «Сохранить изменения» будет недоступна для нажатия). В случае, если указанный адрес хоста Syslog-сервера содержит пробел, в данном поле ввода будет отображаться сообщение об ошибке «Некорректный ввод» (кнопка «Сохранить изменения» будет недоступна для нажатия).
- «Порт». 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 «Сохранить изменения» 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 «Сохранить изменения» будет недоступна для нажатия).
- «Протокол». Допустимые варианты выбора: UDP или TCP.

Рисунок 38 - Окно редактирования Syslog-сервера

После нажатия на кнопку «Сохранить изменения» изменённые параметры Syslog-сервера будут применены.

6.3.7 Удаление Syslog-сервера

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

Для удаления Syslog-сервера:

- В ПО Центра валидации Aladdin eVA необходимо перейти в раздел «Настройки» на вкладку «Syslog».
- В строке любого из имеющихся в списке Syslog-серверов необходимо нажать на кнопку «Удалить».
- При нажатии кнопки «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.

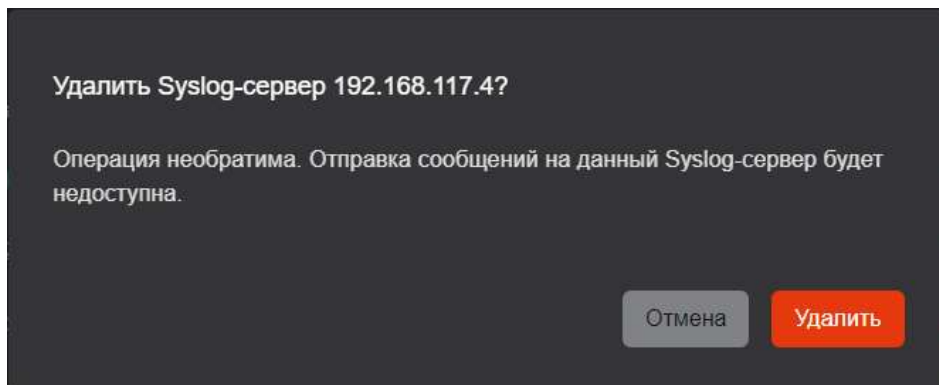


Рисунок 39 - Диалоговое окно подтверждения удаления Syslog-сервера

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).

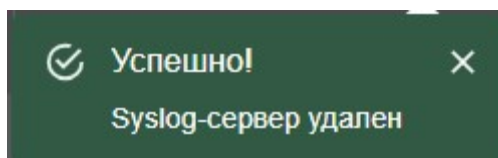


Рисунок 40 - Сообщение об успешном удалении Syslog-сервера

6.3.8 Добавление подключения к Центру сертификации Aladdin eCA

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

Для добавления подключения к Центру сертификации Aladdin eCA:

- В веб-интерфейсе Центра валидации Aladdin eVA 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 Центру сертификации Aladdin eCA:
 - «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 Центра сертификации Aladdin eCA (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 Центру сертификации Aladdin eCA. 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 Центра сертификации Aladdin eCA;

- указать пароль от контейнера закрытого ключа (PKCS#12) администратора Центра сертификации Aladdin eCA.

Рисунок 41 - Окно добавления подключения к Центру сертификации Aladdin eCA

После нажатия на кнопку «Добавить» будет выполнено тестовое подключение к Центру сертификации Aladdin eCA, 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».

6.3.9 Удаление подключения к Центру сертификации Aladdin eCA

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

Для удаления подключения к Центру сертификации Aladdin eCA:

- В ПО Центра валидации Aladdin eVA перейдите в раздел «Настройки» на вкладку «Подключения к eCA-CA».
- В строке любого из имеющихся в списке подключений к Центру сертификации Aladdin eCA нажмите кнопку «Удалить».
- В окне подтверждения удаления подключения к Центру сертификации Aladdin eCA (см. рисунок 42) нажмите кнопку «Удалить». В данном окне в строке «Удалить подключение?» содержится отображаемое имя удаляемого подключения, например, «Удалить подключение «Test»?».

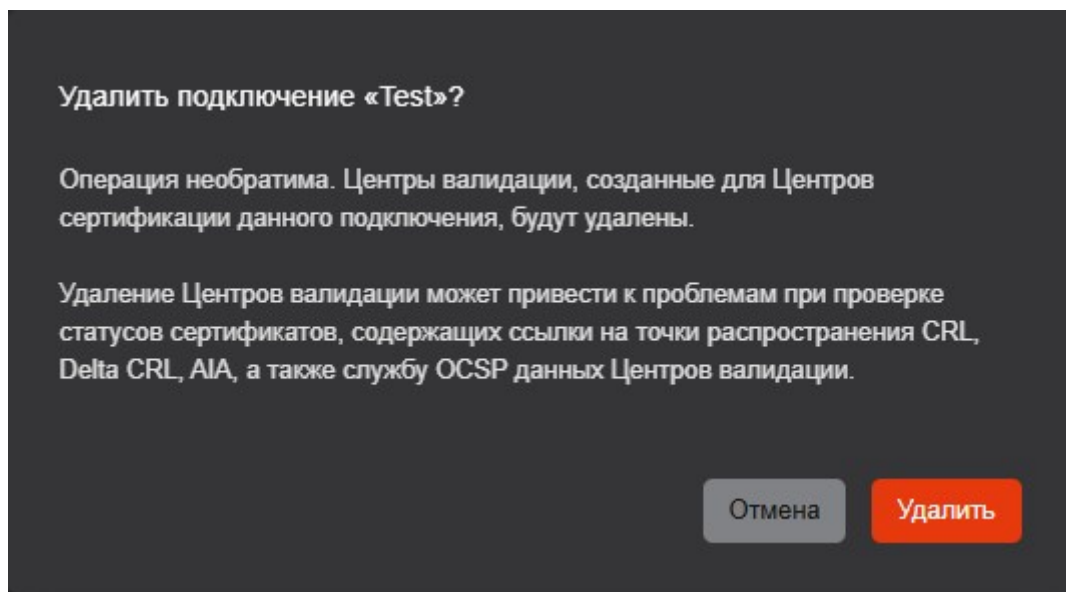


Рисунок 42 - Диалоговое окно подтверждения удаления Syslog-сервера

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

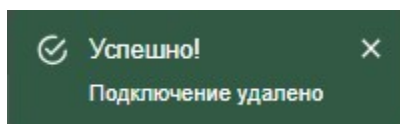


Рисунок 43 - Сообщение об успешном удалении подключения

6.4 Раздел «Журнал событий»

6.4.1 О журнале событий

Журнал событий предназначен для выявления случаев нарушения политики безопасности при эксплуатации Центра валидации Aladdin eVA. В журнале аудита регистрируются системные события, связанные с работой ПО, а также события, связанные с изменениями настроек и действиями пользователей. Записи журнала событий хранятся в базе данных.

Каждая запись в журнале событий содержит следующую информацию:

- Дата и время регистрации с точностью до секунды.
- Имя учетной записи — пользователь, инициировавший событие (для системных событий — SYSTEM).
- Роль - роль пользователя, инициировавшего событие.
- IP-адрес источника - IP-адрес узла, с которого была выполнена аутентификация инициатора события.
- Категория событий («Ошибка» или «Информация»).
- Код события в формате: VAENV [номер события].
- Описание - краткое описание события.
- Причина события (только для событий категорий «Ошибка»).
- Подробное описание события.

Перечень событий с их кодами, категориями и подробным описанием приведен в разделе 6.4.5.


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 включен (параметр `archive_enabled` - флаг управления режимом архивации).

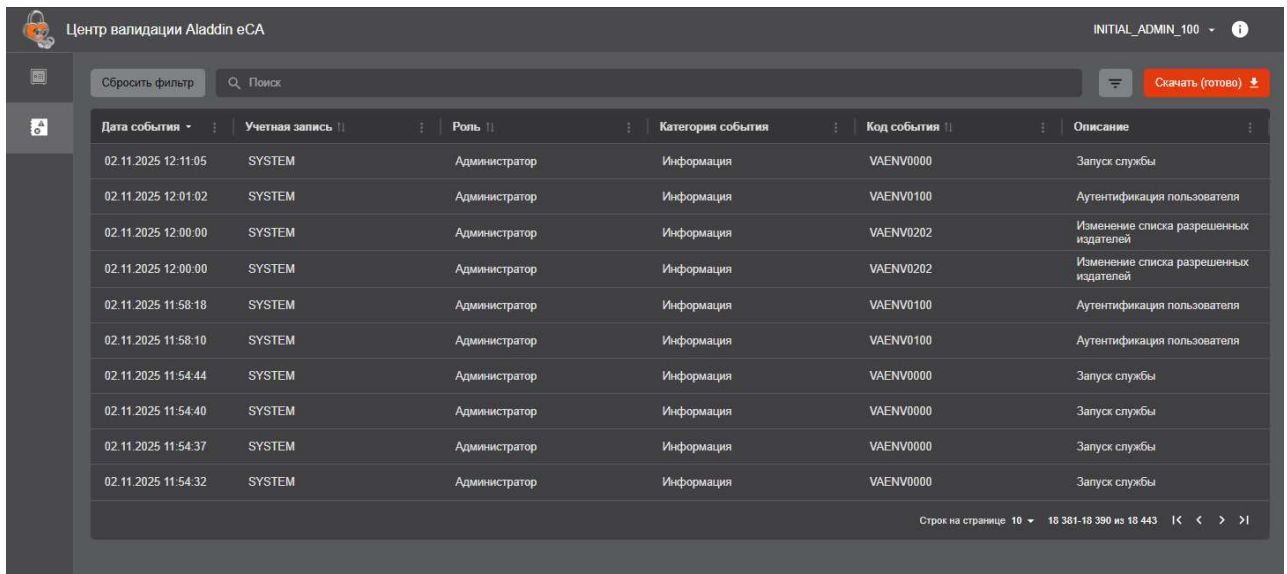
Периодичность запуска архивации регулируется параметром `archive_cron` конфигурационного файла. значение указывается в формате CRON-выражения (значение по умолчанию - '0 0 0 1 * *'). По умолчанию процесс архивации запускается при наступлении первого числа каждого месяца.

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`).

6.4.2 Просмотр записей журнала событий

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

Для просмотра записей журнала событий подключитесь к веб-интерфейсу Центра валидации Aladdin eVA и перейдите в раздел  **Журнал событий**.



Дата события	Учетная запись	Роль	Категория события	Код события	Описание
02.11.2025 12:11:05	SYSTEM	Администратор	Информация	VAENV0000	Запуск службы
02.11.2025 12:01:02	SYSTEM	Администратор	Информация	VAENV0100	Аутентификация пользователя
02.11.2025 12:00:00	SYSTEM	Администратор	Информация	VAENV0202	Изменение списка разрешенных издателей
02.11.2025 12:00:00	SYSTEM	Администратор	Информация	VAENV0202	Изменение списка разрешенных издателей
02.11.2025 11:58:18	SYSTEM	Администратор	Информация	VAENV0100	Аутентификация пользователя
02.11.2025 11:58:10	SYSTEM	Администратор	Информация	VAENV0100	Аутентификация пользователя
02.11.2025 11:54:44	SYSTEM	Администратор	Информация	VAENV0000	Запуск службы
02.11.2025 11:54:40	SYSTEM	Администратор	Информация	VAENV0000	Запуск службы
02.11.2025 11:54:37	SYSTEM	Администратор	Информация	VAENV0000	Запуск службы
02.11.2025 11:54:32	SYSTEM	Администратор	Информация	VAENV0000	Запуск службы

Строк на странице: 10 18 361-18 390 из 18 443

Рисунок 44 - Просмотр журнала событий

Записи о событиях отображаются списком в табличном виде.

По умолчанию в колонках таблицы отображаются следующие атрибуты событий:

- Дата события.
- Учетная запись.
- Роль.
- Категория события.
- Код события.
- Описание.

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.
- [dropdown arrow] — 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 ⁷² выберите [icon] **<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 [icon] **<Показать все колонки>** (см. Рисунок 46).

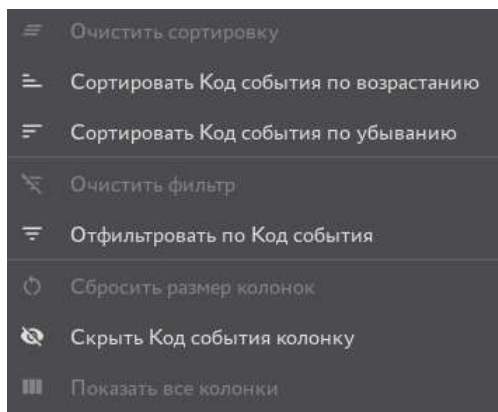


Рисунок 46 - Список действий с колонкой [Код события]

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

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 соответствующей колонки значок ⓘ **<Действие колонки>** и в открывшемся списке ⁷³ (см. Рисунок 46) выберите:

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



Статусы выполненной сортировки отображаются в заголовках колонок следующими значками ⁷⁴:



- [icon] - сортировка выполнена в порядке возрастания.

⁷² Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

⁷³ Набор действий колонок отличается в зависимости от атрибута события, представленного в данной колонке.

⁷⁴ Менять порядок сортировки, а также отменять сортировку можно, последовательно щелкая на значок статуса сортировки по колонке.




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


Чтобы отменить сортировку записей по выбранному атрибуту, щелкните в заголовке соответствующей колонки значок  **<Действие колонки>** и в открывшемся 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 открывшемся 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.


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 колоноки>** и в открывшемся списке выберите **<Очистить фильтр>** или щелкните в заголовке колоноки 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 щелкните в поисковой строке значок .

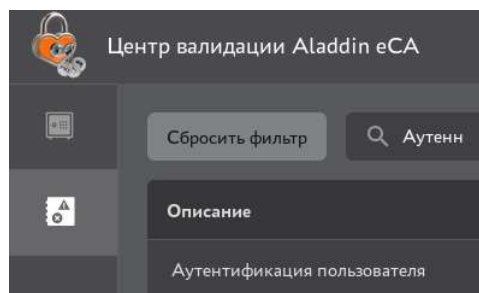


Рисунок 48 - Выборка событий по описанию с помощью поисковой строки

6.4.3 Просмотр карточки события

Карточка события содержит представленную в удобном для анализа виде подробную информацию о событии (описание атрибутов события см. в разделе 6.4.1).

Чтобы открыть карточку события:

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

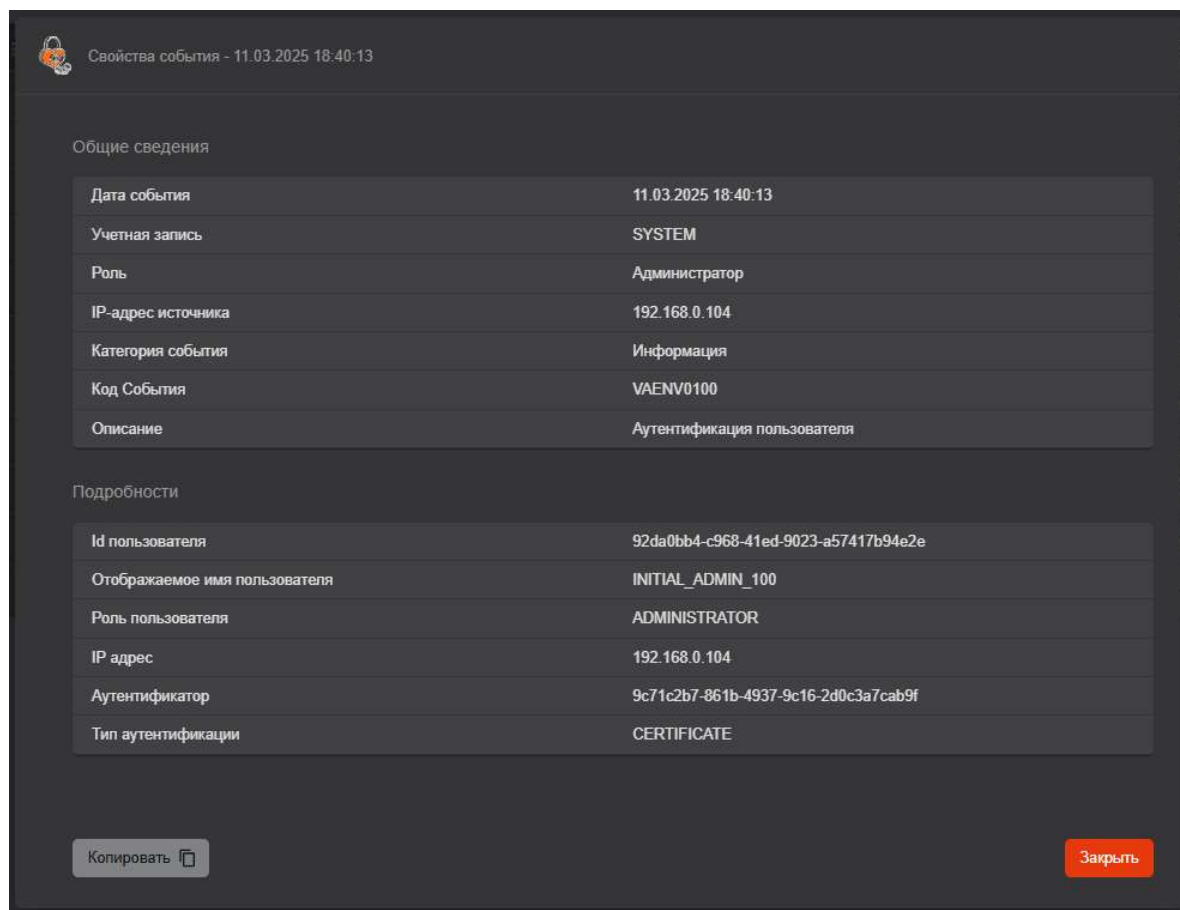



Рисунок 49 - Окно «Свойства события» (карточка события)

Для копирования информации о событии в буфер обмена нажмите кнопку . Содержимое события из буфера обмена можно вставить, например, в текстовый файл (см. Рисунок 50).

```
Общие сведения:
Дата события: 19.08.2025 13:30:01
Учетная запись: SYSTEM
Роль: ADMINISTRATOR
Категория события: INFO
Код События: VAENV0702
Описание: Изменение списка разрешенных издателей




Подробности:
Имя издателя - действие: Sub - обновлен
Имя издателя - действие: Root - обновлен
Имя издателя - действие: INITIAL_CA - обновлен
```

Рисунок 50 - Пример копирования события в текстовый файл

6.4.4 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 Центра сертификации Aladdin eCA и перейдите в раздел  **Журнал событий**.
- Запустите процесс подготовки файла с событиями, нажав на панели инструментов кнопку  **Скачать**. В результате кнопка меняет свое состояние на  **Скачать (выполняется)** (начинается подготовка файла, содержащего записи журнала событий).

- После подготовки файла для экспорта журнала нажмите кнопку .

6.4.5 События, отслеживаемые Центром валидации Aladdin eVA

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

6.4.5.1 События запуска и остановки служб

События запуска служб остановки описаны в таблице 8.

Таблица 8 - События запуска служб остановки

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
Запуск службы	VAENV0000	INFO	Краткое описание: «Запуск службы». Атрибут: «Название службы»
Остановка службы	VAENV0001	INFO	Краткое описание: «Остановка службы». Атрибут: «Название службы»

6.4.5.2 События аутентификации пользователей

События аутентификации пользователей описаны в таблице 9.

Таблица 9 - 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. – Описание ошибки
Выход пользователя	VAENV0102	INFO	Краткое описание: «Выход пользователя»

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			Атрибуты: <ul style="list-style-type: none"> – Id пользователя. – Отображаемое имя пользователя. – Роль пользователя. – Аутентификатор. – Тип аутентификации. – IP адрес

6.4.5.3 События работы с Центрами валидации

События работы с Центрами валидации описаны в таблице 10.

Таблица 10 - 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – Описание ошибки
Создание службы OCSP		VAENV0202	INFO	Краткое описание: «Создание службы OCSP». Атрибуты: <ul style="list-style-type: none"> – 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
Ошибка создания службы OCSP		VAENV0203	ERROR	Краткое описание: «Ошибка создания службы OCSP». Атрибуты: <ul style="list-style-type: none"> – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – ID сертификата (может отсутствовать).

Причина, вызвавшая запись в журнал		Код события	Категория события	Описание в журнале
				<ul style="list-style-type: none"> 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). Описание ошибки
Запуск службы OCSP		VAENV0204	INFO	Краткое описание: «Запуск службы OCSP». Атрибуты: <ul style="list-style-type: none"> ID центра валидации. ID обслуживаемого центра сертификации. Статус OCSP
Ошибка запуска службы OCSP		VAENV0205	ERROR	Краткое описание: «Ошибка запуска службы OCSP». Атрибуты: <ul style="list-style-type: none"> ID центра валидации. ID обслуживаемого центра сертификации. Статус OCSP. Описание ошибки
Остановка службы OCSP		VAENV0206	INFO	Краткое описание: «Остановка службы OCSP». Атрибуты: <ul style="list-style-type: none"> ID центра валидации. ID обслуживаемого центра сертификации. Статус OCSP
Ошибка остановки службы OCSP		VAENV0207	ERROR	Краткое описание: «Ошибка остановки службы OCSP». Атрибуты: <ul style="list-style-type: none"> ID центра валидации. ID обслуживаемого центра сертификации. Статус OCSP. Описание ошибки
Изменение параметров службы OCSP		VAENV0208	INFO	Краткое описание: «Изменение параметров службы OCSP». Атрибуты: <ul style="list-style-type: none"> 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
Ошибка изменения параметров службы OCSP		VAENV0209	ERROR	Краткое описание: «Ошибка изменения параметров службы OCSP». Атрибуты:

Причина, вызвавшая запись в журнал		Код события	Категория события	Описание в журнале
				<ul style="list-style-type: none"> – 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). – Описание ошибки
Обновление сертификата службы OCSP		VAENV0210	INFO	<p>Краткое описание: «Обновление сертификата службы OCSP».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации. – ID обслуживаемого центра сертификации. – ID сертификата. – Алгоритм ключа. – Длина ключа
Ошибка обновления сертификата службы OCSP		VAENV0211	ERROR	<p>Краткое описание: «Ошибка обновления сертификата службы OCSP».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации (может отсутствовать). – ID обслуживаемого центра сертификации (может отсутствовать). – ID сертификата (может отсутствовать). – Алгоритм ключа (может отсутствовать). – Длина ключа (может отсутствовать). – Описание ошибки
Удаление службы OCSP		VAENV0212	INFO	<p>Краткое описание: «Удаление службы OCSP».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка удаления службы OCSP		VAENV0213	ERROR	<p>Краткое описание: «Ошибка удаления службы OCSP».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации. – ID обслуживаемого центра сертификации. – Описание ошибки
Переподключение центра валидации		VAENV0214	INFO	<p>Краткое описание: «Переподключение центра валидации».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации. – ID обслуживаемого центра сертификации
Ошибка переподключения центра валидации		VAENV0215	ERROR	<p>Краткое описание: «Ошибка переподключения центра валидации».</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> – ID центра валидации.

Причина, вызвавшая запись в журнал		Код события	Категория события	Описание в журнале
				<ul style="list-style-type: none"> — ID обслуживаемого центра сертификации. — Описание ошибки
Удаление центра валидации		VAENV0216	INFO	Краткое описание: «Удаление центра валидации». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации
Ошибка удаления центра валидации		VAENV0217	ERROR	Краткое описание: «Ошибка удаления центра валидации». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации. — Описание ошибки
Обновление CRL		VAENV0218	INFO	Краткое описание: «Обновление CRL». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации
Ошибка обновления CRL		VAENV0219	ERROR	Краткое описание: «Ошибка обновления CRL». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации. — Описание ошибки
Обновление Delta CRL		VAENV0220	INFO	Краткое описание: «Обновление Delta CRL». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации
Ошибка обновления Delta CRL		VAENV0221	ERROR	Краткое описание: «Ошибка обновления Delta CRL». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации. — Описание ошибки
Служба OCSP вернула ошибку		VAENV0222	ERROR	Краткое описание: «Служба OCSP вернула ошибку». Атрибуты: <ul style="list-style-type: none"> — ID центра валидации. — ID обслуживаемого центра сертификации. — Описание ошибки

6.4.5.4 События экспорта

События экспорта описаны в таблице 11.

Таблица 11 - 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. – Описание ошибки
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. – Описание ошибки

6.4.5.5 События работы с веб-сервером и издателями

События работы с веб-сервером и издателями описаны в таблице 12.

Таблица 12 - 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). – «Описание 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».

Причина, вызвавшая запись в журнал	Код события	Категория события	Описание в журнале
			Атрибуты: – «Обновленный список разрешенных издателей» (может отсутствовать). – «Описание ошибки»

6.4.5.6 События работы с резервными копиями

События работы с резервными копиями описаны в таблице 13.

Таблица 13 - 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». Атрибут: «Абсолютное имя файла резервной копии»
Ошибка создания резервной копии	VAENV0901	ERROR	Краткое описание: «Ошибка создания резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии» (может отсутствовать). – «Описание ошибки»
Успешное восстановление из резервной копии	VAENV0902	INFO	Краткое описание: «Успешное восстановление из резервной копии». Атрибут: «Абсолютное имя файла резервной копии»
Ошибка восстановления из резервной копии	VAENV0903	ERROR	Краткое описание: «Ошибка восстановления из резервной копии». Атрибуты: – «Абсолютное имя файла резервной копии» (может отсутствовать). – «Описание ошибки»

6.4.5.7 События контроля целостности

События контроля целостности описаны в таблице 14.

Таблица 14 - 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: «Описание ошибки» (может отсутствовать)

6.4.5.8 События архивации и очистки записей аудита

События архивации и очистки записей аудита описаны в таблице 15.

Таблица 15 - 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: «Описание 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». Атрибут: «Описание ошибки»

6.4.5.9 События работы с Syslog

События работы с Syslog описаны в таблице 16.

Таблица 16 - 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). — «Описание 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).

Причина, вызвавшая запись в журнал		Код события	Категория события	Описание в журнале
				<ul style="list-style-type: none"> «Порт» (может отсутствовать). «Протокол» (может отсутствовать). «Флаг отправки сообщений» (может отсутствовать). «Описание ошибки»
Удаление Syslog-сервера		VAENV1204	INFO	<p>Краткое описание: Удаление Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> «Адрес хоста». «Порт». «Протокол». «Флаг отправки сообщений»
Ошибка удаления Syslog-сервера		VAENV1205	ERROR	<p>Краткое описание: Ошибка удаления Syslog-сервера</p> <p>Атрибуты:</p> <ul style="list-style-type: none"> «Адрес хоста». «Порт». «Протокол». «Флаг отправки сообщений». «Описание ошибки»

7 КОНТРОЛЬ ЦЕЛОСТНОСТИ ИСПОЛНЯЕМЫХ ФАЙЛОВ ПРОГРАММЫ

Контроль целостности исполняемых файлов Центра валидации Aladdin eVA необходим для отслеживания неизменности и контроля состояния файлов, перечень которых приведен 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 подкаталогов;
- все файлы в каталоге `/opt/aecaVa/static` и его подкаталогов;
- все файлы в каталоге `/opt/aecaVa/bin` и его подкаталогов;
- все файлы в каталоге `/opt/aecaVa/digsig` и его подкаталогов.

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`⁷⁵.

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 (от имени пользователя `root`, либо с использованием `sudo`):

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

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.

При успешной проверке целостности будет выведено сообщение: «Успешная проверка контрольных сумм». При этом в журнале событий будет зафиксировано событие с кодом VAENV1000 (событие «Успешная проверка контрольных сумм»).

При ошибке проверки целостности будет выведено сообщение «Неуспешная проверка контрольных сумм», а также сообщение об ошибке, генерируемое утилитой `jcverify`. При этом в журнале событий будет зафиксировано событие с кодом VAENV1001 (событие «Неуспешная проверка контрольных сумм»).

⁷⁵ Данная утилита включена в состав Центра валидации Aladdin eVA (каталог `/opt/aecaVa/bin/jcverify`).

8 СБОР ДИАГНОСТИЧЕСКОЙ ИНФОРМАЦИИ ПРОГРАММЫ

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

В процессе автоматизированного сбора диагностической информации в архив будут помещены:

- 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 17.

Таблица 17 - Данные системных логов

Системный лог	РЕД ОС 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/ahhttpd/	-	-	+

Для сбора диагностической информации:

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

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

- Запустите скрипт от имени суперпользователя:

```
sudo 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
```

9 РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ ДАННЫХ

9.1 Резервное копирование данных

Создание резервных копий является неотъемлемой частью работы администратора Центра валидации Aladdin eVA.

Перед выполнением каких-либо настроек, изменений и обновлений функционального компонента следует в обязательном порядке выполнить резервное копирование.

Резервные копии создаются для:

- сертификатов и ключей веб-сервера, а также для файла, содержащего сертификаты разрешенных издателей, из каталога, указанного в параметре «certificates_ssl_path» конфигурационного файла «/opt/aecaVa/scripts/config.sh» (по умолчанию «/opt/aecaVa/dist/certificates/ssl»);
- контейнеров закрытого ключа служб OCSP (файлы в каталоге «/opt/aecaVa/dist/cryptotoken/»);
- базы данных программы, указанной в параметре «database_name» конфигурационного файла «/opt/aecaVa/scripts/config.sh» (по умолчанию «aecaVa»);
- конфигурационного файла «/opt/aecaVa/scripts/config.sh»;
- ключа для шифрования пароля пользователя СУБД в конфигурационном файле (файл «/opt/aecaVa/scripts/key»).

Резервное копирование осуществляется на локальный диск в папку, путь к которой определен значением параметра «backup_path» конфигурационного файла «/opt/aecaVa/scripts/config.sh» (по умолчанию - «/opt/aecaVa/dist/backup/») с указанием даты и времени создания резервной копии в имени архива. Каталог хранения архивов выбран исходя из того, что необходимо хранить резервные копии временно и не увеличивать размер занятого пространства жесткого диска. Для постоянного хранения требуется создать механизм переноса файлов.

Для постоянного хранения резервных копий следует:

- определить каталог для хранения резервных копий;
- составить сценарий для создания резервной копии;
- настроить расписание вызова сценариев.

Создание резервной копии Центра валидации Aladdin eVA выполняется запуском скрипта с правами суперпользователя (root):

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

После запуска скрипта резервного копирования создается каталог «/opt/aecaVa/dist/backup», где будет размещен архив, содержащий в имени дату и время создания полной резервной копии.

9.2 Расписание резервного копирования

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

Выполните переход в режим редактирования crontab, выполнив команду:

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

Укажите время и период запуска сценариев создания резервных копий:

```
0 0 1 * * /opt/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

9.3 Восстановление данных из резервной копии

Восстановление данных производится из папки, путь к которой определен значением параметра `backup_path` конфигурационного файла `/opt/aecaVa/scripts/config.sh` на сервере Центра валидации Aladdin eVA.

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

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

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

Если восстановление происходит после переустановки ОС, выполните:

- подготовку к установке программы в соответствии с разделом ☒ настоящего документа;
- установку программы в соответствии с разделом 4 настоящего документа;
- копирование в созданный каталог файла резервной копии;
- восстановление данных из резервной копии, выполнив команду:

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

10 ОБНОВЛЕНИЕ ПРОГРАММЫ

10.1 Назначение обновлений

Обновление базы данных и модулей Центра валидации Aladdin eVA 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.

10.2 Информирование потребителей о выпуске обновлений

Компания ведёт учёт покупателей Центра валидации Aladdin eVA.

Выполняется регистрация следующей информации:

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

Уведомление пользователей о выпуске обновлений Центра валидации Aladdin eVA выполняется путем публикации информации на [официальном сайте Компании](#) 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.

10.3 Получение обновлений потребителем

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

- С использованием электронной почты.
- Путем загрузки с [веб-сайта изготовителя \(производителя\)](#).

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

10.4 Контроль целостности обновления ПО

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

10.5 Процедура установки обновлений

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

Для обновления продукта:

- перенесите дистрибутив с обновлённой версией компонента на сервер с установленным Центром валидации Aladdin eVA любым удобным способом;

- проверьте целостность дистрибутива путём подсчёта контрольной суммы;
- выполните распаковку инсталляционного комплекта:

РЕД ОС и SberLinux OS Server `sudo dnf install aeca-*.rpm`

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

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

- запустите установку продукта в режиме обновления, выполнив команду:

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

- 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 Центра валидации Aladdin eVA;
- проверьте версию обновлённого Центра валидации Aladdin eVA в окне «О программе».

10.6 Критерий успешности установки обновления

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

11 УДАЛЕНИЕ ПРОГРАММЫ

11.1 Инициализация процесса удаления

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

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

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.

11.2 Удаление установочного пакета

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

- Для удаления необходимо выполнить следующую команду:

РЕД ОС и SberLinux OS Server	<pre>sudo dnf remove aeca-*.rpm</pre>
------------------------------	---------------------------------------

Astra Linux SE	<pre>sudo apt remove aeca-*.deb</pre>
----------------	---------------------------------------

Альт Сервер	<pre>sudo apt-get remove aeca-*.rpm</pre>
-------------	---

12 УДАЛЕНИЕ БАЗЫ ДАННЫХ POSTGRES

12.1 Удаление БД «aecava»

Для удаления ранее созданной базы данных «aecava» (имя БД, заданное по умолчанию) необходимо выполнить команду `drop database aecava;` с правами суперпользователя (root или sudo).

12.2 Удаление пользователя БД «aeca»

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

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

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

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

```
dropuser aeca -i
```

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

```
exit
```

- Перезапустите СУБД Postgres, выполнив команду:

```
sudo systemctl restart postgresql
```

13 МИГРАЦИЯ С ВЕРСИИ ПРОГРАММЫ 1.2 НА ВЕРСИЮ 2.3.0

13.1 Начальное состояние

Установлен Центр валидации Aladdin eVA 1.2.

13.2 Цель

На том же сервере, где ранее был развернут Центр валидации Aladdin eVA версии 1.2, развернуть Центр валидации Aladdin eVA версии 2.3.0 и обеспечить проксирование запросов к старым URL CDP и OCSP на новые URL CDP и OCSP от Центра валидации Aladdin eVA версии 2.3.0.

13.3 Рекомендации

В ходе миграции Центр валидации Aladdin eVA версии 1.2 будет удалён. До полного завершения сценария миграции проверка сертификатов по указанным в них URL CRL DP и OCSP Центра валидации Aladdin eVA 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 Центр валидации Aladdin eVA 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 Центра валидации Aladdin eVA версии 1.2.

Если миграция по какой-либо причине не будет выполнена, то при одновременном использовании Центров валидации Aladdin eVA версии 1.2 и версии 2.3.0 рекомендуется отключить запись точек распространения и служб OCSP от Центра валидации Aladdin eVA версии 1.2 в выпускаемые сертификаты, обеспечивая таким образом постепенный переход на Центр валидации Aladdin eVA версии 2.3.0. Такая возможность доступна в разделе «Центры валидации» программы. Это необходимо сделать для всех Центров сертификации Aladdin eCA, которые обслуживает данный Центр валидации Aladdin eVA версии 1.2. Работоспособность Центра валидации Aladdin eVA 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 Центра валидации Aladdin eVA 1.2.

13.4 План миграции №1⁷⁶

Порядок миграции Центра валидации Aladdin eVA версии 1.2 на версию 2.3.0:

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 Центров сертификации Aladdin eCA, не блокирует процесс миграции.

Пример: Центр валидации Aladdin eVA версии 1.2 зарегистрирован в одном ЦС Центра сертификации Aladdin eCA. Сведения о ЦС:

- URL распространения CRL: <http://va.eca.domain.kg:8080/aecaCdp/api/v2/crl/get-crl/3>
- URL распространения Delta CRL: <http://va.eca.domain.kg:8080/aecaCdp/api/v2/crl/get-delta-crl/3>
- URL AIA: <http://va.eca.domain.kg:8080/aecaCdp/api/v2/aia/get-aia/3>
- URL OCSP: <http://va.eca.domain.kg:8080/aeca-v2/ocsp>
- Идентификатор ЦВ: 2bf441c6-52f7-4204-b6f2-338c5edba38f

⁷⁶ В Центре валидации Aladdin eVA версии 1.2 служба OCSP была создана только для одного Центра сертификации.

2. Если Центр валидации Aladdin eVA версии 1.2 был развернут в виртуальной среде, рекомендуется при наличии возможности сделать снимок состояния виртуальной машины.
3. Обновите все экземпляры Центров сертификации Aladdin eCA до версии 2.3.0, в ЦС которых зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. документ «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
4. Удалите во всех экземплярах Центров сертификации Aladdin eCA ЦВ, в ЦС которых зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. документ «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
5. Удалите Центр валидации Aladdin eVA версии 1.2 (см. раздел 11 настоящего руководства администратора).
6. Выполните установку Центра валидации Aladdin eVA версии 2.3.0 в соответствии с настоящим руководством администратора (см. разделы **3** и **4**).
7. В Центре валидации Aladdin eVA версии 2.3.0 создайте подключения ко всем экземплярам Центра сертификации Aladdin eCA, в ЦС которых ранее был зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. раздел 6.3.8 настоящего руководства администратора).
8. В Центре валидации Aladdin eVA версии 2.3.0 создайте ЦВ для всех ЦС, в которых ранее был зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. раздел 6.2.2).

Примечания:

- 1 Если ЦС принадлежат к разным экземплярам Центра сертификации Aladdin eCA, создавать ЦВ необходимо под учётной записью пользователя с ролью «Администратор», созданной в соответствующем экземпляре Центра сертификации Aladdin eCA.
- 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 Центра валидации Aladdin eVA версии 1.2 (URL сохранены на шаге 1 настоящего сценария) укажите пути проксирования к соответствующим URL ЦВ Центра валидации Aladdin eVA версии 2.3.0.

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 Центра валидации Aladdin eVA 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.kg/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.kg/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.kg/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.kg/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:

```
sudo 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:

- `sudo systemctl restart nginx` - для веб-сервера Nginx
- `sudo 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 Центра валидации Aladdin eVA 2.3.0 - 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.kg/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.kg/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.kg/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.kg/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.kg/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.kg/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.kg/validation-authority-
service/api/v2/public/validation-authorities/2bf441c6-52f7-4204-b6f2-
338c5edba38f/ocsp/engine

ProxyPassReverse /aeca-va/ocsp http://va.eca.domain.kg/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:

- `sudo systemctl restart apache2`
- `sudo systemctl restart httpd`

10. Выполните проверку результатов миграции. Убедитесь в доступности точек распространения и службы OCSP (при наличии) по URL ЦВ Центра валидации Aladdin eVA версии 1.2.

13.5 План миграции №2⁷⁷

1. Составьте список издателей (ЦС), в которых зарегистрирован Центр валидации Aladdin eVA 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 руководства.
Примечание - Сценарий, при котором ЦС принадлежат разным экземплярам Центров сертификации Aladdin eCA, не блокирует процесс миграции.
2. Если Центр валидации Aladdin eVA версии 1.2 был развернут в виртуальной среде, рекомендуется при наличии возможности сделать снимок состояния виртуальной машины.
3. Обновите все экземпляры Центров сертификации Aladdin eCA до версии 2.3.0, в ЦС которых зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. документ «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
4. Удалите во всех экземплярах Центров сертификации Aladdin eCA ЦВ, в ЦС которых зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. документ «Aladdin Enterprise Certificate Authority Certified Edition. Руководство администратора. Часть 1. Установка и обслуживание Центра сертификации Aladdin Enterprise Certification Authority»).
5. Удалите Центр валидации Aladdin eVA версии 1.2 (см. раздел 11 настоящего руководства администратора).
6. Выполните установку Центра валидации Aladdin eVA версии 2.3.0 в соответствии с настоящим руководством администратора (см. разделы [3](#) и [4](#)).
7. В Центре валидации Aladdin eVA версии 2.3.0 создайте подключения ко всем экземплярам Центра сертификации Aladdin eCA, в ЦС которых ранее был зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. раздел 6.3.8 настоящего руководства администратора).
8. В Центре валидации Aladdin eVA версии 2.3.0 создайте ЦВ для всех ЦС, в которых ранее был зарегистрирован Центр валидации Aladdin eVA версии 1.2 (см. раздел 6.3.8).

Примечания:

1 Если ЦС принадлежат к разным экземплярам Центра сертификации Aladdin eCA, создавать ЦВ необходимо под учётной записью пользователя с ролью «Администратор», созданной в соответствующем экземпляре Центра сертификации Aladdin eCA.

2 В ходе создания ЦВ создайте службу OCSP, если она ранее использовалась для ЦС.

9. Установите на сервер, где развернут Центр валидации Aladdin eVA, средство балансирования нагрузки HAProxy, и отредактируйте конфигурационный файл согласно примеру⁷⁸, приведенному ниже:⁷⁹

```
global
    log /dev/log local0 debug
    tune.bufsize 32768

defaults
    mode http
    timeout connect 5s
    timeout client 30s
```

⁷⁷ Служба OCSP была создана для нескольких Центров сертификации.

⁷⁸ В примере представлена настройка проксирования для двух служб OCSP разных Центров сертификации.

```

    timeout server 30s
    option httplog
frontend ocspl_reader
    bind *:8080

    # В строке выше указывается порт, по которому осуществлялся доступ к Центру
    # валидации Aladdin eVA 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 Центре
    # валидации Aladdin eVA 1.2
    acl is_delta_crl1 path_beg /aecaCdp/api/v2/crl/get-delta-crl/3

    #В строке выше необходимо указать путь к точке распространения DELTA CRL ЦС1 в
    # Центре валидации Aladdin eVA 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 Центре
    # валидации Aladdin eVA 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 Центре
    # валидации Aladdin eVA 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
    # Центре валидации Aladdin eVA 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 Центре
    # валидации Aladdin eVA 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 Центра валидации
Aladdin eVA 2.3.0
    server ocsp01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центра
валидации Aladdin eVA 2.3.0

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 Центра валидации
Aladdin eVA 2.3.0
    server ocsp02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центра
валидации Aladdin eVA 2.3.0

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 Центра валидации
Aladdin eVA 2.3.0
    server crl01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центра
валидации Aladdin eVA 2.3.0

backend deltacr11
    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 Центра валидации
Aladdin eVA 2.3.0
    server deltacr101 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центра
валидации Aladdin eVA 2.3.0

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 Центру валидации
Aladdin eVA2.x
    server aia01 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центру
валидации Aladdin eVA2.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 Центру валидации
Aladdin eVA2.x
    server crl02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центру
валидации Aladdin eVA2.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 Центру валидации
Aladdin eVA2.x
    server deltacrl02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центру
валидации Aladdin eVA2.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 Центру валидации
Aladdin eVA2.x
    server aia02 aecava:80 check
    #В строке выше вместо "aecava:80" необходимо указать имя хоста и порт Центру
валидации Aladdin eVA2.x

```

10. Выполните проверку результатов миграции. Убедитесь в доступности точек распространения и служб OCSP по URL ЦВ Центра валидации Aladdin eVA версии 1.2.

14 ПОИСК И УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ

Проблема	Возможная причина	Способы решения
Ошибка при запуске скрипта установки install.sh «error obtaining MAC configuration for user «аеса»»	У пользователя postgres нет прав на чтение БД атрибутов конфиденциальности	Для предоставления дополнительных прав пользователю postgres выполните команды:
		<pre>sudo usermod -a -G shadow postgres sudo setfacl -d -m u:postgres:r /etc/parsec/macdb sudo setfacl -R -m u:postgres:r /etc/parsec/macdb sudo setfacl -m u:postgres:rx /etc/parsec/macdb</pre>
Прекращение установки ПО или обновления Центра валидации Aladdin eVA	1. Нехватка аппаратных ресурсов	Произведите оценку ресурса вашего ПК в соответствии с требованием к аппаратным ресурсам, указанным в первой части Руководства администратора
	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 команды:	<pre>sudo update-alternatives --config java sudo update-alternatives --config javac sudo update-alternatives --config javap</pre>
Нет подключения к ресурсной системе	1. Включён протокол TLS	Измените настройку конфигурационного файла контроллера домена /etc/samba/smb.conf, добавив в раздел [global]:
		ldap server require strong auth = no
	2. Проверить подключение к контроллеру домена Samba	Проверьте подключение к контроллеру домена, используя инструмент ldapsearch:
		- получение списка пользователей
		<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=user)"</pre>
		- получение списка компьютеров
		<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=local" -H "ldap://192.168.111.148" "(objectCategory=computer)"</pre>
		- получение списка групп безопасности
		<pre>ldapsearch -D "Administrator@pki-test.local" -w "Qwerty1234" -b "DC=pki-test,DC=</pre>

Проблема	Возможная причина	Способы решения
		<p><code>pki-test " -H "ldap://192.168.111.148" "(objectCategory=group) "</code></p> <p>где:</p> <p><code>Administrator@pki-test.local</code> - имя администратора домена;</p> <p><code>Qwerty1234</code> - пароль администратора домена;</p> <p><code>pki-test, pki-test</code> - доменное имя;</p> <p><code>192.168.111.148</code> - ip-адрес контроллера домена.</p> <p>В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.</p>
	3. Проверить подключение к контроллеру домена ALD PRO	<p>Проверьте подключение к контроллеру домена, используя инструмент <code>ldapsearch</code>:</p> <p>- получение списка пользователей</p> <pre>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=x-ald-user) "</pre> <p>- получение списка компьютеров</p> <pre>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) "</pre> <p>- получение списка групп безопасности</p> <pre>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) "</pre> <p>где:</p> <p><code>admin</code> - имя администратора домена;</p> <p><code>users, accounts</code></p> <p><code>Qwerty1234</code> - пароль администратора домена;</p> <p><code>domain, local</code> - доменное имя;</p> <p><code>192.168.111.148</code> - ip-адрес контроллера домена.</p> <p>В ответ на запрос вы должны получить список объектов, чтобы убедиться, что установлено соединение с ldap-сервером и он отвечает на запросы.</p>

Проблема	Возможная причина	Способы решения
Вход в интерфейс Центра валидации Aladdin eVA с выпущенным сертификатом невозможен в браузере Chromium	Браузер Chromium не поддерживает сертификаты с алгоритмом шифрования ECDSA512	Использовать другой браузер
Вход в интерфейс Центра валидации Aladdin eVA 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 <code>top</code> : - в <code>MiB Mem</code> значение <code>total</code> - это общий объем оперативной памяти; - в <code>MiB Mem</code> значение <code>free</code> - это свободная оперативная память; - в строке таблицы <code>USER=aeca</code> значение в колонке <code>RES</code> - это потребляемая ЦВ оперативная память.

Проблема	Возможная причина	Способы решения
		<p>Для корректной работы ЦВ сумма <code>free</code> и <code>RES</code> должна быть не менее 8 Гб (см. 2.2).</p> <p>2. Если полученное значение меньше 8 Гб, то при исчерпании свободной оперативной памяти <code>oom-killer</code> останавливает ЦВ.</p> <p>В данном случае рекомендуется проанализировать состав стороннего ПО на хосте и его потребление памяти, например, с помощью команд <code>top</code> или <code>htop</code>.</p> <p>3. После этого следует либо добавить необходимое количество оперативной памяти, либо удалить с хоста стороннее ПО, освободив этим оперативную память.</p> <p>В итоге для ЦВ должно быть доступно не менее 8 Гб оперативной памяти (см. 2.2).</p>

ПРИЛОЖЕНИЕ 1. РАЗРЕШЕНИЕ КОНФЛИКТА «ПРИ УСТАНОВКЕ СУБД POSTGRES И POSTGRES PRO⁸⁰»

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

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

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

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

- Для настройки 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 (root или sudo):

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

⁸⁰ 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, необходимо разрешить подключение по протоколу TCP для порта СУБД, выполнив в терминале на данном хосте следующую команду:

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

где `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432). Данная команда разрешит подключение к СУБД с любого IP-адреса. В случае, если необходимо ограничить доступ к порту СУБД, предоставив его только для определенного IP-адреса, необходимо использовать следующую команду:

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

где `IP` - IP-адрес, доступ с которого необходимо разрешить, а `port` - порт для подключения к СУБД (по умолчанию в поддерживаемых СУБД используется порт 5432).

- Если в качестве ОС на хосте с СУБД используется РЕД ОС, 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)⁸¹, 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)⁸², указав для параметра `listen_addresses` значение `*`:

```
listen_addresses = '*'
```

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

⁸¹ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

⁸² Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba

```
listen_addresses = '192.168.111.100'
```

- Затем на хосте СУБД необходимо перезапустить используемую СУБД, выполнив команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).
- Затем на хосте СУБД необходимо выполнить создание и настройку базы данных. В результате должна быть создана база данных с выбранными параметрами (имя пользователя, пароль, имя базы данных).

2.2 Настройка на хосте Центра валидации Aladdin eVA

На хосте Центра валидации Aladdin eVA предварительно должна быть выполнена установка СУБД.

При этом не нужно настраивать СУБД, установленную на хосте Центра валидации Aladdin eVA.

На хосте Центра валидации Aladdin eVA 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 ⁸³ . Допустимые значения: true, false
database_username	'aeca'	Имя пользователя базы данных, используемое для работы Центра валидации Aladdin eVA. Необходимо внести значение, указанное при создании и настройке базы данных на хосте СУБД
database_password	'#CHANGEIT'	Пароль пользователя базы данных, используемый для работы Центра валидации Aladdin eVA. 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 Центром валидации Aladdin eVA. 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 ⁸⁴

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

⁸³ Подробная информация о параметре `use_tls` приведена в приложении 3.

⁸⁴ Подробная информация о параметре `root_cert_path` приведена в приложении 3.

ПРИЛОЖЕНИЕ 3. НАСТРОЙКА TLS-СОЕДИНЕНИЯ С СУБД

Для настройки TLS-соединения Центра валидации Aladdin eVA с СУБД необходимо в предварительно развернутом и инициализированном программном компоненте «Центр сертификации Aladdin Enterprise Certification Authority» создать сертификат с закрытым ключом (PKCS#12) для сервера СУБД. При этом в сертификате сервера СУБД в атрибуте Common Name или в атрибуте Subject Alternative Name типа dNSName обязательно должно быть указано доменное сервера СУБД (или IP-адрес)⁸⁵, так как Центра валидации Aladdin eVA 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 Центре валидации Aladdin eVA, указав ему необходимые атрибуты CN и DNS Name).

Во избежание ошибок в работе Центра валидации Aladdin eVA перед началом настройки TLS-соединения с СУБД рекомендуется остановить работу Центра валидации Aladdin eVA путем выполнения команды `sudo systemctl stop aeca-va.service`.

Для настройки TLS-соединения Центра валидации Aladdin eVA с СУБД необходимо:

- выполнить настройку СУБД в соответствии с разделом 3.1, представленным ниже;
- выполнить настройку Центра валидации Aladdin eVA 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)⁸⁶, указав в параметре:

- «ssl» значение «on»;
- «ssl_cert_file» абсолютный путь к файлу сертификата сервера СУБД⁸⁷;
- «ssl_key_file» абсолютный путь к файлу закрытого ключа сервера СУБД⁸⁸;
- «ssl_ca_file» абсолютный путь к файлу цепочки сертификатов издателя сертификата СУБД⁸⁹.

⁸⁵ Указанное в сертификате доменное сервера СУБД (или IP-адрес) должно соответствовать значению параметра «database_host» конфигурационного файла программного компонента Центра валидации Aladdin eVA.

⁸⁶ Путь к файлу может отличаться в зависимости от версии PostgreSQL или Jatoba.

⁸⁷ Файл сертификата сервера СУБД может быть скачан из пользовательского интерфейса программного компонента Центра валидации Aladdin eVA. Например, в карточке локального субъекта сервера СУБД.

⁸⁸ 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.

⁸⁹ Файл цепочки сертификатов издателя сертификата СУБД может быть скачан в карточке ЦС, выпустившего сертификат сервера СУБД.

При этом указанные выше файлы должны иметь метку доступа «600», установить которую можно с помощью команды `sudo chmod 600 путь_к_файлу` для каждого файла. Владелец всех указанных выше файлов необходимо назначить пользователя «postgres», выполнив команду `sudo chown postgres:postgres путь_к_файлу` для всех перечисленных файлов. Указанные файлы должны располагаться в каталоге, к которому имеет доступ пользователь postgres (например, /tmp). В случае использования ОС РЕД ОС 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.

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 команду `sudo systemctl restart postgresql` (или `sudo systemctl restart jatoba-4` если используется СУБД Jatoba).

3.2 Настройка Центра валидации Aladdin eVA

На хосте Центра валидации Aladdin eVA 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 СУБД⁹⁰.

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

На хосте Центра валидации Aladdin eVA примените изменения конфигурационного файла путём запуска команды `sudo bash /opt/aecaVa/scripts/install.sh` и дальнейшего выбора действия «[Update]».

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

⁹⁰ 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 Центр валидации Aladdin eVA может взаимодействовать со средством криптографической защиты информации (СКЗИ) - криптопровайдером СКЗИ «КриптоПро CSP».

Взаимодействие Центра валидации Aladdin eVA с криптопровайдером СКЗИ «КриптоПро CSP» осуществляется через модуль «КриптоПро Java CSP»⁹¹. При каждом запуске Центр валидации Aladdin eVA определяется наличие на его хосте активного криптопровайдера СКЗИ «КриптоПро CSP».

До выполнения настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром валидации Aladdin eVA необходимо подготовить внешнюю гамму⁹². Подключение внешней гаммы необходимо для генерации ключевых пар центров сертификации, субъектов и пользователей по алгоритмам, криптопровайдером которых является СКЗИ «КриптоПро CSP».

При разворачивании нескольких экземпляров Центра валидации Aladdin eVA под одним средством балансирования нагрузки необходимо для каждого экземпляра программного средства подготовить уникальную внешнюю гамму, чтобы исключить совпадения ключевых пар.

Порядок настройки взаимодействия СКЗИ «КриптоПро CSP» с Центром валидации Aladdin eVA:

- На сервере Центра валидации Aladdin eVA выполнить установку криптопровайдера СКЗИ «КриптоПро CSP» в соответствии с инструкцией, описанной в разделе 2 документа «СКЗИ «КриптоПро CSP». Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux» ЖТЯИ.00101-03 91 03.

Внимание! Перед установкой СКЗИ «КриптоПро CSP» в ОС Альт 8 СП Сервер установите пакет newt52 командой `sudo apt-get install newt52`.

- При отсутствии создайте каталог `/opt/aecaVa/services/cryptoproviders` командой:

```
sudo 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:

```
sudo 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 Центра валидации Aladdin eVA, то назначьте файлам права доступа (`chmod 777`) командой:

```
sudo chmod 777 /opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar,sspiSSL.jar} -R
```

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

⁹¹ Модуль «КриптоПро Java CSP» входит в состав СКЗИ «КриптоПро CSP».

⁹² 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».

```
sudo chown aeca:aeca
/opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar,sspiSSL.jar} -R
sudo chmod 700
/opt/aecaVa/services/cryptoproviders/{ASN1P.jar,asn1rt.jar,JCP.jar,JCSP.jar,cpSSL.jar,sspiSSL.jar} -R
```

- Если используется уже заранее подготовленная внешняя гамма, то пропустите этот пункт. Иначе подготовьте внешнюю гамму с помощью утилиты `/opt/cproscsp/bin/amd64/genkpm` (утилита `genkpm` входит в состав дистрибутива СКЗИ «КриптоПро CSP») командами:

```
mkdir -p ~/gamma
/opt/cproscsp/bin/amd64/genkpm <количество ключей> 0x12345678 ~/gamma
```

- На хосте Центра валидации Aladdin eVA поместите каталог с заранее подготовленной внешней гаммой в каталог `/opt/aecaVa/dist/` командой:

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

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

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

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

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

- Подключить данную внешнюю гамму к СКЗИ «КриптоПро CSP» посредством следующих команд⁹³:

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

- Если Центр валидации Aladdin eVA был ранее установлен, перезапустите сервис `aeca-va.service` командой:

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

Если в дальнейшем к СКЗИ «КриптоПро CSP» будет подключён ПАКМ «КриптоПро HSM», для обнаружения Центра валидации Aladdin eVA наличия такого подключения необходимо перезапустить сервис `aeca-va.service`.

⁹³ Подключение осуществляется с помощью файла `cpconfig` (находится в `/opt/cproscsp/sbin/amd64`). Путь к файлу в командах приведен с учётом нахождения в каталоге `/opt/cproscsp/sbin/amd64`.

ПРИЛОЖЕНИЕ 5. НАСТРОЙКА KERBEROS В ВЕБ-БРАУЗЕРЕ

Предварительно на клиенте должен быть настроен Kerberos, клиент должен быть подключён к домену и клиент должен использовать браузер с поддержкой Kerberos.

Для того, чтобы в браузере клиента при работе с Центром валидации Aladdin eVA была доступна аутентификация по Kerberos необходимо внести доменное имя Центра валидации Aladdin eVA 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`, `aecal.al.rd.kg` - доменные имена Центров регистрации Aladdin eRA
- `al.rd.kg` - домен, (`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` одно из следующих значений (см. Рисунок 51):
 - Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, введите полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.rd.kg`).
 - Чтобы разрешить SPNEGO аутентификацию для целого домена, введите имя домена с точкой в начале (например, `.al.rd.kg`).
 - Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, введите их полные доменные имена через запятую (например, `aeca.al.rd.kg, aecal.al.rd.kg`).
- Продублируйте введенное значение параметра `network.negotiate-auth.trusted-uris` в параметре `network.negotiate-auth.delegation-uris`.

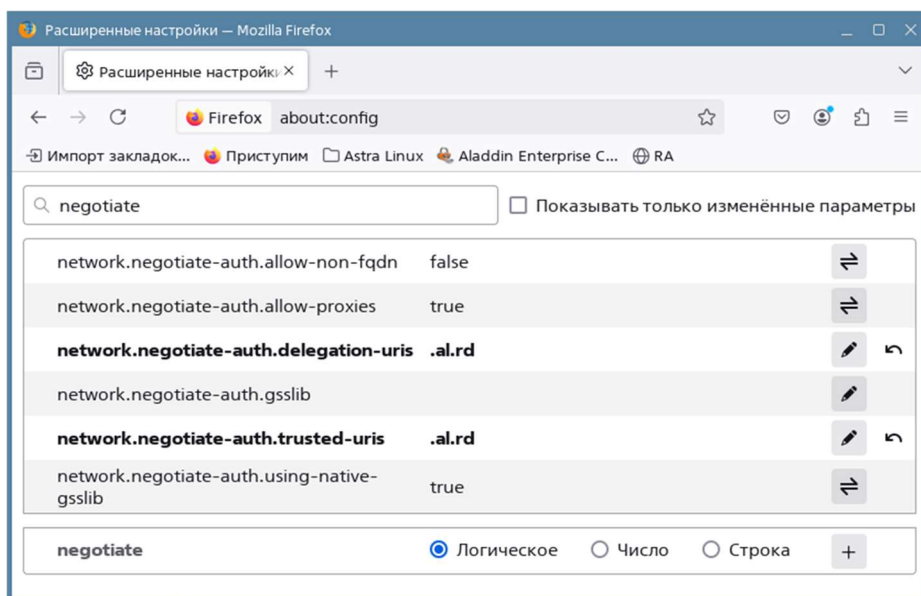


Рисунок 51 - Настройка Kerberos-аутентификации в веб-браузере Firefox

5.2 Настройка веб-браузера Chromium

Далее в примере:

- `aeca.al.kg`, `aecal.al.kg` - доменные имена Центров регистрации Aladdin eRA
- `al.kg` - домен, (`AL.KG` - 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:

```
sudo touch /etc/chromium/policies/managed/policies.json
```

- Откройте файл для редактирования, выполнив следующую команду с правами суперпользователя:

```
sudo nano /etc/chromium/policies/managed/policies.json
```

- В файле `policies.json` укажите следующие политики в формате JSON:

```
{
  "AuthServerAllowlist": "*.al.kg",
  "AuthSchemes": "ntlm,negotiate"
}
```

Примечания:

- Чтобы разрешить SPNEGO аутентификацию по конкретной ссылке, укажите для политики «AuthServerAllowlist» полное доменное Центра регистрации Aladdin eRA (например, `aeca.al.kg`).
- Чтобы разрешить SPNEGO аутентификацию для целого домена, укажите для политики «AuthServerAllowlist» имя домена (например, `*.al.kg`).
- Чтобы разрешить SPNEGO аутентификацию для нескольких Центров регистрации Aladdin eRA, укажите для политики «AuthServerAllowlist» их полные доменные имена через запятую (например, `aeca.al.kg, aecal.al.kg`).
- Запустите веб-браузер Chromium и введите в адресной строке `chrome://policy`.
- Убедитесь, что политики были применены (см. Рисунок 52).

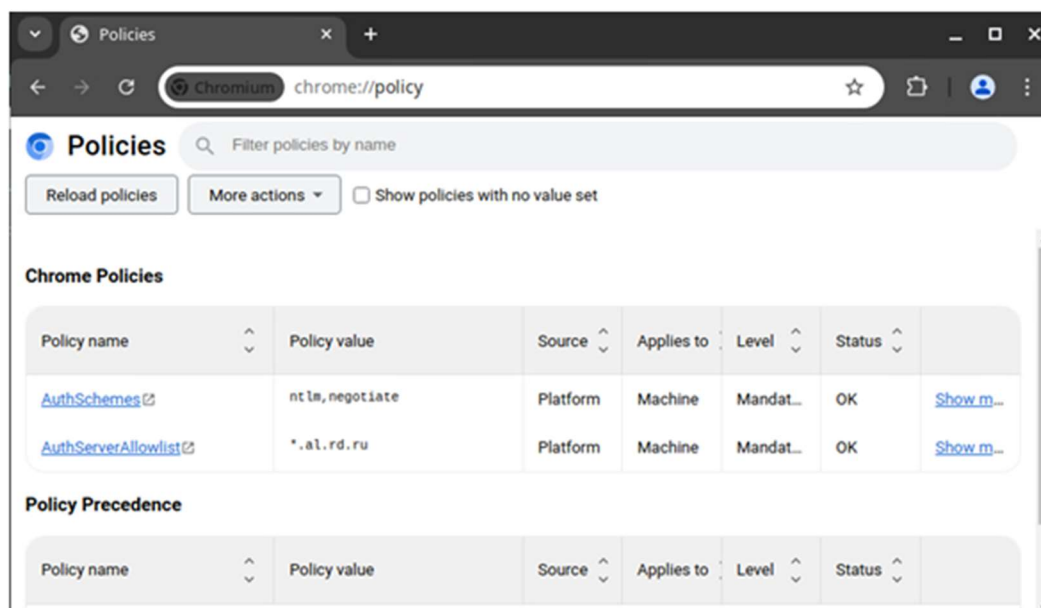


Рисунок 52 - Настройка Kerberos-аутентификации в веб-браузере Chromium

ПЕРЕЧЕНЬ ДОКУМЕНТАЦИИ ДЛЯ ОЗНАКОМЛЕНИЯ

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

- [официальная документация РЕД ОС 7.1;](#)
- [официальная документация Astra Linux Special Edition 1.7;](#)
- [официальная документация Альт Сервер 8, релиз 10;](#)
- [официальная документация Postgres;](#)
- [официальная документация Jatoba 4;](#)

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 Центре валидации Aladdin eVA.

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 Центре валидации Aladdin eVA, соответствующая физическому токenu, программному или аппаратному модулю безопасности Hardware Security Module (HSM). С помощью крипто-токена ЦС осуществляет хранение ключей и выполнение криптографических операций.

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

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

Оператор - сотрудник (специалист) или система (приложение, сервис) и соответствующая роль в Центре валидации Aladdin eVA, 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.

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

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

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

Список отозванных сертификатов (Certificate Revocation List - **CRL**) - список аннулированных (отозванных) сертификатов, 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 программного компонента «Центр сертификации Aladdin Enterprise Certification Authority».

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

[illegible]