Руководство пользователя Clearway CA 26.3.0

Документация Clearway CA

6 November, 2026

Table of Contents

1 Термины и сокращения 7
1.1 Принятые сокращения 7
1.2 Термины и определения 8
2 Введение 10
2.1 Идентификационные данные 10
2.2 Общее описание 10
3 Начало работы 13
3.1 Вход в систему 13
3.2 Интерфейс и навигация 14
3.2.1 Левое меню 14
3.2.2 Меню пользователя 16
3.2.3 Заголовок страницы 16
3.2.4 Текущий ЦС 16
3.3 Профиль и права доступа 17
3.4 Ролевая модель и разграничение полномочий 18
4 Общие элементы интерфейса 21
4.1 Страница-реестр 21
4.2 Постраничная навигация 22
4.3 Сортировка 22
4.4 Фильтры в заголовках столбцов 23
4.5 Боковая панель фильтров 24
4.6 Сброс условий отбора 24
4.7 Выделение строк и групповые действия 25
4.8 Настройка таблицы 25
4.9 Выгрузка отчёта в файл 27
4.10 Меню «Действия» и закрепление действий 28
4.11 Нижняя панель 28
4.12 Окна, формы и уведомления 29
5 Сертификаты 31

5.1 Реестр сертификатов ... 31
5.1.1 Кнопки реестра ... 31
5.1.2 Столбцы и фильтры ... 32
5.2 Выпуск сертификата ... 34
5.2.1 Запрос сертификата ... 34
5.2.2 Просмотр структуры запроса ... 38
5.2.3 Пакетный запрос сертификатов ... 39
5.3 Конструктор CSR-запросов ... 40
5.3.1 Порядок работы ... 41
5.3.2 Шаблон и хранилище ключа ... 41
5.3.3 Параметры запроса ... 42
5.3.4 Результат для Linux и Windows ... 43
5.3.5 Создание ключа и CSR на носителе ... 44
5.3.6 Выпуск сертификата и запись на носитель ... 45
5.4 Карточка сертификата ... 46
5.4.1 Реквизиты сертификата ... 47
5.4.2 Подписки ... 47
5.4.3 Скачивание сертификата ... 48
5.4.4 Отзыв сертификата ... 49
5.4.5 Восстановление сертификата ... 51
6 Шаблоны сертификатов ... 52
6.1 Реестр шаблонов ... 52
6.2 Карточка шаблона ... 54
6.2.1 Параметры шаблона ... 55
6.2.2 Блок «Дополнительно» ... 55
6.3 Создание, изменение, копирование и удаление шаблона ... 57
6.3.1 Создание шаблона ... 57
6.3.2 Изменение шаблона ... 59
6.3.3 Копирование шаблона ... 59
6.3.4 Удаление шаблона ... 60
6.4 Разграничение прав доступа к шаблонам ... 61
6.4.1 Настройка разрешений ... 61

6.5 Экспорт и импорт шаблонов в формате JSON ... 62
6.6 Ограничения для Subject и SAN ... 63
6.6.1 Способы проверки значения ... 64
6.6.2 Добавление ограничения ... 64
6.6.3 Изменение и удаление ограничения ... 67
6.6.4 Проверка запроса при выпуске ... 68
6.7 Справочник значений ... 70
6.7.1 Типы и размеры ключей ... 70
6.7.2 Значения Key Usage ... 70
6.7.3 Значения Extended Key Usage ... 71
6.7.4 Значения Authority Key Identifier ... 72
7 Запросы и согласование выпуска ... 73
7.1 Реестр запросов ... 73
7.1.1 Статусы запроса ... 74
7.1.2 Карточка запроса ... 75
7.2 Одобрение и отклонение запросов ... 75
7.2.1 Групповое одобрение и отклонение ... 76
8 Журнал событий ... 78
9 Списки отзыва CRL и Delta CRL ... 82
9.1 Страница «Информация о CRL и Delta CRL» ... 82
9.1.1 Вкладка «Отозванные сертификаты» ... 83
9.2 Действия со списками отзыва ... 83
9.2.1 Скачивание CRL и Delta CRL ... 84
9.2.2 Обновление CRL ... 84
10 Самодиагностика ... 87
10.1 Страница «Статистика ЦС» ... 88
10.1.1 Настройка вида страницы ... 89
10.2 Команда mclient stat ... 91
11 Задачи ... 92
11.1 Задачи публикации ... 92
11.2 Управление задачами публикации ... 94
11.2.1 Добавление задачи публикации сертификатов ... 94

11.2.2 Добавление задачи публикации CRL ... 97
11.2.3 Просмотр, запуск, изменение и удаление задачи ... 100
11.3 Резервное копирование ... 102
11.3.1 Список заданий ... 103
11.3.2 Добавление задания ... 103
11.3.3 Карточка задания ... 105
11.3.4 Состав и хранение копии ... 106
11.3.5 Восстановление из копии ... 107
11.4 Типовые задачи ... 109
11.4.1 Шаг 1. Подключение к серверу ... 109
11.4.2 Шаг 2. Пути к сертификату и ключу ... 110
11.4.3 Шаг 3. Параметры выпуска и замена ... 111
11.4.4 Замена сертификата postgres ... 111
12 Настройки ... 112
12.1 Конфигурация ... 112
12.1.1 Выбор экземпляра ЦС ... 112
12.1.2 Действия на странице ... 113
12.1.3 Добавление ЦС ... 114
12.1.4 Изменение подключения к ЦС ... 116
12.1.5 Скачивание цепочки сертификатов ... 116
12.2 Ротация ключей ... 116
12.2.1 Формирование CSR ... 118
12.2.2 Замена сертификата ЦС ... 118
13 Аппаратные токены ... 120
13.1 Требования к рабочему месту ... 120
13.2 Карточки производителей и устройств ... 121
13.3 Просмотр содержимого носителя ... 122
13.4 Операции с объектами на носителе ... 122
14 Защита ключей и конфиденциальных данных ... 124
14.1 Шифрование закрытого ключа при подготовке запроса ... 124
14.2 Шифрование данных сертификата в базе данных ... 124
14.3 Хранение и восстановление закрытых ключей (KRA) ... 124

15 Выпуск и проверка сертификатов по протоколам 126
15.1 SCEP 126
15.1.1 Получение одноразового пароля 127
15.1.2 Получение сертификата с помощью certmonger 128
15.2 MS-WSTEP 131
15.2.1 Подготовка домена 132
15.2.2 Регистрация политики на компьютере 132
15.2.3 Запрос сертификата 133
15.3 Проверка статуса по протоколу OCSP 134
15.4 Другие протоколы 136
16 Работа через командную строку (mclient) 137
16.1 Подготовка 137
16.2 Основные команды 137

1 Термины и сокращения

1.1 Принятые сокращения

Термин	Расшифровка
API	Application Programming Interface: прикладной программный интерфейс компонента ИС.
CRL	Certificate Revocation List (список отзыва сертификатов): подписанный ЦС перечень сертификатов, отозванных до окончания срока действия.
CSR	Certificate Signing Request: запрос на выпуск сертификата в формате PKCS#10. Содержит открытый ключ и сведения о владельце и подписан парным закрытым ключом; сам закрытый ключ в запрос не входит.
Delta CRL	Разностный список отзыва: содержит только изменения с момента публикации последнего полного CRL, поэтому меньше по объёму и публикуется чаще.
JWT	JSON Web Token: подписанный набор сведений о пользователе или программном клиенте, по которому ЦС определяет его права.
CEP / CES	Certificate Enrollment Policy / Certificate Enrollment Service (службы адаптера MS-WSTEP): служба политик регистрации сообщает компьютеру Windows доступные шаблоны, служба регистрации принимает запрос и возвращает сертификат.
KRA	Key Recovery Agent (агент восстановления ключей): сертификат, которым ЦС шифрует хранимые закрытые ключи.
MS-WSTEP	WS-Trust X.509v3 Token Enrollment Protocol: протокол Microsoft, по которому компьютеры и пользователи Windows запрашивают сертификаты штатными средствами ОС.
OCSP	Online Certificate Status Protocol: протокол проверки статуса отдельного сертификата в реальном времени.
RSA	Rivest-Shamir-Adleman: криптосистема на основе закрытого и открытого ключей.

SAN	Subject Alternative Name (дополнительные имена владельца сертификата): DNS-имена, IP-адреса, адреса электронной почты, URI.
SCEP	Simple Certificate Enrollment Protocol: протокол автоматического выпуска сертификатов для сетевого оборудования и серверов; право на выпуск подтверждается одноразовым паролем (challenge).
SSO	Single Sign-On (единый вход): однократная аутентификация для доступа ко всем компонентам.
TLS / mTLS	Transport Layer Security / mutual TLS: криптографический протокол на основе сертификатов X.509 для защищённой сетевой связи и взаимной аутентификации клиента и сервера. Развитие протокола SSL (Secure Sockets Layer).
Clearway CA, Система	Система централизованного анализа и управления гетерогенными инфраструктурами — Clearway CA.
EXC	Внешнее хранилище секретов. В полях паролей вместо самого пароля указывается ссылка на секрет вида mountPoint:path:key.
ИС	Информационная система.
ЦС (CA)	Центр сертификации (Certification Authority): сервер, который выпускает и отзывает сертификаты и формирует списки отзыва (CRL).

1.2 Термины и определения

Термин	**Определение**
Контрольная панель	Веб-интерфейс Clearway CA, через который пользователи работают с центром сертификации.
Право	Разрешение на просмотр или изменение данных определённого типа, например `rleMiniCACertList-r`. Суффикс -r означает просмотр, а -w означает изменение.
Роль	Набор прав, назначаемый пользователю через группу каталога (Active Directory или LDAP). Права роли передаются в токене JWT при входе в Контрольную панель.

Реестр	Страница Контрольной панели со списком записей в виде таблицы, например реестр сертификатов.
Шаблон сертификата	Именованный набор ограничений и расширений, по которому ЦС проверяет запрос и выпускает сертификат.
Cron-выражение	Расписание запуска задачи в формате cron, например 0 12 * * * (каждый день в 12:00 UTC). Время в расписаниях задач Clearway CA задаётся в UTC.

2 Введение

Настоящий документ относится к эксплуатационной документации ПО «Система централизованного анализа и управления гетерогенными инфраструктурами — Clearway CA» (далее Clearway CA). Разработчик Clearway CA: ООО «Клируэй Текнолоджис».

Центр сертификации Clearway CA выпускает сертификаты X.509v3 по запросам CSR в формате PKCS#10 с использованием шаблонов. Система позволяет создавать и настраивать шаблоны, отзывать сертификаты с указанием причины, формирует списки отзыва (CRL и Delta CRL) и предоставляет статус сертификатов по протоколу OCSP. Все запросы, сертификаты, события и списки отзыва сохраняются в базе данных. Управление выполняется через веб-интерфейс Контрольной панели и API; для выпуска сертификатов поддерживается протокол SCEP.

Документ предназначен для ознакомления технического персонала с основными операциями по работе с системой.

2.1 Идентификационные данные

Идентификационные данные приведены в таблице ниже.

Параметры документа	**Содержание данных**
Название документа	Руководство пользователя
Децимальный номер документа	RU.69639709.00002-01 34 01
Версия документа	1.0
Автор документа, предприятие-изготовитель	ООО «Клируэй Текнолоджис»

2.2 Общее описание

Основная функция Clearway CA состоит в управлении жизненным циклом сертификатов:

- Выпуск сертификатов:
  - выпуск сертификатов X.509v3 на основе запросов CSR в формате PKCS#10;
  - поддержка шаблонов сертификатов для наполнения и контроля атрибутов сертификатов;
  - поддержка выпуска сертификатов по протоколу SCEP, а при наличии соответствующих адаптеров также по MS-WSTEP и другим протоколам (см. «Выпуск и проверка сертификатов по протоколам»).
- Предоставление сертификата по запросу:
  - возможность получения выпущенных сертификатов по запросу;

    - возможность получения различных выборок и отчётов о выпущенных сертификатах.
- Отзыв сертификата:
    - отзыв сертификатов с указанием причины;
    - формирование списка отзыва сертификатов (CRL);
    - формирование разностных списков отзыва (Delta CRL);
    - предоставление информации о статусе сертификата по протоколу OCSP (см. «Проверка статуса по протоколу OCSP»).
- Вспомогательные функции:
    - сохранение информации обо всех запросах, сертификатах, CRL и Delta CRL в базе данных;
    - текстовый журнал событий;
    - поддержка функций самодиагностики;
    - поддержка хранения ключа ЦС на аппаратных носителях HSM.

Сведения, предусмотренные п. 16.2 Требований по безопасности информации, устанавливающих уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, и необходимые для эксплуатации Системы, приведены в соответствующих разделах эксплуатационной документации согласно таблице ниже.

№ п/п	**Сведения, предусмотренные п. 16.2 Требований доверия**	**Соответствующий раздел эксплуатационной документации**
1	Описание режимов работы средства	п. 2.2 «Общее описание» Руководства пользователя RU.69639709.00002-01 34 01
2	Описание принципов безопасной работы средства	раздел 6 «Обеспечение безопасной среды» Руководства администратора RU.69639709.00002-01 32 01 раздел 3 «Требования к среде» Руководства администратора RU.69639709.00002-01 32 01
3	Описание функций и интерфейсов функций средства, доступных каждой роли пользователей	п. 4.3 «Стандартные роли и матрица доступа» Руководства администратора RU.69639709.00002-01 32 01 п. 3.3 «Профиль и права доступа» Руководства пользователя RU.69639709.00002-01 34 01 п. 3.4 «Ролевая модель и разграничение полномочий» Руководства пользователя RU.69639709.00002-01 34 01 п. 6.4 «Разграничение прав доступа к шаблонам» Руководства пользователя RU.69639709.00002-01 34 01

4	Описание параметров (настроек) безопасности средства, доступных каждой роли пользователей, и их базовых значений	раздел 4 «Описание ролевой модели» Руководства администратора RU.69639709.00002-01 32 01
5	Описание типов событий безопасности, связанных с доступными пользователю функциями средства	раздел 8 «Журнал событий» Руководства пользователя RU.69639709.00002-01 34 01 п. 8.3 «Отказоустойчивый журнал событий безопасности (secLog)» Руководства администратора RU.69639709.00002-01 32 01
6	Описание действий после сбоев и ошибок эксплуатации средства	раздел 9 «Диагностика и устранение неисправностей» Руководства администратора RU.69639709.00002-01 32 01 п. 7.6 «Резервное копирование» Руководства администратора RU.69639709.00002-01 32 01

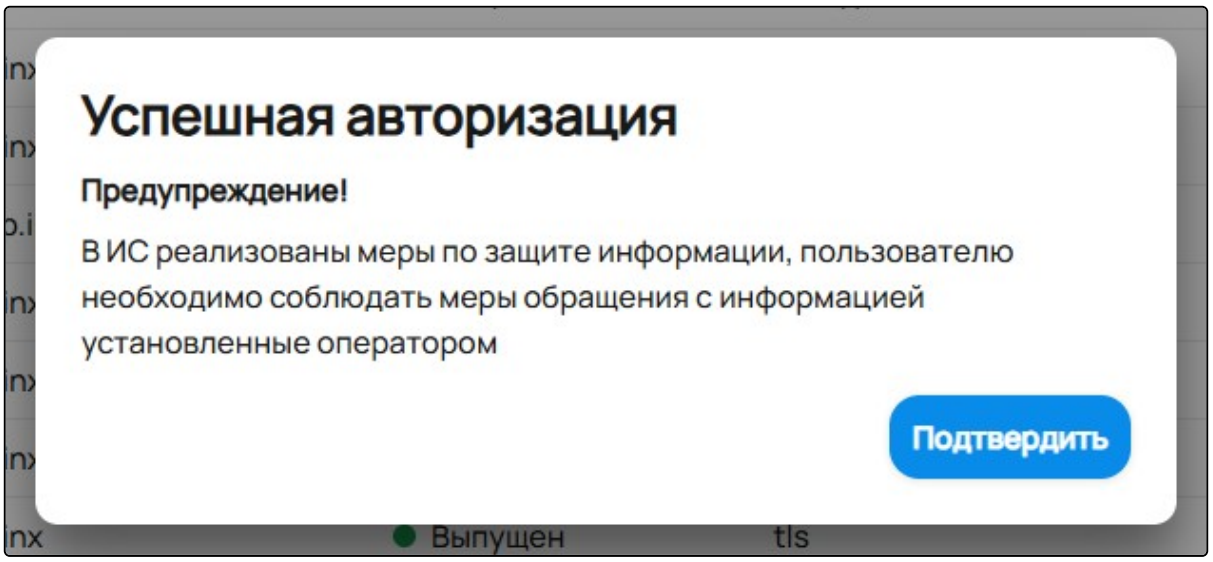
3 Начало работы

В этой главе описаны первые действия при работе с центром сертификации: вход в Контрольную панель, ориентирование в интерфейсе и проверка собственных прав доступа. Выполните их до перехода к операциям с сертификатами.

3.1 Вход в систему

Вход выполняется через веб-интерфейс Контрольной панели по технологии единого входа (SSO): одни и те же доменные учётные данные используются для всех компонентов Clearway CA, отдельная регистрация не требуется.

1. Откройте адрес Контрольной панели в браузере.
2. Войдите доменной учётной записью. Аутентификацию выполняет служба единого входа по протоколу OpenID Connect.
3. В окне «Успешная авторизация» ознакомьтесь с предупреждением о мерах защиты информации и нажмите **Подтвердить**. Откроется запрошенная страница, например карточка сертификата по ссылке; если открыт адрес Контрольной панели, открывается реестр «Сертификаты».



1 Окно «Успешная авторизация» с предупреждением о мерах защиты информации

Окно с предупреждением относится к обязательным мерам информационной безопасности. Нажатие **Подтвердить** означает, что пользователь ознакомлен с правилами обращения с защищаемой информацией. Окно появляется после каждого входа; закрыть его крестиком или клавишей Esc нельзя, без подтверждения рабочая область не открывается.

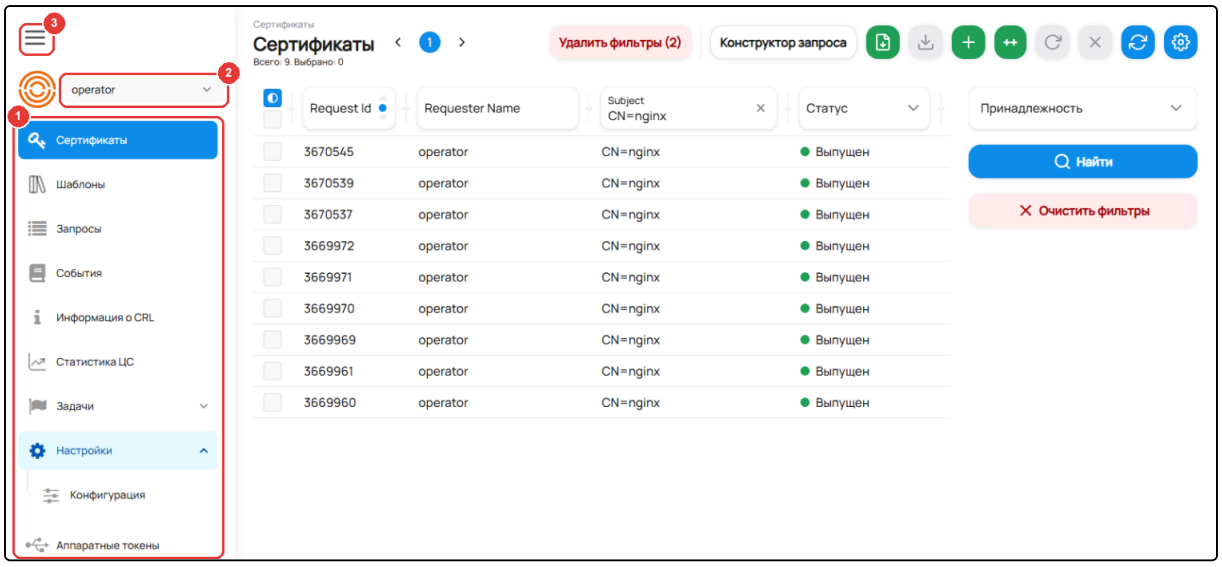
Если сеанс завершился, например истёк срок его действия, Контрольная панель откроет страницу входа. Войдите снова.

Если войти не удаётся, окно входа не открывается, отображается ошибка или доступ отклонён:

- убедитесь, что используется действующая доменная учётная запись и пароль введён верно;
- проверьте сетевой доступ к Контрольной панели и к службе аутентификации;
- обратитесь к администратору: учётная запись может быть заблокирована, отключена или не иметь прав на работу с центром сертификации.

3.2 Интерфейс и навигация

Экран Контрольной панели состоит из левого меню, заголовка страницы и рабочей области. На страницах-реестрах внизу экрана расположена нижняя панель (см. «Нижняя панель»).



2 Главный экран: развёрнутое левое меню и реестр сертификатов

На рисунке: **1** пункты левого меню; **2** имя пользователя (открывает профиль); **3** кнопка ≡ (разворачивает или сворачивает меню).

3.2.1 Левое меню

- Кнопка ≡ в верхней части меню разворачивает его: становятся видны названия пунктов и имя пользователя. Повторное нажатие сворачивает меню до значков; в свёрнутом меню название пункта показывается в подсказке.
- Пункт со стрелкой содержит вложенные пункты: щелчок по нему открывает или закрывает их список.
- Пункт открытого раздела выделен цветом.

Пункт меню отображается, только если у пользователя есть указанное право.

Пункт меню	Вложенные пункты	Право	Назначение

Сертификаты	Нет	`rleMiniCACertList-r`	Реестр и карточки сертификатов, выпуск, отзыв, конструктор CSR-запросов
Шаблоны	Нет	`rleMiniCATemplList-r`	Реестр и карточки шаблонов сертификатов
Запросы	Нет	`rleMiniCAReqList-r`	Запросы на выпуск сертификатов и их согласование
События	Нет	`rleMiniCAEventList-r`	Журнал событий ЦС
Информация о CRL	Нет	`rleMiniCACRL-r`	Сведения о CRL и Delta CRL, скачивание и обновление списков отзыва
Статистика ЦС	Нет	`rleMiniCAConfig-r`	Показатели состояния ЦС
Задачи	Публикация сертификатов, Публикация CRL	`rleMiniCACRL-w`	Задачи публикации сертификатов и списков отзыва
	Резервное копирование	`rleMiniCABackup-r`	Резервное копирование и восстановление ЦС
	Типовые → Замена сертификата nginx, Замена сертификата postgres	`rleMiniCACertReq-w`; функция типовых задач включена на сервере	Пошаговая замена TLS-сертификатов на серверах
Настройки	Конфигурация	`rleMiniCAConfig-r`	Выбор ЦС, состояние компонентов, подключение ЦС к Контрольной панели
	Ротация ключей	`rleMiniCARotation-w`	Замена сертификата и ключевой пары ЦС
Аппаратные токены	Нет	не требуется	Проверка компонентов и содержимого аппаратных носителей на компьютере пользователя

Группа «Задачи» отображается только при наличии права `rleMiniCACRL-w`: без него скрыты и вложенные пункты «Резервное копирование» и «Типовые». Группа «Настройки» отображается при наличии хотя бы одного из прав `rleMiniCAConfig-r` и `rleMiniCARotation-w`.

Страницы «Сертификаты», «Шаблоны», «Запросы», «События», «Информация о CRL», «Статистика ЦС», «Конфигурация», «Ротация ключей» и страницы типовых задач без соответствующего права не открываются и по прямой ссылке: вместо них открывается главная страница. Страницы «Профиль пользователя» и «Аппаратные токены» доступны всем пользователям.

3.2.2 Меню пользователя

В развёрнутом меню выводится имя текущего пользователя. Щелчок по имени открывает меню:

Пункт	Что делает
Профиль	Открывает страницу «Профиль пользователя»
Выйти	Завершает сеанс работы с Контрольной панелью

3.2.3 Заголовок страницы

В верхней части рабочей области расположены:

- хлебные крошки (путь к текущей странице, например «Шаблоны / Шаблон»). Названия разделов в крошках служат ссылками: при возврате в реестр по такой ссылке восстанавливаются условия отбора и страница, с которых вы перешли;
- название страницы;
- кнопки действий страницы (справа);
- постраничная навигация и счётчик записей на страницах-реестрах (см. главу «Общие элементы интерфейса»).

Пока загружаются данные, поверх страницы отображается индикатор загрузки.

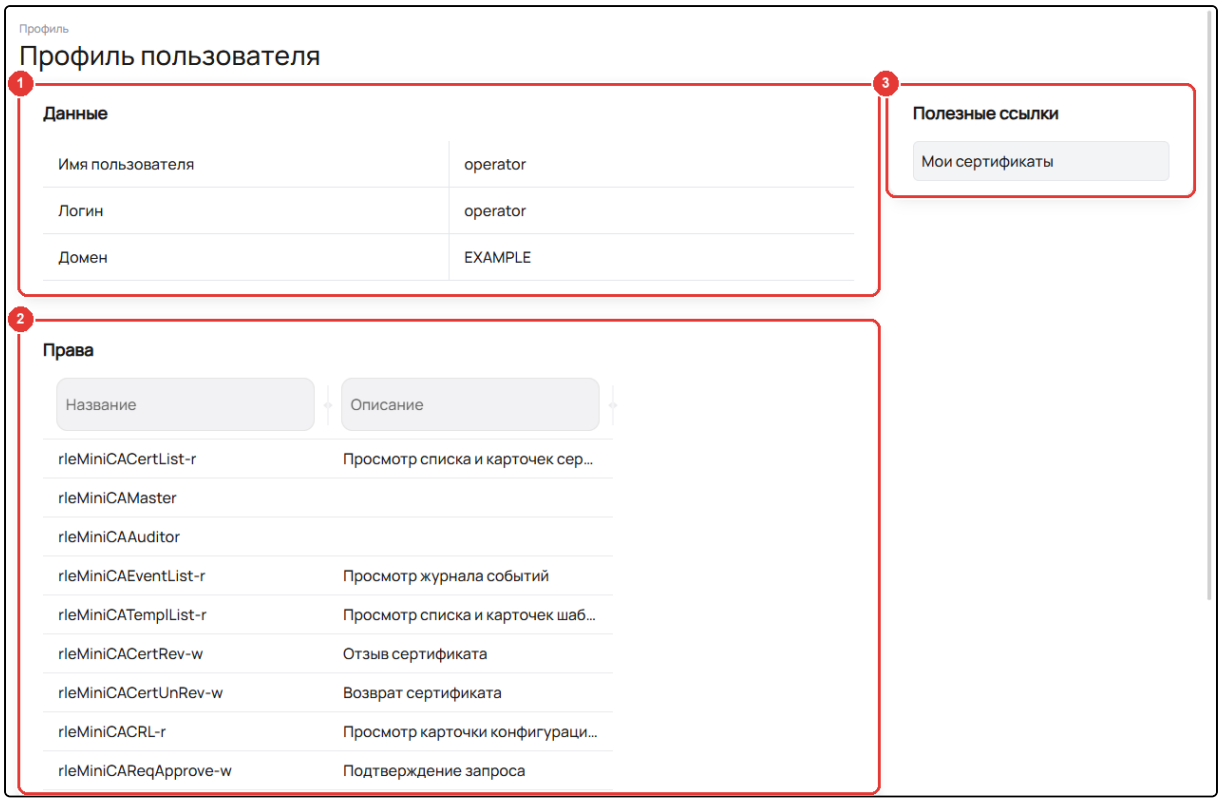
3.2.4 Текущий ЦС

Контрольная панель может работать с несколькими экземплярами ЦС. Данные большинства страниц и выполняемые операции относятся к ЦС, выбранному на странице «Настройки → Конфигурация» в карточке «Выбор Clearway CA» (см. «Конфигурация»). Выбор хранится в браузере пользователя: он действует во всех вкладках этого браузера и не меняет выбор других пользователей. Перед работой убедитесь, что выбран нужный ЦС.

3.3 Профиль и права доступа

Набор доступных операций определяется назначенными правами (см. «Ролевая модель и разграничение полномочий»). Свои учётные данные и права пользователь проверяет на экране профиля.

1. Разверните левое меню, щёлкните своё имя и выберите «Профиль».
2. В блоке «Данные» проверьте имя пользователя, логин и домен.
3. В блоке «Права» просмотрите назначенные роли и права. Назначение прав и маркеров ролей приведено в разделе «Ролевая модель и разграничение полномочий». Поиска и сортировки в таблице нет.
4. Чтобы открыть реестр своих сертификатов, в блоке «Полезные ссылки» нажмите «Мои сертификаты». Откроется реестр «Сертификаты» с фильтром «Принадлежность: Мои».



3 Экран «Профиль пользователя»: блоки «Данные», «Права» и «Полезные ссылки»

На рисунке: **1** блок «Данные»; **2** блок «Права»; **3** блок «Полезные ссылки».

Если нужной кнопки или пункта меню нет либо пункт меню «Действия» бледный и не срабатывает, пользователю не назначено соответствующее право. Групповые кнопки реестров неактивны, пока не отмечены подходящие строки; с правами это не связано. Состав прав меняет только администратор.

3.4 Ролевая модель и разграничение полномочий

Доступ к функциям Clearway CA ограничивается ролевой моделью. Каждая операция требует отдельного права: право с суффиксом -r разрешает просмотр данных определённого типа, право с суффиксом -w разрешает их изменение. Набор прав пользователя определяется его ролью.

Как система определяет права:

- При входе в Контрольную панель сервис аутентификации проверяет доменную учётную запись и выдаёт токен JWT. В токене передаётся перечень прав пользователя.
- Контрольная панель и центр сертификации проверяют этот токен при каждом обращении. Интерфейс показывает только разделы и кнопки, на которые у пользователя есть права, а запрос на операцию без нужного права отклоняется сервером, даже если он отправлен в обход интерфейса.
- Программные клиенты центра сертификации (утилита mclient и сервисы Clearway CA) также обращаются к нему с токеном JWT. Роль, записанная в таком токене, определяет, какие функции API клиенту разрешены: например, клиент с ролью crluser может только формировать и получать списки отзыва. Токены для клиентов выпускает администратор.

Права пользователей:

Право	**Что разрешает**
`rleMiniCACertList-r`	Реестр и карточки сертификатов, конструктор CSR-запросов; список отозванных сертификатов на странице «Информация о CRL и Delta CRL»
`rleMiniCATemplList-r`	Реестр и карточки шаблонов, экспорт шаблонов
`rleMiniCAReqList-r`	Реестр и карточки запросов на выпуск
`rleMiniCAEventList-r`	Журнал событий, вкладка «События» в карточке сертификата
`rleMiniCACRL-r`	Сведения о CRL и Delta CRL, скачивание списков отзыва
`rleMiniCAConfig-r`	Страницы «Конфигурация» и «Статистика ЦС», скачивание цепочки сертификатов
`rleMiniCACertReq-w`	Запрос сертификата (одиночный и пакетный), выпуск из конструктора; типовые задачи замены сертификата
`rleMiniCACertRev-w`	Отзыв сертификатов

`rleMiniCACertUnRev-w`	Восстановление сертификатов, приостановленных с причиной CertificateHold
`rleMiniCATempl-w`	Создание, изменение, копирование, удаление и импорт шаблонов
`rleMiniCACRL-w`	Обновление CRL; раздел меню «Задачи»: списки и карточки задач публикации, запуск задач вне расписания
`rleMiniCAConfig-w`	Добавление ЦС и изменение подключения к ЦС; добавление, изменение и удаление задач публикации и заданий резервного копирования
`rleMiniCAReqApprove-w`	Одобрение и отклонение запросов на выпуск
`rleMiniCABackup-r`	Раздел «Резервное копирование»: задания, ход операций, список копий
`rleMiniCABackup-w`	Запуск резервного копирования вне расписания
`rleMiniCABackupRestore-w`	Восстановление ЦС из резервной копии
`rleMiniCARotation-w`	Ротация ключей ЦС: просмотр действующего сертификата ЦС, формирование CSR ЦС и замена сертификата ЦС (отдельного права на просмотр нет)

Без нужного права кнопка скрыта. Исключение составляет меню «Действия» на страницах «Информация о CRL и Delta CRL» и «Настройки → Конфигурация»: действие без права остаётся в меню бледным и не выполняется.

В поставке три стандартные роли, каждой соответствует группа каталога: администратор ЦС (`CWCA_Administrator`) получает все 17 прав; аудитор (`CWCA_Auditor`) получает 6 прав на просмотр сертификатов, шаблонов, запросов, журнала событий, списков отзыва и конфигурации; пользователь (`CWCA_User`) получает 3 права: просмотр сертификатов и шаблонов и создание запросов на выпуск. Если администратор назначил учётной записи маркеры ролей `rleMiniCAMaster` , `rleMiniCAOperator` или `rleMiniCAAuditor` , они тоже видны в блоке «Права» профиля, но сами по себе прав не дают. Состав ролей и имена групп в конкретной установке может изменить администратор.

Администратор включает учётную запись пользователя в группу каталога (Active Directory или LDAP), а сервис аутентификации сопоставляет каждой группе набор прав согласно своей конфигурации. Чтобы изменить права пользователя, достаточно изменить его членство в группах или сопоставление групп и прав; для программных клиентов состав ролей задаётся в

конфигурации центра сертификации. Порядок настройки и матрица прав приведены в разделе 4 «Описание ролевой модели» Руководства администратора.

Права передаются в токене, который выдаётся при входе. Если администратор изменил ваши права, выйдите из Контрольной панели и войдите снова, чтобы они вступили в силу.

4 Общие элементы интерфейса

В главе описаны элементы, которые одинаково работают на разных страницах. В разделах конкретных страниц указаны только их особенности: столбцы, фильтры и кнопки.

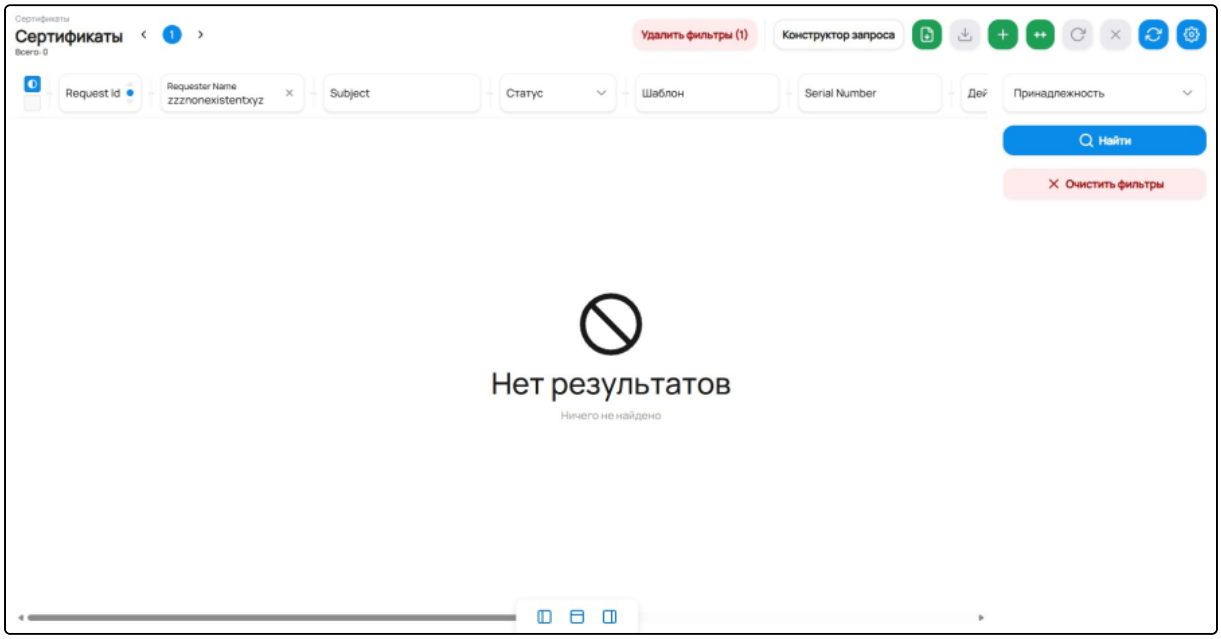
4.1 Страница-реестр

Реестрами называются страницы со списком записей в виде таблицы: «Сертификаты», «Шаблоны», «Запросы», «События», «Публикация сертификатов», «Публикация CRL и Delta CRL», «Резервное копирование». Такие же таблицы встроены в другие страницы, например список отозванных сертификатов на странице «Информация о CRL и Delta CRL» и вкладка «События» карточки сертификата. У встроенных таблиц нет хлебных крошек и нижней панели.

Элемент	**Назначение**
Хлебные крошки и название	Путь к странице и название реестра
Постраничная навигация	Справа от названия, см. «Постраничная навигация»
Всего: N. Выбрано: M	Под названием: число записей, удовлетворяющих условиям отбора, и число отмеченных строк
Кнопки реестра	Набор зависит от страницы и описан в её разделе
Удалить фильтры (N)	Появляется, если задано хотя бы одно условие отбора, см. «Сброс условий отбора»
Обновить (значок круговых стрелок)	Повторно загружает данные с текущими условиями отбора и открывает первую страницу
Параметры таблицы (значок шестерёнки)	Открывает окно «Настройки таблицы»
Поля над столбцами	Фильтры по значениям столбцов
Переключатель в заголовке столбца	Сортировка
Боковая панель	Дополнительные фильтры (только в реестрах «Сертификаты» и «Запросы»)
Нижняя панель	Скрытие меню, заголовка и боковой панели

Щелчок по строке открывает карточку записи в реестрах, где есть карточки; в реестре «Шаблоны» карточка открывается щелчком по названию шаблона. Если в строке выделен текст, карточка не открывается: так можно скопировать значение из таблицы.

Если ни одна запись не подходит под условия, вместо таблицы выводится сообщение «Нет результатов» с пояснением «Ничего не найдено», а счётчик показывает «Всего: 0». Измените или сбросьте условия.



4 Сообщение «Нет результатов»

Номер страницы, условия отбора и сортировка сохраняются в адресной строке браузера. Ссылку на реестр с условиями можно добавить в закладки, а кнопка браузера «Назад» возвращает предыдущее состояние реестра.

4.2 Постраничная навигация

- На странице выводится 50 записей.
- Кнопки ‹ и › открывают предыдущую и следующую страницу, а номер открывает нужную страницу. Всегда видны первая и последняя страницы и страницы рядом с текущей; пропущенные номера заменены многоточием.
- После изменения условий отбора реестр открывается с первой страницы.

4.3 Сортировка

В заголовке столбца, по которому возможна сортировка, есть переключатель из трёх элементов:

Элемент	Порядок

▲ (верхний треугольник)	По возрастанию
● (кружок)	Без сортировки, порядок по умолчанию
▼ (нижний треугольник)	По убыванию

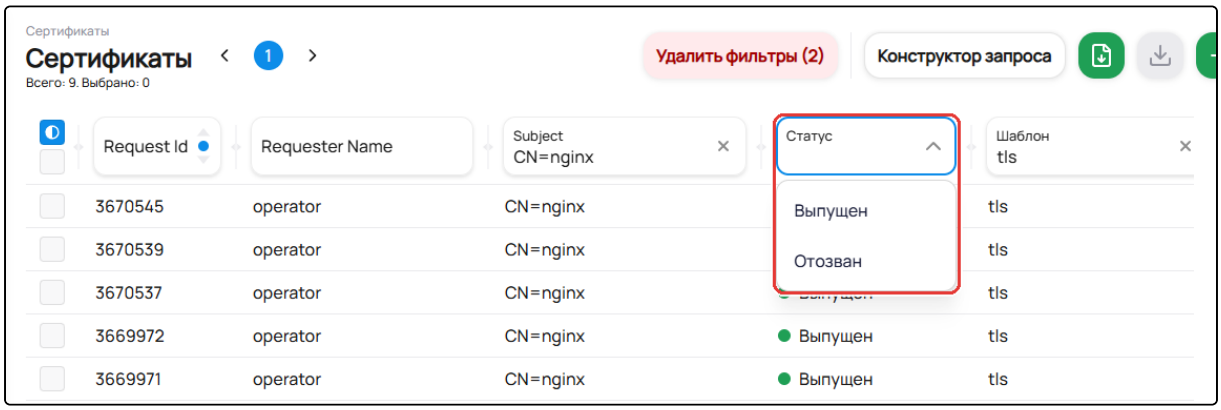
Выбранный элемент выделен цветом. Сортировка действует только по одному столбцу: при выборе порядка в другом столбце прежняя отменяется. Кнопка **Удалить фильтры (N)** также сбрасывает сортировку. По каким столбцам можно сортировать, указано в разделах реестров.

4.4 Фильтры в заголовках столбцов

Над столбцом расположено поле фильтра с названием столбца. Вид поля зависит от данных столбца:

Вид поля	**Как задать условие**	**Когда применяется**
Текстовое	Введите значение	После нажатия Enter или при переходе из поля
Числовое (например, Request Id)	Введите число	После нажатия Enter или при переходе из поля
Список (со стрелкой, например «Статус»)	Выберите значение	Сразу после выбора
Период (даты, например «Действителен с»)	Выберите в календаре дату начала и дату окончания или введите период в формате дд.мм.гггг - дд.мм.гггг	Сразу после выбора периода

- Условия по нескольким столбцам объединяются: в таблице остаются записи, удовлетворяющие всем условиям.
- Чтобы снять условие одного столбца, нажмите × в поле фильтра или очистите поле.
- Серое неактивное поле означает, что отбор по этому столбцу не предусмотрен.
- В календаре периода после выбора первого дня становятся доступны кнопки **Не указывать начало** (период без начальной даты) и **Не указывать конец** (период без конечной даты).
- Способ сравнения текста задан отдельно для каждого столбца: в одних столбцах ищется часть значения, в других ищется полное значение; регистр букв может учитываться. Особенности указаны в разделах реестров.



5 Фильтр-список в заголовке столбца «Статус»

4.5 Боковая панель фильтров

В реестрах «Сертификаты» и «Запросы» справа от таблицы расположена боковая панель:

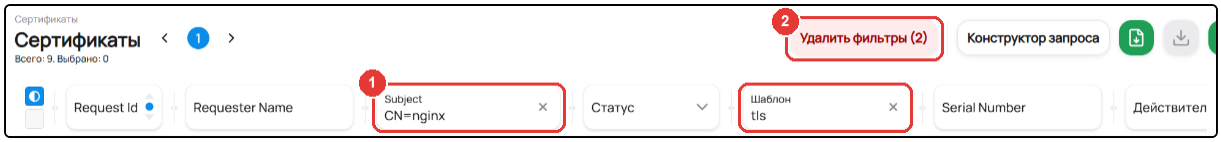
Элемент	Что делает
Принадлежность	Список: «Мои» (только записи, запрошенные текущим пользователем); «Все» (все записи). Применяется сразу после выбора
Найти	Применяет все условия отбора: на панели и в полях над столбцами, включая ещё не применённые изменения
Очистить фильтры	Снимает все условия отбора на панели и в полях над столбцами. Сортировка сохраняется

Панель скрывается и возвращается кнопкой **Скрыть/показать боковые фильтры** на нижней панели.

4.6 Сброс условий отбора

Способ	Что сбрасывается
× в поле фильтра	Условие одного столбца
Очистить фильтры (боковая панель)	Все условия отбора; сортировка сохраняется

Удалить фильтры (N) (заголовок реестра)	Все условия отбора и сортировка. N означает число заданных условий; кнопка видна, только если задано хотя бы одно условие



6 Заданные условия и кнопка «Удалить фильтры (2)»

На рисунке: **1** поля фильтров с заданными условиями; **2** кнопка «Удалить фильтры (N)», где N означает число условий.

4.7 Выделение строк и групповые действия

В реестрах с групповыми действиями («Сертификаты», «Запросы», список отозванных сертификатов на странице «Информация о CRL и Delta CRL») первый столбец содержит флажки.

Элемент	Что делает
Флажок в строке	Отмечает строку или снимает отметку
Нижний флажок в заголовке столбца	Отмечает все строки текущей страницы или снимает отметки. Если отмечена часть строк, во флажке виден знак «–»
Верхний флажок «Инвертировать выделение»	Меняет отметки на текущей странице на противоположные

- Счётчик «Выбрано» учитывает отмеченные строки на всех страницах: отметки сохраняются при переходе между страницами.
- Групповая кнопка становится активной, когда среди отмеченных есть подходящие записи, и обрабатывает только их. Например, отзыв пропускает уже отозванные сертификаты, а одобрение пропускает запросы не в статусе Pending.
- Групповое действие подтверждается в окне, где указано число обрабатываемых записей («Всего: N») и их список. По итогам выводится уведомление с числом обработанных записей.
- После выполнения группового действия отметки снимаются.

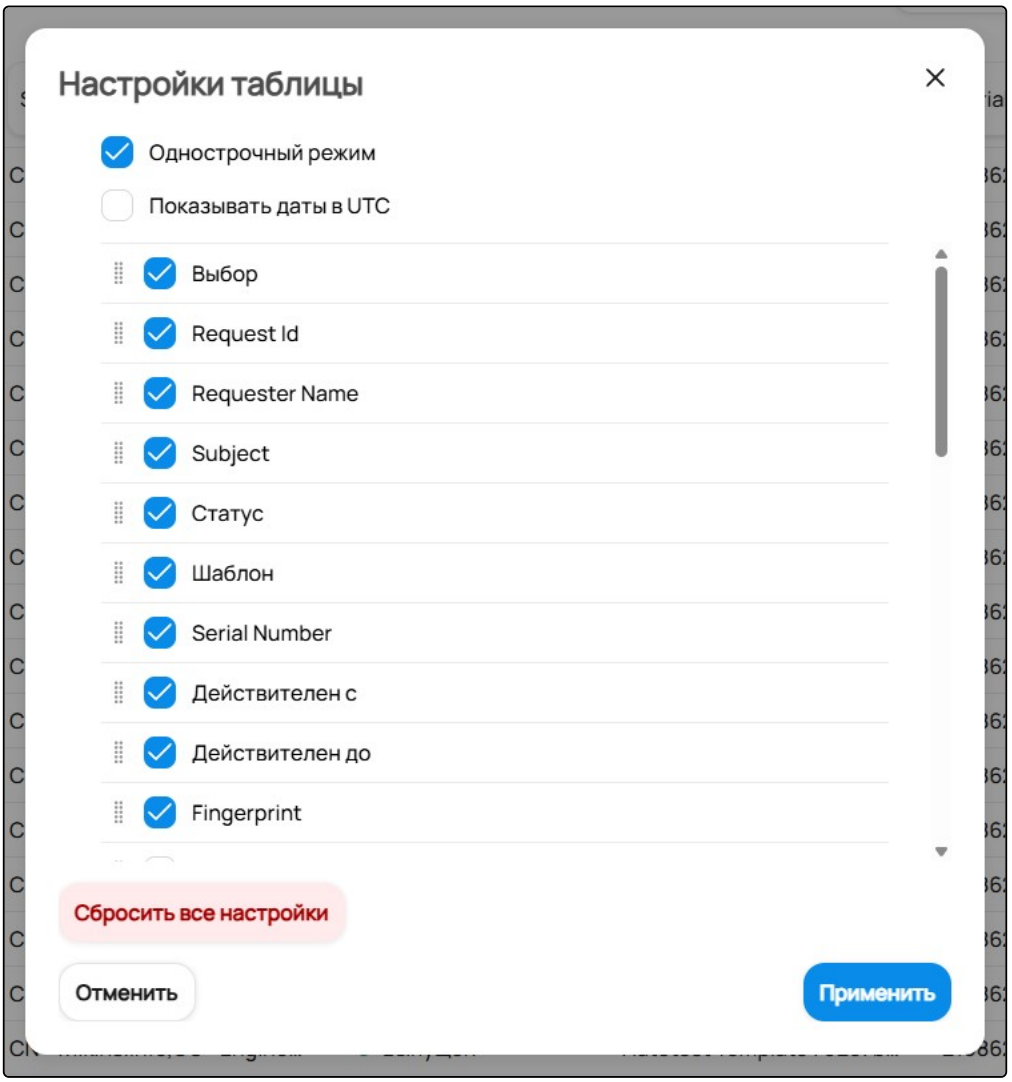
4.8 Настройка таблицы

Нажмите **Параметры таблицы** (значок шестерёнки). Откроется окно «Настройки таблицы».

Элемент	Что делает
Однострочный режим	Выводит содержимое ячеек в одну строку, длинные значения обрезаются. Включён по умолчанию
Показывать даты в UTC	Показывает дату и время в UTC вместо часового пояса компьютера. Удобно при сверке событий между площадками
Список столбцов	Флажок включает показ столбца в таблице. Порядок меняется перетаскиванием за значок слева от названия. Здесь же включаются столбцы, скрытые по умолчанию
Сбросить все настройки	После подтверждения «Вы действительно хотите сбросить настройки таблицы?» возвращает стандартный состав, порядок и ширину столбцов и закрывает окно
Отменить, ×	Закрывают окно без изменений
Применить	Применяет и сохраняет настройки

Ширину столбца меняют перетаскиванием разделителя у правого края заголовка; двойной щелчок по разделителю подбирает ширину по содержимому.

Настройки таблицы и ширина столбцов сохраняются в браузере отдельно для каждого реестра. На другом компьютере или в другом браузере таблица откроется в стандартном виде.



7 Окно «Настройки таблицы»

4.9 Выгрузка отчёта в файл

В реестрах «Сертификаты», «Шаблоны», «Запросы», «События» и на вкладке «События» карточки сертификата есть зелёная кнопка со значком файла для выгрузки отчёта в файл Excel. При наведении на неё выводится подсказка «Файл с отчётом формируется по применённым фильтрам. Ограничение по количеству записей - 10000.»

1. Задайте условия отбора и при необходимости сортировку.
2. Нажмите кнопку выгрузки. Браузер сохранит файл.

- В файл попадают все записи, удовлетворяющие условиям отбора, со всех страниц реестра. Порядок записей соответствует текущей сортировке.
- В файл выгружается не более 10 000 записей. Если записей больше, сузьте выборку фильтрами, например по периоду дат.

- Состав столбцов файла не зависит от настроек таблицы.

4.10 Меню «Действия» и закрепление действий

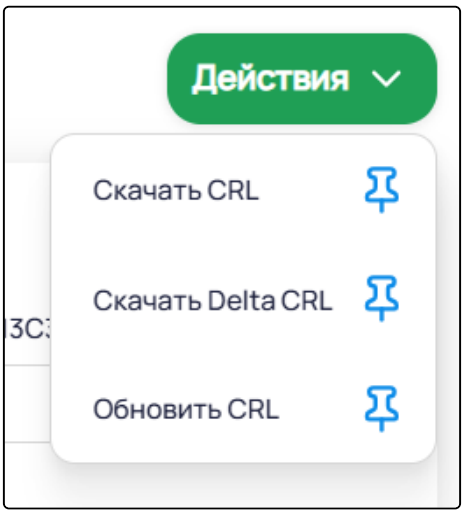
На страницах «Информация о CRL и Delta CRL» и «Настройки → Конфигурация» операции собраны в меню **Действия** (кнопка в правом верхнем углу). Действие, на которое у пользователя нет права, отображается в меню бледным и не выполняется.

Часто используемое действие можно закрепить: оно появится отдельной кнопкой-значком слева от «Действия», а его название будет показываться в подсказке при наведении.

1. Откройте меню «Действия».
2. Нажмите значок булавки справа от действия.

Чтобы открепить действие, откройте меню и нажмите значок перечёркнутой булавки .

Закрепление сохраняется в браузере. Действия, закреплённые по умолчанию, указаны в разделах страниц.



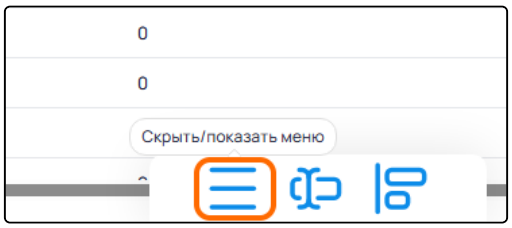
8 Меню «Действия» со значками закрепления

4.11 Нижняя панель

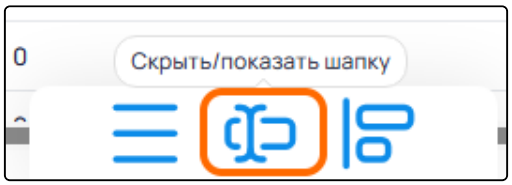
На страницах-реестрах внизу по центру экрана расположена панель из трёх кнопок. Название кнопки показывается при наведении.

Кнопка	Что делает
Скрыть/показать меню	Скрывает левое меню целиком или возвращает его

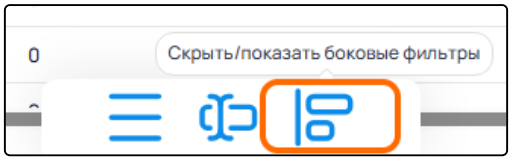
Скрыть/показать шапку	Сворачивает заголовок реестра (крошки, название, навигацию, кнопки, счётчик) в узкую полосу или разворачивает его; таблице достаётся больше места
Скрыть/показать боковые фильтры	Скрывает или показывает боковую панель фильтров. В реестрах без боковой панели кнопка неактивна



9 Кнопка «Скрыть/показать меню»



10 Кнопка «Скрыть/показать шапку»



11 Кнопка «Скрыть/показать боковые фильтры»

Значок скрытого элемента становится бледным. Выбранное состояние сохраняется при переходе между страницами до обновления страницы в браузере. На карточках и других страницах без таблицы нижней панели нет.

4.12 Окна, формы и уведомления

- Обязательные поля форм отмечены звёздочкой «*». Подсказка к полю открывается по значку «?» рядом с его названием. Если обязательное поле не заполнено, под ним выводится «Обязательно к заполнению», и форма не отправляется.
- Файл в поле загрузки перетащите в область поля или щёлкните её и выберите файл. Принимается один файл размером до 30 МБ. После выбора выводится «Файл добавлен» и имя файла; чтобы выбрать другой файл, удалите текущий крестиком.
- Перед операциями, которые нельзя отменить, запрашивается подтверждение. Окно «Подтверждение» с вопросом содержит кнопки **Нет** и **Да**; окно с названием операции содержит кнопки **Отменить** и **Подтвердить**. Крестик в заголовке окна закрывает его без выполнения операции.

- Результаты операций и ошибки выводятся всплывающими уведомлениями. Уведомление об успешной операции закрывается само через несколько секунд. Уведомление об ошибке остаётся на экране, пока его не закроют крестиком; если сервер передал подробности, в нём есть кнопки **Копировать** (копирует текст ошибки) и **Подробнее** (открывает окно «Детали ошибки»). Скопированный текст ошибки передайте администратору.

Типовые сообщения об ошибках:

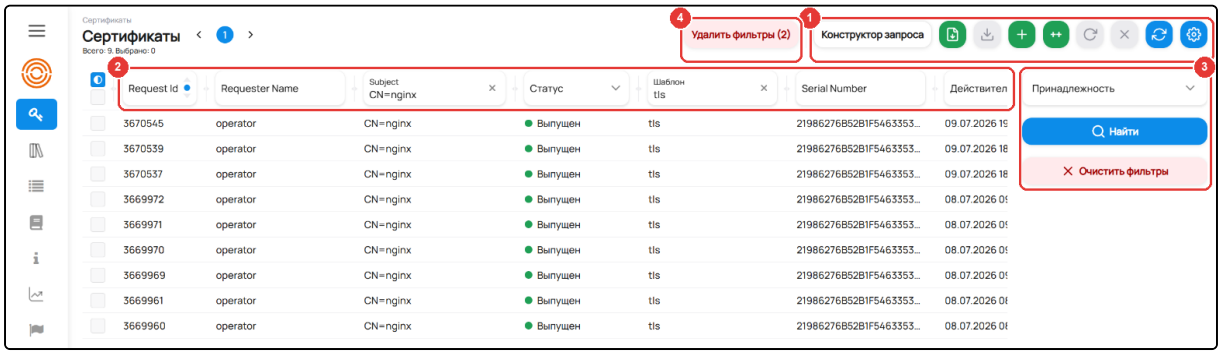
Сообщение	**Причина**
Нет доступа к данному ресурсу	Сервер отклонил запрос: у пользователя нет нужного права
Ресурс не найден	Запрошенный объект не найден; в пояснении указан адрес запроса
Не удалось подключиться к серверу авторизации	Служба аутентификации недоступна
Произошла ошибка	Прочие ошибки, если сервер не передал собственное описание

5 Сертификаты

5.1 Реестр сертификатов

Раздел «Сертификаты» содержит реестр всех сертификатов, выпущенных центром сертификации, включая отозванные. Для работы с разделом нужно право `rleMiniCACertList-r`. В реестре можно найти сертификат и открыть его карточку, скачать сертификаты, запросить выпуск новых, отозвать и восстановить сертификаты, выгрузить отчёт.

Общие приёмы работы с реестром (фильтры, сортировка, постраничная навигация, выделение строк, настройка таблицы, выгрузка отчёта) описаны в главе «Общие элементы интерфейса». Ниже приведены только особенности реестра сертификатов.



12 Реестр «Сертификаты»

На рисунке: **1** кнопки реестра (см. «Кнопки реестра»); **2** фильтры в заголовках столбцов; **3** боковая панель фильтров; **4** кнопка «Удалить фильтры (N)».

Чтобы открыть карточку сертификата, щёлкните его строку.

5.1.1 Кнопки реестра



13 Кнопки над таблицей реестра сертификатов

№	Кнопка (значок)	Что делает	Условие
1	**Конструктор запроса**	Открывает конструктор CSR-запросов (см. «Конструктор CSR-запросов»)	Нет

2	Выгрузка отчёта (зелёный значок файла)	Выгружает отчёт в файл Excel (см. «Выгрузка отчёта в файл»)	Нет
3	**Скачать сертификаты** (значок загрузки)	Открывает меню PEM / DER и скачивает отмеченные сертификаты в выбранном формате	Активна, если отмечена хотя бы одна строка
4	**Запрос сертификата** («+»)	Открывает окно «Запрос сертификата»	Видна при праве `rleMiniCACertReq-w`
5	**Пакетный запрос сертификатов** («++»)	Открывает окно «Запрос сертификатов»	Видна при праве `rleMiniCACertReq-w`
6	**Восстановить выбранные сертификаты** (круговая стрелка)	Открывает окно «Восстановление сертификатов»	Видна при праве `rleMiniCACertUnRev-w`; активна, если среди отмеченных есть сертификат, отозванный с причиной CertificateHold
7	**Отозвать выбранные сертификаты** (крестик)	Открывает окно «Отзыв сертификатов»	Видна при праве `rleMiniCACertRev-w`; активна, если среди отмеченных есть неотозванный сертификат

5.1.2 Столбцы и фильтры

Столбец	Что показывает	Фильтр	По умолчанию
Request Id	Номер запроса на выпуск; по нему сертификат связан с запросом в разделе «Запросы». Сортировка	Число	Показан
Requester Name	Учётная запись, от имени которой запрошен сертификат	Текст	Показан
Subject	Имя владельца сертификата (DN целиком), например CN=host.example.local,O=Example	Текст	Показан

Статус	«Выпущен» (зелёная метка) или «Отозван» (красная)	Список	Показан
Шаблон	Шаблон, по которому выпущен сертификат. Фильтр находит только полное название шаблона, регистр букв не важен	Текст	Показан
Serial Number	Серийный номер, который ЦС присвоил сертификату; по нему сертификат указывается в CRL	Текст	Показан
Действителен с, Действителен до	Срок действия. Сортировка	Период	Показаны
Fingerprint	Отпечаток сертификата	Текст	Показан
Отпечаток ключа шифрования	Заполняется, если ЦС хранит закрытый ключ сертификата в зашифрованном виде (KRA)	Нет	Показан
Скачать	Значок для скачивания сертификата в формате PEM; карточка при нажатии не открывается	Нет	Показан
Тип ключа, Размер ключа	Алгоритм и длина ключа	Нет	Скрыты
Common Name	Значение атрибута CN из Subject	Текст	Скрыт
Subject Key Identifier, Authority Key Identifier	Идентификаторы ключа владельца и ключа ЦС	Нет	Скрыты
Key Usage, Extended Key Usage	Разрешённые назначения сертификата	Нет	Скрыты
SAN DNS, SAN IP, SAN URI, SAN Email, SAN Other Name	Альтернативные имена владельца	Нет	Скрыты
Authority Information Access, CRL Distribution Point	Адреса службы OCSP и сертификата ЦС, адрес CRL	Нет	Скрыты
Выпущен, Обновлено	Дата выпуска и дата последнего изменения записи. Сортировка	Нет	Скрыты

Причина отзыва	Причина отзыва у отозванных сертификатов	Нет	Скрыт
Basic Constraints	Расширение Basic Constraints	Нет	Скрыт
В CRL	Сведения о включении сертификата в CRL	Нет	Скрыт

Чтобы найти сертификаты с истёкшим сроком действия, задайте период в фильтре «Действителен до».

Значение «Мои» фильтра «Принадлежность» на боковой панели отбирает сертификаты, у которых в столбце Requester Name указан текущий пользователь.

5.2 Выпуск сертификата

Выпуск сертификата означает подписание запроса (CSR) закрытым ключом центра сертификации. В результате владелец получает сертификат X.509, который подтверждает, что открытый ключ принадлежит указанному владельцу.

Выпустить сертификат можно тремя способами:

- в окне «Запрос сертификата» по готовому CSR;
- в окне «Запрос сертификатов» (пакетный запрос) по списку Subject из файла;
- в конструкторе CSR-запросов с подготовкой CSR или созданием ключа на носителе (см. «Конструктор CSR-запросов»).

Если в шаблоне включён признак «Создавать запрос на выпуск», сертификат выпускается только после одобрения запроса в разделе «Запросы» (см. «Запросы и согласование выпуска»).

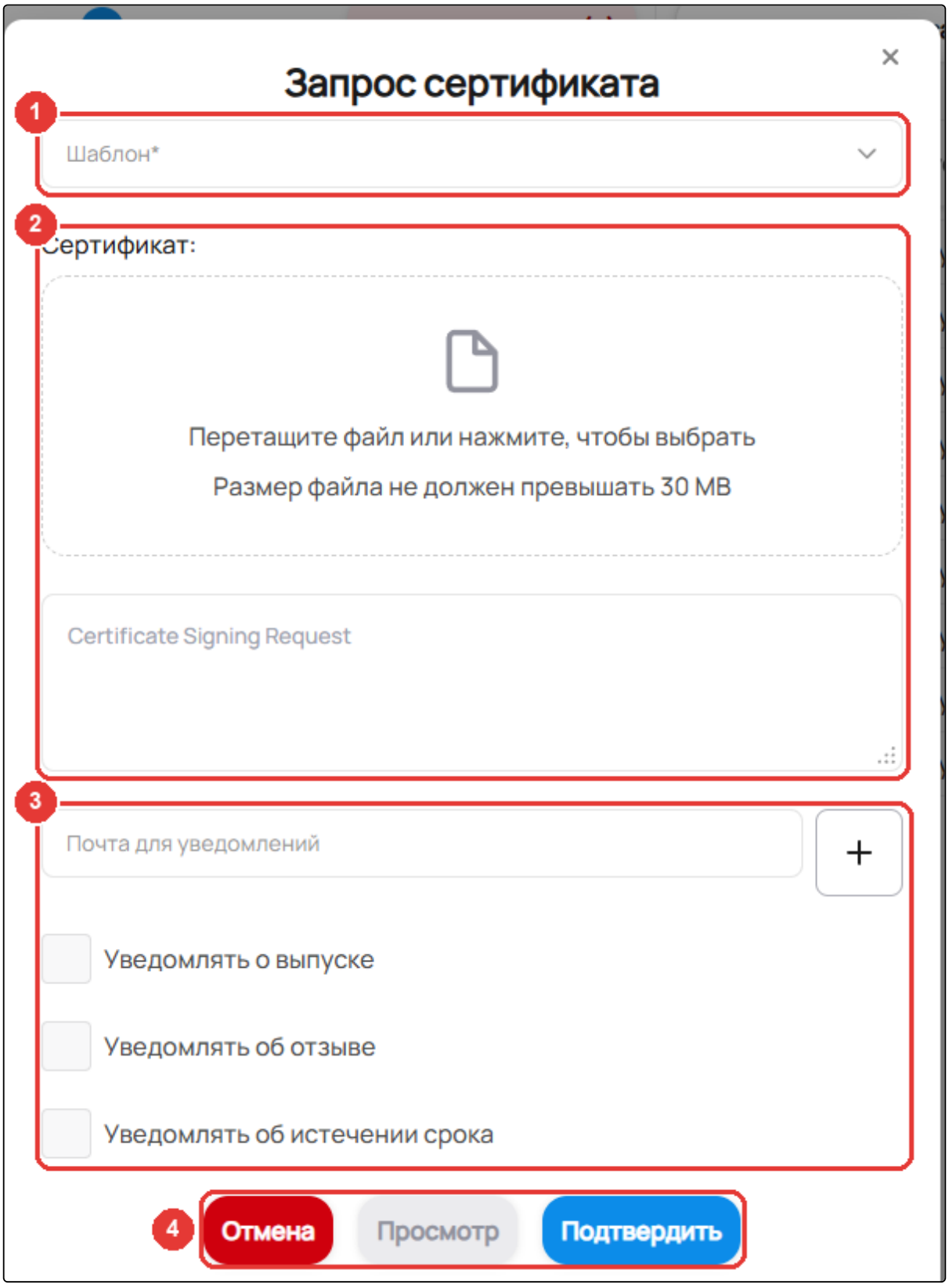
> **Важно**
>
> Если шаблон не сохраняет закрытый ключ, ЦС ключ не получает и восстановить его не может. Храните ключ в надёжном месте: без него выпущенным сертификатом пользоваться нельзя. Исключение составляют шаблоны с признаком «Сохранять приватный ключ, зашифрованный сертификатом KRA»: для них файл закрытого ключа загружается вместе с запросом, и ЦС хранит ключ в зашифрованном виде (см. «Хранение и восстановление закрытых ключей (KRA)»).

5.2.1 Запрос сертификата

Для запроса нужно право `rleMiniCACertReq-w`.

1. В реестре сертификатов нажмите **Запрос сертификата** («+»).
2. Выберите шаблон.

3. В блоке «Сертификат:» загрузите файл CSR либо вставьте текст запроса в поле «Certificate Signing Request». Способы взаимоисключающие: после выбора файла поле текста скрывается, и наоборот.
4. Если шаблон сохраняет закрытый ключ, загрузите файл ключа в поле «Приватный ключ:».
5. При необходимости укажите адреса и события для уведомлений.
6. Чтобы проверить содержимое запроса, нажмите **Просмотр**.
7. Нажмите **Подтвердить**.



14 Окно «Запрос сертификата»

На рисунке: **1** шаблон; **2** блок «Сертификат:» (файл CSR или текст запроса); **3** адреса и события уведомлений; **4** кнопки «Отмена», «Просмотр», «Подтвердить».

Поле	Что указать
Шаблон*	Шаблон, по которому выпускается сертификат. Шаблоны, в названии которых есть «auto_», в списке не показываются
Сертификат:	Файл CSR или текст CSR в поле «Certificate Signing Request»
Приватный ключ:	Файл закрытого ключа. Поле есть только у шаблонов с признаком «Сохранять приватный ключ, зашифрованный сертификатом KRA»
Почта для уведомлений	Адрес электронной почты; кнопка «+» добавляет его в список, лишний адрес удаляется крестиком
Уведомлять о выпуске, Уведомлять об отзыве, Уведомлять об истечении срока	События, о которых нужно сообщать на указанные адреса

Для шаблонов с признаком «Создавать запрос на выпуск» блока уведомлений нет. Адреса и флажки уведомлений запоминаются в браузере и подставляются при следующем запросе.

Кнопка	Что делает
Отмена	Закрывает окно без отправки
Просмотр	Показывает структуру запроса (см. «Просмотр структуры запроса»). Доступна, когда загружен файл или введён текст CSR
Подтвердить	Проверяет запрос по шаблону и отправляет его в ЦС. Пока запрос отправляется, окно нельзя закрыть

Результат:

Ситуация	Что происходит
Запрос нарушает ограничения шаблона	Открывается окно «Ошибки» со списком нарушений (см. «Ограничения для Subject и SAN»), сертификат не выпускается. Исправьте CSR по ограничениям шаблона и отправьте запрос заново

Шаблон выпускает сертификат сразу	Сообщение «Сертификат выпущен», окно закрывается, сертификат появляется в реестре
У шаблона включено «Создавать запрос на выпуск»	Сообщение «Заявка на сертификат создана». Запрос ждёт одобрения в разделе «Запросы»
У шаблона включено «Не добавлять сгенерированный сертификат в базу данных»	Сообщение «Сертификат выпущен», браузер сразу сохраняет файл <серийный номер>.crt в формате PEM. В реестр сертификат не попадает, поэтому сохраните этот файл
Ошибка на стороне ЦС	Сообщение с текстом ошибки, окно остаётся открытым

Если поля не заполнены, выводятся сообщения «Не выбран шаблон!», «Не выбран CSR!» или «Не выбран приватный ключ!»; при неверном адресе почты выводится «Неверный формат email».

5.2.2 Просмотр структуры запроса

Кнопка **Просмотр** в окне «Запрос сертификата» показывает, что содержится в CSR. Если шаблон выбран, рядом выводятся его значения.



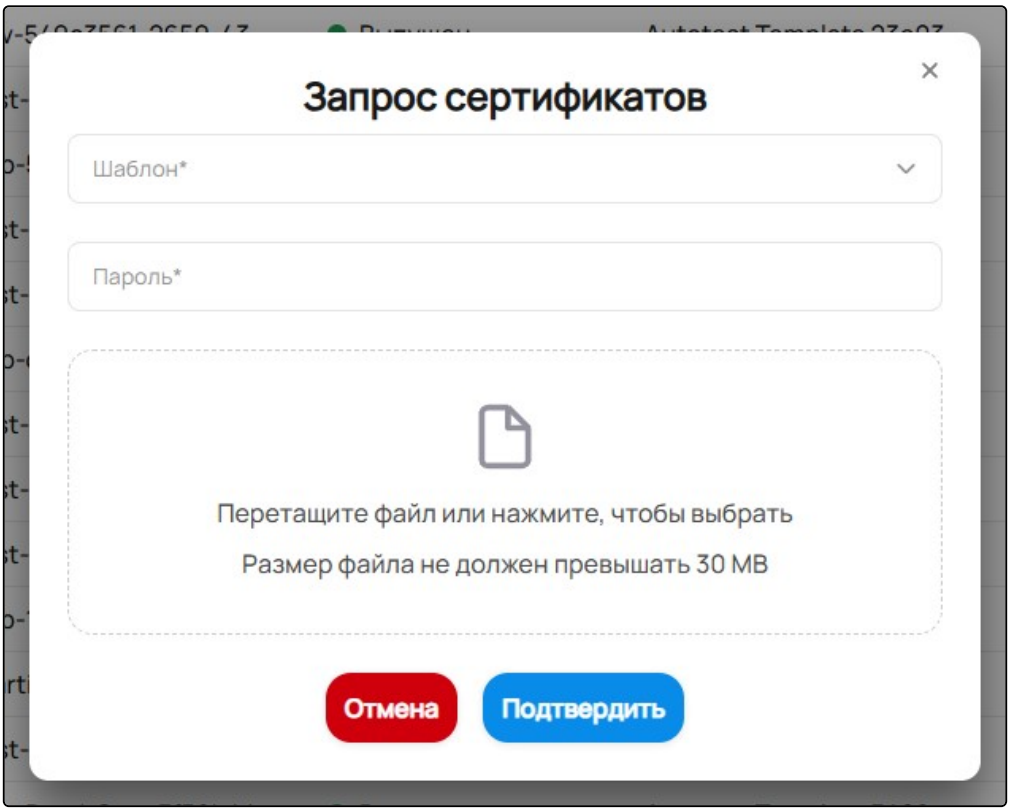
15 Структура запроса и сравнение с шаблоном

В таблице три столбца: «Имя параметра», «Значение в csr» и «Значение в шаблоне». Строки: тип ключа, алгоритм, длина ключа, срок действия в днях (из шаблона), Subject, затем атрибуты и расширения запроса. Красным выделяются расхождения с шаблоном: другой тип ключа, длина ключа меньше заданной в шаблоне, отличающийся набор Extended Key Usage. Окно закрывается крестиком или клавишей Esc.

5.2.3 Пакетный запрос сертификатов

Пакетный запрос выпускает сразу несколько сертификатов по списку Subject из файла. Нужно право `rleMiniCACertReq-w`.

1. В реестре нажмите **Пакетный запрос сертификатов** («++»).
2. Заполните поля и загрузите файл.
3. Нажмите **Подтвердить**.



16 Окно «Запрос сертификатов»

Поле	Что указать
Шаблон*	Шаблон для всех сертификатов пакета
Пароль*	Пароль, который передаётся в ЦС вместе с пакетным запросом
Файл*	Текстовый файл со списком Subject

Формат файла: одна строка соответствует одному сертификату, строки заголовка нет; атрибуты Subject разделяются точкой с запятой; пустые строки пропускаются. Например, для строки

`CN=host1.example.local;O=Example` будет запрошен Subject `CN=host1.example.local,O=Example`.

После выпуска появится сообщение «Сертификаты выпущены успешно», и браузер сохранит файл с результатом, сформированный ЦС. При ошибке появится сообщение «Не удалось выпустить сертификаты».

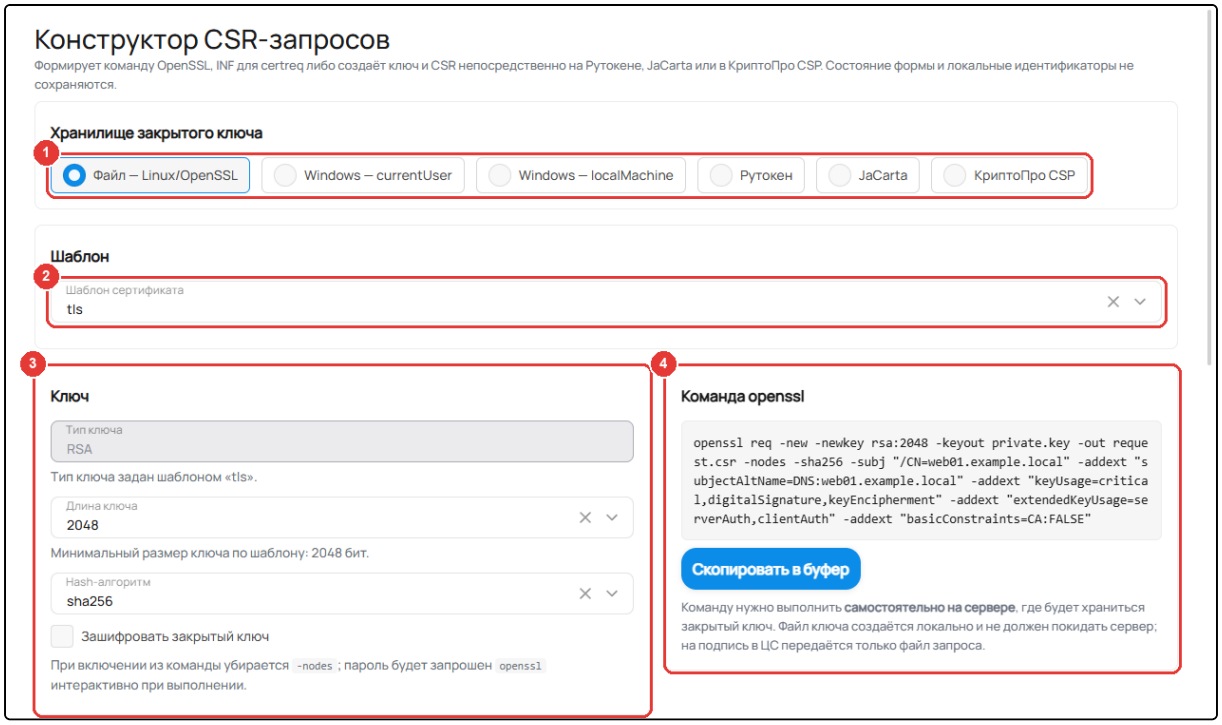
5.3 Конструктор CSR-запросов

Конструктор помогает подготовить запрос на сертификат по выбранному шаблону. В зависимости от выбранного хранилища закрытого ключа он:

- формирует команду openssl для сервера Linux;
- формирует INF-файл и команду certreq для сервера Windows;
- создаёт ключ и CSR прямо на носителе пользователя: Рутокене, JaCarta или в новом контейнере КриптоПро CSP.

Закрытый ключ создаётся на стороне пользователя и в ЦС не передаётся: на подпись уходит только запрос. Конструктор работает в браузере и ничего не сохраняет: после перезагрузки или ухода со страницы все поля и созданный на странице CSR сбрасываются.

Чтобы открыть конструктор, в разделе «Сертификаты» нажмите **Конструктор запроса** над таблицей. Для возврата в реестр нажмите «Сертификаты» в хлебных крошках.



17 Конструктор CSR-запросов: хранилище «Файл — Linux/OpenSSL» и команда openssl

На рисунке: **1** хранилище закрытого ключа; **2** шаблон сертификата; **3** параметры ключа; **4** результат (команда и кнопка «Скопировать в буфер»).

5.3.1 Порядок работы

1. В блоке «Шаблон» выберите шаблон сертификата. Пока шаблон не выбран, остальные блоки не отображаются.
2. В блоке «Хранилище закрытого ключа» выберите, где будет создан ключ.
3. Проверьте блок «Ключ» и при необходимости измените имена файлов.
4. Заполните Subject и (или) SAN: нужно хотя бы одно значение в любом из блоков, а для КриптоПро CSP хотя бы один атрибут Subject.
5. Получите результат в правой карточке: для Linux скопируйте команду openssl; для Windows скачайте или скопируйте INF-файл и скопируйте команду certreq; для Рутокена, JaCarta и КриптоПро CSP создайте CSR на носителе и скопируйте или скачайте его.
6. Для носителей при необходимости выпустите сертификат прямо из конструктора и запишите его на носитель (см. «Выпуск сертификата и запись на носитель»).

Пока в форме есть ошибки, правая карточка показывает список «Запрос не сформирован — исправьте ошибки:», а кнопки результата неактивны. Ошибка по конкретному полю выводится красным текстом под этим полем. Форма пересчитывается сразу после изменения любого поля.

5.3.2 Шаблон и хранилище ключа

В списке «Шаблон сертификата» не показываются шаблоны, в названии которых есть «auto_». Шаблон определяет тип ключа, минимальный размер ключа и значения extendedKeyUsage и keyUsage. В конструкторе их изменить нельзя. Если тип ключа шаблона не поддерживается выбранным хранилищем, выводится «Тип ключа шаблона не поддерживается выбранным хранилищем.». Выберите другое хранилище или другой шаблон.

Хранилище	Где создаётся ключ	Результат в правой карточке	Допустимые ключи
Файл — Linux/ OpenSSL (по умолчанию)	В файле на сервере Linux при выполнении команды	«Команда openssl»	RSA, ECDSA, Ed25519, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Windows — currentUser	В хранилище текущего пользователя Windows	«INF-файл и команда certreq»	RSA, ECDSA, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Windows — localMachine	В хранилище компьютера Windows	«INF-файл и команда certreq»	То же
Рутокен	На подключённом Рутокене	«CSR на Рутокене»	RSA 2048 или ГОСТ Р 34.10-2012 256 бит, в зависимости от возможностей устройства

JaCarta	В логическом слоте JaCarta-2 PKI или ГОСТ	«CSR на JaCarta»	RSA 2048 или ГОСТ Р 34.10-2012 256 бит (набор параметров A)
КриптоПро CSP	В новом контейнере на выбранном считывателе	«CSR в КриптоПро CSP»	ГОСТ Р 34.10-2012, 256 или 512 бит

5.3.3 Параметры запроса

Блок, поле	**Что указать**
Ключ → Тип ключа	Задаётся шаблоном, изменить нельзя
Ключ → Длина ключа (RSA)	1024, 2048 или 4096; в списке только значения не меньше минимума из шаблона. Для Рутокена и JaCarta допускается только 2048
Ключ → Кривая (ECDSA)	P-256, P-384 или P-521
Ключ → Размер ключа (ГОСТ Р 34.10-2012)	256 или 512 бит; для Рутокена и JaCarta допускается только 256
Ключ → Набор параметров (paramset)	Для ключей ГОСТ, кроме КриптоПро CSP
Ключ → Hash-алгоритм	Для RSA и ECDSA: sha256, sha384 или sha512 (для Рутокена и JaCarta допускается только sha256). Для Ed25519 и ГОСТ алгоритм определяется ключом
Ключ → Имя GOST-провайдера	Только для «Файл — Linux/OpenSSL» и ключей ГОСТ: имя провайдера OpenSSL, по умолчанию gostprov
Ключ → Зашифровать закрытый ключ	Только для «Файл — Linux/OpenSSL»: защитить ключ паролем (см. «Шифрование закрытого ключа при подготовке запроса»)
Параметры Windows → Exportable	Только для хранилищ Windows: сделать закрытый ключ экспортируемым
Имена выходных файлов	Имя файла запроса (по умолчанию request.csr), файла ключа (private.key, только Linux) и INF-файла (params.inf, только Windows). Имя не может быть пустым, содержать символы < > : " / \ | ? * и заканчиваться пробелом или точкой

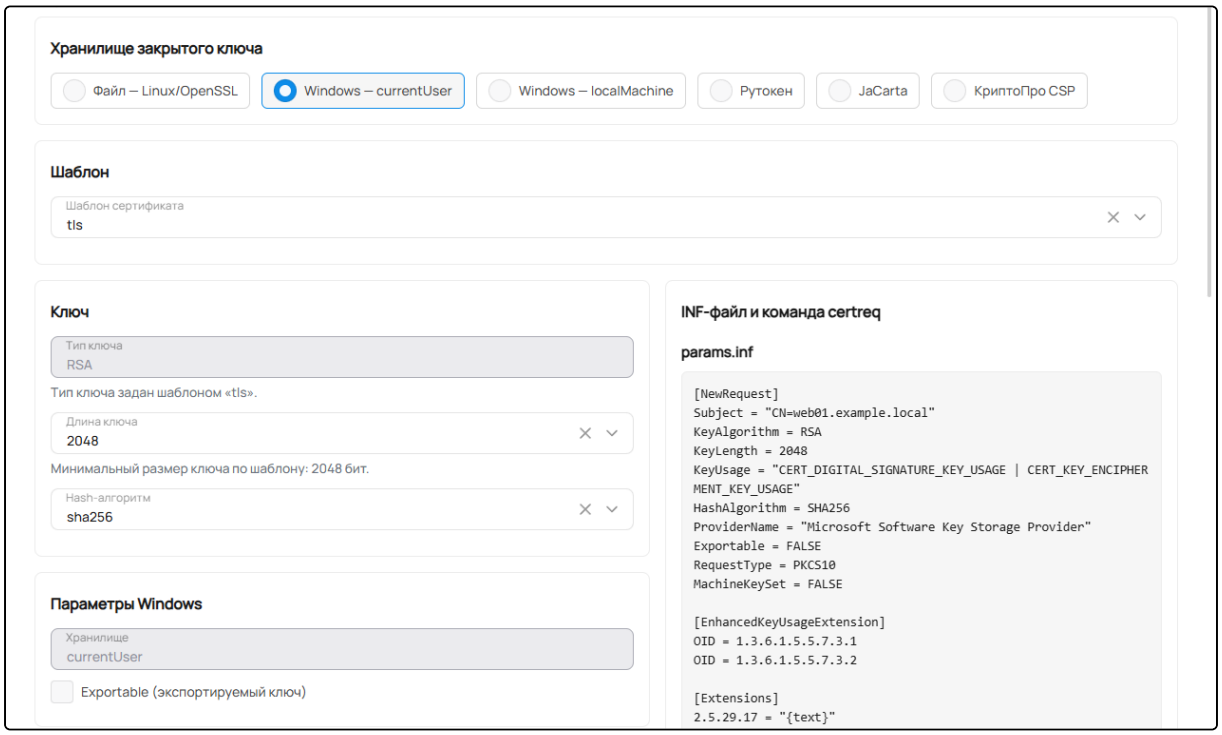
Subject (DN)	Атрибуты владельца: CN, O, OU, C (ровно две латинские буквы, например RU), ST, L, emailAddress. Кнопка **+ Добавить RDN** добавляет строку, крестик удаляет её
Subject Alternative Name (SAN)	Имена DNS (допускается маска *.), IP (IPv4 или IPv6), email и URI (абсолютный адрес со схемой). Кнопка **+ Добавить SAN** добавляет строку. Для носителей значения DNS, email и URI вводятся только латиницей
basicConstraints	Только для «Файл — Linux/OpenSSL»: флажки CA и critical, поле pathlen (при отмеченном CA, целое неотрицательное число)

Один тип атрибута можно добавить несколько раз, например несколько DNS-имён. Строки с пустым значением не учитываются. Блоки extendedKeyUsage и keyUsage показывают значения шаблона без возможности изменения.

5.3.4 Результат для Linux и Windows

Для хранилища «Файл — Linux/OpenSSL» кнопка **Скопировать в буфер** копирует команду openssl. Выполните её на сервере, где будет храниться ключ: она создаст файл ключа и файл запроса. Файл ключа не должен покидать сервер; для выпуска сертификата в ЦС передаётся только файл запроса.

Для хранилищ Windows правая карточка содержит кнопки **Скопировать в буфер** (содержимое INF-файла), **Скачать INF-файл** и **Скопировать команду** (команда вида certreq -new params.inf request.csr). Сохраните INF-файл на сервере Windows и выполните команду в каталоге с ним: ключ будет создан в выбранном хранилище Windows, рядом появится файл запроса.



18 Хранилище «Windows — currentUser»: INF-файл и команда certreq

5.3.5 Создание ключа и CSR на носителе

Ключи на носителях создаются локальными программами производителя, которые работают в браузере пользователя. Поддерживаемая платформа: Windows и браузер на основе Chromium. Требования к рабочему месту и состояние компонентов показывает раздел «Аппаратные токены».

Носитель	Поля	Кнопка создания
Рутокен	«Устройство»: подключённый Рутокен; «Метка ключа*»: имя, под которым ключ будет виден на носителе	**Создать CSR на Рутокене**
JaCarta	«Logical slot JaCarta»: слот с приложением PKI или ГОСТ; «Метка ключа*». Кнопка **Обновить список JaCarta** заново опрашивает носители	**Создать CSR на JaCarta**
КриптоПро CSP	«Логический считыватель CSP»; «Имя нового контейнера» (1–64 символа: буквы, цифры, пробел, «_», «.», «-»). Кнопка **Обновить считыватели** перечитывает список	**Создать контейнер, ключ и CSR**

1. Выберите хранилище и дождитесь окончания проверки компонентов.
2. Заполните поля носителя и остальные блоки формы.
3. Нажмите кнопку создания. Если она неактивна, причины перечислены над ней в списке «Создание CSR недоступно:», например «Подключите и выберите Рутокен.» или «Укажите метку ключа.».
4. Подтвердите создание: для Рутокена и JaCarta введите PIN-код пользователя носителя и нажмите **Подтвердить и создать**; для КриптоПро CSP нажмите **Подтвердить и создать** и при необходимости введите пароль или PIN-код в окне КриптоПро CSP. Кнопка **Отмена** закрывает панель без изменений.
5. После создания в карточке отобразятся CSR с кнопками **Скопировать CSR** и **Скачать CSR** и сведения о созданном ключе или контейнере.

Генерация ключа на JaCarta может занимать несколько минут: не обновляйте и не закрывайте страницу и не извлекайте носитель до завершения. PIN-код вводится только на компьютере пользователя и в ЦС не передаётся. Если после ошибки в карточке выводится «Возможно оставшийся ключ» или «Возможно созданный контейнер», проверьте носитель в разделе «Аппаратные токены» и при необходимости удалите лишний объект.

5.3.6 Выпуск сертификата и запись на носитель

После создания CSR на носителе сертификат можно выпустить прямо из конструктора. Кнопка **Выпустить сертификат** (для JaCarta и КриптоПро CSP это кнопка **Выпустить**) доступна при праве `rleMiniCACertReq-w`: она проверяет CSR по ограничениям шаблона и отправляет запрос в ЦС. Без этого права вместо неё выводится **Добавить выпущенный сертификат**.

- Если CSR не соответствует ограничениям шаблона, открывается окно «Ошибки» со списком нарушений (см. «Ограничения для Subject и SAN»).
- Если выпуск требует одобрения, выводится «Заявка на сертификат создана — после подтверждения установите сертификат вручную.». После одобрения скачайте сертификат из реестра; для Рутокена и JaCarta добавьте его к ключу на носителе в разделе «Аппаратные токены».
- Если сертификат выпущен, для Рутокена и JaCarta открывается блок «Добавление выпущенного сертификата»: введите PIN-код и нажмите **Добавить на Рутокен** или **Добавить на JaCarta**. В контейнер КриптоПро CSP сертификат устанавливается автоматически.

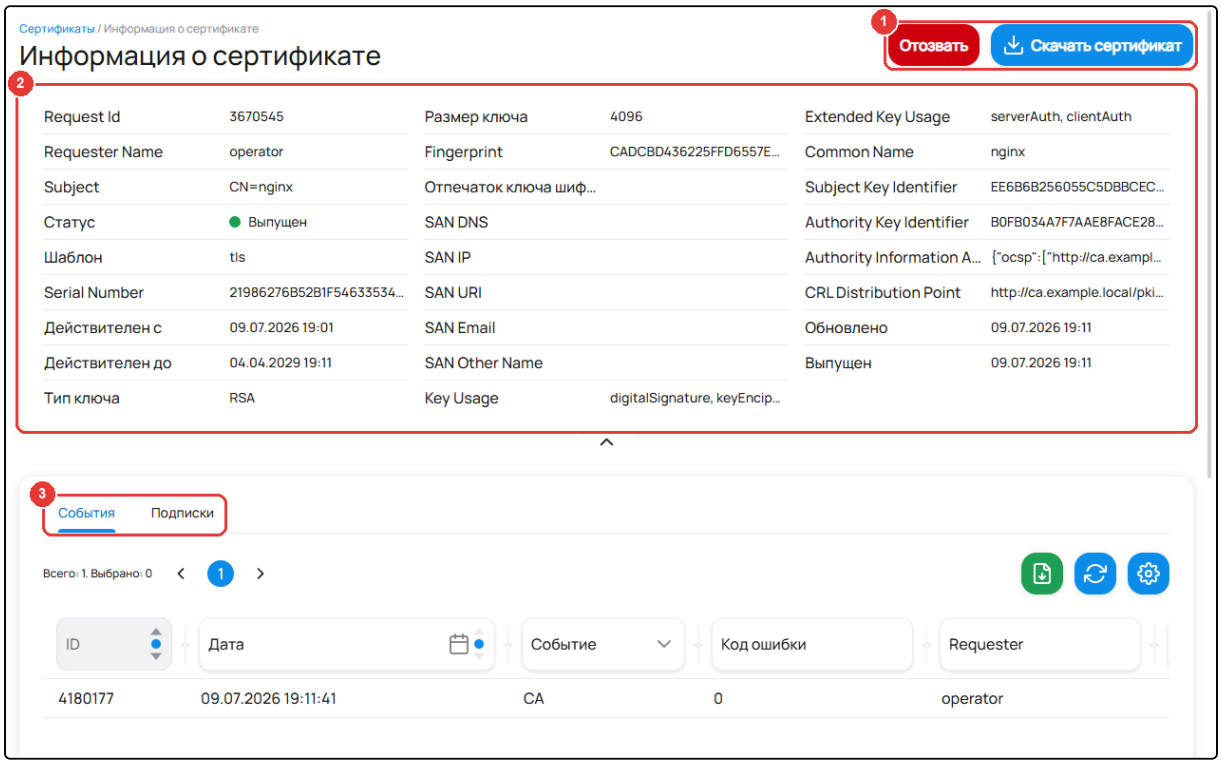
В блоке «Добавление выпущенного сертификата» можно также добавить сертификат, выпущенный ранее: выберите файл (.crt, .cer, .pem или .der, не более 128 КиБ) или вставьте текст в поле «Сертификат PEM», нажмите **Проверить сертификат**, сверьте «Предварительный просмотр» и нажмите кнопку добавления. Добавить сертификат в конструкторе можно только к ключу, созданному на этой странице, и только до её перезагрузки.

5.4 Карточка сертификата

Карточка открывается щелчком по строке реестра. Вверху страницы расположен блок реквизитов сертификата, ниже находятся вкладки «События» (открыта по умолчанию) и «Подписки». Блоки сворачиваются стрелкой.

Кнопка	Что делает	Когда видна
Отозвать	Открывает окно «Отзыв сертификата»	Право `rleMiniCACertRev-w`, сертификат не отозван
Скачать зашифрованный ключ	Скачивает закрытый ключ сертификата, который ЦС хранит в зашифрованном виде (KRA)	ЦС хранит ключ этого сертификата
Скачать сертификат	Открывает меню PEM / DER для скачивания	Содержимое сертификата доступно для скачивания

Кнопки восстановления в карточке нет. Восстановить сертификат можно в реестре сертификатов или на вкладке «Отозванные сертификаты» страницы «Информация о CRL и Delta CRL» (см. «Восстановление сертификата»).



19 Карточка «Информация о сертификате»

На рисунке: **1** кнопки карточки; **2** реквизиты сертификата; **3** вкладки «События» и «Подписки».

5.4.1 Реквизиты сертификата

Блок реквизитов содержит поля: Request Id, Requester Name, Subject, Статус, Шаблон, Serial Number, Действителен с, Действителен до, Тип ключа, Размер ключа, Fingerprint, Отпечаток ключа шифрования, SAN DNS, SAN IP, SAN URI, SAN Email, SAN Other Name, Key Usage, Extended Key Usage, Common Name, Subject Key Identifier, Authority Key Identifier, Authority Information Access, CRL Distribution Point, Обновлено, Выпущен. У отозванного сертификата есть поле «Причина отзыва».

- Fingerprint: отпечаток сертификата, по которому его можно однозначно опознать.
- Subject Key Identifier (SKI) и Authority Key Identifier (AKI): идентификаторы ключа владельца и ключа выпустившего ЦС. По совпадению AKI сертификата с SKI сертификата ЦС строится цепочка доверия.
- Authority Information Access (AIA): адреса службы OCSP и сертификата выпустившего ЦС. По OCSP приложение узнаёт актуальный статус сертификата, не загружая список отзыва целиком.
- CRL Distribution Point (CDP): адрес, по которому публикуется список отзыва.
- Key Usage и Extended Key Usage: разрешённые криптографические операции и сценарии применения, например аутентификация сервера или клиента (см. «Справочник значений»).

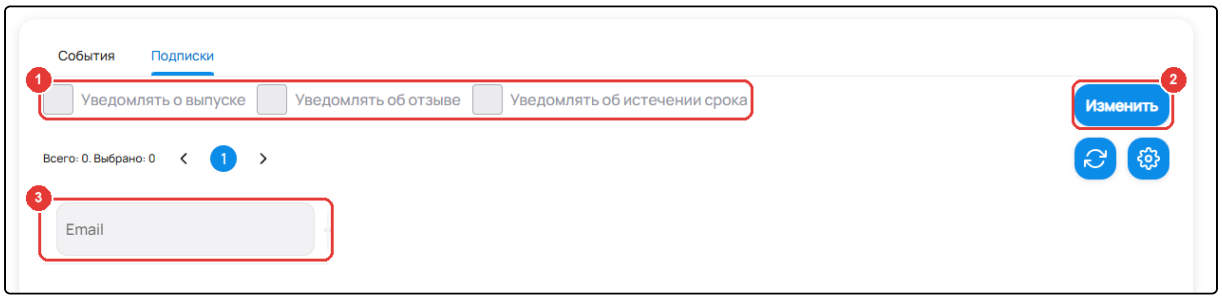
Вкладка «События» содержит журнал событий только по этому сертификату: столбцы и выгрузка такие же, как в разделе «Журнал событий». Для просмотра нужно право `rleMiniCAEventList-r`.

5.4.2 Подписки

На вкладке «Подписки» настраиваются уведомления по электронной почте о событиях сертификата: выпуске, отзыве и истечении срока действия. Уведомление об истечении срока помогает вовремя перевыпустить сертификат.

На вкладке видны текущие настройки: три флажка (только для просмотра) и таблица адресов «Email».

1. Нажмите **Изменить**.
2. В окне «Изменение параметров уведомления» введите адрес в поле «Почта для уведомлений» и нажмите «+». Повторите для каждого адреса; лишний адрес удаляется крестиком.
3. Отметьте события: «Уведомлять о выпуске», «Уведомлять об отзыве», «Уведомлять об истечении срока».
4. Нажмите **Подтвердить**. Появится сообщение «Обновлено».



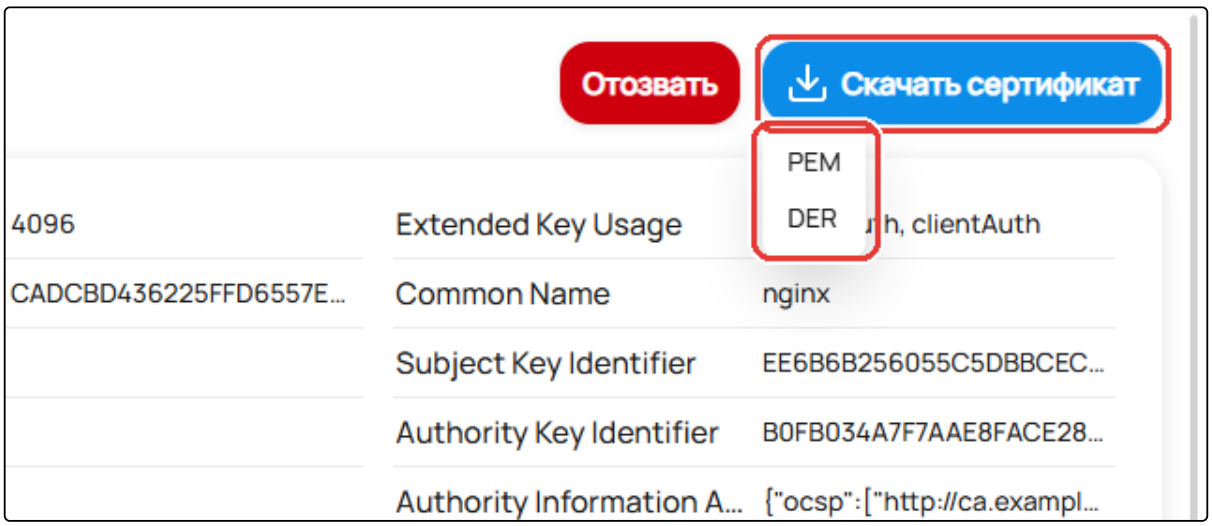
20 Вкладка «Подписки»

На рисунке: **1** события, о которых отправляются уведомления; **2** кнопка «Изменить»; **3** адреса для уведомлений.

Если адрес введён неверно, появится сообщение «Неверный формат email». Те же уведомления можно задать сразу при запросе сертификата (см. «Запрос сертификата»).

5.4.3 Скачивание сертификата

Где	Как	Формат
Карточка	**Скачать сертификат** → PEM или DER	PEM или DER
Реестр, один сертификат	Значок в столбце «Скачать» его строки	PEM
Реестр, несколько сертификатов	Отметьте строки, нажмите **Скачать сертификаты** и выберите PEM или DER	PEM или DER



21 Меню «Скачать сертификат» в карточке

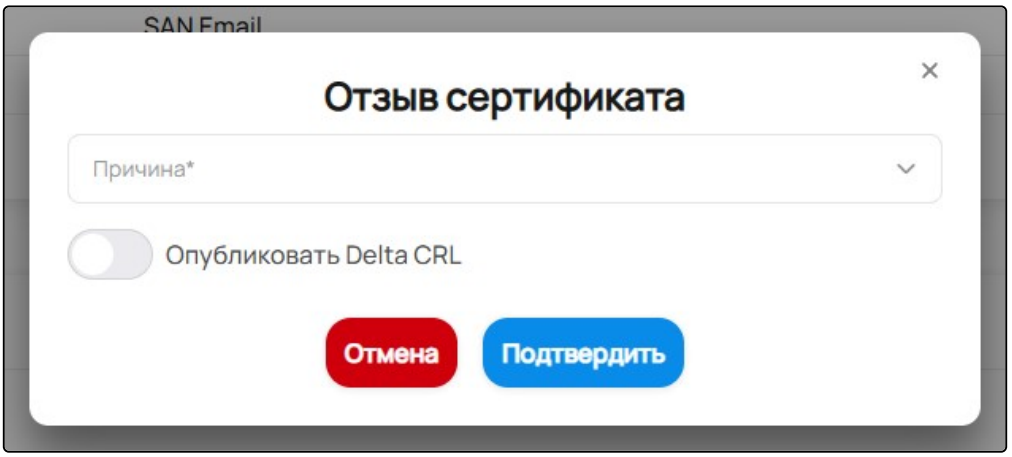
Формат PEM текстовый (Base64), файл можно открыть в текстовом редакторе; формат DER двоичный. Содержимое сертификата в обоих форматах одинаковое, различается только кодировка. Выбирайте формат, который требует принимающая система.

5.4.4 Отзыв сертификата

Сертификат отзывают, если он скомпрометирован или больше не должен считаться доверенным. Проверяющие стороны узнают об отзыве из списков отзыва и через службу OCSP. Отзыв необратим для всех причин, кроме CertificateHold (см. «Восстановление сертификата»). Нужно право `rleMiniCACertRev-w`.

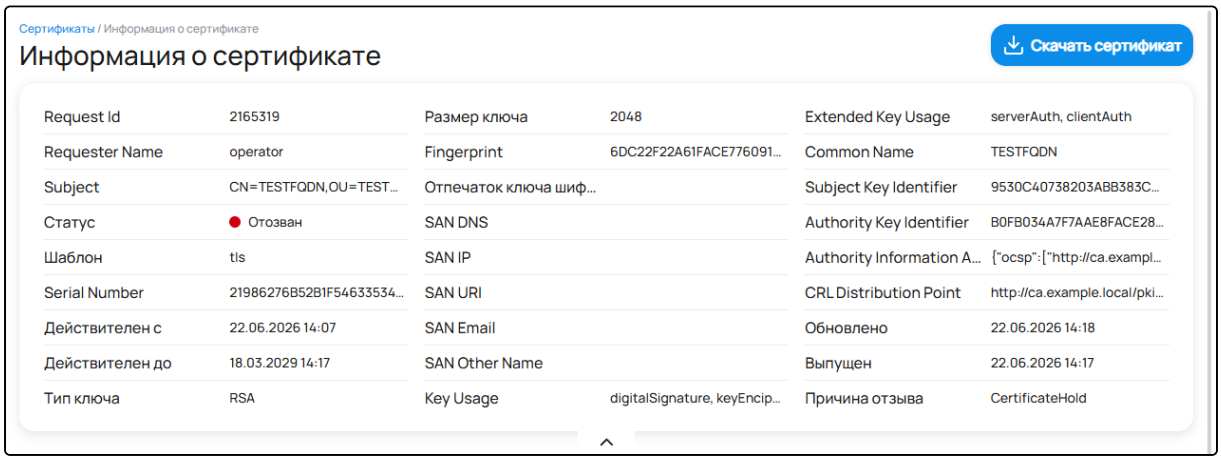
Отзыв одного сертификата:

1. Откройте карточку сертификата и нажмите **Отозвать**.
2. Выберите причину.
3. При необходимости включите «Опубликовать Delta CRL».
4. Нажмите **Подтвердить**.



22 Окно «Отзыв сертификата»

Появится сообщение «Сертификат отозван». Статус станет «Отозван», в карточке появится поле «Причина отзыва», кнопка **Отозвать** пропадёт. Операция отразится на вкладке «События».



23 Карточка отозванного сертификата

Причина	Когда выбирать
Unspecified	Причину раскрывать не требуется
KeyCompromise	Закрытый ключ сертификата мог стать доступен посторонним
CaCompromise	Скомпрометирован ключ ЦС, выпустившего сертификат
AffiliationChanged	Изменились сведения о владельце, например организация или подразделение
Superseded	Сертификат заменён новым
CessationOfOperation	Сертификат или обслуживаемая им система выведены из эксплуатации
CertificateHold	Временная приостановка. Единственная причина, после которой сертификат можно восстановить

Причина записывается в список отзыва и сообщает проверяющим сторонам, почему сертификату больше нельзя доверять.

Переключатель «Опубликовать Delta CRL» есть, если доступен сервис публикации. Когда он включён, после отзыва сразу публикуется Delta CRL и появляется сообщение «Delta CRL опубликован». Если переключатель выключен или его нет, сведения об отзыве попадут в списки отзыва при их следующем формировании.

Групповой отзыв из реестра:

1. Отметьте строки сертификатов в реестре.

2. Нажмите **Отозвать выбранные сертификаты** (крестик).
3. В окне «Отзыв сертификатов» выберите причину и при необходимости включите «Опубликовать Delta CRL». В окне видно, сколько сертификатов будет отозвано («Всего»), и их список.
4. Нажмите **Отозвать**.

Уже отозванные сертификаты в операцию не попадают. По итогам появится сообщение «Сертификаты отозваны! Количество: N»; если не удалось отозвать ни одного, появится «Не удалось отозвать сертификаты».

5.4.5 Восстановление сертификата

Восстановление возвращает в действие сертификат, отозванный с причиной CertificateHold. Выполняется из реестра сертификатов или со вкладки отозванных сертификатов на странице «Информация о CRL и Delta CRL». Нужно право `rleMiniCACertUnRev-w`.

1. Отметьте сертификаты со статусом «Отозван» и причиной CertificateHold. Чтобы видеть причину, включите столбец «Причина отзыва» в окне «Настройки таблицы».
2. Нажмите **Восстановить выбранные сертификаты** (круговая стрелка). Кнопка активна, если среди отмеченных есть хотя бы один такой сертификат.
3. В окне «Восстановление сертификатов» проверьте список и нажмите **Восстановить**.

Сертификаты, отозванные по другим причинам, в операцию не попадают. По итогам появится сообщение «Сертификаты восстановлены! Количество: N» или «Не удалось восстановить сертификаты», если не восстановлен ни один.

> **Важно**
>
> Отзыв по любой причине, кроме CertificateHold, окончательный: восстановить такой сертификат нельзя, нужно выпустить новый.

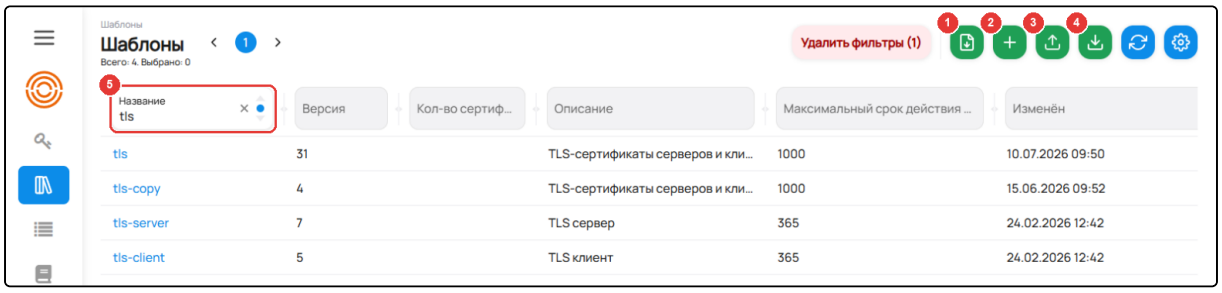
6 Шаблоны сертификатов

Шаблоном сертификата называется именованный набор ограничений и расширений, который центр сертификации применяет при обработке запроса на выпуск. Шаблоны контролируют состав атрибутов запроса и упрощают его подготовку: часть атрибутов и расширений задаётся самим шаблоном, а запрос перед выпуском проверяется на соответствие политике шаблона.

Шаблоны хранятся в базе данных центра сертификации. Каждое сохранение шаблона создаёт его новую версию: номер версии увеличивается на единицу, а прежняя версия отмечается как удалённая. В реестре всегда показана действующая версия. Разрешения шаблона разграничивают доступ на просмотр, изменение и выпуск сертификатов по шаблону, а ограничения задают допустимые значения Subject и SAN в запросе.

6.1 Реестр шаблонов

Раздел «Шаблоны» доступен пользователю с правом `rleMiniCATemplList-r`. Общие приёмы работы с реестром описаны в главе «Общие элементы интерфейса». Строки реестра не отмечаются, групповых действий у шаблонов нет, боковой панели фильтров нет.



24 Реестр шаблонов

На рисунке: **1**, **2**, **3**, **4** кнопки реестра (см. таблицу ниже); **5** фильтр по названию.

№	Кнопка (значок)	Что делает	Право
1	Выгрузка отчёта (зелёный значок файла)	Выгружает отчёт в файл Excel (см. «Выгрузка отчёта в файл»)	`rleMiniCATemplList-r`
2	**Создать шаблон** («+»)	Открывает окно «Новый шаблон»	`rleMiniCATempl-w`
3	**Импортировать шаблоны** (стрелка вверх)	Открывает окно «Импорт шаблонов»	`rleMiniCATempl-w`

4	**Экспортировать шаблоны** (стрелка вниз)	Сохраняет файл minica-templates-export.json со всеми шаблонами реестра, подходящими под заданные фильтры	`rleMiniCATemplList-r`

Столбец	**Что показывает**
Название	Название шаблона; щелчок по названию открывает карточку шаблона. Фильтр ищет часть названия с учётом регистра букв: например, «tls» находит tls-server, а «TLS» не находит. Сортировка
Версия	Номер действующей версии шаблона
Кол-во сертификатов	Число сертификатов, выпущенных по шаблону с этим названием
Описание	Описание шаблона
Максимальный срок действия сертификата	Предельный срок действия сертификата в днях
Изменён	Дата и время сохранения действующей версии. Сортировка
Basic Constraints, Key Usage, Extended Key Usage	Значения соответствующих расширений
Subject Key Identifier, Authority Key Identifier	Способ формирования идентификатора ключа субъекта и состав идентификатора ключа издателя
Секция конфигурации в файле OpenSSL, Произвольные опции OpenSSL	Значения одноимённых полей блока «Дополнительно»
Привилегии	Привилегии шаблона; в карточке не редактируются
Шифрование ключа	Галочка: у шаблона установлен флажок «Сохранять приватный ключ, зашифрованный сертификатом KRA»

6.2 Карточка шаблона

Чтобы открыть карточку, щёлкните название шаблона в реестре. В заголовке карточки указаны название и номер версии: «Шаблон <название> (версия N)». Если карточка открыта по ссылке на удалённый шаблон или на прежнюю версию, рядом с заголовком красным выводится «Удалён».

№	Кнопка	Что делает
1	**Сертификаты**	Открывает реестр «Сертификаты» с фильтром по этому шаблону
2	**Удалить** (корзина)	Удаляет шаблон после подтверждения (см. «Удаление шаблона»)
3	**Копировать**	Открывает окно «Копировать шаблон» (см. «Копирование шаблона»)
4	**Сохранить** (дискета)	Сохраняет изменения как новую версию шаблона (см. «Изменение шаблона»)

Кнопки видны только пользователю с правом `rleMiniCATempl-w`; без этого права изменения в полях карточки сохранить нельзя.

Карточка содержит те же поля, что и окно «Новый шаблон», кроме названия: название после создания изменить нельзя. Ниже расположены блоки разрешений (см. «Разграничение прав доступа к шаблонам») и ограничений (см. «Ограничения для Subject и SAN»).



25 Карточка шаблона

На рисунке: **1**, **2**, **3**, **4** кнопки карточки (см. таблицу выше); **5** блок «Дополнительно» (свёрнут).

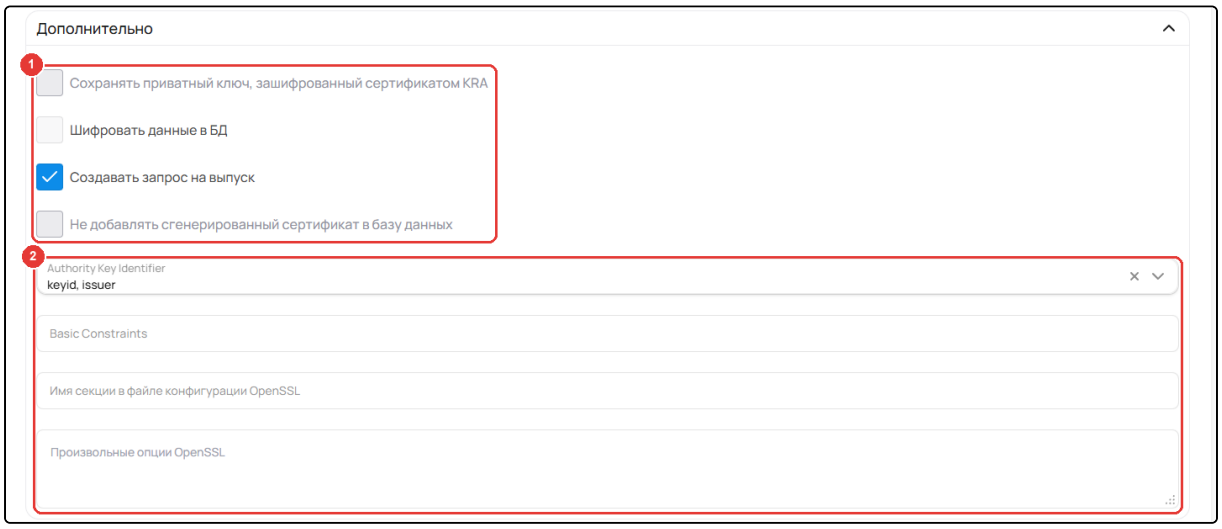
6.2.1 Параметры шаблона

Поле	Что указать
Название*	Название шаблона. Задаётся только при создании или копировании
Описание	Назначение шаблона. Поле обязательное
Максимальный срок действия сертификата*	Предельный срок действия выпускаемых сертификатов в днях, число не меньше 0. Запрошенный срок не может его превышать
Не добавлять в сертификат расширение AIA (-noaia)	Установите, если адреса доступа к сведениям ЦС (в том числе службы OCSP) в сертификате не нужны
Не добавлять в сертификат расширение CDP (-nocdp)	Установите, если адрес точки распространения CRL в сертификате не нужен
Допустимый тип ключа*	RSA, ECDSA, Ed25519, GOST2001 или GOST2012. Ключ запроса должен быть этого типа
Минимально допустимый размер ключа*	Размер ключа запроса не может быть меньше. При смене типа ключа значение сбрасывается, его нужно выбрать заново (см. «Типы и размеры ключей»)
Key Usage	Одно или несколько значений (см. «Справочник значений»); нужно хотя бы одно. Значения записываются в расширение Key Usage сертификата
Extended Key Usage	Одно или несколько значений (см. «Справочник значений»); нужно хотя бы одно

Если обязательное поле не заполнено, под ним появляется сообщение «Обязательно к заполнению», и шаблон не сохраняется.

6.2.2 Блок «Дополнительно»

Блок свёрнут; чтобы раскрыть его, щёлкните заголовок «Дополнительно».



26 Блок «Дополнительно» карточки шаблона

На рисунке: **1** флажки хранения ключа, шифрования и согласования выпуска; **2** поля расширений и параметров OpenSSL.

Поле	**Что указать**
Сохранять приватный ключ, зашифрованный сертификатом KRA	Закрытый ключ сертификата хранится в базе ЦС в зашифрованном виде (см. «Хранение и восстановление закрытых ключей (KRA)»)
Шифровать данные в БД	Данные сертификатов, выпущенных по шаблону, хранятся в базе в зашифрованном виде (см. «Шифрование данных сертификата в базе данных»)
Создавать запрос на выпуск	Выпуск по шаблону оформляется запросом, который нужно одобрить в разделе «Запросы»
Не добавлять сгенерированный сертификат в базу данных	Выпущенный сертификат не сохраняется в базе данных ЦС
Authority Key Identifier	Одно или несколько значений (см. «Справочник значений»). Поле обязательное; в новом шаблоне выбрано keyid
Basic Constraints	Значение расширения Basic Constraints, например critical,CA:true,pathlen:0 для сертификата подчинённого ЦС
Имя секции в файле конфигурации OpenSSL	Имя секции конфигурации OpenSSL

Произвольные опции OpenSSL	Дополнительные параметры в формате конфигурации OpenSSL

Флажки блока совместимы не во всех сочетаниях, несовместимый флажок становится недоступным:

Флажок	**Недоступен, если установлен**
Сохранять приватный ключ, зашифрованный сертификатом KRA	«Создавать запрос на выпуск» или «Не добавлять сгенерированный сертификат в базу данных»
Шифровать данные в БД	«Не добавлять сгенерированный сертификат в базу данных»
Создавать запрос на выпуск	«Сохранять приватный ключ, зашифрованный сертификатом KRA» или «Не добавлять сгенерированный сертификат в базу данных»
Не добавлять сгенерированный сертификат в базу данных	Любой из трёх других флажков

Идентификатор ключа субъекта (Subject Key Identifier) в интерфейсе не задаётся: у шаблонов, сохранённых через Контрольную панель, он равен hash.

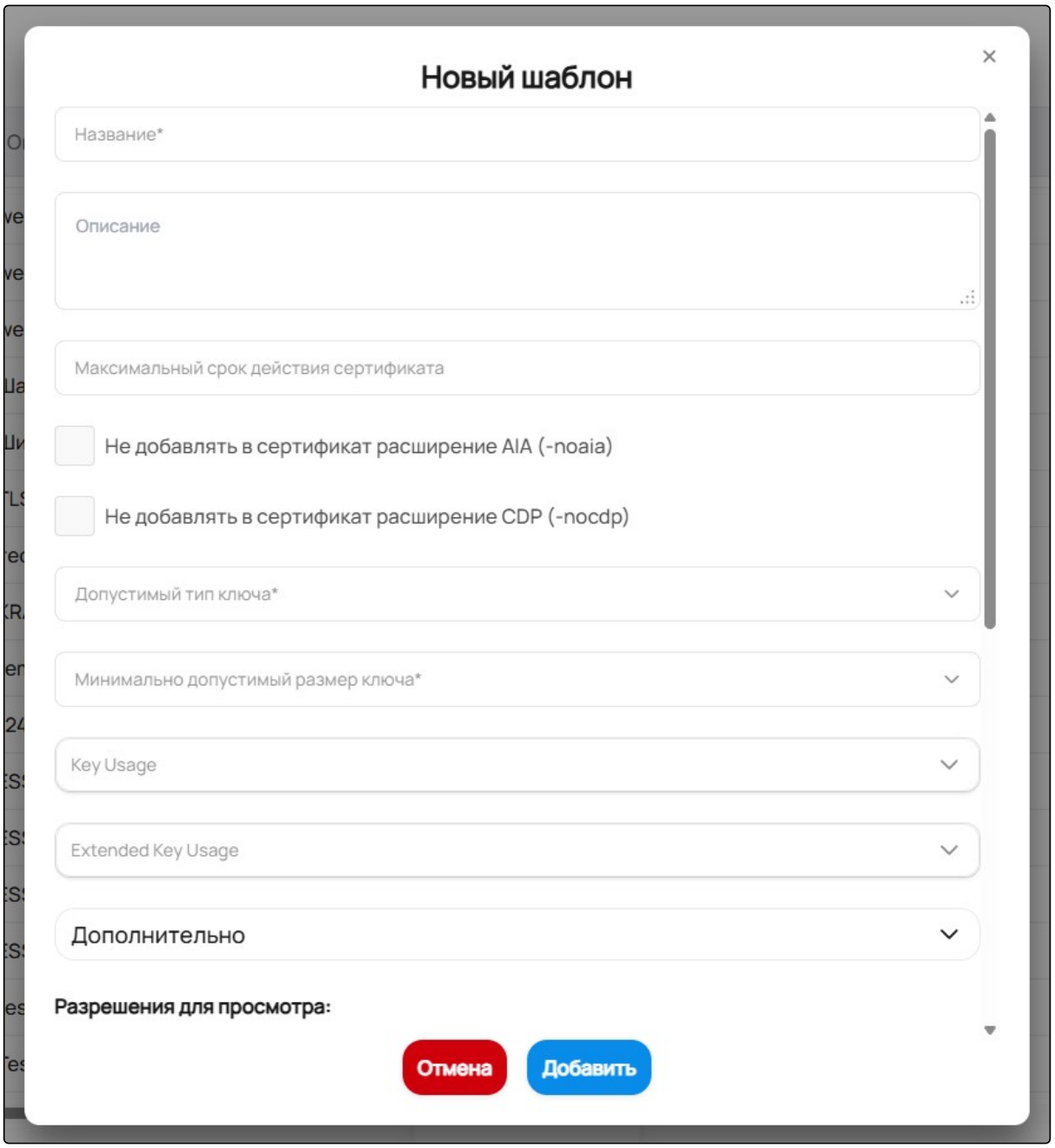
6.3 Создание, изменение, копирование и удаление шаблона

Эти операции доступны пользователю с правом `rleMiniCATempl-w`.

6.3.1 Создание шаблона

Создайте шаблон, когда нужна новая политика выпуска со своими ограничениями на ключ и расширениями сертификата. Шаблоны, в названии которых есть «auto_», в списке при выпуске сертификата не показываются.

1. В реестре шаблонов нажмите **Создать шаблон** («+»). Откроется окно «Новый шаблон».
2. Заполните параметры шаблона (см. «Параметры шаблона»). При необходимости раскройте блок «Дополнительно».
3. При необходимости задайте разрешения (см. «Разграничение прав доступа к шаблонам») и ограничения (см. «Ограничения для Subject и SAN»).
4. Нажмите **Добавить**.



27 Окно «Новый шаблон»

Если шаблон с таким названием уже есть, откроется окно «Перезаписать?» с вопросом «Данный шаблон уже существует. Вы уверены, что хотите перезаписать?». **Подтвердить** сохраняет параметры как новую версию существующего шаблона, **Отменить** возвращает в окно «Новый шаблон» без сохранения.

После сохранения появится сообщение «Шаблон сохранён», окно закроется, а реестр обновится; карточка нового шаблона автоматически не открывается. При ошибке выводится «Не удалось сохранить шаблон» или текст ошибки сервера. Чтобы закрыть окно без сохранения, нажмите **Отмена** или крестик.

6.3.2 Изменение шаблона

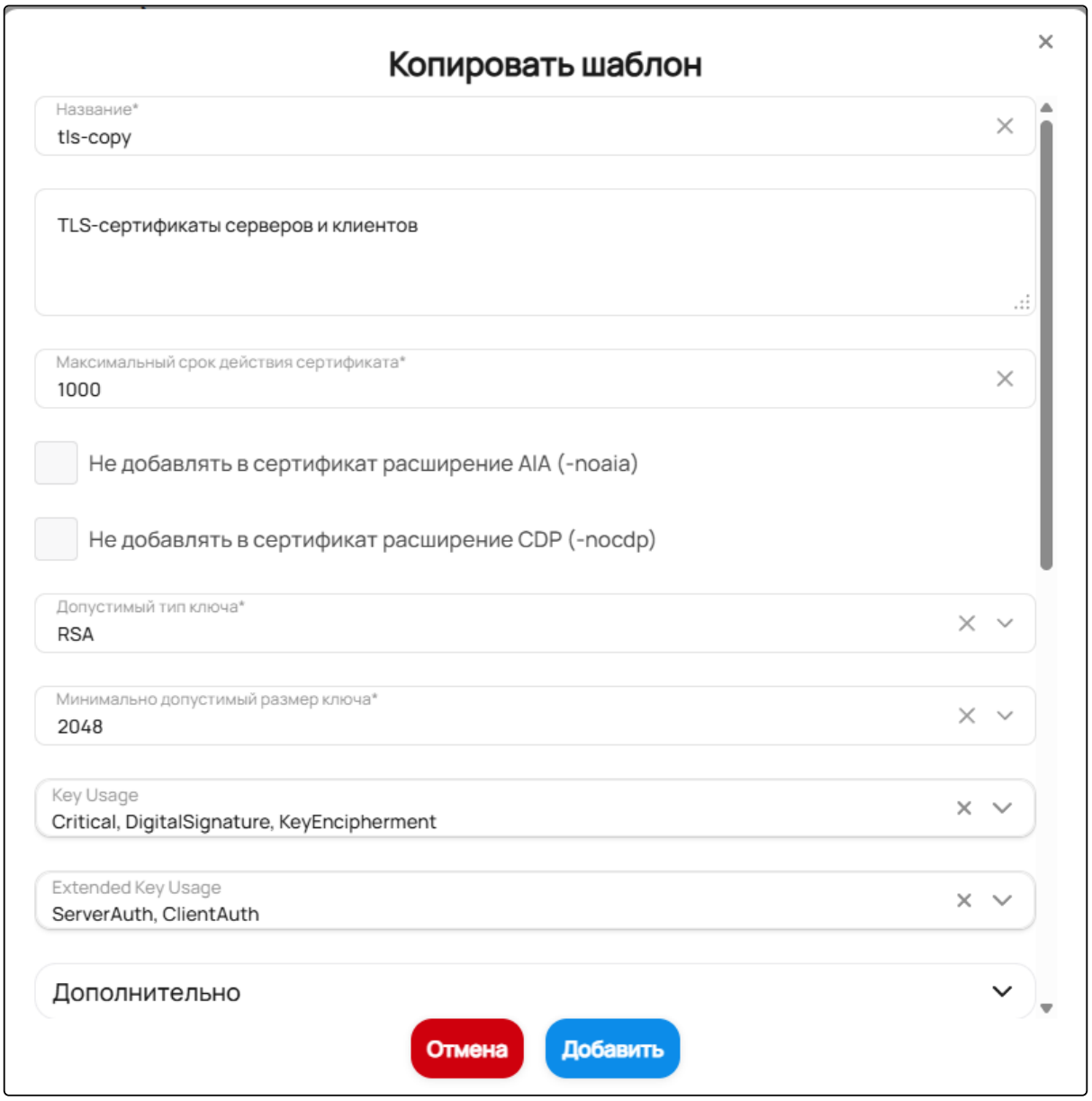
1. Откройте карточку шаблона.
2. Измените параметры, разрешения или ограничения.
3. Нажмите **Сохранить** (дискета).

После сохранения появится сообщение «Шаблон сохранён» и откроется карточка новой версии: номер версии увеличится. Прежняя версия остаётся доступной по старой ссылке с отметкой «Удалён». При ошибке выводится «Не удалось сохранить шаблон» или текст ошибки сервера.

Название шаблона изменить нельзя. Чтобы переименовать шаблон, скопируйте его под новым названием и удалите исходный.

6.3.3 Копирование шаблона

1. Откройте карточку шаблона и нажмите **Копировать**.
2. В окне «Копировать шаблон» уже заполнены все параметры, разрешения и ограничения исходного шаблона, а в поле «Название» указано «<название>-copy». При необходимости измените название и другие параметры.
3. Нажмите **Добавить**. Если шаблон с таким названием уже существует, подтвердите перезапись или отмените её.
4. После сообщения «Шаблон сохранён» система спросит «Перейти в карточку нового шаблона?». **Подтвердить** открывает копию, **Отменить** оставляет в карточке исходного шаблона.



28 Окно «Копировать шаблон»

6.3.4 Удаление шаблона

1. Откройте карточку шаблона и нажмите **Удалить** (корзина).
2. В окне «Подтверждение» с вопросом «Удалить шаблон?» нажмите **Да**. **Нет** отменяет удаление.

После удаления появится сообщение «Шаблон удалён» и откроется реестр шаблонов. При ошибке выводится «Не удалось удалить шаблон» или текст ошибки сервера.

6.4 Разграничение прав доступа к шаблонам

Доступ к шаблону можно ограничить отдельно для трёх операций: просмотра, изменения и выпуска сертификатов. Каждому разрешению назначается список ролей.

Разрешение	Назначение	Поведение при отсутствии роли
Просмотр	Просмотр шаблона	Шаблон скрыт в реестре, карточка не открывается
Изменение	Редактирование параметров	При сохранении выводится сообщение об ошибке, изменения не сохраняются
Выпуск	Использование шаблона при выпуске сертификата	Шаблон скрыт в списке шаблонов при запросе сертификата

Разрешение может быть не задано (доступ не ограничен) или задано списком ролей.

6.4.1 Настройка разрешений

Разрешения задаются в карточке шаблона (или в окне «Новый шаблон») в блоках «Разрешения для просмотра», «Разрешения для изменения» и «Разрешения для выпуска». Изменять их может пользователь с правом `rleMiniCATempl-w`, если разрешение на изменение шаблона его не ограничивает.

1. Перейдите в раздел «Шаблоны» и откройте карточку шаблона.
2. В блоке нужного разрешения нажмите кнопку «+». Появится пустое поле.
3. Введите в поле название роли точно так, как оно назначено пользователям, например `rleMiniCATemplList-r`. Названия ролей показаны на экране «Профиль пользователя» в блоке «Права» (см. «Профиль и права доступа»); состав ролей определяет администратор.
4. Чтобы указать несколько ролей, нажмите «+» ещё раз и заполните новое поле. Операция доступна пользователю, у которого есть хотя бы одна из перечисленных ролей.
5. Чтобы удалить роль из списка, нажмите кнопку «−» справа от её поля. Если в блоке не осталось ни одной роли, операция доступна без ограничений. Пустое поле роли не допускается: заполните его или удалите, иначе шаблон не сохранится.
6. Сохраните шаблон кнопкой **Сохранить** в карточке.



29 Добавление роли в разрешения шаблона

> Разрешение на просмотр скрывает шаблон и от пользователя, который его задал, если у него нет ни одной из указанных ролей: после сохранения шаблон исчезнет из реестра, а его карточка станет недоступна.

Если разрешения не заданы, шаблон виден всем, его можно изменять и выбирать при запросе сертификата. Разрешения независимы: например, разрешение на выпуск не влияет на просмотр и изменение шаблона.

6.5 Экспорт и импорт шаблонов в формате JSON

Экспорт и импорт нужны, чтобы переносить шаблоны между контурами, делать их резервные копии и тиражировать настройки.

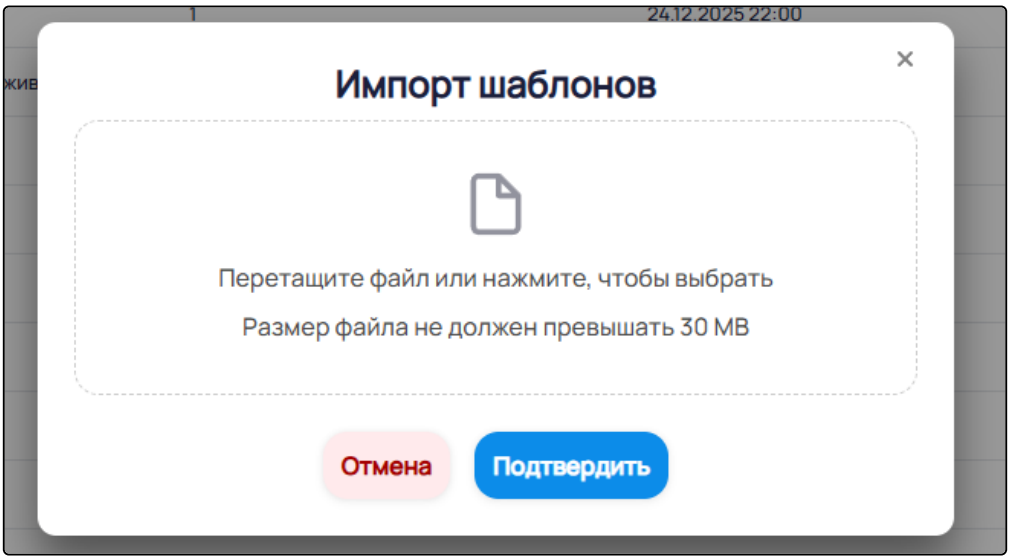
Экспорт шаблонов (право `rleMiniCATemplList-r`):

1. Откройте раздел «Шаблоны». Чтобы выгрузить не все шаблоны, отберите нужные фильтром по названию.
2. Нажмите «Экспортировать шаблоны» (стрелка вниз).

Браузер сохранит файл minica-templates-export.json со всеми шаблонами реестра, подходящими под заданные фильтры.

Импорт шаблонов (право `rleMiniCATempl-w`):

1. Нажмите «Импортировать шаблоны» (стрелка вверх). Откроется окно «Импорт шаблонов».
2. Перетащите в область окна файл, полученный экспортом, или щёлкните область и выберите файл. Размер файла должен быть не более 30 МБ.
3. Нажмите **Подтвердить**.



30 Окно «Импорт шаблонов»

Как выполняется импорт:

- Сначала проверяется весь файл. У каждого шаблона в файле должны быть название, значения Key Usage и Extended Key Usage и размер ключа. При ошибке выводится сообщение «Ошибка: …» с описанием, и ни один шаблон не загружается.
- Затем шаблоны обрабатываются по очереди. Если шаблон с таким названием уже есть, создаётся его новая версия с параметрами из файла; подтверждение перезаписи не запрашивается. Если такого шаблона нет, он создаётся.
- По каждому шаблону выводится сообщение «Шаблон "<название>" сохранён» или «Не удалось сохранить шаблон: "<название>"». Ошибка по одному шаблону не останавливает обработку остальных.
- Если параметр в файле не задан, подставляется значение по умолчанию: тип ключа RSA, для Subject Key Identifier значение hash, для Authority Key Identifier значения keyid и issuer, флажки выключены, разрешения не заданы.
- Шаблоны, которых нет в файле, не изменяются. Перезапуск сервиса не требуется.

6.6 Ограничения для Subject и SAN

Ограничения шаблона задают, какие значения допустимы в именах, указанных в запросе на выпуск сертификата:

- Subject содержит имя владельца сертификата и состоит из атрибутов: Common Name (CN, обычно имя узла или пользователя), Organization (O, организация), Organization Unit (OU, подразделение) и других.
- SAN (Subject Alternative Name) содержит дополнительные имена владельца: DNS-имена, IP-адреса, адреса электронной почты и URI. По ним клиенты проверяют, что сертификат предъявлен именно тем узлом, к которому они подключились.

Перед выпуском центр сертификации сверяет запрос с ограничениями выбранного шаблона. Если нарушено хотя бы одно ограничение, сертификат не выпускается, а пользователь видит перечень всех нарушений. Так шаблон не позволяет выпустить сертификат на имя, не предусмотренное политикой организации: например, на чужой домен или с неверным названием организации.

6.6.1 Способы проверки значения

Каждое ограничение относится к одному атрибуту Subject или одному типу имени SAN. Для него можно задать обязательность и способ проверки значения.

Параметр	Как проверяется	Пример
Признак обязательного поля	Атрибут должен присутствовать в запросе. Если флажок не установлен, атрибут можно не указывать, но указанное значение всё равно проверяется	Для атрибута O установлен флажок, а в запросе организации нет: запрос отклоняется
Требуемое значение	Точное совпадение строки с учётом регистра букв	Задано «Example»: значение «Example» допускается, «example» не допускается
Допустимое значение в формате glob	Совпадение с шаблоном строки. Знак * заменяет любую последовательность символов, в том числе содержащую точки	Задано *.example.local: допускаются www.example.local и app.int.example.local, не допускается www.example.org
Допустимое значение в формате regexp	Совпадение с регулярным выражением. Чтобы проверялась вся строка целиком, начинайте выражение с ^ и заканчивайте $	Задано ^[a-z0-9-]+\.example\.local$: допускается web-01.example.local, не допускается Web_01.example.local

Для ограничения SAN проверяется каждое имя выбранного типа, указанное в запросе. Если в запросе два DNS-имени и одно из них не соответствует ограничению, запрос отклоняется целиком.

6.6.2 Добавление ограничения

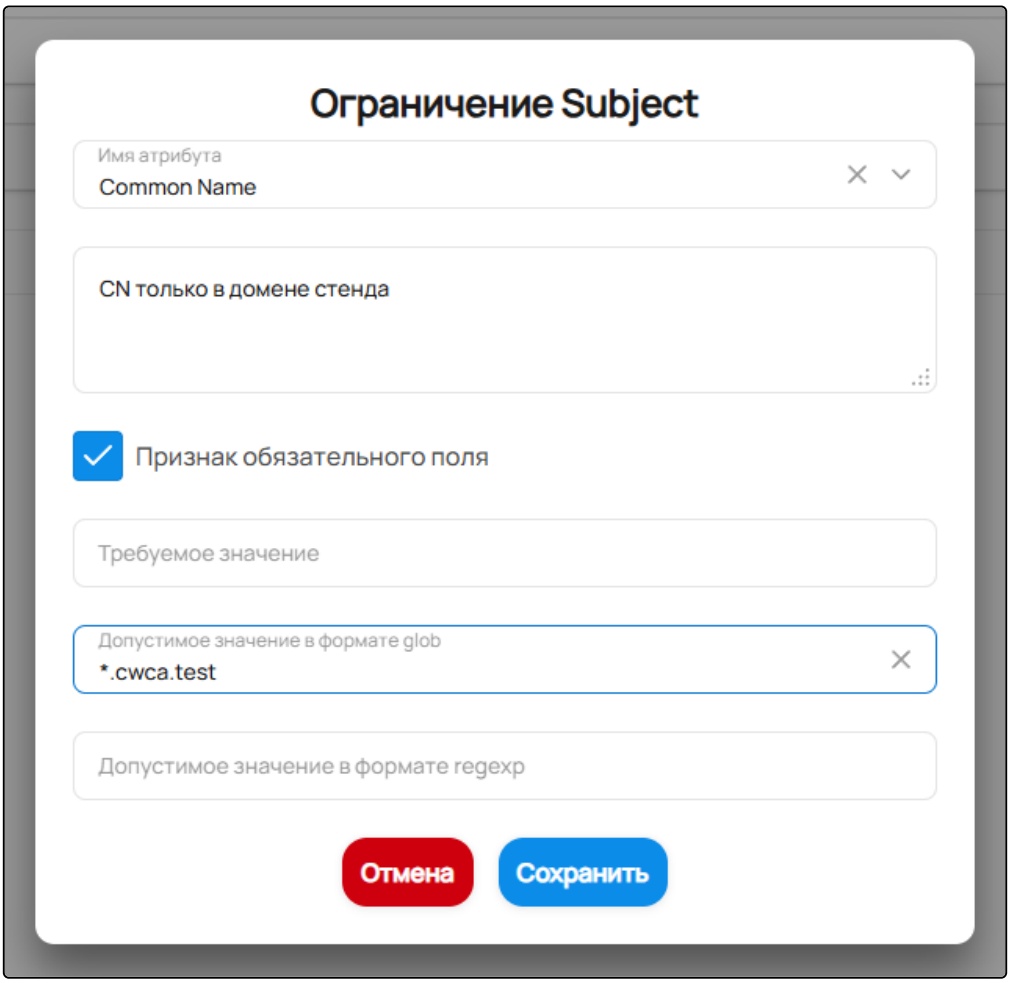
Ограничения может изменять пользователь, которому разрешено изменение шаблона (см. «Настройка разрешений»).

1. Откройте карточку шаблона (или окно «Новый шаблон») и в блоке «Ограничения для Subject или SAN» нажмите «+».
2. Выберите, к чему относится ограничение: Subject или SAN. Откроется окно «Ограничение Subject» или «Ограничение SAN».
3. Укажите, какое имя проверяется:

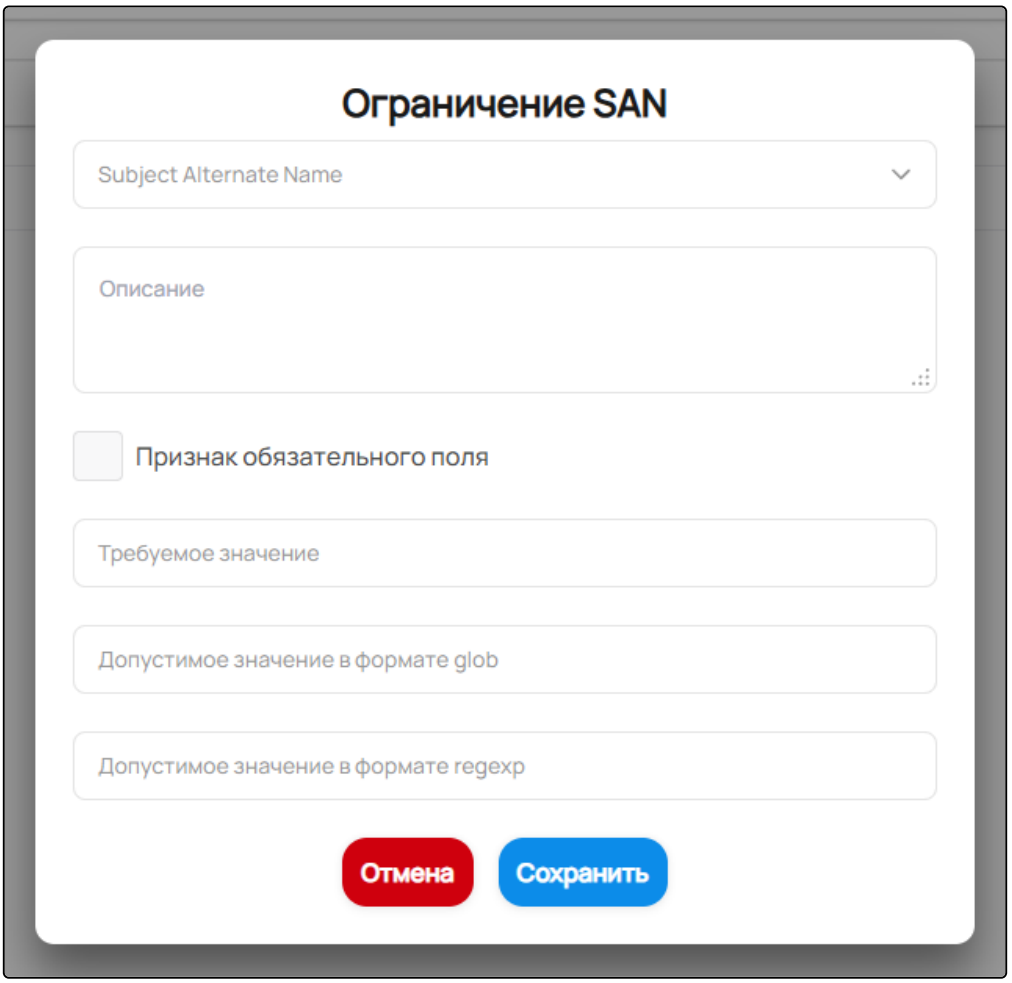
- в окне «Ограничение Subject» выберите атрибут в списке «Имя атрибута»: Common Name, Country, Domain Component, Email, Given Name, Initials, Locality, Organization, Organization Unit, State, Street Address, Surname, Title. Если нужного атрибута нет, введите его объектный идентификатор (OID) в поле «Идентификатор атрибута». Поля взаимоисключающие: после выбора атрибута поле OID скрывается, и наоборот;
- в окне «Ограничение SAN» выберите тип имени в списке «Subject Alternate Name»: Dns, Ip, Email или Uri.

4. В поле «Описание» кратко поясните назначение ограничения, например «DNS-имя только в домене организации». Описание отображается в таблице ограничений и помогает другим операторам понять правило.
5. Если атрибут или имя обязательно должны присутствовать в запросе, установите флажок «Признак обязательного поля».
6. Задайте допустимое значение в одном из полей: «Требуемое значение», «Допустимое значение в формате glob» или «Допустимое значение в формате regexp».
7. Нажмите **Сохранить** в окне ограничения. Если не указаны имя атрибута или OID, появится сообщение «Имя или идентификатор атрибута должны быть заполнены!»; если не выбран тип SAN, появится сообщение «SAN должен быть заполнен!». Ограничение появится строкой в таблице блока.
8. Сохраните шаблон кнопкой **Сохранить** в карточке (или **Добавить** в окне «Новый шаблон»). Ограничения начинают действовать после сохранения шаблона, при этом номер версии шаблона увеличивается.

Окна ограничений не закрываются крестиком и клавишей Esc: чтобы выйти без изменений, нажмите **Отмена**.

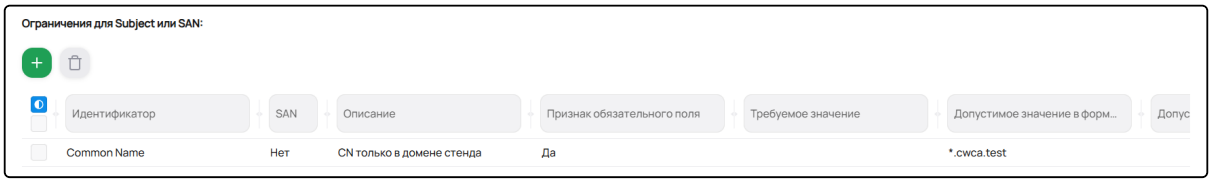


31 Окно «Ограничение Subject»



32 Окно «Ограничение SAN»

В таблице блока «Ограничения для Subject или SAN» для каждого ограничения отображаются столбцы «Идентификатор» (атрибут или тип имени), «SAN» (Да для ограничения SAN, Нет для ограничения Subject), «Описание», «Признак обязательного поля», «Требуемое значение», «Допустимое значение в формате glob» и «Допустимое значение в формате regexp».



33 Таблица ограничений в карточке шаблона

6.6.3 Изменение и удаление ограничения

- Чтобы изменить ограничение, щёлкните его строку в таблице. Откроется то же окно с заполненными полями. Нажмите **Сохранить**, а затем сохраните шаблон.

- Чтобы удалить ограничения, отметьте их строки (флажок в заголовке отмечает все) и нажмите кнопку с корзиной; пока строки не отмечены, кнопка неактивна. В окне «Подтверждение» нажмите **Да**, затем сохраните шаблон.

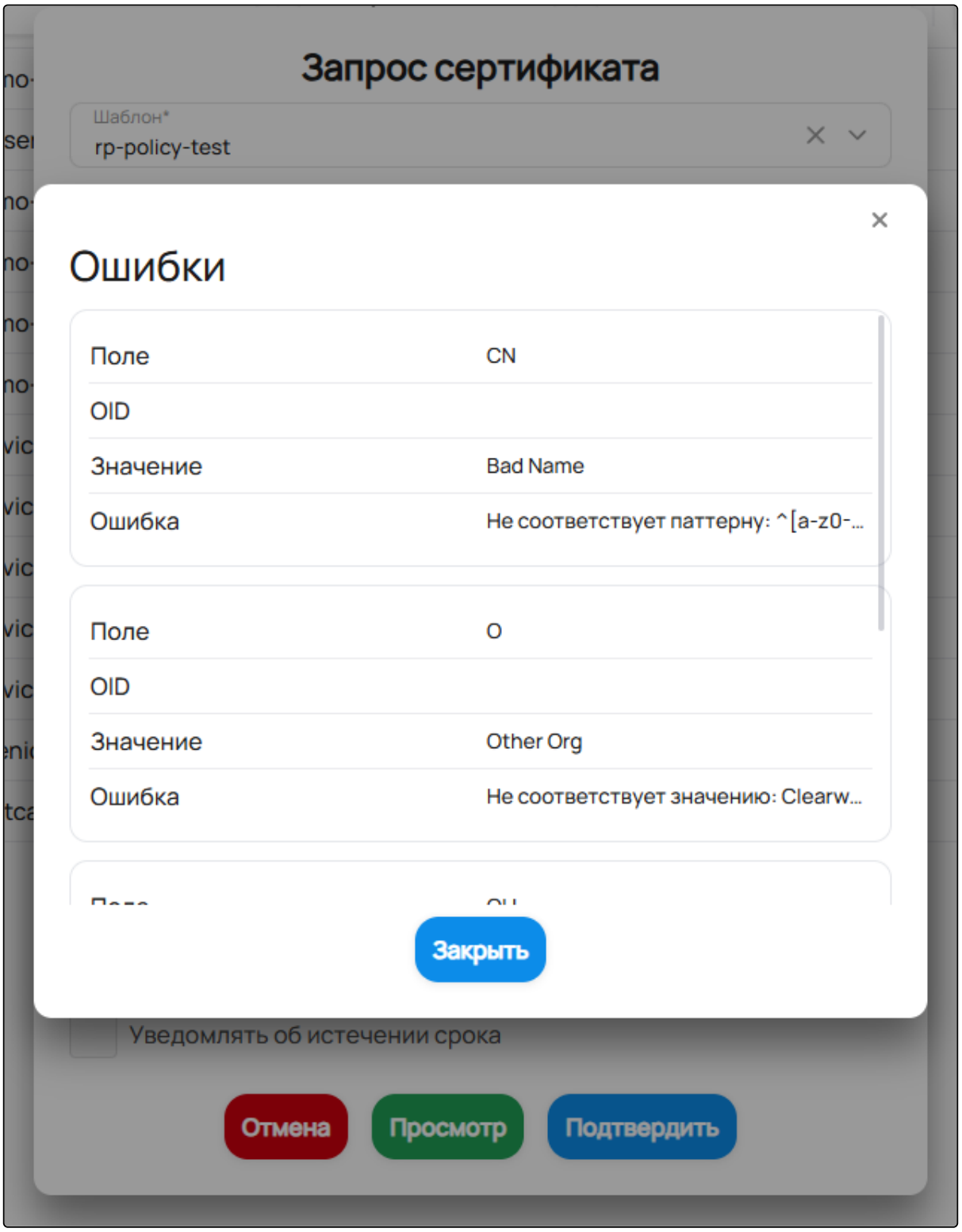
6.6.4 Проверка запроса при выпуске

Запрос проверяется при нажатии **Подтвердить** в окне «Запрос сертификата» (см. «Запрос сертификата») и при выпуске из конструктора CSR-запросов. Если запрос соответствует всем ограничениям шаблона, сертификат выпускается как обычно.

Если хотя бы одно ограничение нарушено, сертификат не выпускается и открывается окно «Ошибки». В нём перечислены сразу все нарушения. Для каждого указаны:

- Поле: атрибут Subject (например, CN или O) или тип имени SAN (например, dns);
- OID: объектный идентификатор атрибута, если ограничение задано через него;
- Значение: значение из запроса; пусто, если атрибут в запросе отсутствует;
- Ошибка: причина отказа.

Текст ошибки	**Причина**
Не соответствует значению: <требуемое значение>	Значение в запросе не совпадает с требуемым значением
Не соответствует паттерну: <шаблон glob или регулярное выражение>	Значение в запросе не подходит под шаблон glob или регулярное выражение
Обязательно к заполнению	Обязательный атрибут или имя SAN отсутствует в запросе
Неизвестная ошибка!	Причина отказа не распознана. Обратитесь к администратору



34 Окно «Ошибки» при нарушении ограничений шаблона

Нажмите **Закрыть**. Исправьте запрос (сформируйте CSR с допустимыми значениями) или выберите другой шаблон и отправьте запрос заново.

Проверку выполняет и сам центр сертификации: запрос, нарушающий ограничения шаблона, отклоняется, даже если он поступил не через Контрольную панель.

6.7 Справочник значений

6.7.1 Типы и размеры ключей

Тип ключа	Допустимые размеры
RSA	1024, 2048, 4096
ECDSA	256, 384, 521
Ed25519	256
GOST2001	256
GOST2012	256, 512

6.7.2 Значения Key Usage

В списке Key Usage интерфейса значения подписаны с заглавной буквы (DigitalSignature, CRLSign и т. д.); в реестре они выводятся в исходном написании.

Значение	Назначение
digitalSignature	Проверка цифровой подписи, например при аутентификации по TLS
nonRepudiation	Защита от отказа от авторства операции
keyEncipherment	Шифрование ключей другим ключом
dataEncipherment	Прямое шифрование данных
keyAgreement	Выработка общего секретного ключа сторонами
keyCertSign	Подпись других сертификатов

cRLSign	Подпись списков отзыва
encipherOnly	Закрытый ключ используется только для шифрования
decipherOnly	Закрытый ключ используется только для расшифровки
critical	Расширение Key Usage помечается как критичное

6.7.3 Значения Extended Key Usage

Значение	OID	Назначение
serverAuth	1.3.6.1.5.5.7.3.1	Аутентификация серверов (например, HTTPS)
clientAuth	1.3.6.1.5.5.7.3.2	Аутентификация клиентов (например, TLS-клиентов)
codeSigning	1.3.6.1.5.5.7.3.3	Подпись программного обеспечения
emailProtection	1.3.6.1.5.5.7.3.4	Защита электронной почты (S/MIME)
ipsecEndSystem	1.3.6.1.5.5.7.3.5	Оконечная система IPsec
ipsecTunnel	1.3.6.1.5.5.7.3.6	Туннель IPsec
ipsecUser	1.3.6.1.5.5.7.3.7	Пользователь IPsec
timeStamping	1.3.6.1.5.5.7.3.8	Создание меток времени
OCSPSigning	1.3.6.1.5.5.7.3.9	Подпись ответов OCSP
ipsecIKE	1.3.6.1.5.5.7.3.17	Обмен ключами IKE в IPsec
msCodeInd	1.3.6.1.4.1.311.2.1.21	Подпись кода Authenticode (индивидуальная)
msCodeCom	1.3.6.1.4.1.311.2.1.22	Подпись кода Authenticode (коммерческая)

msCTLSign	1.3.6.1.4.1.311.10.3.1	Подпись списков доверия (CTL)
msEFS	1.3.6.1.4.1.311.10.3.4	Шифрование файловой системы (EFS)
secureShellClient	1.3.6.1.5.5.7.3.21	Аутентификация SSH-клиента
msSmartcardLogin	1.3.6.1.4.1.311.20.2.2	Вход по смарт-карте
pkInitKDC	1.3.6.1.5.2.3.5	Центр распределения ключей Kerberos (PKINIT)

6.7.4 Значения Authority Key Identifier

Значение	Что включается в расширение
none	Расширение Authority Key Identifier не добавляется в сертификат
issuer	Имя и серийный номер сертификата издателя
issuer:always	Сведения об издателе включаются всегда
keyid	Идентификатор ключа издателя
keyid:always	Идентификатор ключа включается обязательно, независимо от наличия другой информации

В новом шаблоне по умолчанию выбрано keyid; при импорте шаблона без этого параметра подставляются keyid и issuer.

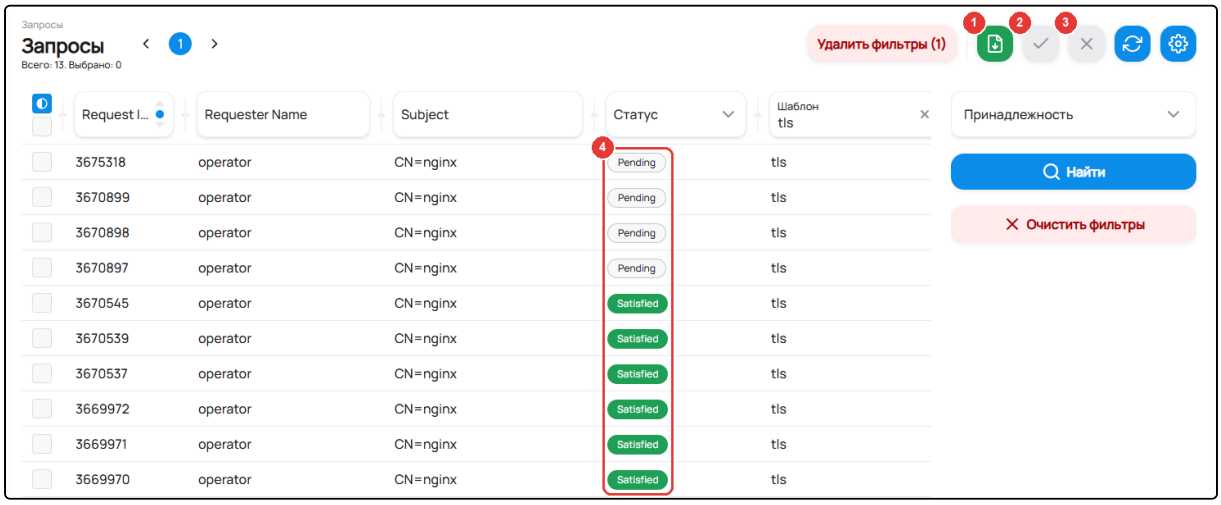
7 Запросы и согласование выпуска

Глава описывает работу с запросами на выпуск сертификатов: просмотр реестра и карточки запроса, одобрение и отклонение запросов.

Согласование выпуска служит точкой контроля: пока запрос не одобрен, сертификат по нему не выпускается. Согласования требуют шаблоны с признаком «Создавать запрос на выпуск» (см. «Блок „Дополнительно“»).

7.1 Реестр запросов

Раздел «Запросы» содержит реестр запросов на выпуск сертификатов (CSR в формате PKCS#10). Для доступа нужно право `rleMiniCAReqList-r`. Общие приёмы работы с реестром описаны в главе «Общие элементы интерфейса».



35 Реестр запросов

На рисунке: **1**, **2**, **3** кнопки реестра (см. таблицу кнопок ниже); **4** статусы запросов.

Столбец	Что показывает	Фильтр
Request ID	Идентификатор запроса. Сортировка	Число
Requester Name	Инициатор запроса	Текст
Subject	Subject из запроса	Текст
Статус	Текущий статус (см. «Статусы запроса»)	Список
Шаблон	Шаблон выпуска	Текст

Common Name	Common Name из запроса	Текст
Тип ключа	RSA, ECDSA, Ed25519, GOST2001 или GOST2012	Список
Размер ключа	Длина ключа, бит	Число
Причина отклонения	Причина, указанная при отклонении	Текст
Создан	Дата и время создания запроса. Сортировка	Период
Сертификат	Ссылка «Посмотреть сертификат» на выпущенный сертификат	Нет
Скачать запрос	Значок скачивания файла CSR	Нет

Столбцы SAN DNS, SAN IP, SAN URI, SAN Email и SAN Other Name по умолчанию скрыты.

№	Кнопка (значок)	Что делает
1	Выгрузка отчёта (зелёный значок файла)	Выгружает отчёт в файл Excel (см. «Выгрузка отчёта в файл»)
2	**Одобрение запросов** (галочка)	Одобряет отмеченные запросы в статусе Pending (см. «Групповое одобрение и отклонение»). Видна при праве `rleMiniCAReqApprove-w`
3	**Отклонение запросов** (крестик)	Отклоняет отмеченные запросы в статусе Pending. Видна при праве `rleMiniCAReqApprove-w`

7.1.1 Статусы запроса

Статус	Что означает	Что можно сделать
Pending	Запрос ожидает согласования	Одобрить или отклонить (право `rleMiniCAReqApprove-w`)

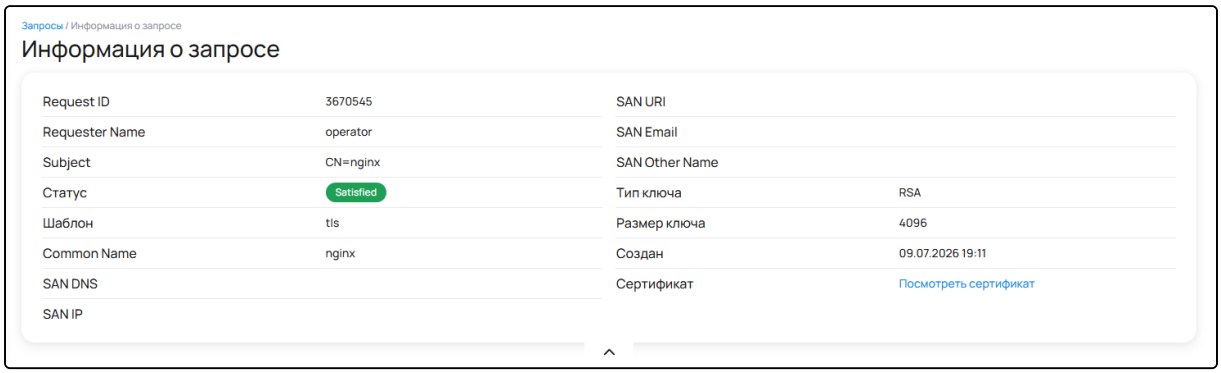
Satisfied	Сертификат выпущен	Перейти к сертификату по ссылке «Посмотреть сертификат»
Rejected	Запрос отклонён; причина указана в поле «Причина отклонения»	Действий нет
Erroneous	При выпуске произошла ошибка, сертификат не выпущен; подробности смотрите в журнале событий по Request ID	Действий нет

Если в шаблоне включён признак «Создавать запрос на выпуск», новый запрос получает статус Pending и ждёт решения. Иначе сертификат выпускается сразу, и запрос получает статус Satisfied или, при ошибке, Erroneous. Статусы Satisfied, Rejected и Erroneous считаются итоговыми.

7.1.2 Карточка запроса

Чтобы открыть карточку «Информация о запросе», щёлкните строку запроса в реестре. В карточке выводятся поля Request ID, Requester Name, Subject, Статус, Шаблон, Common Name, SAN DNS, SAN IP, SAN URI, SAN Email, SAN Other Name, Тип ключа, Размер ключа и Создан. Поле «Сертификат» со ссылкой «Посмотреть сертификат» выводится, только если сертификат выпущен; поле «Причина отклонения» выводится, только если запрос отклонён.

При проверке убедитесь, что Subject и Common Name соответствуют узлу или службе, для которых запрашивается сертификат, а перечень SAN охватывает все имена и адреса, под которыми узел должен быть доступен.

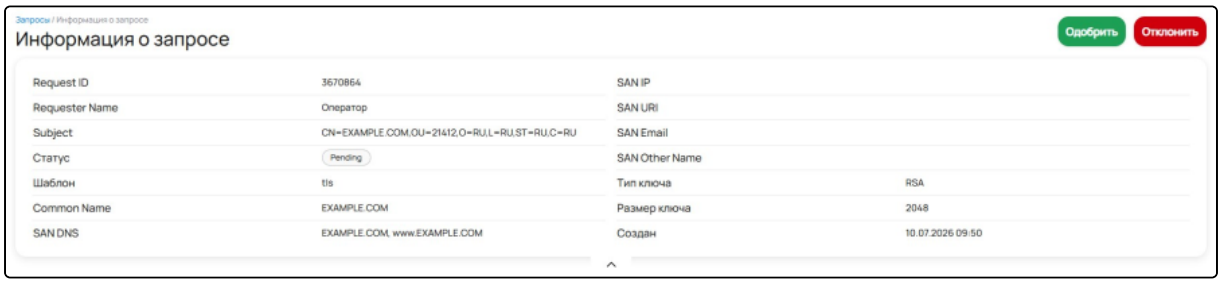


36 Карточка «Информация о запросе»

Файл CSR скачивается из столбца «Скачать запрос» реестра; в карточке такой кнопки нет.

7.2 Одобрение и отклонение запросов

Кнопки **Одобрить** и **Отклонить** выводятся в карточке запроса в статусе Pending при наличии права `rleMiniCAReqApprove-w`.



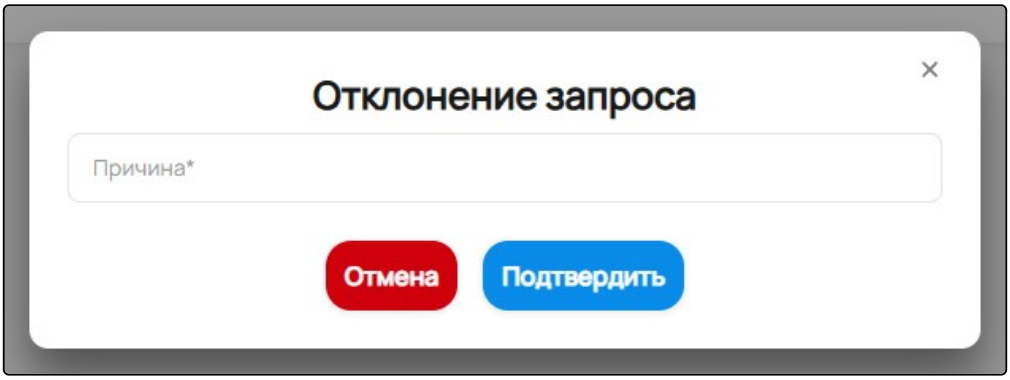
37 Запрос в статусе Pending с кнопками одобрения и отклонения

Чтобы одобрить запрос:

1. Нажмите **Одобрить**.
2. В окне «Подтверждение» с вопросом «Вы действительно хотите одобрить запрос?» нажмите **Да**. **Нет** закрывает окно без действия.
3. Появится сообщение «Запрос одобрен». Запрос получит итоговый статус, а при выпуске сертификата в карточке появится ссылка «Посмотреть сертификат».

Чтобы отклонить запрос:

1. Нажмите **Отклонить**.
2. В окне «Отклонение запроса» заполните обязательное поле «Причина»: введите текст или выберите вариант из списка («Некорректные параметры запроса», «Несоответствие политике»). Причина сохранится в карточке запроса и объяснит, почему в выпуске отказано.
3. Нажмите **Подтвердить**. Появится сообщение «Запрос отклонен!», запрос перейдёт в статус Rejected. **Отмена** закрывает окно без действия.



38 Окно «Отклонение запроса»

7.2.1 Групповое одобрение и отклонение

Несколько запросов можно одобрить или отклонить за одно действие. Нужно право `rleMiniCAReqApprove-w`.

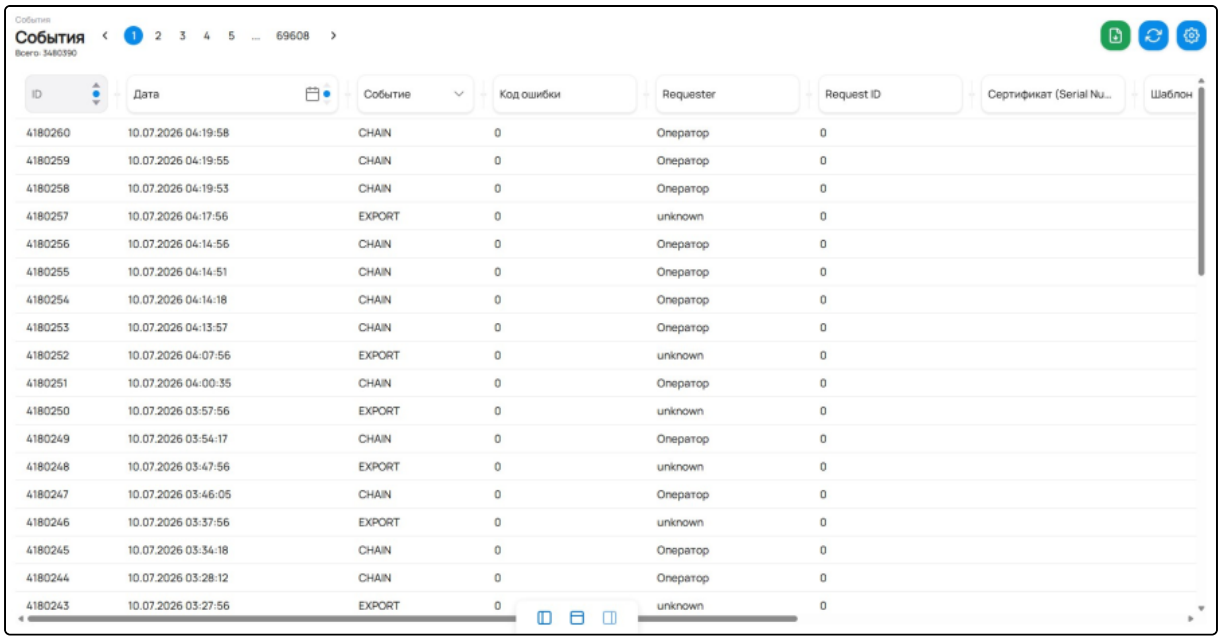
1. В реестре отметьте запросы флажками. Удобно сначала задать фильтр «Статус» = Pending.

2. Нажмите над таблицей **Одобрение запросов** (галочка) или **Отклонение запросов** (крестик). Пока среди отмеченных нет запроса в статусе Pending, кнопки неактивны.
3. Проверьте окно: в нём показаны только отмеченные запросы в статусе Pending и их число («Всего: N»); остальные отмеченные запросы пропускаются.
4. Для одобрения нажмите **Одобрить**. Для отклонения заполните обязательное поле «Причина» (одна причина для всех запросов) и нажмите **Отклонить**. **Отменить** закрывает окно без действия.

Результат выводится сообщением «Запросы одобрены! Количество: N» или «Запросы отклонены! Количество: N». Если не удалось обработать ни один запрос, выводится «Не удалось одобрить запросы» или «Не удалось отклонить запросы».

8 Журнал событий

Раздел «События» содержит журнал операций центра сертификации. По нему видно, кто выполнил операцию, когда и с каким результатом: журнал используется для аудита, расследования инцидентов и подтверждения факта выпуска или отзыва сертификата. Для доступа нужно право `rleMiniCAEventList-r`. Общие приёмы работы с реестром описаны в главе «Общие элементы интерфейса»; боковой панели фильтров и флажков выбора в журнале нет.



39 Журнал «События»

Столбец	Что показывает	Фильтр
ID	Порядковый номер записи. Сортировка	Нет
Дата	Дата и время операции. Сортировка	Период
Событие	Тип операции (см. таблицу ниже)	Список
Код ошибки	Результат операции: 0 при успешном выполнении, иначе код ошибки. Расшифровка кодов приведена в Руководстве администратора	Текст
Requester	Инициатор операции: учётная запись или программный клиент	Текст
Request ID	Номер запроса, к которому относится операция	Число

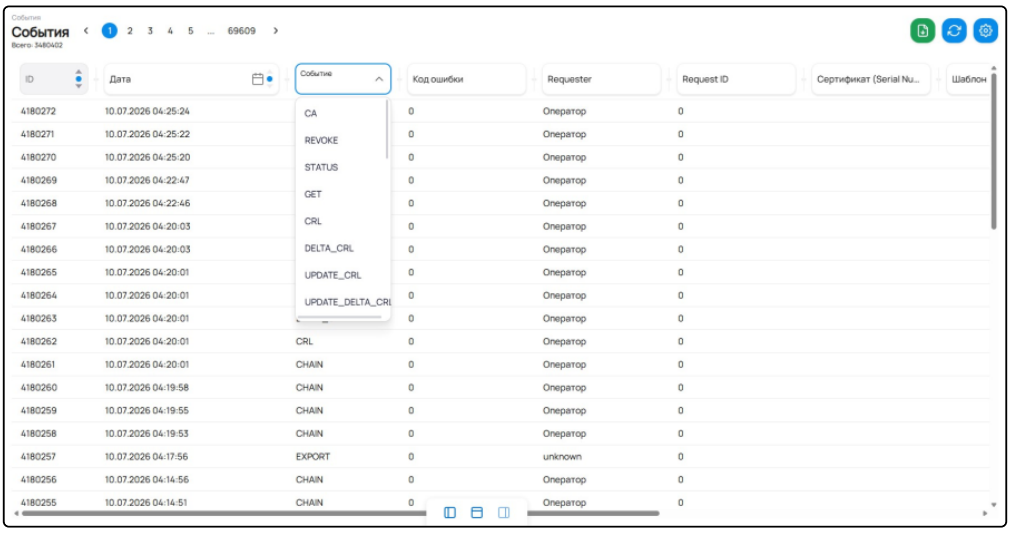
Сертификат (Serial Number)	Серийный номер сертификата	Текст
Шаблон	Шаблон сертификата	Текст
Номер CRL	Номер списка отзыва	Текст
Сообщение криптопровайдера	Сообщение криптографической библиотеки, например текст ошибки	Нет
Дополнительная информация	Параметры исходного обращения к ЦС	Нет

Строки журнала не открываются в отдельной карточке: подробности операции смотрите в столбцах «Сообщение криптопровайдера» и «Дополнительная информация».

Типы событий (значения фильтра «Событие»):

Событие	**Операция**
CA	Выпуск сертификата
CA_APPROVE	Одобрение запроса на выпуск
CA_REJECT	Отклонение запроса на выпуск
REVOKE	Отзыв сертификата
REPAIR	Восстановление сертификата после отзыва с причиной CertificateHold
STATUS	Проверка статуса сертификата
GET	Получение сертификата из базы данных ЦС
FIND	Поиск сертификатов
EXPORT	Массовая выгрузка сертификатов
DELETE	Удаление сертификата и связанного запроса из базы данных
CSR	Получение запроса на сертификат (CSR)

CHAIN	Получение цепочки сертификатов ЦС
CRL	Получение полного списка отзыва
DELTA_CRL	Получение Delta CRL
UPDATE_CRL	Обновление полного списка отзыва
UPDATE_DELTA_CRL	Обновление Delta CRL
TEMPLATES	Получение списка шаблонов
GET_TEMPL	Получение параметров шаблона
ADD_TEMPL	Создание шаблона
DEL_TEMPL	Удаление шаблона
MAKE_JWT	Выпуск токена JWT программного клиента
GET_JWT	Получение токена JWT
RENEW_JWT	Продление срока действия токена JWT
REVIVE_JWT	Повторная активация истёкшего токена JWT
REVOKE_JWT	Отзыв токена JWT
REPAIR_JWT	Восстановление отозванного токена JWT
DEL_JWT	Удаление токена JWT из базы данных
PING	Проверка связи с ЦС
STAT	Получение статистики ЦС



40 Фильтр по столбцу «Событие»

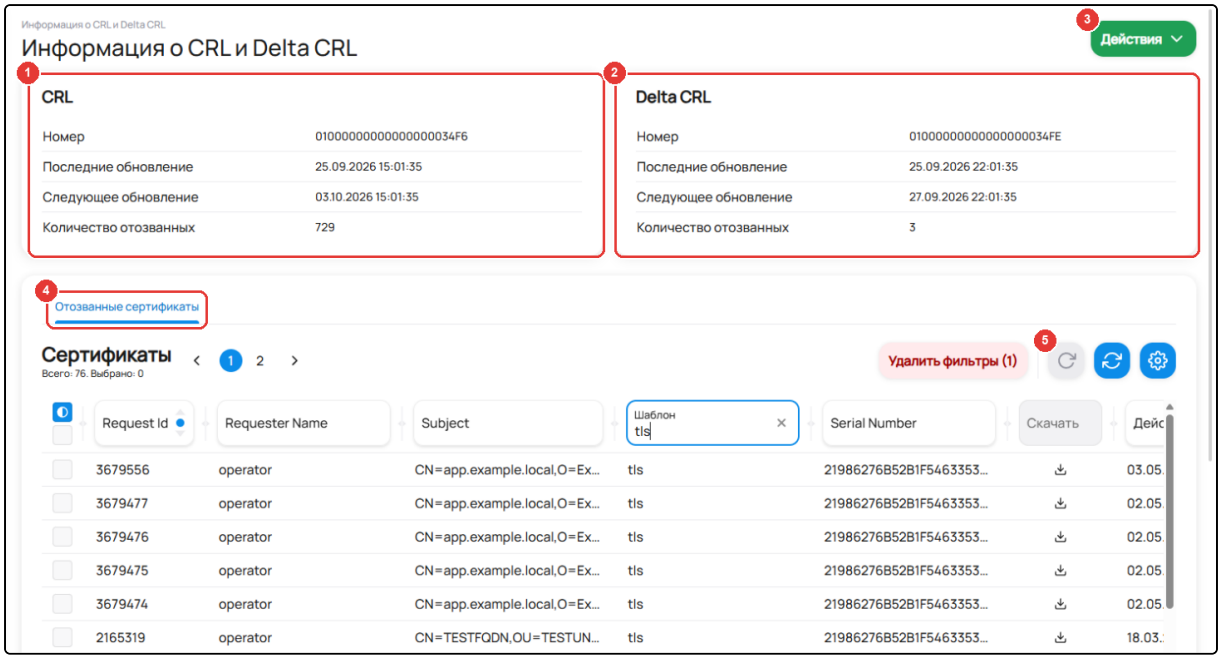
9 Списки отзыва CRL и Delta CRL

Страница отражает текущее состояние полного списка отзыва (CRL) и Delta CRL и позволяет скачать или обновить их. Списки отзыва нужны, чтобы участники обмена могли убедиться, что сертификат не был досрочно отозван (например, при компрометации закрытого ключа), и вовремя прекратить доверие к нему.

Списки отзыва отражают состояние на момент формирования и публикуются по расписанию (см. поле «Следующее обновление»). Чтобы проверить статус одного сертификата без ожидания публикации CRL, используйте протокол OCSP (см. «Проверка статуса по протоколу OCSP»).

9.1 Страница «Информация о CRL и Delta CRL»

Откройте раздел «Информация о CRL» (право `rleMiniCACRL-r`). На странице «Информация о CRL и Delta CRL» выводятся карточки «CRL» и «Delta CRL», а под ними расположена вкладка «Отозванные сертификаты».



41 Страница «Информация о CRL и Delta CRL»

На рисунке: **1** карточка «CRL»; **2** карточка «Delta CRL»; **3** меню «Действия»; **4** вкладка «Отозванные сертификаты»; **5** кнопка «Восстановить выбранные сертификаты».

Поле карточки	Что показывает
Номер	Номер текущей версии списка (шестнадцатеричное число). При каждом обновлении увеличивается

Последнее обновление	Дата и время формирования текущей версии
Следующее обновление	Плановое время следующего обновления
Количество отозванных	Число сертификатов в списке

9.1.1 Вкладка «Отозванные сертификаты»

На вкладке перечислены все отозванные сертификаты из базы данных ЦС, включая не входящие в текущий CRL. Для просмотра нужно право `rleMiniCACertList-r`. Общие приёмы работы с таблицей описаны в главе «Общие элементы интерфейса»; выгрузки отчёта и боковой панели на вкладке нет.

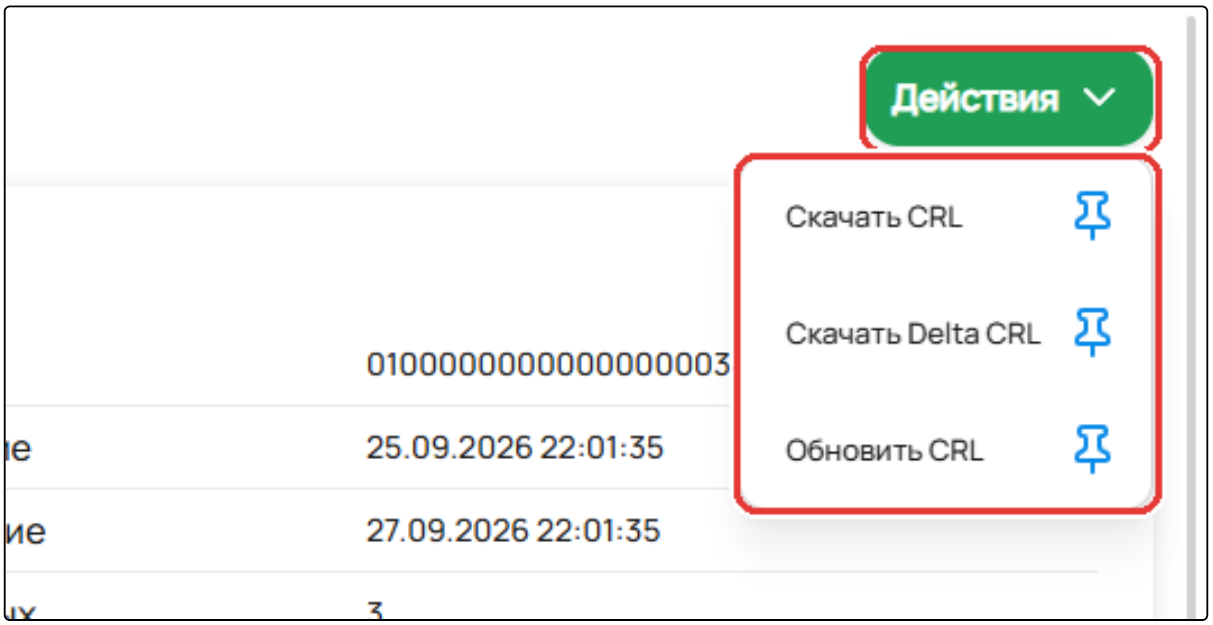
Видимые по умолчанию столбцы: Request Id, Requester Name, Subject, Шаблон, Serial Number, Скачать (значок скачивания сертификата), Действителен до, Действителен с. Среди скрытых по умолчанию столбцов есть «В CRL» (входит ли сертификат в список отзыва) и «Причина отзыва».

Щелчок по строке открывает карточку сертификата. Кнопка **Восстановить выбранные сертификаты** (круговая стрелка, право `rleMiniCACertUnRev-w`) работает так же, как в реестре сертификатов (см. «Восстановление сертификата»).

9.2 Действия со списками отзыва

Действия собраны в меню **Действия** в правом верхнем углу страницы (см. «Меню „Действия“ и закрепление действий»).

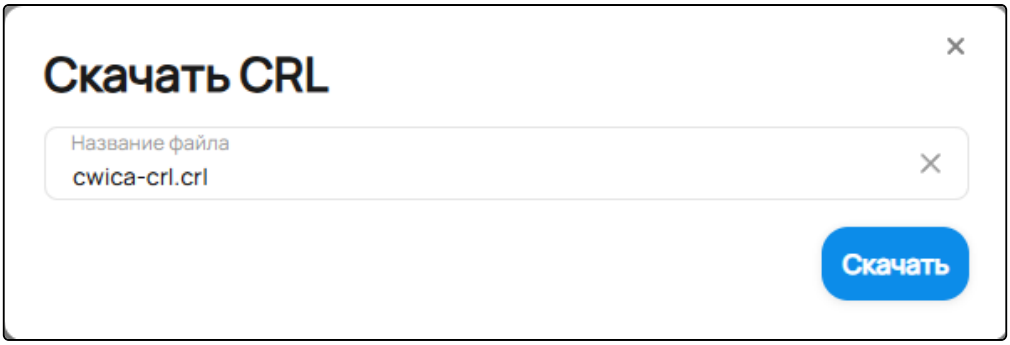
Пункт	Что делает	Право
Скачать CRL	Сохраняет текущий полный список отзыва в файл	`rleMiniCACRL-r`
Скачать Delta CRL	Сохраняет текущий Delta CRL в файл	`rleMiniCACRL-r`
Обновить CRL	Формирует новую версию списков и при необходимости публикует её	`rleMiniCACRL-w`



42 Меню «Действия» на странице «Информация о CRL и Delta CRL»

9.2.1 Скачивание CRL и Delta CRL

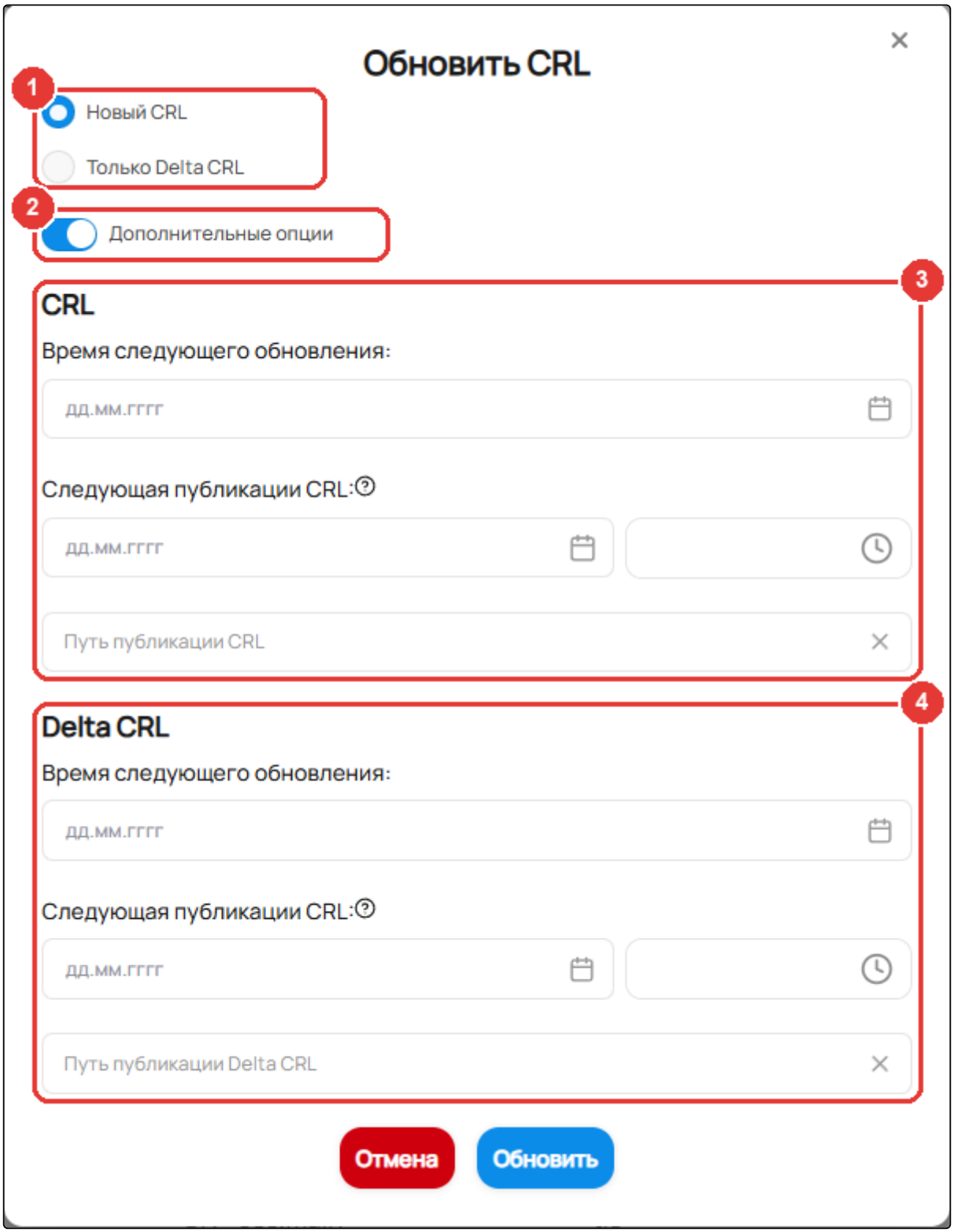
1. Выберите «Действия» → «Скачать CRL» или «Скачать Delta CRL».
2. В поле «Название файла» при необходимости измените имя. По умолчанию подставляется имя из настроек Контрольной панели.
3. Нажмите **Скачать**. Крестик закрывает окно без скачивания.



43 Окно «Скачать CRL»

9.2.2 Обновление CRL

1. Выберите «Действия» → «Обновить CRL».
2. Выберите режим и при необходимости задайте дополнительные параметры.
3. Нажмите **Обновить**. **Отмена** закрывает окно без действия.



44 Окно «Обновить CRL» с дополнительными опциями

На рисунке: **1** режим обновления; **2** переключатель «Дополнительные опции»; **3** сроки и путь публикации CRL; **4** сроки и путь публикации Delta CRL.

Поле	Что указать
Новый CRL / Только Delta CRL	«Новый CRL» (по умолчанию) обновляет полный список и Delta CRL; «Только Delta CRL» обновляет только разностный список
Дополнительные опции	Включите, чтобы задать сроки и пути публикации. Если опции выключены, сроки берутся из настроек ЦС
CRL → Время следующего обновления	Дата следующего обновления CRL; срок считается в целых днях от текущего момента. Если дата не выбрана, применяется срок из настроек ЦС. Блок выводится только в режиме «Новый CRL»
CRL → Следующая публикация CRL	Дата и время следующей публикации. Промежуток между следующей публикацией и окончанием действия CRL называется интервалом перекрытия: в это время действуют и старый, и новый список
CRL → Путь публикации CRL	Путь, по которому нужно опубликовать CRL после обновления. Если поле пустое, список только обновляется
Delta CRL → Время следующего обновления, Следующая публикация, Путь публикации Delta CRL	То же для Delta CRL

По результату выводятся сообщения «CRL обновлен», «CRL опубликован», «Delta CRL обновлен», «Delta CRL опубликован» или текст ошибки. После обновления увеличивается «Номер» и меняются поля «Последнее обновление» и «Следующее обновление».

Важно

Введённые пути публикации запоминаются в браузере и подставляются при следующем открытии окна. Если в этот раз публикация не нужна, очистите поля путей.

10 Самодиагностика

Clearway CA сообщает основные показатели своего состояния двумя способами: на странице «Статистика ЦС» Контрольной панели и по команде mclient stat. По этим показателям можно убедиться, что служба центра сертификации работает, узнать, сколько сертификатов и списков отзыва выпущено за всё время, и оценить, сколько сертификатов, запросов и шаблонов сейчас хранится в базе данных ЦС.

Способы различаются тем, когда рассчитываются показатели. Страница «Статистика ЦС» показывает результат последнего расчёта, который выполняется в фоне по расписанию. Команда mclient stat считает показатели в момент вызова. Поэтому, если после расчёта по расписанию выпускались или отзывались сертификаты, значения на странице и в выводе команды могут различаться.

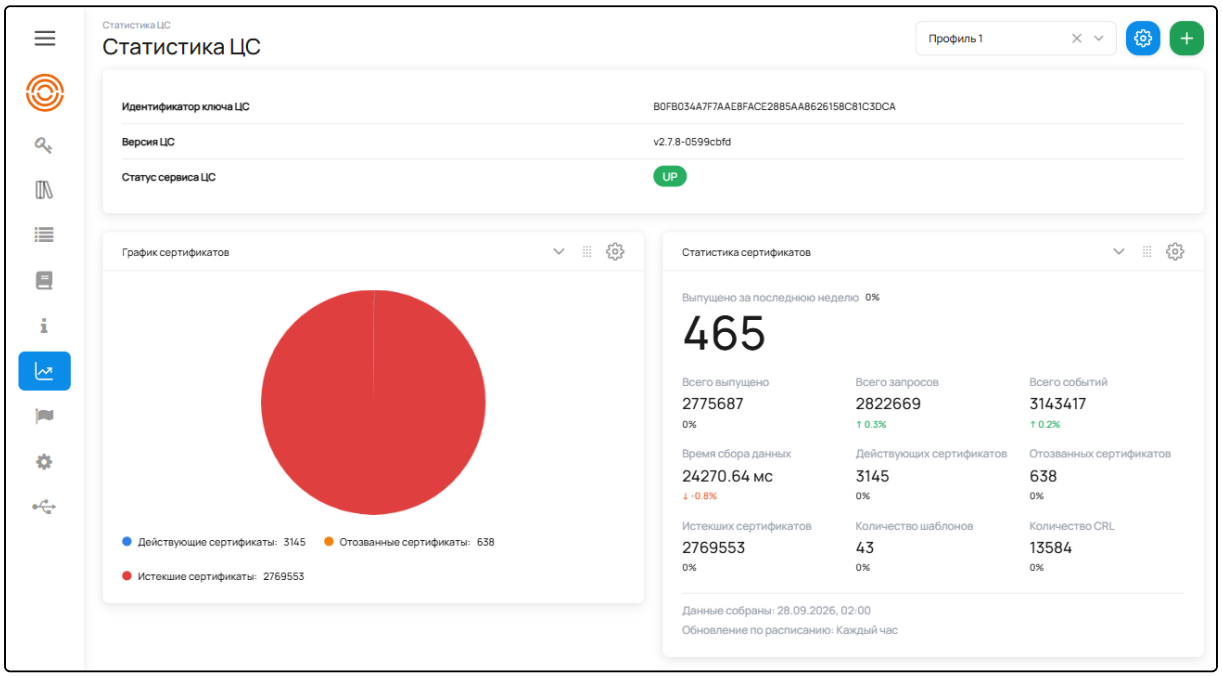
Соответствие показателей на странице и в выводе команды:

Показатель	**Страница «Статистика ЦС»**	**Вывод mclient stat**
Общее количество выпущенных сертификатов (сколько сертификатов ЦС выпустил за всё время работы)	Всего выпущено	`AllIssuedCertificates`
Общее количество сертификатов в базе данных ЦС	Отдельным значением не выводится; состав показывает виджет «График сертификатов»	Сумма `validCnt`, `revokedCnt`, `expiredCnt` и `unknownCnt`
Действующие сертификаты в базе данных	Действующих сертификатов	`validCnt`
Отозванные сертификаты в базе данных	Отозванных сертификатов	`revokedCnt`
Сертификаты с истёкшим сроком действия в базе данных	Истекших сертификатов	`expiredCnt`
Сертификаты, которые не относятся ни к одной из трёх групп выше (статус UNKNOWN)	Не выводится	`unknownCnt`
Запросы на выпуск сертификатов в базе данных	Всего запросов	`csrCnt`
Выпущенные списки отзыва CRL	Количество CRL	`crlCnt`

Шаблоны сертификатов	Количество шаблонов	`templCnt`
Записи журнала событий	Всего событий	`evtCnt`
Токены JWT программных клиентов, учтённые в базе данных ЦС	Не выводится	`jwtCnt`
Сертификаты, выпущенные за последнюю неделю	Выпущено за последнюю неделю	Не выводится
Время подсчёта показателей	Время сбора данных (в миллисекундах)	`dt`

10.1 Страница «Статистика ЦС»

Пункт меню «Статистика ЦС» отображается пользователю с правом `rleMiniCAConfig-r`. Страница показывает показатели ЦС, выбранного на странице «Настройки → Конфигурация» в карточке «Выбор Clearway CA» (см. «Текущий ЦС»).



45 Страница «Статистика ЦС»

Показатели загружаются при открытии страницы. Сам расчёт выполняется в фоне по расписанию, потому что на большой базе данных подсчёт занимает десятки секунд. Открытие страницы новый расчёт не запускает: показывается результат последнего расчёта. Чтобы увидеть результат более позднего расчёта, откройте страницу заново.

Виджет	Что показывает
Информация о ЦС (верхний блок без заголовка)	Идентификатор ключа ЦС (по нему можно убедиться, что показатели относятся к нужному ЦС); Версия ЦС; Статус сервиса ЦС: UP (зелёный), если служба ЦС работает, DOWN (красный), если не работает. Сведения приходят вместе с результатом расчёта: пока статистика не собрана, блок пуст
График сертификатов	Круговая диаграмма сертификатов в базе данных ЦС: действующие, отозванные и истекшие. Точные количества указаны в подписях под диаграммой
Статистика сертификатов	Крупным числом выводится «Выпущено за последнюю неделю», ниже перечислены остальные показатели (см. таблицу соответствия выше). Внизу указаны «Данные собраны» (дата и время последнего расчёта) и «Обновление по расписанию» (расписание расчёта)

Рядом с каждым значением указано изменение в процентах: стрелка вверх зелёным обозначает рост, стрелка вниз красным обозначает снижение, 0% без стрелки означает, что значение не изменилось.

Вместо показателей в виджетах «График сертификатов» и «Статистика сертификатов» может выводиться сообщение:

Сообщение	Что означает
Статистика ещё не собрана	Результатов расчёта пока нет. Ниже указано расписание: показатели появятся после ближайшего расчёта
Ошибка загрузки данных	Контрольной панели не удалось получить показатели. Обновите страницу; если ошибка повторяется, обратитесь к администратору

10.1.1 Настройка вида страницы

Набор и расположение виджетов можно настроить под себя. Настройки хранятся в браузере: они действуют только на этом компьютере и в этом браузере, не видны другим пользователям и не влияют на значения показателей.

Элемент	Что делает
Список профилей (справа вверху)	Выбирает профиль (сохранённую раскладку виджетов)

Шестерёнка рядом со списком	Меню «Создать профиль», «Редактировать профиль», «Удалить профиль»
«+» («Добавить виджет»)	Открывает форму «Создать виджет»
Стрелка в заголовке виджета	Сворачивает и разворачивает виджет
Значок из точек в заголовке виджета	Перетащите за него виджет на другое место
Шестерёнка в заголовке виджета	«Редактировать виджет» или «Удалить виджет» (после подтверждения виджет удаляется из всех профилей)

У блока «Информация о ЦС» нет заголовка: его нельзя свернуть, переместить, изменить или удалить.

Форма профиля («Создать профиль» / «Изменить профиль»):

Поле	**Что указать**
Название*	Имя профиля в списке
Размер*	Маленький, Средний, Большой, Огромный или Максимальный. При выборе размера поле «Максимальное количество колонок» заполняется значением по умолчанию
Максимальное количество колонок*	Сколько виджетов помещается в ряд; не меньше значения по умолчанию для выбранного размера

Продолжить сохраняет профиль (сообщение «Профиль сохранен.»). **Отменить** закрывает форму; если данные изменены, появится вопрос «Закрытие окна приведет к потере введённых данных. Закрыть окно?». Новый профиль создаётся пустым: добавьте в него виджеты кнопкой «+». При удалении профиля или виджета запрашивается подтверждение, затем выводится «Профиль удален.» или «Виджет удален.».

Форма виджета («Создать виджет» / «Изменить виджет») состоит из двух шагов: на шаге «Основное» укажите «Название*» и выберите «Виджет*» («Информация о ЦС», «График сертификатов» или «Статистика сертификатов»); на шаге «Данные виджета» дополнительных параметров у этих виджетов нет. **Продолжить** переходит к следующему шагу и на последнем шаге сохраняет виджет, **Назад** возвращает на предыдущий шаг, **Отменить** закрывает форму. Новый виджет добавляется отдельным рядом внизу профиля.

10.2 Команда mclient stat

Команда mclient stat запрашивает показатели у центра сертификации и выводит их сразу, без расписания. Её удобно использовать в сценариях проверки и в системах мониторинга.

Команду выполняют на сервере с установленной утилитой mclient, как и остальные команды mclient (см. «Работа через командную строку (mclient)»): укажите путь к файлу конфигурации клиента в переменной MCLIENT_CONF и выполните из каталога утилиты:

```
./mclient stat
```

Команда выводит одну строку со временем, уровнем сообщения INFO, названием операции minica stat и показателями в виде пар имя=значение. Пример вывода:

```
2026/09/28 14:25:42.594 INFO minica stat errno=0 validCnt=11 revokedCnt=3 expiredCnt=0
unknownCnt=0 AllIssuedCertificates=14 csrCnt=14 crlCnt=21 templCnt=5 jwtCnt=3
evtCnt=465 dt=12.102487ms
```

Значение errno=0 означает, что показатели получены без ошибок. Назначение остальных полей приведено в таблице соответствия в начале главы. Поле dt показывает, сколько времени заняло получение показателей. В примере общее количество сертификатов в базе данных равно 11 + 3 + 0 + 0 = 14.

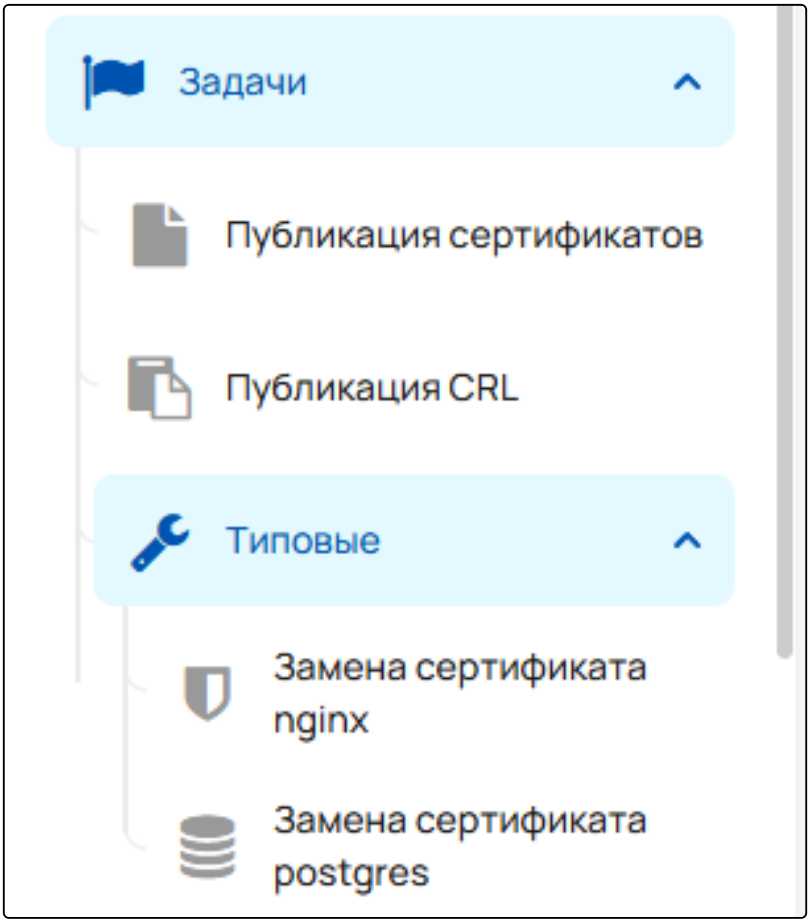
Для обработки вывода программами используйте формат JSON:

```
./mclient -log-format json stat
```

В этом формате команда выводит те же поля в виде объекта JSON, а время подсчёта dt указывается в наносекундах.

11 Задачи

Раздел «Задачи» объединяет задачи публикации сертификатов и списков отзыва, резервное копирование ЦС и типовые сценарии обслуживания. Пункт «Задачи» и его подпункты видны по правам, указанным в таблице левого меню (см. «Интерфейс и навигация»).



46 Меню «Задачи» с подпунктами

11.1 Задачи публикации

Публикацию по расписанию cron выполняет сервис публикации: он выгружает выпущенные сертификаты в каталоги LDAP (Active Directory или Samba), а списки отзыва выгружает в каталог на сервере, на удалённый сервер по SCP или в каталог LDAP. Благодаря этому клиенты и серверы получают актуальные сертификаты и сведения об отзыве без ручных действий.

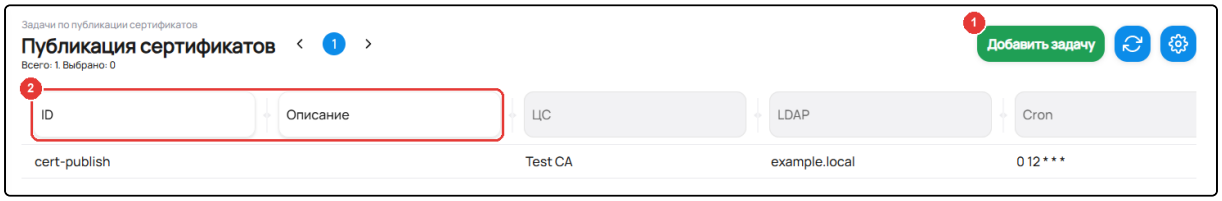
1. В левом меню откройте «Задачи» → «Публикация сертификатов» или «Задачи» → «Публикация CRL».
2. Откроется список задач: «Публикация сертификатов» или «Публикация CRL и Delta CRL».

Столбец	Сертификаты	CRL	Что показывает

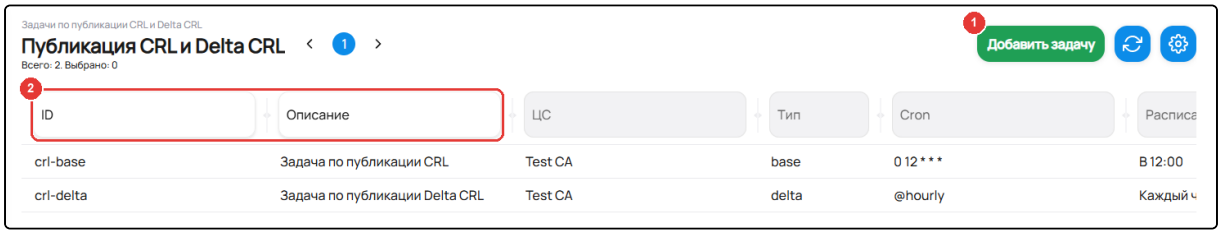
ID	да	да	Название (ключ) задачи
Описание	да	да	Комментарий к задаче
ЦС	да	да	ЦС, из которого берутся данные для публикации
LDAP	да	Нет	Адрес LDAP-сервера, в который публикуются сертификаты
Тип	Нет	да	base (полный CRL) или delta (Delta CRL)
Cron	да	да	Расписание в формате cron (время UTC), например 0 12 * * *
Расписание	да	да	То же расписание словами, например «В 12:00» или «Каждый час»

Полный список отзыва (тип base) содержит все действующие отметки об отзыве и публикуется реже. Delta CRL (тип delta) содержит только изменения с момента публикации полного списка, поэтому его публикуют чаще, например каждый час (@hourly).

Фильтровать списки можно по столбцам ID и Описание. Общие приёмы работы со списком описаны в главе «Общие элементы интерфейса». Чтобы открыть карточку задачи, щёлкните её строку.



47 Список задач публикации сертификатов



48 Список задач публикации CRL и Delta CRL

На рисунках: **1** кнопка «Добавить задачу»; **2** столбцы с фильтром (ID и Описание).

11.2 Управление задачами публикации

Задачи публикации хранятся в конфигурации сервиса публикации. В Контрольной панели их можно добавлять, изменять, запускать вне расписания и удалять, не редактируя файл конфигурации на сервере. Контрольная панель записывает изменения в конфигурацию сервиса после нажатия **Сохранить** и сообщает об этом уведомлением «Настройки сохранены».

> **Конфигурация, созданная при развёртывании**
>
> Конфигурация сервиса публикации создаётся при его развёртывании и может включать в себя задания публикации. Удалить такие задания или отредактировать через графический интерфейс невозможно.

Перед началом работы учтите:

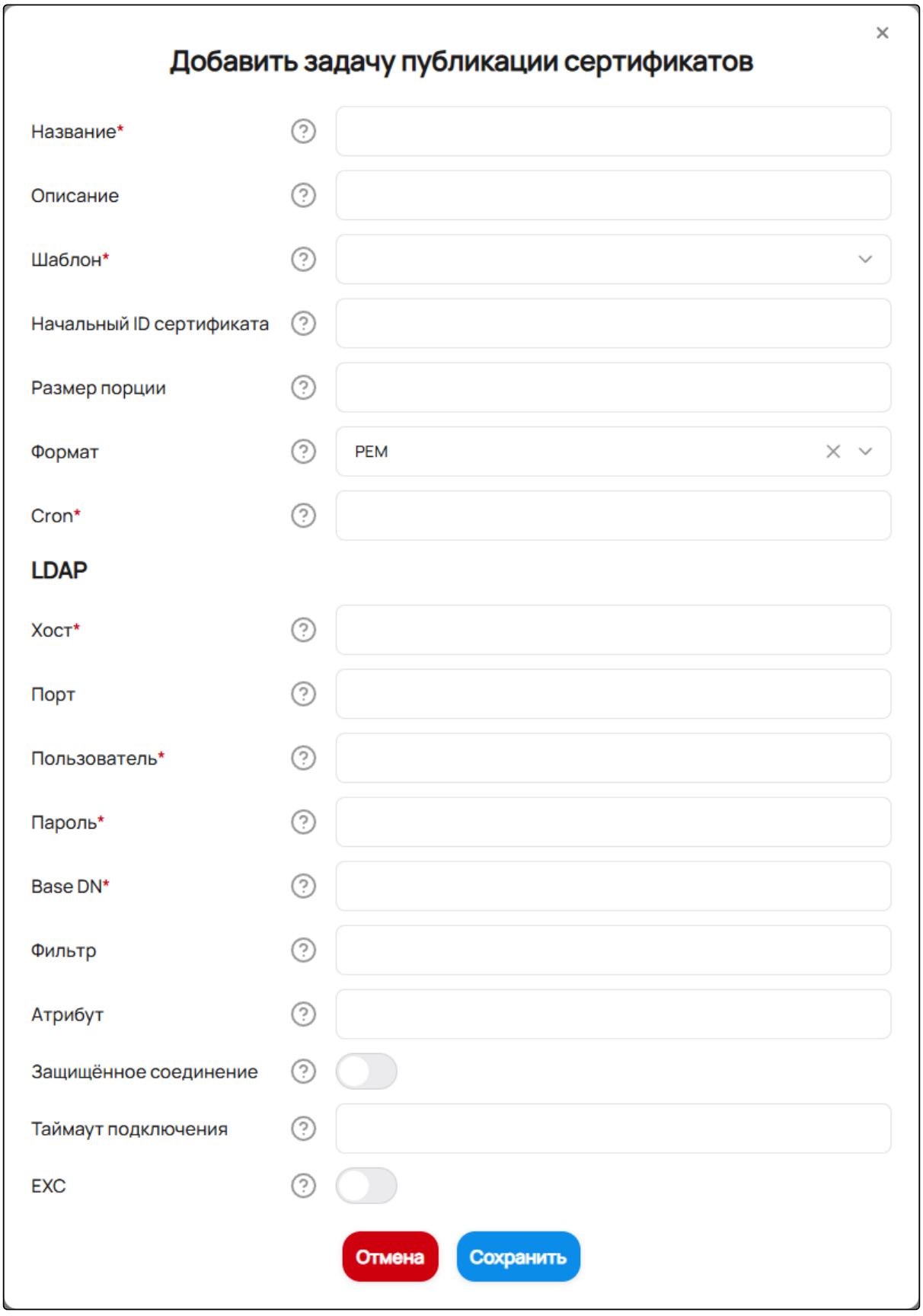
- кнопки **Добавить задачу**, **Изменить** и **Удалить** видны только пользователю с правом `rleMiniCAConfig-w`, а кнопка **Выполнить** видна всем, кому доступен раздел «Задачи»;
- в форме задачи нет поля выбора ЦС: задача создаётся для текущего ЦС (см. «Текущий ЦС»);
- если обязательное поле не заполнено или выражение cron записано неверно, задача не сохраняется, а ошибочные поля подсвечиваются;
- задача с уже существующим названием не создаётся: сервер отклонит сохранение, и появится сообщение об ошибке.

11.2.1 Добавление задачи публикации сертификатов

Задача публикации сертификатов по расписанию выгружает выпущенные сертификаты в каталог LDAP, например в Active Directory.

1. В левом меню откройте «Задачи» → «Публикация сертификатов».
2. Нажмите **Добавить задачу** в правом верхнем углу списка. Откроется форма «Добавить задачу публикации сертификатов».
3. Заполните параметры задачи и блок LDAP.
4. Нажмите **Сохранить**. **Отмена** закрывает форму без сохранения.

Задача сохранена, если появилось уведомление «Настройки сохранены», форма закрылась, а новая задача появилась в списке. Если сервер не принял задачу, появится сообщение об ошибке, а форма останется открытой: исправьте значения и сохраните снова.


Добавить задачу публикации сертификатов
Название*
Описание
Шаблон*
Начальный ID сертификата
Размер порции
Формат
PEM
Cron*
LDAP
Хост*
Порт
Пользователь*
Пароль*
Base DN*
Фильтр
Атрибут
Защищённое соединение
Таймаут подключения
EXC
Отмена
Сохранить

49 Форма добавления задачи публикации сертификатов

Параметры задачи:

Поле	Что указать
Название*	Уникальный ключ задачи, который отображается в столбце «ID» списка. После создания задачи название изменить нельзя
Описание	Короткий комментарий к задаче. Виден только в интерфейсе, на публикацию не влияет
Шаблон*	Шаблон сертификата из списка шаблонов выбранного ЦС. По нему отбираются сертификаты для публикации
Начальный ID сертификата	ID последнего уже опубликованного сертификата: публикация продолжится со следующего. Если поле не заполнено, публикуются все доступные сертификаты
Размер порции	Сколько сертификатов обрабатывается за одну итерацию публикации
Формат	Формат публикуемых сертификатов: PEM (текстовый, выбран по умолчанию) или DER (двоичный)
Cron*	Расписание запуска в формате cron. Например, 0 12 * * * запускает задачу каждый день в 12:00 UTC (15:00 по Москве)

Блок LDAP задаёт, куда и под какой учётной записью публикуются сертификаты. Адрес каталога, учётную запись и точку публикации сообщает администратор каталога.

Поле	Что указать
Хост*	Адрес LDAP-сервера, например контроллера домена Active Directory
Порт	Порт LDAP-сервера. Если поле пустое, используется стандартный порт 389
Пользователь*	Учётная запись, от имени которой сервис публикации подключается к каталогу

Пароль*	Пароль этой учётной записи. Если включён переключатель EXC, вместо пароля укажите ссылку на секрет вида mountPoint:path:key
Base DN*	Точка каталога, в которую публикуются записи, например DC=example,DC=local
Фильтр	Условие отбора записей каталога. Можно оставить пустым
Атрибут	Атрибут записи, в который записывается сертификат, например userCertificate
Защищённое соединение	Включите, чтобы подключаться к каталогу по защищённому протоколу LDAPS
Таймаут подключения	Сколько миллисекунд ждать подключения к LDAP-серверу
EXC	Включите, если пароль хранится во внешнем хранилище секретов EXC. Тогда в поле «Пароль» указывается ссылка на секрет, а не сам пароль

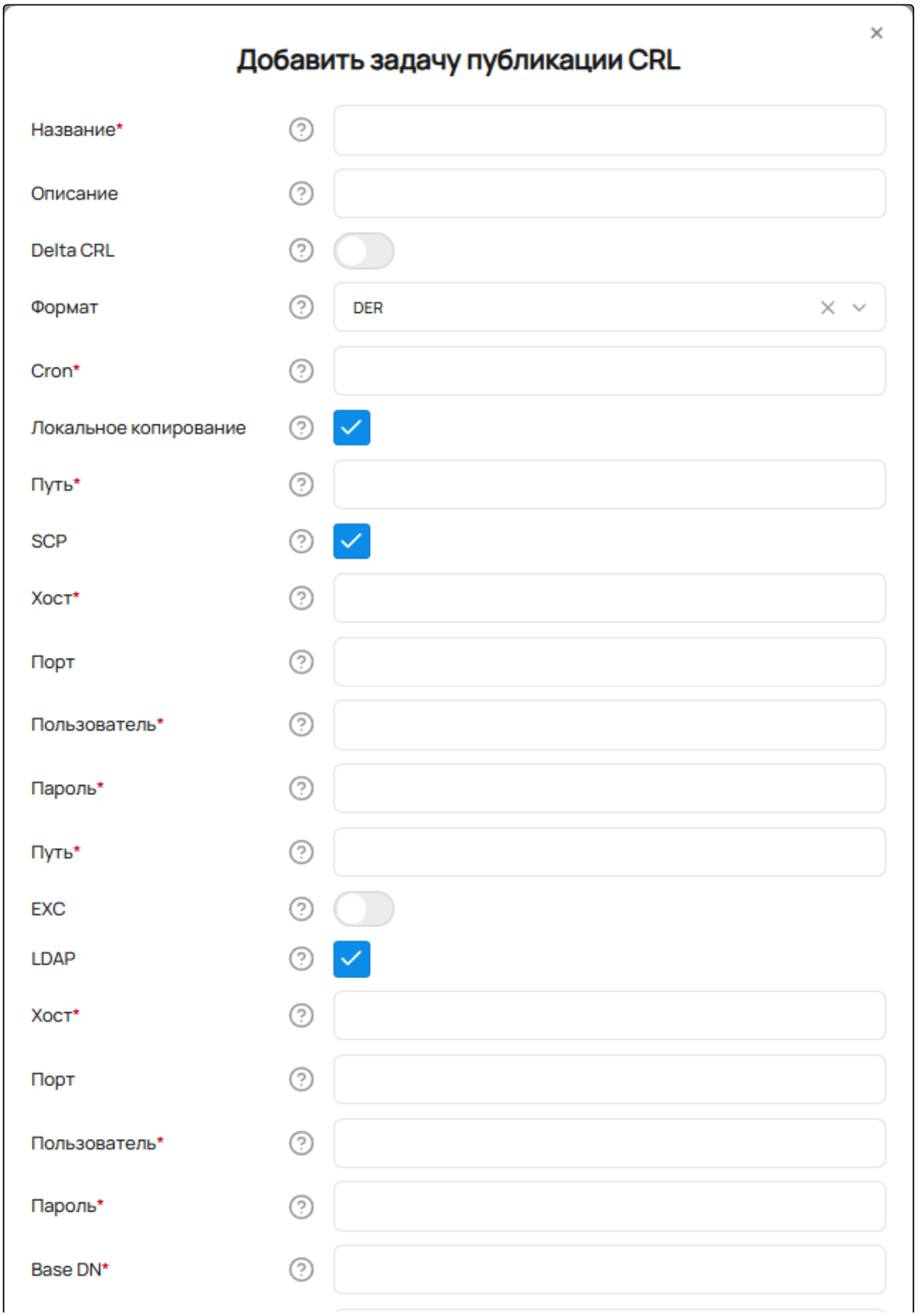
11.2.2 Добавление задачи публикации CRL

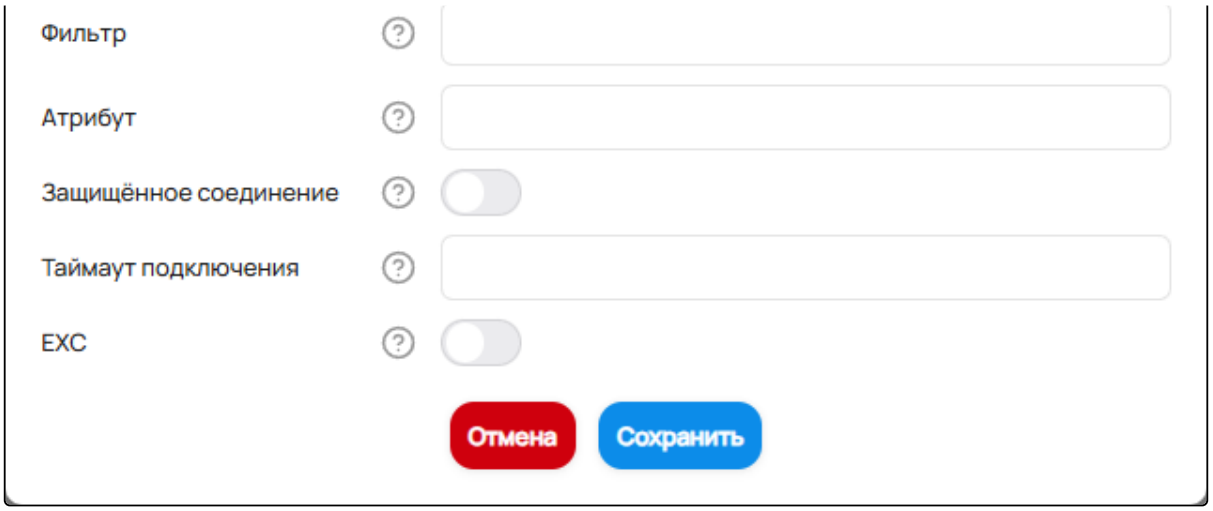
Задача публикации CRL по расписанию выгружает список отзыва ЦС: полный (CRL) или разностный (Delta CRL). В одной задаче можно включить несколько способов публикации одновременно:

- Локальное копирование: копия файла сохраняется в каталог на сервере, где работает сервис публикации;
- SCP: файл передаётся на удалённый сервер по протоколу SCP;
- LDAP: список отзыва записывается в каталог LDAP, например в Active Directory.

1. В левом меню откройте «Задачи» → «Публикация CRL».
2. Нажмите **Добавить задачу**. Откроется форма «Добавить задачу публикации CRL».
3. Заполните общие параметры задачи.
4. Отметьте флажками нужные способы публикации. Заполните поля, которые появятся под каждым отмеченным способом.
5. Нажмите **Сохранить**.

Нужно выбрать хотя бы один способ публикации. Если ни один флажок не отмечен, при сохранении появится сообщение «Укажите хотя бы один способ публикации: локальное копирование, SCP или LDAP». Признаки успешного сохранения те же, что у задачи публикации сертификатов.


Добавить задачу публикации CRL
Название*
Описание
Delta CRL
Формат
DER
Cron*
Локальное копирование
Путь*
SCP
Хост*
Порт
Пользователь*
Пароль*
Путь*
EXC
LDAP
Хост*
Порт
Пользователь*
Пароль*
Base DN*



50 Форма добавления задачи публикации CRL (отмечены все способы публикации)

Общие параметры задачи:

Поле	Что указать
Название*	Уникальный ключ задачи. После создания задачи изменить его нельзя
Описание	Короткий комментарий к задаче. Виден только в интерфейсе
Delta CRL	Включите, чтобы публиковать Delta CRL (в списке задач указывается тип delta). Если переключатель выключен, публикуется полный CRL (тип base)
Формат	Формат публикуемого файла: DER (двоичный, выбран по умолчанию) или PEM (текстовый)
Cron*	Расписание запуска в формате cron. Например, 0 12 * * * запускает задачу каждый день в 12:00 UTC (15:00 по Москве)

Поля способа «Локальное копирование»:

Поле	Что указать
Путь*	Полный путь к файлу на сервере, где работает сервис публикации, например /var/pub/ca.crl

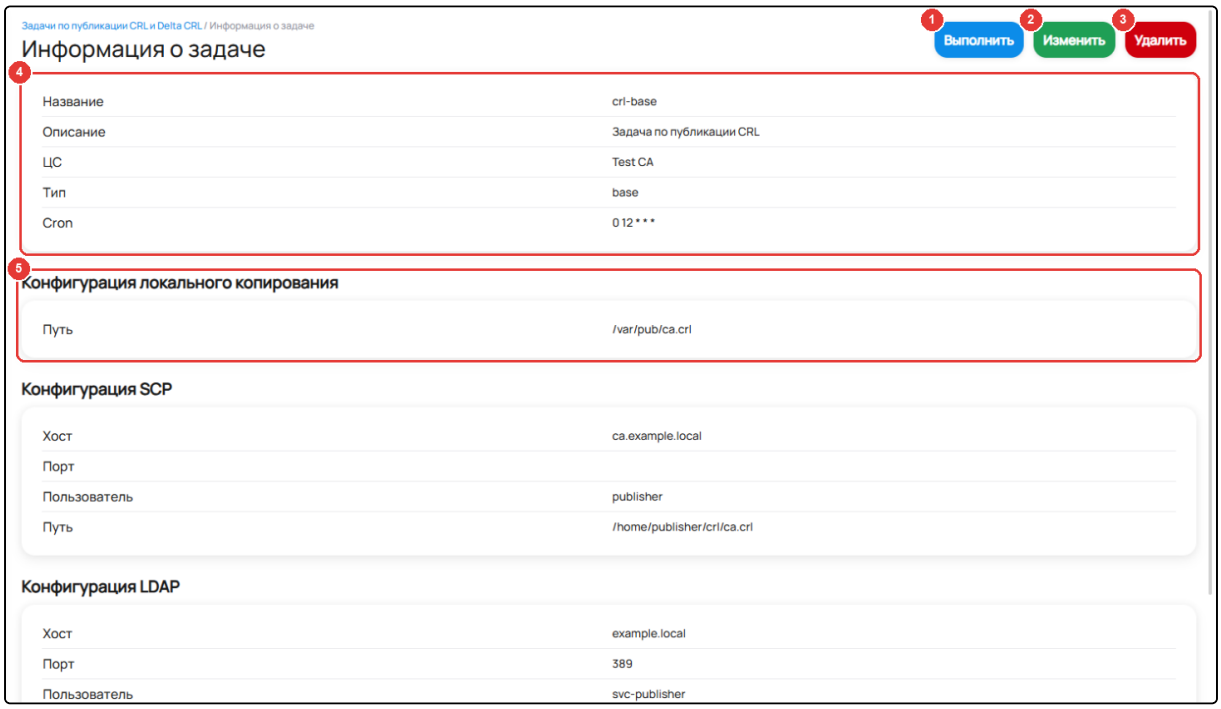
Поля способа «SCP» (адрес сервера, учётную запись и путь сообщает администратор сервера, на который публикуется список отзыва):

Поле	Что указать
Хост*	Адрес сервера, на который передаётся файл
Порт	Порт SSH. Если поле пустое, используется стандартный порт 22
Пользователь*	Имя пользователя для подключения по SCP
Пароль*	Пароль этого пользователя либо, при включённом переключателе EXC, ссылка на секрет вида mountPoint:path:key
Путь*	Путь к файлу на удалённом сервере, например /home/publisher/crl.crl
EXC	Включите, если пароль хранится во внешнем хранилище секретов EXC

Поля способа «LDAP» те же, что в блоке LDAP задачи публикации сертификатов. Отличается только значение поля «Атрибут»: укажите атрибут записи, в который записывается список отзыва, например certificateRevocationList.

11.2.3 Просмотр, запуск, изменение и удаление задачи

Чтобы открыть карточку задачи, щёлкните её строку в списке. Откроется страница «Информация о задаче». В верхнем блоке показаны основные параметры: название, описание, ЦС и расписание cron. У задачи публикации CRL к ним добавляется тип, у задачи публикации сертификатов добавляются шаблон и начальный ID сертификата. Ниже для каждого настроенного способа публикации выводится свой блок: «Конфигурация локального копирования», «Конфигурация SCP», «Конфигурация LDAP». Пароли, формат, размер порции, защищённое соединение, таймаут и признак EXC в карточке не показываются; их видно в форме изменения.



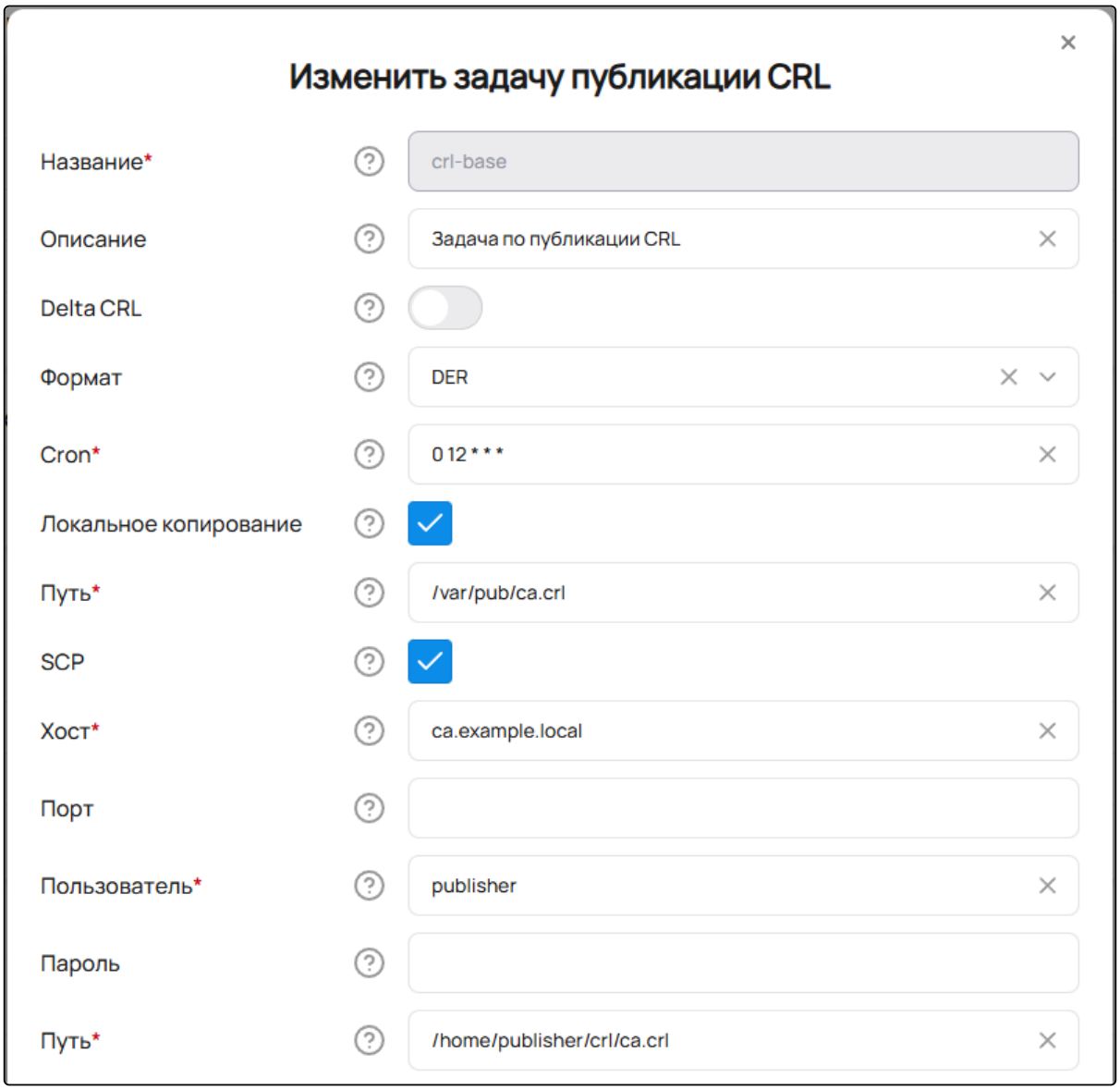
51 Карточка задачи публикации CRL с кнопками «Выполнить», «Изменить» и «Удалить»

На рисунке: **1**, **2**, **3** кнопки карточки (см. таблицу ниже); **4** основные параметры задачи; **5** блок способа публикации (ниже расположены такие же блоки SCP и LDAP).

№	Кнопка	Что делает
1	**Выполнить**	Запускает задачу, не дожидаясь времени по расписанию. В окне «Выполнить задачу» нажмите **Подтвердить**. После выполнения появится уведомление «Задача по публикации выполнена». Кнопка пригодится, например, чтобы проверить только что добавленную задачу
2	**Изменить**	Открывает форму «Изменить задачу публикации CRL» (или «Изменить задачу публикации сертификатов») с текущими значениями. После нажатия **Сохранить** появится уведомление «Настройки сохранены», и карточка покажет новые значения
3	**Удалить**	Удаляет задачу из конфигурации сервиса публикации. В окне «Удалить задачу» с вопросом «Вы действительно хотите удалить задачу?» нажмите **Подтвердить**. Появится уведомление «Задача публикации CRL удалена» (или «Задача публикации сертификатов удалена»), и откроется список задач

Особенности формы изменения:

- Поле «Название» заблокировано: ключ задачи после создания не меняется. Чтобы переименовать задачу, создайте новую и удалите прежнюю.
- Поля «Пароль» открываются пустыми: сохранённый пароль в интерфейс не передаётся. Если оставить поле пустым, сохранится прежний пароль; если ввести новое значение, оно заменит прежнее.



52 Форма изменения задачи публикации CRL

11.3 Резервное копирование

Задание резервного копирования по расписанию или по команде копирует базу данных ЦС и файлы узлов ЦС: файлы конфигурации и исполняемый файл ЦС. Из полученной копии ЦС можно восстановить.

Задания выполняет отдельный сервис резервного копирования. Контрольная панель передаёт ему команды пользователя, а подключается к узлам ЦС и к базе данных, хранит копии и запускает задания по расписанию сам сервис. Если сервис не настроен или недоступен, раздел не работает: обратитесь к администратору. Настройка сервиса описана в п. 7.6 «Резервное копирование» Руководства администратора.

Действие	**Право**
Открыть раздел, просмотреть задания, ход операций и копии	`rleMiniCABackup-r`
Добавить, изменить, удалить задание	`rleMiniCAConfig-w`
Запустить копирование вне расписания	`rleMiniCABackup-w`
Восстановить ЦС из копии	`rleMiniCABackupRestore-w`

11.3.1 Список заданий

Откройте «Задачи» → «Резервное копирование». В списке показаны задания текущего ЦС (см. «Текущий ЦС») со столбцами «Ключ», «Описание», «Узлов» (число узлов ЦС в задании) и «Расписание» (cron словами, время в UTC). Щелчок по строке открывает карточку задания.

11.3.2 Добавление задания

1. Нажмите **Добавить задание**. Откроется окно «Создать задание».
2. Заполните общие параметры и блок «База данных ЦС».
3. Нажмите **Добавить узел** и заполните параметры узла. Повторите для каждого узла ЦС; лишний блок удаляется кнопкой **Удалить узел**.
4. Нажмите **Сохранить**.

Задание сохранено, если появилось уведомление «Настройки сохранены» и задание появилось в списке. Пока не добавлен ни один узел, под заголовком «Узлы» выводится «Добавьте хотя бы один узел», и задание не сохраняется. Задание создаётся для текущего ЦС.

Поле	**Что указать**
Ключ*	Уникальный ключ задания. После создания изменить нельзя. Ключ входит в имя файла копии
Описание*	Короткий комментарий, виден только в интерфейсе

Cron*	Расписание копирования в формате cron из пяти полей. Время задаётся в UTC. По умолчанию 0 2 * * *, то есть каждый день в 02:00 UTC (05:00 по московскому времени)

Блок «База данных ЦС» заполняется один раз: база данных ЦС в задании одна и общая для всех узлов. Параметры сообщает администратор базы данных.

Поле	**Что указать**
Хост*	Адрес сервера базы данных ЦС
Порт	Порт сервера базы данных. По умолчанию 5432
Имя БД*	Имя базы данных ЦС
Пользователь*	Пользователь базы данных ЦС
Пароль*	Пароль пользователя либо ссылка на секрет EXC вида mountPoint:path:key
Пароль из EXC	Включите, если в поле «Пароль» указана ссылка EXC

Блок «Узел N» описывает сервер, на котором работает сервис ЦС (параметры сообщает администратор ЦС). Требования к учётной записи SSH и к настройке узла приведены в п. 7.6 «Резервное копирование» Руководства администратора.

Поле	**Что указать**
Имя узла*	Произвольное обозначение узла, например node1. Имена узлов в задании не должны повторяться
Бинарник*	Полный путь к исполняемому файлу сервиса ЦС на узле, например /opt/itc/minica/minica. Файл входит в копию и возвращается при восстановлении
systemd-юнит	Имя юнита сервиса ЦС, по умолчанию minica
Пользователь сервиса	Пользователь, от имени которого работает сервис ЦС (владелец юнита), по умолчанию itc-svc; обычно не совпадает с пользователем SSH

systemctl --user	Включено по умолчанию: сервис ЦС запущен как пользовательский юнит systemd. Выключите для системного юнита
SSH: Хост*, Порт	Адрес узла и порт SSH (по умолчанию 22)
SSH: Пользователь*	Пользователь для подключения к узлу. Должен иметь право sudo
SSH: Пароль*	Пароль пользователя SSH, он же используется для sudo. Сервис входит на узел только по паролю, вход по ключу SSH не поддерживается
SSH: Пароль из EXC	Включите, если пароль задан ссылкой EXC
Файлы конфигурации*	Полные пути к файлам и каталогам конфигурации узла, по одному на строку, например /opt/itc/minica/ca и /opt/itc/minica/conf. Каталог ключевого материала укажите раньше каталога настроек: в этом порядке файлы будут восстанавливаться. Каждый путь должен существовать на узле, иначе копирование завершится ошибкой. Символьные ссылки в копию не попадают

11.3.3 Карточка задания

Кнопка	Что делает	Право
Запустить копирование	В окне «Запустить копирование» с вопросом «Вы действительно хотите запустить копирование всех узлов?» нажмите **Подтвердить**. Появится уведомление «Копирование запущено». Пока идёт операция, вместо неё видна неактивная кнопка **Выполняется**	`rleMiniCABackup-w`
Изменить	Открывает окно «Изменить задание». Ключ заблокирован. Поля паролей открываются пустыми: сохранённые пароли в интерфейс не передаются, а пустое поле оставляет прежний пароль	`rleMiniCAConfig-w`
Удалить	В окне «Удалить задание» нажмите **Подтвердить**. Появится уведомление «Задание удалено», и откроется список	`rleMiniCAConfig-w`
Назад	Возвращает к списку заданий	Не требуется

Для одного ЦС одновременно выполняется одна операция: копирование или восстановление. Запуск по расписанию, который пришёлся на время другой операции, пропускается, и следующая копия создаётся уже по расписанию. Прервать запущенную операцию из интерфейса нельзя.

Блок	Что показывает
Основные параметры	Ключ, описание, ЦС задания, расписание, база данных, число узлов
Узлы	По каждому узлу: имя, путь к исполняемому файлу, адрес SSH, systemd-юнит и его вид, пользователь сервиса, файлы конфигурации
Текущая операция	Вид и статус выполняемой операции, имя архива, шаги по базе данных и по каждому узлу, ошибки. Если операции нет, выводится «Операция не выполняется». Сведения обновляются автоматически
Последний запуск	Статус, время начала (UTC) и результат последнего резервного копирования и последнего восстановления
Копии	Таблица созданных копий: «Имя файла», «Дата», «Размер», «Узлы», «Пригодность» («Пригодна» или «Непригодна» с причиной) и кнопка **Восстановить** у пригодных копий

Статусы шагов и операций: «Ожидает», «Выполняется», «Завершено», «Неуспех» (рядом выводится текст ошибки), «Возвращено к сохранённому состоянию» (узел возвращён к состоянию, сохранённому перед восстановлением), «Пропущено».

Если администратор настроил почтовые уведомления, о неуспешном копировании или восстановлении сервис резервного копирования сообщает письмом.

11.3.4 Состав и хранение копии

В копию входят:

- база данных ЦС;
- файлы и каталоги из поля «Файлы конфигурации» каждого узла с исходными правами доступа и владельцем;
- исполняемый файл ЦС каждого узла.

В копию не входят архивная база данных, база данных OpenID, конфигурации и сертификаты сервера служб, в том числе конфигурация самого сервиса резервного копирования и ключ шифрования копий. Их копирует администратор средствами СУБД и ОС (см. п. 7.6 «Резервное копирование» Руководства администратора).

Ход копирования виден в блоке «Текущая операция». Сначала копируется база данных ЦС и подсчитывается число записей о сертификатах, запросах и событиях: эти числа показываются при подтверждении восстановления. Затем с каждого узла по очереди копируются файлы конфигурации и исполняемый файл ЦС. Сервис ЦС при копировании не останавливается.

Готовая копия упаковывается в архив и проверяется, результат проверки показан в столбце «Пригодность» таблицы «Копии». Если копирование завершилось неуспешно, неполная копия не сохраняется. Перед копированием и восстановлением сервис резервного копирования проверяет свободное место на своём сервере: если места мало, операция не начинается.

Копии хранятся на сервере сервиса резервного копирования. Имя файла копии содержит ключ задания и время создания в UTC, имя зашифрованной копии оканчивается на .enc. Скачать копию из Контрольной панели нельзя: при необходимости её забирает администратор с диска сервера. Копии старше срока хранения, который задаёт администратор (по умолчанию 30 дней), удаляются после очередного успешного копирования по заданию, последняя пригодная копия сохраняется всегда.

Копия содержит ключ ЦС

Если в задание включён каталог ключевого материала, копия содержит закрытый ключ ЦС. Шифрование копий включает администратор. Незашифрованную копию защищайте так же, как ключ ЦС.

11.3.5 Восстановление из копии

Внимание

При восстановлении сервис ЦС на выбранных узлах останавливается. База данных ЦС и файлы выбранных узлов, включая исполняемый файл ЦС, заменяются данными копии. Записи, появившиеся после создания копии, будут удалены. Сертификаты, отозванные после создания копии, снова будут числиться действительными: отзовите их повторно.

Кнопка **Восстановить** видна только пользователю с правом `rleMiniCABackupRestore-w` и только пока по заданию не выполняется другая операция.

1. В карточке задания найдите копию в таблице и нажмите **Восстановить** в её строке.
2. В окне «Восстановление копии» в блоке «Выберите узлы для восстановления» оставьте отмеченными нужные узлы. В списке только узлы, которые входят и в задание, и в копию; по умолчанию отмечены все. База данных ЦС общая для всех узлов и восстанавливается при любом выборе.
3. Проверьте таблицу «Число записей, которые будут удалены при восстановлении» (столбцы «Таблица», «Сейчас», «В копии», «Будет удалено»). Для сертификатов, запросов и событий в ней указано число записей в текущей базе данных и в копии и сколько записей будет потеряно. Числа относятся ко всей базе данных ЦС и от выбора узлов не зависят.
4. Отметьте «Подтверждаю: данные выбранных узлов будут заменены данными копии».

5. Нажмите **Восстановить**. Кнопка активна, если выбран хотя бы один узел и отмечено подтверждение.

Перед запуском сервис резервного копирования повторно проверяет пригодность копии: если копия не прошла проверку, восстановление не запускается и выводится сообщение об ошибке. После успешной проверки появится уведомление «Восстановление запущено», окно закроется, а ход операции отобразится в блоке «Текущая операция».

Если копия отличается от текущего состояния, например набор узлов в задании не совпадает с набором узлов в копии, сервер сообщает о расхождении. В окне появится блок «Расхождение: …» с описанием и флажок «Продолжить несмотря на расхождение». Чтобы всё равно восстановить копию, отметьте флажок и снова нажмите **Восстановить**; чтобы отказаться, нажмите **Отмена**.

Одновременно выполняется только одно восстановление, даже для разных ЦС: пока идёт другое восстановление, новое не запускается.

Восстановление выполняется в таком порядке:

1. Сервис резервного копирования сохраняет текущую базу данных ЦС, чтобы вернуть её при ошибке.
2. На каждом выбранном узле по очереди останавливает сервис ЦС, проверяет, что он остановлен, и сохраняет текущие файлы узла.
3. Восстанавливает базу данных ЦС из копии.
4. На каждом выбранном узле восстанавливает файлы в порядке путей из поля «Файлы конфигурации», затем исполняемый файл ЦС, запускает сервис ЦС и в течение 30 секунд проверяет, что он запустился.

При ошибке на любом шаге сервис резервного копирования возвращает базу данных ЦС и файлы узлов к сохранённому состоянию и снова запускает сервис ЦС. Такой узел получает статус «Возвращено к сохранённому состоянию», а операция завершается со статусом «Неуспех».

Файлы, которые есть на узле, но отсутствуют в копии, при восстановлении не удаляются. Конфигурацию systemd сервис резервного копирования не перечитывает: если среди путей задания есть файл юнита, после восстановления администратор выполняет на узле `systemctl daemon-reload` (для пользовательского юнита `systemctl --user daemon-reload`).

Вместе с исполняемым файлом возвращается версия ЦС на момент создания копии. Если ЦС обновлялся после создания копии, после восстановления он работает в прежней версии.

Проверка результата: в блоке «Последний запуск» восстановление завершилось со статусом «Завершено», а на странице «Настройки → Конфигурация» индикатор карточки «Конфигурация Clearway CA» зелёный и поле «Версия» показывает ожидаемую версию ЦС.

11.4 Типовые задачи

Типовыми задачами называются пошаговые мастера замены TLS-сертификата на сервере nginx или PostgreSQL. Контрольная панель подключается к серверу по SSH и находит файлы сертификата и ключа, затем выпускает в ЦС новый сертификат по выбранному шаблону, записывает его в эти файлы и при необходимости перезапускает сервис. Мастер удобен для плановой замены сертификата: действия каждый раз выполняются одинаково.

Перед началом учтите:

- мастер доступен пользователю с правом `rleMiniCACertReq-w`, если на сервере включена функция типовых задач. Если функция выключена, пункта меню нет, а по прямому адресу страница показывает «Функционал недоступен»;
- учётной записи SSH нужны права на изменение файлов сертификата и ключа, а если нужен перезапуск, то и на перезапуск сервиса; для выпуска сертификата у вас должен быть доступ к выбранному шаблону. Эти требования перечислены на странице в блоке «Требуются разрешения».

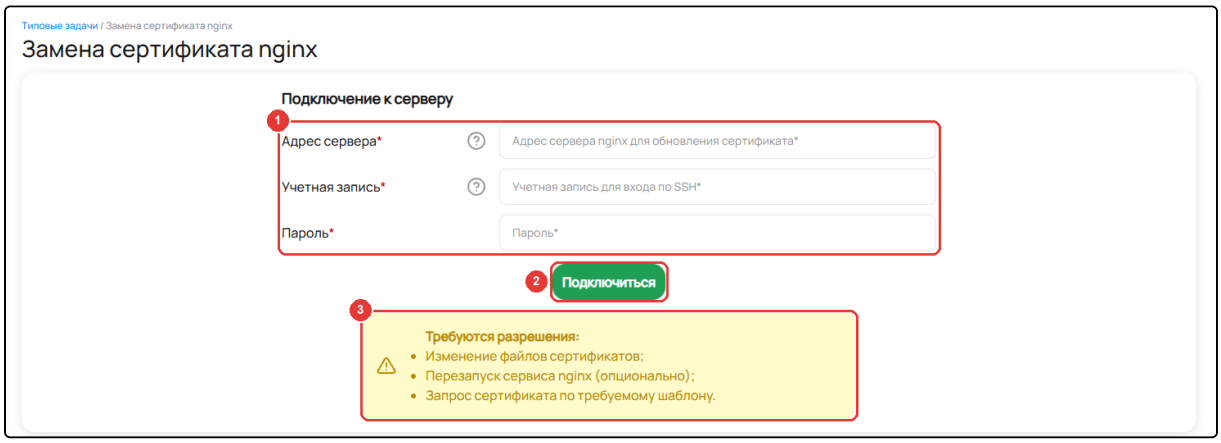
11.4.1 Шаг 1. Подключение к серверу

1. В левом меню откройте «Задачи» → «Типовые» → «Замена сертификата nginx».
2. Заполните поля:

Поле	Что указать
Адрес сервера*	Имя или IP-адрес сервера nginx, на котором заменяется сертификат, например web01.example.local
Учетная запись*	Учётная запись для входа по SSH
Пароль*	Пароль этой учётной записи

1. Нажмите **Подключиться**.

Контрольная панель проверит сервер и сообщит результат: «Nginx установлен.» или «Nginx не установлен.», а также «Найдено сертификатов: N» или «Сертификатов не найдено. Укажите пути к сертификату и ключу вручную.». Затем откроется шаг «Пути к сертификату и ключу». Если подключиться не удалось, появится текст ошибки или «Ошибка подключения к серверу».



53 Замена сертификата nginx, шаг «Подключение к серверу»

На рисунке: **1** параметры подключения по SSH; **2** кнопка «Подключиться»; **3** требования к правам.

11.4.2 Шаг 2. Пути к сертификату и ключу

- Если сертификаты на сервере найдены, выберите нужный файл в поле «Выбрать из найденных». Путь к ключу подставится автоматически, и откроется блок «Параметры выпуска».
- Если сертификаты не найдены, укажите «Путь к сертификату» и «Путь к ключу» и нажмите **Проверить наличие файлов**. После проверки откроется блок «Параметры выпуска».

Сообщение	Что означает
Файлы сертификата и ключа найдены.	Можно выбрать любой режим замены
Файлы сертификата и ключа не найдены. Будут созданы новые.	Файлы будут созданы по указанным путям
Файл ключа не найден. Доступен только режим "Выпустить с новым ключом".	Режим замены зафиксирован на новом ключе
Файл сертификата не найден. Будет создан новый.	Файл сертификата будет создан
Укажите пути к сертификату и ключу.	Одно из полей пути не заполнено
Ошибка проверки путей	Не удалось проверить файлы на сервере. Проверьте подключение и пути

11.4.3 Шаг 3. Параметры выпуска и замена

Поле	Что указать
Режим замены	В режиме «Выпустить с новым ключом» (по умолчанию) создаётся новый закрытый ключ. В режиме «Обновить с тем же ключом» сертификат выпускается для существующего ключа; этот режим доступен, только если файл ключа найден
Шаблон сертификата	Шаблон ЦС, по которому выпускается новый сертификат
Перезагрузить nginx после замены	Отмечено по умолчанию. Снимите флажок, если перезапустите сервис сами

Назад возвращает к шагу подключения; найденные пути и параметры сбрасываются. **Заменить сертификат** выпускает сертификат и записывает его на сервер. При успехе появится уведомление «Сертификат успешно заменён. Серийный номер: …». Если поля не заполнены, выводится «Заполните все обязательные поля.», при ошибке выводится текст ошибки или «Ошибка замены сертификата».

После замены убедитесь, что сервер отдаёт новый сертификат, например сравните серийный номер из уведомления с сертификатом, полученным при обращении к серверу по HTTPS.

11.4.4 Замена сертификата postgres

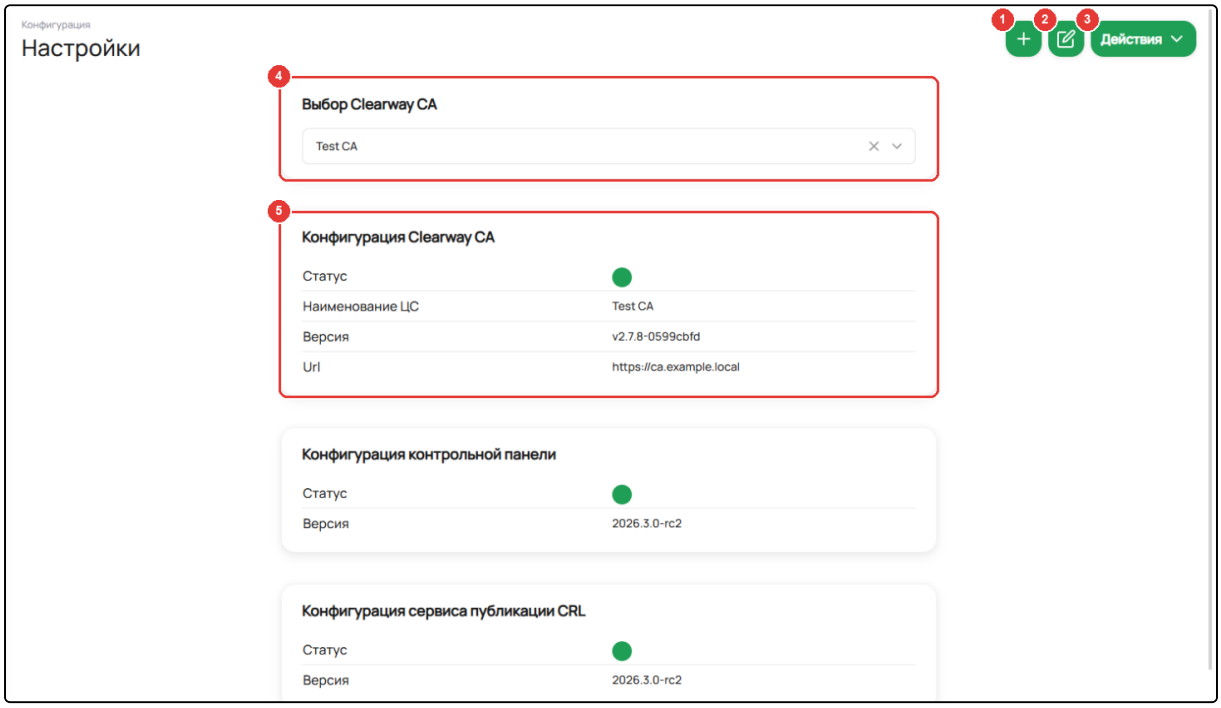
Сценарий «Задачи» → «Типовые» → «Замена сертификата postgres» работает так же, как замена сертификата nginx. Отличия: в подсказках и блоке «Требуются разрешения» указан сервис postgres, после подключения выводится «PostgreSQL установлен.» или «PostgreSQL не установлен.», если сертификаты не найдены, выводится «Сертификаты не найдены. Укажите пути к сертификату и ключу вручную.», а флажок перезапуска называется «Перезагрузить postgres после замены».

12 Настройки

Группа меню «Настройки» содержит страницы «Конфигурация» (выбор экземпляра ЦС, проверка состояния компонентов и подключение ЦС к Контрольной панели) и «Ротация ключей» (замена сертификата и ключевой пары ЦС).

12.1 Конфигурация

Страница «Настройки» открывается пунктом меню «Настройки» → «Конфигурация» и доступна пользователю с правом `rleMiniCAConfig-r`.



54 Страница «Настройки»: выбор ЦС и карточки состояния

На рисунке: **1** «Добавить новый ЦС»; **2** «Обновить конфигурацию»; **3** меню «Действия»; **4** выбор ЦС; **5** карточка состояния компонента.

12.1.1 Выбор экземпляра ЦС

Контрольная панель может работать с несколькими экземплярами ЦС, например с отдельными центрами для разных сред. Все разделы показывают данные и выполняют операции для ЦС, выбранного на этой странице.

1. В левом меню откройте «Настройки» → «Конфигурация».
2. В карточке «Выбор Clearway CA» раскройте список и выберите ЦС. В списке показаны наименования подключений, заданные при добавлении ЦС.
3. Проверьте карточки состояния.

Если в браузере ЦС ещё не выбирался или выбранного подключения больше нет в списке, при открытии страницы выбирается первый ЦС списка (см. «Текущий ЦС»).

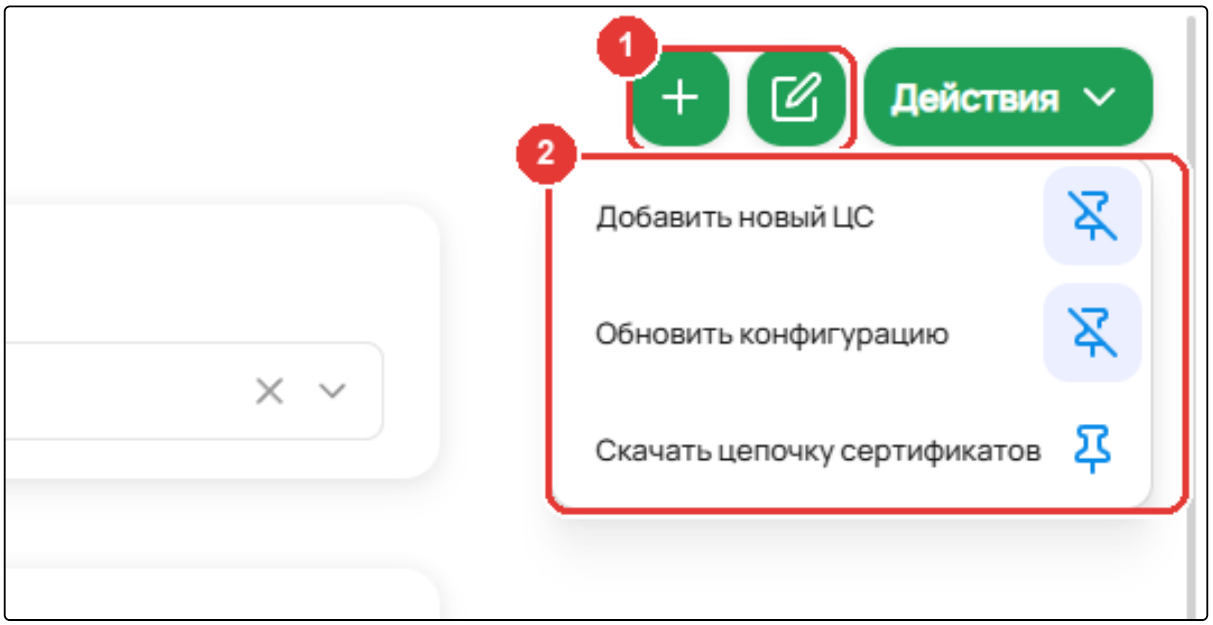
Карточка	Поле	Что показывает
Конфигурация Clearway CA	Статус	Зелёный индикатор означает, что ЦС отвечает; красный означает, что ЦС не отвечает
	Наименование ЦС	Наименование, которое сообщает ЦС. Может не совпадать с наименованием подключения в карточке «Выбор Clearway CA»
	Версия	Версия ЦС
	Url	Адрес, по которому Контрольная панель подключается к ЦС
Конфигурация контрольной панели	Статус, Версия	Состояние и версия серверной части Контрольной панели
Конфигурация сервиса публикации CRL	Статус, Версия	Состояние и версия сервиса публикации

Если индикатор красный, компонент не отвечает: не выполняйте операции над ЦС и обратитесь к администратору.

12.1.2 Действия на странице

Действие	Что делает	Право
Добавить новый ЦС	Открывает окно «Добавить новый ЦС» для подключения ещё одного ЦС	`rleMiniCAConfig-w`
Обновить конфигурацию	Открывает окно «Изменить конфигурацию» для текущего ЦС	`rleMiniCAConfig-w`
Скачать цепочку сертификатов	Сохраняет файл цепочки сертификатов выбранного ЦС	`rleMiniCAConfig-r`

Действия «Добавить новый ЦС» и «Обновить конфигурацию» закреплены по умолчанию и выведены значками «+» и «карандаш» слева от **Действия** (см. «Меню „Действия“ и закрепление действий»). Без права `rleMiniCAConfig-w` значки и пункты меню бледные и не срабатывают.



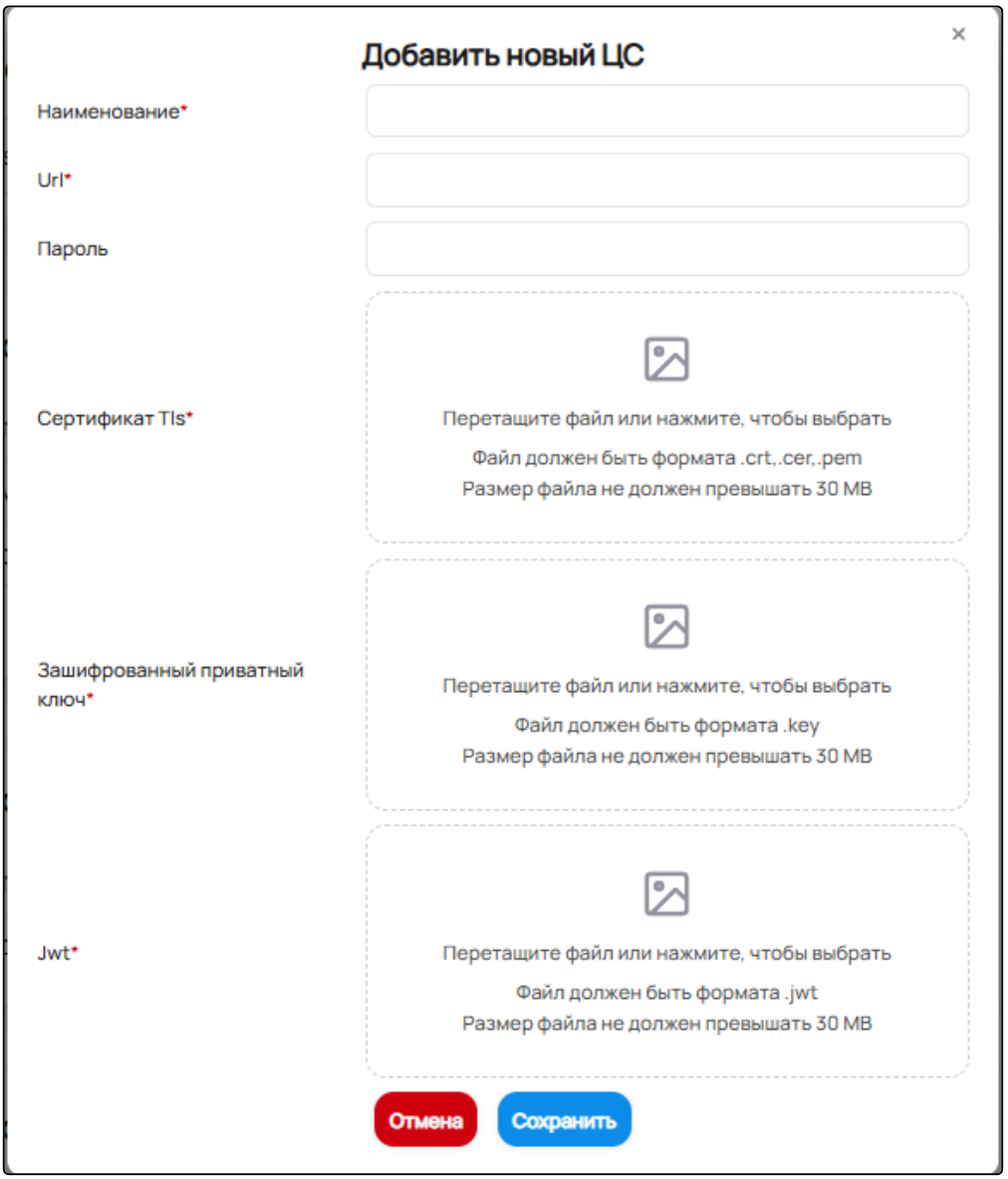
55 Меню «Действия» на странице «Настройки»

На рисунке: **1** закреплённые действия; **2** меню «Действия».

12.1.3 Добавление ЦС

Для подключения нужны TLS-сертификат, зашифрованный закрытый ключ и токен JWT, выпущенные администратором для Контрольной панели.

1. Нажмите «Действия» → «Добавить новый ЦС» или значок «+».
2. Заполните поля окна «Добавить новый ЦС».
3. Нажмите **Сохранить**. Чтобы выйти без сохранения, закройте окно крестиком.



56 Окно «Добавить новый ЦС»

Поле	Что указать
Наименование*	Имя подключения. Под этим именем ЦС появится в карточке «Выбор Clearway CA». После сохранения изменить нельзя
Url*	Адрес ЦС, начинается с http:// или https://, например https://ca.example.local
Пароль	Пароль зашифрованного закрытого ключа

Сертификат Tls*	Файл TLS-сертификата: .crt, .cer или .pem
Зашифрованный приватный ключ*	Файл зашифрованного закрытого ключа: .key
Jwt*	Файл токена JWT: .jwt

При успешном сохранении появится уведомление «Добавлена конфигурация ЦС», окно закроется, а ЦС появится в карточке «Выбор Clearway CA» у всех пользователей. При ошибке появится «Произошла ошибка при добавлении конфигурации ЦС», окно останется открытым: проверьте адрес и файлы. Если адрес указан без http:// или https://, под полем «Url» появится сообщение о неверном формате.

12.1.4 Изменение подключения к ЦС

1. В карточке «Выбор Clearway CA» выберите ЦС.
2. Нажмите «Действия» → «Обновить конфигурацию» или значок «карандаш».
3. В окне «Изменить конфигурацию» поле «Наименование» заполнено и недоступно для изменения, поле «Url» заполнено текущим адресом. Поле «Пароль» открывается пустым: введите пароль ключа снова. Заново выберите все три файла: они обязательны и в форму не подставляются.
4. Нажмите **Сохранить**.

При успешном сохранении появится уведомление «Обновлена конфигурация ЦС», при ошибке выводится «Произошла ошибка при обновлении конфигурации ЦС».

12.1.5 Скачивание цепочки сертификатов

Нажмите «Действия» → «Скачать цепочку сертификатов». Браузер сохранит файл цепочки сертификатов текущего ЦС.

Цепочку доверия устанавливают на каждом узле, который должен доверять сертификатам этого ЦС: на рабочих станциях-клиентах и на серверах, проверяющих клиентские или серверные сертификаты. После добавления корневого и промежуточных сертификатов в хранилище доверенных центров выпущенные сертификаты перестают вызывать предупреждения о недоверенном издателе.

12.2 Ротация ключей

Страница «Ротация ключей» нужна, чтобы заменить сертификат ЦС, в том числе с переходом на новую ключевую пару. По команде со страницы ЦС формирует запрос на сертификат (CSR); его подписывает центр сертификации, который выпускает сертификат для этого ЦС, и полученный сертификат загружают на этой же странице. Ключевую пару создаёт и хранит сам ЦС: Контрольная панель передаёт ему команды и получает от него только CSR, а к серверам ЦС не подключается.

Пункт меню «Настройки» → «Ротация ключей» отображается пользователю с правом `rleMiniCARotation-w`. Это право нужно для всех действий на странице, включая просмотр действующего сертификата: отдельного права на просмотр нет. Ротация выполняется для ЦС, выбранного на странице «Конфигурация» (см. «Текущий ЦС»); при смене ЦС страница обновляется.

Если ключ ЦС хранится в КриптоПро CSP или на аппаратном носителе (HSM, Рутокен), ротация из Контрольной панели недоступна: ЦС вернёт ошибку.

Элемент	Что показывает или делает
Карточка «Действующий сертификат ЦС»	Субъект, Издатель, Серийный номер, Действует с, Действует по, Идентификатор ключа (SKI), Отпечаток (SHA-256)
Плашка «CSR сформирован, ожидается загрузка сертификата»	CSR сформирован, сертификат ещё не загружен; в скобках указано время формирования CSR
Плашка «Замена сертификата выполнена»	Последняя замена завершена; в скобках указано время завершения
Пересоздать CSR	Открывает окно формирования CSR
Скачать CSR	Сохраняет CSR в файл csr-<наименование ЦС>.pem. Доступна, пока CSR ожидает сертификата
Заменить сертификат	Открывает окно загрузки нового сертификата ЦС. Доступна, пока CSR ожидает сертификата

Порядок ротации:

1. Проверьте сведения о действующем сертификате в карточке.
2. Нажмите **Пересоздать CSR** и сформируйте запрос (см. «Формирование CSR»).
3. Нажмите **Скачать CSR** и передайте файл центру сертификации, который выпускает сертификат для этого ЦС.
4. Получив сертификат, нажмите **Заменить сертификат** и загрузите его (см. «Замена сертификата ЦС»).
5. Согласуйте с администратором действия вне Контрольной панели: обновление доверенных сертификатов на узлах, публикацию нового сертификата ЦС, а после «Перевыпуска» и отдельный OCSP-ответчик для нового ключа. Порядок описан в разделе «Ротация ключа ЦС» Руководства администратора.

Сохранять прежнюю ключевую пару вручную не нужно: при замене сертификата ЦС делает это сам и начинает работать с новым сертификатом без перезапуска (см. «Замена сертификата

ЦС»). После «Перевыпуска» у нового сертификата ЦС будет другой SKI, а для ранее выпущенных сертификатов по-прежнему нужны отзыв, выпуск CRL и ответы OCSP.

12.2.1 Формирование CSR

Окно называется «Сформировать CSR». Если CSR уже сформирован и ожидает сертификата, окно называется «Пересоздать CSR», и новый запрос заменит ожидающий. Ключ прежнего запроса больше не используется: сертификат, выпущенный по прежнему CSR, установить будет нельзя. Отдельной отмены запроса нет: ожидающий запрос можно только заменить новым или завершить заменой сертификата.

Поле	**Что указать**
Режим	«Продление» (по умолчанию): CSR формируется на действующем ключе ЦС, ключевая пара и SKI не меняются. «Перевыпуск»: ЦС создаёт новую ключевую пару и формирует CSR на ней
Причина перевыпуска	Только для режима «Перевыпуск», обязательно: «Плановая замена» или «Компрометация»
Тип ключа	Только для режима «Перевыпуск»: «Как у текущего ключа» (по умолчанию, тип и размер наследуются от действующего ключа), RSA, ECDSA, Ed25519, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012
Размер ключа	Для всех типов, кроме «Как у текущего ключа» и Ed25519: RSA (1024, 2048, 4096), ECDSA (256, 384, 512), ГОСТ Р 34.10-2001 (256), ГОСТ Р 34.10-2012 (256, 512). Для RSA выбирайте не менее 2048 бит. Допустимость типа и размера проверяет ЦС и отклоняет недопустимые значения

Субъект и срок действия в окне не задаются: субъект и расширения запроса ЦС берёт из действующего сертификата ЦС, а срок действия нового сертификата определяет центр сертификации, который его выпускает. Ожидающий запрос хранится в ЦС и сохраняется при перезапуске ЦС.

Причина перевыпуска записывается в журнал Контрольной панели и в ЦС не передаётся. Ни одна из причин не отзывает прежний сертификат ЦС и не выпускает CRL: при компрометации ключа эти действия выполняются отдельно.

Нажмите **Сформировать**; **Отмена** закрывает окно без изменений. При успехе появится сообщение «CSR сформирован», на странице появится плашка ожидания, станут доступны **Скачать CSR** и **Заменить сертификат**. Если в режиме «Перевыпуск» не выбрана причина, выводится «Укажите причину перевыпуска»; если не заполнены обязательные поля, выводится «Заполните обязательные поля».

12.2.2 Замена сертификата ЦС

1. Нажмите **Заменить сертификат**.

2. В окне «Заменить сертификат» нажмите **Выберите файл сертификата** и укажите файл .pem, .crt, .cer или .der (сертификат X.509 в формате PEM или DER).
3. Контрольная панель прочитает файл, и окно покажет его сведения: Издатель, Серийный номер, Действует с, Действует по, Отпечаток (SHA-256). Сверьте их и нажмите **Заменить**. **Выбрать другой файл** возвращает к выбору файла, **Отмена** закрывает окно без замены.
4. Прочитайте результат и нажмите **Готово**. Страница обновится.

На шаге 3 сертификат только читается. Если выбранный файл не является сертификатом X.509 в формате PEM или DER, появится сообщение об ошибке, и сведения не отобразятся.

После нажатия **Заменить** сертификат проверяет ЦС:

- поля сертификата совпадают с действующим сертификатом ЦС, кроме серийного номера и срока действия;
- открытый ключ совпадает с ключом последнего CSR;
- сертификат подписан родительским ЦС из цепочки сертификатов этого ЦС;
- срок действия сертификата наступил и не истёк;
- у сертификата есть признаки сертификата ЦС: расширение Basic Constraints с CA=TRUE и назначения ключа keyCertSign и cRLSign.

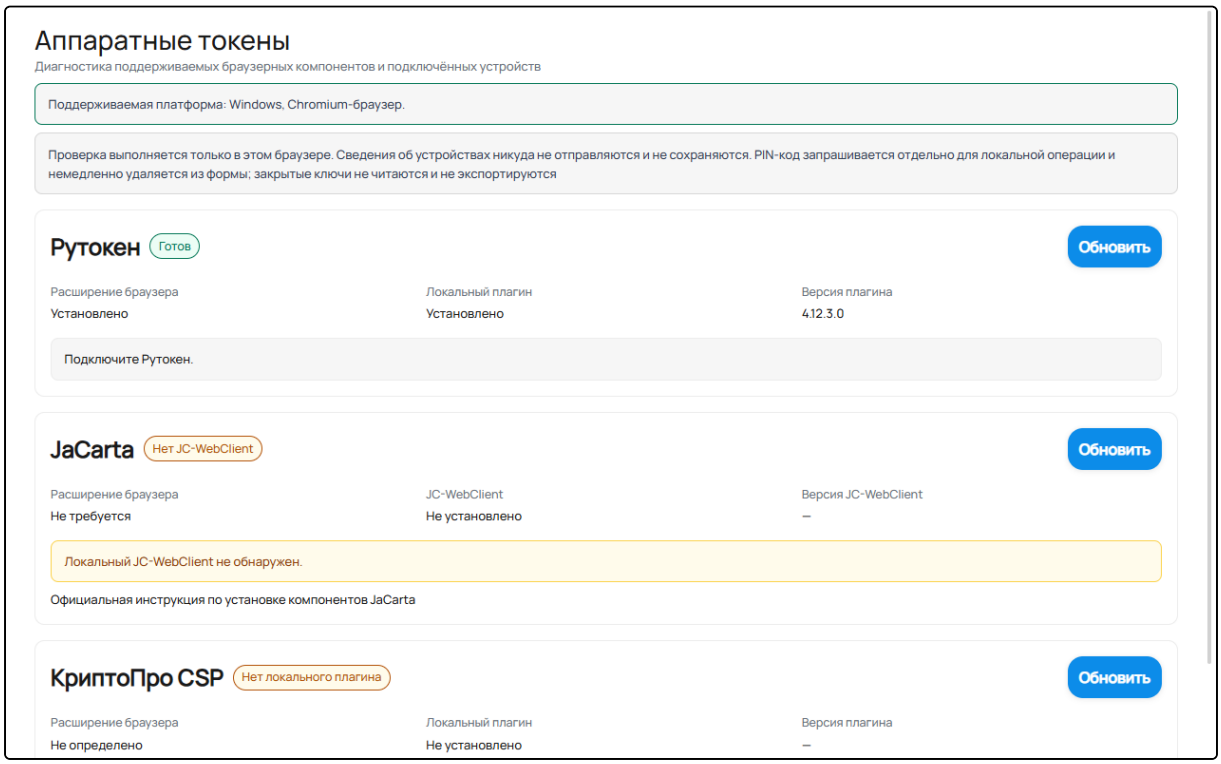
Если проверки пройдены, ЦС сохраняет прежний сертификат, а при «Перевыпуске» и прежний ключ, в архиве прежних ключей, заменяет сертификат ЦС и цепочку сертификатов и сразу начинает работать с новым сертификатом. Перезапуск ЦС не нужен.

Результат	**Что означает**
Замена завершена	Сертификат ЦС заменён
Сертификат уже установлен	Этот сертификат уже установлен у ЦС и повторно не применяется
Сертификат отклонён проверкой ЦС	ЦС не принял сертификат, например он выпущен не по последнему CSR, подписан не родительским ЦС или срок его действия истёк; ниже перечислены причины. Нажмите **Выбрать другой файл** и загрузите сертификат, выпущенный по последнему сформированному CSR
Не удалось прочитать файл	Браузер не смог прочитать выбранный файл

13 Аппаратные токены

Раздел «Аппаратные токены» проверяет, установлены ли на компьютере пользователя компоненты для работы с носителями, и позволяет просмотреть и изменить содержимое носителя: ключи, сертификаты и контейнеры КриптоПро CSP. Все операции выполняются локально в браузере; сведения об устройствах и PIN-коды в ЦС не передаются и нигде не сохраняются. Пункт меню виден всем пользователям, отдельного права не требуется.

Используйте раздел, чтобы проверить готовность рабочего места перед созданием ключа в конструкторе CSR-запросов, добавить сертификат к ранее созданному ключу или удалить лишний ключ или контейнер, оставшийся после ошибки.



57 Раздел «Аппаратные токены»

13.1 Требования к рабочему месту

Поддерживается Windows с браузером на основе Chromium; на другой платформе выводится предупреждение, и работа не гарантируется.

Носитель	Что должно быть установлено
Рутокен	Расширение браузера «Адаптер Рутокен Плагин» и локальный Рутокен Плагин

JaCarta	Локальный JC-WebClient (расширение браузера не требуется)
КриптоПро CSP	КриптоПро CSP с действующей лицензией и КриптоПро Browser plug-in (расширение браузера и локальный компонент). Сайт Контрольной панели должен быть добавлен в доверенные узлы КриптоПро и открыт по HTTPS

13.2 Карточки производителей и устройств

На странице выводятся карточки Рутокен, JaCarta и КриптоПро CSP.

Элемент	**Описание**
Статус	«Проверка», «Готов», «Нет расширения», «Нет локального плагина» (для JaCarta выводится «Нет JC-WebClient»), «Несовместимый плагин» или «Ошибка»
Расширение браузера, Локальный плагин, Версия плагина	Установлены ли компоненты и их версии
Сообщение и ссылка	Описание проблемы и ссылка на официальную инструкцию по установке компонентов
Обновить	Заново проверяет компоненты и список устройств; прочитанное содержимое и открытые формы сбрасываются

Список устройств обновляется автоматически, пока вкладка открыта. Для каждого подключённого устройства выводится карточка «Устройство N» с его сведениями (метка, серийный номер, свободная память и др.); у JaCarta выводятся карточки логических слотов. Для КриптоПро CSP выводится локальная диагностика: версия, тип и срок лицензии, режимы, число считывателей и контейнеров.

Возможность	**Рутокен**	**JaCarta**	**КриптоПро CSP**
Просмотр ключей и сертификатов	По PIN-коду	Без PIN-кода	Считыватели, контейнеры, ключи и сертификаты, без PIN-кода
Скачать сертификат (PEM)	Да	Да	Да

Добавить сертификат к ключевой паре	Да	Только к ключевой паре без сертификата	Нет
Переименовать ключевую пару или сертификат	Да	Да	Нет
Удалить сертификат	Да	Да	Нет
Удалить ключевую пару или контейнер	Ключевую пару, если с ней не связаны сертификаты	Ключевую пару без сертификата или контейнер целиком	Контейнер целиком

13.3 Просмотр содержимого носителя

1. В карточке устройства Рутокен или в карточке слота JaCarta нажмите **Показать ключи и сертификаты**. Для КриптоПро CSP нажмите **Показать считыватели, контейнеры, ключи и сертификаты**.
2. Для Рутокена введите PIN-код и нажмите **Прочитать**. JaCarta и КриптоПро CSP читаются без PIN-кода.
3. Появится содержимое носителя. Для Рутокена и JaCarta выводится таблица «Ключевая пара / Сертификат»: ключи с алгоритмом, назначением и сроком использования и связанные с ними сертификаты со сроком действия; сертификаты без ключа выводятся отдельной строкой. Для КриптоПро CSP выводятся таблицы логических считывателей и контейнеров с ключами и сертификатами.

Щелчок по сертификату открывает окно с его сведениями (Subject, Issuer, серийный номер, срок действия, открытый ключ, SAN, KU, EKU). Кнопка **Скачать PEM** сохраняет сертификат в файл. Если содержимое носителя изменилось, выводится «Требуется повторное чтение»: прочитайте носитель ещё раз. Кнопка **Обновить инвентарь** перечитывает данные КриптоПро CSP; **Скрыть содержимое** и **Скрыть инвентарь** убирают прочитанные данные со страницы.

13.4 Операции с объектами на носителе

Операция	**Как выполнить**
Добавить сертификат	У ключевой пары нажмите **Добавить сертификат**, выберите файл (.crt, .cer, .pem или .der, до 128 КиБ) или вставьте текст PEM, нажмите **Проверить сертификат**, сверьте «Предварительный просмотр», введите PIN-код и нажмите **Добавить на Рутокен** или **Добавить на JaCarta**

Переименовать	Нажмите **Переименовать**, укажите «Новая метка» (от 1 до 64 символов) и PIN-код, нажмите **Сохранить метку**. Меняется только метка, ключ и содержимое сертификата не меняются
Удалить	Нажмите кнопку удаления: **Удалить ключевую пару**, **Удалить сертификат**, **Удалить контейнер**, для JaCarta также **Удалить сертификат (сохранить ключ)** и **Удалить отдельный сертификат**. Проверьте в панели название объекта и последствия, введите PIN-код и нажмите **Удалить**. Для контейнера КриптоПро CSP пароль или PIN-код при необходимости запрашивает окно КриптоПро CSP

Внимание

Удаление с носителя необратимо. Удаление ключа или контейнера не отзывает сертификат в ЦС: для отзыва используйте карточку сертификата. У Рутокена ключевую пару можно удалить только после удаления связанных с ней сертификатов.

14 Защита ключей и конфиденциальных данных

Clearway CA предоставляет несколько механизмов защиты закрытых ключей и данных сертификатов. Ниже описаны те из них, которые затрагивают работу пользователя.

14.1 Шифрование закрытого ключа при подготовке запроса

Если ключ создаётся командой openssl (хранилище «Файл — Linux/OpenSSL» в конструкторе CSR-запросов), его можно сразу защитить паролем:

1. В конструкторе в блоке «Ключ» отметьте «Зашифровать закрытый ключ».
2. Скопируйте команду и выполните её на сервере. Из команды убирается параметр -nodes, поэтому openssl запросит пароль и сохранит ключ в зашифрованном виде.

Для хранилищ Windows флажок не отображается. Ключи на Рутокене, JaCarta и в КриптоПро CSP защищаются средствами носителя: PIN-кодом или паролем контейнера.

Внимание

Храните пароль к закрытому ключу надёжно и не передавайте его по незащищённым каналам. Без пароля зашифрованный закрытый ключ использовать невозможно, а восстановить его нельзя.

14.2 Шифрование данных сертификата в базе данных

Данные выпущенного сертификата можно хранить в базе данных центра сертификации в зашифрованном виде. Это снижает риск несанкционированного доступа к ним при прямом обращении к базе. Режим включается на уровне шаблона: в карточке шаблона раскройте блок «Дополнительно» и установите флажок «Шифровать данные в БД». Флажок недоступен, если установлен «Не добавлять сгенерированный сертификат в базу данных».

Сертификаты, выпущенные по этому шаблону, шифруются перед сохранением и хранятся в базе в зашифрованном виде. При скачивании данные расшифровываются автоматически, дополнительных действий от пользователя не требуется. Шифрование данных в базе может незначительно снижать производительность.

14.3 Хранение и восстановление закрытых ключей (KRA)

Помимо ключей, создаваемых на стороне пользователя, центр сертификации может хранить закрытые ключи выпущенных сертификатов в своей базе данных в зашифрованном виде. Шифрование выполняется с помощью сертификата агента восстановления ключей (Key Recovery Agent, KRA). Это позволяет восстановить закрытый ключ сертификата, например при его утрате владельцем.

Для шаблона хранение закрытого ключа включается флажком «Сохранять приватный ключ, зашифрованный сертификатом KRA» в блоке «Дополнительно» карточки. Такие шаблоны отмечены в реестре шаблонов в столбце «Шифрование ключа». При запросе сертификата по такому шаблону вместе с CSR загружается файл закрытого ключа, а в карточке выпущенного сертификата появляется кнопка **Скачать зашифрованный ключ**.

Функции агента восстановления ключей настраиваются администратором при развёртывании (см. Руководство администратора). Кнопка **Скачать зашифрованный ключ** выводится в карточке сертификата, если ЦС хранит закрытый ключ этого сертификата.

15 Выпуск и проверка сертификатов по протоколам

Сертификат можно получить через Контрольную панель или автоматически, по стандартному протоколу выпуска. Клиент сам создаёт закрытый ключ и запрос и отправляет запрос адаптеру протокола. Клиентом может быть сетевое устройство, сервер Linux или компьютер Windows. Адаптер проверяет право клиента на сертификат и передаёт запрос в ЦС. Закрытый ключ остаётся на клиенте.

Выпущенные так сертификаты попадают в реестр «Сертификаты» того ЦС, к которому подключён адаптер. Искать, скачивать и отзывать их нужно там же (см. «Сертификаты»). Проверить, не отозван ли сертификат, приложения могут по протоколу OCSP (см. «Проверка статуса по протоколу OCSP»).

Протокол	**Кому подходит**	**Как клиент подтверждает право на сертификат**	**Поставка**
SCEP	Сетевое оборудование, серверы Linux со службой certmonger, другие клиенты SCEP	Одноразовым паролем (challenge), полученным заранее	Устанавливается установщиком Clearway CA (группа SCEP)
MS-WSTEP	Компьютеры и пользователи Windows в домене Active Directory	Доменной учётной записью (Kerberos)	Устанавливается установщиком Clearway CA (группа MS-WSTEP); нужен домен Active Directory
ACMEv2, CMP, EST, MS-RPC	Клиенты этих протоколов	Зависит от адаптера	Отдельные адаптеры, в штатную поставку не входят

Адаптеры устанавливает и настраивает администратор. Он же задаёт в настройках адаптера шаблон ЦС, по которому выпускаются сертификаты; по умолчанию это шаблон tls.

Перед началом узнайте у администратора:

- адрес службы протокола;
- шаблон, по которому выпускаются сертификаты;
- как получить корневой сертификат ЦС и его отпечаток для сверки.

15.1 SCEP

Простой протокол выпуска сертификатов SCEP (Simple Certificate Enrollment Protocol) поддерживается сетевым оборудованием и многими операционными системами. Выпуск проходит в три шага:

1. Пользователь или администратор под своей учётной записью получает у адаптера одноразовый пароль.
2. Клиент SCEP создаёт ключ и запрос, вкладывает в запрос пароль и отправляет его адаптеру.
3. Адаптер проверяет пароль, передаёт запрос в ЦС и возвращает клиенту выпущенный сертификат. Пароль после этого считается использованным.

Параметр	Назначение и источник значения
Адрес службы SCEP	Адрес, по которому клиент обращается к адаптеру. Сообщает администратор; при установке по умолчанию он имеет вид `https://<сервер служб>/api/v1/scep`. Путь указывайте точно так, как его сообщил администратор, с учётом регистра букв
Корневой сертификат ЦС	Нужен клиенту, чтобы доверять HTTPS-соединению с адаптером. Получите его у администратора и сверьте отпечаток
Сертификат адаптера (RA) и сертификат выдающего ЦС	Адаптер подписывает ответы сертификатом RA. Оба сертификата клиент получает запросом GetCACert (см. шаг 2 в «Получение сертификата с помощью certmonger»)
Одноразовый пароль (challenge)	Подтверждает право на выпуск. Подходит только для одного запроса; по умолчанию действует 60 минут

15.1.1 Получение одноразового пароля

Адаптер выдаёт пароль по адресу `<адрес службы SCEP>/challenge-password`. Запрос выполняется от имени пользователя: подлинность подтверждается токеном доступа, который выдаёт служба аутентификации OpenID. Как получить токен в вашей инсталляции, уточните у администратора. Токен по умолчанию действует две минуты, поэтому запрашивайте пароль сразу после получения токена.

Получайте пароль непосредственно перед запросом сертификата и сохраняйте его на сервере, которому нужен сертификат. Команда ниже создаёт файл пароля, доступный только владельцу:

```
(umask 077; curl -sSf --cacert /root/scep/root-ca.pem \
  -H "Authorization: Bearer <токен доступа>" \
  "<адрес службы SCEP>/challenge-password" -o /root/scep/challenge.txt)
```

В успешном ответе приходит пароль одной строкой, без кавычек и перевода строки. Если curl сообщает об ошибке, получите новый токен и повторите запрос. Если ошибка повторяется, сверьте адрес службы с администратором.

15.1.2 Получение сертификата с помощью certmonger

Служба Linux certmonger запрашивает сертификаты и следит за их сроком действия. Команды ниже выполняются от имени root на сервере, которому нужен сертификат. Пакет certmonger устанавливается из репозитория дистрибутива, например `apt-get install certmonger`.

В примере файлы хранятся в каталоге /root/scep: корневой сертификат root-ca.pem, файл пароля challenge.txt, а закрытый ключ находится в подкаталоге private. certmonger сам создаёт файлы ключа и сертификата, но не каталоги, поэтому создайте их заранее:

```
mkdir -p /root/scep/private && chmod 700 /root/scep/private
```

Шаг 1. Добавьте корневой сертификат ЦС в системное хранилище доверия. certmonger проверяет по нему HTTPS-соединение с адаптером; без этого запрос завершится ошибкой (см. таблицу ошибок ниже).

```
# Альт
cp /root/scep/root-ca.pem /etc/pki/ca-trust/source/anchors/clearway-root-ca.pem &&
update-ca-trust extract
# Astra Linux, Debian
cp /root/scep/root-ca.pem /usr/local/share/ca-certificates/clearway-root-ca.crt &&
update-ca-certificates
```

Шаг 2. Получите сертификаты адаптера и ЦС:

```
cd /root/scep
curl -sSf --cacert root-ca.pem "<адрес службы SCEP>?operation=GetCACert" -o scep-ca.p7b
openssl pkcs7 -inform DER -in scep-ca.p7b -print_certs
```

Ответ содержит сертификат адаптера (RA) и сертификаты ЦС. Чей это сертификат, видно в строке `subject=` перед ним: у сертификата RA в поле CN указано имя сервера служб. Скопируйте каждый блок от строки BEGIN CERTIFICATE до строки END CERTIFICATE включительно: сертификат RA в файл `scep-ra.pem`, сертификат выдающего ЦС в файл `issuing-ca.pem`. Если одна из команд завершается ошибкой, сверьте адрес службы с администратором.

Шаг 3. Зарегистрируйте адаптер в certmonger и проверьте запись:

```
getcert add-scep-ca -c Clearway-SCEP -u "<адрес службы SCEP>" \
  -R /root/scep/root-ca.pem -N /root/scep/issuing-ca.pem -r /root/scep/scep-ra.pem
```

```
getcert list-cas -c Clearway-SCEP
```

Параметр	Назначение
`-c`	Имя подключения в certmonger, выбирается произвольно
`-u`	Адрес службы SCEP
`-R`	Корневой сертификат ЦС
`-N`	Сертификат выдающего ЦС. Если сертификаты выпускает сам корневой ЦС, укажите корневой сертификат
`-r`	Сертификат адаптера (RA)

Файлы указывайте полными путями: служба certmonger читает их позже, при каждом обращении к адаптеру. При успехе выводится сообщение `New CA "Clearway-SCEP" added.`, а `getcert list-cas` показывает подключение с указанным адресом.

Шаг 4. Получите одноразовый пароль (см. «Получение одноразового пароля») и запросите сертификат:

```
getcert request -c Clearway-SCEP -I web01 -G RSA -g 2048 \
  -k /root/scep/private/web01.key -f /root/scep/web01.crt \
  -N CN=web01.example.local -D web01.example.local \
  -l /root/scep/challenge.txt -R -w --wait-timeout 90
```

Параметр	Назначение
`-c`	Имя подключения из шага 3
`-I`	Имя задачи в certmonger, по нему задача указывается в следующих командах
`-G`, `-g`	Тип и длина ключа. Должны удовлетворять требованиям шаблона к типу и размеру ключа
`-k`, `-f`	Файлы закрытого ключа и сертификата

`-N`, `-D`	Subject и DNS-имя в SAN сертификата
`-l`	Файл с одноразовым паролем
`-R`	Не продлевать сертификат автоматически. Повторный выпуск описан ниже
`-w`, `--wait-timeout`	Дождаться результата, но не дольше указанного числа секунд. По истечении времени задача не отменяется

Шаг 5. Проверьте результат:

```
getcert list -i web01
openssl x509 -in /root/scep/web01.crt -noout -subject -issuer -serial -dates -ext
subjectAltName
```

Выпуск прошёл успешно, если задача в состоянии `status: MONITORING`, `stuck: no`, файл сертификата создан, а Subject и SAN совпадают с запросом. В реестре «Сертификаты» сертификат появляется с шаблоном, заданным для адаптера.

Чтобы выпустить сертификат повторно, например перед окончанием срока действия, получите новый одноразовый пароль, запишите его в тот же файл и выполните `getcert resubmit -i web01`. Прежний сертификат автоматически не отзывается. Если он больше не нужен, отзовите его в Контрольной панели.

Что видно в `getcert list`	**Причина**	**Что сделать**
`CA_UNREACHABLE`, `Error 60 … SSL peer certificate or SSH remote key was not OK`	Клиент не доверяет TLS-сертификату адаптера	Выполните шаг 1, затем `getcert resubmit -i <имя задачи>`
Задача не перешла в состояние `MONITORING`, сертификат не выпущен	Адаптер отклонил запрос, например одноразовый пароль уже использован или не передан	Получите новый пароль, запишите его в файл и выполните `getcert resubmit -i <имя задачи>`. Если выпуск снова не удался, обратитесь к администратору

`NEED_CSR_GEN_PIN`, `stuck: yes`	Файл пароля пуст	Запишите в файл новый пароль и выполните `getcert resubmit -i <имя задачи>`

Сетевое оборудование с поддержкой SCEP подключается по тем же данным. В настройках оборудования укажите адрес службы SCEP, корневой сертификат ЦС и одноразовый пароль. Порядок команд описан в документации производителя.

15.2 MS-WSTEP

Windows запрашивает сертификаты у служб регистрации по протоколу Microsoft MS-WSTEP. Для клиента выпуск выглядит так же, как в центре сертификации Microsoft: используются штатные оснастки и команды Windows. Адаптер состоит из двух служб:

- CEP (служба политик регистрации) сообщает компьютеру, какие шаблоны доступны и куда отправлять запрос;
- CES (служба регистрации) принимает запрос, передаёт его в ЦС и возвращает сертификат.

Подлинность клиента подтверждается доменной учётной записью по протоколу Kerberos: учётной записью компьютера при выпуске сертификата компьютера или учётной записью пользователя при выпуске личного сертификата.

Параметр	**Назначение и источник значения**
Адрес службы политик (CEP)	`https://<сервер служб>/CEP_Kerberos/service.svc/CEP`. Сообщает администратор; также указан в сценарии add_enrollment_policy.ps1, который формирует установщик
Адрес службы регистрации (CES)	`https://<сервер служб>/CES_Kerberos/service.svc/CES`. Windows получает его из политики сама, вручную он не вводится
Шаблон	Имя шаблона, опубликованного в Active Directory, по умолчанию tls. Описание шаблона в Active Directory только делает шаблон видимым для Windows. Срок действия и расширения сертификата определяет шаблон ЦС, заданный в настройках адаптера
Контекст	Сертификат компьютера (оснастка certlm.msc, нужны права локального администратора) или сертификат пользователя (оснастка certmgr.msc)

Требования к компьютеру-клиенту:

- компьютер входит в домен Active Directory;
- корневой сертификат ЦС установлен в хранилище «Доверенные корневые центры сертификации». Для сертификата компьютера нужно хранилище компьютера (certlm.msc);
- имя сервера служб разрешается в DNS и совпадает с именем в его TLS-сертификате.

15.2.1 Подготовка домена

Выполняется один раз администратором домена. После настройки MS-WSTEP установщик формирует три файла. Администратор Clearway CA скачивает их в карточке завершённой настройки группы MS-WSTEP:

- template_tls_export.ldf: описание шаблона;
- enrollment_services.ldf: описание службы регистрации;
- add_enrollment_policy.ps1: сценарий, который импортирует оба описания и регистрирует политику на компьютере в контексте компьютера. Его можно запустить от имени администратора вместо ручных шагов ниже.

Вручную описания импортируются в Active Directory командами:

```
New-Item -ItemType Directory -Path .\template-log,.\enrollment-log -Force
ldifde -i -h -f .\template_tls_export.ldf -s <контроллер домена> -j .\template-log
ldifde -i -h -f .\enrollment_services.ldf -s <контроллер домена> -j .\enrollment-log
```

Каждая команда должна сообщить об одной успешно изменённой записи (в английской версии Windows: `1 entry modified successfully`) и завершиться с кодом 0. Для импорта нужны права на изменение раздела конфигурации Active Directory. Шаблон становится доступен клиентам после того, как службы CEP и CES перечитают каталог.

15.2.2 Регистрация политики на компьютере

Выполняется один раз на каждом компьютере-клиенте.

1. Откройте оснастку certlm.msc (сертификаты компьютера) или certmgr.msc (сертификаты пользователя).
2. Щёлкните правой кнопкой папку «Личное» (Personal) и выберите «Все задачи» → «Дополнительные операции» → «Управление политиками регистрации» (All Tasks → Advanced Operations → Manage Enrollment Policies).
3. Нажмите «Добавить» (Add), введите адрес службы политик (CEP) и выберите тип проверки подлинности «Встроенная проверка подлинности Windows» (Windows integrated).
4. Нажмите «Проверить сервер» (Validate Server). Дождитесь сообщения об успешной проверке.
5. Нажмите «Добавить» (Add). Новая политика появится в списке; нажмите «Применить» (Apply).

То же самое в PowerShell:

```
$cepUrl = 'https://<сервер служб>/CEP_Kerberos/service.svc/CEP'
Add-CertificateEnrollmentPolicyServer -Url $cepUrl -Context Machine
-RequireStrongValidation -NoClobber
Get-CertificateEnrollmentPolicyServer -Url $cepUrl -Context Machine -Scope All
```

Для контекста компьютера (`-Context Machine`) PowerShell запускается от имени администратора. Для политики пользователя укажите `-Context User` ; команду выполняет сам пользователь. Политика зарегистрирована, если вторая команда выводит её с этим же адресом (`Url`) и типом проверки подлинности `AuthType: Kerberos` .

15.2.3 Запрос сертификата

1. В certlm.msc или certmgr.msc щёлкните правой кнопкой «Личное» → «Сертификаты» и выберите «Все задачи» → «Запросить новый сертификат» (All Tasks → Request New Certificate).
2. Нажмите «Далее» (Next), выберите зарегистрированную политику и снова нажмите «Далее».
3. Отметьте шаблон. Если под шаблоном есть ссылка на ввод дополнительных сведений, заполните их.
4. Нажмите «Заявка» (Enroll). Дождитесь сообщения об успешном выпуске и нажмите «Готово» (Finish).

Запрос сертификата компьютера из командной строки (PowerShell от имени администратора):

```
$cepUrl = 'https://<сервер служб>/CEP_Kerberos/service.svc/CEP'
certreq -enroll -machine -q -kerberos -policyserver $cepUrl tls
$LASTEXITCODE
Get-ChildItem Cert:\LocalMachine\My | Sort-Object NotBefore -Descending |
  Select-Object -First 1 Subject, Issuer, SerialNumber, NotAfter, HasPrivateKey
```

В команде certreq указано имя шаблона tls. Выпуск прошёл успешно, если `$LASTEXITCODE` равен 0, а в хранилище «Личное» появился новый сертификат с закрытым ключом (`HasPrivateKey: True`). В реестре «Сертификаты» Контрольной панели он появляется с тем же серийным номером; в столбце Requester Name указана учётная запись компьютера, например WS01$.

Чтобы проверить цепочку и отзыв, сохраните сертификат в файл и проверьте его:

```
$cert = Get-ChildItem Cert:\LocalMachine\My | Sort-Object NotBefore -Descending |
Select-Object -First 1
Export-Certificate -Cert $cert -FilePath .\cert.cer
certutil -verify -urlfetch .\cert.cer
```

Код завершения certutil здесь ничего не доказывает: он равен 0, даже если отзыв проверить не удалось. Смотрите на вывод. В английской версии Windows проверка пройдена, если вывод содержит `Leaf certificate revocation check passed` и `CertUtil: -verify command completed successfully`. Сообщение `CRYPT_E_REVOCATION_OFFLINE` означает, что по адресам из сертификата недоступны сведения об отзыве: CRL, Delta CRL или OCSP-ответчик. В этом случае проверьте публикацию списков отзыва (см. «Задачи публикации») и доступность ответчика (см. «Проверка статуса по протоколу OCSP»).

Что происходит	Причина	Что сделать
Проверка сервера или Add-CertificateEnrollmentPolicyServer завершается ошибкой	Служба CEP недоступна по сети, адрес неверен, компьютер не доверяет TLS-сертификату сервера служб или не входит в домен	Сверьте адрес с администратором, проверьте доступность сервера служб и наличие корневого сертификата в доверенных
В окне запроса нет нужного шаблона	Описание шаблона или службы регистрации не импортировано в Active Directory, либо службы CEP и CES не перечитали каталог после импорта	Обратитесь к администратору домена и администратору Clearway CA
Политика зарегистрирована, но certreq завершается ошибкой	Службы CEP и CES не прочитали описания из Active Directory	Сообщите администратору Clearway CA текст ошибки

15.3 Проверка статуса по протоколу OCSP

Протокол OCSP (Online Certificate Status Protocol) служит для проверки статуса одного сертификата. Приложение отправляет OCSP-ответчику серийный номер сертификата и получает подписанный ответ: сертификат действителен, отозван или неизвестен. Скачивать весь список отзыва (CRL) при этом не нужно.

Ответчик Clearway CA по умолчанию определяет статус по базе данных ЦС в момент запроса. Поэтому он не зависит от расписания публикации CRL. Источник статуса (база данных ЦС или CRL) задаёт администратор (см. Руководство администратора).

Параметр	Назначение и источник значения
Адрес OCSP-ответчика	Записан в поле Authority Information Access (AIA) сертификата, в строке OCSP; его также сообщает администратор. При установке по умолчанию: `http://<сервер служб>:8888/ocsp`

Сертификат выдающего ЦС	ЦС, выпустивший проверяемый сертификат. Нужен, чтобы сформировать запрос
Корневой сертификат ЦС	Нужен, чтобы проверить подпись ответа
Проверяемый сертификат	Файл сертификата или его серийный номер из столбца Serial Number реестра «Сертификаты»

Приложения, например браузеры, Windows и веб-серверы, берут адрес ответчика из поля AIA и проверяют статус сертификата сами. Посмотреть адрес можно в карточке сертификата, в поле Authority Information Access.

Проверить статус вручную можно командой openssl:

```
openssl ocsp -issuer issuing-ca.pem -cert web01.crt \
  -url "http://<сервер служб>:8888/ocsp" -CAfile root-ca.pem
```

Параметр	Назначение
`-issuer`	Сертификат выдающего ЦС
`-cert`	Проверяемый сертификат. Вместо файла можно указать серийный номер: `-serial 0x<Serial Number>`, например `-serial 0x100000000000000000009`
`-url`	Адрес OCSP-ответчика
`-CAfile`	Корневой сертификат ЦС для проверки подписи ответа

Первая строка вывода показывает, можно ли доверять ответу, вторая показывает статус сертификата:

Вывод	Что означает
`Response verify OK`	Подпись ответа проверена: ответ выдал ответчик вашего ЦС
`web01.crt: good`	Сертификат не отозван

`revoked`, `Reason: …`, `Revocation Time: …`	Сертификат отозван; указаны причина и время отзыва. Причина `certificateHold` означает, что сертификат приостановлен
`unknown`	ЦС не знает сертификата с таким серийным номером
`This Update`, `Next Update`	Время формирования ответа и срок, до которого ответ считается актуальным. По умолчанию это один час

Ошибка	**Причина**	**Что сделать**
`Response Verify Failure`	Подпись ответа не проверена: в `-CAfile` указан не тот сертификат	Укажите корневой сертификат ЦС. Статусу, напечатанному после этой ошибки, доверять нельзя
`Responder Error: unauthorized (6)`	В `-issuer` указан не тот ЦС, которым выпущен сертификат	Укажите сертификат ЦС из поля «Издатель» (Issuer) проверяемого сертификата
`Error querying OCSP responder … Code=404`	Неверный путь в адресе ответчика	Сверьте адрес с администратором
`Error connecting BIO`, `Connection refused`	Ответчик недоступен по указанному адресу и порту	Проверьте адрес и сетевую доступность, обратитесь к администратору

15.4 Другие протоколы

Адаптеры ACMEv2, CMP, EST и MS-RPC в штатную поставку не входят и устанавливаются отдельно. Если такой адаптер установлен, адрес службы и способ подтверждения права на сертификат сообщает администратор. Порядок работы описан в документации адаптера.

16 Работа через командную строку (mclient)

Утилита mclient служит для управления центром сертификации из командной строки. Она выполняет те же операции, что и веб-интерфейс, обращаясь к API центра сертификации, и применяется для автоматизации и пакетной обработки. Команды mclient авторизуются на ЦС по токену JWT, а назначенная роль определяет доступный набор операций.

16.1 Подготовка

Перед вызовом укажите путь к файлу конфигурации клиента и проверьте связь с ЦС:

```
export MCLIENT_CONF=/opt/itc/minica/conf/mclient.yml
# связь со службой ЦС, версия ЦС и SKI
./mclient ping
```

Настройка mclient (путь к конфигурации, учётные данные и JWT) выполняется при развёртывании и описана в Руководстве администратора. Полный перечень команд и их параметров выводится при запуске ./mclient без аргументов.

16.2 Основные команды

Операция	**Команда**	**Аналог в интерфейсе**
Выпуск сертификата по шаблону	`./mclient ca -csr request.csr -template tls -out cert.crt`	«Запрос сертификата»
Проверка статуса сертификата	`./mclient status`	Столбец «Статус» реестра сертификатов
Получение сертификата из базы данных	`./mclient get`	«Скачивание сертификата»
Массовая выгрузка сертификатов	`./mclient export`	«Скачать сертификаты» в реестре
Отзыв сертификата	`./mclient revoke`	«Отзыв сертификата»
Восстановление сертификата (для причины CertificateHold)	`./mclient repair`	«Восстановление сертификата»

Обновление CRL	`./mclient updcrl`	«Обновление CRL»
Обновление Delta CRL	`./mclient updeltacrl`	«Обновление CRL», режим «Только Delta CRL»
Список шаблонов	`./mclient templates`	Реестр шаблонов
Параметры шаблона	`./mclient gettempl`	Карточка шаблона
Создание шаблона	`./mclient addtempl`	«Создание шаблона»
Удаление шаблона	`./mclient deltempl`	«Удаление шаблона»
Показатели состояния ЦС	`./mclient stat`	Страница «Статистика ЦС» (см. «Самодиагностика»)

Пример: выпуск сертификата по шаблону tls из файла запроса request.csr в файл cert.crt.

```
export MCLIENT_CONF=/opt/itc/minica/conf/mclient.yml
./mclient ca -csr request.csr -template tls -out cert.crt
```