Общее описание Clearway CA 26.3.0

Документация Clearway CA

6 November, 2026

Table of Contents

1 О продукте ... 3
2 Архитектура и компоненты ... 4
3 Ключевые возможности ... 6
4 Редакции: бесплатная и платная ... 7
5 Веб-интерфейс (Контрольная панель) ... 8
5.1 Вход и авторизация ... 8
5.2 Навигация по разделам ... 9
5.3 Профиль и права доступа ... 9
5.4 Реестр сертификатов: поиск и фильтрация ... 10
5.5 Конструктор CSR-запросов ... 13
5.6 Выпуск сертификата ... 14
5.7 Карточка сертификата и жизненный цикл ... 17
5.8 Шаблоны сертификатов ... 19
5.9 Запросы и согласование выпуска ... 21
5.10 События (аудит) ... 23
5.11 Списки отзыва (CRL и Delta CRL) ... 24
5.12 Статистика ЦС ... 26
5.13 Задачи публикации ... 26
5.14 Резервное копирование и восстановление ЦС ... 28
5.15 Типовые задачи ... 28
5.16 Настройки центра сертификации ... 29
5.17 Ротация ключа ЦС ... 31
5.18 Аппаратные токены ... 31

1 О продукте

Clearway CA служит центром сертификации (Certification Authority, ЦС) инфраструктуры открытых ключей (PKI). Система выпускает по шаблонам сертификаты стандарта X.509v3 по запросам CSR в формате PKCS#10, отзывает сертификаты с указанием причины, формирует списки отзыва (CRL и Delta CRL) и сообщает статус сертификатов по протоколу OCSP. Запросы, сертификаты, журналы событий и списки отзыва хранятся в базе данных. Управляют системой через веб-интерфейс (Контрольную панель) и API, а для автоматического выпуска сертификатов она поддерживает протоколы SCEP и MS-WSTEP.

Разработчик: ООО «Клируэй Текнолоджис». Clearway CA создан на основе одного из модулей ПО «Система централизованного анализа и управления гетерогенными инфраструктурами», зарегистрированного в Реестре российского ПО (реестровая запись № 13033 от 21.03.2022). У продукта расширенный состав функций, его можно устанавливать отдельно.

Документ наглядно показывает возможности Clearway CA версии 26.3.0: назначение продукта, состав компонентов и работу с системой через веб-интерфейс на примере реальных экранов. Данные в примерах (имена, домены, счётчики) обезличены и служат иллюстрацией.

2 Архитектура и компоненты

Clearway CA построен по модульному принципу: ядро центра сертификации дополняют сервисы аутентификации, публикации, проверки статуса, обслуживания и адаптеры протоколов выпуска. Компоненты работают на серверах под управлением ОС Linux. Основные из них устанавливает веб-установщик (графический мастер установки, который открывается в браузере и разворачивает компоненты на серверы по SSH). При необходимости сервисы можно развернуть и вручную. Контрольная панель, сервис публикации и адаптеры протоколов обращаются к ядру ЦС по HTTPS, предъявляют выданный ЦС токен JWT и подписывают запросы своим ключом. Пароли и другие секреты компонентов можно хранить не в файлах конфигурации, а во внешнем хранилище секретов (EXC).

Компонент	**Назначение**
Центр сертификации (ядро)	Выпускает и отзывает сертификаты X.509v3 по шаблонам, формирует CRL и Delta CRL, хранит запросы, сертификаты и журнал событий в БД. Одна и та же программа работает корневым и выдающим ЦС (двухуровневая иерархия). При ротации ключа ядро формирует запрос на новый сертификат ЦС и устанавливает его
База данных (PostgreSQL)	Хранит запросы, сертификаты, шаблоны, события и списки отзыва; для архива и сервиса аутентификации заведены отдельные базы данных
Сервис аутентификации (OpenID)	Даёт единый вход (SSO) по OpenID Connect, проверяет учётные записи в каталоге LDAP/Active Directory, сопоставляет группы каталога с правами Clearway CA; для входа без каталога есть встроенная учётная запись
Контрольная панель	Веб-интерфейс для работы с одним или несколькими ЦС через браузер. Из неё также управляют задачами публикации, резервным копированием, ротацией ключа ЦС и типовыми задачами замены сертификатов
Сервис публикации	По расписанию cron публикует сертификаты в каталоги LDAP (Active Directory, Samba), а списки отзыва в каталог на сервере, на удалённый сервер по SCP или в каталог LDAP
OCSP-ответчик (mOCSP)	Сообщает статус отдельного сертификата по протоколу OCSP в момент запроса. По умолчанию берёт статус из БД ЦС, источником может быть и CRL
Архиватор	По расписанию (по умолчанию раз в сутки) переносит истёкшие сертификаты вместе с запросами и событиями из рабочей БД в отдельную архивную БД

Сервис резервного копирования	Выполняет задания резервного копирования и восстановления ЦС, которые настраиваются в Контрольной панели: копирует БД ЦС, а с узлов ЦС по SSH файлы конфигурации и исполняемый файл ЦС, хранит копии и восстанавливает из них ЦС
Адаптер SCEP	Выпускает и обновляет сертификаты по протоколу SCEP для сетевого оборудования, серверов Linux (служба certmonger) и других клиентов SCEP. Право на выпуск клиент подтверждает одноразовым паролем
Адаптер MS-WSTEP	Выпускает сертификаты компьютерам и пользователям Windows в домене Active Directory через штатные средства ОС. Состоит из службы политик регистрации (CEP) и службы регистрации (CES), подлинность клиента подтверждается по Kerberos
Точка распространения (CDP)	Раздаёт по HTTP файлы CRL, Delta CRL и сертификаты ЦС по адресам CDP и AIA, которые ЦС записывает в выпускаемые сертификаты

Кроме веб-интерфейса, функции центра сертификации доступны через утилиту командной строки mclient и через API ядра ЦС: те же операции API вызывает и серверная часть Контрольной панели. Адаптеры SCEP и MS-WSTEP разворачивает штатный установщик, а адаптеры ACMEv2, CMP, EST и MS-RPC поставляются отдельно.

3 Ключевые возможности

- Выпуск сертификатов X.509v3 по запросам CSR (PKCS#10) с контролем атрибутов по шаблонам: одиночный и пакетный выпуск, выпуск с согласованием запроса.
- Автоматический выпуск сертификатов по протоколам SCEP (сетевое оборудование, серверы Linux) и MS-WSTEP (компьютеры и пользователи Windows в домене Active Directory).
- Конструктор CSR-запросов: команда openssl для Linux, INF-файл и команда certreq для Windows или ключ и запрос прямо на аппаратном токене (Рутокен, JaCarta, КриптоПро CSP).
- Управление жизненным циклом: просмотр, скачивание в форматах PEM и DER, отзыв с указанием причины и возврат в действие сертификата, отозванного с причиной CertificateHold.
- Формирование и публикация списков отзыва CRL и Delta CRL, проверка статуса сертификата по протоколу OCSP (OCSP-ответчик mOCSP).
- Поиск, выборки и отчёты с фильтрацией, выгрузка отчёта в файл Excel и массовая выгрузка сертификатов.
- Журнал событий и аудит всех операций ЦС, отдельный журнал событий безопасности ядра ЦС.
- Уведомления по электронной почте о выпуске, отзыве и истечении срока действия сертификата.
- Ролевая модель из 17 прав со стандартными ролями (администратор ЦС, аудитор, пользователь) и единый вход по OpenID Connect с интеграцией LDAP/Active Directory.
- Защита ключей и секретов: хранение закрытых ключей в БД в зашифрованном виде (агент восстановления ключей, KRA), ключ ЦС на аппаратном модуле HSM, шифрование данных сертификатов в БД, хранение паролей во внешнем хранилище секретов (EXC).
- Публикация сертификатов и CRL в каталоги LDAP (Active Directory, Samba) и на внешние серверы по расписанию.
- Самодиагностика: страница «Статистика ЦС» в Контрольной панели и команда mclient stat.
- Работа с несколькими ЦС из одной Контрольной панели.
- Резервное копирование и восстановление ЦС из Контрольной панели: задания выполняет отдельный сервис резервного копирования.
- Ротация ключа ЦС из Контрольной панели: запрос на новый сертификат ЦС формирует, а полученный сертификат проверяет и устанавливает ядро ЦС.
- Типовые задачи: пошаговая замена TLS-сертификатов на серверах nginx и PostgreSQL.
- Раздел «Аппаратные токены» для проверки рабочего места и работы с носителями Рутокен, JaCarta и КриптоПро CSP.
- Автоматизированная установка компонентов веб-установщиком и архивирование истёкших сертификатов.

4 Редакции: бесплатная и платная

Clearway CA распространяется в бесплатной и платной редакциях. Функциональные ограничения бесплатной редакции:

Параметр	Бесплатная редакция	Платная редакция
Скорость выпуска сертификатов	Не более 10 в минуту	Лицензионное ограничение бесплатной редакции не применяется
Общее количество сертификатов	Не более 2000	Лицензионное ограничение бесплатной редакции не применяется
Стартовый серийный номер	Фиксирован (нумерация с 1)	Настраивается
Кластеризация Active-Active	Недоступна	Настраивается
Хранение ключа ЦС на HSM (PKCS#11)	Недоступно	Доступно

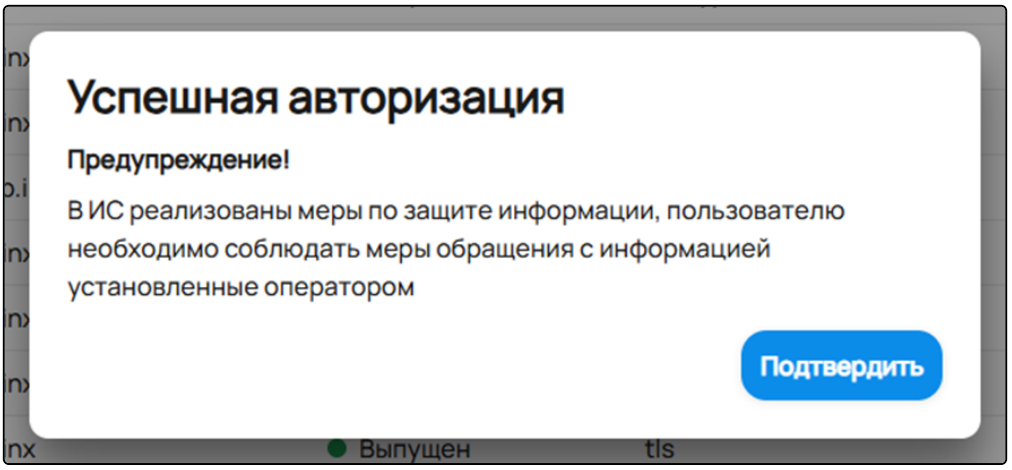
Производительность зависит от конфигурации инфраструктуры и выполняемых операций.

5 Веб-интерфейс (Контрольная панель)

Контрольная панель служит основным инструментом оператора: она даёт наглядный доступ к функциям центра сертификации через браузер и не требует высокой квалификации пользователя. Пользователь входит через сервис аутентификации OpenID (OpenID Connect с интеграцией каталогов LDAP/Active Directory), а какие разделы и кнопки ему доступны, определяют его права. Одна Контрольная панель может работать с несколькими ЦС: разделы показывают данные ЦС, выбранного на странице «Настройки → Конфигурация». Ниже разделы интерфейса показаны в порядке левого меню: от входа и реестра сертификатов до задач, настроек и аппаратных токенов.

5.1 Вход и авторизация

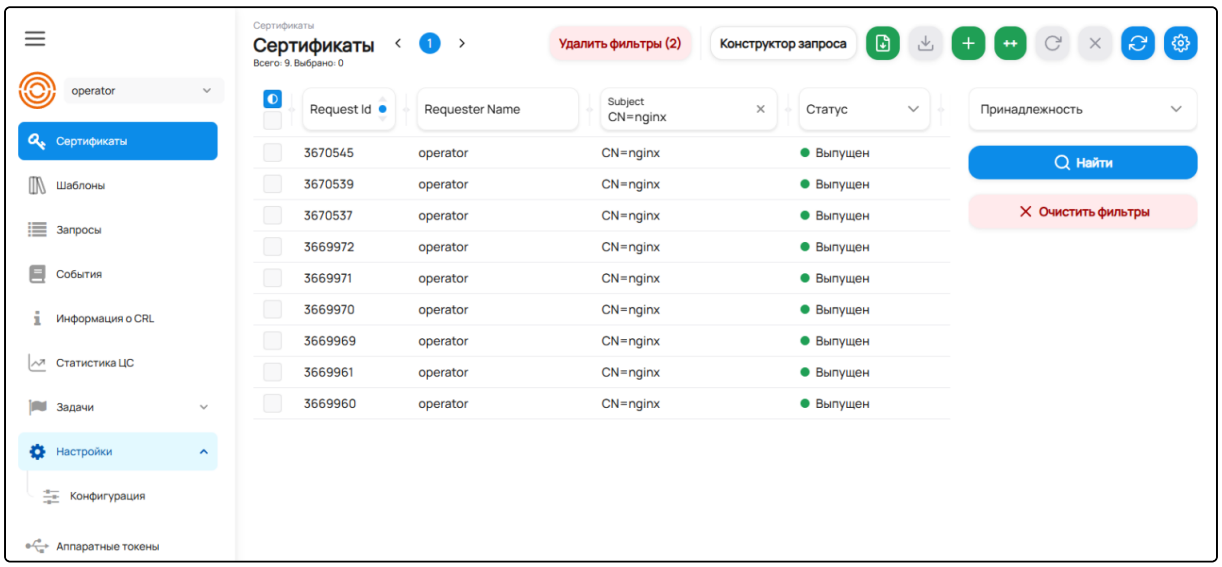
Контрольная панель Clearway CA открывается в обычном браузере. Система использует единую точку входа (SSO) по протоколу OpenID Connect: пользователь входит доменной учётной записью LDAP или Active Directory, поэтому отдельные учётные записи для ЦС заводить не нужно. Управлять доступом так проще, а вход опирается на правила безопасности, которые уже действуют в организации.



После входа открывается окно «Успешная авторизация» с предупреждением: в информационной системе реализованы меры по защите информации, и пользователю нужно соблюдать правила обращения с ней, установленные оператором. Нажатие **Подтвердить** означает, что пользователь ознакомлен с правилами; без подтверждения рабочая область не открывается. Окно появляется после каждого входа, затем открывается запрошенная страница или реестр «Сертификаты».

5.2 Навигация по разделам

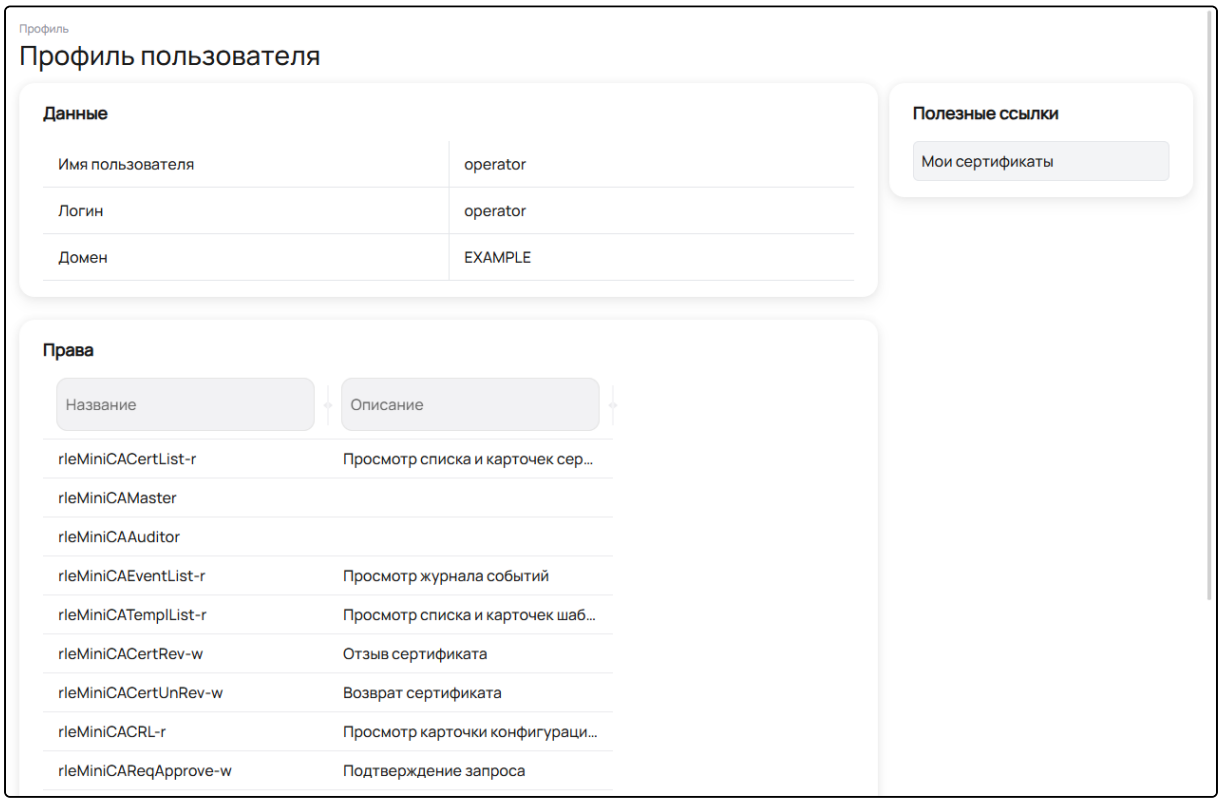
Левое меню всегда на экране: из любого места системы оператор одним щелчком переходит к нужному разделу, а справа открывается его рабочая область. Кнопка ☰ разворачивает меню или сворачивает его до значков, а пункт со стрелкой раскрывает вложенные пункты.



Левое меню содержит пункты «Сертификаты», «Шаблоны», «Запросы», «События», «Информация о CRL», «Статистика ЦС», «Задачи», «Настройки» и «Аппаратные токены»; пункт виден, только если у пользователя есть нужное право. Под логотипом выводится имя пользователя: щелчок по нему открывает меню с пунктами «Профиль» и «Выйти». По умолчанию открыт реестр «Сертификаты». Над столбцами расположены фильтры, справа боковая панель с полем «Принадлежность» и кнопками **Найти** и **Очистить фильтры**; в примере два условия отбора оставили 9 записей, а кнопка **Удалить фильтры (2)** сбрасывает оба условия. Номер страницы, условия отбора и сортировка сохраняются в адресной строке, поэтому ссылку на выборку можно добавить в закладки.

5.3 Профиль и права доступа

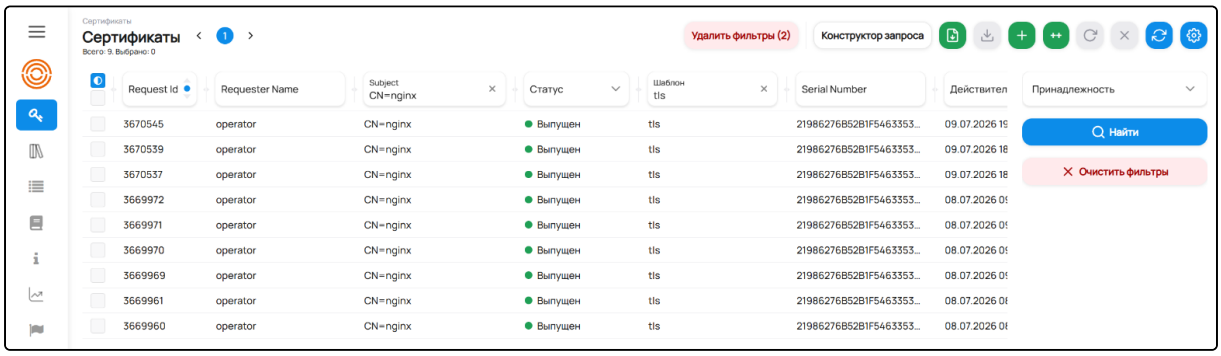
Доступ к функциям Контрольной панели разграничивает ролевая модель. В версии 26.3.0 определено 17 прав вида rleMiniCA<Право>: суффикс -r разрешает просматривать данные определённого типа, суффикс -w разрешает их изменять; четыре права добавлены для резервного копирования, восстановления и ротации ключа ЦС. Права не назначаются поштучно: пользователя включают в группу каталога LDAP или Active Directory, а сервис OpenID сопоставляет группе набор прав и передаёт его в токене JWT при входе. Стандартных ролей три: администратор ЦС (все 17 прав), аудитор (шесть прав на просмотр) и пользователь (просмотр сертификатов и шаблонов и запрос сертификата). Программные клиенты, например утилита mclient, обращаются к ЦС с сервисными токенами JWT, и набор их операций определяет роль в токене.



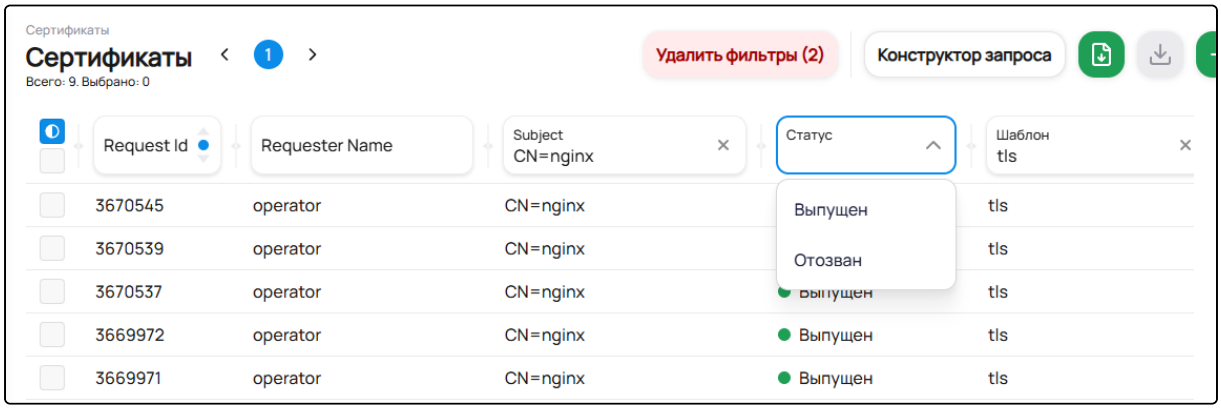
Экран «Профиль пользователя» открывается из меню пользователя. Блок «Данные» содержит имя пользователя, логин и домен (в примере учётная запись operator в домене EXAMPLE), а блок «Права» перечисляет назначенные права с названием и описанием, например rleMiniCACertList-r (просмотр списка и карточек сертификатов), rleMiniCACertRev-w (отзыв сертификата) или rleMiniCAReqApprove-w (подтверждение запроса). Ссылка «Мои сертификаты» в блоке «Полезные ссылки» открывает реестр сертификатов, запрошенных текущим пользователем. Если администратор изменил права, они вступают в силу после повторного входа.

5.4 Реестр сертификатов: поиск и фильтрация

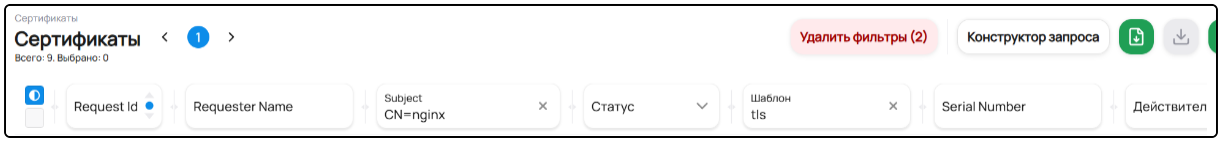
Раздел «Сертификаты» содержит реестр всех сертификатов, выпущенных центром сертификации, включая отозванные. Записи реестра можно искать, фильтровать, сортировать и листать постранично, а выборку выгрузить в файл Excel (до 10 000 записей). Так оператор быстро находит нужные записи даже в базе из миллионов сертификатов и готовит по ним отчётность.



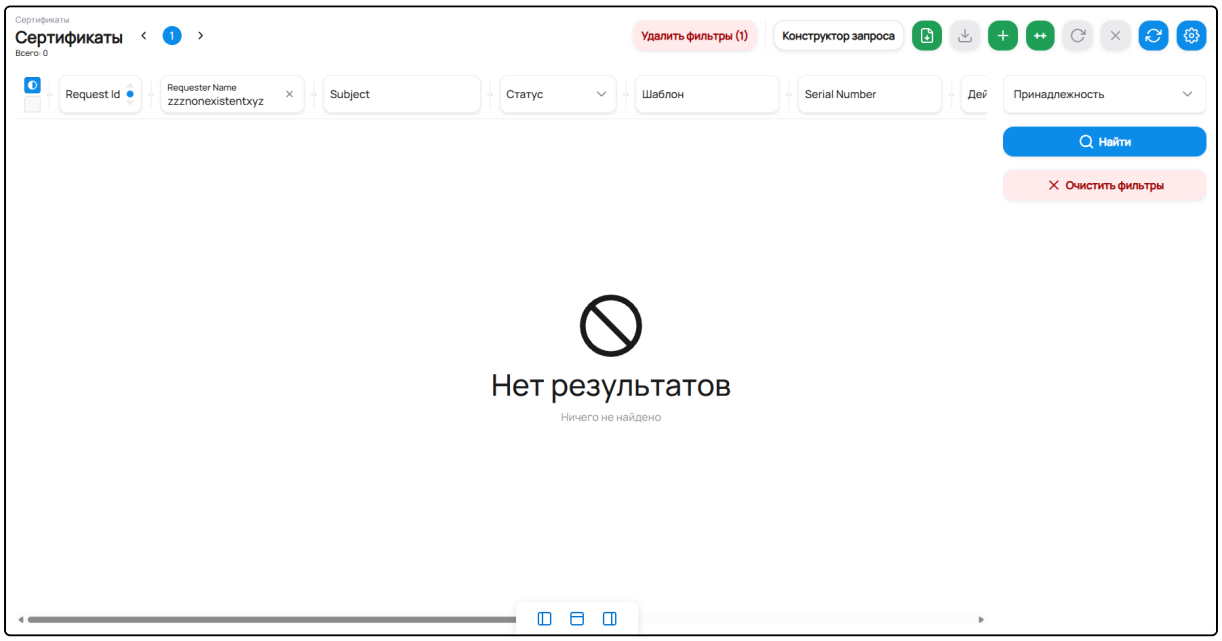
Каждая строка описывает один сертификат: Request Id (номер запроса), Requester Name (инициатор), Subject, статус, шаблон, Serial Number и срок действия. Кнопки над таблицей открывают конструктор CSR-запросов, выгружают отчёт, скачивают отмеченные сертификаты в формате PEM или DER, запрашивают один или сразу несколько сертификатов, восстанавливают приостановленные и отзывают выбранные сертификаты. Дополнительные столбцы, например SAN, Key Usage или причина отзыва, включаются в окне «Настройки таблицы».



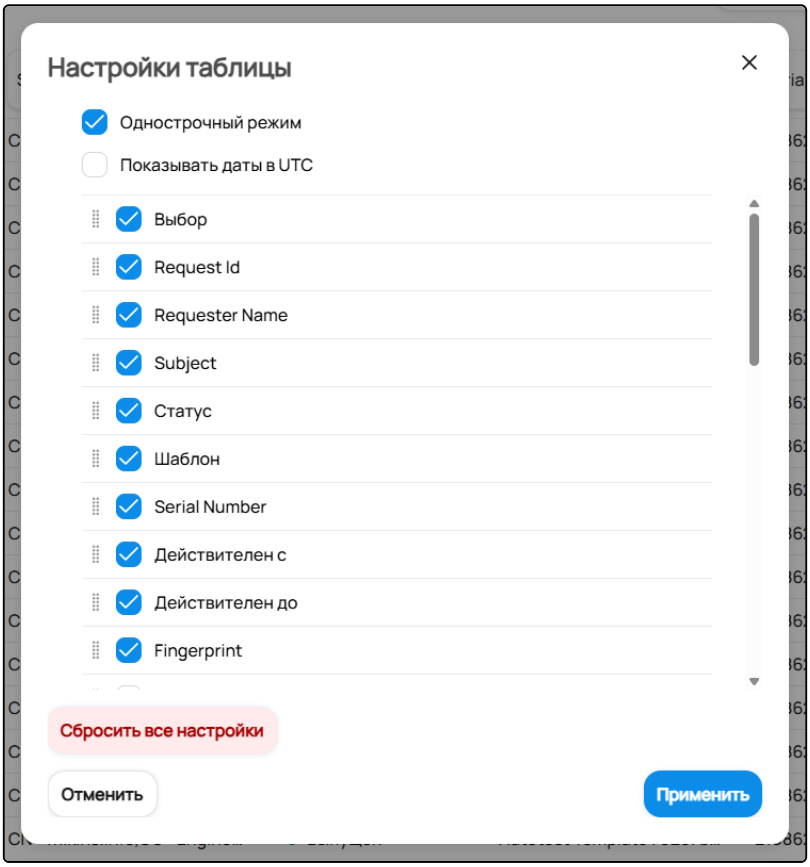
Поля над столбцами служат фильтрами: по тексту, числу, периоду дат или значению из списка. Щелчок по полю «Статус» раскрывает список значений «Выпущен» и «Отозван». Условия по нескольким столбцам объединяются, а кнопка **Найти** на боковой панели применяет все условия сразу.



Заданные условия видны в полях фильтров, а кнопка **Удалить фильтры (N)** показывает их число и одним нажатием сбрасывает все условия и сортировку. Кнопка **Очистить фильтры** на боковой панели снимает условия отбора, но сохраняет сортировку.



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

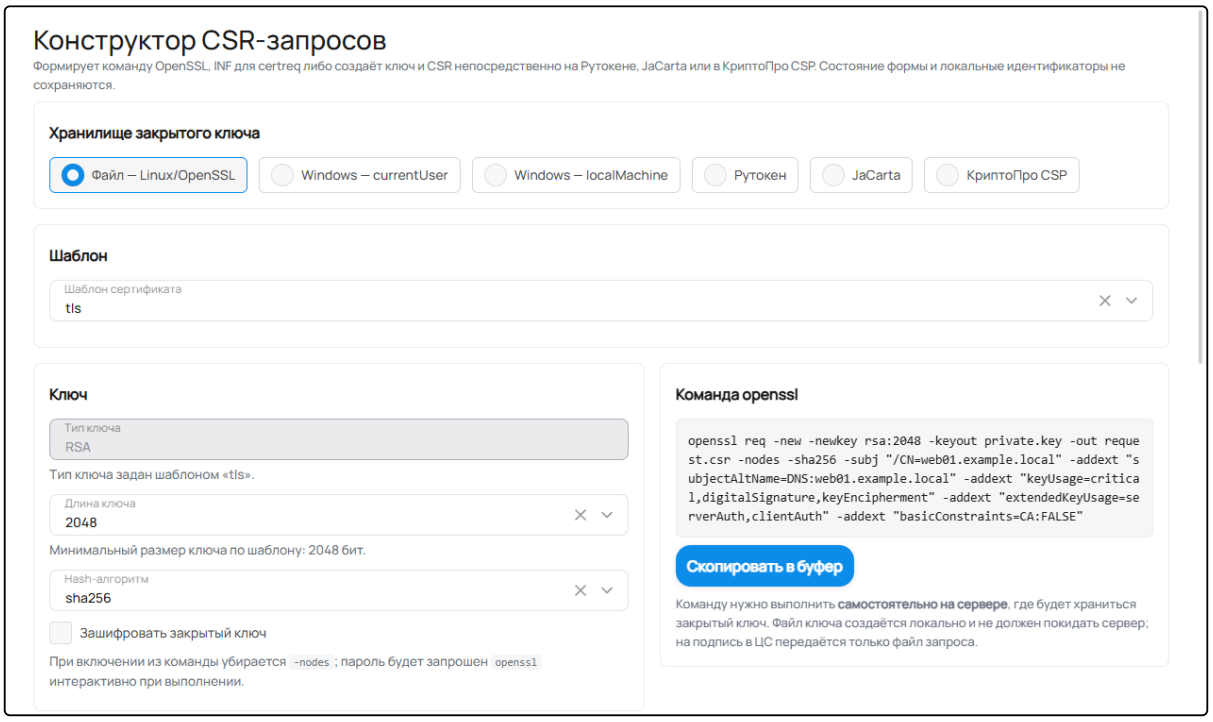


Окно «Настройки таблицы» управляет видом реестра: флажки включают и отключают столбцы, а перетаскивание за значок слева от названия меняет их порядок. Переключатели «Однострочный режим» и «Показывать даты в UTC» задают компактный вид строк и формат времени, а кнопки

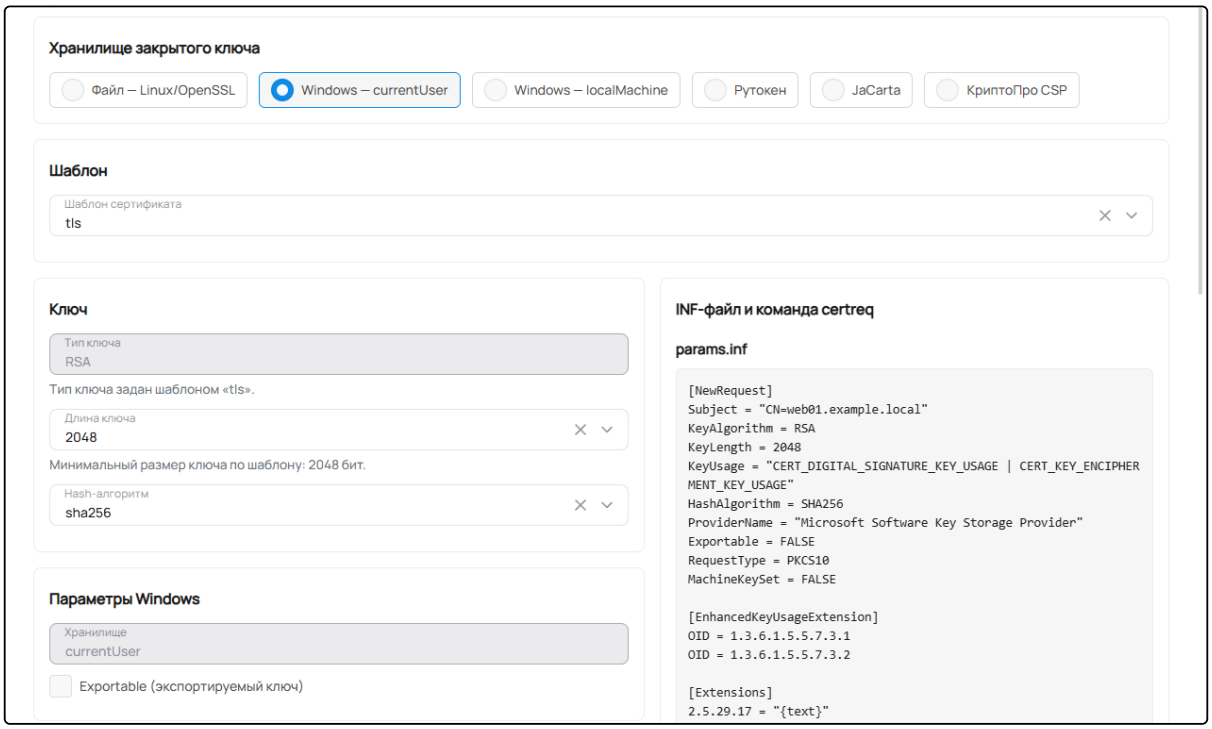
Сбросить все настройки, **Отменить** и **Применить** управляют сохранением изменений. Настройки хранятся в браузере отдельно для каждого реестра.

5.5 Конструктор CSR-запросов

Конструктор помогает подготовить запрос на сертификат (CSR) по выбранному шаблону так, чтобы закрытый ключ оставался на стороне пользователя: в ЦС уходит только запрос. Конструктор открывается кнопкой **Конструктор запроса** в реестре «Сертификаты», работает в браузере и ничего не сохраняет. В зависимости от выбранного хранилища закрытого ключа он формирует команду openssl для Linux, INF-файл и команду certreq для Windows или создаёт ключ и CSR прямо на носителе: Рутокене, JaCarta или в новом контейнере КриптоПро CSP.



В блоке «Хранилище закрытого ключа» выбирается, где будет создан ключ, а в блоке «Шаблон» выбирается шаблон сертификата. Шаблон задаёт тип ключа, минимальный размер ключа и значения extendedKeyUsage и keyUsage, в конструкторе их изменить нельзя; длину ключа, hash-алгоритм и имена файлов можно выбрать, а флажок «Зашифровать закрытый ключ» защищает ключ паролем. Имя владельца задаётся в блоке «Subject (DN)» (кнопка **+ Добавить RDN**), альтернативные имена в блоке «Subject Alternative Name (SAN)» (кнопка **+ Добавить SAN**). Как только заполнено хотя бы одно значение, в карточке «Команда openssl» собирается готовая команда: её копируют кнопкой **Скопировать в буфер** и выполняют на сервере, где будет храниться ключ.

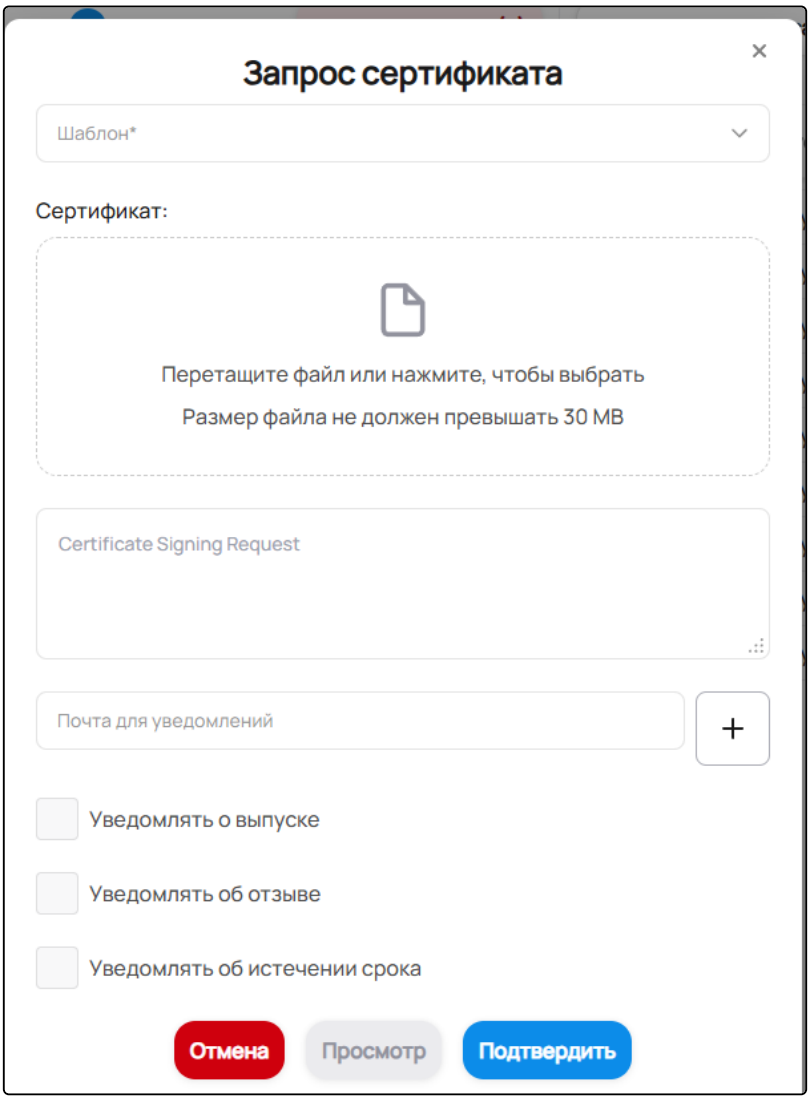


Для хранилищ Windows (currentUser и localMachine) конструктор формирует INF-файл (params.inf) и команду certreq -new. В блоке «Параметры Windows» ключ можно сделать экспортируемым флажком Exportable. INF-файл сохраняется кнопкой **Скачать INF-файл** или копируется кнопкой **Скопировать в буфер**, команду копирует кнопка **Скопировать команду**.

Для Рутокена, JaCarta и КриптоПро CSP ключ и CSR создаются прямо на носителе после ввода PIN-кода, который в ЦС не передаётся. По такому запросу сертификат можно сразу выпустить из конструктора и записать на носитель.

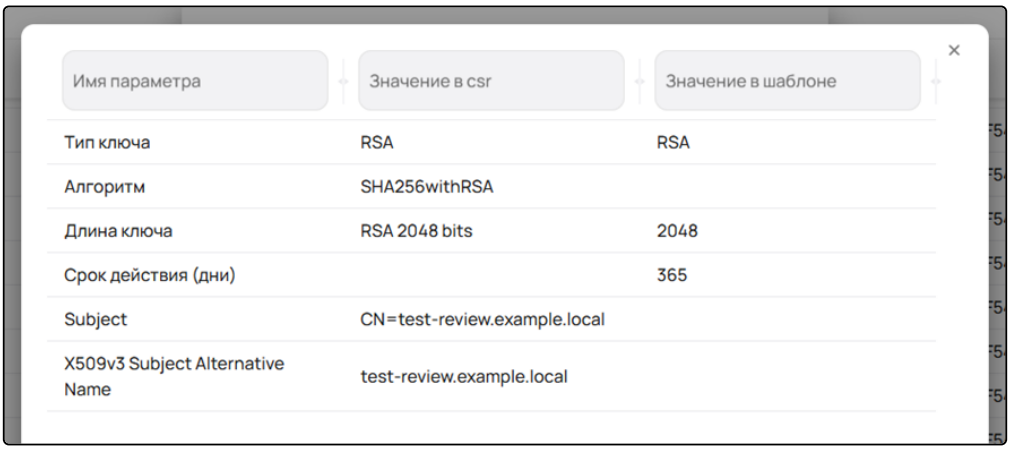
5.6 Выпуск сертификата

Прежде всего центр сертификации выпускает сертификаты. Оператор передаёт запрос на сертификат (CSR) и выбирает шаблон, а ЦС проверяет запрос по ограничениям шаблона и выпускает сертификат X.509. Запрос можно загрузить файлом или вставить текстом, заранее сверить с шаблоном и указать адреса для уведомлений. Сертификаты выпускают по одному, пакетом или из конструктора CSR-запросов.



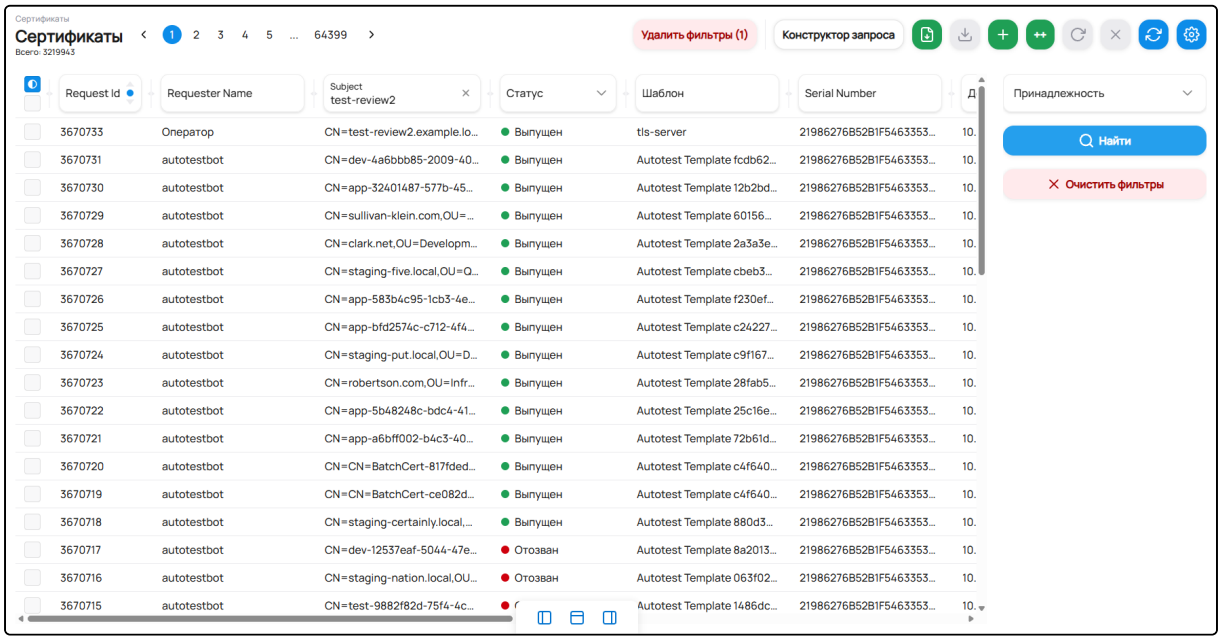
В окне «Запрос сертификата» оператор выбирает шаблон, затем перетаскивает файл запроса в блок «Сертификат:» (размер до 30 МБ) или вставляет текст CSR в поле «Certificate Signing Request». В поле «Почта для уведомлений» кнопкой «+» добавляются адреса, а флажки «Уведомлять о выпуске», «Уведомлять об отзыве» и «Уведомлять об истечении срока» выбирают события. Если шаблон хранит закрытый ключ под KRA, вместе с запросом загружается файл закрытого ключа. Кнопка **Просмотр** показывает структуру запроса, а **Подтвердить** отправляет его в ЦС.

Перед выпуском ЦС сверяет запрос с ограничениями шаблона для Subject и SAN. Если запрос их нарушает, сертификат не выпускается, а окно «Ошибки» перечисляет все нарушения: поле, значение из запроса и причину отказа. Если в шаблоне включён признак «Создавать запрос на выпуск», сертификат выпускается только после одобрения запроса в разделе «Запросы».

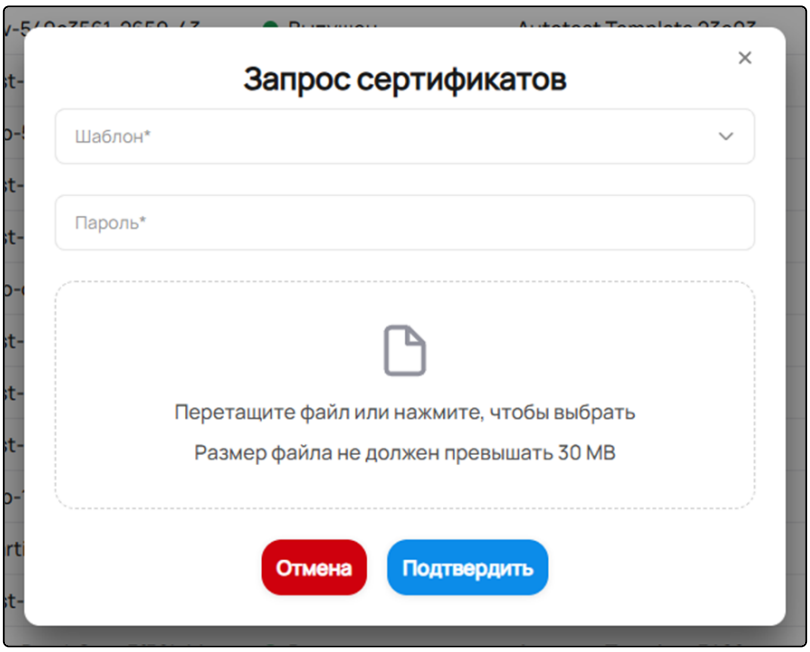


Имя параметра	Значение в csr	Значение в шаблоне
Тип ключа	RSA	RSA
Алгоритм	SHA256withRSA	
Длина ключа	RSA 2048 bits	2048
Срок действия (дни)		365
Subject	CN=test-review.example.local	
X509v3 Subject Alternative Name	test-review.example.local	

Окно просмотра построчно сопоставляет параметры запроса и шаблона в столбцах «Имя параметра», «Значение в csr» и «Значение в шаблоне». Здесь оператор сверяет тип и длину ключа, алгоритм, срок действия, Subject и SAN (в примере ключ RSA длиной 2048 бит и алгоритм SHA256withRSA), а расхождения с шаблоном выделяются красным.



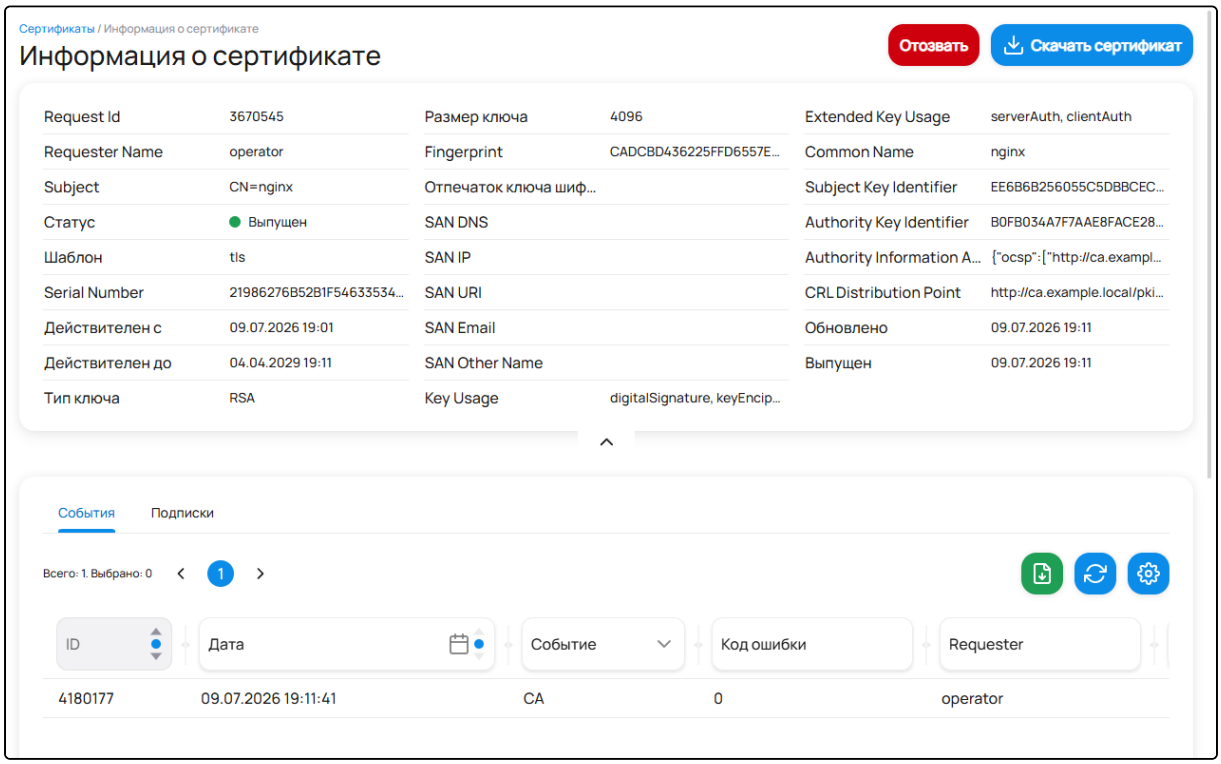
После выпуска сертификат появляется в реестре «Сертификаты» со статусом «Выпущен». В примере это запись с субъектом CN=test-review2.example.local по шаблону tls-server; найти её удобно фильтром по столбцу Subject.



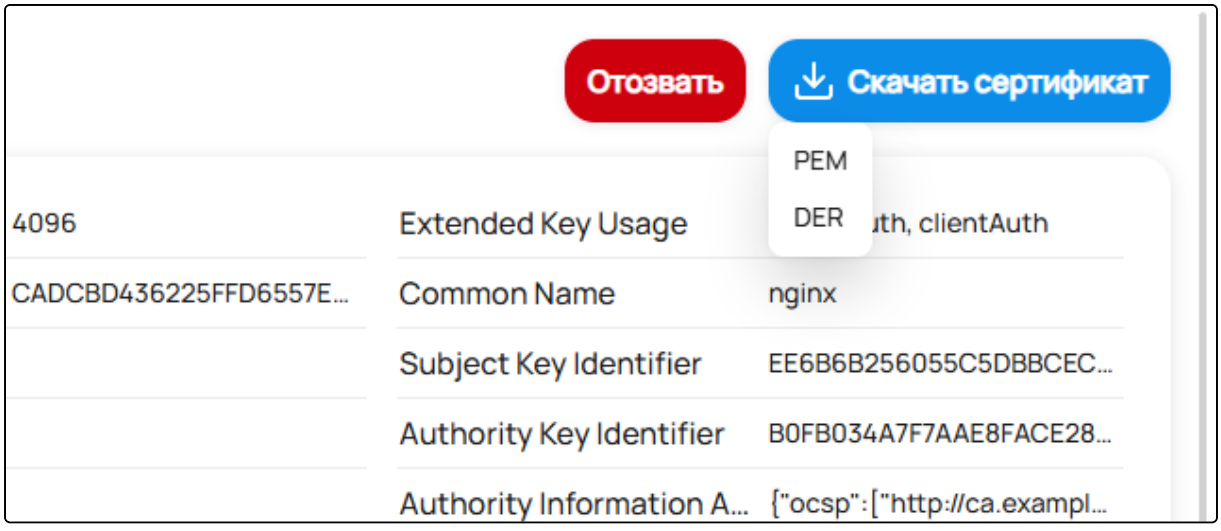
Пакетный запрос (кнопка **Пакетный запрос сертификатов** в реестре) выпускает сразу несколько сертификатов по списку Subject из текстового файла: в окне «Запрос сертификатов» выбираются шаблон, пароль и файл (до 30 МБ), где одна строка соответствует одному сертификату. Кнопка **Подтвердить** запускает выпуск, после которого браузер сохраняет файл с результатом, а **Отмена** закрывает окно без изменений.

5.7 Карточка сертификата и жизненный цикл

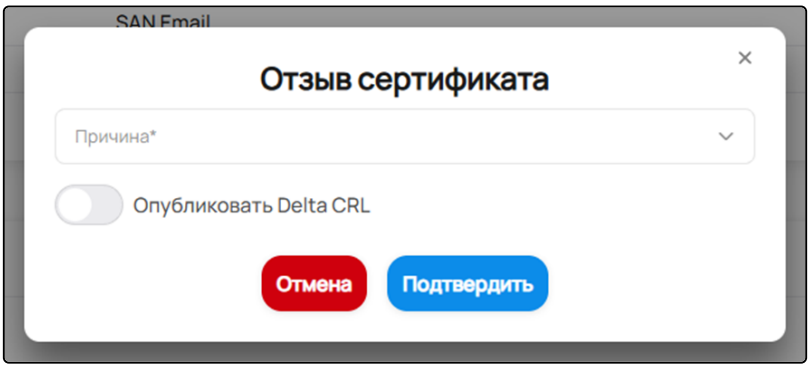
Щелчок по строке реестра открывает карточку «Информация о сертификате»: в ней собраны реквизиты сертификата, точки распространения и журнал операций по нему. Здесь же оператор скачивает и отзывает сертификат и настраивает уведомления, не переходя на другие экраны.



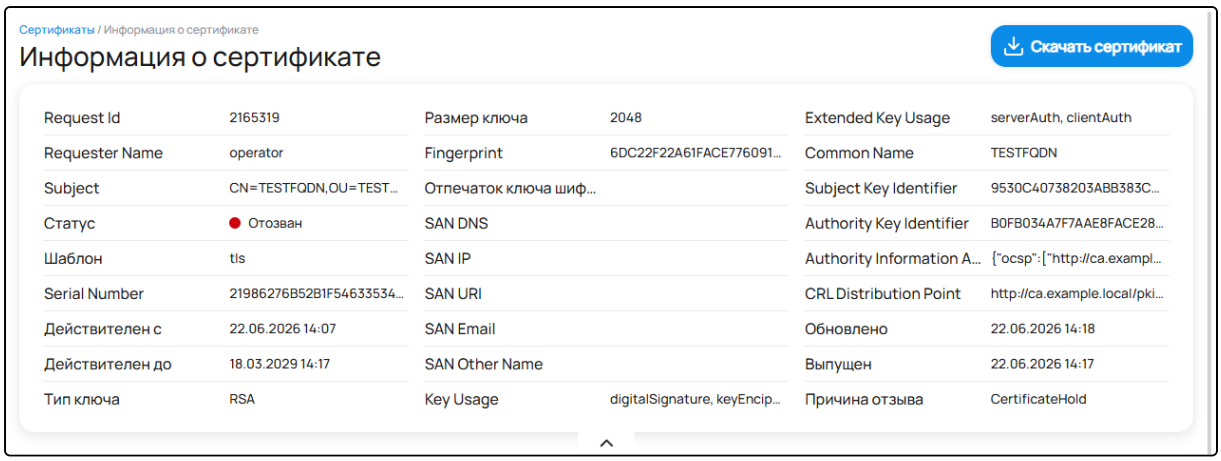
В блоке реквизитов есть поля Request Id, Subject и Serial Number, отпечаток Fingerprint, значения SAN, поля Key Usage и Extended Key Usage, идентификаторы Subject Key Identifier и Authority Key Identifier и точки распространения Authority Information Access (OCSP) и CRL Distribution Point. В примере это сертификат с ключом RSA длиной 4096 бит в статусе «Выпущен». Кнопки **Отозвать** и **Скачать сертификат** в правом верхнем углу управляют жизненным циклом, а вкладки «События» и «Подписки» показывают журнал операций по этому сертификату и настройку уведомлений по почте о выпуске, отзыве и истечении срока. Если ЦС хранит закрытый ключ сертификата (KRA), в карточке есть кнопка **Скачать зашифрованный ключ**.



Кнопка **Скачать сертификат** раскрывает меню с двумя форматами: PEM (текстовый) и DER (двоичный). Выбирают формат, который требует принимающая система. Несколько сертификатов сразу скачиваются из реестра кнопкой **Скачать сертификаты**.



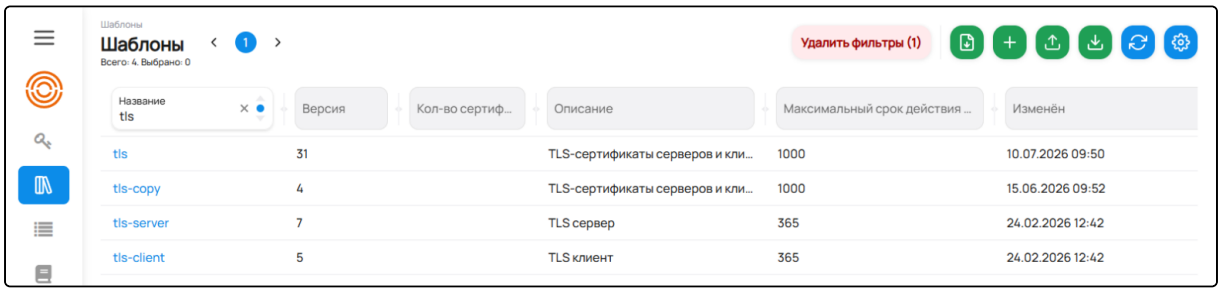
Отзыв запускается в окне «Отзыв сертификата»: в списке «Причина» выбирается основание, а переключатель «Опубликовать Delta CRL» сразу после отзыва публикует разностный список отзыва. Сертификат отзывается после нажатия **Подтвердить**, кнопка **Отмена** закрывает окно без изменений. Несколько сертификатов, отмеченных в реестре, отзываются за одно действие.



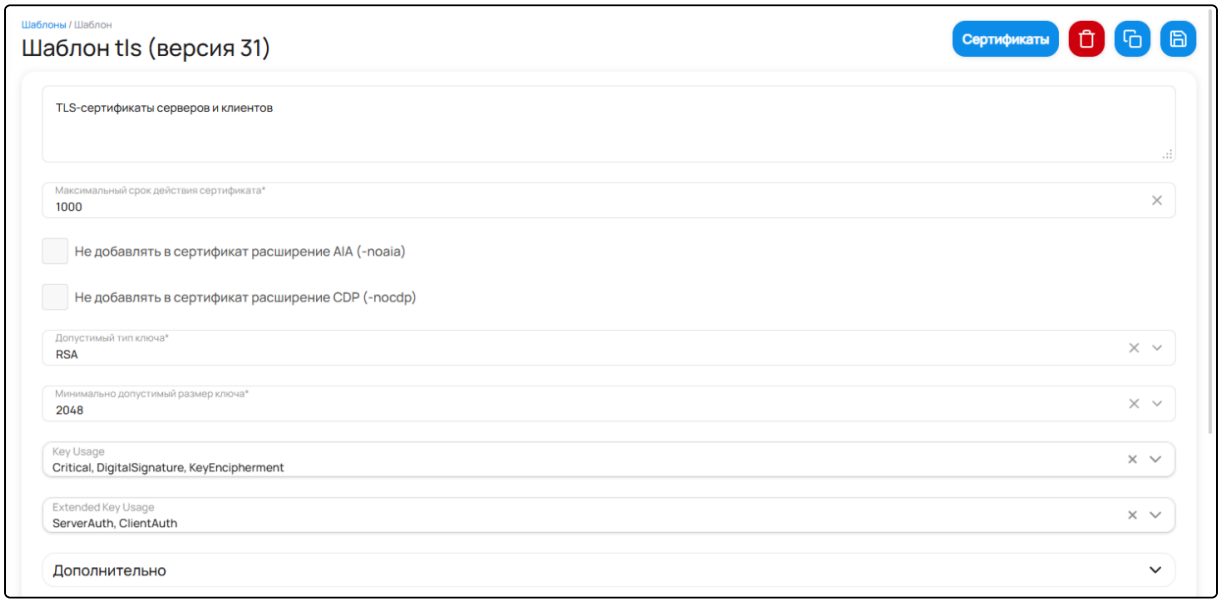
После отзыва статус меняется на «Отозван», в карточке появляется поле «Причина отзыва», а кнопка **Отозвать** пропадает. Отзыв необратим для всех причин, кроме CertificateHold (временная приостановка): такой сертификат, как в примере, возвращается в действие кнопкой **Восстановить выбранные сертификаты** в реестре или на странице «Информация о CRL и Delta CRL». Проверяющие стороны узнают об отзыве из списков отзыва и по протоколу OCSP.

5.8 Шаблоны сертификатов

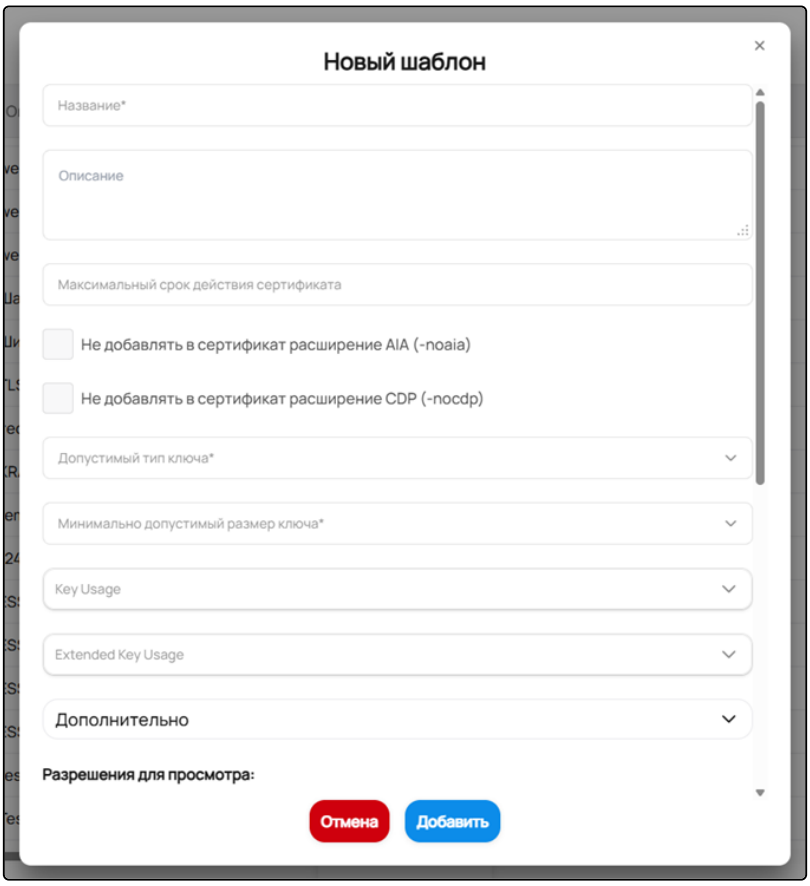
Шаблон сертификата задаёт политику выпуска: состав атрибутов и расширений сертификата и требования к запросу. Оператору не нужно каждый раз вручную указывать параметры ключа и назначение сертификата, а запрос перед выпуском проверяется на соответствие шаблону. Шаблоны хранятся в базе данных ЦС, каждое сохранение создаёт новую версию шаблона. В шаблоне фиксируются максимальный срок действия, допустимый тип и минимальный размер ключа, значения Key Usage и Extended Key Usage, флаги отключения расширений AIA и CDP, разрешения на просмотр, изменение и выпуск и ограничения для Subject и SAN.



Реестр шаблонов показывает название, версию, число выпущенных по шаблону сертификатов, описание, максимальный срок действия и дату изменения; в примере фильтр по названию «tls» оставил четыре шаблона. Кнопки в правом верхнем углу выгружают отчёт, создают шаблон, импортируют и экспортируют шаблоны в формате JSON, обновляют список и открывают настройки таблицы.



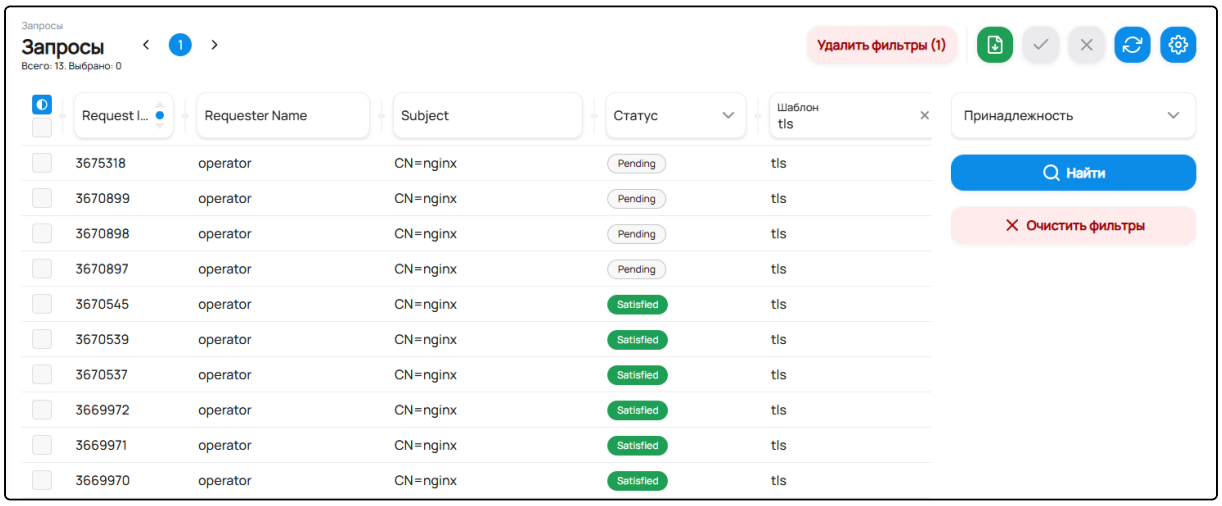
Карточка открывает шаблон для просмотра и правки: в примере это шаблон tls версии 31 с максимальным сроком действия 1000 дней, типом ключа RSA, минимальным размером ключа 2048 и значениями ServerAuth, ClientAuth в поле Extended Key Usage. Здесь же переключаются флаги «-noaia» и «-nocdp», раскрывается блок «Дополнительно» (хранение закрытого ключа под KRA, шифрование данных в БД, выпуск через согласование) и задаются разрешения и ограничения для Subject и SAN. Кнопки в правом верхнем углу открывают связанные сертификаты, удаляют, копируют и сохраняют шаблон.



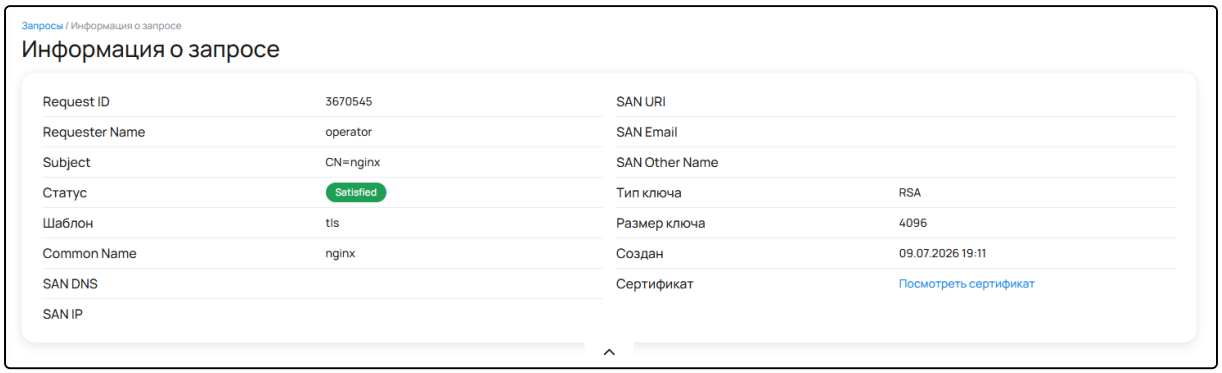
Окно «Новый шаблон» содержит те же поля, что и карточка, и поле «Название», которое после создания изменить нельзя. Заполненную форму подтверждают кнопкой **Добавить** или закрывают кнопкой **Отмена**. Готовый шаблон можно скопировать под новым названием или перенести в другой контур экспортом и импортом в формате JSON.

5.9 Запросы и согласование выпуска

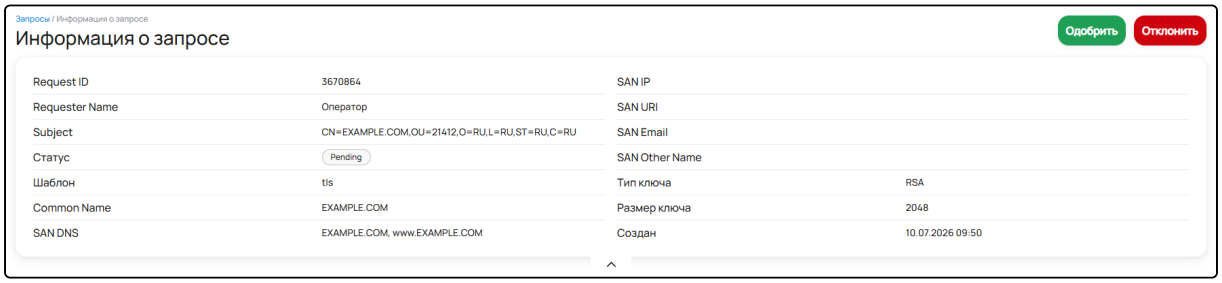
Раздел «Запросы» собирает все заявки на выпуск сертификатов (запросы CSR) в единый реестр, и здесь же их согласуют. Согласования требуют шаблоны с признаком «Создавать запрос на выпуск»: запрос по такому шаблону получает статус Pending и ждёт решения, а сертификат пока не выпускается. Итоговые статусы запроса: Satisfied (сертификат выпущен), Rejected (запрос отклонён) и Erroneous (ошибка при выпуске). Согласование держит выпуск под контролем, а причина каждого отказа сохраняется.



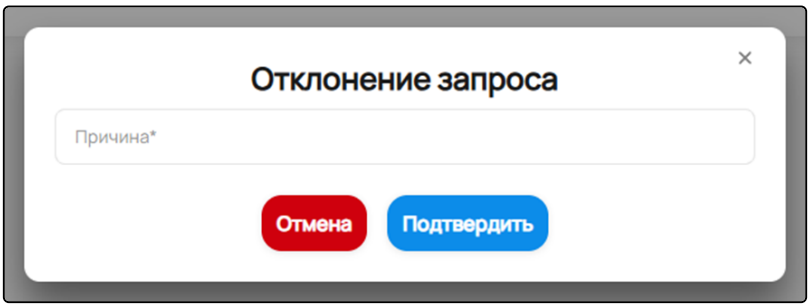
В реестре видны Request ID, инициатор, Subject, статус и шаблон запроса, а в скрытых по умолчанию столбцах есть Common Name, тип и размер ключа и причина отклонения; в примере отобраны запросы по шаблону tls, часть из них ждёт согласования. Над столбцами доступны фильтры, справа боковая панель с полем «Принадлежность» и кнопками **Найти** и **Очистить фильтры**. Отметив строки флажками, администратор одобряет или отклоняет сразу несколько запросов кнопками **Одобрение запросов** и **Отклонение запросов** над таблицей.



Карточка «Информация о запросе» раскрывает параметры заявки: Request ID, инициатора, Subject, Common Name, поля SAN, тип и размер ключа (в примере RSA 4096) и дату создания. У выполненного запроса в статусе Satisfied есть ссылка «Посмотреть сертификат», которая ведёт к выпущенному сертификату.



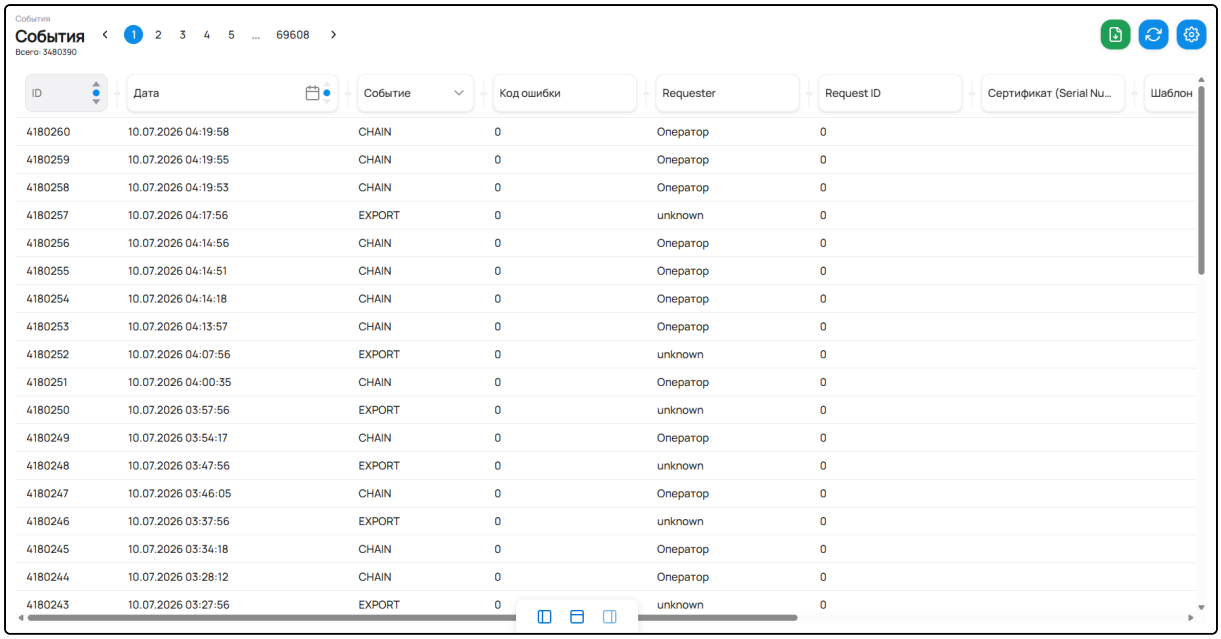
У запроса в статусе Pending карточка дополняется кнопками **Одобрить** и **Отклонить** в правом верхнем углу. Администратор проверяет субъект, шаблон (в примере tls), список SAN и тип ключа и решает, выпускать ли сертификат.



При отклонении открывается окно «Отклонение запроса» с обязательным полем «Причина»: текст можно ввести или выбрать из списка. Кнопка **Подтвердить** переводит запрос в статус Rejected и сохраняет причину, а **Отмена** закрывает окно без изменений.

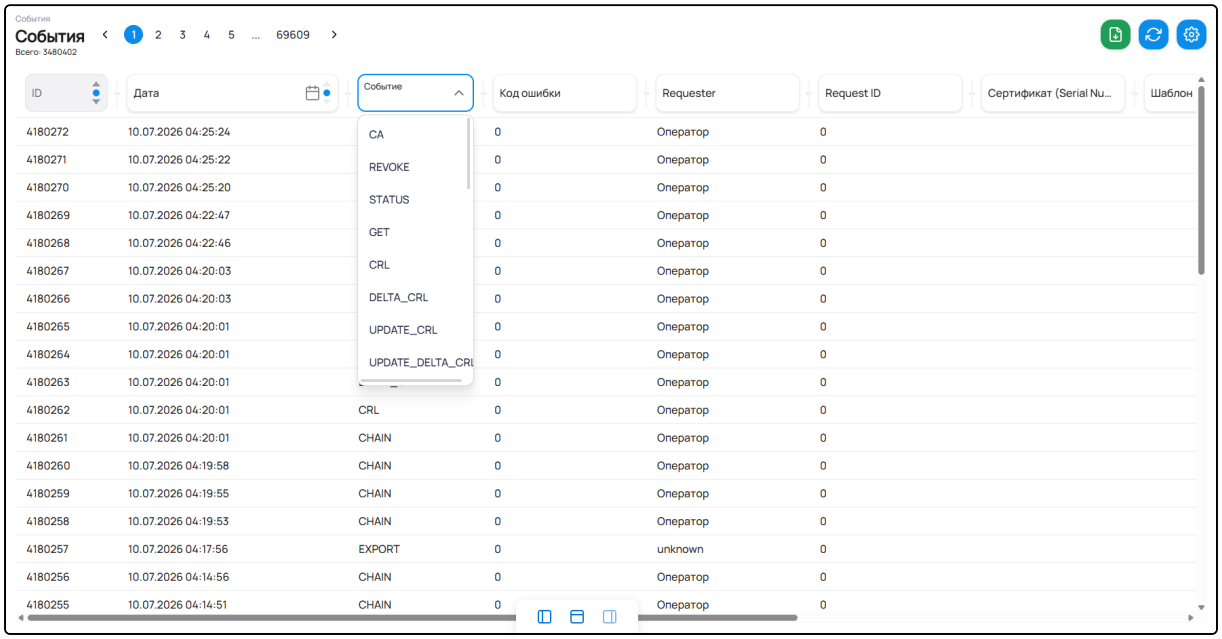
5.10 События (аудит)

Раздел «События» содержит журнал операций центра сертификации: выпуск и отзыв сертификатов, одобрение и отклонение запросов, проверку статуса, операции со списками отзыва, шаблонами и токенами JWT. По каждой записи сохраняются номер, время, тип операции, код ошибки и инициатор, поэтому по журналу видно, кто, когда и с каким результатом выполнил операцию. Журнал нужен, чтобы регулярно проверять работу ЦС, расследовать инциденты и готовить отчётность.



Записи выводятся таблицей со столбцами «ID», «Дата», «Событие», «Код ошибки», «Requester», «Request ID», «Сертификат (Serial Number)» и «Шаблон»; в столбце Requester указана учётная запись или программный клиент, которые выполнили операцию. Журнал может насчитывать миллионы записей (в примере более 3,4 млн), поэтому выводится постранично. Кнопки в правом

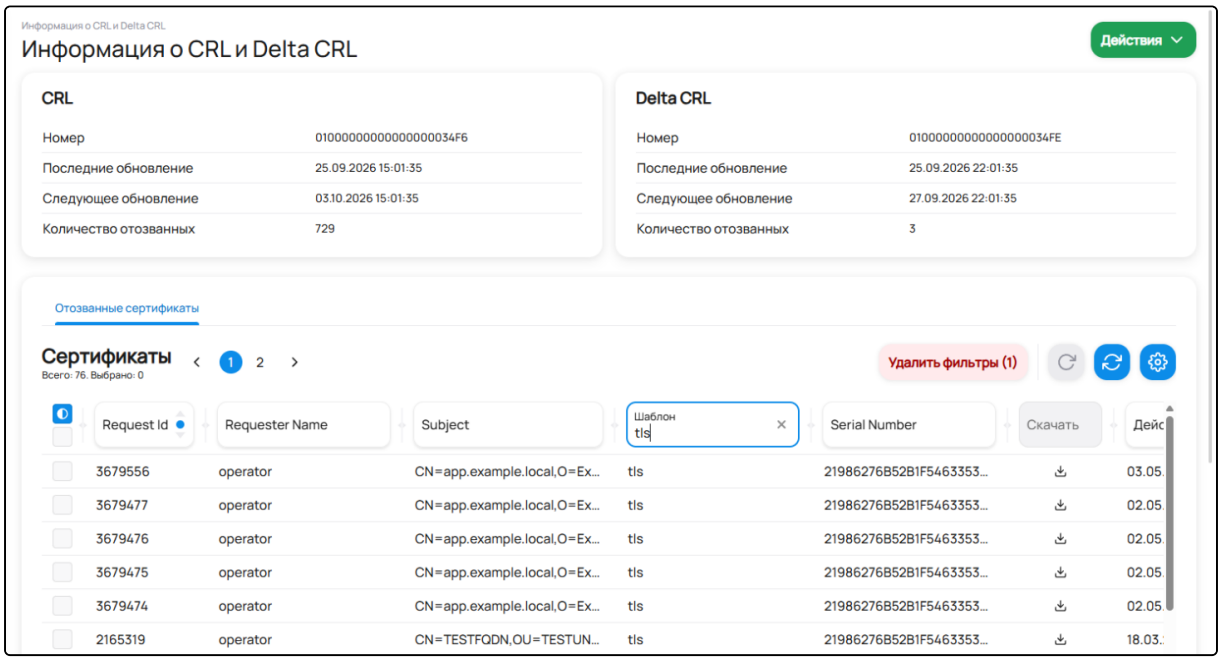
верхнем углу выгружают отчёт в файл Excel по применённым фильтрам, обновляют таблицу и открывают её настройки.



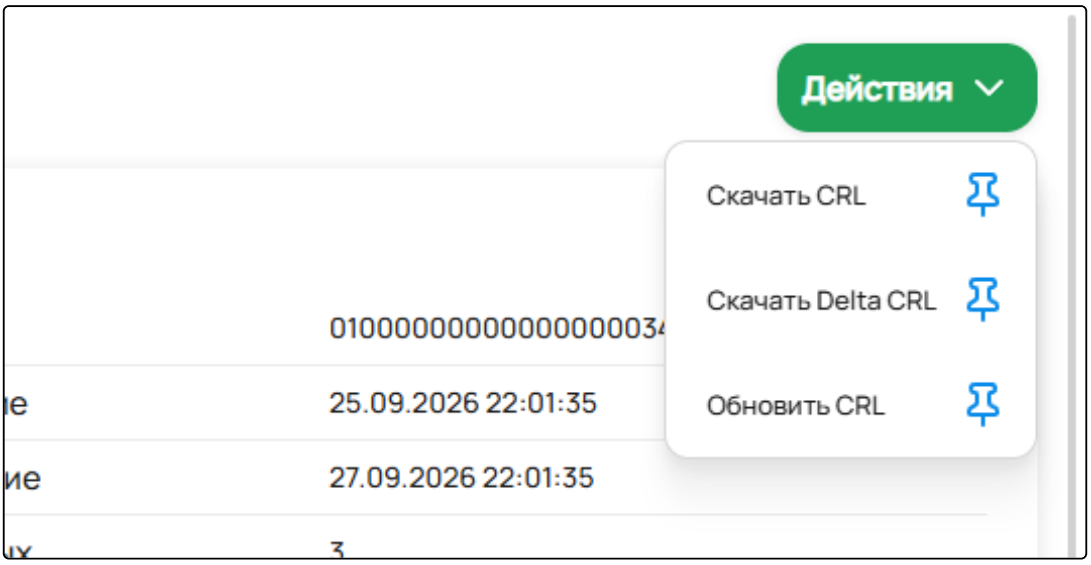
Щелчок по полю над столбцом «Событие» открывает список типов операций, например CA, REVOKE, STATUS, GET, CRL, DELTA_CRL или UPDATE_CRL. Так удобно отобрать только отзывы сертификатов или только обновления списков отзыва, не просматривая весь журнал. Фильтры по разным столбцам можно сочетать, а полученную выборку выгрузить для анализа.

5.11 Списки отзыва (CRL и Delta CRL)

Центр сертификации формирует и публикует списки отзыва двух видов: полный CRL и разностный Delta CRL, который содержит только изменения с момента последнего полного списка и поэтому меньше по объёму. Раздел «Информация о CRL» показывает текущее состояние обоих списков и перечень отозванных сертификатов. Статус отдельного сертификата в момент запроса сообщает OCSP-ответчик mOCSP: по умолчанию он берёт статус из базы данных ЦС и не зависит от расписания публикации CRL; собственного веб-интерфейса у ответчика нет.



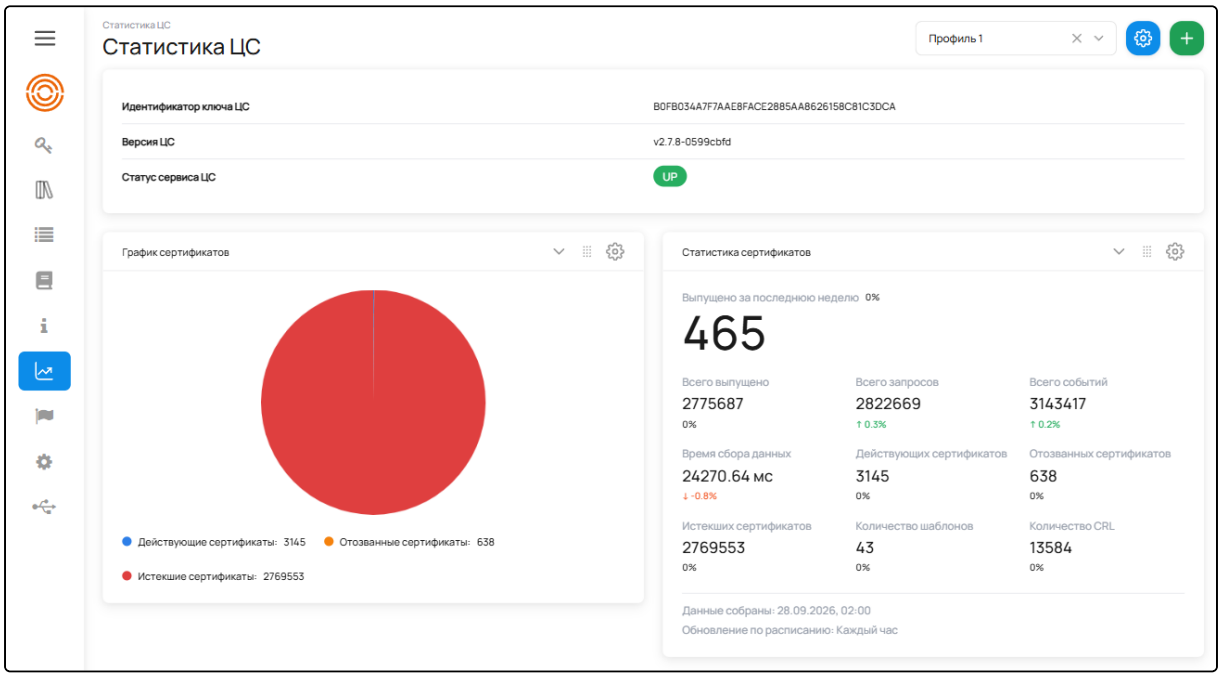
Карточки «CRL» и «Delta CRL» показывают номер списка, время последнего и следующего обновления и количество отозванных сертификатов (в примере 729 в полном CRL и 3 в Delta CRL). Ниже на вкладке «Отозванные сертификаты» перечислены все отозванные сертификаты из базы данных ЦС: строку можно открыть в карточке сертификата, файл сертификата скачать по значку в столбце «Скачать», а приостановленные сертификаты восстановить.



Меню **Действия** в правом верхнем углу содержит команды «Скачать CRL», «Скачать Delta CRL» и «Обновить CRL». Первые две сохраняют текущие списки в файл, а «Обновить CRL» сразу формирует новую версию списков, не дожидаясь планового обновления, и при необходимости публикует её. Часто используемую команду можно закрепить значком булавки: она появится отдельной кнопкой рядом с меню.

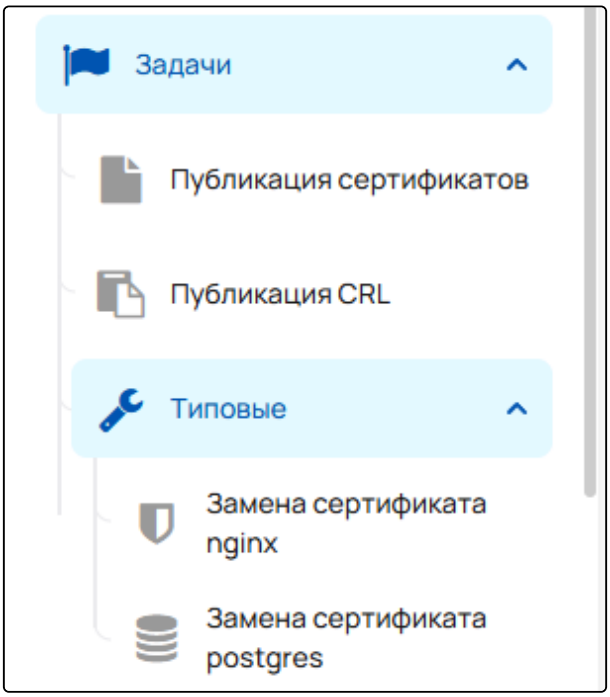
5.12 Статистика ЦС

Страница «Статистика ЦС» показывает основные показатели выбранного ЦС: идентификатор ключа и версию ЦС, состояние службы ЦС (UP или DOWN), диаграмму действующих, отозванных и истекших сертификатов, число сертификатов, выпущенных за последнюю неделю и за всё время, а также число запросов, списков отзыва, шаблонов и событий. Показатели рассчитываются в фоне по расписанию, поэтому страница открывается быстро даже на большой базе данных; время последнего расчёта указано в поле «Данные собраны». Рядом с каждым значением видно его изменение в процентах. Набор и расположение виджетов пользователь настраивает под себя, а те же показатели в момент вызова выдаёт команда mclient stat.

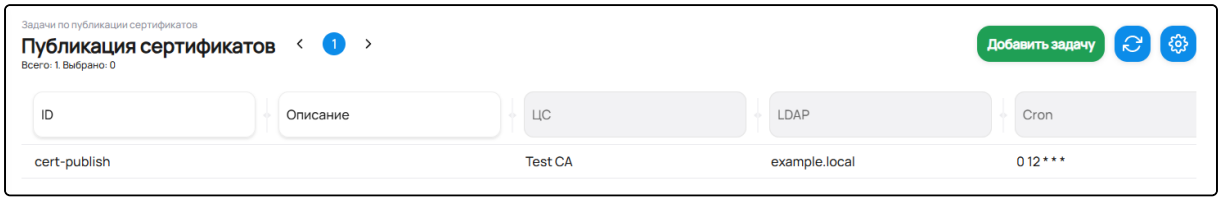


5.13 Задачи публикации

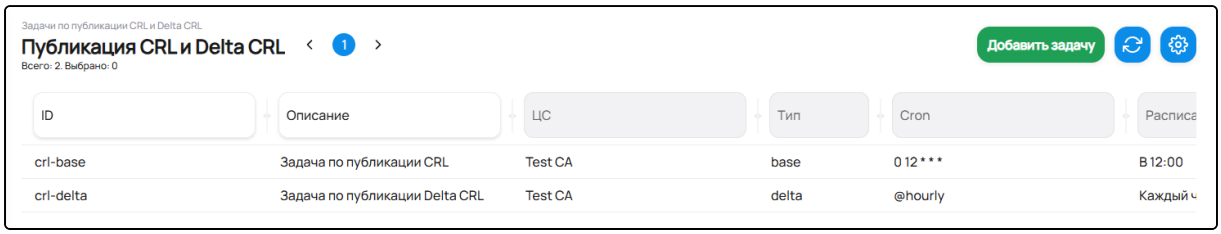
Группа меню «Задачи» объединяет задачи публикации, резервное копирование ЦС и типовые задачи замены сертификатов. Задачи публикации выполняет по расписанию cron сервис публикации: он выгружает выпущенные сертификаты в каталоги LDAP (Active Directory или Samba), а списки отзыва копирует в каталог на сервере, передаёт на удалённый сервер по SCP или записывает в каталог LDAP. Так клиенты и серверы получают актуальные сертификаты и сведения об отзыве без ручных действий.



В левом меню группа «Задачи» раскрывается в пункты «Публикация сертификатов», «Публикация CRL», «Резервное копирование» и «Типовые»; каждый пункт виден только пользователю с нужными правами, поэтому состав пунктов у разных пользователей различается.



Список «Публикация сертификатов» показывает задачи выгрузки сертификатов в каталог LDAP: название задачи (ID), описание, ЦС, из которого берутся сертификаты, адрес LDAP-сервера, выражение cron и расписание словами. В примере задача cert-publish по выражению 0 12 * * * каждый день в 12:00 UTC выгружает сертификаты ЦС Test CA в каталог example.local. Кнопка **Добавить задачу** создаёт задачу, а в карточке задачу можно изменить, удалить или запустить вне расписания кнопкой **Выполнить**, не редактируя файл конфигурации на сервере.



Список «Публикация CRL и Delta CRL» устроен так же, но вместо адреса LDAP содержит столбец «Тип»: base для полного списка отзыва и delta для разностного. В примере задача crl-base публикует полный CRL ежедневно в 12:00 UTC (0 12 * * *), а crl-delta публикует Delta CRL каждый

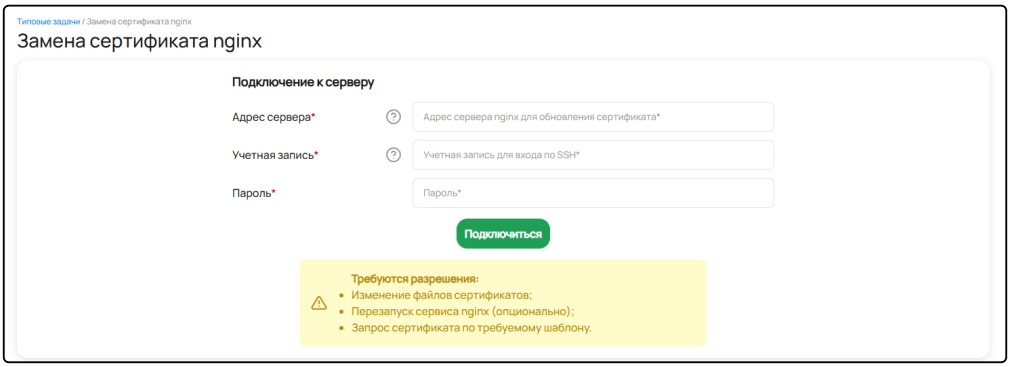
час (@hourly). В одной задаче можно включить несколько способов публикации, а пароль для SCP или LDAP указать ссылкой на секрет во внешнем хранилище секретов (EXC).

5.14 Резервное копирование и восстановление ЦС

Раздел «Задачи → Резервное копирование» управляет заданиями, которые по расписанию cron (время UTC) или по команде копируют базу данных ЦС, а с узлов ЦС по SSH копируют файлы конфигурации и исполняемый файл ЦС. Задания выполняет отдельный сервис резервного копирования: Контрольная панель только передаёт ему команды пользователя, а сам сервис подключается к узлам и базе данных, хранит копии и запускает задания по расписанию. В карточке задания видны блоки «Текущая операция», «Последний запуск» и «Копии» с отметкой о пригодности каждой копии. Из пригодной копии ЦС восстанавливается на выбранных узлах: перед запуском окно «Восстановление копии» показывает, сколько записей сертификатов, запросов и событий будет удалено, а при ошибке сервис возвращает базу данных и файлы узлов к сохранённому состоянию. Просмотр, запуск копирования и восстановление разрешают отдельные права: rleMiniCABackup-r, rleMiniCABackup-w и rleMiniCABackupRestore-w.

5.15 Типовые задачи

Типовые задачи (пункт «Задачи → Типовые») помогают заменить TLS-сертификат на сервере nginx или PostgreSQL. Пошаговый мастер подключается к серверу по SSH, находит файлы сертификата и ключа, выпускает в ЦС новый сертификат по выбранному шаблону, записывает его в эти файлы и при необходимости перезапускает сервис. Плановая замена сертификата при этом каждый раз проходит одинаково, копировать файлы вручную не нужно. Мастер доступен пользователю с правом rleMiniCACertReq-w, если функция типовых задач включена на сервере Контрольной панели.

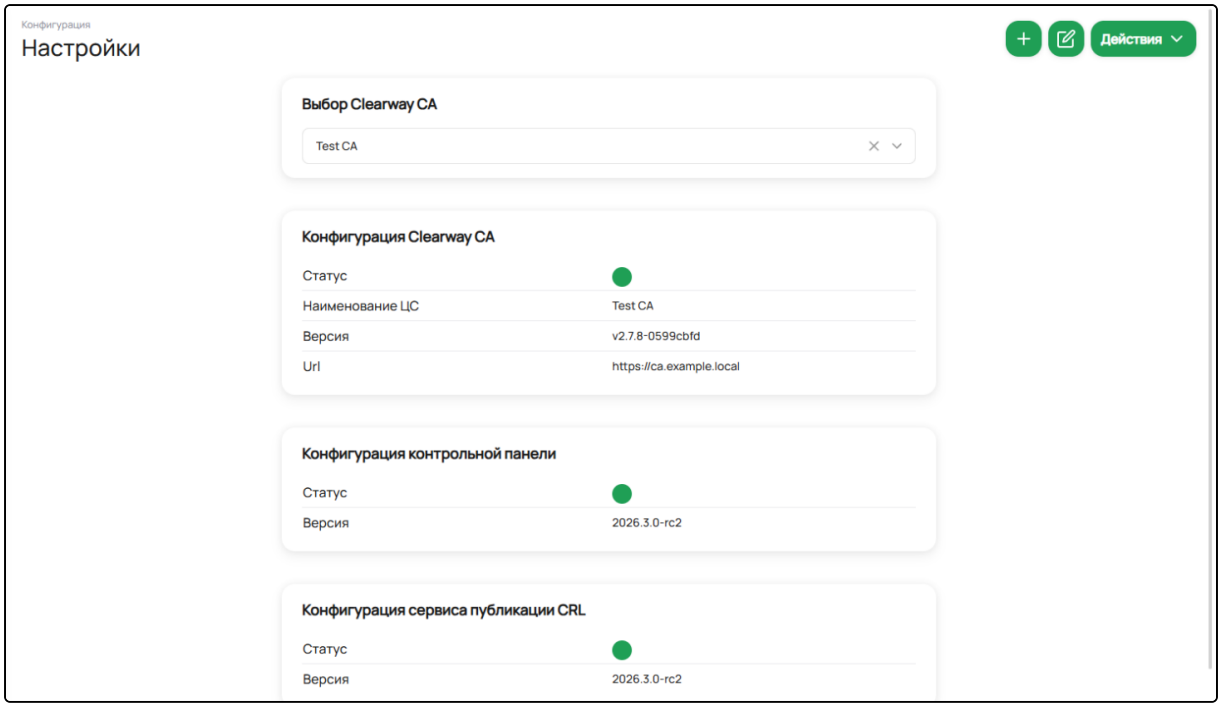


Сценарий «Замена сертификата nginx» начинается с шага «Подключение к серверу»: указываются адрес сервера, учётная запись для входа по SSH и пароль, а блок «Требуются разрешения» напоминает, какие права нужны этой учётной записи. После нажатия

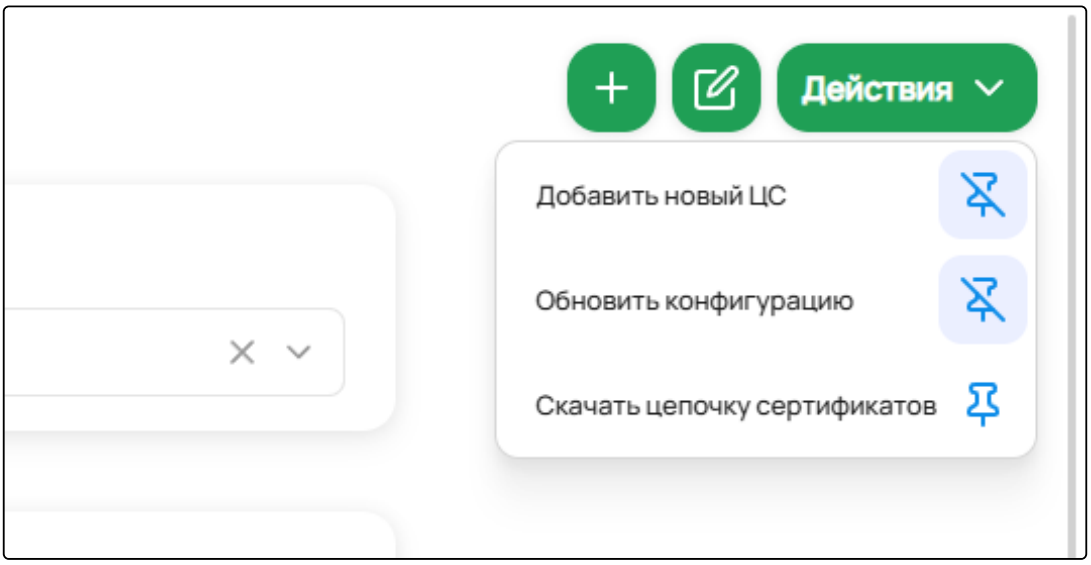
Подключиться мастер проверяет сервер и предлагает найденные файлы сертификата и ключа, а на последнем шаге кнопка **Заменить сертификат** выпускает и записывает новый сертификат: с новым ключом или для прежнего ключа. Сценарий «Замена сертификата postgres» устроен так же и отличается только целевым сервисом.

5.16 Настройки центра сертификации

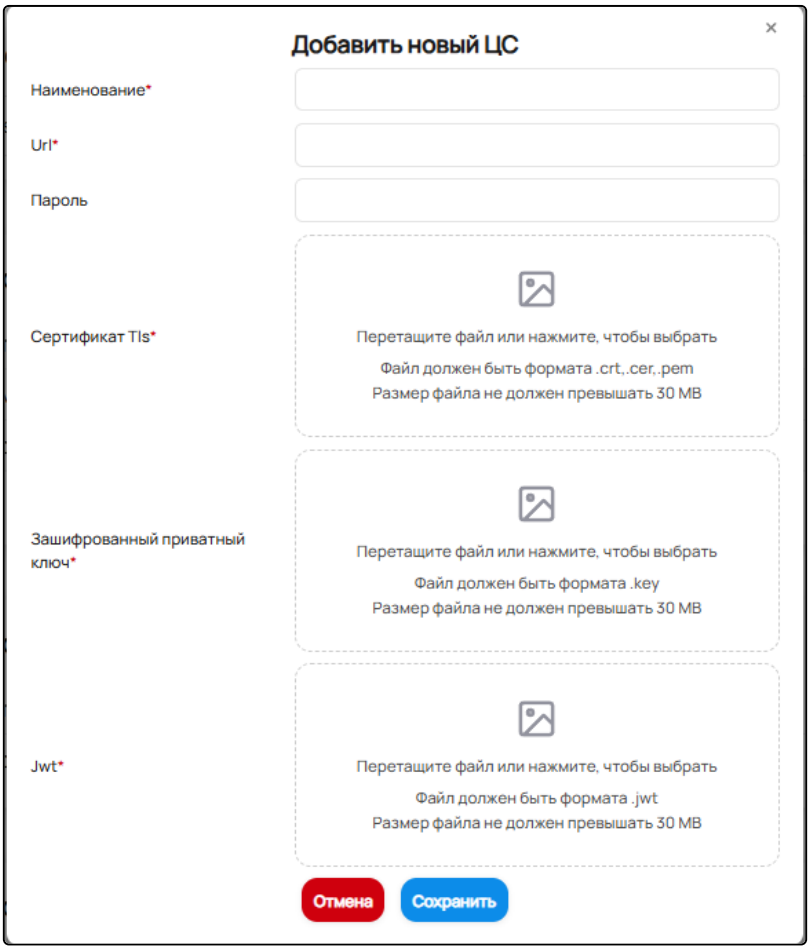
На странице «Настройки → Конфигурация» выбирают текущий ЦС и смотрят сводку состояния компонентов. Контрольная панель может работать с несколькими экземплярами ЦС, например с отдельными центрами для разных сред: все разделы показывают данные и выполняют операции для ЦС, выбранного здесь. Выбор хранится в браузере пользователя и не меняет выбор других пользователей.



Список в карточке «Выбор Clearway CA» задаёт текущий ЦС (в примере Test CA). Карточка «Конфигурация Clearway CA» показывает статус ЦС (зелёный индикатор означает, что ЦС отвечает), наименование ЦС, его версию и адрес подключения, а карточки «Конфигурация контрольной панели» и «Конфигурация сервиса публикации CRL» показывают статус и версию этих компонентов. По этим карточкам легко убедиться, что все части системы работают и совместимы по версиям.



Меню **Действия** собирает операции страницы: «Добавить новый ЦС» подключает ещё один экземпляр ЦС, «Обновить конфигурацию» меняет подключение к текущему ЦС, а «Скачать цепочку сертификатов» сохраняет цепочку доверия для установки на клиентах и серверах. Первые два действия закреплены по умолчанию и доступны значками «+» и «карандаш» слева от меню.



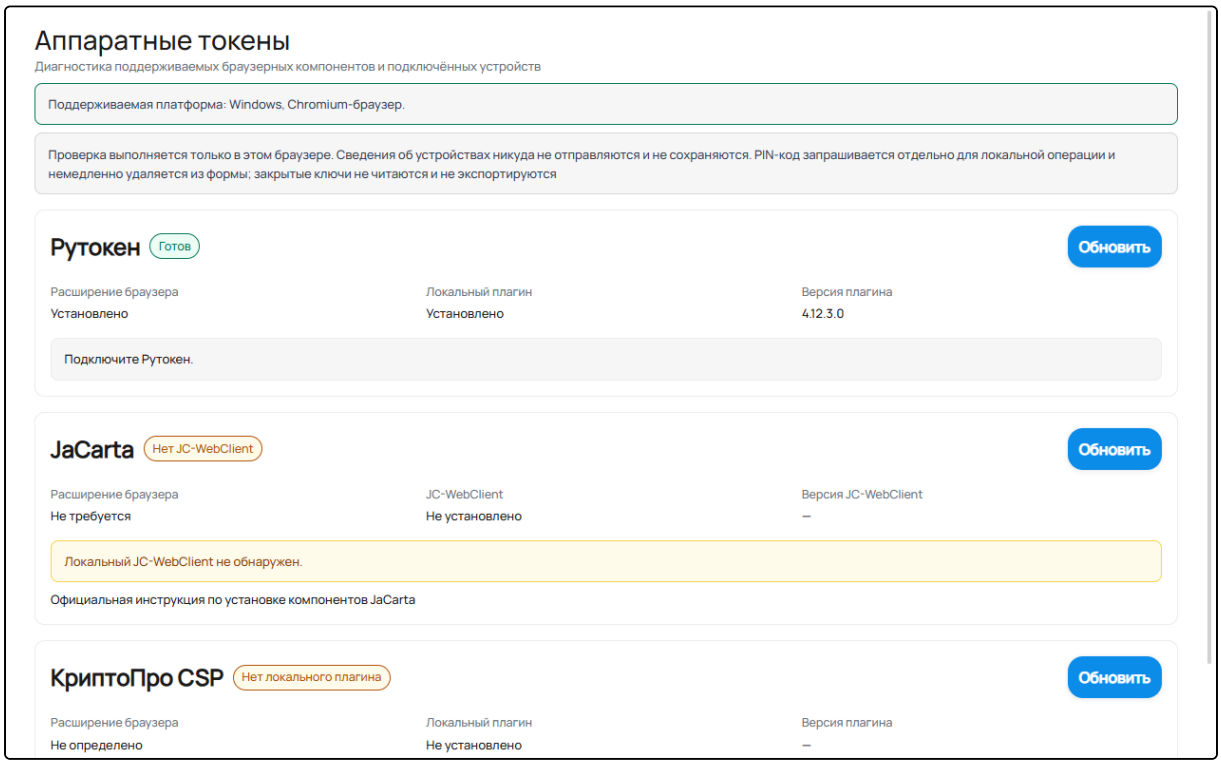
Чтобы подключить ЦС, в окне «Добавить новый ЦС» указывают наименование подключения, адрес ЦС и файлы, которые администратор выпускает для Контрольной панели: TLS-сертификат, зашифрованный закрытый ключ с паролем и токен JWT. После сохранения новый ЦС появляется в списке выбора у всех пользователей.

5.17 Ротация ключа ЦС

На странице «Настройки → Ротация ключей» заменяют сертификат ЦС, в том числе с переходом на новую ключевую пару. Сама Контрольная панель ротацию не выполняет: по её команде ядро ЦС формирует запрос на сертификат (CSR) в режиме «Продление» на действующем ключе или «Перевыпуск» на новой ключевой паре, которую ядро создаёт и хранит само. Запрос подписывает центр сертификации, который выпускает сертификат для этого ЦС, а полученный сертификат загружают кнопкой **Заменить сертификат** на той же странице. Ядро ЦС проверяет сертификат, сохраняет прежний сертификат (при «Перевыпуске» и прежний ключ) в архиве прежних ключей и начинает работать с новым сертификатом без перезапуска службы. Отдельно отзывают прежний сертификат ЦС, выпускают CRL и публикуют новый сертификат ЦС, а все действия страницы требуют права rleMiniCARotation-w.

5.18 Аппаратные токены

Раздел «Аппаратные токены» проверяет, установлены ли на компьютере пользователя компоненты для работы с носителями Рутокен, JaCarta и КриптоПро CSP, и показывает содержимое носителя: ключи, сертификаты и контейнеры. Здесь же можно добавить сертификат к ключевой паре, переименовать или удалить ключевую пару, сертификат или контейнер. В этом разделе удобно подготовить рабочее место, прежде чем создавать ключ в конструкторе CSR-запросов. Все операции выполняются локально в браузере: сведения об устройствах и PIN-коды в ЦС не передаются. Раздел доступен всем пользователям без отдельного права, поддерживается Windows с браузером на основе Chromium.


Аппаратные токены
Диагностика поддерживаемых браузерных компонентов и подключённых устройств
Поддерживаемая платформа: Windows, Chromium-браузер.
Проверка выполняется только в этом браузере. Сведения об устройствах никуда не отправляются и не сохраняются. PIN-код запрашивается отдельно для локальной операции и немедленно удаляется из формы; закрытые ключи не читаются и не экспортируются
Рутокен
Готов
Обновить
Расширение браузера
Установлено
Локальный плагин
Установлено
Версия плагина
4.12.3.0
Подключите Рутокен.
JaCarta
Нет JC-WebClient
Обновить
Расширение браузера
Не требуется
JC-WebClient
Не установлено
Версия JC-WebClient
–
Локальный JC-WebClient не обнаружен.
Официальная инструкция по установке компонентов JaCarta
КриптоПро CSP
Нет локального плагина
Обновить
Расширение браузера
Не определено
Локальный плагин
Не установлено
Версия плагина
–