Центр Управления Гетерогенными Инфраструктурами

Руководство пользователя. Версия 26.2.0

ООО «Клируэй Текнолоджис»

2026

Оглавление

1 Термины и сокращения

1.1 Принятые сокращения

Термин	Расшифровка
API	Application Programming Interface, Прикладной программный интерфейс компонента ИС.
PKI (ИОК)	Public Key Infrastructure, инфраструктура открытых ключей (ИОК) — набор средств, распределенных служб и компонентов, используемых для поддержки крипто-задач (шифрования, аутентификации, подписи) на основе закрытого и открытого ключей.
RSA	Rivest - Shamir -Adleman - реализация криптосистемы на основе закрытого и открытого ключей.
TLS / mTLS	Transport Level Security / mutual Transport Level Security — развитие протокола SSL, криптографический протокол на основе сертификатов x509, обеспечивающий организацию безопасной сетевой связи и взаимную аутентификацию клиента и сервера. SSL (Secure Socket Layers) — криптографический протокол, обеспечивающий организацию безопасной сетевой связи между клиентом и сервером и упрощенной проверкой подлинности сторон связи с применением сертификатов x509.
Clearway CA, Система	Система Автоматизированного Управления Инфраструктурой Центра Сертификации.
ИС	Информационная система.
ОС	Операционная система.
ЦС (CA)	Центр Сертификации (Certification Authority) — сервер, предназначенный для выпуска и отзыва сертификатов, а также публикации CRL (СОС).
ЦУГИ	Центр Управления Гетерогенными Инфраструктурами — набор (система) программ для управления и мониторинга различных компонентов ИТ инфраструктуры, разработанный и лицензируемый предприятием ООО "Клируэй Текнолоджис".

1.2 Термины и определения

Термин	Определение
Kubernetes	Платформа управления контейнеризацией с открытым исходным кодом
Микросервис	Отдельная программа, являющаяся частью программной системы или проекта, реализующая отдельный функциональный или информационный блок и тесно связанная с другими частями системы или проекта через сетевые вызовы API.
Роль	Набор системных и объектных прав, которые могут быть выданы и отозваны как единое целое, и после добавления этой Роли, могут быть временно активированы и деактивированы во время существования сессии.

2 Введение

Настоящий документ относится к эксплуатационной документации ПО "Система централизованного анализа и управления гетерогенными инфраструктурами — Clearway CA" (далее — Clearway CA). Разработчиком Clearway CA является ООО "Клируэй Текнолоджис".

Clearway CA — это центр сертификации, который выполняет выпуск сертификатов X.509v3 на основе CSR-запросов в формате PKCS#10, используя готовые шаблоны. Система позволяет создавать и настраивать эти шаблоны, а также отзыв сертификатов с указанием причины. Clearway CA формирует списки отозванных сертификатов (CRL и DeltaCRL), предоставляет статус сертификатов через протокол OCSP и обеспечивает доступ к ним по серийному номеру или SHA1-отпечатку. Все запросы, сертификаты, журналы событий и CRL/DeltaCRL сохраняются в базе данных. Управление осуществляется через веб-интерфейс Clearway CA и API, а также поддерживается работа с протоколом SCEP для выпуска сертификатов.

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

Основной функцией Clearway CA является управление жизненным циклом сертификатов:

1. Выпуск сертификатов:
   - выпуск сертификатов X.509v3 на основе CSR запросов в формате PKCS#10;
   - поддержка шаблонов сертификатов для наполнения и контроля атрибутов сертификатов;
   - поддержка выпуска сертификатов по различным протоколам – SCEP, WSTEP и др.
2. Предоставление сертификата по запросу:
   - возможность получения выпущенных сертификатов по запросу;

- возможность получения различных выборок и отчетов о выпущенных сертификатах.

3. Отзыв сертификата:
   - отзыв сертификатов с указанием причины;
   - формирование Списка Отозванных Сертификатов (COC, CRL);
   - формирование разностных списков отозванных сертификатов DeltaCRL;
   - предоставление информации о статусе сертификата по протоколу OCSP.
4. Вспомогательные функции:
   - сохранение информации о всех запросах, сертификатах, CRL/DeltaCRL в базе данных;
   - текстовый журнал событий;
   - поддержка функций самодиагностики;
   - поддержка хранения ключа ЦС на аппаратных носителях HSM.

Сведения, предусмотренные п. 16 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. 16.1 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	п. 4.3 "Приведение продукта в безопасное состояние" Руководства администратора RU.69639709.00002-01 32 01 п. 4.1.2 "Технические требования" Руководства администратора RU.69639709.00002-01 32 01
3	Описание функций и интерфейсов функций средства, доступных каждой роли пользователей	п. 4.2 "Матрица доступов для пользователей системы" Руководства администратора RU.69639709.00002-01 32 01 п. 5.5 "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	п. 4.2 "Матрица доступов для пользователей системы" Руководства администратора RU.69639709.00002-01 32 01
5	Описание типов событий безопасности, связанных с доступными пользователю функциями средства	п. 4.4 "Описание ошибок Clearway CA" Руководства администратора RU.69639709.00002-01 32 01

6	Описание действий после сбоев и ошибок эксплуатации средства	п. 4.3 "Приведение продукта в безопасное состояние" Руководства администратора RU.69639709.00002-01 32 01 п. 4.4 "Описание ошибок Clearway CA" Руководства администратора RU.69639709.00002-01 32 01 п. 8.7 "Обработка ошибок" Руководства администратора RU.69639709.00002-01 32 01

3 Ограничения для бесплатной редакции Clearway CA

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	Без ограничений
Общее количество сертификатов	Не более 2000 единиц	Без ограничений
Стартовый серийный номер	Фиксирован (нумерация с 1)	Настраивается
Кластеризация Active-Active	Недоступно	Настраивается
Хранение ключа ЦС на HSM (PKCS#11)	Недоступно	Доступно

4 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.

4.1 Вход в систему

Вход в систему выполняется перед началом любой работы с центром сертификации через веб-интерфейс Контрольной панели. Доступ построен на технологии единого входа (SSO): одни и те же доменные учётные данные используются для всех компонентов Clearway CA, поэтому отдельная регистрация и повторный ввод логина и пароля для каждого раздела не требуются — достаточно однократной аутентификации в домене.

1. Откройте адрес **Контрольной панели** в браузере.
2. Пройдите единый вход (SSO) по протоколу OpenID Connect с доменной учётной записью (интеграция LDAP/Active Directory) — отдельная регистрация не требуется.
3. В открывшемся окне *Успешная авторизация* ознакомьтесь с предупреждением о мерах защиты информации и нажмите **Подтвердить**.

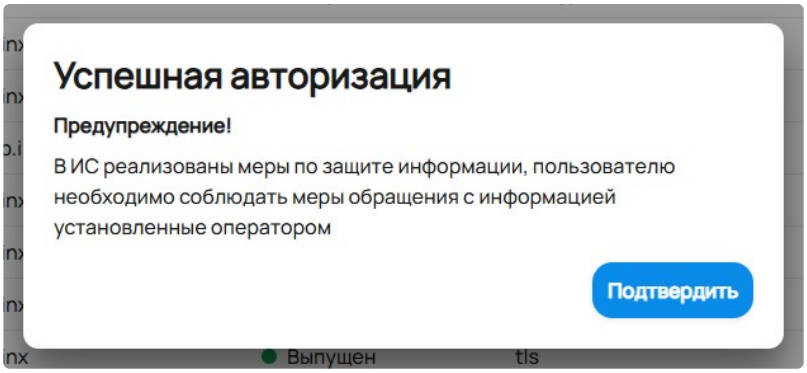


Рисунок 1 Окно «Успешная авторизация» с предупреждением о мерах защиты информации

Окно с предупреждением о мерах защиты информации — обязательная мера информационной безопасности. Нажатие на **Подтвердить** означает, что пользователь ознакомлен с правилами обращения с защищаемой информацией. Без подтверждения доступ к рабочей области не предоставляется.

В ситуациях, когда вход в систему не осуществляется, окно авторизации не открывается, отображается ошибка или доступ отклонён, выполните следующие проверки:

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

> Для одной учётной записи может действовать ограничение на число одновременных сессий. Если лимит исчерпан, завершите неиспользуемые сессии (выйдите из системы в других вкладках или на других устройствах) либо обратитесь к администратору.

После подтверждения откроется рабочая область:

4.2 Интерфейс и навигация

Навигация по разделам выполняется через постоянное меню в левой части экрана; используйте его для перехода к нужной операции.

1. Выберите в левом меню нужный раздел:
   - Сертификаты;
   - Шаблоны;
   - Запросы;
   - События;
   - Информация о CRL;
   - Задачи;
   - Настройки;
   - Типовые задачи.
2. Соответствующая рабочая область откроется справа. По умолчанию открыт реестр "Сертификаты".

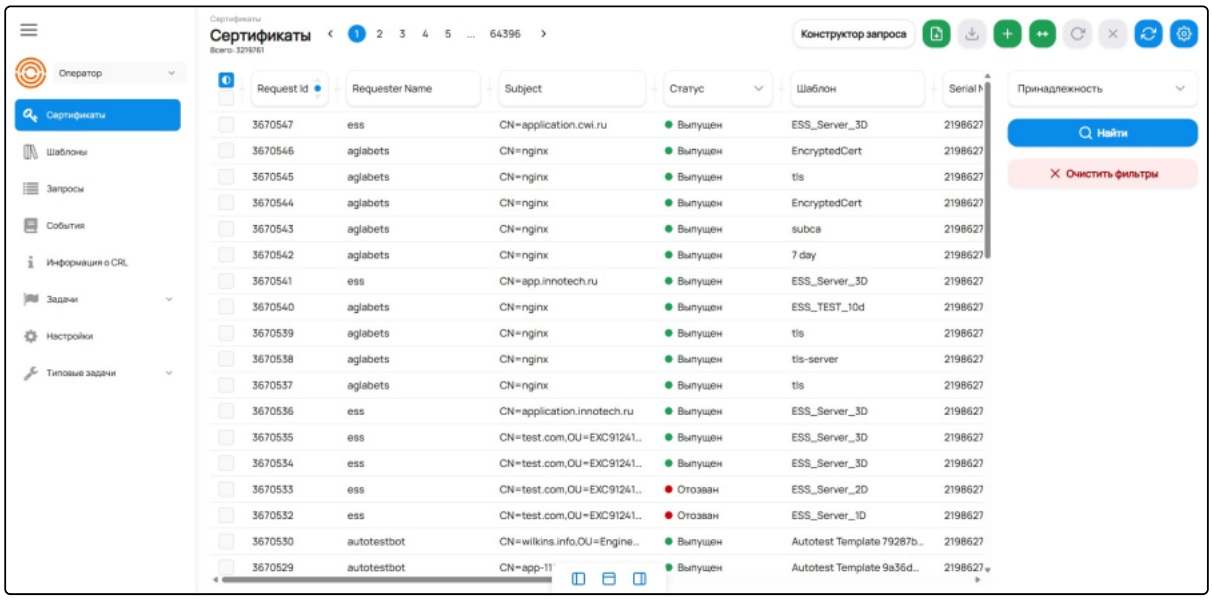


Рисунок 2 Главный экран: левое меню разделов и реестр сертификатов в рабочей области

- Сертификаты — реестр выпущенных сертификатов: просмотр, поиск и открытие карточек сертификатов;
- Шаблоны — политики выпуска: наборы параметров и правил, по которым формируются сертификаты;

- Запросы — заявки на выпуск сертификатов, поступившие на обработку (запросы CSR);
- События — журнал аудита действий, выполненных в системе;
- Информация о CRL — списки отзыва сертификатов (CRL, включая Delta CRL);
- Задачи — задачи публикации (размещение сертификатов и списков отзыва в точках распространения);
- Настройки — экземпляры центра сертификации и их текущее состояние;
- Типовые задачи — готовые сценарии обслуживания (частые операции, собранные в виде пошаговых действий).

Назначение разделов меню:

4.3 Профиль и права доступа

Набор доступных операций определяется назначенными ролями (ролевая модель). Проверьте свои учётные данные и права на экране профиля.

Роли построены по принципу "раздел + уровень доступа", а уровень доступа обозначается суффиксом в названии роли:

- суффикс -r означает право только на просмотр (чтение) данных соответствующего раздела;
- суффикс -w означает право на изменение (запись): создание, редактирование и выполнение операций.

Типовые роли пользователей:

- администратор — настройка и управление центром сертификации;
- оператор — повседневные операции с сертификатами, запросами и задачами;
- аудитор — просмотр журнала событий и данных без права изменения.

1. Откройте экран "Профиль пользователя".
2. В блоке "Данные" проверьте учётные данные: имя пользователя, логин, домен.
3. В блоке "Права" просмотрите назначенные роли и их описания. При необходимости воспользуйтесь поиском по полям **Название** и **Описание** (в примере назначены роли с префиксом rleMiniCA, например rleMiniCACertList-r — просмотр списка и карточек сертификатов).

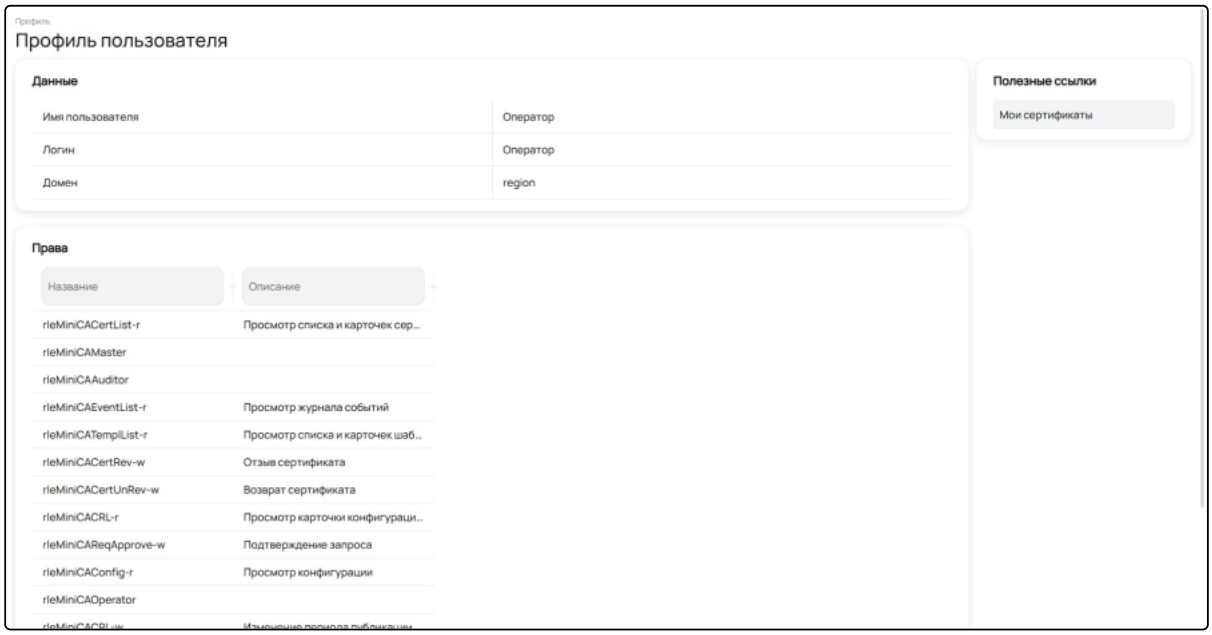


Рисунок 3 Экран «Профиль пользователя»: блоки «Данные» и «Права», ссылка «Мои сертификаты»

Если в интерфейсе отсутствует нужная кнопка или действие, значит соответствующая роль (в частности, роль с суффиксом -w для изменения данных) пользователю не назначена. Состав ролей меняет только администратор.

Чтобы перейти к сертификатам, выпущенным на текущего пользователя, откройте ссылку "Мои сертификаты" в блоке "Полезные ссылки". Если нужного действия нет, обратитесь к администратору за назначением соответствующей роли.

5 Сертификаты

5.1 Реестр сертификатов

Раздел "Сертификаты" — это реестр всех выпущенных и отозванных сертификатов, используемый для просмотра ранее выпущенных сертификатов и поиска нужной записи.

Реестр — основной инструмент оператора для контроля жизненного цикла сертификатов. Он показывает, какие сертификаты выпущены, какие отозваны, кому они принадлежат и по какому шаблону созданы. Отсюда осуществляется большинство операций: поиск конкретной записи, проверка статуса, переход к связанной заявке и выгрузка отчёта.

1. Откройте раздел "Сертификаты".
2. Проверьте строки реестра: в каждой строке отображаются Request Id (идентификатор запроса), Requester Name (инициатор), Subject (субъект, CN), Статус (*Выпущен* или *Отозван*), Шаблон и Serial Number (серийный номер).
3. Для перехода между страницами используйте постраничную навигацию вверху таблицы. Общее число записей показано в поле **Всего** (в примере — 3 219 761).

Ключевые поля строки помогают быстро определить тип сертификата:

- Request Id — идентификатор заявки (запроса) на выпуск сертификата. По нему сертификат связывается с исходной заявкой в разделе "Запросы".
- Serial Number — уникальный серийный номер сертификата, присваиваемый центром сертификации при выпуске. Данный серийный номер идентифицирует сертификат и используется при ссылке на сертификат, в том числе при его отзыве и включении в список отозванных сертификатов CRL.
- Subject (CN) — субъект сертификата, (кому выдан сертификат): имя пользователя, узла или сервиса.

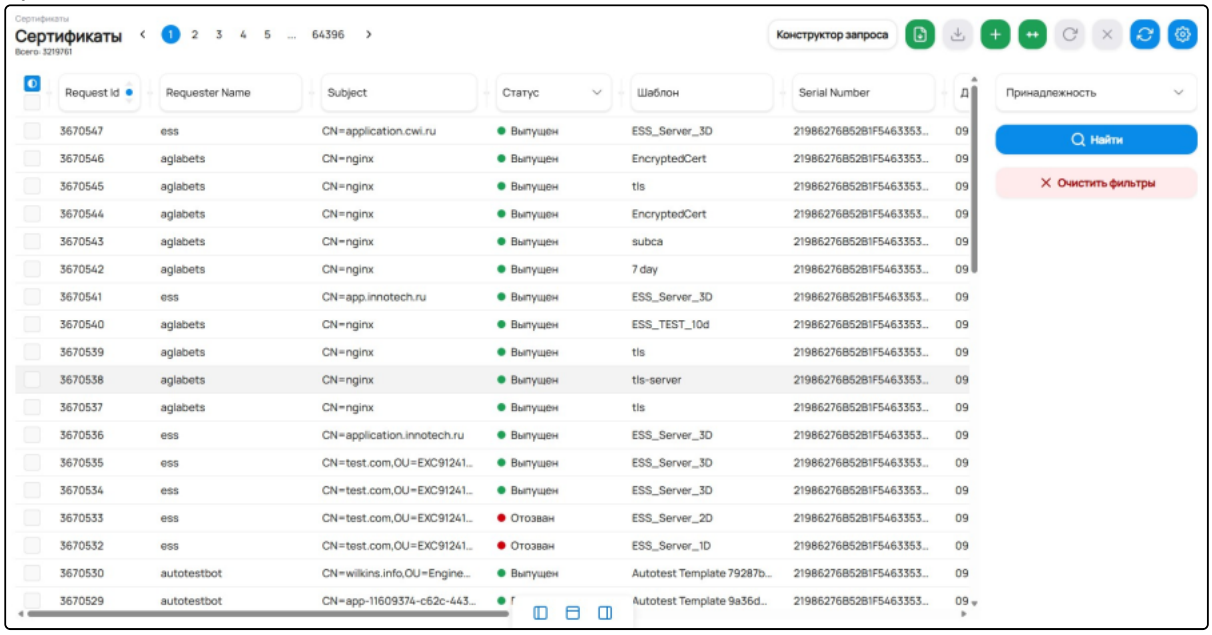


Рисунок 4 Реестр «Сертификаты»указанное в поле CN

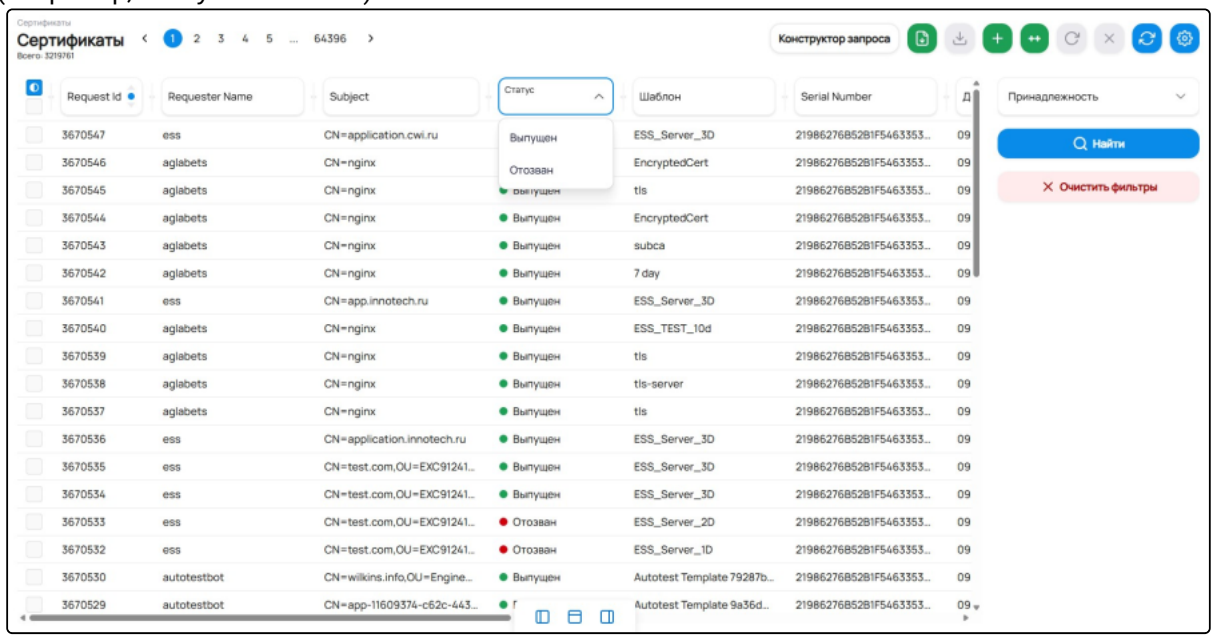
Значение "Статус" отражает текущее состояние сертификата: *Выпущен* — сертификат действует, *Отозван* — досрочно выведен из обращения, и доверять ему нельзя.

5.2 Поиск и фильтрация

Когда нужно отобрать сертификаты по определённому признаку (например, только отозванные), примените фильтры над колонками таблицы.

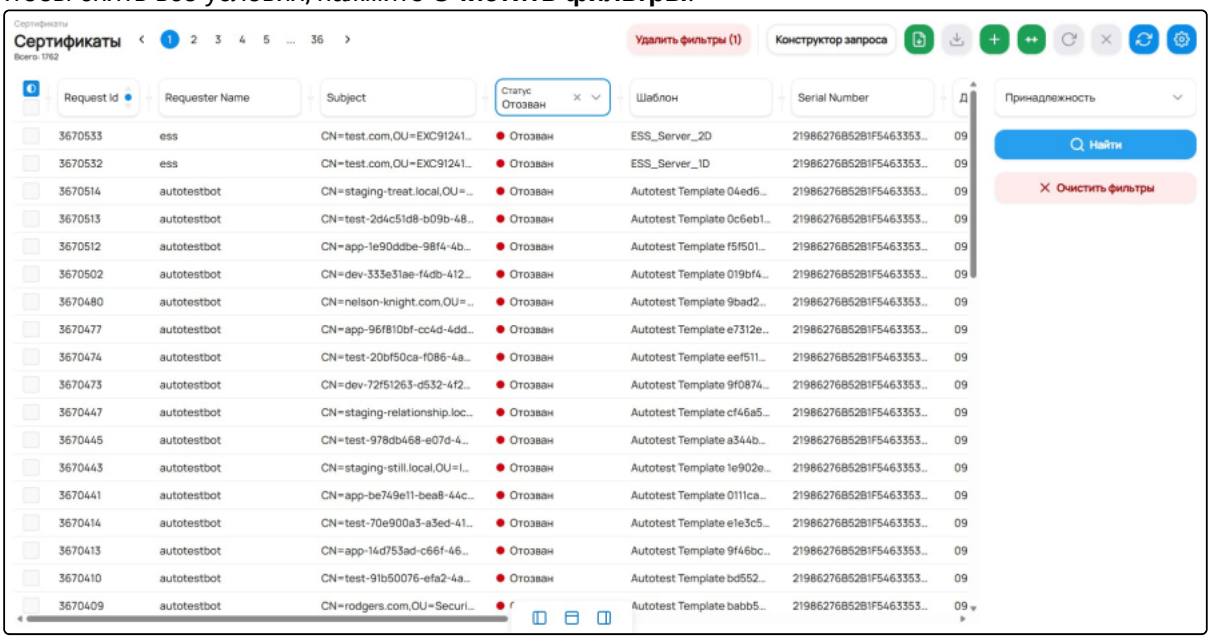
Фильтры можно комбинировать сразу по нескольким колонкам: заданные условия объединяются, и в выборке остаются только записи, удовлетворяющие всем условиям одновременно.

1. Введите условия в поля-фильтры над колонками или выберите значение в выпадающем фильтр (например, Статус = *Отозван*).



2. Нажмите **Найти**, в таблице останутся только записи, удовлетворяющие условиям. Активные фильтры отмечает индикатор "Удалить фильтры (N)".

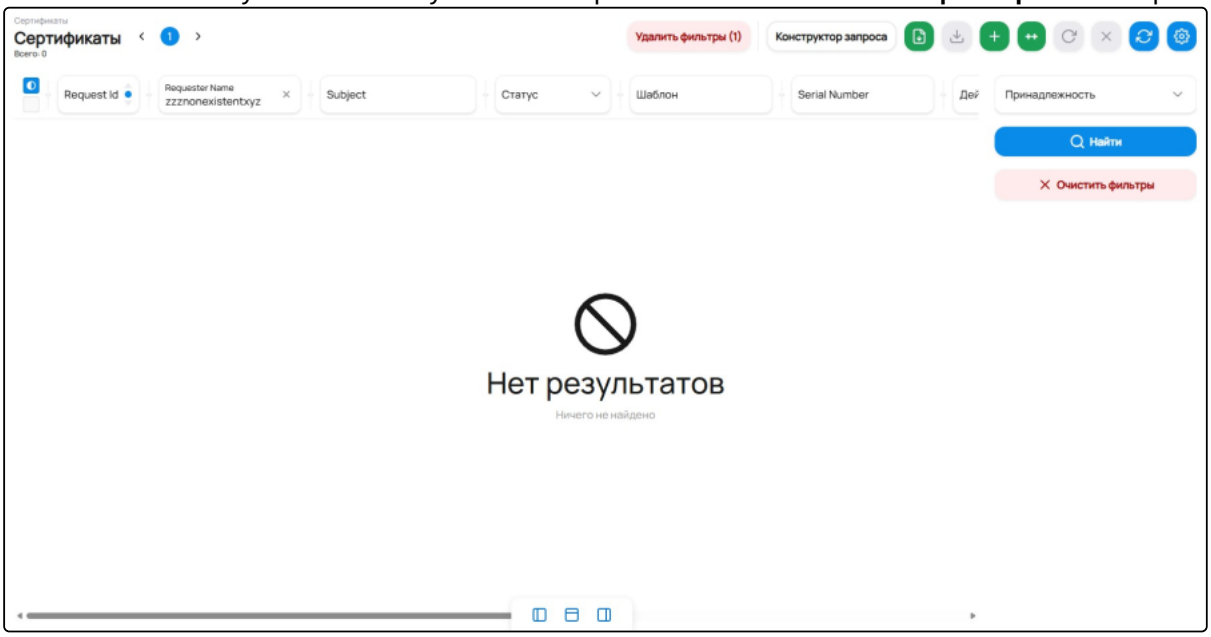
Чтобы снять все условия, нажмите **Очистить фильтры**.



Для дополнительных условий отбора используйте панель "Принадлежность" и "Конструктор запроса". Эти инструменты расширяют возможности обычных фильтров по колонкам:

- Конструктор запроса — расширенный отбор: позволяет задать условия сразу по нескольким атрибутам сертификата и объединить их в один запрос, когда простого фильтра по колонке недостаточно;
- панель "Принадлежность" — ограничивает выборку по владельцу или области: в таблице остаются только сертификаты, относящиеся к выбранному владельцу/области ответственности.

Если ни одна запись не подходит под условия, отображается "Нет результатов", а счётчик показывает "Всего: 0". В этом случае измените условия отбора или нажмите **Очистить фильтры** и повторите поиск.



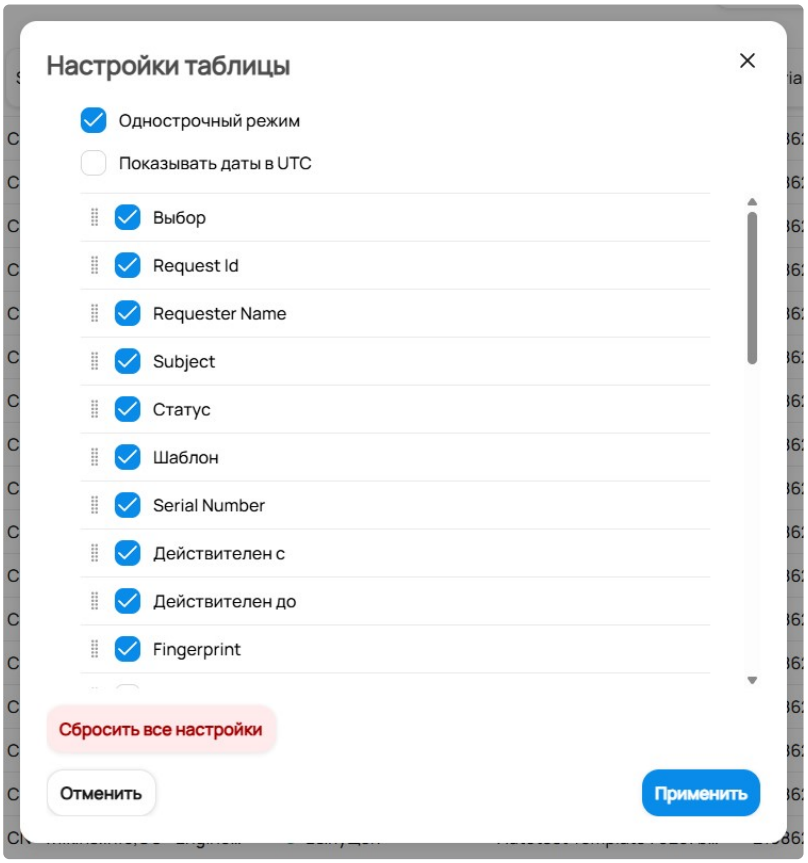
5.3 Настройка отображения таблицы

Настройте состав и порядок колонок под требуемые условия:

1. Нажмите кнопку с шестерёнкой над таблицей, откроется окно *Настройки таблицы*.
2. Проставьте чекбоксы напротив нужных пунктов для отображения соответствующих колонок в таблице.
3. Перетаскиванием (значок слева от названия колонки) измените порядок колонок.
4. При необходимости включите "Однострочный режим" и "Показывать даты в UTC".

Нажмите **Применить**. Для отказа от изменений нажмите **Отменить**, для возврата к значениям по умолчанию – **Сбросить все настройки**.

Однострочный режим размещает содержимое каждой записи в одну строку для отображения большего количества записей на экране. Режим "Показывать даты в UTC" отображает даты и время в едином часовом поясе UTC (применимо при сверке событий между разными площадками).



5.4 Выгрузка выборки (отчёт)

Сформированную поиском и фильтрами выборку можно сохранить в файл (для отчётов по выпущенным и отозванным сертификатам). Выгрузка доступна в разделах "Сертификаты", "Запросы" и "События".

Кнопка выгрузки сохраняет в файл именно текущую отфильтрованную выборку (то, что в данный момент отображается в таблице с учётом всех применённых условий). Так формируются отчёты по сертификатам, запросам и событиям для дальнейшего анализа, хранения или передачи.

1. Настройте поиск и фильтры так, чтобы в таблице осталась нужная выборка.
2. Нажмите кнопку выгрузки файла на панели действий, выборка будет сохранена в файл отчёта.

Сначала настройте фильтры, затем выполняйте выгрузку: в файл попадёт ровно тот набор записей, который виден в таблице. Чтобы получить полный отчёт, снимите все фильтры перед выгрузкой.

5.5 Выпуск сертификата

Выпуск сертификата — это подписание пользовательского запроса (CSR) закрытым ключом центра сертификации (УЦ): в результате пользователь получает готовый к использованию сертификат X.509, который подтверждает принадлежность открытого ключа указанному субъекту. Процедура состоит из двух этапов:

1. Формируется запрос на сертификат.
2. По сформированному запросу УЦ выпускает сертификат.

CSR (Certificate Signing Request) — это запрос на сертификат в формате PKCS#10. Он содержит открытый ключ и атрибуты субъекта (Subject (DN), при необходимости — Subject Alternative Name и набор расширений) и заверяется подписью парного закрытого ключа. Сам закрытый ключ в запрос не входит и в УЦ не передаётся. На подпись отправляется только файл запроса, поэтому закрытый ключ не покидает сервер владельца (отсутствует риск компрометации).

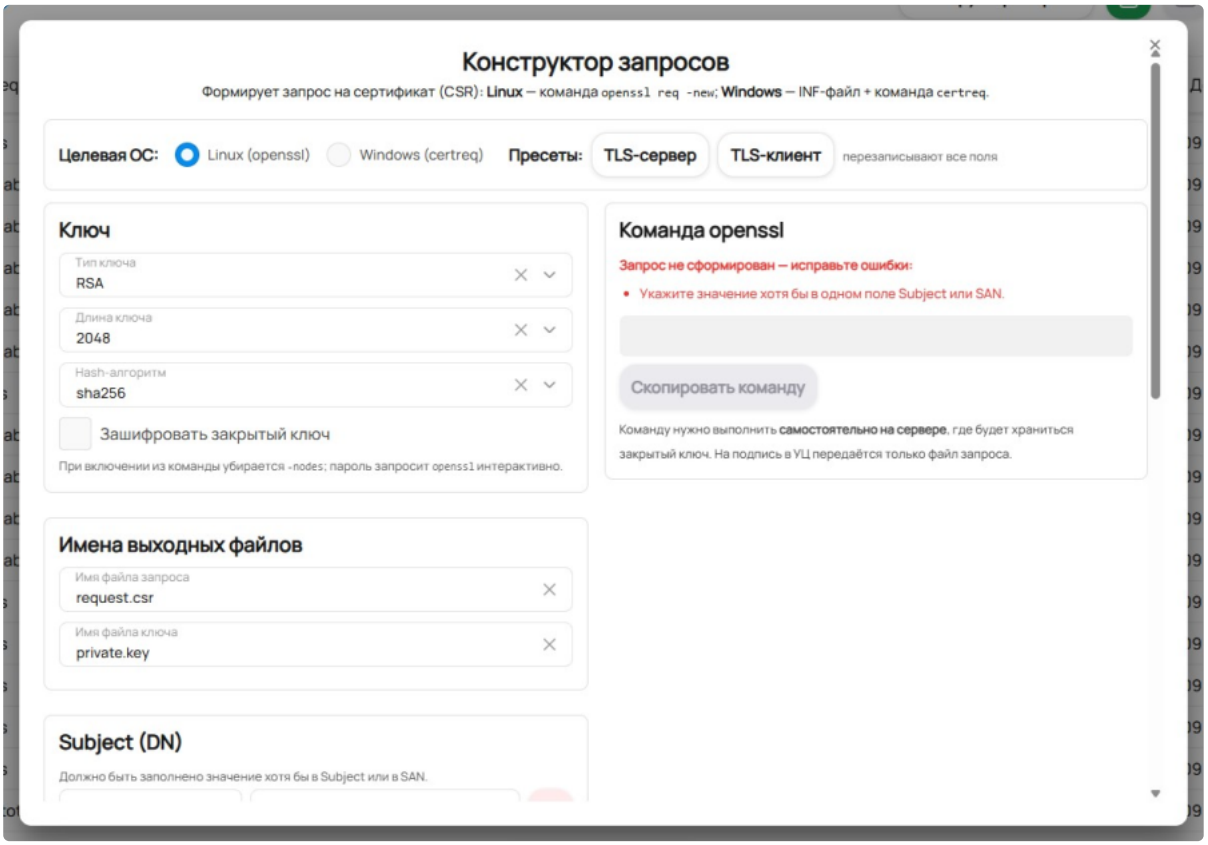
Важно

Центр сертификации не хранит закрытый ключ пользователя и не способен его восстановить при необходимости. Храните ключ в надёжном месте: он потребуется, чтобы пользоваться выпущенным сертификатом.

5.6 Подготовка запроса (CSR) через Конструктор

При отсутствии файла запроса (CSR) подготовьте его в Конструкторе: нажмите **Конструктор запроса** над реестром. Закрытый ключ при этом остаётся для подписи в центре сертификации (передаётся только файл запроса).

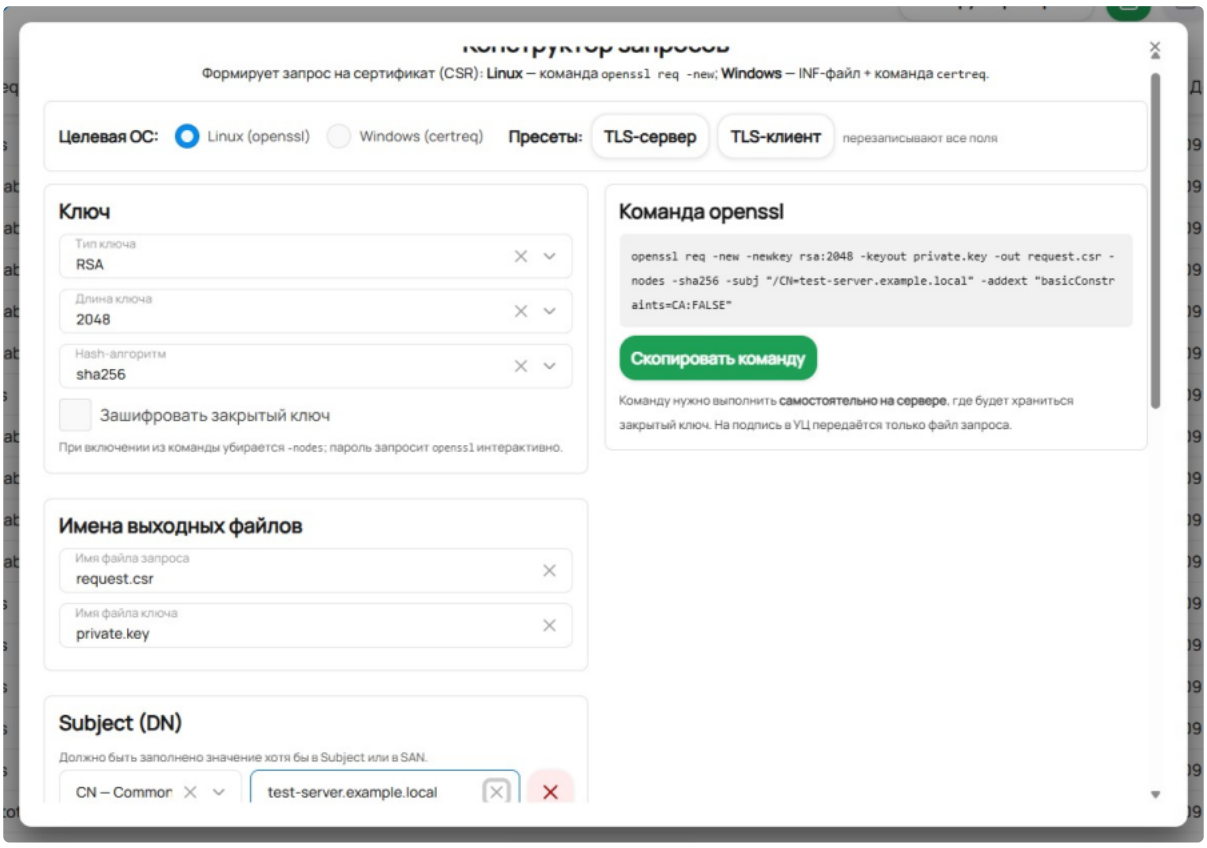
Конструктор не создаёт ключ и запрос за пользователя, однако он помогает собрать корректную команду по заданным параметрам. Команду пользователь выполняет самостоятельно на собственном сервере, где формируются пара ключей и файл CSR.



Заполните поля Конструктора:

1. Выберите Целевую ОС: — Linux (openssl) или Windows (certreq).
2. Задайте параметры в блоке "Ключ":
   - **Тип ключа** (в примере выше RSA);
   - **Длину ключа** (в примере выше 2048);
   - **Hash-алгоритм** (в примере выше sha256);
   - при необходимости установите чекбокс напротив опции "Зашифровать закрытый ключ" (закрытый ключ будет дополнительно защищён паролем).
3. При необходимости примените пресет "TLS-сервер" или "TLS-клиент". Они заполняют поля **keyUsage** и **extendedKeyUsage** типовым набором расширений для соответствующего сценария (пресеты перезаписывают все поля).
4. Заполните **Subject (DN)** (например, поле CN) и/или добавьте Subject Alternative Name (SAN, тип по умолчанию — DNS) и отметьте нужные расширения (extendedKeyUsage, keyUsage) — см. рисунок ниже. Значение должно быть указано хотя бы в Subject или в SAN, иначе команда не сформируется и отобразится подсказка "Укажите значение хотя бы в одном поле Subject или SAN".
5. Скопируйте собранную команду кнопкой **Скопировать команду** и выполните её на собственном сервере. Для Linux Конструктор формирует команду openssl req, для выходных файлов по умолчанию используются имена request.csr (запрос) и private.key (ключ).

> Чекбокс "Зашифровать закрытый ключ" добавляет в команду шифрование ключа паролем (без пароля воспользоваться таким ключом невозможно). Подробнее о защите ключей паролем см. в разделе **Защита ключей и конфиденциальных данных**.

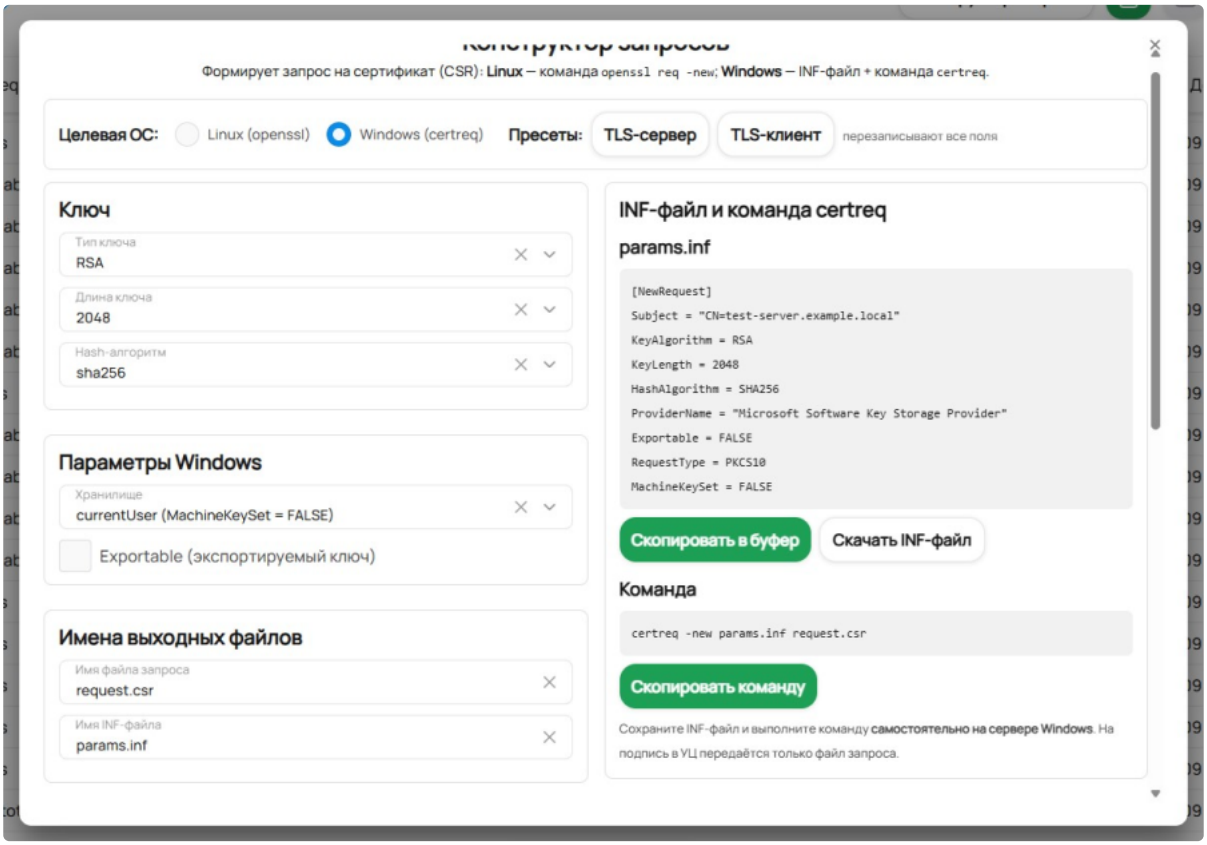



```
openssl req -new -newkey rsa:2048 -nodes -sha256 -keyout private.key -out request.csr
-subj "/CN=test-server.example.local"
```

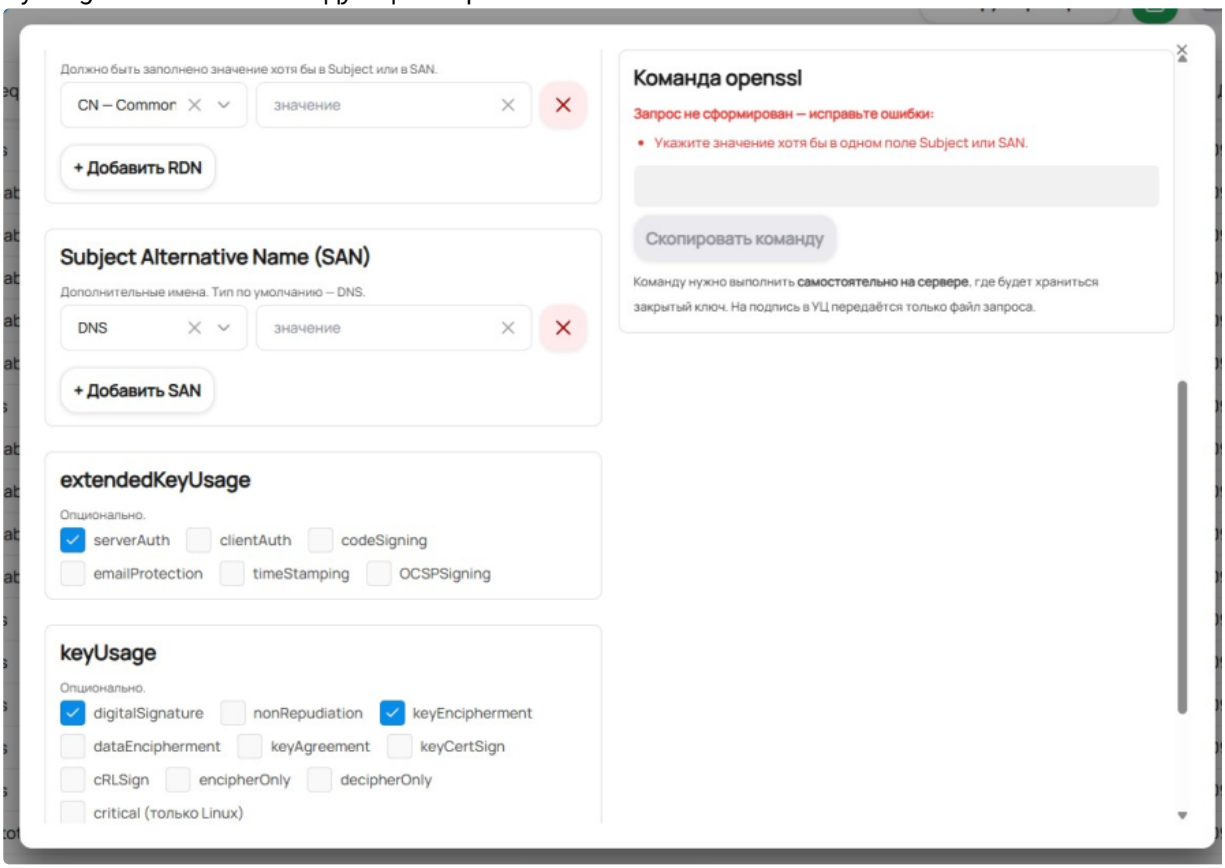
Важно

Для Windows Конструктор готовит INF-файл params.inf и команду certreq. Сохраните INF-файл ("Скачать INF-файл" или "Скопировать в буфер") и выполните команду на сервере Windows:

```
certreq -new params.inf request.csr
```



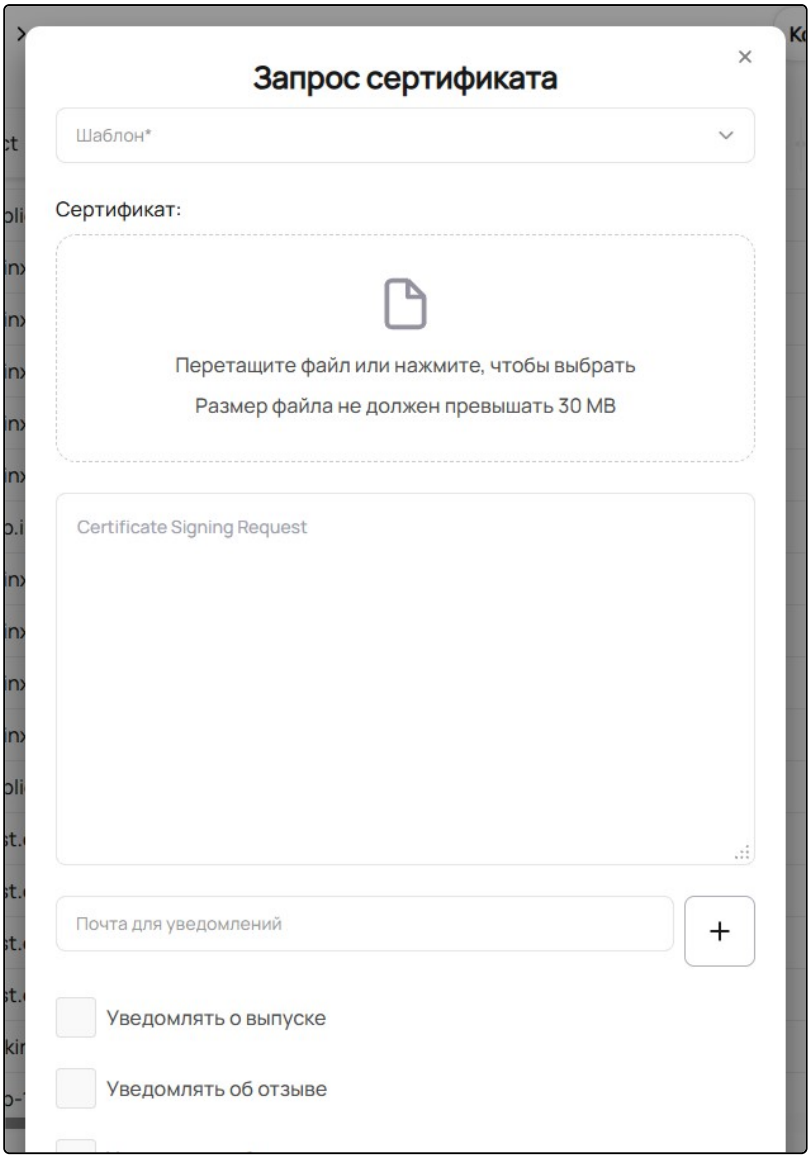
6. Поля **Subject (DN)**, **Subject Alternative Name (SAN)** и списки расширений extendedKeyUsage/ keyUsage заполняются следующим образом:



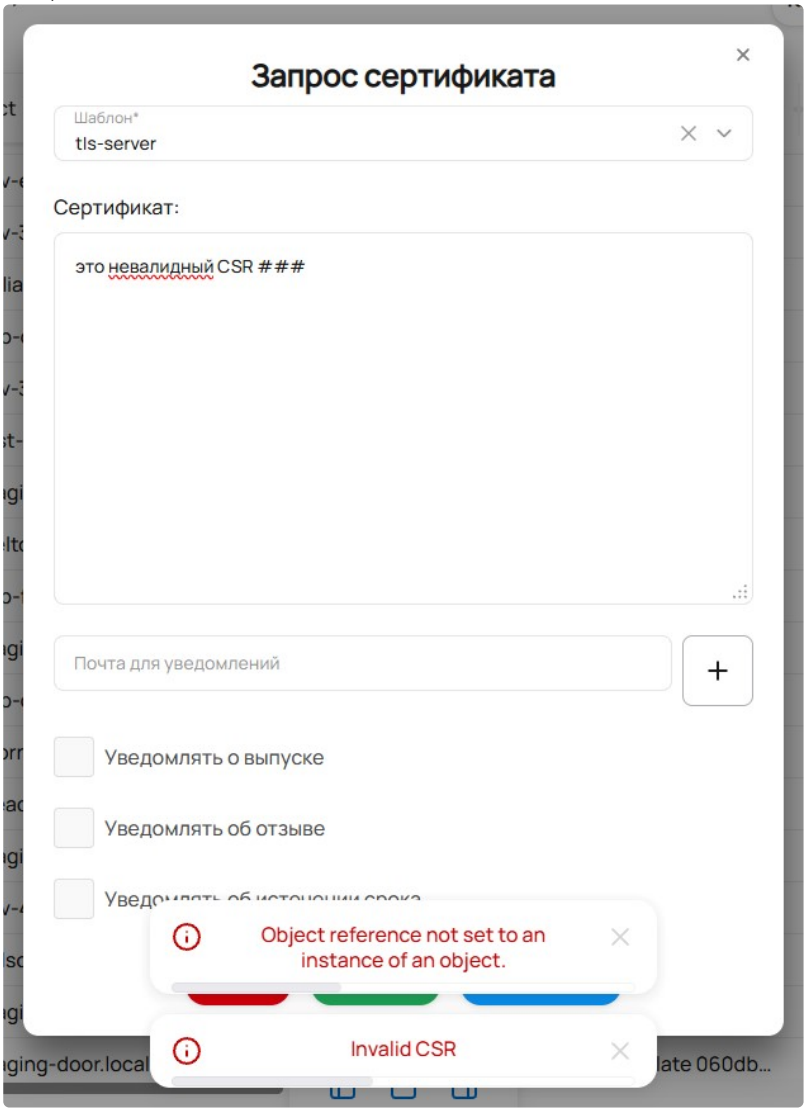
7. Нажмите **Запрос сертификата**.

8. Выберите Шаблон (в примере выше tls-server). Шаблон задаёт политику выпуска: допустимые тип и длину ключа, алгоритм, срок действия и набор расширений, которым должен соответствовать запрос.
9. Вставьте текст запроса в поле **Certificate Signing Request** или загрузите файл запроса в область добавления файла.
10. При необходимости укажите почту для уведомлений в соответствующем поле и включите оповещения по сертификату с помощью чекбоксов "Уведомлять о выпуске", "Уведомлять об отзыве" и "Уведомлять об истечении срока".
11. При наличии предпросмотра сверьте параметры запроса с шаблоном.
12. Нажмите **Подтвердить**.

Уведомления позволяют получать оповещения о ключевых событиях жизненного цикла сертификата: его выпуске, отзыве и истечении срока действия. В поле **Почта для уведомлений** можно указать несколько адресов.

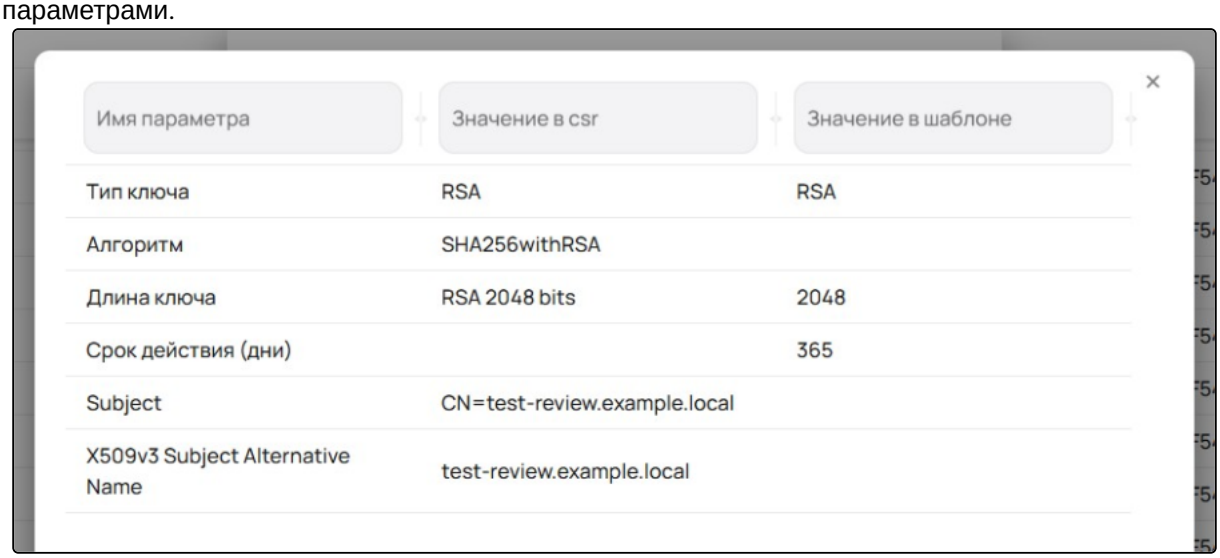


13. Система проверит запрос. При некорректном CSR она оповестит об ошибке (например "Invalid CSR").



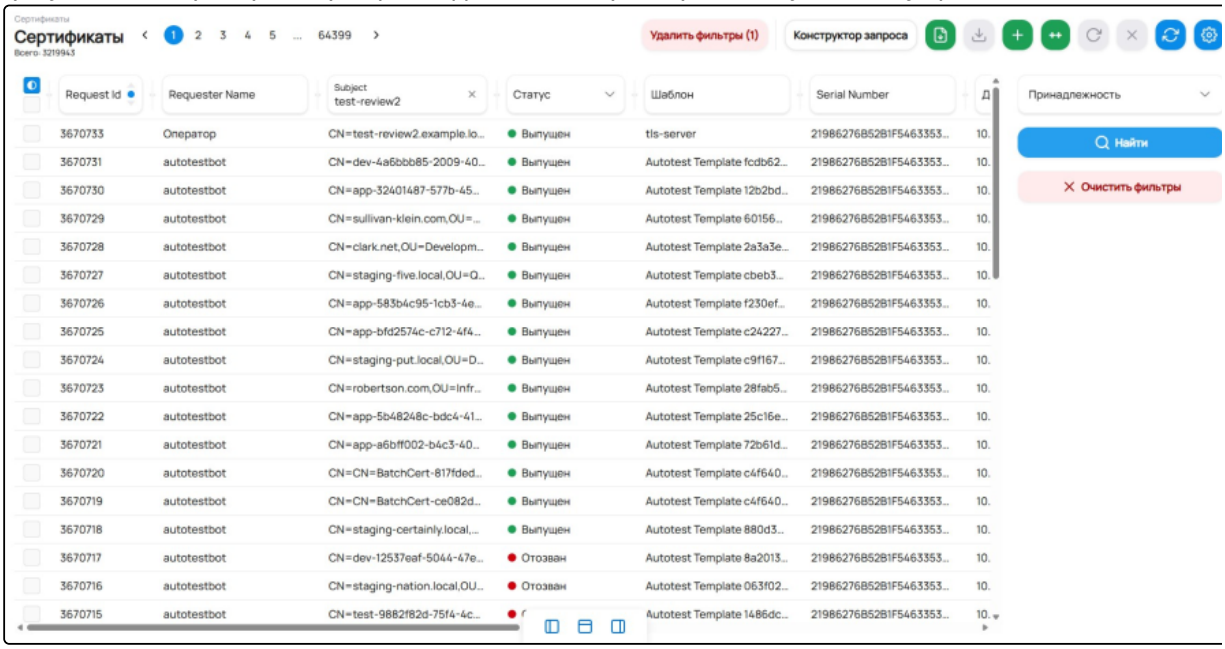
14. В предпросмотре сверьте Значение в CSR со Значением в шаблоне: тип и длину ключа, алгоритм, срок действия, Subject и SAN (в примере — тип ключа RSA, алгоритм SHA256withRSA, длина 2048, срок действия 365 дней). Такая сверка позволяет убедиться, что параметры запроса соответствуют политике шаблона ещё до выпуска и не выпустить сертификат с неподходящими

параметрами.



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	

15. При успешной проверке сертификат добавится в реестр со статусом *Выпущен*.



Обратите внимание, что ту же операцию можно выполнить через командную строку. УЦ выпустит сертификат по указанному файлу запроса и шаблону:

```
./mclient ca -csr request.csr -template tls -out cert.crt4.3
```

Когда нужно выпустить сразу множество сертификатов, используйте пакетный выпуск через форму "Запрос сертификатов". На вход подаётся файл со списком запросов (CSR), и по каждому из них выпускается сертификат. Результат выпуска защищается заданным паролем.

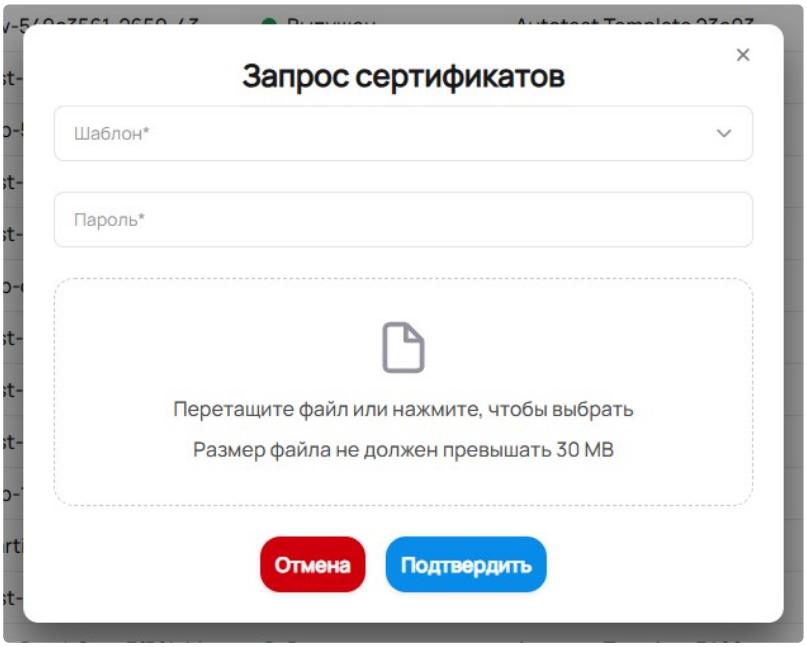
Алгоритм действий для пакетного выпуска:

1. Откройте пакетный выпуск (Запрос сертификатов).
2. Заполните поле **Шаблон** (выберите шаблон из списка).

3. Заполните поле **Пароль**. Заполненным паролем будет защищён сформированный пакет с результатами выпуска.
4. Загрузите файл со списком запросов в область добавления файла.

Нажмите **Подтвердить**.

> Для всех запросов пакета применяется один выбранный шаблон, поэтому включите в пакет запросы, которым соответствует одинаковая политика выпуска.



6 Карточка сертификата

Карточка сертификата — это подробное представление одной записи реестра, в котором собраны все реквизиты сертификата и доступны основные операции над ним: просмотр параметров, оформление подписок на события, скачивание, отзыв и восстановление. Данные распределены по вкладкам: *Информация о сертификате*, *События* и *Подписки*.

Ниже будут подробнее рассмотрены все доступные операции в рамках работы с сертификатами.

6.1 Просмотр карточки

Карточка содержит полный набор реквизитов и точек распространения.

Откройте карточку, чтобы проверить параметры и текущий статус выпущенного сертификата, свериться с цепочкой доверия при диагностике или подготовить сертификат к передаче:

1. В реестре сертификатов выберите нужную строку и перейдите в неё, после чего откроется раздел "Информация о сертификате".
2. На вкладке *Информация о сертификате* проверьте реквизиты: Request Id, Subject, Serial, срок действия, тип и размер ключа, Fingerprint, SAN, Key Usage/EKU, SKI/AKI, а также точки распространения — AIA (OCSP) и CDP (CRL Distribution Point).
3. Для просмотра истории операций по сертификату откройте вкладку *События*, для оповещений — вкладку *Подписки*.

Рисунок 5 Карточка "Информация о сертификате"

- Fingerprint (отпечаток сертификата) — контрольное хеш-значение, идентифицирующее сертификат.
- SKI (идентификатор ключа субъекта) и AKI (идентификатор ключа издателя) — значения, которые связывают сертификат с его открытым ключом и с ключом выпустившего удостоверяющего центра. По паре SKI/AKI выстраивается и проверяется цепочка доверия AIA (Authority Information Access), включая адрес OCSP.

- OCSP — точка, по которой приложение в реальном времени запрашивает актуальный статус сертификата (действителен или отозван), не загружая целиком список отзыва.
- CDP (CRL Distribution Point) — адрес, по которому публикуется и откуда загружается список отзыва (CRL).
  Key Usage и Extended Key Usage (EKU) — разрешённое назначение сертификата: допустимые криптографические операции (например, цифровая подпись, согласование ключей) и прикладные сценарии применения (например, аутентификация сервера или клиента).

Через командную строку пользователю доступно:

- получение сертификата:

```
./mclient get
```

- отображение статуса сертификата:

```
./mclient status
```

Назначение ключевых реквизитов и точек распространения:

6.2 Подписки

На вкладке *Подписки* пользователь может оформить оповещения по конкретному сертификату. Система будет уведомлять о значимых событиях его жизненного цикла (например, о приближающемся истечении срока действия сертификата).

1. Откройте карточку сертификата и перейдите на вкладку *Подписки*.
2. Оформите подписку на нужные события сертификата.

Отслеживаемые события:

- выпуск сертификата;
- отзыв сертификата;
- истечение срока действия.

Подписка действует в пределах выбранного сертификата, поэтому оповещения касаются только этой записи. Заблаговременное уведомление об истечении срока позволяет вовремя перевыпустить сертификат и избежать перерыва в обслуживании.

6.3 Скачивание сертификата

Данное действие требуется, когда сертификат необходимо передать на конечную систему или сохранить в архив. Формат файла выбирают под требования принимающей стороны. Содержимое сертификата при этом одинаково, различается лишь способ кодирования.

1. Откройте карточку сертификата и нажмите **Скачать сертификат**.
2. В открывшемся меню выберите формат файла: PEM (текстовый) или DER (двоичный).

Рисунок 6 Меню "Скачать сертификат" с выбором формата

- PEM — текстовый формат (данные в кодировке Base64, файл можно открыть в текстовом редакторе). Подходит для веб-серверов и систем на базе Linux.
- DER — двоичный формат (компактное бинарное представление). Подходит для платформы Windows и аппаратных устройств.

Если принимающая система не задаёт формат явно, для веб-серверов и Linux обычно используется PEM, а для Windows и устройств — DER. При необходимости файл можно перекодировать из одного формата в другой.

Чтобы выгрузить несколько сертификатов сразу, отметьте нужные строки в реестре с помощью чекбоксов и нажмите **Скачать сертификат**.

Для массовой выгрузки сертификатов через командную строку выполните следующую команду:

```
./mclient export
```

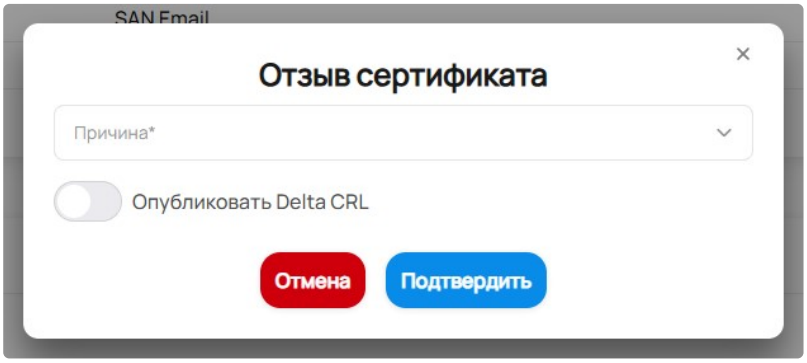
Какой формат выбрать:

6.4 Отзыв сертификата

Отзыв применяют, когда сертификат скомпрометирован или больше не считается доверенным. Отозванный сертификат перестаёт быть доверенным до истечения своего срока, а проверяющие стороны получают об этом информацию через списки отзыва (CRL) и службу OCSP. Для большинства причин отзыв необратим (исключение — временная приостановка, см. раздел "Восстановление сертификата").

1. Откройте карточку сертификата (или отметьте его строку в реестре) и нажмите **Отозвать**.

2. Выберите причину отзыва.
3. При необходимости включите опцию "Опубликовать Delta CRL".
4. Нажмите **Подтвердить**.



Причина отзыва фиксируется в списке отзыва и сообщает проверяющей стороне, почему сертификат перестал быть доверенным. Доступные причины:

- unspecified — причина не указана. Применяется, когда конкретную причину раскрывать не требуется.
- keyCompromise — компрометация закрытого ключа сертификата (ключ мог стать доступен посторонним).
- CACompromise — компрометация ключа удостоверяющего центра, выпустившего сертификат.
- affiliationChanged — изменение принадлежности владельца (например, смена организации, подразделения или реквизитов).
- superseded — сертификат заменён новым (перевыпущен).
- cessationOfOperation — прекращение эксплуатации сертификата или обслуживаемой им системы.
- certificateHold — временная приостановка действия сертификата. Является единственной обратимой причиной (см. раздел "Восстановление сертификата").
- removeFromCRL — исключение сертификата из списка отзыва. Применяется, чтобы снять ранее установленную приостановку (certificateHold).

Переключатель "Опубликовать Delta CRL" сразу отражает отзыв в разностном (инкрементальном) списке отзыва — Delta CRL. Такой список содержит только изменения, произошедшие после последнего полного CRL, поэтому проверяющие стороны информируются об отзыве быстрее, не дожидаясь планового формирования полного списка.

Статус изменится на *Отозван*, а сертификат попадёт в списки отзыва (CRL/OCSP). Операция зафиксируется на вкладке *События*.

Отзыв сертификата через командную строку:

```
/mclient revoke
```

6.5 Восстановление сертификата

Восстановление возвращает в действие сертификат, ранее приостановленный с причиной Certificate Hold.

1. В реестре отметьте сертификат, отозванный с причиной Certificate Hold.
2. Нажмите **Восстановить выбранные сертификаты**.

Сертификат будет исключён из списков отзыва при их следующем формировании.

> **Важно**
>
> Вернуть в действие можно только сертификат, приостановленный с причиной certificateHold (в карточке — Certificate Hold). Эта причина изначально используется как временная и обратимая. Отзыв по любой другой причине (keyCompromise, CACompromise, affiliationChanged, superseded, cessationOfOperation, unspecified) является окончательным. Восстановить такой сертификат нельзя, потребуется выпустить новый.

Восстановление сертификата через командную строку:

```
./mclient repair
```

7 Шаблоны сертификатов

Шаблон сертификата — именованный набор ограничений и расширений, который центр сертификации применяет при обработке запроса на выпуск сертификата (CSR). Шаблоны контролируют состав атрибутов запроса и упрощают его подготовку: часть атрибутов и расширений задаётся самим шаблоном, поэтому указывать их в запросе вручную не требуется, а сам запрос перед выпуском проверяется на соответствие заданной шаблоном политике.

Шаблоны хранятся в базе данных центра сертификации. Каждый шаблон имеет версию (её номер меняется при изменении параметров) и разрешения, которые разграничивают доступ на просмотр и на изменение. Кроме того, у шаблона предусмотрен признак "Шифровать данные в БД". При его включении данные сертификатов хранятся в базе в зашифрованном виде (подробнее см. в разделе "Защита ключей и конфиденциальных данных".

7.1 Просмотр шаблонов

Просмотр шаблонов позволяет просматривать политики выпуска — набор ограничений и расширений, которые центр сертификации применяет при формировании сертификатов.

Раздел "Шаблоны" содержит реестр шаблонов. Для каждого шаблона в списке отображаются столбцы "Название", "Версия", "Описание", "Максимальный срок действия", "Изменён", "Basic Constraints" и "Key Usage". Над таблицей расположена панель действий (в примере на рисунке ниже в реестре 29 шаблонов). Реестр даёт сводное представление о действующих политиках: по столбцам видно версию шаблона, предельный срок действия и ключевые расширения без раскрытия карточки.

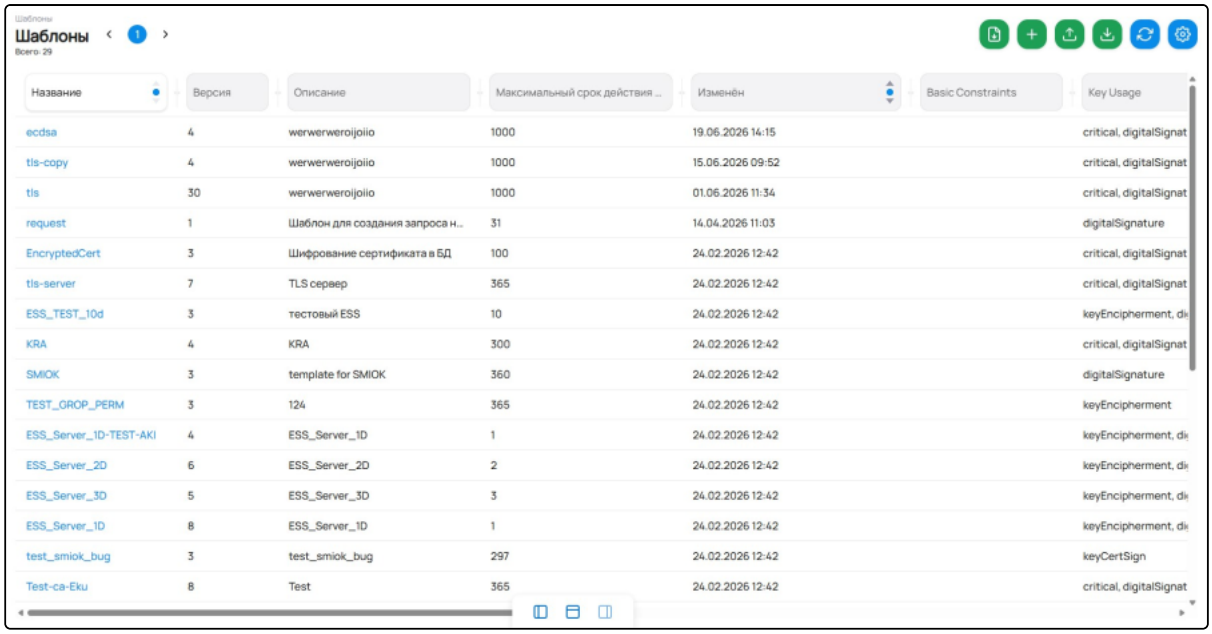


Рисунок 7 Список шаблонов

Чтобы посмотреть параметры шаблона, выберите его в списке. В карточке шаблона отображаются:

- Максимальный срок действия.
- Допустимый тип ключа и иинимально допустимый размер ключа.
- Наборы Key Usage и Extended Key Usage.

- Чекбоксы отключения расширений AIA (-noaia) и CDP (-nocdp).
- Разрешения для просмотра и разрешения для изменения. Эти параметры определяют, каким требованиям должен удовлетворять запрос и какие расширения получит выпущенный по шаблону сертификат:
- Максимальный срок действия — верхняя граница срока действия сертификата. Запрошенный срок не может её превышать.
- Допустимый тип ключа и минимально допустимый размер ключа — ограничения на ключ запроса. Его алгоритм (например, RSA) должен соответствовать допустимому типу, а размер быть не меньше указанного минимума. Запрос должен удовлетворять этим ограничениям.
- Key Usage и Extended Key Usage — разрешённое назначение сертификата (допустимые способы использования ключа и прикладные роли сертификата). Значения из этих наборов записываются в соответствующие расширения выпускаемого сертификата.
- Чекбоксы -noaia и -nocdp отключают добавление в сертификат расширений AIA (адрес доступа к сведениям центра сертификации, в том числе службы OCSP) и CDP (адрес точки распространения списка отзыва CRL). Их необходимо проставить, когда соответствующие адреса в сертификате не нужны.
- Разрешения для просмотра и разрешения для изменения — списки, определяющие, какие операторы могут просматривать шаблон и изменять его параметры.

В примере открыт шаблон ecdsa (версия 4) с максимальным сроком 1000 и минимально допустимым размером ключа 256.

Рисунок 8 Карточка шаблона

Через командную строку пользователю доступно:

- получение списка шаблонов:

```
./mclient templates
```

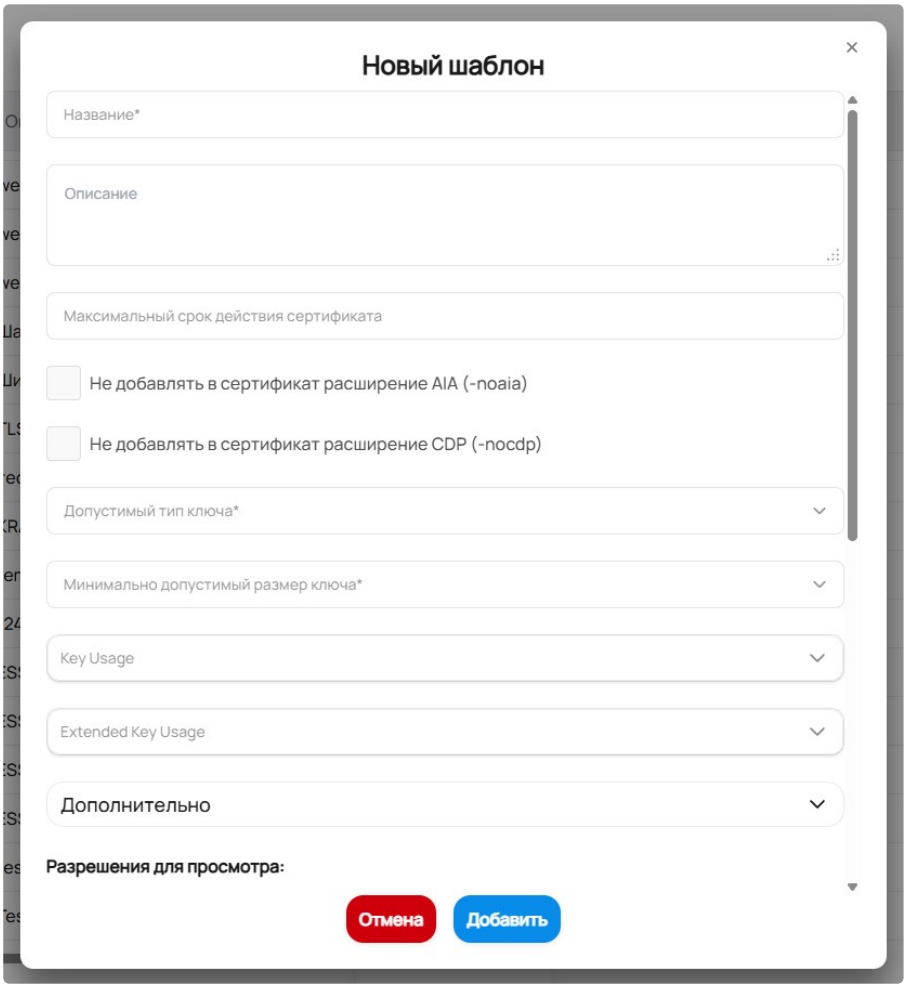
- отображение параметров шаблона:

```
./mclient gettempl
```

7.2 Создание шаблона

Создайте шаблон, когда требуется новая политика выпуска с собственным набором ограничений на ключ и расширений сертификата. Заранее определите допустимые тип и размер ключа, предельный срок действия и требуемые назначения сертификата. Эти значения станут ограничениями для всех запросов, обрабатываемых по шаблону.

1. Нажмите **Создать шаблон**, откроется окно *Новый шаблон*.
2. Укажите название и описание в соответствующих полях.
3. Задайте максимальный срок действия сертификата, выберите допустимый тип ключа и минимально допустимый размер ключа.
4. Выберите значения Key Usage и Extended Key Usage.
5. При необходимости установите чекбоксы "Не добавлять в сертификат расширение AIA (-noaia)" и "Не добавлять в сертификат расширение CDP (-nocdp)" и задайте разрешения для просмотра и разрешения для изменения.
6. Нажмите **Добавить**.



Если данные сертификатов, выпускаемых по шаблону, требуется хранить в базе в зашифрованном виде, включите признак "Шифровать данные в БД" (см. раздел "Защита ключей и конфиденциальных данных"). После сохранения шаблон получит номер версии, который увеличивается при каждом последующем изменении его параметров.

Создание шаблона через командную строку:

```
./mclient addtempl
```

Удаление шаблона через командную строку:

```
./mclient deltempl
```

8 Запросы и согласование выпуска

Раздел описывает работу с заявками на выпуск сертификатов: просмотр реестра, одобрение и отклонению заявок.

Согласование выпуска — это точка контроля. Подтверждая или отклоняя заявки, пользователь определяет, какие сертификаты выпустит центр сертификации, а какие — нет. Пока заявка не одобрена, сертификат по ней не выпускается.

8.1 Реестр запросов

Раздел "Запросы" содержит реестр заявок на выпуск сертификатов (CSR) и позволяет отслеживать их обработку.

Заявка формируется на основании запроса на подпись сертификата — CSR в формате PKCS#10, который содержит открытый ключ будущего владельца и параметры запрашиваемого сертификата (Subject, SAN и другие).

Реестр формирует единое представление обо всех поступивших заявках и текущем этапе их обработки. Каждая строка реестра — отдельная заявка, для которой отображаются столбцы "Request ID", "Инициатор (Requester Name)", "Subject", "Статус", "Шаблон" и "Common Name". Заявка может находиться в одном из статусов: *Pending* (ожидает согласования), *Satisfied* (выполнена) или *Rejected* (отклонена).

Столбцы помогают оценить заявку, не открывая карточку заявки:

- Request ID — уникальный идентификатор заявки, по которому заявку можно идентифицировать, а также на сам идентификатор можно ссылаться;
- Requester Name — инициатор заявки;
- Subject и Common Name — для кого и на какое имя выпускается сертификат;
- Шаблон — применяемый шаблон выпуска сертификата;
- Статус — текущий этап обработки.

Жизненный цикл заявки: новая заявка попадает в реестр в статусе *Pending* и ожидает решения о согласовании. После обработки она переходит в один из двух статусов:

- *Satisfied* — заявка одобрена, и по ней выпущен сертификат;
- *Rejected* — заявка отклонена, сертификат по ней не выпускается.

> **Важно**
>
> Обрабатывать (одобрять или отклонять) можно только заявки в статусе *Pending*. Статусы *Satisfied* и *Rejected* — итоговые, они фиксируют результат согласования заявки.

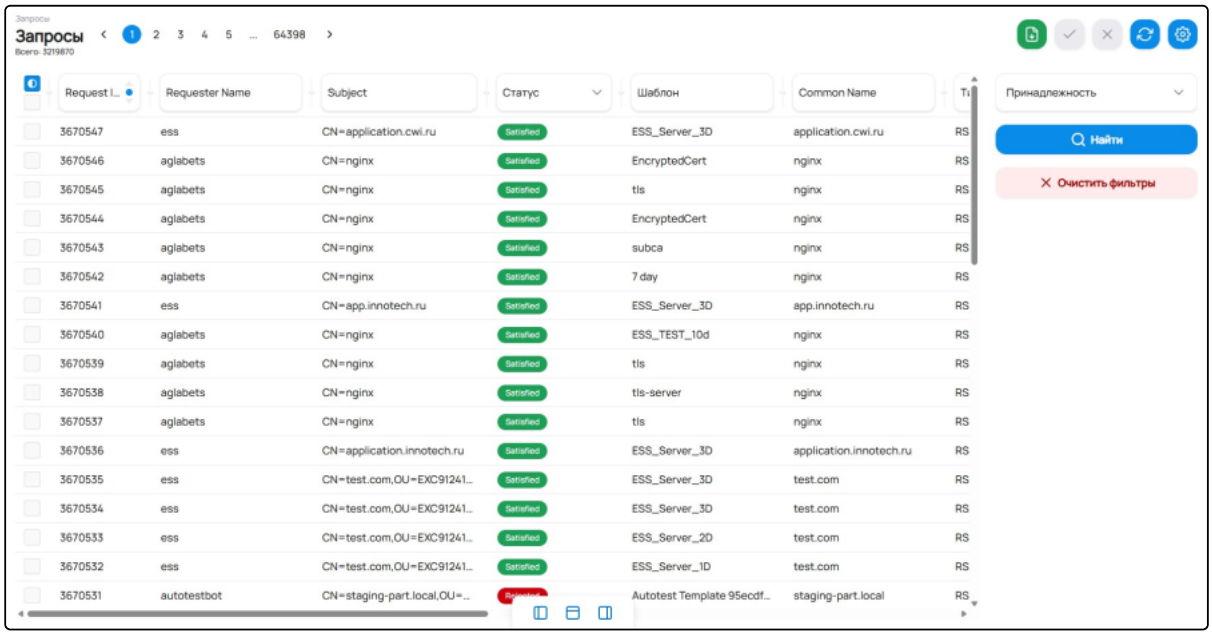


Рисунок 9 Реестр запросов на выпуск

Чтобы принять решение по конкретной заявке, откройте её карточку и сверьте параметры запроса с ожидаемыми.

Чтобы изучить заявку:

1. Выберите нужную строку в реестре, откроется карточка "Информация о запросе".
2. Изучите параметры запроса: Subject, Common Name, значения SAN (SAN DNS, SAN IP и другие), а также Тип ключа и Размер ключа (в примере на рисунке ниже RSA, 2048).
3. Для заявки в статусе *Satisfied* перейдите по ссылке "Посмотреть сертификат" в поле **Сертификат**, чтобы открыть выпущенный сертификат.

При проверке убедитесь, что Subject и Common Name соответствуют имени узла или службы, для которых запрашивается сертификат, а перечень SAN (SAN DNS, SAN IP) охватывает все адреса, под которыми этот узел должен быть доступен. Поля **Тип ключа** и **Размер ключа** (в примере на рисунке RSA, 2048) показывают криптографические параметры запроса.

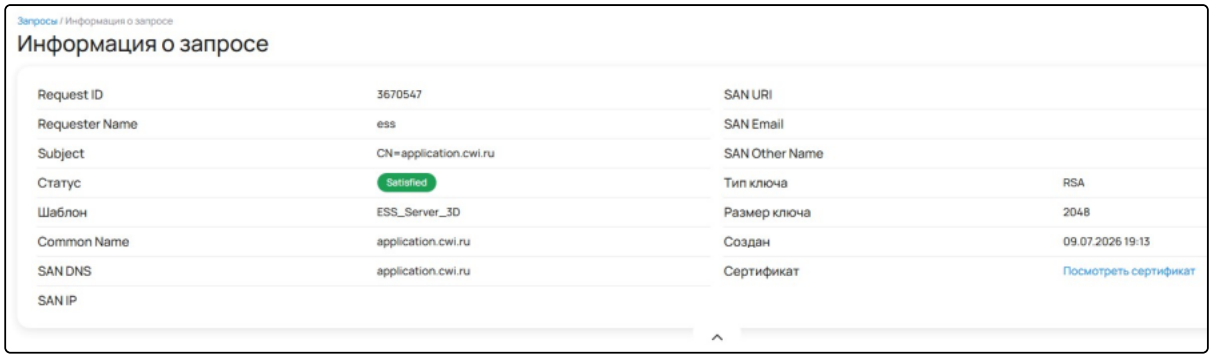


Рисунок 10 Карточка "Информация о запросе"

Важно

Ссылка "Посмотреть сертификат" доступна только у заявок в статусе *Satisfied* (только по ним выпущен сертификат). У заявок в статусах *Pending* и *Rejected* выпущенного сертификата нет.

8.2 Одобрение и отклонение заявок

Согласование выпуска выполняется по заявкам в статусе *Pending*. Их нужно либо одобрить (тогда сертификат будет выпущен), либо отклонить. Таким образом контролируется, какие именно сертификаты выпускает центр сертификации.

Откройте заявку в статусе *Pending*, в карточке "Информация о запросе" будут доступны кнопки **Одобрить** и **Отклонить**.

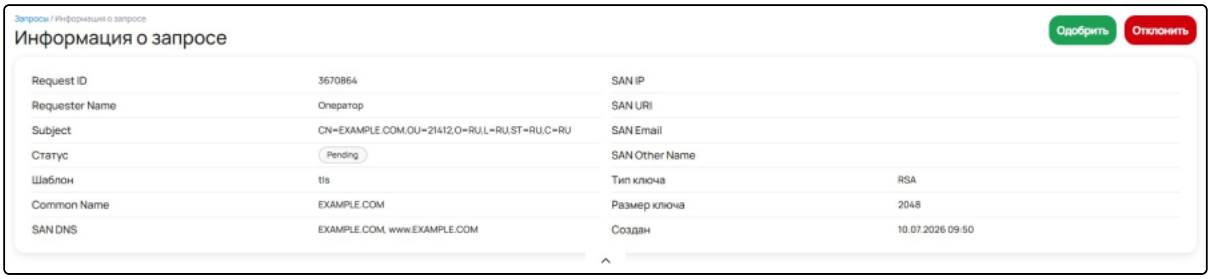


Рисунок 11 Заявка в статусе Pending с кнопками одобрения и отклонения

Чтобы согласовать выпуск, нажмите **Одобрить** (по заявке будет выпущен сертификат). Чтобы отказать в выпуске, нажмите **Отклонить**, укажите причину в обязательном поле **Причина** и нажмите **Подтвердить**, после чего заявка перейдёт в статус *Rejected*.

> Поле **Причина** при отклонении обязательно к заполнению. Укажите исчерпывающую в плане информации причину отказа. Она объяснит, почему в выпуске сертификата было отказано.

После одобрения заявка перейдет в статус *Satisfied*, и выпущенный сертификат станет доступен по ссылке "Посмотреть сертификат" в её карточке.

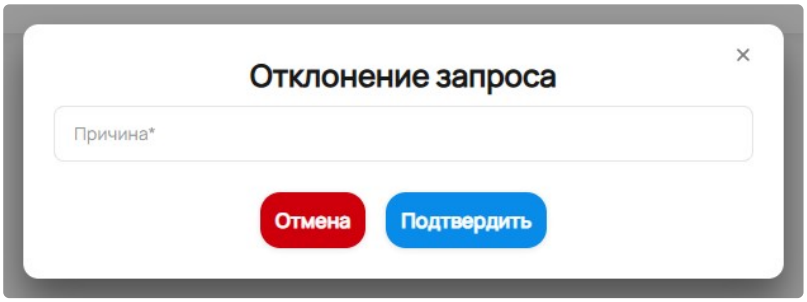


Рисунок 12 Диалог «Отклонение запроса» с обязательным полем «Причина»

8.3 Групповые действия над заявками

При большом количестве заявок их можно обрабатывать группой (одобрить, отклонить или обновить одновременно несколько заявок):

Отметьте через чекбоксы нужные заявки в реестре.

На панели над реестром выберите действие необходимое действие: "Одобрить", "Отклонить" или "Обновить", после этого примените его к отмеченным заявкам.

Групповое действие применяется сразу ко всем отмеченным заявкам. Для группового одобрения или отклонения отмечайте только заявки в статусе *Pending*, так как именно такие заявки ожидают согласования.

9 Аудит и списки отзыва

Раздел объединяет средства аудита работы центра сертификации (журнал событий) и управление списками отзыва сертификатов (CRL и Delta CRL).

9.1 Журнал событий

Журнал событий фиксирует все операции центра сертификации и необходим для аудита — просмотра и отбора выполненных действий. С его помощью можно установить инициатора операции, время её выполнения и результат, расследовать инциденты и подтвердить факт выпуска или отзыва конкретного сертификата.

1. Откройте раздел "События", отобразится журнал аудита с колонками "ID", "Дата", "Событие", "Код ошибки", "Requester", "Request ID", "Serial Number" и "Шаблон". Записи распределены по страницам.

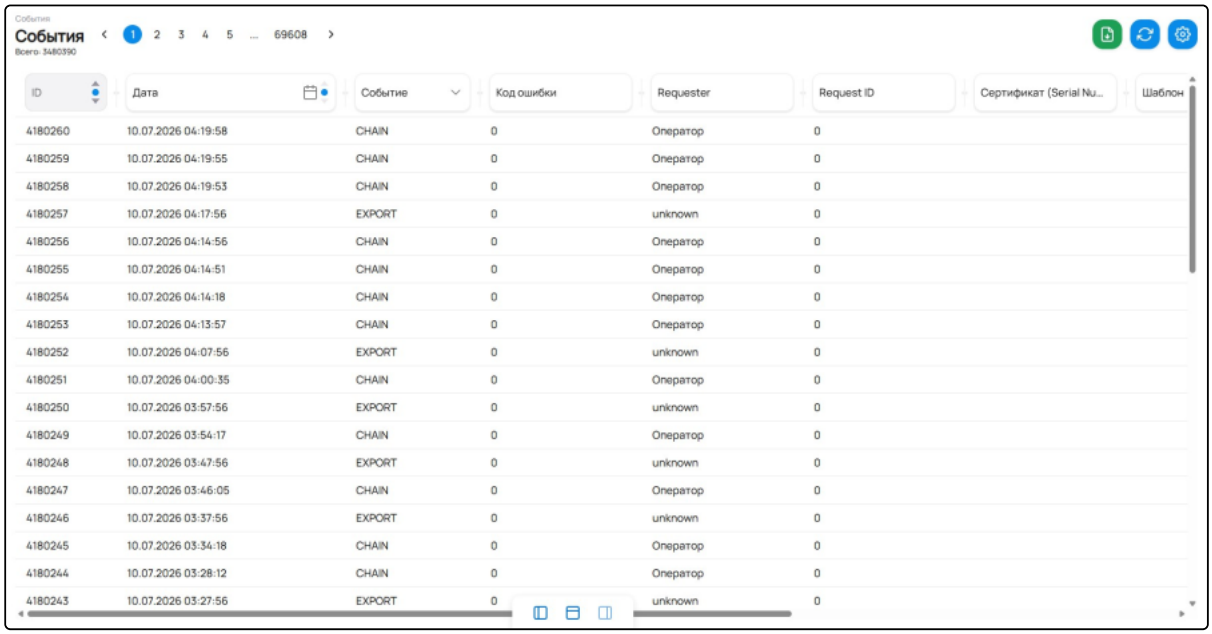


Рисунок 13 Журнал "События"

- ID — порядковый идентификатор записи журнала;
- Дата — дата и время выполнения операции;
- Событие — тип выполненной операции (перечень значений приведён на шаге № 2);
- Код ошибки — код результата операции, позволяющий различить успешно выполненные операции от завершившихся с ошибкой;
- Requester — инициатор операции (учётная запись или клиент, от имени которого она выполнена);
- Request ID — идентификатор исходного запроса, по которому проведена операция;
- Serial Number — серийный номер сертификата, к которому относится операция;
- Шаблон — шаблон сертификата, использованный в операции.

Таким образом, по каждой записи видно инициировавшего операцию (Requester), её результат (Код ошибки) и к какому сертификату она относится (Serial Number).

Чтобы отобрать нужные записи, используйте фильтры над колонками. Для отбора по типу операции нажмите на фильтр в колонке "Событие" и выберите значение: CA, REVOKE, STATUS, GET, CRL, DELTA_CRL, UPDATE_CRL, UPDATE_DELTA_CRL.

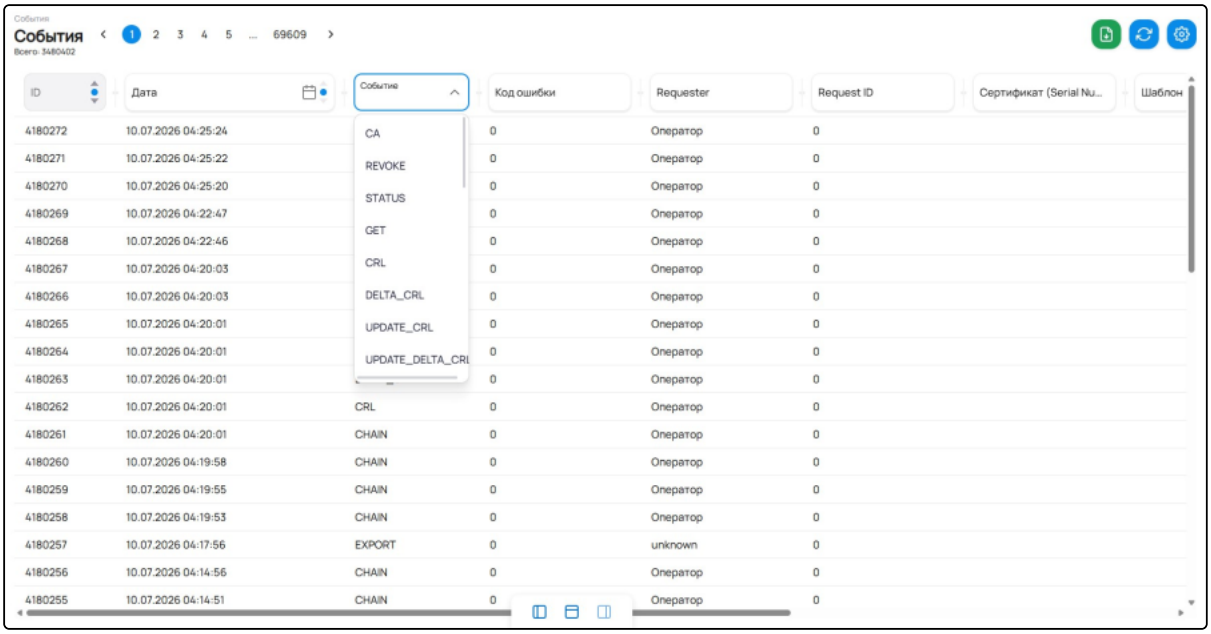


Рисунок 14 Фильтр по колонке "Событие"

Основные типы событий (значения фильтра "Событие"):

- CA — выпуск сертификата;
- REVOKE — отзыв сертификата;
- STATUS — проверка статуса сертификата;
- GET — получение (выгрузка) сертификата;
- CRL, DELTA_CRL — операции с полным и разностным списками отзыва;
- UPDATE_CRL, UPDATE_DELTA_CRL — обновление полного и разностного списков отзыва соответственно.

Чтобы сохранить полученную выборку в файл, нажмите кнопку выгрузки в правом верхнем углу журнала. Выгрузка сохраняет текущую выборку с учётом применённых фильтров. Это применимо для передачи данных аудита во внешние системы или для формирования отчётов за определенный период.

Значения колонок:

9.2 Списки отзыва CRL и Delta CRL

Раздел отражает текущее состояние полного списка отзыва (CRL) и разностного (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 или прекращении полномочий владельца) и своевременно прекратить доверие к нему.

Различие между списками:

- CRL — полный список всех отозванных сертификатов, действительных на момент публикации. Клиент загружает его целиком.

- Delta CRL — разностный (дополнительный) список, содержащий только изменения с момента публикации последнего полного CRL, то есть сертификаты, отозванные после него. Он существенно меньше по объёму и снижает нагрузку на сеть и вычислительные ресурсы. Таким образом, клиенту требуется только догрузить различия.

> Списки отзыва отражают состояние на момент их формирования и публикуются по расписанию (см. поле **Следующее обновление**). Чтобы проверить статус одного конкретного сертификата в реальном времени, используйте протокол OCSP.

Откройте раздел "Информация о CRL и Delta CRL", отобразятся карточки CRL и Delta CRL с полями "Номер", "Последнее обновление", "Следующее обновление" и "Количество отозванных, а ниже, на вкладке *Отозванные сертификаты* — таблица отозванных сертификатов (Request Id, Requester Name, Subject, Шаблон, Serial Number, срок действия).

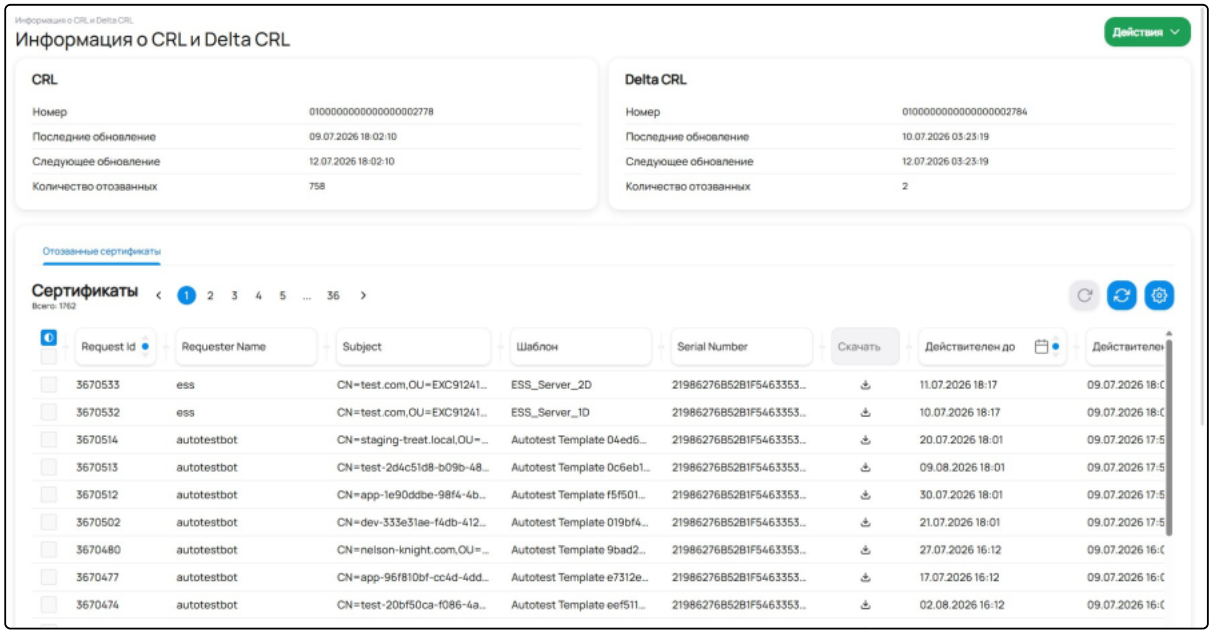


Рисунок 15 Информация о CRL и Delta CRL

- **Номер** — порядковый номер выпуска списка. При каждом обновлении увеличивается.
- **Последнее обновление** — дата и время формирования текущей версии списка.
- **Следующее обновление** — плановое время следующей публикации.
- **Количество отозванных** — число сертификатов, включённых в список.

На вкладке *Отозванные сертификаты* приведён их перечень: для каждого сертификата указаны запрос (Request Id), инициатор (Requester Name), владелец (Subject), Шаблон, серийный номер (Serial Number) и срок действия.

Чтобы скачать или обновить список, откройте меню **Действия** в правом верхнем углу и выберите нужное действие: **Скачать CRL**, **Скачать Delta CRL** или **Обновить CRL**:

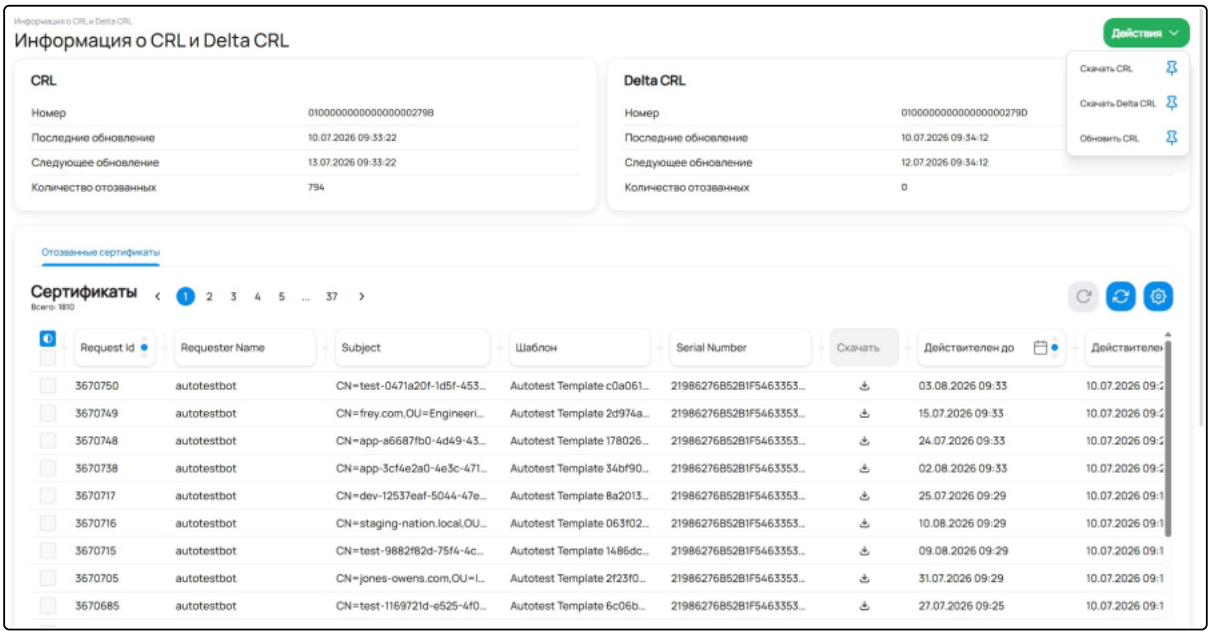


Рисунок 16 Меню "Действия"

Команды **Скачать CRL** и **Скачать Delta CRL** сохраняют соответствующий список в файл, а **Обновить CRL** формирует и публикует новую версию списка. После обновления увеличивается **Номер** и обновляются поля **Последнее обновление** и **Следующее обновление**.

Через командную строку пользователю доступно:

- обновить CRL:

```
./mclient updcrl
```

- обновить Delta CRL:

```
./mclient updeltacrl
```

Значение полей карточек:

10 Настройки, задачи и обслуживание

Раздел объединяет инструменты администрирования удостоверяющего центра: выбор активного экземпляра ЦС и просмотр его состояния, контроль автоматических задач публикации и запуск готовых сценариев обслуживания.

10.1 Выбор экземпляра ЦС и его состояние

Раздел "Настройки" используется, когда нужно переключить активный экземпляр удостоверяющего центра или проверить его текущее состояние.
Система поддерживает несколько экземпляров ЦС одновременно (например, отдельные центры для разных сред или подразделений). Переключение между ними выполняется именно в этом разделе. Выбранный экземпляр становится активным, остальные разделы контрольной панели показывают данные и выполняют операции в рамках этого ЦС, поэтому перед работой убедитесь, что выбран нужный ЦС.

1. Откройте раздел "Настройки".
2. В поле **Выбор Clearway CA** выберите нужный экземпляр удостоверяющего центра.
3. В карточке "Конфигурация Clearway CA" проверьте поля **Статус**, **Наименование ЦС**, **Версия** и **Url**, а в карточках "Конфигурация контрольной панели" и "Конфигурация сервиса публикации CRL" — **Статус** и **Версия**.

Поля карточек предоставляют информацию на предмет того, что выбранный экземпляр работоспособен, прежде чем выполнять над ним операции.

Ниже подробнее рассмотрены указанные выше поля:

- **Статус** — текущее состояние компонента. Штатное значение означает, что компонент запущен и доступен.
- **Наименование ЦС** — отображаемое имя удостоверяющего центра, по которому его отличают отдругих экземпляров.
- **Версия** — версия соответствующего компонента (ядра ЦС, контрольной панели, сервиса публикации CRL).
- **Url** — сетевой адрес, по которому доступен экземпляр ЦС.

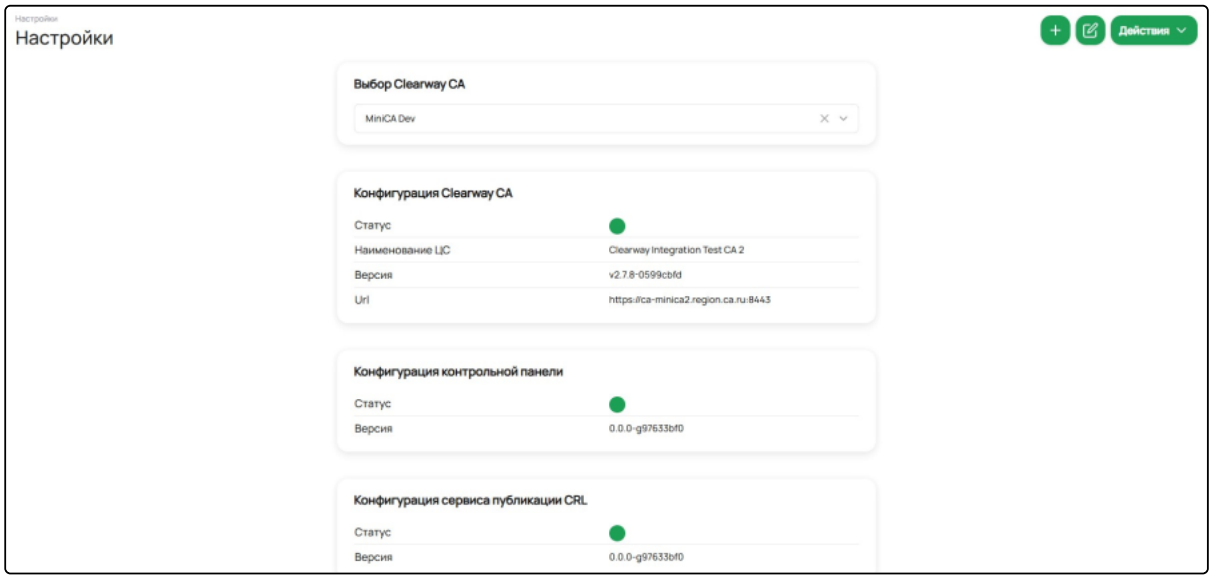


Рисунок 17 Настройки: выбор экземпляра ЦС и сводка конфигурации

Для обслуживания откройте меню **Действия** и выберите операцию: **Добавить новый ЦС**, **Обновить конфигурацию** или **Скачать цепочку сертификатов**. Последняя операция выгружает цепочку сертификатов ЦС (цепочку доверия) для установки на клиентах и серверах, чтобы выпущенные этим центром сертификаты считались доверенными.

Цепочку доверия устанавливают на каждом узле, который должен доверять сертификатам данного 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.

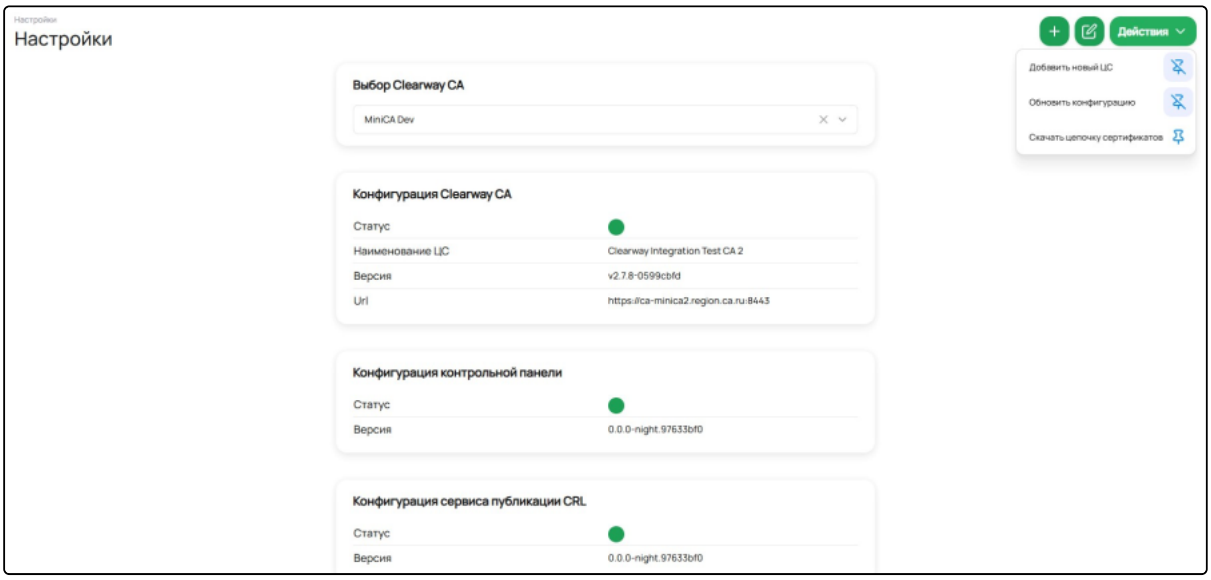


Рисунок 18 Меню "Действия" в разделе "Настройки"

10.2 Задачи публикации

Раздел "Задачи" необходим для мониторинга заданий, которые центр сертификации выполняет автоматически по расписанию.

Публикация выполняется по расписанию cron и не требует ручных действий: центр сертификации регулярно выгружает выпущенные сертификаты и списки отзыва в каталоги LDAP (Active Directory или Samba) и на внешние точки распространения — CDP (точки распространения списков отзыва, CRL Distribution Points) и AIA (точки доступа к сведениям об издателе, Authority Information Access). Благодаря этому клиенты и серверы получают актуальные сертификаты и сведения об отзыве, а точки распространения поддерживаются в согласованном состоянии без необходимости действий со стороны администратора.

В боковом меню раскройте раздел "Задачи", в нём фигурируют два подпункта: "Публикация сертификатов" и "Публикация CRL".

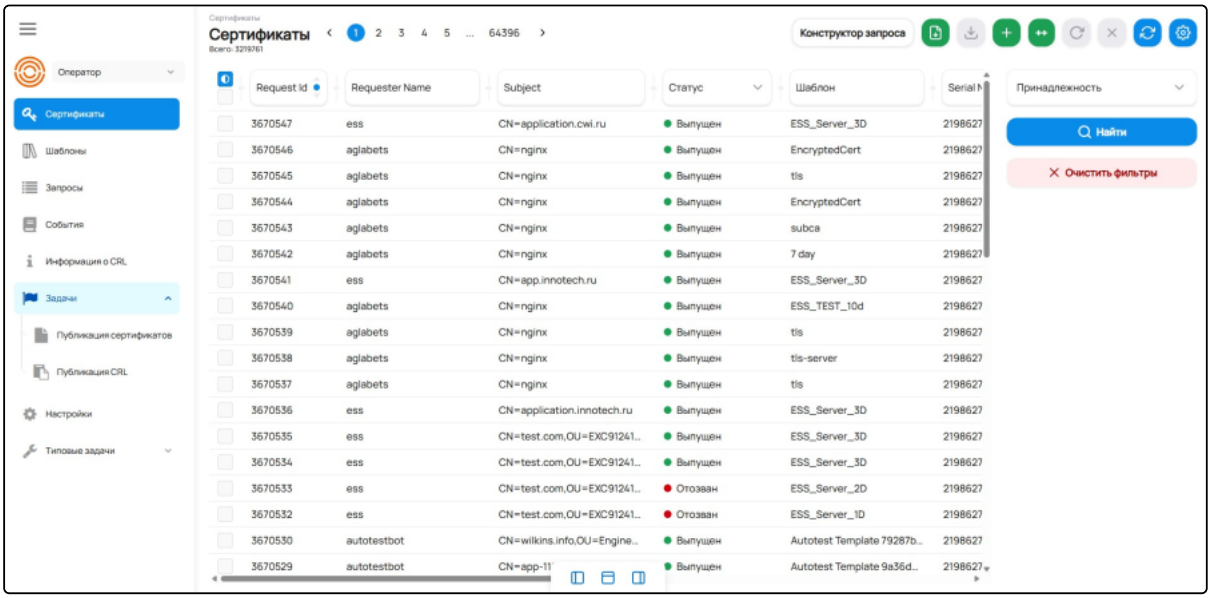


Рисунок 19 Раздел "Задачи" с подпунктами "Публикация сертификатов" и "Публикация CRL"

Откройте "Публикация сертификатов", чтобы увидеть задачи выгрузки выпущенных сертификатов в каталог LDAP. Для каждой задачи отображаются колонки "ID", "Описание", "MiniCA" (источник), "LDAP" (назначение), "Cron" и "Расписание". В примере на рисунке ниже настроена задача PublishingCertificationDev: источник — MiniCA Dev, назначение — каталог region.ca.ru, расписание — 0 12 * * * (в колонке Расписание — "В 12:00").

Колонки списка описывают, что, откуда и по какому расписанию публикуется:

- ID — идентификатор задачи публикации.
- Описание — краткое назначение задачи.
- MiniCA — экземпляр-источник, из которого берутся выпущенные сертификаты.
- LDAP — каталог-назначение, куда они выгружаются.
- Cron — расписание запуска в формате cron (в примере 0 12 * * * — ежедневно в 12:00). Расписание — то же расписание в удобочитаемом виде.

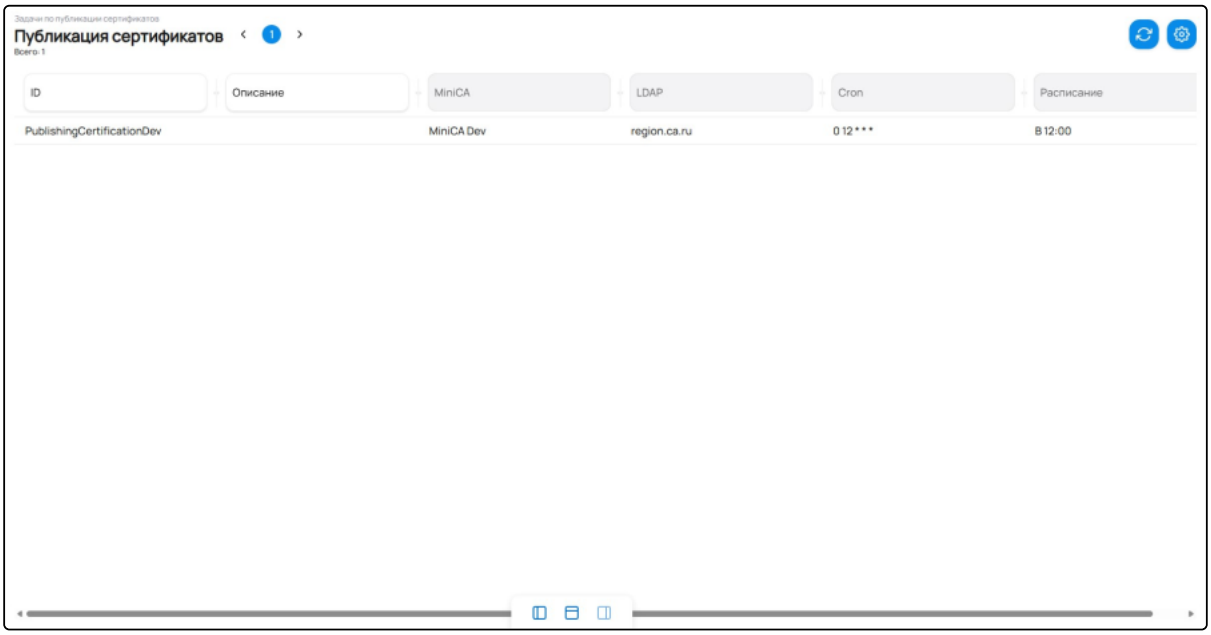


Рисунок 20 Список задач публикации сертификатов

Откройте "Публикация CRL", чтобы увидеть задачи публикации CRL и Delta CRL. Здесь добавлена колонка "Тип" со значением base или delta. В примере на рисунке ниже задача PublicCrlForDev (тип base) выполняется по cron-расписанию 0 12 * * * ("В 12:00"), а PublicDeltaCrlForDev (тип delta) — по расписанию @hourly ("Каждый час").

Полный список отзыва (CRL, тип base) содержит все действующие отметки об отзыве и публикуется реже. Разностный список (Delta CRL, тип delta) содержит только изменения, накопившиеся с момента последней публикации полного списка, поэтому его выгружают чаще (в примере — @hourly).

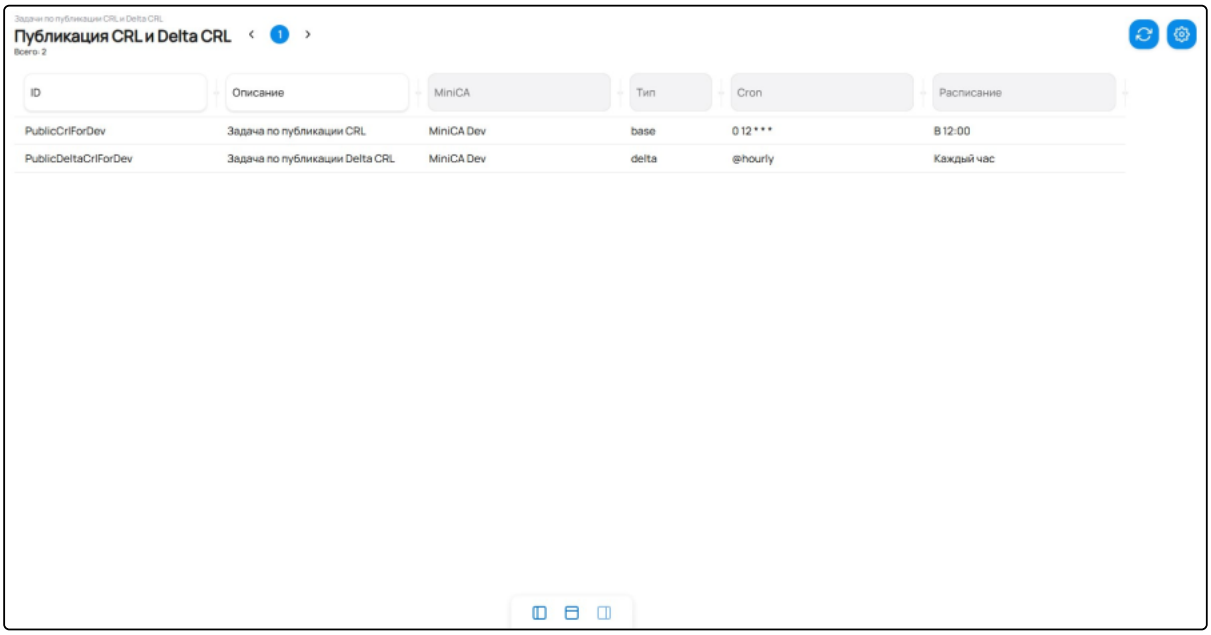


Рисунок 21 Список задач публикации CRL и Delta CRL

10.3 Типовые задачи

Раздел "Типовые задачи" используется для готовых сценариев обслуживания, выполняемых в одно действие (например, для замены tls-сертификата веб-сервера nginx). Такой сценарий подключается к целевому серверу по SSH и выполняет многошаговую операцию автоматически без ручного ввода команд на сервере. Готовые сценарии применимы в рамках регулярных операций обслуживания (например, для плановой замены tls-сертификата, поскольку повторяют одну и ту же последовательность действий одинаково и без ошибок).

В боковом меню раскройте раздел **Типовые задачи** и выберите сценарий **Замена сертификата nginx**.

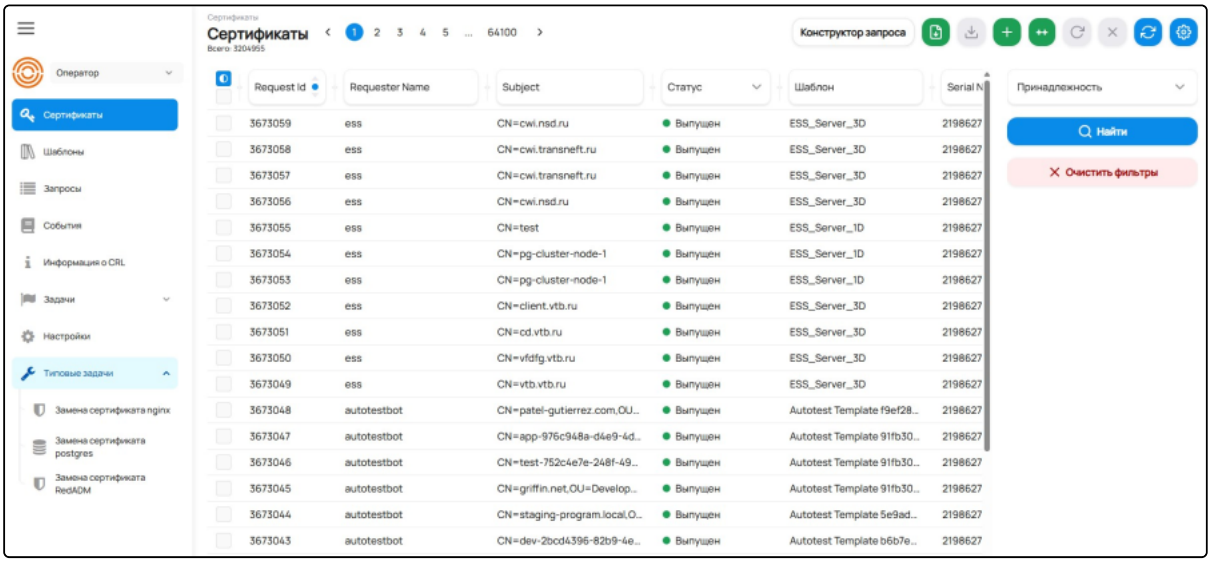


Рисунок 22 Раздел "Типовые задачи" с пунктом "Замена сертификата nginx"

На шаге "Подключение к серверу" укажите в полях **Адрес сервера**, **Имя пользователя** и **Пароль** необходимые данные.

Перечисленные выше поля являются реквизитами учётной записи SSH на целевом сервере:

- **Адрес сервера** — сетевой адрес (имя узла или IP-адрес) сервера, на котором заменяется сертификат;
- **Имя пользователя** — учётная запись, под которой выполняется подключение по SSH;
- **Пароль** — пароль этой учётной записи.

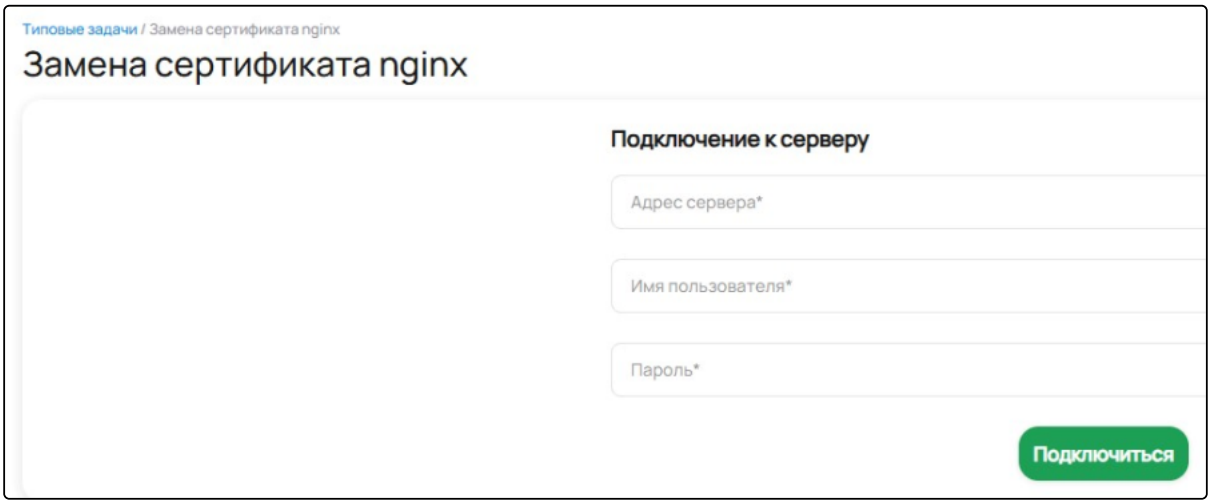


Рисунок 23 Сценарий "Замена сертификата nginx", шаг "Подключение к серверу"

Нажмите **Подключиться**, после чего центр сертификации подключится к серверу по SSH и на следующих шагах автоматически выпустит и установит новый TLS-сертификат в конфигурации nginx.

> **Важно**
>
> Указанная учётная запись должна иметь права на изменение конфигурации nginx на целевом сервере? иначе установка сертификата не завершится. После выполнения сценария рекомендуется убедиться, что веб-сервер отдаёт новый сертификат (например, проверив его срок действия и издателя при обращении к серверу по HTTPS).

Аналогичные сценарии предусмотрены и для других сервисов — Замена сертификата RedAdm и Замена сертификата postgres. Они доступны в том же разделе "Типовые задачи", а принцип их работы полностью аналогичен описанному выше сценарию для nginx: сценарий подключается к целевому серверу по SSH, автоматически выпускает и устанавливает новый TLS-сертификат в конфигурации соответствующего сервиса. Требования к правам учётной записи и рекомендации по проверке результата также совпадают.

11 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: шифрование закрытого ключа при подготовке запроса, шифрование данных сертификата в базе данных и хранение/восстановление закрытых ключей средствами Агента восстановления ключей (KRA).

11.1 Шифрование закрытого ключа при подготовке запроса

Когда закрытый ключ создаётся на сервере пользователя (через Конструктор запросов), его можно сразу защитить паролем.

1. В **Конструкторе запросов** в блоке "Ключ" проставьте чекбокс "Зашифровать закрытый ключ".
2. Сформируйте и выполните команду стандартным образом. При активном чекбоксе из команды openssl убирается параметр -nodes и openssl запрашивает пароль при создании ключа. При этом закрытый ключ будет сохранён в зашифрованном виде.

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.

11.2 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 шаблоне сертификата (раздел "Шаблоны") включите опцию "Шифровать данные в БД".

Сертификаты, выпущенные по этому шаблону, будут шифроваться перед сохранением и храниться в базе в зашифрованном виде. При скачивании данные расшифровываются автоматически, дополнительных действий от пользователя не требуется.

Шифрование данных в базе может незначительно снижать производительность. Признак задаётся в шаблоне и применяется ко всем сертификатам, выпускаемым по этому шаблону.

11.3 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 даёт возможность:

- восстановить закрытый ключ сертификата (например, при его утрате владельцем) средствами KRA;
- выгрузить сертификат вместе с закрытым ключом в формате PFX (PKCS#12) — единым защищённым файлом, удобным для переноса на конечную систему.

Хранение закрытых ключей в базе и функции Агента восстановления ключей (KRA) настраиваются администратором при развёртывании (подробнее см. в документе **Руководство администратора**). Доступность выгрузки закрытого ключа зависит от конфигурации центра сертификации и назначенных прав пользователю.

12 Работа через командную строку (mclient)

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

12.1 Подготовка

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

1. ```
   export MCLIENT_CONF=/opt/itc/minica/conf/mclient.yml
   ```

2. ```
   # связь со службой ЦС, версия ЦС и SKI

   ./mclient ping
   ```

3. ```
   # статистика ЦС

   ./mclient stat
   ```

12.2 Основные команды

Операция	Команда
Выпуск сертификата по шаблону	./mclient ca -csr request.csr -template tls -out cert.crt
Проверка статуса сертификата	./mclient status
Получение сертификата из БД	./mclient get
Массовая выгрузка сертификатов	./mclient export
Отзыв сертификата	./mclient revoke
Возврат в действие (для причины Certificate Hold)	./mclient repair
   ```

Операция	Команда
Обновление списка отзыва CRL	./mclient updcrl
Обновление разностного списка Delta CRL	./mclient updeltacrl
Список шаблонов	./mclient templates
Параметры шаблона	./mclient gettempl
Создание шаблона	./mclient addtempl
Удаление шаблона	./mclient deltempl

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

1. ```
   export MCLIENT_CONF=/opt/itc/minica/conf/mclient.yml
   ```

2. ```
   ./mclient ca -csr request.csr -template tls -out cert.crt
   ```

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