

Центр Управления Гетерогенными Инфраструктурами

Система централизованного анализа и
управления гетерогенными
инфраструктурами — MiniCA

Руководство пользователя

RU.CLRW.00947-01 34 01

ООО «Клируэй технолоджис»

Релиз Q2 2025

Содержание

1. Термины и сокращения	3
2. Введение.....	5
2.1. Идентификационные данные.....	5
2.2. Общее описание	5
3. Общие действия	6
3.1. Поиск на странице	6
3.2. Фильтрация	6
3.3. Отображение элементов страницы.....	10
3.4. Настройка отображения таблицы страницы	11
3.5. Выгрузка отчета.....	14
4. Сертификаты	15
4.1. Запрос сертификата	15
4.2. Просмотр карточки сертификата	17
4.3. Восстановление и отзыв сертификата	20
4.3.1. Восстановление сертификата:	20
4.3.2. Отзыв сертификата:.....	22
5. Шаблоны.....	26
5.1. Создание шаблона	26
5.2. Редактирование шаблона.....	28
5.3. Удаление шаблона.....	30
6. Запросы.....	31
6.1. Просмотр списка запросов	31
7. События.....	33
7.1. Просмотр событий	33
8. Текущий CRL.....	35
9. Выпуск сертификата на MiniCA вручную	36
9.1. Таблица основных команд.	36
Приложение А Значения параметров.....	38
А.1 Значение keyUsage	38
А.2 Значения Extended Key Usage	38
А.3 Значения Authority Key Identifier	38
Приложение Б Причины отзыва сертификата	40

1. Термины и сокращения

Принятые сокращения

Сокращение	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.
САУИ УЦ, Система	Система Автоматизированного Управления Инфраструктурой Удостоверяющего Центра.
ИС	Информационная система.
ОС	Операционная система.
УЦ	Удостоверяющий Центр — программный или программно-аппаратный комплекс, обеспечивающий управление жизненным циклом сертификатов x509.
ЦС (CA)	Центр Сертификации (Certification Authority) — сервер, предназначенный для выпуска и отзыва сертификатов, а также публикации CRL (COC). Часть Удостоверяющего Центра.
ЦУГИ	Центр Управления Гетерогенными Инфраструктурами — набор (система) программ для управления и мониторинга различных компонентов ИТ инфраструктуры, разработанный и лицензируемый предприятием ООО "Клируэй Текнолоджис".

Термины и определения

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 является составной частью эксплуатационной документации на Систему Автоматизированного Управления Инфраструктурой Удостоверяющего Центра (САУИ УЦ), которая создана как составная часть Центра управления гетерогенными инфраструктурами (ЦУГИ) в ООО «Клируэй Текнолоджис».

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

2.1. Идентификационные данные

Идентификационные данные приведены в таблице 1

Таблица 1 — Идентификационные данные

Идентификационные данные ОО	
Название документа	Руководство пользователя
Децимальный номер документа	RU.CLRW.00947-01 34 01
Версия документа	1.0
Автор документа, предприятие-изготовитель	ООО «Клируэй Текнолоджис»

2.2. Общее описание

САУИ УЦ реализует автономный сервер центра сертификации на базе **OpenSSL**. Микросервис, который реализует программный интерфейс с использованием протокола **HTTP** (или **HTTPS**). Основные функции сервиса:

- выпуск сертификатов **X.509v3** на основе **CSR** запросов в формате **PKCS#10**;
- отзыв сертификатов в соответствии с заданной причиной;
- формирование списка отозванных сертификатов **CRL (RFC 5280)**;
- формирование разностных списков отозванных сертификатов **DeltaCRL**;
- предоставление информации о статусе сертификата;
- предоставление сертификатов по их серийному номеру или **SHA1** отпечатку;
- сохранение информации о всех запросах, сертификатах, **CRL/DeltaCRL** и журнала событий в базе данных.

3. Общие действия

3.1. Поиск на странице

- 1) На странице раздела выбрать колонку с полем поиска.

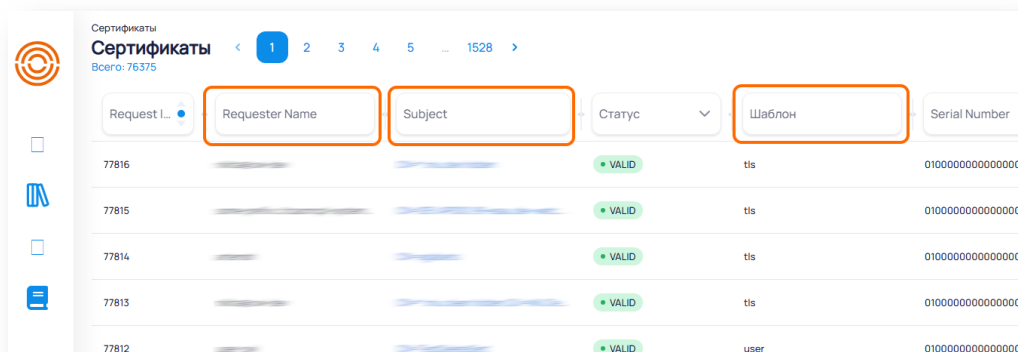


Рисунок 1 — Поля поиска в колонках на странице «Сертификаты»

- 2) Ввести символы для поиска значения на странице и нажать кнопку **Enter** либо сделать щелчок левой кнопкой мыши вне зоны поля ввода.

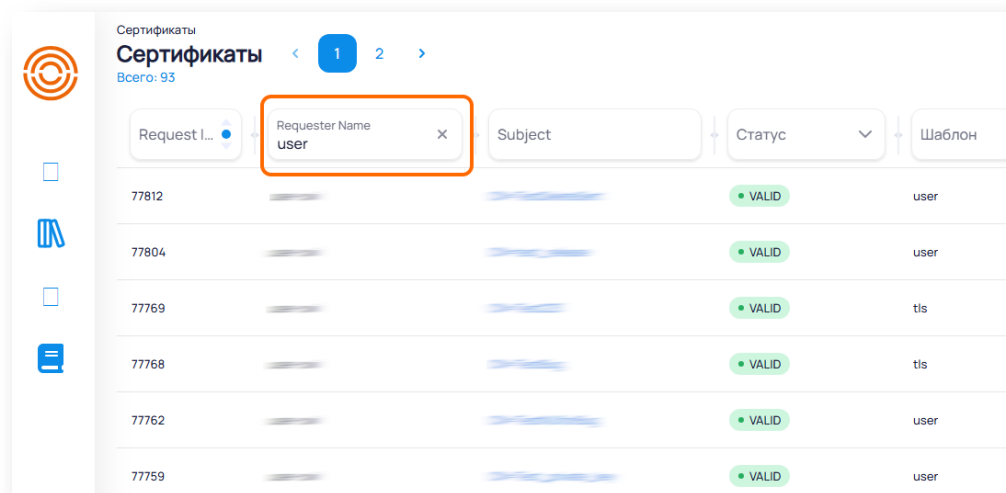


Рисунок 2 — Поиск в колонке

- 3) Отобразятся результаты согласно введенным символам.

3.2. Фильтрация

- 1) На странице раздела выбрать колонку с полем выпадающего списка.

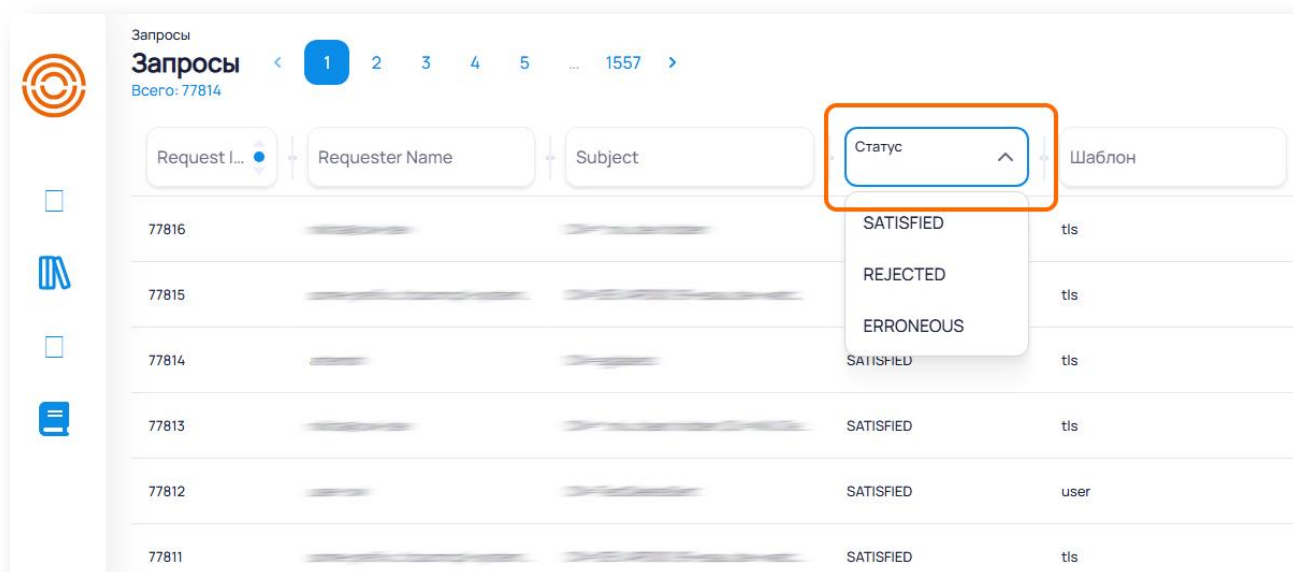


Рисунок 3 — Поле выпадающего списка в колонке

- 2) Выбрать значение выпадающего списка.

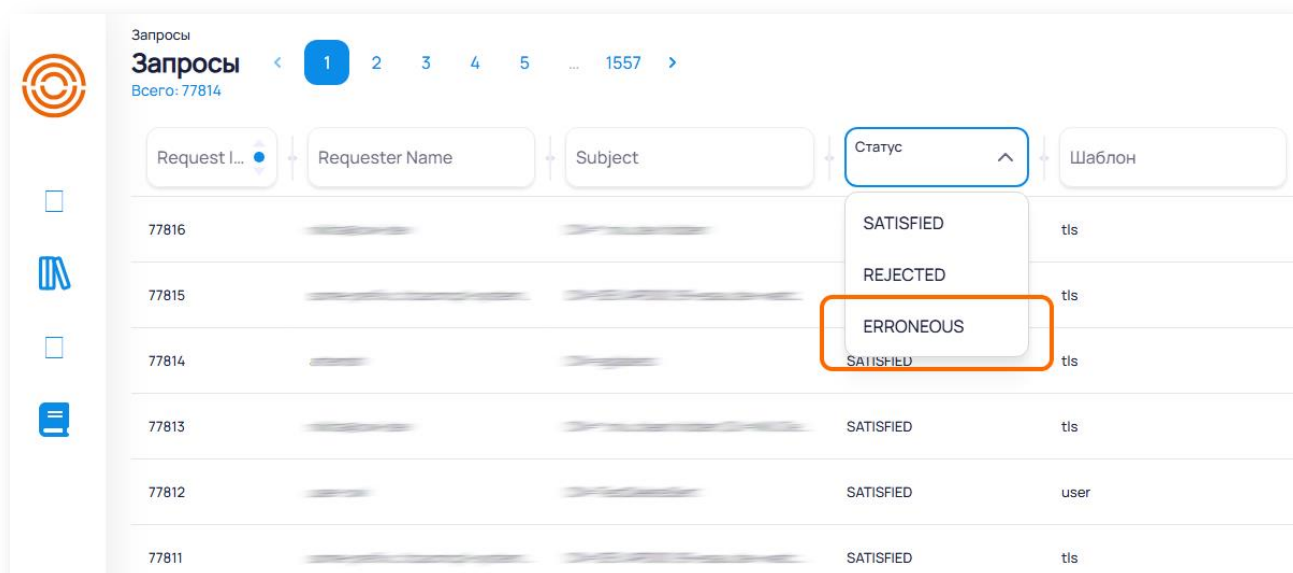
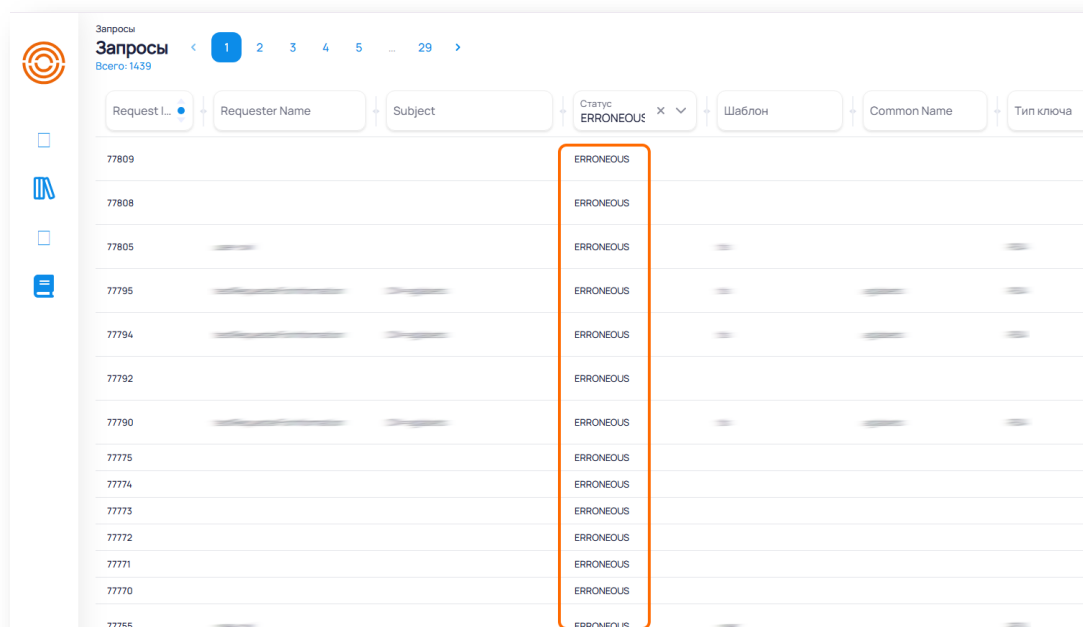


Рисунок 4 — Выбор значения выпадающего списка

- 3) Отобразятся результаты согласно выбранному значению из списка.

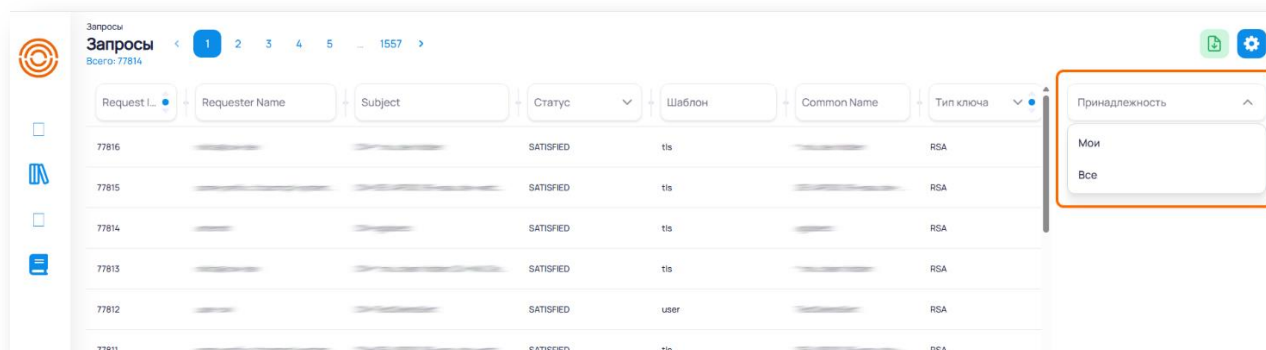


Request ID	Requester Name	Subject	Статус	Шаблон	Common Name	Тип ключа
77809			ERRONEOUS			
77808			ERRONEOUS			
77805			ERRONEOUS			
77795			ERRONEOUS			
77794			ERRONEOUS			
77792			ERRONEOUS			
77790			ERRONEOUS			
77775			ERRONEOUS			
77774			ERRONEOUS			
77773			ERRONEOUS			
77772			ERRONEOUS			
77771			ERRONEOUS			
77770			ERRONEOUS			
77755			ERRONEOUS			

Рисунок 5 — Отфильтрованные результаты

Также можно отфильтровать по принадлежности:

- 1) Включить отображение боковых фильтров, если не включено (см. 3.3).
- 2) Выбрать значение из выпадающего списка «Принадлежность»:
 - Мои — отображаются только результаты пользователя;
 - Все — отображаются все результаты.



Request ID	Requester Name	Subject	Статус	Шаблон	Common Name	Тип ключа	Принадлежность
77816			SATISFIED	tls		RSA	Мои
77815			SATISFIED	tls		RSA	Мои
77814			SATISFIED	tls		RSA	Мои
77813			SATISFIED	tls		RSA	Мои
77812			SATISFIED	user		RSA	Мои
77811			SATISFIED	tls		RSA	Мои

Рисунок 6 — Фильтрация по принадлежности

Реализована возможность фильтрации по возрастанию/убыванию:

- 1) Выбрать колонку со стрелками в поле названия.

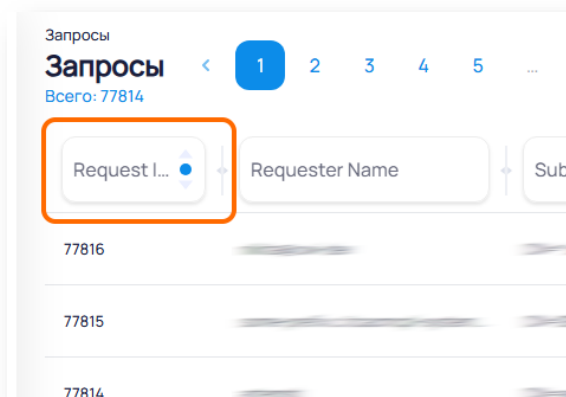


Рисунок 7 — Стрелки фильтрации

- 2) Нажать кнопку **Стрелка вниз** для фильтрации записей по убыванию.

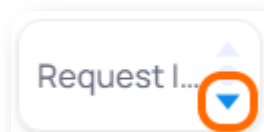


Рисунок 8 — Кнопка Стрелка вниз

- 3) Нажать кнопку **Стрелка вверх** для фильтрации записей по возрастанию.

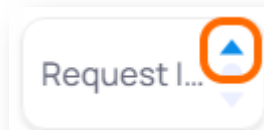


Рисунок 9 — Кнопка Стрелка вверх

- 4) Нажать круглую кнопку между стрелками для возврата к первоначальному значению.

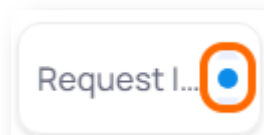


Рисунок 10 — Кнопка возврата к первоначальному значению

Для сброса фильтрации следует нажать кнопку **Очистить фильтры**.

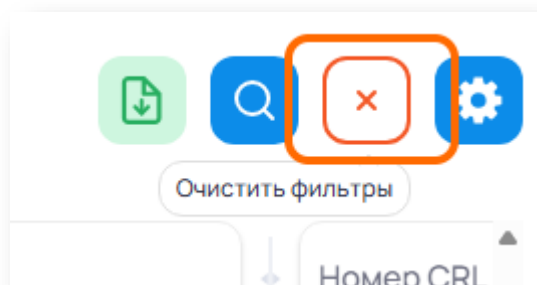


Рисунок 11 — Кнопка **Очистить фильтры**

3.3. Отображение элементов страницы



Рисунок 12 — Нижнее меню

На страницах раздела отображается нижнее меню с тремя кнопками:

- **Скрыть\показать меню** — для отображения или сокрытия бокового меню;

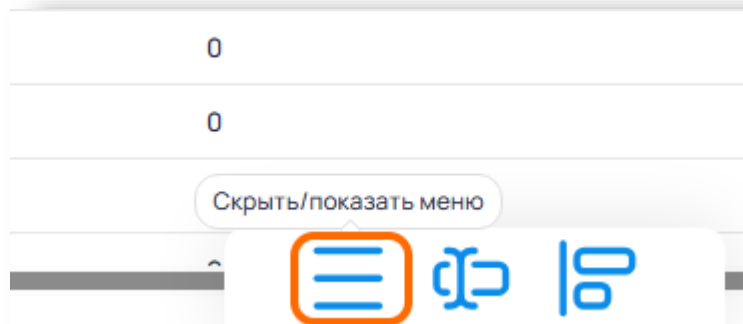


Рисунок 13 — Кнопка **Скрыть\показать меню**

- **Скрыть\показать шапку** — для отображения или сокрытия шапки страницы;

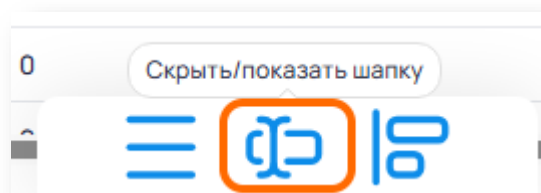


Рисунок 14 — Кнопка **Скрыть\показать шапку**

- **Скрыть\показать боковые фильтры** — для отображения или сокрытия боковых фильтров.

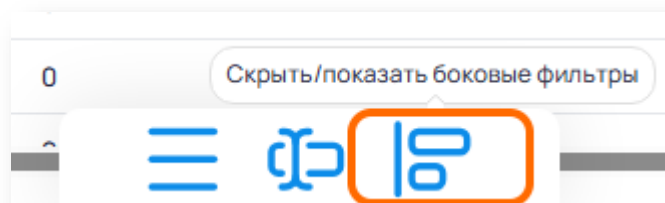


Рисунок 15 — Кнопка **Скрыть\показать боковые фильтры**

3.4. Настройка отображения таблицы страницы

- 1) Нажать на странице кнопку **Параметры таблицы**.

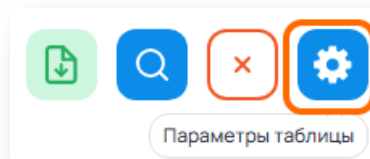


Рисунок 16 — Кнопка **Параметры таблицы**

- 2) В открывшемся окне отметить флажками необходимые колонки.

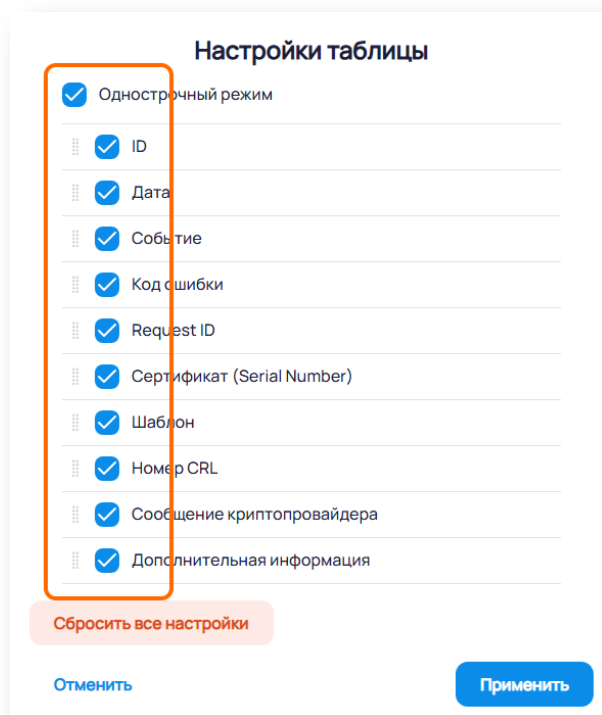


Рисунок 17 — Выбор колонок для отображения

- 3) При необходимости, упорядочить порядок отображения колонок перетаскиванием.

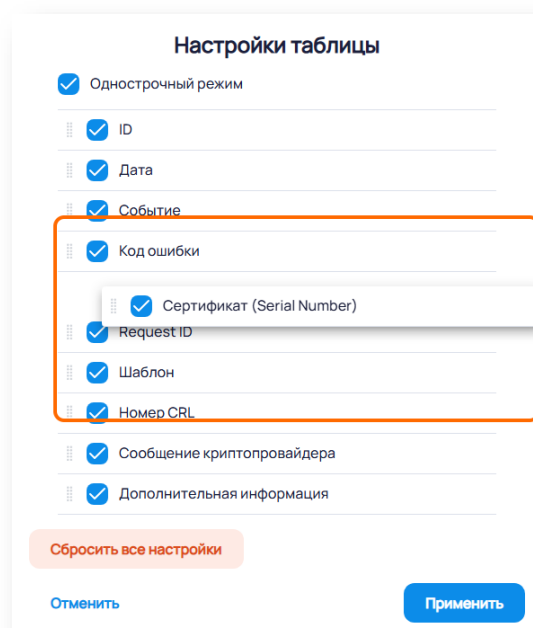


Рисунок 18 — Упорядочить колонки

- 4) Кнопка **Сбросить все настройки** сбрасывает настройки отображения таблицы к значению по умолчанию.

Настройки таблицы

☒ Однострочный режим

☒ ID

☒ Дата

☒ Событие

☒ Код ошибки

☒ Request ID

☒ Сертификат (Serial Number)

☒ Шаблон

☒ Номер CRL

☒ Сообщение криптопровайдера

☒ Дополнительная информация

Сбросить все настройки

Отменить Применить

Рисунок 19 — Кнопка **Сбросить все настройки**

- 5) Нажать кнопку **Применить** для сохранения изменений.

Настройки таблицы

☒ Однострочный режим

⋮

☒ ID

⋮

☒ Дата

⋮

☒ Событие

⋮

☒ Код ошибки

⋮

☒ Request ID

⋮

☒ Сертификат (Serial Number)

⋮

☒ Шаблон

⋮

☒ Номер CRL

⋮

☒ Сообщение криптопровайдера

⋮

☒ Дополнительная информация

Сбросить все настройки

Применить

Отменить

Рисунок 20 — Кнопка **Применить**

3.5. Выгрузка отчета

- 1) При необходимости, применить фильтры на странице — см. 3.2.
- 2) Нажать на странице кнопку выгрузки отчета.

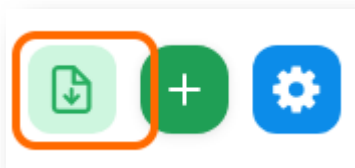


Рисунок 21 — Кнопка выгрузки процесса

- 3) Сформируется файл отчета согласно примененным фильтрам. Количество записей в отчете не превышает 10000. Файл отчета будет сохранен в локальное хранилище пользователя.

4. Сертификаты

4.1. Запрос сертификата

- 1) Выбрать раздел **Сертификаты**.

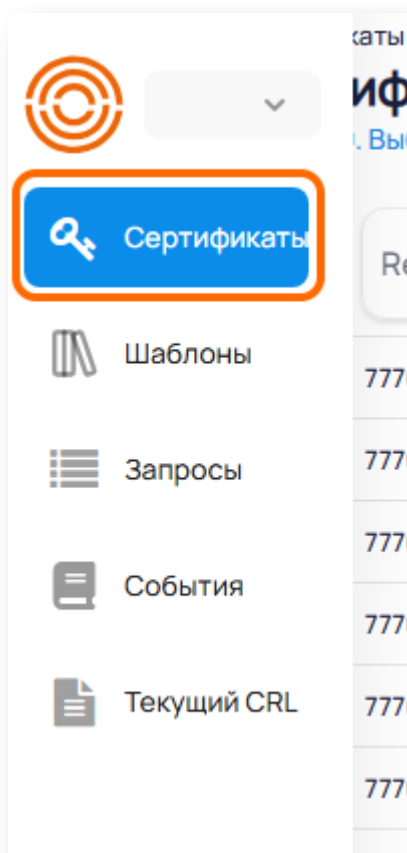


Рисунок 22 — Раздел **Сертификаты**

- 2) Нажать кнопку **Запрос сертификата** в виде знака +

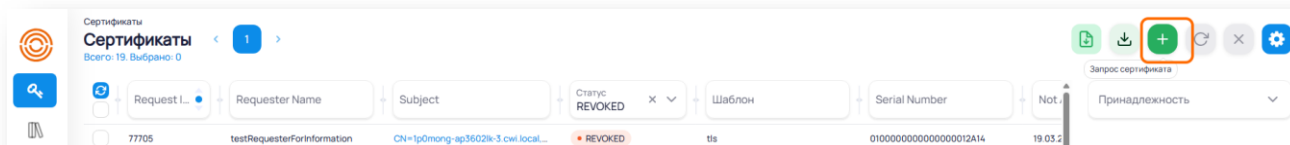


Рисунок 23 — Кнопка «Запрос сертификата»

- 3) Откроется окно запроса сертификата.
- 4) Выбрать шаблон сертификата — см. п. 4.2.

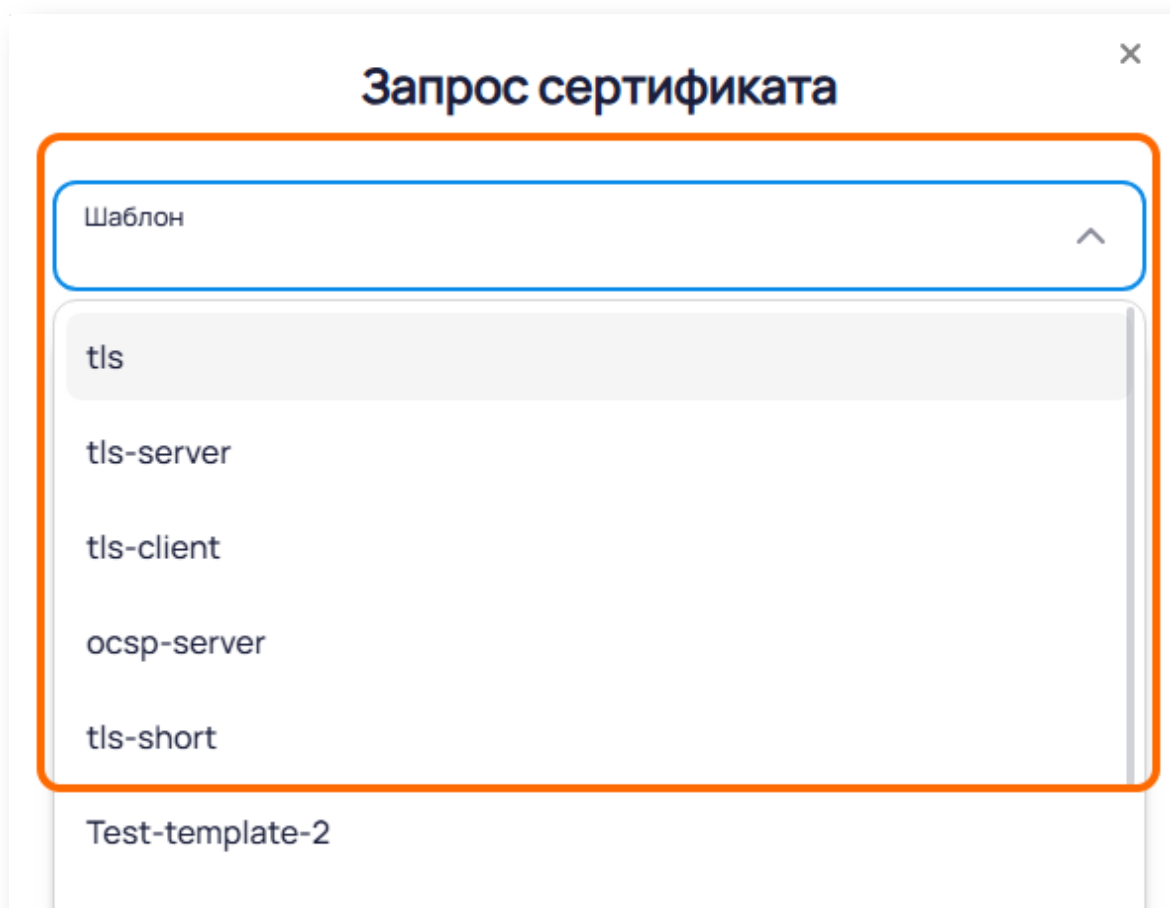


Рисунок 24 — Выбор шаблона сертификата

- 5) Вставить сформированный запрос на сертификат.

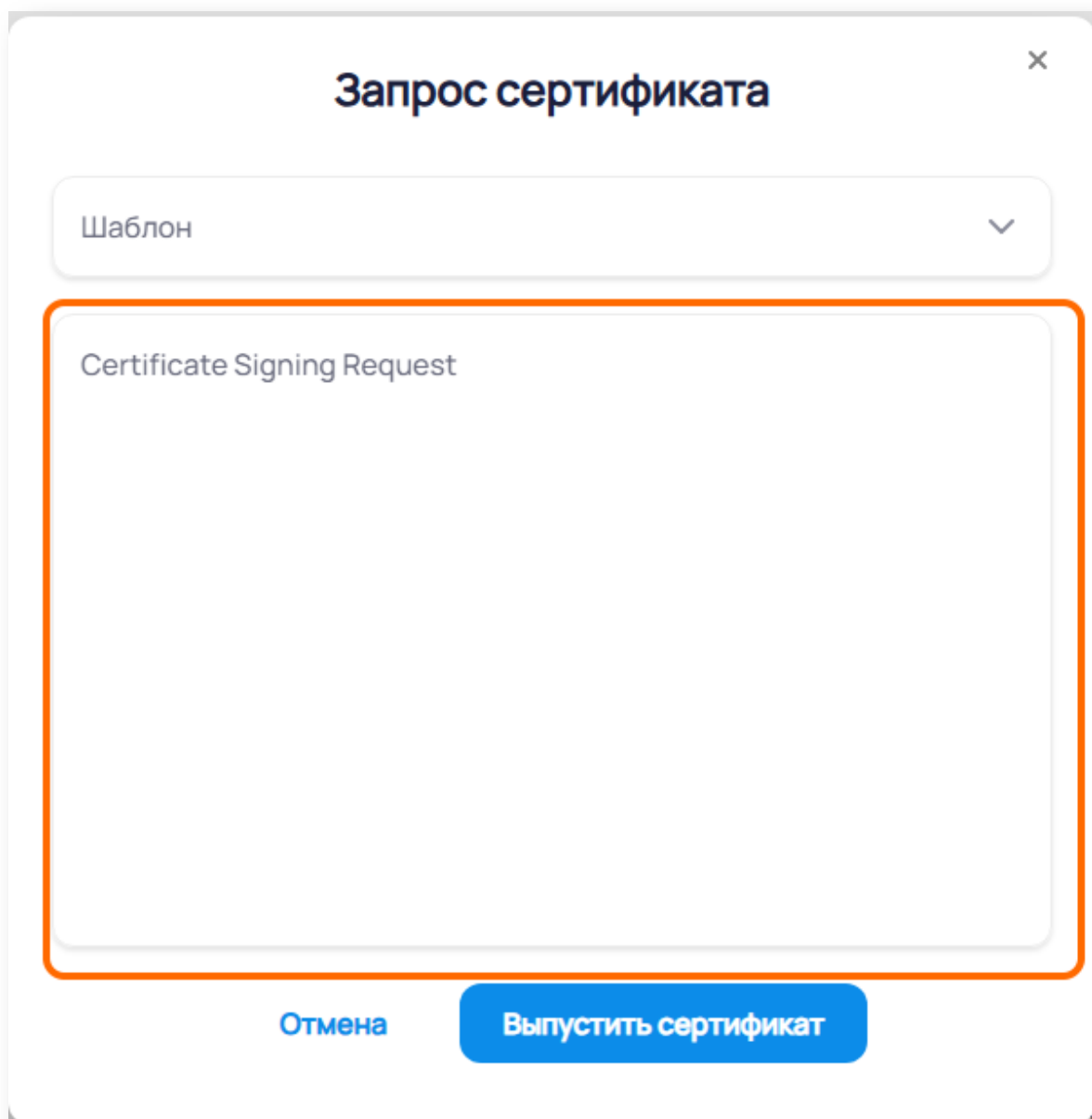


Рисунок 25 — Окно ввода запроса сертификата

Внимание! Формирование цепочки сертификатов требует правильного составления запроса и выбора соответствующего шаблона.

- 6) Нажать кнопку **Сохранить**.

4.2. Просмотр карточки сертификата

- 1) Выбрать раздел **Сертификаты**.

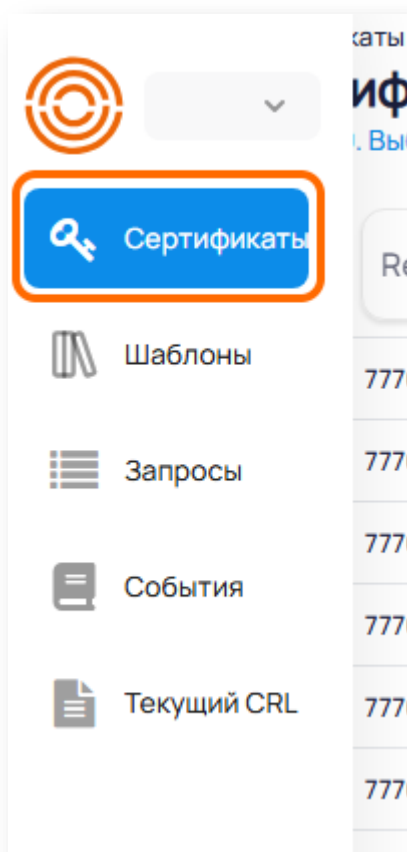


Рисунок 26 — Раздел Сертификаты

- 2) Нажать на информацию о владельце сертификата в колонке **Subject** в строке с сертификатом, карточку которого необходимо просмотреть.

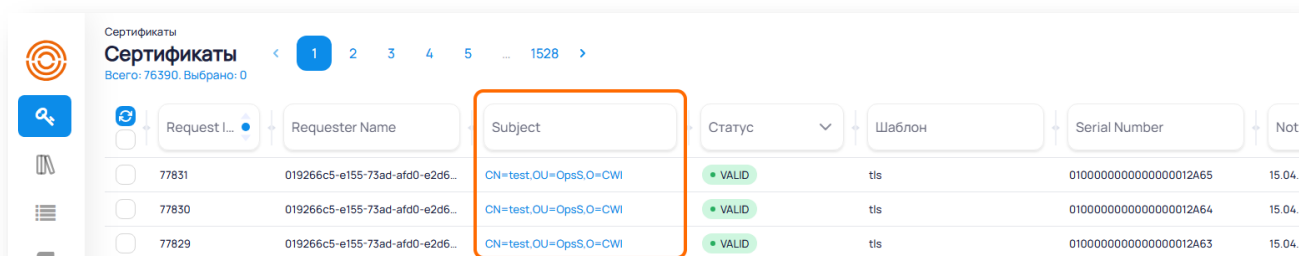


Рисунок 27 — Колонка Subject

- 3) Откроется карточка сертификата.

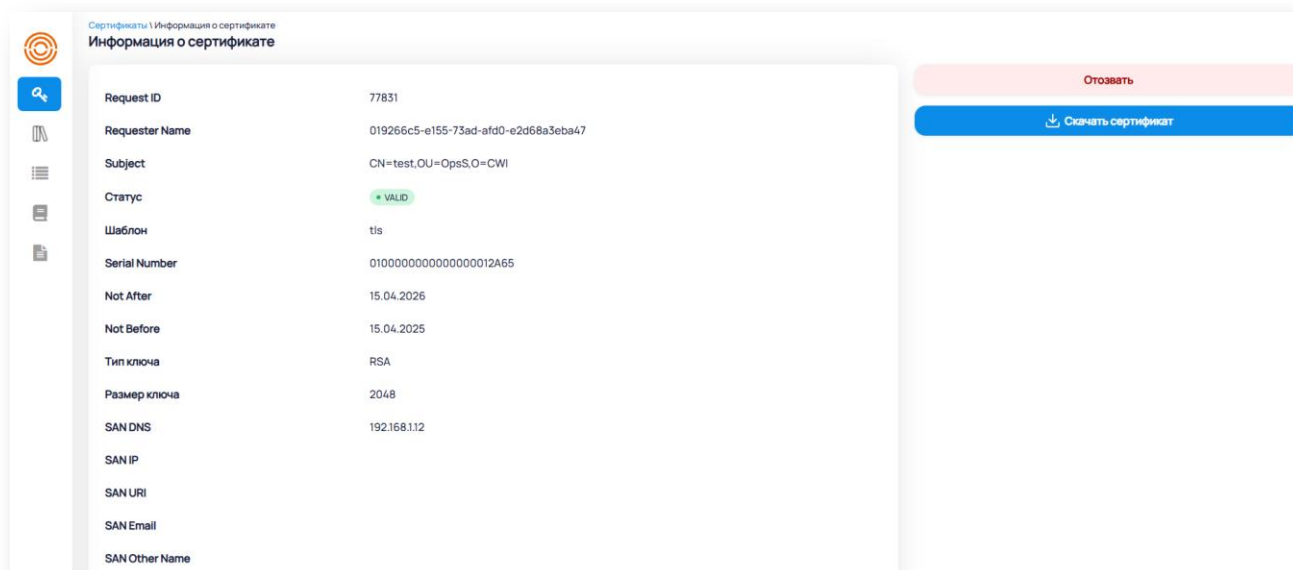


Рисунок 28 — Карточка сертификата

4) В карточке возможно:

- Скачать сертификат при помощи кнопки **Скачать сертификат**;
- Отозвать сертификат — актуально для сертификатов со статусом VALID. См. п.4.3.2

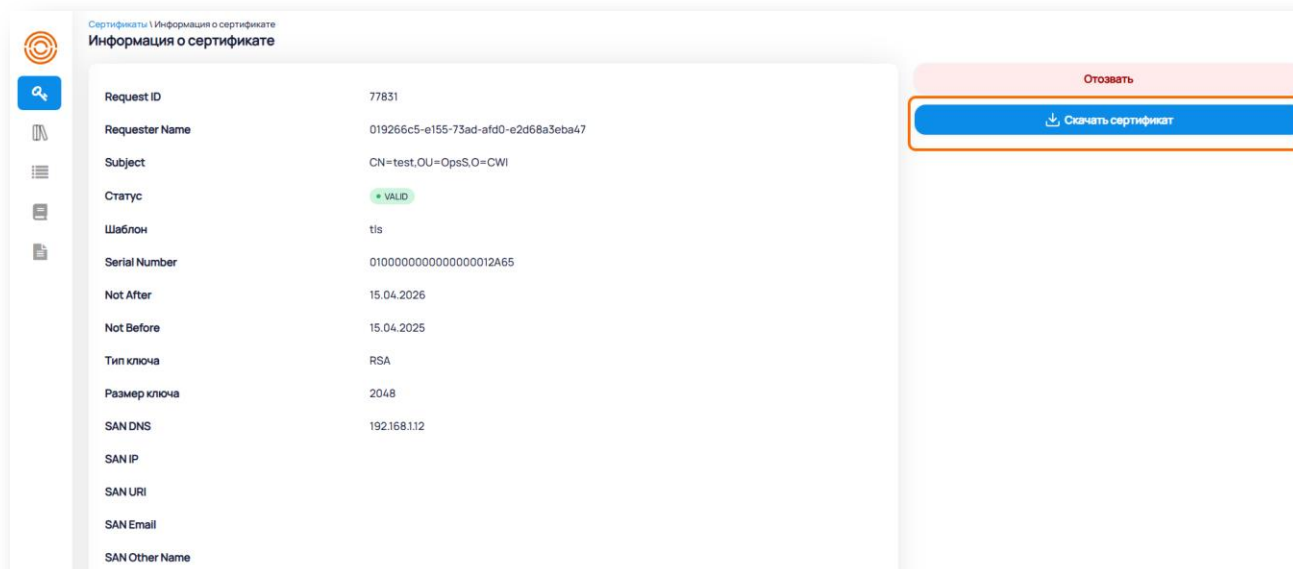


Рисунок 29 — Кнопка **Скачать сертификат**

4.3. Восстановление и отзыв сертификата

4.3.1. Восстановление сертификата:

- 1) Выбрать раздел **Сертификаты**.

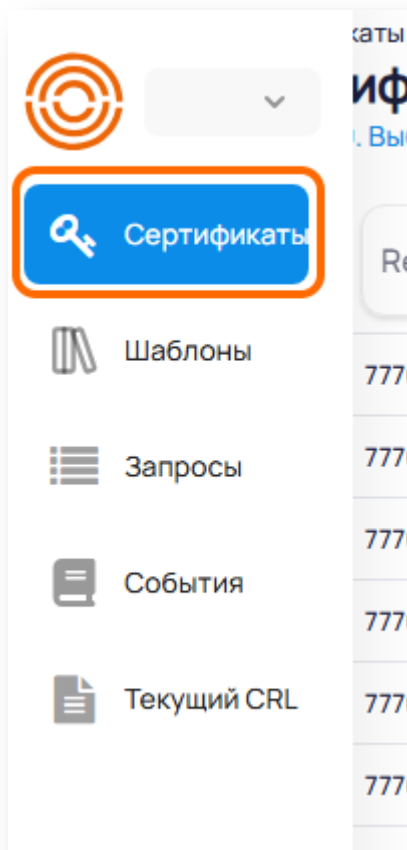


Рисунок 30 — Раздел Сертификаты

- 2) Отметить отозванный сертификат (статус REVOKED). Можно отметить несколько сертификатов.

Request ID	Requester Name	Subject	Статус	Шаблон	Serial Number	Not. (Expiry Date)
35			VALID	tts	010000000000000000000020	04.12.2
36			VALID	tts	010000000000000000000021	04.12.2
37			VALID	tts	010000000000000000000022	04.12.2
38			VALID	tts	010000000000000000000023	04.12.2
39			VALID	tts-server	010000000000000000000024	04.12.2
40			VALID	tts-server	010000000000000000000025	04.12.2
41			VALID	tts-server	010000000000000000000026	05.12.2
42			VALID	tts	010000000000000000000027	05.12.2
43			VALID	tts-server	010000000000000000000028	05.12.2
44			VALID	tts-server	010000000000000000000029	05.12.2
45			VALID	tts-server	01000000000000000000002A	05.12.2
46	QAadmin	CN=QAadminTest3A1	REVOKED	tts-server	01000000000000000000002B	05.12.2
47			VALID	tts-server	01000000000000000000002C	05.12.2
48			VALID	tts-server	01000000000000000000002D	05.12.2
49			VALID	tts-server	01000000000000000000002E	06.12.2

Рисунок 31 — Отмеченный сертификат

- 3) Нажать кнопку **Восстановить выбранные сертификаты**.

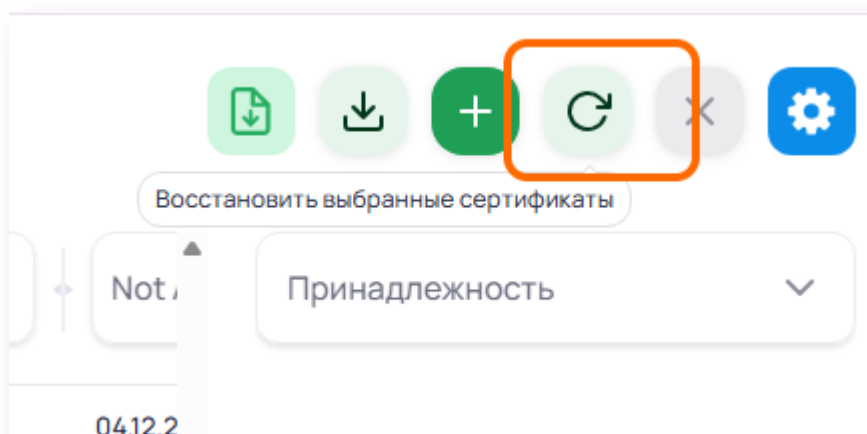


Рисунок 32 — Кнопка **Восстановить выбранные сертификаты**

- 4) В открывшемся окне **Восстановление сертификатов** ознакомится с данными сертификата и нажать кнопку **Восстановить**.

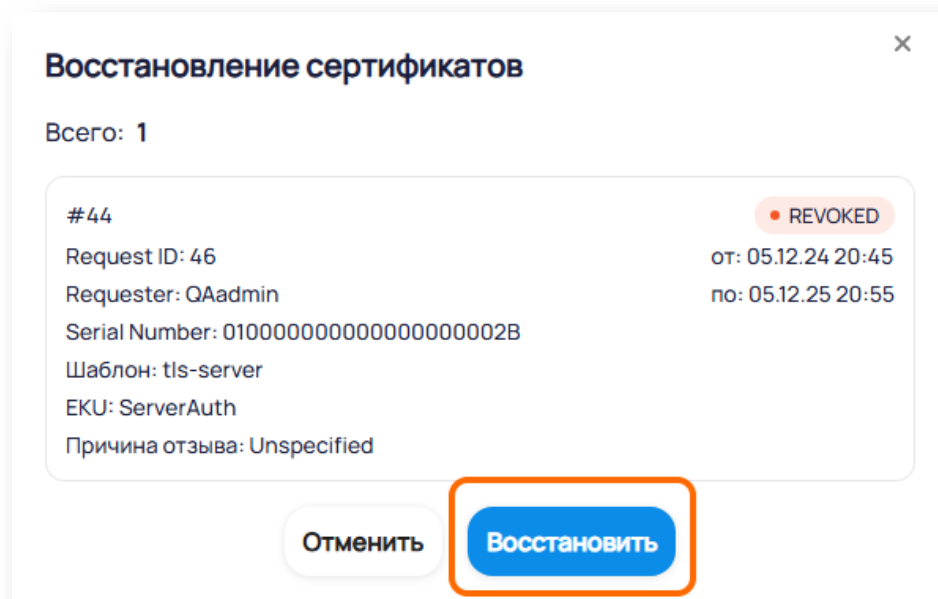


Рисунок 33 — Кнопка **Восстановить**

4.3.2. Отзыв сертификата:

- 1) Выбрать раздел **Сертификаты**.

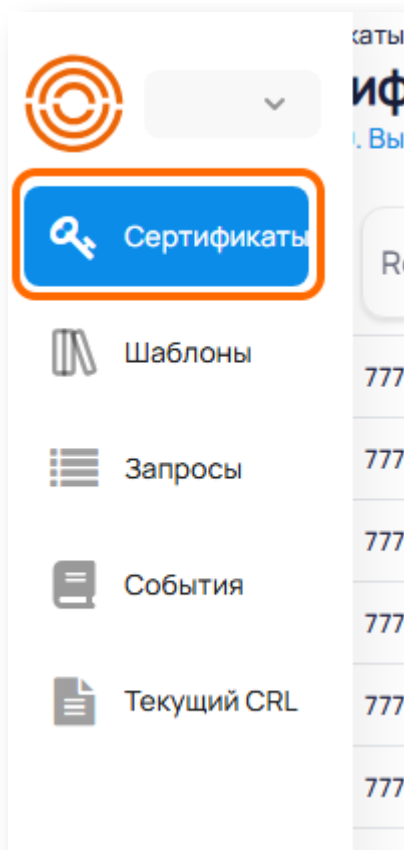


Рисунок 34 — Раздел Сертификаты

- 2) Отметить действующий сертификат (статус VALID). Можно отметить несколько сертификатов.

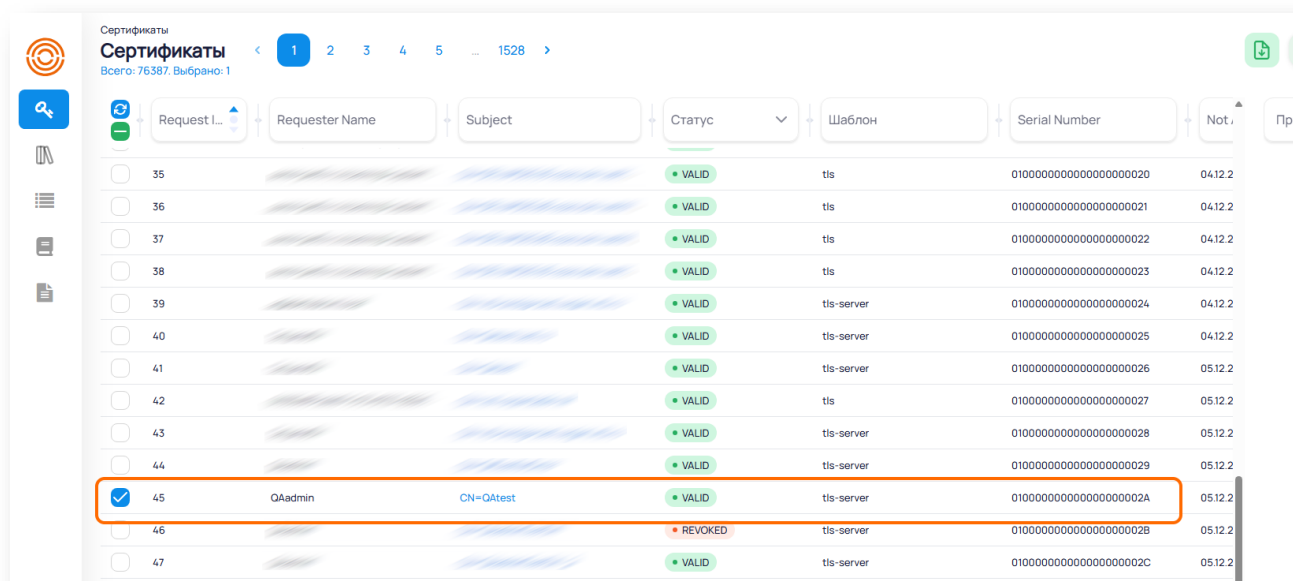


Рисунок 35 — Отмеченный сертификат

- 3) Нажать кнопку **Отозвать выбранные сертификаты**.

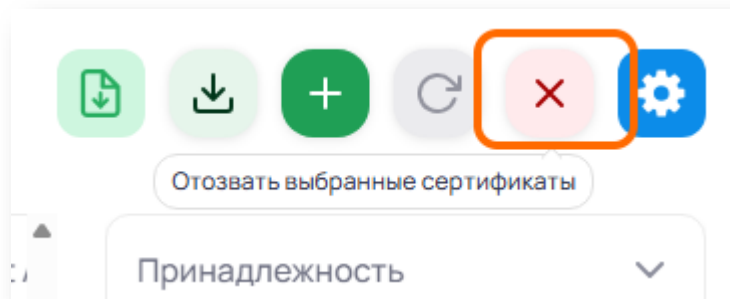


Рисунок 36 — Кнопка **Отозвать выбранные сертификаты**

- 4) Либо нажать кнопку **Отозвать** при просмотре карточки сертификата.
5) Откроется окно **Отзыв сертификата**.

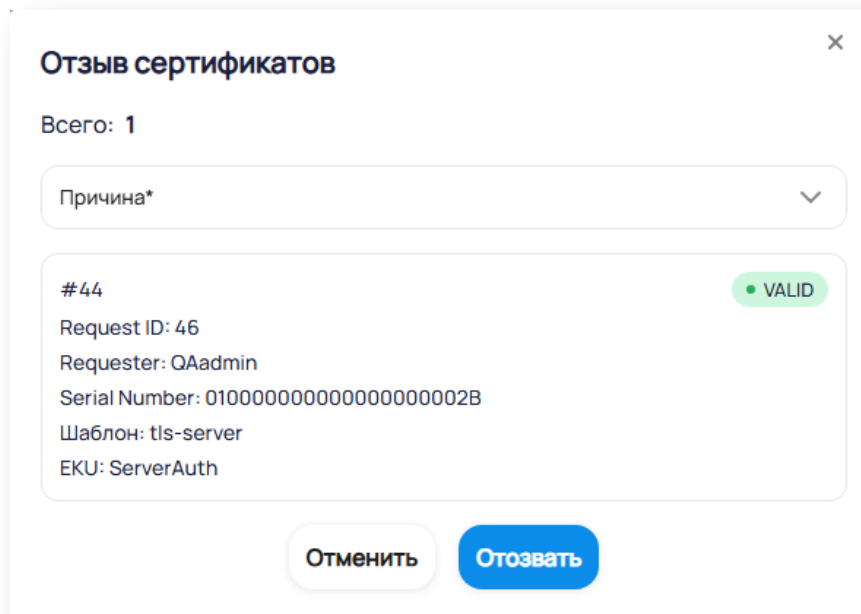


Рисунок 37 — Окно **Отзыв сертификата**

- 6) Выбрать из списка причину отзыва — см. Приложение Б. Обязательно к выбору.

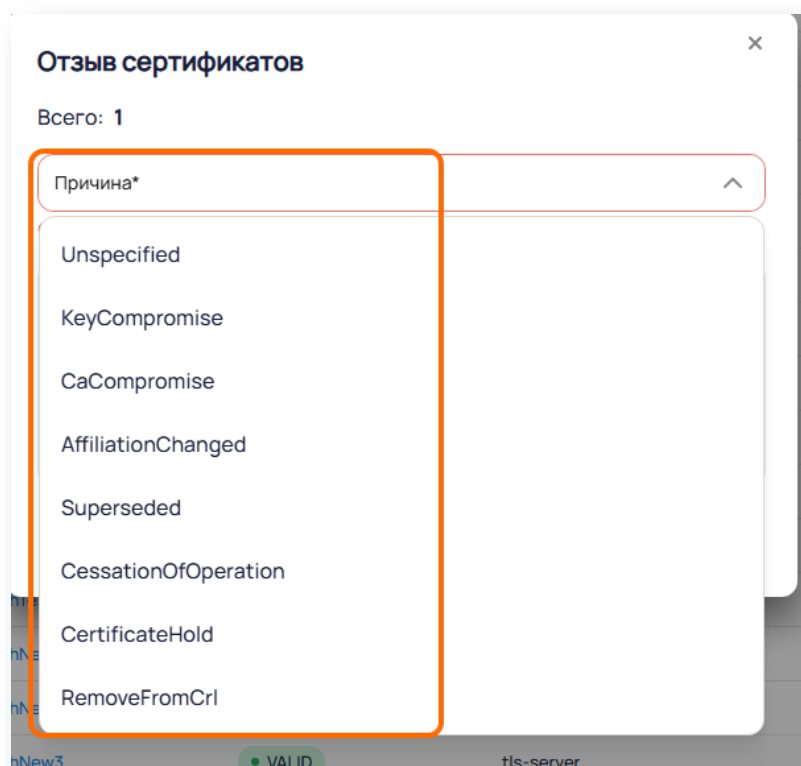


Рисунок 38 — Выбор причины отзыва сертификатов

7) Нажать кнопку **Отозвать**.

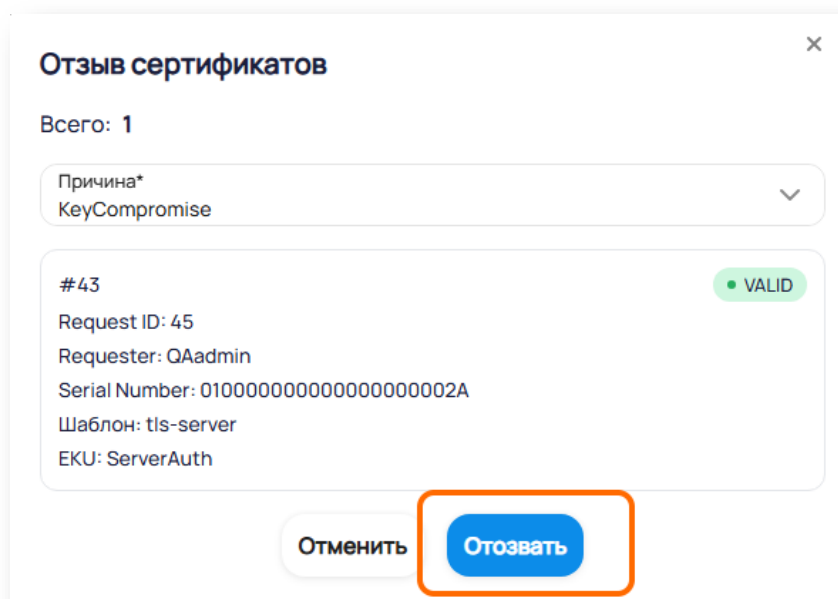


Рисунок 39 — Кнопка **Отозвать**

5. Шаблоны

5.1. Создание шаблона

- 1) Выбрать раздел **Шаблоны**.

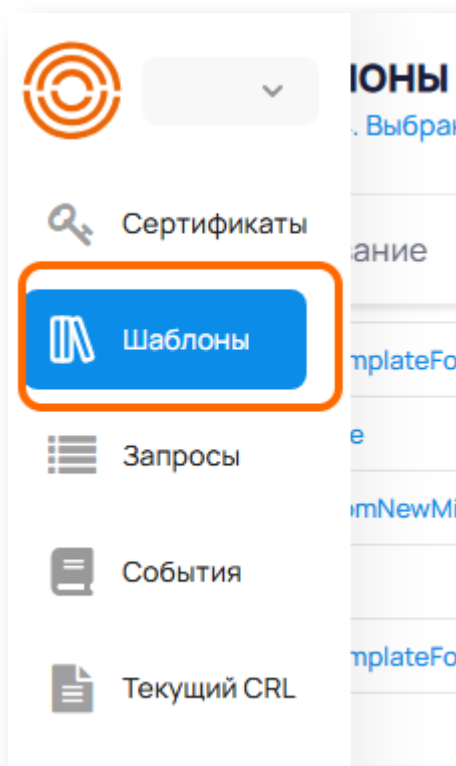


Рисунок 40 — Раздел **Шаблоны**

- 2) Нажать кнопку добавления шаблона в виде +



Рисунок 41 — Кнопка добавления шаблона

- 3) Откроется окно **Новый шаблон**.
- 4) Заполнить поля:
 - **Название**. Ввести название шаблона. Обязательно к заполнению;
 - Поле без названия;

- **Максимальный срок действия сертификата.** Указать максимальный срок действия сертификата. Обязательно к заполнению;
 - Отметить флажок **Признак короткоживущего сертификата.** Логический флажок, указывающий, предназначен ли сертификат для краткосрочного использования (например, тестовые среды или временные проекты). Обязательно к выбору;
 - **Допустимый тип ключа.** Выбрать допустимый тип ключа из представленных. Обязательно к выбору;
 - **Минимальный допустимый размер ключа.** Выбрать размер ключа из представленных. Обязательно к выбору;
 - **Key Usage (keyUsage).** Поле сертификата X.509, которое определяет разрешенные цели использования закрытого ключа владельца сертификата. Выбрать из представленных. Значения параметров представлены в Приложении А.1;
 - **Extended Key Usage (extKeyUsage).** Дополнительное поле сертификата X.509, уточняющее специализированные сценарии использования ключа. Значения приведены в Приложении А.2А.2
 - **Subject Key Identifier.** Уникальный идентификатор открытого ключа субъекта сертификата, представляющий собой хэш SHA-1 открытого ключа. Служит для однозначного сопоставления ключей в цепочках сертификатов. Выбрать из представленных. Обязательно к заполнению.
 - **Authority Key Identifier.** Элемент сертификата X.509, предназначенный для уникальной идентификации публичного ключа выдавшего сертификата (удостоверяющий центр, CA). Выбрать из доступных. Значения приведены в Приложении А.3
 - **Basic Constraints.** Обязательный элемент сертификата X.509, содержащий две части:
 - `ca` (булево значение) — определяет, является ли обладатель сертификата удостоверяющим центром (CA). `True` — да, `False` — нет.
 - `pathLenConstraint` (целое число) — устанавливает максимальную глубину дерева сертификатов (количество промежуточных удостоверяющих центров). Отсутствие значения — неограниченный путь.
 - **Секция конфигурации в файле OpenSSL.** Специальный раздел файла конфигурации OpenSSL, содержащий детальные инструкции по созданию конкретного типа сертификата;
 - **Производные опции OpenSSL.** Дополнительные настройки OpenSSL, влияющие на поведение команд OpenSSL при работе с указанным типом сертификата:
 - Ограничения формата входных данных.
 - Управление выводом диагностической информации.
 - Дополнительные расширения, добавляемые к запросу на сертификат.
- 5) Нажать кнопку **Добавить**.

Новый шаблон

×

Название*

Максимальный срок действия сертификата*

☐ Признак короткоживущего сертификата*

Допустимый тип ключа* ▾

Минимально допустимый размер ключа* ▾

Key Usage ▾

Extended Key Usage*

Subject Key Identifier ▾

Authority Key Identifier ▾

Basic Constraints

Секция конфигурации в файле OpenSSL

Произвольные опции OpenSSL

Отмена

Добавить

Рисунок 42 — Окно создания шаблона

5.2. Редактирование шаблона

- 1) Выбрать раздел **Шаблоны**.

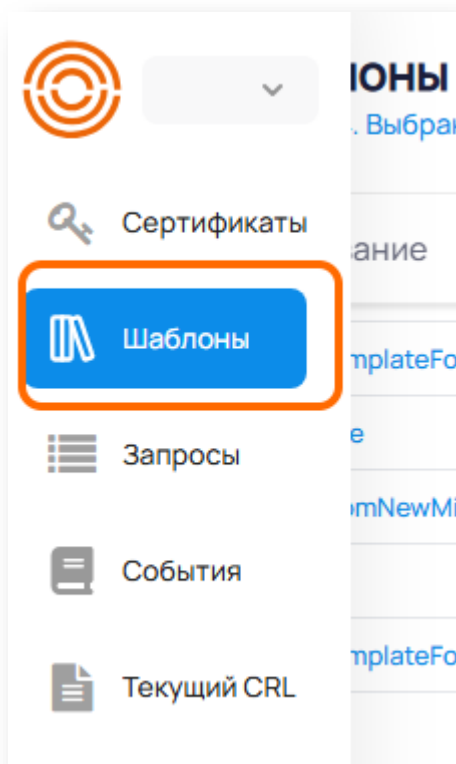


Рисунок 43 — Раздел **Шаблоны**

- 2) Нажать на наименование шаблона, который необходимо изменить.



Название	Версия	Описание	Изменён	Basic Constraints	Key Usage
TestTemplateForCheckSync	4	Для проверки синхронизации	14.04.2025 19:38		digitalSignature, keyEncipherment
qwewqe	1	qwewqwewqwewq	08.04.2025 20:20		KeyCertSign, KeyEncipherment
TestFromNewMiniCACP	1	description	08.03.2025 17:52		keyAgreement
subca	1	Subordinate CA	06.03.2025 17:46	critical, CA: true, pathlen: 0	critical, cRLSign, digitalSignature
TestTemplateForCheckSync2	1	test	28.02.2025 18:12		digitalSignature
User template	3	User template	23.01.2025 20:36		critical, digitalSignature

Рисунок 44 — Наименование шаблона

- 3) Внести необходимые изменения в шаблон и нажать кнопку **Сохранить**.



Рисунок 45 — Карточка редактирования шаблона и кнопка **Сохранить**

5.3. Удаление шаблона

- 1) Открыть карточку редактирование шаблона.
- 2) Нажать кнопку **Удалить**.

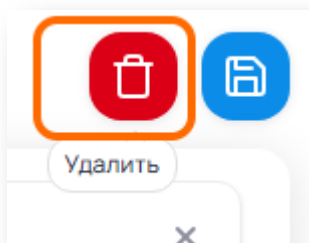


Рисунок 46 — Кнопка удаления шаблона

6. Запросы

6.1. Просмотр списка запросов

- 1) Выбрать раздел **Запросы**.

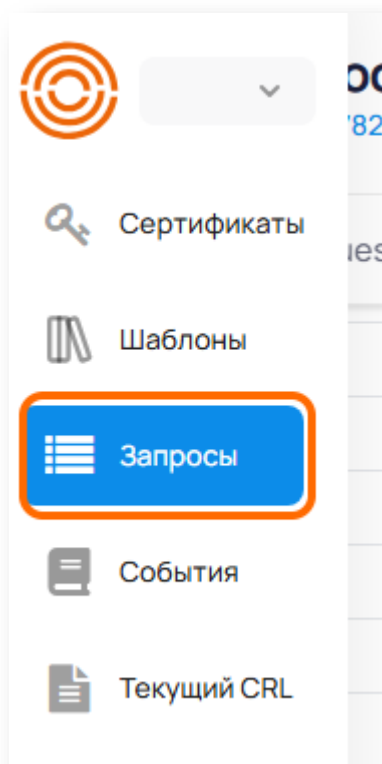


Рисунок 47 — Раздел **Запросы**

- 2) Откроется страница со списком запросов.

Запросы

Всего: 77826. Выбрано: 0

Request ID... Requester Name... Subject... Статус... Шаблон... Common Name... Тип ключа... Принадлежность...

77828	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77827	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77826	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77825	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77824	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77823	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77822	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77821	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77820	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77819	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77818	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77817	019266c5-e155-73ad-af50-e2d6...	CN=test.OU=OpsS.O=CWI	SATISFIED	tls	test	RSA
77816	nikita@cw-dev	CN=*miu.dev.hidden	SATISFIED	tls	*miu.dev.hidden	RSA
77815	some-prefix.c.itsacmcp1-system...	CN=DEV APD00 99-esau dev-watc...	SATISFIED	tls	DEV APD00 99-esau dev...	RSA
77814	artemsh	CN=aglabets	SATISFIED	tls	aglabets	RSA
77813	nikita@cw-dev	CN=*miu.clean.hidden.OU=MIU De...	SATISFIED	tls	*miu.clean.hidden	RSA
77812	user-cwi	CN=TestDeleteSert	SATISFIED	user	TestDeleteSert	RSA
77811	some-prefix.c.itsacmcp1-system...	CN=DEV APD00 99-esau dev-watc...	SATISFIED	tls	DEV APD00 99-esau dev...	RSA
77810	testRequesterForInformation	CN=aglabets	SATISFIED	tls	aglabets	RSA
77809			ERROR			

Рисунок 48 — Страница со списком запросов

7. События

7.1. Просмотр событий

- 1) Выбрать раздел **События**.

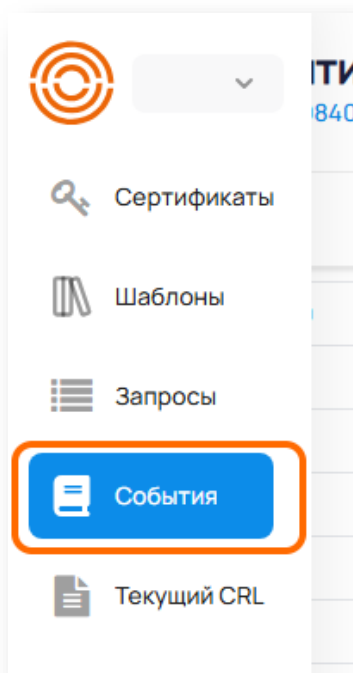


Рисунок 49 — Раздел **События**

- 2) Откроется страница со списком событий.

События

События

Всего: 108403. Выбрано: 0

1 2 3 4 5 — 2169 >

ID	Дата	Событие	Код ошибки	Request ID	Сертификат (Serial Nu...	Шаблон	Номер CRL
108460	15.04.2025 12:44:45	EXPORT	0				
108459	15.04.2025 12:43:27	EXPORT	0				
108458	15.04.2025 12:42:07	EXPORT	0				
108457	15.04.2025 12:40:49	EXPORT	0				
108456	15.04.2025 12:39:31	EXPORT	0				
108455	15.04.2025 12:38:12	EXPORT	0				
108454	15.04.2025 12:36:52	EXPORT	0				
108453	15.04.2025 12:35:35	EXPORT	0				
108452	15.04.2025 12:34:16	EXPORT	0				
108451	15.04.2025 12:32:57	EXPORT	0				
108450	15.04.2025 12:31:39	EXPORT	0				
108449	15.04.2025 12:30:19	EXPORT	0				
108448	15.04.2025 12:29:02	EXPORT	0				
108447	15.04.2025 12:27:44	EXPORT	0				
108446	15.04.2025 12:26:25	EXPORT	0				
108445	15.04.2025 12:25:07	EXPORT	0				
108444	15.04.2025 12:23:49	EXPORT	0				
108443	15.04.2025 12:23:01	EXPORT	0				
108442	15.04.2025 12:22:30	EXPORT	0				
108441	15.04.2025 12:21:11	EXPORT	0				

Рисунок 50 — Страница списка событий

8. Текущий CRL

CRL (Certificate Revocation List) — это список отозванных сертификатов, предоставляемый Центром сертификации (CA), содержащий серийные номера и причины отзыва всех недействительных сертификатов.

Delta CRL (Delta Certificate Revocation List) — это дифференциальный список отозванных сертификатов, содержащий только вновь добавленные или изменённые записи с момента последнего опубликованного базового списка CRL.

9. Выпуск сертификата на MiniCA вручную

- 1) Подключится по протоколу SSH к серверу с настроенным клиентом `mclient`.
- 2) Переключится на пользователя, который имеет права на доступ к директории с `mclient`:

```
$ sudo -su itc-svc
```

- 3) Перейти в папку с `mclient`:

```
cd /app/itc/minica
```

- 4) Скопировать в любую удобную директорию файл запроса сертификата CSR. Например, в `/app/itc/minica/testcerts`. Скопировать файл можно по протоколу SCP или содержимое файла через буфер обмена.
- 5) Выполнить команду:

```
./mclient ca -csr "<путь к файлу csr>" -template "<имя шаблона>" -requester "<имя учетной записи>" -out "<путь к сертификату>"
```

Где:

- `<путь к файлу csr>` – путь к скопированному файлу запроса,
- `<имя шаблона>` – имя предварительно настроенного шаблона. Получить список шаблонов можно командой из таблицы в пункте 7, номер строки 3. Настройка шаблонов не входит в данную инструкцию.
- `<имя учетной записи>` – имя вашей доменной учетной записи. Будет занесена в БД в качестве инициатора запроса.

Пример команды

```
./mclient ca -csr "/app/itc/minica/certs/request_file.req" -template "tls" -out  
"/app/itc/minica/certs/cert_file.crt"
```

- 6) Забрать сертификат в директории, которая была указана в команде выпуска.

9.1. Таблица основных команд

№	Команда	Описание
1)	<code>./mclient --help</code>	Вывод справки по командам <code>mclient</code>
2)	<code>./mclient ping</code>	Проверка доступности miniCA
3)	<code>./mclient templates</code>	Список доступных шаблонов
4)	<code>./mclient revoke -serial 01000000000000000000c -reason certificateHold</code>	Отзыв сертификата: — <code>-serial</code> — серийный номер сертификата; <code>-reason</code> — причина отзыва.
5)	<code>./mclient updcr1 -out ./crlfile.crl</code>	Обновление файла CRL: <code>-out</code> — путь к файлу CRL.
6)	<code>./mclient updeltacr1 -out ./deltacr1file+.crl</code>	Обновление файла deltaCRL: <code>-out</code> — путь к файлу deltaCRL.
7)	<code>./mclient ca -csr ./ request_file.req -template tls -requester vtb4005704 -out ./ cert_file.crt</code>	Выпуск сертификата: — <code>ca</code> — ключ для выпуска сертификата; — <code>-csr</code> — путь к файлу запроса; — <code>-template</code> — имя шаблона; — <code>-requester</code> — имя УЗ, запросившей сертификат; <code>-out</code> — путь к файлу сертификата.

Приложение А Значения параметров

A.1 Значение keyUsage

- `digitalSignature` — Используется для подписи цифровых документов.
- `nonRepudiation` — Подтверждение авторства документа.
- `keyEncipherment` — Шифрование ключей другим ключом.
- `dataEncipherment` — Прямое шифрование данных.
- `keyAgreement` — Обмен секретными ключами между сторонами.
- `keyCertSign` — Возможность подписывать другие сертификаты.
- `cRLSign` — Возможность подписания списков отзыва сертификатов.
- `encipherOnly` — Разрешено использовать закрытый ключ только для шифрования.
- `decipherOnly` — Разрешено использовать закрытый ключ только для дешифровки.

A.2 Значения Extended Key Usage

- `anyExtendedKeyUsage` — Любой сценарий использования ключа.
- `serverAuth` — Аутентификация серверов (например, HTTPS).
- `clientAuth` — Аутентификация клиентов (например, TLS-клиентов).
- `codeSigning` — Подпись программного обеспечения.
- `emailProtection` — Защита электронной почты (например, S/MIME).
- `timeStamping` — Создание временных меток (timestamping).
- `ocspSigning` — Подписание OCSP-отзывов.
- `ipsecEndSystem` — Конец туннеля IPsec.
- `ipsecTunnel` — Точка входа в IPsec-туннель.
- `ipsecUser` — Пользовательское устройство в IPsec.
- `msCodeInd` — Промежуточная подпись кода (Windows Authenticode).
- `msCodeCom` — Коммерческая подпись кода (Windows Authenticode).
- `msCTLSign` — Подписание доверительных списков (Trusted Lists).
- `msEFS` — Шифрование файловых систем (EFS).
- `msSmartCardLogin` — Вход по смарт-карте.
- `msKernelModeCodeSigning` — Подпись драйверов ядра ОС.
- `msProtectedHealthInformation` — Обработка защищённой медицинской информации PHI.
- `microsoftEVCodeSigning` — Усиленная подпись программного кода (EV-кодирование).
- `netscapeStepUpOID` — Повышение уровня привилегий (специфично Netscape).

A.3 Значения Authority Key Identifier

- `none` — Поле Authority Key Identifier вообще не добавляется в сертификат.
- `issuer` — Включается только информация об имени издателя (Issuer Name).

`issuer:always` — Всегда включается информация об имени издателя, даже если невозможно включить остальные компоненты (например, отсутствует ключевая информация).

`keyid` — Включается только идентификатор ключа (hash open key).

`keyid:always` — Идентификатор ключа обязательно включается независимо от наличия другой информации.

Приложение Б Причины отзыва сертификата

Причина	Описание
Unspecified	Нет конкретной причины отзыва.
KeyCompromise	Компрометация закрытого ключа, связанного с сертификатом.
CACompromise	Центр сертификации признан скомпрометированным, следовательно, все его сертификаты подлежат отзыву.
AffiliationChanged	Изменилась принадлежность владельца сертификата к какой-либо организации или изменилась форма юридического лица.
Superseded	Выдан новый сертификат взамен старого.
CessationOfOperation	Деятельность владельца сертификата прекращена.
CertificateHold	Временный отзыв сертификата без полного прекращения его действия.
RemoveFromCRL	Удаление сертификата из списка отозванных (редкое событие).