Цифровые технологии

КриптоАРМ CA

Документация продукта

Релиз v1.0

Исходная документация на Trusted.ru

Редакция от 30.10.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

О продукте 3
Установка и запуск 4
Руководство администратора и оператора 6
Руководство пользователя веб-интерфейса 18
Справочник REST API 26
Часто задаваемые вопросы 28
Глоссарий 30

Открыть статью на сайте

О продукте

О продукте КриптоАРМ CA

КриптоАРМ CA — самостоятельный Центр сертификации (Удостоверяющий центр), не требующий Microsoft CA. Продукт поддерживает российские ГОСТ-алгоритмы и международные RSA/ECDSA.

Основные сценарии

- именные сертификаты сотрудников для аутентификации, ЭП и шифрования;
- обезличенные сертификаты ИС для TLS и технологической подписи;
- автоматический выпуск **Unattended**;
- отзыв, приостановка и возобновление сертификатов;
- **Auto-Rollover** за 30 дней до окончания срока;
- CRL и OCSP;

Компоненты

- **КриптоАРМ ID** — единый вход OIDC;
- **КриптоАРМ IDM** — Центр регистрации, сбор и верификация данных;
- **КриптоАРМ CA / CA CORE** — исполняющий УЦ;
- **КриптоАРМ Документы** — работа с электронными документами;
- **КриптоАРМ Server** — низкоуровневые криптографические операции.

Роли

Администратор настраивает систему и инфраструктуру. **Оператор** работает с заявками и жизненным циклом сертификатов. Используется RBAC и двухфакторная аутентификация.

Безопасность сети

Наружу через Traefik публикуются веб-интерфейсы ID, Документы APP и CA APP. `ca-core` и КриптоАРМ Server наружу не публикуются и работают во внутренней Docker-сети.

Криптографическое окружение

Для ГОСТ используется КриптоПро CSP 5.0+, для RSA/ECDSA — OpenSSL 3.x. Для веб-консоли необходимо использовать Яндекс.Браузер 21.11+, Chrome 122+, Firefox 93+, Edge 95+.

Подробнее о работе пользователя: 07-ui-guide-ca.md.

Открыть статью на сайте

Установка и запуск

Установка и запуск КриптоАРМ CA

Требования

Параметр	Ориентир
ОЗУ	8 ГБ и более
Диск	100 ГБ и более
CPU	x86_64/amd64
Docker	Engine 19.03+ с `docker compose`
Сеть	80/443
DNS	`ID_HOST`, `DOCS_HOST`, `CA_HOST`

Поддерживаются Linux-дистрибутивы, перечисленные в исходной документации, а также Windows; полный стек запускается контейнерами Linux.

Каталоги

```
.
├── docker-compose.yml
├── .env
├── acme.json
├── id/
├── documents/
├── ca/
├── ca-core/
│   ├── .env
└── server/
    ├── .env
    ├── Dockerfile
    ├── cryptopro/linux-amd64_deb.tgz
    └── certs/
```

Конфигурация

```
cp .env.example .env
cp id/.env.example id/.env
cp documents/.env.example documents/.env
cp ca/.env.example ca/.env
cp ca-core/.env.example ca-core/.env
cp server/.env.example server/.env
```

В корневом `.env` задаются `ID_HOST`, `DOCS_HOST`, `CA_HOST`, `ADMIN_MAIL`. Во всех `.env` нужно заменить стандартные пароли и секреты.

Сквозные ключи:

- `ca-core: API_KEY` = `ca: CA_API_TOKEN`;
- `server: API_KEYS` = `documents: SIGN_SERVICE_API_KEY`.

⚠️ **Важно:** До первого запуска обязательно настройте файл `ca-core/.env`. После генерации ключей изменение данных DN потребует полного пересоздания УЦ!

Основная настройка `ca-core/.env`: * **Публичный адрес:** Задайте `CA_HOST=https://ca.example.ru` (адреса CRL/OCSP/AIA соберутся автоматически). * **Переопределение адресов (опционально):** Расскомментируйте и измените `CRL_URL`, `OCSP_URL` или `CA_ISSUERS_URL`, если структура ссылок отличается от стандартной. * **Subject (DN) корневого сертификата:** Заполните переменные `CA_C`, `CA_ST`, `CA_L`, `CA_O`, `CA_OU`, `CA_CN` и `CA_EMAIL` своими актуальными данными (применяется только при первом создании каталога `data/`).

Запуск

```
touch acme.json && chmod 600 acme.json
docker compose build cryptoarm-server
docker compose up -d
```

Логи:

```
docker compose logs -f documents-api ca-api cryptoarm-server ca-core
```

Первичная настройка

1. Войти в `https://ID_HOST` и сменить стандартный пароль `admin/admin`.
2. В КриптоАРМ ID создать OIDC-клиенты **Документы** и **CA**.
3. Для CA использовать callback `https://ca.example.ru/api/auth/callback`, scopes `openid email profile`.
4. Перенести Client ID/Secret в `ca/.env`.
5. Скопировать `ca-core/data/certs/ca.cert.pem` в `server/certs/root/ca.cert.cer` и перезапустить Server.
6. Проверить вход в CA и выпуск тестового сертификата.

Обслуживание

```
docker compose stop
docker compose pull
docker compose build --pull cryptoarm-server
docker compose up -d
```

Открыть статью на сайте

Руководство администратора и оператора

Руководство администратора и оператора

1. Роли

Администратор

Настройка OIDC, конфигурации, доверия между CA и Server, резервного копирования, лицензий и диагностики.

Оператор

Повседневная работа с сертификатами: просмотр, выпуск, скачивание, смена PIN PFX, отзыв и контроль событий.

2. Вход

Консоль CA: `https://CA_HOST`. Аутентификация выполняется через настроенный механизм КриптоАРМ ID.

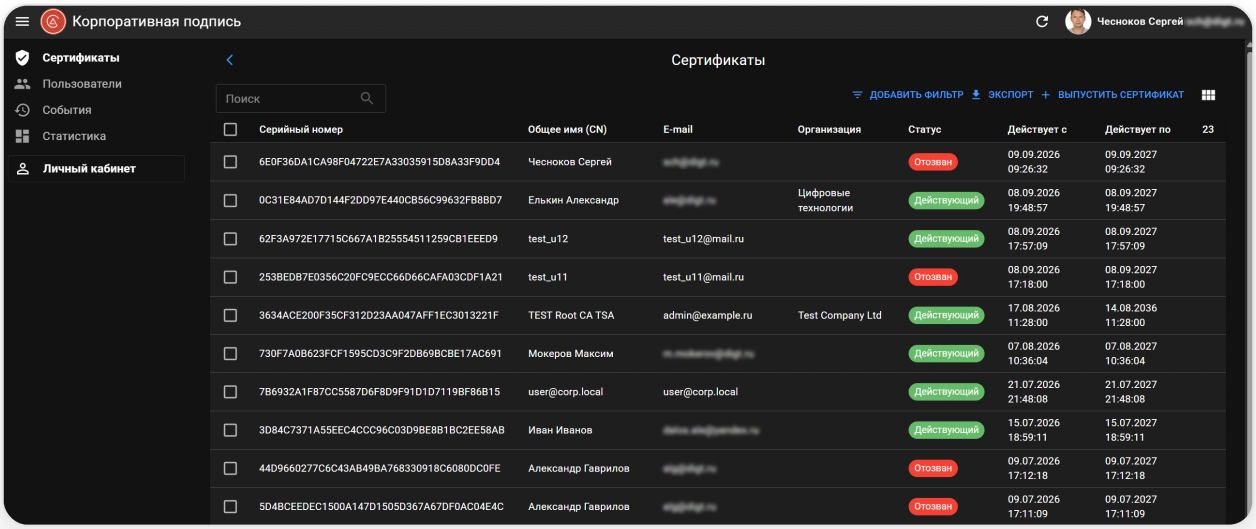
3. Основные разделы

В левом боковом навигационном меню веб-консоли доступны следующие основные разделы: * **Сертификаты** — управление реестром и выпуск цифровых сертификатов. * **Пользователи** — ведение учетных записей, групп и контроль их прав. * **События** — сквозной аудит всех действий в системе. * **Статистика** — аналитический дашборд для мониторинга состояния УЦ. * **Личный кабинет** — персональные настройки текущего оператора.

В верхней панели отображается текущий статус системы (**«Корпоративная подпись»**), кнопка принудительного обновления данных, а также профиль авторизованного пользователя с аватаром и e-mail.

Подробное описание GUI — в 07-ui-guide-ca.md.

Раздел «Сертификаты» с правами администратора.



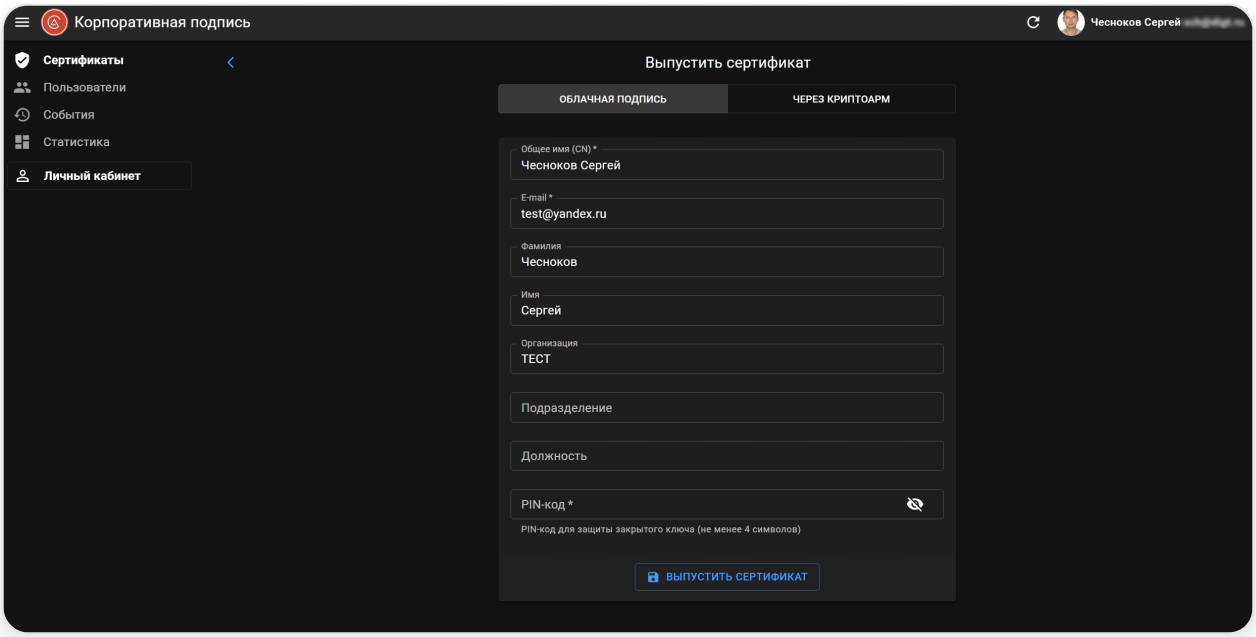
4. Выпуск

Облачная подпись

Форма создания облачного сертификата (**Сертификаты → Создать → Облачная подпись**) содержит следующие поля для заполнения: * **Общее имя (CN)*** — ФИО или имя сущности. * **E-mail*** — адрес электронной почты владельца. * **Фамилия** и **Имя** — персональные данные. * **Организация**, **Подразделение**, **Должность** — служебная принадлежность. * **PIN-код*** — поле ввода пароля для защиты закрытого ключа (не менее 4 символов) с возможностью скрытия/просмотра по клику на иконку «глаз».

Эмиссия и привязка выполняются на стороне сервера после нажатия синей кнопки **«ВЫПУСТИТЬ СЕРТИФИКАТ»**.

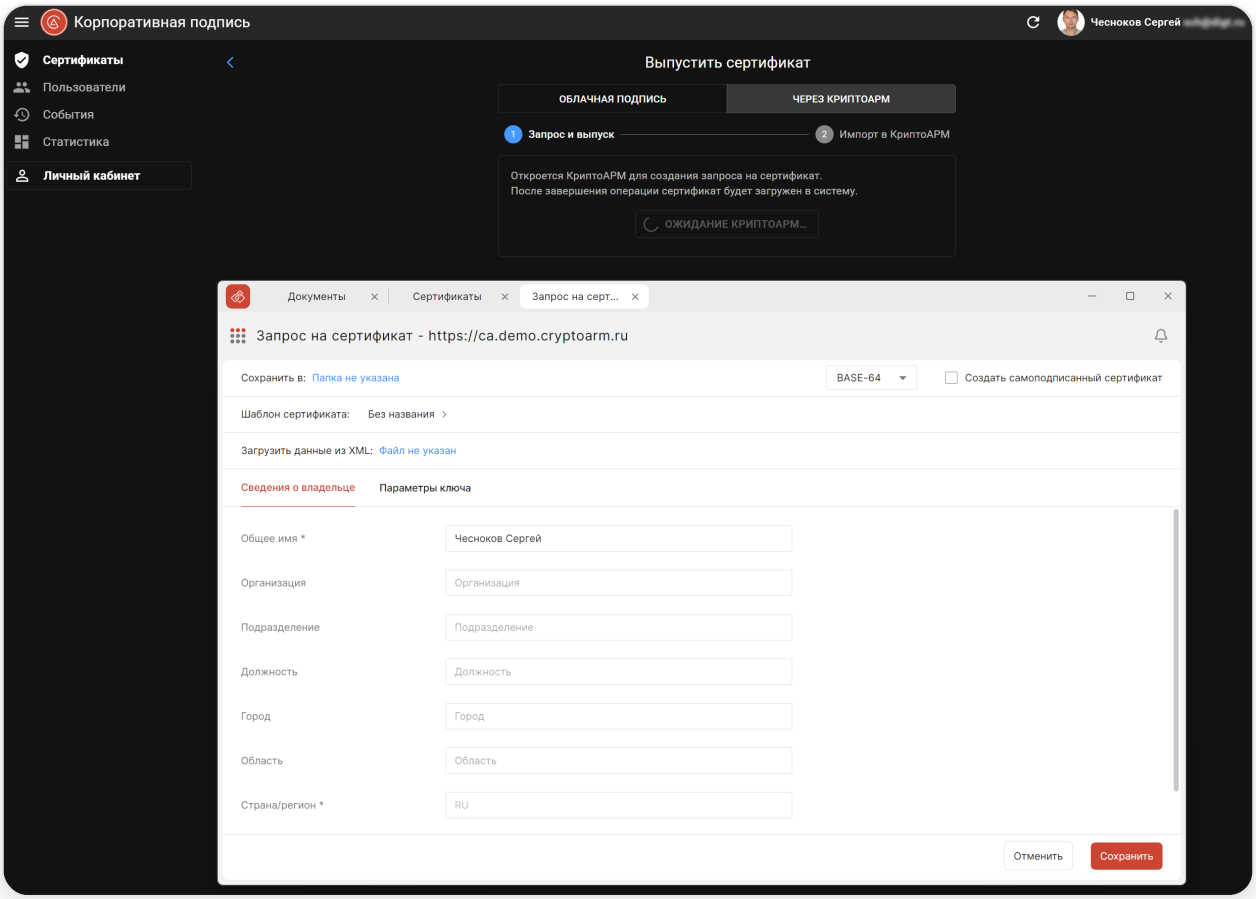
Форма создания сертификата.



Через КриптоАРМ

При выборе вкладки **«Через КриптоАРМ»** операция становится асинхронной. Процесс разделяется на два последовательных шага, отображаемых на индикаторе прогресса: 1. **Запрос и выпуск** — веб-консоль переходит в состояние «ОЖИДАНИЕ КРИПТОАРМ...» и выводит сообщение: «Откроется КриптоАРМ для создания запроса на сертификат. После завершения операции сертификат будет загружен в систему». На переднем плане запускается десктопное приложение КриптоАРМ с формой «Запрос на сертификат» (содержащей URL-адрес УЦ, сведения о владельце и параметры ключа) для генерации ключей на токене или смарт-карте. CSR возвращается в УЦ. 2. **Импорт в КриптоАРМ** — финальная стадия сохранения готового сертификата на физический носитель.

Выпуск сертификата через приложение КриптоАРМ.



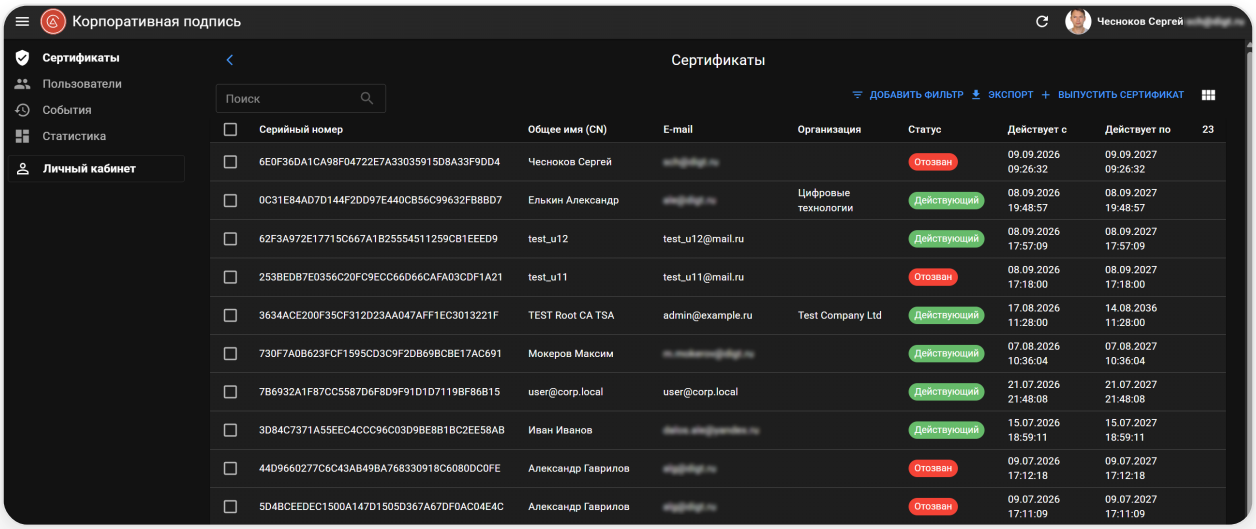
5. Работа со списком и карточкой

Список сертификатов

Основной реестр представляет собой таблицу со следующими колонками: * Чекбокс выбора (для групповых операций). * **Серийный номер** (уникальный хэш-идентификатор сертификата). * **Общее имя (CN)**. * **E-mail**. * **Организация**. * **Статус** — цветовой индикатор (зеленый `Действующий`, красный `Отозван`). * **Действует с** / **Действует по** — точное время и дата окончания действия в формате `ДД.ММ.ГГГГ ЧЧ:ММ:СС`.

Над таблицей расположены инструменты управления: строка **Поиска**, кнопки **«ДОБАВИТЬ ФИЛЬТР»**, **«ЭКСПОРТ»**, синяя кнопка **«ВЫПУСТИТЬ СЕРТИФИКАТ»**, а также переключатель режима отображения (таблица/плитка). В правом верхнем углу выводится общий счетчик записей. Для перехода в карточку необходимо открыть строку конкретного сертификата.

Список сертификатов с поиском, владельцем, статусом и сроками действия.

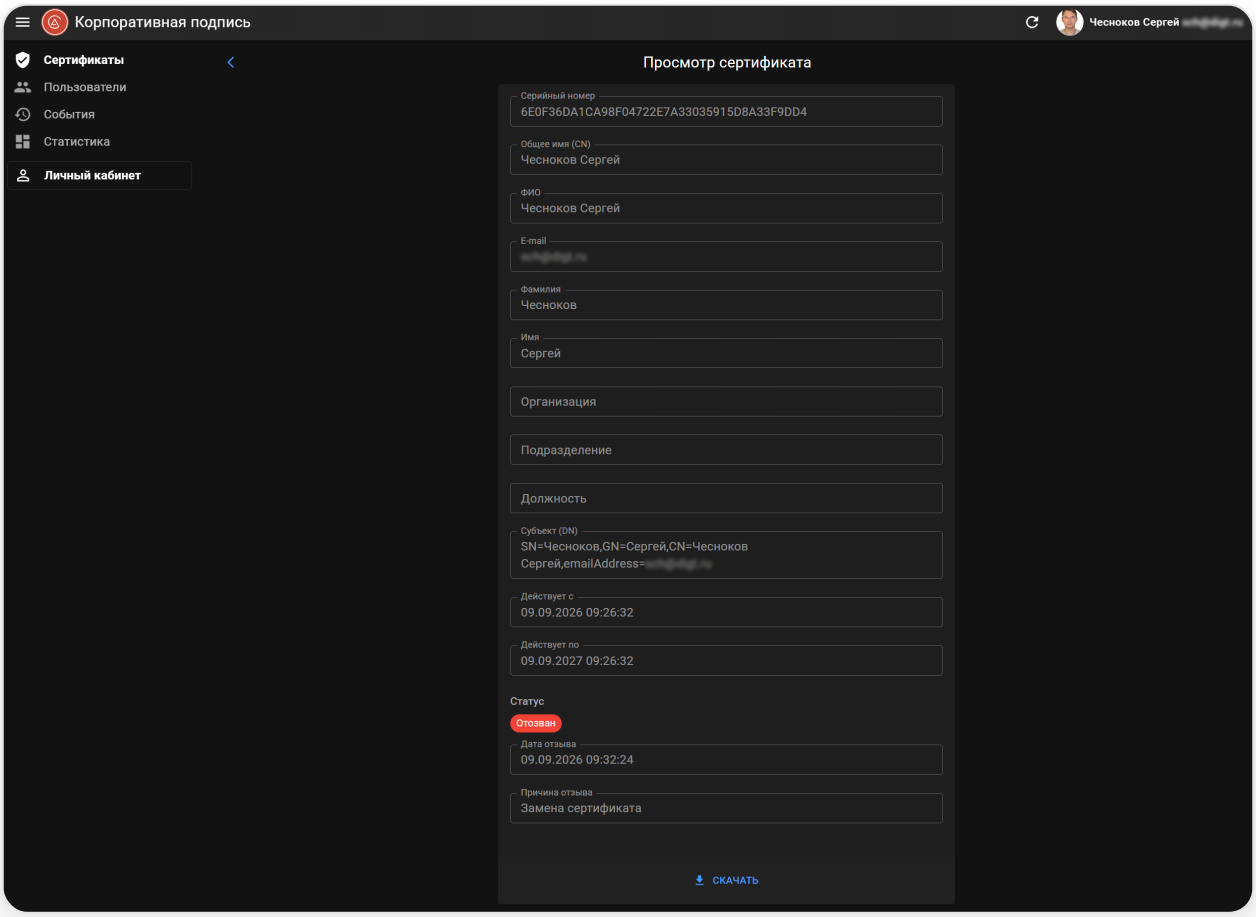


Карточка сертификата

В режиме **«Просмотр сертификата»** открывается форма, содержащая все заполненные атрибуты ключа (Серийный номер, Общее имя, ФИО, E-mail, Фамилия, Имя, Организация, Подразделение, Должность). * Для отозванных сертификатов дополнительно выводится текстовый блок **Субъект (DN)** с полной строкой идентификации (например, `SN=..., GN=..., CN=..., emailAddress=...`). * В нижней части карточки отображаются временные метки (**Действует с**, **Действует по**), **Статус**, а также **Дата отзыва** и **Причина отзыва** (если сертификат неактивен).

В подвале карточки доступны следующие действия: * ⬇ `СКАЧАТЬ` (доступно для всех статусов); * 🔑 `СМЕНИТЬ PIN-КОД` (только для действующих); * 🚫 `ОТОЗВАТЬ` (только для действующих).

Карточка сертификата с атрибутами, сроками, статусом и действиями.

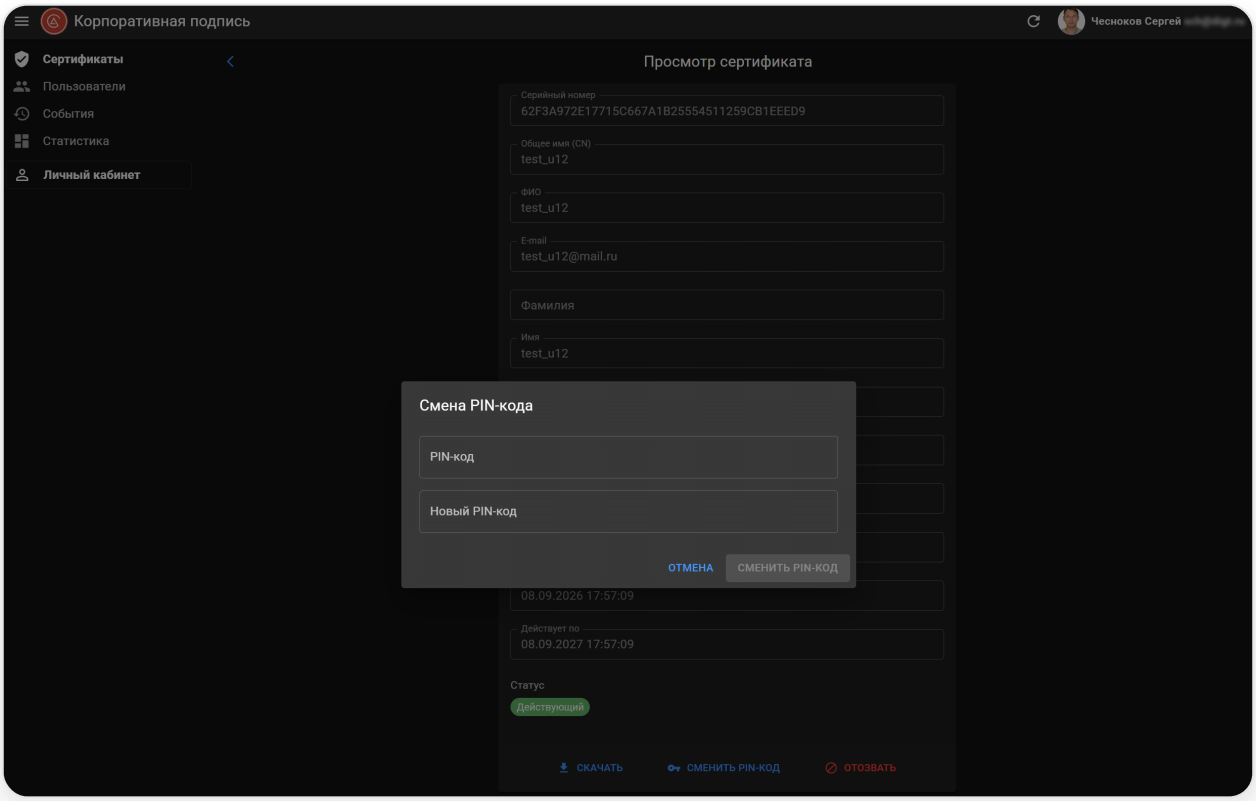


6. Смена PIN

При клике на «Сменить PIN-код» поверх карточки открывается модальное окно **«Смена PIN-кода»**. Оно содержит два поля ввода: 1. **PIN-код** (текущий пароль). 2. **Новый PIN-код**.

Ниже расположены кнопки управления: синяя текстовая кнопка **«ОТМЕНА»** и кнопка **«СМЕНИТЬ PIN-КОД»** для подтверждения изменений. Не передавайте PIN по незащищенным каналам.

Диалог смены PIN-кода с текущим и новым PIN.



Не передавайте PIN по незащищенным каналам.

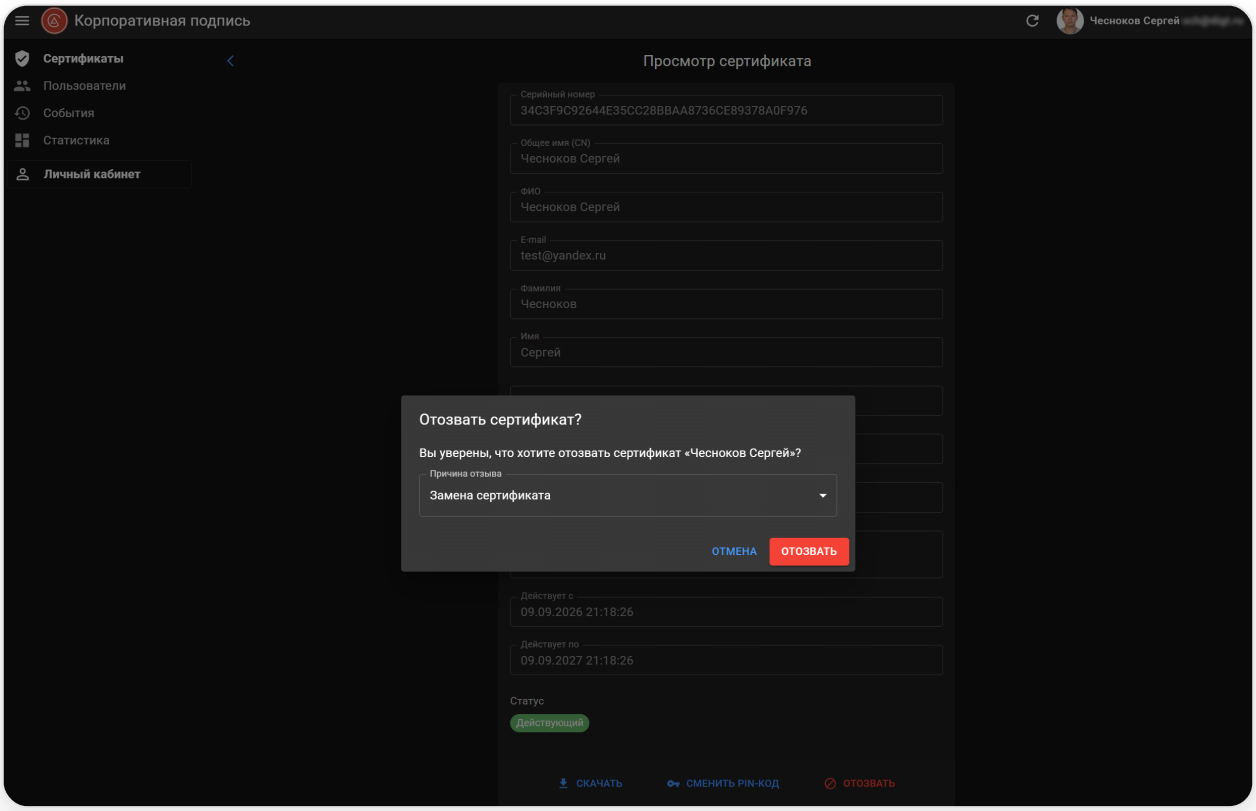
7. Отзыв

При нажатии кнопки «Отозвать» в карточке появляется модальное окно **«Отозвать сертификат?»** с предупреждением: «Вы уверены, что хотите отозвать сертификат «[Имя Владельца]»?».

Оператор обязан выбрать значение в выпадающем списке **Причина отзыва**: * Замена сертификата (superseded); * Компрометация ключа; * Прекращение деятельности; * Изменение принадлежности; * Не указана; * Компрометация УЦ; * Приостановление.

Подтверждение операции выполняется по нажатию красной кнопки **«ОТОЗВАТЬ»**, отмена — по кнопке **«ОТМЕНА»**.

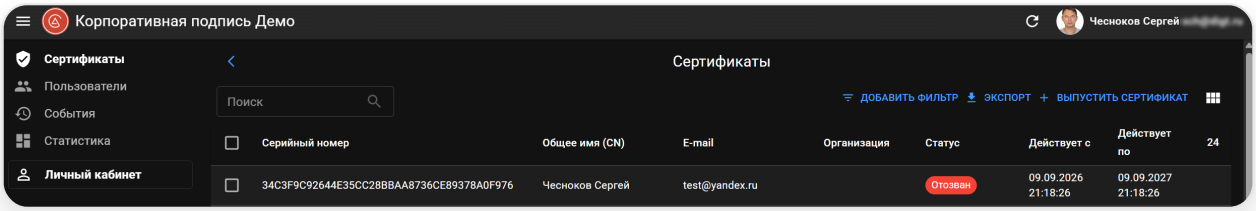
Диалог выбора причины отзыва сертификата.



В исходном PDF видны причины: замена сертификата, компрометация ключа, прекращение деятельности, изменение принадлежности, не указана, компрометация УЦ, приостановление.

После аннулирования сертификат отображается в общем списке с измененным красным статусом `Отозван`.

Сертификат в общем списке после отзыва с измененным статусом.



8. Пользователи

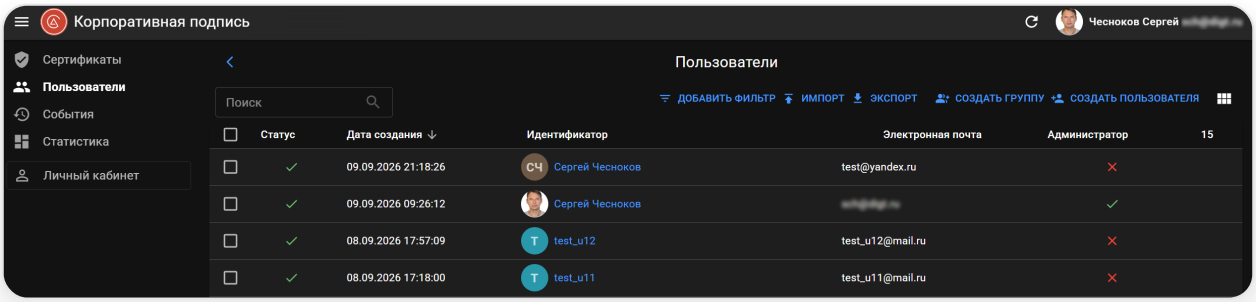
Раздел **«Пользователи»** предназначен для управления учетными записями операторов, администраторов и пользователей системы, а также для гибкого разграничения их полномочий.

Список пользователей

Интерфейс реестра представляет собой таблицу со следующими колонками: * Чекбокс выбора записи. * **Статус** — графический маркер состояния учетной записи (зеленая галочка означает активный аккаунт). * **Дата создания ↓** — временная метка регистрации пользователя (с возможностью сортировки). * **Идентификатор** — блок, содержащий иконку/аватар пользователя с его инициалами или фотографией и полное имя (например, `Сергей Чесноков`, `test_u12`). * **Электронная почта** — e-mail адрес учетной записи. * **Администратор** — индикатор наличия максимальных прав доступа в системе (зеленая галочка для администраторов, красный крестик для рядовых пользователей и операторов).

В верхнем правом углу над таблицей выводится общий счетчик зарегистрированных пользователей (например, 15). Над списком расположены инструменты управления: строка **Поиска**, кнопки **«ДОБАВИТЬ ФИЛЬТР»**, **«ИМПОРТ»**, **«ЭКСПОРТ»**, а также кнопки **«СОЗДАТЬ ГРУППУ»** и **«СОЗДАТЬ ПОЛЬЗОВАТЕЛЯ»**.

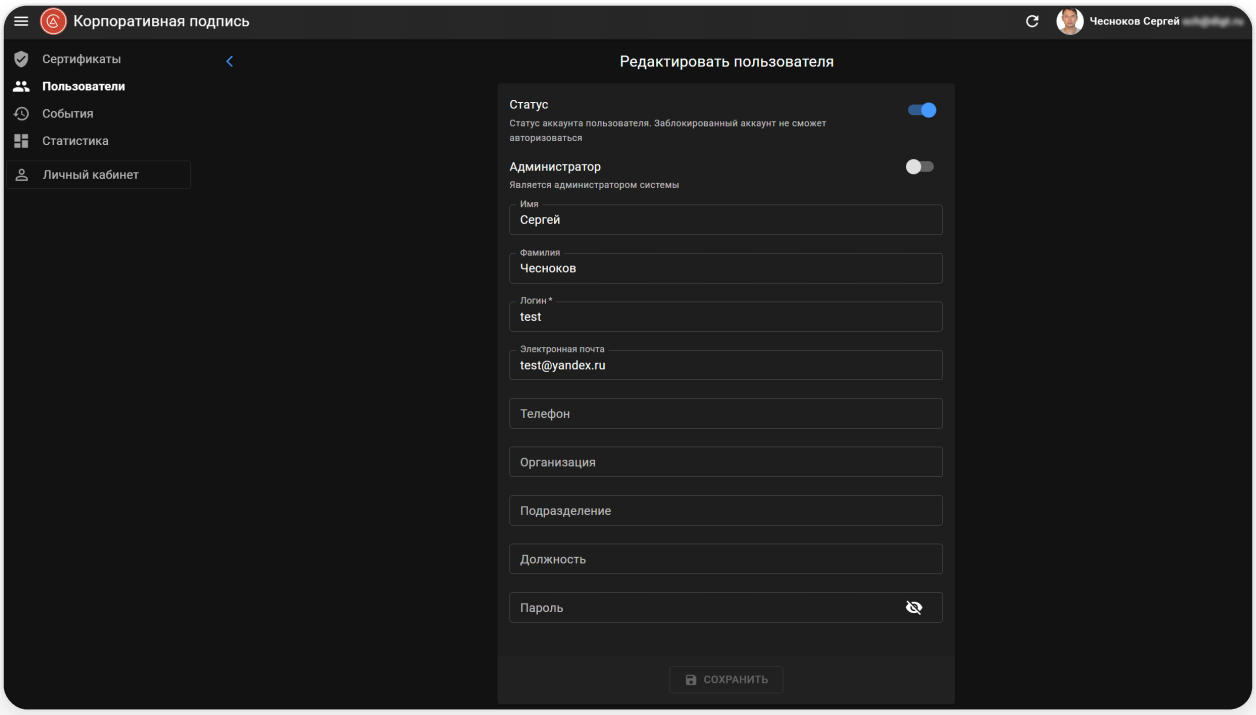
Табличный журнал пользователей: статус, дата создания учетной записи, e-mail и права.



Редактирование и создание пользователя

При создании нового сотрудника или клике на строку существующего для перехода в режим **«Редактировать пользователя»** открывается форма со следующими параметрами: * **Статус (переключатель)** — ползунок активации/деактивации аккаунта. Сопровождается пояснением: «Статус аккаунта пользователя. Заблокированный аккаунт не сможет авторизоваться». * **Администратор (переключатель)** — ползунок наделения учетной записи правами глобального администратора системы. Сопровождается пояснением: «Является администратором системы». * **Имя** и **Фамилия** — персональные текстовые поля. * **Логин*** — уникальный идентификатор пользователя для авторизации в системе. * **Электронная почта** — e-mail сотрудника. * **Телефон**, **Организация**, **Подразделение**, **Должность** — дополнительные информационные поля для формирования структуры компании. * **Пароль** — поле для задания или изменения пароля учетной записи (с кнопкой скрытия/отображения символов). * Сохранение внесенных изменений производится нажатием кнопки **«СОХРАНИТЬ»** внизу формы.

Карточное представление событий с деталями операции.

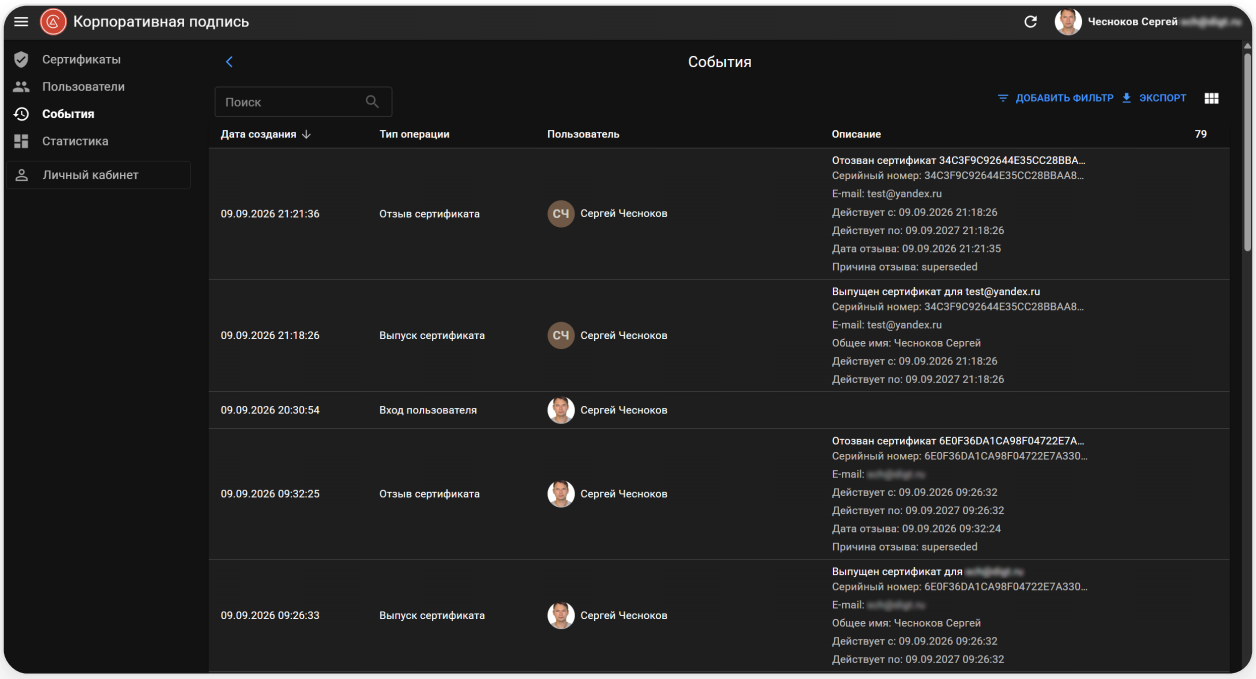


9. События

Раздел предназначен для непрерывного мониторинга безопасности и представляет собой структурированную таблицу. Справа сверху выводится общий счетчик зафиксированных логов. Таблица содержит следующие столбцы: * **Дата создания ↓** — временная метка события с возможностью сортировки по убыванию/возрастанию. * **Тип операции** — категория действия: * Выпуск сертификата * Отзыв сертификата * Вход пользователя * **Пользователь** — имя и аватар оператора или пользователя, совершившего действие. * **Описание** — детальный лог операции в текстовом виде (информация о том, кому выпущен сертификат, его e-mail, серийный номер, точный период действия, а также технический код причины отзыва, например, `Причина отзыва: superseded`).

Над таблицей доступны поисковая строка, функции **«ДОБАВИТЬ ФИЛЬТР»**, **«ЭКСПОРТ»** данных и переключение структуры интерфейса.

Табличный журнал событий: дата, тип и описание операции.



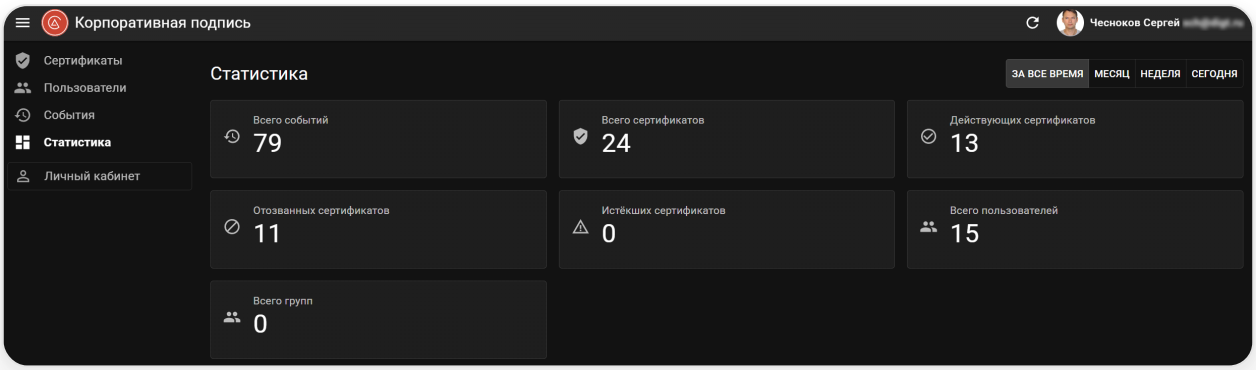
На скриншоте также видны поиск, фильтрация и экспорт.

10. Статистика

Вкладка представляет собой аналитическую панель (дашборд) для быстрой оценки состояния компонентов УЦ. В правом верхнем углу находится фильтр временных периодов: **«ЗА ВСЕ ВРЕМЯ»**, **«МЕСЯЦ»**, **«НЕДЕЛЯ»**, **«СЕГОДНЯ»**.

Аналитика распределена по следующим информационным карточкам-виджетам: * **Всего событий** — суммарное количество записей в журнале аудита. * **Всего сертификатов** — общее число выпущенных за все время сертификатов. * **Действующих сертификатов** — количество активных в данный момент подписей. * **Отозванных сертификатов** — число аннулированных сертификатов. * **Истёкших сертификатов** — количество документов, у которых закончен срок действия. * **Всего пользователей** — число зарегистрированных в системе учетных записей. * **Всего групп** — количество созданных объединений пользователей.

Отображение статистики по собитиям в системе.



9. Резервное копирование

Приоритетный объект — `ca-core/data/` (ключ УЦ и реестр сертификатов). Также сохраняйте `id/data/`, `documents/data/`, `ca/data/`, `server/cert_storage/`, `server/certs/`, `.env`, `id/data/jwks/`, `acme.json`.

10. Диагностика

Симптом	**Проверка**
TLS/ACME	DNS, 80/443, `ADMIN_MAIL`, права `acme.json` = 600
OIDC loop	Client ID/Secret, Redirect URI, `TRUST_PROXY=true`
401 от Server	`AUTH_MODE=apikey`, совпадение ключей
«Подпись не доверяется»	корневой сертификат в `server/certs/root/` и restart Server
CA не выпускает	`CA_API_URI`, `CA_API_TOKEN = API_KEY`

Открыть статью на сайте

Руководство пользователя веб-интерфейса

Руководство по веб-интерфейсу КриптоАРМ СА

О документе

Настоящий раздел предназначен для рядовых сотрудников и пользователей системы «КриптоАРМ СА», не имеющих административных полномочий. Функционал веб-консоли в данном режиме ограничен рамками **Личного кабинета** сотрудника. Пользователь обладает правами только на управление собственными ключевыми носителями, выпуск личных сертификатов и просмотр персонального журнала безопасности.

1. Ограничения прав доступа (Ролевая модель)

В отличие от консоли администратора или оператора УЦ, для обычного пользователя действуют строгие политики конфиденциальности и разграничения доступа: * **Изоляция данных:** Пользователь не имеет доступа к глобальному списку сотрудников организации и не может просматривать чужие сертификаты. * **Доступные разделы:** В боковом навигационном меню пользователю отображаются только те вкладки, которые необходимы для персональной работы. Из меню убраны глобальные административные модули (такие как «Пользователи» и «Статистика»). * **Персональный аудит:** В разделе «События» отображаются исключительно те действия, которые были инициированы самим пользователем или совершены системой в отношении его учетной записи.

2. Общая структура

Интерфейс представляет собой веб-консоль в темной и светлой цветовой гамме (теме). Пользователю доступны следующие элементы управления: * **Боковое меню:** Содержит разделы **«Сертификаты»** и **«События»**. * **Верхняя панель:** Название системы (**«КриптоАРМ СА»**), индикатор принудительного обновления данных страницы, а также профиль пользователя с аватаром и отображением его ФИО (например, Чесноков Сергей) и e-mail. * **Рабочая область:** Меняется в зависимости от выбранного пункта меню. При отсутствии выпущенных сертификатов рабочая область раздела «Сертификаты» переходит в состояние «Нет записей».

3. Личный реестр сертификатов

При открытии раздела **«Сертификаты»** пользователь видит таблицу, содержащую только его собственные цифровые удостоверения.

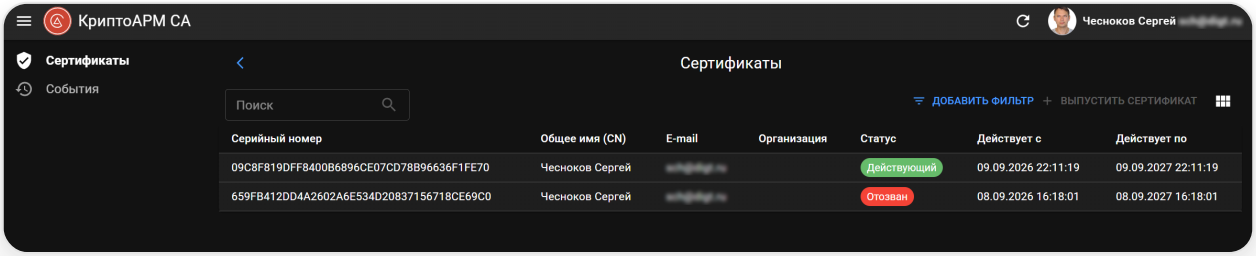
Структура таблицы:

- **Серийный номер** — уникальный хэш-идентификатор сертификата.

- **Общее имя (CN)** — ФИО пользователя.
- **E-mail** — адрес электронной почты, привязанный к сертификату.
- **Организация** — наименование компании сотрудника.
- **Статус** — текущее состояние подписи (зеленый маркер `Действующий` или красный `Отозван`).
- **Действует с / Действует по** — точные временные рамки легитимности ключа в формате `ДД.ММ.ГГГГ ЧЧ:ММ:СС`.

Над таблицей пользователю доступны поисковая строка по серийному номеру, фильтры и кнопка **«ВЫПУСТИТЬ СЕРТИФИКАТ»**. Для перехода в карточку конкретной подписи необходимо кликнуть на соответствующую строку в таблице.

Консоль КриптоАРМ CA: раздел «Сертификаты».



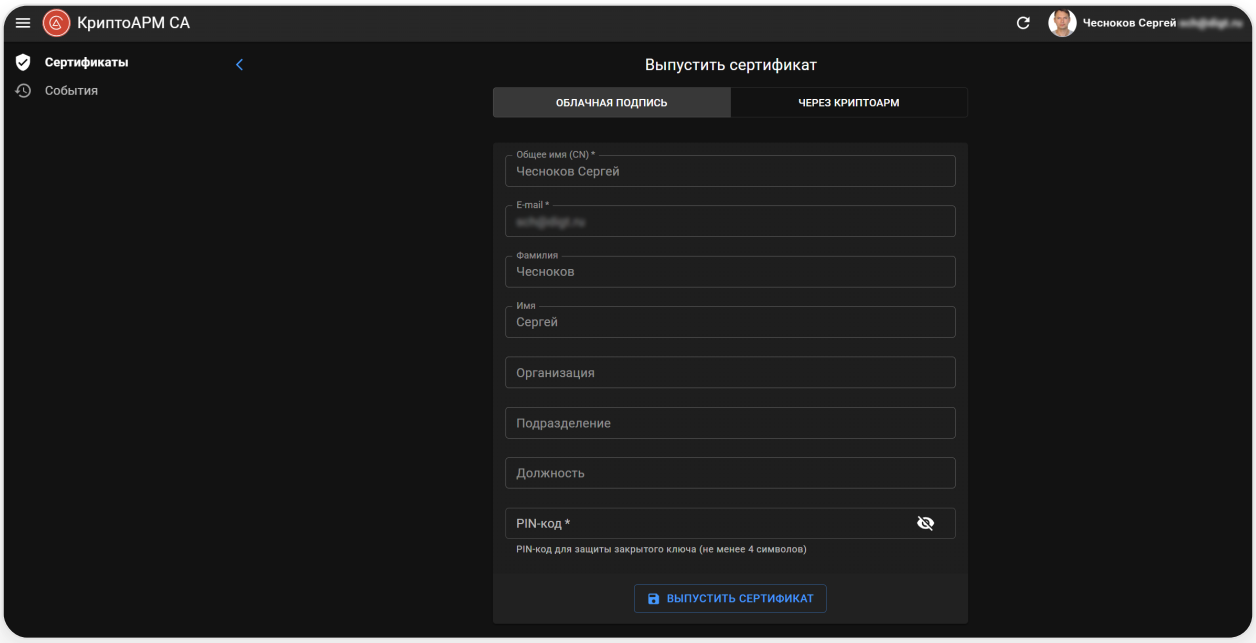
4. Самостоятельный выпуск сертификата

Пользователю доступны два альтернативных сценария получения подписи, переключаемые через вкладки формы создания:

Облачная подпись (Эмиссия на стороне сервера)

1. Перейдите в **Сертификаты → Выпустить сертификат**.
2. Выберите вкладку **«ОБЛАЧНАЯ ПОДПИСЬ»**.
3. Проверьте или заполните персональные данные: Общее имя (CN) (например, Чесноков Сергей), E-mail, Фамилия, Имя, а также служебные атрибуты (Организация, Подразделение, Должность).
4. В поле **«PIN-код*»** задайте пароль для защиты создаваемого закрытого ключа. Пароль должен содержать не менее 4 символов. Для проверки корректности ввода используйте иконку «глаз» справа от поля.
5. Нажмите синюю кнопку **«ВЫПУСТИТЬ СЕРТИФИКАТ»**. Ключи генерируются и защищенно хранятся на сервере.

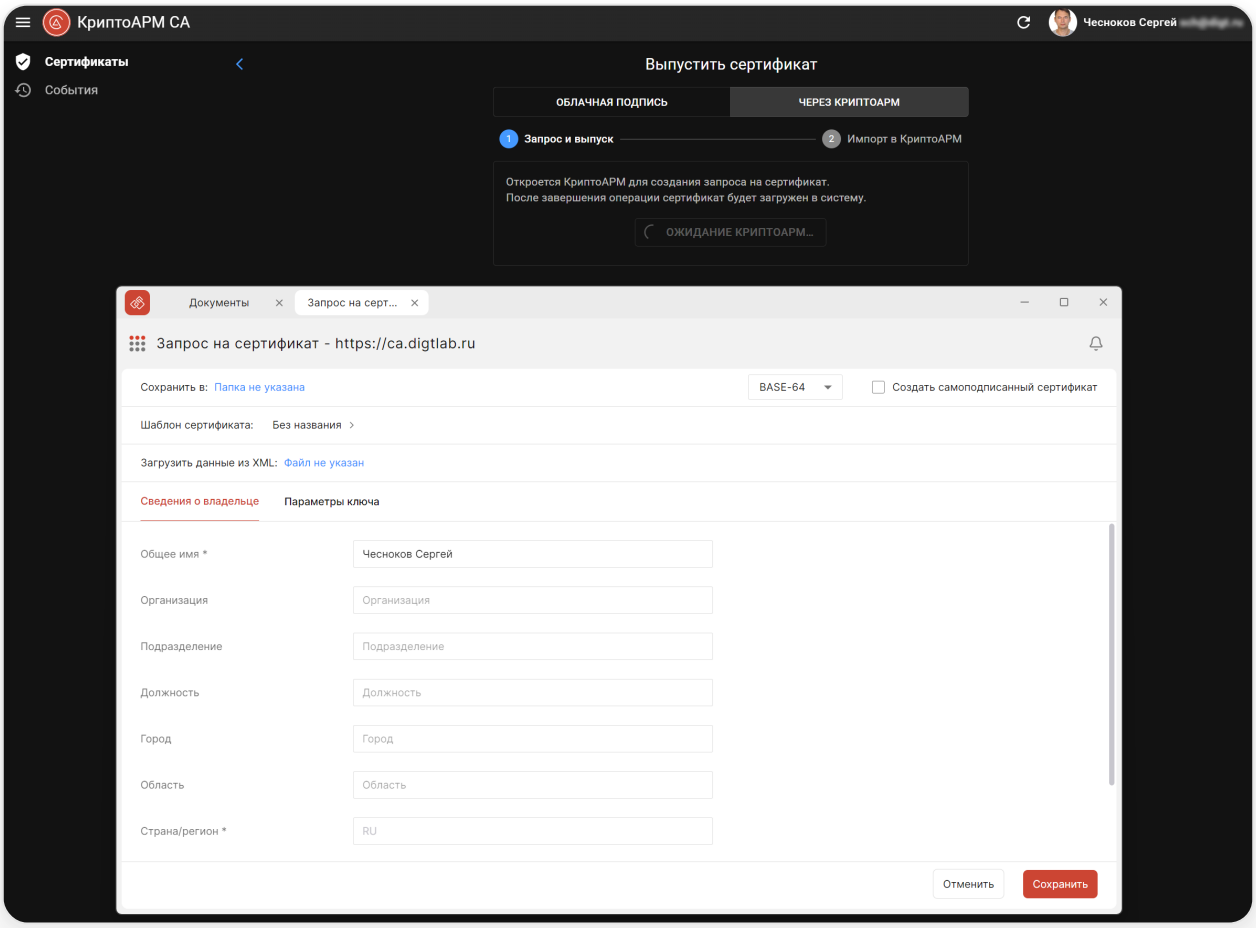
Форма создания сертификата.



Через КриптоАРМ (Эмиссия на локальный токен)

1. В форме создания выберите вкладку **«ЧЕРЕЗ КРИПТОАРМ»**.
2. Процесс перейдет в асинхронный режим ожидания («ОЖИДАНИЕ КРИПТОАРМ...»). На экране отобразится подсказка: «Откроется КриптоАРМ для создания запроса на сертификат. После завершения операции сертификат будет загружен в систему».
3. Локально на компьютере запустится десктопное приложение «КриптоАРМ» со встроенным окном **«Запрос на сертификат»** под уникальным URL-адресом УЦ (например, `https://digtlab.ru`).
4. Пользователь настраивает параметры ключа и генерирует их непосредственно на своем физическом носителе (токене или смарт-карте).
5. Сформированный запрос (CSR) автоматически отправляется в УЦ, подписывается, и готовый сертификат импортируется обратно на токен.

Выпуск сертификата через приложение КриптоАРМ.



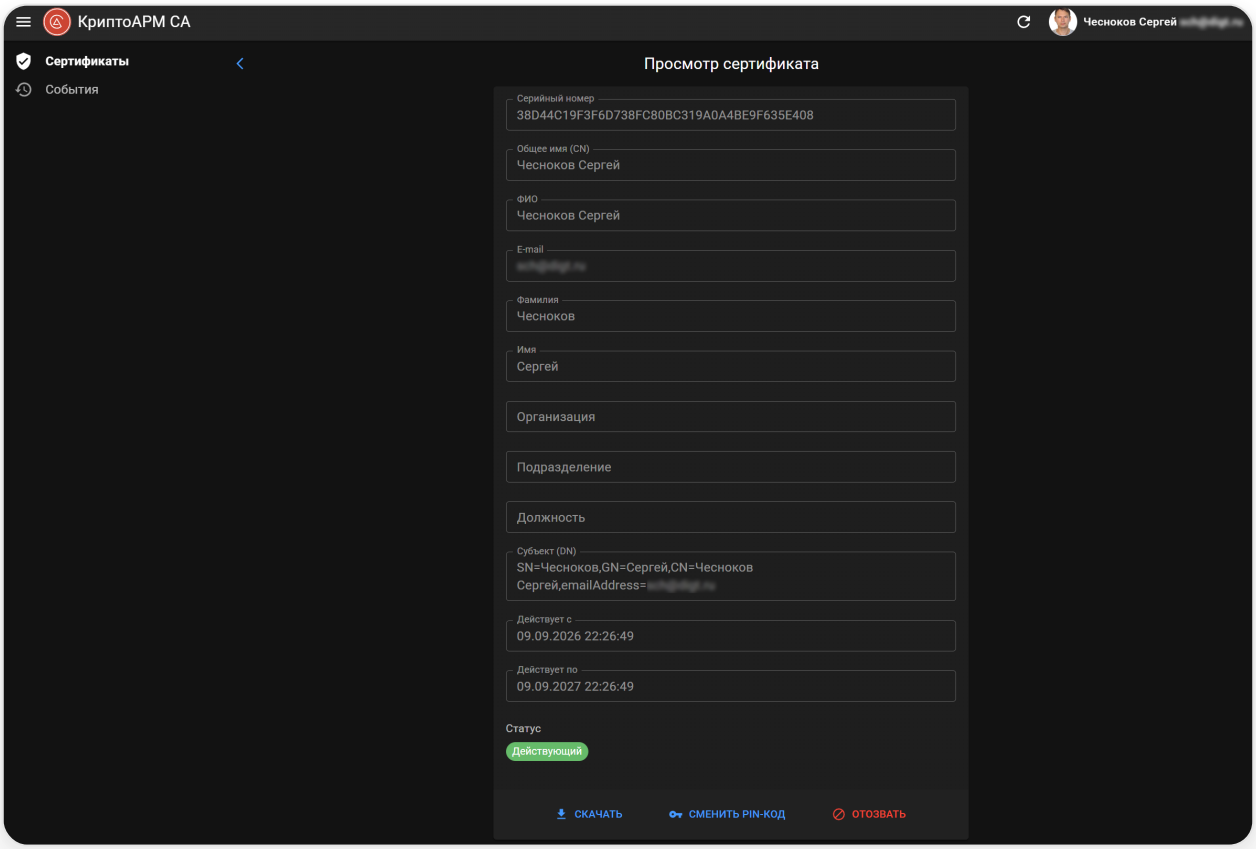
5. Карточка и операции с сертификатом

В режиме **«Просмотр сертификата»** пользователь видит подробную информацию о выбранном ключе. В форме содержатся поля: Серийный номер, Общее имя (CN), ФИО, E-mail, Фамилия, Имя, Организация, Подразделение и Должность.

Ниже основных полей отображается текстовый блок **Субъект (DN)** с полной строкой идентификации (например, `SN=Чесноков, GN=Сергей, CN=Чесноков Сергей, emailAddress=...`). В нижней части карточки выводятся временные метки **Действует с** и **Действует по** (в формате `ДД.ММ.ГГГГ ЧЧ:ММ:СС`), а также цветной статус (например, зеленый индикатор `Действующий`).

В зависимости от текущего статуса, в подвале формы пользователю доступны следующие управляющие действия: * ⬇ `СКАЧАТЬ` — экспорт файла открытого ключа на локальный компьютер (доступно всегда). * 🔑 `СМЕНИТЬ PIN-КОД` — изменение защитного пароля облачного ключа (доступно только для действующих сертификатов). * 🚫 `ОТОЗВАТЬ` — досрочное аннулирование сертификата (доступно только для действующих сертификатов).

Отображение сведений о сертификате.

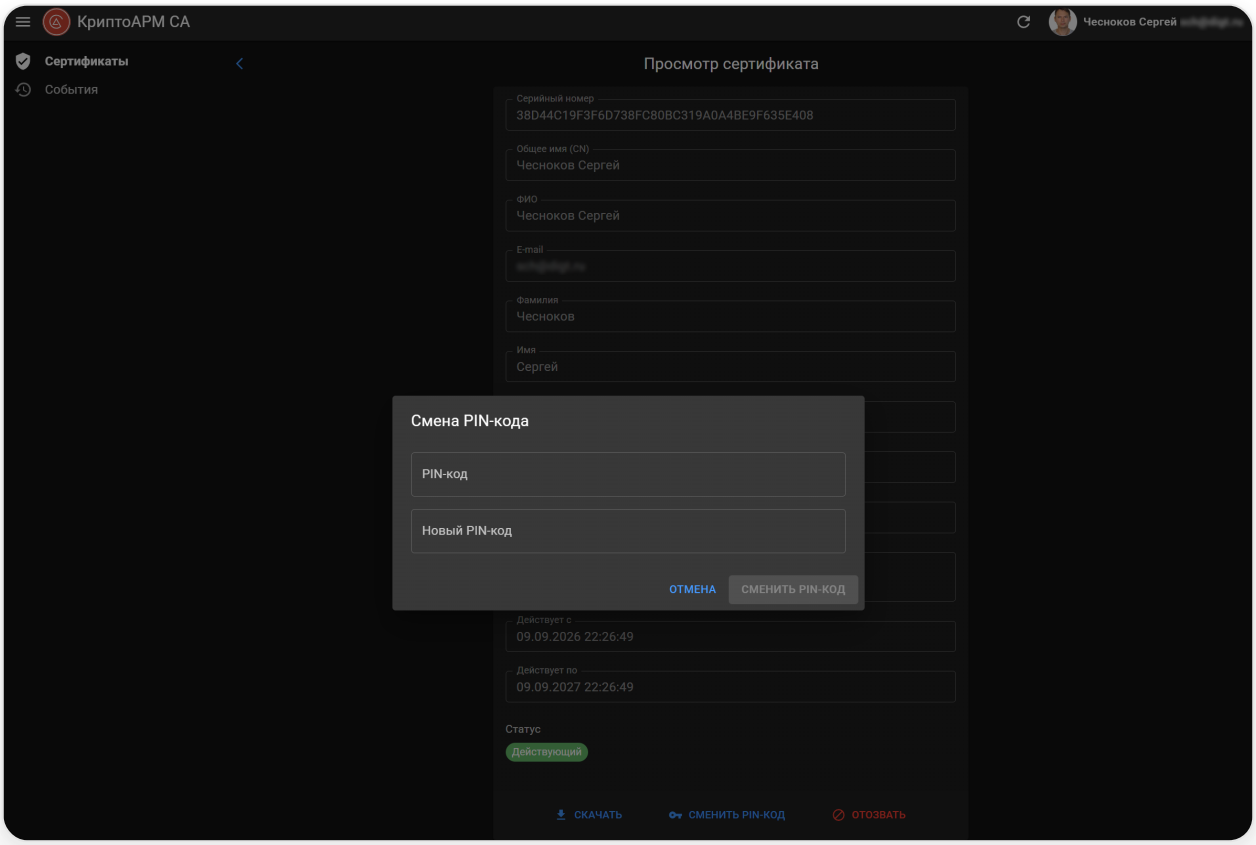


Смена PIN-кода

При клике на кнопку «Сменить PIN-код» поверх карточки открывается модальное окно **«Смена PIN-кода»**. Пользователю необходимо заполнить два поля: 1. **PIN-код** (ввести текущий действующий пароль). 2. **Новый PIN-код** (ввести измененное значение).

Для отмены операции служит текстовая кнопка **«ОТМЕНА»**, для подтверждения изменений — кнопка **«СМЕНИТЬ PIN-КОД»**. Важно: PIN-код является строго конфиденциальной информацией и не подлежит передаче третьим лицам.

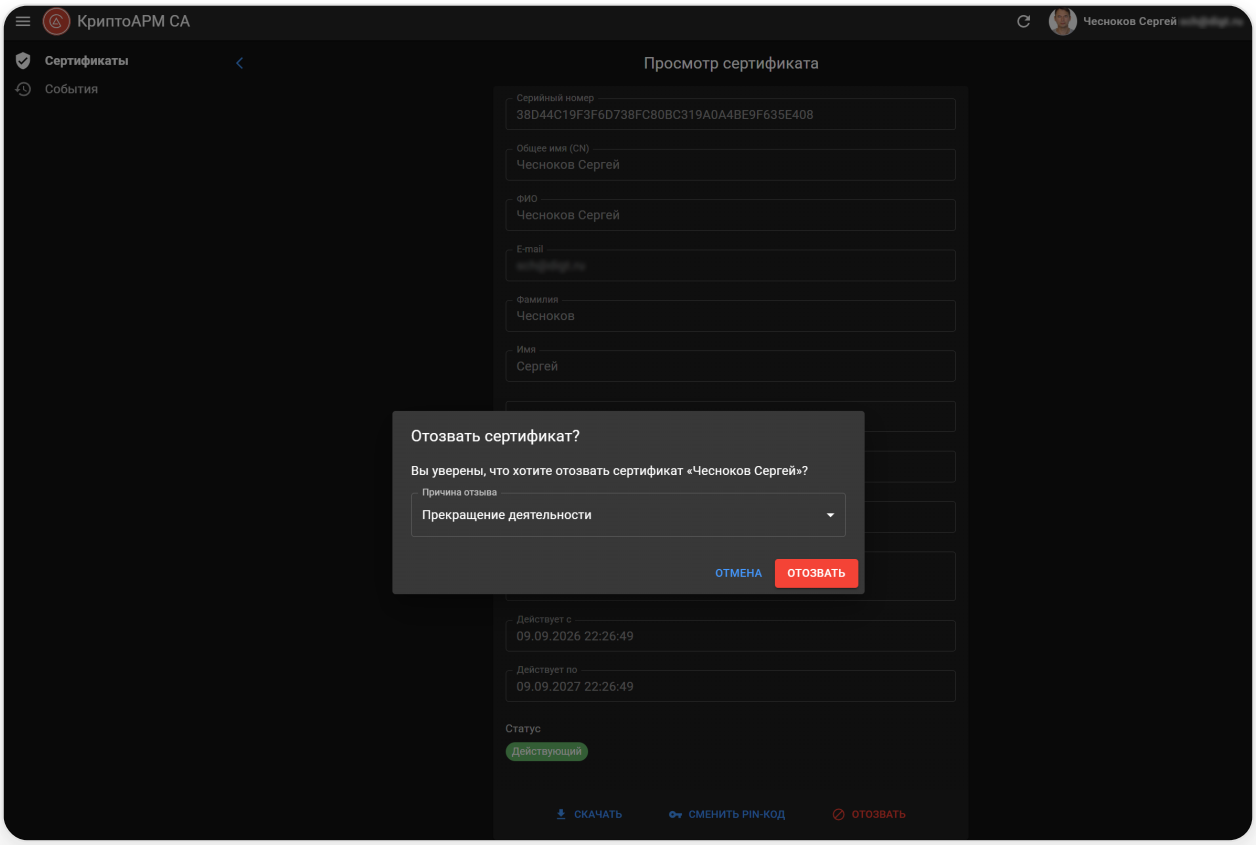
Диалоговое окно изменения PIN-кода.



Самостоятельный отзыв сертификата

Если ключ скомпрометирован или сотрудник меняет место работы, он обязан отозвать сертификат: 1. В подвале карточки нажмите кнопку **«Отозвать»**. 2. Появится модальное окно **«Отозвать сертификат?»** с предупреждением: «Вы уверены, что хотите отозвать сертификат «[ФИО Пользователя]»?». 3. Пользователь обязан выбрать причину в выпадающем списке **Причина отзыва** (доступны варианты: «Прекращение деятельности», «Замена сертификата», «Компрометация ключа» и др.). 4. Нажмите красную кнопку **«ОТОЗВАТЬ»** (или «ОТМЕНА» для возврата к карточке). После этого статус подписи мгновенно меняется на аннулированный.

Окно подтверждения отзыва сертификата с выбором причины.



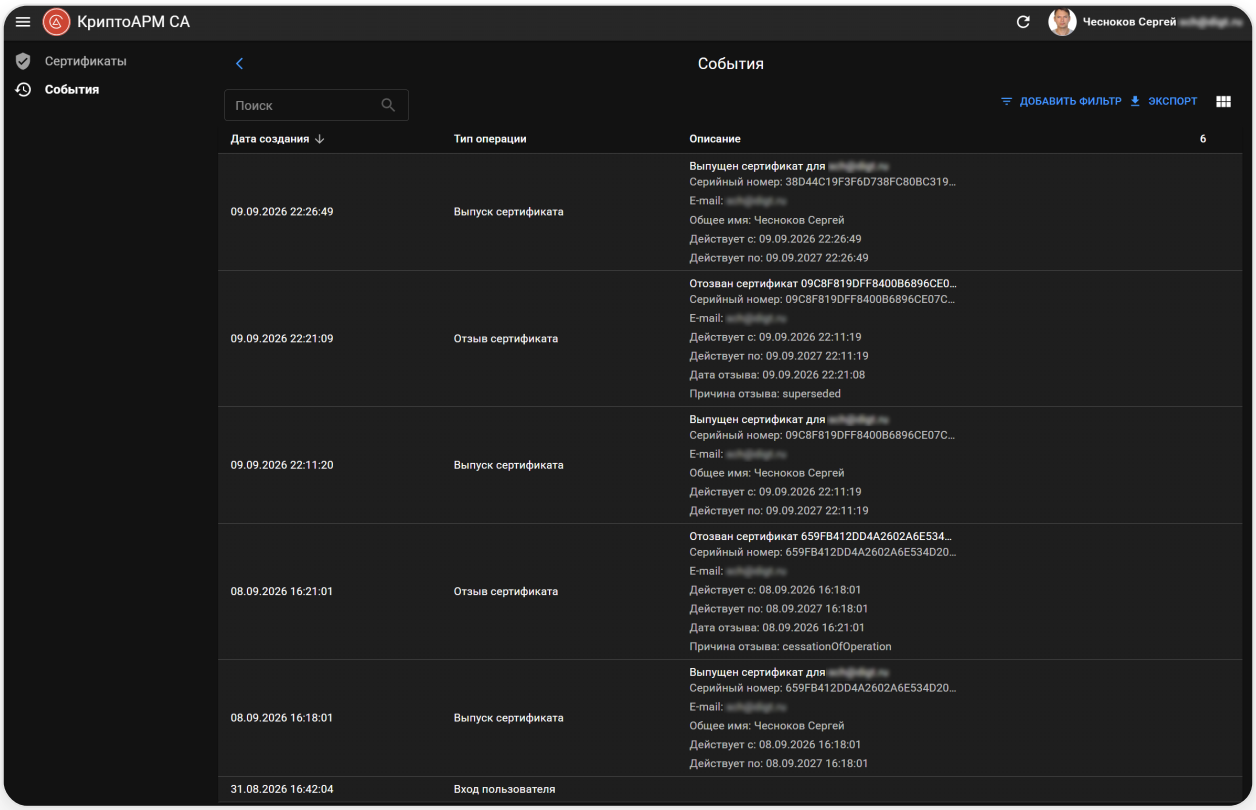
6. Персональный журнал событий

Раздел **«События»** служит инструментом личного контроля безопасности. Пользователь видит изолированный список логов, что позволяет вовремя отследить несанкционированный доступ к его кабинету. В верхнем правом углу выводится общее количество зафиксированных операций (например, 6).

Таблица аудита включает следующие столбцы: * **Дата создания ↓** — точное время фиксации действия с индикатором сортировки по убыванию. * **Тип операции** — стандартизированная категория («Вход пользователя», «Выпуск сертификата», «Отзыв сертификата»). * **Пользователь** — в режиме личного кабинета данная колонка остается пустой, так как журнал изолирован под текущую учетную запись. * **Описание** — подробный технический лог. В описании фиксируются: серийный номер документа, e-mail, общее имя владельца, сроки действия `Действует с/по`, а в случае отзыва — точный программный код причины (например, `Причина отзыва: superseded` при плановой замене или `Причина отзыва: cessationOfOperation` при прекращении деятельности).

Над таблицей пользователю доступны: строка поиска, кнопка **«ДОБАВИТЬ ФИЛЬТР»**, кнопка **«ЭКСПОРТ»** и переключатель отображения интерфейса.

Журнал персональных событий безопасности.



Открыть статью на сайте

Справочник REST API

Справочник REST API

Базовая версия API — `v1`; доступны `/api/v1/*` и `/api/*`. Спецификация — OpenAPI 3.x.

Авторизация

Поддерживаются `X-API-KEY`, `Authorization: Bearer <token>` и cookie-сессия после OIDC-входа.

Конвенции

Мутирующие `POST/PUT/PATCH` принимают `Idempotency-Key`. Повтор с тем же ключом и телом возвращает исходный ответ и может содержать `Idempotency-Replayed: true`.

Списки используют `range`, `sort`, `filter`; ответы содержат `X-Total-Count` и `Content-Range`. При превышении лимита — `429` и `Retry-After`, `RateLimit-*`.

Ошибки имеют форму `{"error":{"code","message","field?","hint?","details?"}}`; ответы содержат `X-Request-Id`.

Discovery

- `GET /api/health` — liveness;
- `GET /api/ready` — readiness и проверка БД;
- `GET /api/version` — версия;
- `GET /openapi.json` и `GET /.well-known/openapi.json` — OpenAPI;
- `GET /llms.txt` — карта ресурсов;
- `/api` — интерактивная документация / Try it out.

Аутентификация

`GET /api/auth`, `POST /api/login`, `GET /api/login`, `POST|GET /api/logout`, `GET /api/profile`, `GET /api/auth/jwt`, `GET /api/auth/callback`.

Пользователи

`GET/POST /api/users`, `GET/PUT/DELETE /api/users/{id}`.

Сертификаты

Метод	Назначение
`GET /api/certificates`	список

Метод	Назначение
`POST /api/certificates`	выпуск
`POST /api/certificates/issue`	выпуск, алиас
`GET /api/certificates/{id}`	просмотр
`GET /api/certificates/{id}/download`	скачивание
`PUT /api/certificates/{id}`	отзыв
`PUT /api/certificates/{id}/pin`	смена PIN PFX
`GET /api/events`	аудит

Десктопный адаптер

`POST /api/operations/start`, `POST /api/operations/params`, `POST /api/operations/upload`, `GET /api/operations/result`.

Связь GUI и API

Список → `GET /api/certificates`; выпуск → `POST /api/certificates`; просмотр → `GET /api/certificates/{id}`; скачивание → `/download`; отзыв → `PUT /api/certificates/{id}`; PIN → `/pin`; аудит → `GET /api/events`.

Открыть статью на сайте

Часто задаваемые вопросы

FAQ

Нужен ли Microsoft CA?

Нет. КриптоАРМ CA является самостоятельным корпоративным УЦ.

Нужен ли Windows Server?

Нет для контейнерного стека: исходная инструкция предусматривает Linux-контейнеры Docker и перечисляет поддерживаемые ОС.

Какие лицензии нужны?

КриптоАРМ CA (`ca-core`), КриптоАРМ Документы, КриптоАРМ Server (`TRUSTED_LICENSE`) и КриптоПро CSP 5.0+.

Можно ли выпускать без оператора?

Да, через Unattended. При коллизии заявка может перейти на ручную проверку.

Что доступно оператору в GUI?

Просмотр списка сертификатов, выпуск, просмотр карточки, скачивание, смена PIN PFX, отзыв с выбором причины и просмотр событий. Подробно: 07-ui-guide-ca.md.

Как отозвать сертификат?

Открыть карточку → **«Отозвать»** → выбрать причину → подтвердить → проверить статус и событие.

Какие причины отзыва показаны?

Замена сертификата, компрометация ключа, прекращение деятельности, изменение принадлежности, не указана, компрометация УЦ, приостановление.

Как проверить API?

`/api/health`, `/api/ready`, `/api/version`, `/openapi.json`.

Что делать при «подпись не доверяется»?

Проверить корневой сертификат в `server/certs/root/` и перезапустить `cryptoarm-server`.

Что делать при 401 от Server?

Проверить `AUTH_MODE=apikey` и совпадение ключей `documents/server`.

Что делать при OIDC loop?

Проверить Client ID/Secret, Redirect URI и `TRUST_PROXY=true`.

Открыть статью на сайте

Глоссарий

Глоссарий

УЦ и сертификаты

Исполняющий УЦ — `ca-core`, выполняющий генерацию, подписание, отзыв и публикацию сертификатов.

Именной сертификат — X.509-сертификат физического лица с атрибутами вроде ФИО, СНИЛС, ИНН, Email.

Сертификат ИС — технологический сертификат для TLS или автоматической подписи; может использовать FQDN вместо персональных данных.

RA / Registration Authority — Центр регистрации; в экосистеме роль выполняет КриптоАРМ IDM.

CRL — подписанный УЦ список отозванных/приостановленных сертификатов.

OCSP — протокол проверки статуса сертификата в реальном времени.

Криптография

ГОСТ-алгоритмы — российские криптографические стандарты, поддерживаемые через КриптоПро CSP.

RSA/ECDSA — международные асимметричные алгоритмы, поддержка которых в исходных материалах связана с OpenSSL 3.x.

Автоматизация

Unattended — автоматический выпуск по API без непосредственного участия оператора.

Auto-Rollover — плановый перевыпуск сертификата за 30 дней до окончания действия.

Idempotency-Key — ключ, предотвращающий дублирование результата при повторе мутирующего API-запроса.

Роли и интерфейс

Администратор — пользователь с правами настройки и обслуживания системы.

Оператор — пользователь, выполняющий операции жизненного цикла сертификатов.

RBAC — управление доступом на основе ролей.

Карточка сертификата — экран с атрибутами, сроками, статусом и действиями над сертификатом.

Событие — запись аудита об операции пользователя или системы.