Документация

КриптоАРМ ID

ООО «Цифровые технологии»
Версия 1.0
2026 г.

Документация

Оглавление

Введение

- Описание системы

Установка и первый запуск

- Установка и первый запуск
- Настройка переменных окружения

Администрирование системы

- Настройка системы (интерфейс, безопасность и доступ)
- Настройка профиля пользователя
- Управление лицензиями
- Настройка мини-виджета
- Управление пользователями

Организация

- Управление своей организацией

Приложения

- Управление приложениями

Настройка способов входа

- Настройка способов входа
- Настройка доверенных провайдеров

Инструкции для подключения способов входа

- Вход через 1С
- Вход через ALD Pro
- Вход через LDAP
- Вход через ЕСИА
- Вход через Email
- Вход через HOTP
- Вход через Mail.ru
- Вход через mTLS
- Вход через OIDC

- Вход через TOTP
- Вход через ВКонтакте
- Вход через WebAuthn
- Вход через Яндекс

Руководство пользователя

- Регистрация и вход
- Личный профиль

Введение

Описание системы

КриптоАРМ ID — это Single Sign-On (SSO) система для централизованной аутентификации пользователей и управления доступом к корпоративным приложениям.

Система обеспечивает безопасную централизованную аутентификацию с поддержкой SSO, OAuth 2.0, OpenID Connect и двухфакторной аутентификацией.

Для каких задач подходит КриптоАРМ ID

КриптоАРМ ID — система для организации централизованного входа пользователей на корпоративные информационные ресурсы с использованием единой учетной записи.

КриптоАРМ ID ориентирован на компании, которым требуется:

- **Единое окно входа** для внутренних и внешних сервисов
- **Централизованное управление доступом** для разных категорий пользователей (сотрудники, подрядчики, клиенты)
- **Повышенная безопасность** с поддержкой многофакторной аутентификации
- **Строгий контроль и аудит** действий пользователей
- **Безопасная интеграция** множества приложений с разными системами аутентификации

Основные возможности КриптоАРМ ID

1. Аутентификация и вход

Система обеспечивает централизованную аутентификацию и поддержку нескольких протоколов и методов аутентификации.

Поддерживаемые протоколы

- **OpenID Connect (OIDC)** — аутентификация пользователей и передача идентификационных данных
- **OAuth 2.0** — авторизация и управление доступом к ресурсам

Методы аутентификации

- **Базовые методы**: логин и пароль, электронная почта,
- **Внешние провайдеры идентификации**: социальные сети, доверенные корпоративные системы и другие сервисы,

- **Усиленные и беспарольные методы:** криптографическая аутентификация через **mTLS** (клиентские сертификаты) и **WebAuthn** (биометрия, аппаратные ключи), а также одноразовые пароли **TOTP/HOTP**.

Двухфакторная аутентификация (2FA / MFA)

КриптоАРМ ID поддерживает многофакторную аутентификацию (MFA), при которой доступ предоставляется только после успешного подтверждения личности пользователя несколькими независимыми факторами (знание, владение, биометрия).

2. Управление приложениями и пользователями

- **Создание и настройка приложений:** веб-приложения, нативные мобильные приложения
- **Кастомизация виджета:** настройка внешнего виджета аутентификации под бренд компании
- **Управление пользователями:** регистрация, редактирование, блокировка, смена паролей

3. Безопасность и аудит

- **Разграничение прав доступа**
- **Подробное журналирование** всех событий и действий

4. Мини-виджет

Лёгкий JavaScript-компонент, который обеспечивает быстрый доступ к функциям аутентификации и информации о пользователе. Легко встраивается в любые веб-сайты и интерфейсы и предоставляет переход к профилю, кабинету организации и приложениям.

Уровни доступа

Система предоставляет гибкую модель ролевого доступа:

Роль	Полномочия	Для кого предназначена
Администратор сервиса	Полный доступ ко всем приложениям, пользователям и глобальным настройкам	Администраторы системы, суперпользователи

Роль	Полномочия	Для кого предназначена
Управленец	Управление приложениями и способами входа своей организации/ подразделения	Руководители отделов, менеджеры проектов
Администратор приложения	Управление конкретными приложениями и их пользователями	Разработчики, администраторы приложений
Участник	Управление своим профилем и разрешениями на доступ к личным данным	Обычные пользователи, сотрудники

Модули системы КриптоАРМ ID

1. Профиль

Модуль «Профиль» обеспечивает управление персональными данными пользователя и настройками доступа. Включает функции редактирования личной информации, настройки приватности, управления правами приложений, а также просмотра журнала активности. Также модуль предоставляет доступ к каталогу публичных приложений.

2. Кабинет администратора

Модуль «Кабинет администратора» предназначен для централизованного управления системой **КриптоАРМ ID**. Включает функции настройки глобальных параметров системы, методов аутентификации и внешнего вида страницы входа. В модуле можно управлять приложениями и учетными записями пользователей, а также отслеживать их активность через единый журнал событий.

3. Кабинет организации

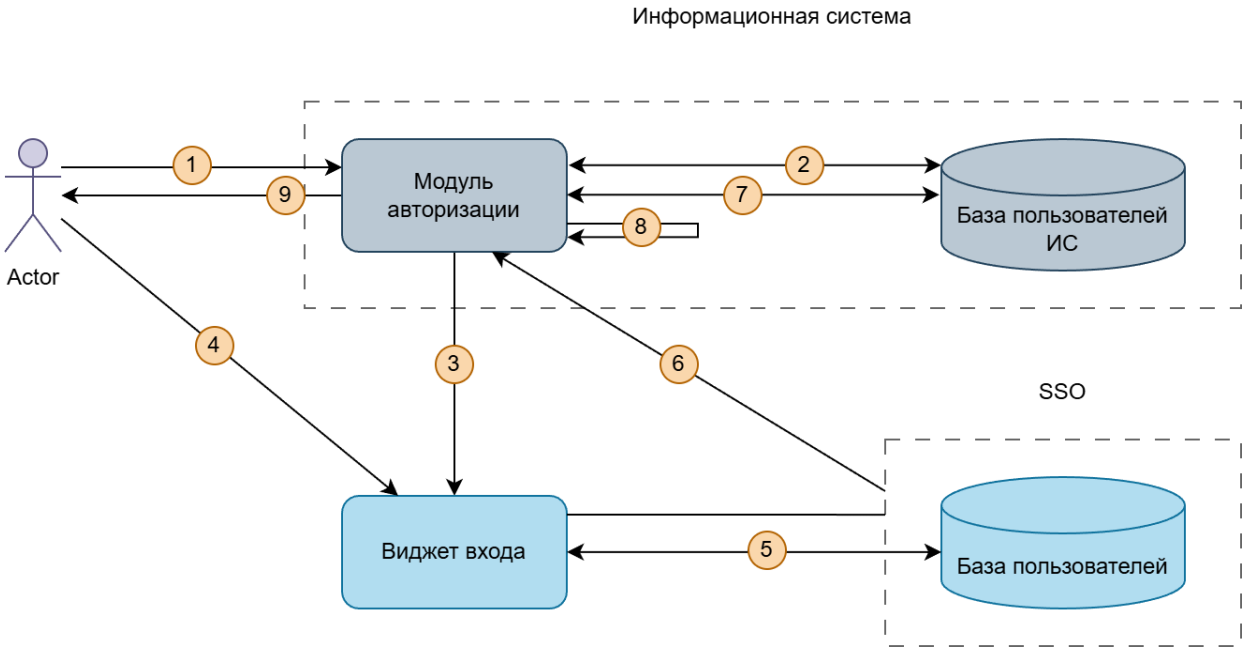
Модуль «Кабинет организации» обеспечивает управление приложениями, методами аутентификации и политиками доступа в рамках организации. Включает настройку параметров организации, конфигурацию способов входа, управление приложениями организации и мониторинг активности пользователей.

4. Кабинет приложения (ADM)

Модуль «Кабинет приложения» предназначен для администрирования отдельных приложений. Содержит функции управления назначенными приложениями и контроля активности пользователей, имеющих доступ к данным приложениям.

Концепция и принципы работы КриптоАРМ ID

Общая схема взаимодействия

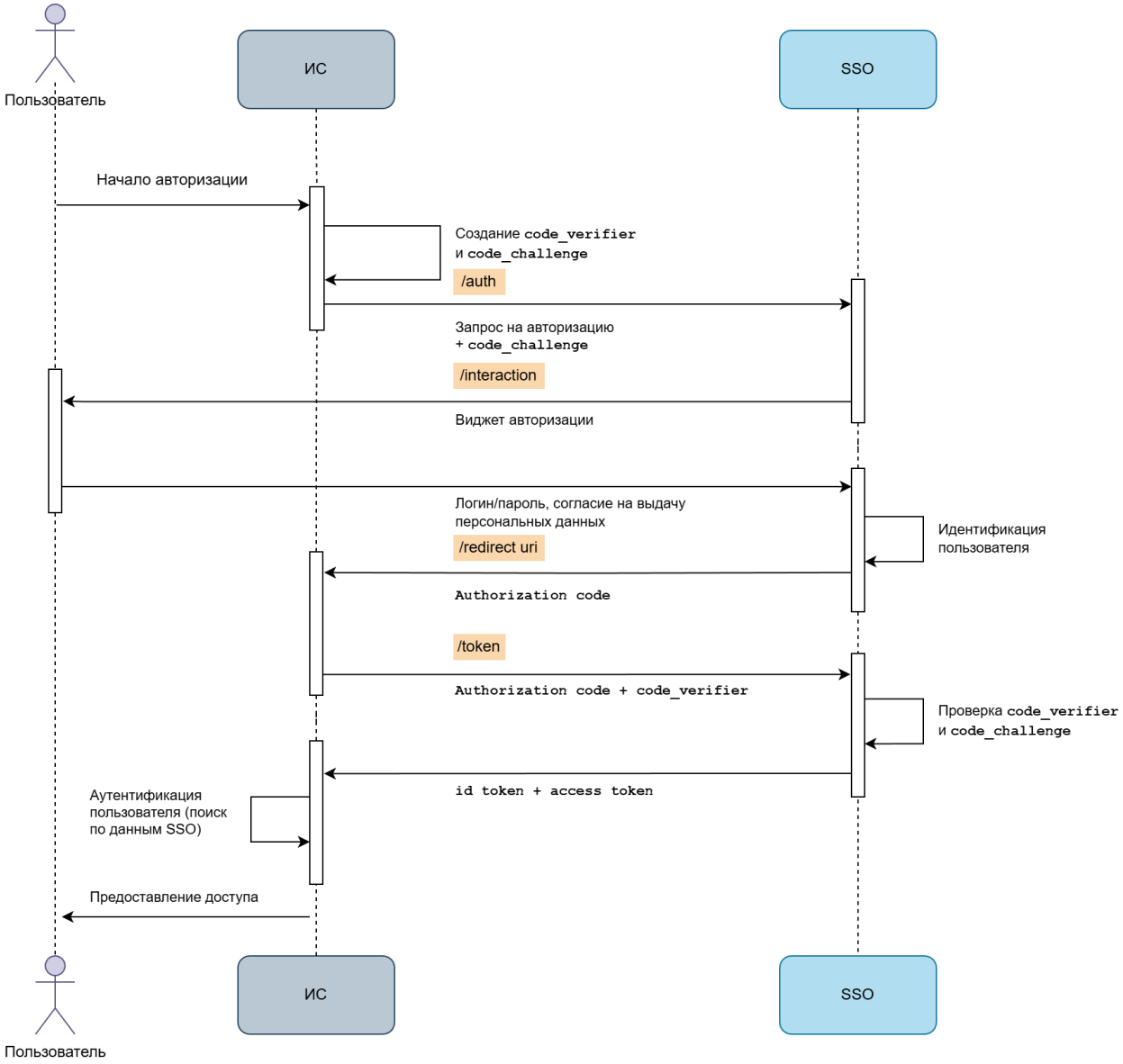


Последовательность взаимодействия:

1. **Запрос доступа** — пользователь обращается к информационной системе (ИС).
2. **Проверка в БД ИС** — система проверяет наличие пользователя.
3. **Перенаправление на виджет** — пользователь направляется в **КриптоАРМ ID**.
4. **Аутентификация** — пользователь проходит процедуру входа.
5. **Проверка в БД КриптоАРМ ID** — валидация учетных данных.
6. **Предоставление профиля** — возврат данных пользователя.
7. **Сопоставление в ИС** — поиск пользователя по данным из **КриптоАРМ ID**.
8. **Проверка прав** — авторизация в целевой системе.
9. **Предоставление доступа** — успешный вход в систему.

> 📌 **Требования для интеграции:** Для подключения информационной системы к **КриптоАРМ ID** необходимо наличие базы данных пользователей и модуля авторизации, поддерживающего OpenID Connect или OAuth 2.0.

Схема авторизации по OpenID Connect

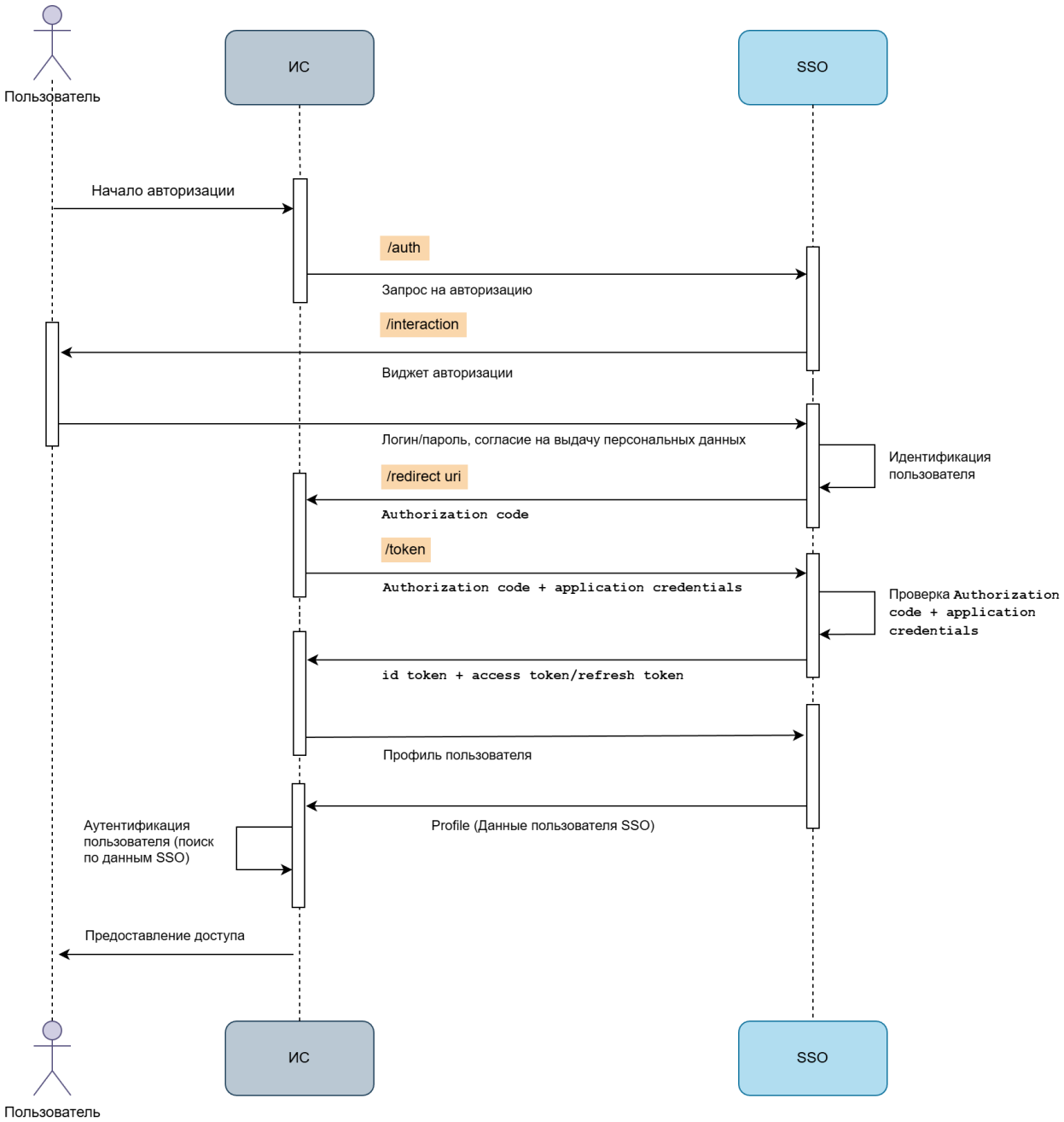


Ключевые этапы OIDC:

1. Пользователь обращается к ИС.
2. ИС (клиент) генерирует `code_verifier` и `code_challenge`.
3. ИС перенаправляет пользователя на `/authorize` **КриптоАРМ ID**.
4. Пользователь перенаправляется на виджет авторизации **КриптоАРМ ID**.
5. Пользователь вводит логин/пароль и предоставляет согласие на передачу данных.
6. Выполняется проверка пользователя в БД **КриптоАРМ ID**.
7. Перенаправление пользователя обратно в ИС (клиент) с `Authorization code`.
8. ИС отправляет запрос на `/token` в **КриптоАРМ ID**.
9. Проверка `code_challenge` and `code_verifier` в **КриптоАРМ ID**.
10. Предоставление в ИС `id token`, содержащего профиль пользователя **КриптоАРМ ID**, и `access token` (опционально `refresh token`).
11. Аутентификация пользователя ИС.

12. Пользователь получает доступ к ИС.

Схема авторизации по OAuth 2.0

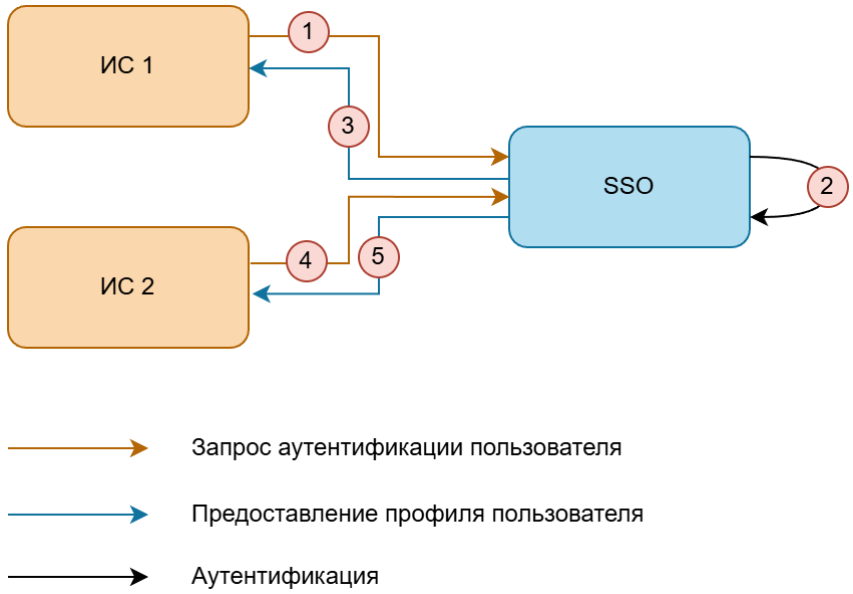


Особенности OAuth 2.0 потока:

1. Пользователь обращается к ИС.
2. ИС перенаправляет пользователя на `/authorize` **КриптоАРМ ID**.
3. Пользователь перенаправляется на виджет авторизации **КриптоАРМ ID**.
4. Пользователь вводит логин/пароль и предоставляет согласие на передачу данных.
5. Выполняется проверка пользователя в БД **КриптоАРМ ID**.
6. **КриптоАРМ ID** перенаправляет пользователя обратно в ИС с `Authorization code` на `Redirect_URI`.
7. ИС отправляет запрос на `token` по `Authorization code`.

8. **КриптоАРМ ID** валидирует запрос.
9. **КриптоАРМ ID** возвращает токены `id token` и `access token` (опционально `refresh token`).
10. ИС запрашивает профиль пользователя.
11. **КриптоАРМ ID** предоставляет профиль пользователя.
12. ИС валидирует ответы и устанавливает локальную сессию пользователя.
13. Пользователь получает доступ к ИС.

Схема Single sign-on (SSO)



Типичный сценарий:

1. Запрос доступа к ИС1.
2. Аутентификация пользователя в **КриптоАРМ ID**.
3. Предоставление профиля пользователя **КриптоАРМ ID** в ИС1.
4. Запрос доступа к ИС2.
5. Предоставление профиля пользователя **КриптоАРМ ID** в ИС2 без повторной процедуры аутентификации пользователя.

Установка и первый запуск

Установка

Требования к установке

Системные требования сервера

Перед установкой системы **КриптоАРМ ID** убедитесь, что ваша инфраструктура соответствует требованиям.

Системные требования зависят от планируемой нагрузки. Для тестовых сред достаточно минимальной конфигурации, для production-среды лучше использовать рекомендованные параметры.

Минимальная конфигурация

Компонент	Требования
Оперативная память (RAM)	4 ГБ
Дисковое пространство	50 ГБ SSD
Процессор (CPU)	2 ядра x86_64
Сетевой интерфейс	1 Гбит/с

Рекомендуемая конфигурация

Компонент	Требования
Оперативная память (RAM)	8 ГБ и более
Дисковое пространство	100 ГБ SSD/NVMe
Процессор (CPU)	4+ ядра x86_64
Сетевой интерфейс	1 Гбит/с и выше

> **Совет:** Для высоконагруженных систем с тысячами пользователей рекомендуется:
>
> - 16+ ГБ оперативной памяти
> - 8+ ядер процессора
> - Использование NVMe дисков для максимальной скорости работы БД

Требования к программному обеспечению

Программное обеспечение

Компонент	Поддерживаемые версии	Дополнительная информация
Операционная система	Ubuntu 18.04 LTS (Bionic Beaver), Ubuntu 20.04 LTS (Focal Fossa), Debian 11 (Bullseye)	Любой linux-дистрибутив с поддержкой Docker
Docker Engine	19.03+	-
Docker Compose	1.27+	-
Nginx/Apache	Любая современная версия	-

Общие требования

Для успешной установки и корректной работы **КриптоАРМ ID** необходимо выполнить несколько условий:

- Наличие сервера с постоянным IP-адресом.
- Доступ ко всем рабочим станциям через порт, который будет использоваться для доступа к системе.
- Наличие сервера электронной почты (SMTP-сервера).
- Подключение к сервису должно осуществляться по протоколу HTTPS.

Установка Docker и Docker Compose

КриптоАРМ ID разворачивается в виде набора Docker-контейнеров и может использоваться как корпоративный OAuth 2.0 Authorization Server и OpenID Connect Provider (IdP).

> Документация Docker

Шаг 1. Установка Docker Engine

Для Ubuntu/Debian:

```
# Обновление пакетов
sudo apt update && sudo apt upgrade -y
```

```
# Установка зависимостей
sudo apt install -y apt-transport-https ca-certificates curl
software-properties-common

# Добавление GPG-ключа Docker
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg -
-dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg

# Добавление репозитория
echo "deb [arch=$(dpkg --print-architecture) signed-
by=/usr/share/keyrings/docker-archive-keyring.gpg]
https://download.docker.com/linux/ubuntu $(lsb_release -cs) stable"
| sudo tee /etc/apt/sources.list.d/docker.list > /dev/null

# Установка Docker
sudo apt update
sudo apt install -y docker-ce docker-ce-cli containerd.io

# Проверка установки
sudo docker --version
```

Для CentOS/RHEL:

```
# Установка yum-utils
sudo yum install -y yum-utils

# Добавление репозитория Docker
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo

# Установка Docker
sudo yum install -y docker-ce docker-ce-cli containerd.io

# Запуск и автозагрузка Docker
sudo systemctl start docker
sudo systemctl enable docker

# Проверка установки
sudo docker --version
```

Шаг 2. Установка Docker Compose

```
# Скачивание Docker Compose
sudo curl -L
"https://github.com/docker/compose/releases/latest/download/docker-
compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose

# Установка прав на исполнение
sudo chmod +x /usr/local/bin/docker-compose

# Проверка установки
docker-compose --version
```

> Требования к версиям: **Docker Engine 20.10+** и **Docker Compose 1.29+**. Для проверки используйте команды `docker --version` и `docker-compose --version`.

Установка SSO системы

Шаг 1. Подготовка рабочей директории

Создайте и перейдите в директорию для установки:

```
# Создание директории
mkdir trusted-id && cd trusted-id

# Проверка текущего пути
pwd  # Должно отобразить: /home/ваш_пользователь/trusted-id
```

Шаг 2. Загрузка конфигурационных файлов

Загрузите необходимые файлы конфигурации:

```
# Загрузка основных файлов
curl -O https://git.digtlab.ru/trusted/id/-/raw/main/docker-
compose.yaml
curl -O https://git.digtlab.ru/trusted/id/-/raw/main/nginx.conf
curl -O https://git.digtlab.ru/trusted/id/-/raw/main/build.sh
curl -O https://git.digtlab.ru/trusted/id/-/raw/main/.env

# Проверка загрузки
ls -la
```

Скачанные файлы:

Файл	Назначение
docker-compose.yaml	Конфигурация Docker-контейнеров
nginx.conf	Настройки веб-сервера Nginx
build.sh	Скрипт настройки и сборки
.env	Переменные окружения и настройки

Шаг 3. Настройка прав доступа

Сделайте скрипт сборки исполняемым:

```
# Установка прав на скрипт сборки
chmod +x ./build.sh

# Проверка прав
ls -l build.sh
```

Шаг 4. Настройка конфигурации

Отредактируйте файл `.env` с основными настройками:

```
# Открываем файл для редактирования (используйте nano или vim)
nano .env
```

Обязательные настройки:

```
# Основной домен системы
ID_HOST=id.example.ru  # Замените на ваш домен или IP

# Email администратора
ADMIN_MAIL=example@mail.ru  # Замените на реальный email
```

Шаг 5. Запуск скрипта сборки

Запустите скрипт настройки:

```
./build.sh
```

В результате выполнения в файле **nginx.conf** прописывается значение переменной **ID_HOST** и в файле **.env** прописываются переменные **CLIENT_ID** и **CLIENT_SECRET**.

Шаг 6. Запуск системы

Запустите проект:

```
docker compose up -d
```

Полезные команды Docker Compose

Команда	Описание	Пример использования
Просмотр логов	Отслеживание логов в реальном времени	`docker compose logs -f`
Остановка	Остановка всех контейнеров	`docker compose stop`
Запуск	Запуск остановленных контейнеров	`docker compose start`
Перезагрузка	Перезапуск всех контейнеров	`docker compose restart`
Статус	Просмотр состояния контейнеров	`docker compose ps`

Первый вход в систему

Учетные данные администратора по умолчанию

После установки создается административный аккаунт с правами **Администратор**:

- **Логин** — `root`,
- **Пароль** — `changethis`,
- **Роль** — **Администратор**.

> 📌 Эти данные предоставляют полный доступ к системе. Обязательно измените пароль сразу после первого входа.

Первый вход

Для входа в веб-интерфейс **КриптоАРМ ID** необходимо перейти по адресу: `https://ID_HOST`.

1. На первом шаге виджета входа введите логин и нажмите **Войти**.
2. Введите пароль на втором шаге и нажмите **Войти**.

Переход в кабинет администратора

Настройки администрирования размещены в кабинете администратора.

Чтобы перейти в кабинет:

1. Нажмите на свое имя в правом верхнем углу окна.
2. В открывшемся окне мини-виджета нажмите на название сервиса **КриптоАРМ ID**.
3. Вы будете перенаправлены в **Кабинет администратора**.

Настройка переменных окружения

> 💡 Чтобы изменить переменные окружения, нужно внести изменения в файл **docker-compose.yml**.

Общие переменные окружения

Эти переменные определяют базовое поведение и идентификацию сервиса.

Переменная	Описание	Значение по умолчанию
`NODE_ENV`	Среда выполнения приложения (`development` или `production`)	`production`
`DOMAIN`	Домен сервиса	—
`ADMIN_LOGIN`	Логин администратора	`root`
`ADMIN_PASSWORD`	Пароль администратора	`changethis`
`DELETE_PROFILE_AFTER_DAYS`	Количество дней, через которое профиль пользователя будет удален	`30`
`CLIENT_ID`	Уникальный идентификатор приложения (рекомендуется UUID)	—
`CLIENT_SECRET`	Уникальный секрет приложения (рекомендуется UUID)	—

Переменная	Описание	Значение по умолчанию
`MANUAL_URL`	Ссылка на документацию для пользователей	`https://ваш-домен/docs/`

> ⚠ Переменные `CLIENT_ID` и `CLIENT_SECRET` используются для идентификации **КриптоАРМ ID** как OAuth 2.0 / OpenID Connect клиента и должны храниться в секрете.

Переменные окружения базы данных (PostgreSQL)

Параметры для подключения к СУБД PostgreSQL.

Переменная	Описание	Значение по умолчанию
`POSTGRES_USER`	Имя пользователя для подключения к PostgreSQL	`user`
`POSTGRES_PASSWORD`	Пароль пользователя PostgreSQL	`password`
`POSTGRES_DB`	Название базы данных	`mydb`
`POSTGRES_HOST`	Хост базы данных	`localhost`
`POSTGRES_PORT`	Порт подключения к базе	`5432`
`DATABASE_URL`	Полная строка подключения в формате PostgreSQL	—

Redis, сессии и OIDC cookies

Настройки для хранения сессий, кэширования данных и безопасности аутентификации.

Переменная	Описание	Значение по умолчанию
`REDIS_HOST`	Хост Redis	`127.0.0.1`
`REDIS_PORT`	Порт Redis	`6379`
`OIDC_COOKIE_SECRET`	Секрет для подписи и проверки cookie	—
`OIDC_SESSION_TTL`	Время жизни сессии в секундах	`86400` (24 часа)

Ограничение скорости и логирование

Настройки для защиты от злоупотреблений и контроля логирования.

Переменная	Описание	Значение по умолчанию
`RATE_LIMIT`	Количество запросов для ограничения скорости	`15`
`RATE_LIMIT_TTL_SEC`	Период времени в секундах для лимита	`900`
`CONSOLE_LOG_LEVELS`	Уровни логирования для консоли	`log warn error`

Почта и уведомления

Настройки SMTP-сервера для отправки писем (подтверждение регистрации, сброс пароля и т.д.).

Переменная	Описание	Значение по умолчанию	Пример
`EMAIL_PROVIDER`	Настройки почтового провайдера в формате JSON	—	`{"hostname":"smtp.example.com", "port":465, "root_mail":"admin@example.com", "password":"SecretPass"}`

Кастомизация интерфейса

Внешний вид кнопок, ссылок и вкладок настраивается через JSON-объект в переменной `CUSTOM_STYLES`.

Переменная `CUSTOM_STYLES` позволяет кастомизировать интерфейс **КриптоАРМ ID** без изменения кода.

```
# Перейдите в папку проекта
cd /home/els/nodetrustedserverconfig

# Остановите сервис перед изменением
docker compose stop

# Отредактируйте .env файл
nano .env
```

```
# Пример минимальной кастомизации
CUSTOM_STYLES=`{"palette":{"white":
{"accent":"#2c5aa0","accentHover":"#1e3a6f"}},"button":
{"borderRadius":"8px"}}`

# Запустите сервис снова
docker compose up -d
```

Описание переменной `CUSTOM_STYLES`:

Переменная	Описание	Пример
`CUSTOM_STYLES`	Настройки внешнего вида интерфейса, включая цвета, стили кнопок и виджетов. Значение должно быть строго JSON в одну строку.	`CUSTOM_STYLES={"palette":{"white":{"accent":"#ff6f00", "accentHover":"#f56b00", "onAccentColor":"#fff"}}, "button":{"borderRadius":"4px"}, "widget":{"backgroundColor":"#ff6f00", "color":"#fff", "isHideText":false, "button":{"background":"#ffffff", "hover":"#fadfcd", "color":"#ff6f00"}}, "isAccordionIconColored":true, "contentPosition":"center"}`

Параметр	Описание	Пример
`accent`	Основной цвет акцентных элементов в HEX-формате	`"#ff6f00"`
`accentHover`	Цвет при наведении в HEX-формате	`"#f56b00"`
`onAccentColor`	Цвет текста на акцентном фоне в HEX-формате	`"#fff"`
`secondaryAccent`	Цвет второстепенных элементов в HEX-формате	`"#fae9de"`
`borderColor`	Цвет границ элементов в HEX-формате	`"#858BA0"`
`borderRadius`	Закругление углов кнопок (`button`)	`4px`, `8px` и т.д.
`isAccordionIconColored`	Раскрашивать иконки аккордеона	`true`/`false`

Параметр	Описание	Пример
`contentPosition`	Выравнивание контента	`"start"`, `"center"`, `"end"`

Права и лицензии

Переменная	Описание	Значение по умолчанию	Пример
`COPYRIGHT`	Информация о правах в формате JSON	`{"ru":" ","en":" "}`	`{"ru":"© Компания","en":"© Company"}`

Метрики

Переменная	Описание
`YANDEX_METRICA_ID`	ID для интеграции с Яндекс.Метрикой
`GOOGLE_METRICA_ID`	ID для интеграции с Google Analytics

Администрирование системы

Настройка системы

Настройка интерфейса и локализации

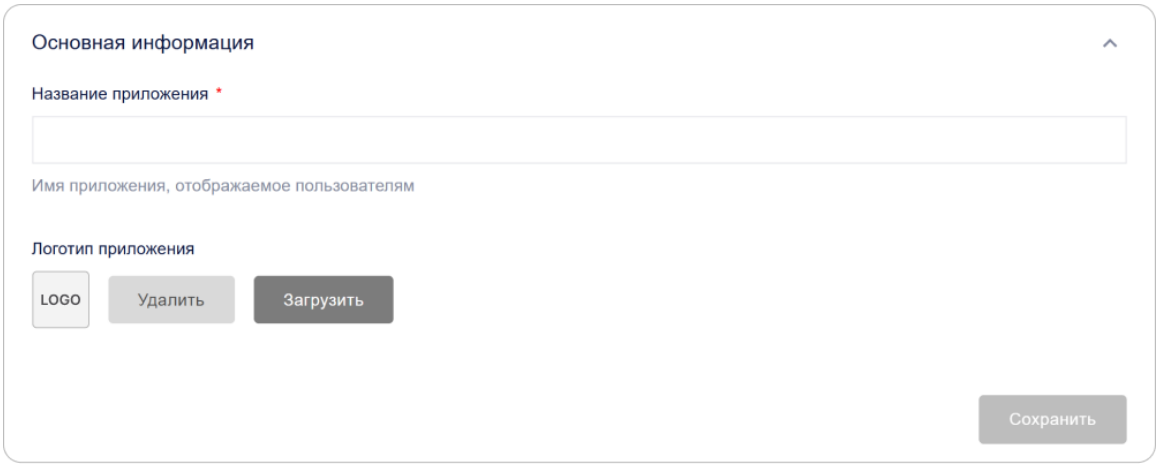
> 💡 Настройка цветов, шрифтов и внешнего вида элементов интерфейса доступна в переменной `CUSTOM_STYLES` в файле `.env`. Подробнее в разделе Настройка переменных окружения.

Настройка названия и логотипа системы

Название и логотип отображаются в интерфейсе системы **КриптоАРМ ID**, а также в мини-виджете и виджете входа.

Чтобы настроить название и логотип:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Основная информация**.



3. Укажите новое название в поле **Название приложения**.
4. В блоке **Логотип приложения** нажмите **Загрузить** и выберите файл с логотипом.

> Допустимые форматы: JPG, GIF, PNG, WEBP; максимальный размер 1 МБ.

5. Настройте отображение и нажмите **Применить**.

6. Нажмите **Сохранить**.

> **Совет:** Используйте SVG-формат для векторного логотипа, чтобы обеспечить четкое отображение на всех устройствах и разрешениях экрана.

Настройка локализации

КриптоАРМ ID поддерживает интерфейс на **шести языках**:

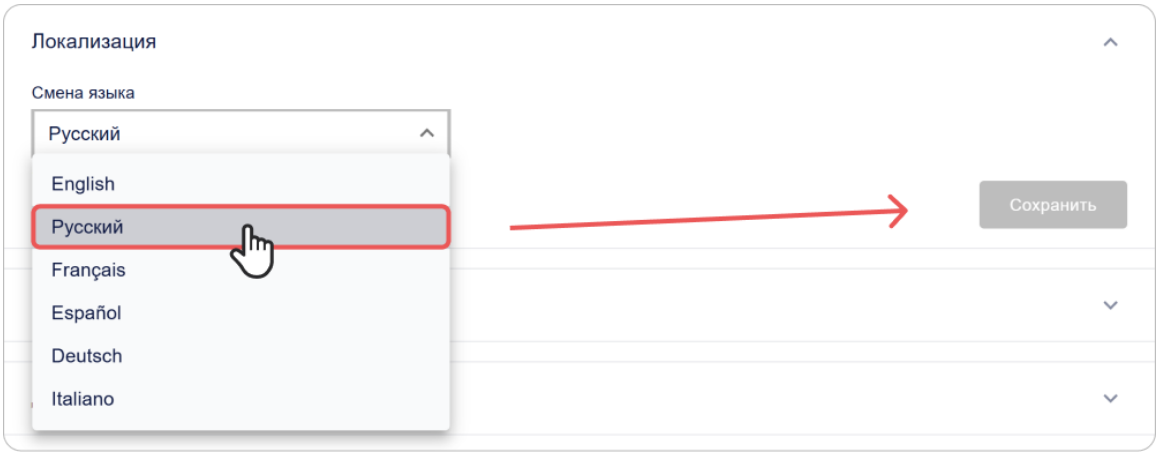
- Русский (ru)
- English (en)
- Français (fr)
- Español (es)
- Deutsch (de)
- Italiano (it)

Выбранный язык влияет на отображение текста во всех интерфейсах **КриптоАРМ ID**, включая виджет входа и мини-виджет.

Если вы используете дополнительные поля профиля пользователя и шаблоны писем — убедитесь, что они отображаются правильно.

Как изменить язык интерфейса

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Локализация** и выберите необходимый язык из списка.



3. Нажмите **Сохранить**.

Изменение языка произойдет автоматически, без перезапуска сервиса или обновления страницы.

> **Предупреждение:** После смены языка все тексты в интерфейсе, включая системные сообщения и уведомления, будут отображаться на выбранном языке. Убедитесь, что ваши пользователи понимают выбранный язык.

Настройка шаблонов email-уведомлений

Шаблоны писем — это заготовки электронных писем, которые содержат предустановленное форматирование и элементы оформления. Они используются для создания автоматических уведомлений, таких как письма о регистрации, восстановлении пароля и других событиях.

Что такое Mustache?

Mustache — это простой шаблонизатор для подстановки данных в текстовые шаблоны. В **КриптоАРМ ID** он используется для:

- Подстановки данных пользователя (`{{user.name}}`),
- Динамического формирования ссылок (`{{confirmation_link}}`),
- Условного отображения блоков.

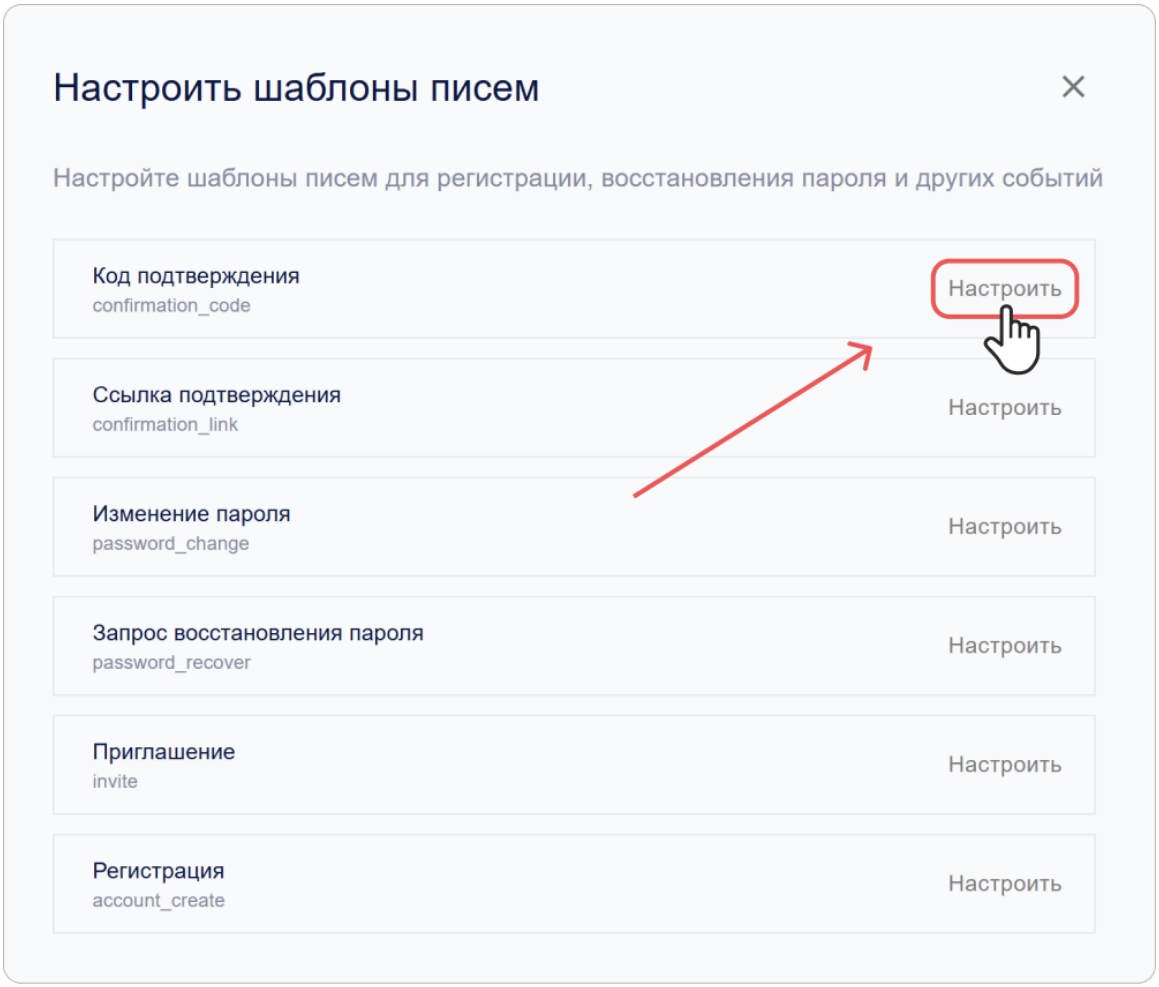
> Официальная документация Mustache

Доступные типы писем

Тип письма	Событие	Назначение
Регистрация	`account_create`	Приветственное письмо новому пользователю
Код подтверждения	`confirmation_code`	Письмо с кодом верификации
Ссылка подтверждения	`confirmation_link`	Письмо с верификационной ссылкой
Изменение пароля	`password_change`	Уведомление о смене пароля
Запрос восстановления пароля	`password_recover`	Письмо с кодом верификации
Приглашение	`invite`	Письмо с приглашением в приложение

Как настроить шаблон

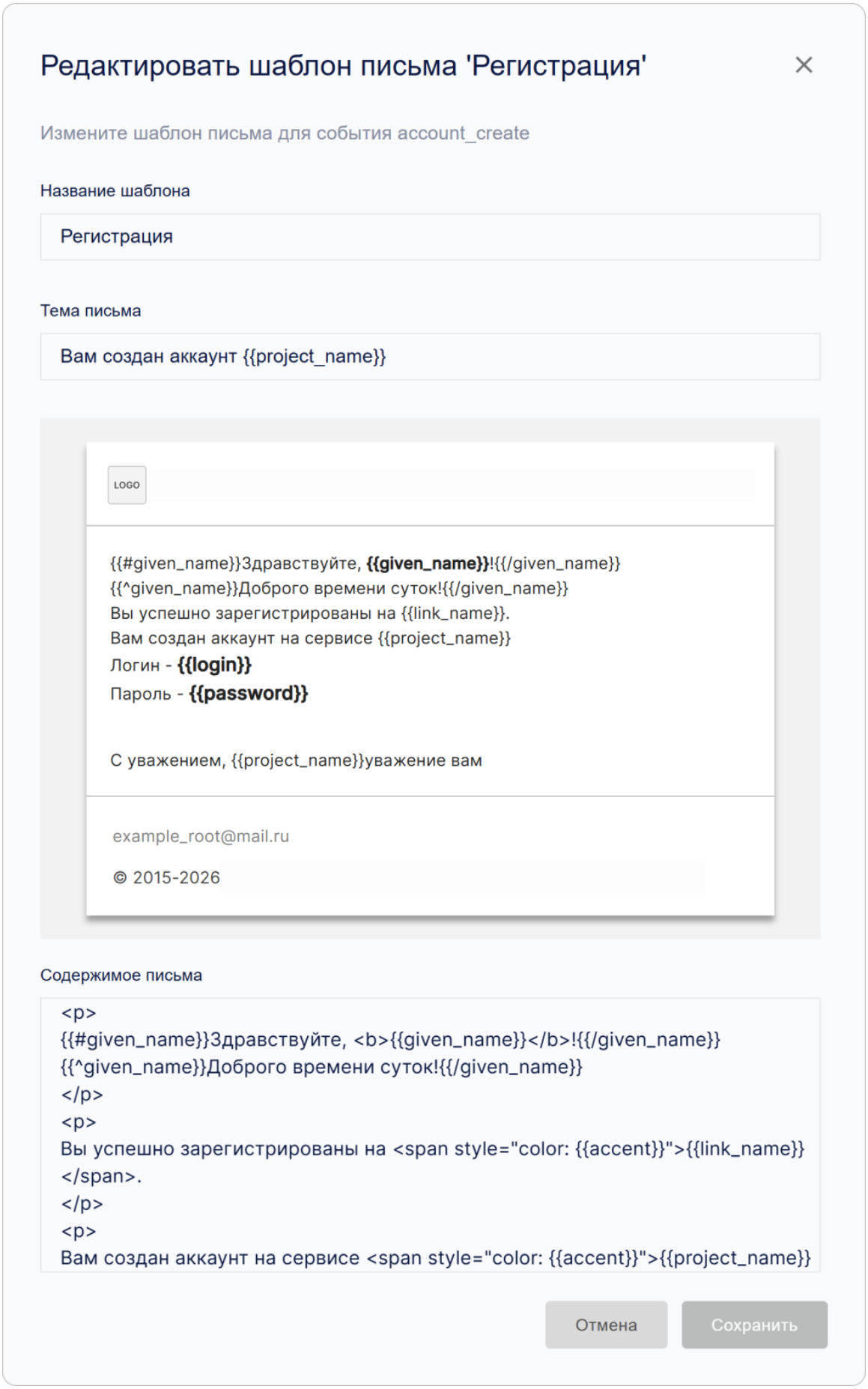
1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Найдите блок **Шаблоны писем** и нажмите **Настроить**.
3. Выберите нужный шаблон и нажмите **Настроить**.



4. В открывшейся форме редактирования укажите:

   - **Название шаблона**,
   - **Тему письма**,
   - **Содержимое письма**.

> 💡 Используйте HTML-разметку и переменные в формате `{{variable_name}}`. Убедитесь, что используемые переменные совпадают с доступными полями профиля пользователя, чтобы избежать ошибок при отправке письма.



5. Нажмите **Сохранить**.

Безопасность и доступ

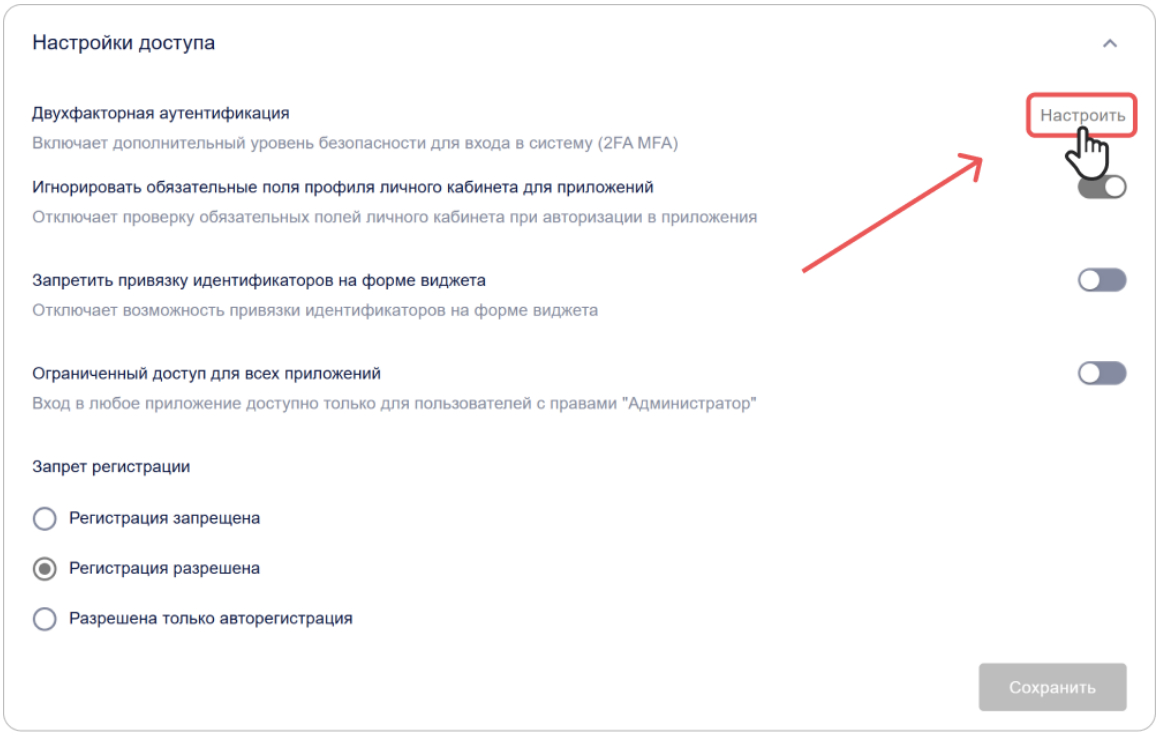
Настройки доступа

Двухфакторная аутентификация

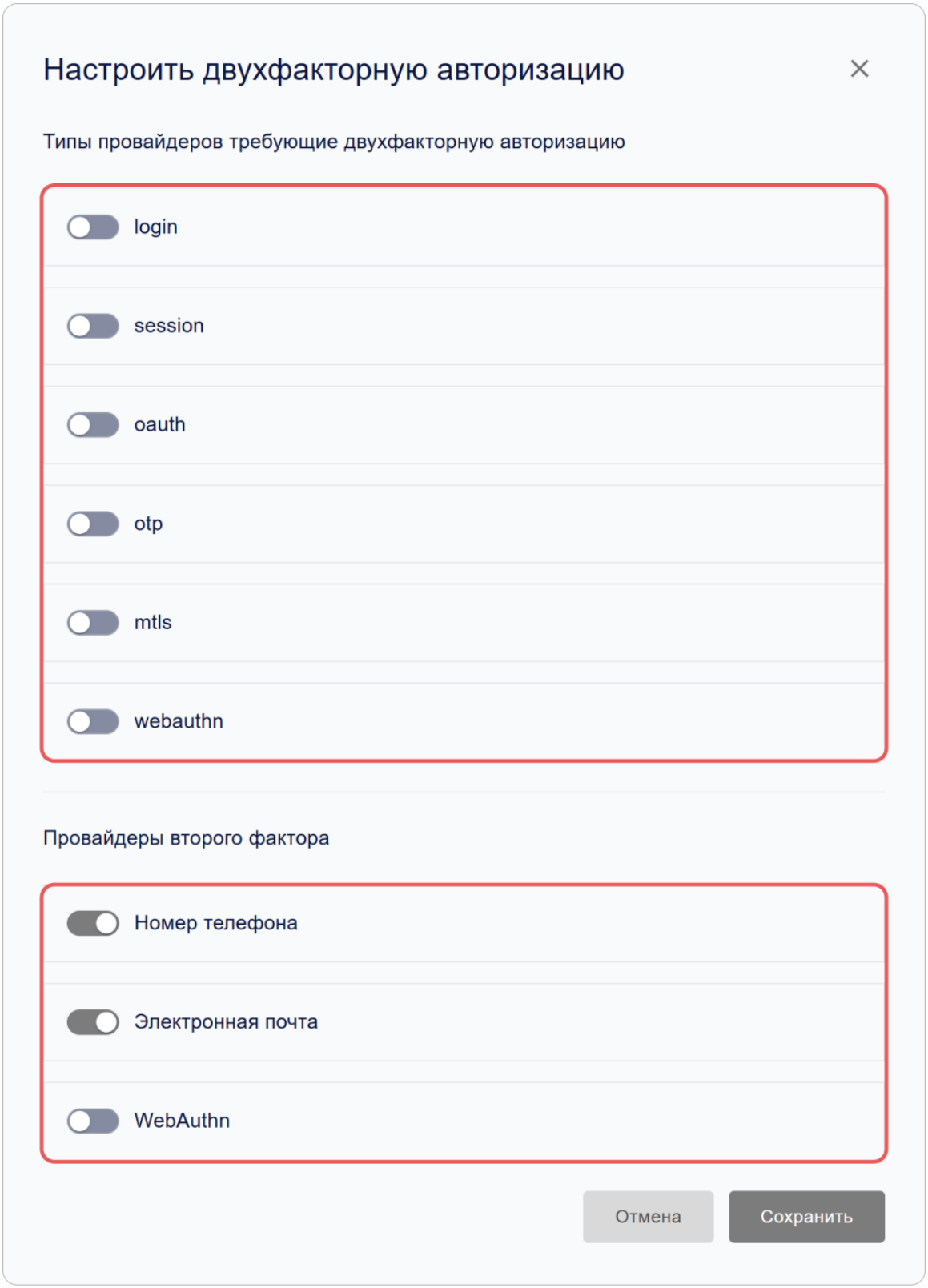
Двухфакторная аутентификация (2FA) добавляет дополнительный уровень защиты при входе в систему. После ввода первого фактора (логин/пароль или другой способ аутентификации) пользователь должен подтвердить свою личность вторым фактором (телефон, электронная почта, WebAuthn).

Как настроить двухфакторную аутентификацию

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа** и нажмите **Настроить**.



3. Укажите провайдеры первого и второго факторов:
    - Провайдер **первого фактора** — основной способ аутентификации (логин/пароль или другой способ аутентификации).
    - Провайдер **второго фактора** — способ подтверждения личности (телефон, e-mail, WebAuthn).



4. Нажмите **Сохранить**.

Игнорирование обязательных полей профиля при входе в приложение

Некоторые поля профиля пользователя (например, телефон, почта и прочие) могут быть отмечены как обязательные для заполнения в личном кабинете.

По умолчанию при авторизации в приложения **КриптоАРМ ID** проверяет наличие всех обязательных полей и может приостанавливать вход, пока пользователь не заполнит недостающие данные. Настройка **Игнорировать обязательные поля профиля личного кабинета для приложений** позволяет отключить эту проверку.

Это может быть полезно, если организация использует внешние источники данных о пользователях и не требует заполнения профиля вручную.

Что будет при включении настройки

- Пользователи смогут авторизоваться в приложениях, даже если их профиль в личном кабинете заполнен не полностью.
- Проверка обязательных полей выполняться не будет.
- В интерфейсе личного кабинета уведомления о незаполненных полях сохраняются.

Как включить настройку

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Включите переключатель **Игнорировать обязательные поля профиля личного кабинета для приложений**.
4. Нажмите **Сохранить**.

После применения настройки пользователи смогут проходить авторизацию без проверки обязательных полей профиля.

> 💡 **Рекомендация**: Включайте опцию только в том случае, если контроль полноты профиля осуществляется другими средствами.

Запрет привязки идентификаторов

Эта настройка запрещает пользователям самостоятельно привязывать новые внешние идентификаторы к своему профилю через виджет входа.

Чтобы запретить привязку:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Активируйте переключатель **Запретить привязку идентификаторов на форме виджета**.
4. Нажмите **Сохранить**.

Ограничения доступа

Эта настройка позволяет ограничить вход в приложение для всех пользователей, кроме **Администратор** сервиса. Все остальные пользователи не смогут авторизоваться.

> **Важно:** при включении ограничения доступа все пользователи, кроме администраторов сервиса, потеряют возможность входа. Используйте настройку для технических работ или аварийных ситуаций.

Чтобы ограничить доступ:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Активируйте переключатель **Ограниченный доступ для всех приложений**.
4. Нажмите **Сохранить**.

Запрет регистрации

Эта настройка позволяет запретить создание новых аккаунтов в виджете входа.

Чтобы настроить запрет регистрации:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройки доступа**.
3. Выберите необходимую настройку:
   - **Регистрация запрещена** — полностью блокирует создание новых аккаунтов.
   - **Регистрация разрешена** (по умолчанию) — стандартный режим работы, пользователи могут создавать аккаунты самостоятельно.
4. Нажмите **Сохранить**.

Технические параметры

Технические настройки, такие как идентификаторы клиента, параметры безопасности, URL-адреса авторизации, способы аутентификации клиента и параметры токенов и другие, находятся в разделе **Параметры приложения**.

Ниже перечислены настройки, доступные для редактирования в кабинете администратора. Остальные параметры изменяются через конфигурационный файл.

Чтобы изменить параметры в кабинете администратора:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Параметры приложения**.

3. Настройте параметры:
    - Ограничение доступа
    - Время аутентификации
    - Токен доступа
    - Токен обновления
4. Нажмите **Сохранить**.

Описание параметров

Основные идентификаторы

Название	Параметр	Описание
Идентификатор (client_id)	`client_id`	Уникальный идентификатор приложения
Секретный ключ (client_secret)	`client_secret`	Конфиденциальный ключ приложения
Адрес приложения	-	Базовый URL сервиса **КриптоАРМ ID** в формате `протокол://доменное имя:порт`

Ограничение доступа

Ограничивает вход в личный кабинет только пользователям с административными ролями.

Название	Описание
Ограниченный доступ	Если включено, доступ в личный кабинет будет разрешён только пользователям с правами **Администратор** сервиса

Возвратный URL

Название	Параметр	Описание
Возвратный URL #	`Redirect_uri`	URL, на который пользователь будет перенаправлен после успешной аутентификации

URL выхода из системы

Название	Параметр	Описание

Название	Параметр	Описание
URL выхода из системы #	`post_logout_redirect_uri`	URL, на который сервис будет перенаправлять пользователя после выхода. Если значение не указано, то используется `Redirect_uri`.

URL запроса аутентификации

Название	Параметр	Описание
URL запроса аутентификации или восстановления после аутентификации #	`request_uris`	Список URL для размещения JWT-запросов авторизации `Request Object`. Сервер извлекает JWT с указанного URL при авторизации.

Типы ответов

Название	Параметр	Описание
Тип ответов (response_types)	`response_types`	Определяет какие токены и коды возвращаются авторизационным сервером: - `code` — только код авторизации - `id_token` — только ID токен - `code id_token` — код + ID токен - `code token` — код + токен доступа - `code id_token token` — код + ID токен + токен доступа - `none` — только подтверждение аутентификации

Типы предоставления доступа

Название	Параметр	Описание

Название	Параметр	Описание
Типы предоставления доступа (grant_types)	`grant_types`	Способы получения авторизации: - `authorization code` — безопасный код через сервер клиента (рекомендуется); - `implicit` — прямое получение токена (для публичных клиентов) - `refresh_token` — обновление токена без повторного входа

Метод аутентификации клиента

> 💡 Выбор метода зависит от требований безопасности и возможностей клиента. JWT-методы обеспечивают повышенную безопасность, так как не передают секрет напрямую.

Название	Параметр	Описание

Название	Параметр	Описание
Аутентификация клиента	`token_endpoint_auth_method`, `introspection_endpoint_auth_method`, `revocation_endpoint_auth_method`	Определяет метод аутентификации клиента при обращении к различным конечным точкам (`token`, `introspection`, `revocation`). Доступные методы: - `none` — без учетных данных; - `client_secret_post` — учетные данные в теле запроса; - `client_secret_basic` — HTTP Basic Authentication; - `client_secret_jwt` — JWT, подписанный секретом клиента; - `private_key_jwt` — JWT, подписанный приватным ключом клиента.

Алгоритм подписи ID токена

Название	Параметр	Описание

Название	Параметр	Описание
Алгоритм подписи, используемый при создании подписанного ID-токена (id_token_signed_response_alg)	`id_token_signed_response_alg`	Указывает алгоритм, который используется для подписи ID токена. `ID токен` — это JSON Web Token (JWT), который содержит утверждения (claims) о аутентификации пользователя

Время аутентификации

Название	Параметр	Описание
Проверка наличия времени Аутентификации (require_auth_time)	`require_auth_time`	Если включено, в ID токене добавляется `auth_time` — время последней аутентификации пользователя

Дополнительные параметры безопасности

Название	Параметр	Описание

Название	Параметр	Описание
Параметр для обеспечения безопасности передачи данных между клиентом и сервером авторизации	`require_signed_request_object`	Указывает, требуется ли подписанный `Request Object` при отправке запроса на авторизацию. `Request Object` — это способ безопасной передачи параметров авторизации от клиента к серверу авторизации, обычно в форме JWT (JSON Web Token). Когда `require_signed_request_object` включен, клиент должен подписать `Request Object` с использованием заранее согласованного алгоритма подписи, который указан в конфигурации клиента.

Тип передачи идентификатора пользователя

Название	Параметр	Описание
Способ передачи ID пользователя в идентификационном токене (subject_type)	`subject_type`	Определяет, как формируется `sub claim` в ID токене: - `public` — один и тот же идентификатор для всех клиентов - `pairwise` — уникальный идентификатор для каждого клиента, повышает конфиденциальность

Токен доступа

Название	Параметр	Описание

Название	Параметр	Описание
Токен доступа (access_token_ttl)	`access_token_ttl`	Время жизни `access_token` в секундах

Токен обновления

Название	Параметр	Описание
Токен обновления (refresh_token_ttl)	`refresh_token_ttl`	Время жизни `refresh_token` в секундах

Подключение Sentry

Sentry — это платформа для мониторинга ошибок и производительности приложений.

> Официальный ресурс Sentry

Подключение **Sentry** позволяет:

- отслеживать ошибки и исключения в реальном времени;
- получать трассировки событий по пользователям;
- анализировать производительность системы.

Как подключить Sentry

Шаг 1. Создание проекта в Sentry

1. Перейдите на сайт Sentry.io.
2. Зарегистрируйтесь или войдите в свою учетную запись.
3. Создайте новый проект.

После создания проекта **Sentry** предоставит **DSN (Data Source Name)** — уникальный идентификатор для подключения **КриптоАРМ ID** к **Sentry**.

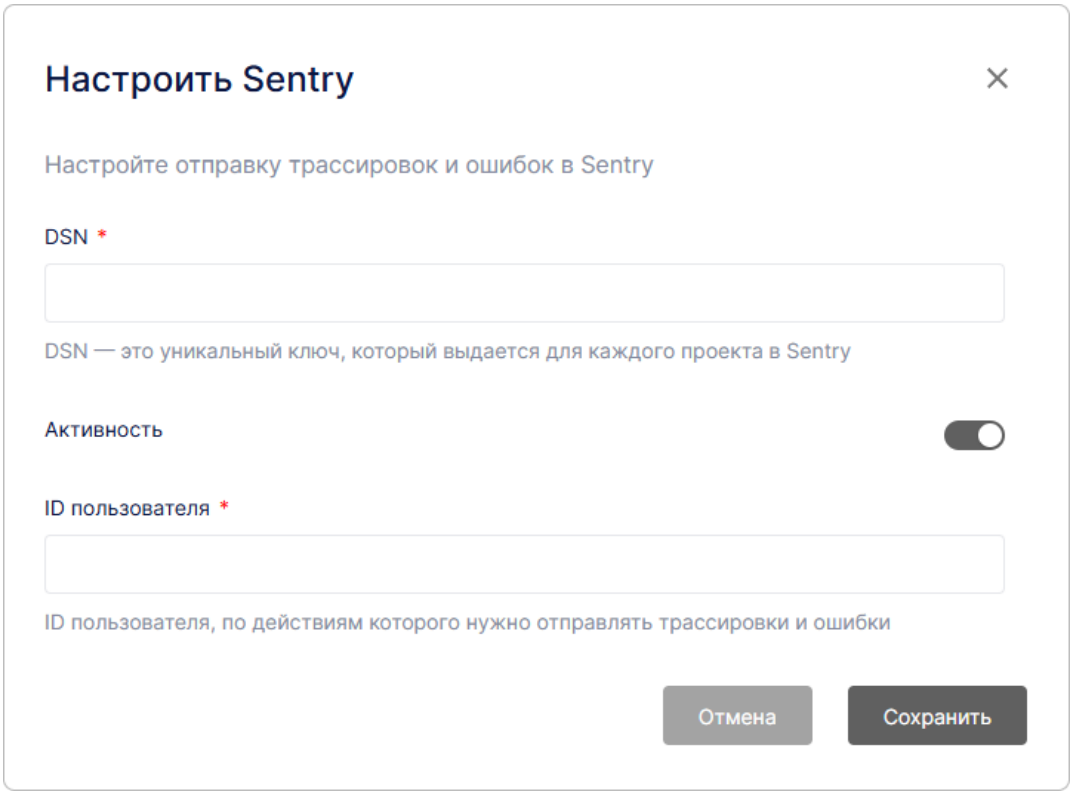
> **Совет**: Скопируйте **DSN (Data Source Name)**, чтобы не потерять его при переходе к следующему шагу.

Шаг 2. Подключение Sentry

Чтобы подключить **Sentry**:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Найдите блок **Sentry** и нажмите **Настроить**.

3. В открывшейся форме подключения укажите:
    - **DSN** — уникальный идентификатор, созданный на **шаге 1**.
    - **Активность** — включите, чтобы начать отправку ошибок и трассировок в **Sentry**.
    - **ID пользователя** (при необходимости) — укажите, если нужно отслеживать ошибки и события по конкретным пользователям.



4. Нажмите **Сохранить**.

Журнал событий

В **Журнале** можно увидеть, откуда и с каких устройств пользователи заходили в личный кабинет или приложения.

Для каждого события доступен просмотр подробных сведений.

Параметр	Что содержит
Заголовок события	Категория действия
Дата и время	Точные временные метки
Приложение	Идентификатор (`client_id`) приложения
Пользователь	Идентификатор (`id`) пользователя

Параметр	Что содержит
Устройство	Тип устройства и браузер
Местоположение	IP-адрес

Как перейти в журнал

1. Перейдите в кабинет администратора.
2. Откройте вкладку **Журнал**.

Типы приложений

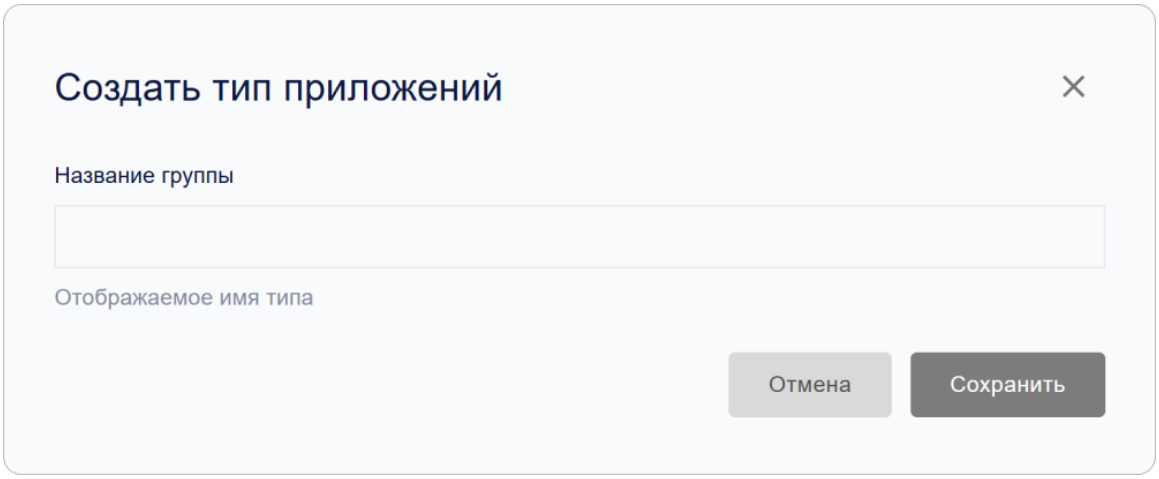
Типы приложений — это категории для систематизации приложений в **каталоге**. Они помогают организовать структуру и упростить навигацию пользователей.

Зачем нужны типы:

- Помогают группировать приложения по категориям
- Упрощают поиск нужных приложений
- Помогают организовывать структуру каталога

Создание типа приложения

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. В появившемся окне нажмите на кнопку **Создать**  .
4. Откроется форма создания.



5. Укажите название типа.

> Название типа должно быть уникальным в рамках системы.

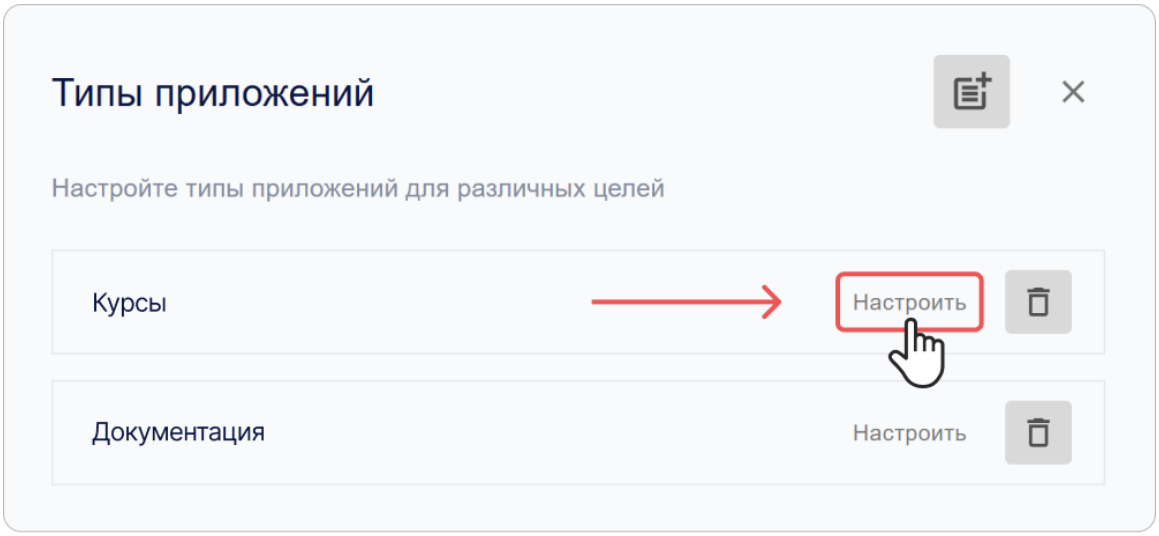
6. Нажмите **Сохранить**.

   Созданный тип отобразится в списке.

> Назначение типа осуществляется при создании приложения.

Редактирование типа приложения

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. Откроется окно со списком типов.



4. Нажмите на кнопку **Настроить** на панели с типом, который необходимо отредактировать.
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

> После редактирования типа все связанные приложения автоматически получают обновленное название категории.

Удаление типа приложения

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Найдите блок **Типы приложений** и нажмите **Настроить**.
3. Откроется окно со списком типов.

4. Нажмите на кнопку **Удалить**  на панели с типом, который необходимо удалить.

Удаление происходит без дополнительного подтверждения.

> 💡 После удаления тип будет удалён из каталога, а приложения, у которых он был назначен, автоматически получат тип **Прочее**.

Экспериментальные функции

Экспериментальные функции — это новые возможности сервиса **КриптоАРМ ID**, находящиеся на стадии тестирования и доработки.

Основные характеристики:

- Регулируются администратором сервиса
- Функционал может изменяться без предварительного уведомления
- Содержат недокументированные особенности работы
- Производительность и стабильность могут отличаться от основных функций

Раздел с экспериментальными функциями доступен по адресу: `https://ID_HOST/experimental`.

> 🚧 **Статус**: Экспериментальные функции могут быть удалены, изменены или переведены в основной функционал без предварительного уведомления.

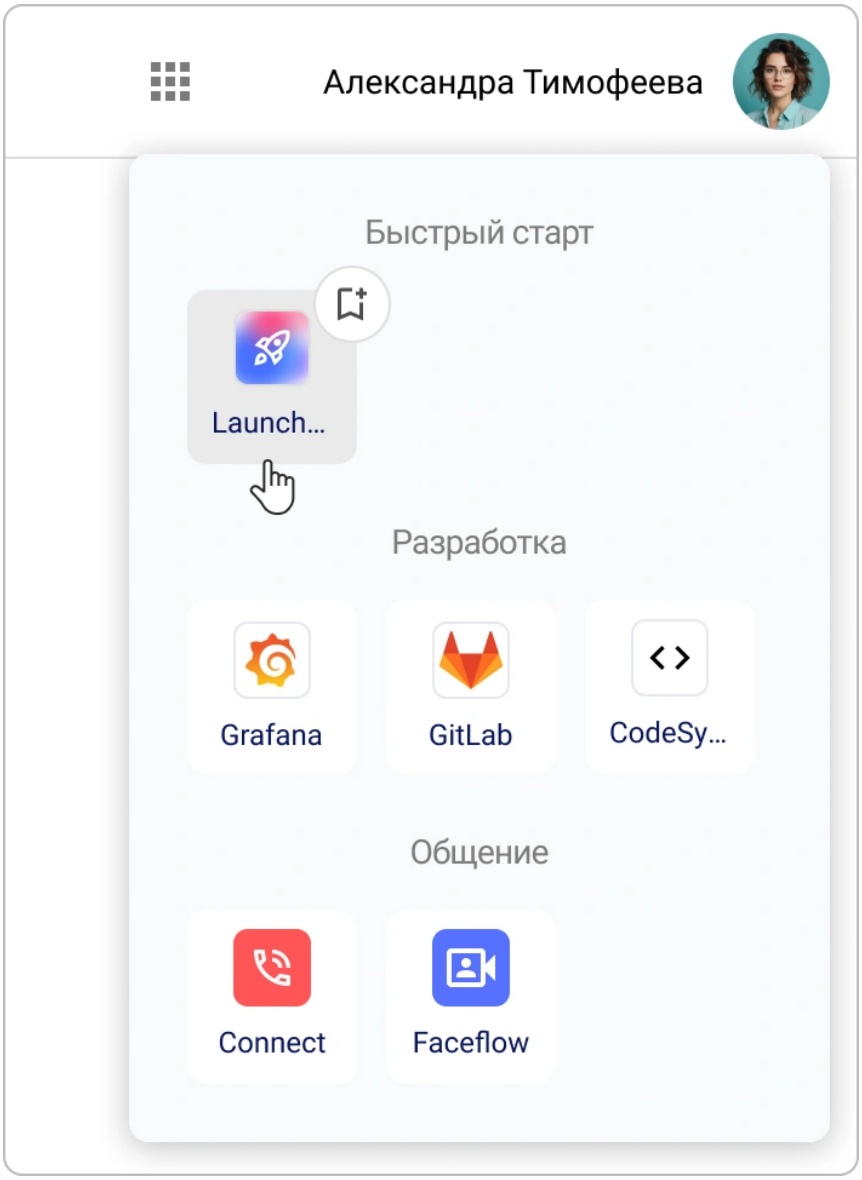
Какие функции доступны

1. **Визитка пользователя**
    - Цифровой аналог визитной карточки с контактными данными
    - Поддержка формата vCard для экспорта
    - Возможность делиться по ссылке или через QR-код

    Подробнее о визитке →

2. **Каталог приложений**
    - Централизованная площадка для приложений системы **КриптоАРМ ID**
    - Содержит удобную систему категорий
    - Возможность добавлять приложения в избранные

    Подробнее о каталоге →



Настройка профиля пользователя

Парольная политика

Парольная политика в КриптоАРМ ID — это набор правил, определяющих требования к сложности и безопасности паролей пользователей. Она помогает защитить учетные записи от взлома и несанкционированного доступа.

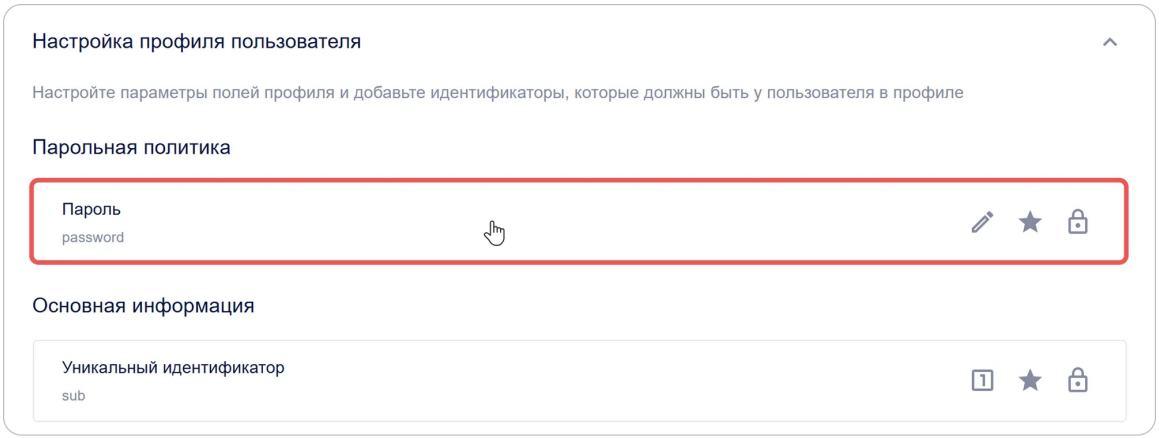
Установленные правила применяются:

- при создании пароля в виджете регистрации,
- при восстановлении пароля в виджете входа,
- при смене пароля в профиле пользователя.

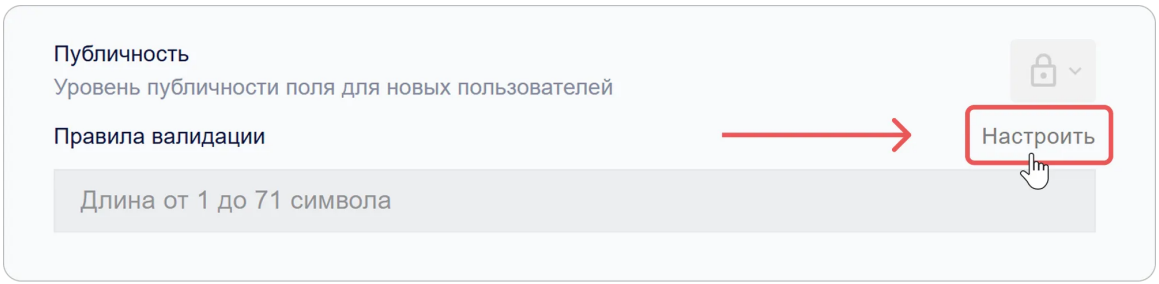
Как настроить правила парольной политики

1. Перейдите в кабинет администратора → вкладка **Настройки**.

2. Раскройте блок **Настройка профиля пользователя** и нажмите на панель **Пароль**.



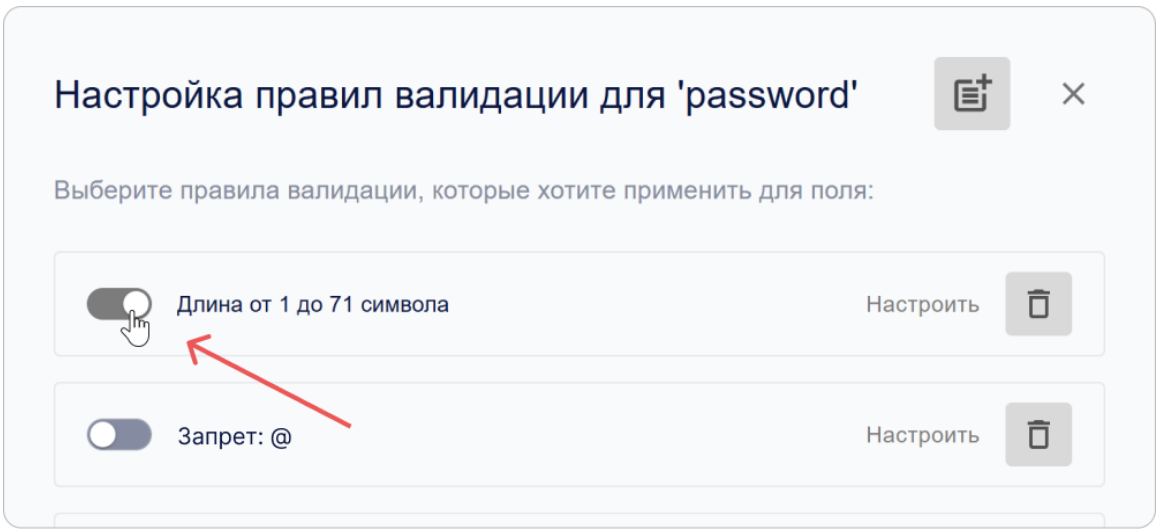
3. В появившемся окне нажмите **Настроить**.



4. Откроется окно со списком доступных правил проверки.

> 🔗 Про создание и настройку правил валидации полей профиля читайте в инструкции Правила валидации полей профиля пользователя.

5. Отметьте флажками правила, которые нужно применить к паролю.



6. Закройте окно со списком правил.

7. Нажмите **Сохранить** в форме редактирования поля.

Изменения применяются автоматически.

Теперь выбранные вами правила будут использоваться для проверки сложности пароля пользователя.

> ⚠ **Примечание**: Новые правила применяются только к создаваемым и изменяемым паролям. Существующие пароли остаются без изменений.

Рекомендации по безопасности

Чтобы обеспечить надёжную защиту учетных записей, рекомендуется включить следующие параметры:

Рекомендация	Пример правила
Минимальная длина пароля — не менее 8 символов	`Минимальная длина = 8`
Использование букв разного регистра	`Содержит строчные и прописные символы`
Обязательное наличие цифр	`Содержит хотя бы одну цифру`
Обязательное наличие спецсимволов	`Содержит специальные символы (!@#$% и т. п.)`

Основные поля профиля пользователя

Основные поля профиля — это обязательные системные атрибуты, которые создаются автоматически для каждого пользователя при его регистрации. Они формируют базовую структуру профиля и обеспечивают корректную работу механизмов аутентификации, идентификации и связи между системами.

Список основных полей

> 📌 Список основных полей фиксирован. Добавление, переименование или удаление этих полей недоступно.

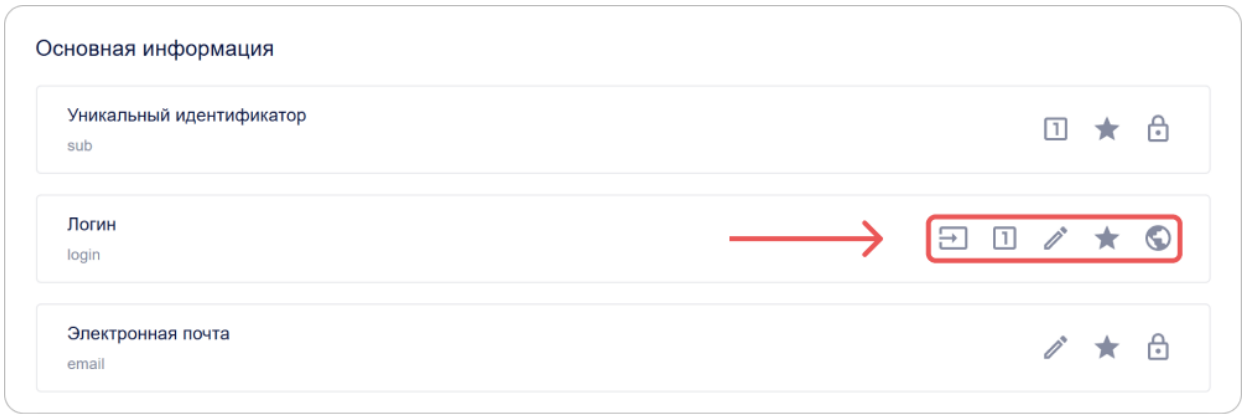
Поле	Идентификатор
Идентификатор	`sub`
Логин	`login`
Электронная почта	`email`
Имя	`given_name`

Поле	Идентификатор
Фамилия	`family_name`
Телефон	`phone_number`
Дата рождения	`birthdate`
Публичное имя	`nickname`
Фото	`picture`
Согласие на обработку данных	`data_processing_agreement`

Обозначения настроек

В интерфейсе для каждого поля доступен быстрый просмотр настроек поля в виде идентификаторов:

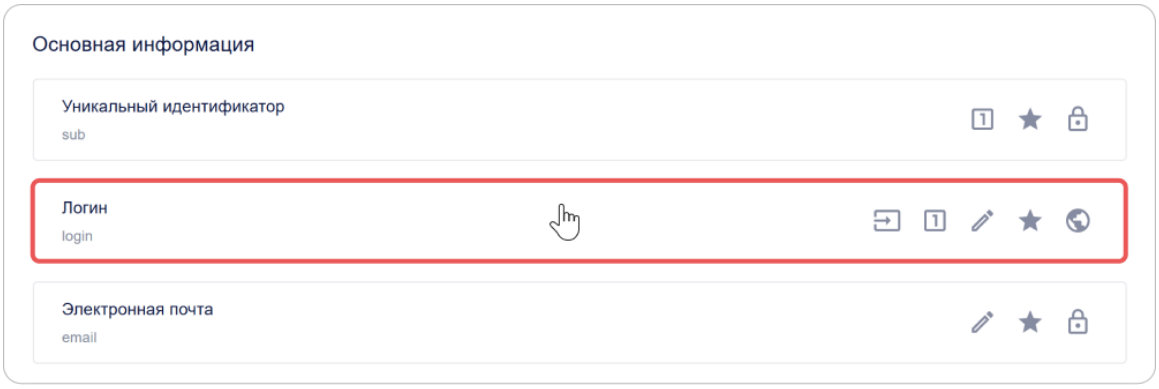
Иконка	Параметр
	Поле доступно пользователю для редактирования
	Поле обязательно для заполнения
	Значение поля должно быть уникальным
	Уровень публичности поля
	Поле можно использовать как логин при входе



Как настроить основное поле

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.

3. Нажмите на панель с полем, которое необходимо настроить.



4. В открывшейся форме укажите параметры и правила валидации.

5. Сохраните изменения в форме редактирования.

Параметры основного поля

Название	Описание
Название	Название поля. Недоступно для редактирования.
Описание поля	Название поля в интерфейсе. Недоступно для редактирования.
Использовать в качестве логина	Позволяет авторизоваться с использованием данного поля. Доступно для настройки в полях **Логин**, **Электронная почта** и **Номер телефона**
Активность	Определяет обязательное наличие поля в профиле пользователя. Неизменяемый параметр.
Редактируемость	Разрешает пользователю изменять значение поля в своём профиле.
Обязательность	Требует заполнения поля при регистрации или входе. Без него аутентификация невозможна.
Уникальность	Проверяет, чтобы значение поля не повторялось среди всех профилей.

Название	Описание
Публичность	Определяет, кому будут доступны данные пользователя:: - **Доступно только вам** - данные приватны и доступны только пользователю. - **Доступно по запросу** - данные пользователя доступны для сторонних систем после его согласия; - **Доступно всем** - данные публичны всегда для сторонних систем, не требуют согласия на доступ к данным. Данные, которые будут передаваться сторонней системе по хешу электронной почты (по аналогии с сервисом Gravatar).
Настройки подтверждения электронной почты	Предназначено для настройки параметров для подтверждения адреса электронной почты в профиле пользователя. 🔗 Подробное описание настроек в инструкции Настройки подтверждения электронной почты.
Настройки подтверждения номера телефона	Предназначено для настройки параметров для подтверждения номера телефона в профиле пользователя. 🔗 Подробное описание настроек в инструкции Настройки подтверждения номера телефона.
Правила валидации	Набор правил проверки корректности введённых данных. 🔗 Подробное описание в инструкции Настройка правил валидации.

Дополнительные поля профиля пользователя

Дополнительные поля профиля — это пользовательские атрибуты, которые можно создавать для хранения любых специфических данных, не входящих в стандартный набор.

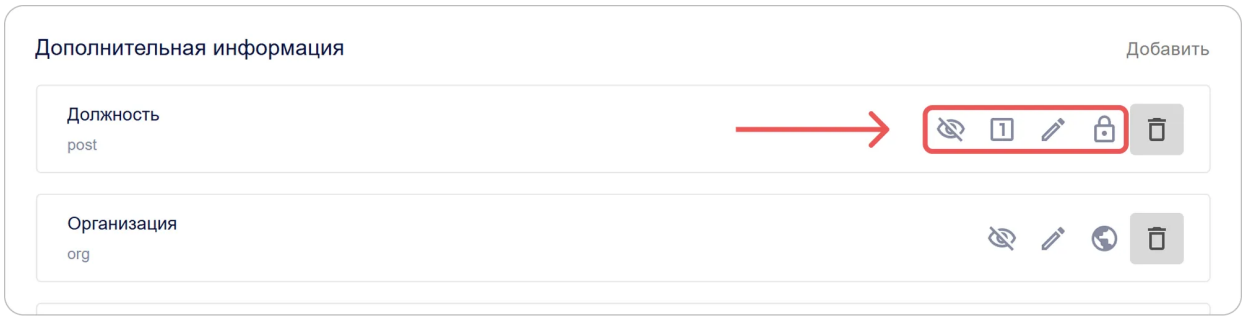
Они помогают адаптировать профиль под конкретные задачи:

- хранить внутренние идентификаторы, должности, роли, отделы и т.д.
- статусы проверки данных и другие бизнес-атрибуты.

Обозначения настроек

В интерфейсе для каждого поля доступен быстрый просмотр настроек поля в виде идентификаторов:

Иконка	Параметр
	Поле доступно пользователю для редактирования
	Поле обязательно для заполнения
	Значение поля должно быть уникальным
	Уровень публичности поля
	Активность поля



Добавление дополнительного поля

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя** .
3. Нажмите кнопку **Добавить** в разделе **Дополнительная информация**.
4. В открывшейся форме укажите параметры и правила валидации.
5. Нажмите **Сохранить**.

Редактирование дополнительного поля

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с дополнительным полем, настройки которого необходимо изменить.
4. В открывшейся форме отредактируйте параметры и правила валидации.
5. Нажмите **Сохранить**.

> Изменения вступают в силу сразу и применяются ко всем профилям, где используется данное поле.

Удаление дополнительного поля

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите кнопку **Удалить**  , напротив поля, которое нужно удалить.

> ⚠ **Примечание**: При удалении поля все сохраненные в нем данные пользователей будут безвозвратно утеряны.

Параметры дополнительного поля

Название	Описание
Описание поля	Название поля в системе
Активность	Определяет, отображается ли поле в профиле пользователя
Редактируемость	Разрешает пользователю изменять значение поля самостоятельно
Обязательность	Требует заполнения поля при регистрации или входе в систему. Без заполненного поля пользователь не сможет войти в систему.
Уникальность	Проверяет, чтобы значение не повторялось среди всех профилей
Публичность	Настраивает, кому будет доступно поле: - **Доступно только вам** - данные приватны и доступны только пользователю. - **Доступно по запросу** - данные пользователя доступны для сторонних систем после его согласия; - **Доступно всем** - данные публичны всегда для сторонних систем, не требуют согласия на доступ к данным. Данные, которые будут передаваться сторонней системе по хешу электронной почты (по аналогии с сервисом Gravatar).

Название	Описание
Атрибут vCard	Позволяет сопоставить поле с атрибутом при экспорте профиля в формат vCard
Значение по умолчанию	Устанавливает предзаполненное значение при создании профиля
Правила валидации	Определяют логику проверки введённого значения. Подробнее в инструкции Настройка правил валидации.

Правила валидации полей профиля пользователя и пароля

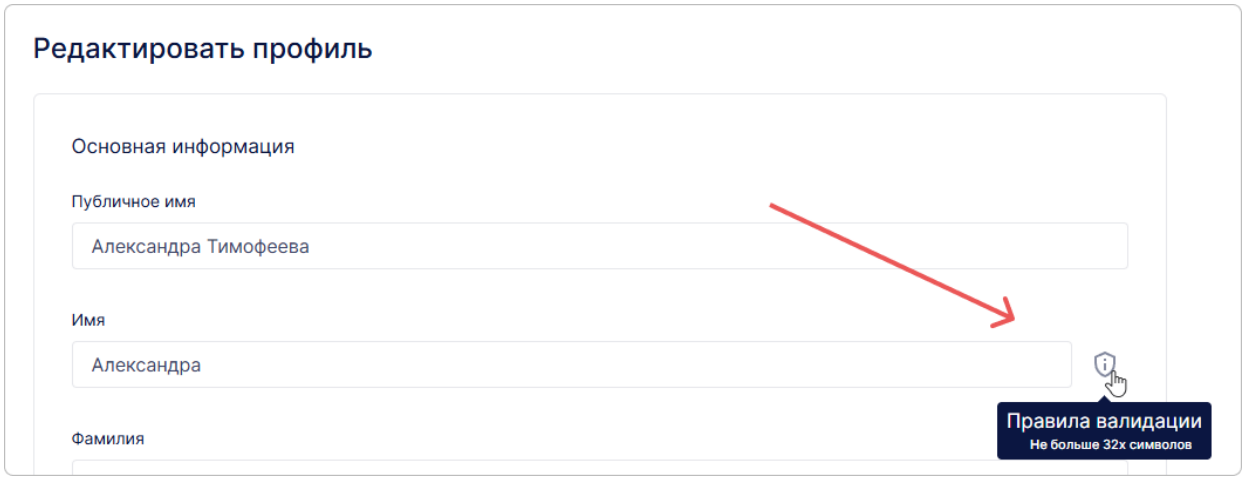
Правила валидации полей — это набор проверок, по которым система оценивает корректность данных, вводимых пользователем.

Вы можете задать собственные правила для:

- пароля аккаунта,
- основных полей профиля пользователя,
- дополнительных полей профиля пользователя.

Такие проверки позволяют повысить качество данных, например, не допускать некорректные email-адреса, номера телефонов или пароли без спецсимволов.

Заданные правила валидации отображаются в интерфейсе. Например, в форме редактирования профиля около основного или дополнительного поля появляется специальная иконка, при наведении на которую открывается список заданных правил.

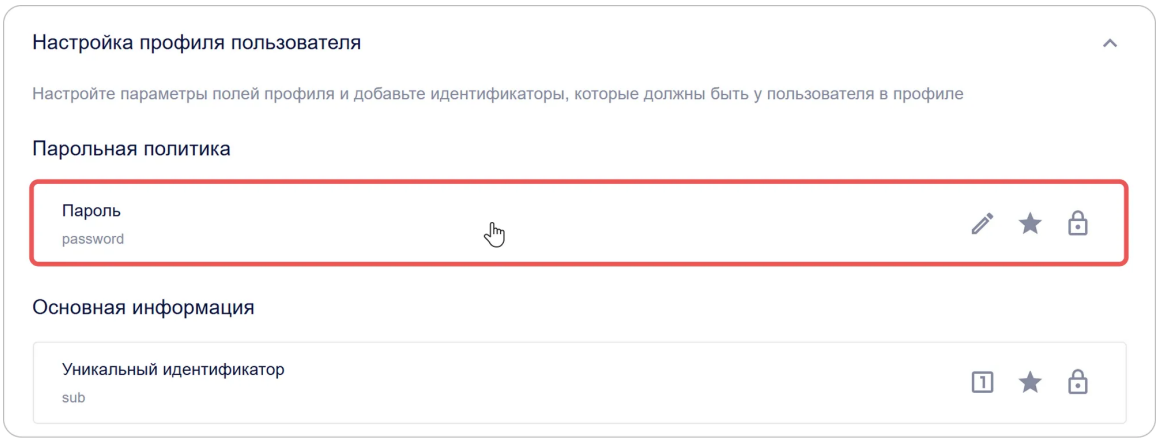


Создание правила

1. Перейдите в кабинет администратора → вкладка **Настройки**.

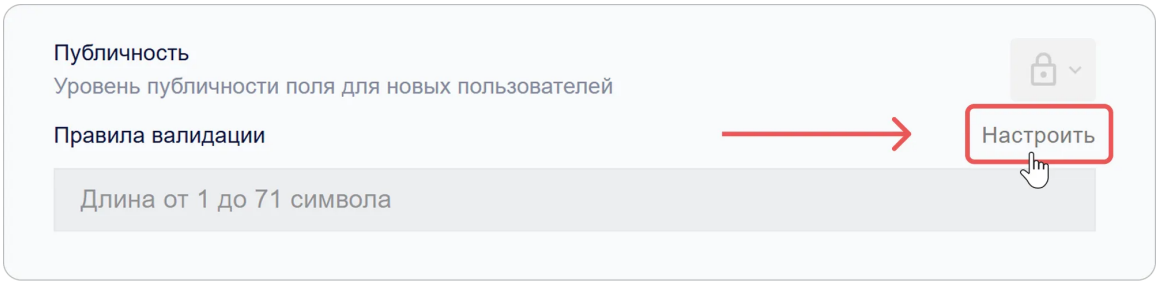
2. Раскройте блок **Настройка профиля пользователя**.

3. Нажмите на панель с паролем, основным или дополнительным полем.



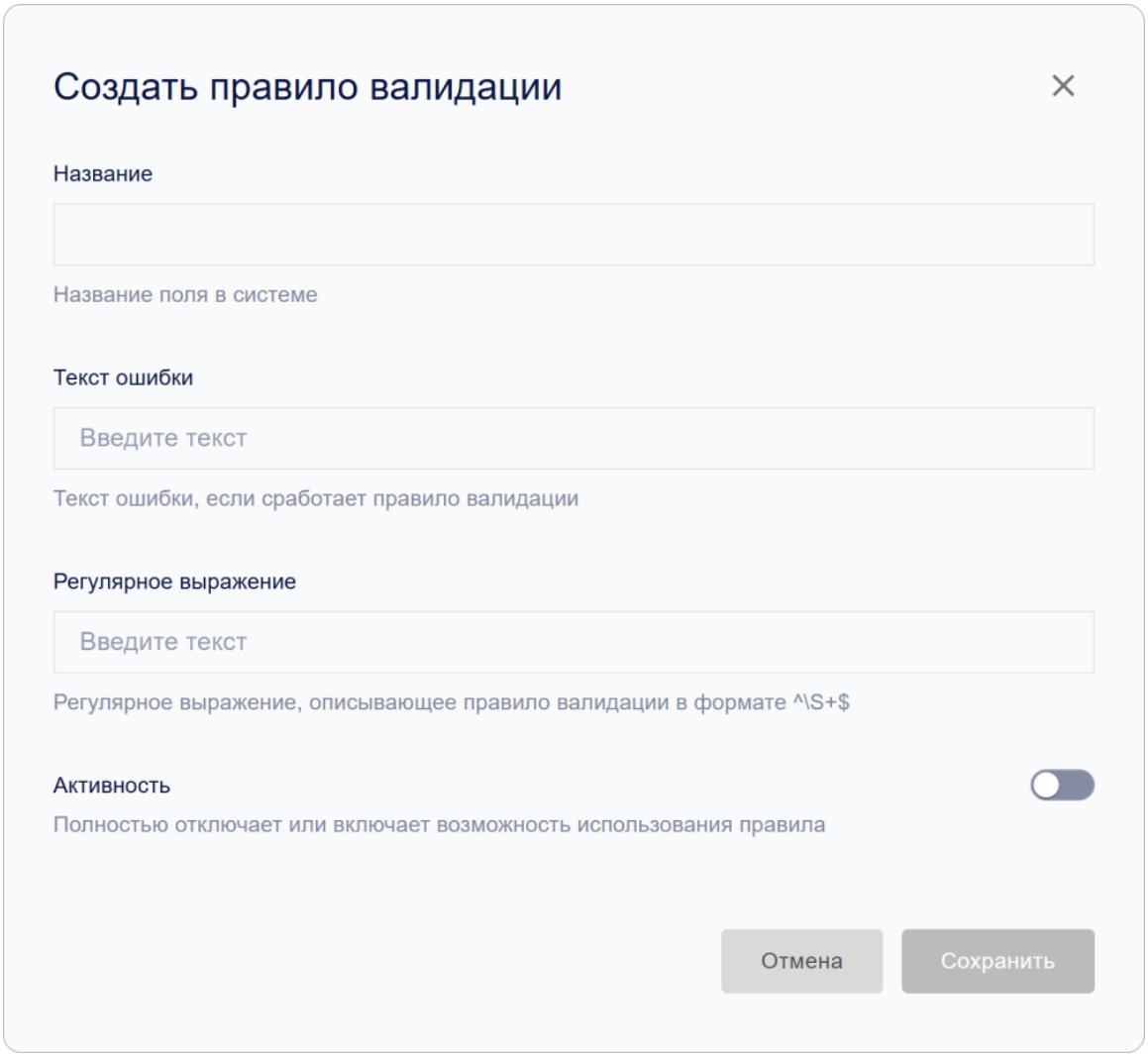
4. Откроется форма редактирования.

5. Нажмите **Настроить** в разделе **Правила валидации**.



6. В открывшемся окне со списком правил валидации нажмите на кнопку **Добавить**  .

7. Откроется форма создания правила.



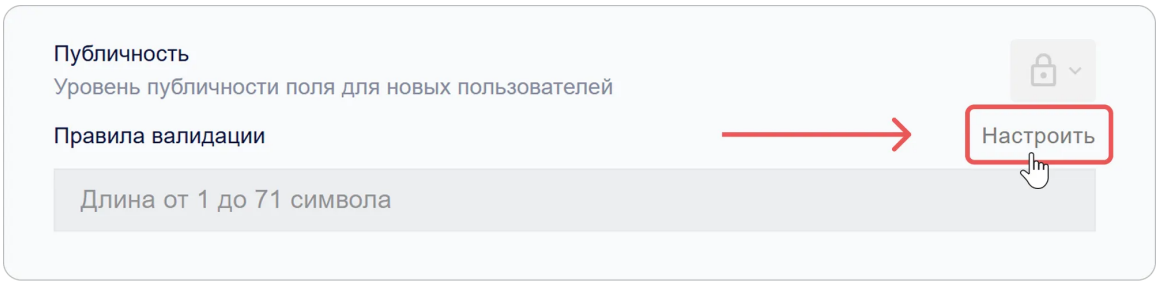
8. Заполните поля правила:
    - **Название**;
    - **Текст ошибки** — сообщение, которое будет отображаться при срабатывании правила;
    - **Регулярное выражение** — выражение, которому должно соответствовать значение в поле;
    - **Активность** — при включении данное правило можно выбрать для валидации поля. Неактивные правила недоступны для выбора и игнорируются при проверке значений в поле.
9. Нажмите **Сохранить**.

Созданное правило добавится в список правил и станет доступно для настройки валидации полей.

Редактирование правила

1. Перейдите в кабинет администратора → вкладка **Настройки**.

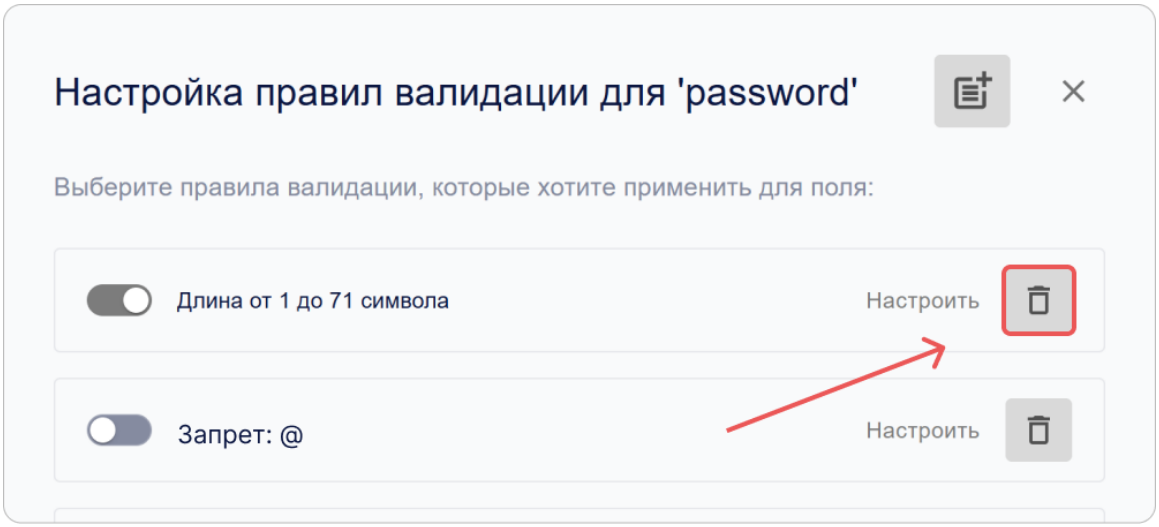
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.
6. Откроется окно со списком правил валидации.
7. На панели с правилом нажмите кнопку **Настроить** .



8. В открывшейся форме редактирования измените необходимые поля.
9. Нажмите **Сохранить**.

Удаление правила

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.
6. Откроется окно со списком правил валидации.
7. На панели с правилом нажмите кнопку **Удалить** .

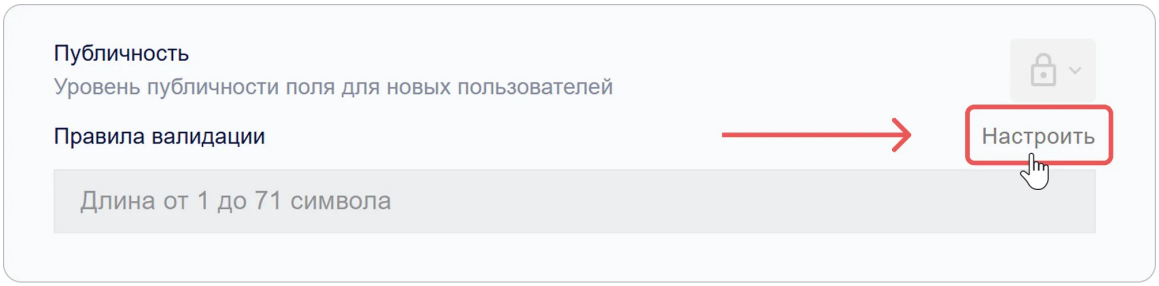


Изменения применяются автоматически.

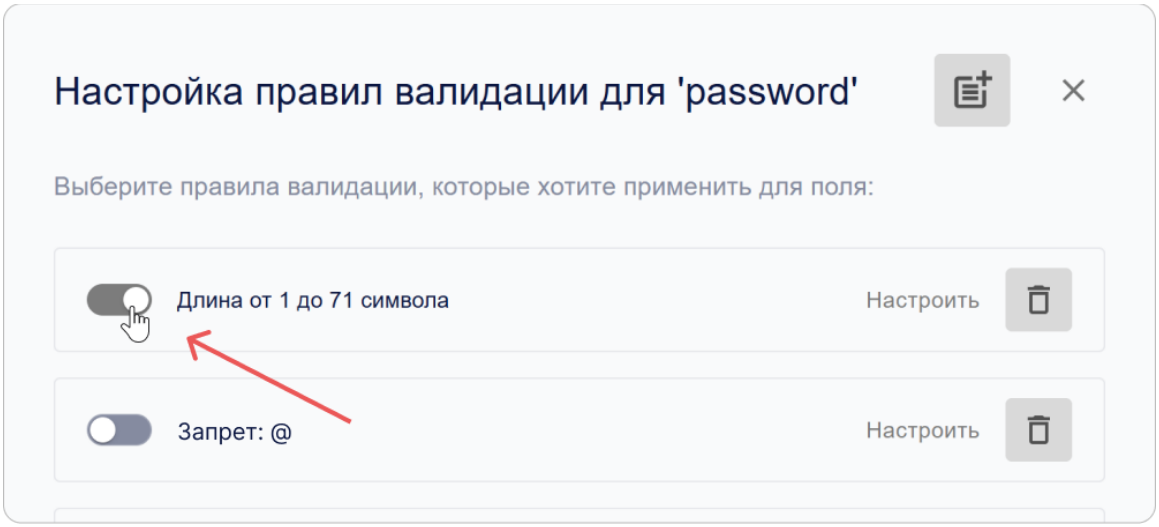
Как добавить правило в поле профиля пользователя

Чтобы настроить правила валидации в основном или дополнительном поле:

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель с основным или дополнительным полем.
4. Откроется форма редактирования.
5. Нажмите **Настроить** в разделе **Правила валидации**.



6. Откроется окно со списком правил валидации.



7. Установите флажок напротив правил, которые необходимо применить к выбранному полю.
8. Закройте окно со списком правил.

Изменения применяются автоматически.

Настройки подтверждения электронной почты

Подтверждение электронной почты в КриптоАРМ ID — это механизм проверки достоверности адреса, указанного пользователем при регистрации, авторизации или изменении данных профиля.

После указания адреса система отправляет письмо с кодом подтверждения или уникальной ссылкой. Пользователь должен перейти по ссылке или ввести код — после этого адрес считается подтверждённым.

Такая проверка обеспечивает:

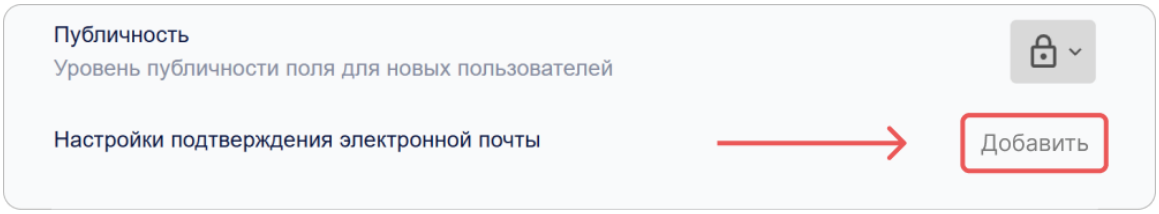
- защиту от регистрации с некорректными или чужими адресами;
- безопасность доступа к учётной записи;
- возможность использовать электронную почту для восстановления доступа и уведомлений;
- контроль за актуальностью контактных данных пользователей.

Настройки подтверждения электронной почты задаются администратором и включают параметры почтового сервера (SMTP), адрес отправителя, время жизни кода подтверждения и другие технические параметры.

> **Совет**: перед сохранением настроек убедитесь, что указанные SMTP-параметры корректны — при ошибке система не сможет отправлять письма.

Добавление настройки

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Электронная почта**.
4. Откроется форма редактирования.
5. В разделе **Настройки подтверждения электронной почты** нажмите **Добавить**.



6. В открывшемся окне укажите параметры:

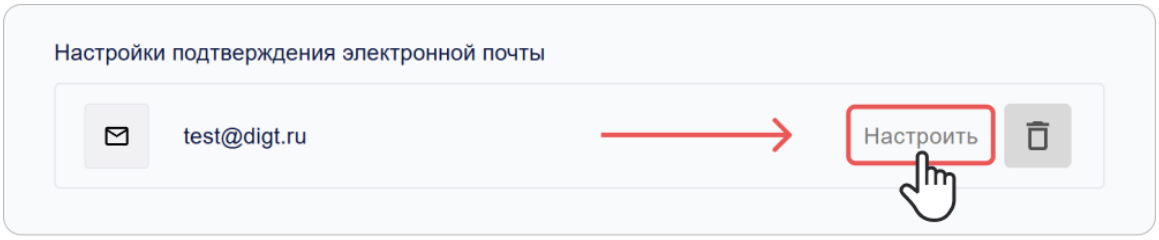
Параметр	Описание
Основной почтовый адрес	Адрес электронной почты, с которого будут отправляться автоматические письма
Адрес сервера исходящей почты	Адрес smtp-сервера
Порт сервера исходящей почты	Порт для smtp-сервера
Пароль почты	Обычный пароль или пароль приложения, который создается в настройках аккаунта почтового сервиса
Использовать для входа по коду	Почта будет использоваться для входа в приложения с помощью одноразовых паролей
Изображение почты	Иконка, которая будет отображаться в интерфейсе сервиса **КриптоАРМ ID**
Время жизни кода подтверждения	Время жизни кодов подтверждения адреса электронной почты в секундах

7. Нажмите **Сохранить**.

Редактирование настройки

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.

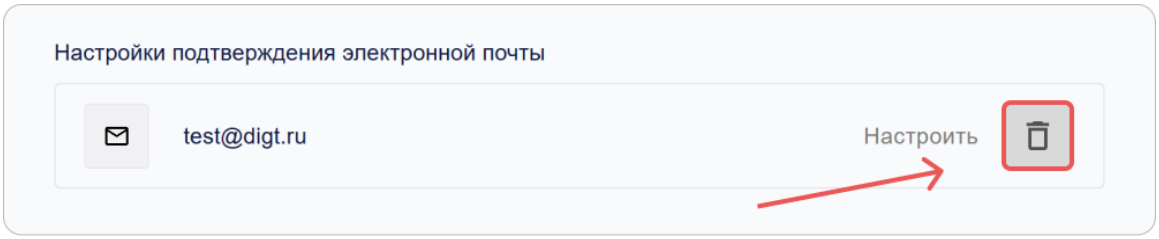
3. Нажмите на панель **Электронная почта**.
4. Откроется форма редактирования.
5. В разделе **Настройки подтверждения электронной почты** нажмите кнопку **Настроить**.



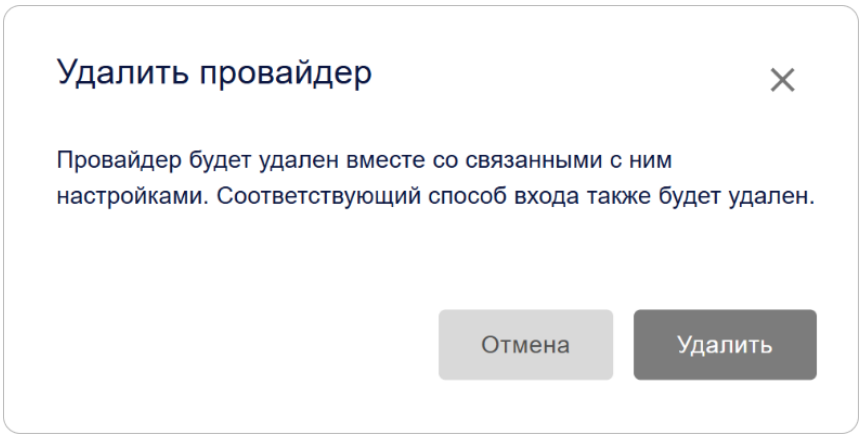
6. Откроется форма редактирования.
7. Внесите необходимые изменения.
8. Нажмите **Сохранить**.

Удаление настройки

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Электронная почта**.
4. Откроется форма редактирования.
5. Нажмите кнопку **Удалить** в разделе **Настройки подтверждения электронной почты**.



6. Подтвердите действие в модальном окне.



Настройки подтверждения номера телефона

Подтверждение номера телефона в КриптоАРМ ID — это механизм проверки достоверности контактного номера, указанного пользователем при регистрации, входе или изменении профиля.

После ввода номера система отправляет пользователю проверочный код или инициирует автоматический звонок. Пользователь вводит полученный код, подтверждая, что указанный номер действительно принадлежит ему.

Такая проверка выполняет несколько ключевых функций:

- предотвращает использование недействительных или чужих номеров;
- обеспечивает дополнительный уровень защиты учётной записи;
- позволяет использовать номер для входа по одноразовому коду;
- гарантирует корректную работу уведомлений, связанных с безопасностью.

В текущей версии **КриптоАРМ ID** подтверждение номеров реализуется через интеграцию с сервисом Авторизация по звонку платформы **Kloud.One**. Для работы этого механизма требуется настроить подключение к **Kloud.One**, указав идентификатор и секрет клиента.

> 💡 **Совет:** перед сохранением настройки убедитесь, что приложение корректно зарегистрировано в **Kloud.One** и указанные данные (`client_id` и `client_secret`) действительны. Без этого подтверждение номеров не будет работать.

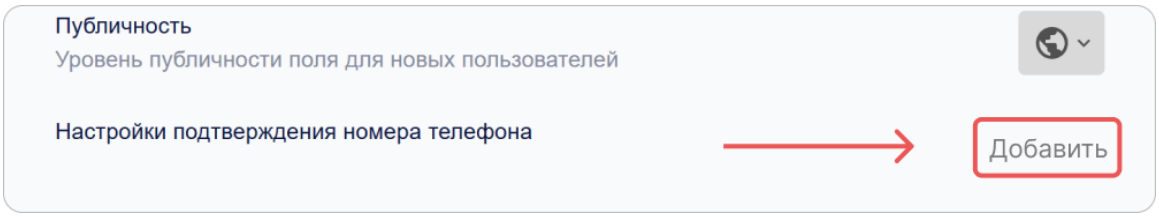
> 📄 Документация Kloud.One

Добавление настройки

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.

4. Откроется форма редактирования.

5. В разделе **Настройки подтверждения номера телефона** нажмите **Добавить**.



6. В появившемся окне задайте необходимые параметры:

Параметр	Название	Описание
Базовый адрес авторизации (issuer)	`issuer`	Адрес приложения Авторизация по звонку. В текущей версии — `<https://flashcall.kloud.one>`
Идентификатор ресурса (client_id)	`client_id`	Идентификатор приложения, созданного в сервисе Авторизация по звонку
Секретный ключ (Client_secret)	`client_secret`	Секретный ключ приложения, созданного в сервисе Авторизация по звонку
Использовать для входа по коду	-	Номер телефона будет использоваться для входа в приложения с помощью одноразовых паролей
Изображение телефона	-	Иконка, которая будет отображаться в интерфейсе сервиса **КриптоАРМ ID**

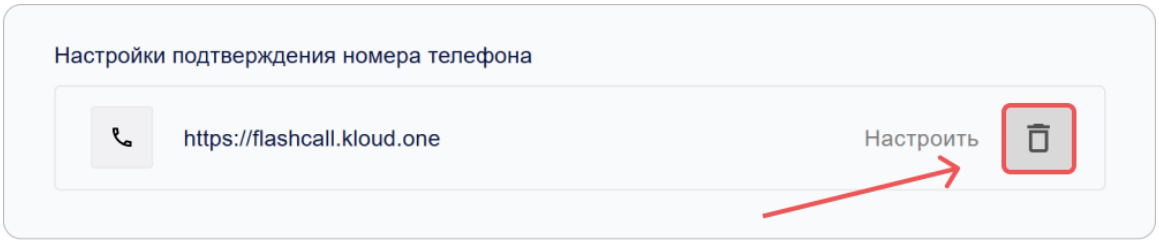
7. Нажмите **Сохранить**.

Редактирование настройки

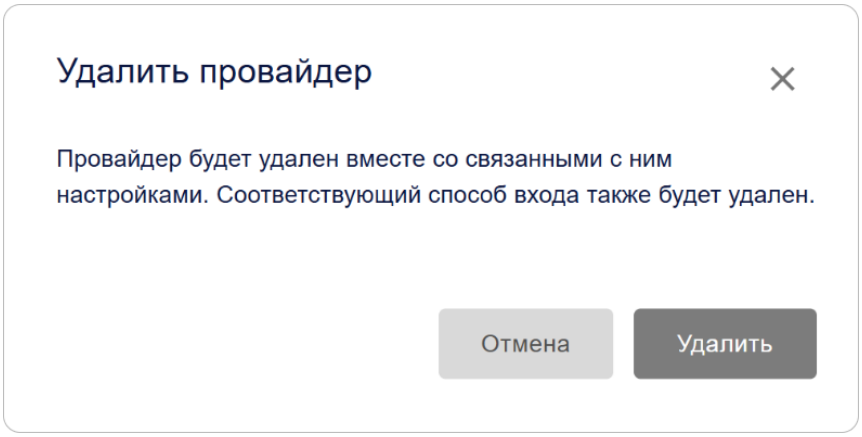
1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.
4. Откроется форма редактирования.
5. В разделе **Настройки подтверждения номера телефона** нажмите **Настроить**.
6. Откроется форма редактирования.
7. Внесите необходимые изменения.
8. Нажмите **Сохранить**.

Удаление настройки

1. Перейдите в кабинет администратора → вкладка **Настройки**.
2. Раскройте блок **Настройка профиля пользователя**.
3. Нажмите на панель **Номер телефона**.
4. Откроется форма редактирования.
5. Нажмите **Удалить**  в разделе **Настройки подтверждения номера телефона**.



6. Подтвердите действие в модальном окне.



Управление лицензиями

На какие функции требуется лицензия

Система использует лицензии для управления доступом к функционалу, включая авторизацию через SSO и подключение доверенных источников данных.

Варианты лицензий:

1. **Базовая лицензия**
   - Разблокирует авторизацию пользователей через любые провайдеры.
   - Позволяет подключить один коннектор (доверенный провайдер) к источнику данных.
   - Может быть бессрочной или с ограниченным сроком действия.

- Для работы системы нужна только одна такая лицензия.

2. **Лицензия на коннектор**

- Позволяет подключать дополнительные коннекторы (по одной лицензии на каждый).
- Может быть бессрочной или с ограниченным сроком действия.

> 💡 **Для быстрого старта:** достаточно одной базовой лицензии. Она включает авторизацию и один коннектор. Остальное можно докупать по мере необходимости.

Лицензия	Авторизация	Подключение коннекторов	Особенности
Без лицензии	✖ Недоступна	✖ Недоступно	Можно запускать и настраивать систему, создавать пользователей
Базовая лицензия	☑ Доступна	☑ 1 коннектор	Бессрочная или с ограничением, только одна лицензия нужна для работы системы
Лицензия на коннектор	–	☑ 1 коннектор	Бессрочная или ограниченная по времени

> ⚠ **Примечание**: Лицензии действуют только для соответствующих глобальных версий. Убедитесь, что цифра в начале номера лицензии совпадает с вашей версией системы.

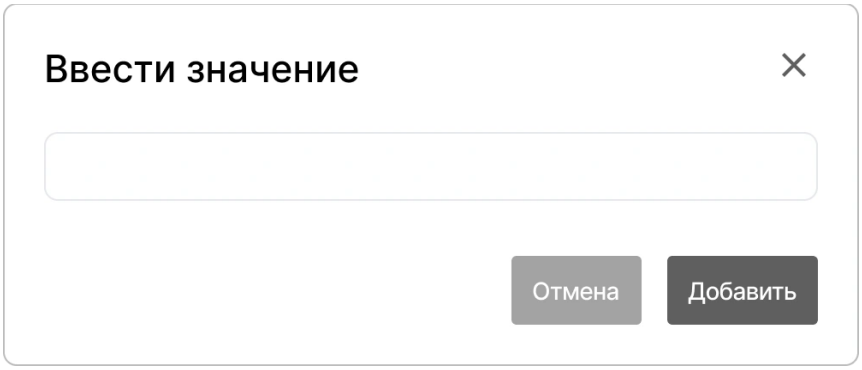
Активация лицензии

Добавление ключа

Чтобы добавить лицензионный ключ для базовой лицензии или лицензии на коннектор:

1. Перейдите в кабинет администратора (или организации) → вкладка **Настройки**.
2. Раскройте блок **Лицензии** и нажмите **Настроить**.

3. Введите лицензионный ключ и нажмите **Добавить**.

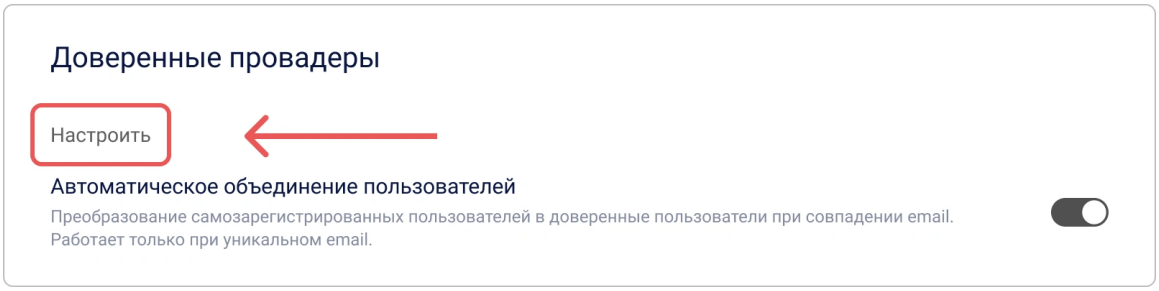


> **Совет**: Лицензионный ключ можно добавить в форме редактирования провайдера.

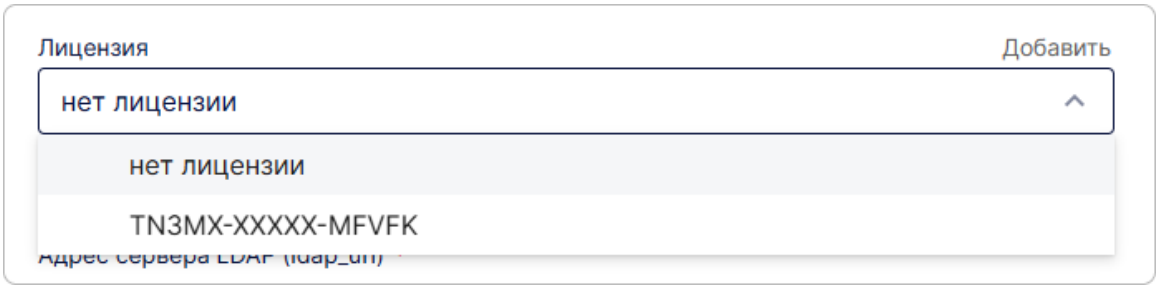
Привязка ключа к способу входа

Чтобы привязать лицензию к коннектору:

1. Перейдите в кабинет администратора (или организации) → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры**.
3. Нажмите на кнопку **Настроить**.



4. Откроется окно со списком провайдеров.
5. Нажмите кнопку **Настроить** на панели с провайдером, к которому необходимо привязать лицензию.
6. Откроется форма редактирования.
7. В настройке **Лицензия** выберите ключ из выпадающего списка.



> 💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

> 💡 **Особые условия:** Если адреса подключения провайдеров совпадают, допускается привязка нескольких таких провайдеров к одной лицензии.

8. Нажмите **Сохранить** в форме редактирования.

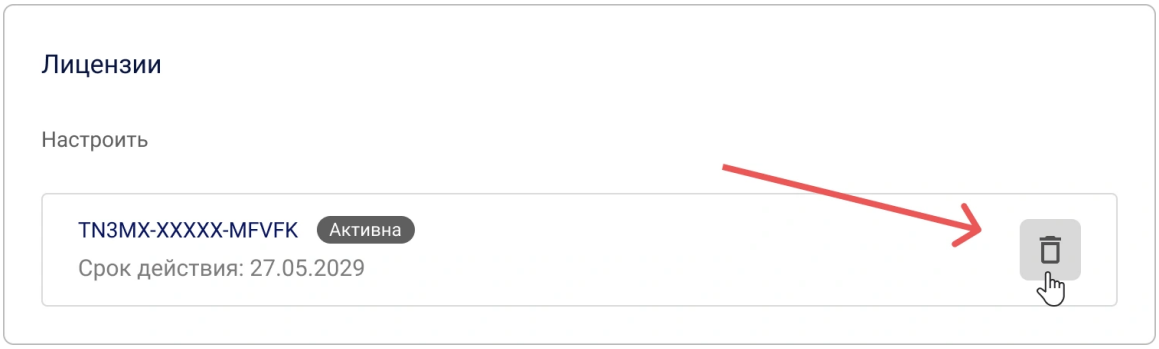
Лицензия привязывается к способу входа.

> 📌 Если срок действия лицензии истечёт или ключ будет удалён, связанный способ входа будет автоматически отключён, и пользователи не смогут авторизоваться через него.

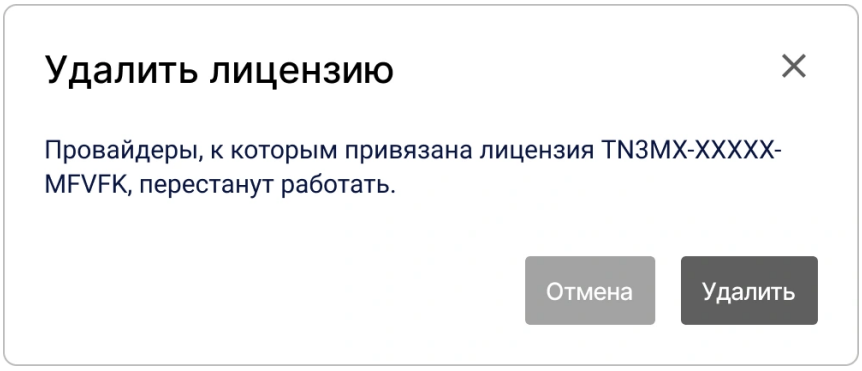
Удаление ключа из системы

Чтобы удалить ключ из системы:

1. Перейдите в кабинет администратора (или организации) → вкладка **Настройки**.
2. Раскройте блок **Лицензии**.
3. Нажмите на кнопку **Удалить** на панели с лицензионным ключом, который требуется удалить из системы.



4. Подтвердите действие в модальном окне.



Настройка мини-виджета

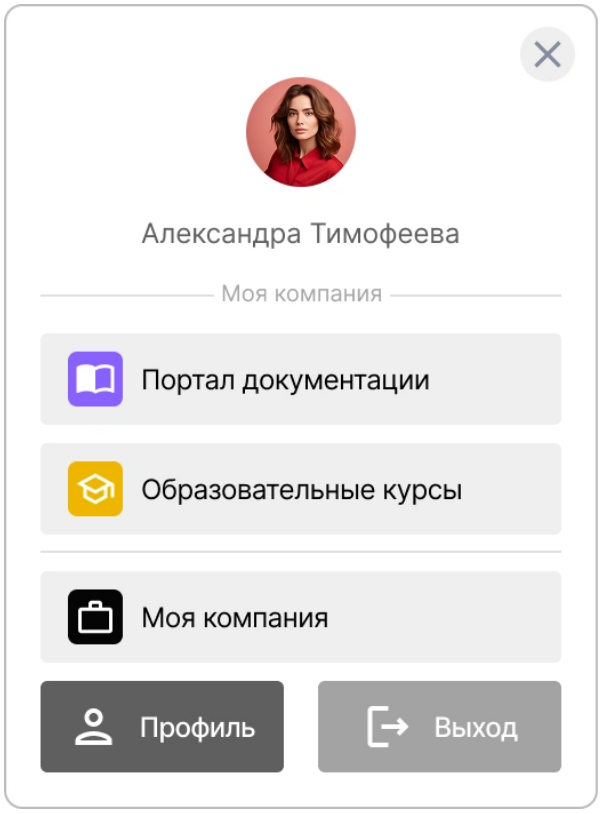
Что такое мини-виджет?

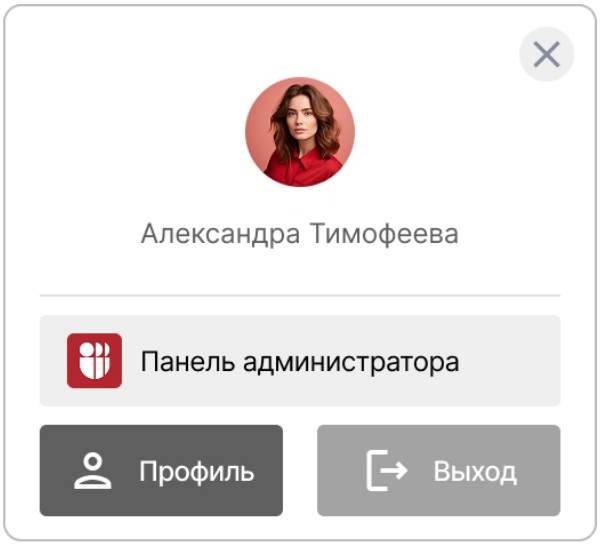
Мини-виджет — это меню с данными о пользователе и важными функциями. В нем доступны профиль, кабинет администратора, организации или малый кабинет, а также выход из системы. Также здесь можно разместить приложение для быстрого доступа. Виджет открывается при клике на аватар пользователя в правом верхнем углу экрана.

Мини-виджет представляет из себя лёгкий JavaScript-компонент для аутентификации пользователей в сервисе **КриптоАРМ ID**. Он работает по стандартам OIDC/OAuth2, PKCE и может быть встроен в любые веб-сайты или интерфейсы — от простого HTML до SPA на React или Vue.

> Чтобы добавить приложение в мини-виджет включите переключатель **Отображать в мини-виджете** в настройках приложения.

Примеры виджетов:





Конфигурация виджета

Обязательные параметры

Для базовой работы виджета необходимо указать три ключевых параметра:

Параметр	Тип	Описание	Пример

Параметр	Тип	Описание	Пример
`appId`	`string`	Уникальный идентификатор приложения в Trusted	`"MTnOOTdx85FgNbOFy2nUsH"`
`backendUrl`	`string`	URL вашего backend API	`"http://localhost:3001"`
`redirectUrl`	`string`	URL для перенаправления после авторизации	`"http://localhost:3000/login"`

Дополнительные параметры

Для расширенной настройки доступны опциональные параметры:

Параметр	Тип	Описание	Значение по умолчанию
`issuer`	`string`	URL Trusted SSO сервера	`"https://id.klouc`
`withOutHomePage`	`boolean`	Автоматический редирект на авторизацию	`false`
`getTokenEndPoint`	`string`	Endpoint для получения токена	`"/api/oidc/token'`
`getUserInfoEndPoint`	`string`	Endpoint для получения данных пользователя	`"/api/oidc/me"`
`scopes`	`string[]`	OAuth2 разрешения	`["openid", "lk", "profile"]`
`profile`	`IProfileConfig`	Настройки профиля пользователя	См. раздел ниже
`loginButton`	`ICustomMenuButton`	Настройки кнопки входа	См. раздел ниже

Параметр	Тип	Описание	Значение по умолчанию
`menuButtons`	`ICustomMenuButton[]`	Массив дополнительных кнопок	См. раздел ниже
`customStyles`	`ICustomStyles`	Глобальные стили виджета	См. раздел ниже

Базовый пример подключения

```
import { TrustedWidget, TrustedWidgetConfig } from "trusted-widget";

const newConfig: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  issuer: "https://id.kloud.one",
  withOutHomePage: false,
  getTokenEndPoint: "/api/oidc/token",
  getUserInfoEndPoint: "/api/oidc/me",
};

// Использование компонента
<TrustedWidget config={newConfig} />;
```

Настройка отображения профиля

Параметры конфигурации профиля

Профиль пользователя — это компонент, который содержит аватар и имя пользователя.

Параметр	Тип	Описание	Значение по умолчанию
`isHideText`	`boolean`	Скрыть отображение имени пользователя	`false`
`wrapper`	`IComponentStyles`	Стили контейнера профиля (только цвета)	См. раздел стилей

Параметр	Тип	Описание	Значение по умолчанию
`button`	`IComponentStyles`	Стили кнопки-аватара пользователя (только цвета)	См. раздел стилей

> ⚠ **Важно:** Для настроек профиля (`profile.wrapper` и `profile.button`) можно изменять только цвета (`color.text`, `color.background`, `color.hover`) и скрывать имя пользователя (`isHideText`). Другие параметры стилизации (такие как `borderRadius`, `padding`, `position`) не применяются к профилю.

Пример настройки профиля

```
// Пример: Только аватар без текста
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  profile: {
    isHideText: true, // Скрыть имя, показывать только аватар
  },
};
```

Настройка кнопки входа

Кнопка входа отображается для неавторизованных пользователей. Вы можете настроить её текст, иконку и стили.

Параметры кнопки входа

Параметр	Тип	Описание	Значение по умолчанию
`text`	`string`	Текст кнопки входа	`"Войти"`
`type`	`string`	Тип кнопки	`"login"`
`icon`	`string | React.ReactElement`	Ссылка на изображение или React элемент	`null`
`customStyles`	`IComponentStyles`	Индивидуальные стили для кнопки	См. раздел стилей

Пример конфигурации

```
// Пример: Кнопка с кастомной иконкой
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  loginButton: {
    text: "Войти через Trusted",
    type: "login",
    icon: "https://id.kloud.one/favicon.ico", // Пользовательская
иконка
  },
};
```

```
// Пример: Простая текстовая кнопка без иконки
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  loginButton: {
    text: "Войти",
    type: "login",
    customStyles: {
      isHideIcon: true, // Скрыть иконку
    },
  },
};
```

Параметры кнопок меню

Обязательные параметры

Параметр	Тип	Описание	Пример
`text`	`string`	Отображаемое название кнопки	`"TestService"`
`link`	`string`	Ссылка на страницу для перехода	`"https://test.com"`

Дополнительные параметры

Параметр	Тип	Описание	Значение по умолчанию

Параметр	Тип	Описание	Значение по умолчанию
`icon`	`string | React.ReactElement`	Ссылка на изображение или React элемент	`null`
`customStyles`	`IComponentStyles`	Индивидуальные стили для кнопки	См. раздел стилей

Пример конфигурации

```
import { TrustedWidget, TrustedWidgetConfig } from "trusted-widget";

const newConfig: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  menuButtons: [
    {
      text: "TestService",
      link: "https://test.com",
      icon: "https://image.png", // | <Icon />
    },
  ],
};
```

Стилизация мини-виджета

Виджет поддерживает детальную кастомизацию внешнего вида через объект `customStyles`. Вы можете управлять цветами, скруглениями, отступами и выравниванием всех элементов.

Структура объекта стилей

```
customStyles: {
  global: {
    borderRadius: "8px",        // Глобальное скругление
    color: { /* цвета */ }      // Глобальные цвета
  },
  components: {
    primaryButton: { /* стили */ },   // Основные кнопки
    secondaryButton: { /* стили */ }, // Второстепенные кнопки
    accountButton: { /* стили */ }    // Кнопки меню аккаунта
```

```
    }
  }
```

Параметры кастомных стилей

Глобальные стили

Параметр	Тип	Описание	Пример
`global.borderRadius`	`string`	Скругление углов для всех элементов	`"12px"`
`global.color`	`IComponentStyles`	Глобальные цвета	См. ниже

Стили компонентов

Параметр	Тип	Описание	Назначение
`components.primaryButton`	`IComponentStyles`	Стиль основной кнопки	Кнопка "Войти", "Профиль"
`components.secondaryButton`	`IComponentStyles`	Стиль второстепенной кнопки	Кнопка "Выход"
`components.accountButton`	`IComponentStyles`	Стиль кнопок меню аккаунта	Кнопки в выпадающем меню

Параметры стилей компонентов IComponentStyles

Параметр	Тип	Описание	Пример
`color.text`	`string`	Цвет текста и иконки (HEX)	`"#ffffff"`
`color.background`	`string`	Цвет фона (HEX)	`"#1976d2"`
`color.hover`	`string`	Цвет фона при наведении (HEX)	`"#1565c0"`
`borderRadius`	`string`	Скругление углов элемента	`"8px"`

Параметр	Тип	Описание	Пример
`padding`	`string`	Внутренние отступы	`"8px 16px"`
`position`	`"left" | "center"`	Выравнивание контента в кнопке	`"center"`
`isHideIcon`	`boolean`	Скрыть иконку в кнопке	`false`

Наследование стилей

Виджет имеет умную систему наследования стилей для кнопки `secondaryButton`:

- **Если заданы стили только для `primaryButton`**, то они автоматически применяются и к `secondaryButton`, но с большей прозрачностью (через уменьшение opacity).
- **Если заданы отдельные стили для `secondaryButton`**, то прозрачность применяться не будет — используются только явно указанные параметры.

Пример конфигурации стилей

Пример настройки глобальных стилей

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Дефолтные значения для глобальных стилей
  customStyles: {
    global: {
      color: {
        text: "#666666",
        background: "#ffffff",
      },
      borderRadius: "8px",
    },
    components: {
      accountButton: {
        color: {
          text: "#fff",
          background: "#efefef",
          hover: undefined, // если не задан применяется filter:
brightness(90%)
        },
        position: "left",
```

```
        isHideIcon: false,
      },
      primaryButton: {
        color: {
          text: "#ffffff",
          background: "#b5262f",
          hover: undefined, // если не задан применяется filter:
brightness(90%)
        },
        position: "left",
        isHideIcon: false,
      },
      // secondaryButton не задан — будет использоваться стиль
primaryButton с прозрачностью (opacity:0.5)
    },
  },
};
```

Пример полной конфигурации стилей

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Настройки профиля
  profile: {
    isHideText: false,
    wrapper: {
      color: {
        text: "#333333",
        background: "#f8f9fa",
      },
    },
    button: {
      color: {
        text: "#333333",
        background: "transparent",
        hover: "rgba(0, 0, 0, 0.08)",
      },
    },
  },
};
```

Пример полной конфигурации с кнопкой входа

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Кнопка входа с иконкой
  loginButton: {
    text: "Войти",
    type: "login",
    icon: "https://id.kloud.one/favicon.ico",
    customStyles: {
      color: {
        text: "#ffffff",
        background: "#4CAF50",
        hover: "#45a049",
      },
      borderRadius: "8px",
      padding: "10px 20px",
    },
  },
};
```

Пример полной конфигурации с глобальными стилями и меню

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  // Глобальные стили
  customStyles: {
    global: {
      borderRadius: "8px",
    },
    components: {
      primaryButton: {
        color: {
          text: "#ffffff",
          background: "#4CAF50",
          hover: "#45a049",
        },
        position: "center",
        isHideIcon: false,
      },
      secondaryButton: {
        color: {
```

```
            text: "#4CAF50",
            background: "transparent",
            hover: "#f1f8e9",
          },
          position: "center",
          isHideIcon: false,
        },
        accountButton: {
          color: {
            text: "#333333",
            background: "#ffffff",
            hover: "#f5f5f5",
          },
          position: "left",
          isHideIcon: false,
        },
      },
    },
  };
```

Индивидуальная стилизация кнопок меню

Для каждой кнопки в `menuButtons` можно задать индивидуальные стили через свойство `customStyles` типа `IComponentStyles`.

Пример с индивидуальными стилями для кнопок

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
  redirectUrl: "http://localhost:3000/login",
  menuButtons: [
    {
      text: "Личный кабинет",
      link: "https://my-account.com",
      icon: "https://icons.com/profile.png",
      customStyles: {
        color: {
          text: "#ffffff",
          background: "#4CAF50", // Зеленый фон
          hover: "#45a049", // Темно-зеленый при наведении
        },
        borderRadius: "8px",
        padding: "8px 16px",
        position: "center",
      },
```

```
    },
    {
      text: "Настройки",
      link: "https://settings.com",
      icon: "https://icons.com/settings.png",
      customStyles: {
        color: {
          text: "#333333",
          background: "#f5f5f5", // Светло-серый фон
          hover: "#e0e0e0", // Серый при наведении
        },
        borderRadius: "6px",
        padding: "6px 12px",
        position: "left",
      },
    },
    {
      text: "Поддержка",
      link: "https://support.com",
      customStyles: {
        color: {
          text: "#ffffff",
          background: "#FF5722", // Оранжевый фон
          hover: "#E64A19", // Темно-оранжевый при наведении
        },
        borderRadius: "4px",
        padding: "10px 20px",
        position: "center",
        isHideIcon: true, // Скрыть иконку для этой кнопки
      },
    },
  ],
};
```

Приоритет применения стилей

1. **Индивидуальные стили кнопки** (`customStyles` в объекте кнопки) — высший приоритет
2. **Стили accountButton** (`customStyles.components.accountButton`) — если не заданы индивидуальные
3. **Дефолтные стили** — если не заданы предыдущие

```
const config: TrustedWidgetConfig = {
  appId: "MTnOOTdx85FgNbOFy2nUsH",
  backendUrl: "http://localhost:3001",
```

```
  redirectUrl: "http://localhost:3000/login",
  // Если у кнопки НЕТ customStyles, то для menuButtons применяются
стили accountButton
  customStyles: {
    components: {
      // дефолтные стили accountButton
      accountButton: {
        color: {
          text: "#666666",
          background: "#efefef",
          hover: undefined, // если не задан применяется filter:
brightness(90%)
        },
        position: "left",
      },
    },
  },
};
```

Принципы стилизации мини-виджета

Принцип	Что это значит	Где и как это применить
Централизованное управление	Все настройки внешнего вида задаются через три ключевых объекта конфигурации.	Настройте общий вид в `customStyles`, профиль — в `profile`, кнопку входа — в `loginButton`.
Гибкая настройка профиля	Внешний вид блока с именем и аватаром авторизованного пользователя настраивается отдельно.	Используйте `profile.wrapper` для фона и `profile.button` для кнопки-аватара. Учтите, что здесь работают только настройки цвета.
Настройка кнопки входа	Стили кнопки, которую видят неавторизованные пользователи, настраиваются независимо.	Задайте текст, иконку и стили в объекте `loginButton` и его свойстве `customStyles`.

Принцип	Что это значит	Где и как это применить
Структура цветов	Цветовая схема для любого элемента описывается единообразно.	Всегда используйте вложенный объект `color` с полями `text`, `background` и `hover` (например, `color: {text: "#fff", background: "#1976d2"}`).
Управление отображением	Можно легко скрывать текстовые метки или иконки.	Используйте флаги `isHideText` (скрыть текст) и `isHideIcon` (скрыть иконку) в стилях компонента.
Гибкое выравнивание	Содержимое внутри кнопок можно выровнять по левому краю или по центру.	Задайте свойство `position: "left"` или `position: "center"` в стилях нужной кнопки.
Умное наследование	Система сама заполняет пробелы в конфигурации, используя логичные значения по умолчанию.	- Для `secondaryButton`: если стили не заданы, он унаследует `primaryButton` с добавлением прозрачности. - Для `hover`: если цвет не указан, к фону при наведении применится `filter: brightness(90%)`.
Fallback-система	Кнопки в выпадающем меню используют общие стили, если для них не заданы индивидуальные.	Если у кнопки в `menuButtons` нет своего `customStyles`, к ней автоматически применяются стили из `accountButton`.
Глобальное скругление	Единое значение скругления углов можно задать для всех элементов виджета.	Укажите `customStyles.global.borderRadius` (например, `"8px"`), и оно повлияет на кнопки и модальные окна.
Индивидуальная кастомизация	Любую кнопку в меню можно стилизовать совершенно уникально.	Добавьте объект `customStyles` для конкретного элемента в массиве `menuButtons`.

Управление пользователями

Обзор и базовые действия

О разделе «Пользователи»

Список всех пользователей, зарегистрированных в **КриптоАРМ ID**, содержится в разделе **Пользователи**. Здесь администраторы могут управлять учетными записями, просматривать профили и контролировать доступ к системе.

> ⚠ **Требования к доступу**: Раздел доступен в кабинете администратора для пользователей с полномочиями **Администратор** системы.

Создание пользователя в КриптоАРМ ID

> 📌 В **КриптоАРМ ID** возможны несколько способов регистрации пользователей: самостоятельная регистрация через виджет и ручное создание пользователем с правами **Администратор**.

В данной инструкции мы рассмотрим, как вручную создать пользователя:

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Нажмите на кнопку **Создать пользователя**  .
3. Откроется форма создания пользователя.
4. На форме создания заполните поля профиля:
    - **Публичное имя** — отображаемое имя пользователя в системе;
    - **Имя** — имя и отчество пользователя;
    - **Фамилия** — фамилия пользователя;
    - **Логин** — должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;
    - **Электронная почта** — адрес должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;
    - **Номер телефона** — должен быть уникальным для сервиса, в дальнейшем с его помощью можно авторизоваться;
    - **Пароль** — должен соответствовать парольной политике, заданной в настройках сервиса.

        > 🔗 Подробнее в инструкции Настройка парольной политики.

- **Дата рождения**;
- **Фото профиля**.

5. Нажмите **Сохранить**.

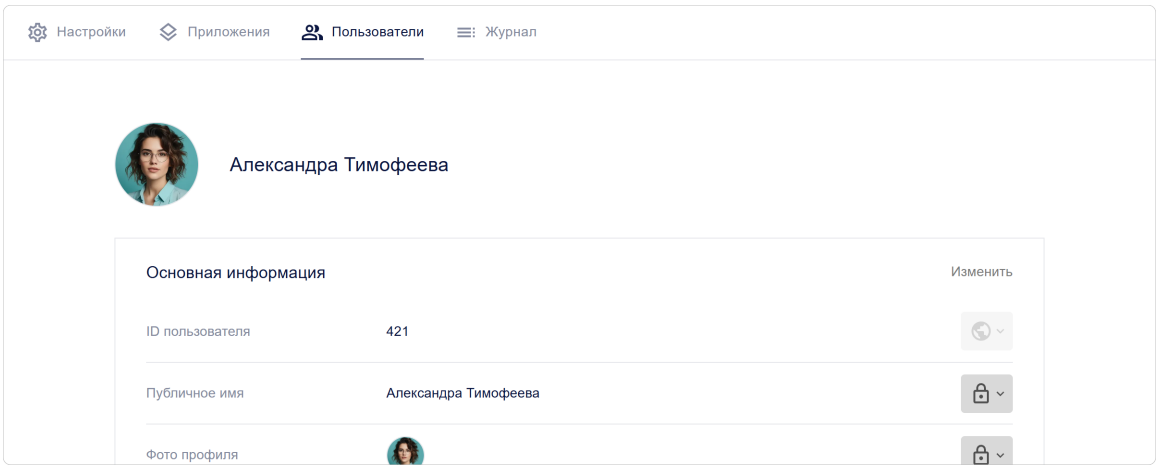
> 📌 Валидация полей осуществляется по правилам валидации. Подробнее в инструкции Правила валидации полей.

Просмотр и редактирование профиля пользователя

Просмотр профиля пользователя

Чтобы получить детальную информацию об аккаунте, откройте его профиль.

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Нажмите на панель с пользователем, профиль которого необходимо просмотреть.
3. Откроется профиль пользователя с детальной информацией: контактные данные, идентификаторы, настройки публичности.



Редактирование данных профиля

Для внесения изменений в профиль пользователя:

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Изменить** в блоке **Основная информация**.
4. В открывшейся форме **Редактировать пользователя** внесите необходимые изменения.
5. Нажмите **Сохранить**.

Управление данными профиля

Управление идентификаторами профиля

В разделе **Идентификаторы** профиля пользователя отображаются способы входа пользователя, которые он добавил самостоятельно или использовал для входа в приложение или в личный кабинет **КриптоАРМ ID**. Администратор может настроить публичность идентификатора и удалить его из профиля пользователя.

> **Важно:** Добавлять новые идентификаторы может только владелец аккаунта.

Чтобы удалить идентификатор:

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите **Удалить** на панели со способом входа, который необходимо удалить из профиля.

Идентификатор будет немедленно удален из профиля.

Настройка публичности полей профиля

В каждом поле профиля можно настроить уровень публичности, определяющий, кто сможет видеть эту информацию. Доступны настройки для основных и дополнительных данных о пользователе, а также для способов входа.

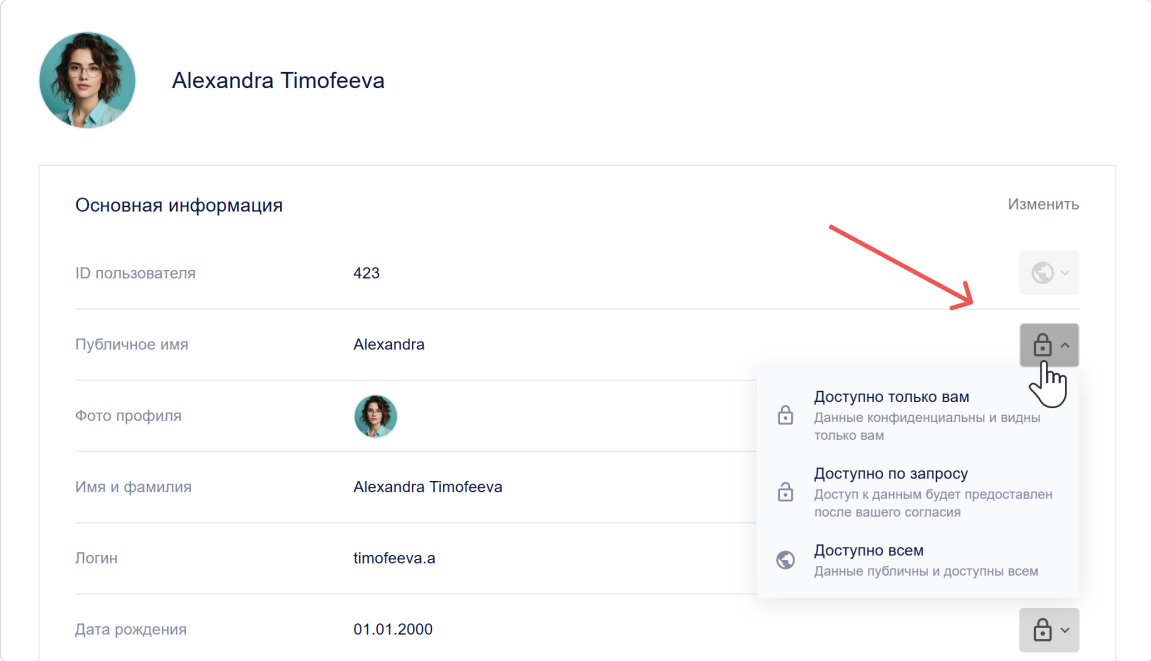
Уровни публичности

Уровень	Иконка	Описание
Доступно только вам		Данные не передаются в сторонние системы и доступны только пользователю.
Доступно по запросу		Данные доступны в сторонних системах, с которыми настроена интеграция **КриптоАРМ ID**. Для доступа к данным требуется согласие пользователя.

Уровень	Иконка	Описание
Доступно всем		Данные публичны всегда. Для доступа к ним не требуется согласие пользователя.

Как изменить публичность поля профиля

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Нажмите на текущую иконку публичности рядом с полем.
4. В выпадающем меню выберите новый уровень.



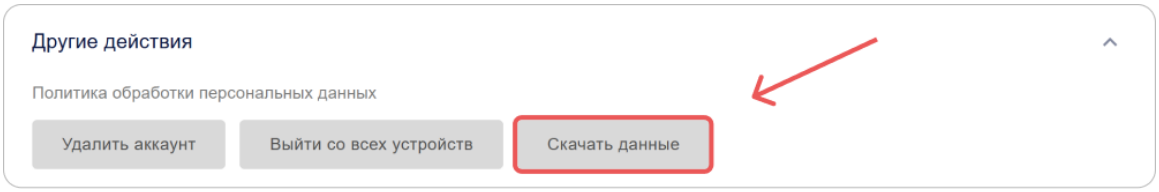
Изменение применяется мгновенно.

Экспорт данных профиля

КриптоАРМ ID позволяет экспортировать все данные профиля в JSON формате.

Чтобы скачать данные профиля:

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Откройте профиль пользователя.
3. Раскройте блок **Другие действия**.



4. Выберите действие **Скачать данные**.

5. Загрузка JSON-файла начнется автоматически.

Структура экспортированного файла

Экспортированный файл содержит полный список данных пользователя:


```
{
  "user": {
    "id": 1573,
    "email": "ivanov.petr89@mail.com",
    "birthdate": "1992-11-14T15:22:11.123Z",
    "family_name": "Иванов",
    "given_name": "Петр",
    "nickname": "Петя",
    "login": "petr_ivanov92",
    "phone_number": "+79991234567",
    "picture":
"public/images/profile/3f7b21d8e4c2a6f1b2c9d3a0e5f7b1c4",
    "public_profile_claims_oauth": "id email family_name given_name
picture",
    "public_profile_claims_gravatar": "family_name given_name email
picture",
    "blocked": false,
    "deleted": null,
    "custom_fields": {
      "country": "Россия"
    },
    "password_updated_at": "2025-10-12T08:45:33.222Z"
  },
  "role": "ADMIN"
}
```


Доступ и безопасность

Завершение сеансов пользователя

Функция принудительного завершения всех активных сессий — важный инструмент безопасности. Используйте его в случае утери устройства, подозрения на взлом

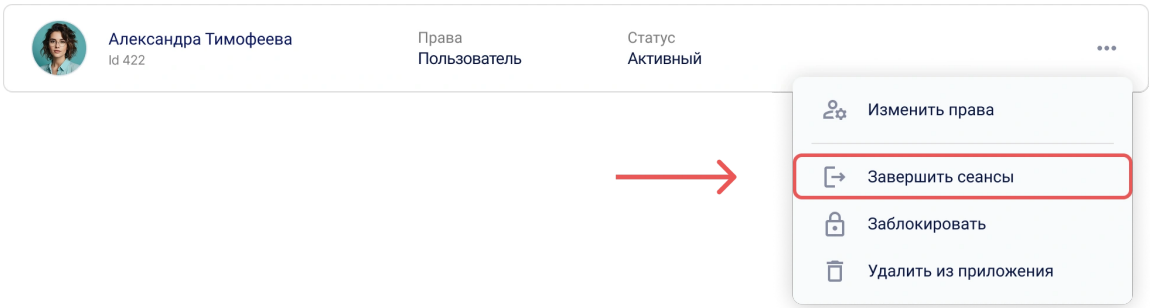
аккаунта или для немедленного обновления токенов доступа.

> 📌 Эта операция немедленно аннулирует все access- и refresh-токены пользователя, завершая все его текущие сессии во всех приложениях. Пользователю потребуется войти заново.

Как завершить сеансы пользователя

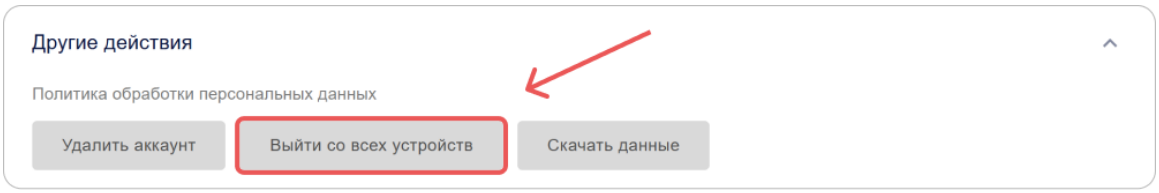
Способ 1: Из общего списка пользователей

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Нажмите **Завершить сеансы** в меню действий с пользователем.



Способ 2: Из профиля пользователя

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Нажмите **Завершить сеансы** в профиле пользователя в блоке **Другие действия**.



Что происходит после подтверждения:

- **Все активные сессии** пользователя завершаются
- **Токены доступа** (`access_token`) становятся недействительными
- **Токены обновления** (`refresh_token`) аннулируются
- Пользователю потребуется **войти заново** при следующем обращении к приложению

> 📌 Эта операция не блокирует пользователя. Он сможет авторизоваться снова.

Назначение и изменение полномочий пользователей

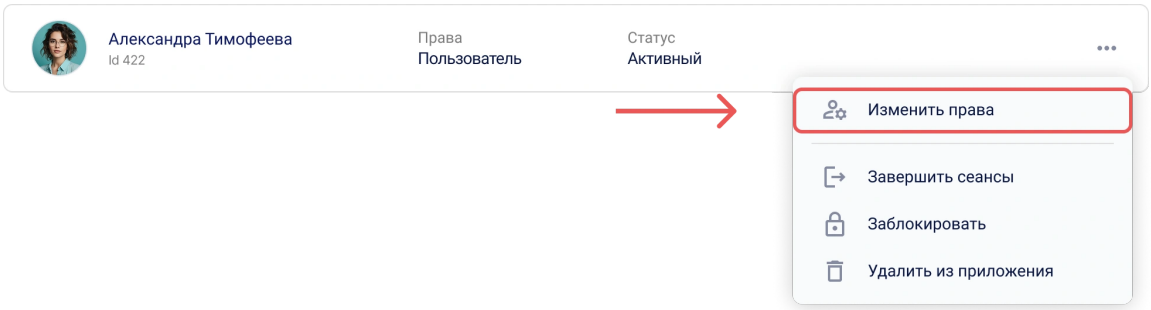
В КриптоАРМ ID действует трехуровневая система доступа, которая четко разграничивает права пользователей:

- **Участник** — базовая роль. Позволяет управлять своим профилем, настраивать разрешения на доступ к личным данным и использовать аккаунт для входа в интегрированные приложения.
- **Управленец** — роль администратора отдельной организации или подразделения. Управляет пользователями и доступом к приложениям в рамках своей организационной единицы.
- **Администратор** — роль с максимальными привилегиями. Предоставляет полный доступ ко всем функциям платформы, включая глобальные настройки безопасности и управление всеми организациями.

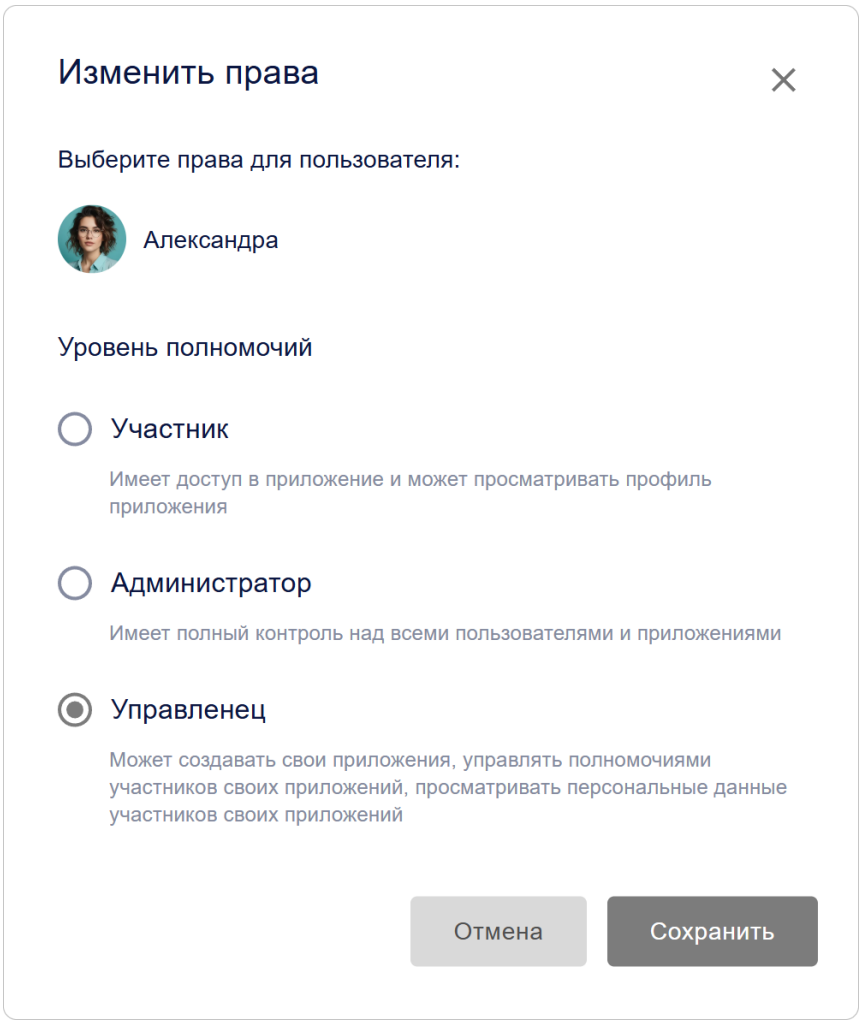
Ниже приведены инструкции по назначению ролей **Управленец** и **Администратор** системы.

Назначение полномочий «Управленец»

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Вызовите меню действий по кнопке **Еще** для пользователя, права которого необходимо изменить.
3. Выберите действие **Изменить права**.



4. В открывшемся окне выберите роль **Управленец** и нажмите **Сохранить**.



Пользователь получит выбранную роль и соответствующие ей права.

Назначение полномочий «Администратор» системы

1. Перейдите в кабинет администратора → вкладка **Пользователи**.
2. Вызовите меню действий по кнопке **Еще** для пользователя, права которого необходимо изменить.
3. Выберите действие **Изменить права**.
4. В открывшемся окне выберите роль **Администратор** и нажмите **Сохранить**.

Пользователь получит выбранную роль и соответствующие ей права.

> 🔍 Для назначения полномочий **Администратор** приложения воспользуйтесь инструкцией.

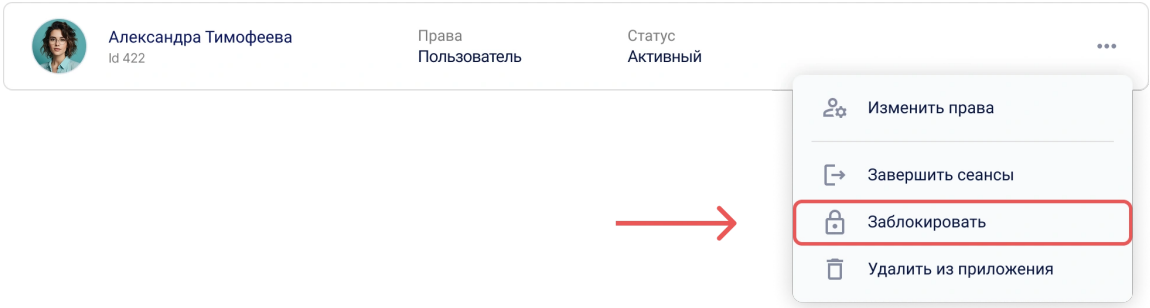
Статус аккаунта

Блокирование пользователей КриптоАРМ ID

Блокировка запрещает доступ ко всем сервисам, использующим **КриптоАРМ ID** для входа.

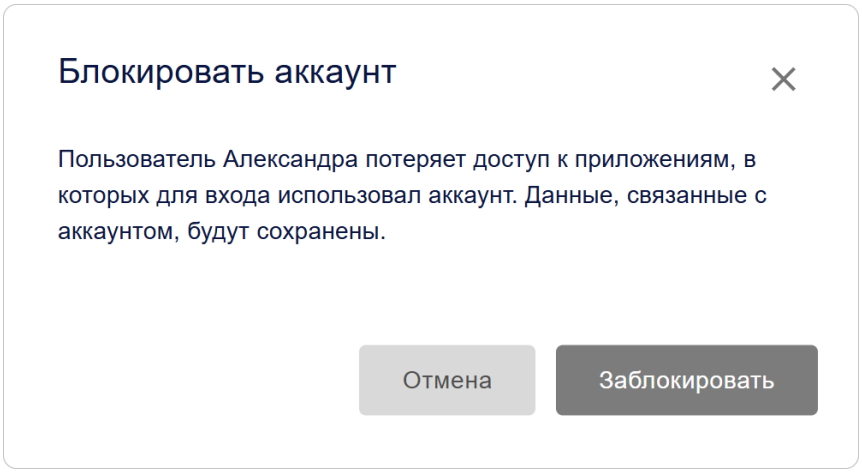
Чтобы заблокировать пользователя:

1. Вызовите меню действий с активным пользователем в одном из интерфейсов:
    - В меню действий с пользователем в профиле приложения.
    - В меню действий с пользователем на вкладке **Пользователи**.



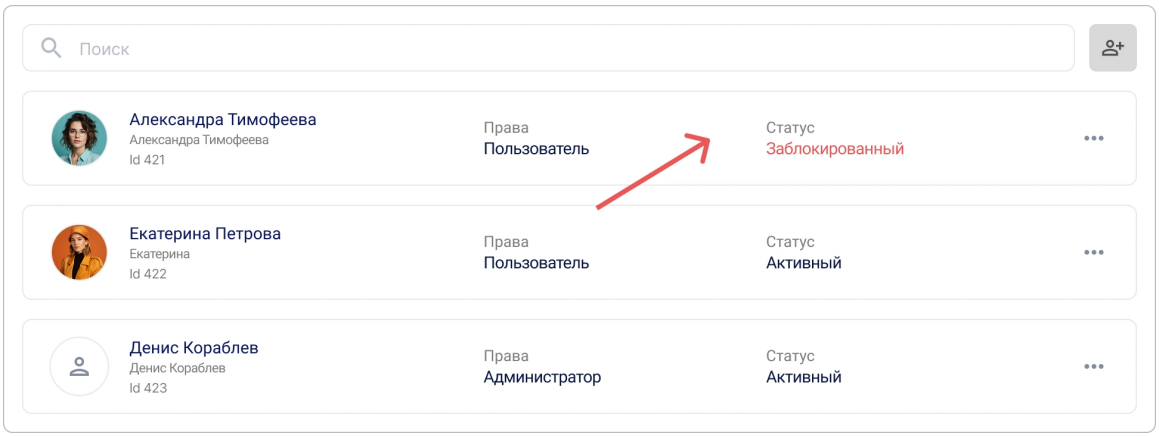
2. Выберите действие **Блокировать в КриптоАРМ ID**.

3. Подтвердите действие в модальном окне.



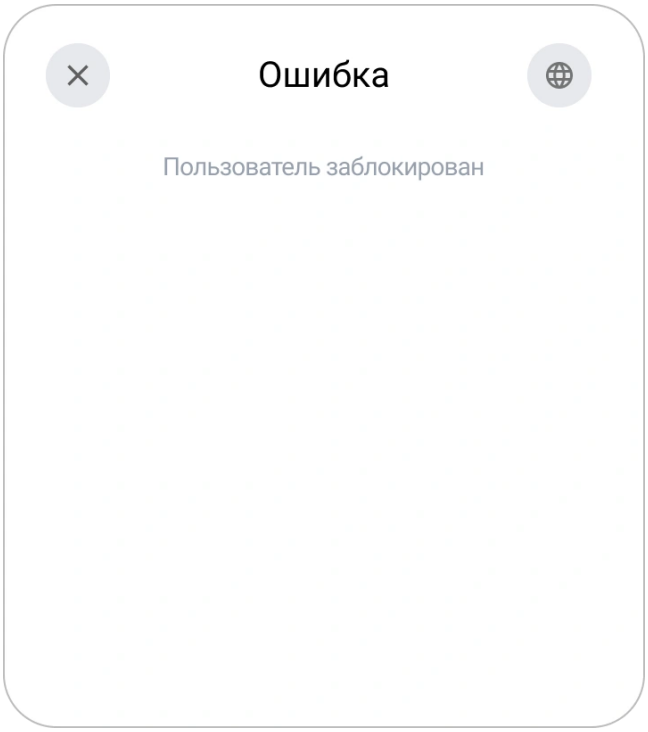
Что происходит после блокировки:

- Статус пользователя изменится на **Заблокированный**.



- Заблокированный пользователь не сможет войти в сервис и приложения.

При попытке входа будет отображаться следующий виджет:



Разблокирование пользователей КриптоАРМ ID

Чтобы разблокировать пользователя:

1. Вызовите меню действий с заблокированным пользователем в одном из интерфейсов:
    - В меню действий с пользователем в профиле приложения.
    - В меню действий с пользователем на вкладке **Пользователи**.
2. Выберите действие **Разблокировать в КриптоАРМ ID**.
3. Подтвердите действие в модальном окне.

После подтверждения действия статус пользователя изменится на **Активный**.

Удаление пользователя

Администратор может навсегда удалить пользователя. После подтверждения удаления аккаунт и все данные исчезнут безвозвратно. Пользователь потеряет доступ ко всем приложениям, где использовался его аккаунт **КриптоАРМ ID**.

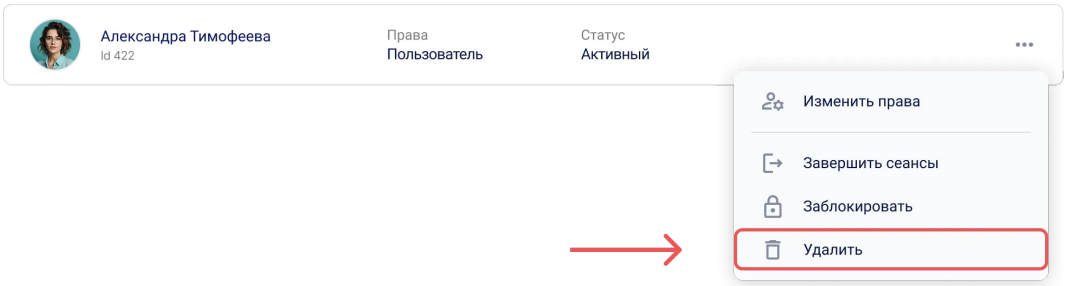
> 💡 Пользователь может самостоятельно удалить свой аккаунт через личный профиль. Удаление реализовано с **механизмом отсрочки**. В течение определенного времени пользователь может восстановить доступ к своему аккаунту.

Как удалить пользователя КриптоАРМ ID

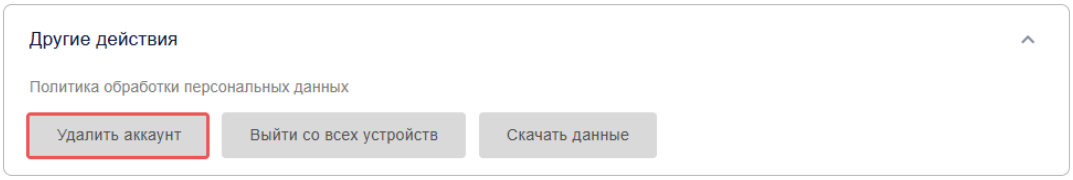
> 💡 **Альтернатива**: Рассмотрите возможность **блокировки аккаунта** вместо удаления, если есть вероятность восстановления доступа.

Чтобы удалить пользователя:

1. Нажмите **Удалить аккаунт** в одном из интерфейсов:
    - В меню действий с пользователем на вкладке **Пользователи**.



    - В профиле пользователя в блоке **Другие действия**.



2. Подтвердите действие в модальном окне.

После подтверждения пользователь будет удален.

Что происходит после удаления:

- Приложения, где удаляемый пользователь является единственным владельцем, будут безвозвратно удалены.
- Все данные аккаунта стираются без возможности восстановления после окончательного удаления.
- Пользователь теряет доступ ко всем интегрированным сервисам.

Организация

Управление организацией

Основные понятия об организациях

Организация в **КриптоАРМ ID** — это структурная единица, которая позволяет:

- **Разграничивать доступ** к приложениям между подразделениями или проектами,
- **Настраивать корпоративные способы входа**,
- **Вести централизованный аудит** активности пользователей,
- **Управлять приложениями** в рамках одной компании,
- **Настраивать брендинг** (логотип, название) для виджетов входа.

> 💡 **Использование:** Организации идеально подходят для компаний, которым нужно управлять несколькими приложениями и группами пользователей с единой точки контроля.

Доступ к кабинету организации

Кабинет организации предназначен для управления настройками, приложениями и пользователями организации.

В кабинете организации доступны следующие разделы:

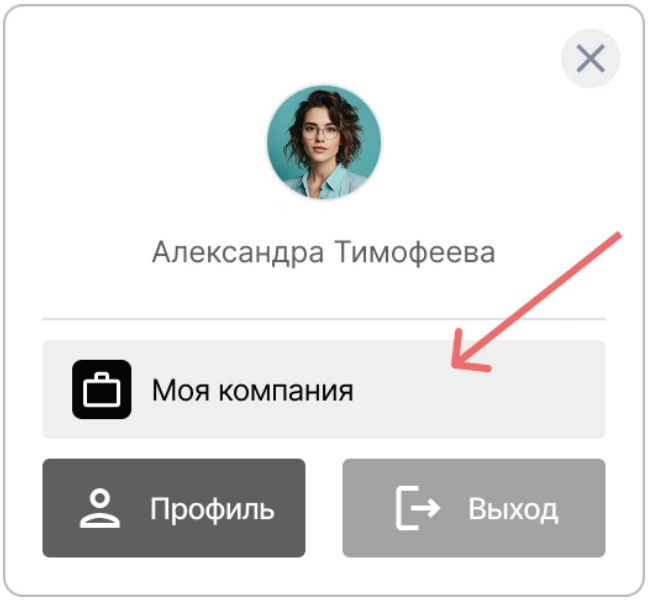
- **Настройки** — параметры организации, способы входа, кастомизация виджета авторизации.
- **Приложения** — управление приложениями организации.
- **Журнал** — история активности пользователей организации.

Как попасть в кабинет организации КриптоАРМ ID

> ⚠ Для доступа в кабинет организации необходимы полномочия **Управленец**. Обратитесь к администратору сервиса для их получения.

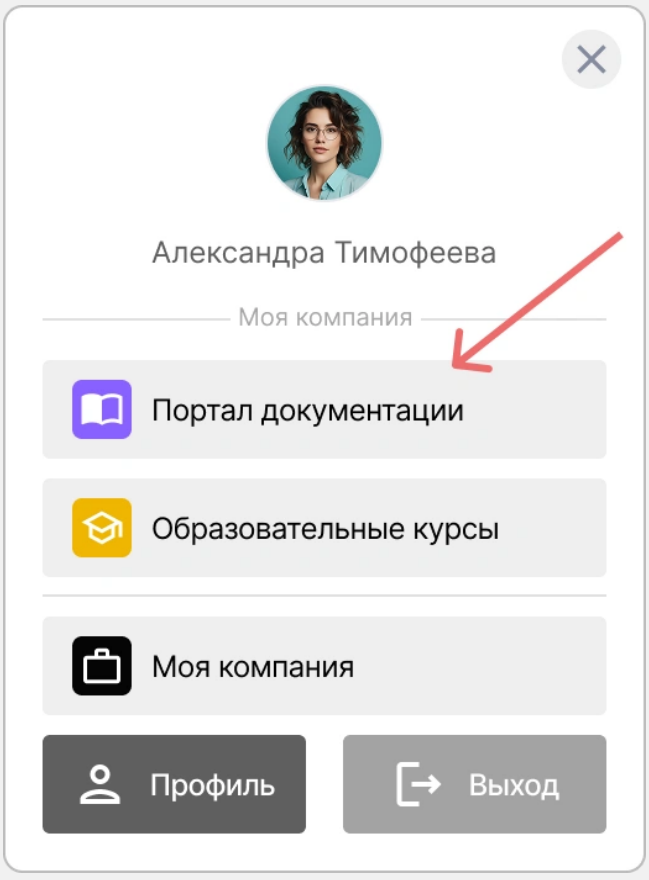
Чтобы открыть кабинет организации:

1. Авторизуйтесь в личном кабинете **КриптоАРМ ID**.
2. Нажмите на свое имя в правом верхнем углу окна.
3. В открывшемся окне мини-виджета нажмите на название своей организации.



Вы будете перенаправлены в **Кабинет организации**.

Добавьте часто используемые приложения в мини-виджет с помощью настройки **Отображать в мини-виджете** для быстрого доступа.



Настройка названия и логотипа организации

Название и логотип отображаются в интерфейсе системы **КриптоАРМ ID**, а также в мини-виджете.

Чтобы настроить название и логотип:

1. Перейдите в кабинет организации → вкладка **Настройки**.
2. Раскройте блок **Основная информация**.
3. Укажите новое название в поле **Название приложения**.
4. В разделе **Логотип приложения** нажмите **Загрузить** и выберите файл с логотипом.

   > Допустимые форматы: JPG, GIF, PNG, WEBP; максимальный размер 1 МБ.

5. Настройте область отображения логотипа.

6. Нажмите **Сохранить**.

Способы входа в организации

Способ входа — это метод аутентификации пользователей, позволяющий им авторизоваться в приложениях.

В организации могут использоваться как публичные способы входа, так и способы входа, созданные для данной организации.

Вы можете:

- Использовать **публичные способы входа**, настроенные администратором **КриптоАРМ ID**
- Добавлять **собственные способы входа** только для вашей организации
- Настраивать **публичность** — определять, где будут доступны ваши способы входа

- Делать идентификаторы **обязательными** для пользователей

> ⚠ **Ограничения:** редактировать публичные способы входа могут только администраторы **КриптоАРМ ID**.

Управление приложениями в организации

> ⚠ **Ограничение**: Управление приложениями доступно в кабинете администратора, организации или приложения (малом кабинете) в зависимости от вашей роли.

Создание приложения

Создание веб-приложения OAuth

> **Веб-приложение** — это стандартное приложение, которое работает в браузере пользователя и взаимодействует с **КриптоАРМ ID** по протоколам OAuth 2.0 и OpenID Connect.

Чтобы создать веб-приложение:

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите кнопку **Создать**  .
4. Откроется форма создания приложения.
5. Укажите обязательные параметры приложения:
   - **Название приложения**,
   - **Адрес приложения** в формате `протокол://доменное имя:порт`,
   - **Возвратный URL #** (`redirect_uris`) — адрес, на который пользователь переадресовывается после авторизации,
   - **URL выхода из системы #** (`post_logout_redirect_uris`) — адрес, на который переадресовывается пользователь после выхода.
6. Нажмите **Создать**.

> 💡 При создании формируются дополнительные поля приложения, которые можно посмотреть и отредактировать в настройках приложения:
>
> - **Идентификатор (client_id)** — используется для идентификации приложения;

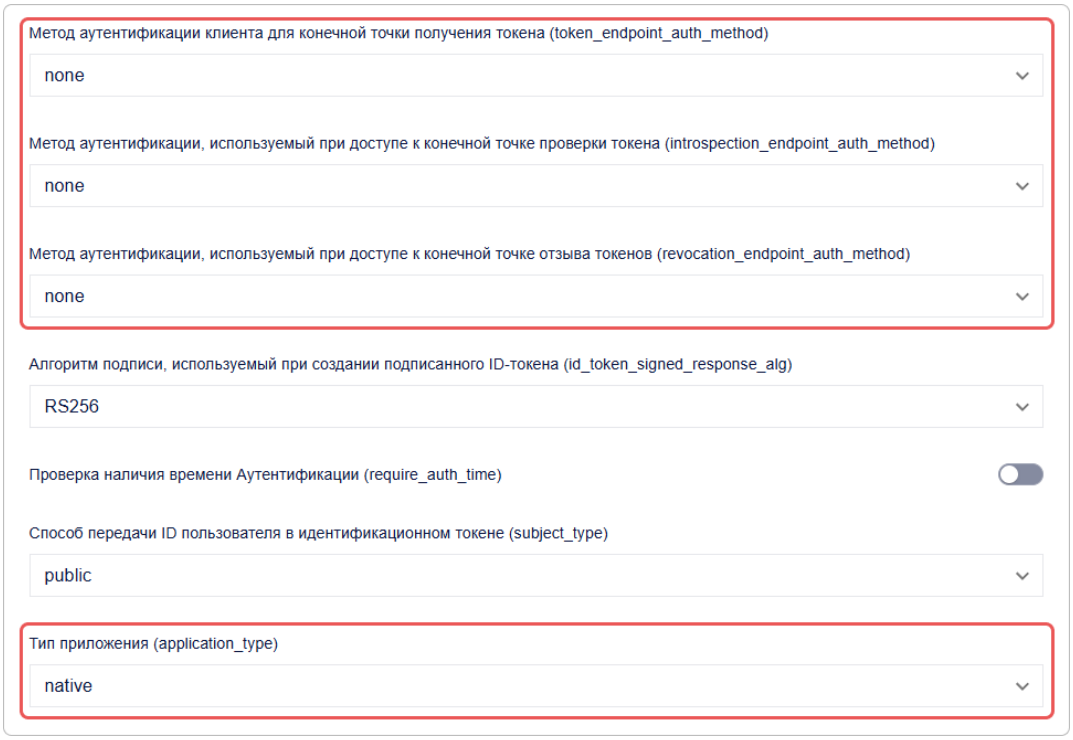
> - **Секретный ключ (client_secret)** — используется для аутентификации подлинности приложения, когда приложение запрашивает доступ к аккаунту пользователя. Секретный ключ должен быть известен только приложению.

Создание нативного OAuth-приложения

> **Нативное приложение** — это приложение, которое разработано специально для определённой операционной системы.

Чтобы создать нативное приложение:

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите кнопку **Создать**  .
4. Откроется форма создания приложения.
5. Укажите обязательные параметры приложения:
   - **Название приложения**,
   - **Адрес приложения** — локальный адрес приложения в формате `myapp://callback` (требуется для завершения создания, но **не используется** в нативных приложениях,),
   - **Возвратный URL #** (`redirect_uris`) — локальный адрес, на который будет возвращён пользователь после авторизации, например, `myapp://callback`,
   - **URL выхода из системы #** (`post_logout_redirect_uris`) — локальный адрес переадресации после выхода (например: myapp://logout).
6. Нажмите **Создать**.
7. Откройте созданное приложение и нажмите на **Редактировать**  .
8. В открывшейся форме редактирования:
   - Выберите `native` в настройке **Тип приложения**;
   - Выберите `none` в настройках с методами аутентификации.



9. Сохраните изменения.

Дальше настройте авторизацию на стороне вашего приложения:

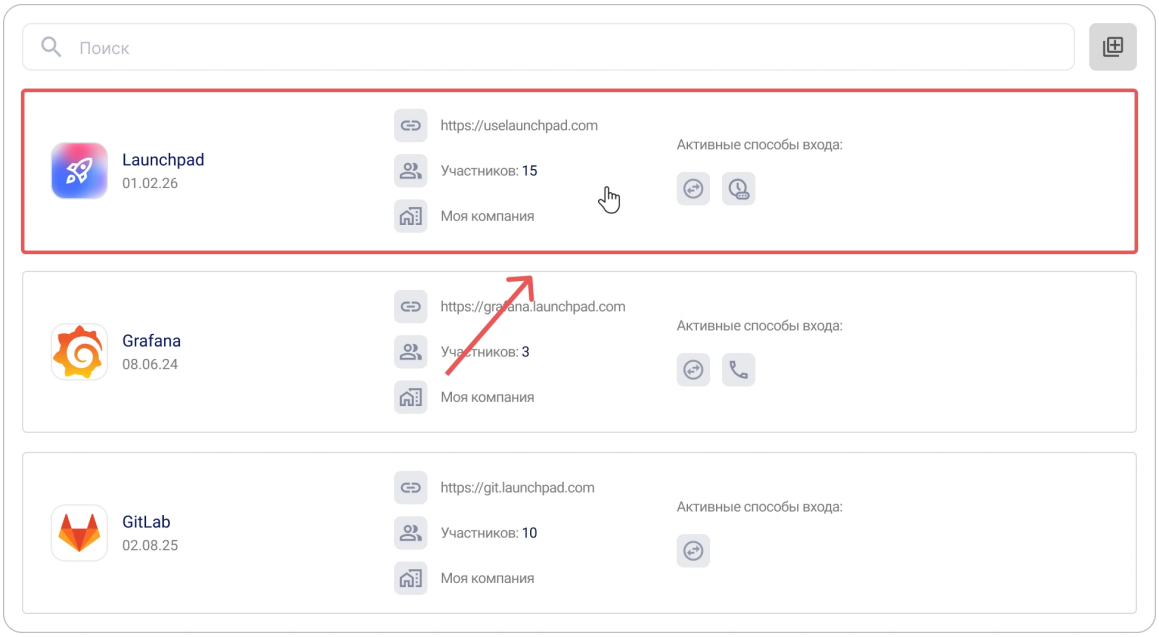
- используйте PKCE (Proof Key for Code Exchange) при запросе авторизационного кода;
- используйте ранее указанный `redirect_uri` для обработки результата авторизации;
- выполняйте обновление токена по протоколу OAuth 2.0.

Приложения

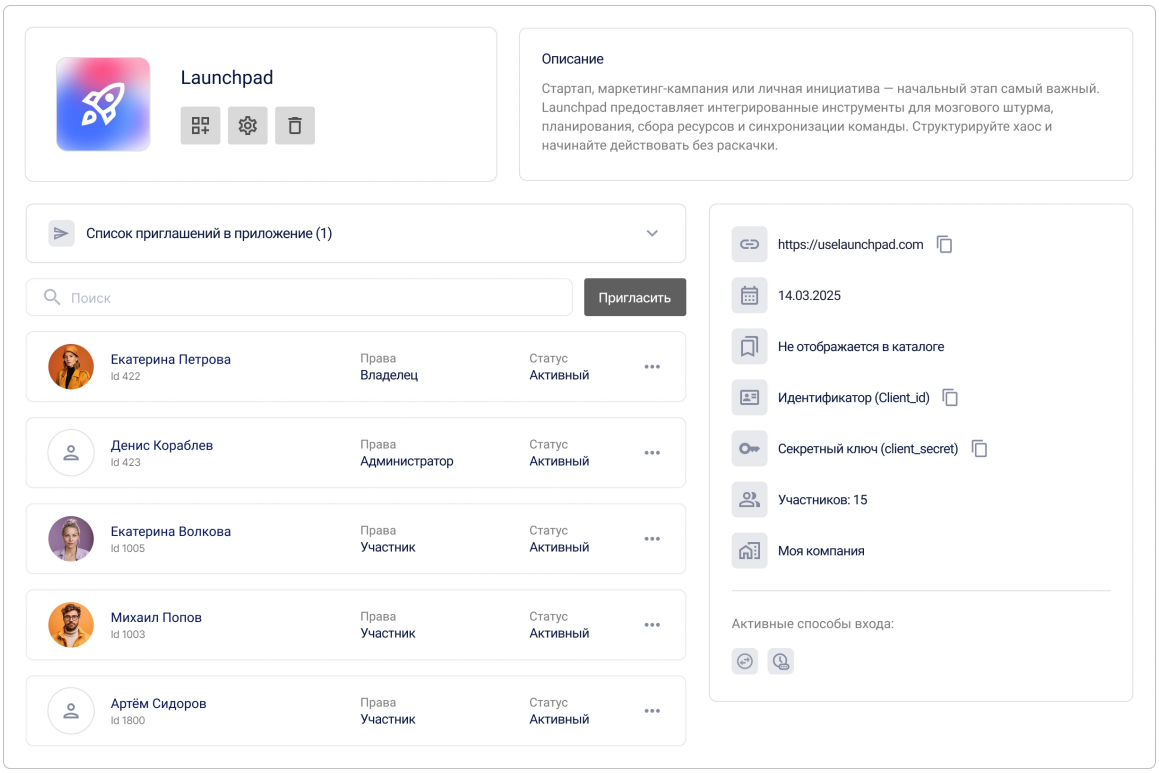
Управление приложениями

Просмотр приложения

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением, профиль которого необходимо просмотреть.



4. Откроется форма с профилем приложения.



Редактирование приложения

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением, которое необходимо отредактировать.
4. Откроется форма просмотра приложения.
5. Нажмите на кнопку **Редактировать**  .
6. Откроется форма редактирования приложения.
7. Внесите необходимые изменения в параметры приложения.
8. Сохраните изменения.

Удаление приложения

> ⚠ **Внимание:** Удаление приложения — необратимая операция. Все связанные данные будут удалены из системы.

Чтобы удалить приложение:

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением, которое необходимо отредактировать.
4. Откроется форма просмотра приложения.

5. Нажмите на кнопку **Удалить**  .
6. Подтвердите действие в модальном окне.

После подтверждения действия приложение удалится из **КриптоАРМ ID**.

Приглашения в приложения

Механизм приглашений позволяет ограничить доступ к приложению и предоставлять его только заранее выбранным пользователям. Это удобно, если приложение предназначено для **закрытого круга пользователей**.

Включение ограничения доступа

Чтобы сделать приложение доступным только для приглашенных пользователей:

1. Откройте форму редактирования приложения. Как открыть форму редактирования →
2. Включите настройку **Запрет доступа для внешних пользователей**
3. Сохраните изменения.

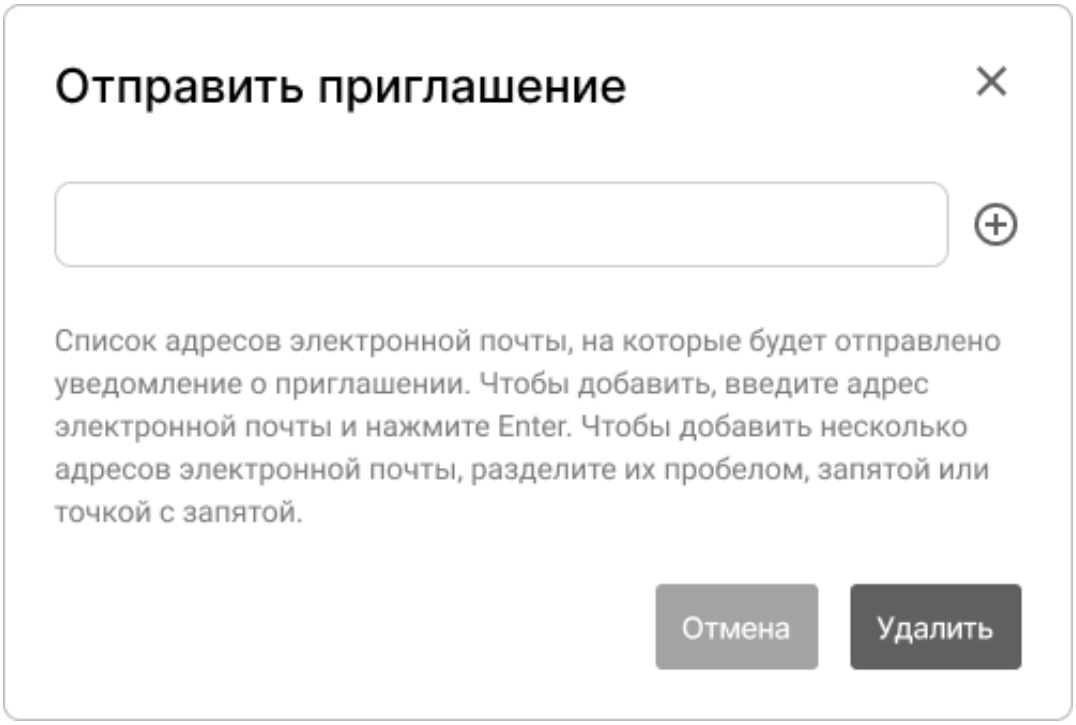
Что происходит после включения:

- Участники приложения — могут войти как обычно.
- Неприглашенные пользователи — видят сообщение об отказе в доступе.
- Новые пользователи — могут войти только после получения приглашения.

Отправка приглашений пользователям

Чтобы отправить приглашение пользователю:

1. Откройте форму просмотра приложения. Как открыть форму просмотра →.
2. Нажмите кнопку **Пригласить**.
3. В открывшемся окне укажите email-адреса пользователей:
    - введите адрес и нажмите **Enter**, либо кнопку  ;
    - для добавления нескольких адресов используйте разделители: пробел, запятую `,`, точку с запятой `;`.



4. Нажмите **Отправить**.

На указанные email-адреса отправляется письмо с ссылкой для быстрого перехода в приложение.

> Приглашения будут активны до отмены или принятия.

Что видят пользователи

Пользователь, получивший приглашение, получает email с письмом, содержащим ссылку для входа в приложение. Приглашение также отображается в разделе **Запросы** личного профиля пользователя. Принять приглашение можно двумя способами: перейдя по ссылке из письма или выбрав приглашение в разделе «Запросы» профиля.

> Как принять приглашение в приложение →

Приглашение защищено механизмом проверки: оно действует только для того email-адреса, на который было отправлено. Пользователь должен войти в систему именно под этим адресом, чтобы принять приглашение. Это предотвращает передачу доступа другим лицам.

Если пользователь еще не зарегистрирован в системе, ему необходимо зарегистрироваться, указав тот же email, на который пришло приглашение. После успешной регистрации доступ к приложению предоставляется автоматически.

Управление приглашениями

Просмотр списка отправленных приглашений

1. Откройте форму просмотра приложения. Как открыть форму просмотра →.
2. Раскройте раздел **Список отправленных приглашений в приложение**

Для каждого приглашения в списке отображается:

- Email получателя
- Дата отправки

Отмена приглашения

Если нужно отозвать отправленное приглашение:

1. Найдите приглашение в списке отправленных.
2. Нажмите кнопку **Удалить**  на панели с приглашением.
3. Подтвердите отмену приглашения.

Последствия отмены:

- Ссылка в письме становится недействительной
- Пользователь не сможет принять приглашение

Настройка виджета входа в приложение

Виджет входа — это форма авторизации, которую видят пользователи при попытке войти именно в **это приложение**. Его настройки позволяют адаптировать внешний вид и способы входа под бренд и потребности вашего сервиса.

Как найти настройки виджета

1. Откройте форму редактирования приложения. Как открыть форму редактирования →
2. Найдите блок **Способы входа** и нажмите **Настроить**.

Что можно настроить:

- **Заголовок и обложка** — адаптируйте под бренд приложения,
- **Цветовая схема** — цвета кнопок, соответствующие вашему дизайну,
- **Способы входа** — выберите, какие провайдеры показывать,
- **Информационные блоки** — добавьте правила использования или ссылки.

> **Полное руководство по всем настройкам:**
> Для детального ознакомления со всеми параметрами и возможностями кастомизации перейдите к полному руководству по настройке виджета входа →.

Пользователи приложения

Пользователи приложения (участники) — это пользователи системы **КриптоАРМ ID**, которые предоставили вашему приложению разрешение на доступ к своим данным.

Как пользователь становится участником:

1. Пользователь впервые обращается к вашему приложению.
2. Система перенаправляет его на виджет входа **КриптоАРМ ID**.
3. Пользователь проходит аутентификацию и **дает согласие** на доступ к запрашиваемым данным.
4. Приложение получает токен доступа, а пользователь добавляется в список участников.

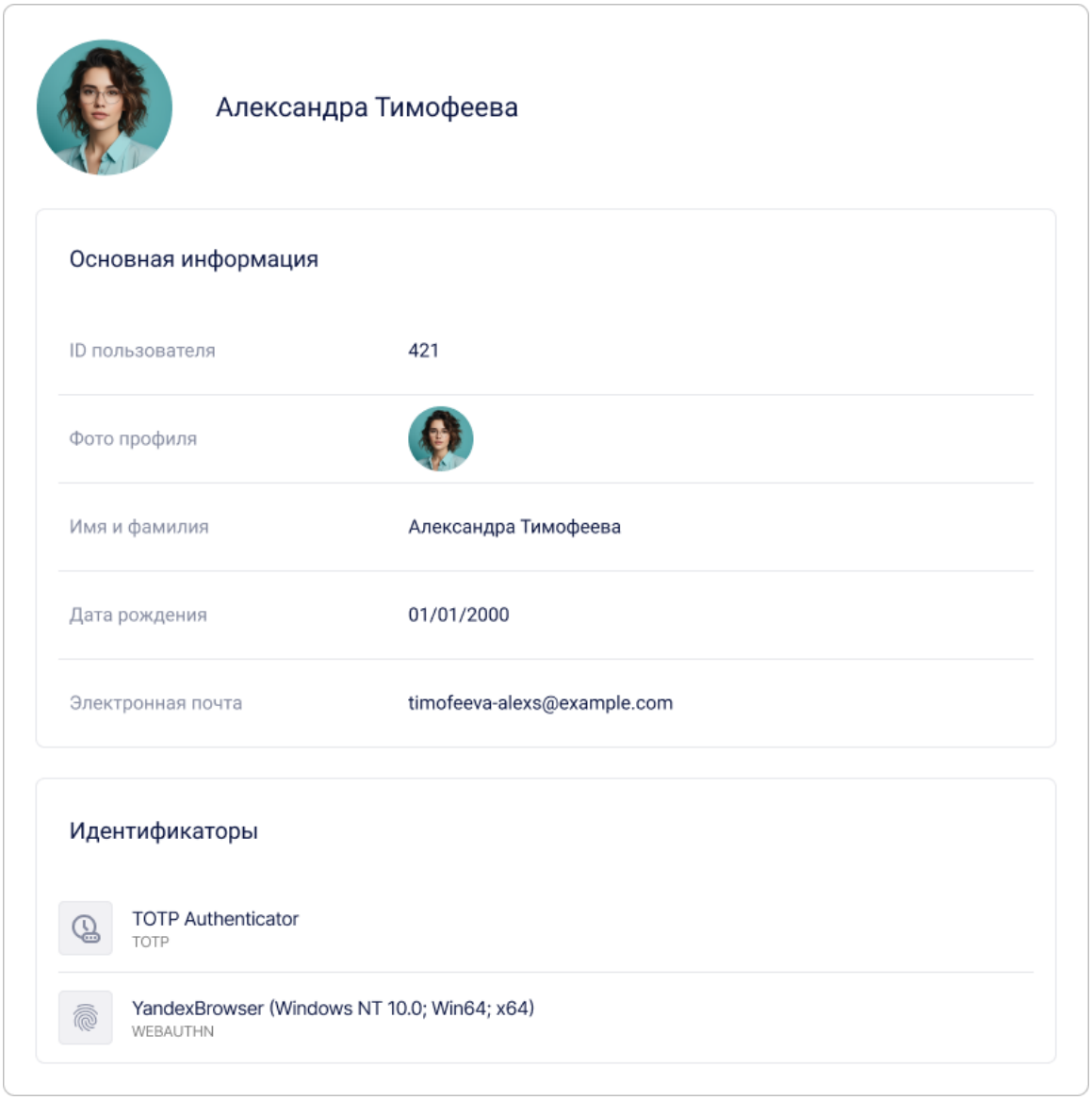
Где управлять участниками:

- **Кабинет администратора** — для управления всеми приложениями сервиса
- **Кабинет организации** — для приложений, принадлежащих организации
- **Малый кабинет (приложения)** — для управления конкретным приложением

> **Важно:** Управление участниками происходит на уровне **приложения**. Действия не влияют на глобальный аккаунт пользователя в **КриптоАРМ ID**, а только на его связь с конкретным приложением.

Просмотр участников приложения

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с нужным приложением.
4. Откроется профиль приложения с общей информацией.
5. В профиле приложения найдите раздел с участниками.
6. Нажмите на панель с пользователем, профиль которого необходимо просмотреть.
7. Откроется профиль пользователя, содержащий перечень данных, доступ к которым предоставил пользователь.



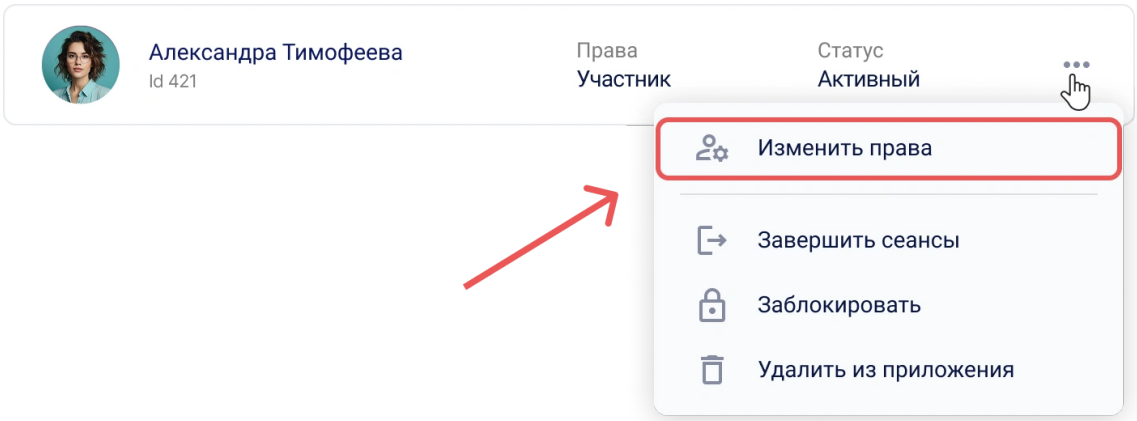
Назначение администратора приложения

Когда это нужно: Чтобы делегировать права управления приложением доверенным пользователям. Администраторы приложения могут управлять его настройками и пользователями.

Чтобы назначить администратора приложения:

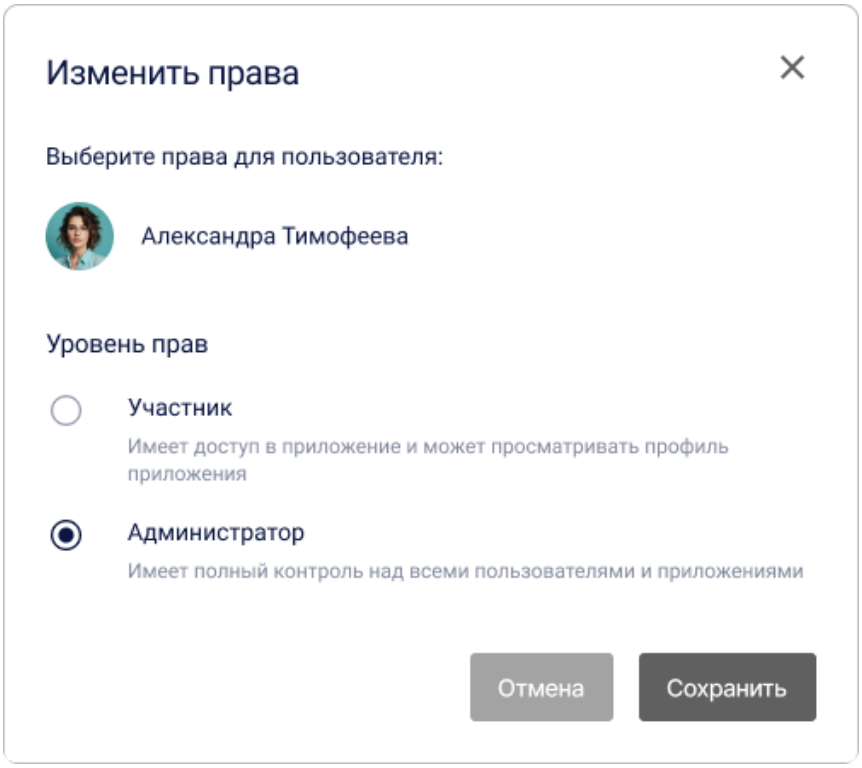
1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением.
4. Откроется профиль приложения.

5. Вызовите меню действий для пользователя, которому необходимо изменить полномочия.



6. Выберите действие **Изменить права**.

7. В появившемся окне выберите уровень полномочий **Администратор**.



8. Нажмите **Сохранить**.

После сохранения изменений полномочия пользователя в приложении будут изменены.

☑ **Что изменится:**

- Пользователь получит доступ к **Малому кабинету** этого приложения
- Сможет управлять настройками приложения и его пользователями
- Не получит доступ к другим приложениям или настройкам организации/сервиса

> ⚠ **Безопасность:** Назначайте права администратора только доверенным пользователям. Администратор приложения может удалять других пользователей и изменять настройки интеграции.

Завершение сеансов пользователя в приложении

Когда это нужно: При подозрении на компрометацию аккаунта, утечке устройства или для принудительного обновления токенов доступа.

Чтобы завершить сеансы пользователя:

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением.
4. Откроется профиль приложения.
5. Вызовите меню действий для пользователя, которому необходимо завершить все сеансы.
6. Выберите действие **Завершить сеансы**.
7. Подтвердите действие в модальном окне.

После подтверждения все сессии и токены для пользователя будут удалены.

☑ **Что происходит после подтверждения:**

- **Все активные сессии** пользователя в этом приложении завершаются
- **Токены доступа** (`access_token`) становятся недействительными
- **Токены обновления** (`refresh_token`) аннулируются
- Пользователю потребуется **войти заново** при следующем обращении к приложению

> 📌 Эта операция не блокирует пользователя. Он сможет авторизоваться снова.

Удаление пользователя из приложения

Когда это нужно: Когда пользователю больше не нужен доступ к приложению, при увольнении сотрудника или по запросу пользователя.

Чтобы удалить пользователя из приложения:

1. Перейдите в кабинет администратора, организации или приложения (малый кабинет).
2. Откройте вкладку **Приложения**.
3. Нажмите на панель с приложением.
4. Откроется профиль приложения.

5. Вызовите меню действий для пользователя, которого необходимо удалить из приложения.
6. Выберите действие **Удалить пользователя**.
7. Подтвердите действие в модальном окне.

После подтверждения пользователь будет удален из приложения.

☑ **Что происходит после удаления:**

- Пользователь **исчезает** из списка участников приложения
- Все его **токены доступа** к этому приложению аннулируются
- При следующем обращении к приложению ему **снова покажут запрос на согласие**
- **Глобальный аккаунт** пользователя в **КриптоАРМ ID** остается нетронутым

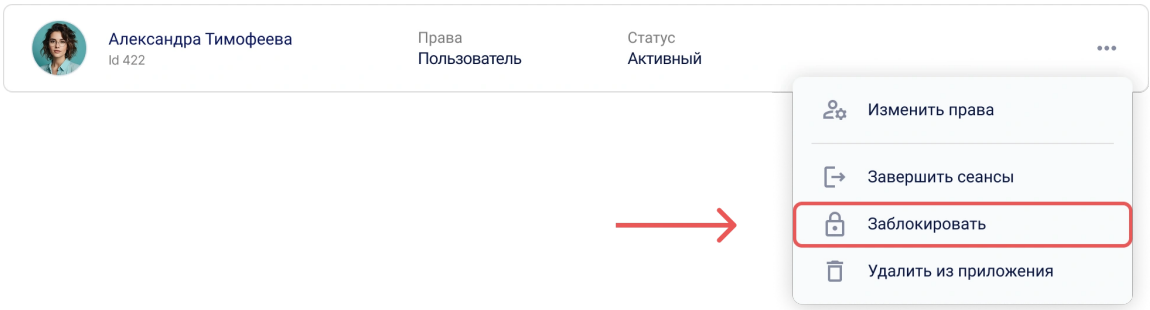
Блокировка пользователя в приложении

Когда это нужно: Для полного и постоянного запрета доступа пользователя к приложению без возможности восстановления.

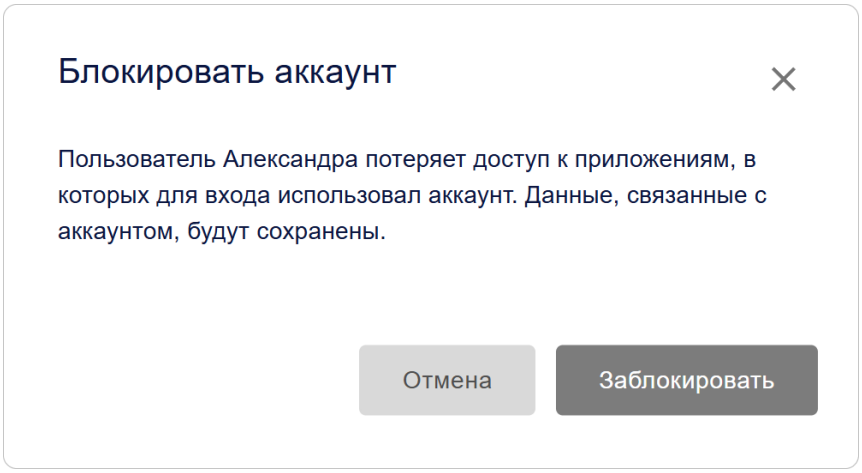
Блокировка — это более серьезное действие, чем удаление. Заблокированный пользователь не сможет получить доступ к приложению.

Чтобы заблокировать пользователя:

1. Вызовите меню действий с активным пользователем в профиле приложения.



2. Выберите действие **Блокировать в КриптоАРМ ID**.
3. Подтвердите действие в модальном окне.



Что происходит после блокировки:

- Статус пользователя изменится на **Заблокированный**.
- Заблокированный пользователь не сможет войти в приложение.

Разблокирование пользователей КриптоАРМ ID

Чтобы разблокировать пользователя:

1. Вызовите меню действий с заблокированным пользователем в профиле приложения.
2. Выберите действие **Разблокировать в КриптоАРМ ID**.
3. Подтвердите действие в модальном окне.

После подтверждения действия статус пользователя изменится на **Активный**.

Полный справочник параметров приложения

Основная информация

Базовые сведения для отображения в интерфейсе и на виджете входа.

Параметр	Описание	Тип	Обязательность
Название приложения	Отображается в интерфейсе личного кабинета и виджете входа	Текст (до 64 символов)	✓
Описание приложения	Краткое описание, отображаемое в интерфейсе сервиса **КриптоАРМ ID**	Текст (до 255 символов)	✗

Параметр	Описание	Тип	Обязательность
Логотип приложения	Отображается в интерфейсе сервиса **КриптоАРМ ID** и виджете входа	Изображение в формате JPG, GIF, PNG, WEBP. Максимальный размер - 1 МБ.	X
Отображать в мини-виджете	Добавляет приложение в мини-виджет для быстрого перехода к нему.	Переключатель (Вкл/Выкл)	-

Каталог

Настройки публикации приложения в **Каталоге**.

Параметр	Описание	Тип	По умолчанию
Отображать в каталоге	Добавляет приложение в Каталог	Переключатель (Вкл/Выкл)	Выкл
Тип приложения	Категория, к которой относится приложение в **Каталоге**. Создание типов доступно **Администратору** сервиса.	Выпадающий список	Прочие

Обязательные поля

Поля профиля пользователя, необходимые для работы приложения.

Параметр	Описание
Основные поля профиля	Определяет список основных и дополнительных полей профиля пользователя, наличие и доступ к которым необходим приложению. - Если поля отсутствуют в профиле пользователя, то их заполнение будет запрошено при авторизации в приложении - Если поля присутствуют в профиле, но для них установлен уровень публичности **Доступно только вам**, пользователю будет предложено изменить этот уровень на **Доступно по запросу**

Параметры приложения

Технические параметры, влияющие на взаимодействие приложения с **КриптоАРМ ID**.

Основные идентификаторы

Название	Параметр	Описание	Тип	Обязательность
Идентификатор (client_id)	`client_id`	Уникальный идентификатор приложения	Текст	Генерируется автоматически
Секретный ключ (client_secret)	`client_secret`	Приватный ключ клиента. Необходимо хранить в безопасности.	Текст	Генерируется автоматически
Адрес приложения	-	URL веб-ресурса, на котором будет использоваться вход через **КриптоАРМ ID**	Текст в формате `протокол://доменное имя:порт`	✓

Настройки доступа

Название	Параметр	Описание	Тип	По умолчанию
Ограниченный доступ	-	Если включено, вход в приложение будет доступен только для пользователей с правами **Администратор**	Переключатель (Вкл/Выкл)	Выкл
Запрет доступа для внешних пользователей	-	Если включено, доступ к приложению будет только у участников или по приглашениям	Переключатель (Вкл/Выкл)	Выкл

Возвратный URL

Название	Параметр	Описание	Обязательность
Возвратный URL #	`Redirect_uri`	URL, на который **КриптоАРМ ID** будет перенаправлять пользователя после аутентификации. После того как пользователь аутентифицируется и даст согласие на доступ к своим данным, сервер перенаправляет пользователя обратно на **Redirect_uri** с кодом авторизации, ID токеном или другой информацией, в зависимости от запрошенного **response_type**.	✓

URL выхода из системы

Название	Параметр	Описание	Обязательность
URL выхода из системы #	`post_logout_redirect_uri`	URL, на который сервис будет перенаправлять пользователя после выхода. Если значение не указано, то используется **Возвратный URL (Redirect_uri)**	✗

URL запроса аутентификации

Название	Параметр	Описание	Обязательность

Название	Параметр	Описание	Обязательность
URL запроса аутентификации или восстановления после аутентификации #	`request_uris`	Список URL, где размещены JWT-запросы авторизации. Когда система отправляет запрос на авторизацию серверу, она может просто указать параметр `request_uri`, который ссылается на один из URL-адресов, определенных в этом списке. Сервер затем извлекает объект запроса JWT по этому URL для обработки запроса.	X

Тип ответов

Название	Параметр	Описание
Тип ответов (response_types)	`response_types`	Определяет, какие токены возвращаются клиенту. - `code` — только код авторизации; - `id_token` — только ID токен; - `code id_token` — код и ID токен; - `code token` — получит код авторизации и токен доступа; - `code id_token token` — полный набор; - `none` — используется, когда не требуется получения кода авторизации, токена доступа или ID токена через перенаправление. Может быть полезным в случаях, когда необходимо подтвердить аутентификацию пользователя, но не требуется доступ к его данным.

Типы предоставления доступа

Название	Параметр	Описание

Название	Параметр	Описание
Типы предоставления доступа (grant_types)	`grant_types`	Способ получения авторизации для доступа к защищенным ресурсам. - `authorization code` — стандартный и безопасный метод; - `implicit` — устаревающий вариант без серверного обмена; - `refresh_token` — обновление токена без повторного входа.

Методы аутентификации

Название	Параметр	Опис
Метод аутентификации клиента для конечной точки получения токена (token_endpoint_auth_method)	`token_endpoint_auth_method`	Метс клие аутен обра endp авто - non пред учет обра endp испо клие конф хран данн аутен треб - clie - отп учет теле -

Название	Параметр	Опи
		clie - исп Basic отпр учет загол - cli - под (JSOI испо свое отпр каче данн - pri подп испо свое ключ его в учет Выбо аутен зави треб безо прил спос безо свои Напр clie priv обес высо безо испо асим шиф позв

Название	Параметр	Опи
		пере клие

Метод аутентификации, используемый при доступе к конечной точке проверки токена (introspection_endpoint_auth_method)	`introspection_endpoint_auth_method`	Метс
		клие
		при
		`intr`
		`endp`
		коне
		испо
		пров
		токе
		полу
		инфс
		
		- `non`
		пред
		учет
		обра
		intro
		-
		`clie`
		- отп
		учет
		теле
		-
		`clie`
		- исп
		Basic
		отпр
		учет
		загол
		- `cli`
		- под
		(JSO
		испо
		свое
		отпр
		каче
		данн

Название	Параметр	Опи
		- pri подп испо свое ключ его в учет Выбо от тр безо возм клие мето испо обес допо уров за сч подп что г необ пере клие
Метод аутентификации, используемый при доступе к конечной точке отзыва токенов (revocation_endpoint_auth_method)	`introspection_endpoint_auth_method`	Опре аутен кото испо обра revo endp коне испо отзы досту обнс Этот совп испо

Название	Параметр	Опи
		toke intr endp - non пред учет обра revoc - clie - отп учет теле clie - исп Basic отпр учет загол - cli - под (JSOI испо свое отпр каче данн - pri подп испо свое ключ его в учет

Алгоритм подписи ID токена

Название	Параметр	Описание

Название	Параметр	Описание
Алгоритм подписи, используемый при создании подписанного ID-токена (id_token_signed_response_alg)	`id_token_signed_response_alg`	Указывает алгоритм, который используется для подписи ID токена. **ID токен** — это JSON Web Token (JWT), который содержит утверждения (`claims`) о аутентификации пользователя

Проверка наличия времени аутентификации

Название	Параметр	Описание
Проверка наличия времени Аутентификации (require_auth_time)	`require_auth_time`	Указывает, должен ли сервер авторизации предоставить время аутентификации пользователя в ID токене. Если этот параметр включен, сервер авторизации включает в ID токен утверждение `auth_time`, которое представляет собой время, когда пользователь в последний раз выполнил аутентификацию

Способ передачи ID пользователя

Название	Параметр	Описание

Название	Параметр	Описание
Способ передачи ID пользователя в идентификационном токене (subject_type)	`subject_type`	Определяет способ, которым идентификатор пользователя (`sub claim`) представляется клиенту. Этот параметр влияет на то, как пользовательские идентификаторы генерируются и управляются. - `public` - идентификатор пользователя является одинаковым для всех клиентов. Это означает, что каждый клиент будет видеть один и тот же `sub claim` для пользователя; - `pairwise` - идентификатор пользователя уникален для каждого клиента. Это обеспечивает большую конфиденциальность, так как разные клиенты не смогут связать активность пользователя между собой. `pairwise` часто используется в сценариях, где необходимо защитить приватность пользователя от различных клиентов.

Тип приложения

Название	Параметр	Описание
Тип приложения (application_type)	`application_type`	Определяет платформу, для которой предназначено приложение: - `web` - веб-приложение, выполняемое в браузере; - `native` - нативное приложение, установленное на устройстве.

Токен доступа

Название	Параметр	Описание

Название	Параметр	Описание
Токен доступа (access_token_ttl)	`access_token_ttl`	Время жизни `access_token` в секундах

Токен обновления

Название	Параметр	Описание
Токен обновления (refresh_token_ttl)	`refresh_token_ttl`	Время жизни `refresh_token` в секундах

Настройка способов входа

Настройка способов входа

Обзор способов входа

Способ входа — это метод аутентификации пользователей, позволяющий им авторизоваться в личном кабинете или подключенных приложениях. Это ключевой элемент системы единого входа, обеспечивающий гибкую и безопасную идентификацию.

Типы провайдеров аутентификации в КриптоАРМ ID

В **КриптоАРМ ID** поддерживаются следующие типы способов входа:

- **Базовые методы**: логин и пароль, электронная почта,
- **Внешние провайдеры идентификации**: социальные сети, доверенные корпоративные системы и другие сервисы,
- **Усиленные и беспарольные методы:** криптографическая аутентификация через **mTLS** (клиентские сертификаты) и **WebAuthn** (биометрия, аппаратные ключи), а также одноразовые пароли **TOTP/HOTP**.

Комбинируйте способы входа для повышения безопасности. Реализуйте **двухфакторную аутентификацию**, при которой после ввода первого фактора (логин, пароль или другой способ) пользователь должен подтвердить свою личность с помощью второго фактора (телефон, электронная почта или WebAuthn). Как настроить двухфакторную аутентификацию →

Уровни управления и публичность способов входа

Способы входа могут создаваться в разных типах кабинетов **КриптоАРМ ID**:

- **Кабинет администратора** — уровень всего сервиса;
- **Кабинет организации** — уровень компании;
- **Кабинет приложения (ADM)** — уровень отдельного приложения.

Для способов входа, созданных на уровне **сервиса** или **организации**, можно настраивать **публичность** — определять, где именно они будут доступны.

Тип способа входа	Настройка публичности	Где доступен	Управление

Тип способа входа	Настройка публичности	Где доступен	Управление
Создан в кабинете администратора	✓ Да	Кабинет администратора и все приложения сервиса	Управляется только из **кабинета администратора**
Создан в кабинете организации	✓ Да	Все приложения данной организации	Управляется только из **кабинета организации**
Создан в приложении (малом кабинете)	✗ Нет	Только в этом приложении	Управляется в **настройках приложения**

Управление способами входа

Создание нового способа входа

Для большинства популярных сервисов в **КриптоАРМ ID** предусмотрены готовые шаблоны с настройками. Они упрощают процесс подключения, так как содержат предзаполненные параметры, специфичные для каждого провайдера.

Процесс настройки включает три шага:

1. **Подготовка:** получите `Client ID` и `Client Secret` в сервисе-поставщике.
2. **Настройка в КриптоАРМ ID:** создайте провайдер соответствующего типа.

   Обратитесь к отдельной инструкции по настройке выбранного провайдера:

   - **Электронная почта**: Email
   - **Социальные сети:** ВКонтакте, Mail.ru, Яндекс
   - **Универсальный:** OpenID Connect (для любых OIDC-совместимых систем)
   - **Усиленные методы:** mTLS, WebAuthn, TOTP, HOTP

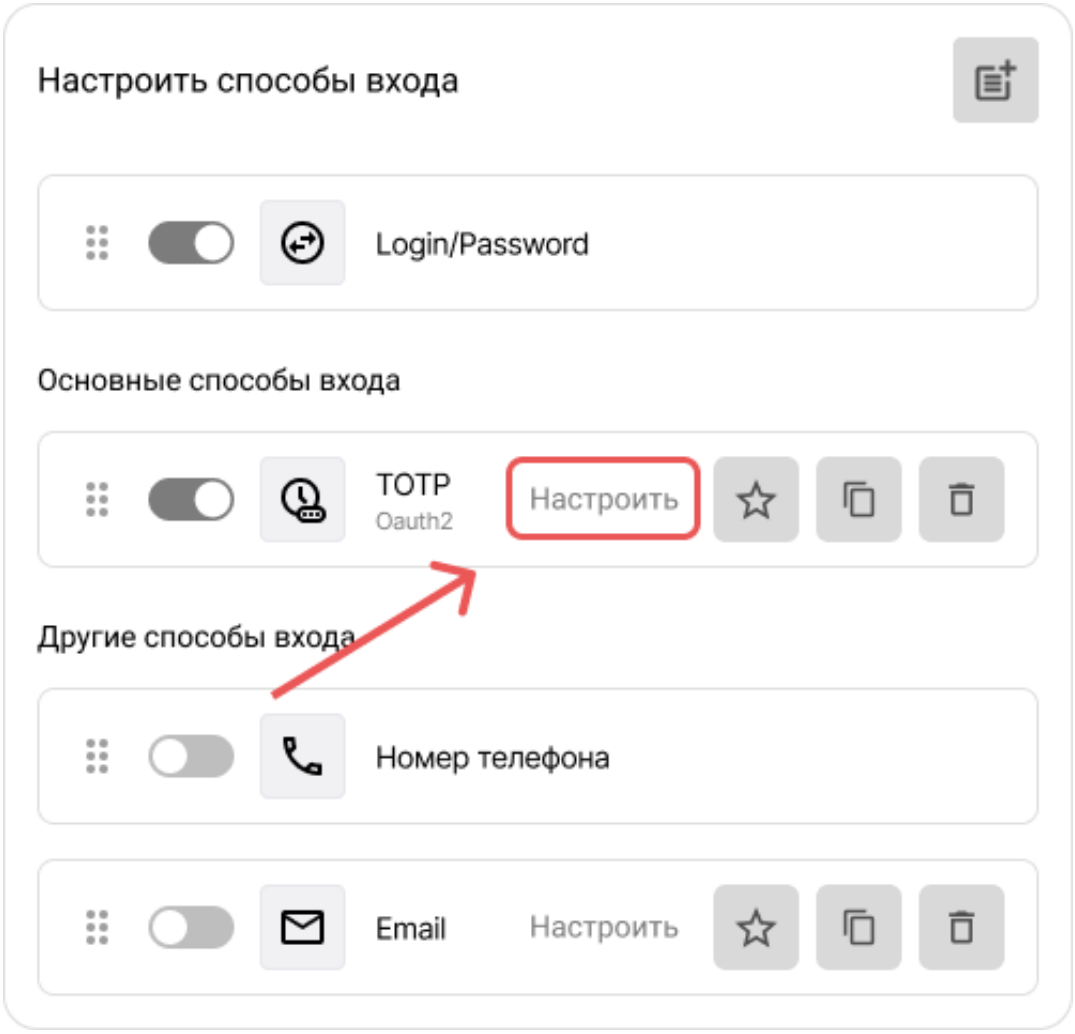
3. **Размещение на виджете:** добавьте способ входа на форму входа, доступную пользователям системы.

Редактирование существующего способа входа

Если необходимо обновить настройки существующего способа входа:

1. Перейдите в кабинет администратора (организации или настройки соответствующего приложения) → раздел **Настройки**.

2. Нажмите **Настроить** в блоке **Способы входа**.
3. Откроется окно со списком созданных способов входа.
4. Нажмите кнопку **Настроить** на панели со способом входа, который необходимо отредактировать.



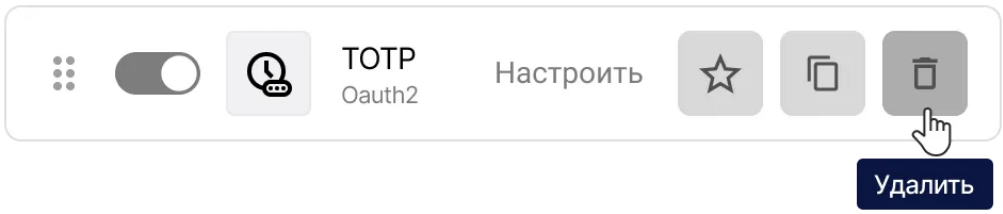
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

Удаление способа входа

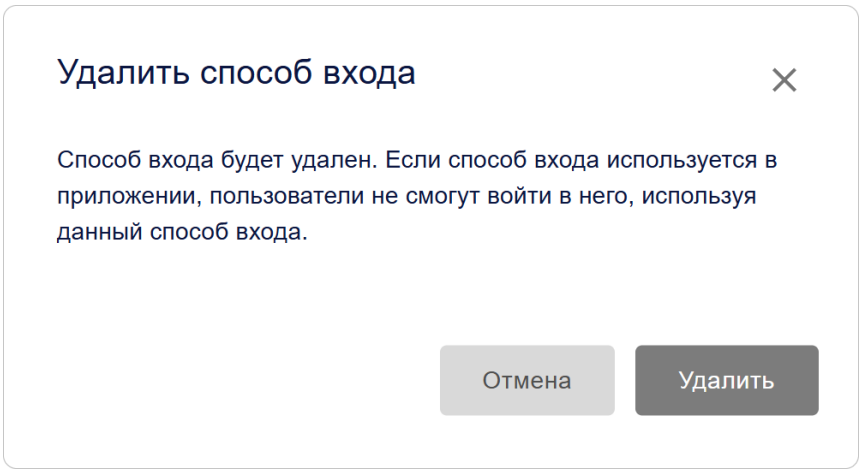
1. Перейдите в кабинет администратора (организации или настройки соответствующего приложения) → раздел **Настройки**.
2. Раскройте блок **Способы входа**.
3. Нажмите **Настроить**.

4. Откроется окно со списком созданных способов входа.

5. Нажмите на кнопку **Удалить**  , размещенную на панели со способом входа, который необходимо удалить.



6. Подтвердите действие в модальном окне.

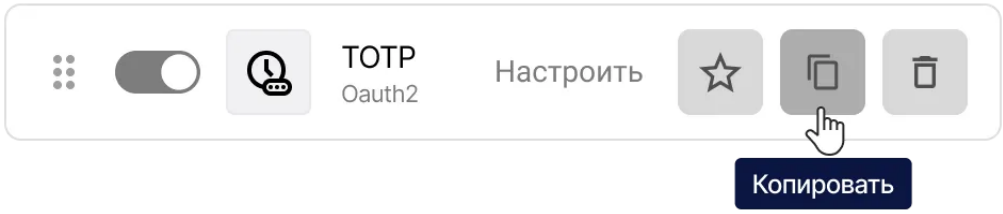


После успешного удаления способ входа исчезнет из виджетов всех связанных приложений.

Копирование настроек способа входа

Копирование настроек позволяет создать новый способ на основе ранее созданного.

1. Скопируйте настройки способа входа по кнопке **Копировать**  , расположенной на панели со способом входа.



2. Далее откройте форму создания нового способа входа по шаблону с аналогичным типом и нажмите **Вставить**  .

> ⚠ **Примечание**: При несовпадении типов новый провайдер может работать некорректно.

Настройка обязательного идентификатора в профиле пользователя

Идентификаторы — это внешние сервисы, которые пользователь добавил в свой профиль или через которые он когда-либо входил в систему.

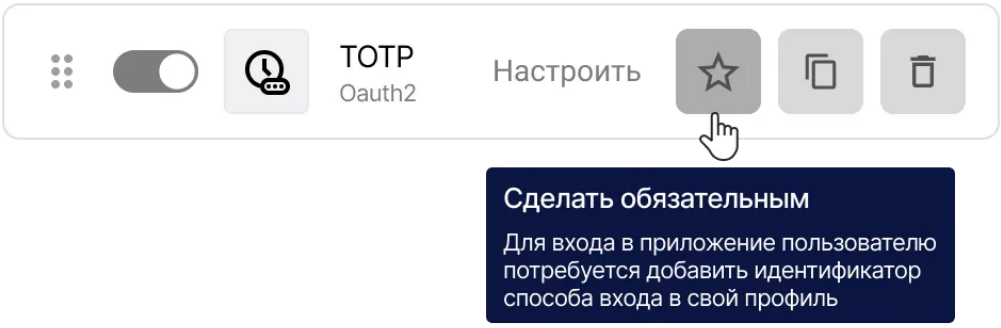
Список доступных для добавления идентификаторов формируется из способов входа в кабинет **КриптоАРМ ID** с активной настройкой публичности.

- Если способ входа настроен как **публичный**, он появится в списке доступных для добавления в профиле пользователя.
- Размещать этот способ входа на виджете приложения необязательно — он может быть доступен в профиле даже без кнопки на главном экране входа.
- Пользователь также может добавить идентификатор во время входа через виджет, если такой способ входа доступен.

В **КриптоАРМ ID** можно настроить требование обязательной привязки идентификатора внешнего аккаунта к профилю пользователя. В этом случае при входе в приложение у пользователя, не имеющего привязанного идентификатора, появится запрос на его добавление к профилю.

Как сделать идентификатор обязательным

1. Перейдите в кабинет администратора (организации или настройки соответствующего приложения) → раздел **Настройки**.
2. Раскройте блок **Способы входа** и нажмите **Настроить**.
3. Откроется окно со списком созданных способов входа.
4. Нажмите на кнопку **Сделать обязательным**  на панели со способом входа, который необходимо сделать обязательным.



Настройка применяется без дополнительного подтверждения.

> **Совет**: При повторном клике на кнопку **Сделать обязательным** наличие идентификатора в профиле станет необязательным.

Настройка виджета входа

Что такое виджет входа?

Виджет входа — это форма авторизации, которая отображается пользователю при попытке входа в приложение или систему **КриптоАРМ ID**, если он ещё не прошёл аутентификацию.

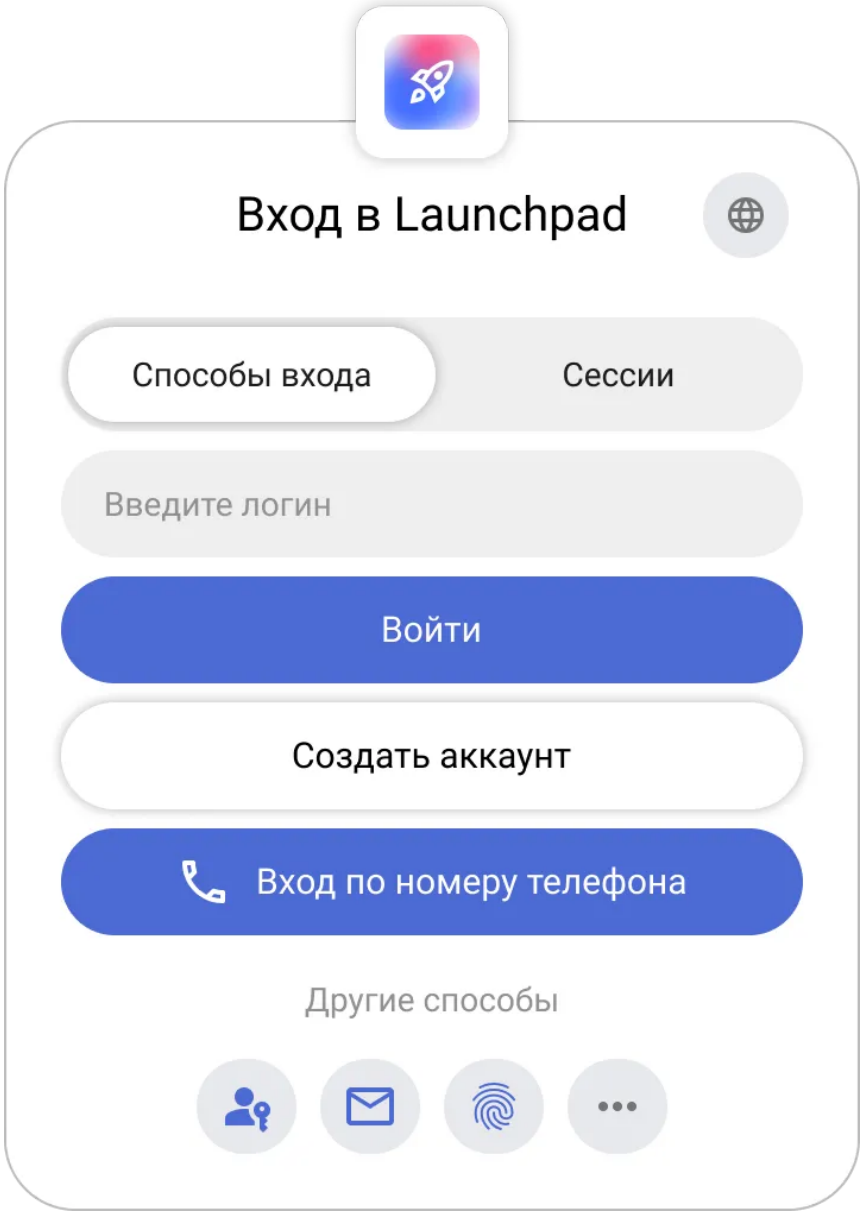
Виджет поддерживает:

- классический вход по логину и паролю,
- вход через различные провайдеры,
- гибкую настройку внешнего вида и структуры,
- группировку способов входа.

В виджете способы входа делятся на:

- **Основные способы** — отображаются в виде отдельных кнопок под кнопкой **Войти** и используются чаще всего.
- **Дополнительные способы** — размещены в блоке **Другие способы** в виде компактных кнопок, чтобы не перегружать интерфейс.

Пример виджета:



> **Виджет входа** — это первое, что видит пользователь при авторизации, поэтому важно, чтобы он соответствовал визуальному стилю компании и был максимально понятен.

Настройка виджета входа: внешний вид и кнопки

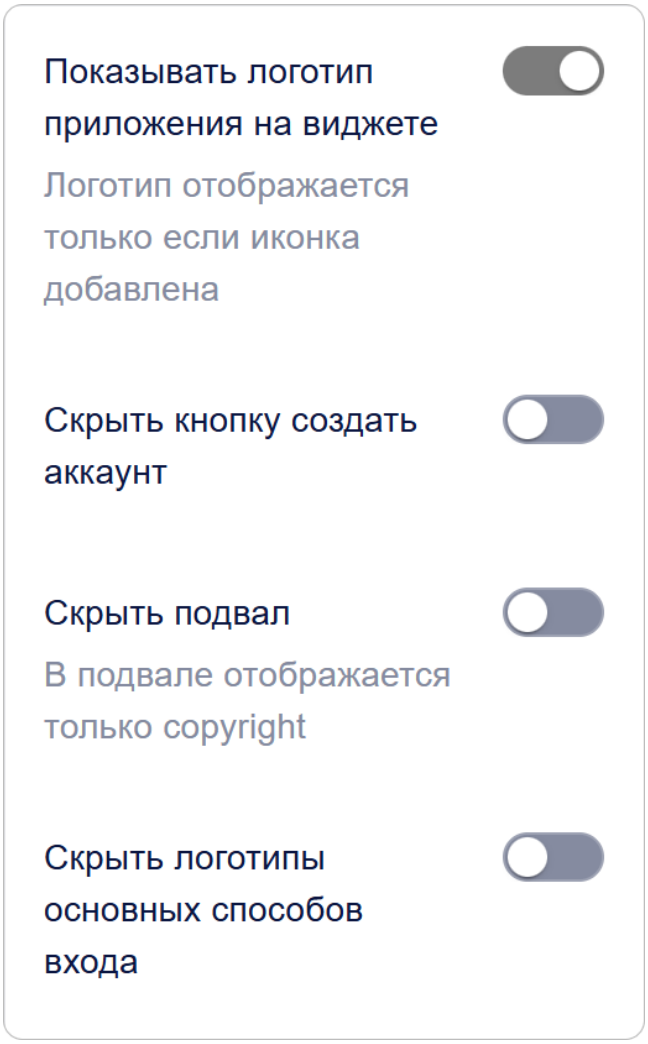
Чтобы настроить внешний вид виджета:

1. Перейдите в кабинет администратора (организации или настройки соответствующего приложения) → раздел **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. Откроется окно **Настроить внешний вид виджета**.
4. В первом блоке задаются ключевые визуальные элементы:

- **Заголовок виджета** — Отображается в верхней части формы. Для отображения названия приложения в заголовке виджета используйте значение `APP_NAME`.
- **Обложка виджета** — Фоновое изображение формы авторизации.
- **Режим автоподстановки обложки на виджетах приложений**:
  - **Отключено** — Используется обложка приложения,
  - **По умолчанию** — Только для приложений без обложки,
  - **Принудительный** — Применяется ко всем приложениям.

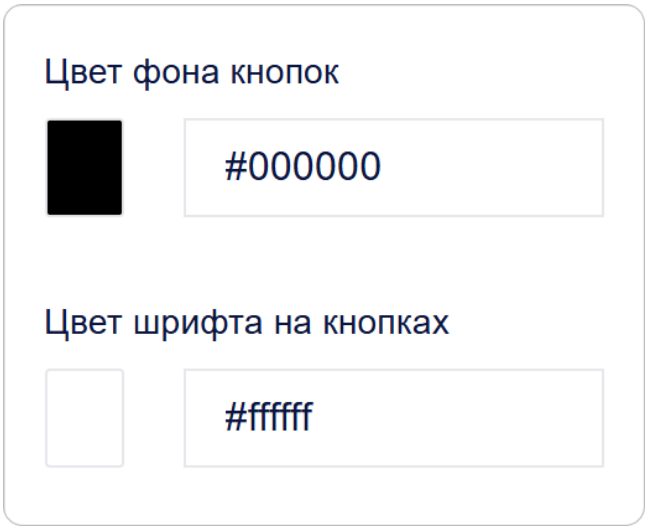
5. Во втором блоке настройте видимость элементов формы входа:

- **Показывать логотип приложения на виджете** — При включении отображает логотип рядом с названием приложения.
- **Скрыть кнопку создать аккаунт** — При включении скрывает кнопку создания аккаунта из виджета.
- **Скрыть подвал** — При включении скрывает подвал виджета с текстом «© 2015-2025».
- **Скрыть логотипы основных способов входа** — При включении скрывает логотипы способов входа из группы **Основные**.



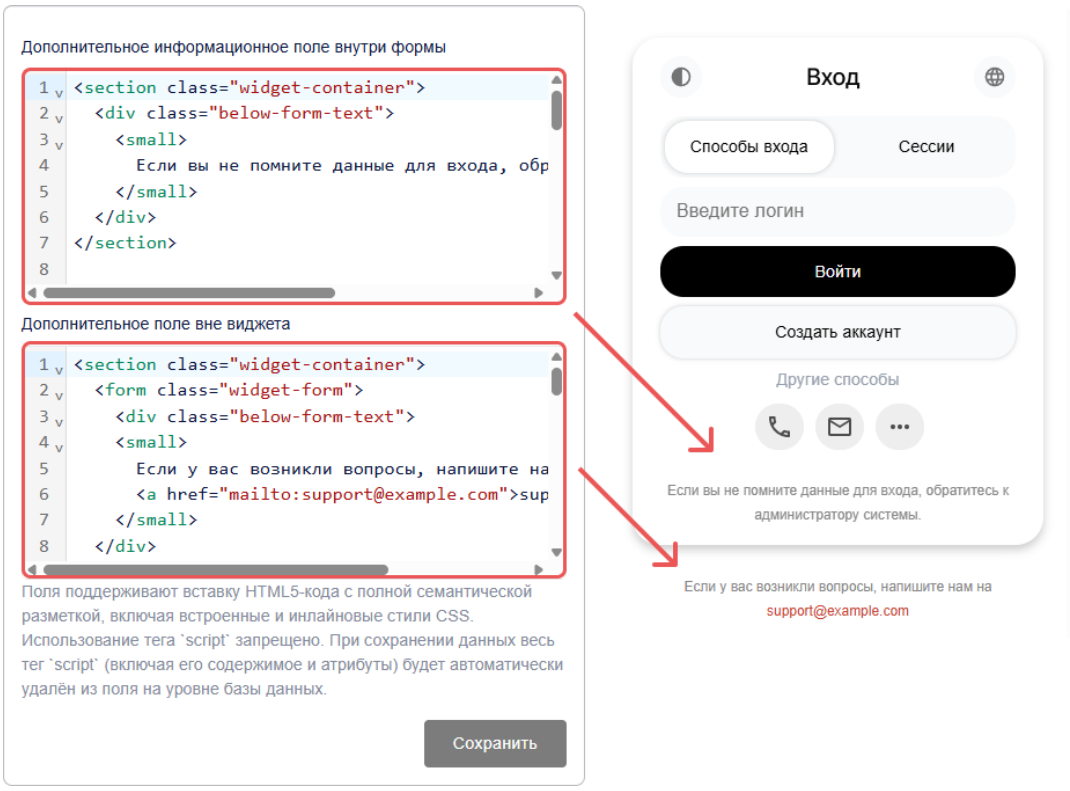
6. В третьем блоке настройте дизайн кнопок:

   - **Цвет фона кнопок** — Цветовая схема для фона кнопки (hex-код).
   - **Цвет шрифта на кнопках** — Задается цветовая схема для текста кнопки (hex-код).



7. При необходимости укажите текст:

- **Дополнительное информационное поле внутри формы** — Дополнительный текст, который будет отображаться в нижней части виджета,
- **Дополнительное поле вне виджета** — Дополнительный текст, который будет отображаться под виджетом.



> Поля поддерживают вставку HTML5-кода с полной семантической разметкой, включая встроенные и инлайновые стили CSS. Использование тега `script` запрещено. При сохранении данных весь тег `script` (включая его содержимое и атрибуты) будет автоматически удалён из поля на уровне базы данных.

8. Нажмите **Сохранить**, чтобы применить изменения.

> 💡 В разделе **Превью** можно посмотреть результаты изменений.

Добавление и отключение способов входа на виджете

Чтобы настроить отображение способа входа в виджете:

1. Перейдите в кабинет администратора (организации или настройки соответствующего приложения) → раздел **Настройки**.
2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. Включите или отключите переключатели для нужных способов входа.
4. При необходимости настройте группы способов входа.

> ⚠ **Примечание**:
>
> 1. Невозможно отключить способ входа **Логин/пароль**. При отключении всех способов входа автоматически включается способ входа **Логин/пароль**, поскольку в виджете должен быть хотя бы один способ для входа.
> 2. Отключение способа входа с виджета не удаляет способ входа из системы.

Настройка доверенных провайдеров

Что такое доверенные провайдеры?

Доверенные провайдеры — это внешние корпоративные или государственные системы (например, Active Directory, 1С), которые выступают **источником верифицированных данных** о пользователе.

Ключевые особенности:

1. При входе через доверенный провайдер автоматически создается пользователь в **КриптоАРМ ID**, профиль которого содержит данные пользователя внешней системы.
2. Профиль пользователя, созданный через доверенный провайдер, не доступен для редактирования пользователю.
3. При авторизации доверенного пользователя его профиль автоматически синхронизируется с внешней системой. Это происходит независимо от того, какой провайдер был использован для входа.

Поддерживаемые доверенные провайдеры

В **КриптоАРМ ID** поддерживаются следующие доверенные провайдеры:

- **LDAP (Active Directory)** — вход по учетным данным пользователя службы каталогов Active Directory;
- **ALD Pro** — вход по учетным данным пользователя службы каталогов ALD Pro;
- **1С** — вход по учетным данным пользователя системы 1С.

Уровни управления

Доверенные провайдеры, как и способы входа, могут создаваться в разных типах кабинетов **КриптоАРМ ID**, в зависимости от вашего уровня доступа. Подробнее читайте в инструкции Как настроить способы входа.

Управление доверенными провайдерами

Создание нового провайдера

Для большинства популярных сервисов и корпоративных систем в **КриптоАРМ ID** предусмотрены готовые шаблоны с настройками. Они упрощают процесс подключения, так как содержат предзаполненные параметры, специфичные для каждого провайдера.

Процесс настройки включает три шага:

1. **Подготовка:** настройка на стороне доверенной системы.
2. **Настройка в КриптоАРМ ID:** создание провайдера соответствующего типа.
3. **Размещение на виджете:** добавление созданного провайдера на форму входа, доступную пользователям системы.

Обратитесь к отдельной инструкции по настройке выбранного провайдера:

- Как подключить вход через LDAP,
- Как подключить вход через 1С,
- Как подключить вход через ALD Pro.

> **Важно:**
> Для подключения доверенного провайдера требуется лицензия.
> Подробнее о лицензировании.

Редактирование существующего провайдера

Если необходимо обновить настройки существующего провайдера:

1. Перейдите в кабинет администратора или организации → вкладка **Настройки**.
2. Нажмите **Настроить** в блоке **Доверенные провайдеры**.
3. Откроется окно со списком созданных провайдеров.
4. Нажмите кнопку **Настроить** на панели с провайдером, который необходимо отредактировать.
5. Откроется форма редактирования.
6. Внесите необходимые изменения.
7. Нажмите **Сохранить**.

Удаление провайдера

1. Перейдите в кабинет администратора или организации → вкладка **Настройки**.
2. Нажмите **Настроить** в блоке **Доверенные провайдеры**.
3. Откроется окно со списком созданных провайдеров.
4. Нажмите на кнопку **Удалить**  , размещенную на панели с провайдером, который необходимо удалить.
5. Подтвердите действие в модальном окне.

После успешного удаления способ входа исчезнет из виджетов всех связанных приложений.

Копирование настроек провайдера

Копирование настроек позволяет создать новый провайдер на основе ранее созданного.

1. Скопируйте настройки провайдера по кнопке **Копировать**  , расположенной на панели со способом входа.
2. Далее откройте форму создания нового провайдера по шаблону с аналогичным типом и нажмите **Вставить**  .

> ⚠ **Примечание**: При несовпадении типов новый провайдер может работать некорректно.

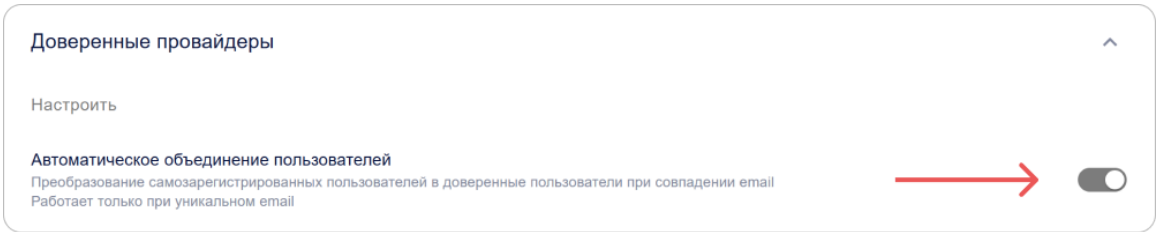
Автоматическое объединение профилей пользователей

Функция **Автоматическое объединение пользователей** автоматически объединяет профили самозарегистрированных пользователей с профилями из доверенных систем при **совпадении email**.

> ⚠ **Ограничения**: Функция работает только при уникальном адресе электронной почты в профилях самозарегистрированных пользователей. Перед активацией выполните проверку дубликатов профилей.

Чтобы включить автоматическое объединение пользователей:

1. Перейдите в кабинет администратора (или кабинет организации) → вкладка **Настройки**.
2. Раскройте блок **Доверенные провайдеры**.
3. Активируйте переключатель **Автоматическое объединение пользователей**.



> 💡 После активации система начнёт автоматически связывать профили при первой авторизации через доверенный источник.

Инструкции для подключения способов входа

Как подключить вход через 1С

Доверенный провайдер **1С** предназначен для организации входа в информационные системы по данным (логин/пароль) учетных записей пользователей системы **1С**.

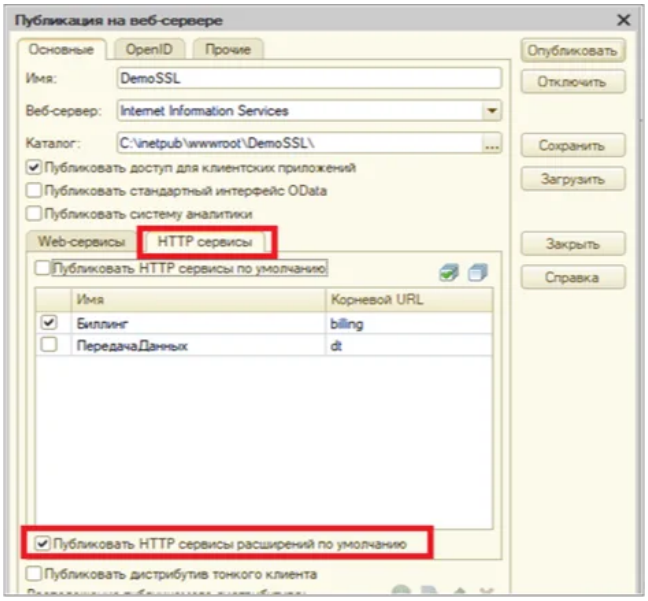
Шаг 1. Настройка на стороне внешней системы

1. Установите расширение конфигурации **1С**.

   Взаимодействие с информационной базой **1С** реализовано через расширение конфигурации (файл расширения предоставляется отдельно), и осуществляется с использованием http-сервисов.

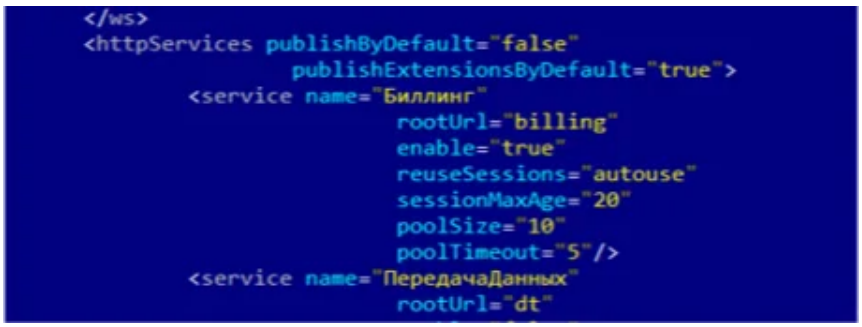
   Расширение конфигурации предоставляется технической поддержкой **КриптоАРМ ID**.

2. Опубликуйте http-сервисы приложения на web-сервере для работы с расширением.



3. Установите признак **Публиковать HTTP сервисов расширения по умолчанию** для работы http-сервисов расширения.

   Для проверки корректности публикации http-сервисов проверяется файл публикации (**.vrd**) на web-сервере. Файл публикации должен содержать свойство `publishExtensionsByDefault`, равное значению `true`.



4. Создайте пользователя, учетные данные которого будут использоваться для авторизации запросов (допускается пользователь без прав).

Шаг 2. Настройка в КриптоАРМ ID

В сервисе **КриптоАРМ ID** необходимо создать доверенный провайдер по шаблону **1С**.

Чтобы создать провайдер:

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать провайдер для организации, откройте **кабинет организации**.

2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.

3. В открывшемся окне нажмите на кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон провайдера **1С**.

6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **1С**:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Адрес сервера 1С** — Название опубликованной базы в формате: `http(s)://[сервер]:[порт]/[база]`.
   - **Логин администратора 1С** — Логин пользователя 1С, учетные данные которого будут использоваться для авторизации запросов (допускается

пользователь без прав).
- **Пароль администратора 1С** — Пароль пользователя 1С.
- **Сопоставление атрибутов 1С** — Соответствие атрибутов профиля пользователя **КриптоАРМ ID** с атрибутами в 1С. Формат: `trusted_id_attribute:1C_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`).

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
- **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.

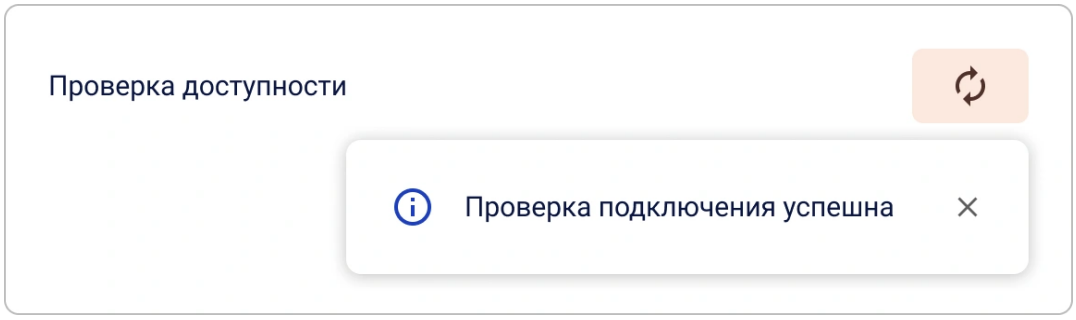
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



В результате проверки возможны два варианта ответа:

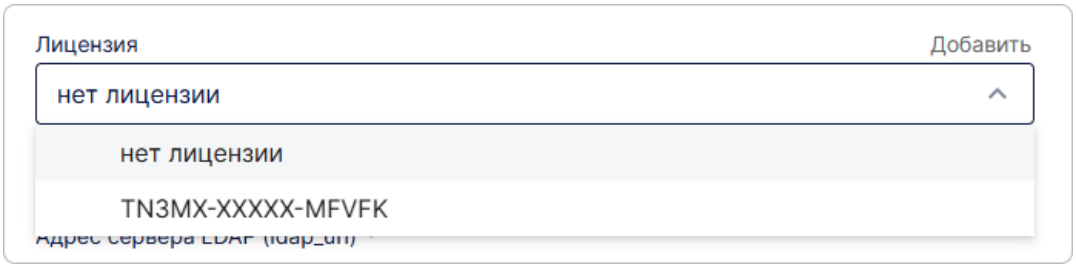
- ☑ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.

- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

> 💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



> 💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ ID** с атрибутом пользователя в **1С**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:firstName`,
- `family_name:lastName`,

- `email:email`,
- `picture:photo`.

Основные поля пользователя КриптоАРМ ID

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения
`picture`	Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
    - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ ID** указывается **Название** дополнительного поля.
2. **Особенности работы с логином**
    - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ ID** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.
    - Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.
3. **Сопоставление с условием «или»**
    - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.

- Пример записи: `<поле_КриптоАРМ ID>:<атрибут1>-<атрибут2>`

Как подключить вход через ALD Pro

Доверенный провайдер **ALD Pro** предназначен для организации входа в информационные системы по данным учетных записей пользователей системы **ALD Pro**.

Шаг 1. Настройка на стороне внешней системы

В **ALD Pro** необходимо создать пользователя:

- Обладающего правами администратора, с возможностью изменять пароль пользователей в **ALD Pro**;
- Состоящего в группе безопасности **Администраторы домена**.

Шаг 2. Настройка в КриптоАРМ ID

В сервисе **КриптоАРМ ID** необходимо создать доверенный провайдер по шаблону **ALD Pro**:

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > 💡 Чтобы создать провайдер для организации, откройте **кабинет организации**.

2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.

3. В открывшемся окне нажмите на кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон провайдера **ALD Pro**.

6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **ALD Pro**:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

- **Адрес сервера ALD Pro (aldpro_url)** — Адрес сервера ALD Pro в формате `ALD Pros://example.com`.
- **База поиска (aldpro_base)** — Объект каталога, начиная с которого будет производиться поиск. Должен быть корректным DN, например, `dc=example,dc=com`.
- **Домен ALD Pro (aldpro_domain)** — Имя домена, которому принадлежат пользователи.
- **Фильтр поиска (aldpro_filter)** — Фильтр для поиска учетной записи пользователя.
- **Сопоставление атрибутов ALD Pro (aldpro_mapping)** — Соответствие атрибутов профиля пользователя **КриптоАРМ ID** с атрибутами в ALD Pro. Формат: `trusted_id_attribute:ALD Pro_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`).
- **Логин администратора (aldpro_admin_dn)** — Логин администратора ALD Pro.
- **Пароль администратора (aldpro_admin_pwd)** — Пароль администратора ALD Pro.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
- **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.

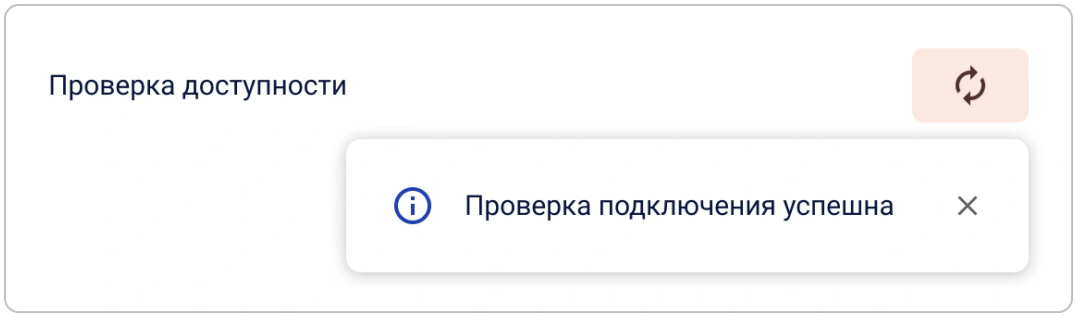
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



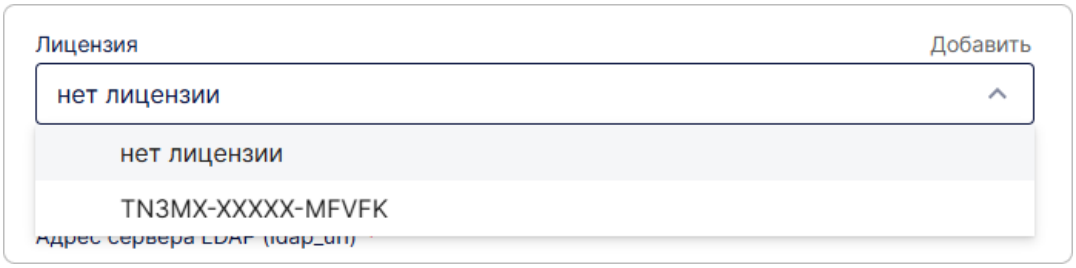
В результате проверки возможны два варианта ответа:

- ☑ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.
- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

> 💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



> 💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ ID** с атрибутом пользователя в **ALD Pro**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:givenName`,
- `family_name:sn`,
- `email:mail`.

Основные поля пользователя КриптоАРМ ID

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения
`picture`	Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
    - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ ID** указывается **Название** дополнительного поля.
2. **Особенности работы с логином**
    - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ ID** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.

- Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.

3. **Сопоставление с условием «или»**

   - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.
   - Пример записи: `<поле_КриптоАРМ ID>:<атрибут1>-<атрибут2>`

Как подключить вход через LDAP

Доверенный провайдер **LDAP** предназначен для организации входа в информационные системы по данным учетных записей пользователей системы **LDAP**.

Шаг 1. Настройка на стороне внешней системы

В **Active Directory** необходимо создать пользователя:

- Обладающего правами администратора, с возможностью изменять пароль пользователей в **Active Directory**;
- Состоящего в группе безопасности **Администраторы домена**.

Шаг 2. Настройка в КриптоАРМ ID

В сервисе **КриптоАРМ ID** необходимо создать доверенный провайдер по шаблону **LDAP**:

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать провайдер для организации, откройте **кабинет организации**.

2. Раскройте блок **Доверенные провайдеры** и нажмите **Настроить**.

3. В открывшемся окне нажмите на кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон провайдера **LDAP**.

6. В форме создания заполните поля или вставьте скопированные значения из ранее созданного доверенного провайдера **LDAP**:

Основная информация

- **Имя** — Название, которое увидят пользователи.
- **Описание** (опционально) — Краткое описание.
- **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

Параметры

- **Адрес сервера LDAP (ldap_url)** — Адрес сервера LDAP в формате `ldaps://example.com`.
- **База поиска (ldap_base)** — Объект каталога, начиная с которого будет производиться поиск. Должен быть корректным DN, например, `dc=example,dc=com`.
- **Домен LDAP (ldap_domain)** — Имя домена, которому принадлежат пользователи.
- **Фильтр поиска (ldap_filter)** — Фильтр для поиска учетной записи пользователя.
- **Сопоставление атрибутов LDAP (ldap_mapping)** — Соответствие атрибутов профиля пользователя **КриптоАРМ ID** с атрибутами в LDAP. Формат: `trusted_id_attribute:ldap_attribute` (например, `given_name:givenName`, `family_name:sn`, `email:mail`, `picture:photo`).
- **Логин администратора (ldap_admin_dn)** — Логин администратора LDAP.
- **Пароль администратора (ldap_admin_pwd)** — Пароль администратора LDAP.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.
- **Запретить сброс пароля** — Пользователь не сможет сменить пароль от учетной записи внешней системы. В виджете входа кнопка **Сменить пароль** будет скрыта.

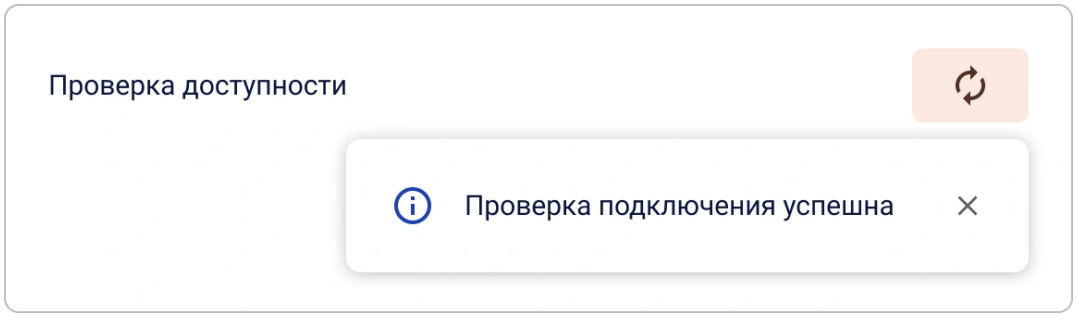
7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 3. Проверка доступности внешней системы

Проверка доступности — это встроенный инструмент, который позволяет убедиться, что указанные параметры подключения к доверенному провайдеру настроены корректно и сервис успешно взаимодействует с внешней системой.

После заполнения параметров провайдера нажмите кнопку **Проверка доступности**. Система выполнит тестовый запрос на указанные конечные точки провайдера.



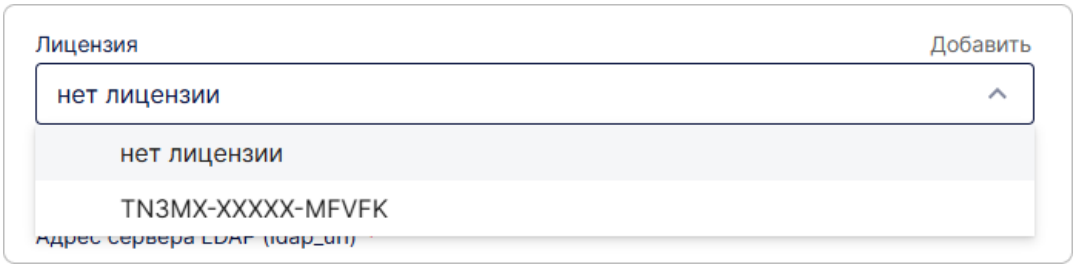
В результате проверки возможны два варианта ответа:

- ☑ **Проверка подключения успешна** — соединение установлено, параметры конфигурации корректны.
- ❌ **Ошибка проверки подключения** — возникла ошибка соединения. В этом случае проверьте правильность указанных URL и корректность клиентских ключей или токенов.

> 💡 Рекомендуется выполнять проверку после каждого изменения настроек, чтобы убедиться, что параметры указаны корректно перед сохранением.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



> 💡 **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Правила сопоставления атрибутов

Сопоставление атрибутов позволяет настроить сопоставление поля профиля пользователя **КриптоАРМ ID** с атрибутом пользователя в **Active Directory**.

Если значение поля не задано, используется значение по умолчанию:

- `given_name:givenName`,
- `family_name:sn`,
- `email:mail`.

Основные поля пользователя КриптоАРМ ID

Поле	Описание
`sub`	Идентификатор пользователя
`email`	Адрес электронной почты
`phone_number`	Номер телефона
`nickname`	Публичное имя
`given_name`	Имя
`family_name`	Фамилия
`login`	Логин
`birthdate`	Дата рождения
`picture`	Фото профиля

Особенности сопоставления атрибутов

1. **Дополнительные поля**:
    - Допускается настройка сопоставления на дополнительные поля профиля пользователя. В таком случае в качестве поля профиля **КриптоАРМ ID** указывается **Название** дополнительного поля.

2. **Особенности работы с логином**
    - Можно задать сопоставление на поле **Логин**, для того, чтобы логины пользователя в **КриптоАРМ ID** и во внешней системе совпадали. В этом случае логин во внешней системе должен иметь уникальное значение.
    - Если в сопоставлении атрибутов отсутствует настройка сопоставления на поле **Логин**, или логин уже используется для другого пользователя, то при автоматической регистрации пользователю присваивается внутренний логин, сгенерированный системой.
3. **Сопоставление с условием «или»**
    - В поле **Сопоставление атрибутов** для доверенных провайдеров можно задать несколько возможных атрибутов через дефис, чтобы использовать значение из одного, если в другом оно отсутствует.
    - Пример записи: `<поле_КриптоАРМ ID>:<атрибут1>-<атрибут2>`

Как подключить вход через ЕСИА

Доверенный провайдер аутентификации **ЕСИА** предназначен для организации входа в информационные системы с помощью учетной записи портала **Госуслуг**. Оператор системы — **Минцифры России**.

В текущей реализации **КриптоАРМ ID** для подписи и проверки запросов используется приложение КриптоАРМ Сервер.

Шаг 1. Настройка на стороне внешней системы

Подключите свою компанию по инструкции.

Шаг 2. Настройка КриптоАРМ Сервер

1. Скачайте и установите **КриптоАРМ Сервер** на выделенный сервер
2. Настройте сертификаты:
    - Установите сертификат КЭП вашей организации
    - Проверьте срок действия сертификата
3. **Проверьте доступность**:
    - Запустите сервис КриптоАРМ Сервер
    - Убедитесь, что эндпоинты подписи и проверки доступны

После настройки КриптоАРМ Сервер вам понадобятся:

- **Адрес получения подписи запроса** (например: `http://ваш-сервер:порт/sign`)

- **Адрес проверки подписи запроса** (например: `http://ваш-сервер:порт/verify`)
- **Сертификат** КЭП вашей организации

> 🔍 Технические вопросы интеграции рассмотрены в Методических рекомендациях по использованию ЕСИА.

Шаг 3. Настройка в КриптоАРМ ID

В сервисе **КриптоАРМ ID** необходимо создать провайдер по шаблону **ЕСИА**.

Чтобы создать провайдер **ЕСИА**:

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > 💡 Чтобы создать провайдер для организации, откройте **кабинет организации**.

2. Раскройте блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите на кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон провайдера **ЕСИА**.

6. В открывшейся форме создания провайдера заполните параметры провайдера:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Идентификатор ресурса (client_id)** — Уникальный идентификатор подключаемого ресурса.
   - **Пароль** — Пароль от ключевого контейнера ключа подписи.
   - **Сертификат подписи и проверки запросов** — Сертификат ключа квалифицированной электронной подписи, выпущенной для подключаемой информационной системы. Необходимо указать путь к файлу с сертификатом.
   - **Адрес получения подписи запроса (sign_endpoint)** — Ресурс, который подписывает запрос.

- **Адрес проверки подписи запроса (verify_endpoint)** — Ресурс, который проверяет подпись ответа от ЕСИА.

Дополнительные настройки

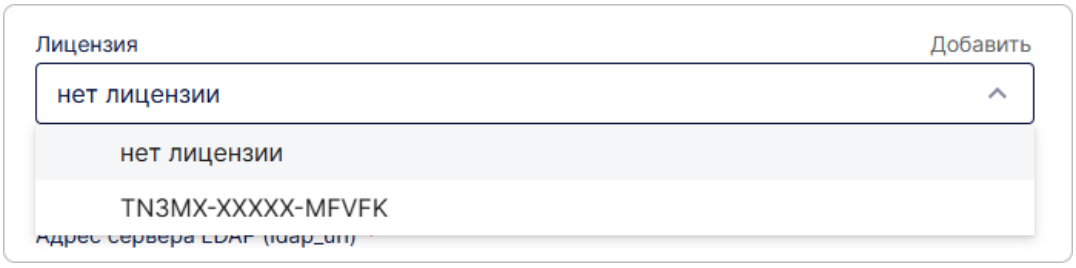
- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Сохранить**.

После успешного создания провайдер отобразится в списке.

Шаг 4. Привязка лицензии

1. В общем списке провайдеров найдите созданный способ входа и нажмите **Настроить**.
2. В **Лицензия** выберите ключ из выпадающего списка.



> **Совет**: Если в списке нет лицензии, сначала загрузите ее через кнопку **Добавить**.

3. Сохраните изменения по кнопке **Сохранить**.

Шаг 5. Добавление на виджет

Чтобы пользователи увидели кнопку входа на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом способа входа.

Как подключить вход по электронной почте

Шаг 1. Создание способа входа

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон **Email**.

6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Основной почтовый адрес** — Основной почтовый адрес, который будет использоваться для рассылки писем.
   - **Адрес сервера исходящей почты** — Адрес сервера исходящей почты.
   - **Порт сервера исходящей почты** — Порт сервера исходящей почты.
   - **Пароль почты** — Обычный пароль или пароль приложения, который создается в настройках аккаунта почтового сервиса.
   - **Время жизни кода подтверждения** — Время жизни кода подтверждения для почтового сервиса в секундах.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Email** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Email**.

Как подключить вход через HOTP

Общая информация

HOTP (HMAC-based One-Time Password) — это алгоритм генерации одноразовых паролей на основе секретного ключа и счетчика, который увеличивается при каждом успешном использовании кода. Это широко используется для двухфакторной аутентификации, добавляя уровень безопасности поверх стандартного логина и пароля.

Главное отличие **HOTP** от **HOTP** — коды не зависят от времени. Каждое использование кода увеличивает счетчик, и сервер проверяет введенный код относительно текущего значения счетчика.

Основные компоненты:

- **Сервер аутентификации** — сервер, который генерирует секретный ключ и проверяет введенные коды,учитывая счетчик.
- **Аутентификатор** — приложение, хранящее секретный ключ и текущий счетчик, генерирующее одноразовые пароли.
- **Секретный ключ** — общая для сервера и приложения база, используемая для генерации кодов.

Процесс работы HOTP

1. **Предварительная настройка**
    - Администратор создает способ входа **HOTP** и активирует его для виджетов нужных приложений.
    - Пользователь в своем профиле добавляет новый идентификатор **HOTP**, сканируя QR-код с секретным ключом через приложение-аутентификатор.
2. **Генерация и проверка кода**
    - Приложение-аутентификатор вычисляет одноразовый пароль на основе секретного ключа и текущего значения счетчика с использованием

алгоритма SHA1, SHA256 или SHA512.
- Когда пользователь вводит код на форме входа, сервер вычисляет ожидаемый код по тому же секрету и текущему счетчику.
- Если код совпадает, сервер увеличивает счетчик и предоставляет доступ пользователю.

> **Важно**: **HOTP** не зависит от времени, поэтому синхронизация часов не требуется.

Настройка аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **HOTP**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры

   - **Количество цифр** — Количество цифр в одноразовом пароле (обычно 6).
   - **Начальное значение счётчика** — Текущий счетчик (не редактируемое).
   - **Алгоритм** — Алгоритм хеширования (SHA1, SHA256 или SHA512) (обычно SHA-1).

   Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера HOTP на виджет

Чтобы пользователи увидели кнопку **HOTP** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **HOTP**.

Привязка HOTP для пользователей

> 📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **HOTP**.

Шаг 1. Установка приложения-аутентификатора

На ваше мобильное устройство необходимо установить приложение, которое генерирует HOTP-коды.

Самые популярные варианты:

- **Яндекс Ключ** (Яндекс)
- **Google Authenticator** (Google)

Шаг 2. Добавление HOTP-идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **HOTP**.
4. Отсканируйте QR-код с помощью приложения-аутентификатора.
5. Введите код из приложения и подтвердите.

> **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **HOTP**.
2. Выберите иконку способа входа **HOTP**.
3. Откроется форма для ввода кода. Не закрывая страницу, откройте приложение-аутентификатор на своем телефоне.
4. Найдите сервис, соответствующий **КриптоАРМ ID** (или названию приложения) и введите свой логин и 6-значный код в поле на форме входа.
5. Нажмите кнопку **Подтвердить**.

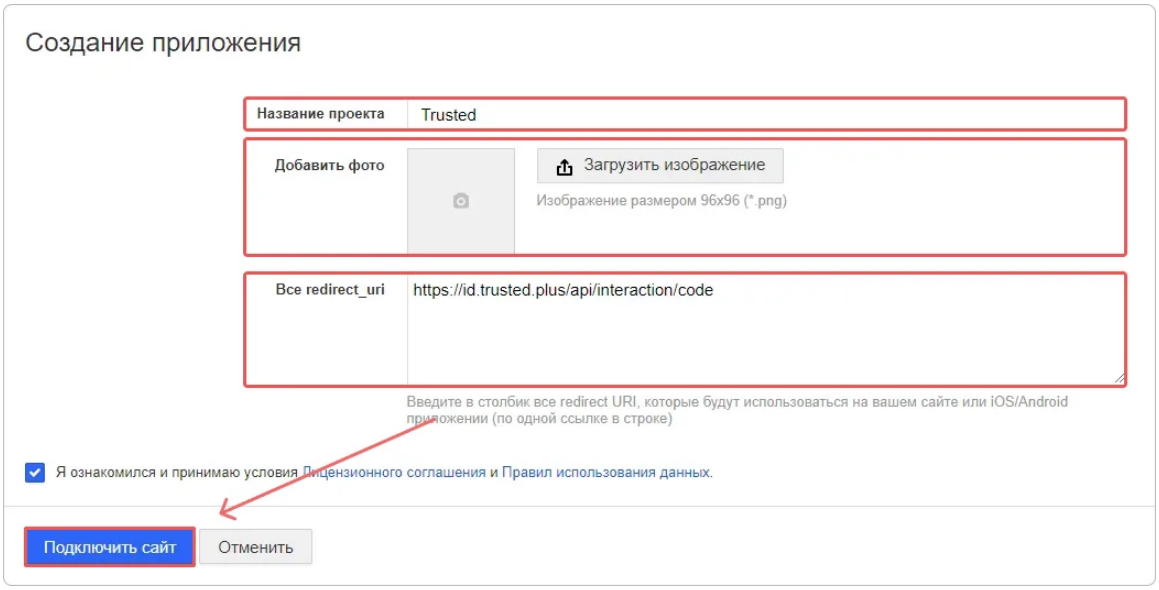
Как подключить вход через Mail.ru

Способ входа **Mail.ru** предназначен для организации входа в информационные системы с помощью учётной записи сервиса **Mail.ru**.

Шаг 1. Настройка приложения в Mail.ru

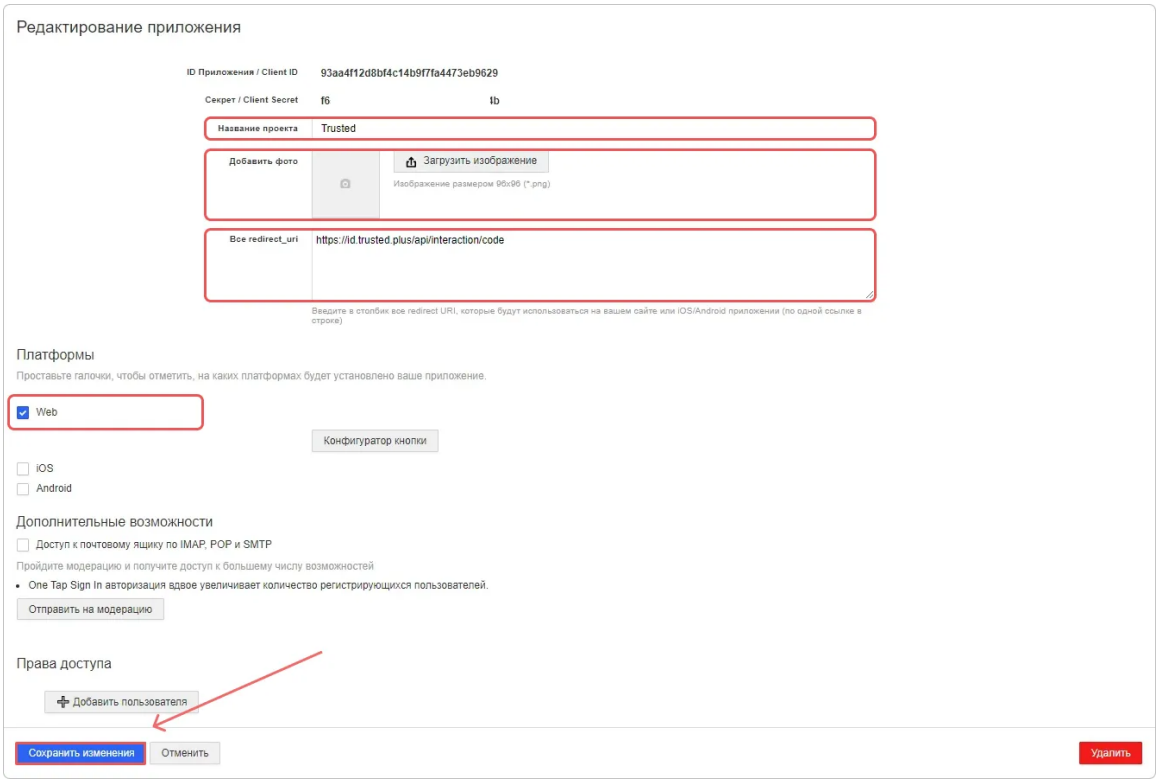
Перед настройкой способа входа в **КриптоАРМ ID** необходимо зарегистрировать ваше приложение в кабинете разработчика **Mail.ru** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь на сайте Mail.ru.
2. Перейдите в личный кабинет управления приложениями.
3. Нажмите **Создать приложение**.
4. В открывшейся форме создания укажите:
   - **Название проекта**,
   - **Фото** (при необходимости),
   - **Все redirect_uri** — возвратный URL #1 (`Redirect_uri`) в формате `https://<адрес инсталляции>/api/interaction/code`.



5. Нажмите кнопку **Подключить сайт**.

6. На следующем шаге формы в блоке **Платформы** выберите **Web**.



7. Нажмите **Сохранения изменения**.

8. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ ID**.

Шаг 2. Создание способа входа

Теперь, имея ключи от **Mail.ru**, создадим соответствующий провайдер в системе **КриптоАРМ ID**.

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > 💡 Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон **Mail.ru**.

6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
   - **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Mail.ru** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Mail.ru**.

Параметры способа входа

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **Mail.ru**
Секретный ключ (client_secret)	`Client_secret`	Сервисный ключ доступа приложения, созданного созданного в **Mail.ru**
Возвратный URL(Redirect URI) (не редактируемое)	`Redirect URI`	Адрес **КриптоАРМ ID**, на который пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Как подключить вход по протоколу mTLS

Общая информация

mTLS (Mutual TLS) — способ аутентификации, основанный на взаимной проверке сертификатов клиента и сервера.

Этот способ обеспечивает высокий уровень доверия и безопасности, так как вход в систему возможен только при наличии у пользователя действительного сертификата, подписанного доверенным центром сертификации (CA).

mTLS особенно полезен для корпоративных или чувствительных систем, где требуется минимизировать риск несанкционированного доступа.

Процесс работы mTLS

1. **Инициация соединения:** Клиент отправляет запрос к серверу **КриптоАРМ ID**.
2. **Запрос сертификата клиента:** Сервер требует предоставления клиентского сертификата.
3. **Отправка клиентского сертификата:** Клиент предоставляет свой сертификат, подписанный доверенным CA.
4. **Проверка сертификата на сервере:**
    - Сервер сверяет сертификат с основным CA.
    - Проверяет срок действия, подпись и соответствие требованиям безопасности.
5. **Аутентификация пользователя:**
    - Если сертификат валиден, сервер сопоставляет его с учетной записью пользователя и разрешает доступ.
    - Если сертификат невалиден или отсутствует — доступ отклоняется.

6. **Установление защищенного канала:** После успешной проверки сертификата устанавливается **шифрованное соединение**, и пользователь получает доступ.

Настройка mTLS-аутентификации для администраторов КриптоАРМ ID

Для работы **mTLS** необходимо:

- настроить веб-сервер **Nginx**, чтобы он принимал только запросы, подписанные доверенным сертификатом;
- создать и активировать провайдер **mTLS** в интерфейсе **КриптоАРМ ID**;
- установить клиентские сертификаты на устройства пользователей.

Шаг 1. Настройка Nginx для mTLS

Перед добавлением провайдера в **КриптоАРМ ID** необходимо подготовить конфигурацию **Nginx**:

1. Откройте файл конфигурации `nginx.local.conf`.
2. Добавьте новый `server` блок:

   Пример конфигурации:

```
server {
    server_name local.trusted.com;
    listen 3443 ssl;

    ## Сертификаты сервера
    ssl_certificate         certs/local.trusted.com.pem;
    ssl_certificate_key     certs/local.trusted.com-key.pem;

    ## Сертификат корневого CA для проверки клиентских
сертификатов
    ssl_client_certificate  certs/ca-bundle.crt;
    ssl_verify_client on;
    ssl_verify_depth 3;

    ## Настройки сессии и протоколов
    ssl_session_timeout 10m;
    ssl_session_cache shared:SSL:10m;
    ssl_protocols TLSv1.2 TLSv1.3;

    ## Ограничение доступа на основной путь, mTLS разрешен
только для /api/mtls
    location / {
        return 404 "mTLS endpoints only. Use port 443 for
regular access.";
```

```
    }

    ## Настройка проксирования запросов на backend
    location /api/mtls {
        proxy_set_header Host $host;
        proxy_set_header X-Real-IP $remote_addr;
        proxy_set_header X-Forwarded-For
$proxy_add_x_forwarded_for;
        proxy_set_header X-Forwarded-Proto $scheme;

        ## Передача информации о клиентском сертификате
        proxy_set_header X-SSL-Client-Verify $ssl_client_verify;
        proxy_set_header X-SSL-Client-DN $ssl_client_s_dn;
        proxy_set_header X-SSL-Client-Serial $ssl_client_serial;
        proxy_set_header X-SSL-Client-Fingerprint
$ssl_client_fingerprint;
        proxy_set_header X-SSL-Client-Issuer $ssl_client_i_dn;

        ## Проксирование на backend
        proxy_pass http://backend;
        proxy_redirect off;
    }
}
```

3. Перезапустите **Nginx** после внесения изменений.

Описание параметров

Параметр	Назначение
`ssl_certificate`	Сертификат сервера, используемый для HTTPS.
`ssl_certificate_key`	Закрытый ключ сервера.
`ssl_client_certificate`	Корневой сертификат CA для проверки клиентских сертификатов.
`ssl_verify_client on`	Включение обязательной проверки клиентских сертификатов.
`ssl_verify_depth`	Максимальная глубина цепочки проверки сертификатов клиента.
`ssl_session_timeout`	Время жизни SSL-сессии.
`ssl_protocols`	Разрешённые версии TLS.

Параметр	Назначение
`proxy_set_header X-SSL-Client-*`	Передача информации о клиентском сертификате на backend.

- Разместите серверные сертификаты (`.pem` и ключ) и корневой CA (`ca-bundle.crt`) в удобной директории, например `certs/`.
- Путь к сертификатам укажите в конфигурации **Nginx**.

Шаг 2. Создание провайдера mTLS

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **mTLS**.
6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, чтобы этот способ входа можно было добавить в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление провайдера mTLS на виджет

Чтобы пользователи увидели кнопку **mTLS** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **mTLS**.

Привязка клиентского сертификата для пользователей КриптоАРМ ID

> 📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **mTLS**.

Шаг 1. Установка клиентского сертификата в браузере

Перед установкой убедитесь, что у вас есть файл сертификата в формате `.p12` или `.pfx`.

Этот файл должен содержать:

- ваш персональный сертификат,
- закрытый ключ,
- и цепочку доверия (если требуется).

Установка в Google Chrome / Microsoft Edge

1. Откройте браузер **Chrome** или **Edge**.
2. Перейдите в **Настройки** → **Конфиденциальность и безопасность**.
3. Найдите раздел **Безопасность**.
4. Нажмите **Управление сертификатами**.
5. Перейдите на вкладку **Личное** / **Ваши сертификаты**.
6. Нажмите **Импорт...**.
7. В мастере импорта нажмите **Далее**.
8. Нажмите **Обзор** и выберите ваш файл `.p12` или `.pfx`.
9. Введите пароль, который вы получили с сертификатом.
10. Выберите **Поместить все сертификаты в следующее хранилище**.
11. Нажмите **Обзор** и выберите **Личное**.
12. Нажмите **Далее** → **Готово**.
13. При появлении предупреждения безопасности нажмите **Да**.

После успешной установки сертификат появится в списке на вкладке **Личное** / **Ваши сертификаты**.

Установка в Mozilla Firefox

1. Откройте меню **Firefox** → **Настройки**
2. Перейдите в раздел **Приватность и защита**
3. Прокрутите вниз до **Сертификаты**
4. Нажмите **Показать сертификаты...**
5. Перейдите на вкладку **Ваши сертификаты**
6. Нажмите **Импорт...**
7. Выберите ваш файл `.p12` или `.pfx`
8. Введите пароль к сертификату
9. Нажмите **OK**

После успешной установки сертификат появится в списке на вкладке **Ваши сертификаты**.

> ⚠ Сертификаты нужно устанавливать только на доверенные устройства и строго следить за сохранностью пароля.

> 💡 После установки сертификата, при входе через **mTLS**, браузер автоматически предложит выбрать соответствующий сертификат для аутентификации.

Шаг 2. Добавление идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **mTLS**.
4. Выберите сертификат, установленный на предыдущем шаге.

> 💡 **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **mTLS**.
2. Выберите иконку способа входа **mTLS**.
    - **Первый вход**: система может запросить выбор клиентского сертификата.

- **Повторные входы**: аутентификация выполняется автоматически с использованием ранее выбранного сертификата.

Как подключить вход через OpenID Connect

Шаг 1. Настройка на стороне внешней системы

1. Создайте приложение во внешнем сервисе идентификации.
2. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ ID**.

Шаг 2. Создание способа входа

1. Перейдите в кабинет администратора → вкладка **Настройки**.

> Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **OpenID Connect**.
6. Заполните форму создания:

Основная информация

- **Имя** — Название, которое увидят пользователи.
- **Описание** (опционально) — Краткое описание.
- **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

Параметры аутентификации

- **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
- **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
- **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.
- **Базовый адрес сервера авторизации (issuer)** — Адрес сервиса внешней идентификации.

- **Адрес авторизации (authorization_endpoint)** — Адрес, на который пользователь переадресовывается для авторизации.
- **Адрес выдачи токена (token_endpoint)** — Ресурс, обеспечивающий выдачу токенов.
- **Адрес получения информации о пользователе (userinfo_endpoint)** — Ресурс, который возвращает информацию о текущем пользователе.
- **Запрашиваемые разрешения (scopes)** — Перечень разрешений, которые должны быть получены при обращении к поставщику идентификации. Для добавления разрешения введите его имя и нажмите **Enter**.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через OpenID Connect** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **OpenID Connect**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 50 символов

Название	Описание	Тип	Ограничения
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`client_id`	ID приложения, созданного во внешней системе
Секретный ключ (client_secret)	`client_secret`	Сервисный ключ доступа приложения, созданного созданного на стороне внешней системы
Возвратный URL(Redirect URI) (не редактируемое)	`redirect URI`	Адрес **КриптоАРМ ID**, на который пользователь перенаправляется после аутентификации в стороннем сервисе
Базовый адрес сервера авторизации (issuer)	`issuer`	Адрес сервиса внешней идентификации
Адрес авторизации (authorization_endpoint)	`authorization_endpoint`	Адрес, на который пользователь переадресовывается для авторизации
Адрес выдачи токена (token_endpoint)	`token_endpoint`	Ресурс, обеспечивающий выдачу токенов
Адрес получения информации о пользователе (userinfo_endpoint)	`userinfo_endpoint`	Ресурс, который возвращает информацию о текущем пользователе

Название	Параметр	Описание
Запрашиваемые разрешения (scopes)	-	Перечень разрешений, которые должны быть получены при обращении к поставщику идентификации. Для добавления разрешения введите его имя и нажмите **Enter**.

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Как подключить вход через TOTP

Общая информация

TOTP (Time-based One-Time Password) — это алгоритм генерации одноразовых паролей, действительных в течение короткого промежутка времени.

Главное отличие **TOTP** от **HOTP** — генерация пароля на основе текущего времени. При этом обычно используется не точное указание времени, а текущий интервал с установленными заранее границами (обычно — 30 секунд).

Основные компоненты:

- **Сервер аутентификации** — сервер, который генерирует секретный ключ и проверяет введенные коды.
- **Аутентификатор** — приложение, хранящее секретный ключ и генерирующее текущий OTP.
- **Секретный ключ** — общая для сервера и приложения база, используемая для генерации кодов.

Процесс работы TOTP

1. **Предварительная настройка**
    - Администратор создает способ входа **TOTP** и активирует его для виджетов нужных приложений.
    - Пользователь в своем профиле добавляет новый идентификатор **TOTP**, сканируя QR-код с секретным ключом через приложение-аутентификатор.
2. **Генерация и проверка кода**
    - Приложение-аутентификатор вычисляет одноразовый пароль на основе секретного ключа и текущего временного интервала (обычно 30 секунд) с использованием алгоритма `SHA1`, `SHA256` или `SHA512`.
    - Когда пользователь вводит код на форме входа, сервер повторно вычисляет ожидаемый код по тому же секрету и текущему времени.
    - Если введенный код совпадает с ожидаемым, пользователю предоставляется доступ.

> **Важно**: Время на устройстве пользователя и на сервере должно быть синхронизировано. Несовпадение времени — самая частая причина отказа кода. Для компенсации небольшой разницы во времени сервер может принимать коды из соседних временных интервалов (обычно ±1 интервал).

Настройка аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в кабинет администратора → вкладка **Настройки**.

    > Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.
3. В открывшемся окне нажмите кнопку **Создать**  .
4. Откроется окно со списком шаблонов.
5. Выберите шаблон **TOTP**.
6. Заполните форму создания:

    Основная информация

- **Имя** — Название, которое увидят пользователи.
- **Описание** (опционально) — Краткое описание.
- **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

Параметры

- **Количество цифр** — Количество цифр в одноразовом пароле (обычно 6).
- **Период действия** — Время действия одноразового пароля в секундах (рекомендуется 30).
- **Алгоритм** — Алгоритм хеширования (`SHA1`, `SHA256` или `SHA512`) (обычно `SHA-1`).

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервис.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера TOTP на виджет

Чтобы пользователи увидели кнопку **TOTP** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **TOTP**.

Привязка TOTP для пользователей

> 📌 Инструкция предназначена для пользователей, которым необходимо выполнить вход в систему через **TOTP**.

Шаг 1. Установка приложения-аутентификатора

На ваше мобильное устройство необходимо установить приложение, которое генерирует TOTP-коды.

Самые популярные варианты:

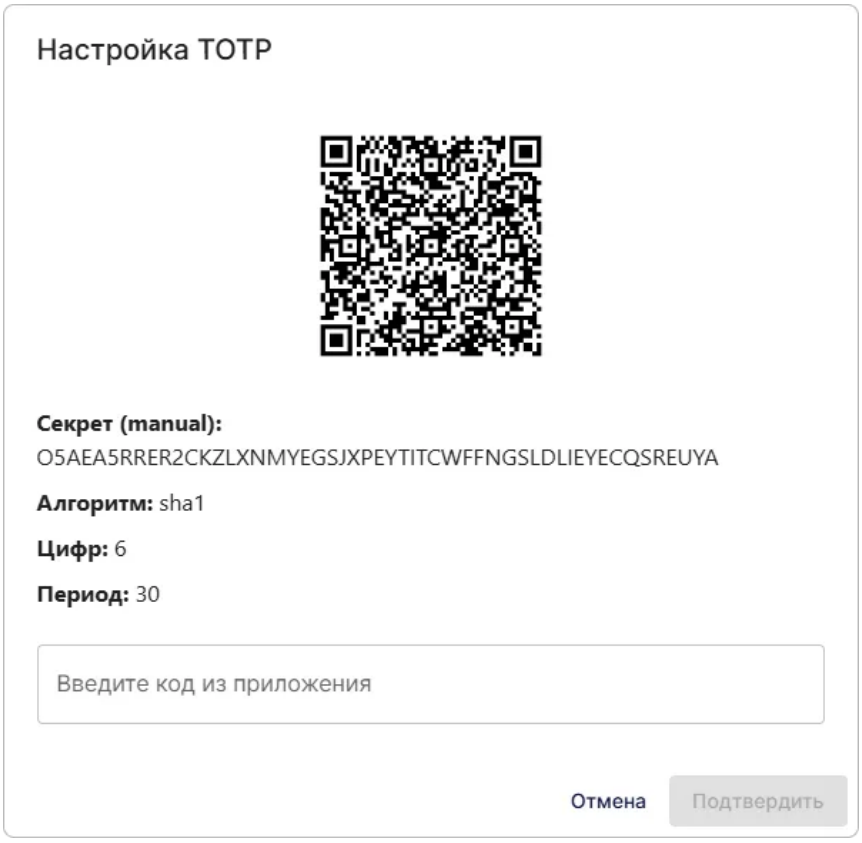
- **Яндекс Ключ** (Яндекс)
- **Google Authenticator** (Google)

> Убедитесь, что время на вашем мобильном устройстве настроено автоматически (через сеть). Неправильное время — самая частая причина того, что коды не принимаются.

Шаг 2. Добавление TOTP-идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **TOTP**.
4. Отсканируйте QR-код с помощью приложения-аутентификатора.

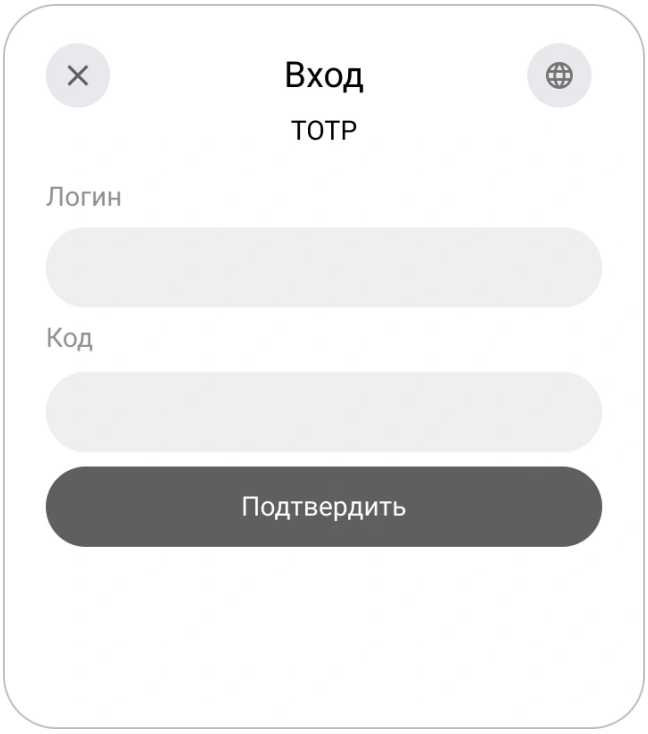


5. Введите код из приложения и подтвердите.

> **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Шаг 3. Проверка

1. Перейдите на страницу входа с включенным способом входа **TOTP**.
2. Выберите иконку способа входа **TOTP**.
3. Откроется форма для ввода кода.
4. Введите свой логин.



5. Не закрывая страницу, откройте приложение-аутентификатор на своем телефоне. Скопируйте 6-значный код и вставьте его в форму.
6. Нажмите кнопку **Подтвердить**.

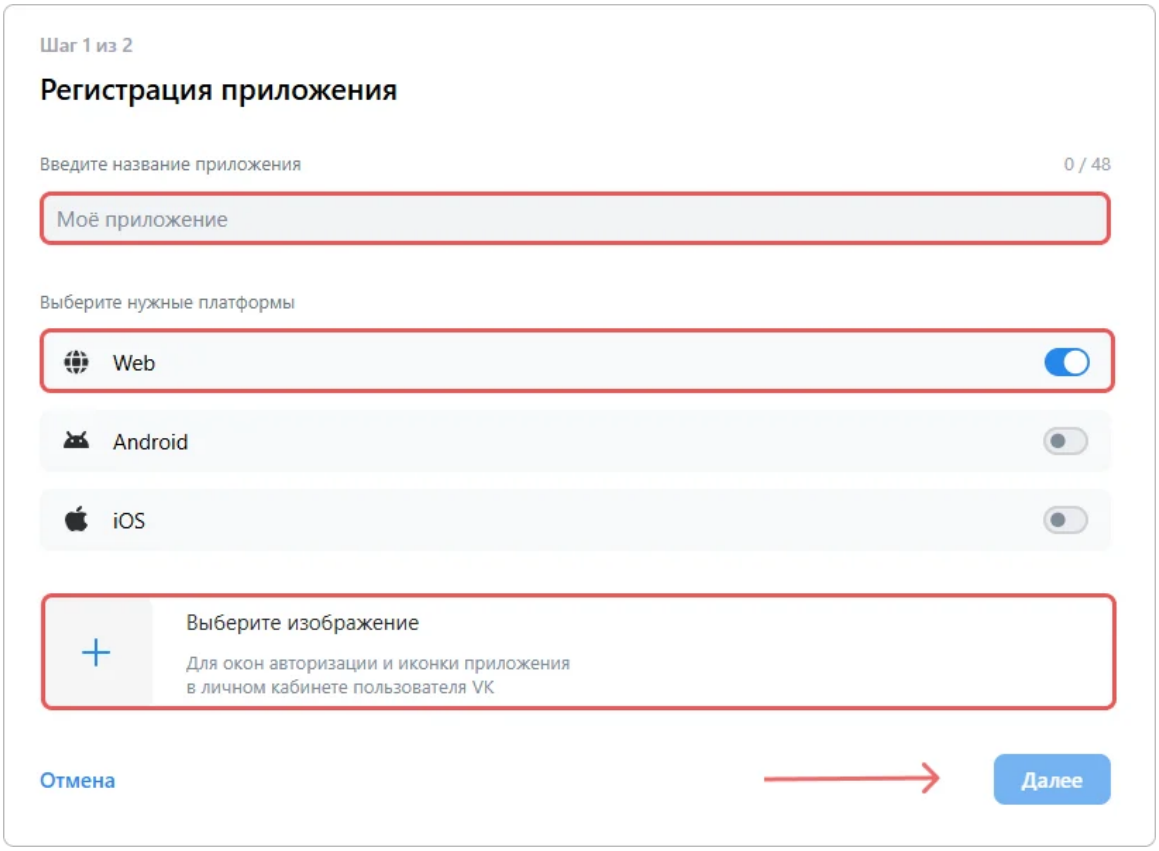
> **Если код не принимается**: Убедитесь, что время на вашем телефоне и сервере синхронизировано. Попробуйте подождать генерации следующего кода (новый появится через 30 секунд). Если проблема не исчезает, обратитесь к администратору.

Как подключить вход через ВКонтакте

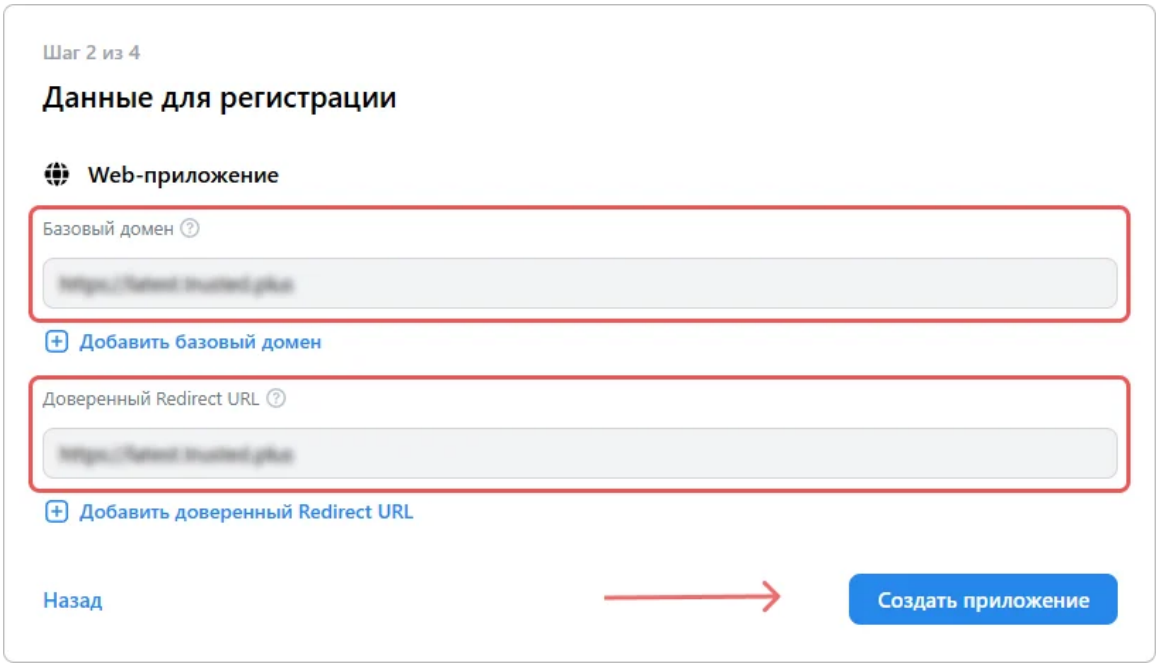
Шаг 1. Настройка приложения во Вконтакте

Перед настройкой способа входа в **КриптоАРМ ID** необходимо зарегистрировать ваше приложение в кабинете разработчика **Вконтакте** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь в сети ВКонтакте.
2. Откройте dev.vk.com и перейдите по ссылке для создания приложения с типом **Сайт**.
3. На первом шаге формы регистрации приложения:
   - Введите название приложения;
   - Выберите платформу **Web**;
   - Добавьте изображение (при необходимости).

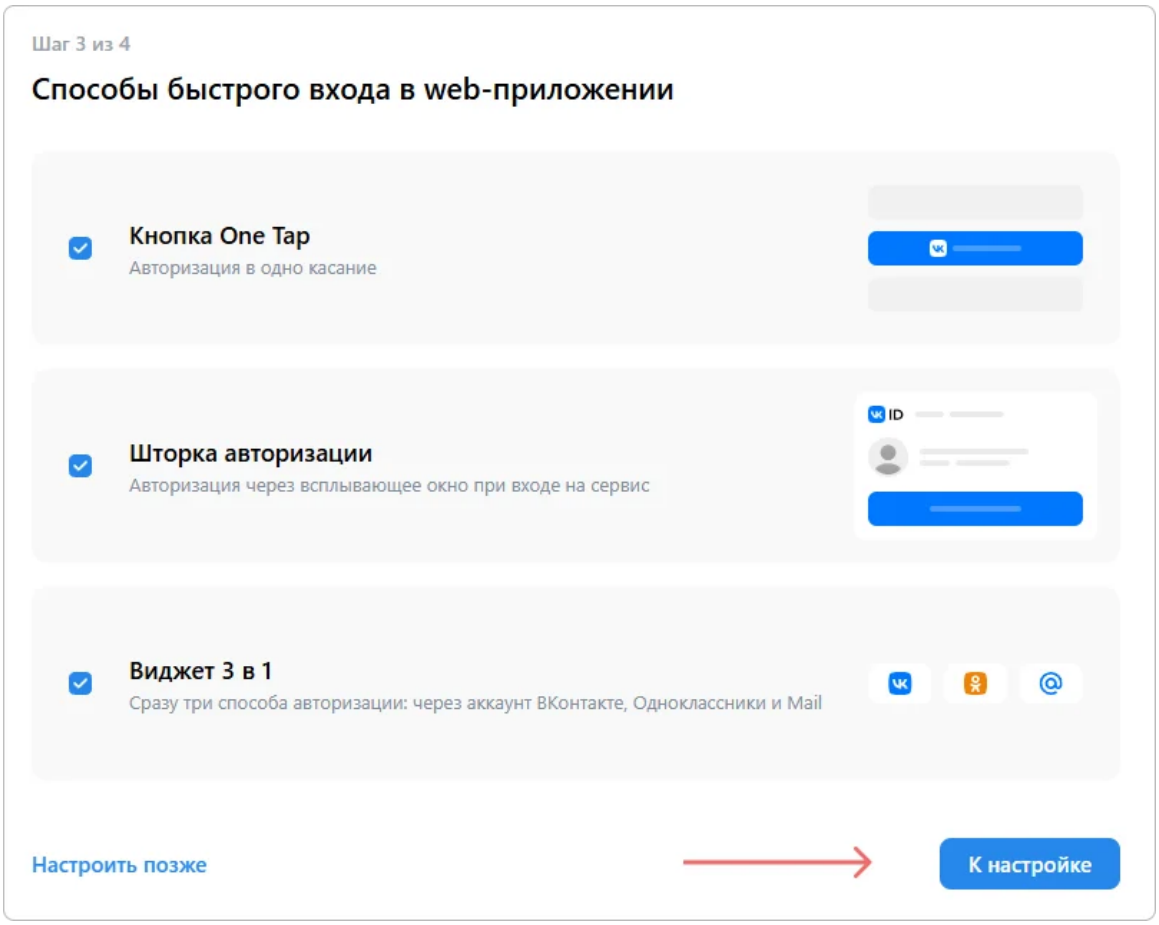


4. На втором шаге формы регистрации приложения укажите:
   - **Базовый домен** - адрес инсталляции сервиса **КриптоАРМ ID**;
   - **Доверенный Redirect URL** - возвратный URL (`Redirect_uri`) в формате `https://<адрес инсталляции>/api/interaction/code`.

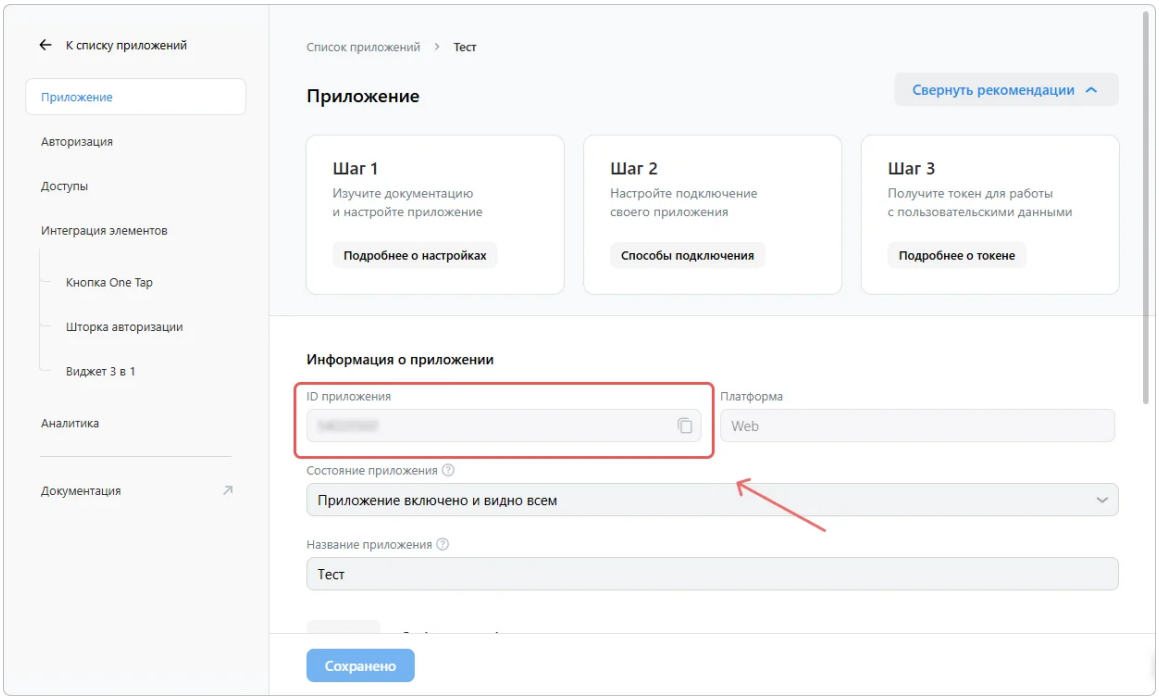


5. Нажмите **Создать приложение**.

6. На третьем шаге с настройкой способов быстрого входа нажмите **К настройке**.



7. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ ID**.



Шаг 2. Создание способа входа

Теперь, имея ключи от **Вконтакте**, создадим соответствующий провайдер в системе **КриптоАРМ ID**.

1. Перейдите в кабинет администратора → вкладка **Настройки**.

> Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон **Вконтакте**.

6. Заполните форму создания:

Основная информация

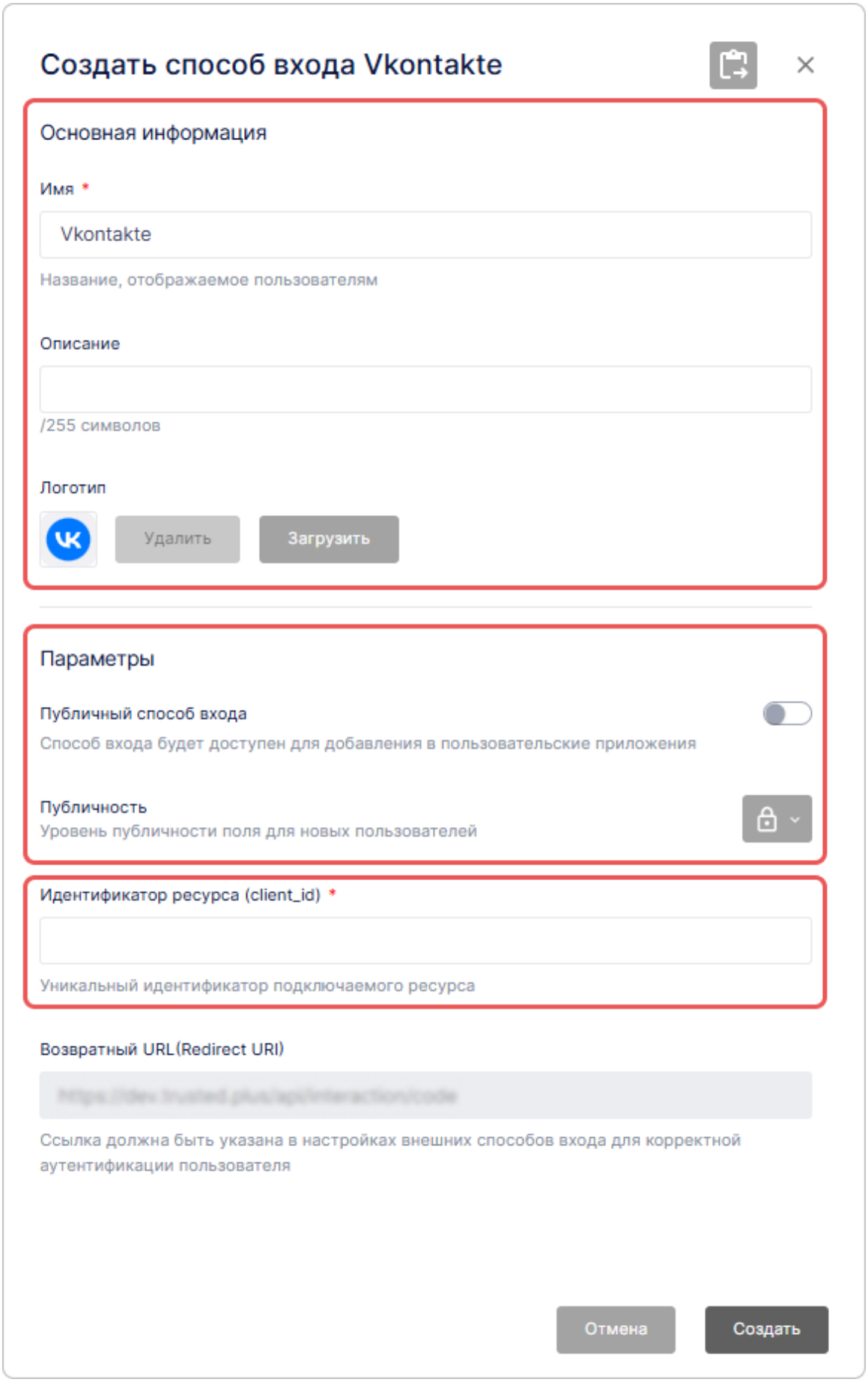
- **Имя** — Название, которое увидят пользователи.
- **Описание** (опционально) — Краткое описание.
- **Логотип** (опционально) — Можно загрузить свою иконку или будет использована стандартная.

Параметры аутентификации

- **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
- **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
- **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

Дополнительные настройки

- **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
- **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.



7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Вконтакте** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Вконтакте**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **ВКонтакте**
Возвратный URL(Redirect URI) (не редактируемое)	`Redirect URI`	Адрес **КриптоАРМ ID**, на который пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Как подключить вход по протоколу WebAuthn

Общая информация

WebAuthn (Web Authentication) — стандарт аутентификации, который позволяет пользователям входить в систему без пароля, используя надёжные методы проверки:

- биометрия (Face ID, Touch ID);
- аппаратные ключи безопасности;
- встроенные модули безопасности устройств.

WebAuthn входит в спецификацию **FIDO2**, поддерживается всеми современными браузерами.

> 🔐 **WebAuthn** можно использовать как основной способ входа, либо как дополнительный — для многофакторной аутентификации.

Процесс работы WebAuthn

1. **Регистрация пользователя:**
    - Пользователь создает ключ аутентификации.
    - Устройство генерирует пару ключей: публичный ключ сохраняется в системе, а приватный остается только у пользователя.
2. **Инициация входа:**
    - Пользователь выбирает способ входа **WebAuthn** на веб-ресурсе.
    - Сервер отправляет вызов (`challenge`) для подтверждения идентичности.
3. **Аутентификация пользователя:**
    - Устройство или токен подписывает `challenge` приватным ключом.
    - Сервер проверяет подпись с помощью сохраненного публичного ключа.
    - Если подпись корректна — пользователь получает доступ.

4. **Установление защищенного канала:** После успешной аутентификации пользователь входит в систему без передачи пароля через сеть.

Настройка WebAuthn-аутентификации для администраторов

Шаг 1. Создание способа входа

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон **WebAuthn**.

6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, чтобы этот способ входа можно было добавить в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 2. Добавление провайдера WebAuthn на виджет

Чтобы пользователи увидели кнопку **WebAuthn** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **WebAuthn**.

Добавление ключа для пользователя

Шаг 1. Добавление ключа на устройство

Регистрация ключа **WebAuthn** — это процесс, при котором создаётся связка публичного и приватного ключей и привязывается к конкретному пользователю.

Чтобы использовать вход по **WebAuthn**, пользователю необходимо сначала зарегистрировать ключ — это может быть встроенный аутентификатор (например, **Touch ID**, **Face ID** или **Windows Hello**), либо внешний физический ключ безопасности.

Во время добавления ключа создаётся уникальная криптографическая пара — **публичный** и **приватный ключи**.

- Приватный ключ надёжно сохраняется на устройстве пользователя и никогда не передаётся в сеть.
- Публичный ключ сохраняется на сервере **КриптоАРМ ID** и используется для последующей проверки подлинности при входе.

После регистрации ключа пользователю необходимо добавить идентификатор **WebAuthn** в своем профиле **КриптоАРМ ID**.

Шаг 2. Добавление идентификатора в профиль

1. Перейдите в свой **Профиль**.
2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите способ входа **WebAuthn**.
4. В системном окне укажите ранее зарегистрированный ключ.

> **Совет**: Если идентификатор уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

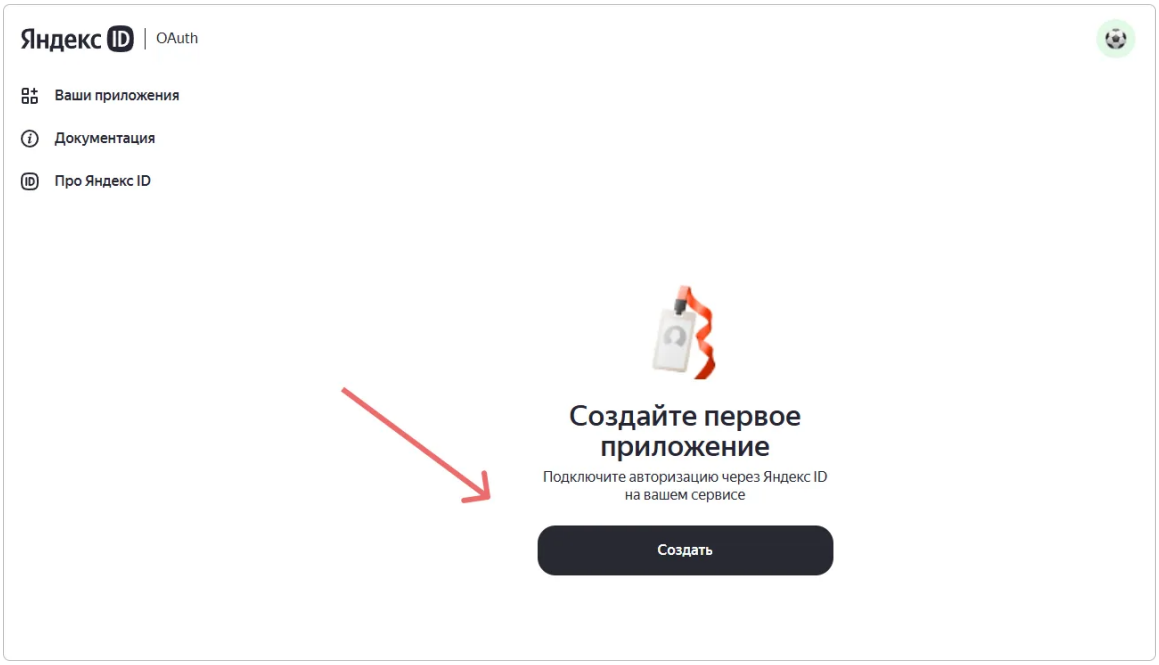
Как подключить вход через Яндекс

Шаг 1. Настройка приложения в Яндекс

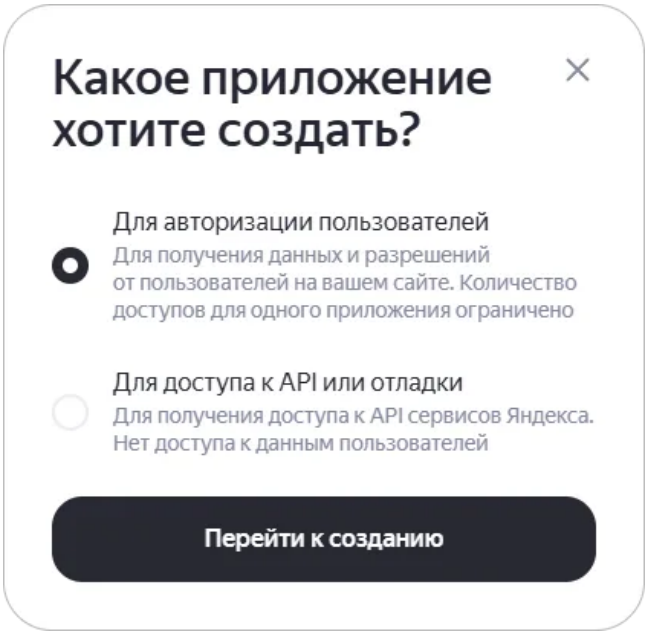
Перед настройкой способа входа в **КриптоАРМ ID** необходимо зарегистрировать ваше приложение в кабинете разработчика **Яндекс** и получить ключи доступа:

1. Зарегистрируйтесь или авторизуйтесь в сервисе Яндекс OAuth.

2. Нажмите кнопку **Создать**.



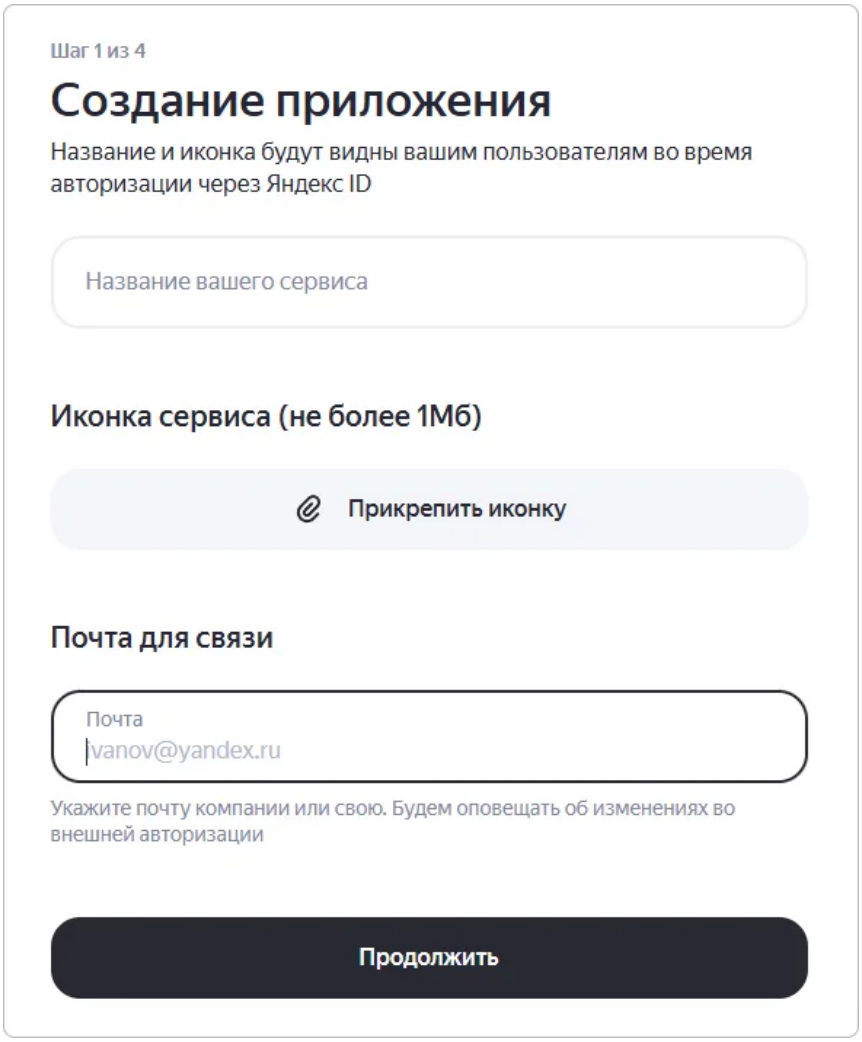
3. Выберите вариант **Для авторизации пользователей** и нажмите **Перейти к созданию**.



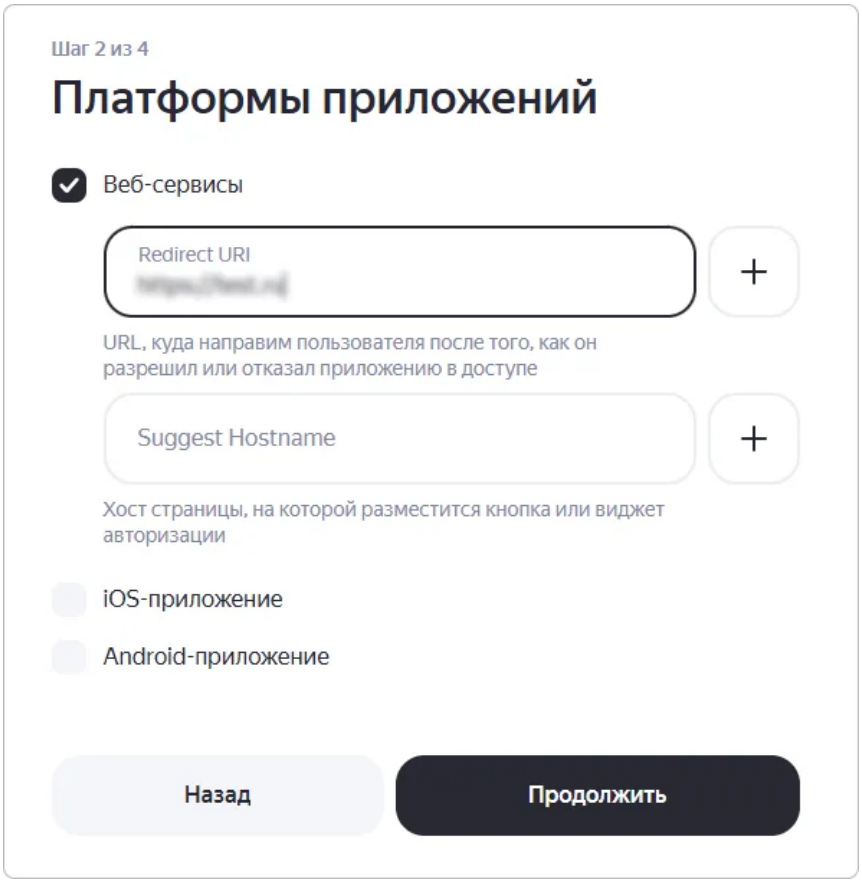
4. Откроется форма создания.

5. На первом шаге формы укажите:

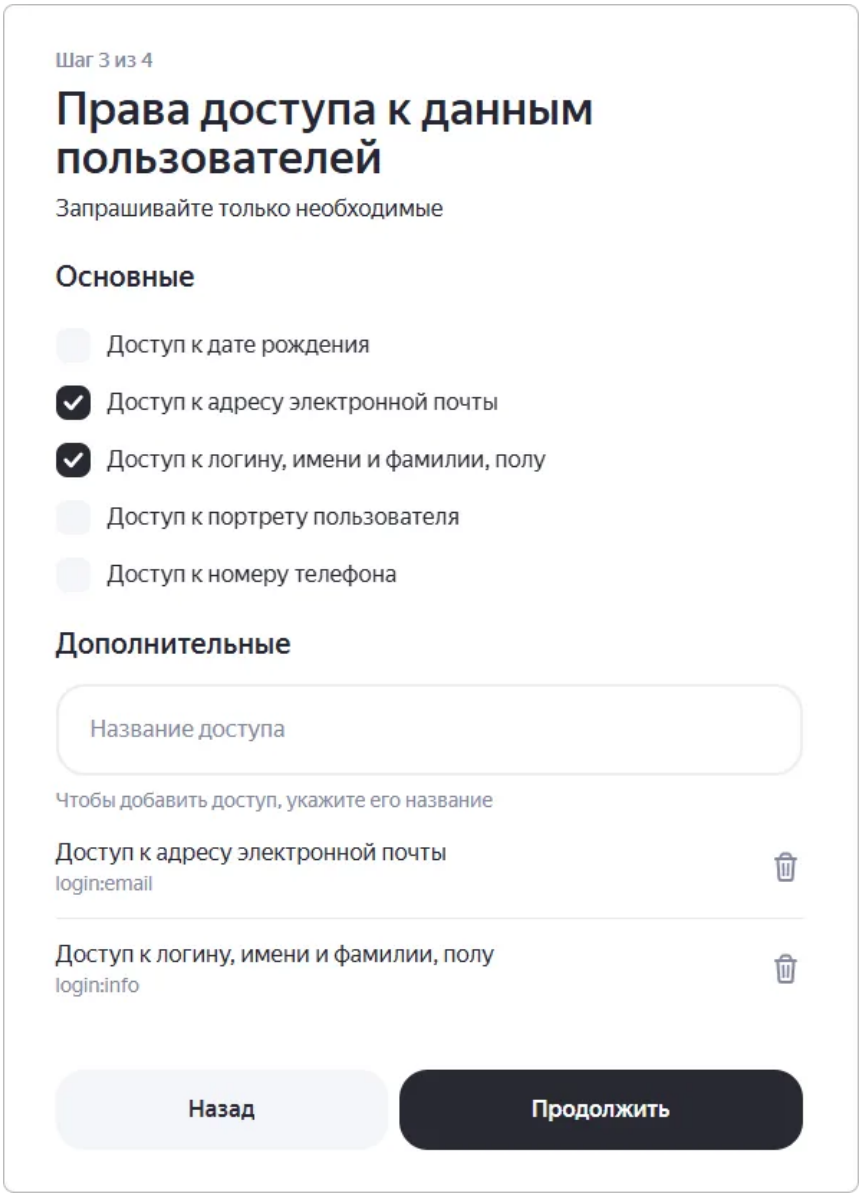
- **Название сервиса**,
- **Иконку сервиса**,
- **Электронную почту**.



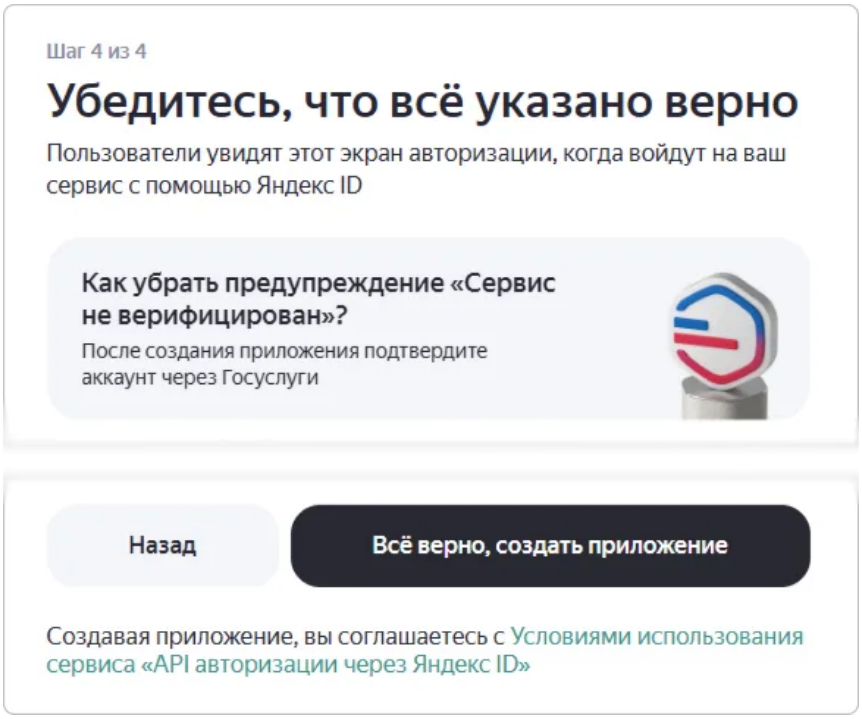
6. На втором шаге установите чекбокс **Веб-сервисы** и укажите **Возвратный URL #1** (`Redirect_uri`) в формате `https://<your-domain>/api/interaction/code`.



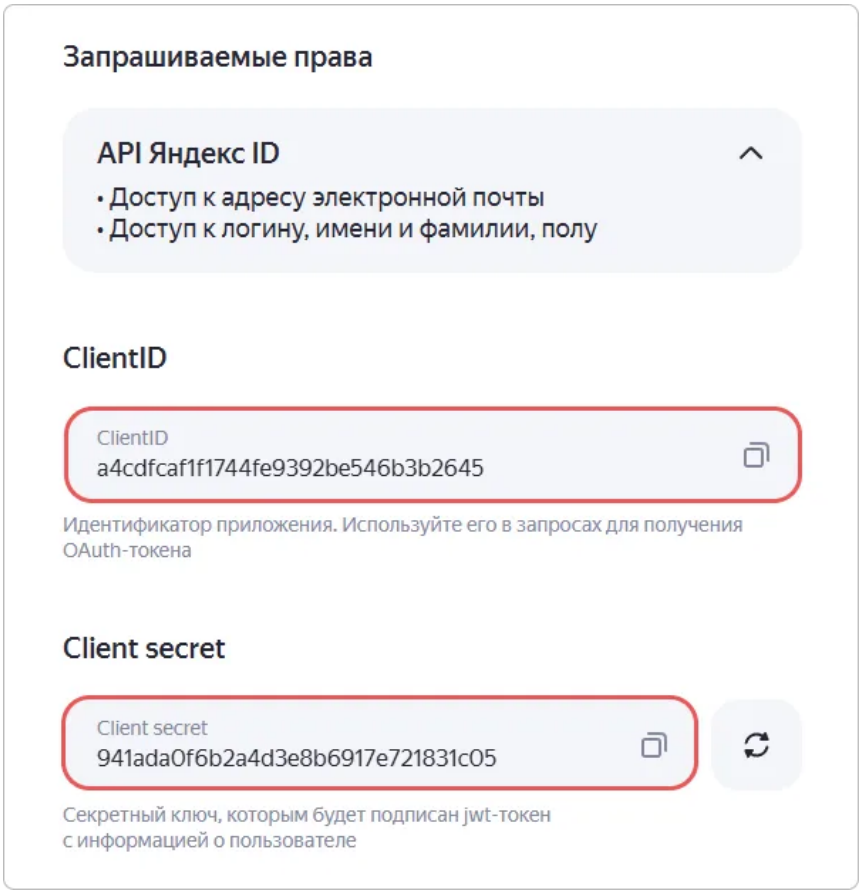
7. На третьем шаге установите чекбоксы:
    - **Доступ к адресу электронной почты**;
    - **Доступ к логину, имени и фамилии, полу**.



8. На четвертом шаге подтвердите создание приложения.



9. Скопируйте значения полей **ID Приложения/Client ID** и **Секрет/Client Secret**. Они понадобятся при создании приложения в **КриптоАРМ ID**.



Шаг 2. Создание способа входа

Теперь, имея ключи от **Яндекс**, создадим соответствующий провайдер в системе **КриптоАРМ ID**.

1. Перейдите в кабинет администратора → вкладка **Настройки**.

   > 💡 Чтобы создать способ входа для организации, откройте **кабинет организации**. Если способ входа нужен для конкретного приложения, откройте **настройки этого приложения**.

2. Найдите блок **Способы входа** и нажмите **Настроить**.

3. В открывшемся окне нажмите кнопку **Создать**  .

4. Откроется окно со списком шаблонов.

5. Выберите шаблон **Яндекс**.

6. Заполните форму создания:

   Основная информация

   - **Имя** — Название, которое увидят пользователи.
   - **Описание** (опционально) — Краткое описание.
   - **Логотип** (опционально) — Можно загрузить свою иконку, или будет использована стандартная.

   Параметры аутентификации

   - **Идентификатор ресурса (client_id)** — Вставьте скопированный **ID Приложения** (`Client ID`).
   - **Секретный ключ (client_secret)** — Вставьте скопированный **Секрет** (`Client Secret`).
   - **Возвратный URL(Redirect URI)** — Поле заполнится автоматически на основе вашего домена.

   Дополнительные настройки

   - **Публичный способ входа** — Включите, если хотите, чтобы этот способ входа можно было добавить в другие приложения системы (или организации), а также в профиль пользователя в качестве идентификатора внешнего сервиса.
   - **Публичность** — Настройте уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя.

7. Нажмите **Создать**.

После успешного создания новый способ входа появится в общем списке провайдеров.

Шаг 3. Добавление на виджет

Чтобы пользователи увидели кнопку **Войти через Яндекс** на форме авторизации, нужно активировать эту функцию в настройках виджета:

1. В общем списке провайдеров найдите созданный способ входа.
2. Включите переключатель на панели с провайдером.

> **Проверка**: После сохранения откройте форму входа в тестовом приложении. На виджете должна появиться новая кнопка с логотипом **Яндекс**.

Описание параметров

Основная информация

Название	Описание	Тип	Ограничения
Имя	Название, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 50 символов
Описание	Краткое описание, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID**	Текст	Макс. 255 символов
Логотип	Изображение, которое будет отображаться в интерфейсе сервиса **КриптоАРМ ID** и виджете входа	JPG, GIF, PNG или WEBP	Макс. размер: 1 МБ

Параметры аутентификации

Название	Параметр	Описание
Идентификатор ресурса (client_id)	`Client_id`	ID приложения, созданного в **Яндекс**
Секретный ключ (client_secret)	`Client_secret`	Секретный ключ доступа приложения, созданного созданного в **Яндекс**
Возвратный URL(Redirect URI) (не редактируемое)	`Redirect URI`	Адрес **КриптоАРМ ID**, на который пользователь перенаправляется после аутентификации в стороннем сервисе

Дополнительные настройки

Название	Описание
Публичный способ входа	При активации настройки: - Способ входа станет доступен для добавления в другие приложения сервиса. - Способ входа станет доступен для добавления в качестве идентификатора внешнего сервиса в профиле пользователя.
Публичность	Задает уровень публичности по умолчанию для идентификатора внешнего сервиса в профиле пользователя

Руководство пользователя

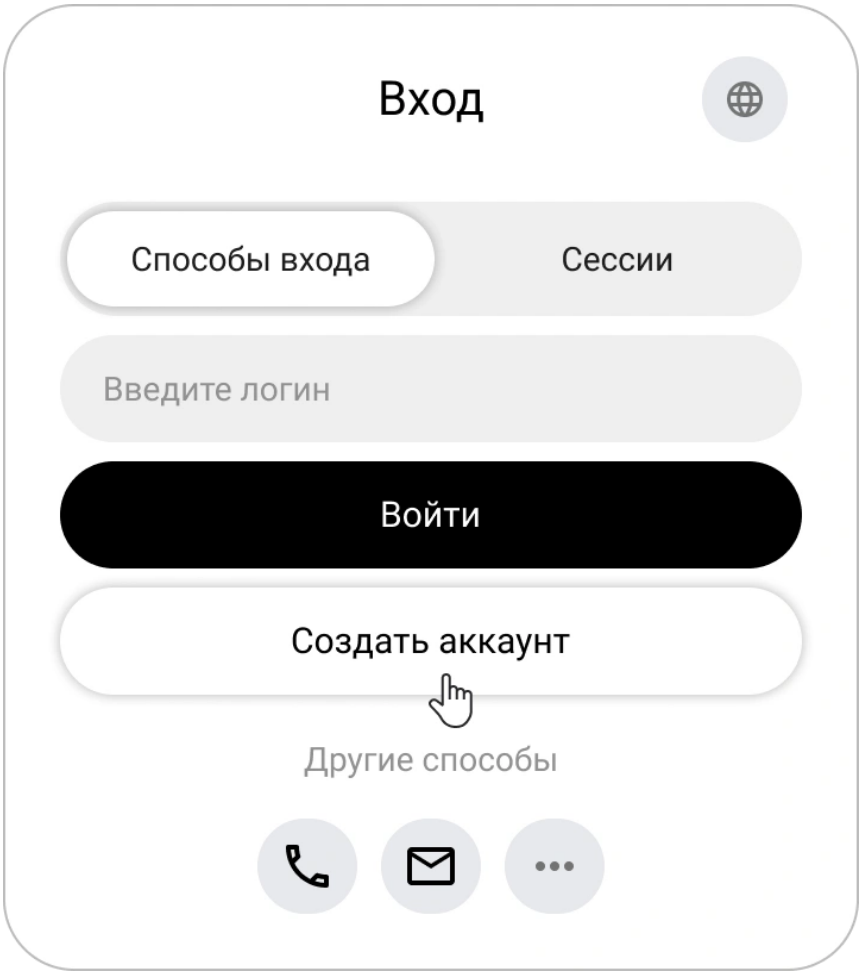
Регистрация и вход

Регистрация нового аккаунта

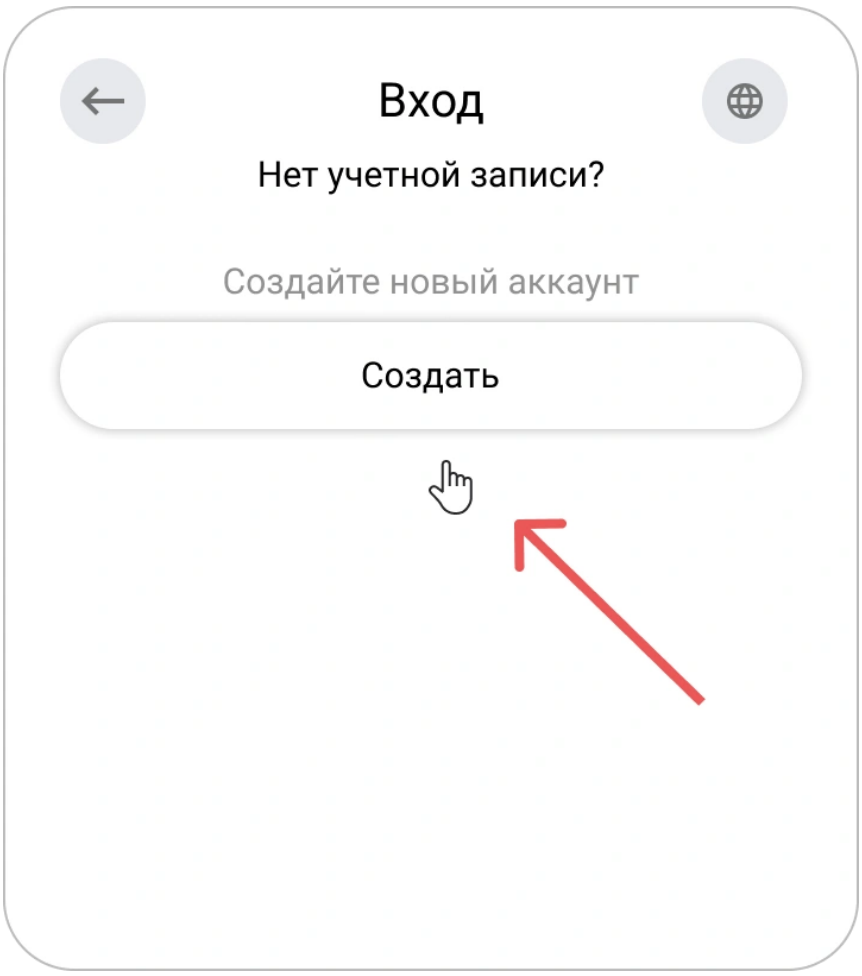
Где доступна регистрация

Функция создания аккаунта может быть доступна в двух случаях:

1. **На форме входа**;



2. **На форме выбора действий при входе через способ входа**, если указанный идентификатор не привязан ни к одному профилю в **КриптоАРМ ID**

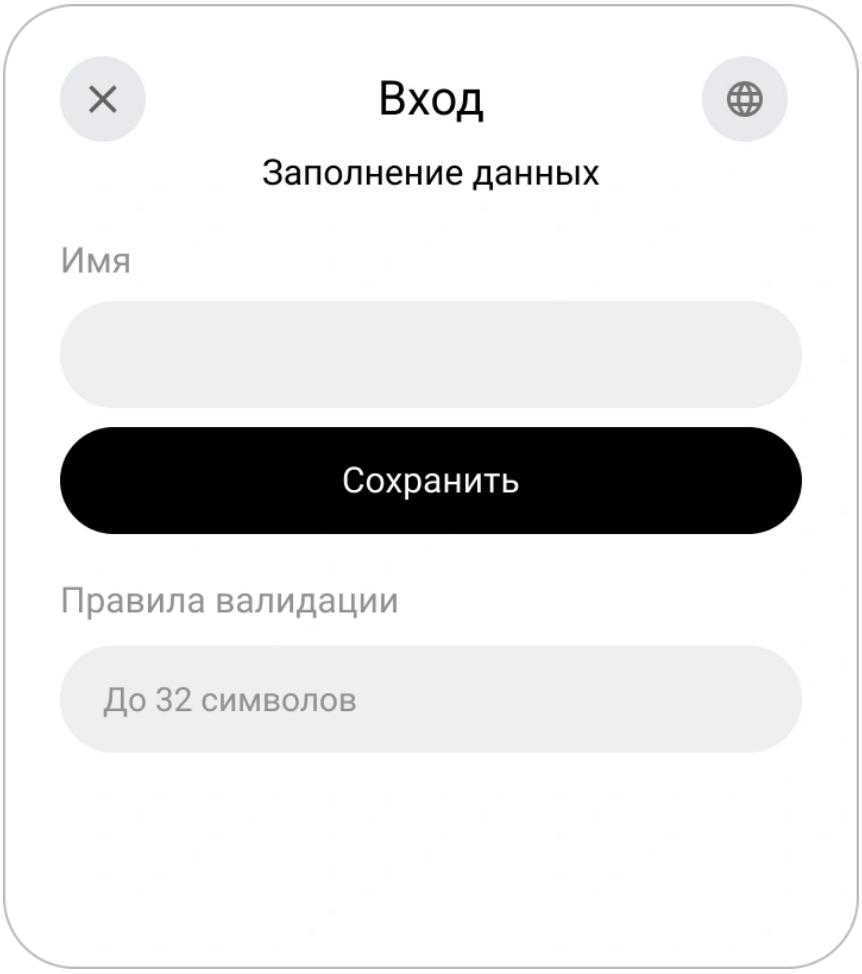


> **Дизайн форм** может отличаться в зависимости от настроек конкретного приложения

Как создать аккаунт в КриптоАРМ ID

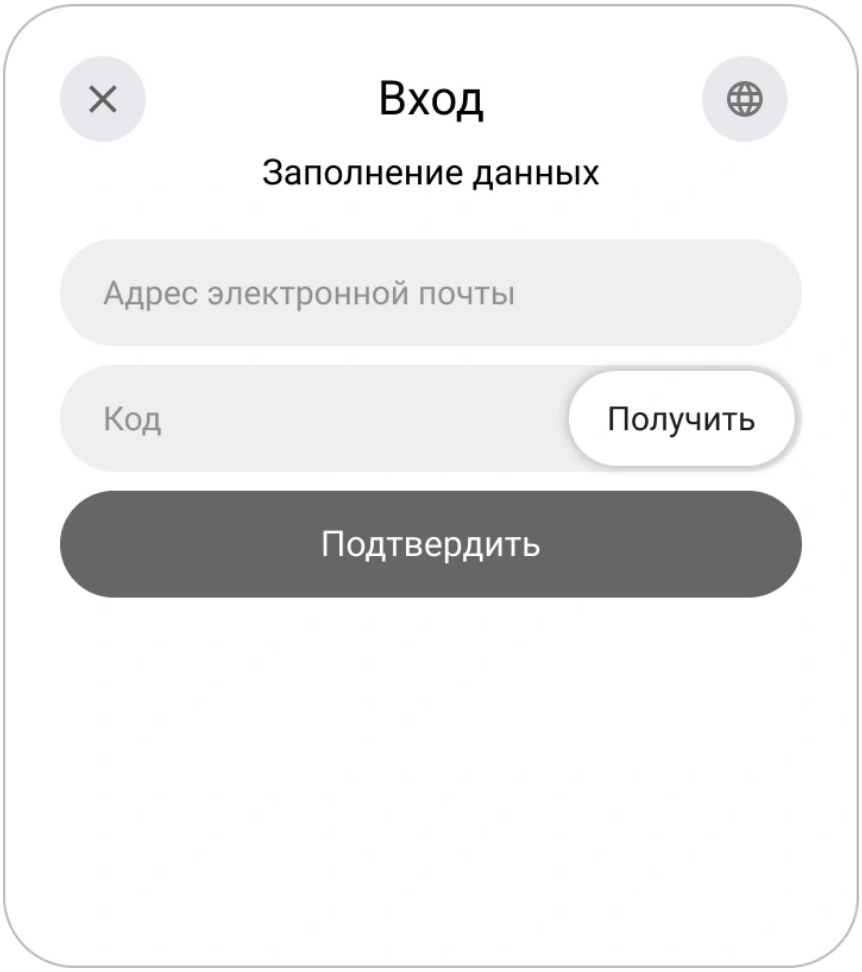
1. Нажмите **Создать аккаунт** на форме входа или выбора действий.
2. Введите необходимые данные в регистрационной форме.

   Пример окна для ввода имени:



3. Если система запросит e-mail — укажите адрес, не привязанный к другим пользователям.

4. Введите код или перейдите по ссылке из письма, отправленного на указанную почту.



> 💡 Если подтверждение выполняется по ссылке, окно ввода кода можно закрыть.

5. При первом входе в приложение разрешите доступ к необходимым данным.

После выполнения шагов аккаунт будет создан, и произойдет вход в систему.

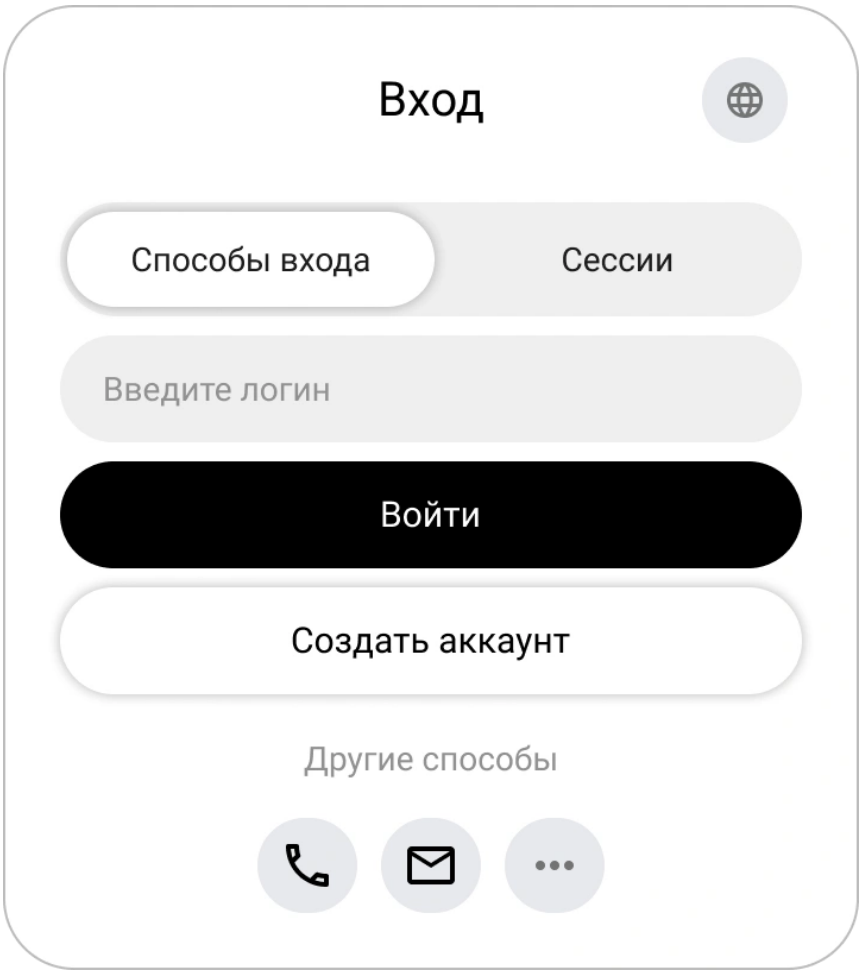
> 🔗 Если регистрация начата через внешний сервис, идентификатор внешней системы автоматически привяжется к новому профилю. Его можно будет использовать для последующих входов.

Вход по логину и паролю

Вы можете авторизоваться в приложении с помощью учетной записи **КриптоАРМ ID**.

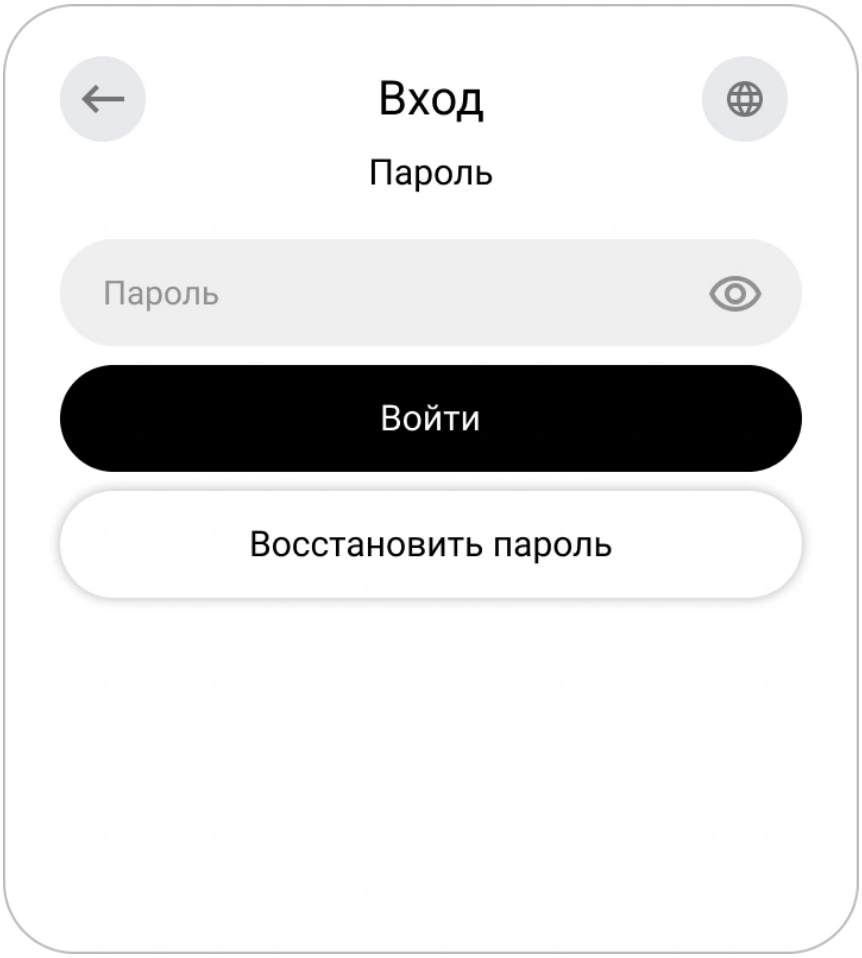
Чтобы войти в систему:

1. На первом шаге виджета входа введите данные для идентификации (например, логин, e-mail или номер телефона) и нажмите **Войти**.



2. Введите пароль на втором шаге и нажмите **Войти**.

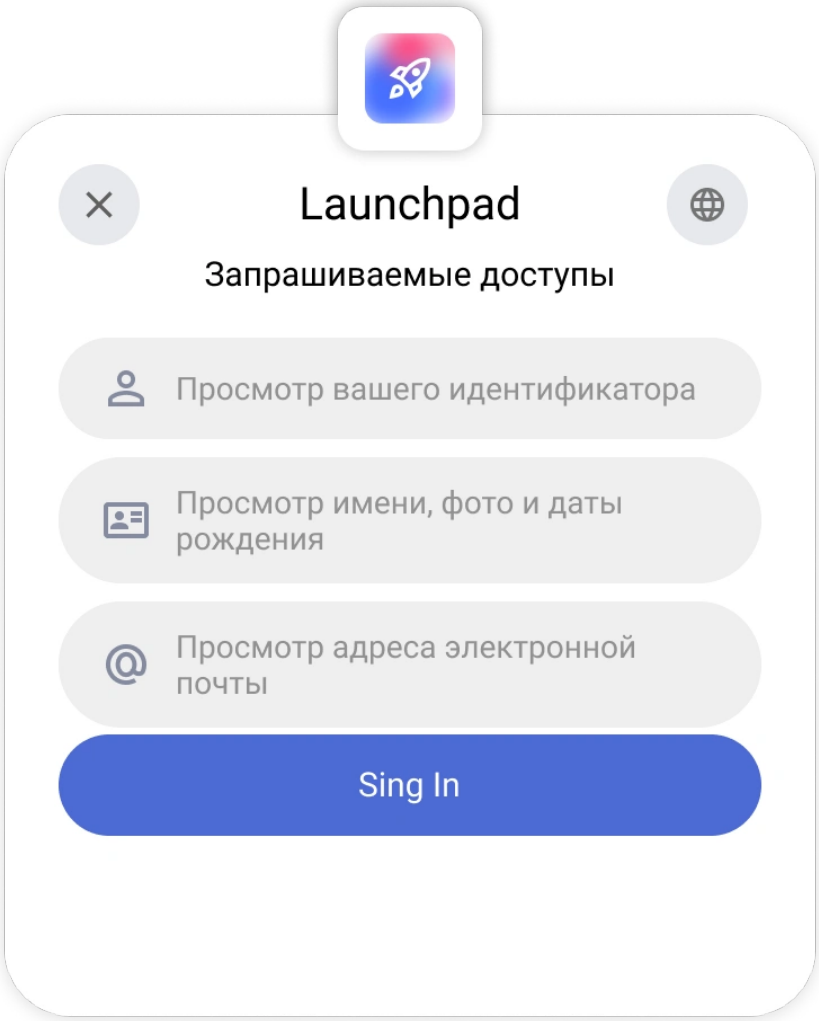
> Если вы допустили ошибку при вводе данных, следуйте подсказкам на экране.



После успешной аутентификации:

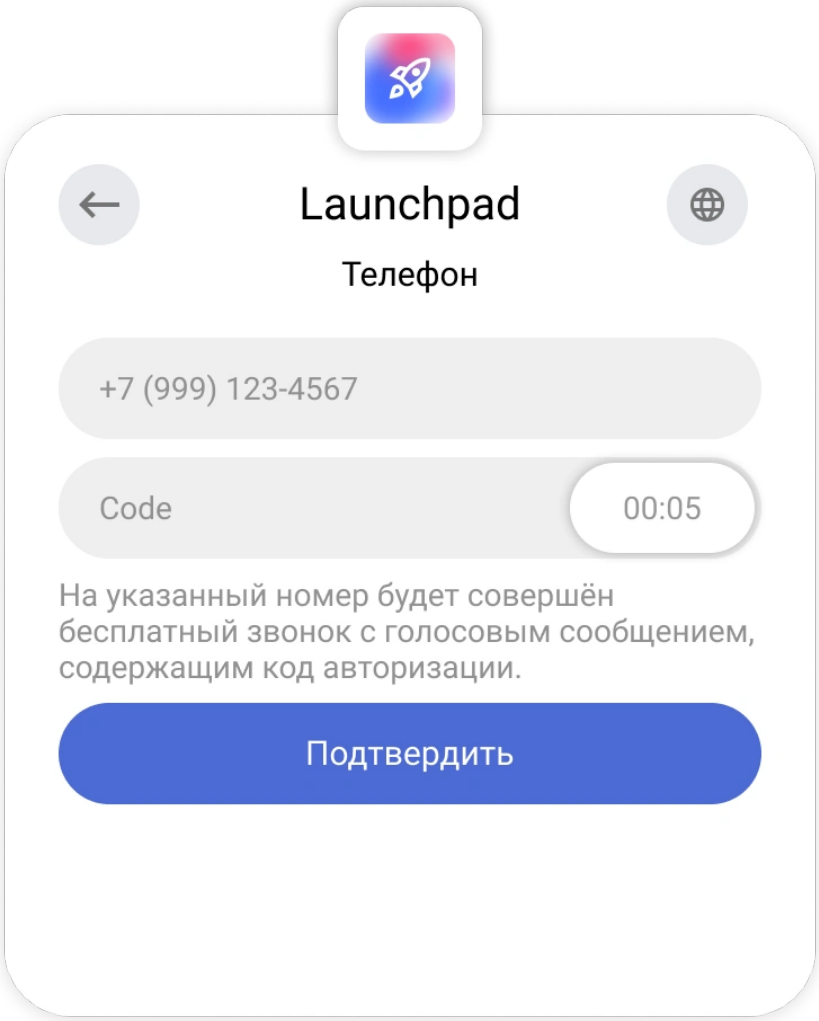
- при первом входе откроется форма подтверждения доступа к данным;

  Пример формы с запросом доступа к данным профиля:



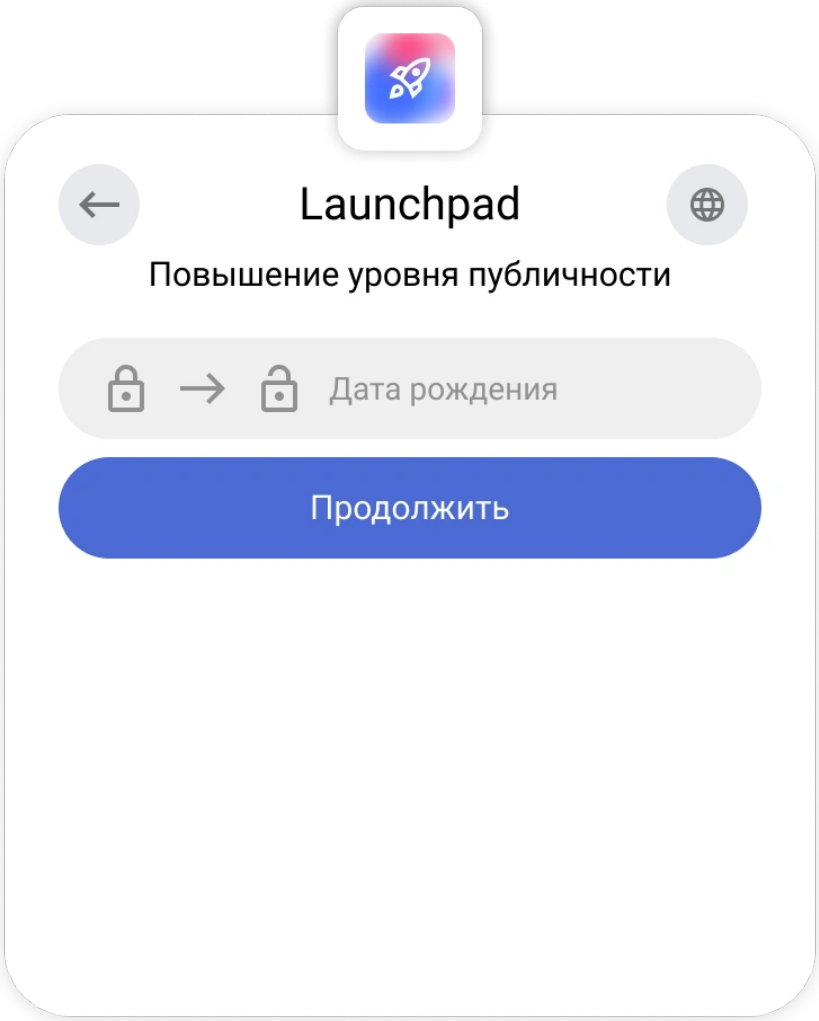
- если приложению требуются обязательные поля профиля, система запросит их заполнение;

  Пример запроса номера телефона:



- если данные скрыты настройками приватности, будет предложено изменить уровень доступа.

  Пример изменения приватности даты рождения:

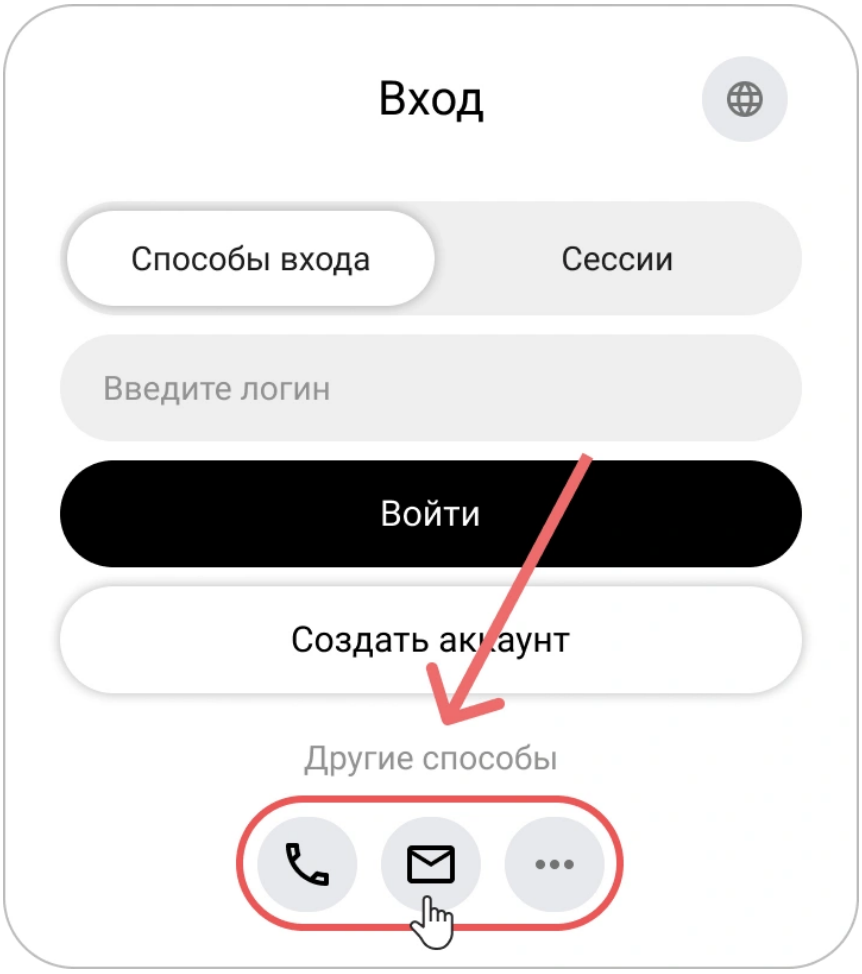


Вход через внешние сервисы

К внешним сервисам идентификации (или способам входа) относятся социальные сети и внешние сервисы (Yandex, Mail, Вконтакте и др.).

Чтобы войти через внешний сервис:

1. Выберите нужный способ входа в виджете.



2. Пройдите авторизацию в выбранном сервисе, используя доступные способы для социальных сетей.

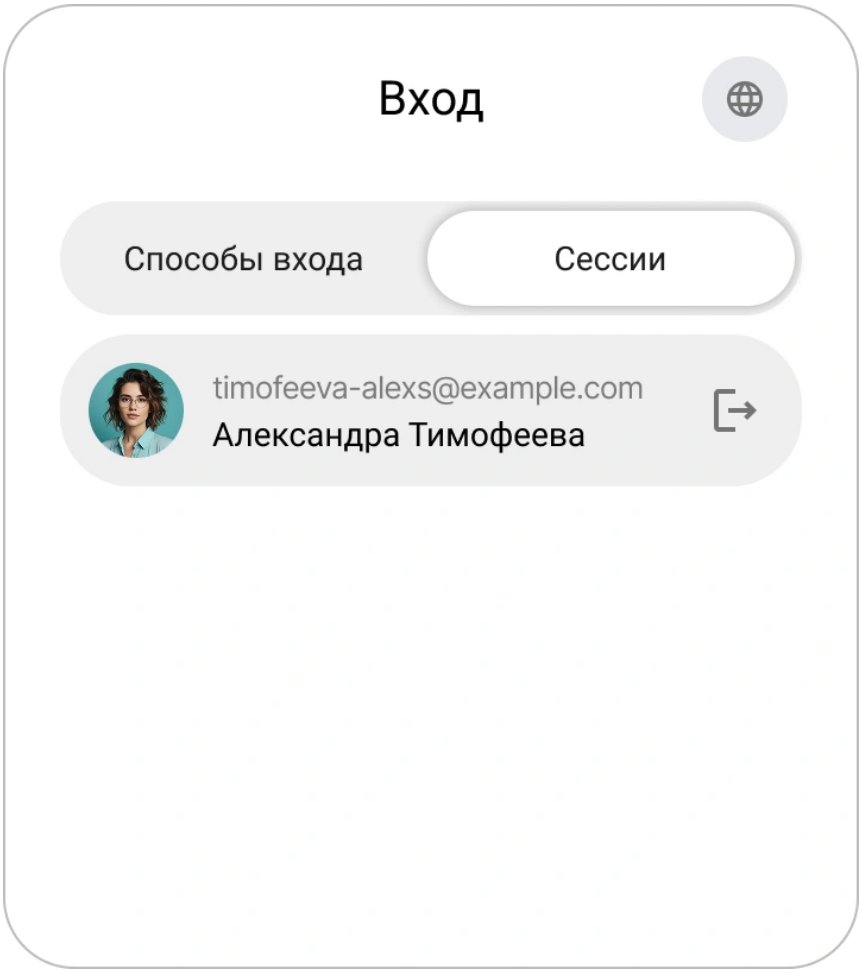
3. При первом входе откроется форма запроса доступа к данным. Предоставьте согласие на доступ к своим данным.

Быстрый вход для аутентифицированных пользователей

Если вы уже выполняли вход в **КриптоАРМ ID** в своем браузере, повторная авторизация не потребуется.

1. При входе откроется окно выбора сохранённого аккаунта.

2. Нажмите на имя пользователя.



3. После выбора пользователя произойдет вход.

Дополнительно:

- Чтобы войти под другим пользователем, выберите **Способы входа** и пройдите авторизацию другим пользователем.
- Чтобы завершить текущую сессию, нажмите кнопку **Выйти из аккаунта**.

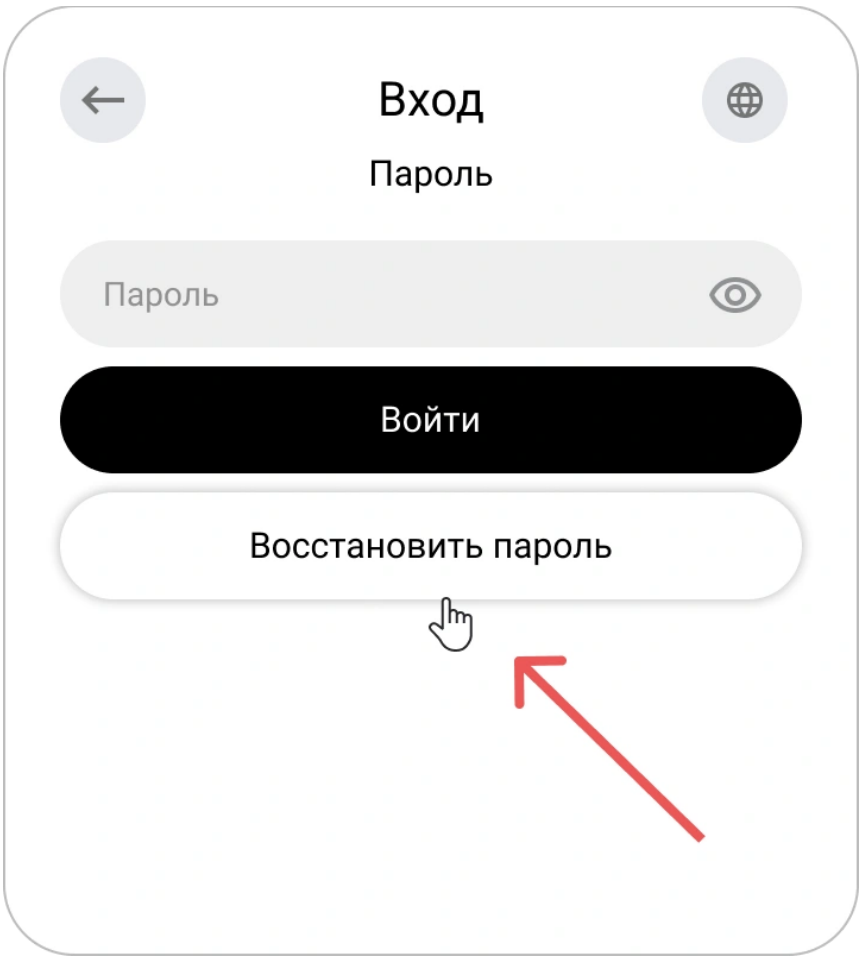
Восстановление пароля

Если вы забыли пароль от своей учётной записи в **КриптоАРМ ID**, вы можете легко его восстановить.

Как восстановить пароль в КриптоАРМ ID

1. На первом шаге виджета входа введите данные для идентификации (например, логин, e-mail или номер телефона) и нажмите **Войти**.

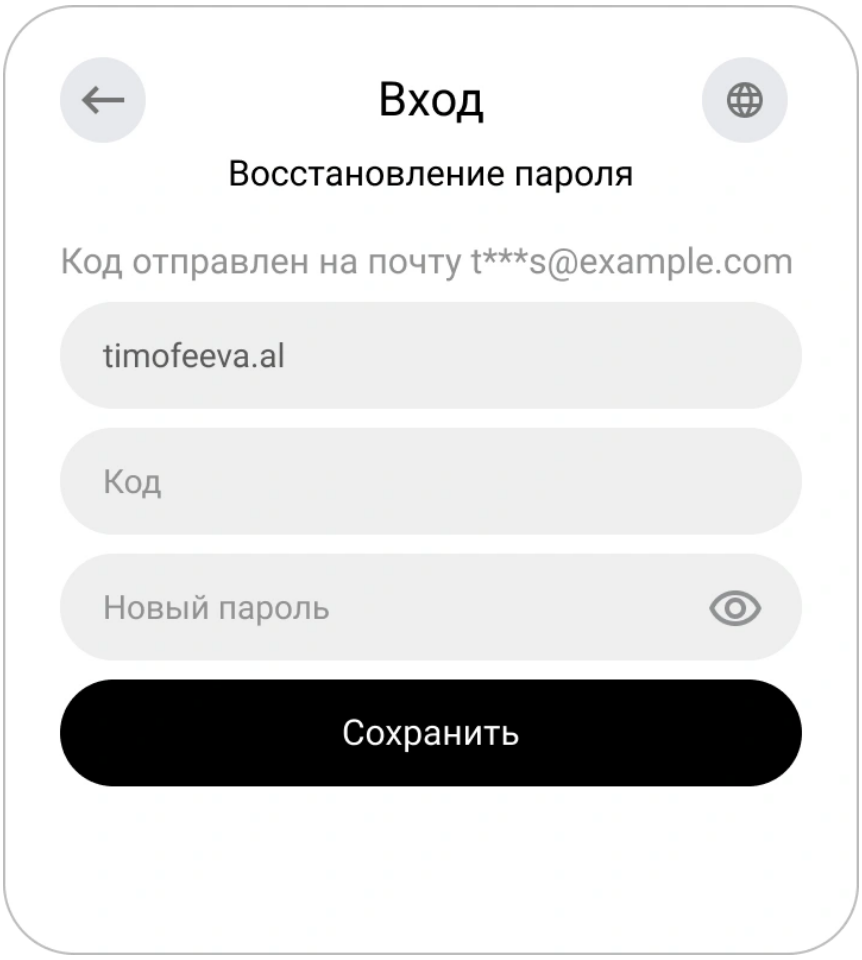
2. На следующем шаге выберите **Восстановить пароль**.



3. На вашу почту будет направлено письмо с кодом подтверждения.

4. Введите код из письма.

> ⚠ Код действует ограниченное время. Если срок действия истёк, запросите новый код.



5. Задайте новый пароль и нажмите **Сохранить**.

После обновления пароля вход будет выполнен автоматически.

> ☑ Пароль успешно восстановлен, теперь вы можете использовать новую комбинацию при входе в систему.

Личный профиль

Профиль в КриптоАРМ ID — ваш центр управления данными и безопасностью аккаунта.

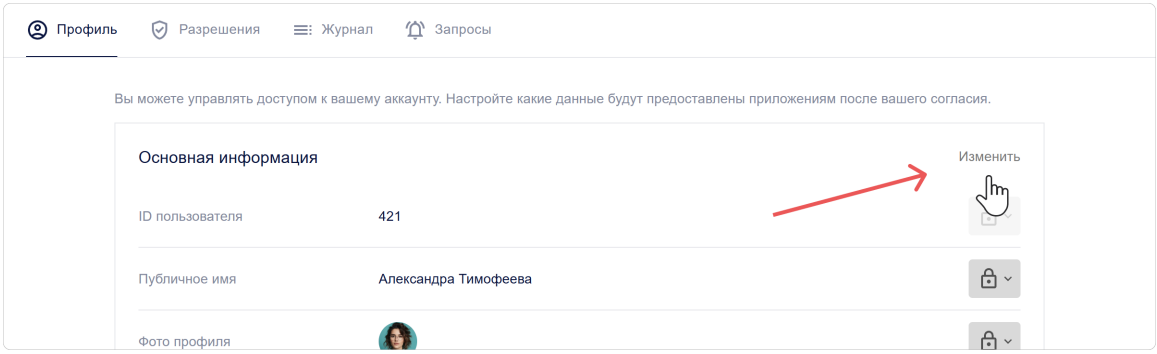
Управление личным профилем

Ваш профиль содержит основную информацию для идентификации в системе. В зависимости от способа регистрации некоторые поля могут быть недоступны для редактирования. Если вам нужно их отредактировать, свяжитесь с администратором сервиса.

Изменение персональной информации

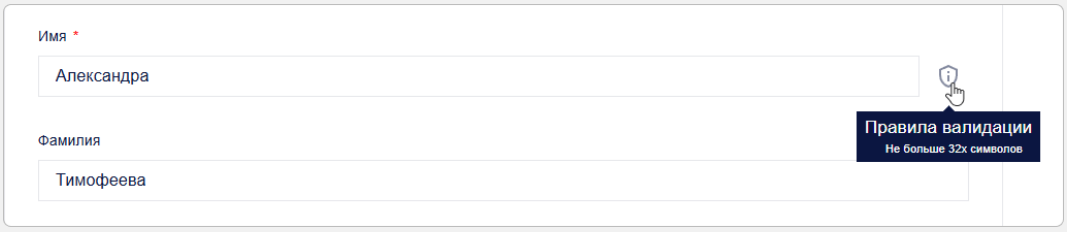
1. Перейдите в свой **Профиль**.

2. Нажмите **Изменить** в блоке **Основная информация**.



3. Внесите необходимые изменения в открывшейся форме.

> Для некоторых полей установлены правила валидации. Будьте внимательны при внесении изменений.



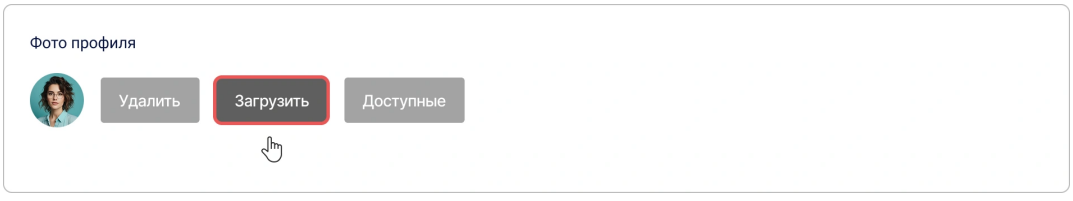
4. Нажмите **Сохранить**.

> **Важно:** Профиль можно сохранить даже с незаполненными обязательными полями. При следующем входе система запросит недостающие данные.

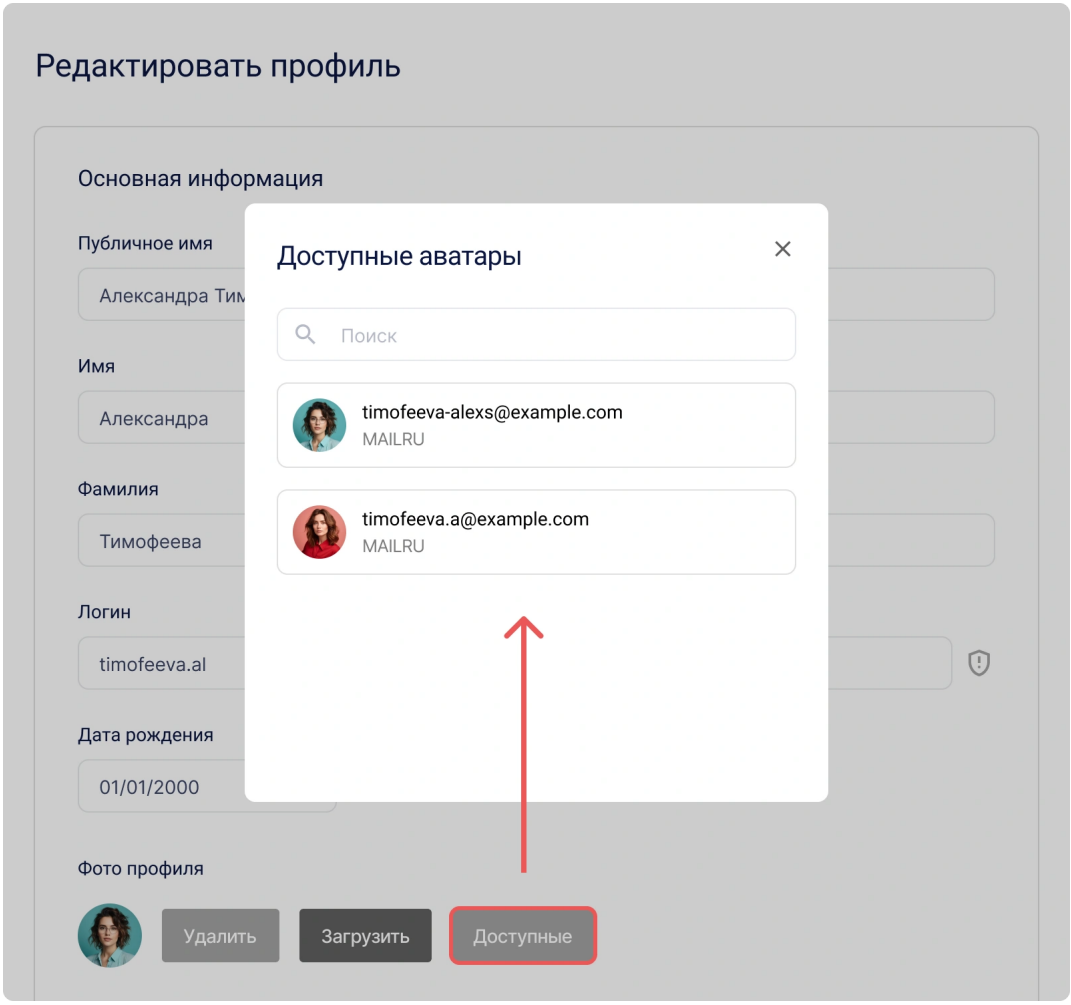
Добавление фото профиля

Вы можете загрузить фото с устройства или использовать аватар из привязанных внешних сервисов.

1. Перейдите в свой **Профиль**.
2. Нажмите **Изменить** в блоке **Основная информация**.
3. Откроется форма редактирования.
4. Добавьте фото одним из способов:
    - Нажмите кнопку **Загрузить** и укажите путь к файлу с фото,



- Нажмите кнопку **Доступные** и выберите фото из внешней системы.



> 📌 Если в профиле нет привязанных идентификаторов внешних систем с фото, то кнопка **Доступные** будет скрыта.

> 💡 **Совет**: Чтобы удалить фото, нажмите на кнопку **Удалить** в блоке **Фото профиля**.

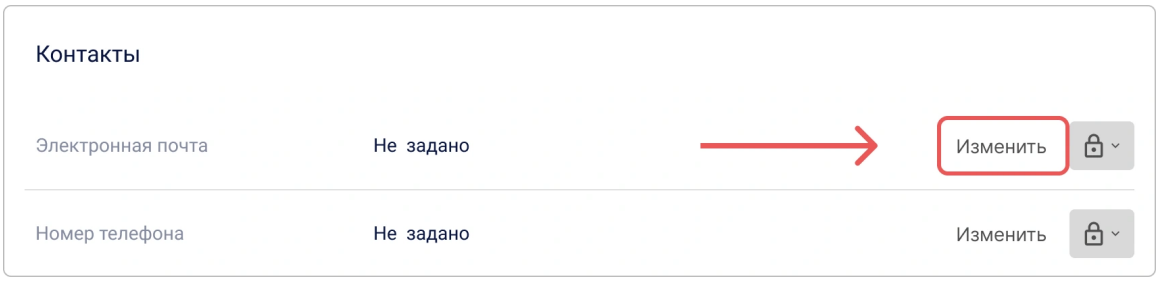
5. Нажмите **Сохранить** в форме редактирования.

Добавление электронной почты

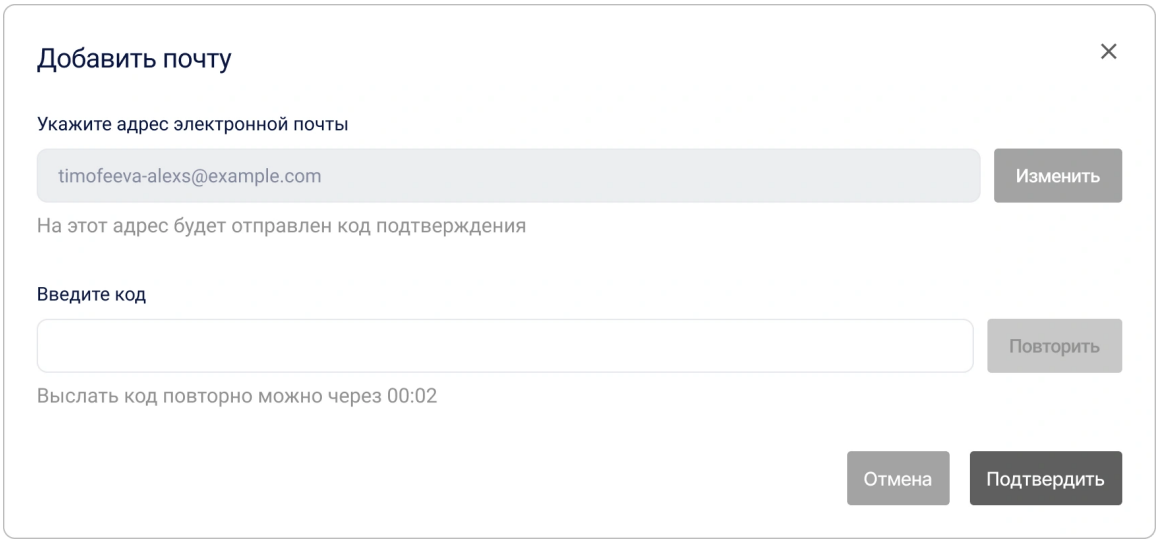
> 💡 Для электронной почты требуется подтверждение — ввод одноразового кода или переход по ссылке из письма.

1. Перейдите в свой **Профиль**.

2. Найдите блок **Контакты** и нажмите **Изменить** на панели **Электронная почта**.



3. Откроется форма добавления.



4. Введите почту и нажмите **Получить код**.

   На указанный адрес будет направлено письмо с кодом подтверждения.

5. Введите код и нажмите **Подтвердить**, либо перейдите по ссылке из письма.

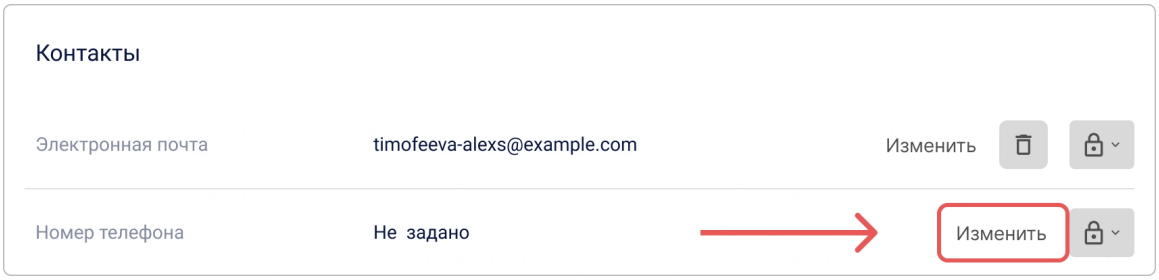
> **Совет**: Чтобы удалить почту, нажмите на кнопку **Удалить** на панели **Электронная почта**.

Добавление номера телефона

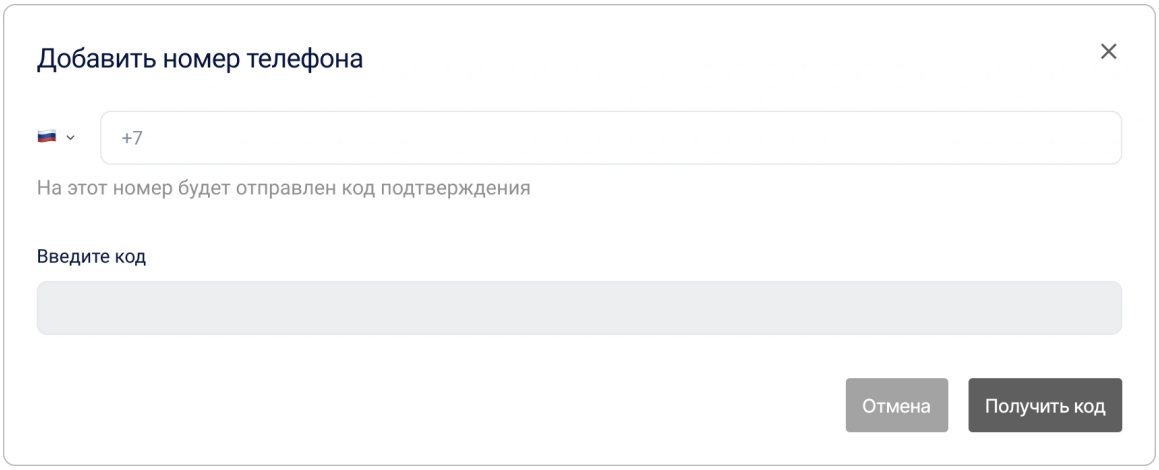
> Для номера телефона требуется подтверждение - ввод одноразового кода из SMS или входящего звонка.

1. Перейдите в свой **Профиль**.

2. Найдите блок **Контакты** и нажмите **Изменить** на панели **Номер телефона**.



3. Откроется форма редактирования.



4. Введите номер и нажмите **Получить код**.

   На указанный номер будет направлено SMS или звонок.

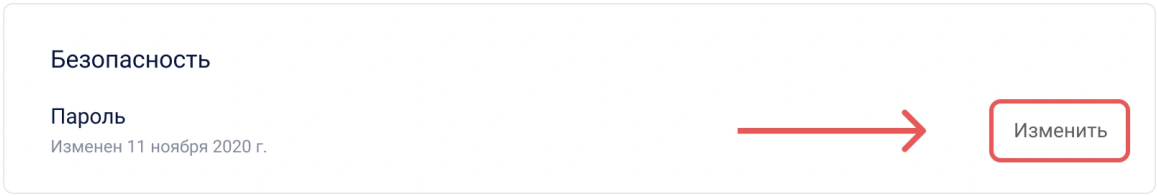
5. Введите код подтверждения и нажмите **Подтвердить**.

> **Совет**: Чтобы удалить телефон, нажмите на кнопку **Удалить** на панели **Номер телефона**.

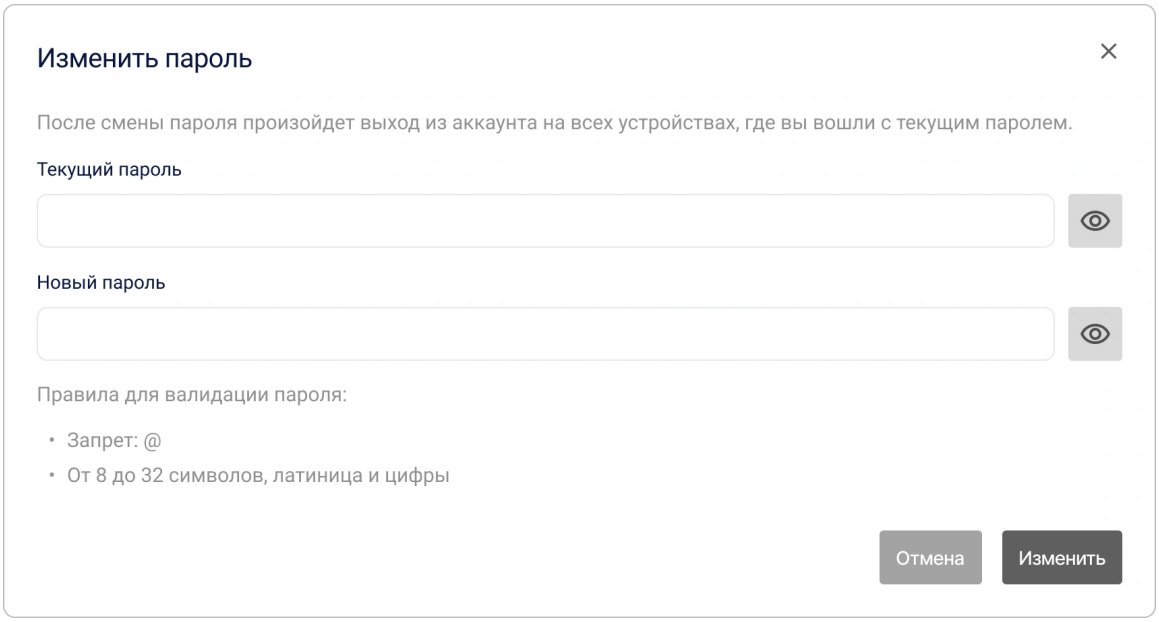
Смена пароля

1. Перейдите в свой **Профиль**.

2. Нажмите **Изменить** в блоке **Безопасность**.



3. В открывшемся окне укажите текущий пароль и новый пароль.



После смены пароля произойдет выход из системы. Для продолжения работы необходимо заново авторизоваться, используя новый пароль.

Настройка публичности

Вы можете самостоятельно контролировать, какая информация будет доступна другим пользователям или сторонним системам. Это осуществляется через настройку публичности поля.

Эта настройка позволяет определять публичность для каждого поля в блоках **Основная информация**, **Дополнительная информация** и **Идентификаторы**.

Уровни публичности

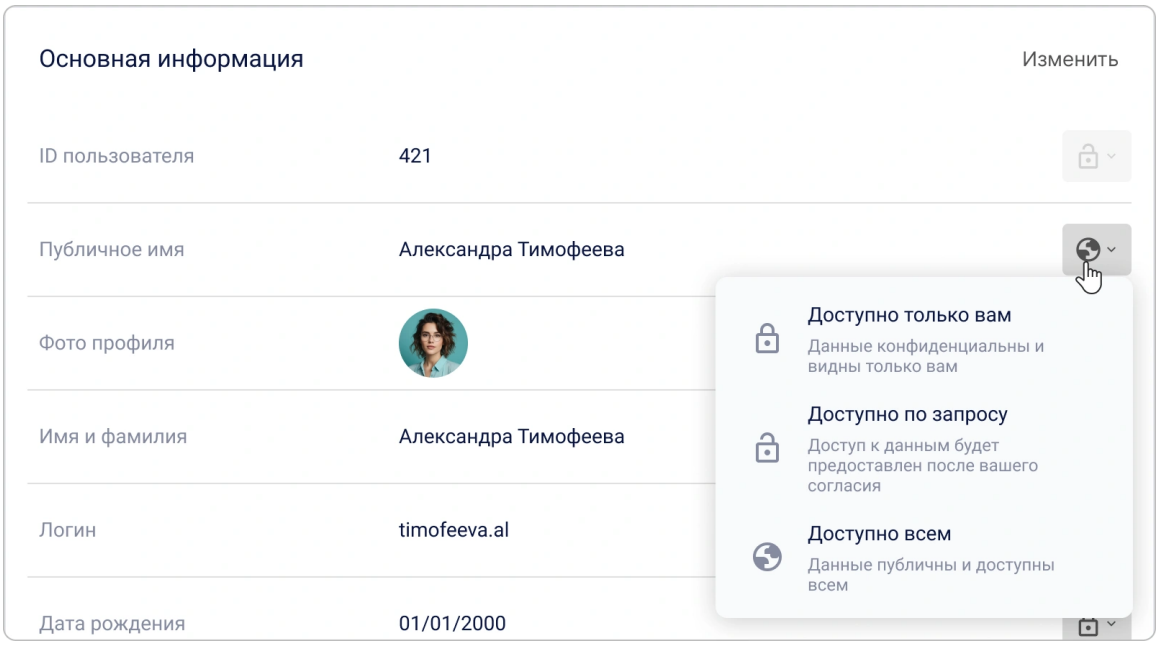
Уровень	Иконка	Описание
Доступно только вам		Данные не передаются в сторонние системы и доступны только вам.
Доступно по запросу		Данные доступны в сторонних системах, с которыми настроена интеграция КриптоАРМ ID. Для доступа к данным требуется ваше согласие.
Доступно всем		Данные публичны всегда. Для доступа к ним не требуется вашего согласия.

Как настроить публичность поля

1. Перейдите в свой **Профиль**.

2. Нажмите на кнопку для настройки публичности рядом с полем.

3. Выберите необходимый уровень.



В зависимости от выбранного значения значение поля в профиле становится публичным или приватным.

Настройка применяется без дополнительного подтверждения.

Управление идентификаторами внешних сервисов

Идентификаторы — внешние сервисы, которые вы добавили в свой профиль или через которые вы когда-либо входили в приложения или личный кабинет.

Список доступных для добавления идентификаторов в профиле формируется из публичных способов входа, созданных в кабинете **КриптоАРМ ID**.

> 🔍 Доступные для привязки идентификаторы настраиваются в кабинете администратора.

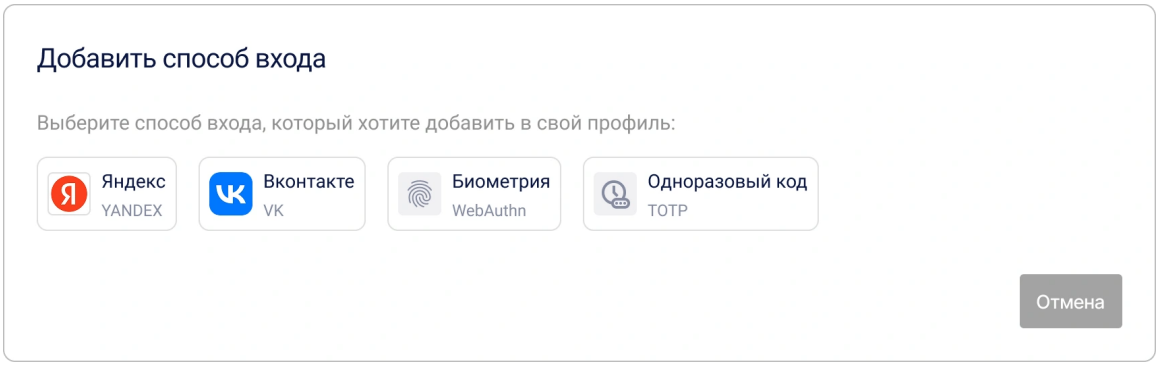
> 💡 Вы можете входить в приложения, используя идентификаторы, при условии, что они добавлены на виджет входа.

Добавление нового идентификатора

1. Перейдите в свой **Профиль**.

2. Нажмите **Добавить** в блоке **Идентификаторы**.

3. В открывшемся окне выберите внешний сервис.



4. Пройдите аутентификацию в сервисе.

   После успешного входа в аккаунт внешнего сервиса, идентификатор будет привязан в профиле.

> **Совет**: Если идентификатор внешнего сервиса уже привязан к другому пользователю, необходимо удалить его из профиля этого пользователя, а затем привязать на новом аккаунте.

Удаление идентификатора

1. Перейдите в свой **Профиль**.
2. Нажмите для идентификатора, который необходимо удалить.
3. Выберите действие **Удалить**.

Идентификатор будет **немедленно удален** из профиля.

Настройка публичного профиля

Публичный профиль — публичные данные, доступные для просмотра другим участникам системы **КриптоАРМ ID** и подключенным приложениям. Он позволяет контролировать, какая информация о пользователе видна другим без необходимости предоставления полного доступа к аккаунту.

Просмотр публичного профиля

1. Перейдите в свой **Профиль**.
2. Нажмите на кнопку **Публичные данные** в блоке **Приватность профиля**.
3. Откроется окно с публичным профилем, который содержит данные с уровнем **Доступно всем**.

Скачивание данных публичного профиля

> 📌 Данные публичного профиля экспортируются в файл формата **vCard**.

1. Перейдите в свой **Профиль**.
2. Нажмите на кнопку **Публичные данные** в блоке **Приватность профиля**.
3. Откроется окно **Публичный профиль** с данными, для которых установлен уровень **Доступно всем**.
4. Нажмите кнопку **Экспортировать vCard** .
5. Запустится загрузка файла.

Пример файла **vCard** с публичными данными профиля:

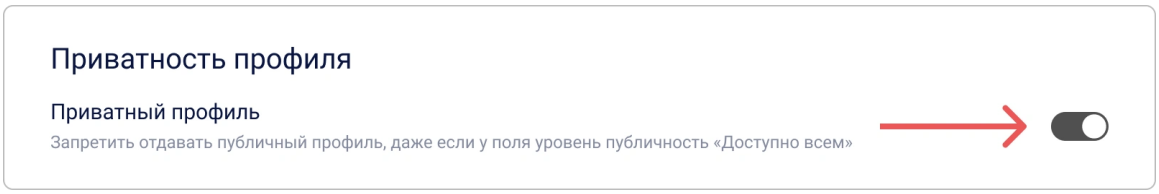
```
BEGIN:VCARD
VERSION:3.0
FN:Timofeeva Alex
N:Timofeeva;Alex;;;
PHOTO:https://service-
adress/public/images/profile/90211313d753e1d1b83ab19ecfd4af5e
EMAIL:timofeeva-alexs@mail.ru
UID:null
REV:2025-05-26T12:52:24.630Z
END:VCARD
```

Отключение публичного профиля

> 💡 **Совет**: Вы можете запретить передачу публичных данных профиля, которые имеют уровень публичности «Доступно всем».

1. Перейдите в свой **Профиль**.

2. Активируйте переключатель **Приватный профиль** в блоке **Приватность профиля**.



   Настройка применяется без дополнительного подтверждения.

После активации настройки данные с уровнем публичности «Доступно всем» стают доступны только по запросу.

Цифровая визитка личного профиля

> 🔬 **Экспериментальная функция**: Доступность регулируется администратором системы.

Визитка в КриптоАРМ ID — это современная цифровая замена бумажной визитке, доступная по уникальной ссылке.

Содержимое визитки:

- Фотография профиля,
- Имя и фамилия,
- Контактные данные (email, телефон),
- Дата рождения.

Особенности:

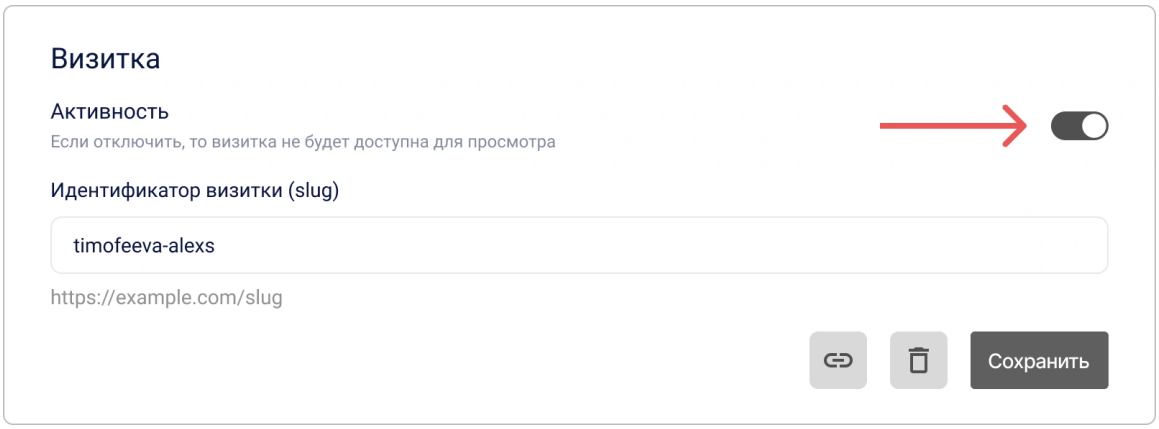
- Данные отображаются независимо от настроек их публичности.
- Визитка доступна по уникальной ссылке: `https://<ваш-сервис>/api/cards/<идентификатор>`.
- Поддерживается экспорт визитки в формате **vCard** для интеграции в различные приложения.

Активность визитки

Для визитки доступна настройка активности.

1. Перейдите в свой **Профиль**.

2. В блоке **Визитка** активируйте переключатель **Активность**.



Убедитесь, что теперь ваша визитка доступна. Для этого перейдите по ссылке: `https://<your-domain>/api/cards/<идентификатор>`:

Настройка персонализированного адреса ссылки

Чтобы ссылка на визитку была короче и легко запоминалась, можно задать собственный уникальный идентификатор.

1. Перейдите в свой **Профиль**.
2. В блоке **Визитка** укажите новый идентификатор.
3. Нажмите **Сохранить**.

> Идентификатор должен быть уникальным в системе и содержать только латинские буквы, цифры и дефисы.

Как поделиться визиткой

1. Перейдите в свой **Профиль**.
2. В блоке **Визитка**:
   - Нажмите **Открыть QR-код** и отсканируйте код камерой устройства.
   - Кнопку **Скопировать ссылку**, чтобы скопировать адрес ссылки на визитку.

Дополнительные действия с личным профилем

Завершение всех сеансов

Функция принудительного завершения всех активных сессий — важный инструмент безопасности. Используйте его в случае утери устройства, подозрения на взлом аккаунта или для немедленного обновления токенов доступа.

> 📌 Эта операция немедленно аннулирует все access- и refresh-токены, завершая ВСЕ его текущие сессии во всех приложениях.

Чтобы завершить все активные сеансы:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Выйти со всех устройств**.

После этого потребуется **войти заново** на всех устройствах.

Скачивание данных личного профиля

КриптоАРМ ID позволяет экспортировать все данные профиля в JSON формате.

Этот файл содержит всю информацию, относящуюся к вашему профилю в **КриптоАРМ ID**, а также сведения о внешних аккаунтах, которые вы добавили в качестве способов входа, независимо от того, установлен ли для них параметр публичности.

Чтобы скачать данные профиля:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Скачать данные**.
3. Загрузка JSON-файла начнется автоматически.

Политика обработки персональных данных

Ознакомьтесь с документом о том, как **КриптоАРМ ID** обрабатывает ваши данные.

Чтобы ознакомиться с политикой:

1. Перейдите в свой **Профиль**.
2. Раскройте блок **Другие действия** и выберите **Политика обработки ПДн**.
3. Запустится скачивание файла с политикой.

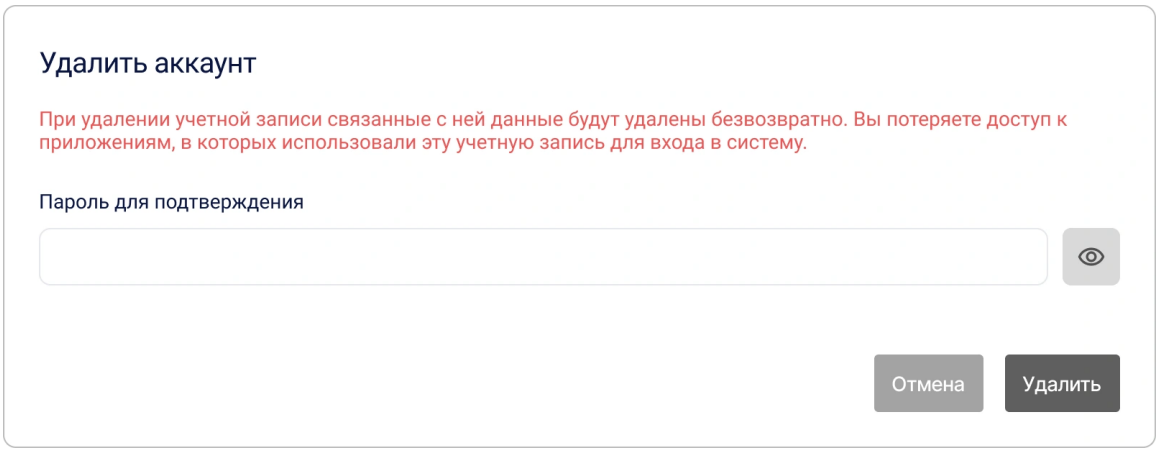
Удаление и восстановление аккаунта

Удаление аккаунта в **КриптоАРМ ID** — необратимая операция, после которой восстановить данные будет невозможно. Система использует механизм отсроченного удаления: ваш аккаунт помечается на удаление, но остается доступным для восстановления в течение определенного времени. Это сделано для защиты от случайного удаления и дает вам время передумать.

Чтобы удалить аккаунт:

1. Перейдите в свой **Профиль**.

2. Раскройте блок **Другие действия** и выберите действие **Удалить аккаунт**.
3. В открывшемся окне введите пароль от аккаунта для подтверждения действия и нажмите **Удалить**.



Что происходит:

- Аккаунт помечается на удаление
- Вы автоматически выходите из системы
- В течение определенного времени доступно восстановление аккаунта

В течение определенного времени после удаления аккаунта у вас есть возможность восстановить доступ к нему. Для этого вам нужно заново авторизоваться в личном кабинете **КриптоАРМ ID**, после этого нажать **Восстановить аккаунт**.

> Восстановление аккаунта доступно только при авторизации в личном кабинете **КриптоАРМ ID**. При входе в приложение через сервис **КриптоАРМ ID** восстановление аккаунта недоступно.

Разрешения приложений и OAuth-доступ

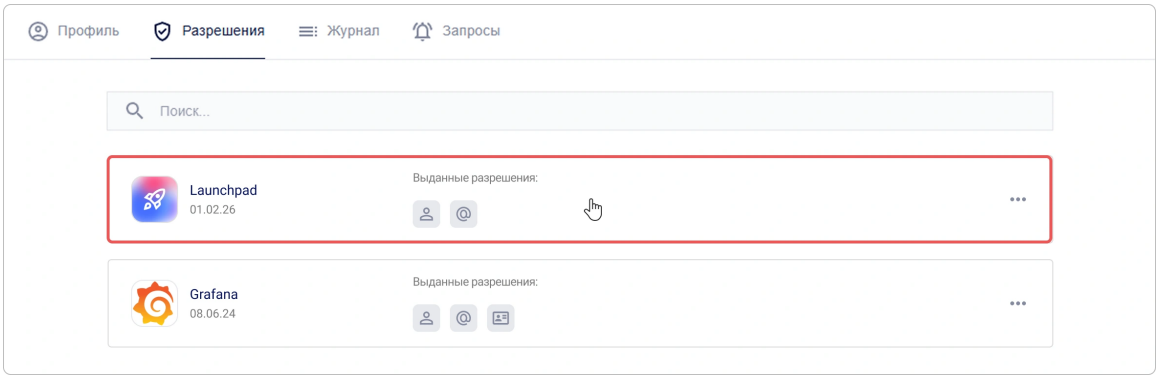
Разрешения — это права, которые вы предоставляете внешним приложениям для доступа к определенным данным вашего профиля **КриптоАРМ ID**. Вы можете в любой момент ограничить доступ, завершить активные сеансы или полностью отозвать разрешения.

Все приложения, имеющие доступ к вашим данным, отображаются в **Профиле** на вкладке **Разрешения**.

Переход в приложение из списка разрешений

Чтобы быстро открыть приложение, которому вы ранее предоставили доступ:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.

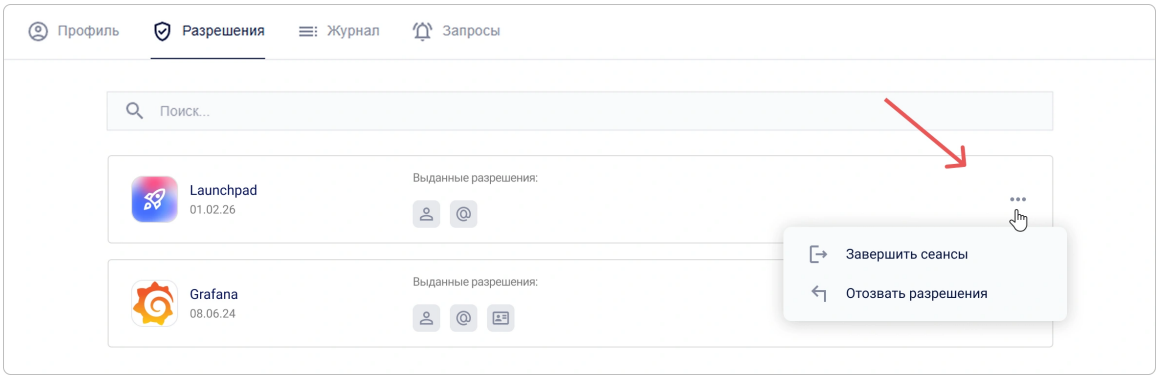


2. Нажмите на **название приложения** в списке.
3. Произойдет автоматический переход в выбранное приложение.

Завершение активных сеансов приложения

Если вы хотите немедленно завершить все сессии в конкретном приложении:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.
2. Вызовите меню действий для приложения, в котором необходимо завершить сеансы.
3. Выберите действие **Завершить сеансы**.



4. Подтвердите действие в модальном окне.

Что произойдет: Все активные сессии в этом приложении будут завершены. При следующем обращении к приложению потребуется **повторная авторизация**.

Завершение сеансов полезно, если вы подозреваете несанкционированный доступ или использовали приложение на общем устройстве.

Отзыв разрешений у приложения

Чтобы полностью запретить приложению доступ к вашим данным:

1. Перейдите в свой **Профиль** → вкладка **Разрешения**.

2. Вызовите меню действий для приложения, у которого необходимо отозвать разрешения.
3. Выберите действие **Отозвать разрешение**.
4. Подтвердите действие в модальном окне.

Последствия: Приложение **потеряет доступ** ко всем данным вашего профиля. При следующем входе система запросит **новое согласие** на доступ.

Приглашения в закрытые приложения

Приглашение — это способ получить доступ к закрытому приложению. Администратор приложения отправляет приглашение на вашу электронную почту, после чего вы сможете войти в приложение, недоступное для остальных пользователей.

Как получить приглашение?

Приглашение приходит двумя способами:

1. **По электронной почте**: Вы получите письмо с приглашением и ссылкой для быстрого перехода в приложение.
2. **В вашем профиле КриптоАРМ ID**: в разделе **Запросы** появляется новое приглашение.

Как принять приглашение?

Вы можете принять приглашение любым удобным способом.

Способ 1: Принять приглашение из письма

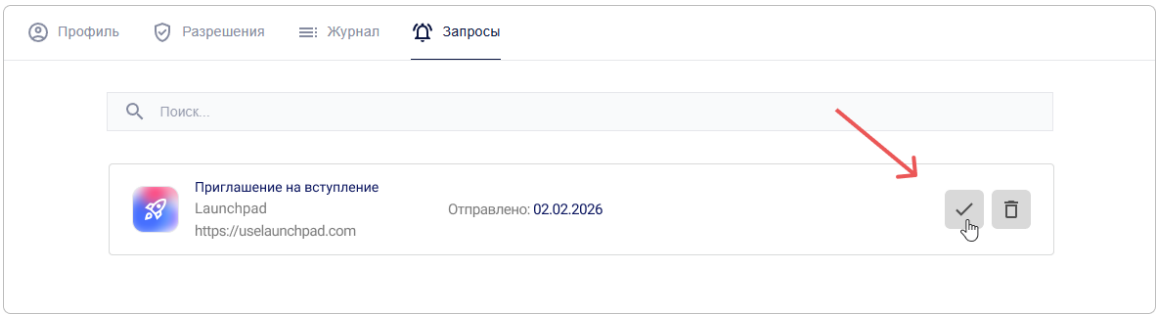
1. Откройте письмо с приглашением.
2. Нажмите на ссылку в письме.
3. Далее возможны два варианта:
    - если вы уже авторизованы в системе — вы сразу попадёте в приложение;
    - если вы не авторизованы — выполните вход в систему.

> 🔐 Вход необходимо выполнить **под тем аккаунтом**, к которому привязан email, указанный в приглашении.

Способ 2: Принять приглашение из профиля

1. Перейдите в свой **Профиль** → вкладка **Запросы**.
2. Найдите нужное приглашение в списке.

3. Нажмите кнопку **Принять**.



После этого доступ к приложению будет активирован, и вы сможете перейти в него.

Если у вас ещё нет аккаунта

Если вы получили приглашение, но ещё не зарегистрированы в системе **КриптоАРМ ID**:

1. Перейдите по ссылке из письма с приглашением.
2. Зарегистрируйтесь в системе **КриптоАРМ ID**.
3. При регистрации укажите тот же почтовый адрес, на который было отправлено приглашение.
4. После завершения регистрации вы автоматически получите доступ к приложению.

Каталог приложений

> **Экспериментальная функция**: Доступность регулируется администратором системы.

Что такое каталог?

Каталог — это централизованный маркетплейс всех приложений, доступных в экосистеме **КриптоАРМ ID**.

Каталог объединяет все публичные приложения в одном месте, что позволяет быстро находить нужные приложения, просматривать названия и описания, получать доступ к приложениям без необходимости запоминать сложные ссылки или пути.

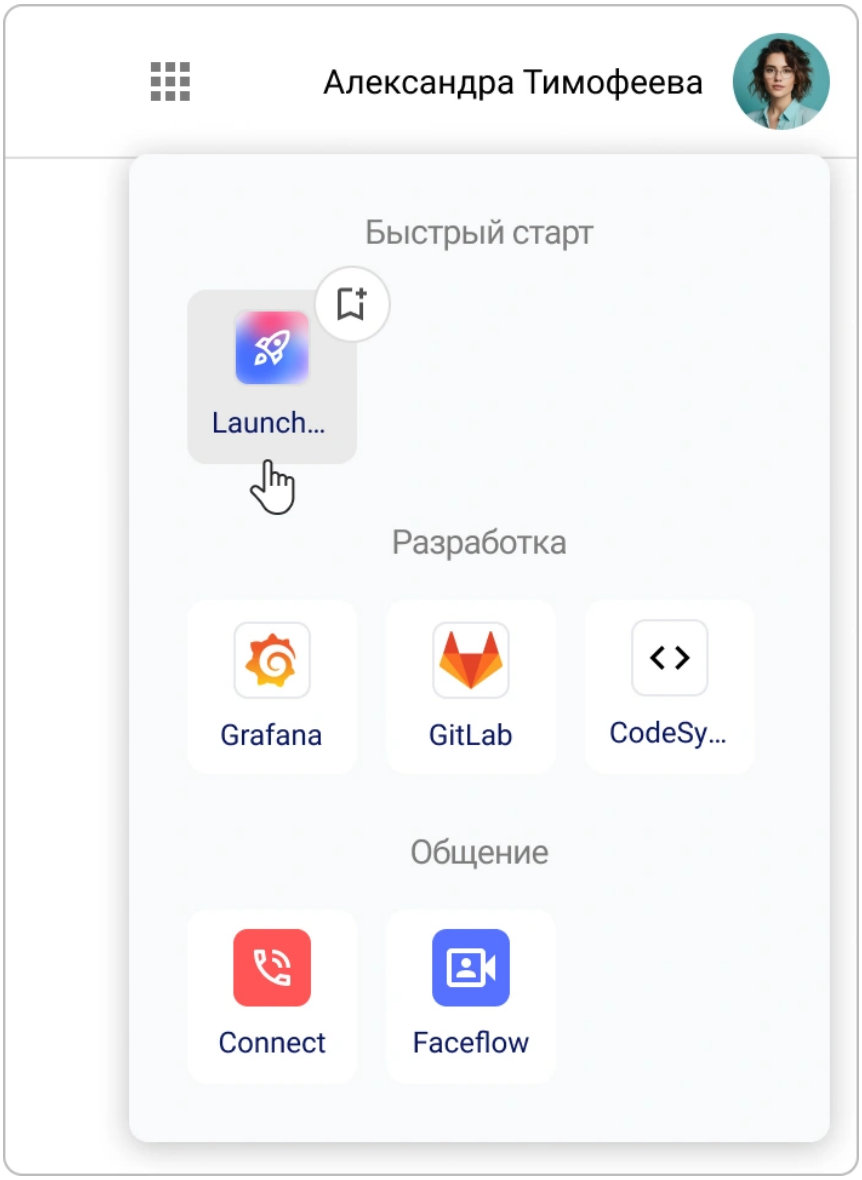
Для удобства все приложения в каталоге разделены по типам.

Приложения из каталога можно добавить в избранные. Для быстрого доступа все избранные приложения отображаются в левой боковой панели.

Как использовать приложения из каталога?

1. Нажмите на кнопку .

2. Откроется окно со списком приложений, добавленных в каталог.



3. Выберите нужное приложение в каталоге.

4. Произойдет автоматический редирект на страницу приложения.

5. Пройдите аутентификацию в приложении с помощью **КриптоАРМ ID** и предоставьте приложению доступ к своим данным.

Теперь вы сможете входить в приложение с вашим профилем **КриптоАРМ ID**.

Действия в каталоге

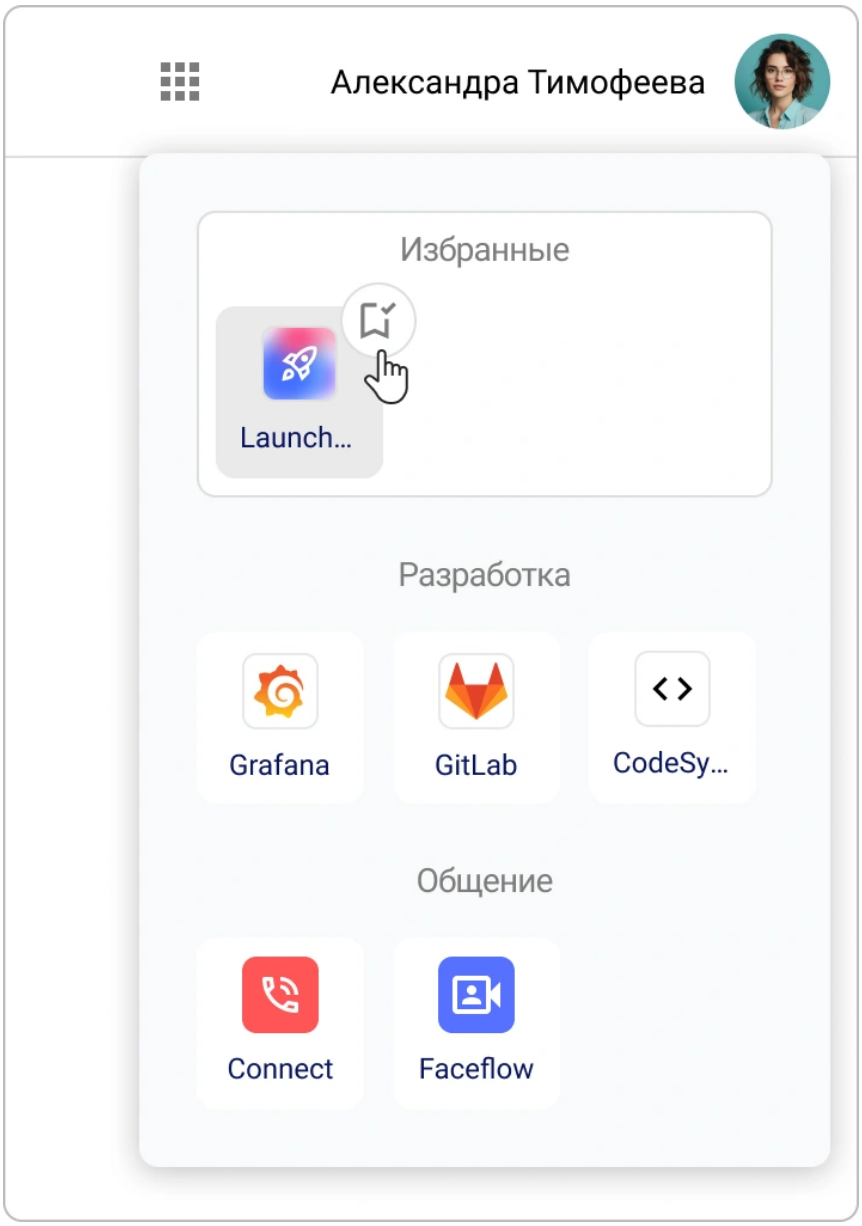
Добавление приложения в избранные

1. Нажмите на кнопку **Каталог приложений** .

2. Откроется окно со списком приложений, добавленных в каталог.

3. Нажмите на кнопку , размещенную рядом с приложением, которое необходимо добавить в избранные.

   Приложение будет добавлено в избранные и отобразится в соответствующей группе.



Удаление приложения из избранных

1. Нажмите на кнопку **Каталог приложений** .
2. Откроется окно со списком приложений, добавленных в каталог.
3. Нажмите на кнопку , размещенную рядом с приложением, которое необходимо удалить из избранных.

Приложение будет удалено из избранных и пропадет из бокового меню.

Журнал активности и история входов

Журнал активности — это инструмент безопасности, который позволяет отслеживать откуда и с каких устройств вы заходили в **КриптоАРМ ID** или приложения.

Детализация событий

Для каждого события доступен просмотр подробных сведений.

Параметр	Что содержит
Заголовок события	Категория действия
Дата и время	Точные временные метки
Приложение	Идентификатор (client_id) приложения
Пользователь	Идентификатор (id) пользователя
Устройство	Тип устройства и браузер
Местоположение	IP-адрес

Как просмотреть журнал активности?

1. Перейдите в свой **Профиль**.
2. Откройте вкладку **Журнал**.