

# Руководство пользователя: Вход, Регистрация, Восстановление доступа и Администрирование системы

## Оглавление:

1. Введение (для конечных пользователей)
2. Страница входа в систему (для конечных пользователей)
3. Двухфакторная аутентификация (2FA) (для конечных пользователей)
4. Регистрация новой учетной записи (для конечных пользователей)
5. Восстановление доступа (для конечных пользователей)
6. Возможные проблемы и их решения (для конечных пользователей)
7. Руководство администратора системы «Identity» (панель Keycloak)
8. Обратная связь и поддержка
9. Обновление руководства

## 1. Введение (для конечных пользователей)

Добро пожаловать! Это руководство пользователя создано, чтобы помочь вам освоить процессы входа в систему, регистрации новой учетной записи и восстановления доступа на нашем сайте. Мы стремимся сделать взаимодействие с нашим продуктом максимально простым и понятным. Следуйте инструкциям, чтобы эффективно использовать все возможности аутентификации.

## 2. Страница входа в систему (для конечных пользователей)

При первом посещении защищенной части сайта или после выхода из системы вы попадаете на страницу входа.

**Страница для входа в систему**

Для входа в систему предлагается 4 варианта авторизации:

- Вход по логину и паролю. Для тестовой учетной записи используйте логин - **userstest**, пароль - **userstest**
- Используя кнопку "Войти через Госуслуги" для авторизации с помощью вашей учетной записи на портале Госуслуг
- Вход с помощью одноразовой ссылки
- С помощью Paycontrol, сканировав QR-code

Так же предусмотрена возможность регистрации новой учетной записи и восстановление доступа к зарегистрированным аутентификационным данным.

Логин  
Ведите логин

Пароль  
Ведите пароль

Запомнить меня

Регистрация Восстановить доступ

**Войти**  Вход по одноразовой ссылке

На этой странице вам доступны следующие варианты авторизации:

## 2.1. Вход по логину и паролю

- В поле "Логин" введите ваше имя пользователя.
  - Для тестового доступа: используйте логин **userstest**.
- В поле "Пароль" введите ваш пароль.
  - Для тестового доступа: используйте пароль **userstest**.
- Нажмите кнопку "Войти".

Если введенные данные верны, вы будете перенаправлены на страницу выбора двухфакторной аутентификации (см. [раздел 3](#)).

## 2.2. Вход через "Госуслуги"

- Нажмите кнопку "Войти через Госуслуги" (значок с логотипом Госуслуг).
- Вы будете перенаправлены на портал Госуслуг для авторизации с помощью вашей учетной записи.
- После успешной авторизации на портале Госуслуг вы вернетесь на наш сайт и войдете в систему (может потребоваться дополнительная двухфакторная аутентификация, если настроена).

## 2.3. Вход по одноразовой ссылке

- Нажмите на ссылку "Вход по одноразовой ссылке".
- Следуйте инструкциям на экране (обычно это ввод email или номера телефона, на который будет отправлена ссылка).

3. Перейдите по ссылке из полученного сообщения для входа в систему.

## 2.4. Вход с помощью Paycontrol (сканирование QR-кода)

1. Выберите опцию входа с помощью Paycontrol (если доступна на странице).
2. Отсканируйте предложенный QR-код с помощью мобильного приложения Paycontrol.
3. Подтвердите вход в приложении.

## 2.5. Опция "Запомнить меня"

Если вы установите галочку "Запомнить меня" перед нажатием кнопки "Войти", ваш браузер запомнит сессию, и вам не придется вводить логин и пароль при последующих визитах с этого же устройства и браузера в течение определенного времени. Используйте эту опцию только на доверенных персональных устройствах.

На странице входа также доступны ссылки:

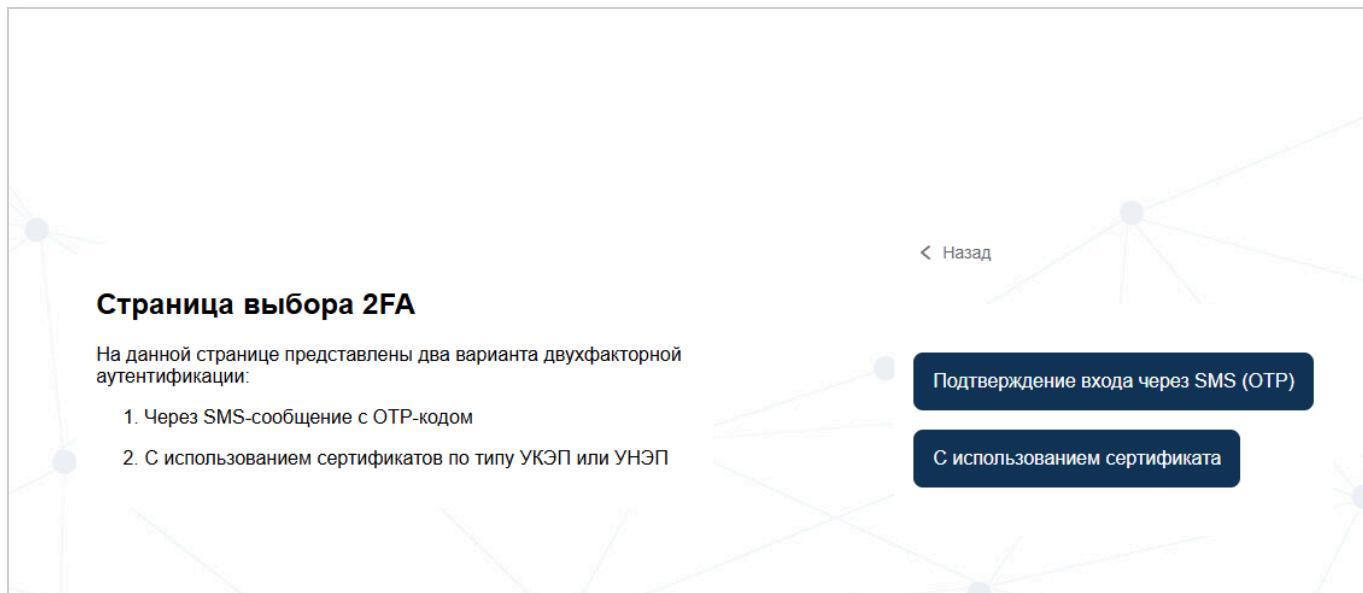
- "Регистрация": для создания новой учетной записи (см. [раздел 4](#)).
- "Восстановить доступ": для восстановления пароля или логина (см. [раздел 5](#)).

## 3. Двухфакторная аутентификация (2FA) (для конечных пользователей)

---

После успешного ввода логина и пароля (или другого основного способа аутентификации) система может потребовать дополнительное подтверждение для повышения безопасности вашей учетной записи.

### 3.1. Выбор способа 2FA

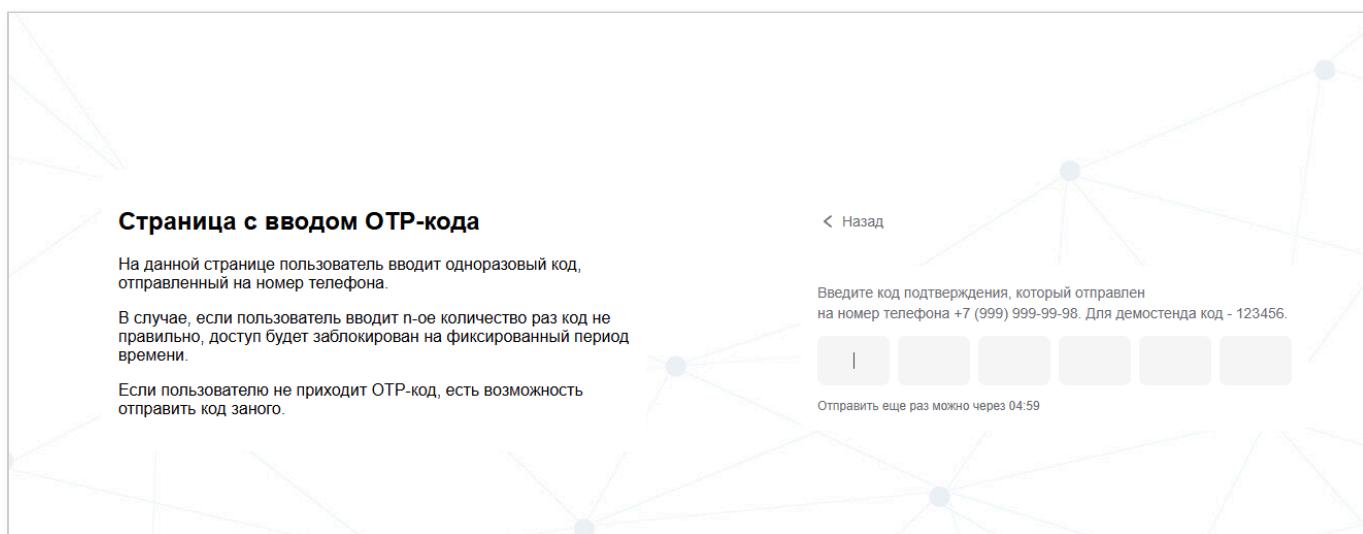


Вам будет предложено выбрать один из доступных вариантов второго фактора аутентификации:

- **Подтверждение входа через SMS (OTP):** Одноразовый пароль (One-Time Password) будет отправлен на ваш зарегистрированный номер телефона.
- **С использованием сертификата:** Подтверждение входа с помощью вашего электронного сертификата (например, УКЭП или УНЭП).

Выберите предпочтительный способ, нажав на соответствующую кнопку.

### 3.2. Подтверждение входа через SMS (OTP)



Если вы выбрали подтверждение через SMS:

1. На ваш зарегистрированный номер телефона будет отправлено SMS-сообщение с одноразовым кодом. На странице будет указан номер телефона, на который

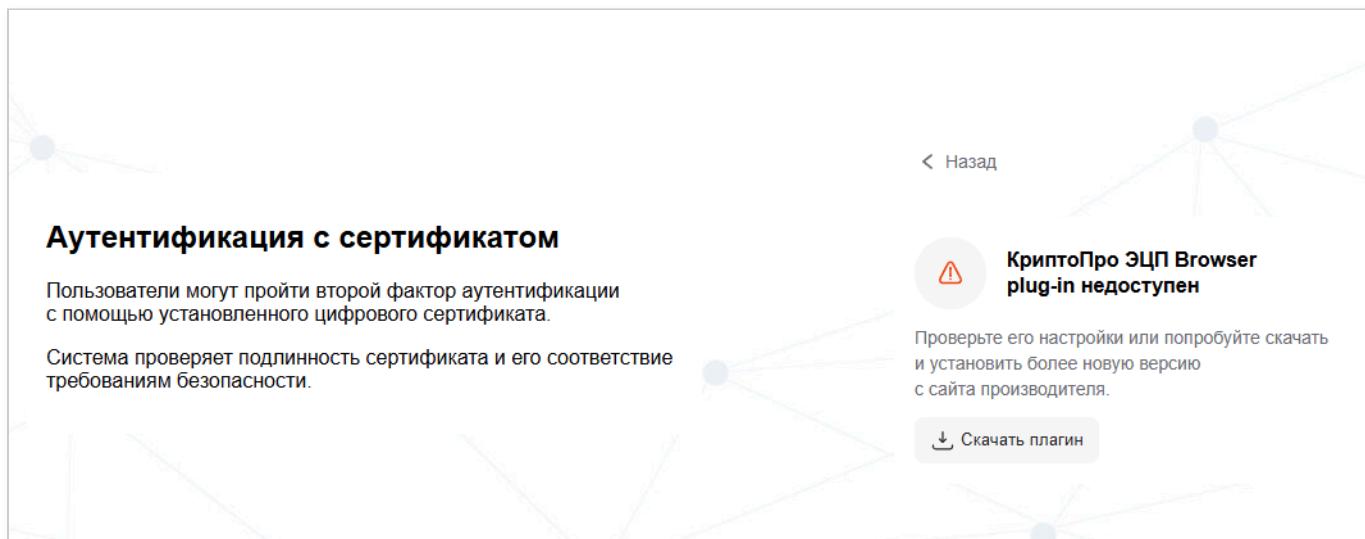
отправлен код (например, +7 (999) 999-99-98), и пример кода для демонстрационных целей (например, 123456).

2. Введите полученный код в поле "Ведите код подтверждения".
3. Нажмите кнопку для подтверждения (обычно она появляется после ввода кода или является неявной).

#### Важно:

- Если вы введете неверный код несколько раз подряд, доступ может быть временно заблокирован на фиксированный период времени для предотвращения подбора кода.
- Если вы не получили ОТР-код, подождите указанное время (например, "Отправить еще раз можно через 04:59") и нажмите на ссылку или кнопку "Отправить код заного" (или аналогичную).

### 3.3. Аутентификация с сертификатом



Если вы выбрали аутентификацию с использованием сертификата:

1. Система попытается обнаружить установленные цифровые сертификаты на вашем компьютере.
2. Вам может быть предложено выбрать нужный сертификат из списка (если их несколько).
3. Система проверит подлинность сертификата и его соответствие требованиям безопасности.

### 3.3.1. Требования к плагину КриптоПро

Для корректной работы аутентификации с сертификатом может потребоваться установка и настройка специального программного обеспечения, такого как "КриптоПро ЭЦП Browser plug-in".

- Если плагин не обнаружен или его версия устарела, вы увидите соответствующее сообщение (например, "КриптоПро ЭЦП Browser plug-in недоступен").
- В этом случае:
  - Проверьте настройки плагина в вашем браузере.
  - Попробуйте скачать и установить более новую версию плагина, нажав на кнопку "Скачать плагин" или перейдя на сайт производителя плагина.
  - Следуйте инструкциям по установке плагина. После установки может потребоваться перезапуск браузера.

## 4. Регистрация новой учетной записи (для конечных пользователей)

Если у вас еще нет учетной записи, вы можете ее создать. На странице входа (см. [Скриншот 1](#)) нажмите ссылку "Регистрация".

« Назад ко входу

Номер телефона \*

+7

Имя \*

Фамилия \*

E-mail \*

Имя пользователя \*

Пароль \* ⓘ

Подтверждение пароля \*

Регистрация

**Страница регистрации**

На странице регистрации пользователь заполняет необходимую информацию, а затем проходит простую процедуру подтверждения номера телефона с помощью OTP-кода, что делает аккаунт более защищенным.

1. На странице регистрации заполните следующие поля:

- **Номер телефона\***: Введите ваш актуальный номер телефона (например, начиная с +7). На этот номер будет отправлен ОТР-код для подтверждения.
- **Имя\***: Ваше имя.
- **Фамилия\***: Ваша фамилия.
- **E-mail\***: Ваш адрес электронной почты.
- **Имя пользователя\***: Уникальное имя, которое будет использоваться для входа в систему.
- **Пароль\***: Придумайте надежный пароль. Обратите внимание на требования к паролю, если они указаны (например, минимальная длина, наличие цифр, букв разного регистра, специальных символов).
- **Подтверждение пароля\***: Повторите введенный пароль.

\*Поля, отмеченные звездочкой (\*), обязательны для заполнения.

2. После заполнения всех полей нажмите кнопку "Регистрация".

3. Далее последует процедура подтверждения номера телефона с помощью ОТР-кода (аналогично описанному в [разделе 3.2](#)). Это делает ваш аккаунт более защищенным.

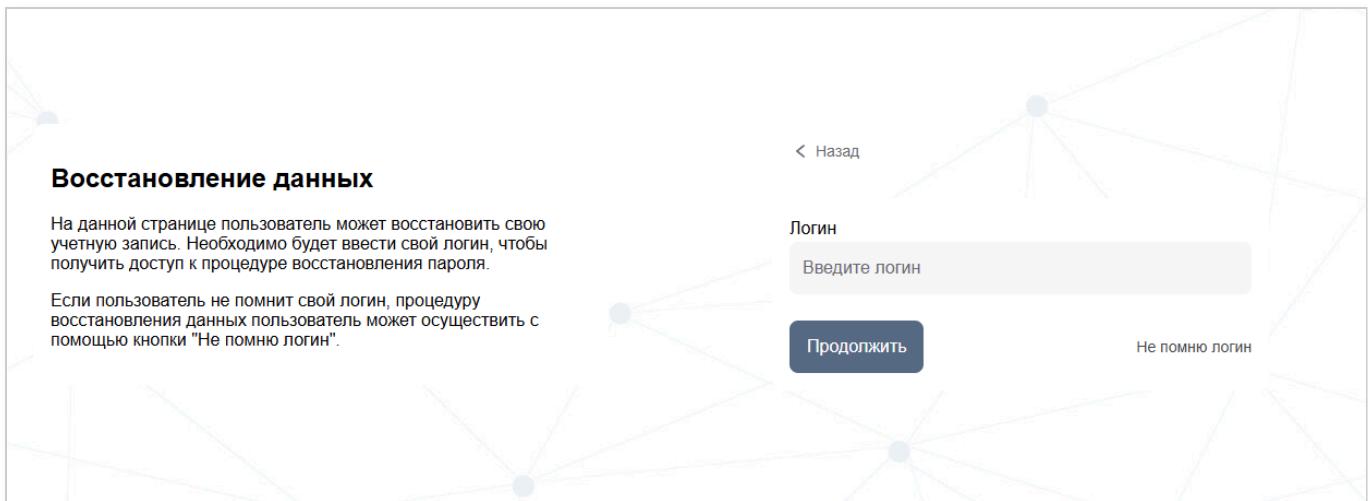
## 5. Восстановление доступа (для конечных пользователей)

---

Если вы забыли свой пароль или логин, вы можете воспользоваться функцией восстановления доступа.

### 5.1. Восстановление пароля (если помните логин)

На странице входа (см. [Скриншот 1](#)) нажмите ссылку "Восстановить доступ".



1. Введите ваш логин в поле "Логин".
2. Нажмите кнопку "Продолжить".
3. Следуйте дальнейшим инструкциям на экране. Обычно это включает отправку ссылки для сброса пароля на ваш зарегистрированный email или подтверждение через SMS.

## 5.2. Восстановление доступа (если забыли логин или другие случаи)

Если вы не помните свой логин, на странице "Восстановление данных" (см. [Скриншот 6](#)) нажмите ссылку "Не помню логин". Также вы можете попасть на эту страницу напрямую через "Восстановить доступ" со страницы входа, если система не может определить вас однозначно.

[Назад](#)

## Восстановление доступа

Email

Введите email

Телефон

+7

Продолжить

1. Введите ваш Email в соответствующее поле.
2. Введите ваш Телефон в соответствующее поле.
3. Нажмите кнопку "Продолжить".
4. Система попытается найти вашу учетную запись по предоставленным данным.  
Следуйте дальнейшим инструкциям на экране для восстановления доступа.

## 6. Возможные проблемы и их решения (для конечных пользователей)

### 6.1. Сообщение "Page has expired"

## Page has expired

To restart the login process [Нажмите сюда](#).  
To continue the login process [Нажмите сюда](#).

Это сообщение обычно означает, что сессия вашей страницы истекла по времени, либо страница была загружена из кэша браузера с устаревшими данными (например, после использования кнопки "Назад" в браузере на определенных этапах).

- To restart the login process [Нажмите сюда](#) (Чтобы перезапустить процесс входа, нажмите сюда): Эта ссылка вернет вас на начальную страницу входа.
- To continue the login process [Нажмите сюда](#) (Чтобы продолжить процесс входа, нажмите сюда): Эта ссылка может попытаться обновить текущую страницу или перенаправить на предыдущий актуальный шаг. Рекомендуется использовать первую опцию для надежного перезапуска.

## 7. Руководство администратора системы «Identity» (панель Keycloak)

Данный раздел предназначен для администраторов системы «Identity», ответственных за управление пользователями, клиентами, ролями и другими аспектами системы через административную панель Keycloak.

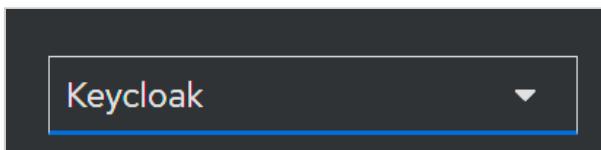
## 7.1. Доступ к административной панели

1. Для доступа к административной панели Keycloak перейдите по соответствующей ссылке, предоставленной вам (обычно это URL вида [https://\[адрес\\_вашего\\_keycloak\\_сервера\]/admin/](https://[адрес_вашего_keycloak_сервера]/admin/)).
2. На странице входа введите ваши учетные данные администратора (логин и пароль).
3. После успешного входа вы попадете в мастер-область (`master realm`) или в последнюю используемую область.

## 7.2. Выбор области (Realm) "identity"

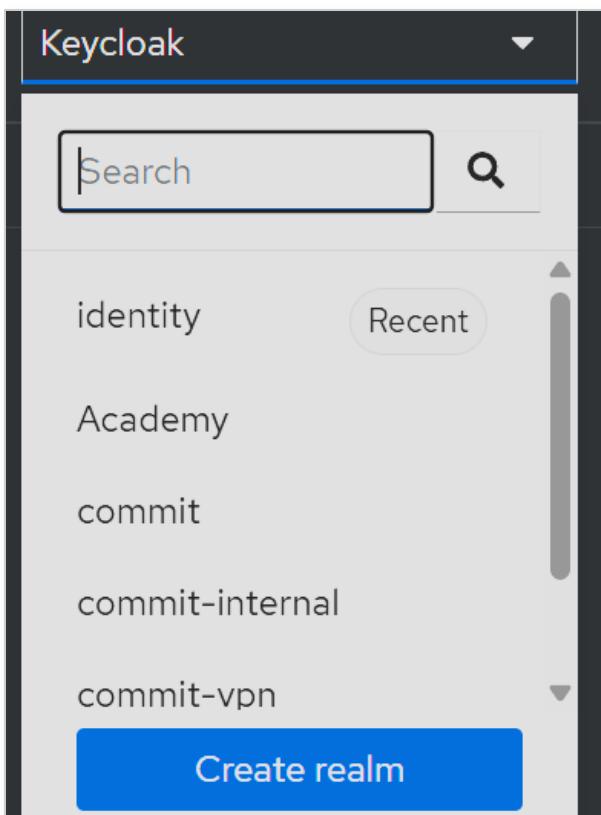
Для управления настройками, специфичными для вашего продукта «Identity», необходимо выбрать соответствующую область (realm).

1. В левом верхнем углу административной панели найдите выпадающий список с названием текущей области (по умолчанию может быть "Keycloak" или "master").



2. Нажмите на этот список. Откроется меню со списком доступных областей и полем поиска.
3. Найдите в списке или введите в поле "Search" название области "**identity**".

4. Выберите область "identity" из списка.



После выбора области "identity" все последующие настройки и операции будут применяться именно к ней.

A screenshot of the Keycloak 'identity' realm dashboard. The top navigation bar shows the Keycloak logo and the word 'KEYCLOAK'. On the far right, there is a user icon and the text 'admin'. The left sidebar has a dropdown menu set to 'identity'. Below it, there are several navigation items: 'Управление' (Manage), 'Клиенты' (Clients), 'Client scopes', 'Роли Realm', 'Пользователи' (Users), 'Пользователь является членом группы. Выберите в списке группу и нажмите кнопку Покинуть, чтобы покинуть группу.', 'Сессии' (Sessions), and 'События' (Events). The main content area features the Keycloak logo and the text 'Welcome to identity'. Below this, a message says: 'If you want to leave this page and manage this realm, please click the corresponding menu items in the left navigation bar.'.

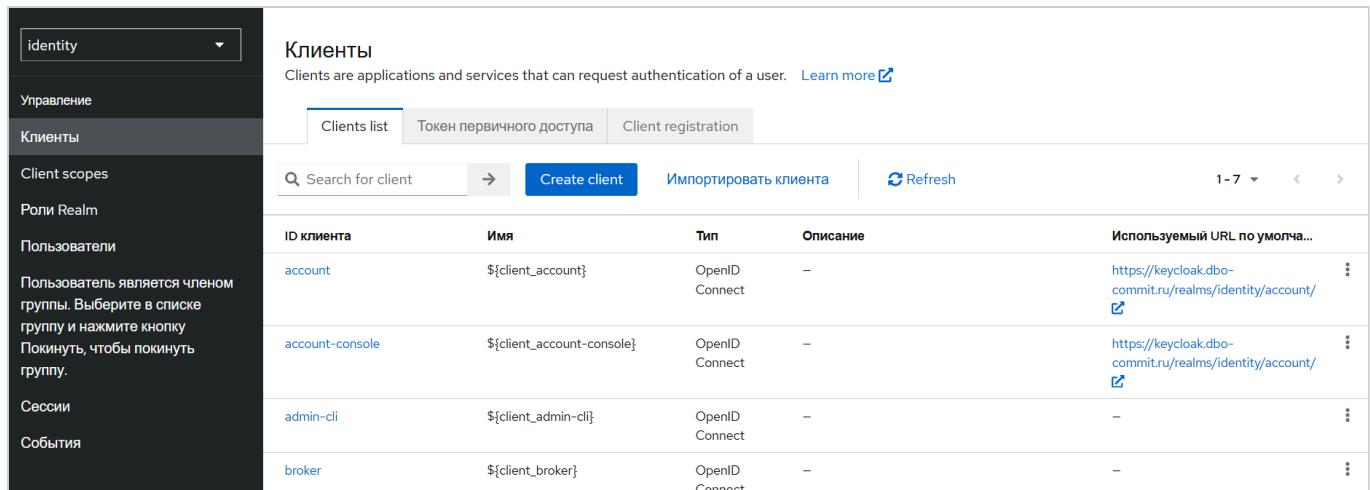
## 7.3. Обзор разделов управления в области "identity"

В левой части экрана находится навигационное меню, разделенное на две основные категории: **Manage (Управление)** и **Configure (Конфигурация)**.

### 7.3.1. Manage (Управление)

Эта категория содержит разделы для управления основными сущностями области.

### 7.3.1.1. Clients (Клиенты)



The screenshot shows the 'Clients' management screen in Keycloak. On the left, there's a sidebar with navigation links: 'Управление' (Management), 'Клиенты' (Clients) which is selected, 'Client scopes', 'Роли Realm', 'Пользователи' (Users), 'Сессии' (Sessions), and 'События' (Events). The main area has a title 'Клиенты' and a subtitle 'Clients are applications and services that can request authentication of a user.' with a 'Learn more' link. Below this are tabs: 'Clients list' (selected), 'Токен первичного доступа' (Initial access token), and 'Client registration'. There's a search bar 'Search for client', a 'Create client' button, and a 'Import client' button. A 'Refresh' button and a page navigation bar '1 - 7' are also present. The main table lists four clients:

ID клиента	Имя	Тип	Описание	Используемый URL по умолч...
account	`\${client_account}`	OpenID Connect	—	<a href="https://keycloak.dbo-commit.ru/realm/identity/account/">https://keycloak.dbo-commit.ru/realm/identity/account/</a>
account-console	`\${client_account-console}`	OpenID Connect	—	<a href="https://keycloak.dbo-commit.ru/realm/identity/account/">https://keycloak.dbo-commit.ru/realm/identity/account/</a>
admin-cli	`\${client_admin-cli}`	OpenID Connect	—	—
broker	`\${client_broker}`	OpenID Connect	—	—

**Назначение:** Клиенты – это приложения и сервисы, которые используют Keycloak (и, следовательно, вашу систему «Identity») для аутентификации и авторизации пользователей.

#### Возможности администратора:

- Просмотр списка существующих клиентов (например, account, account-console, admin-cli, user\_education\_platform и др.).
- Создание новых клиентов (Create client).
- Импорт конфигураций клиентов (Import client).
- Редактирование настроек существующих клиентов (Client ID, Name, протоколы, URL-адреса перенаправления, роли клиента, мапперы и т.д.).
- Управление начальными токенами доступа (Initial access token) и регистрацией клиентов (Client registration).

### 7.3.1.2. Client scopes (Области клиентов)

Name	Assigned type	Protocol	Display order	Description
acr	Default	OpenID Connect	–	OpenID Connect scope for add acr (authentication context class reference) to the token
address	Optional	OpenID Connect	–	OpenID Connect built-in scope: address
email	Default	OpenID Connect	–	OpenID Connect built-in scope: email
micropoprofile-jwt	Optional	OpenID Connect	–	Micropoprofile - JWT built-in scope
offline_access	Optional	OpenID Connect	–	OpenID Connect built-in scope: offline_access
phone	Optional	OpenID Connect	–	OpenID Connect built-in scope: phone

**Назначение:** Области клиентов – это именованные наборы мапперов протоколов и ролей, которые могут быть совместно использованы несколькими клиентами. Они определяют, какая информация о пользователе (claims) будет включена в токены.

### Возможности администратора:

- Просмотр списка существующих областей клиентов (например, acr, address, email, profile, phone, offline\_access).
- Создание новых областей клиентов (Create client scope).
- Редактирование существующих областей: добавление/удаление мапперов, изменение типа (Default/Optional).

#### 7.3.1.3. Realm roles (Роли области)

Наименование роли	Составная	Описание
default-roles-identity	True	\${role_default-roles}
offline_access	False	\${role_offline-access}
test	False	–
test1	True	–
uma_authorization	False	\${role_uma_authorization}

**Назначение:** Роли области – это глобальные роли, определенные на уровне всей области "identity". Они могут быть назначены любому пользователю или группе в этой области.

## Возможности администратора:

- Просмотр списка существующих ролей области (например, default-roles-identity, offline\_access, uma\_authorization).
- Создание новых ролей (Create role).
- Редактирование существующих ролей: изменение имени, описания, создание композитных ролей (объединяющих другие роли).

### 7.3.1.4. Users (Пользователи)

Пользователи			
Users are the users in the current realm. <a href="#">Learn more</a>			
<a href="#">User list</a>			
Default search	Search user	<a href="#">Добавить пользователя</a>	Delete user
<input type="checkbox"/> Имя пользователя	E-mail	Фамилия	Имя
<a href="#">123456aaa</a>	privetie22@yandex.ru	Haha	Igor
<a href="#">1sdfsd sdf</a>	vasiliev.aleksey111y@icloud.com	kjksdfjk	jsdfkj
<a href="#">aiznaz</a>	aiznaz@commit.tech	naz	aiz
<a href="#">daria</a>	dtolstonogova@yandex.ru	Test	Daria
<a href="#">new_test</a>	newtest@gmail.ru	New	Test
<a href="#">someuser</a>	someuser@gmail.com	user	some
<a href="#">test</a>	test@gmail.com	testtest	test
<a href="#">testuser</a>	testuser@commit.tech	testuser	testuser

**Назначение:** Управление учетными записями пользователей в области "identity".

## Возможности администратора:

- Просмотр списка всех пользователей области.
- Поиск пользователей по различным атрибутам (Username, Email, Имя, Фамилия).
- Добавление новых пользователей (Add user).
- Удаление пользователей (Delete user).
- Редактирование данных пользователя:
  - Изменение личных данных (имя, фамилия, email).
  - Управление учетными данными (сброс пароля, настройка требуемых действий).
  - Назначение/снятие ролей (области и клиента).
  - Управление атрибутами пользователя.

- Просмотр и управление сессиями пользователя.
- Включение/отключение учетной записи.

#### 7.3.1.5. Groups (Группы)

Search group  →

Exact search

1-1 < >

test ⋮

1-1 < >

Пользователь является членом группы. Выберите в списке группу и нажмите кнопку Покинуть, чтобы покинуть группу.  
A group is a set of attributes and role mappings that can be applied to a user. You can create, edit, and delete groups and manage their child-parent organization. [Learn more](#)

Filter groups → Создать группу Refresh

Group name

test ⋮

1-1 < >

**Назначение:** Группы позволяют объединять пользователей для удобного управления ролями и атрибутами на коллективной основе.

#### Возможности администратора:

- Создание новых групп (Create group).
- Просмотр иерархии групп (если созданы).
- Редактирование групп: изменение имени, назначение ролей группе, управление атрибутами группы.
- Добавление/удаление пользователей из групп.

#### 7.3.1.6. Sessions (Сессии)

Сессии

Sessions are sessions of users in this realm and the clients that they access within the session. [Learn more](#)

Действие ⋮

No sessions

There are currently no active sessions in this realm.

**Назначение:** Просмотр и управление активными сессиями пользователей в области "identity".

#### **Возможности администратора:**

- Просмотр списка активных сессий (на скриншоте "No sessions", но при наличии будут отображены).
- Просмотр деталей сессии: пользователь, IP-адрес, клиент, время начала.
- Принудительное завершение сессий отдельных пользователей или всех сессий для клиента (через меню "Action").

#### 7.3.1.7. Events (События)

События

Events are records of user and admin events in this realm. To configure the tracking of these events, go to [Event configs](#). [Learn more](#)

User events События администратора

**+**

Nothing to add

There are no more events types left to add

**Назначение:** Просмотр журнала событий, связанных с действиями пользователей и администраторов в области "identity". Это стандартный механизм логирования Keycloak.

#### **Возможности администратора:**

- Переключение между вкладками "User events" (события пользователей: логины, ошибки, обновления профиля и т.д.) и "Admin events" (события администраторов: создание/изменение пользователей, клиентов и т.д.).
- Фильтрация событий по различным критериям.
- Настройка хранения событий (переход по ссылке [Event configs](#)): тип сохраняемых событий, срок хранения.
- *Примечание:* Данный раздел отображает события, хранящиеся непосредственно в Keycloak. Ваша кастомная реализация `LoginEventListenerProvider` дополнительно обрабатывает эти (и другие) события и отправляет их в Apache Kafka в обогащенном виде для более глубокого анализа и интеграции с SIEM-системами.

### 7.3.2. Configure (Конфигурация)

Эта категория содержит разделы для настройки поведения самой области "identity".

#### 7.3.2.1. Realm settings (Настройки области)

**Назначение:** Общие настройки для области "identity".

**Возможности администратора:**

- Вкладка "General": включение/отключение области, настройка отображаемого имени, HTML display name.
- Вкладка "Login": настройка пользовательской регистрации, забыли пароль, запомнить меня, требуемые действия при первом входе. Выбор тем оформления (Themes) для страниц логина, аккаунта, email.
- Вкладка "Email": настройка SMTP-сервера для отправки email-уведомлений.
- Вкладка "Tokens": настройка времени жизни токенов (access token, refresh token, etc.), подписей токенов.
- Вкладка "Security Defenses": настройка защиты от брутфорса, политики заголовков (CSP).
- И другие вкладки с различными настройками области.

#### 7.3.2.2. Authentication (Аутентификация)

**Назначение:** Управление потоками аутентификации, политиками паролей, настройками OTP и другими аспектами процесса входа.

**Возможности администратора:**

- Вкладка "Flows": создание и настройка кастомных потоков аутентификации (например, добавление шага 2FA, интеграция с Госуслугами). Управление привязками потоков (Bindings) к различным ситуациям (браузерный вход, прямой доступ, сброс пароля).
- Вкладка "Required Actions": определение действий, которые пользователь должен выполнить (например, обновить пароль, настроить OTP).
- Вкладка "Password Policy": настройка требований к сложности паролей.
- Вкладка "OTP Policy": настройка параметров для OTP (тип, количество цифр, период, look-ahead window).
- Вкладка "WebAuthn Policy": настройка параметров для аутентификации без пароля по стандарту WebAuthn.

### 7.3.2.3. Identity providers (Поставщики удостоверений)

**Назначение:** Настройка интеграции с внешними поставщиками удостоверений для федеративного входа (например, вход через Google, Facebook, SAML 2.0 IdP, OpenID Connect IdP, включая Госуслуги, если они настроены как внешний IdP).

**Возможности администратора:**

- Добавление новых поставщиков удостоверений из списка предустановленных или настройка кастомного.
- Конфигурация параметров каждого поставщика (Client ID, Client Secret, URL-адреса, сертификаты).
- Настройка мапперов для синхронизации атрибутов пользователей от внешнего IdP.

### 7.3.2.4. User federation (Федерация пользователей)

**Назначение:** Подключение к существующим внешним хранилищам пользователей, таким как LDAP или Active Directory.

**Возможности администратора:**

- Добавление нового провайдера федерации пользователей (например, LDAP, Kerberos).
- Настройка параметров подключения к внешнему хранилищу (URL, bind DN, credentials).
- Настройка мапперов для синхронизации атрибутов, ролей и групп пользователей из внешнего хранилища в Keycloak.

Данное руководство охватывает основные возможности администратора в панели управления Keycloak для области "identity". Для более детальной информации по каждой функции обращайтесь к официальной документации Keycloak.

## 8. Обратная связь и поддержка

---

Если у вас возникли вопросы по использованию функций входа, регистрации или восстановления доступа, или если вы столкнулись с проблемами, не описанными в данном руководстве, пожалуйста, свяжитесь с нашей службой поддержки:

- [info@commit.tech](mailto:info@commit.tech)
- 8 (495) 227-02-30

Мы ценим вашу обратную связь, которая помогает нам улучшать наш продукт и документацию.

## 9. Обновление руководства

---

Данное руководство пользователя актуально на момент его публикации. Поскольку наш сайт и его функции постоянно развиваются и улучшаются, содержание этого руководства может периодически обновляться. Рекомендуем обращаться к последней версии руководства, доступной на нашем сайте.