

АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ПО ТЕХНОЛОГИИ ЕДИНОВОГО ВХОДА

Руководство пользователя

Версия 10.3.0

Настоящая документация может быть использована только для поддержки работоспособности продуктов, установленных на основании договора с АО «Нэксайн». Документация может быть передана на основании договора, по которому производится (производилась или будет производиться) установка продуктов, или явно выраженного согласия АО «Нэксайн» на использование данной документации. Если данный экземпляр документации попал к вам каким-либо иным образом, пожалуйста, сообщите об этом в АО «Нэксайн» по адресу, приведенному ниже.

Все примеры, приведенные в документации (в том числе примеры отчетов и экранных форм), составлены на основании тестовой базы АО «Нэксайн». Любое совпадение имен, фамилий, названий компаний, банковских реквизитов и другой информации с реальными данными является случайным.

Все встречающиеся в тексте торговые знаки и зарегистрированные торговые знаки являются собственностью их владельцев и использованы исключительно для идентификации программного обеспечения или компаний.

Данная документация может не отражать некоторых модификаций программного обеспечения. Если вы заметили в документации ошибки или опечатки или предполагаете их наличие, пожалуйста, сообщите об этом в АО «Нэксайн».

Все имущественные авторские права сохраняются за АО «Нэксайн» в соответствии с действующим законодательством.

© АО «Нэксайн», 1992–2023

АО «Нэксайн»

Россия, 199155, Санкт-Петербург, ул. Уральская, д.4 лит.Б, помещение 22Н

Тел.: + 7 (812) 326-12-99; факс: + 7 (812) 326-12-98.

office@nexign.com; www.nexign.com

Содержание

1. Общие сведения	5
2. Операции	6
2.1. Начало работы	6
2.2. Работа с пользователями	6
2.2.1. Поиск пользователя	6
2.2.2. Добавление пользователя	8
2.2.3. Редактирование данных пользователя	8
2.2.4. Удаление пользователя	9
2.2.5. Блокировка/разблокировка пользователя	9
2.2.6. Отзыв всех токенов пользователя	9
2.2.7. Просмотр истории аутентификаций	9
2.3. Работа с объектами прав	10
2.4. Назначение прав пользователям	11
2.4.1. Создание ролей	11
2.4.2. Выдача ролей пользователям	15
2.5. Работа со справочником атрибутов пользователей	16
2.6. Работа со справочником клиентов	18
2.7. Работа со справочником провайдеров динамических атрибутов	20
2.7.1. Добавление провайдера	21
2.7.2. Редактирование провайдера	22
2.7.3. Удаление провайдера	22
2.8. Работа со справочником парольных политик	22
2.8.1. Добавление парольной политики	22
2.8.2. Редактирование парольной политики	24
2.8.3. Редактирование подсказки	24
2.8.4. Копирование парольной политики	24
2.8.5. Удаление парольной политики	24
2.9. Работа со справочником контрольных вопросов	24
2.9.1. Добавление контрольного вопроса	25
2.9.2. Редактирование контрольного вопроса	25
2.9.3. Удаление контрольного вопроса	25
2.10. Ввод ответов на контрольные вопросы	26
2.11. Работа со справочником типов пользователей	26
2.11.1. Добавление типа пользователей	27
2.11.2. Копирование типа пользователей	28
2.11.3. Редактирование типа пользователей	28
2.11.4. Удаление типа пользователей	28
2.12. Работа со справочником систем, создающих пользователей	28
2.12.1. Добавление системы, создающей пользователей	29
2.12.2. Удаление системы, создающей пользователей	29
2.13. Работа со справочником провайдеров аутентификации	30
2.13.1. Добавление провайдера аутентификации	30

2.13.2. Редактирование провайдера аутентификации	30
2.13.3. Удаление провайдера аутентификации	30
2.14. Работа с сессиями	31
2.14.1. Поиск сессий	31
2.14.2. Закрытие сессии	32
2.14.3. Просмотр и закрытие сессий текущего пользователя	32
2.15. Работа с токенами	32
2.15.1. Поиск токенов	32
2.15.2. Отзыв токена	33
2.15.3. Просмотр и отзыв токенов текущего пользователя	33

1. Общие сведения

Продукт «Аутентификация пользователей по технологии единого входа» (SSO) представляет собой центр управления доступом к продуктам АО «Нэксайн» и содержит унифицированный механизм аутентификации пользователей с поддержкой технологии единого входа.

2. Операции

Глава содержит описание стандартных действий, выполняемых оператором.

2.1. Начало работы

1. Запустите веб-браузер.
2. В адресной панели введите адрес главной страницы сайта системы. Откроется форма регистрации.
3. В поле **Логин** введите логин пользователя.
4. В поле **Пароль** введите пароль пользователя.
5. Нажмите на кнопку **Войти** или . Откроется страница приветствия.

Для возможности восстановления забытого пароля реализована функция восстановления пароля по контрольному вопросу:

1. На странице аутентификации перейдите по ссылке **Восстановление пароля**.
2. В поле **Логин** введите логин пользователя, пароль к которому требуется восстановить.
3. В поле **Вопрос** выберите контрольный вопрос из списка.
4. В поле **Ответ** введите ответ на контрольный вопрос.
5. Нажмите на кнопку **Восстановить пароль**.

Пользователь получит SMS-сообщение с новым паролем.



Примечание.

При превышении количества попыток восстановления пароля, заданного администратором, пользователь будет заблокирован.

Для завершения работы перейдите по ссылке **Выход** в верхнем меню.

2.2. Работа с пользователями

Для работы с пользователями предназначена форма «Список пользователей» (см. [Рис. 1](#)). Для перехода к форме выберите пункт меню **Пользователи > Список пользователей**.

2.2.1. Поиск пользователя

1. Заполните одно или несколько полей фильтрации на форме «Список пользователей» (см. [Рис. 1](#)):

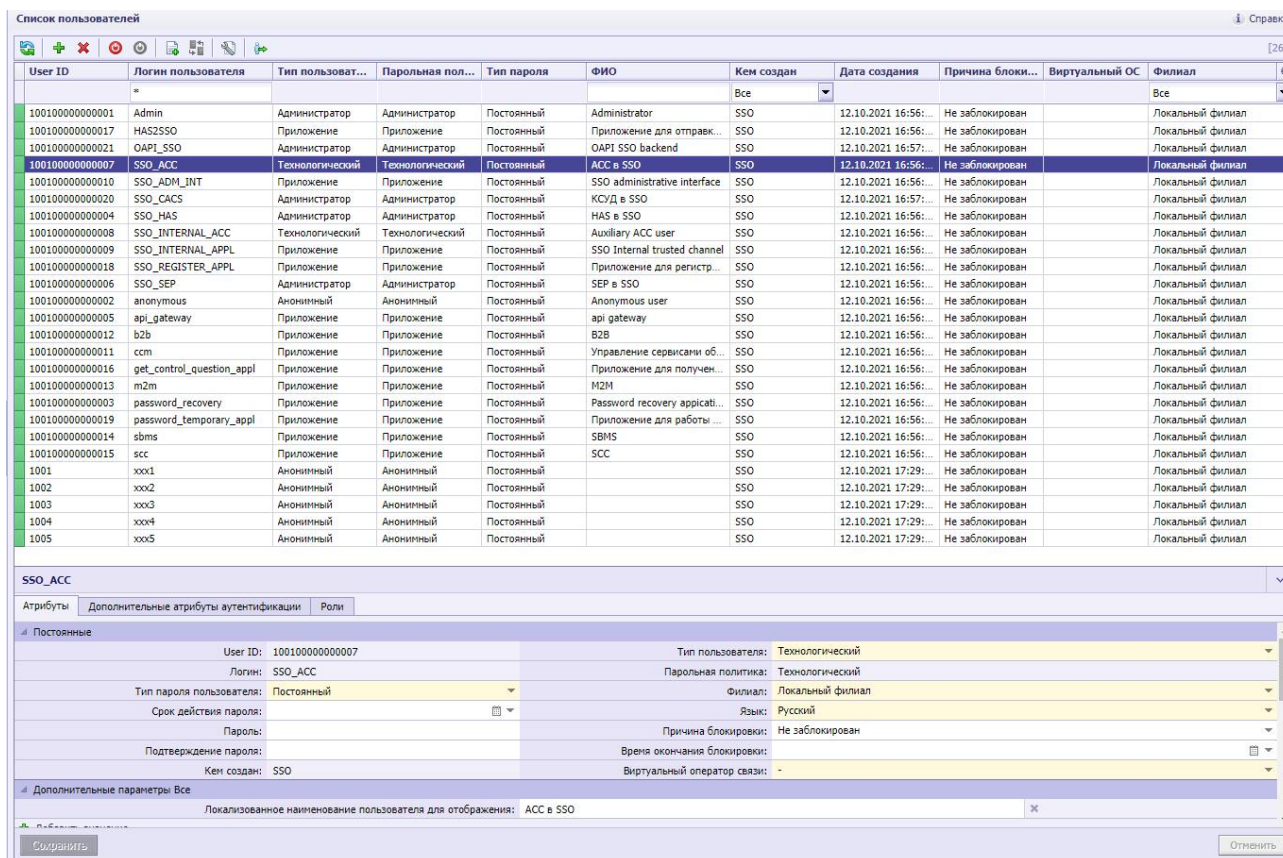



Рис. 1. Список пользователей

- **Логин пользователя** – поиск по полному логину или его части (символы «%» или «*» заменяют последовательность любых символов);
- **ФИО** – поиск имени пользователя (символы «%» или «*» заменяют последовательность любых символов);
- **Филиал** – выбор из списка филиала, в котором осуществляется поиск.

2. Нажмите на кнопку  или **Enter** для запуска поиска. На форме отобразится список результатов по заданным критериям поиска. В случае если результатов нет, отобразится сообщение «Пользователь не найден».

В нижней части формы находится информационная область, в которой отображаются сведения о пользователе, выбранном в таблице выше.

Информационная область содержит вкладки:


- «Атрибуты»;
- «Дополнительные атрибуты аутентификации»;
- «Роли».

Вкладка «Атрибуты» содержит подробную информацию об атрибутах выбранного пользователя. В верхней части вкладки отображаются постоянные атрибуты пользователя, в нижней части – дополнительные атрибуты для площадок.

Вкладка «Дополнительные атрибуты аутентификации» отображает информацию о дополнительных атрибутах аутентификации пользователя.

Вкладка «Роли» отображает список ролей, назначенных пользователю для каждой из площадок.

2.2.2. Добавление пользователя

1. Нажмите на кнопку  на панели инструментов формы «Список пользователей» (см. [Рис. 1](#)). В нижней части экрана откроется форма «Создание пользователя».
2. На вкладке «Атрибуты» заполните поля:
 - **Логин** – введите логин пользователя (пробел недопустим);
 - **Тип пароля пользователя** – выберите из выпадающего списка: временный/постоянный;
 - **Пароль** – введите пароль пользователя;
 - **Подтверждение пароля** – введите пароль пользователя;
 - **Тип пользователя** – выберите тип пользователя из выпадающего списка, при этом автоматически будет заполнено поле **Парольная политика**;



Примечание.




Тип пользователя должен соответствовать роли пользователя. Например, если пользователю будут назначены роли администратора, выберите в поле **Тип пользователя** значение «Администратор».

- **Филиал** – выберите филиал пользователя из выпадающего списка;
- **Язык** – выберите из выпадающего списка язык пользователя (английский/русский);
- **Причина блокировки** – выберите из выпадающего списка причину блокировки пользователя, если он создается в статусе «Заблокирован».



Примечание.


Для пользователей, добавляемых с помощью формы добавления пользователей, в поле **Кем создан** в таблице «Список пользователей» автоматически устанавливается значение SSO; это значение не подлежит редактированию.

- При необходимости добавьте дополнительные параметры для филиалов, нажав на кнопку , после чего выберите из выпадающего списка параметр и введите его значение.
3. Нажмите на кнопку **Сохранить** для сохранения изменений или кнопку **Отменить** для отмены введенных данных.
 4. Перейдите на вкладку «Дополнительные атрибуты аутентификации» и при необходимости добавьте дополнительные атрибуты аутентификации пользователя. Для этого нажмите на кнопку  и в открывшейся форме выберите тип и значение атрибута.
 5. Перейдите на вкладку «Роли» и задайте роли для пользователя. По нажатию на кнопку  для каждой площадки открывается окно «Добавление роли для площадки» (см. [Рис. 11](#)). В открывшемся окне выберите одну или несколько ролей и нажмите на кнопку **Добавить**. Выбранные роли будут назначены пользователю.



2.2.3. Редактирование данных пользователя

1. Выберите пользователя в списке результатов поиска в таблице пользователей формы «Список пользователей» (см. [Рис. 1](#)).
2. Внесите необходимые изменения в поля в нижней части формы (область редактирования атрибутов пользователя аналогична виду формы «Создание пользователя» (см. подраздел «[Добавление пользователя](#)»)) и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены внесенных изменений.


2.2.4. Удаление пользователя

1. Выберите пользователя из списка результатов на форме «Список пользователей» (см. [Рис. 1](#)).
2. Нажмите на кнопку  на панели инструментов, после чего подтвердите выполнение операции в открывшемся окне.

2.2.5. Блокировка/разблокировка пользователя

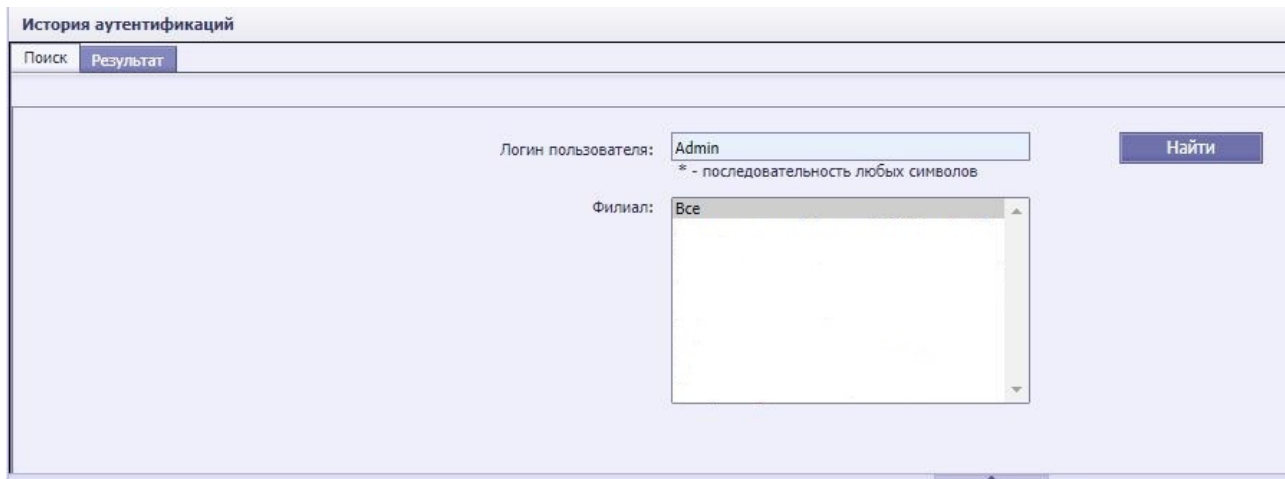
Пользователь может быть активен или заблокирован. Активные пользователи отмечены на форме «Список пользователей» (см. [Рис. 1](#)) зеленым цветом, заблокированные – красным. Для блокировки/разблокировки пользователя выберите пользователя из списка результатов и нажмите на соответствующую кнопку ( / ) на панели инструментов.

2.2.6. Отзыв всех токенов пользователя

1. Выберите пользователя из списка результатов на форме «Список пользователей» (см. [Рис. 1](#)).
2. Нажмите на кнопку  на панели инструментов, после чего подтвердите выполнение операции в открывшемся окне.


2.2.7. Просмотр истории аутентификаций

1. Выберите в меню **Пользователи > История аутентификаций**.
2. На вкладке «Поиск» формы «История аутентификаций» (см. [Рис. 2](#)) введите логин в поле **Логин пользователя**, выберите площадку в поле **Филиал**, после чего нажмите на кнопку **Найти**. Откроется вкладка «Результат» (см. [Рис. 3](#)).



История аутентификаций

Поиск **Результат**

Логин пользователя: 
* - последовательность любых символов

Филиал:

Рис. 2. История аутентификаций, вкладка «Поиск»

ИД	Логин пользователя	Тип пользователя	Парольная политика	Тип пароля	ФИО	Дата создания	Причина блокировки	Файл ав
10010000000001	Админ	Администратор	Администратор	Постоянный	Администратор	22.10.2021 09:19:46	Не заблокирован	Паспортный файл ав

Дата и время аутентификации	Результат аутентификации	Приложение	Тип аутентификации	IP-адрес пользователя	Интерфейс аутентификации
22.10.2021 09:25:59	успешно	api_gateway	с пароля	172.21.98.146	oidc
22.10.2021 09:25:51	InvalidControlQuestionAnswer	api_gateway	с ответом на контрольный вопрос	172.21.98.146	oidc#2
22.10.2021 09:25:17	успешно	api_gateway	с пароля	172.21.98.146	oidc#2
22.10.2021 09:25:10	успешно	api_gateway	без пароля	172.21.98.146	oidc#2

Рис. 3. История аутентификаций, вкладка «Результат»

3. Выберите строку найденного пользователя. В нижней части формы отобразится список аутентификаций выбранного пользователя.

2.3. Работа с объектами прав

Для работы со справочником объектов прав предназначена форма «Объекты прав» (см. Рис. 4).

Наименование объекта	Описание объекта
/ps/acc/api/has/batch	Пакет изменений прав от HAS
/ps/acc/api/role	Роль
/ps/acc/api/role/hierarchy	Дерево наследования ролей
/ps/auth/api/grants	Права
/ps/auth/api/grants/current	Права запрашивающего пользователя
/ps/auth/api/has/grants	Права HAS
ACC_SRV_GRANTS_DEFAULT_ROLES	Права на предустановленные роли
ACC_SRV_GRANTS_ROLES	Права на типы ролей
ACC_SRV_GRANTS_USER_ROLES	Права на пользовательские роли
ACC_SRV_RESOURCES	Корневой ресурс LDAP
HAS_RESOURCES	Корневой ресурс HAS
OAPI1_RESOURCES	Корневой ресурс OAPI1
SSO_RESOURCES	Корневой ресурс SSO
grant_type	Аргумент функции получения токена grant_type
sso.attribute	Атрибут
sso.attribute.elements	Список значений атрибута
sso.attribute.type	Тип атрибута
sso.attribute.value_type	Тип значений атрибута
sso.auth.token	Auth токен
sso.auth.code	Получение кода авторизации
sso.captcha	Капча
sso.client	Клиент
sso.client.type	Тип клиента
sso.cmn_dictionary	Значение словаря
sso.current.control_questions	Контрольные вопросы текущего пользователя
sso.current.control_questions.controlQuestionId	Идентификатор контрольного вопроса
sso.current.password.change	Операции с паролем (изменение)
sso.current.password.expiration	Изменения срока действия пароля

Наименование объекта: sso.attribute.elements

Свойства: Ограничения [0] Допустимые операции [4] Родительские объекты [1] Дочерние объекты [0] Дополнительные свойства [0]

Наименование объекта: sso.attribute.elements
 Отображаемое наименование: sso.attribute.elements
 Описание объекта: Список значений атрибута

Сервис: Сервер аутентификации Родитель: SSO_RESOURCES
 Тип: Ресурс Тип значений объект.: Нет значения
 HTTP маска: /ps/auth/api/attributes/{_}/elements/ps/auth/api/attributes/{_}/elements/{_}/ps/auth/api/attributes/{_}/elements/department/{_}

Рис. 4. Объекты прав

Форма содержит элементы:

- панель инструментов;
- таблицу, отображающую список объектов прав;
- область отображения информации о выбранном объекте.


При нажатии на кнопку  откроется форма «Проверка наличия у пользователя права на объект».

Таблица на форме отображает список объектов в виде иерархического дерева.


В нижней части формы находится информационная область, в которой отображается информация о выбранном объекте:

- «Свойства» – подробная информация о выбранном объекте;
- «Ограничения» – информация об ограничениях, связанных с объектом, с их предустановленными значениями и атрибутами;
- «Допустимые операции» – список операций, допустимых для выбранного объекта;
- «Родительские объекты» – подробная информация о родительских объектах выбранного объекта;
- «Дочерние объекты» – подробная информация о дочерних объектах выбранного объекта;
- «Дополнительные свойства» – информация о произвольных свойствах выбранного объекта.

2.4. Назначение прав пользователям

Назначение прав пользователям осуществляется поэтапно: сначала создайте роли, затем выдайте их пользователям. Для создания ролей предназначена форма «Роли» (см. [Рис. 5](#)). Для перехода к форме выберите пункт меню **Справочники > Роли**.

2.4.1. Создание ролей

1. На форме «Роли» (см. [Рис. 5](#)) нажмите на кнопку  и в нижней части формы заполните необходимые поля во вкладке «Свойства».

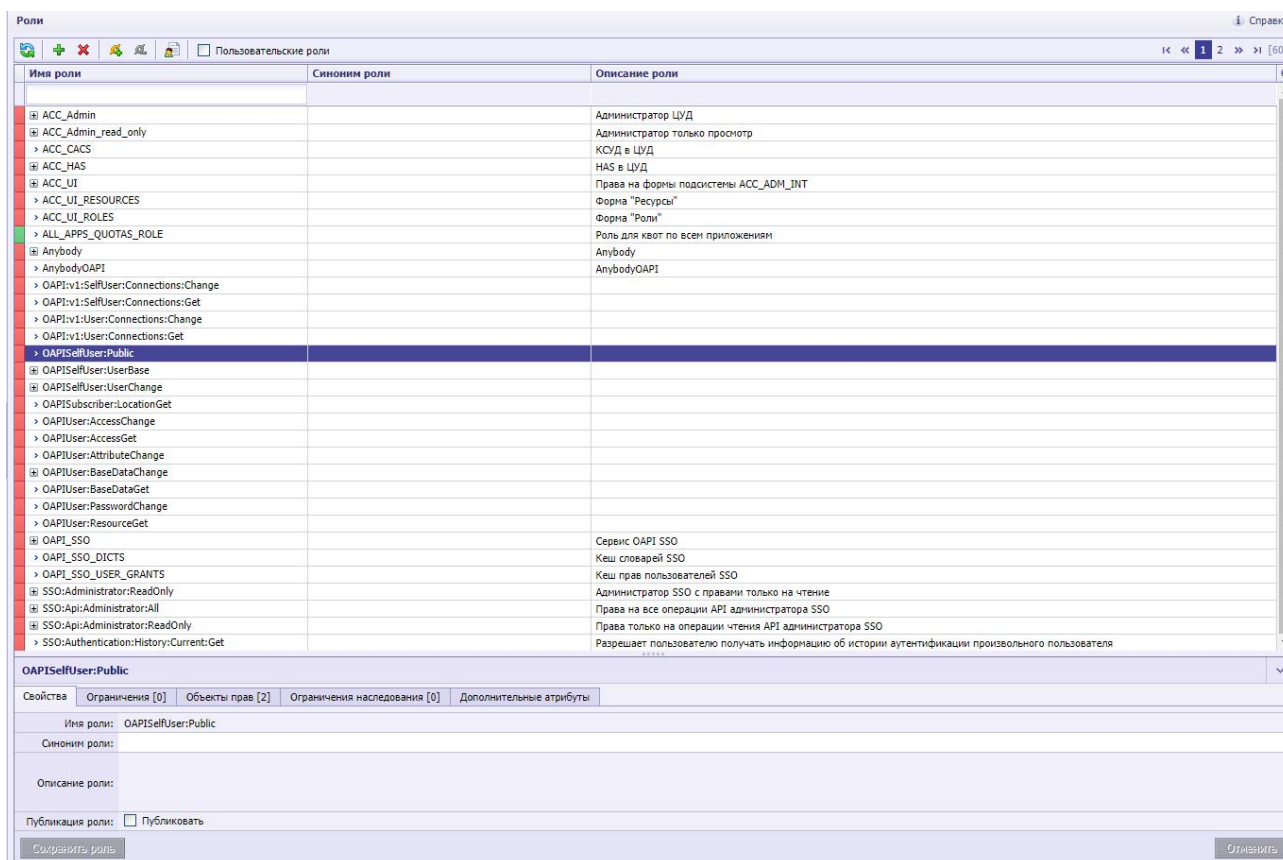

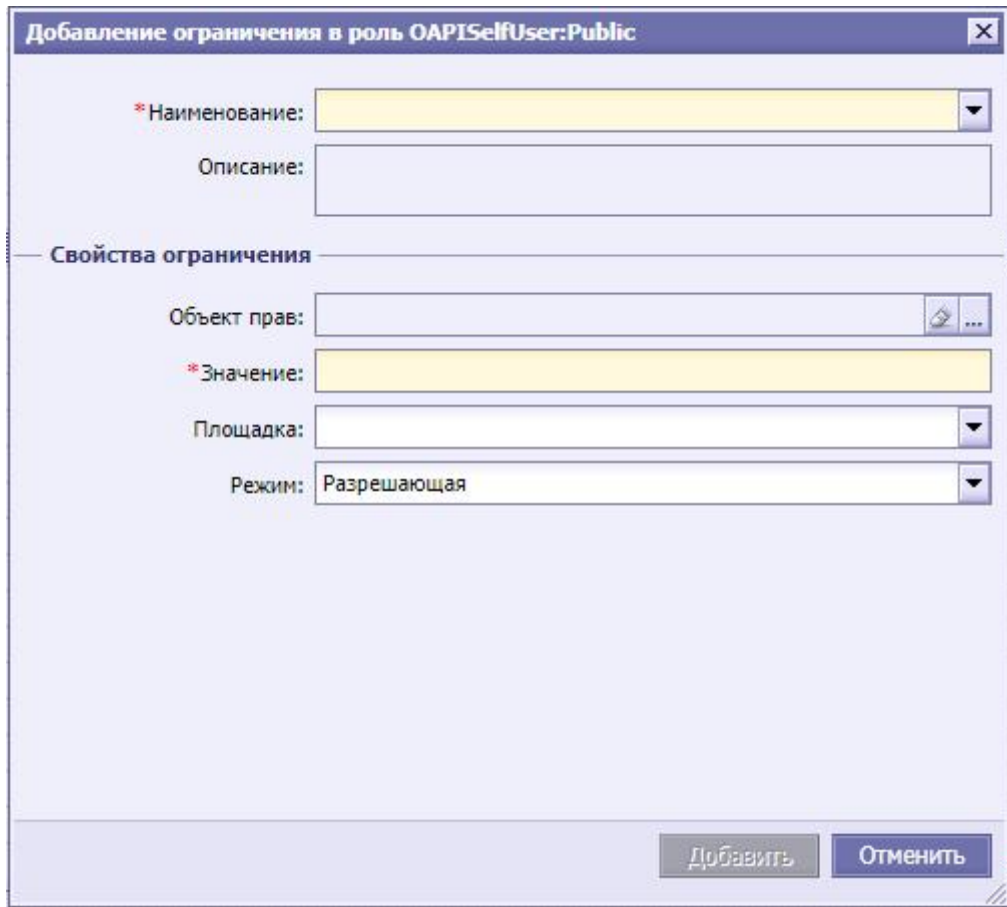


Рис. 5. Роли

2. Для созданной роли:

- на вкладке «Ограничения» задайте ограничения для выбранной роли:
 -  – открыть форму «Добавление ограничения в роль» (см. [Рис. 6](#));



Добавление ограничения в роль OAPISelfUser:Public

* Наименование:

Описание:

Свойства ограничения

Объект прав:




* Значение:

Площадка:

Режим: Разрешающая

Добавить Отменить

Рис. 6. Добавление ограничения в роль

-  – открыть форму для редактирования значения и режима использования ограничения;
-  – удалить выбранное ограничение;
- на вкладке «Объекты прав» выдайте права на объекты:
 -  – открыть форму «Добавить право на объект» (см. [Рис. 7](#));

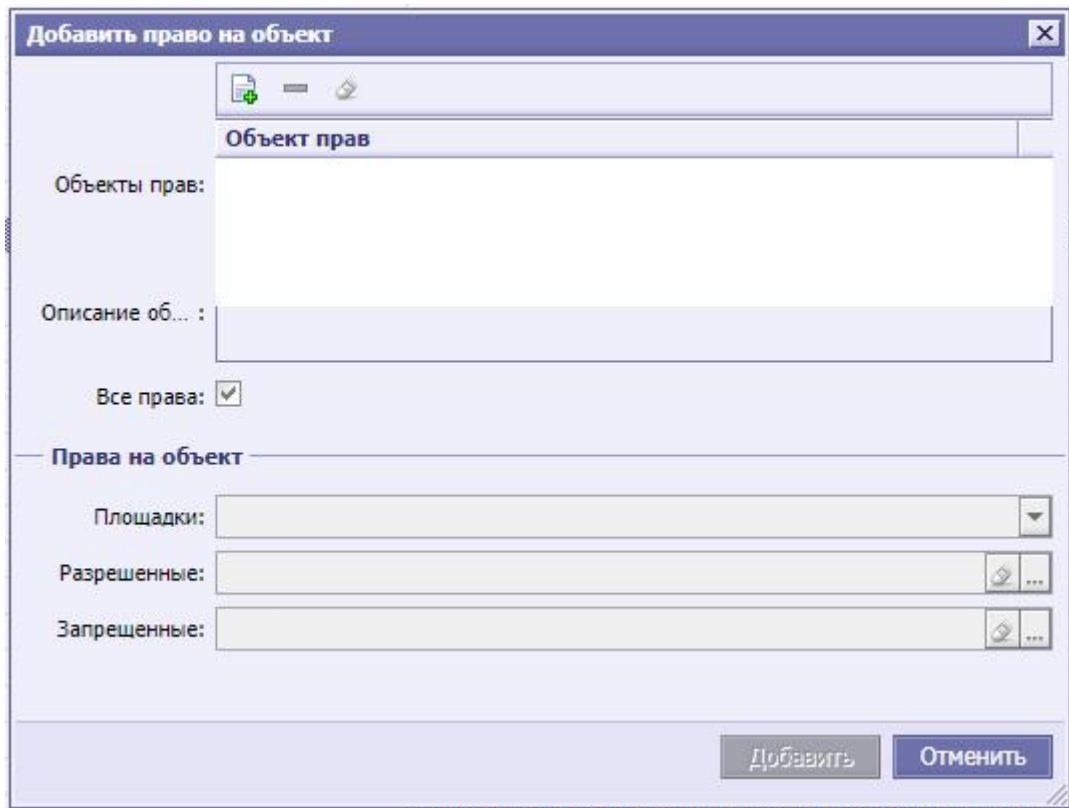





Рис. 7. Добавить право на объект

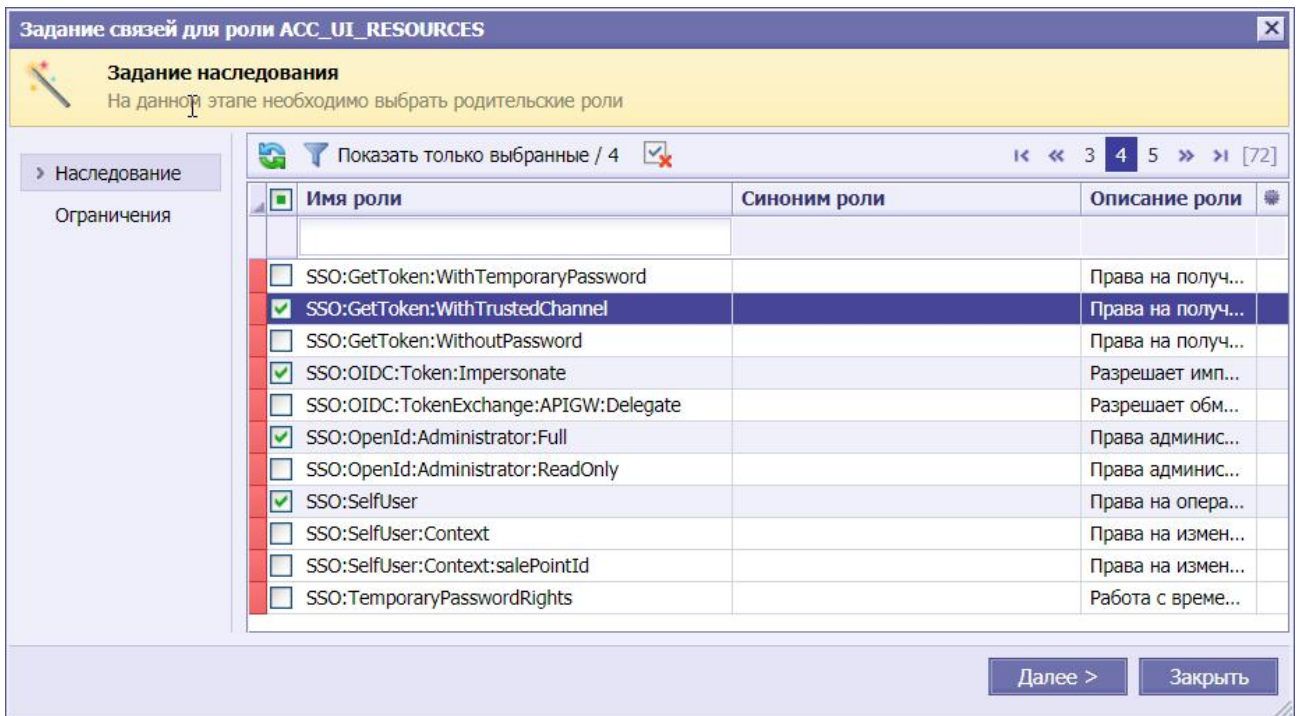
-  – открыть форму для редактирования площадки и списка операций для выбранного объекта;
-  – удалить права на выбранный объект.
- на вкладке «Ограничения наследования» задайте ограничения наследования прав данной роли:
 - **Редактируемая** – наименование выбранной роли;
 - **Дочерняя роль** – наименование роли, от которой наследуются права;
 - **Ограничения** – область, отображающая список ограничений:
 - **Площадка** – поле с выпадающим списком для выбора площадки;
 - **Уровень аутентификации** – поле с выпадающим списком для выбора уровня аутентификации;
 - **Приложение** – поле с выпадающим списком для выбора приложения;
 - кнопка  – добавляет строку для ввода значений нового ограничения;
 - в конце каждой строки ограничения находится кнопка  для удаления ограничения из списка;
 - кнопка **Сохранить** – предназначена для сохранения в базе данных внесенных изменений;
 - кнопка **Отменить** – предназначена для отмены внесенных изменений;
- на вкладке «Дополнительные атрибуты» задайте список дополнительных атрибутов данной роли в разрезе площадок.



Примечание.

Права могут быть выданы как для всех филиалов, так и для конкретного филиала. Права могут разрешать / запрещать выполнение операции / всех операций. Запрещенные операции приоритетны по отношению к разрешенным. Роль может быть включена в иерархию, то есть для роли может быть назначена родительская роль. Следует иметь в виду, что роль наследует права родительских ролей. Право на объект прав означает право на дочерние объекты.

3. Для назначения родительской роли и ограничений нажмите на кнопку  – откроется форма «Задание связей для роли» (см. [Рис. 8](#) и [Рис. 9](#)), на которой выберите родительскую роль и добавьте ограничения для роли.



Задание связей для роли ACC_UI_RESOURCES

Задание наследования
На данном этапе необходимо выбрать родительские роли

Показать только выбранные / 4

Имя роли	Синоним роли	Описание роли
<input type="checkbox"/> SSO:GetToken:WithTemporaryPassword		Права на получ...
<input checked="" type="checkbox"/> SSO:GetToken:WithTrustedChannel		Права на получ...
<input type="checkbox"/> SSO:GetToken:WithoutPassword		Права на получ...
<input checked="" type="checkbox"/> SSO:OIDC:Token:Impersonate		Разрешает имп...
<input type="checkbox"/> SSO:OIDC:TokenExchange:APIGW:Delegate		Разрешает обм...
<input checked="" type="checkbox"/> SSO:OpenId:Administrator:Full		Права админис...
<input type="checkbox"/> SSO:OpenId:Administrator:ReadOnly		Права админис...
<input checked="" type="checkbox"/> SSO:SelfUser		Права на опера...
<input type="checkbox"/> SSO:SelfUser:Context		Права на измен...
<input type="checkbox"/> SSO:SelfUser:Context:salePointId		Права на измен...
<input type="checkbox"/> SSO:TemporaryPasswordRights		Работа с време...

Далее > Закреть

Рис. 8. Форма «Задание связей для роли» – вкладка «Наследование»

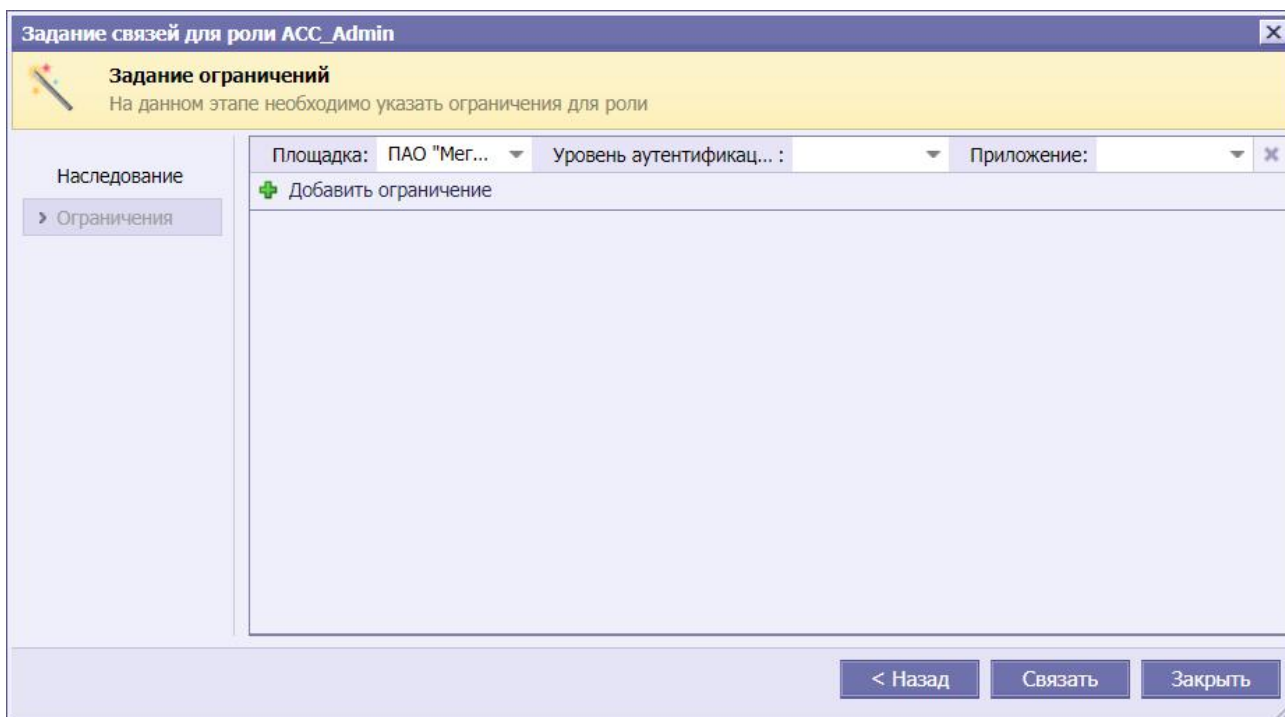




Рис. 9. Форма «Задание связей для роли» – вкладка «Ограничения»

4. Для удаления выбранной роли из иерархии нажмите на кнопку .
5. Для просмотра списка пользователей, которым выдана выбранная роль, нажмите на кнопку  – откроется форма «Список пользователей с ролью» (см. [Рис. 10](#)):

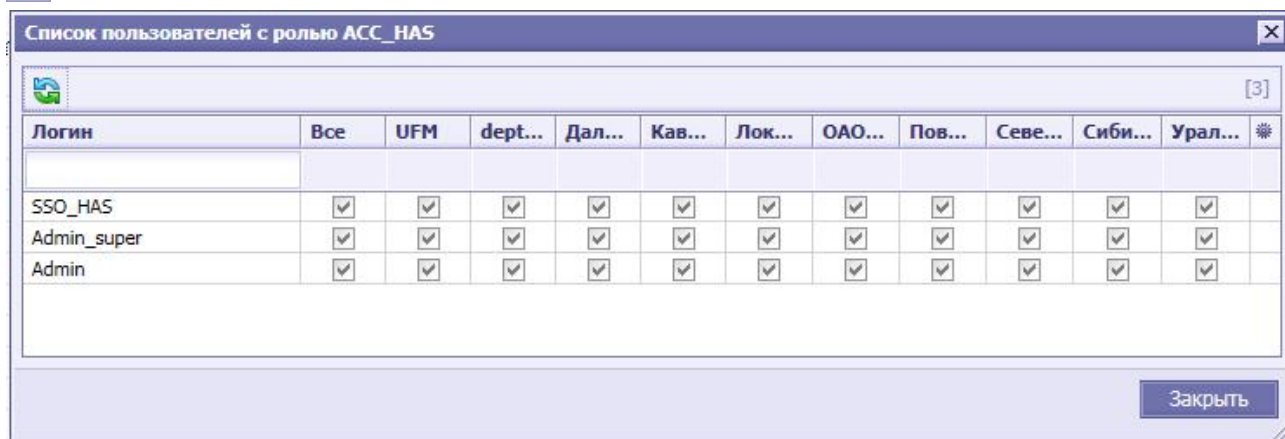


Рис. 10. Список пользователей с ролью

- в поле **Логин** допустим поиск пользователя по маске – символ «%» заменяет последовательность любых символов;
- отмеченное поле **Все** говорит о том, что данная роль выдана пользователю на всех площадках;
- отмеченное поле **<Наименование площадки>** говорит о том, что данная роль выдана пользователю на данной площадке.

2.4.2. Выдача ролей пользователям



1. На форме «Список пользователей» (см. [Рис. 1](#)) выполните поиск пользователя по логину или Ф.И.О.

2. На вкладке «Роли» в нижней части формы назначьте роли выбранному пользователю.



Примечание.

Роли могут быть заданы для всех филиалов или для конкретного филиала.

Вкладка «Роли» содержит список ролей, назначенных пользователю для каждой из площадок. При нажатии на кнопку  роль будет удалена. При нажатии на кнопку  **Добавить роль** открывается форма «Добавление роли для площадки» (см. [Рис. 11](#)).

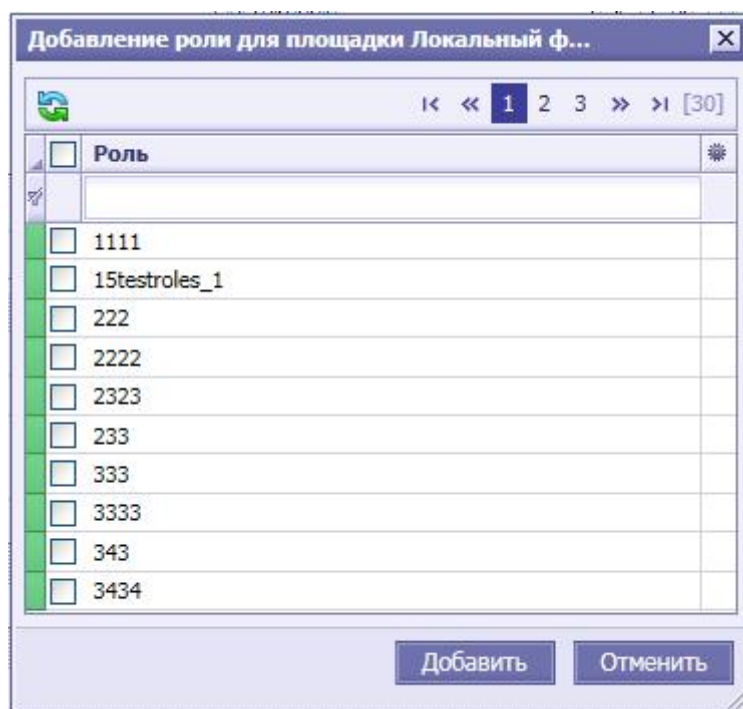


Рис. 11. Добавление роли для площадки

В поле **Роль** допустим поиск роли по маске: символ «%» заменяет последовательность любых символов.

2.5. Работа со справочником атрибутов пользователей

В качестве дополнительных атрибутов пользователя могут быть заданы (помимо логина) такие значения, как: псевдоним пользователя, связи с социальными сетями, например, логин Google и т.п.

Реализована возможность добавления, редактирования и удаления дополнительных атрибутов пользователя.

Для работы со справочником дополнительных атрибутов предназначена форма «Атрибуты пользователей» (см. [Рис. 12](#)), которая открывается при выборе пункта меню **Справочники > Атрибуты пользователей**.

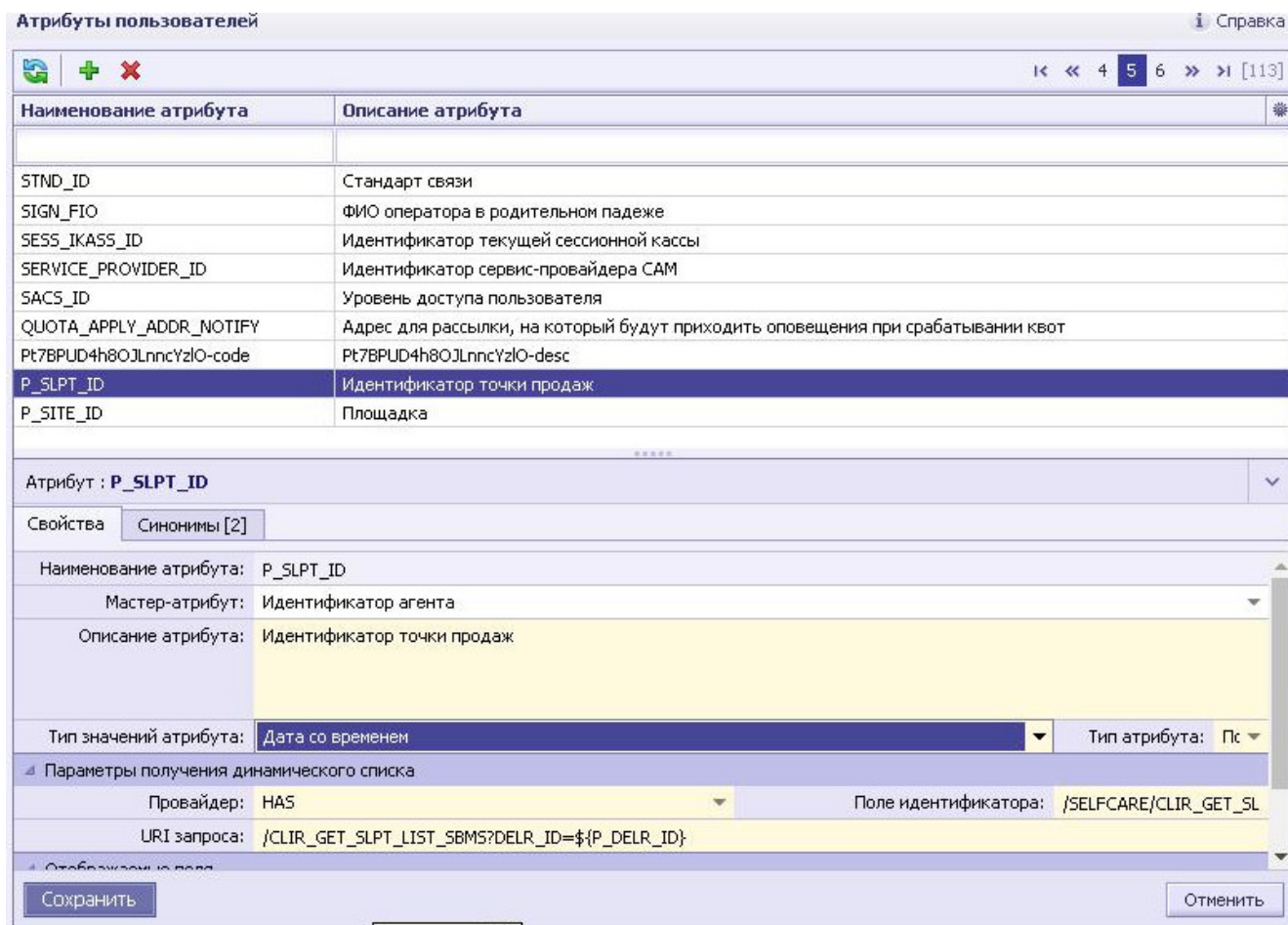


Рис. 12. Атрибуты пользователей

Для добавления атрибута пользователей:


1. Нажмите на кнопку . В нижней части окна откроется форма «Создание атрибута».
2. Заполните поля:
 - **Наименование** – введите наименование атрибута;
 - **Мастер-атрибут** – выберите из списка мастер-атрибут (родительский атрибут) для создаваемого атрибута;
 - **Описание** – введите описание атрибута;
 - **Тип значений атрибута** – выберите тип значений из выпадающего списка (строка, число, дата со временем, булево);
 - **Тип атрибута** – выберите тип атрибута из выпадающего списка (простое значение, по статическому списку, по динамическому списку, флажок).
3. Добавьте значения статического списка, в случае если атрибут имеет тип «По статическому списку»:
 - нажмите на кнопку **Добавить значение** для заполнения статического списка значений атрибута (значения добавляются по одному); поле отображается при выборе значения «По статическому списку» в поле **Тип атрибута**;
 - нажмите на кнопку **Добавить список значений** для заполнения статического списка значений атрибута (значения добавляются списком); поле отображается при выборе значения «По статическому списку» в поле **Тип атрибута**.
4. Заполните параметры получения динамического списка, в случае если атрибут имеет тип «По динамическому списку». Для этого нажмите на кнопку . Поле отображается при выборе значения «По динамическому списку» в поле **Тип атрибута**.

5. Нажмите на кнопку **Создать** для добавления атрибута или **Отменить** для отмены добавления атрибута.

Для изменения атрибута пользователей:

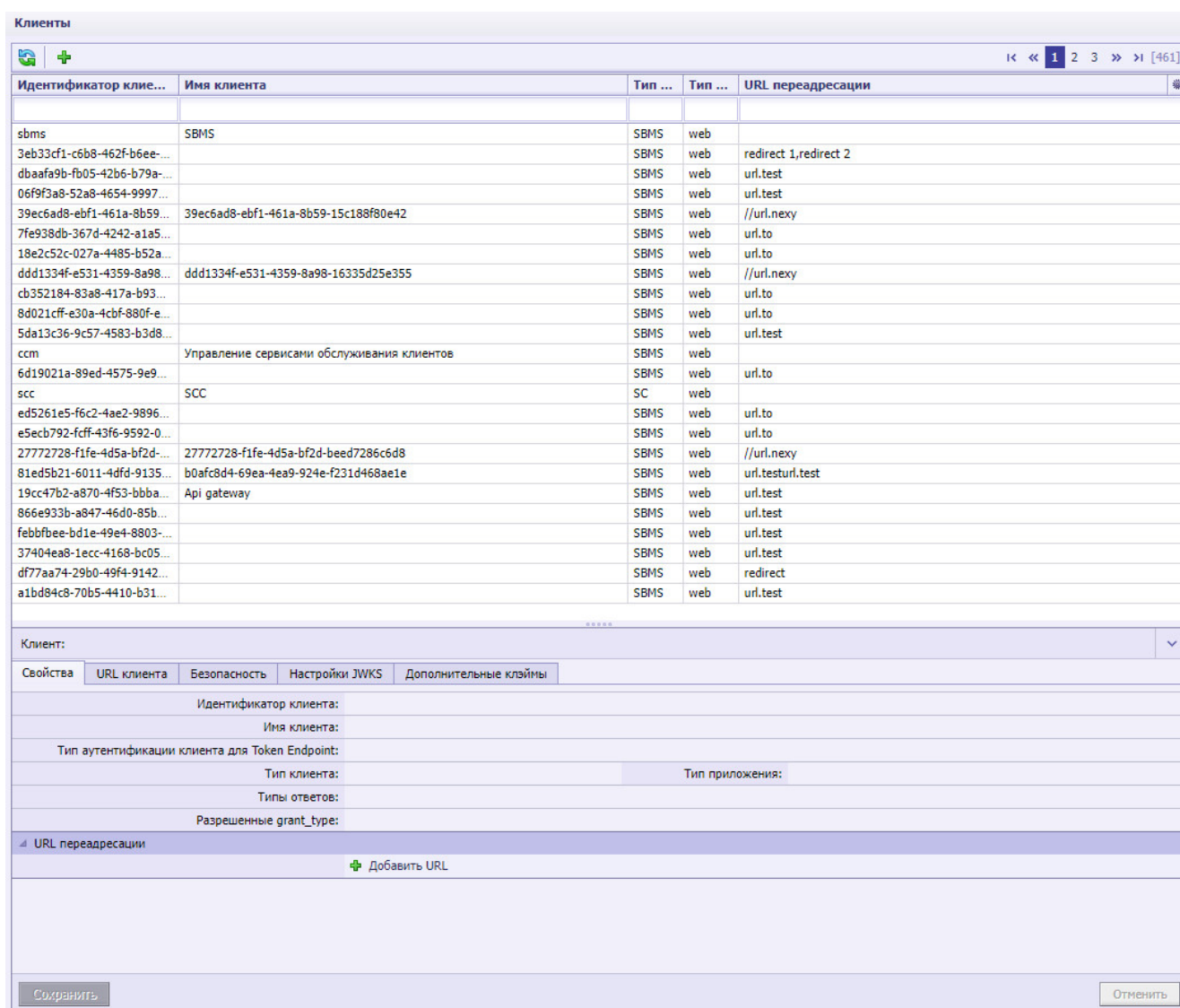
1. Выберите атрибут из списка.
2. В нижней части формы внесите необходимые изменения в параметры атрибута и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены внесенных изменений.

Для удаления атрибута пользователей:

1. Выберите атрибут из списка.
2. Нажмите на кнопку  на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.6. Работа со справочником клиентов

Для работы со справочником клиентов OpenID Connect предназначена форма «Клиенты» (см. [Рис. 13](#)), которая открывается при выборе пункта меню **Справочники > Клиенты**.



Идентификатор клиент...	Имя клиента	Тип ...	Тип ...	URL перенаправления
sbms	SBMS	SBMS	web	
3eb33cf1-c6b8-462f-b6ee-...		SBMS	web	redirect 1,redirect 2
dbaafa9b-fb05-42b6-b79a-...		SBMS	web	url.test
06f9f3a8-52a8-4654-9997-...		SBMS	web	url.test
39ec6ad8-ebf1-461a-8b59-...	39ec6ad8-ebf1-461a-8b59-15c188f80e42	SBMS	web	//url.nexy
7fe938db-367d-4242-a1a5-...		SBMS	web	url.to
18e2c52c-027a-4485-b52a-...		SBMS	web	url.to
ddd1334f-e531-4359-8a98-...	ddd1334f-e531-4359-8a98-16335d25e355	SBMS	web	//url.nexy
cb352184-83a8-417a-b93-...		SBMS	web	url.to
8d021cff-e30a-4cbf-880f-e-...		SBMS	web	url.to
5da13c36-9c57-4583-b3d8-...		SBMS	web	url.test
ccm	Управление сервисами обслуживания клиентов	SBMS	web	
6d19021a-89ed-4575-9e9-...		SBMS	web	url.to
scc	SCC	SC	web	
ed5261e5-f6c2-4ae2-9896-...		SBMS	web	url.to
e5ecb792-fcff-43f6-9592-0-...		SBMS	web	url.to
27772728-f1fe-4d5a-bf2d-...	27772728-f1fe-4d5a-bf2d-beed7286c6d8	SBMS	web	//url.nexy
81ed5b21-6011-4dfd-9135-...	b0afc8d4-69ea-4ea9-924e-f231d468ae1e	SBMS	web	url.testurl.test
19cc47b2-a870-4f53-bbba-...	Api gateway	SBMS	web	url.test
866e933b-a847-46d0-85b-...		SBMS	web	url.test
febbfbee-bd1e-49e4-8803-...		SBMS	web	url.test
37404ea8-1ecc-4168-bc05-...		SBMS	web	url.test
df77aa74-29b0-49f4-9142-...		SBMS	web	redirect
a1bd84c8-70b5-4410-b31-...		SBMS	web	url.test

Клиент: ▼

Свойства | URL клиента | Безопасность | Настройки JWKS | Дополнительные ключи

Идентификатор клиента:

Имя клиента:


Тип аутентификации клиента для Token Endpoint:

Тип клиента: Тип приложения:

Типы ответов:

Разрешенные grant_type:



URL перенаправления

 Добавить URL

Сохранить Отменить

Рис. 13. Клиенты

Для добавления клиента OpenID Connect:

1. Нажмите на кнопку . В нижней части окна откроется форма «Новый клиент».
2. На вкладке «Свойства» заполните поля:
 - **Идентификатор клиента** – введите идентификатор клиента;
 - **Имя клиента** – введите наименование клиента;
 - **Тип аутентификации клиента для Token Endpoint** – выберите тип аутентификации клиента из выпадающего списка (client_secret_basic, client_secret_post);
 - **Тип клиента** – выберите тип клиента из выпадающего списка;
 - **Тип приложения** – выберите тип приложения из выпадающего списка (web, native);
 - **Типы ответов** – выберите один или несколько типов ответов из выпадающего списка (code, id_token, token);
 - **Разрешенные grant_type** – выберите один или несколько grant_type из выпадающего списка (authorization_type, client_credentials, password, refresh_token, ietf:params:oauth:token-type:token_exchange);
 - **URL переадресации** – добавьте один или несколько URL для переадресации.
3. На вкладке «URL клиента» введите значения URL создаваемого клиента:
 - **URL домашней страницы клиента;**
 - **URL страницы с описанием правил использования данных профиля пользователя клиентом (Policy);**
 - **URL страницы правил использования сервиса клиента (Term of service);**
 - **URL для перенаправления пользователя после завершения сессии.**
4. На вкладке «Безопасность» выберите из выпадающего списка значения алгоритмов (A128CBC-HS256 или none):
 - **Алгоритм подписи ID токена, выдаваемого клиенту;**
 - **Алгоритм шифрования содержимого ID токена, выдаваемого клиенту;**
 - **Алгоритм шифрования ключа ID токена, выдаваемого клиенту;**
 - **Алгоритм подписи Access токена, выдаваемого клиенту;**
 - **Алгоритм шифрования содержимого Access токена, выдаваемого клиенту;**
 - **Алгоритм шифрования ключа Access токена, выдаваемого клиенту;**
 - **Алгоритм подписи ответов User Info Endpoint;**
 - **Алгоритм шифрования ответов User Info Endpoint;**
 - **Алгоритм шифрования ключа ответов User Info Endpoint.**
5. На вкладке «Настройки JWKS» введите значения в поля:
 - **URL для получения JSON Web Key Set;**
 - **Значение JSON Web Key Set.**
6. На вкладке «Дополнительные клэймы» нажмите на кнопку  **Добавить клэйм** и заполните поля:
 - **Имя клэйма** – введите наименование клэйма;
 - **Источник данных клэйма** – выберите значение из выпадающего списка;
 - **Добавлять клэйм в** – выберите одно или несколько значений из выпадающего списка (UserInfo endpoint, access_token, id_token, Introspection endpoint);
 - **Роли** – нажмите на кнопку **Добавить роль** и в открывшейся форме «Добавить роли в клэйм» (см. [Рис. 14](#)) выберите одну или несколько ролей и нажмите на кнопку **Сохранить**, после чего для каждой выбранной роли укажите филиалы в поле **Только в филиалах** (доступен выбор нескольких значений);

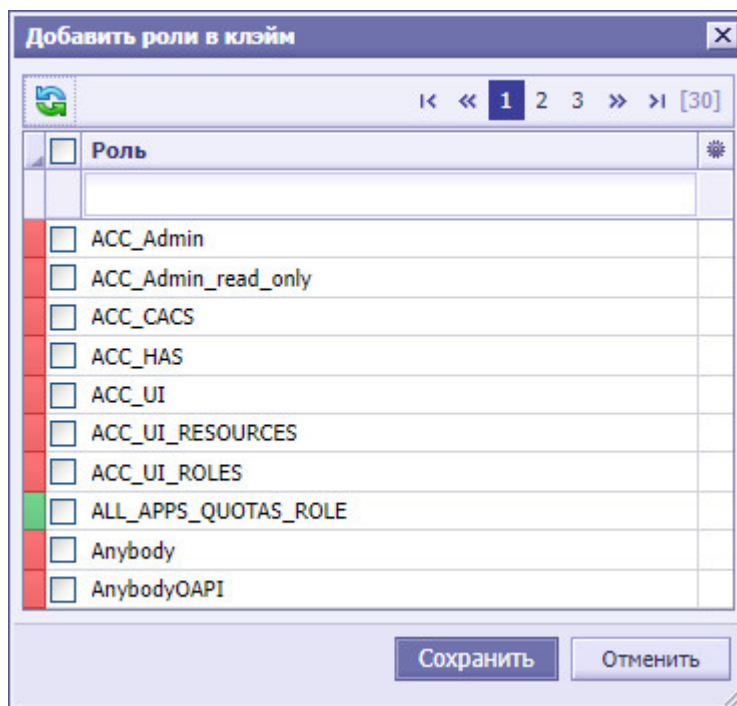



Рис. 14. Добавление роли в клэйм

В поле **Роль** допустим поиск роли по маске: символ «%» заменяет последовательность любых символов.

- для добавления еще одного клэйма нажмите на кнопку  **Добавить клэйм** и заполните поля.

7. Нажмите на кнопку **Создать** для добавления клиента или **Отменить** для отмены.

Для изменения данных клиента:

1. Выберите клиента из списка.
2. В нижней части формы внесите необходимые изменения (для редактирования доступны только поля с выпадающими списками) и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены внесенных изменений.

2.7. Работа со справочником провайдеров динамических атрибутов

Для структурирования информации по подключениям к точкам, предоставляющим динамические атрибуты, предусмотрена сущность провайдера. Для провайдера задается список по площадкам, содержащий адрес и порт подключения (в формате url), логин и пароль для запросов, при необходимости.

Работа со справочником провайдеров динамических атрибутов осуществляется через форму «Провайдеры дин. атрибутов» (см. [Рис. 15](#)). Для перехода к форме выберите пункт меню **Справочники > Провайдеры дин. атрибутов**.

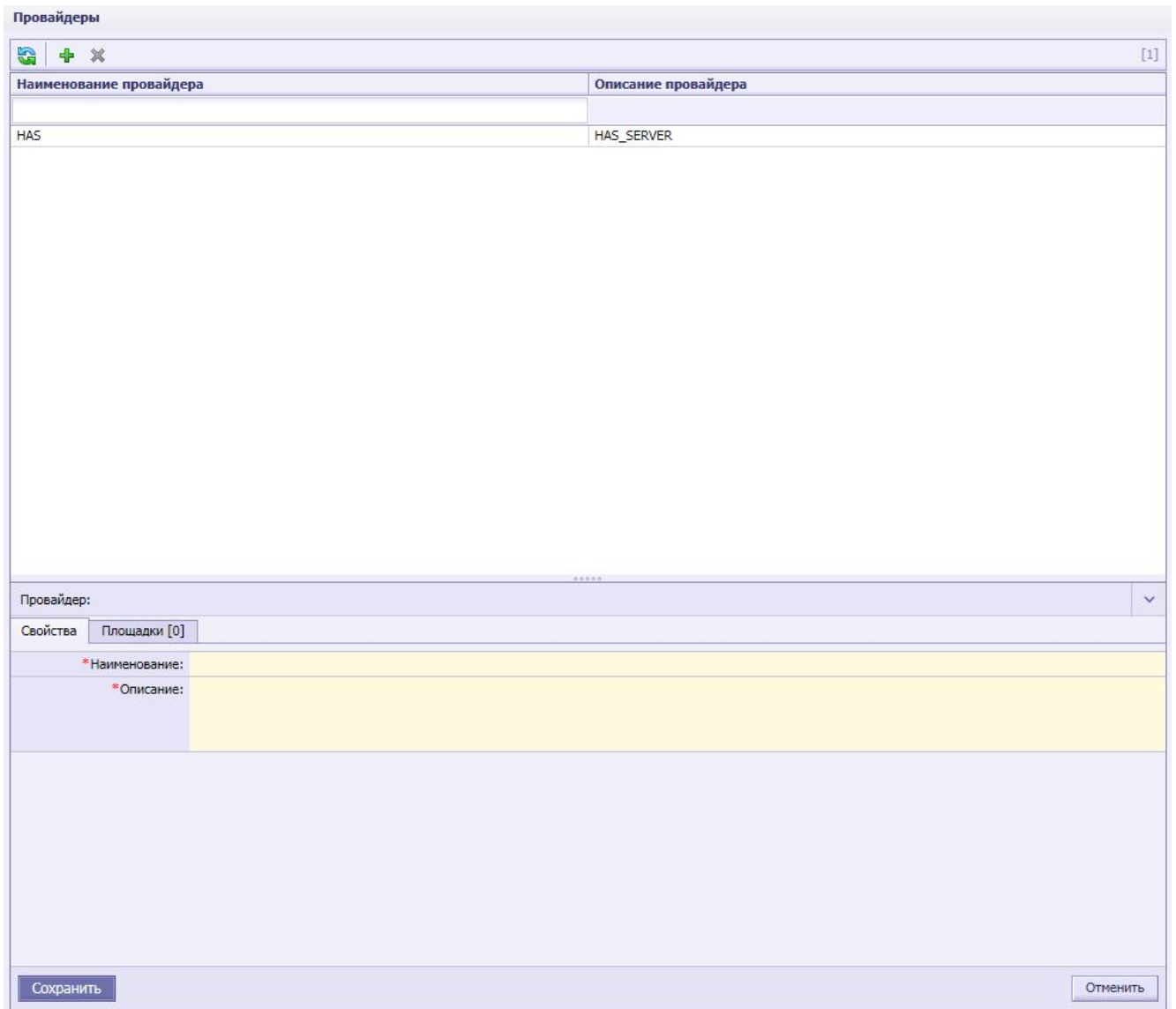




Рис. 15. Провайдеры динамических атрибутов


2.7.1. Добавление провайдера

1. Нажмите на кнопку  на панели инструментов формы «Провайдеры дин. атрибутов» (см. [Рис. 15](#)). В нижней части экрана откроется форма «Создание провайдера».
2. На вкладке «Свойства» заполните поля **Наименование** и **Описание** для создаваемого провайдера.
3. Нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены введенных данных.
4. Перейдите на вкладку «Площадки» для указания параметров подключения по площадкам. Для этого нажмите на кнопку  **Добавить площадку** и в появившейся строке заполните поля:
 - наименование площадки из выпадающего списка;
 - адрес и порт подключения;
 - логин и пароль для запросов.
5. Нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены введенных данных.

2.7.2. Редактирование провайдера

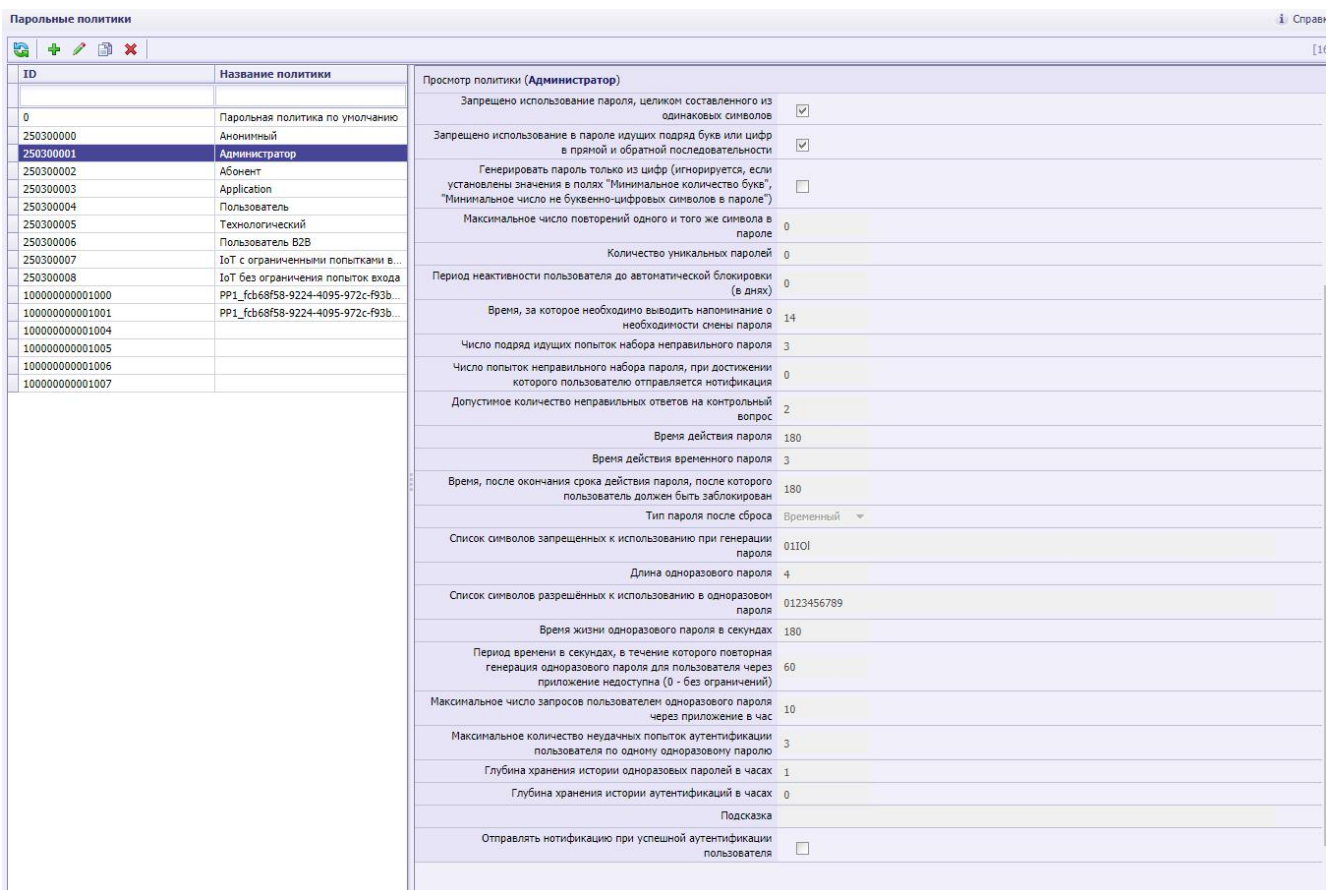
1. Выберите провайдера в списке – в нижней части формы отобразятся данные выбранного провайдера. Область редактирования параметров провайдера аналогична виду формы «Создание провайдера» (см. подраздел «[Добавление провайдера](#)»).
2. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены внесенных изменений.


2.7.3. Удаление провайдера

1. Выберите провайдера из списка на форме «Провайдеры дин. атрибутов» (см. [Рис. 15](#)).
2. Нажмите на кнопку  на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.8. Работа со справочником парольных политик

Для перехода к форме «Парольные политики» (см. [Рис. 16](#)) выберите пункт меню **Справочники > Парольные политики**.



Панель инструментов: 


ID	Название политики
0	Парольная политика по умолчанию
250300000	Анонимный
250300001	Администратор
250300002	Абонент
250300003	Application
250300004	Пользователь
250300005	Технологический
250300006	Пользователь B2B
250300007	IoT с ограничениями попытками в...
250300008	IoT без ограничения попыток входа
100000000001000	PP1_fcb68f58-9224-4095-972c-f93b...
100000000001001	PP1_fcb68f58-9224-4095-972c-f93b...
100000000001004	
100000000001005	
100000000001006	
100000000001007	

Просмотр политики (Администратор)

- Запрещено использование пароля, целиком составленного из одинаковых символов
- Запрещено использование в пароле идущих подряд букв или цифр в прямой и обратной последовательности
- Генерировать пароль только из цифр (игнорируется, если установлены значения в полях "Минимальное количество букв", "Минимальное число не буквенно-цифровых символов в пароле")
- Максимальное число повторений одного и того же символа в пароле: 0
- Количество уникальных паролей: 0
- Период неактивности пользователя до автоматической блокировки (в днях): 0
- Время, за которое необходимо выводить напоминание о необходимости смены пароля: 14
- Число подряд идущих попыток набора неправильного пароля: 3
- Число попыток неправильного набора пароля, при достижении которого пользователю отправляется нотификация: 0
- Допустимое количество неправильных ответов на контрольный вопрос: 2
- Время действия пароля: 180
- Время действия временного пароля: 3
- Время, после окончания срока действия пароля, после которого пользователь должен быть заблокирован: 180
- Тип пароля после сброса: Временный
- Список символов запрещенных к использованию при генерации пароля: 0110I
- Длина одноразового пароля: 4
- Список символов разрешенных к использованию в одноразовом пароле: 0123456789
- Время жизни одноразового пароля в секундах: 180
- Период времени в секундах, в течение которого повторная генерация одноразового пароля для пользователя через приложение недоступна (0 - без ограничений): 60
- Максимальное число запросов пользователем одноразового пароля через приложение в час: 10
- Максимальное количество неудачных попыток аутентификации пользователя по одному одноразовому паролю: 3
- Глубина хранения истории одноразовых паролей в часах: 1
- Глубина хранения истории аутентификаций в часах: 0
- Подсказка:
- Отправлять нотификацию при успешной аутентификации пользователя:

Рис. 16. Парольные политики

2.8.1. Добавление парольной политики


1. Нажмите на кнопку  на панели инструментов. В правой части экрана станет доступна для заполнения область «Создание новой парольной политики».
2. Заполните поля формы:

- **ID** – идентификатор записи (добавляется автоматически);
- **Название** – название парольной политики; поле обязательно для заполнения;
- **Уровень сложности** – задается сложность пароля; поле обязательно для заполнения;
- **Минимальная длина пароля**;
- **Максимальная длина пароля**;
- **Минимальное количество цифр**;
- **Минимальное количество букв**;
- **Минимальное число не буквенно-цифровых символов в пароле**;
- **Разрешено использование пробела**;
- **Запрещено совпадение пароля и логина**;
- **Запрещено использование пароля, целиком составленного из одинаковых символов**;
- **Запрещено использование в пароле идущих подряд букв или цифр в прямой и обратной последовательности**;
- **Генерировать пароль только из цифр** (игнорируется, если установлены значения в полях **Минимальное количество букв**, **Минимальное число не буквенно-цифровых символов в пароле**);
- **Максимальное число повторений одного и того же символа в пароле**;
- **Количество уникальных паролей** – ограничение на повторное использование прежних паролей пользователя;
- **Период неактивности пользователя до автоматической блокировки (в днях)** – количество дней, когда пользователь неактивен, по истечении которых пользователь будет автоматически заблокирован;
- **Время, за которое необходимо выводить напоминание о необходимости смены пароля** – количество дней, за которое необходимо выводить напоминание о необходимости смены пароля;
- **Число подряд идущих попыток набора неправильного пароля** – после превышения количества попыток, заданных в этом параметре, пользователь блокируется с причиной «Количество попыток»;
- **Число попыток неправильного набора пароля, при достижении которого пользователю отправляется нотификация** – количество подряд идущих попыток набора пароля, после которого пользователю будет отправлено сообщение;
- **Допустимое количество неправильных ответов на контрольный вопрос** – количество попыток ответа на контрольный вопрос, превышение которого приведет к блокировке пользователя;
- **Время действия пароля** – установка срока действия пароля в днях;
- **Время действия временного пароля** – установка срока действия временного пароля в днях;
- **Время, после окончания срока действия пароля, после которого пользователь должен быть заблокирован** – установка срока действия пароля, по истечении которого пользователь будет заблокирован автоматически; значение задается в днях;
- **Количество одновременно активных сессий пользователя**;
- **Количество неудачных попыток аутентификации пользователя**;
- **Тип пароля после сброса**;
- **Список символов, запрещенных к использованию при генерации пароля**;
- **Длина одноразового пароля**;
- **Список символов, разрешенных к использованию в одноразовом пароле**;
- **Время жизни одноразового пароля в секундах** – срок действия одноразового пароля в секундах;
- **Период времени в секундах, в течение которого повторная генерация пароля для пользователя через приложение недоступна (0 – без ограничений)**;
- **Максимальное число запросов пользователем одноразового пароля через**

приложение в час;

- **Максимальное количество неудачных попыток аутентификации пользователя по одному одноразовому паролю;**
 - **Глубина хранения истории одноразовых паролей в часах** – срок хранения истории одноразовых паролей в часах (используется время жизни одноразового пароля, если оно больше значения данного параметра);
 - **Глубина хранения истории аутентификаций в часах** – срок хранения истории аутентификации пользователя в часах (0 – история не хранится);
 - **Подсказка** – сообщение отображается, если пользователь попытался установить пароль, который не соответствует его парольной политике;
 - **Отправлять нотификацию при успешной аутентификации пользователя** – флаг отправки нотификации в случае успешной аутентификации пользователя.
3. Нажмите на кнопку **Создать** для сохранения политики или **Отменить** для отмены введенных данных.


2.8.2. Редактирование парольной политики

1. Выберите парольную политику, которую требуется изменить.
2. Нажмите на кнопку  – поля формы парольной политики станут доступными для редактирования.
3. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения политики или **Отменить** для отмены введенных данных.


2.8.3. Редактирование подсказки

Для редактирования подсказки нажмите на кнопку «...» рядом с полем **Подсказка**, откроется окно «Редактирование подсказки» с полями для заполнения подсказки на русском и английском языках. Заполнив поля, нажмите на кнопку **Сохранить**.

2.8.4. Копирование парольной политики

1. Выберите парольную политику, которую требуется скопировать.
2. Нажмите на кнопку  – поля формы парольной политики заполнятся данными выбранной политики и станут доступными для редактирования.
3. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения новой политики или **Отменить** для отмены введенных данных.

2.8.5. Удаление парольной политики

1. Выберите политику, которую необходимо удалить.
2. Нажмите на кнопку  на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.9. Работа со справочником контрольных вопросов

Для работы со справочником контрольных вопросов предназначена форма «Контрольные вопросы» (см. [Рис. 17](#)). Для перехода к форме выберите пункт меню **Справочники > Контрольные вопросы**.

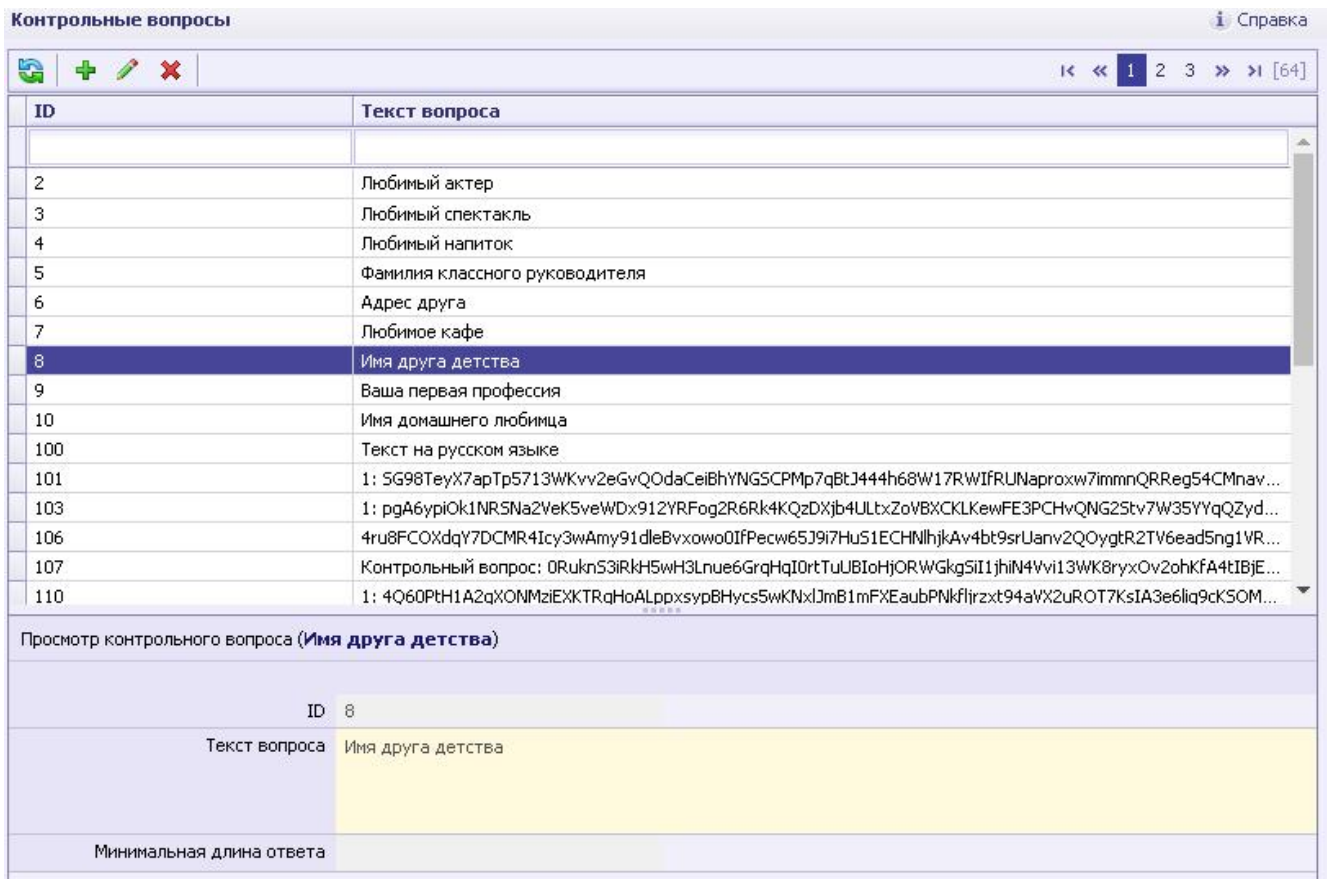




Рис. 17. Контрольные вопросы


2.9.1. Добавление контрольного вопроса

1. Нажмите на кнопку  на панели инструментов. В нижней части экрана откроется форма «Создание нового контрольного вопроса».
2. Заполните поля **Текст вопроса** и **Минимальная длина ответа** для создаваемого контрольного вопроса.
3. Нажмите на кнопку **Создать** для добавления контрольного вопроса (идентификационный номер контрольного вопроса будет присвоен автоматически) или **Отменить** для отмены введенных данных.

2.9.2. Редактирование контрольного вопроса

1. Выберите контрольный вопрос в списке.
2. Нажмите на кнопку .
3. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены изменений.

2.9.3. Удаление контрольного вопроса

1. Выберите контрольный вопрос в списке.
2. Нажмите на кнопку  на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.10. Ввод ответов на контрольные вопросы

Для работы со справочником ответов на контрольные вопросы предназначена форма «Ответ на контрольный вопрос» (см. [Рис. 18](#)). Для перехода к форме выберите пункт меню **Справочники > Ответ на контрольный вопрос**.



Рис. 18. Ответ на контрольный вопрос

Для сохранения ответа на контрольный вопрос:

1. Выберите контрольный вопрос в списке.
2. Введите значение ответа в поле **Ответ**.
3. Нажмите на кнопку **Сохранить** для сохранения изменений.

2.11. Работа со справочником типов пользователей

Работа со справочником типов пользователей осуществляется через форму «Типы пользователей» (см. [Рис. 19](#)). Для перехода к форме выберите пункт меню **Справочники > Типы пользователей**.

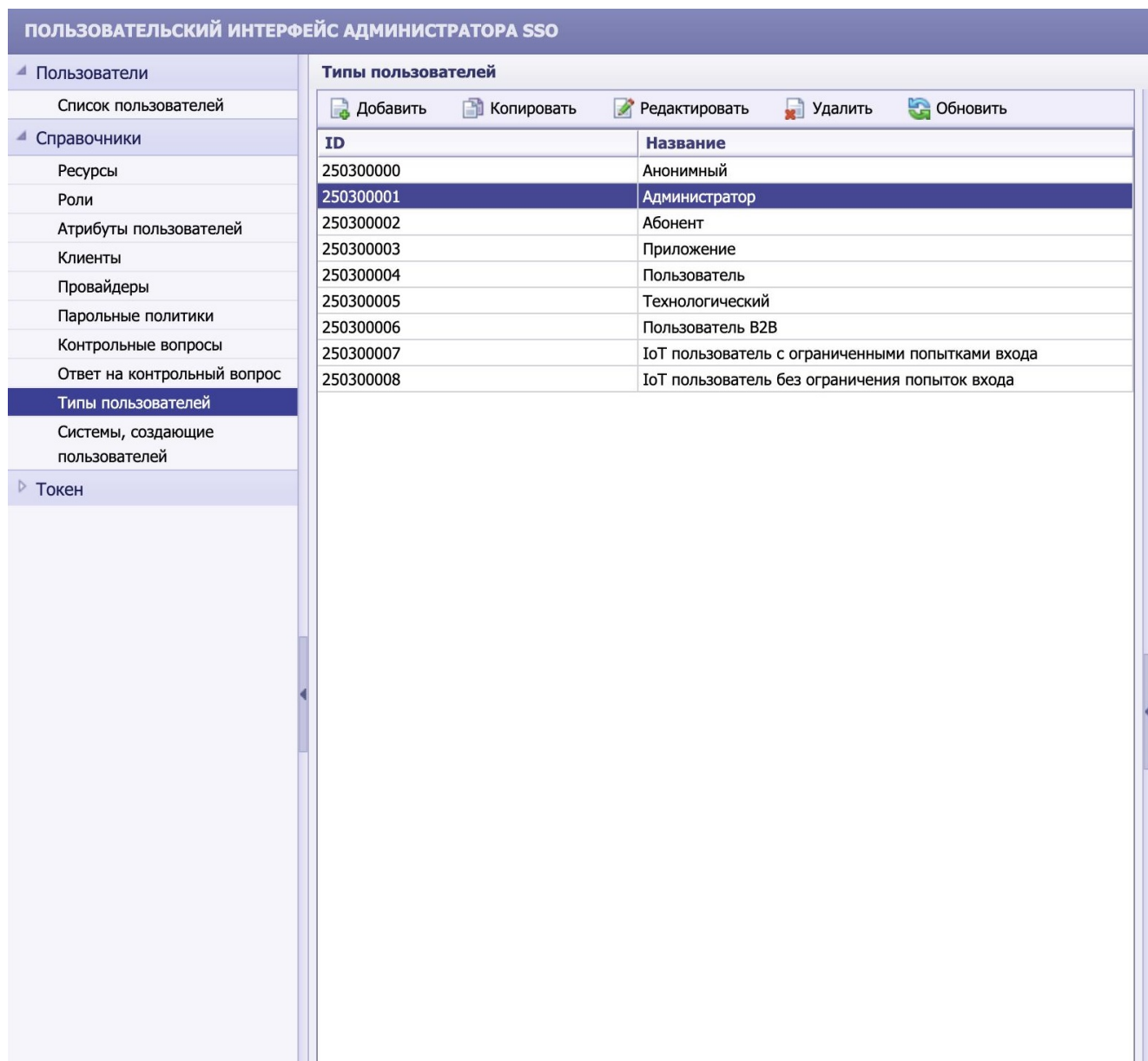





Рис. 19. Типы пользователей


2.11.1. Добавление типа пользователей

1. Нажмите на кнопку  **Добавить** на панели инструментов формы «Типы пользователей» (см. [Рис. 19](#)). В правой части экрана откроется форма «Добавление записи».
2. Заполните поля **Название**, **Краткое наименование** и **Парольная политика** для создаваемого типа пользователей.
3. Перейдите на вкладку «Роли» и задайте роли для типа пользователей. Данные роли будут назначены пользователям создаваемого типа по умолчанию. По нажатию на кнопку  **Добавить роль** для каждой площадки открывается окно «Добавление роли для площадки» (см. [Рис. 11](#)). В открывшемся окне выберите одну или несколько ролей и нажмите на кнопку **Добавить**. Выбранные роли будут назначены типу пользователей.
4. Нажмите на кнопку **Добавить** для добавления типа пользователей (идентификационный номер будет присвоен автоматически).


2.11.2. Копирование типа пользователей

1. Выберите тип пользователей в списке.
2. Нажмите на кнопку  **Копировать**. В правой части экрана откроется форма «Добавление записи» с полями, заполненными данными копируемого типа пользователей.
3. Внесите необходимые изменения в поля формы и нажмите на кнопку **Добавить** для добавления нового типа пользователей.

2.11.3. Редактирование типа пользователей

1. Выберите тип пользователей в списке.
2. Нажмите на кнопку  **Редактировать**.
3. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения изменений.

2.11.4. Удаление типа пользователей

1. Выберите тип пользователей в списке.
2. Нажмите на кнопку  **Удалить** на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.12. Работа со справочником систем, создающих пользователей

Работа со справочником систем, создающих пользователей, осуществляется через форму «Системы, создающие пользователей» (см. [Рис. 20](#)). Для перехода к форме выберите пункт меню **Справочники > Системы, создающие пользователей**.

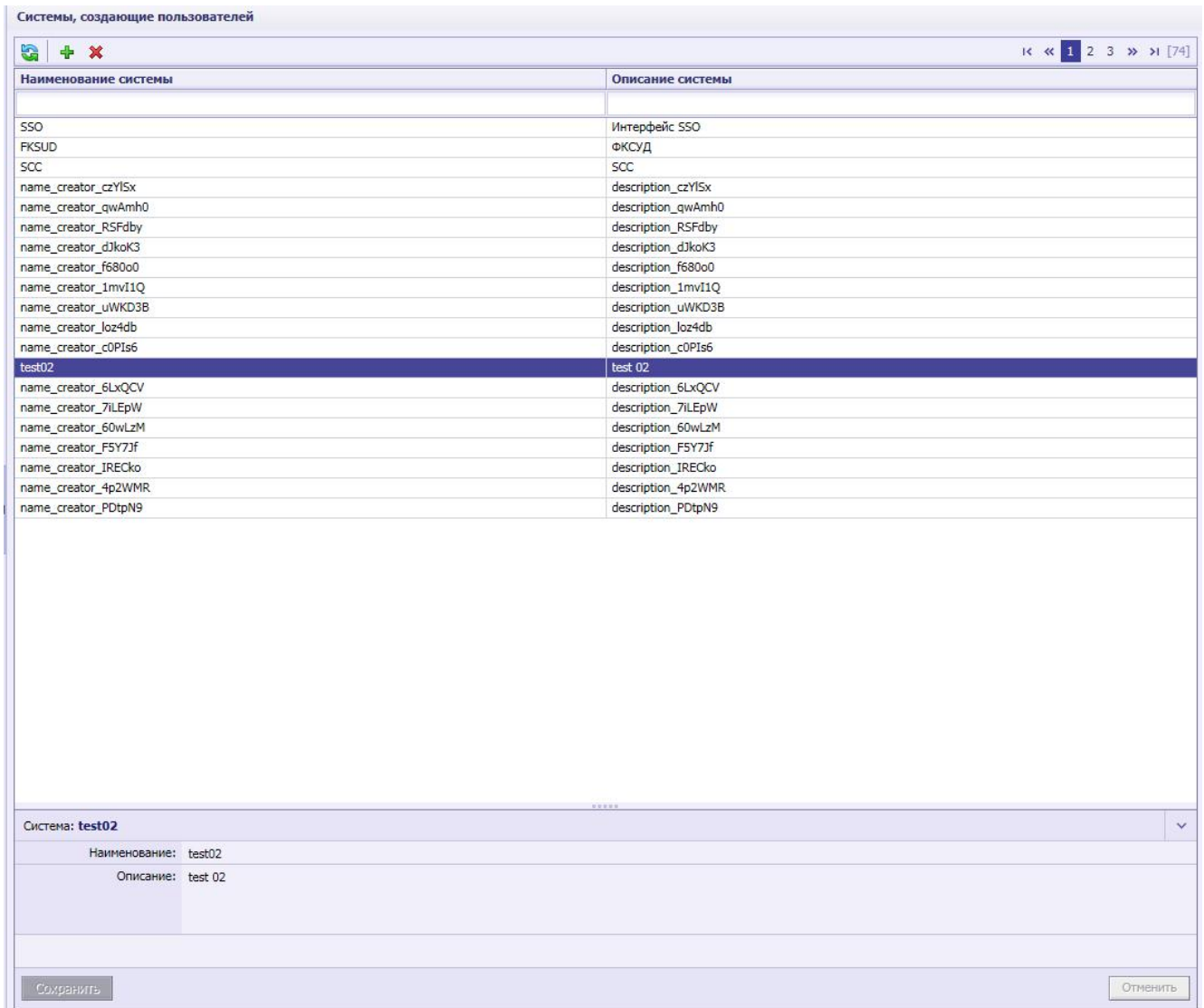




Рис. 20. Системы, создающие пользователей

2.12.1. Добавление системы, создающей пользователей

1. Нажмите на кнопку  на панели инструментов. В нижней части экрана откроется форма «Регистрация системы».
2. Заполните поля **Наименование** и **Описание** для создаваемой системы.
3. Нажмите на кнопку **Сохранить** для добавления системы или **Отменить** для отмены введенных данных.

2.12.2. Удаление системы, создающей пользователей

1. Выберите систему в списке.
2. Нажмите на кнопку  на панели инструментов. Подтвердите выполнение операции в открывшемся окне.

2.13. Работа со справочником провайдеров аутентификации

Работа со справочником внешних провайдеров аутентификации осуществляется через форму «Провайдеры аутентификации» (см. [Рис. 21](#)). Для перехода к форме выберите пункт меню **Справочники > Провайдеры аутентификации**.

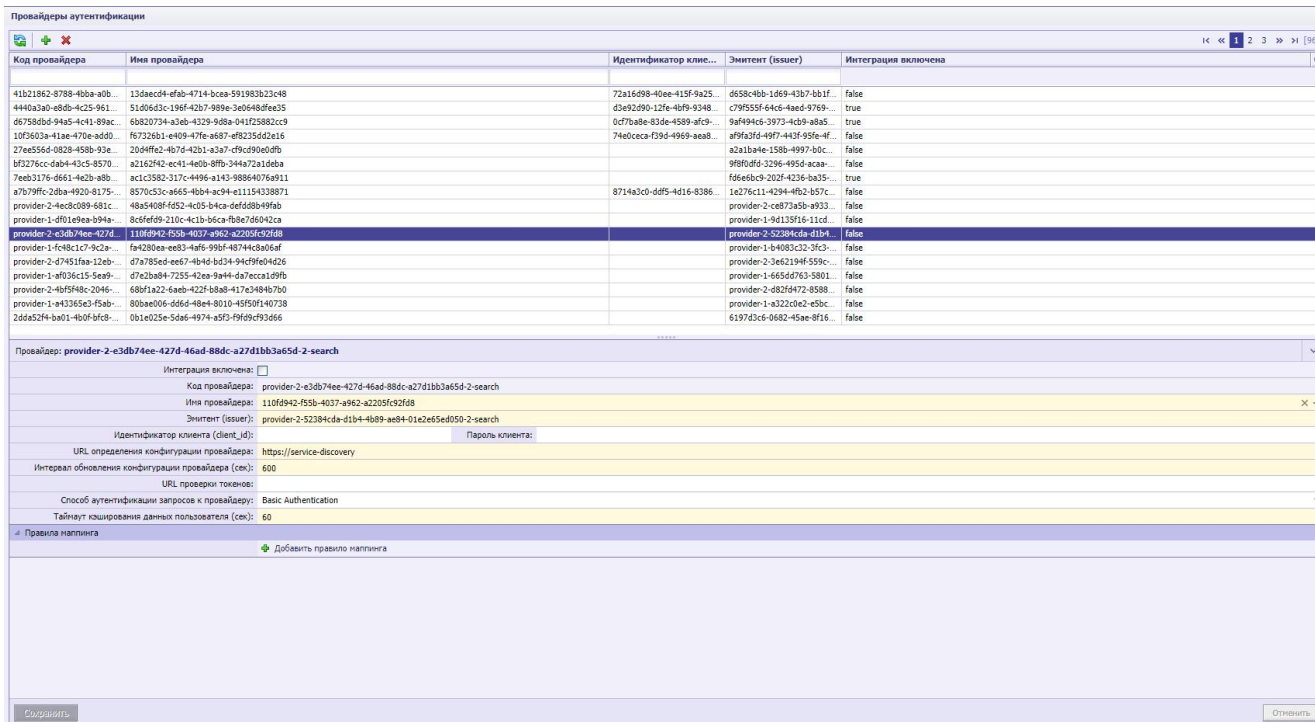



Рис. 21. Провайдеры аутентификации


2.13.1. Добавление провайдера аутентификации

1. Нажмите на кнопку  на панели инструментов формы «Провайдеры аутентификации» (см. [Рис. 21](#)). В нижней части экрана откроется форма «Новый провайдер».
2. Заполните поля формы для создаваемого провайдера.
3. Нажмите на кнопку **Создать** для сохранения изменений или **Отменить** для отмены введенных данных.

2.13.2. Редактирование провайдера аутентификации

1. Выберите провайдера в списке. В нижней части формы отобразятся данные выбранного провайдера. Область редактирования параметров провайдера аналогична виду формы «Создание провайдера» (см. подраздел «[Добавление провайдера аутентификации](#)»).
2. Внесите необходимые изменения в поля формы и нажмите на кнопку **Сохранить** для сохранения изменений или **Отменить** для отмены внесенных изменений.

2.13.3. Удаление провайдера аутентификации

1. Выберите провайдера аутентификации из списка на форме «Провайдеры аутентификации» (см. [Рис. 21](#)).
2. Нажмите на кнопку  на панели инструментов.

2.14. Работа с сессиями

Работа с сессиями пользователей осуществляется через формы «Поиск сессий» (см. [Рис. 22](#)) и «Мои сессии» (см. [Рис. 24](#)). Для перехода к форме выберите пункт меню **Сессии > Поиск сессий** или **Сессии > Мои сессии**.

2.14.1. Поиск сессий

1. Выберите в меню **Сессии > Поиск сессий**.
2. На вкладке «Поиск» формы «Поиск сессий» (см. [Рис. 22](#)):
 - введите логин в поле **Логин пользователя** (символ «*» заменяет последовательность любых символов);
 - выберите площадку в поле **Филиал**;
 - нажмите на кнопку **Найти** – откроется вкладка «Результат» (см. [Рис. 23](#)).
3. Выберите строку найденного пользователя. В нижней части формы отобразится список сессий выбранного пользователя.

Поиск сессий

Поиск Результат

Логин пользователя:

* - последовательность любых символов

Филиал: **Все**
GF
НАС
SBMS 1
dept_2
dpt100
Локальный филиал

Рис. 22. Поиск сессий, вкладка «Поиск»

Поиск сессий

Поиск Результат

UID	Логин пользователя	Тип пользователя	Парольная политика	Тип пароля	ФИО	Дата создания	Причина блокировки	Филиал
100100000000001	Admin	Администратор	Администратор	Постоянный	Administrator	13.11.2022 12:18:39	Не заблокирован	Локальный филиал


[1]

Сессия	Приложение	Тип аутентификации	Дата создания	Дата окончания действия	Дата закрытия	IP
<input type="checkbox"/> oas-40015b21-8d02-423d-ab5f-0d3401d88b18	SSO_ADM_INT	login	13.11.2022 23:57:25	14.11.2022 00:57:25		172.25.128.43
<input checked="" type="checkbox"/> oas-603e035c-b300-454f-885a-1d78deb0c704	api_gateway	password	13.11.2022 23:57:24	14.11.2022 00:57:24		172.25.128.43, 192.168.20.75

Закрывать сессии Обновить

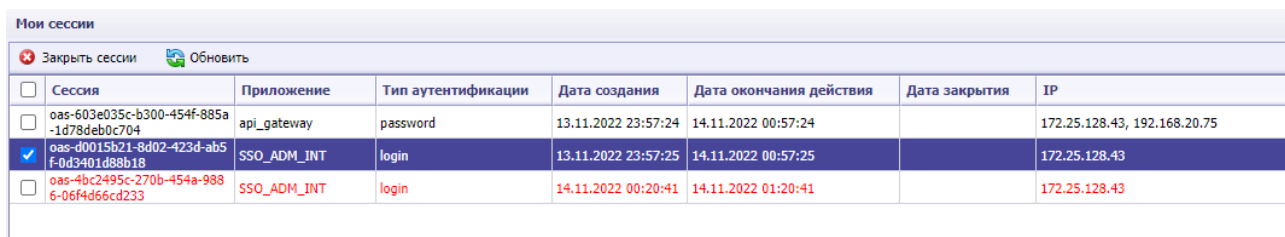
Рис. 23. Поиск сессий, вкладка «Результат»

2.14.2. Закрытие сессии

1. Проведите поиск сессии, которую нужно закрыть (см. раздел «[Поиск сессий](#)»).
2. Установите флаги в строках сессий, которые необходимо закрыть.
3. Нажмите на кнопку  **Закрыть сессии**.

2.14.3. Просмотр и закрытие сессий текущего пользователя

1. Выберите в меню **Сессии > Мои сессии**.
2. Установите флаги в строках сессий, которые необходимо закрыть (см. [Рис. 24](#)).



Сессия	Приложение	Тип аутентификации	Дата создания	Дата окончания действия	Дата закрытия	IP
<input type="checkbox"/> oas-603e035c-b300-454f-885a-1d78deb0c704	api_gateway	password	13.11.2022 23:57:24	14.11.2022 00:57:24		172.25.128.43, 192.168.20.75
<input checked="" type="checkbox"/> oas-d0015b21-8d02-423d-ab5f-0d3401d88b18	SSO_ADM_INT	login	13.11.2022 23:57:25	14.11.2022 00:57:25		172.25.128.43
<input type="checkbox"/> oas-4bc2495c-270b-454a-9886-06f4d66cd233	SSO_ADM_INT	login	14.11.2022 00:20:41	14.11.2022 01:20:41		172.25.128.43

Рис. 24. Мои сессии

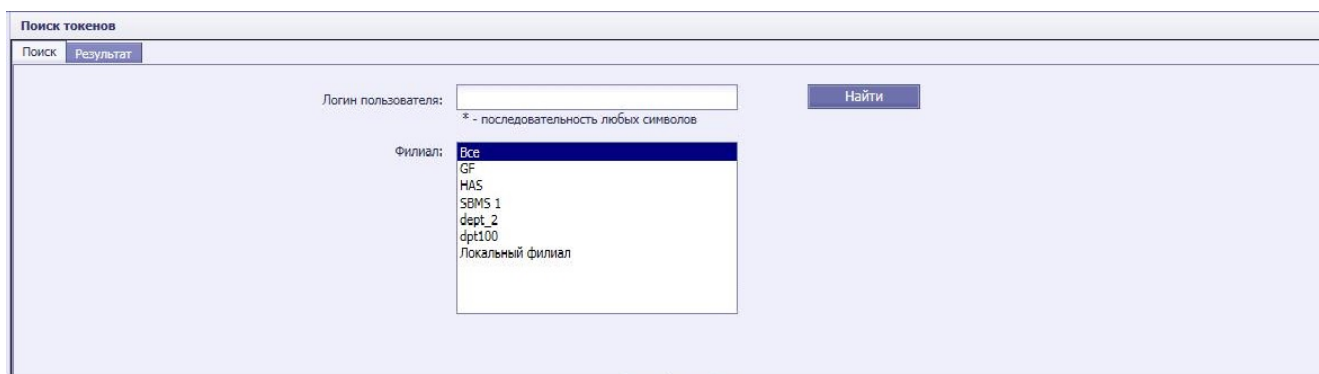
3. Нажмите на кнопку  **Закрыть сессии**.

2.15. Работа с токенами

Работа с токенами пользователей осуществляется через формы «Поиск токенов» (см. [Рис. 25](#)) и «Мои токены» (см. [Рис. 27](#)). Для перехода к форме выберите пункт меню **Сессии > Поиск токенов** или **Сессии > Мои токены**.

2.15.1. Поиск токенов

1. Выберите в меню **Сессии > Поиск токенов**.
2. На вкладке «Поиск» формы «Поиск токенов» (см. [Рис. 25](#)):
 - введите логин в поле **Логин пользователя** (символ «*» заменяет последовательность любых символов);
 - выберите площадку в поле **Филиал**;
 - нажмите на кнопку **Найти** – откроется вкладка «Результат» (см. [Рис. 26](#)).
3. Выберите строку найденного пользователя. В нижней части формы отобразится список токенов выбранного пользователя.



Поиск токенов

Поиск Результат

Логин пользователя:

* – последовательность любых символов

Филиал:

- Все
- GF
- HAS
- SBMS 1
- dept_2
- dpt100
- Локальный филиал

Рис. 25. Поиск токенов, вкладка «Поиск»

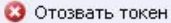
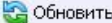


Поиск токенов								
Поиск		Результат						
UID	Логин пользователя	Тип пользователя	Парольная политика	Тип пароля	ФИО	Дата создания	Причина блокировки	Филиал
100100000000001	Admin	Администратор	Администратор	Постоянный		11.02.2019 17:45:43	Не заблокирован	Локальный филиал
[1]								
 								
<input type="checkbox"/>	Токен	Тип токена	Приложение	Дата выдачи	Дата окончания действия	Дата закрытия	IP	
<input checked="" type="checkbox"/>	LOCAL.AABbCljxKAEkxpkVskCLrnUOfXCQUuJiQY3yaIEqKpAE3asvqgNr5dA	tokens	Single Entry Point Server Application	18.02.2019 23:23:06	19.02.2019 00:23:06		172.21.97.219	

Рис. 26. Поиск токенов, вкладка «Результат»

2.15.2. Отзыв токена

1. Проведите поиск токена, который нужно отозвать (см. раздел «[Поиск токенов](#)»).
2. Установите флаги в строках токенов, которые необходимо отозвать.
3. Нажмите на кнопку  **Отозвать токен**.

2.15.3. Просмотр и отзыв токенов текущего пользователя

1. Выберите в меню **Сессии > Мои токены**.
2. Установите флаги в строках токенов, которые необходимо отозвать (см. [Рис. 27](#)).
3. Нажмите на кнопку  **Отозвать токен**.

Мои токены								
 								
<input type="checkbox"/>	Токен	Тип токена	Приложение	Дата выдачи	Дата окончания действия	Дата закрытия	IP	
<input checked="" type="checkbox"/>	LOCAL.AABbCljxKAEkxpkVskCLrnUOfXCQUuJiQY3yaIEqKpAE3asvqgNr5dA	tokens	Single Entry Point Server Application	18.02.2019 23:23:06	19.02.2019 00:23:06		172.21.97.219	

Рис. 27. Мои токены