# AccessGuide

*Выпуск 0.0.1*

**июн. 16, 2024**

## Содержание

# 1 Предисловие

## 1.1 Назначение

Руководство по администрированию полномочий пользователей в Системе `Global`.

## 1.2 Аудитория

Руководство предназначено для:

- Аналитиков Системы
- Администраторов Системы

## 1.3 Общее описание курса

В данном руководстве представлена теоретическая информация по подсистеме администрирования полномочий пользователя в Системе Global: описаны используемые объекты механизмы и отчеты Системы. Также в формате прецедентов пошагово разобран процесс настройки полномочий прав условных пользователей, по аналогии с которым возможна самостоятельная работа в Системе.

# 2 Курс для самостоятельного выполнения

Доступен курс обучения, состоящий из набора практических занятий с разобранными ответами и набора заданий для самостоятельного выполнения.

# 3 Введение, основные положения

В системе Global реализована мощная подсистема администрирования, предназначенная для разграничения пользовательского доступа к объектам и интерфейсам системы. Настройка доступа осуществляется путем настройки ролей и предоставления их конечным пользователям в приложении «Администратор».

- Каждому конечному пользователю соответствует одна учетная запись — Пользователь системы;
- Пользователю соответствует набор профилей, каждый из которых может включать в себя несколько ролей;
- Права назначаются на уровне ролей системы Global. Пользователь может получить неограниченное количество ролей, получая в результате суммарные права по всем назначенным ролям;
- Каждой роли ставится в соответствие администрируемый объекта системы и уровень доступа к нему: чтение, добавление, редактирование и удаление, либо их отсутствие;
- Имеется возможность настройки доступности операций в интерфейсах через настройку интерактивных прав;
- Для объектов, имеющих состояния, доступна настройка прав на переводы состояний;
- Доступ к специальным действиям над объектами системы осуществляется выдачей объектных прав — привилегий на конкретные действия с настраиваемым объектом.

## 3.1 Selection Debug Window

Selection Debug Window — отладочное окно, при администрировании используемое для просмотра системных кодов администрируемых объектов, в том числе и системных имен требуемых атрибутов и операций. Для его вызова необходимо выделить интересующий объект и выполнить Ctrl+Shift+Alt+W.

# 4 Пользователи

Пользователь — объект системы, определяющий права конечного пользователя, сопоставляющий учетную запись системы и физическое лицо. В карточке пользователя настраиваются параметры авторизации в системе и список профилей, определяющих права пользователя.

## 4.1 Атрибуты пользователя:

| Наименование | Описание |
|---|---|
| Учетная запись | Системное имя пользователя — логин, под которым пользователь авторизовывается в системе |
| Физическое лицо | Сопоставленное пользователю физическое лицо из справочника физлиц |
| Пользователь заблокирован | Показывает блокировку пользователя. Заблокированный пользователь не сможет зайти в систему |
| Супер-пользователь | Показывает, что пользователь имеет права супер-пользователя |
| Список приложений ограничен правами ролей | Показывает, что перечень доступных пользователю приложений определяется списком объектов, к которым пользователь имеет доступ, а не списком доступных ролям приложений. Данный признак позволяет ограничивать выбор доступных супер-пользователю приложений |
| Пользователь должен сменить пароль после авторизации | При входе в систему пользователю будет предложено сменить пароль. После смены пароля признак автоматически снимется |
| Шаблон | Шаблон, по которому создан пользователь. См. главу 2.3 (Создание пользователей по шаблону) |
| Active Directory | Данные доменной авторизации пользователя. См. главу 2.4 (Синхронизация с Active Directory) |
| Профили доступа | Список профилей, выданных пользователю. Доступно добавление новых профилей. В детализации профилей указаны входящие в них роли. Доступны операции добавления профилей пользователю или удаления имеющихся |
| Роли доступа | Список выданных пользователю ролей. На данную закладку роли попадают автоматически при выдаче пользователю их профилей |

## 4.2 Операции справочника и карточки пользователя

| Наименование | Описание |
|---|---|
| Группировка | Редактирование дерева групп пользователей: позволяет распределять пользователей по группам и редактировать дерево группировки |
| Пересчитать индексацию системных привилегий для текущего пользователя | Производит обновление индексов системных привилегий для текущего пользователя, либо для всех пользователей. В результате операции обновятся записи по всем элементам администрируемых объектов, на привилегии которых у пользователя есть права, а также записи по всем администрируемым объектам, на объектные права которых у пользователя есть права (см. 2.8 Пересчет индексации системных привилегий) |
| Анализ прав доступа пользователя | Отображает перечень всех объектов системы, показывает, какие действия над ними может производить пользователь, указывает роли, дающие данные права (см. 2.7 Анализ прав доступа пользователя) |
| Создать шаблон | Сохранение пользователя как шаблона для дальнейшего создания пользователей по его образцу (см. 2.3 Создание пользователей по шаблону) |
| Синхронизация пользователей Active Directory | Загрузка или обновление пользователей из Microsoft Active Directory (см. 2.4 Синхронизация с Active Directory) |
| Изменить пароль | Открытие модального окна для смены пароля. Требования по количеству символов в пароле или наличию спецсимволов не применяются |

## 4.3 Создание пользователей по шаблону

Для быстрого создания типовых пользователей Система предлагает сохранение карточек пользователей в качестве шаблонов. При создании нового пользователя по шаблону к нему будут применены параметры пароля и группа шаблона, также пользователю будут выданы все профили и роли шаблона. Параметры шаблона:

| Наименование | Описание |
|---|---|
| Является шаблоном | Показывает, что данная карточка является шаблоном и на ее основании будут создаваться другие пользователи |
| Наименование шаблона | Наименование шаблона, которое будет выводиться при выборе из шаблонов |
| Шаблон по умолчанию | При отметке все новые пользователи будут создаваться на основании данного шаблона. Может быть только один умолчательный шаблон |
| Выводить под операцией создания | При отметке шаблон будет отображен в выпадающем меню операции создания в списке пользователей |

## 4.4 Синхронизация с Active Directory

Система Global поддерживает синхронизацию с Microsoft Active Directory. В случае использования AD первичная загрузка и дальнейшая синхронизация пользователей осуществляется операцией «Синхронизация пользователей Active Directory» в справочнике или карточках пользователей и автоматически согласно настроенному расписанию. Если пользователя домена еще нет в системе Global, для него будет автоматически создана запись в группе LDAP - Active Directory. Если у сотрудника уже есть пользователь Global, данные о нем будут обновлены. При синхронизации для пользователя происходит попытка подстановки физ. лица по совпадению из домена.

### Настройка подключения к AD

Для настройки подключения к AD необходимо в справочнике общих настроек системы (доступном в приложении Администратор, Настройки -> Общие настройки системы) открыть настройки модуля btk и в json-контейнере для записи «ldapSync» указать URL сервера, пароль и логин для доступа, имя домена AD. Настройка авторизации через AD (т.е. с проверкой пароля пользователя не системой Global, а службой AD) производится в основном конфигурационном файле /usr/local/globalserver/application/config/global3.config.xml. Процесс описан в руководстве системного администратора.

### Синхронизация с AD

При выполнении операции «Синхронизация пользователей Active Directory» будет открыт интерфейс «Синхронизация пользователей Active Directory», в котором потребуется выбрать шаблон для создания новых пользователей и выполнить операцию «Синхронизировать». Созданные пользователи будут размещены в группе LDAP - Active Directory и подгруппах на один уровень ниже.

### 4.5 Передача прав при замещении

В случае установки замещения пользователей (Доступна в приложении Администратор, Доступ -> Замещение прав) замещающий получает дополнительно все права замещаемого пользователя. По окончании периода замещения выданные права автоматически снимаются.

### 4.6 Супер-пользователь

Супер-пользователь — администратор системы, имеющий все возможные привилегии на все объекты системы. Однако супер-пользователю не будут доступны некоторые объекты, требующие указания конкретных ролей. Например, клонируемые пункты меню для отображения виджетов доступны только пользователям, имеющим специально указанные роли. Супер-пользователь, не имеющий данных ролей, к данным меню доступа иметь не будет.

### 4.7 Пересчет индексации системных привилегий

Пользователь создается в рассинхронизированном состоянии, рассинхронизируется при назначении или изменении ролей. Чтобы настройки вступили в силу, роль необходимо синхронизировать операцией «Пересчитать индексацию системных привилегий». При настройке ролей рекомендуется сначала пересчитывать роли только для тестового пользователя операцией «Пересчитать индексацию системных привилегий для текущего пользователя», доступной в списке пользователей, карточке пользователя и в списках пользователей роли/профиля, оставляя реальных пользователей рассинхронизированными, чтобы в случае ошибки откатить нежелательные изменения.

## 5 Профили

Профили служат быстрому назначению пользователям уже готовых ролей, которые в свою очередь определяют доступ к объектам системы. Предполагается, что профили соответствуют должностям пользователей. В случае совмещения пользователем нескольких должностей или при необходимости расширения возможностей пользователя в системе возможна выдача пользователю нескольких профилей. Каждый профиль может содержать любое количество ролей.

### 5.1 Справочник профилей

Справочник профилей служит для хранения списка профилей и операций над ними. Список профилей находится в приложении Администратор, Доступ -> Профили.

### 5.2 Карточка профиля

Карточка профиля содержит основную информацию о нем, список ролей, включенных в данный профиль, список пользователей профиля. Закладки «Роли доступа» и «Пользователи» позволяют привязку и удаление ролей и пользователей соответственно.

# 6 Роли

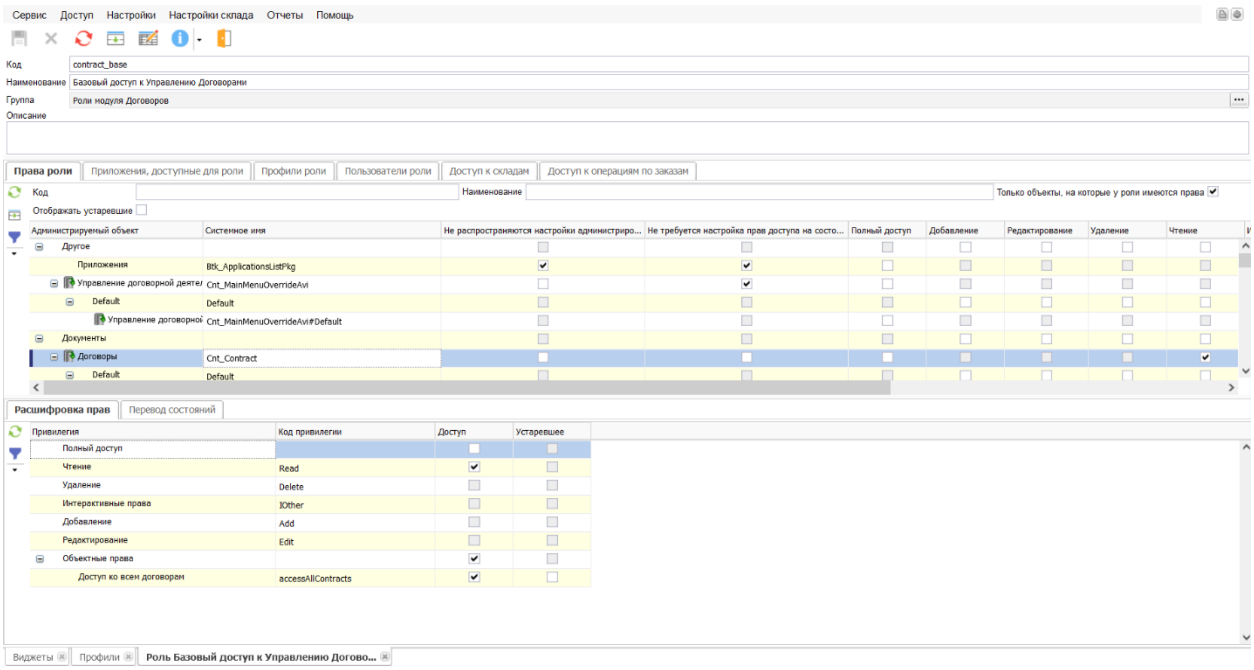
Роль является основным объектом администрирования: содержит в себе соответствия привилегий объектов системы и уровней доступа владельца роли к ним.

## 6.1 Справочник ролей

Справочник ролей служит для хранения списка ролей и операций над ними. Список ролей находится в приложении Администратор, Доступ -> Роли.

## 6.2 Права роли

«Права роли» — основная закладка карточки роли. Она содержит список администрируемых объектов и доступных пользователю роли действий с ними. Детализация администрируемых объектов — расшифровка прав — содержит список привилегий администрируемого объекта. Настройка доступа пользователя к операциям и объектам системы осуществляется отметкой доступности объектов и операций для ролей пользователя.




Атрибуты закладки «Права роли»:

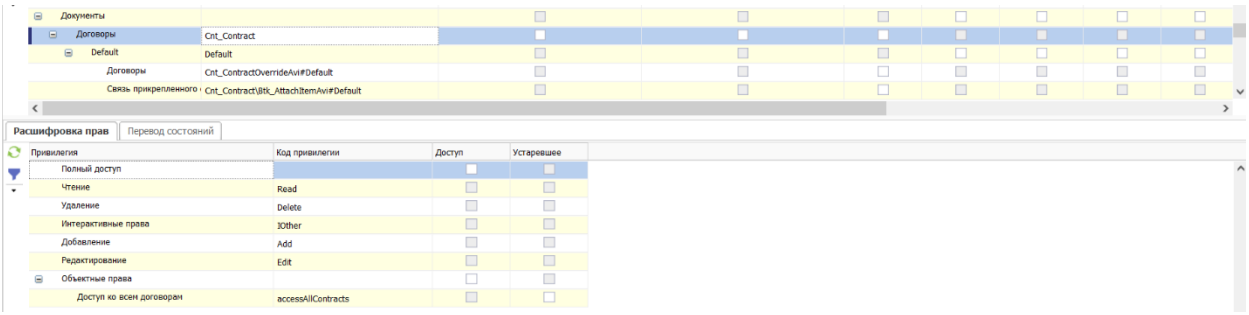
| Наименование | Описание |
|---|---|
| Администрируемый объект | Наименование администрируемого объекта |
| Системное имя | Системное имя администрируемого объекта |
| Не распространяются настройки администрирования | Означает, что на права пользователей по объекту не влияют настройки администрирования |
| Не требуется настройка прав доступа на состояния | Означает, что на права пользователей по объекту не влияют настройки прав доступа на состояния |
| Полный доступ, добавление, чтение, редактирование, удаление | Отмечает, что пользователь имеет право на соответствующее действие с самим объектом и всеми нижнеуровневыми объектами, в том числе его атрибутами |
| Интерактивные права | Отмечает, что пользователю доступны операции в карточке объекта |
| Объектные права | Обозначает наличие, частичное или полное отсутствие у пользователя объектных прав |
| Права на состояния | Обозначает, что роли выданы права хотя бы на один перевод состояний |
| Устаревшее | Обозначает, что доступа к объекту больше нет по причине его устаревания |

### Детализация администрируемого объекта

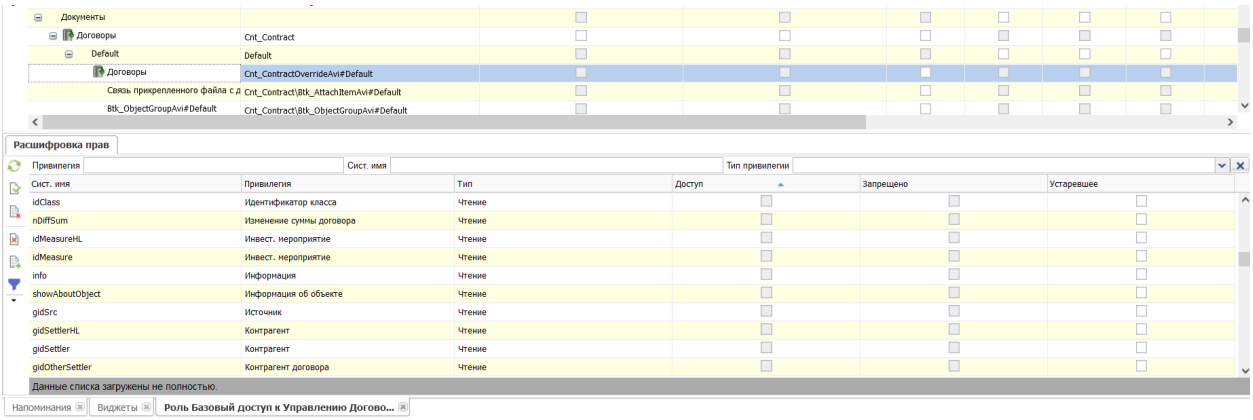
«Расшифровка прав» — закладка детализации администрируемого объекта, содержащая перечень привилегий объекта. Содержимое закладки различается в зависимости от того, открыта она для верхнеуровневого администрируемого объекта или для его элемента

- При открытии расшифровки прав для администрируемого объекта закладка содержит привилегии на Полный доступ, добавление, чтение, редактирование, удаление объектов класса. Например, в случае выдачи прав на редактирование для объекта справочника пользователи роли получат возможность редактирования объектов справочника, а также редактирования всех атрибутов всех нижнеуровневых объектов — элементов справочника.
- При открытии расшифровки прав для элемента администрируемого объекта закладка содержит перечень всех привилегий (атрибутов и операций) объекта, доступна фильтрация по наименованию и системному имени привилегий, а также отбор по типу привилегии: добавление, редактирование, удаление, чтение и интерактивные права.

Расшифровка прав для БО:




Расшифровка прав для элемента администрируемого объекта:




### Интерактивные права

Интерактивные права — операции в справочниках и карточках объектов, такие как печать, запуск процесса документооборота, подписание ЭП и пр. В случае выдачи доступа на интерактивные права для верхнеуровневого объекта администрирования пользователю будут доступны все операции во всех нижнеуровневых объектах кроме тех, у которых отмечен признак «Запрещено», так что рекомендуется отмечать доступность конкретных операций для конкретных объектов.

### Объектные права

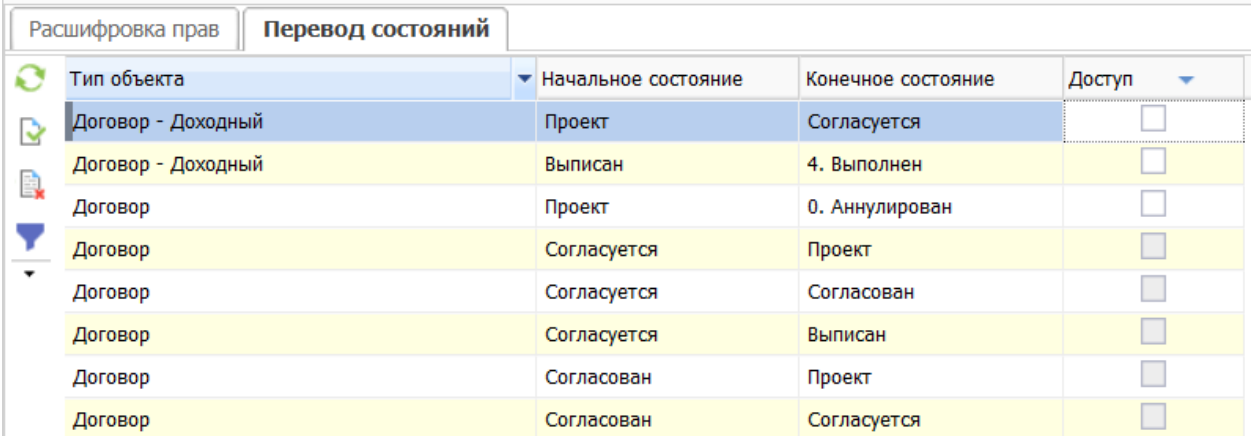
Содержат список системных привилегий — особых прав для данного объекта. Например, для договоров имеется объектное право «Доступ ко всем договорам», которое открывает владельцу возможность просмотра договоров любых ОФС. Активный признак «Не распространяются настройки администрирования» не дает доступ к объектным правам

### Ограничение дискретного доступа

Подробнее см. «Дискретный доступ»

### Перевод состояний

Закладка содержит список всех возможных переходов всех типов объектов класса, для которых отмечается признак доступности для роли.



#### Признак «Не распространяются настройки администрирования»

Признак отключает обработку всех настроек администрирования данного и всех нижнеуровневых объектов, обозначая, что у всех пользователей есть полные права на объект. Данный признак является характеристикой не роли, а самого администрируемого объекта: будучи снят при настройке одной из ролей, он автоматически снимется во всех. По умолчанию признак активен для всех объектов администрирования. После настройки и пересчета индексации должен быть снят. Переключение данного признака не требует пересчета индексации прав и вступает в силу в момент сохранения.

#### Признак «Не требуется настройка прав на состояния»

Отмеченный признак дает доступ к любым переходам между состояниями объектов класса. Для настройки переходов требуется для типа объекта задать возможные переходы, затем на закладке «Перевод состояний» детализации класса выдать права на доступные переходы. Аналогично предыдущему признак является характеристикой самого администрируемого объекта и потому одинаков для всех ролей, по умолчанию установлен для всех объектов и после настройки прав на переводы состояний и пересчета индексации должен быть снят.

### 6.3 Приложения, доступные для роли

Закладка содержит список приложений системы и позволяет обозначать, к каким приложениям пользователь роли получит доступ . Детализация содержит список пунктов меню приложения.

### 6.4 Профили роли

Закладка содержит список профилей, включающих в себя данную роль. Доступны операции включения роли в профили и удаления из них, открытия карточек профилей.

### 6.5 Пользователи роли

Закладка содержит список пользователей, обладающих данной ролью. Роли выдаются пользователям не напрямую, а через профили так что данная закладка нередактируема. Содержимое закладки обновляется при изменении профилей роли или при изменении профилей пользователей. Для каждого пользователя указано, от какого профиля он получил данную роль. Доступна операция «Пересчитать индексацию системных привилегий для данного пользователя», удобная при тестировании изменений в настройках доступа на конкретных тестовых пользователях.

## 7 Дискретный доступ

Описанные в предыдущих уроках настройки доступа применяются ко всем объектам справочников (и их атрибутам): например, пользователю либо доступны абсолютно все договора, либо недоступны никакие. Функционал дискретного доступа позволяет настраивать доступ пользователя к объектам справочников (и их атрибутам) в зависимости от значений атрибутов этих объектов, к примеру, настроить доступ пользователя к редактированию договоров только своего подразделения. Ограничения дискретного доступа применяются перед отображением списков, так что при открытии, например, перечня договоров, пользователь увидит только те договоры, правом на чтение которых он обладает.

## 7.1 Администрируемые объекты

Справочник администрируемых объектов содержит перечень объектов администрирования системы (бизнес-объектов) с детализацией по элементам администрируемого объекта. В карточке администрируемого объекта настраиваются дискретные ограничения доступа.

## 7.2 Скрипты дискретного доступа

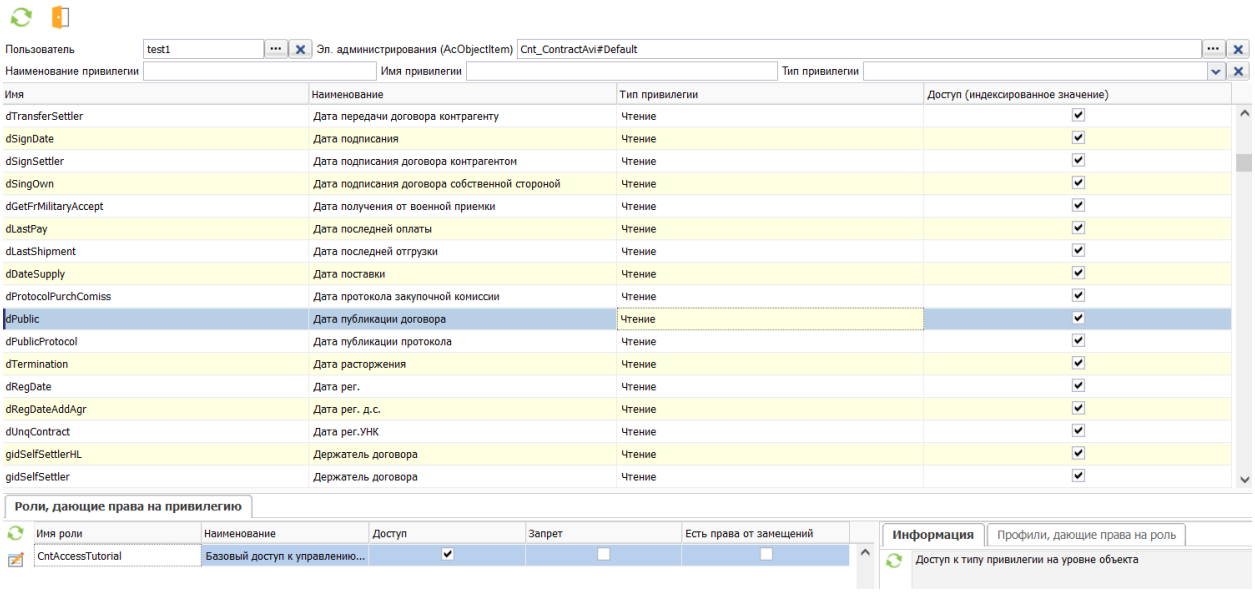
При настройке дискретного доступа используется два вида скриптов:

- Скрипт для фильтрации объектных привилегий: отвечает за фильтрацию объектов в списках. В примере данного урока — скрывает из реестра договоры других типов и ОФС;
- Скрипт проверки строк по объектному кешу: блокирует возможность открытия недоступных договоров по ссылке из прочих документов, например, запрещает пользователю открыть карточку недоступного договора из лота.

# 8 Отчеты

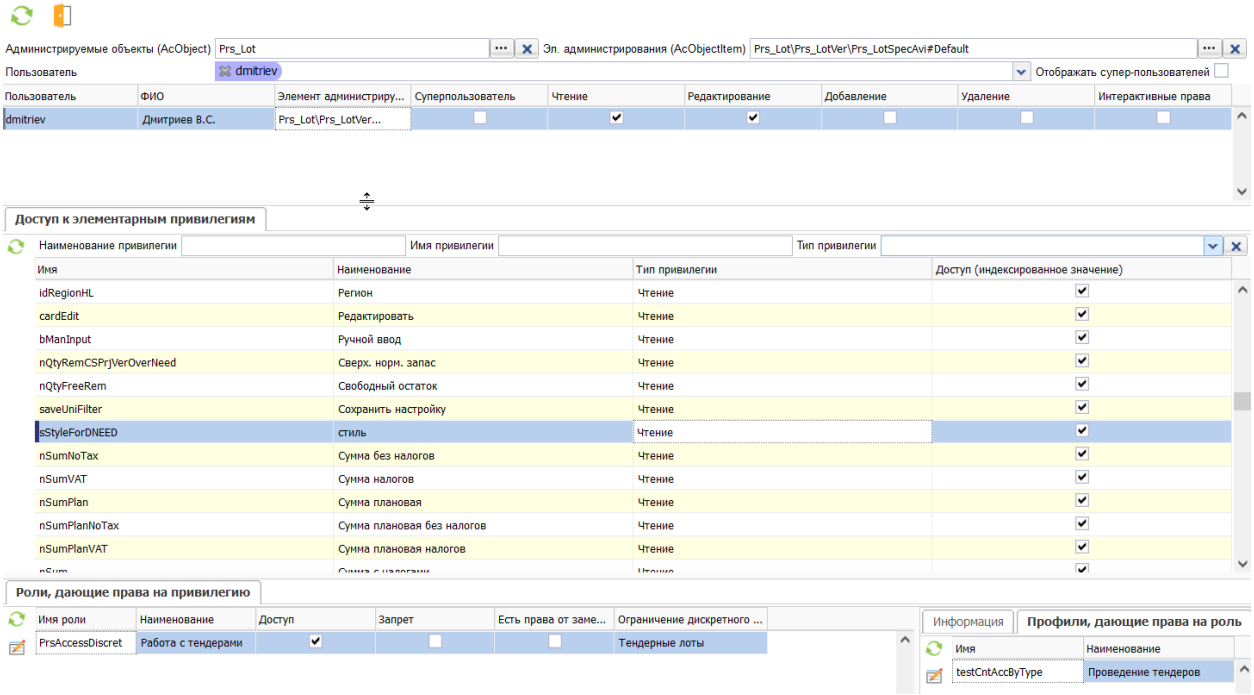
## 8.1 Анализ доступа к элементарным привилегиям

Отчет «Анализ доступа к элементарным привилегиям» позволяет просматривать источники прав доступа пользователя к элементарным привилегиям выбранного администрируемого объекта. Доступен также режим работы без указания пользователя: в таком случае будет отражена информация о всех ролях Системы, имеющих доступ к выбранной привилегии.



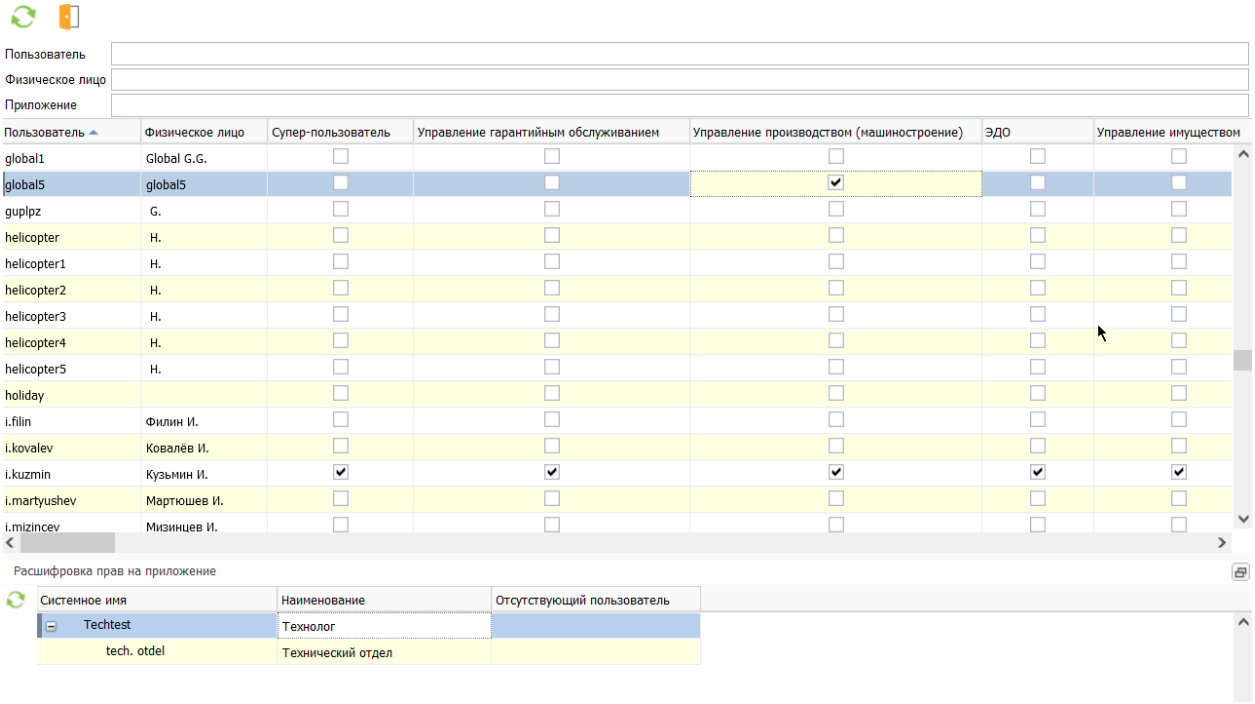
## 8.2 Анализ доступа к бизнес-объектам

Отчет «Анализ доступа к бизнес-объектам» позволяет, указав интересующий администрируемый объект, просмотреть информацию о доступности привилегий указанного администрируемого объекта в детализации по пользователям.



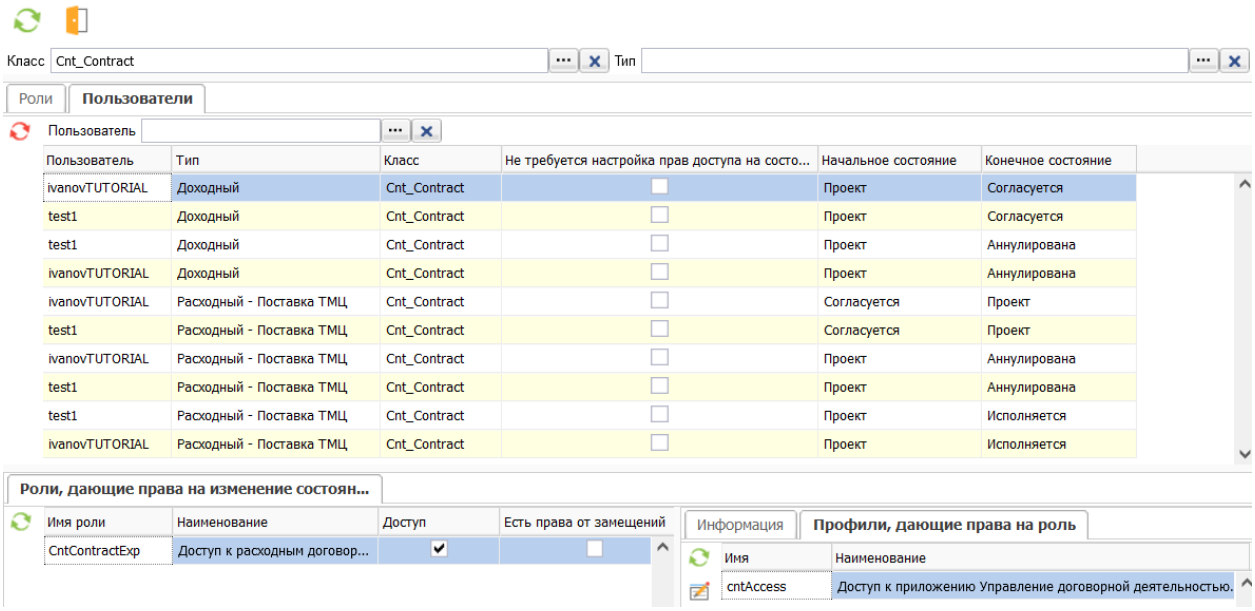

## 8.3 Анализ доступа пользователей к приложениям

Отчет отображает перечень приложений (рабочих столов пользователей), к которым выбранные пользователи имеют доступ. При этом для каждого приложения выводится информация об источнике прав для выбранного пользователя: какие профиль и роль, либо замещение какого сотрудника дают пользователю права на приложение.



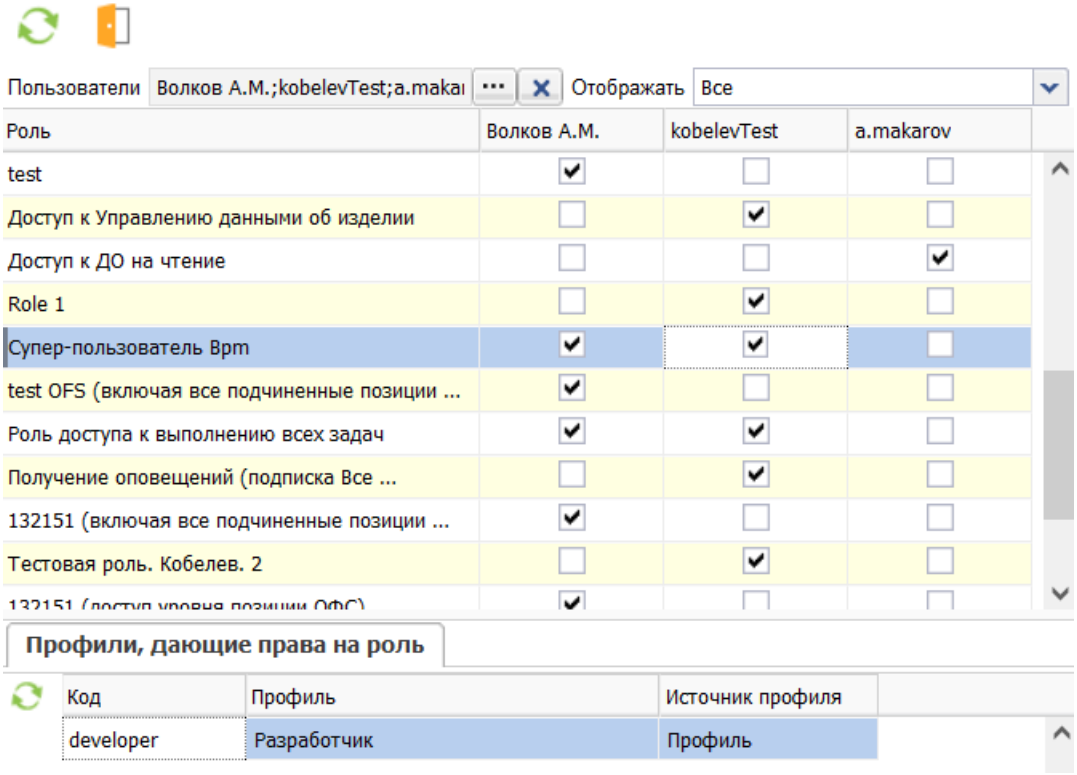

## 8.4 Анализ доступа к изменению состояния пользователем

Отчет отображает информацию обо всех переходах состояний (изменений одного состояния на другое состояние), доступных для объектов выбранного типа. Отчет содержит две закладки, представляющие информацию о правах ролей на переходы состояний и о правах пользователей на переходы состояний.



## 8.5 Отчет по сравнению ролей пользователей

Отчет позволяет производить наглядное сравнение наличия ролей у нескольких пользователей. Столбцы соответствуют добавленным в отчет пользователям, а строки — их ролям. По умолчанию в отчете отображаются все роли, доступные хотя бы одному из выбранных пользователей. Доступны режимы отображения только совпадающих, либо только различающихся ролей. В детализации каждой ячейки отчета указывается источник роли для этого пользователя.




## 8.6 Отчет по сравнению прав пользователей

Отчет позволяет сравнивать права доступа нескольких выбранных пользователей по администрируемым объектам и привилегиям Системы. Для работы с отчетом необходимо в поле «Пользователи» выбрать интересующие учетные записи. По необходимости выбрать требуемый БО и привилегию, выбрать режим сравнения прав: все/совпадающие/различающиеся.

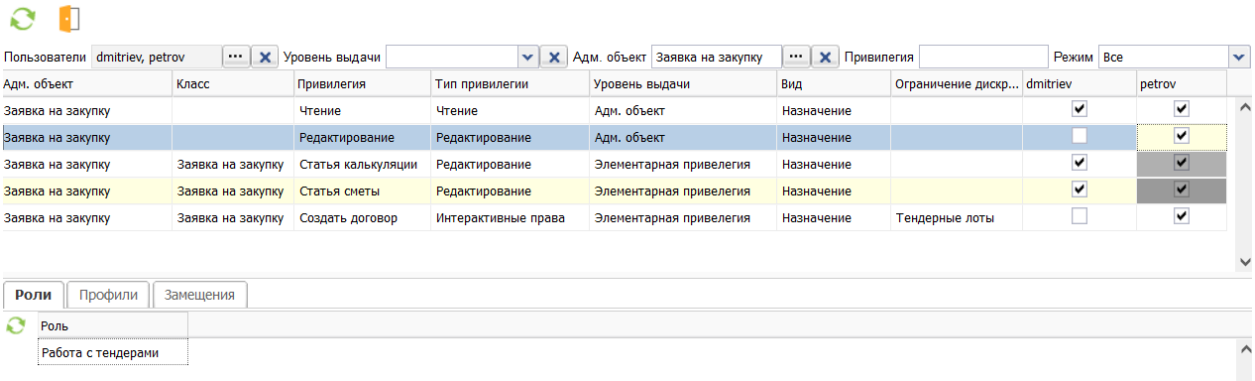


Рисунок иллюстрирует отчет, построенный для пользователей dmitriev и petrov по бизнес-объекту «Заявка на закупку», ниже приведен построчный анализ данного отчета.

| № строки | Анализ |
|---|---|
| 1 | На уровне администрируемого объекта обоим пользователям дано право на чтение всех атрибутов всех классов бизнес-объекта «Заявка на закупку» |
| 2 | На уровне администрируемого объекта пользователю petrov дано право на редактирование всех атрибутов всех классов этого бизнес-объекта |
| 3, 4 | На уровне элементарных привилегий пользователю dmitriev дан доступ на редактирование атрибутов «Статья калькуляции» и «Статья сметы». Пользователь petrov также имеет право на редактирование этих атрибутов, но для него такое право выдано не к конкретным привилегиям напрямую, а унаследовано с уровня бизнес-объекта, что обозначено серой заливкой |
| 5 | Пользователю petrov дано право на выполнение операции «Создать договор от закупки», но только с ограничением дискретного доступа «Тендерные лоты» |

В данном примере выделена ячейка, в которой отмечен признак права пользователя petrov на редактирование БО «Заявка на закупку». Детализация содержит информацию об источниках такого права: ролях и профилях, либо о том, что пользователь замещает сотрудника, имеющего соответствующие права.

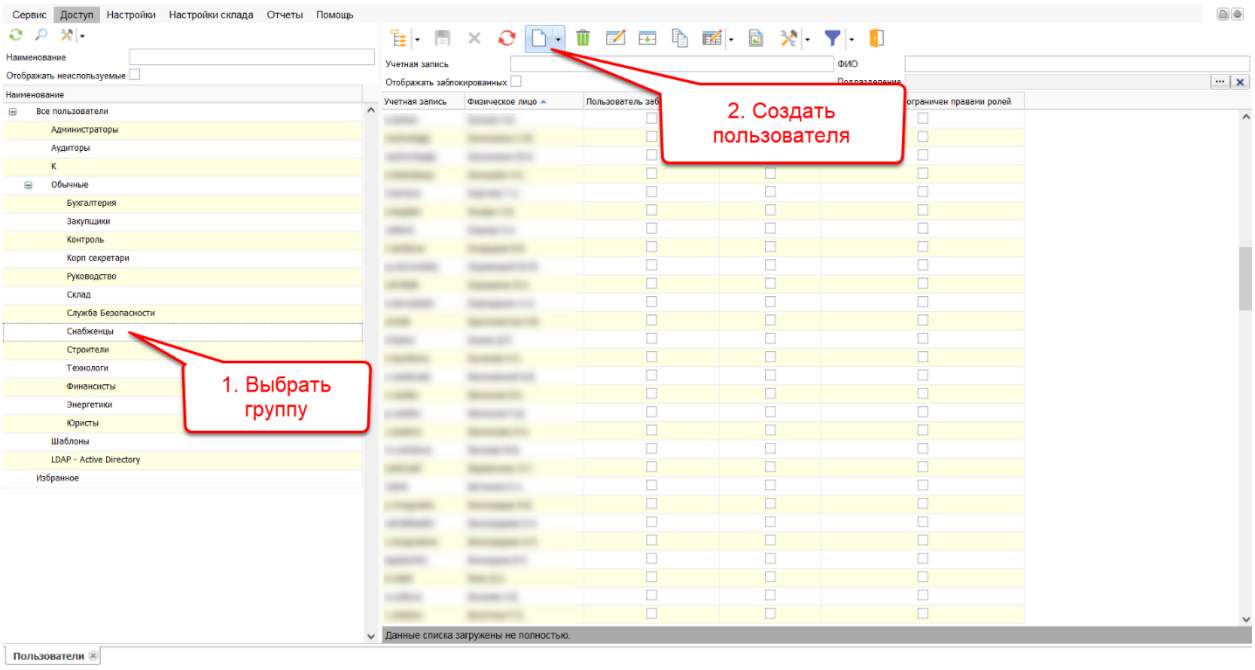
Дополнительная информация по отчету:

- Колонка «Вид» может принимать два значения: Назначение и Запрет. Запрет пишется в случае, если для одного из добавленных пользователей отмечен запрет привилегии. Ячейка привилегии для этого пользователя будет выделена красным цветом.
- Неинформативные строки отчета не отображаются: если всем добавленным пользователям права выданы на одном из верхних уровней (БО или классе БО) и нет запретов, строки нижних уровней скрываются. Поэтому в данном примере не отражена информация о праве добавленных в отчет пользователей на чтение конкретных атрибутов.

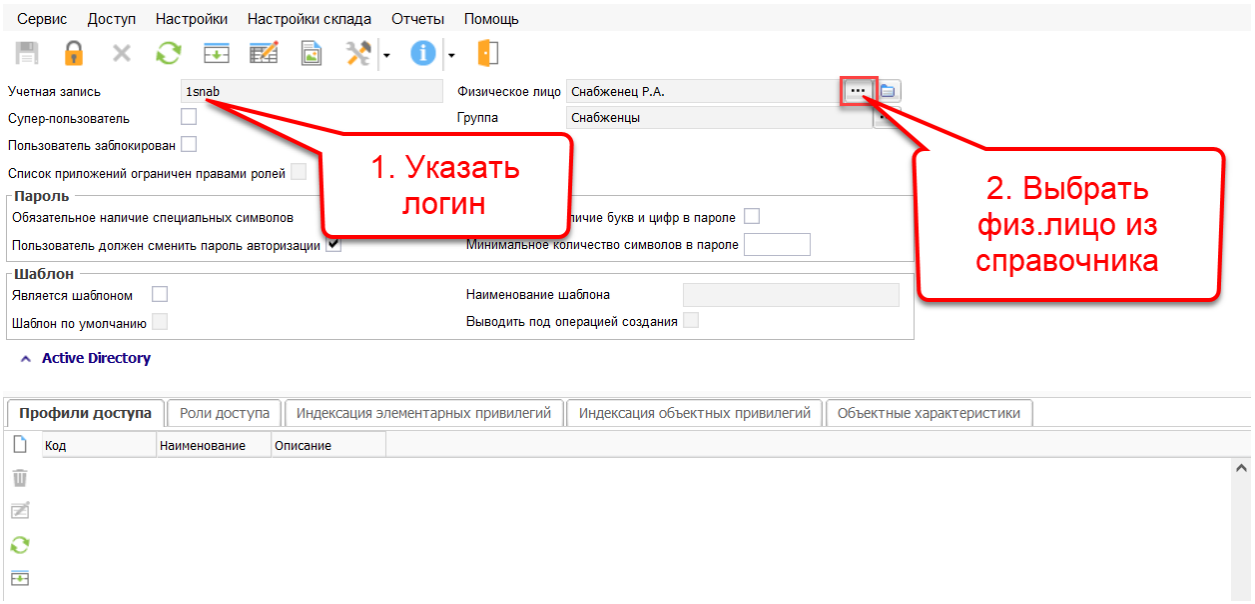
# 9 Прецедент создания пользователей

Цель: создать учетные записи, через которые пользователи смогут авторизоваться в системе.

- В справочнике пользователей выделить группу, в которой будет создана запись пользователя, выполнить операцию создания.




- В открывшейся карточке заполнить поле «Учетная запись» — это логин, под которым будет авторизовываться пользователь. При создании пароль устанавливается равным логину, доступно его редактирование. Выбрать Физическое лицо из справочника.

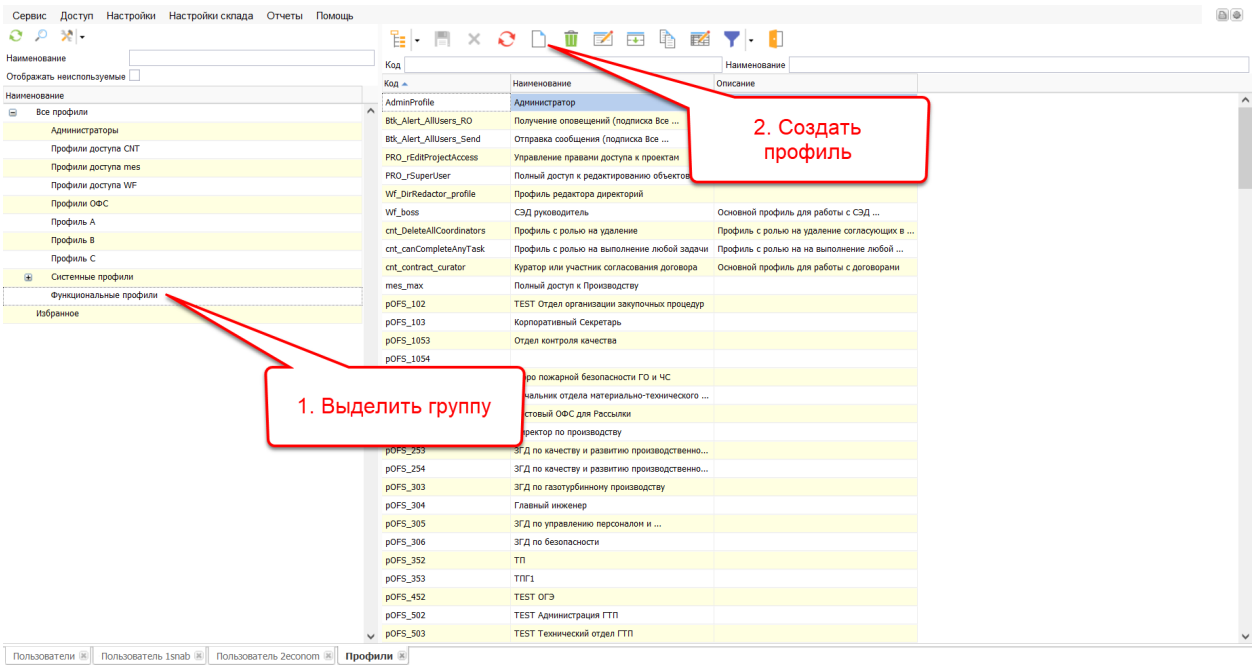


# 10 Прецедент настройки доступа к приложениям

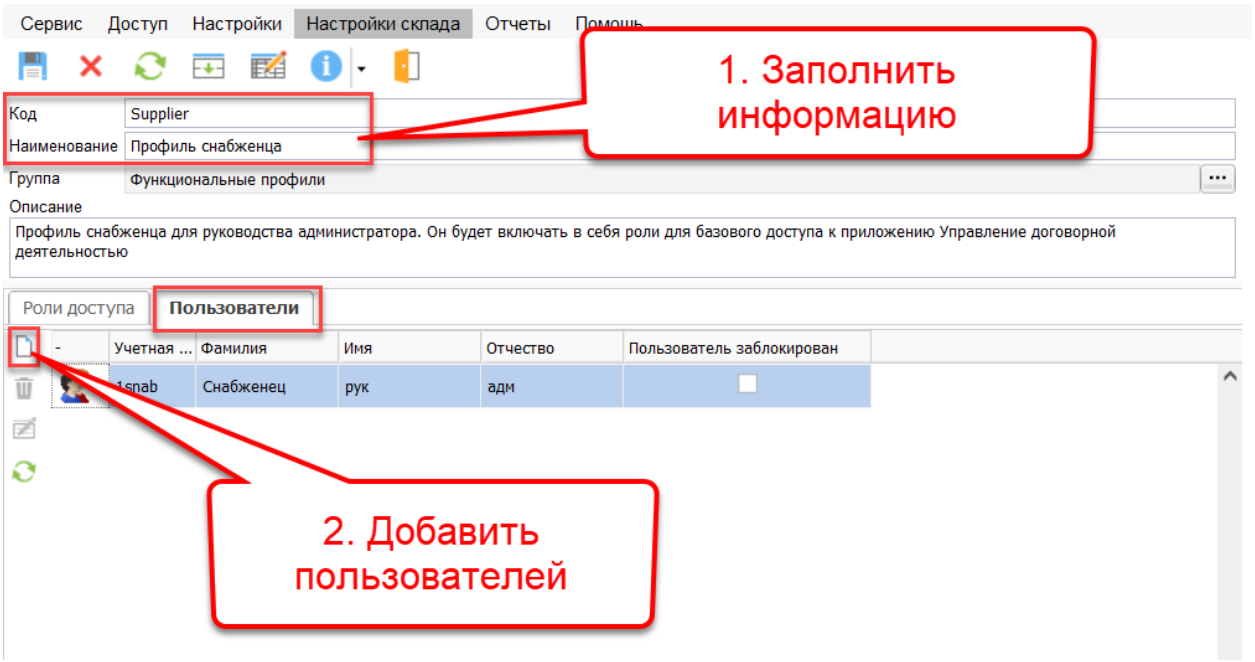
Цель: дать обоим пользователям доступ к приложению «Управление договорной деятельностью», причем Экономисту выдать права на меню Отчеты, а Снабженцу — нет. Для обоих пользователей скрыть меню «Настройка».

Так как потребуется различная настройка для двух пользователей, потребуется создать и настроить два профиля: профиль «Снабженец» и профиль «Экономист».

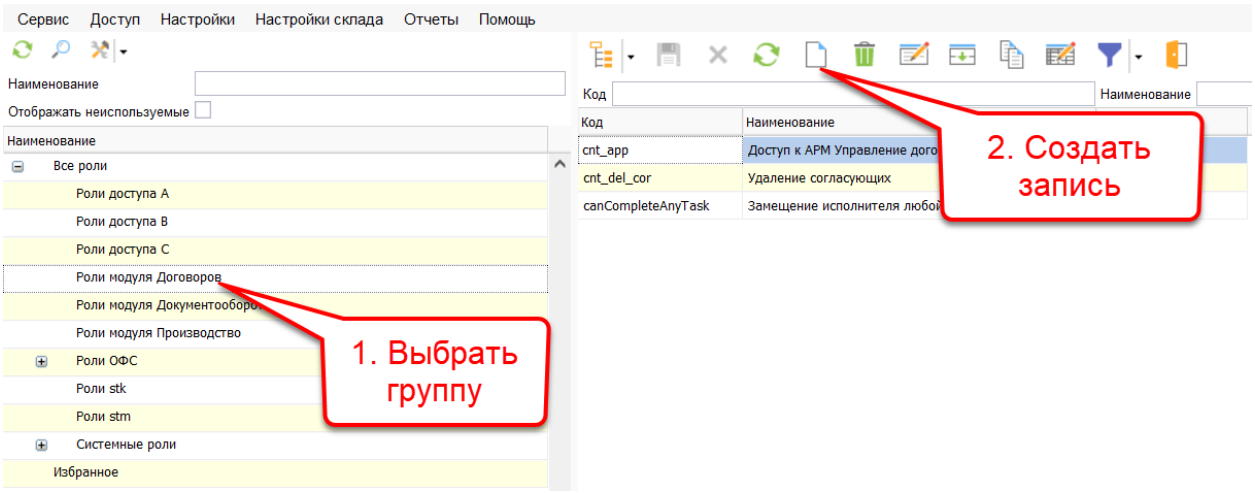
- В справочнике профилей выбрать группу, к которой будет отнесен профиль и выполнить операцию создания.



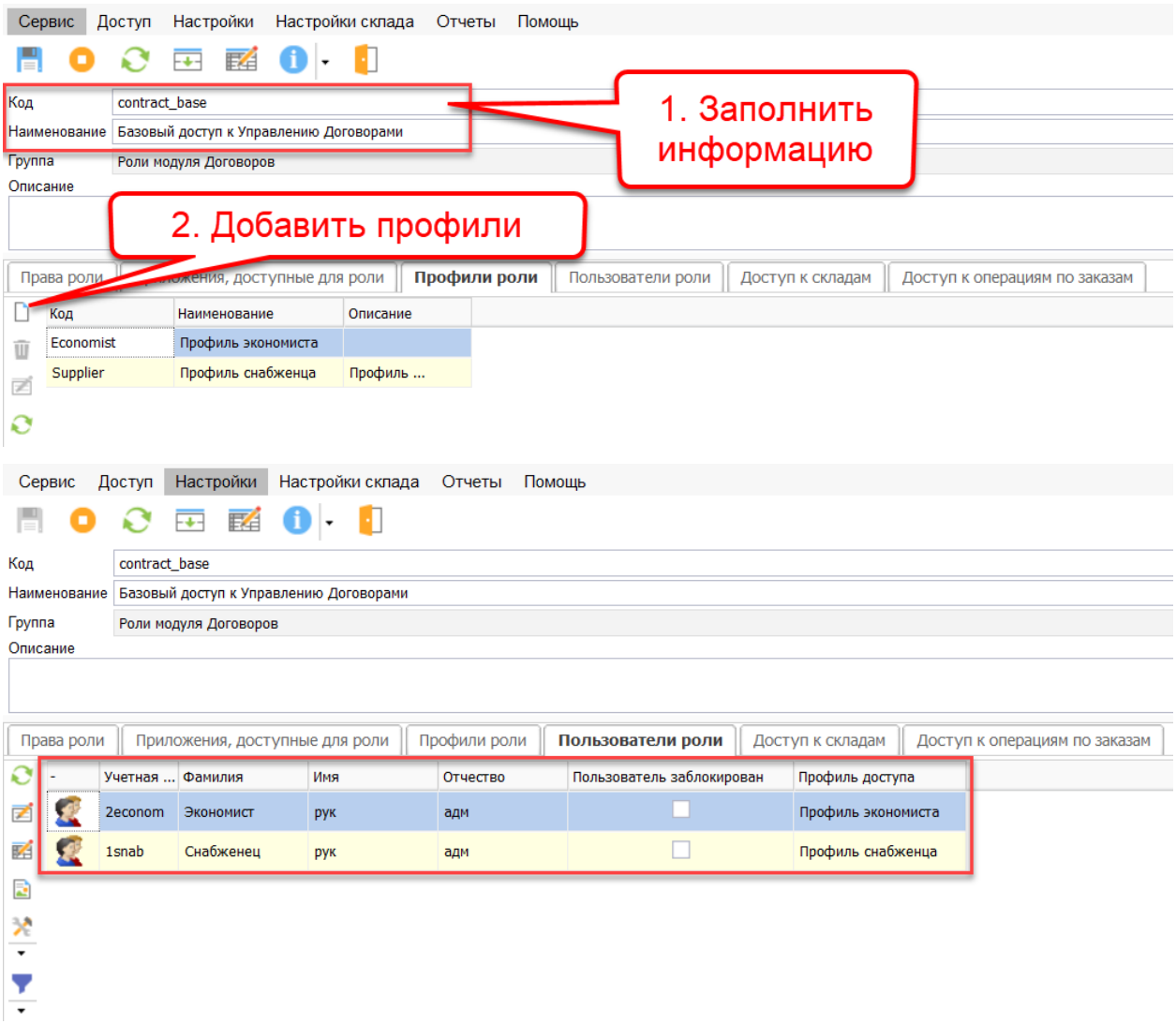

- В созданной карточке указать код и наименование, на закладке «Пользователи» добавить пользователей профиля. Аналогичным образом создать Профиль Экономиста и добавить пользователей.



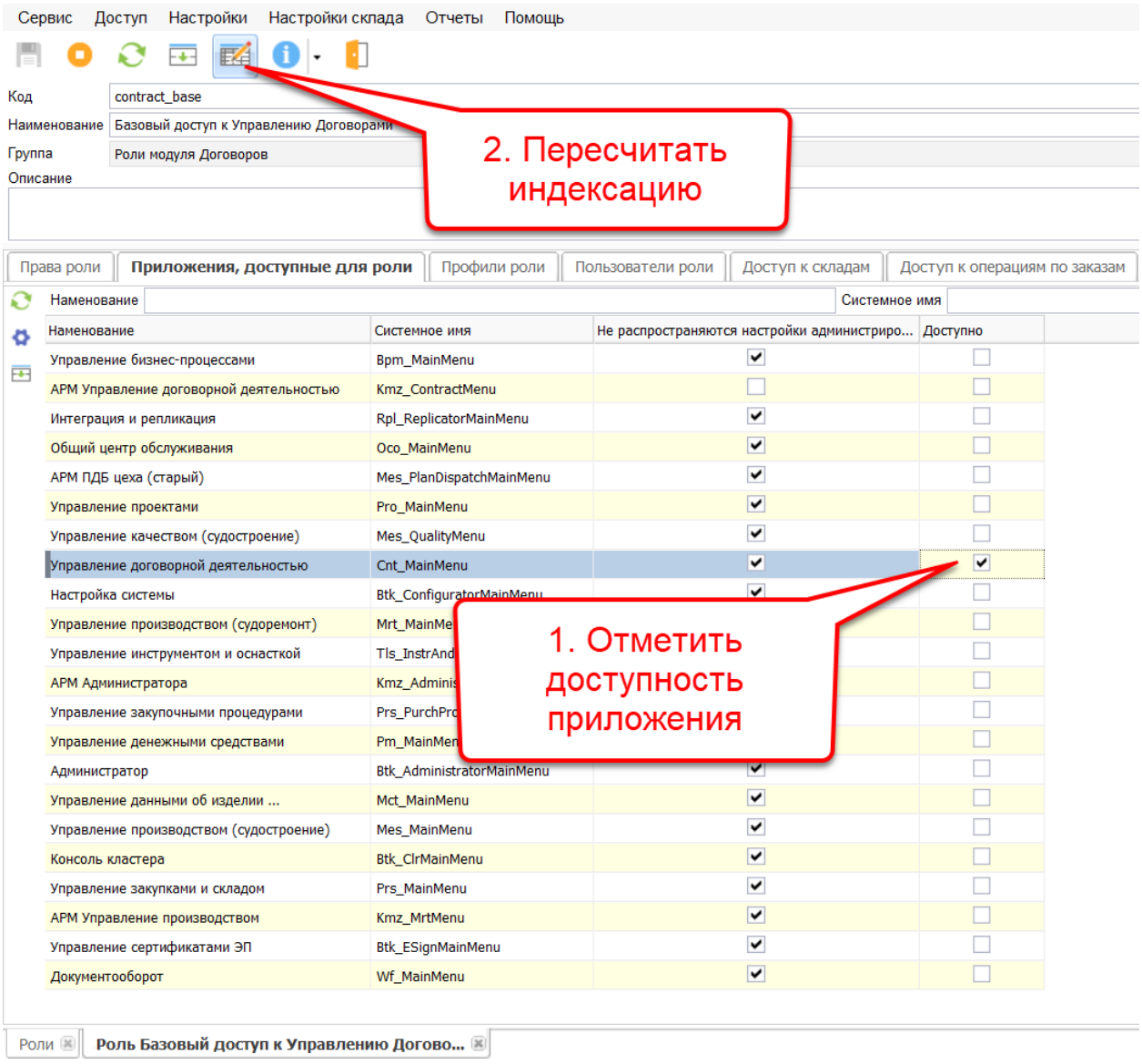

- В нужной группе справочника ролей создать новую роль.



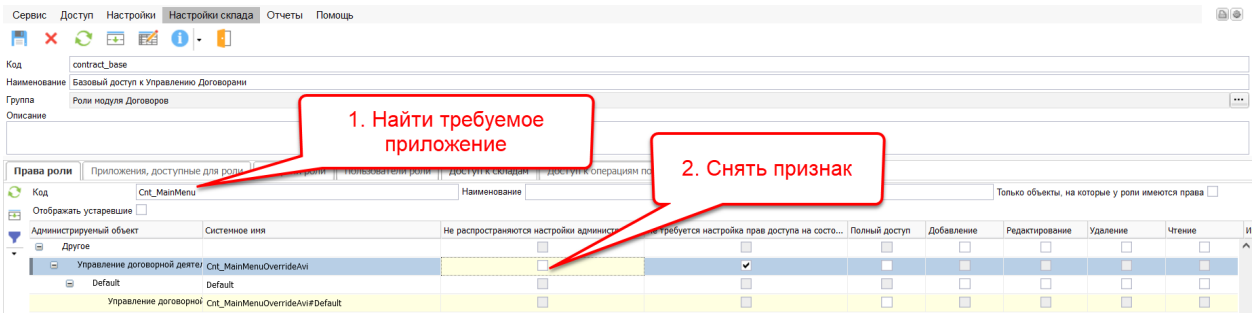

- В открывшейся карточке роли указать код и наименование, на закладке «Профили роли» выбрать ранее созданные профили Экономиста и Снабженца. На закладке «Пользователи роли» автоматически будут указаны все пользователи, обладающие хотя бы одним из добавленных профилей.




- На закладке «Приложения, доступные для роли» отметить доступность приложения «Управление договорной деятельностью», после чего выполнить операцию «Пересчитать индексацию системных привилегий для всех пользователей роли».

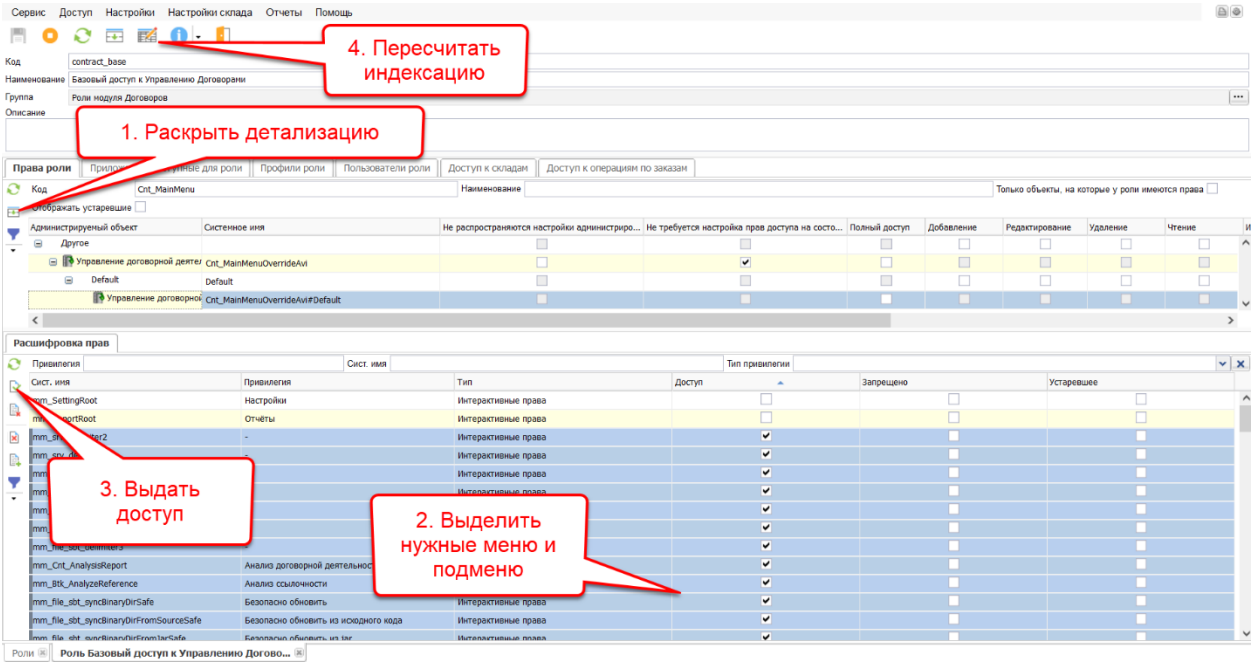



- Требуется детально настроить права на приложение, а именно скрыть у обоих пользователей меню «Настройки» и меню «Отчеты» у Снабженца. Для этого необходимо на закладке «Права роли» найти нужное приложение по коду (узнать его можно на закладке «Приложения, доступные для роли») и снять признак «Не распространяются настройки администрирования», сохранить изменения. После авторизации пользователям не будет доступно ни одно меню приложения.

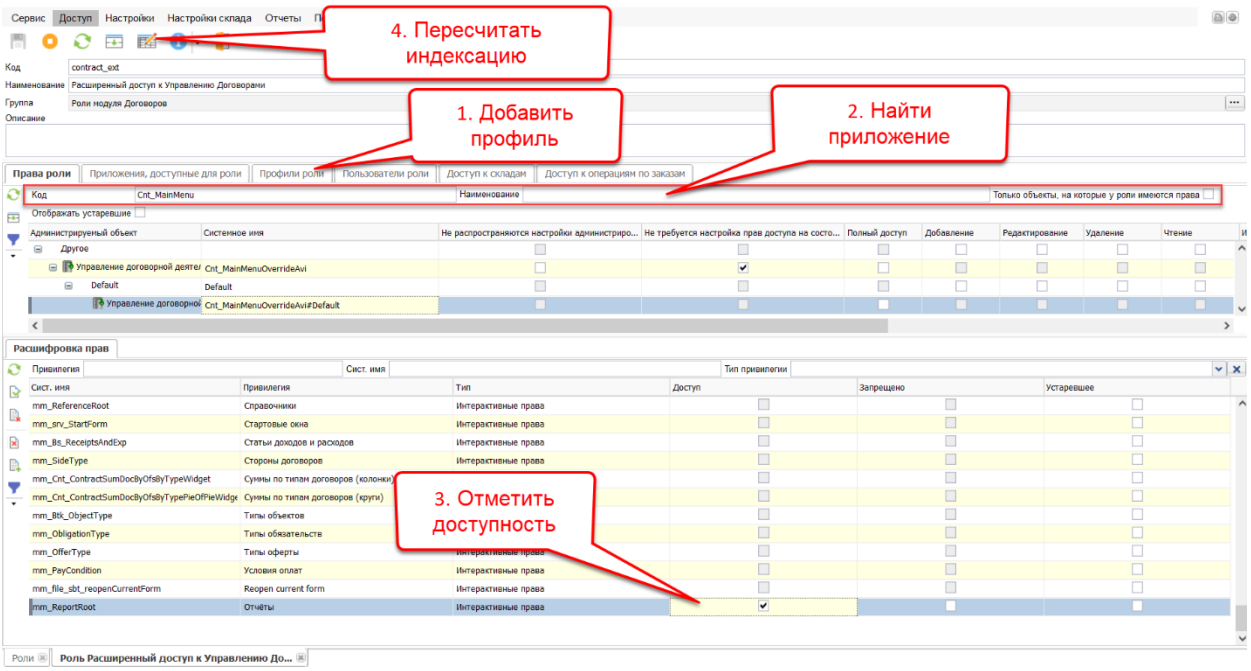



- Требуется выдать пользователям права на нужные пункты меню. Для этого необходимо на за-

кладке «Права роли» открыть детализацию и отметить признак «Доступ» для тех пунктов меню, с которыми будут работать пользователи данной роли. Также удобно это сделать, выделив все позиции комбинацией ctrl+A, выдав доступ ко всем позициям, а затем сняв признак «Доступ» с тех, к которым выдавать доступ не требуется. Затем следует пересчитать индексацию системных привилегий. В данном случае для роли «Базовый доступ к управлению Договорами» выдан доступ ко всем пунктам меню кроме Настроек и Отчетов, так что при входе в систему пользователю роли будут доступны все меню кроме указанных (и их подменю).



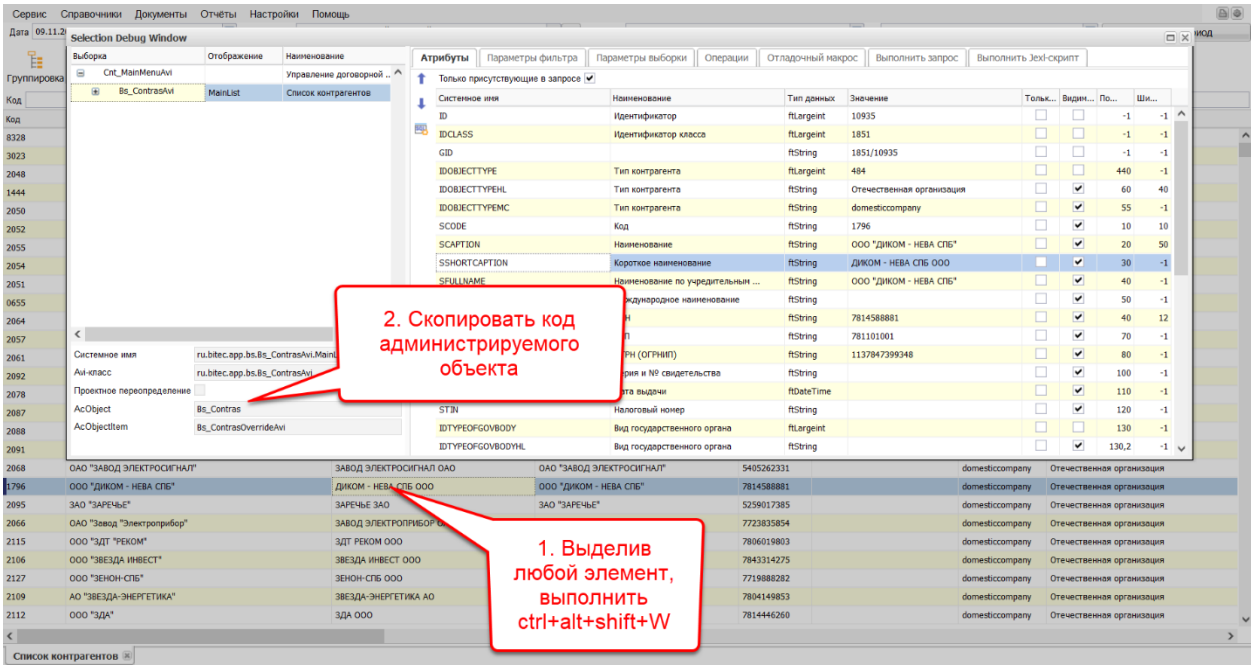

- Необходимо выдать доступ к меню «Отчеты» экономисту. Для этого требуется создать еще одну роль и выдать ее только Профилю Экономиста (соответственно на закладке Пользователи роли будут только пользователи, владеющие Профилем Экономиста). В списке прав роли найти нужное приложение, сняв признак «Только объекты, на которые у роли имеются права». В детализации отметить доступность меню «Отчеты», пересчитать индексацию. При авторизации экономист, обладающий как базовой ролью доступа, так и расширенной, будет иметь доступ к тем пунктам меню, к которым имеет доступ хотя бы одна из его ролей.



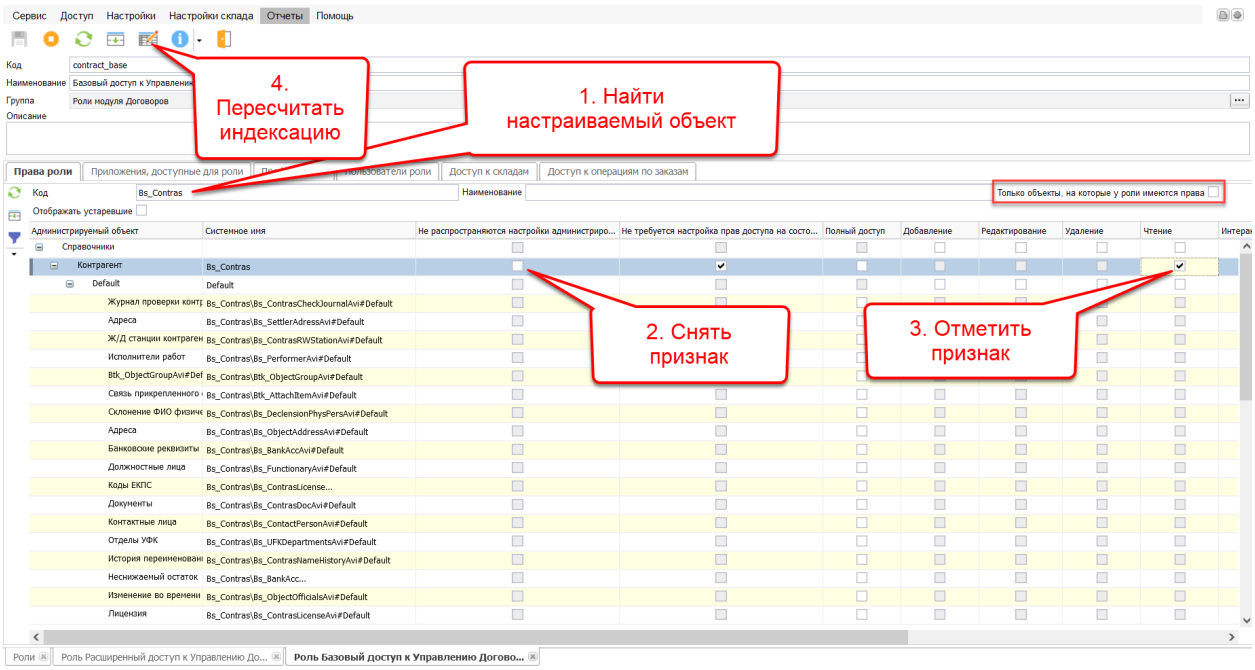

# 11 Прецедент настройки доступа к действиям с объектами Системы

После выдачи прав пользователям на приложение Управление Договорной деятельностью у пользователей появились полные права на все доступные в приложении объекты — чтение, редактирование, удаление, создание записей в них. Требуется оставить обоим пользователям права на просмотр справочника контрагентов, но пользователю Экономист сделать доступным также редактирование, добавление и удаление. Пользователю Снабженец сделать доступным к редактированию только атрибут «Не используется».

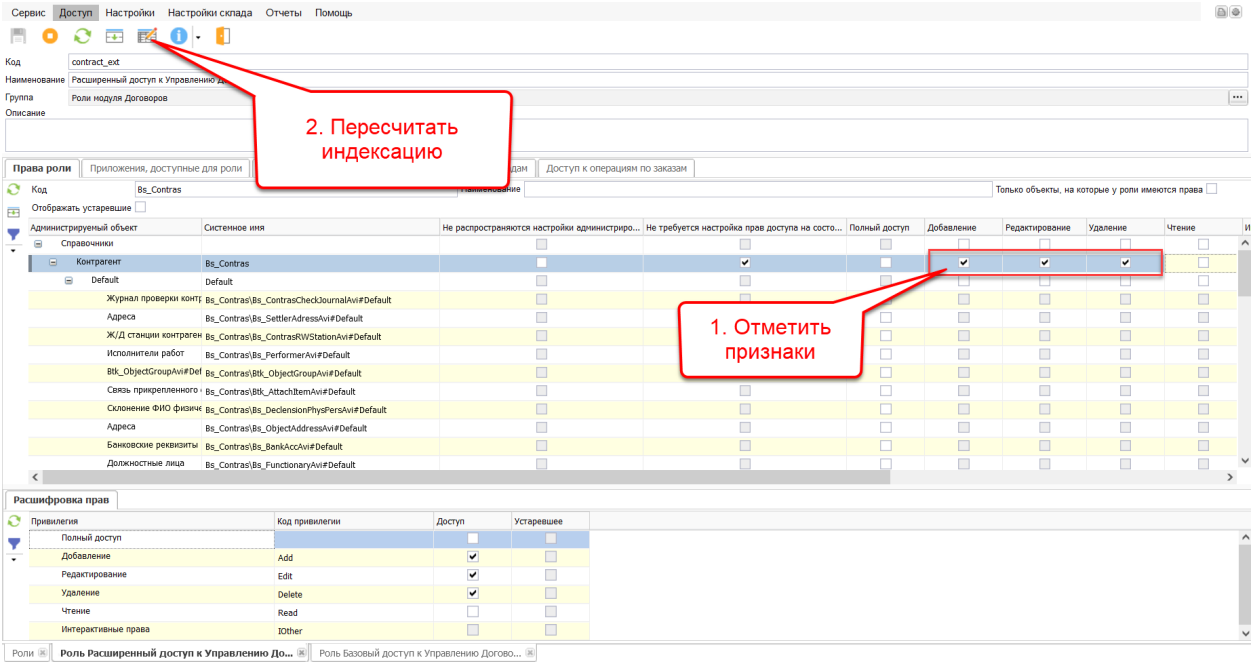
- Авторизовавшись как супер-пользователь, открыть справочник, права на доступ к которому требуется настроить, выделить любую позицию и комбинацией клавиш ctrl+alt+shift+W открыть Selection Debug Window. Из поля AcObject скопировать код администрируемого объекта.



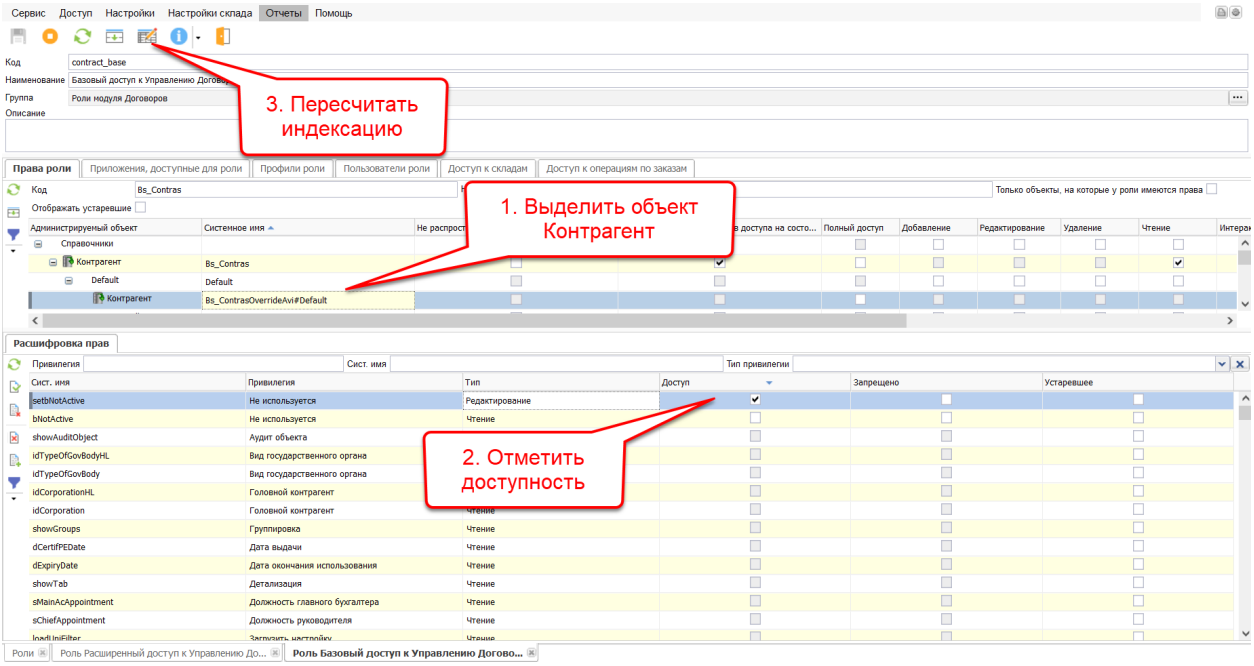

- Для роли «Базовый доступ к Управлению договорами» найти в списке прав роли объект «Контрагент» по скопированному коду. Снять установленный по умолчанию признак «Не распространяются настройки администрирования», отметить признак «Чтение», пересчитать индексацию. Выдача какого-либо права на верхнеуровневый объект автоматически выдает аналогичное право и на все нижнеуровневые объекты и атрибуты. Следовательно, в данном случае выдано право на чтение, но не создание, редактирование или удаление элементов справочника и всех их атрибутов.




- Требуется выдать Экономисту право на создание, редактирование и удаление записей в справочнике и их атрибутов. Следует аналогично предыдущему пункту для роли «Расширенный доступ к Управлению договорами» отметить доступность Добавления, Редактирования и Чтения. Пользователю расширенной роли в справочнике контрагентов стали доступны операции Создания, Удаления и Копирования, в карточке контрагента поля обозначены редактируемыми.



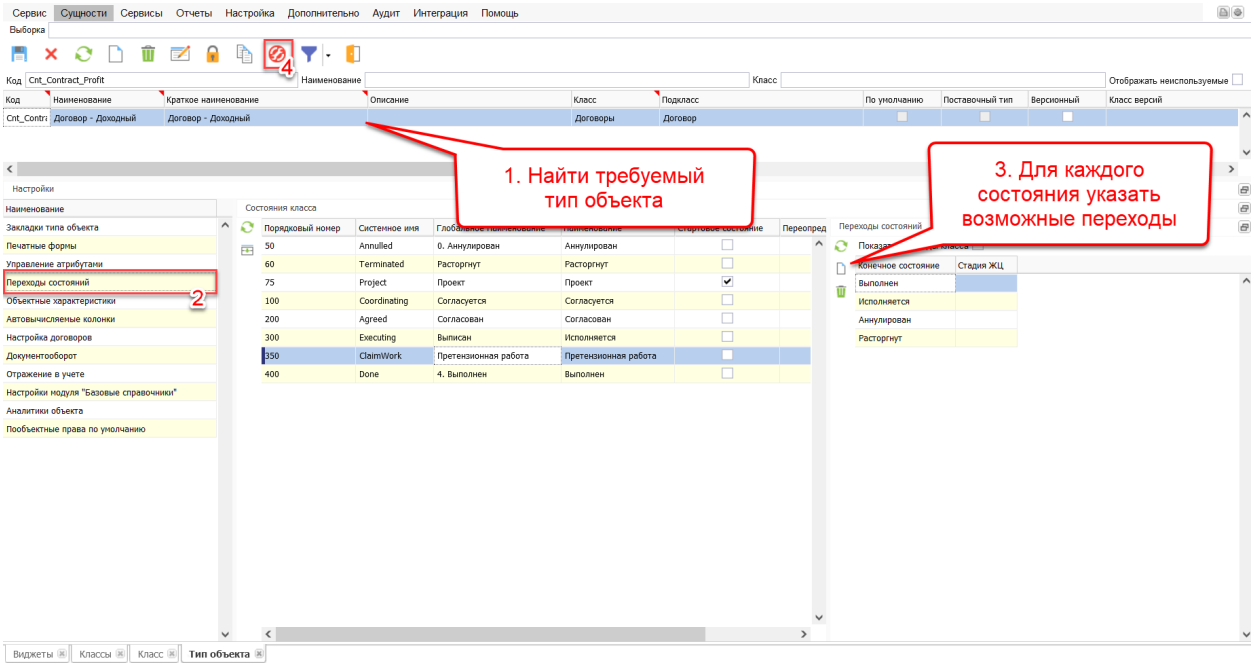

- Требуется выдать Снабженцу право на установку признака «Не используется». Для этого необходимо вернуться в роль «Базовый доступ к договорам» и в детализации к элементу администрируемого объекта «Контрагент» справочника Контрагентов выдать доступ к привилегии редактирования атрибута. Право на чтение данного атрибута выдавать не обязательно, так как оно уже включено в Базовую роль. После пересчета индексации атрибут «Не используется» стал доступен к редактированию Снабженцем — пользователем Базовой роли.



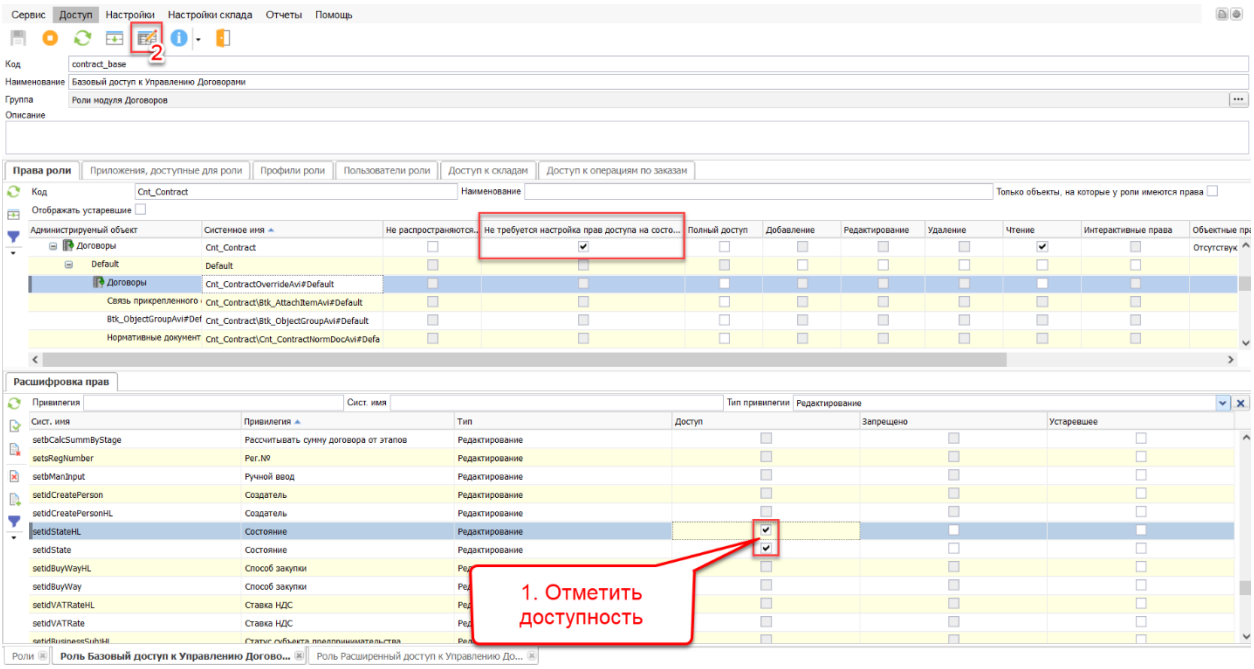
# 12 Прецедент настройки доступа к переводам состояний

Требуется дать Снабженцу право на перевод договора из состояния «Проект» в «Согласуется». Экономисту дать право на все предусмотренные переходы.

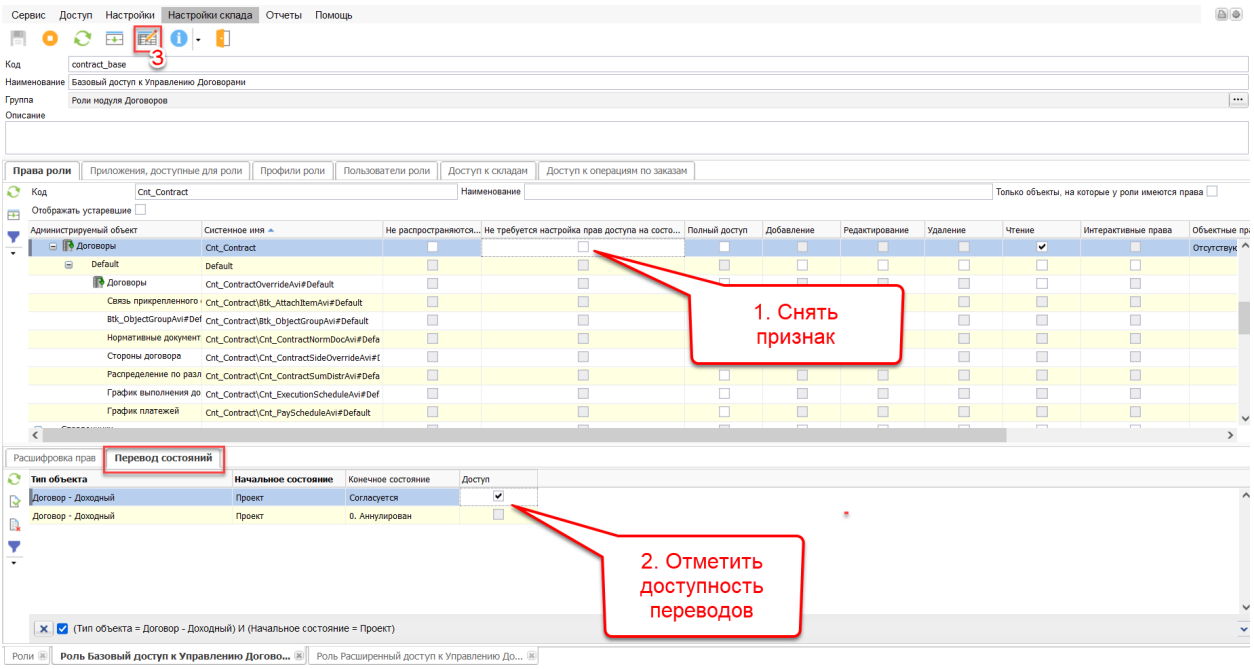
- Для настройки прав на переводы состояний требуется сначала обозначить список всех возможных переводов состояний. Для этого необходимо открыть настройку типов объектов (Настройка системы, Сущности -> Типы объектов), найти настраиваемый объект, перейти на закладку «Переходы состояний» и для каждого состояния указать состояния, в которые возможен переход из данного.



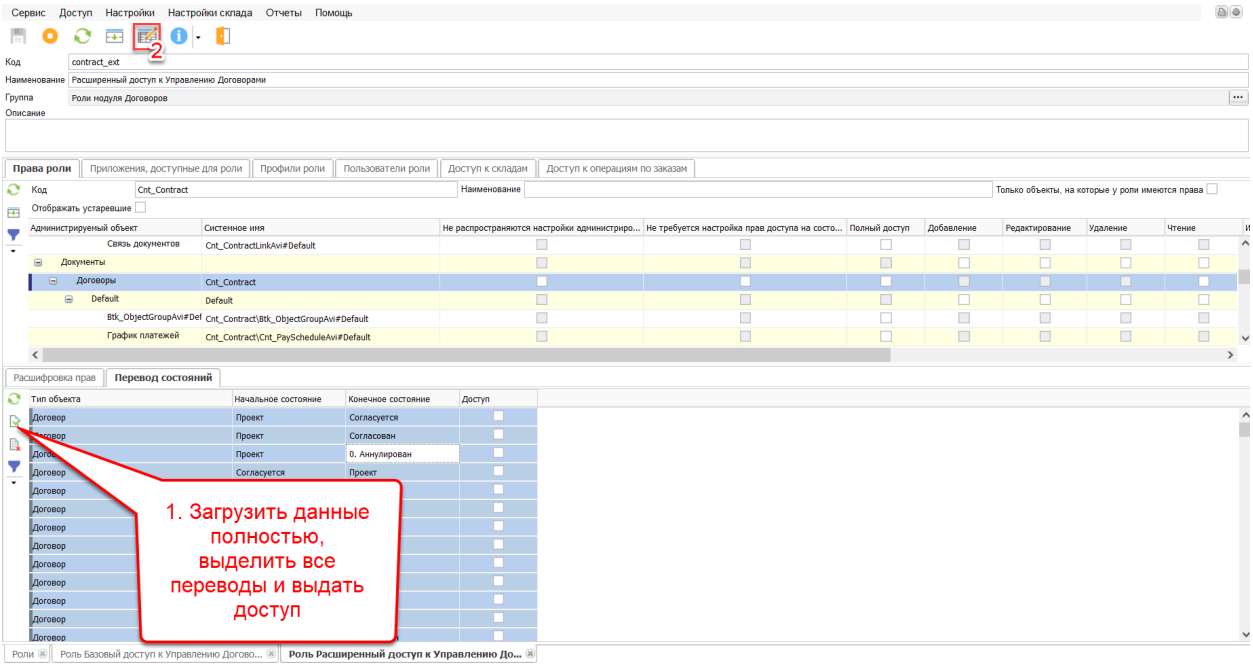

- Выдать Базовой роли к Управлению договорами доступ на редактирование атрибута «Состояние» Договора.




- Для настройки доступности переходов состояний требуется снять признак «Не требуется настройка прав доступа на состояния» и для Базовой роли на закладке детализации «Перевод состояний» отметить, какие переходы будут доступны данной роли. По умолчанию на закладке выводятся все возможные переходы всех типов объектов класса, так что удобно применять автофильтр по нужному типу объекта и начальному состоянию. После пересчета прав и новой авторизации пользователю роли будут доступны только указанные переводы состояний.



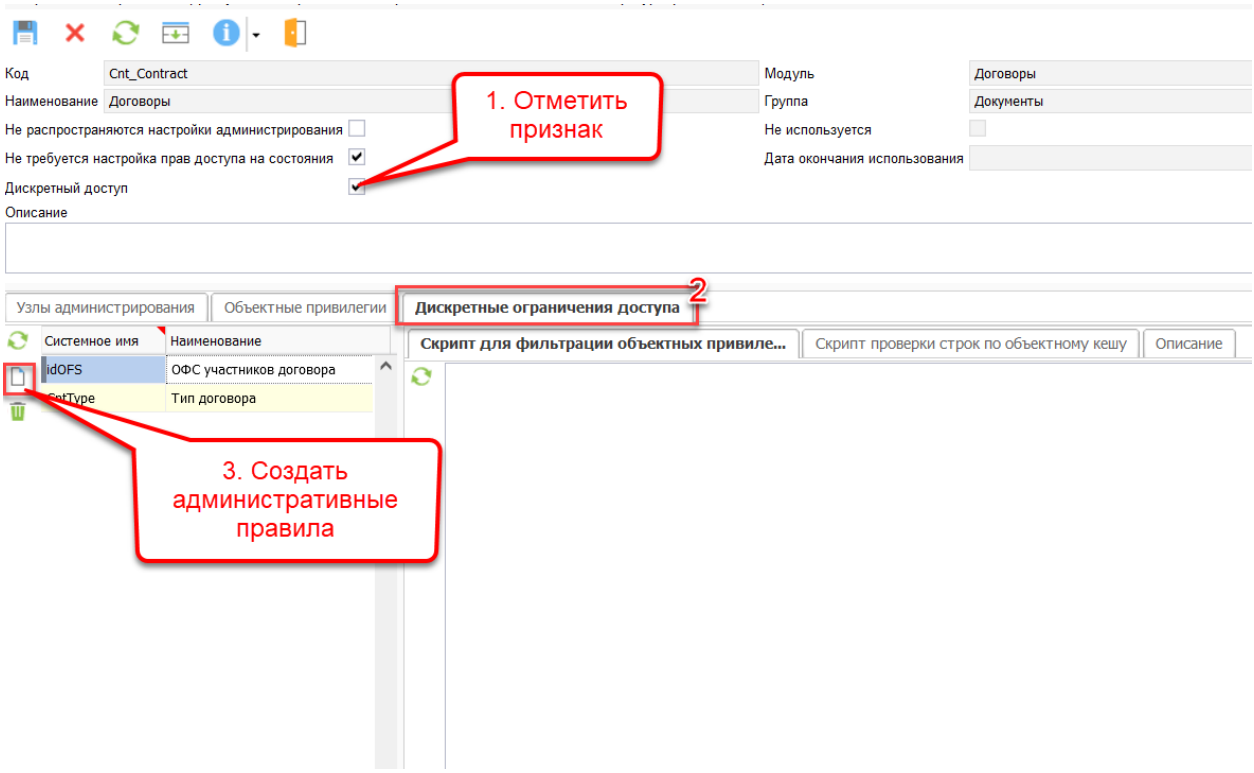

- Для выдачи прав Экономисту на прочие переходы необходимо аналогично предыдущему пункту выдать Расширенной роли права на требуемые переходы операцией «Разрешить для выделенных», загрузив все строки и выделив их комбинацией ctrl+a. После пересчета индексации и следующей авторизации пользователю профиля, содержащего расширенную роль, будут доступны все необходимые переходы состояний.




# 13 Прецедент настройки доступа к переводам состояний

Требуется администрируемый объект «Договоры» таким образом, чтобы пользователю роли были доступны только расходные договоры определенных подразделений.

- В справочнике администрируемых объектов (Приложение «Администратор», Настройки -> Администрируемые объекты) найти требуемый — Cnt_Contract и перейти в его карточку.
- В карточке администрируемого объекта отметить признак «Дискретный доступ». На закладке «Дискретные ограничения доступа» создать административные правило с типом «Примитивное правило».




- Для каждого правила вставить переданные разработчиками скрипты на закладках «Скрипт для фильтрации объектных привилегий» (отвечает за фильтрацию объектов в списках. В примере данного прецедента — скрывает из перечня договоры других типов и ОФС) и «Скрипт проверки строк по объектному кешу» (блокирует возможность открытия недоступных договоров по ссылке из прочих документов, например, запрещает пользователю открыть карточку недоступного договора из лота).

ОФС участников договора: Скрипт для фильтрации объектных привилегий

```
select 1
     from cnt_Contract tt
     join Cnt_ContractOFSParticipants cp
       on tt.id = cp.idcontract
     join Bs_OFStructure ofs
       on cp.idofstructure = ofs.id
    where tt.id = (&id)
      and exists (
      select 1 from (select cast(json_array_elements_text(cast((&params) as json)) as␣
↪int8) as id) ids where ids.id = ofs.id
      )
```

ОФС участников договора: Скрипт для проверки строк по объектному кешу

```
for (p: params) {
  var idv = row.id;
  var ropObj = Cnt_ContractApi.load(idv);
  var colRops = Cnt_ContractOFSParticipantsApi.byParent(ropObj);
  var colJRops = toJRops(colRops).asList();
  for (colRop: colJRops) {
```

(continues on next page)

(продолжение с предыдущей страницы)

```
      if (colRop.idOFStructure != null) {
        if (colRop.idOFStructure.toString() == p.toString()) {
          return true;
        }
    }
  }
}
```

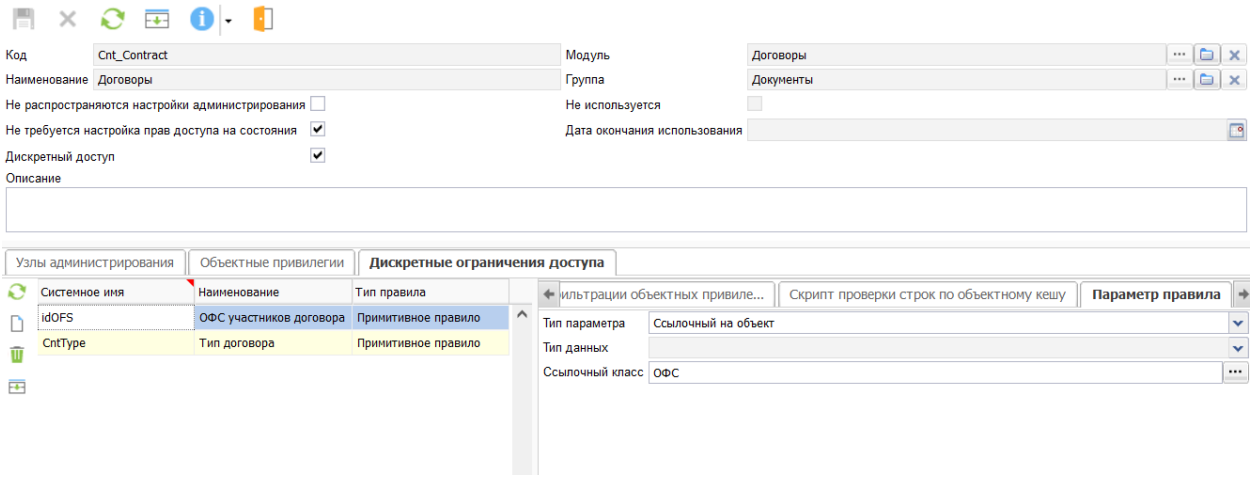
Тип договора: Скрипт для фильтрации объектных привилегий

```
select 1
     from cnt_Contract tt
     join (
     select cast(json_array_elements_text(cast((&params) as json)) as int8) as id
      )  as ids
     on tt.idobjecttype = ids.id
    where tt.id = (&id)
```

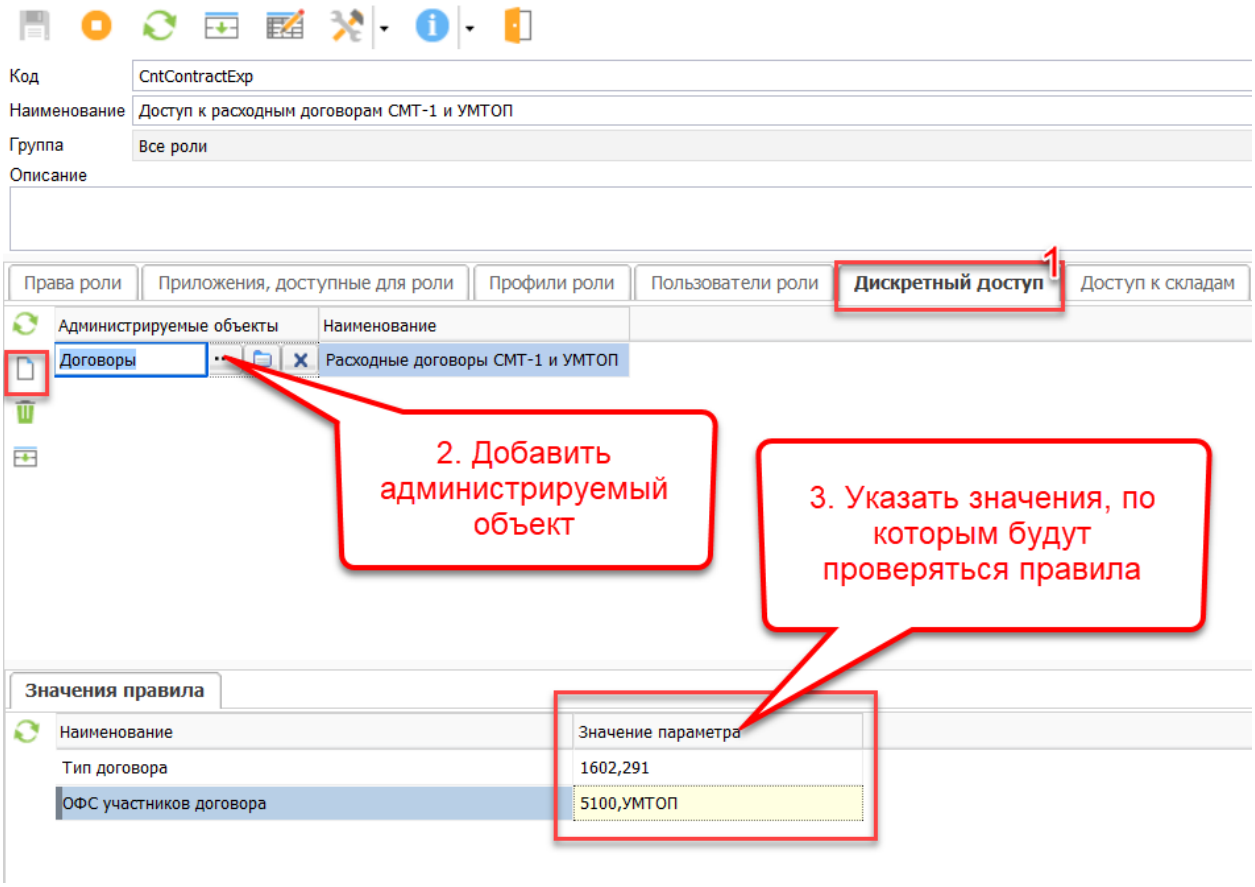
Тип договора: Скрипт для проверки строк по объектному кешу

```
for (p: params) {
  var idv = row.id;
  var ropObj = Cnt_ContractApi.load(idv);
var idObjectType = Cnt_ContractApi.getAttrValue(ropObj,"idObjectType");
    if (idObjectType.toString() == p.toString()) {
     return true;
    }
}
```

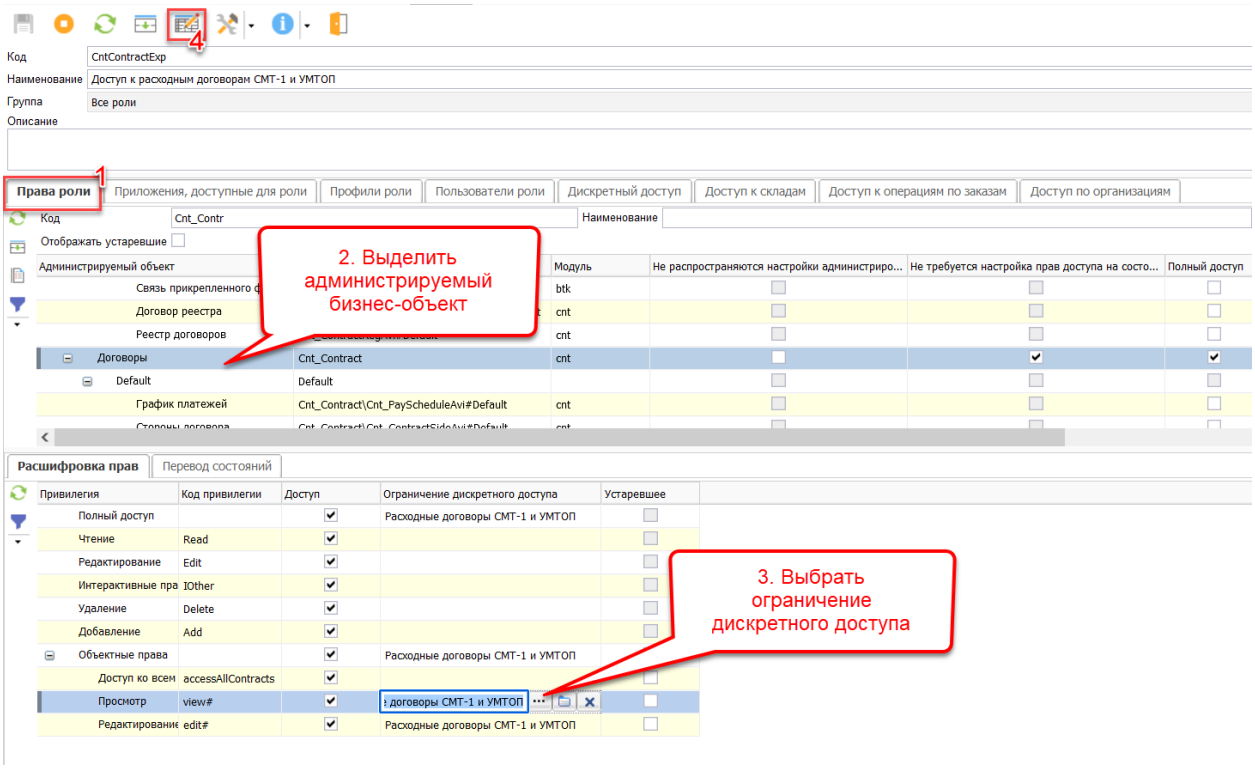
- На закладке «Параметр правила» для каждого правила выбрать Тип параметра — «Ссылочный на объект» и выбрать класс, из которого будут выбираться значения. В данном случае — Bs_OFStructure (ОФС) и Btk_ObjectType (Тип объекта)




- В карточке роли перейти на закладку «Дискретный доступ» и добавить администрируемый объект, доступ к которому необходимо настроить. В детализации на закладке «Значения правила» указать значения, по которым будут проверяться правила.




- На закладке «Права роли» найти и выделить администрируемый бизнес-объект. В детализации «Расшифровка прав» выбрать настроенное ограничение для прав на просмотр или редактирование объектов.


4
Код
CntContractExp
Наименование
Доступ к расходным договорам СМТ-1 и УМТОП
Группа
Все роли
Описание
1
Права роли
Приложения, доступные для роли
Профили роли
Пользователи роли
Дискретный доступ
Доступ к складам
Доступ к операциям по заказам
Доступ по организациям
Код
Cnt_Contr
Наименование
Отображать устаревшие
2. Выделить администрируемый бизнес-объект
Администрируемый объект
Модуль
Не распространяются настройки администриро...
Не требуется настройка прав доступа на состо...
Полный доступ
Связь прикрепленного
btk
Договор реестра
cnt
Реестр договоров
cnt
Договоры
Cnt_Contract
cnt
Default
Default
График платежей
Cnt_Contract\Cnt_PayScheduleAvi#Default
cnt
Расшифровка прав
Перевод состояний
Привилегия
Код привилегии
Доступ
Ограничение дискретного доступа
Устаревшее
Полный доступ
Расходные договоры СМТ-1 и УМТОП
Чтение
Read
Редактирование
Edit
Интерактивные пра
IOther
Удаление
Delete
Добавление
Add
Объектные права
Расходные договоры СМТ-1 и УМТОП
Доступ ко всем
accessAllContracts
Просмотр
view#
договоры СМТ-1 и УМТОП
Редактирование
edit#
Расходные договоры СМТ-1 и УМТОП
3. Выбрать ограничение дискретного доступа