# Права Доступа в системе Alisa

## Содержание

[Права Доступа в системе Alisa 1](#_Toc382988863)

[Содержание 1](#_Toc382988864)

[Сокращения и термины 2](#_Toc382988865)

[Описание 3](#_Toc382988866)

[Функции администратора прав 4](#_Toc382988867)

[Реализация 6](#_Toc382988868)

[База данных 7](#_Toc382988869)

[Схема 7](#_Toc382988870)

[Описания таблиц и примеры их заполнения 8](#_Toc382988871)

[ResourceClasses 8](#_Toc382988872)

[Resources 9](#_Toc382988873)

[Roles 10](#_Toc382988874)

[Users 11](#_Toc382988875)

[Sections 13](#_Toc382988876)

[RoleResources 14](#_Toc382988877)

[UserResources 15](#_Toc382988878)

[Lines 16](#_Toc382988879)

[UserRoles 17](#_Toc382988880)

[UserSections 18](#_Toc382988881)

## Сокращения и термины

|  |  |
| --- | --- |
| Слово | Описание |
| Фоллоуап-мэнеджер  Букинг-менеджер  Офис-менеджер  TO-менеджер  ... | Должности сотрудников, каждой из которых могут быть сопоставлены роли и разрешения |
| Рутокен | Устройство, подключаемое к USB и заменяющее небезопасную аутентификацию по связке «логин-пароль» на двухфакторную аппаратную аутентификацию. Первым фактором аутентификации является наличие у пользователя USB-токена, вторым — знание уникального PIN-кода к нему. Решение основано на технологии электронной подписи и позволяет свести к минимуму риск неправомерного использования данных Web-ресурса. |
| Ресурс | Функциональность системы, реализуемая рабочим местом или его элементом, которой может быть назначено право доступа |

## Описание

Права доступа в системе Alisa реализуются в специальном модуле приложения называемом «Модуль назначения прав и разрешений».

Есть несколько требований, которые этот модуль должен реализовывать:

1. Ограничение доступа персонала к различным ресурсам (функциям) приложения
2. Ограничение прав относительно ресурса на создание/редактирование/удаление

Пункты 1) и 2) укладываются в “классическую” схему ограничения прав доступа (аналог GRANT в SQL).

1. Ограничение прав доступа только оговоренными наборами данных при работе с функциональностью

Пункт 3) представляет “ограничение по сегментам данных”, другое название – row level security (доступ только к некоторым строкам данных)

## Функции администратора прав

1. Создание пользователя

Таблица Users

1. Создание класса ресурса

Таблица ResourceClasses

1. Создание ресурса

Таблица Resources

1. Создание роли

Таблица Roles - справочник

1. Присвоение пользователю ролей
2. Присвоение пользователю прав на ресурсы
3. Создание секции - справочник

Таблица Sections

1. Ограничение прав пользователя в соответствии с секциями
2. Формирование отчетов “Карта роли-права”, “Карта пользователи-роли”.

*Пример: карта роли-права:*

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Класс прав | Права | ADM | Booking manager | Finance-Manager | | FollowUp | | | KASSIR | Office-manager | | REP | TO | | PR-manager | Traveler manager | Account manager | |
| Работа с клиентами | Контракты | W | W | R | | W | | | R | W | | R | R | |  | R |  | |
|  | Платежи | W |  | R | | R | | | R | R | |  | R | |  | R |  | |
|  | Planning Calls | R |  | R | | R | | |  | R | |  | R | |  |  |  | |
| Контракты | Список контрактов | W |  | R | | W | | |  | W | |  | R | |  | R |  | |
|  | Составление контракта | W |  | R | |  | | |  | W | |  | R | |  |  |  | |
| Клиенты | Список клиентов | W | W | R | | R | | |  | W | | R | R | |  | R |  | |
|  | Заведение нового клиента | W | W |  | |  | | |  | W | |  |  | |  |  |  | |
| Балансы | Просмотр балансов | W |  | W | |  | | |  |  | |  | R | |  |  |  | |
| Букинг | Список заявок | W | W | R | |  | | | R | W | | R | R | |  | W |  | |
|  | Составление заявок | W | W |  | |  | | |  | W | |  |  | |  |  |  | |
| Касса на курорте | Работа с букинг-платежами | W | R | R | |  | | | W | W | |  | R | |  |  |  | |
|  | Работа с платежами по контракту | W |  | R | | W | | | W | W | |  | R | |  |  |  | |
|  | Офис-менеджер | W |  | W | |  | | | W | W | |  | R | |  |  |  | |
| Финансы | Работа с букинг-платежами | W | W | R | |  | | | W | W | |  | R | |  |  |  | |
|  | Банковские платежи | W |  | W | |  | | | W | W | |  | R | |  |  |  | |
| Класс прав | Права | ADM | Booking manager | | Finance-Manager | | FollowUp | KASSIR | | Office-manager | REP | | TO | PR-manager | | Traveler manager | | Account manager |
| Отчеты | отчет по деятельности рэпов, ТО и фоллоуап | R |  | | R | |  |  | | R |  | | R |  | |  | | R |
|  | Статистика продаж | R |  | | R | |  |  | | R |  | | R |  | |  | | R |
| Документы | Список документов | W |  | | R | |  |  | | W |  | | R |  | |  | |  |
|  | Добавить документ | W |  | | R | |  |  | | W |  | | R |  | |  | |  |
|  |  |  |  | |  | |  |  | |  |  | |  |  | |  | |  |
| Справочники |  | W |  | | R | |  |  | | R |  | | R |  | |  | |  |
|  |  |  |  | |  | |  |  | |  |  | |  |  | |  | |  |
| Экскурсии |  | W | W | | R | |  | W | | W | R | | R | R | |  | |  |
|  |  |  |  | |  | |  |  | |  |  | |  |  | |  | |  |
| Работа с владельцами | Контракты | W |  | | R | |  | R | | W | R | | R |  | | W | |  |
|  | Платежи | W |  | | R | |  | R | | R |  | | R |  | | W | |  |
|  | Planning Calls | R |  | | R | |  |  | | R |  | | R |  | | R | |  |

## Реализация

Схемы таблиц разработаны с учетом следующих требований:

1. Ограничение по доступу к функционалу программы (рабочие места, действия, шаблоны, кнопки) – роли и отдельные права на доступ помимо ролей, которые могут быть закреплены за конкретным пользователем.

2. Ограничение по доступу к информации внутри функционала.

*Пример:*

*Фолоуап-менеджер Алеся*

*1. Функциональный (ролевой) доступ:*

*- рабочее место фолоуап: просматривает контракты в любом статусе, кроме "completed".*

*- право выставления счетов клиентам,*

*- право подтверждения платежей,*

*- право поставить контракту статус "completed".*

*2. Сегментный доступ: имеет доступ к контрактам,  подготовленным только*

*- офис-менеджерами Елдашева, Кононенко*

*- на линиях продаж: Самуи, Вьетнам, Прага*

При этом пока не учтены следующие требования:

Двухфакторная аутентификация и шифрование данных

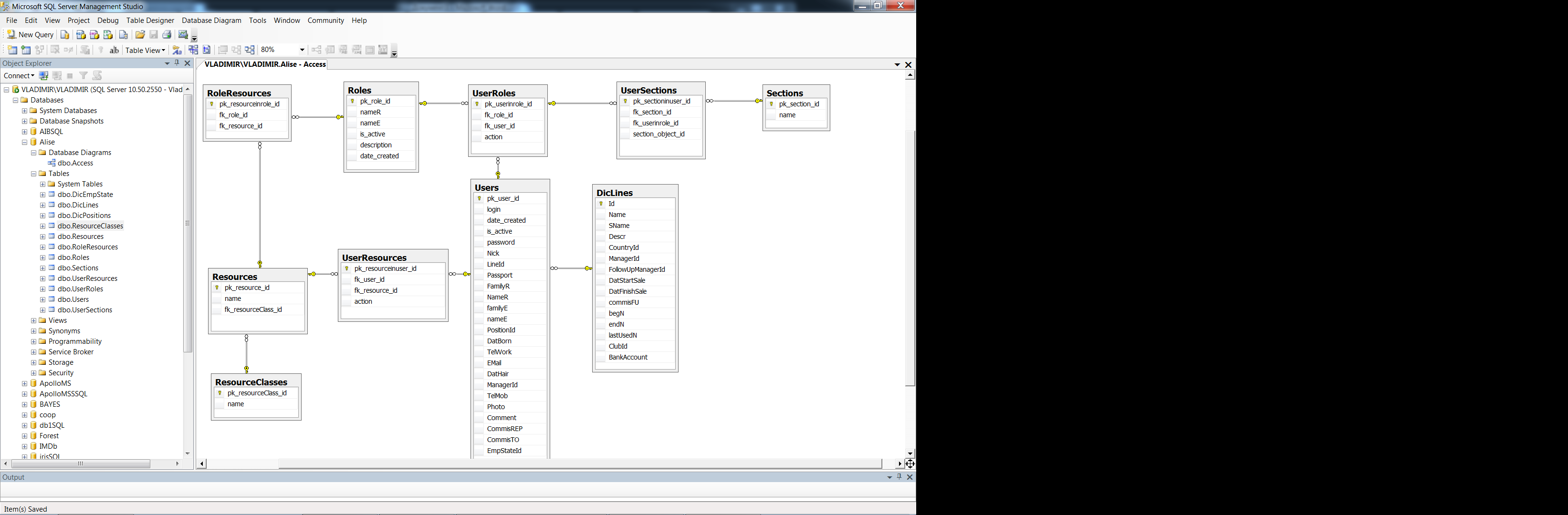
Для повышения безопасности ввода и хранения чувствительной информации, необходимо организовать доступ к программе только посредством двухфакторной аутентификации к WEB-интерфейсу на базе «Рутокен Web» и пароля-логина, используя шифрование данных (SSL).

Пути реализации

1. Доступ к данным через программу должен совершаться только в зашифрованном виде по протоколу SSL.
2. Пользователь получает доступ в программу только подписавшись электронным ключом (Рутокен) и авторизовавшись логином-паролем.
3. Электронный ключ (Рутокен) должен быть подключен к компьютеру пользователя в течение всего времени работы пользователя с программой.

## База данных

### Схема



## Описания таблиц и примеры их заполнения

ResourceClasses – классы ресурсов, рабочие места (нужна для организации лаконичного интерфейса определения прав)

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_resourceClass\_id | int IDENTITY(1б1) NOT NULL | Идентификатор класса ресурса |
| Name | nvarchar(255) | название класса ресурса |

*Пример:*

*pk\_resourceClass\_id name*

*1 Работа с клиентами*

*2 Финансы*

*3 Контракты*

*4 Балансы*

*5 Букинг*

*6 Касса на курорте*

*7 Отчеты*

*8 Документы*

*9 Справочники*

*10 Экскурсии*

*11 Работа с владельцами*

Resources – ресурсы (функционал, раздел рабочего места, элемент рабочего места, др.)

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_resource\_id | int NOT NULL | Идентификатор, который будет использоваться в коде для написания фильтров акций контроллеров и хелперах доступа (нет IDENTITY) |
| Name | nvarchar(255) | название роли |
| Fk\_resourceClass\_id | Int NULL | Ссылка на класс ресурса |

*Пример:*

*pk\_resource\_id name fk\_resourceClass\_id*

*1 Работа с заявкой 5*

*2 Список заявок по линии 5*

*3 Раздел "Презентация" 5*

*в заявке*

*4 Перевод контракта*

*в состояние "complited" 3*

*5 Работа с контрактом 3*

*6 Список контрактов 3*

*9 Финансовые*

*условия контракта 3*

*…*

### Roles

-роли с точки зрения доступа к ресурсам, примерно соответствуют должностям сотрудников.

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_role\_id | int IDENTITY(1,1) NOT NULL | Идентификатор, который будет использоваться в коде для написания фильтров акций контроллеров и хелперах доступа |
| NameR | nvarchar(50) NOT NULL | Название роли по русски |
| NameE | nvarchar(50) | Название роли по английски |
| is\_active | Bit | Активна ли роль? Если не активна, то пользователи, входящие в нее, не получают соотвтетствующих прав. |
| description | nvarchar(MAX) NULL | Описание роли на русском |
| Date\_created | DateTime | Дата, время создания роли |

*Пример:*

*pk\_role\_id name is\_active description*

*1 Офис-менеджер 1 Сотрудник, готовящий контракты, подписывающий их и принимающий депозиты на курорте*

*2 Фоллоуап-менеджер 1 NULL*

*3 Директор 1 NULL*

*…*

### Users

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_user\_id | Int IDENTITY(1,1) NOT NULL | Идентификатор, который будет использоваться в коде для написания фильтров акций контроллеров и хелперах доступа |
| Login | nvarchar(50) | Имя пользователя |
| Password | nvarchar(MAX) | Пароль в зашифрованном виде |
| is\_active | Bit | Активен ли пользователь? |
| Date\_created | DateTime | Дата, время создания записи |
| Nick | nvarchar(50) | Ник сотрудника для формирования списков быстрого выбора |
| LineId | int | Линия продаж (офис), где работает сотрудник |
| Passport | nvarchar(30) |  |
| FamilyR | nvarchar(50) | Фамилия и имя по русски |
| NameR | nvarchar(50) |
| FamilyE | nvarchar(50) | Фамилия и имя по английски |
| NameE | nvarchar(50) |
| PositionId | int | Ссылка на должность |
| DatBorn | datetime | Дата рождения |
| TelWork | nvarchar(30) | Раб.тел. |
| EMail | nvarchar(50) | Почта |
| DatHair | datetime | Дата приема на работу |
| ManagerId | int | Ссылка на сотрудника-начальника |
| TelMob | nvarchar(50) | Моб.тел. |
| Photo | image |  |
| Comment | nvarchar(MAX) |  |
| CommisREP | int | Фикс.комиссионные сотруднику как РЭПу (редко назначаются) |
| CommisTO | int | Фикс.комиссионные сотруднику как ТО (редко назначаются) |
| EmpStateId | int | Ссылка на статус занятости (работает, уволен,…) |

*Пример:*

*pk\_user\_id login date\_created is\_active FamilyR NameR*

*1 alis 2014-03-13 1 Алеся*

*2 krug 2014-03-13 1 Елдашева*

*3 flt 2014-03-13 1 Кононенко*

*…*

Sections – секции доступа, ограничивающие пользователя частью данных

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_section\_id | int NOT NULL | Идентификатор, который будет использоваться в коде для написания фильтров акций контроллеров и хелперах доступа  ***(нет IDENTITY)*** |
| Name | nvarchar(50) | Имя секции |

*Пример:*

*pk\_section\_id name*

*1 Ограничение контрактов определенными линиями продаж*

*2 Ограничение заявок определенными клубами*

*3 Ограничение контрактов определенными офис- менеджерами*

…

RoleResources– доступность ресурса роли (или роли, владеющие ресурсами)

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_resourceinrole\_id | int IDENTITY(1,1) NOT NULL |  |
| fk\_Role\_id | int NOT NULL | Идентификатор роли, ссылка на roles |
| fk\_Resource\_id | int NOT NULL | Идентификатор ресурса, ссылка на resources |
| action | Tinyint | тип доступа  0-просмотр,  1-создание,  2-изменение,  3-создание и изменение |

*Пример:*

*Pk\_resourceinrole\_id fk\_role\_id fk\_resource\_id action*

*Офис-менеджер имеет доступ к Работа с контрактом, может создавать и изменять*

*1 1 5 3*

*Офис-менеджер имеет доступ к Список контрактов*

*2 1 6 0*

*Фоллоуап-менеджер имеет доступ к Перевод контракта в состояние complited*

*3 2 4 2*

UserResources – доступность ресурса для пользователя (помимо ролей)

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_resourceinuser\_id | int IDENTITY(1,1) NOT NULL |  |
| fk\_user\_id | int NOT NULL | Идентификатор пользователя, ссылка на users |
| fk\_Resource\_id | int NOT NULL | Идентификатор ресурса, ссылка на resources |
| action | Tinyint | тип доступа  0-просмотр,  1-создание,  2-изменение,  3-создание и изменение |

Pk\_resourceinuser\_id fk\_user\_id fk\_resource\_id action

*Алеся имеет доступ к Работа с контрактом, может читать*

*1 1 5 0*

Lines - Линии продаж:

|  |  |  |
| --- | --- | --- |
| *Имя поля* | *Тип* | *Описание* |
| *Id* | *Int IDENTITY(1,1)* |  |
| *Name* | *nvarchar(50) NOT NULL* |  |
| *SName* | *nchar(10) NULL* |  |
| *Descr* | *nvarchar(MAX)* |  |
| *CountryId* | *Int* | *Ссылка на страну* |
| *ManagerId* | *int* | *Ссылка на руководителя линии* |
| *FollowUpManagerId* | *int* | *Ссылка на фоллоуап-менеджера* |
| *DatStartSale* | *datetime* | *Дата начала продаж* |
| *DatFinishSale* | *datetime* | *Дата окончания продаж* |
| *commisFU* | *int* | *% комиссии followup-менеджерам от суммы выплат followup* |
| *begN* | *int* | *начало диапозона номеров контрактов* |
| *endN* | *int* | *конец диапозона номеров контрактов* |
| *lastUsedN* | *int* | *Последний использованный номер контракта* |
| *ClubId* | *int* | *Ссылка на клуб* |
| *BankAccount* | *nvarchar(MAX)* | *Банковские реквизиты* |

*Пример данных:*

*Id Name SName*

*2 Самуи*

*5 Вьетнам В*

*8 Чехия ЧХ*

UserRoles – роли пользователя

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_userinrole\_id | int IDENTITY(1,1) NOT NULL |  |
| fk\_user\_id | int NOT NULL | Идентификатор пользователя, ссылка на users |
| fk\_role\_id | int NOT NULL | Идентификатор роли, ссылка на roles |

*Пример:*

*pk\_userinrole\_id fk\_role\_id fk\_user\_id*

*1 1 (фоллоуап) 1 (Алеся)*

*2 2 (офис-менеджер) 2 (Елдашева)*

*3 2 (офис-менеджер) 3 (Кононенко)*

UserSections – секции, ограничивающие доступ к данным пользователя (независимо от его ролей)

|  |  |  |
| --- | --- | --- |
| Имя поля | Тип | Описание |
| pk\_sectioninuser\_id | int IDENTITY(1,1) NOT NULL |  |
| fk\_userinrole\_id | int NOT NULL | Ссылка на UserRoles – сегменты задаются для роли пользователя. |
| fk\_section\_id | int NOT NULL | Идентификатор секции, ссылка на sections |
| section\_object\_id | Int NOT NULL | ссылка на конкретный объект(запись) таблицы,  соответствующей селектору fk\_section\_id |

***Пример:***

*Фолоуап-менеджер Алеся*

*просматривает контракты в рабочем месте фолоуап-менеджера только подготовленные*

*- офис-менеджерами Елдашева, Кононенко*

*- на линиях продаж: Самуи, Вьетнам, Прага*

*Для реализации таких ограничений следует создавать ссылки на заранее не определенные таблицы, в данном случае на Users, Lines.*

*В частности следует заполнить таблицу UserSections**следующими данными (в поле fk\_section\_object\_id следует поместить ссылки на Lines (линии) и Users (сотрудники) (в зависимости от селектора fk\_section\_id), которыми права на данные будут ограничены у Алеси):*

pk\_sectioninuser\_id fk\_section\_id fk\_userinrole\_id section\_object\_id

Ограничение контрактов по линиям для Алеся

Ссылка на DicLines

1 1(Lines) 1(Алеся в роли 2 (Самуи)

фоллоуап)

2 1 1 5 (Вьетнам)

3 1 1 8 (Чехия)

Ограничение контрактов по сотрудникам для Алеся

Ссылка на Users

4 3(Users) 1(Алеся в роли 2 (Елдашева)

фоллоуап)

5 3 1 3 (Кононенко)