

# Управляем ролями с помощью IDM

Андрей Каганский  
Начальник отдела систем управления  
учетными данными и доступом



# Какие существуют способы назначения доступа сотруднику?





# Автоматическое назначение ролей





# Автоматическое назначение ролей



## Обновление мастер-данных

Изменение данных о сотруднике в доверенном источнике

## Определение бизнес-роли

В IDM назначаются роли в соответствии с моделью

## Актуализация доступа

Доступ к ресурсам назначается и отзывается в соответствии с ролью



# Это и есть RBAC!



# Автоматическое назначение ролей



Обновление  
мастер-данных

Изменение данных  
о сотруднике в доверенном  
источнике

Определение  
бизнес-роли

В IDM назначаются роли  
в соответствии с моделью

Актуализация  
доступа

Доступ к ресурсам  
назначается и отзывается  
в соответствии с ролью



## Это и есть RBAC! Или нет?



# Функция IDM – гибко управлять доступом к ресурсам





# Учет контекста при назначении ролей





# Пример правила назначения роли

ПРАВИЛО АВТОНАЗНАЧЕНИЯ

▼ Пользователи

<input type="checkbox"/>	Основное подразделение	▼	В иерархии	▼	Департамент продаж	×
<input type="checkbox"/>	Основная должность	▼	Равно без уч. р...	▼	Помощник менеджера по продажам	
<input type="checkbox"/>	Город	▼	Равно	▼	Екатеринбург	
<input type="checkbox"/>	Офис	▼	Равно	▼	ул. Ленина, 1, 3 этаж	

И ▼

+ Добавить условие

> Трудоустройства

+ Добавить условие

▼ Наличие роли у пользователя

<input type="checkbox"/>	Название	▼	Равно	▼	Менеджер по продажам	
<input type="checkbox"/>	Название	▼	Равно	▼	Доступ к КТ	

И ▼

+ Добавить условие

▼ Наличие УЗ ресурса у пользователя

<input type="checkbox"/>	Название	▼	Равно	▼	1С ERP	
--------------------------	----------	---	-------	---	--------	--

ИЛИ ▼





# Наследование ролей



ERP



CRM



FS



BI



СЭД



# Доступ по запросу – возможности и ограничения

## 1. Кто может запросить

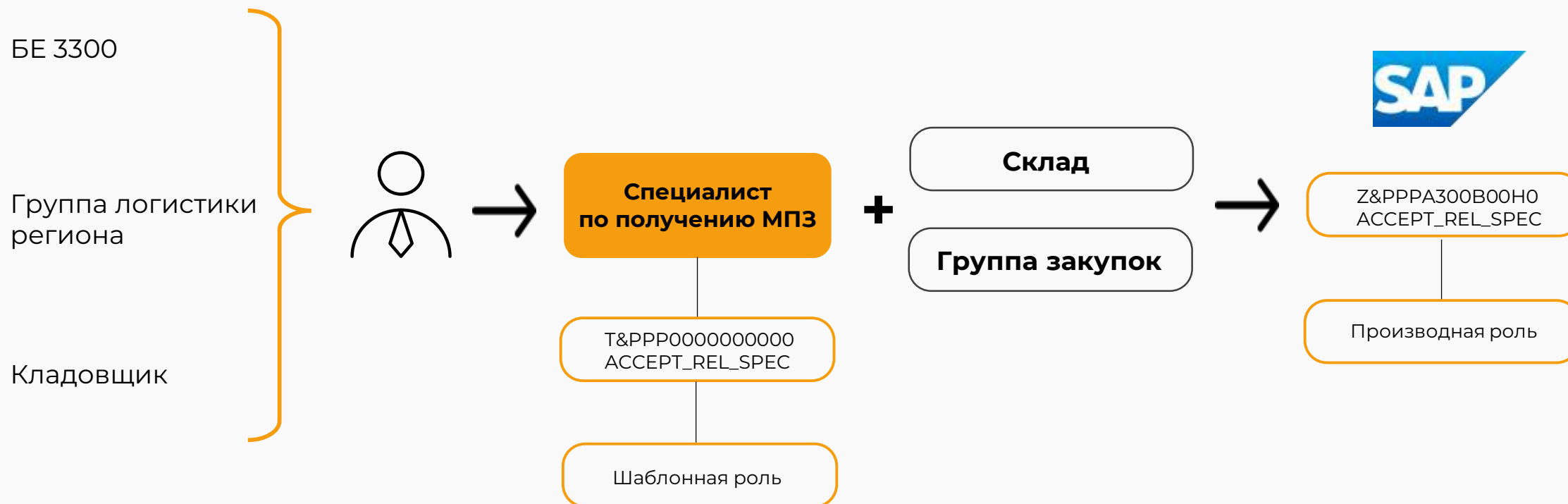
- Сотрудник (себе)
- Руководитель (подчиненному)
- «Оператор» (1 линия ТП)

## 2. Что может запросить

- Ограничение видимости
- Учет контекста
- Обязательные атрибуты (срок, обоснование)
- Дополнительные параметры



с учетом контекста и дополнительных параметров





# Подведем итог

## Возможности IDM

Которые позволяют эффективно и гибко реализовать автоматизированное управление ролями пользователей и которые следует учитывать при разработке ролевой модели

### 01

Работа  
с КОНТЕКСТОМ

### 02

Наследование  
и вложенность

### 03

Разграничение  
видимости ролей





USSC.RU

# Спасибо за внимание!

Вопросы?

Андрей Каганский  
Начальник отдела систем  
управления учетными данными  
и доступом

akaganskiy@ussc.ru