

# Безопасность SAP HCM

*Как узнать зарплату коллеги,  
не вставая с рабочего места*

Евгения Шумахер  
Positive Technologies



# Наш план

## Мы не будем говорить

- Об уязвимостях
- О SAP Notes
- О SAP-окружении

## Мы поговорим

- О типах авторизаций в SAP HCM
- О настройках авторизаций в SAP HCM
- Об основных объектах авторизаций SAP HCM
- Об аудите безопасности SAP HCM



# SAP HCM – решение для управления персоналом

Хранятся критические данные:

- ФИО, дата рождения
- Паспортные данные, ИНН, СНИЛС
- Банковские реквизиты
- Заработная плата и другие вознаграждения
- Данные об отработанном времени

Выполняются финансовые операции:

- Расчет зарплаты
- Выплаты премий/бонусов

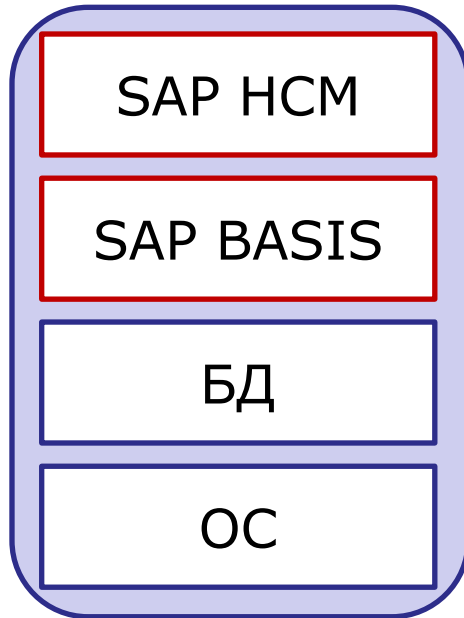
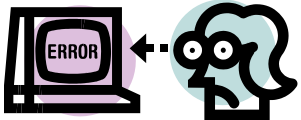
*Изменение данных может привести к финансовым потерям*

*Просмотр данных может привести к нарушениям требований законодательства*

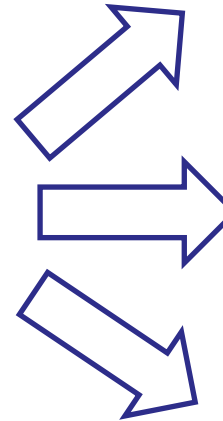


# SAP HCM: угрозы и их последствия

Человеческий фактор



Мошенничество



Утечка данных

Финансовые потери

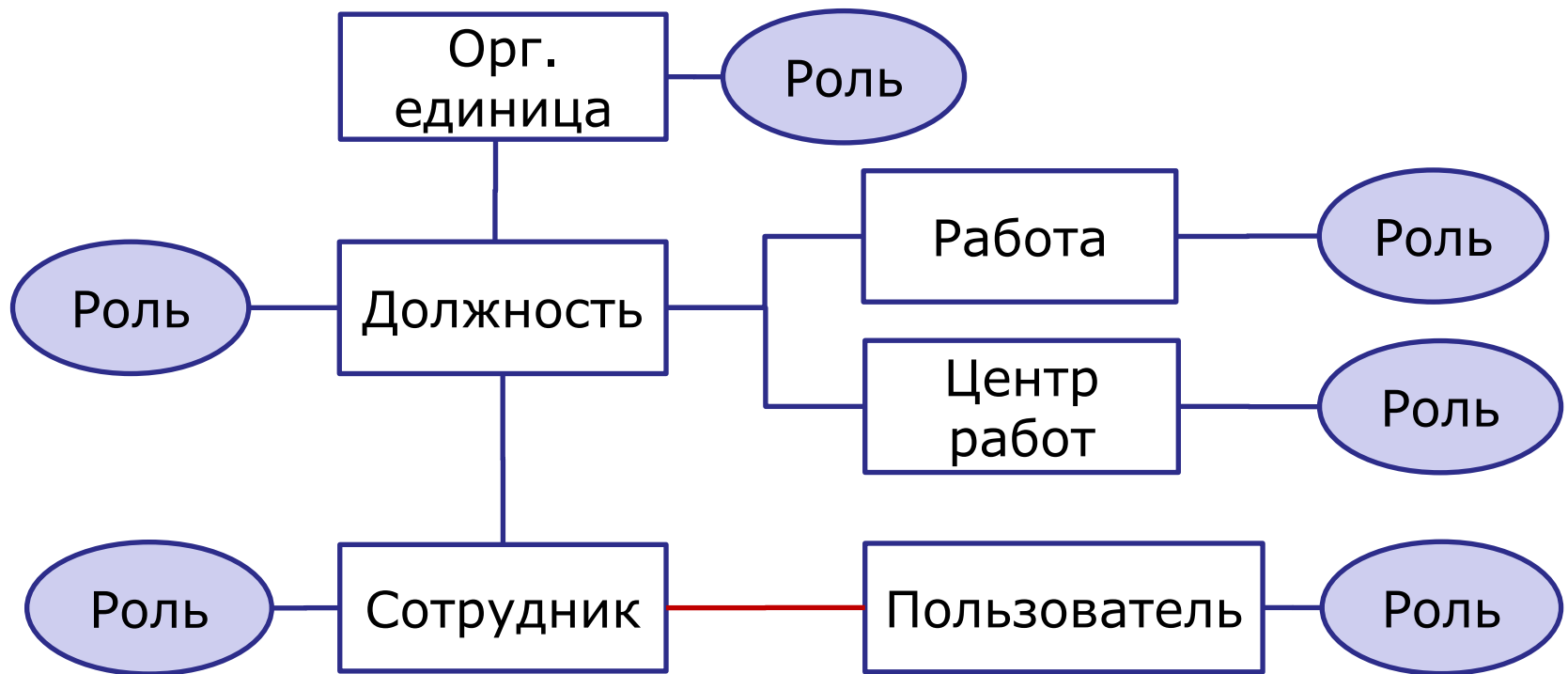
Нарушение требований  
законодательства



# Особенности настроек авторизаций SAP HCM



# Косвенное присвоение ролей

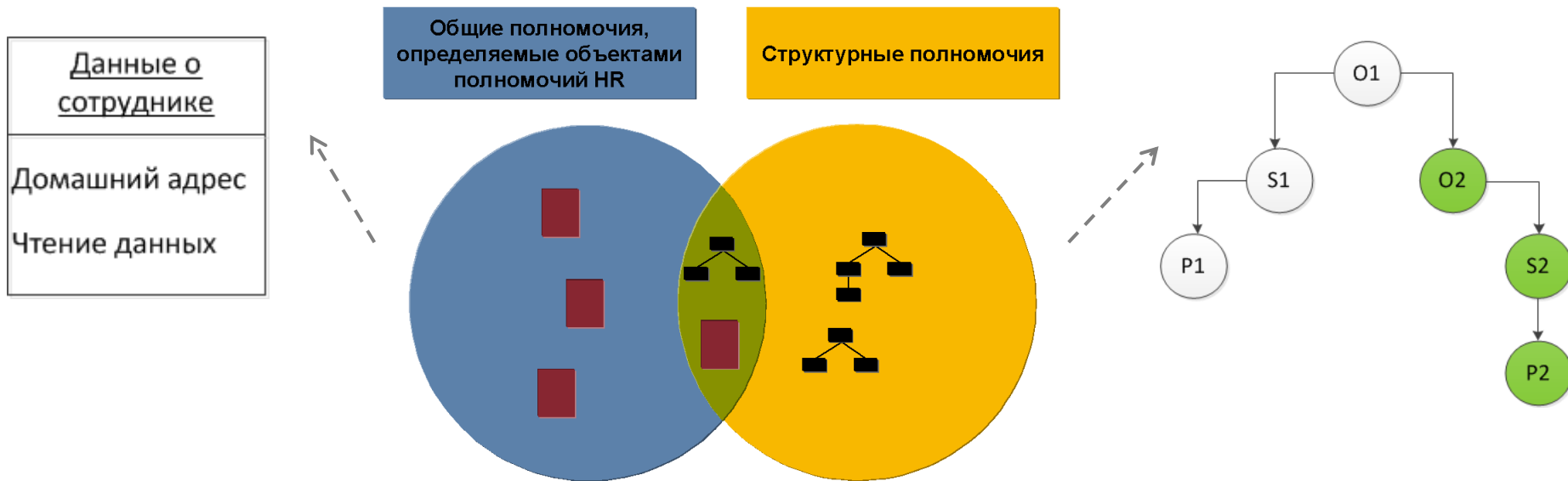


*Сложно контролировать набор ролей пользователя*



# Общие и структурные полномочия

- *Общие полномочия* определяют, к какой информации об объекте пользователь имеет доступ, а также вид доступа (чтение, запись)
- *Структурные полномочия* определяют, к какому объекту в организационной структуре у пользователя есть доступ



*Пересечение структурных и общих полномочий делает контроль доступа нетривиальной задачей*

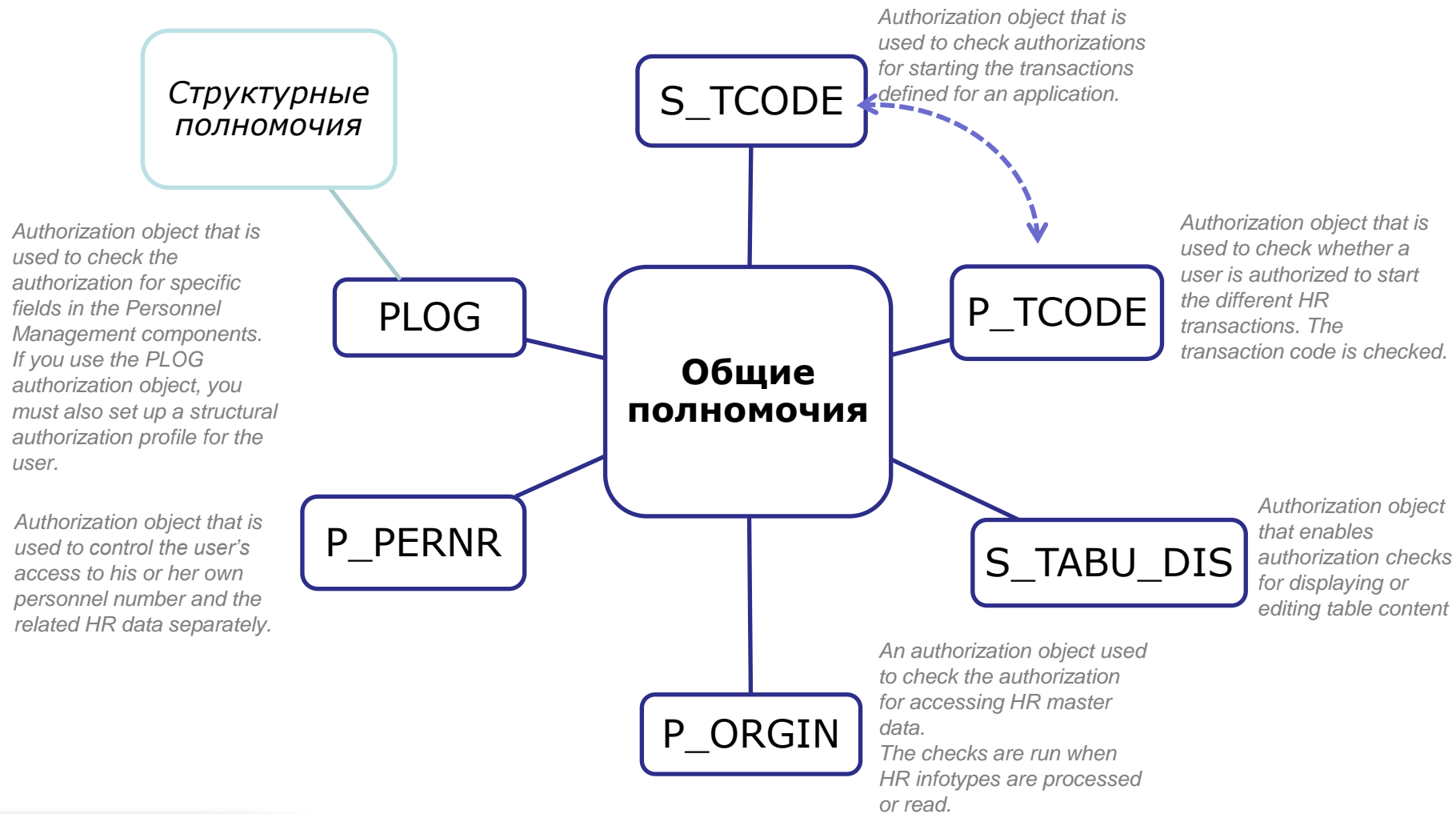


# **Общие полномочия в SAP HCM В чем особенности?**








# Полномочия = комбинация объектов авторизации






# Настройки HR-авторизаций

Транзакция **OOAC** (таблица **T77S0**)

-  **AUTSW-ORGIN** – Включение/выключение объекта авторизации P\_ORGIN (доступ к данным HR)
-  **AUTSW-PERNR** – Включение/выключение объекта авторизации P\_PERNR (проверка собственного табельного номера)
-  **AUTSW-ORGPD** – Включение/выключение проверки структурных полномочий

*Change View "HR: Authorization main switch": Overview*

Documentation   

System Switch (from Table T77S0)

Group	Sem. abbr.	Value abbr.	Description
AUTSW	ADAYS	15	<input type="checkbox"/> : Tolerance Time for Authorization Check
AUTSW	APPRO	0	HR: Test Procedures
AUTSW	DFCON	1	HR: Default Position (Context)
AUTSW	INCON	0	HR: Master Data (Context)
AUTSW	NNCON	0	HR:Customer-Specific Authorization Check (Context)
AUTSW	NNNNN	0	HR: Customer-Specific Authorization Check
AUTSW	ORGIN	1	HR: Master Data
AUTSW	ORGPD	1	HR: Structural Authorization Check
AUTSW	ORGXX	0	HR: Master Data - Extended Check
AUTSW	PERNR	1	HR: Master Data - Personnel Number Check
AUTSW	XXCON	0	HR: Master Data - Enhanced Check (Context)



# Способы доступа к данным сотрудника

- HR-транзакции: **PA20, PA30, PRMS, PRMD** и др.
- Транзакции доступа к таблицам: **SE16, SE16N, SE17**
- Запуск SAP-программ: **SA38, SE38**

The screenshot displays the SAP 'Maintain Time Data' (PA20) transaction. The main window shows employee details for Personnel No. 8999999, Name John Doe, and Pers.Assgn 08999999 Sales Manager Active. The 'Additional account assignments' tab is active, showing a list of infotypes. A 'Data Browser: Table PA0002 Select Entries' window is overlaid, displaying a table with columns MANDT, PERNR, SUBTY, OBJPS, SPRPS, ENDDA, BEGDA, SEQNR, AEDTM, UNAME, and HISTO. The table contains one entry for MANDT 800, PERNR 08999999, ENDDA 31.12.9999, BEGDA 28.07.1960, SEQNR 000, and AEDTM 16.07.2012, with UNAME JEAN.

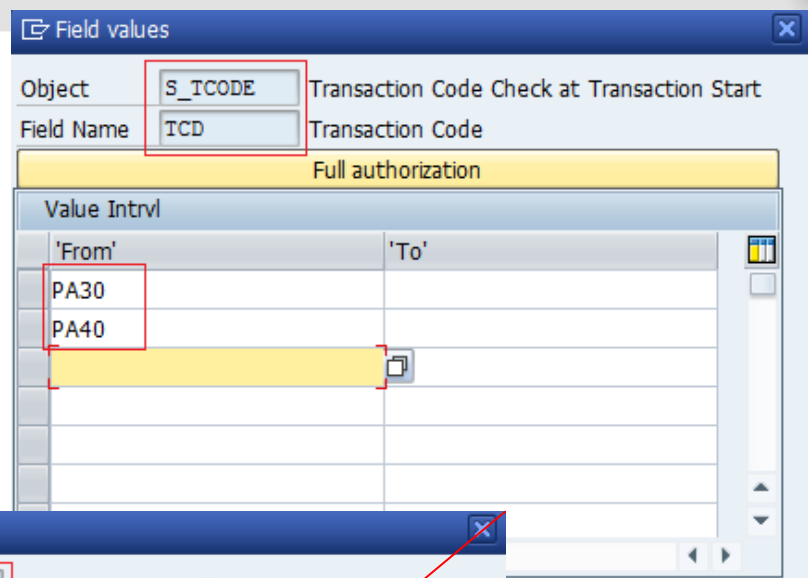
MANDT	PERNR	SUBTY	OBJPS	SPRPS	ENDDA	BEGDA	SEQNR	AEDTM	UNAME	HISTO
800	08999999				31.12.9999	28.07.1960	000	16.07.2012	JEAN	

# S\_TCODE, P\_TCODE - полномочия для запуска транзакции

**S\_TCODE** – транзакции всех модулей  
**P\_TCODE** – только HR-транзакции

## Настройки

Authorization Field	Description
TCD	Transaction Code



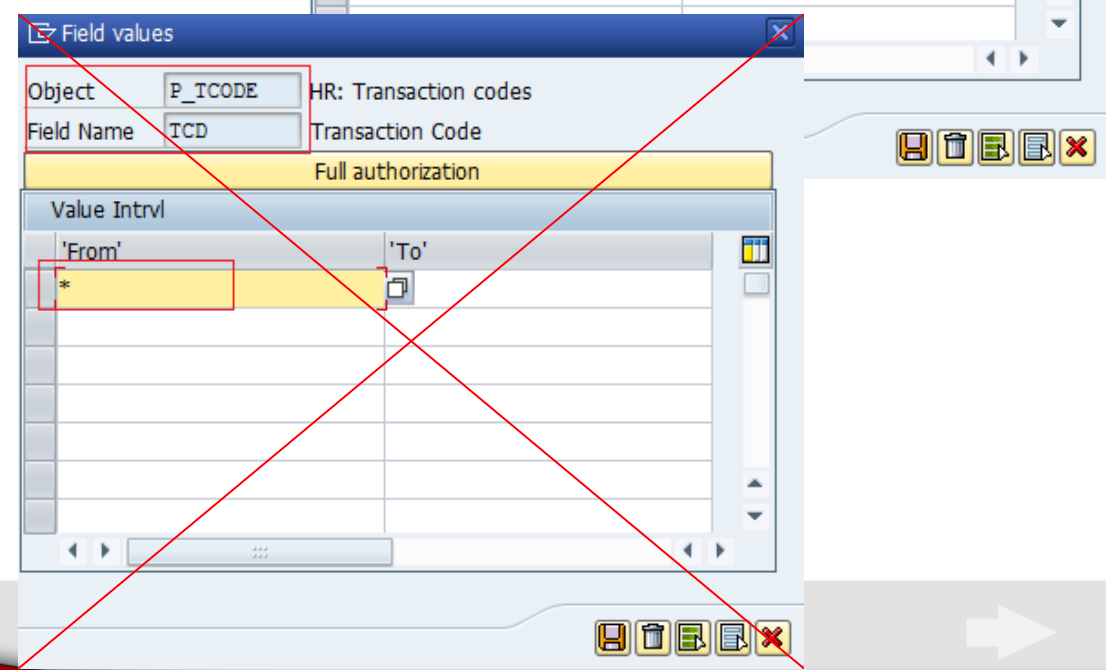
## Типовые ошибки

Все транзакции

$TCD = *$

С ... по ...

$TCD = PA01 - PA61$



# S\_TABU\_DIS - полномочия для доступа к таблицам

Необходим для транзакций SE16 и др.

## Настройки

Authorization Field	Description	Values
DICBERCLS	Authorization group	<b>PA:</b> Employee data
ACTVT	Activity	<b>02:</b> Change <b>03:</b> Display

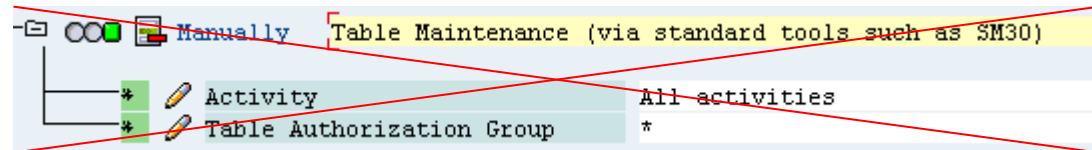
## Типовые ошибки

Все группы таблиц

DICBERCLS = \*

Все действия

ACTVT = **All activities**



# Данные сотрудника хранятся в инфотипах

Единицы информации для введения основных данных в системе управления персоналом называются **инфотипами**

- **0002** – личные данные
- **0006** – адресные данные
- **0008** – данные о заработной плате
- **0009** – банковские данные

Address type	Permanent residence ▼	
Care Of		
Street and House No.	65 Wedgewood Crescent	
2nd Address Line		
City	Victoria	
Province	British Columbia ▼	
Postal code/Country	V1B 6Y7	Canada ▼
Telephone Number	250	231-4514



# P\_ORGIN – полномочия для доступа к данным HR

## Настройки

Authorization Field	Description
INFT	Infotype
SUBTY	Subtype
AUTHC	Authorization level (such as read, write, matchcode)
PERSA	Personnel area (from infotype 0001)
PERSG	Employee group (from infotype 0001)
PERSK	Employee subgroup (from infotype 0001)
VDSK1	Organizational key (from infotype 0001)

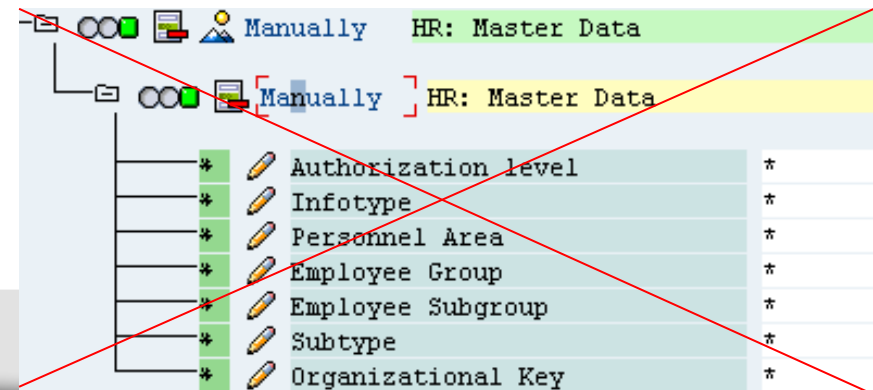
## Типовые ошибки

Все действия

*AUTHC* = \*

Все данные

*INFT* = \*



The screenshot shows the SAP HR Master Data authorization settings. The table lists the following fields and their authorization levels:

Field	Authorization Level
Authorization level	*
Infotype	*
Personnel Area	*
Employee Group	*
Employee Subgroup	*
Subtype	*
Organizational Key	*

The entire screenshot is crossed out with a large red 'X', indicating that these settings are a common error.



# Ограничение по табельному номеру сотрудника

**P\_PERNR** – объект авторизации, используемый для назначения полномочий сотруднику на доступ к собственным данным. Имеет самый высокий приоритет


*У сотрудника должен быть табельный номер!*

## Пользователь

- Логин
- Пароль
- Полномочия

## Сотрудник

- ФИО
- Табельный номер
- Должность
- Отдел

Pers. No.	8999999	Pers.Assgn	08999999 Sales Manager Active		
Name	John Doe				
	New York	Active			
	Manhattan	Salaried staff		US:Semi-Monthly - US	
Start	01.05.2012	to	31.12.9999	Chng	25.06.2012 JEAN
Communication					
Type	0001	System user name (SY-UNAME)			
ID/number	HRUSER				





# P\_PERNR – полномочия для доступа к собственным данным

## Настройки

Authorization Field	Description	Values
AUTHC	Authorization Level	
PSIGN	Interpretation of Assigned Authorization	I: include E: exclude *=I >E>I
INFTY	Infotype	
SUBTY	Subtype	



# P\_PERNR – полномочия для доступа к собственным данным

## Типовые ошибки

Редактирование всей собственной информации

*AUTHC* = \*

*PSIGN* = **I**

*INFTY* = \*

*SUBTY* = \*

Можно все

*AUTHC* = \*

*PSIGN* = \*

*INFTY* = \*

*SUBTY* = \*

Неоднозначная трактовка

*PSIGN* = \* = **I**

The screenshot shows a table with the following columns: Authorization level, Infotype, Interpretation of assigned per, and Subtype. Each row has a green checkmark in the first column and an asterisk in the last column. The entire screenshot is crossed out with a large red 'X'.

Authorization level	Infotype	Interpretation of assigned per	Subtype
*	*	*	*

Отсутствие P\_PERNR (*PSIGN* = E) тоже необходимо проверять!



# Авторизации пересекаются

## P\_PERNR #1

AUTHC = \*  
PSIGN = I  
INFTY = 0014  
SUBTY = M\*

## P\_PERNR #2

AUTHC = W, S, D, E  
PSIGN = E  
INFTY = 0014  
SUBTY = \*

AUTHC = R  
INFTY = 0014  
SUBTY = M120

ДА

AUTHC = W  
INFTY = 0014  
SUBTY = B030

НЕТ

AUTHC = W  
INFTY = 0014  
SUBTY = M120

НЕТ



# Выводы

- ≡ Полномочия на выполнение действия – это не просто права на запуск транзакции; это комбинация авторизаций
- ≡ Авторизации пересекаются
- ≡ P\_PERNR имеет наивысший приоритет, но его применимость зависит от многих настроек
- ≡ \* - это почти всегда плохо



**Что дальше?**



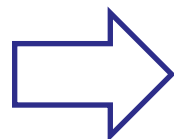
# Просмотр данных о зарплате коллег



*Пользователь имеет полномочия для просмотра данных других сотрудников*



*Пользователь узнает зарплату своего коллеги*



*Демотивация*

## Проверка

- Получить список пользователей, имеющих полномочия для просмотра данных о заработной плате других сотрудников
- Сравнить полученный список со списком пользователей, с утвержденными полномочиями выполнения данного действия



# Способы просмотра заработной платы

## Экранные формы

HR-транзакции: PA30, PA20, PRMS, PRMD, TPMD, TPMS, TPED, TPES, PA61, т.д.

Инфотипы: 0008 (основные выплаты), 0014 (периодические выплаты/удержания), 0015 (дополнительные выплаты)

Pers. No.	8999999	Pers.Assgn	08999999 Sales Manager Active	
Name	John Doe			
	New York	Active		
	Manhattan	Salaried staff	US:Semi-Monthly - US	
Start	01.05.2012	to	31.12.9999	Chng 17.07.2012 JEAN
Subtype	0	Basic contract		
<b>Pay scale</b>				
Reason	<input type="checkbox"/>	Cap.util.M	100,00	
PS type	01 Standard contract	WkHrs/period	86,67	Semi-monthly
PS Area	01 Philadelphia	Next inc.		
PS group	GRD01	Level	03	Ann.salary 60.000,00 USD
W...	Wage Type Long Text	O.	Amount	Curr... I... A.. Number/Unit Unit
1002	Salary		2.500,00	USD <input checked="" type="checkbox"/> 0,00



# Способы просмотра заработной платы

## Чтение данных из таблиц

Транзакции для доступа к таблицам: SE16, SE16N, SE17

Таблицы: PA0008, PA0014, PA0015

**Data Browser: Table PA0008 Select Entries 1**

☞ 🔍 ⏪ ⏩ 🖨️ 📄 📁 📄 📄 📄 📄 Check Table...

Table: PA0008  
Displayed Fields: 34 of 284 Fixed Columns: [ 8 ] List Width 0250

	MANDT	PERNR	SUBTY	OBJPS	SPRPS	EMDDA	BEGDA	SEQMR	AEDTM	UNAME
<input type="checkbox"/>	800	089999999	0			31.12.9999	01.05.2012	000	17.07.2012	JEAN

BSGRD	100,00
DIVGV	86,67
ANSAL	60.000,00
FALGK	
FALGR	
LGA01	1002
BET01	2.500,00
ANZ01	0,00
EIN01	
OPK01	
LGA02	
BET02	0,00
ANZ02	0,00

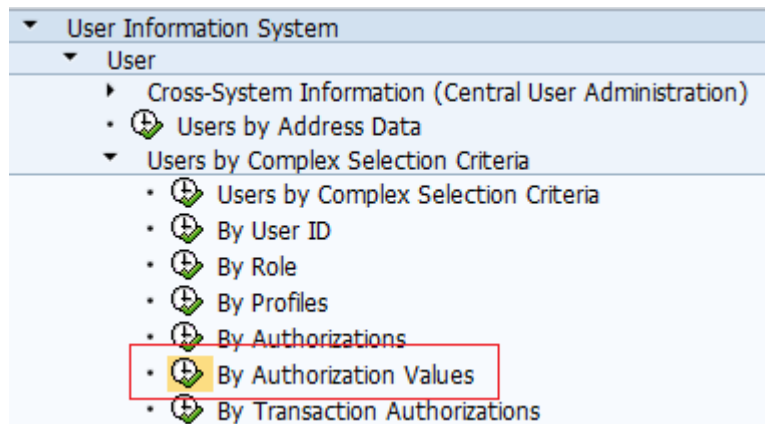




# Выполнение проверок в SAP HCM

Транзакция **SUIM**:

User -> Users By Complex Selection Criteria -> By Authorization Values



A screenshot of the 'Selection by values' dialog box in SAP SUIM. The dialog has the following structure:

- Always Convert Values Entry values
- Authorization object 1
  - Authorization Object
- AND authorization object 2
  - Authorization Object
- AND authorization object 3
  - Authorization Object



# Пользователи, имеющие полномочия для просмотра данных о заработной плате сотрудников

## Транзакция PA20:

**AUTHORIZATION OBJECT 1: S\_TCODE**  
 TCD: PA20 (Display HR Master Data)

**AUTHORIZATION OBJECT 2: P\_ORGIN**  
 SUBTY: \*  
 PERSA: \*  
 PERSG: \*  
 PERSK: \*  
 VDSK1: \*  
 INFTY: 0008  
 AUTHC: R

Authorization object 1			
Authorization Object	S_TCODE		
Transaction Code			
Value	PA20	OR	
AND		OR	
AND authorization object 2			
Authorization Object	P_ORGIN		
Infotype			
Value	0008	OR	
AND		OR	
Subtype			
Value	*	OR	
AND		OR	
Authorization level			
Value	R	OR	
AND		OR	
Personnel Area			
Value	*	OR	
AND		OR	
Employee Group			
Value	*	OR	
AND		OR	
Employee Subgroup			
Value	*	OR	
AND		OR	
Organizational Key			
Value	*	OR	
AND		OR	

User name	Complete name	User Type	Account no	Locked	Reason	Valid From	Val
ACHILAKOS	Alex Chilakos	GRC-FI_GROUP					
AHARTZELL	Alan Hartzell	GRC-HR_GROUP					
AHILDEBRAND	Alaric Hildebrand	GRC-HR_GROUP					
AITIM	Adolf ITIM	GRC-HR_GROUP					
AJANZ	Abir Janz	GRC-HR_GROUP					
AJUVONEN	Alan Juvonen	GRC-HR_GROUP					
AKRISA	Aaron Krisa	GRC-HR_GROUP					

# Пользователи, имеющие полномочия для просмотра данных о заработной плате сотрудников

## Транзакция SE16 и таблица PA0008:

### AUTHORIZATION OBJECT 1: **S\_TCODE**

TCD: SE16 (Display HR Master Data)

### AUTHORIZATION OBJECT 2: **S\_TABU\_DIS**

DICBERCLS: PA (Employee Data)

ACTVT: 03 (Display)

The screenshot shows the SAP authorization configuration interface. It is divided into three sections, each representing an authorization object. The first section, 'Authorization object 1', is for 'S\_TCODE' and has 'Transaction Code' set to 'SE16'. The second section, 'AND authorization object 2', is for 'S\_TABU\_DIS' and has 'Table Authorization Group' set to 'PA' and 'Activity' set to '03'. The third section, 'AND authorization object 3', is currently empty.

User name	Complete name	User Type	Account no	Locked	Reason	Valid From	Valid To	User Ty...	Reference user
ALADMIN	ALADMIN	TECHNICAL						A Dialog	
ALE_MASTER	ALE_MASTER	TECHNICAL						A Dialog	
ALE-WM-01	ALE-WM-01	TECHNICAL						A Dialog	
ALEREMOTE	ALEREMOTE	TECHNICAL						A Dialog	
ANDERSON	Jamie Anderson	GFO						A Dialog	
APOADMIN	Michael Douglas	TECHNICAL						A Dialog	

## Отчет о результатах внутреннего аудита CIDA (Canadian International Development Agency)

В организации численностью более **1700** человек

- ☰ **Всем пользователям SAP HCM** были доступны данные более **1700** сотрудников через транзакцию **SE16**
- ☰ Вся группа поддержки SAP имела доступ к данным сотрудников
- ☰ У **14** ролей были полномочия для выполнения транзакции **SA38**
- ☰ Отсутствовали какие-либо механизмы аудита

<http://www.acdi-cida.gc.ca>



# Резюме

- Существуют общие и структурные авторизации; они могут пересекаться
- Косвенное присвоение ролей в системе усложняет настройку полномочий
- Данные HR хранятся в инфотипах; необходимо ограничивать доступ к ним
- Доступ к данным можно получить через HR-транзакции и непосредственно через таблицы
- Можно ограничивать доступ сотрудника к его собственным данным по табельному номеру
- Полномочия для выполнения действия определяется комбинацией нескольких авторизаций



# Что почитать?

## Курсы SAP HCM

- HR940
- HR990

## Книги SAP Press

- *Discover SAP ERP HCM* (Greg Newman)
- *Authorizations in SAP HR* (Martin Esch, Anja Junold)
- *SAP Security and Risk Management* (Mario Linkies, Horst Karin)

## Лучшие практики от АНАО

- [Human Resource Information Systems](#)
- [SAP ECC 6.0 Security and Control](#)

## Блоги

- <http://saphr.ru>



**Спасибо за внимание**

Евгения Шумахер  
*[eshumaher@ptsecurity.ru](mailto:eshumaher@ptsecurity.ru)*



POSITIVE TECHNOLOGIES