Безопасность SAP HCM

Как узнать зарплату коллеги,
не вставая с рабочего места

Евгения Шумахер
Positive Technologies

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:

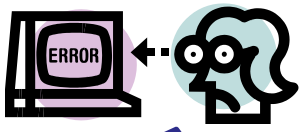
- Расчет зарплаты
- Выплаты премий/бонусов

Изменение данных может привести к финансовым потерям

Просмотр данных может привести к нарушениям требований законодательства

SAP HCM: угрозы и их последствия

Человеческий фактор



SAP HCM

SAP BASIS

БД

ОС

Утечка данных

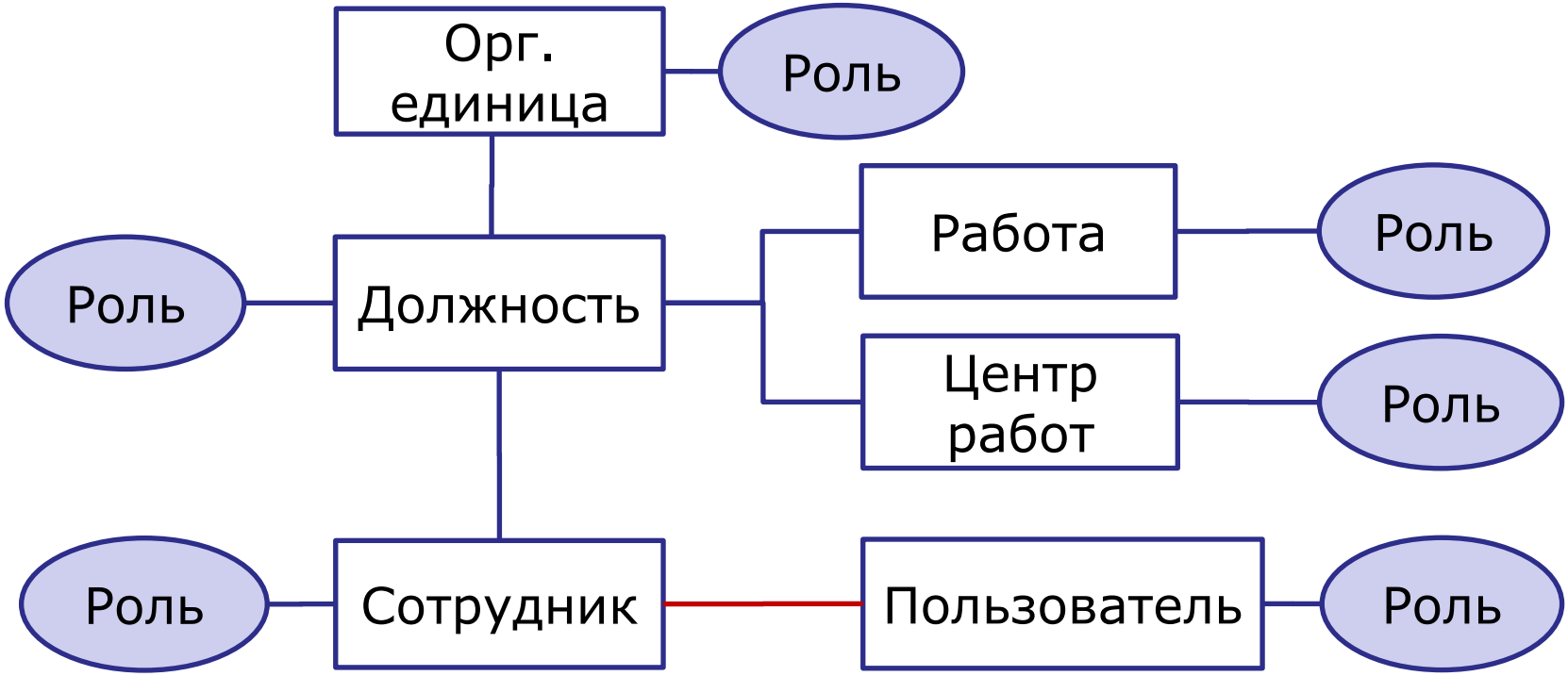
Финансовые потери

Нарушение требований законодательства

Мошенничество

Особенности настроек авторизаций SAP HCM

Косвенное присвоение ролей

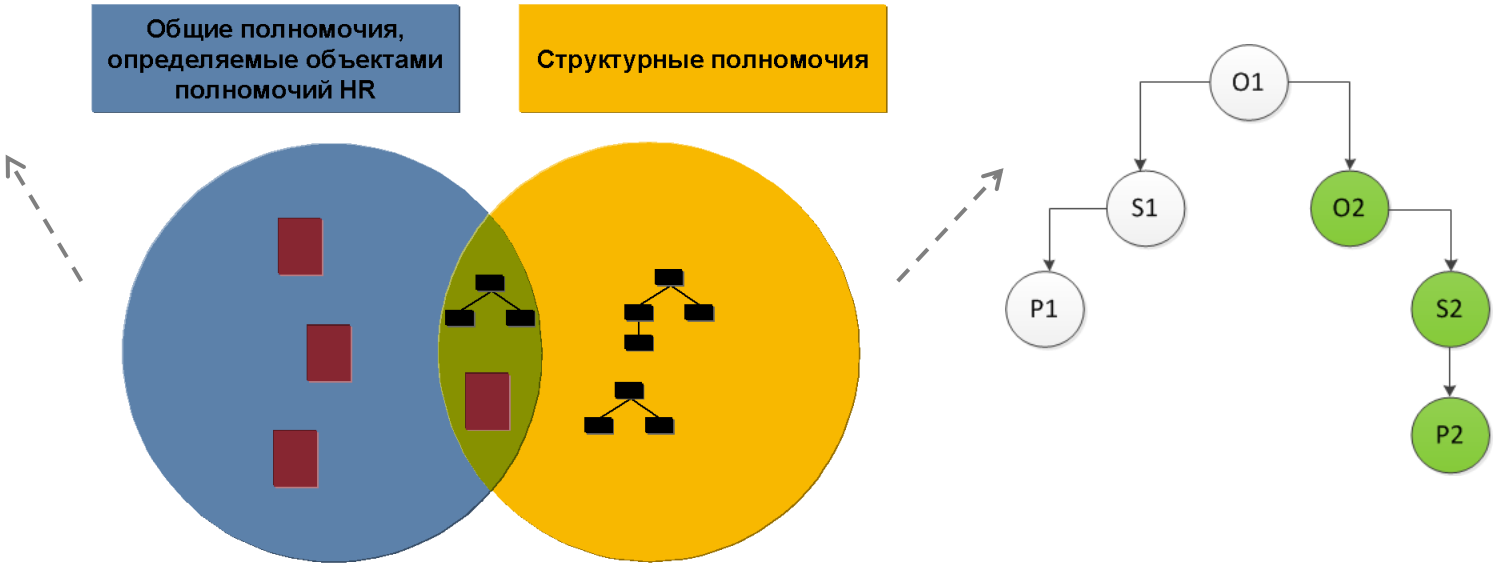


Сложно контролировать набор ролей пользователя

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

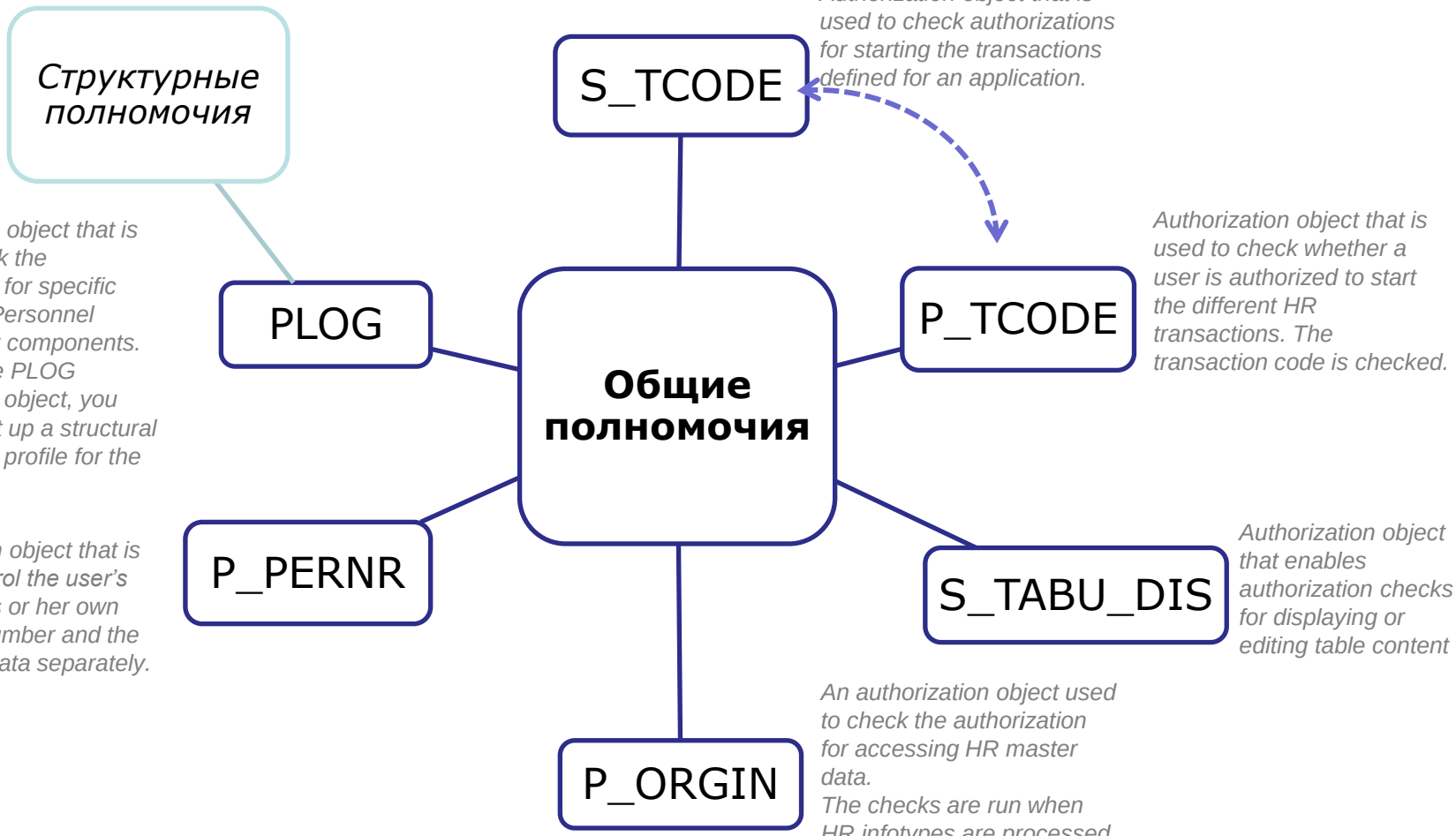
Данные о сотруднике
Домашний адрес
Чтение данных



Пересечение структурных и общих полномочий делает контроль доступа нетривиальной задачей

Общие полномочия в SAP HCM
В чем особенности?

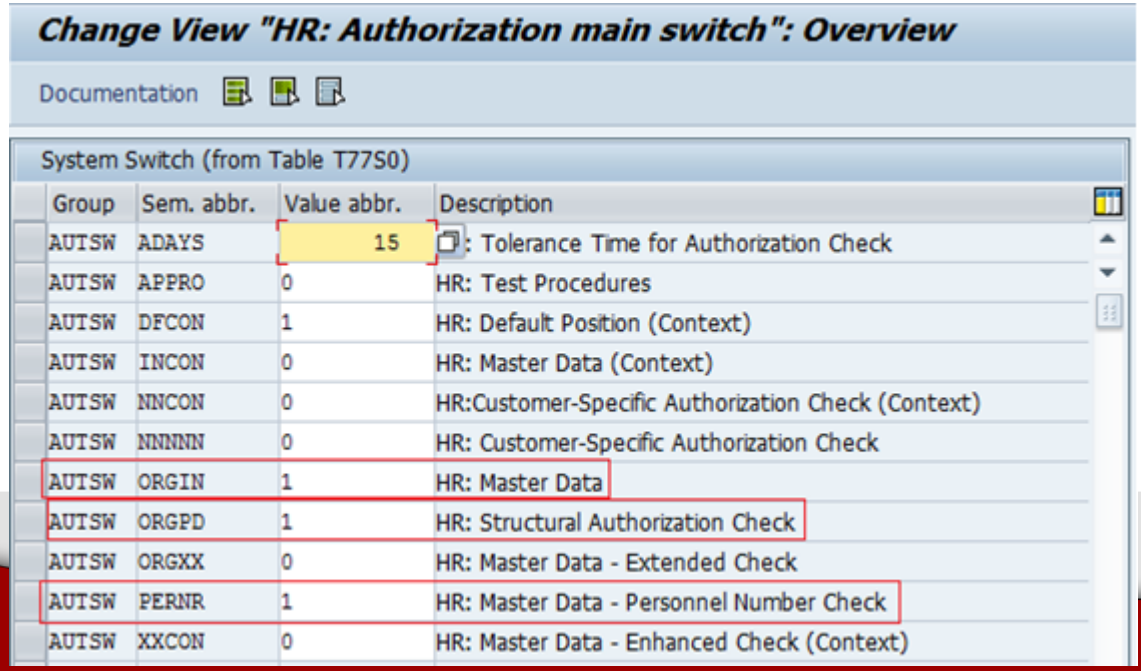
Полномочия = комбинация объектов авторизации



Настройки HR-авторизаций

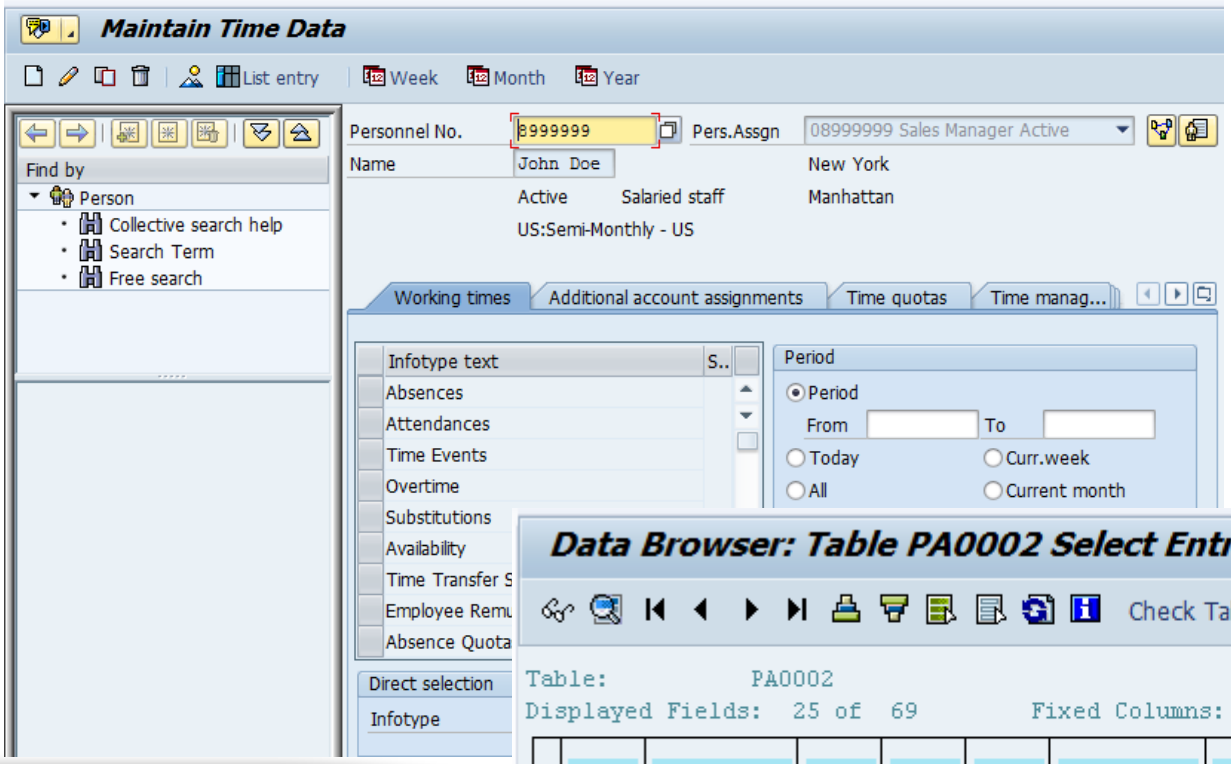
Транзакция **OOAC** (таблица **T77S0**)

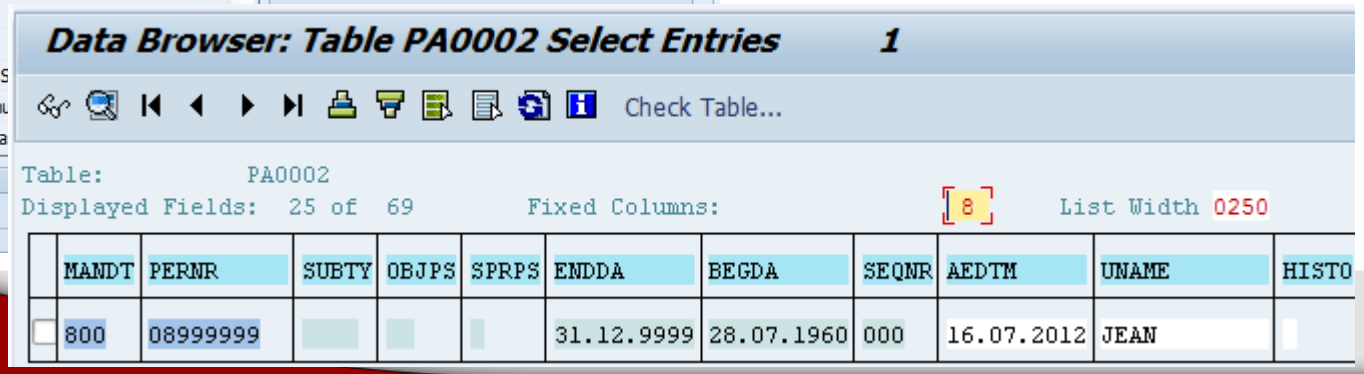
- **AUTSW–ORGIN** – Включение/выключение объекта авторизации P_ORGIN (доступ к данным HR)
- **AUTSW–PERNR** – Включение/выключение объекта авторизации P_PERNR (проверка собственного табельного номера)
- **AUTSW–ORGPD** – Включение/выключение проверки структурных полномочий



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**





POSITIVE TECHNOLOGIES

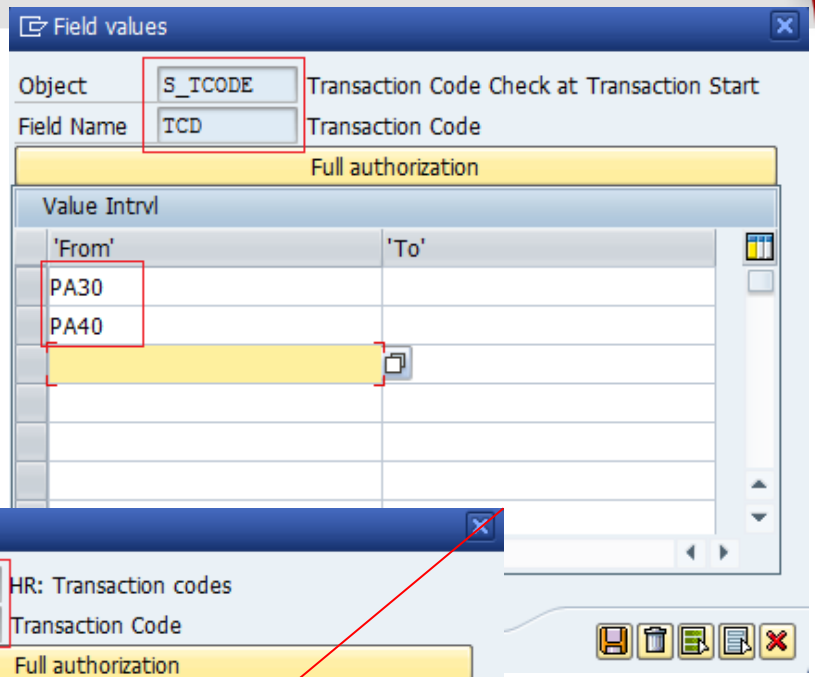
S_TCODE, P_TCODE - полномочия для запуска транзакции

S_TCODE – транзакции всех модулей

P_TCODE – только HR-транзакции

Настройки

Authorization Field	Description
TCD	Transaction Code



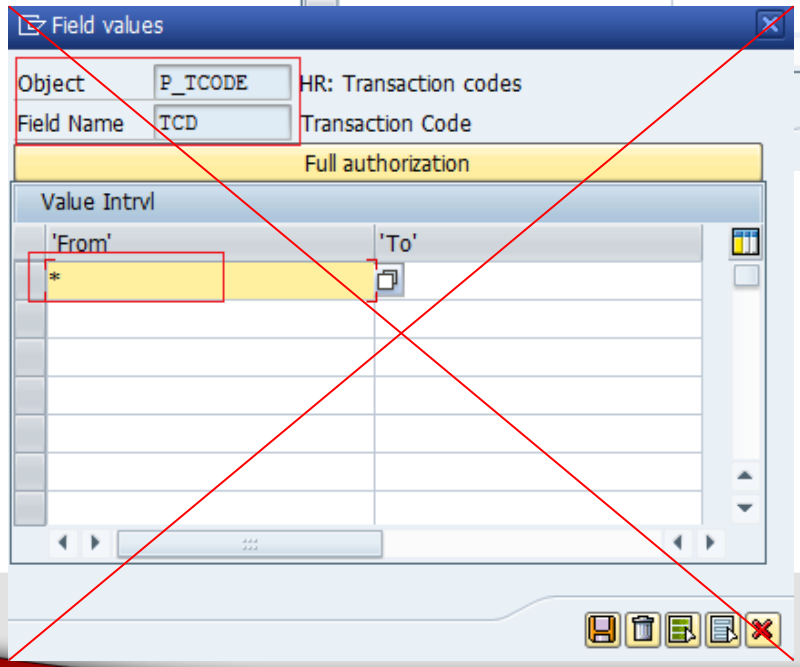
Типовые ошибки

Все транзакции

TCD = *

С … по …

TCD = ***PA01 – PA61***



POSITIVE TECHNOLOGIES

S_TABU_DIS - полномочия для доступа к таблицам

Необходим для транзакций SE16 и др.

Настройки

Authorization Field	Description	Values
DICBERCLS	Authorization group	**PA:** Employee data
ACTVT	Activity	**02:** Change **03:** Display

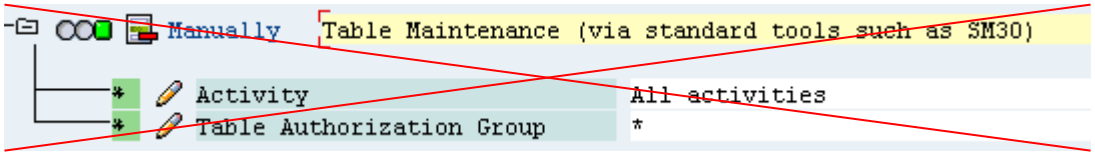
Типовые ошибки

Все группы таблиц

DICBERCLS = *****

Все действия

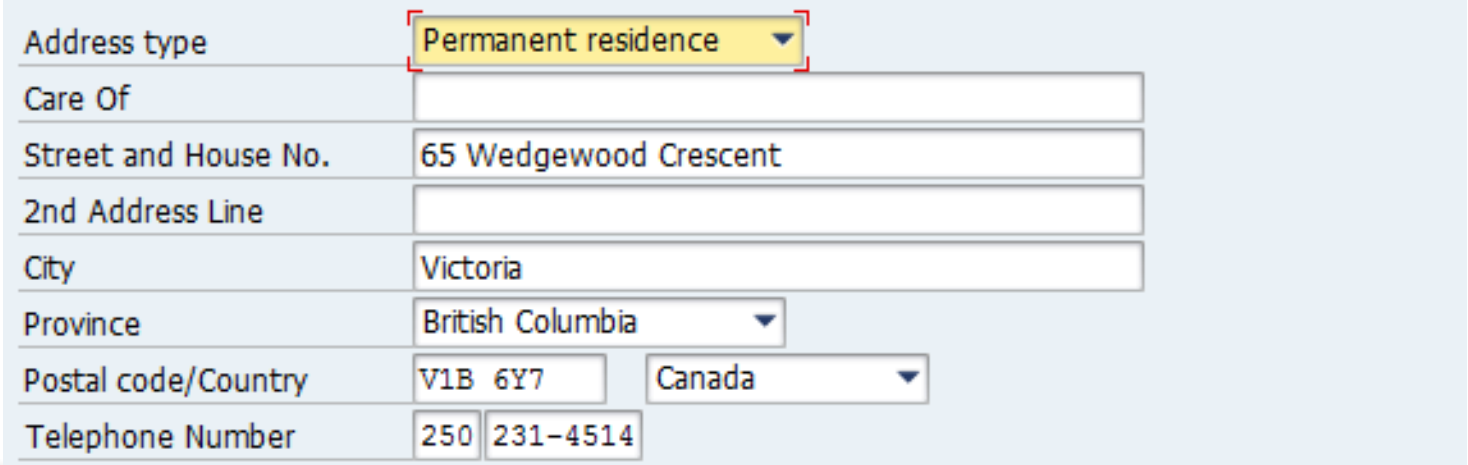
ACTVT = **All activities**



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



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)

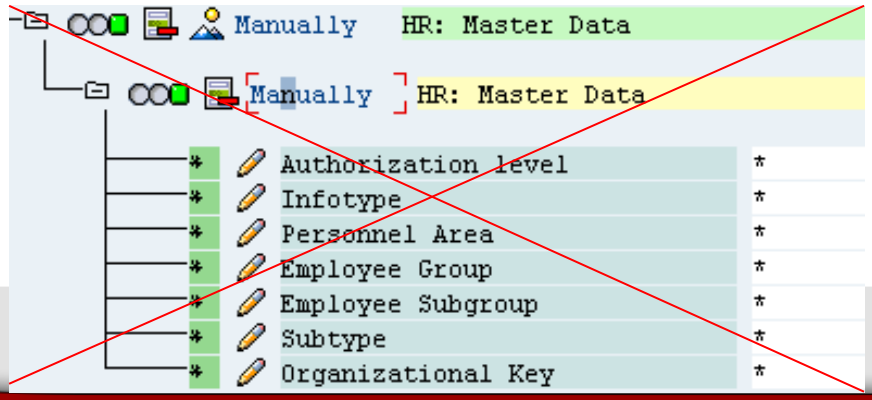
Типовые ошибки

Все действия

AUTHC = *

Все данные

INFT = *



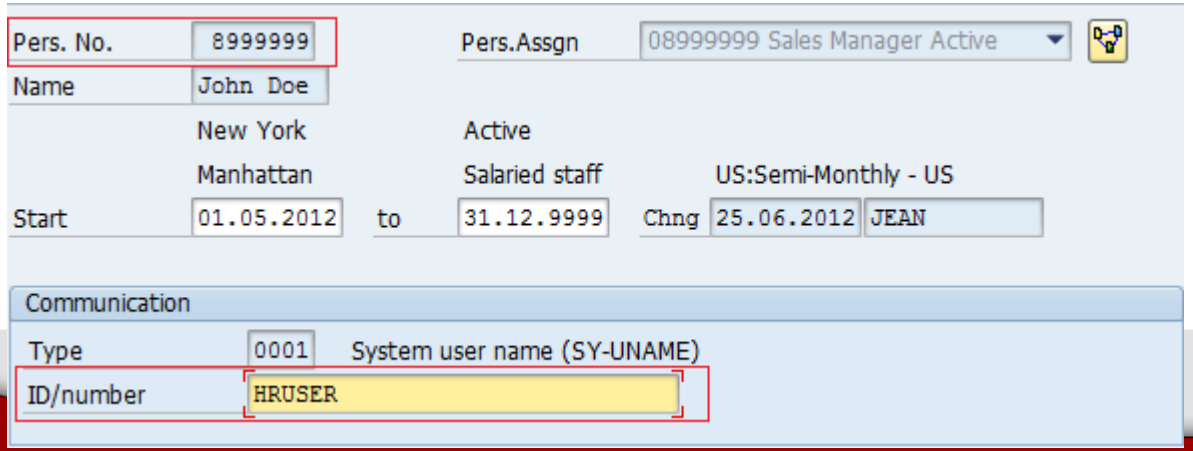
Ограничение по табельному номеру сотрудника

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



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

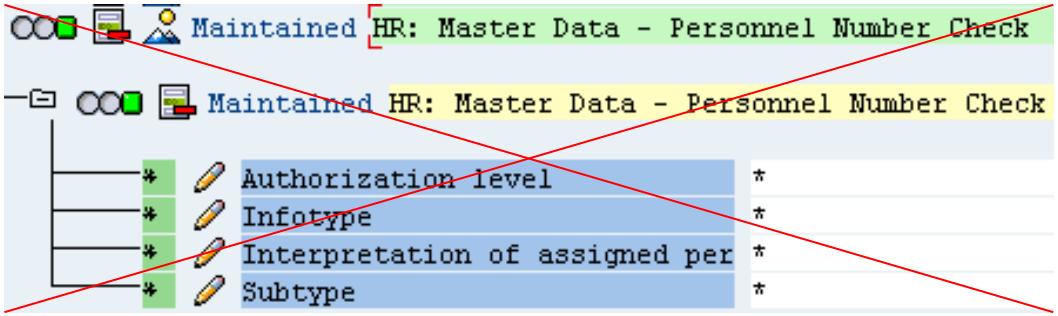
- *AUTHC* = *
- *PSIGN* = ***I***
- *INFTY* = *
- *SUBTY* = *

Неоднозначная трактовка

- *PSIGN* = * **= *I***

Можно все

- AUTHC = *
- PSIGN = *
- INFTY = *
- SUBTY = *



Отсутствие P_PERNR (*PSIGN = E)* тоже необходимо проверять!

Авторизации пересекаются

P_PERNR #1

AUTHC = *

PSIGN = **I**

INFTY = **0014**

SUBTY = **M***

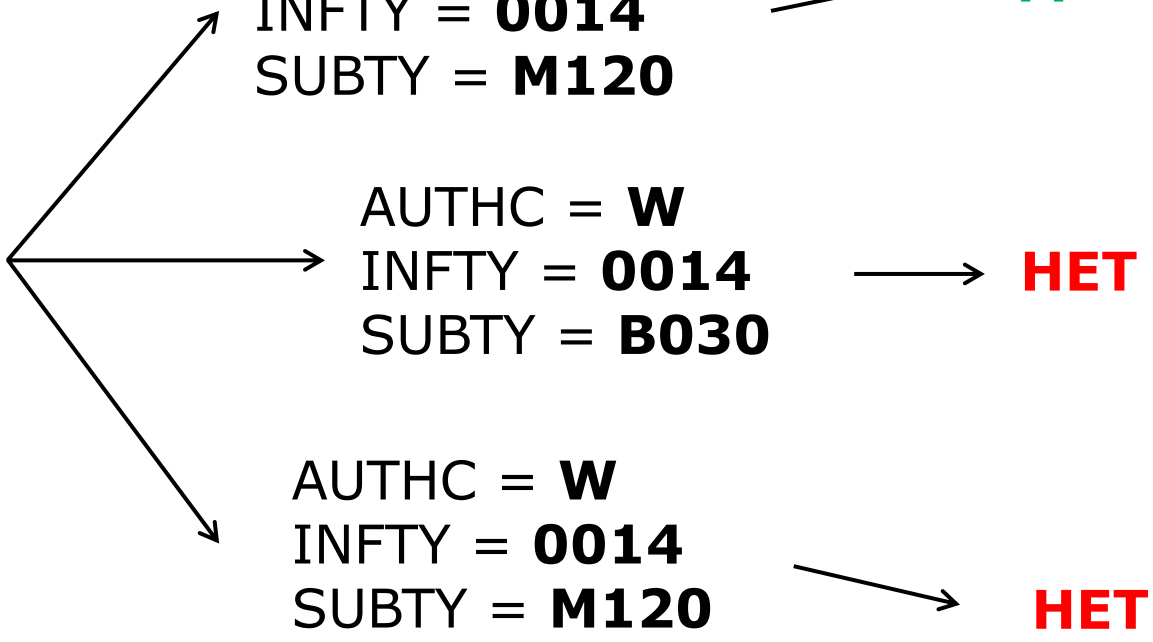
P_PERNR #2

AUTHC = **W**, **S**, **D**, **E**

PSIGN = **E**

INFTY = **0014**

SUBTY = *



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

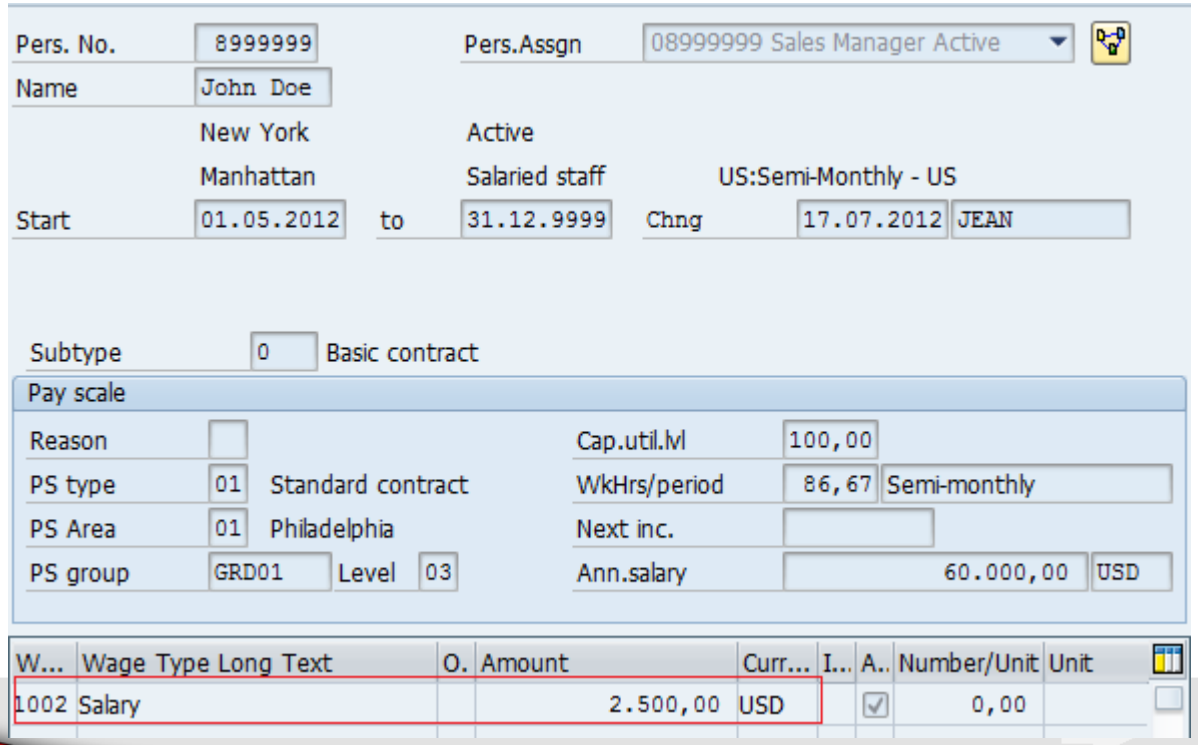
- Получить список пользователей, имеющих полномочия для просмотра данных о заработной плате других сотрудников
- Сравнить полученный список со списком пользователей, с утвержденными полномочиями выполнение данного действия

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)*



POSITIVE TECHNOLOGIES

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

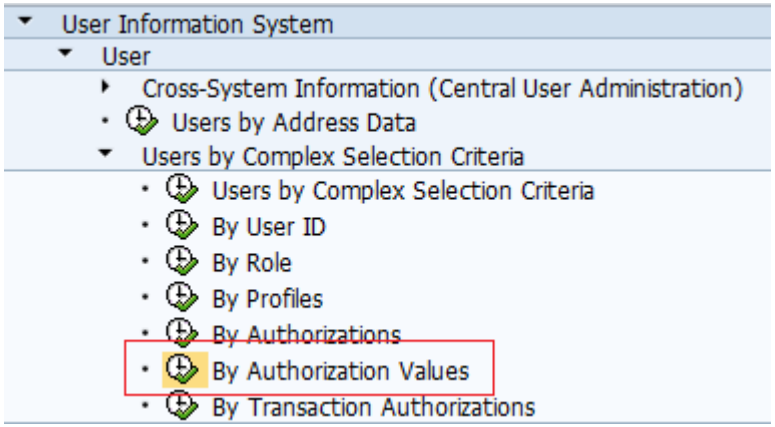
MANDT	PERNR	SUBTY	OBJPS	SPRPS	ENDDA	BEGDA	SEQNR	AEDTM	UNAME
800	08999999	0			31.12.9999	01.05.2012	000	17.07.2012	JEAN

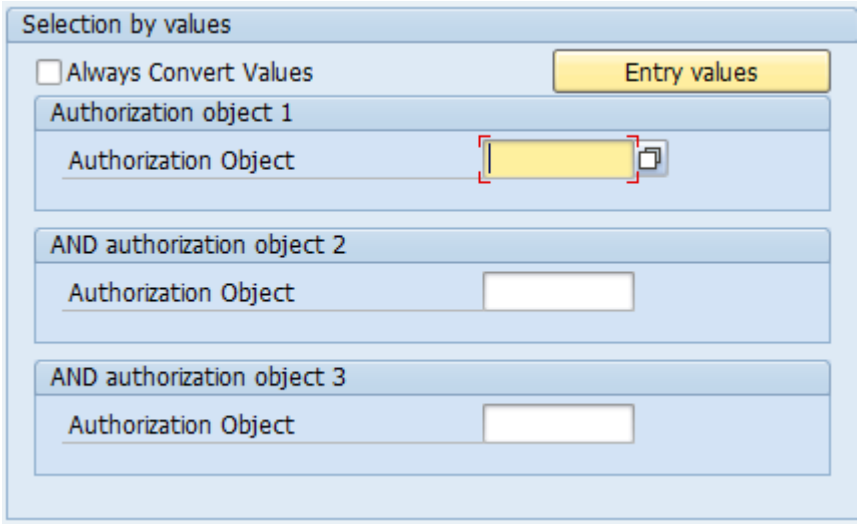
BSGRD	100,00
DIVGV	86,67
ANSAL	60.000,00
FALGK	
FALGR	
LGA01	1002
BET01	2.500,00
ANZ01	0,00
EIN01	
OPK01	
LGA02	
BET02	0,00
ANZ02	0,00

Выполнение проверок в SAP HCM

Транзакция **SUIM**:

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





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: *

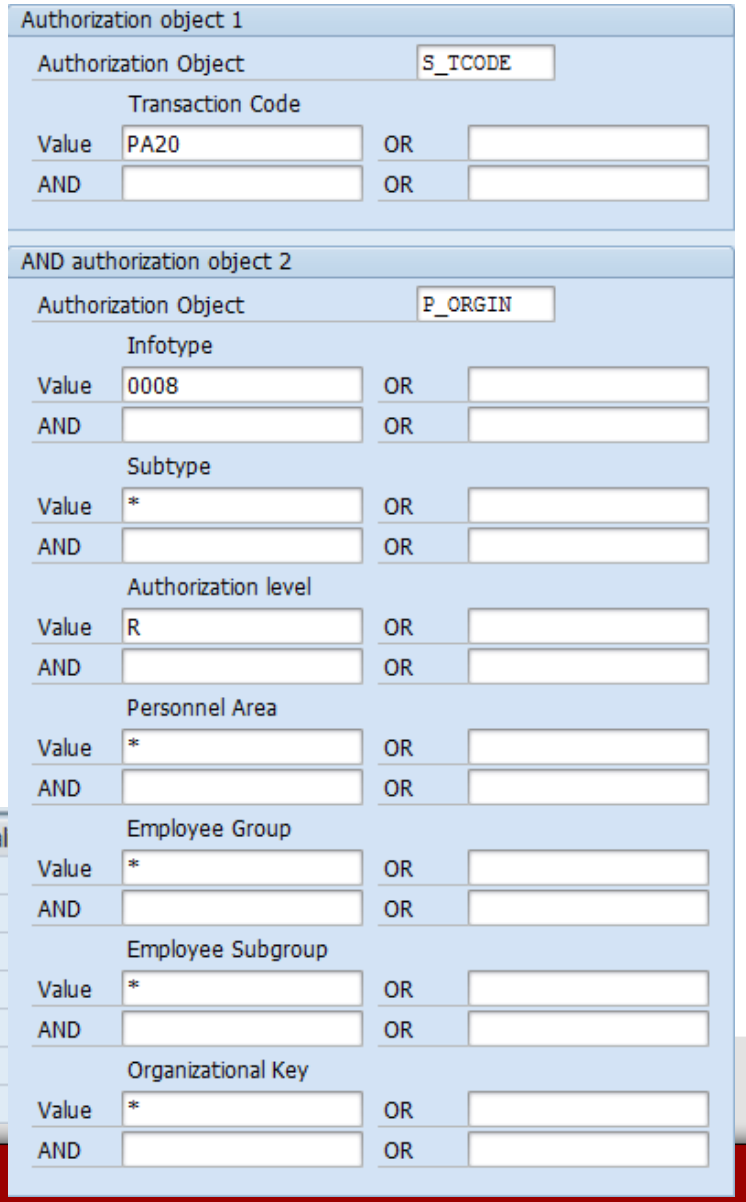
PERSK: *

VDSK1: *

INFTY: 0008

AUTHC: R

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:

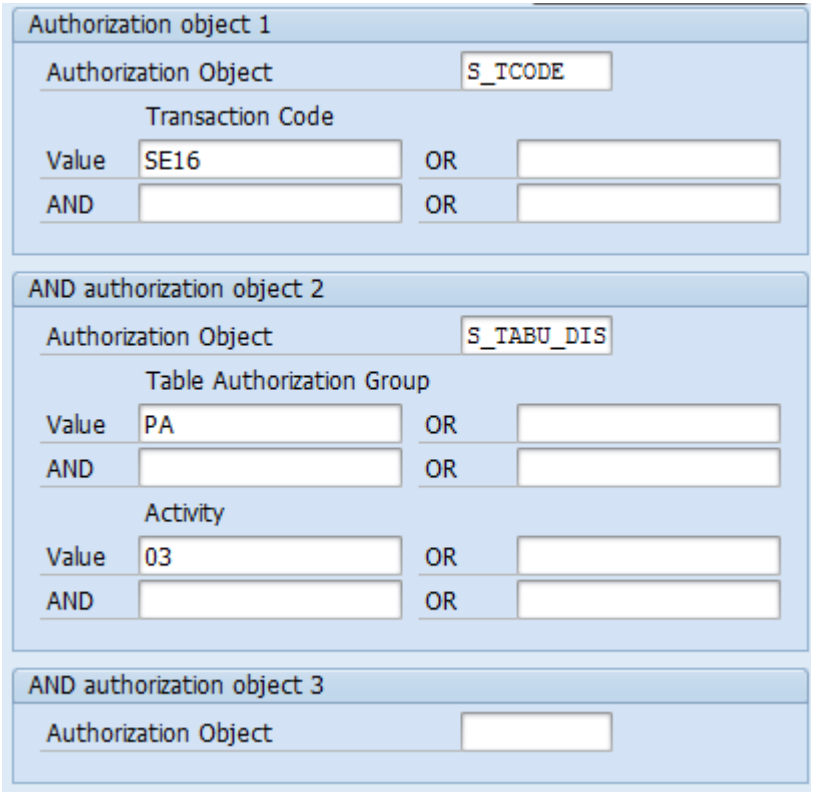
AUTHORIZATION OBJECT 1: **S_TCODE**

TCD: SE16 (Display HR Master Data)

AUTHORIZATION OBJECT 2: **S_TABU_DIS**

DICBERCLS: PA (Employee Data)

ACTVT: 03 (Display)



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 ANAO**
  - **Human Resource Information Systems**
  - **SAP ECC 6.0 Security and Control**
- **Блоги**
  - **http://saphr.ru**

Спасибо за внимание

Евгения Шумахер
eshumaher@ptsecurity.ru

POSITIVE TECHNOLOGIES