Реализация концепции ролей и полномочий в SAP ERP

Терентьев Илья Михайлович

Аннотация: в статье рассматриваются технические особенности подготовки и реализации ролей и полномочий в системе SAP ERP. Обсуждаются одиночные, наследуемые, композитные PFCG-роли, роли меню, а также состав матрицы ролей и полномочий. Анализируются два подхода к организации концепции ролей и полномочий в SAP: применение наследуемых ролей, уточняющих оргуровни и отдельно созданные роли для организационных уровней.

Введение

Вне зависимости от поставщика программного обеспечения концепция ролей и полномочий регламентирует доступ группам пользователей к всевозможным бизнес-объектам и соответствующим документам информационной системы. Часто порядок разграничения доступа называют SOD (segregation of duties). SOD – это превентивный контроль, чтобы не допустить концентрацию важных прав доступа в одних руках. Высококритичные операции должны быть разделены в программе на несколько этапов, каждый из которых выполняется разными людьми, что позволяет предотвратить мошенничество, а заодно и обезопасить сам процесс от ошибок.

Система SAP ERP позволяет строить подобные ограничения, имея в арсенале набор всевозможных технических средств: от объектов авторизации до композитных бизнес-ролей. Более того, среда ABAP позволяют гибко кодировать и модифицировать логику проверки полномочий. Давайте попытаемся раскрыть тематику ролей и полномочий для системы SAP ERP, что позволит обеспечить всесторонний взгляд на различные опции технической реализации.

Концептуальное представление логики ведения ролей и полномочий приведено в работе [1], интерпретируем его в терминах SAP. В ERP-системе готовится PFCG-роли, объединение которых будет порождать композитную или бизнес-роль. Именно бизнес-роль в дальнейшем присваивается конечному пользователю. Способ настройки PFCG и композитных ролей задаст концепцию авторизации. Для рассмотрения концепции следует проанализировать содержимое технических ролей.

Роль в системе SAP ERP представляет собой следующую тройку:

- определенный объект полномочий, включающий параметры организационного уровня и разрешенные операции над объектом данных;
- техническая роль PFCG, включающая коды транзакций SAP, а также объекты полномочий с указанными значениями параметров организационных уровней и операций, допустимых над объектами. Кроме того, в роли доступно указание кодов транзакций, которые будут отображаться в области SAP Easy Access для быстрого запуска программ;
- ABAP-код в транзакции, проверяющий объект полномочий и в зависимости от значения параметров выполняющий ту или иную бизнес логику. Одна транзакция в SAP может включать в себя проверку одного или нескольких объектов полномочий.

1. Настройка PFCG-ролей

Для настройки PFCG-роли функциональный консультант должен определить все объекты полномочий, относящиеся к требуемой транзакции, для чего можно воспользоваться SU21 или SU22. Далее создать техническую роль, внося в нее найденные объекты полномочий и указывая для них конкретные значения параметров. На финальном шаге осуществляется присвоение созданной роли пользователю SAP, например, через транзакцию SU02. Тогда в момент запуска пользователем той или иной транзакции, ABAP-логика выявит все подлежащие проверке объекты полномочий, далее проверит значения параметров этих объектов у пользователя, что доступно за счет присвоения пользователю PFCG-роли, и, наконец, выполнит бизнес-логику.

С точки зрения ведения PFCG-ролей следует выделить также ряд технических особенностей. Во-первых, в роли присутствуют объекты полномочий, включающие как оргуровни, так и без них. Во-вторых, несколько ролей можно объединить в одну композитную для удобства. В-третьих, возможно создавать наследуемые PFCG-роли, которые копируют значения объектов полномочий из исходной роли и заменяют лишь те из них, которые вручную определит функциональный консультант.

Введя все необходимые технические детали, зададим концепцию ролей и полномочий в SAP ERP и рассмотрим ее вариации. В первую очередь давайте опишем матрицу ролей и полномочий. Матрица представляет собой электронную таблицу, например, MS Excel, объединяющую в себе все данные, необходимые для технической настройки PFCG-ролей:

- объекты полномочий с указанными значениями параметров, объединенные в одиночные/наследуемые роли;
- одиночные/наследуемые роли, соединенные в композитную роль SAP, непосредственно присваиваемую пользователю. Обычно композитные роли называют бизнес-ролями, например, закупщик, складской сотрудник, бухгалтер и др.;
- а также для целей удобства перечень доступных транзакций в разрезе бизнес-ролей.

Тогда для рассмотрения доступны два типовых подхода к организации ролей в SAP ERP:

- ведение наследуемых ролей, уточняющих оргуровни;
- отдельно созданные роли с/без оргуровней.

Вне зависимости от выбираемого подхода обычно дополнительно создают новую PFCG-роль только для ведения меню транзакций в секции SAP Easy Access.

2. Стратегии ведения ролей в SAP

Первая стратегия ведения ролей в SAP подразумевает наличие четырех видов PFCG-ролей, среди которых можно выделить следующие:

- одиночные роли, каждая такая роль содержит объекты полномочий, связанные преимущественно с одной транзакцией. Для каждого параметра объекта полномочий указаны конкретные значения, за исключением оргуровней, которые остаются незаполненными;
- наследуемая роль, имеет ссылку на одиночную роль, тем самым наследует значения параметров всех объектов полномочий из исходной роли. В роли вручную указывается значение конкретного оргуровня;
- роль меню, необходимая для отображения иерархии папок и транзакций в видимой области SAP Easy Access;
- и, наконец, композитная роль, объединяющая в себе несколько наследуемых ролей и одиночных, если для них не ведется оргуровень, а также роль меню. Композитная роль задает бизнес-роль, понятную по смыслу всем пользователям.

Конечному пользователю присваивается лишь последняя роль: композитная. Большое число PFCG-ролей порождает необходимость их обособления, для чего ведутся правила наименования, например:

$$ZA\_BB\_CCCC\_DDDD\_EEEEEE, \quad (1)$$

где A – тип роли (S, I – одиночная или наследуемая роль), BB – технический код модуля (MM – закупки, SD – сбыт, FI – финансы, CO – контроллинг и др.), CCCC – объект (PURO – заказ на закупку, PURR – заявка на закупку, MATD – документ материала и др.), DDDD – операция (DISP – показать единичный документ, EDIT – изменить, REPT – отчет и др.), а EEEEEE – код оргуровня (001000 – завод 1000, 100001 – завод 1000 и склад 01 и др.), а также отдельная маска:

$$ZH\_BB\_FFFFFFFFF\_EEEEEE, \quad (2)$$

задающая две оставшиеся роли, где H – вид роли (C, M – композитная роль или роль меню), параметры BB и EEEEEE аналогичны (1), а FFFFFFFFF характеризует бизнес-роль (PURCHASER – закупщик, ACCOUNTANT – бухгалтер, STOCKER – кладовщик и др.). Для роли меню параметр EEEEEE из (2) может принимать константное значение, так как не зависит от оргуровня, к примеру: «XXXXXX». Основное преимущество подхода состоит в том, что, если изменились значения какого-либо объекта полномочий одиночной роли, они автоматически обновляются в наследуемой роли SAP.

Второй подход имеет схожие с первым моменты, но порядок заведения ролей состоит в следующем:

- создаются одиночные роли, подобно первому подходу, однако значения параметров, характеризующих организационные уровни, заполняются только в том случае, если они в последующем не будут ограничиваться, т.е. всегда принимают значения '*' (все). Кодировка ролей может вестись согласно (1);
- формируются дополнительные роли, включающие только объекты полномочий с оргуровнями. Нейминг для них похож на (2), но имеет незначительные отличия:

$$ZO\_BB\_FFFFFFFFF\_EEEEEE, \quad (3)$$

  в частности, начальный префикс 'ZO';

- роли меню и композитные роли заводятся аналогично первому подходу.

Таким образом, композитная роль содержит одиночную роль, роли организационного уровня и меню. Функционал по наследованию ролей здесь отсутствует, что делает метод весьма трудоемким к реализации. Как легко заметить из описания, текущий подход ориентирован на ситуацию, когда компания имеет распределенную орг-

структуру и одни и те же отделы в разных подразделениях могут иметь отличающийся доступ для обработки объектов.

Несмотря на кажущееся отличие двух подходов, они, в общем-то, об одном и том же: принципиальное отличие состоит лишь в использовании наследуемых ролей, что непременно является плюсом первого способа. Например, у вас есть две схожие роли, относящиеся к разным заводам 1000 и 2000, создаем одиночную роль без указания оргуровней и привязываем к ней две наследуемые роли каждого из заводов. Как результат, если что-то меняется в исходной роли, ее изменения автоматически наследуются связанным ролям через процедуру выравнивания. Теперь, представьте, что у вас ни один завод, а около сотни. Оцениваете объем сэкономленных трудозатрат на ведение ролей?

К сожалению, в случае создания Z-объекта полномочий стандартный механизм наследования ролей перестает работать. Что касается роли меню, то ситуация с ней следующая, от нее можно вообще отказаться и вести «дерево» транзакций SAP Easy Access в одиночной или наследуемой роли, проблема состоит в том, что если вы планируете присваивать пользователям более одной роли, список транзакций в навигационном меню пользователя будет дублироваться. Отдельная роль меню решает эту сложность.

Заключение

В заключении хочется отметить следующее. Система SAP обеспечивает гибкий функционал, позволяющий формировать различные стратегии разграничения полномочий. Концепция ролей и полномочий формируется заранее на базе выбранного подхода к технической реализации. Каких-либо преднастроенных типовых композитных ролей в системе SAP нет. Поэтому трудозатраты проектирования и реализации концепции достаточно велики и требуют выделение как минимум одного функционального SAP-консультанта.

Литература

1. Петров С.В. Стратегия ролей и полномочий в ERP-проектах // Корпоративные информационные системы. – 2018. – №3 – С. 53-58. – URL: https://corpinfosys.ru/archive/issue-3/143-2018-3-authorizationstrategy.

Выходные данные статьи

Терентьев И.М. Реализация концепции ролей и полномочий в SAP ERP // Корпоративные информационные системы. – 2022. – №4 (20) – С. 25-30. – URL: https://corpinfosys.ru/archive/issue-20/207-2022-20-segregationofduties.

Об авторе

Терентьев Илья Михайлович – эксперт по системам управления складами. Сертифицированный консультант SAP по модулю управление материальными потоками. Принимал участие более чем в 10 проектах имплементации корпоративных систем. Имеет обширный опыт внедрения складских систем в проектах «с нуля», а также тиражирования. Регулярно издает статьи в электронно-сетевом журнале «САПер». Электронный адрес: mail@corpinfosys.ru.