SoD-матрица как средство управления рисками в ERP-системе (на примере модуля MM в системе SAP R/3)

И. В. Илларионов, e-mail: igor.illarionov@gmail.com
С. Ю. Архипов, e-mail: arkhipov_sy@cs.vsu.ru

Воронежский государственный университет

Аннотация. *На основе матричного подхода к описанию SoD-рисков разработана матрица возможных SoD-рисков в модуле MM системы SAP R/3 и составлены технические описания полномочий, конституирующих выявленные SoD-риски.*

Ключевые слова: *SoD-риск, матрица SoD-рисков, риск-менеджмент, SAP, модуль MM, механизм авторизации.*

Введение

Риск-менеджмент как один из факторов, влияющих на организацию процесса управления информационными системами предприятий, вот уже на протяжении нескольких десятилетий является предметом неослабевающего интереса со стороны экспертного сообщества. Стремление минимизировать риски мошенничества, сознательных или случайных ошибок со стороны пользователей, разглашения конфиденциальной корпоративной информации и т.д., способных привести к серьезным финансовым и репутационным потерям для предприятия, неизбежно ставит перед экспертами, отвечающими за разработку и поддержку той или иной информационной системы, вопрос о наиболее оптимальных механизмах минимизации бизнес-рисков. Одним из средств минимизации угроз в информационных бизнес-системах на сегодняшний день является учет SoD-рисков в авторизационных политиках предприятий.

Под SoD (от англ. segregation of duties / separation of duties) в IT принято понимать такой принцип разграничения полномочий, когда никто из пользователей не может выполнить все этапы некоторого критичного процесса в системе и как следствие сознательно или случайно изменить / сфальсифицировать данные [1]. Примером, иллюстрирующим данное понятие, является пользователь, обладающий одновременно полномочиями на составление счетов и выполнение платежей. Обладая подобными правами, рассматриваемый пользователь может по ошибке или сознательно указать неверные сумму или реквизиты получателя (например, свои банковские реквизиты), а затем

произвести фактическую оплату по данному счету. В случае же, когда данные полномочия разделены между двумя пользователями риск сознательного или ошибочной фальсификации данных при фактурировании счета и выполнении оплаты по нему снижается. Таким образом, в случае SoD-рисков речь идет не о критичных полномочиях как таковых, а о критичных комбинациях полномочий.

Целью предлагаемого исследования является выявление и техническое описание SoD-рисков на примере модуля MM (управление материальными потоками) в системе SAP R/3. Выбор SAP-системы в качестве материала для нашего анализа обусловлен тем, что данная ERP-система, предлагаемая компанией SAP AG, является на текущий момент одной из наиболее востребованных ERP-систем, функционал которой покрывает практически все сферы деятельности крупного современного предприятия. В связи с этим принято делить обширный функционал системы SAP на отдельные модули, или компоненты: MM – управление материальными потоками, SD – сбыт, FI – финансы и т.д. В фокусе рассмотрения в рамках нашего исследования находятся SoD-риски в модуле MM, предназначенного для администрирования данных и процессов в сфере закупок товаров и/или услуг и инвентаризации материалов (товаров, запчастей и т.п.) на некотором предприятии.

1. Механизм авторизации в системе SAP R/3

Выше мы рассмотрели конкретный пример SoD-риска, однако данный пример был сформулирован в качестве вербального описания критичной комбинации полномочий пользователя. Такая формулировка малопригодна для использования разработчиком полномочий или администратором пользователей в некоторой SAP системе; им нужно понимать, какие технические объекты (транзакции, объекты полномочий и т.п.), позволяющие пользователям выполнить описанные действия, могут привести к SoD-конфликту. Иными словами, для эффективного учета SoD-рисков при разработке ролей и администрировании пользователей, вербальные описания SoD-рисков необходимо «перевести» в технические описания, составленные в опоре на те технические средства, которые используются для обеспечения авторизации в SAP. В связи с этим представляется целесообразным рассмотреть основные конструкты механизма авторизации в SAP.

Авторизация в SAP представляет собой реализацию модели RBAC (role-based access control). Суть данной модели авторизации состоит в том, что полномочия не присваиваются непосредственно каждому пользователю, а вводится промежуточный уровень между полномочиями и пользователями – роль. Именно роли присваиваются полномочия, а затем роль может быть присвоена одному или

нескольким пользователям. Модель RBAC используется для обеспечения авторизации во многих современных информационных системах и различается лишь техническими деталями реализации. Рассмотрим, как реализованы основные элементы данной модели – полномочие, роль, пользователь – в системе SAP R/3.

Минимальным конструктом механизма авторизации в SAP является объект полномочий. В SAP существует более 2000 стандартных объектов полномочий (кроме этого есть возможность создавать дополнительные объекты полномочий). Каждый объект полномочий предназначен для проверки прав доступа к определенным данным (например, доступ к данным заказов определенного вида, доступ к данным определенных складов и т.п.) и/или функциям (например, закладка закупочного заказа, изменение данных кредитора и т.п.) в SAP системе [2]. Объект полномочий имеет определенную внутреннюю структуру: он состоит из полей, число которых в зависимости от объекта полномочий варьируется от 1 до 10. Так, например, объект полномочий S_TABU_NAM, предназначенный для проверки прав доступа к таблицам, включает 2 поля – TABNAME, в котором задаются названия разрешенных таблиц, и ACTVT, в котором задаются коды разрешенных операций для разрешенных таблиц (например, просматривать, изменять и т.д.). Таким образом, объект полномочий выступает лишь структурой для создания полномочий. Для того, чтобы объект полномочий действительно предоставлял какие-то права, необходимо заполнить его поля конкретными значениями. Именно объект полномочий с заполненными полями называется в SAP полномочием [2] (и соответствует понятию «полномочие» в модели RBAC).

Уровень роли из модели RBAC представлен в SAP тремя конструктами – профилем, простой ролью и составной ролью. Рассмотренные выше полномочия должны быть встроены в профиль. Профиль по сути выступает контейнером для группировки полномочий [2]. В ранних версиях SAP профиль был конечным элементом в механизме авторизации, т.е. именно профиль присваивался пользователям. В современных версиях SAP профиль встроен в простую роль (single role). Если профиль является контейнером только для полномочий, то роль помимо собственно профиля содержит дополнительную информацию с описанием роли, список пользователей, обладающих данной ролью и т.п., а также имеет ряд функций, позволяющих частично автоматизировать генерацию профиля [2]. Несколько простых ролей могут быть объединены в составную роль (composite role).

Роли в SAP вносятся в учетную запись пользователя. Когда пользователь выполняет ту или иную транзакцию происходит проверка на наличие в присвоенных ему ролях тех полномочий, которые указаны в коде программы выполняемой транзакции [2].

2. Матричный подход к описанию SoD-конфликтов

Одним из наиболее распространенных подходов к техническому описанию SoD-рисков для некоторой системы выступает подход, заключающийся в разработке SoD-матрицы [3]. В рамках данного подхода SoD-риск представляется как пара двух конфликтующих функций. Под функцией при этом понимается перечень изофункциональных полномочий, т.е. различных полномочий, позволяющих пользователю выполнить одну и ту же задачу, или функцию, в системе [2-3]. Так, например, просмотреть основные данные клиента в SAP можно различными способами: через транзакции VD03, XD03, VD02, XD02, FD03, FD02, XD99 и т.д. Данные транзакции не идентичны сами по себе: они различаются режимом доступа (изменение/просмотр), ракурсом (сбытовой/финансовый), массовой/поштучной обработкой дебиторов и т.д., но так или иначе через каждую из данных транзакций можно посмотреть основные данные дебиторов, т.е. все они позволяют реализовать функцию «просмотр основных данных клиента». Обычно функции в рамках матричного подхода принято описывать с помощью таблиц со структурой, представленной в табл. 1 [3].

Таблица 1

Техническое описание функции «просмотр данных клиента»

группа полномочий	объект полномочий	поле	начальное значение	конечное значение	оператор
FD03	F_KNA1_APP	ACTVT	03		
FD02	F_KNA1_APP	ACTVT	02		OR
FD02	F_KNA1_APP	ACTVT	03		OR
…					

Каждая группа полномочий в данной таблице представляет собой набор полномочий, позволяющий выполнить соответствующую функцию [3]. Иными словами, группа полномочий служит для демаркации границ автономных изофункциональных полномочий: каждая группа полномочий в отдельности предоставляет пользователю права на выполнении заявленной функции (в данном случае функции «просмотр данных дебитора»). Таким образом, группы полномочий внутри функции связаны дизъюнктивно: пользователю достаточно

иметь полномочия из одной группы, чтобы обладать правами на выполнение рассматриваемой функции (просмотр дебиторов). Обычно колонка «группа полномочий» заполняется либо кодом транзакции, если указанные далее объекты полномочий связаны с конкретной транзакцией, либо просто уникальной букво-численной комбинацией, если указанные далее объекты полномочий не связаны с определенной транзакцией [3].

Далее в колонках «объект полномочий», «поле» (объекта полномочий), «начальное значение» и «конечное значение» (поля объекта полномочий) приводится детальное техническое описание соответствующего полномочия [3] (в таблицах, приводимых в следующем разделе, колонка «конечное значение» опущена, поскольку указание диапазона значений нерелевантно для выявленных SoD-рисков). При этом, если в колонке «группа полномочий» в соответствующей строке указан код транзакции, то доступ к транзакции и указанное полномочие всегда связаны конъюнктивно, т.е. пользователю необходимо иметь и доступ к транзакции, и указанное полномочие, чтобы считаться пользователем, обладающим правами на выполнение рассматриваемой функции [3].

Если некоторая группа полномочий состоит не из одного, а нескольких полномочий, в колонке «оператор» указывается, как связаны перечисленные полномочия внутри данной группы (OR или AND) [3].

Таким образом при разработке SoD-матрицы для некоторой системы следует начать с определения всех функций, входящих в состав SoD-рисков, и составления технических дефиниций для данных функций, т.е. заполнения таблиц с указанной выше структурой, содержащих техническое описание всех возможных полномочий, позволяющих выполнить анализируемую функцию. На следующем этапе, после того как будут исчислены все функции, входящие в состав SoD-рисков, и для них будут составлены технические описания, можно составить матрицу SoD-рисков. Матрица SoD-рисков представляет собой квадратную матрицу, по обеим сторонам которой перечислены релевантные для описания SoD-рисков функции, а на пересечении строки и колонки двух функций, вызывающих SoD-риск, отмечается наличие SoD-риска. Поскольку две конфликтующие функции вызывают SoD-риск вне зависимости от очередности их указания, то, очевидно, что матрица SoD-рисков симметрична относительно главной диагонали.

3. SoD-матрица для модуля MM

Для выявления потенциальных SoD-рисков на первом этапе исследования был проведен анализ специальной литературы, посвященной описанию бизнес-процессов, администрируемых в модуле

MM в SAP. Это позволило выявить 5 потенциальных SoD-рисков. На следующем этапе с помощью метода трассировки полномочий были составлены технические описания полномочий из функций, конституирующих выявленные SoD-риски.

Первый SoD-риск представлен конфликтом следующих функций: «создание/изменение основных данных кредитора» и «создание/изменение закупочного заказа». Риск, возникающий в случае реализации данного SoD-конфликта, заключается в том, что пользователь может одновременно изменять основные данные кредитора, в частности банковские реквизиты кредитора, и создавать или изменять закупочные заказы. Таким образом, у пользователя появляется возможность сфальсифицировать банковские реквизиты некоторого поставщика, а затем создать заказ с этим поставщиком (или же изменить поставщика в существующем заказе), в результате чего будут созданы условия для перевода денежных средств предприятия на сфальсифицированный счет, хотя с технической точки зрения проведенный процесс закупки будет корректным. В табл. 2 и 3 представлены полученное с помощью трассировки технические описания полномочий, предоставляющих доступ к обеим фунциям.

Таблица 2

Функция «создание/изменение основных данных кредитора»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
XK01	F_LFA1_APP	ACTVT	01	
XK02	F_LFA1_APP	ACTVT	02	
MK01	F_LFA1_APP	ACTVT	01	
MK02	F_LFA1_APP	ACTVT	02	
XK99	F_LFA1_APP	ACTVT	01	OR
XK99	F_LFA1_APP	ACTVT	02	OR

Таблица 3

Функция «создание/изменение закупочного заказа»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
ME21	M_BEST_EKO	ACTVT	01	
ME22	M_BEST_EKO	ACTVT	02	
ME21N	M_BEST_EKO	ACTVT	01	
ME22N	M_BEST_EKO	ACTVT	02	
MEMASSPO	M_BEST_EKO	ACTVT	01	OR
MEMASSPO	M_BEST_EKO	ACTVT	02	OR

Второй анализируемый SoD-риск заключается в конфликте функций «создание/изменение закупочного заказа» и «одобрение закупочного заказа». Риск заключается в следующем: пользователь, способный одновременно создавать и одобрять закупочные заказы, чреват для предприятия тем, что нежелательный / неоптимальный с точки зрения бизнес-процесса заказ будет одобрен и тем самым передан на выполнение поставщику. При этом, пользователь, который закладывал закупочный заказ, потенциально может в случае сговора с некоторым поставщиком заменить изначального поставщика на нужного ему (даже если это экономически невыгодно предприятию) или же по недосмотру допустить ошибку при создании заказа. В данной ситуации, если одобрении закупочного заказа будет осуществляться другим пользователем (не тем, который создавал заказ), то шансов выявить ошибки или манипуляции, допущенные в отношении заказа, сравнительно выше, чем в случае, когда создание и одобрение заказа производит один и тот же пользователь. Техническое описание полномочий, предоставляющих доступ к функции «создание/изменение закупочного заказа» представлено выше (см. табл. 3), а к функции «одобрение закупочного заказа» – в табл. 4.

Таблица 4

Функция «одобрение закупочного заказа»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
ME28	M_EINK_FRG	FRGGR	‘ ’[1]	

Третий SoD-риск образован конфликтующими функциями «создание/изменение закупочного заказа» и «проводка поставленного материала». Данный риск делает возможным следующий сценарий, способный нанести урон предприятию: сотрудник, обладающий полномочиями для обеих названных выше функций, может, вступив в сговор с некоторым поставщиком, создать в системе закупочные заказы

[1] Обозначение ‘ ’ используется при описании полномочий в SAP для указания на любое значение. В данном случае невозможно указать конкретное значение для поля объекта полномочий, поскольку список возможных значений, ассоциированный с данным полем, предоставляется не разработчиками SAP, а формируется на основании данных в настроечных таблицах, которые каждый клиент SAP настраивает в соответствие со спецификой своего бизнес-процесса.

для данного поставщика, а затем подтвердить поступление товара по данным заказам без реальной поставки заказанного товара, в результате чего предприятие вновь может понести финансовые потери, произведя оплату за фиктивные поставки. Полученные нами с помощью трассировки технические описания полномочий, предоставляющих доступ к конфликтующим функциям в рамках данного SoD-риска, представлены в табл. 3 и 5.

Таблица 5

Функция «проводка поставленного материала»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
MIGO	M_MSEG_WWE	ACTVT	01	
MB01	M_MSEG_WWE	ACTVT	01	
MB0A	M_MSEG_WWE	ACTVT	01	

Четвертый выявленный SoD-риск образован конфликтующими функциями «создание счета-фактуры для поставщика» и «выполнение платежа». Следует заметить, что данный SoD-риск представляет собой пример кросс-модульного риска: функция «создание счета-фактуры для поставщика» относится к рассматриваемому модулю MM, в то время как функция «выполнение платежа» локализована в модуле FI. Риск в данном случае заключается в следующем: пользователь, одновременно обладающий правами на фактурирование счета и на оплату счетов за поставки по заказам, может при фактурировании счета изменить кредитора или изменить условия оплаты, а затем запустить платеж, в результате которого сумма, предназначенная для оплаты поставленного товара, будет переведена либо на сфальсифицированный счет, либо не в том объеме, которые предусматривали изначальные условия поставки. В табл. 6 и 7 приведены технические дефиниции полномочий из обеих функций, вызывающих данный SoD-риск.

Таблица 6

Функция «создание счета-фактуры для поставщика»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
MIRO	M_RECH_WRK	ACTVT	01	

Таблица 7

Функция «выполнение платежа»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
FF110	F_REGU_BUK	BUKRS	‘ ’	

Пятый из выявленных на первом этапе анализа SoD-рисков представляет собой конфликт функций «проводка движения материала» и «ведение инвентаризации» (см. техническое описание полномочий, относящихся к обеим функциям, в табл. 8 и 9). Риск, возникающий в случае данного SoD-конфликта, заключается в том, что у пользователя одновременно появляются права создание документов, подтверждающих движение материалов, например, фактические поступление заказанного материала на склад, перемещение материала с одного склада на другой, забор материала со склада и т.д., и вместе с тем на создание документов, отражающих результаты инвентаризации, т.е. проверки результата состояния складов. В данной ситуации перед пользователем, обладающим данными полномочиями, открывается возможность скрыть выявленную в ходе инвентаризации нехватку того или иного материала на некотором складе за счет создания фиктивных документов, подтверждающих движение материалов.

Таблица 8

Функция «создание счета-фактуры для поставщика»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
MIGO	M_MSEG_WWE	ACTVT	01	OR
MIGO	M_MSEG_WWE	ACTVT	01	OR
MIGO	M_MSEG_WWF	ACTVT	01	OR
MB01	M_MSEG_WWE	ACTVT	01	
MB0A	M_MSEG_WWE	ACTVT	01	
MB11	M_MSEG_WWA	ACTVT	01	
MB1A	M_MSEG_WWA	ACTVT	01	
MB1B	M_MSEG_WWA	ACTVT	01	
MB1C	M_MSEG_WWA	ACTVT	01	
MB31	M_MSEG_WWF	ACTVT	01	

Таблица 9

Функция «создание счета-фактуры для поставщика»

группа полномочий	**объект полномочий**	**поле**	**начальное значение**	**оператор**
MI04	M_ISEG_WZL	ACTVT	01	
MI05	M_ISEG_WZL	ACTVT	02	
MI07	M_ISEG_WDB	ACTVT	01	
MI08	M_ISEG_WZB	ACTVT	01	

На завершающем этапе нашего исследования мы систематизировали информацию о выявленных в ходе анализа SoD-рисках для модуля MM в виде матрицы SoD-рисков (см. табл. 10).

Таблица 10

Матрица SoD-рисков для модуля MM в системе SAP R/3

	Ф1	Ф2	Ф3	Ф4	Ф5	Ф6	Ф7	Ф8
Ф1		риск 1						
Ф2	риск 1		риск 2	риск 3				
Ф3		риск 2						
Ф4		риск 3						
Ф5						риск 4		
Ф6					риск 4			
Ф7								риск 5
Ф8							риск 5	

Условные обозначения функций: Ф1 – создание/изменение основных данных кредитора; Ф2 – создание/изменение закупочного заказа; Ф3 – одобрение закупочного заказа; Ф4 – проводка поставленного материала; Ф5 – создание счета-фактуры для поставщика; Ф6 – выполнение платежа; Ф7 – проводка движения материала; Ф8 – ведение инвентаризации.

Заключение

В результате проведенного анализа выявлены 5 SoD-рисков, релевантных для модуля MM в системе SAP R/3 и составлены технические описания функций, вызывающих рассмотренные SoD-риски. Анализ позволяет заключить, что SoD-риски существуют и требуют учета не только в таких традиционно «рискованных» сферах бизнес-процесса как финансы, но и в области ведения материальных потоков. Результаты анализа могут найти практическое применение при разработке ролей и администрировании пользователей в системе SAP.

Литература

1. Wilding E. Information Risk and Security: Preventing and Investigating Workplace Computer Crime / E. Wilding. – Burlington : Gower, 2006. – 341 p.

2. Lehnert V. SAP-Berechtigungswesen: Konzeption und Realisierung / V. Lehnert. – 3. Auflage. – Bonn: Rheinwerk, 2016. – 847 S.

3. Folkerts B. Praxishandbuch für die Risikoanalyse mit SAP GRC Access Control / B. Folkerts. – Gleichen : Espresso Tutorials GmbH, 2019. – 172 S.