Математические структуры и моделирование
2009, вып. 19, с. 108–113

УДК 65.012.810

МОДЕЛИРОВАНИЕ РОЛЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ В СООТВЕТСТВИИ СО СТАНДАРТОМ СТО БР ИББС-1.0-2008

Ю.С. Ракицкий, С.В. Белим

В статье рассматривается вопрос моделирования ролевой политики безопасности в соответствии с ее описанием в стандарте Банка России для организаций банковской системы Российской Федерации.

Введение

Анализ различных организационно - управленческих и организационно - технологических схем показывает, что в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как определенную роль, представляет некоторую абстрактную, точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий. Ролевое разграничение доступа является развитием политики дискреционного разграничения доступа, при этом права доступа субъектов системы (т.е. сотрудников предприятия, занимающих определенную должность) на объекты с учетом специфики их применения, образуя роли.

Ярким примером описанных предприятий являются коммерческие банки. Учитывая законодательство в области банковской деятельности (ст. 26 «Банковская тайна» закона «О банках и банковской деятельности» и закон «О персональных данных»), проблема обеспечения информационной безопасности компьютерных систем в организациях банковской системы является весьма актуальной. Центральный Банк Российской Федерации (Банк России) выпустил серию документов, посвященных обеспечению информационной безопасности

Омский государственный университет им. Ф.М. Достоевского.
E-mail: yrakitsky@rambler.ru

организаций банковской системы. Одним из таких документов является стандарт Банка России СТО БР ИББС-1.0-2008 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации». Авторы данного стандарта предлагают при построении политики информационной безопасности определить и разграничить роли сотрудников банка.

1. Описание политики информационной безопасности в стандарте СТО БР ИББС-1.0-2008

Согласно пункту стандарта 7.2.1 «Роль – это заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом, например сотрудником организации, и объектом, например программно - аппаратным средством. Для эффективного выполнения целей организации и задач по управлению активами должны быть выделены и определены соответствующие роли персонала организации». Таким образом, в любой автоматизированной компьютерной системе предоставление доступа должно осуществляться в соответствии с ролевой моделью разграничения доступа.

Согласно пункту стандарта 7.2.3 «Не рекомендуется, чтобы одна персональная роль целиком отражала цель, например включала все правила, требуемые для реализации бизнес-процесса. Совокупность правил, составляющих роли, не должна быть критичной для организации с точки зрения последствий успешного нападения на ее исполнителя. Не следует совмещать в одном лице (в любой комбинации) роли разработки, сопровождения, исполнения, администрирования или контроля, например, исполнителя и администратора, администратора и контролера или других комбинаций». Таким образом, выделяются роли исполнителей, контролеров, администраторов и сопровождения, которые должны в какой-либо комбинации присутствовать в любом процессе в каждой автоматизированной компьютерной системе.

Согласно пункту стандарта 7.2.4 «Роль должна быть обеспечена ресурсами, необходимыми и достаточными для ее исполнения». Следовательно, любая роль не должна содержать избыточных прав доступа в автоматизированной компьютерной системе, то есть не должна обладать доступом к объектам, которые не используются при исполнении данной роли. Например, сотрудник банка, оформляющий в автоматизированной системе заявки на выдачу кредита клиенту банка не должен иметь доступ к информации о принятии вкладов от населения, но при этом должен обладать правами доступа на просмотр и редактирование анкетных данных клиентов, подавших заявку на получение кредита.

Приведенные выше требования являются частью общих требований по обеспечению информационной безопасности при назначении и распределении ролей и обеспечении доверия к персоналу. На основании этих требований можно сформулировать формальную модель ролевой политики безопасности в соответствии со стандартом СТО БР ИББС-1.0-2008.

2. Формализация политики безопасности

Базовая модель ролевого разграничения доступа включает в себя следующие множества: U — множество пользователей, R -– множество ролей, P – множество прав на работу в системе. Важную роль играет отображение

$$PA: \ R \longrightarrow 2^P, \tag{1}$$

определяющее множество прав доступа для заданной роли, при этом для каждого $p \in P \ \exists \ r \in R$ такая, что $p \in PA(r)$.

Для введения в модель контролирующих функций необходимо множество ролей R, которые в дальнейшем будем называть исполнительскими, дополнить множеством административных ролей ACR и множеством контролирующих ролей CR. При этом

$$R \cap ACR = \oslash, ACR \cap CR = \oslash, R \cap CR = \oslash. \tag{2}$$

Введем дополнительные множества: ACP — множество прав для административных ролей, CP — множество прав для контролирующих ролей. Множества P, CP и ACP также не имеют общих элементов. ACR осуществляют администрирование контролирующих ролей.

Для каждого права $p \in P$ должно быть определено множество контролирующих прав, обладание которыми необходимо для контроля над p. Введем соответствующее отображение

$$ControlRight: \ P \longrightarrow 2^{CP}, \tag{3}$$

при этом $\forall p \in P \ ConrolRight(p) \neq \oslash$.

Для любой роли также должен существовать набор контролирующих ролей, осуществляющих контроль над ней. Введем отображение

$$ControlRole: R \longrightarrow 2^{CR}, \tag{4}$$

при этом

$$PA(r) = p_{i1}, p_{i2}, ..., p_{in} \Rightarrow PA(ControlRole(r)) = \bigcup ControlRight(p_{ij}). \tag{5}$$

Определение 1. В системе выполняются функции контроля, если в любой момент времени для любого $p \in P \ \exists \ cp_{i1}$, cp_{i2}, ..., $cp_{in} \subseteq CP$ такое, что cp_{i1}, cp_{i2}, ..., $cp_{in} \subseteq ControlRight(p)$, а для любой $r \in R \ \exists \ cr_{k1}$, cr_{k2}, ..., $cr_{kl} \subseteq CR$ такое, что cr_{k1}, cr_{k2}, ..., $cr_{kl} \subseteq ControlRole(r)$.

Аналогично введем отображение

$$AdminRight: CP \longrightarrow 2^{ACP}, \tag{6}$$

при этом $\forall p \in P \ AdminRight(p) \neq \oslash$.

Введем отображение

$$AdminRole: \ CR \longrightarrow 2^{ACR}, \tag{7}$$

при этом

$$PA(cr) = cp_{i1}, cp_{i2}, ..., cp_{in} \Rightarrow PA(AdminRole(ar)) = ap_1, ap_2, ..., ap_m. \tag{8}$$

Определение 2. В системе выполняются функции администрирования, если в любой момент времени для любого $cp \in CP \; \exists \; ap_{i1}$, ap_{i2}, ..., $ap_{in} \subseteq ACP$ такое, что ap_{i1}, ap_{i2}, ..., $ap_{in} \subseteq AdminRight(cp)$, а для любой $cr \in CR \; \exists \; ar_{k1}$, ar_{k2}, ..., $ar_{kl} \subseteq ACR$ такое, что ar_{k1}, ar_{k2}, ..., $ar_{kl} \subseteq AdminRole(cr)$.

Аналогичным образом можно выделить в системе роли разработки и сопровождения.

3. Соответствие модели стандарту СТО БР ИББС-1.0-2008

Теперь покажем, что построенная модель соответствует требованиям стандарта СТО БР ИББС-1.0-2008.

Теорема 1. *Построенная модель удовлетворяет требованиям стандарта СТО БР ИББС-1.0-2008.*

Доказательство. Для доказательства теоремы необходимо показать, что введенные отображения соответствуют требованиям стандарта, и, наоборот, для каждого требования стандарта существует соответствующее отображение. Как было показано в пункте 2, в стандарте ролевой политике безопасности посвящено три пункта.

Согласно пункту 7.2.1 разграничение доступа должно производиться по ролевому принципу, что очевидно выполняется.

Согласно пункту 7.2.3 должны существовать исполнительские, административные, контролирующие роли, а также роли сопровождения, которые не должны совмещаться в одном лице. Это задается соотношением (2).

Согласно пункту 7.2.4 любая роль должна обладать необходимыми и достаточными правами на свое исполнение, что задается соотношениями (3), (4), (6), (7), согласно которым для любой роли существует контролирующая и административная роль, обладающая достаточными правами для исполнения своих функций. В то же время административная и контролирующая роли не обладают правами на исполнение других функций, что обозначено соотношением (2). ■

4. Пример построения модели

Для наглядности построим модель политики безопасности на основании введенных определений. Пусть задана иерархия исполнительских ролей, а также иерархия административных и контролирующих ролей.

Управляющий DIR является максимальной ролью в иерархии, минимальной ролью является служащий E. В каждом направлении деятельности определяется максимальная роль исполнительного директора TM, минимальной ролью направления является операционист O (рис. 1).

Каждый из контролеров направления C_1, C_2 обеспечивают функции контроля за исполнителями начиная с начальников отделов, при этом функции

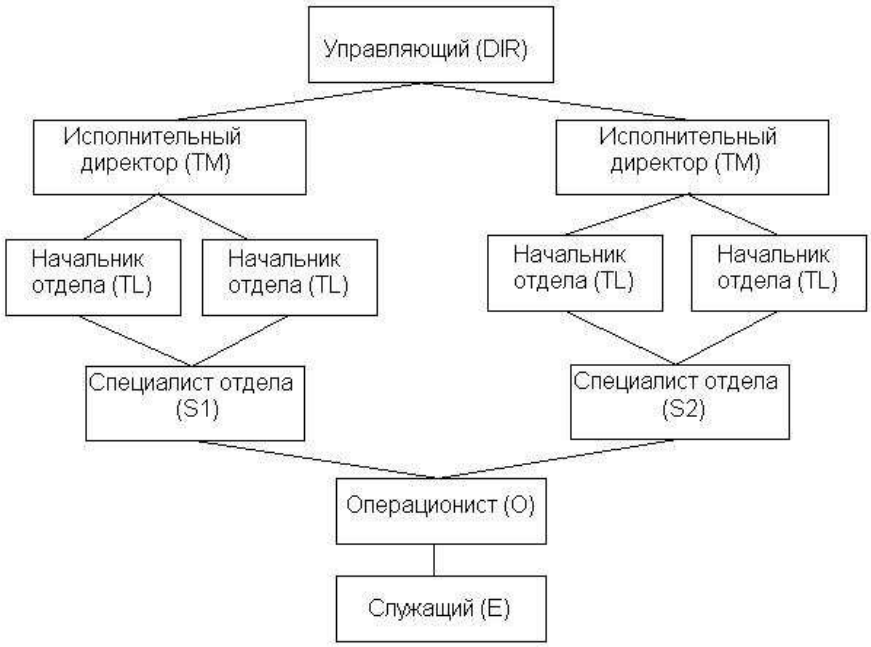

Рис. 1. Иерархия исполнительских ролей

контроля для C_1 и C_2 не пересекаются, т.е. C_1 не может контролировать направление деятельности 2 (рис. 2).

Рис. 2. Иерархия контролирующих ролей

Старший администратор A выполняет административные функции для SC и C, администраторы A_1 и A_2 выполняют административные функции по направлениям деятельности (рис. 3).

Ниже приведены таблицы, в которых описано соотношение между контролирующими ролями и множествами сопоставленных им исполнительских ролей, а также между администраторскими правами и множествами сопоставленных им контролирующих ролей.

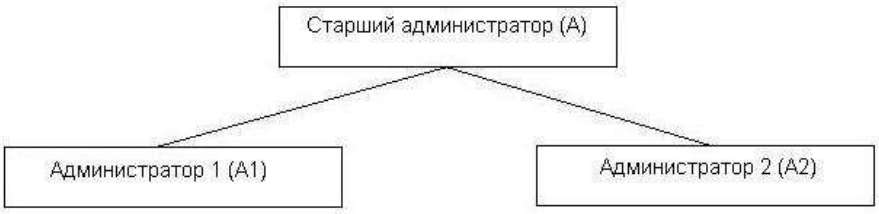

Рис. 3. Иерархия административных ролей

Контролирующая роль	Множество ролей
C_1	$[S_1, TM_1)$
C_2	$[S_2, TM_2)$
C	$[TM_1, TM_1]$
C	$[TM_2, TM_2]$

Административная роль	Множество ролей
A_1	$[C_1, C)$
A_2	$[C_2, C)$
A	$[C, C]$

Литература

1. Грушо, А.А. Теоретические основы защиты информации / А.А. Грушо, Е.Е. Тимонина. – М.: Издательство Агенства Яхтсмен, 1996.
2. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000.
3. Щербаков, А.Ю. Введение в теорию и практику компьютерной безопасности / А.Ю. Щербаков. – М.: Издатель Молгачева С.В., 2001.