УДК 681.3

А.В. ФУРМАНЮК

Тернопільський національний економічний університет, Україна

КОНТРОЛЬ ДОСТУПУ В СИСТЕМАХ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ НА БАЗІ РЕЛЯЦІЙНИХ СУБД

В статті описані задачі по розмежуванню доступу до конфіденційної інформації в системах електронного документообігу, які використовують у своїй роботі реляційні системи управління базами даних. Запропоновано підхід до їх вирішення, що ґрунтується на контролі доступу з використанням власних створених ролей і представлень. Це дозволяє встановити відповідність між учасниками документообігу та інформацією, отриманою із документів. Ролями визначається можливість доступу до даних, джерелом яких є конфіденційні документи, та набір допустимих операцій для авторизованих користувачів.

Ключові слова: *СУБД, контроль доступу, електронний документообіг, захист інформацій, безпека баз даних.*

Вступ

Поширення систем електронного документообігу (Workflow Management Systems – WFMS) у нашій державі відбувається швидкими темпами. Цьому сприяє ряд чинників: прийняття Закону України "Про електронний цифровий підпис" у 2003р.; зниження встановлюваних провайдерами Інтернет цін на використання каналів зв'язку; розвиток всіх форм бізнесу і, як наслідок, зростаюча потреба у технічному забезпеченні підтримки прийняття рішень та оптимізації господарської діяльності в цілому.

Серед беззаперечних переваг електронного документообігу перед традиційним – швидкість надходження документів до адресатів, зручність редагування і архівації документів, можливість командної роботи над документами, контроль виконавчої дисципліни та економія коштів. Поступовий перехід від традиційного до електронного документообігу здійснюють зараз як комерційні організації, так і державні установи із значним штатом службовців.

Захист інформації в системах електронного документообігу є на сьогодні одним із основних напрямків академічних досліджень в області забезпечення безпеки баз даних [1]. Значна частина систем електронного документообігу, доступних на нашому ринку, використовують реляційні системи управління базами даних за основу для зберігання інформації. В основному це популярні комерційні СУБД реляційного типу – Interbase, Oracle або Microsoft SQL Server. Існує думка, що більш підходящими для зберігання таких даних, як документи або мультимедійна інформація, є об'єктні бази даних. Їх комерційні реалізації значно поступаються в своїх можливостях вже згаданим РСУБД, тому використання останніх є більш доцільним, не в останню чергу завдяки великій кількості доступних технологій "клієнт-сервер", які можуть бути обрані розробниками систем електронного документообігу для реалізації власного проекту. І коли середовище для розробки ПЗ вже обране, на передній план виходить задача забезпечення конфіденційності та цілісності даних документів, які зберігаються у СУБД.

Практично всі системи електронного документообігу містять в собі функції захисту від несанкціонованого доступу, організовані через механізми аутентифікації. Але важливо не просто авторизувати користувача, а й забезпечити контроль доступу для того, щоб не допустити користувачів до документів, робота з якими не входить до їх функціональних обов'язків, або до таких, що містять комерційну таємницю, відому лише вузькому колу осіб.

Запропоновано підхід до контролю доступу, який ґрунтується на механізмі ролей і використанні представлень та дозволяє вирішити описану вище задачу.

1. Теоретичні засади рольового контролю доступу

Роль – це поіменований набір привілеїв. Існує ряд стандартних ролей, які визначені в момент інсталяції серверу БД. Також є можливість створювати нові ролі, групуючи у них будь-які привілеї. Контроль доступу, оснований на ролях (RBAC), в такому вигляді, яким він є зараз [2], був запропонований Ferraiolo і Kuhn у 1992р. і ґрунтується на наступних засадах:

1. Для кожного суб'єкта активною роллю є лише одна – та, яку він зараз використовує.

2. Кожен суб'єкт може бути вповноважений виконувати одну або декілька ролей.

3. Кожна роль може бути вповноважена виконувати одну або декілька трансакцій.

Суб'єкти можуть виконувати трансакції. Далі із цього випливає призначення ролі – суб'єкт може виконувати трансакцію тільки тоді, коли ним вибрана певна роль:

$$s : \text{subject}, t : \text{tran} \cdot \text{exec}(s,t) \Rightarrow \text{AR}(s) \neq 0 \qquad (1)$$

де s – суб'єкт,

t – трансакція,

AR() – активна роль.

Активна роль суб'єкта має бути вповноважена для нього.

Суб'єкт може виконувати трансакцію, тільки якщо вона вповноважена для активної ролі:

$$s:\text{subject},t:\text{tran} \cdot \text{exec}(s,t) \Rightarrow t \in \text{TA}(\text{AR}(s)) \qquad (2)$$

де TA() – авторизована трансакція.

Рис. 1 показує двосторонні відношення між користувачами і ролями, та між ролями і привілеями:

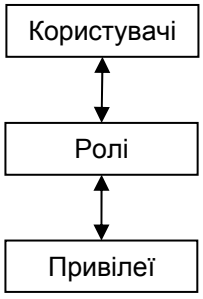

Рис. 1. Відношення у RBAC

Як бачимо, згідно принципів рольового управління доступом, користувачі здійснюють свої повноваження в системі використовуючи ролі, а не звертаючись до об'єктів напряму.

2. Розробка удосконаленого підходу до розмежування доступу

Найчастіше при допомозі механізму ролей надаються привілеї користувачам на операції із певними таблицями. Таблиці при цьому формуються на основі документів, що у своїй сукупності становлять документообіг. Проте часто інформація з одного документа знаходяться у декількох таблицях, або навпаки – дані із різних документів зберігаються в одній таблиці.

Пропонується делегувати привілеї не на таблиці, а на документи, це дозволить не допустити випадковий перегляд конфіденційних даних. Це реалізується за допомогою системи таблиць і відношень, показаної на рис. 2.

В табл. 1 описані поля таблиць, що використовує дана система.

В таблиці Users міститься інформація про користувачів системи – код, ім'я та прізвище, код відділу. Останнє поле посилається на довідник відділів (таблиця Departments), що дозволяє удосконалити облік користувачів, забезпечивши рекурсивне видалення записів при закритті відділу або імпорт записів при підключенні нового відділу до системи. Інші довідники в системі:

Roles – довідник ролей,

Documents – довідник документів.

Таблиця User_roles показує зв'язок між користувачами і відповідними ролями.

Як відомо, один і той же користувач може мати декілька ролей. Додаткове поле blocked за замовчуванням має значення '0'.

Змінивши його на одиницю, можна тимчасово заблокувати пару «користувач – роль», не видаляючи її із системи повністю. Цю можливість можна використовувати, коли користувач йде у відпустку або переводиться на іншу ділянку роботи.

Таблиця Entitys показує взаємозв'язок таблиць і документів, а ключова таблиця цієї системи – Permissions показує привілеї певної ролі на конкретний документ. Поле grants може приймати наступні значення: s (select), i (insert), u (update), d (delete), а також їх комбінації через кому.

Опишемо дію системи на прикладі. Ідентифікатор працівника податкової інспекції (його код, login) при успішній аутентифікації знаходиться у таблиці Users.

Далі перевіряється наявність цього ж коду у таблиці User_roles, і виявляється, що за користувачем закріплена роль «Облік платників ПДВ».

Згідно даних таблиці Permissions вона передбачає будь-які операції з документами «Реєстраційна заява платника податку на додану вартість», «Акт про анулювання реєстрації платника податку на додану вартість» (таблиця vat_pay у Entitys) і вибірку даних (grants='s') із документа «Свідоцтво платника податку на додану вартість» (таблиця vat_svd у Entitys).

Таблиця 1

Поля таблиць БД

Назва таблиці	Поле таблиці	Тип поля	Опис поля
Departments (довідник відділів)	depid	Number	Код відділу
	department_name	Character	Назва відділу
Documents (довідник документів)	dtid	Number	Код документу
	doc_name	Character	Назва документу
Entitys (сутності)	tableid	Number	Код таблиці або представлення
	dtid	Number	Код документу
Permissions (дозволи)	dtid	Number	Код документу
	grants	Character	Набір привілеїв
	rid	Number	Код ролі
Roles (довідник ролей)	rid	Number	Код ролі
	name	Character	Назва ролі
User_roles (ролі користувачів)	rid	Number	Код ролі
	userid	Number	Код користувача
	blocked	Boolean	Ознака блокування (1 – запис заблоковано, 0 – розблоковано
Users (користувачі)	userid	Number	Код користувача
	user_name	Character	П.І.Б. користувача
	depid	Number	Код відділу

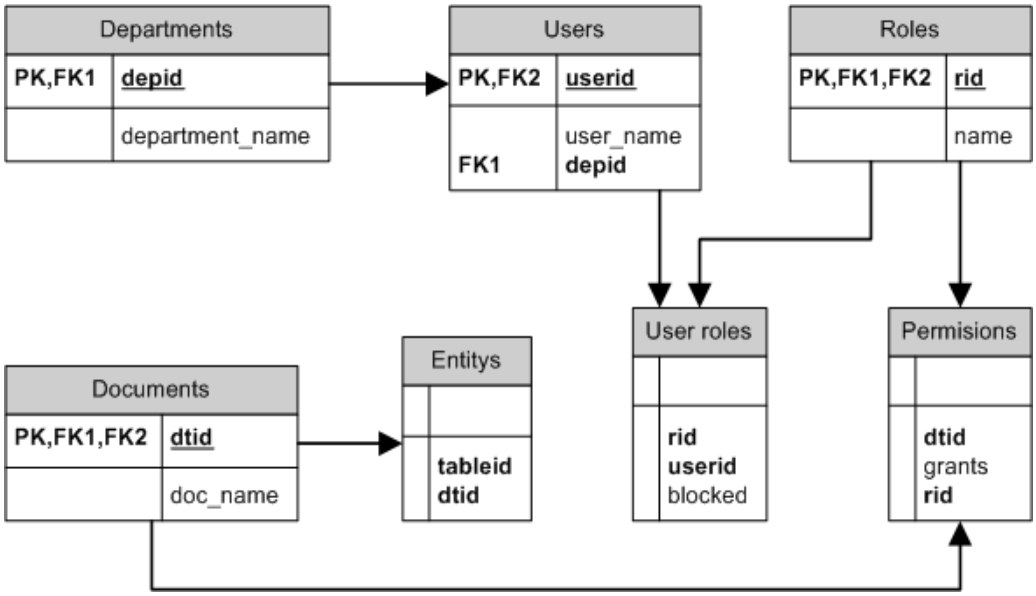

Рис. 2. Реалізація рольового підходу

3. Використання представлень

Даний підхід використовує переваги об'єктних СУБД, даючи можливість встановлювати привілеї на документи як об'єкти системи електронного документообігу. Його можна додатково удосконалити за допомогою використання представлень.

Представлення (view) – це сформована вибірка кортежів, які зберігаються у таблиці. До представлень можна звертатися так само, як і до таблиць, за винятком операцій модифікації даних, оскільки деякі типи представлень є такими, що не модифікуються. Зазвичай в реалізаціях представлень зберігається SQL-код, що описує запит вибірки, а не власне вибірка даних; вибірка ж створюється динамічно на момент виконання запиту.

Уявімо ситуацію, коли виникла необхідність обмежити привілеї для інспекторів – дозволити їм здійснювати вибірку із БД лише тих даних, що стосуються фізичних осіб – платників ПДВ. Оскільки таблиця vat_pay є спільною для юридичних і фізичних осіб, потрібно передбачити в ній поле subject_type, яке прийматиме значення '1' для юридичних осіб і '0' – для фізичних. Створимо нове представлення vat_pay_f на основі SQL-запиту:

```
select * from vat_pay where subject_type=0.
```

Створимо роль «Облік платників ПДВ – фіз. особи» та занесемо дані про неї у таблиці Roles, User roles та Permissions. Створимо новий документ, занісши його dtid у необхідні таблиці, а у таблиці Entitys співставимо його із представленням vat_pay_f, адже з ним можна працювати, як із звичайною таблицею.

Цей приклад показав, як представлення дозволяють удосконалити контроль доступу у СУБД.

Висновки

Запропонований підхід використання контролю доступу, основаного на ролях, доповнений механізмом представлень, дозволяє підняти якість контролю доступу в системах електронного документообігу, а невелика кількість потрібних для його реалізації таблиць спрощує адміністрування і видачу привілеїв. Однак, щоб досягти максимальної ефективності, слід подбати про безпечну аутентифікації користувачів і знизити ризик розкриття їх паролів сторонніми особами. Реалізувати це можна, прийнявши в організації строгі політики інформаційної безпеки та використовуючи додаткові технічні засоби захисту інформації, наприклад, електронні ключі eToken [4].

Література

1. Piattini M. Advanced Database Technology and Design / M. Piattini, O. Díaz. - Artech House, Norwood, MA. - 2000. - 535 p.

2. Ferraiolo D. Role-Based Access Contro. / D. Ferraiolo, D.R. Kuhn // Proc. of the NIST-NSA National (USA) Computer Security Conference. 1992. - P. 554-563.

3. Козленко З. Информационная безопасность в современных системах управления базами данных. // Компьютер Пресс. – 2002. – № 3 [Электронный ресурс]. – Режим доступа к ресурсу: http://www.compress.ru/Archive/CP/2002/3/46.

4. Карпінський М.П. Аутентифікація у СУБД та збереження таємниці паролів / М.П. Карпінський, А.В. Фурманюк // Вісник Тернопільського державного технічного університету. - 2005. - № 2. - С. 128-131.

Надійшла до редакції 10.01.2009

Рецензент: д-р техн. наук, проф., зав. каф. І.Б. Туркін, Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», Харків, Україна.

КОНТРОЛЬ ДОСТУПА В СИСТЕМАХ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА НА БАЗЕ РЕЛЯЦИОННЫХ СУБД

А.В. Фурманюк

В статье описаны задачи по разграничению доступа к конфиденциальной информации в системах электронного документооборота, которые используют в своей работе реляционные системы управления базами данных. Предложен подход к их решению, который основан на контроле доступа с использованием собственных созданных ролей и представлений. Это позволяет установить соответствие между участниками документооборота и информацией, полученной из документов. Ролями определяется возможность доступа к данным, источником которых являются конфиденциальные документы, и набор допустимых операций для авторизированных пользователей.

Ключевые слова: СУБД, контроль доступа, электронный документооборот, защита информации, безопасность баз данных.

ACCESS CONTROL IN WORKFLOW MANAGEMENT SYSTEMS BASED RELATIONAL DBMS

A.V. Furmanyuk

In article are described tasks on access differentiation to the confidential information in Workflow Management Systems which use relational database management systems in the operation. The approach to their solution which is grounded on access control with usage of the own created roles and representations is offered. It allows to install correspondence between participants of document circulation and the information received from documents. Roles define possibility of the data access which source are confidential documents, and a set of admissible operations for legal users.

Key words: DBMS, access control, workflow, information protection, safety of databases.

Фурманюк Андрій Володимирович – аспірант кафедри безпеки інформаційних технологій Тернопільського національного економічного університету, Тернопіль, Україна, e-mail: a.furmanyuk@gmail.com.