Система захисту користувачів при обліку господарських операцій

Василь Литвин[1], Софія Гуц[2]

Кафедра інформаційних систем та мереж, Національний університет "Львівська політехніка", УКРАЇНА, м. Львів, вул. С. Бандери, 12,
E-mail: 1. vasyl17.lytvyn@gmail.com, 2. sofia.huts@gmail.com

Abstract – This paper analyzes models, methods and algorithms for information security and their applications in information systems***, based on*** a relational DB. ***When designing my model IS based on it are carried out: development and implementation of functional tasks on delimitation and access control equipment and information both within the information system as a whole, and to separate information resources.***

Keywords: access control, authentication, identification, model of authority, model of truth.

I. Вступ. Загальна постановка проблеми

Питання безпеки – невід'ємна частина концепції впровадження нових інформаційних технологій у всі сфери життя суспільства. Широкомасштабне використання обчислювальної техніки і телекомунікаційних систем у межах територіально-розподіленої мережі, збільшення обсягів інформації, яка обробляється, і розширення кола користувачів приводять до якісно нових можливостей несанкціонованого доступу до ресурсів і даних інформаційної системи, до їх високої уразливості.

Враховуючи масовість використання реляційних баз даних (БД), велику кількість накопиченої в наявних БД інформації з різних предметних областей, існування стандартизованого інструментарію систем керування базами даних (СКБД), у роботі основна увага звертається на моделювання СЗІ саме реляційних баз даних, розглядаючи захист інших компонент ІС в міру необхідності.

II. Основні завдання дослідження та їх значення

Основними завданнями дослідження є розробка моделей, методів та алгоритмів захисту інформації і їх застосування в інформаційних системах, побудованих на основі реляційних СКБД.

Мета роботи визначає необхідність розв'язання наступних задач:

- Аналіз наявних моделей СЗІ реляційних БД та загроз, які виникають при використанні ІС на основі реляційних БД.
- Побудова моделі СЗІ БД, яка б враховувала особливості та характерні риси задач захисту інформації в інформаційних системах, що функціонують на основі реляційних БД.
- Побудова моделі СЗІ, використовуючи розмежування доступу до окремих об'єктів бази даних, таких як, наприклад, значення атрибутів кортежів для певного користувача на існуючій фірмі.

III. Основна частина

Основною концепцією безпеки БД є перевірка повноважень та істинності (автентифікації) користувачів. Вона реалізується за допомогою найпростіших моделей повноважень , істинності та базової моделі розмежування доступу.

Існують такі методи розмежування доступу: розмежування доступу за списками, використання матриці встановлення повноважень, розмежування доступу за рівнями таємності і категоріям, парольне розмежування доступу.

При розмежуванні доступу за списками задаються відповідності: кожному користувачеві – список ресурсів і прав доступу до них або кожному ресурсу – список користувачів і їх прав доступу до даного ресурсу. Розмежування доступу за рівнями таємності і категоріями полягає в поділі ресурсів інформаційної системи по рівням секретності і категоріям. Парольне розмежування, очевидно, представляє використання методів доступу суб'єктів до об'єктів за паролем. Перевірка повноважень базується на тому, що кожному користувачеві або процесу КМ ставиться у відповідність набір дозволених дій, виконуваних стосовно визначених об'єктів КМ.

Наукова новизна роботи полягає у досягненні наступних результатів: вдосконалення моделі безпечної БД та формулювання вимог до даної БД з врахуванням потреб у захисті інформації, оптимізації ресурсоємності СЗІ, доступі до окремих значень атрибутів кортежів, аудиті оновлень на рівні відношень, удосконалення моделі примусового керування доступом для забезпечення сучасних потреб захисту груп користувачів при обліку господарських операцій та автоматизації захисту керування СЗІ.

Висновки

В результаті проведеного дослідження було розглянуто існуючі проблеми у сфері безпеки реляційних БД та описано основні підходи, що застосовуються для їх вирішення. Визначено послідовність етапів запропонованої методики розмежування доступу користувачів: формування структури облікового процесу підприємства; формування організаційної структури; розподіл обов’язків між користувачами, визначення прав доступу користувачів до функцій програми та інформаційних ресурсів.

Література

1. Автореферат дисертації на здобуття наукового ступеня кандидата технічних наук Д.О.Тарасова. Моделювання системи захисту інформації у реляційних базах даних [Електронний ресурс] / Режим доступу: http://dtarasov.net/system/files/arfmdbsec.pdf
2. Верига Ю.А., Деньга С.М. Захист інформації в комп’ютерних інформаційних системах бухгалтерського обліку // Бухгалтерський облік і аудит. – 2004. – № 5. – С. 59–65.