Потреба у сховищі даних виникає і у разі відсутності цілісної OLTP-системи: на підприємстві, з історичних причин, може існувати кілька оперативних ІС з власними БД; оперативні БД можуть містити семантично еквівалентну інформацію, подану у різних форматах, іноді навіть суперечливу. У такому випадку сховище даних виконує і впорядковуючу, фільтрувальну функцію.

Якщо СППР будують на основі сховища даних, комплексну ІС можна отримати, доповнивши СППР рисами, характерними для OLTP-систем (інтерактивні засоби вводу інформації, відповідні функції прикладної логіки системи). Отже, друга стратегія побудови комплексної інформаційної системи має вигляд:

СППР → комплексна інформаційна система (включно з OLTP)

Наявність у проекті інформаційної системи інтегрованої компоненти підтримки прийняття рішень свідчить про технологічну зрілість і завершеність проекту.

1. Васкевич Д. Стратегии клиент/сервер. Руководство по выживанию для специалистов по реорганизации бизнеса. К., 1996. 2. Любінець Я.В. Моделювання інформації з часовими параметрами засобами традиційних СУБД. //Вісник Державного університету "Львівська політехніка". 1998. №330. 3. В.Львов. Создание систем поддержки принятия решений на основе хранилищ данных. //СУБД №3 — 1997. 4. С.Кузнецов, В.Артемьев. Обзор возможностей применения ведущих СУБД для построения хранилищ данных (Data Warehouse). 5. Кравець Р.Б. Багатовимірна модель даних у системах аналітичної обробки інформації. //Вісник Державного університету "Львівська політехніка". 1998. №330.

УДК 681.3

Д.О.Тарасов

НУ "Львівська політехніка", кафедра інформаційних систем та мереж

ОСНОВНІ ЗАДАЧІ ЗАХИСТУ БАЗ ДАНИХ

This paper describes reasons of information security break and topical problems of database defense. Methods of database protection improvement are considered.

Швидкий розвиток галузі інформаційних технологій, широке застосування інформаційних систем (ІС) для розв'язання прикладних задач спричинили зростання уваги науковців, фахівців та пересічних користувачів до питань безпеки інформації. Основні підстави зростання уваги до питань безпеки інформації — розповсюдження ІТ у бізнесі, поширення використання Internet, а також розподілених ІС. Як загрозу для інформації розглядають несанкціоновані знищення, зміну, копіювання, блокування санкціонованого доступу до даних. Порушенням безпеки ІС вважають реалізацію загроз

для інформації. У цьому контексті захист інформації — комплекс заходів для забезпечення фізичної цілісності інформації, запобігання несанкціонованим змінам і отриманню даних.

Основні характеристики захисту інформації — гарантована достовірність даних, конфіденційність, цілісність та доступність інформації. Залежно від призначення ІС важливість характеристик захисту змінюється. Наприклад, в ІС економічного напрямку найбільше значення має цілісність та доступність даних, у військових та урядових ІС конфіденційність та достовірність інформації є однією з головних вимог.

Для оцінки захищеності ІС розробляються критерії оцінки та проводиться сертифікація систем на відповідність класам захищеності. Серед найвідоміших — європейські критерії ITSEC та американські TCSEC. Уряди багатьох країн, міжнародні організації, у тому числі ISO, розробляють та впроваджують стандарти для розв'язання конкретних задач в галузі безпеки інформації.

Розроблення стандартів та засобів захисту інформації розвивається в кількох напрямках. Серед них:

- методи та засоби захисту ІС різних видів та призначення від несанкціонованого доступу;
- міжмережеві екрани;
- схеми аутентифікації;
- криптографічний захист даних, механізми цифрових підписів та системи розповсюдження ключів (паролів);
- безпека операційних систем (ОС) та іншого системного програмного забезпечення;
- побудова надійних апаратних платформ;
- забезпечення конфіденційності дій користувачів;
- антивірусні засоби.

Ці засоби, разом з організаційними, технічними та іншими спеціальними заходами зменшують імовірність порушення безпеки ІС сторонніми особами та дозволяють розпізнати легальних користувачів ІС.

Згідно з даними Computer Security Institute (США) [1] причинами порушення безпеки ІС є у 3% — віруси, 2% — нелегальні втручання у ІС сторонніх осіб з інших ІС (у т. ч. з Internet), 20% — помилки та аварії апаратного забезпечення, 55% — помилки та некваліфіковані дії легальних користувачів ІС та обслуговуючого персоналу, 20% — свідомі дії легальних користувачів ІС, спрямовані на завдання шкоди ІС та порушення безпеки (рис. 1).

Отже, перше місце за частотою (75%) займають порушення безпеки ІС, пов'язані з некоректною роботою легальних користувачів ІС. Вберегти від таких дій (у тому числі помилкових 55%, свідомих 20%) не допоможуть ні біометричні засоби аутентифікації, ні криптографічний захист ліній зв'язку, ні міжмережеві екрани або VPN продукти.

Рис. 1. Причини порушення безпеки інформації

Враховуючи масовість застосування в ІС технології збереження інформації в БД, великі обсяги важливої інформації, яка зберігається у БД, та наведені статистичні дані, постає ряд задач:

1. Необхідно сформувати для користувачів БД безпечне середовище роботи, у якому забезпечується цілісність даних, неможливе несанкціоноване розголошення та зміна даних іншими користувачами БД.

2. Для зменшення кількості помилкових та свідомих порушень захисту інформації безпечне середовище роботи повинно мінімізувати доступ користувачів до непотрібних даних як на читання, так і на створення, зміну, знищення.

3. Повинна забезпечуватись достовірність та цілісність даних в ІС [2].

4. Для підтримки безпеки на належному рівні протягом життя ІС необхідно розробити ефективні засоби адміністрування політики безпеки.

5. Інтеграція системи захисту інформації (СЗІ) у ІС на етапі проектування схеми БД.

На практиці, на жаль, засобами поширених СУБД неможливо реалізувати захист деяких практичних задач.

СУБД дозволяють обмежити доступ до об'єктів БД на рівні таблиць, представлень (view), окремих атрибутів таблиць тощо [3]. Доступ розмежовується для читання даних, зміни, видалення, запису нових даних. На практиці необхідно надавати доступ користувачам (наприклад, різних підрозділів) до конкретних записів (полів у деяких записах), обмежуючи доступ до інших записів таблиці. Стандартними командами CREATE ROLE..., GRANT..., REVOKE... це зробити неможливо.

Існує ряд спеціалізованих СУБД (наприклад, Trusted ORACLE), які використовують багаторівневу систему захисту (multilevel), моделі примусового контролю доступу [4].

Реалізація цієї моделі дозволяє обмежити доступ до окремих записів (полів записів) на основі ієрархії класів доступу. Додатково підтримується багатоверсійність даних. Водночас ієрархія не є розгалуженою, що не відображає особливості розподілу повноважень відповідно до функціональних обов'язків. Механізми забезпечення багатоверсійності є надлишковими для ІС економічного характеру та створюють додаткове навантаження на обчислювальні ресурси. Сфера використання спеціалізованих СУБД обмежується також недоступністю відповідного програмного забезпечення на нашому ринку.

Пропонується варіант розв'язання задачі обмеження доступу на рівні записів — проектування схеми БД з використанням правил для збільшення захисту інформації, використання системи спеціалізованих представлень та ролей як частини СЗІ. Така система впроваджується для захисту лише об'єктів з класифікованими даними (що зменшує навантаження) та є прозорою для користувачів ІС.

Форма та механізми фіксації авторства інформації стандартних засобів аудиту, наявних на ринку СУБД, складні для поточного використання та аналізу.

Наприклад, кілька користувачів у різний час дають команди INSERT для занесення у БД записів зі значеннями деякої складної функції багатьох аргументів. У журналі аудиту зберігаються дані про виконання команд, час, назви користувачів, можливо, текст команд. Подальший аналіз авторства конкретного запису вимагає пов'язаної з записом позначки (мітку), яка вказує на автора. У БД ця мітка відсутня. Тому необхідно проведення аналізу:

- оцінити (можливо, евристично) проміжок часу, у який міг бути створений запис;
- обрати з журналів аудиту команди, які здійснюють операцію INSERT... у даний об'єкт (таблицю);
- відкинути з аналізу команди, які не належать до транзакцій, завершених у проміжок часу створення запису;
- серед обраних команд провести зіставлення значень у БД та результатів виконання команд та подальший аналіз з урахуванням відмінностей між значеннями у БД з результатами виконання команд.

Як бачимо, такий аналіз є складною задачею. Складність може завадити знайти єдиний розв'язок — точний час створення запису та його автора. У практичних задачах спростити процедуру аналізу авторства дозволяє співставлення мітки автора (наприклад, назви користувача) з об'єктами аудиту (наприклад записами).

Спростити аудит БД дозволяє заборона зміни даних. В окремих випадках виправлення за допомогою DELETE + INSERT не тільки дає змогу спростити аудит, а й знімає ряд проблем захисту інформації.

Адміністрування користувачів СУБД та адміністрування прав доступу до конкретних об'єктів БД розглядають як дві окремі задачі. Процеси фіксації у ІС даних щодо графіка роботи, посади, зміни статусу працівників тощо не змінюють права доступу працівників до інформації. Зміна прав доступу виноситься в окрему задачу адміністрування БД. У

системах, які проектувалися окремо від СЗІ, зміна прав доступу до інформації часто є складною адміністративною задачею.

Наведені задачі автором пропонується розв'язувати, доповнюючи СЗІ БД рядом об'єктів (таблиць, представлень, ролей, процедур тощо) та правил роботи з ІС та СЗІ. Ці об'єкти є прошарком між об'єктами ІС та діями користувачів БД, які пропущено обмеженнями СУБД (рис. 2).

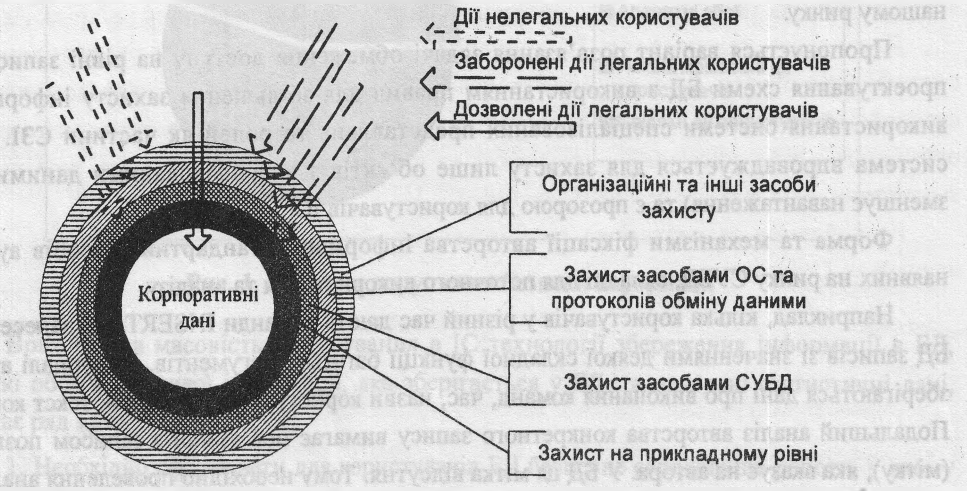

Рис. 2. Схема рівнів захисту БД

Прошарок забезпечує реалізацію прийнятої політики безпеки та виконує такі функції:

1. Обмеження доступу до даних.

2. Забезпечення цілісності даних.

3. Фіксацію та контроль авторства.

4. Автоматизацію адміністрування СЗІ.

5. Забезпечення активності СЗІ (зокрема виконання превентивних дій).

6. Контроль квот ресурсів.

Висновки

Для запобігання значній частині порушень безпеки інформації недостатньо стандартних механізмів СЗІ промислових СУБД. Для таких задач, як обмеження доступу, забезпечення конфіденційності та цілісності даних, аудиту БД необхідно доповнити СЗІ БД спеціальним прошарком. Прошарок реалізується включенням у схему БД додаткових об'єктів — таблиць, представлень, ролей тощо і є надбудовою на прикладному рівні ІС над схемою БД та використовує наявні засоби СУБД.

Отже, СЗІ БД складається із:

· об'єктів та засобів СУБД (рівень СУБД);

· об'єктів та засобів БД (рівень схеми БД із засобами СЗІ);

· правил роботи із СЗІ та БД.

Необхідними вимогами для побудови безпечного середовища збереження та опрацювання даних є продумане проектування ІС, схеми БД, методик опрацювання інформації та функціональних обов'язків, попередня класифікація та оцінка даних, нормативна документація.

Напрямком подальших досліджень є побудова формальної моделі СЗІ бази даних, з урахуванням імовірностей причин втрати інформації та моделей можливих порушників безпеки інформації у БД та реалізація формальної моделі СЗІ у вигляді програмних моделей для захисту промислових СУБД.

1. Ильницкий А.Е., Шорошев В.В., Обзор зарубежных аппаратно-програмных средств защиты компьютерных систем // Бизнес и безопасность №6. 1998. 2. Тарасов Д.О., Забезпечення цілісності даних у реляційних структурах // Вісник ДУ "Львівська політехніка" 1999 №383. С. 213-226. 3. Дейт К. Дж. Введение в системы баз данных. :Пер. с англ. 6-е изд. К., 1998. 4. X. Qian and T.F. Lunt. Tuple-level vs. element-level classification. Database security, VI: Status and Prospects, North-Holland, 1993. Pp. 301-315.

УДК 681.3.06

М.Ю.Щербина

Військовий інститут при НУ "Львівська політехніка"

ДЕЯКІ МЕТОДОЛОГІЇ МОДЕЛЮВАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ INTERNET/INTRANET

Contemporary approaches for modeling Web information systems (WIS) are considered. The RMM and Extended RMM methodologies based on entity-relationship model are described in detail. Some enhancements of relational methodologies are proposed.

Методології моделювання систем гіпермедіа почали активно розробляти на початку 90-х років, особливо після широкого впровадження мови HTML та інших Web-технологій. Методології базуються на різних фундаментальних засадах, наприклад, на моделі "сутність-зв'язок" (*entity-relationship model*) [1, 2] або на принципах об'єктно-орієнтованого моделювання. На принципах ER-моделювання основані, зокрема,