УДК 004.065

Касянчук Н.В.
Ткачук Л.М.

Захист інформації в базах даних

Вінницький національний технічний університет

Анотація

В даній статті розглянуто питання захисту інформації в базах даних та методи їх захисту. Проаналізовано основні методи захисту інформацію в базах даних,виявлено їх позитивні та негативні сторони. А також в даній роботі розглянуто основні моделі безпеки для організації доступу до бази даних та процедури ідентифікації, аутентифікації та авторизації в СУБД.

Ключові слова: *інформація, захист інформації, база даних (БД), система управління базами даних (СУБД), цілісність, конфіденційність, доступність, несанкціонований доступ, моделі безпеки, управління доступом, ідентифікація, аутентифікація, авторизація.*

Abstract

This article deals with the protection of information in databases and methods of protection. The basic methods of protecting information in databases revealed their positive and negative sides. Also in this paper, the basic security model to provide access to the database and procedures identification, authentication and authorization in the DBMS.

Key words: *information, information security, database (DB) database management system (DBMS), integrity, confidentiality, availability, unauthorized access, security model, access control,identification, authentication, authorization.*

Вступ

За умови стрімких темпів розвитку інформаційних технологій, збільшення кількості загроз інформації, ступеня невизначеності їх виникнення і реалізації, а також складності систем захисту інформації та їх спеціалізованої спрямованості, набуває актуальності завдання побудови системи захисту інформації.

Захист інформації – це сукупність організаційно-технічних заходів і правових норм для попередження заподіяння збитку інтересам власника інформації. Тривалий час методи захисту інформації розроблялися тільки державними органами, а їхнє впровадження розглядалося як виключне право тієї або іншої держави. Проте в останні роки з розвитком комерційної і підприємницької діяльності збільшилося число спроб несанкціонованого доступу до конфіденційної інформації, а проблеми захисту інформації виявилися в центрі уваги багатьох вчених і спеціалістів із різноманітних країн. Слідством цього процесу значно зросла потреба у захисті конфіденційної інформації.

На сьогоднішній день об’єм інформації в світі є настільки великим, що самим оптимальним методом роботи з нею є база даних. База даних – це представлена в об’єктивній формі сукупність матеріалів, систематизованих так, щоб ці матеріали могли бути найдені і оброблені з допомогою комп’ютера. Її захист є одною із найважчих задач на сьогоднішній день.

Результати досліджень

Поняття захисту інформації

Захист інформації – комплекс заходів, спрямованих на забезпечення найважливіших аспектів інформаційної безпеки. На сьогоднішній день існують такі аспекти захисту інформації, як:

- цілісність – захист інформації від несанкціонованої модифікації;
- конфіденційність – захист від несанкціонованого ознайомлення з інформацією;
- доступність – захист (забезпечення) доступу до інформації, а також можливості її використання. Доступність забезпечується як підтриманням систем в робочому стані так і завдяки способам, які дозволяють швидко відновити втрачену чи пошкоджену інформацію.

Відповідно, до даних аспектів захисту інформації, виділяють наступні загрози інформації:

- загрози цілісності (знищення та модифікація інформації);
- загрози доступності (блокування та знищення інформації);
- загрози конфіденційності (несанкціонований доступ (НСД), витік та розголошення інформації).

Система називається безпечною, якщо вона, використовуючи відповідні апаратні і програмні засоби, управляє доступом до інформації так, що тільки належним чином авторизовані особи або ж діють від їхнього імені процеси отримують право читати, писати, створювати і видаляти інформацію. Очевидно, що абсолютно безпечних систем немає, і тут мова йде про надійну систему у сенсі "система, якій можна довіряти" (як, наприклад, можна довіряти людині). Система вважається надійною, якщо вона з використанням достатніх апаратних і програмних засобів забезпечує одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу. Основними критеріями оцінки надійності є:

- політика безпеки;
- гарантованість.

Політика безпеки, будучи активним компонентом захисту (включає в себе аналіз можливих загроз і вибір відповідних заходів протидії), відображає той набір законів, правил і норм поведінки, яким користується конкретна організація при обробці, захисту та поширенні інформації. Вибір конкретних механізмів забезпечення безпеки системи здійснюється відповідно до сформульованої політики безпеки.

Гарантованість, будучи пасивним елементом захисту, відображає міру довіри, яка може бути надана архітектурі та реалізації системи (іншими словами, показує, наскільки коректно обрано механізми, що забезпечують безпеку системи).

У надійній системі повинні реєструватися всі події, що відбуваються і стосуються безпеки (повинен використовуватися механізм підзвітності протоколювання, що доповнює аналізом заповненої інформації, тобто аудитом). При оцінці ступеня гарантованості, з якою систему можна вважати надійною, центральне місце займає достовірна (надійна) обчислювальна база. Достовірна обчислювальна база (ДОБ) являє собою повну сукупність захисних механізмів комп'ютерної системи, яка використовується для втілення в життя відповідної політики безпеки. Надійність ДОБ залежить виключно від її реалізації та коректності введених даних (наприклад, даних про благонадійність користувачів, які визначаються адміністрацією). Кордон ДОБ утворює периметр безпеки. Компоненти ДОБ, що знаходяться всередині цього кордону, повинні бути надійними (отже, для оцінки надійності комп'ютерної системи досить розглянути тільки її ДОБ). Від компонентів, що знаходяться поза периметром безпеки не потрібно надійності. Однак це не повинно впливати на безпеку системи.

Так як зараз широко застосовуються розподілені системи обробки даних, то під "периметром безпеки" розуміється межа володінь певної організації, у підпорядкуванні якої знаходиться ця система. Тоді за аналогією те, що знаходиться всередині цього кордону, вважається надійним. За допомогою шлюзової системи, яка здатна протистояти потенційно ненадійній, а може навіть і ворожого оточення, здійснюється зв'язок через цей кордон. Контроль допустимості виконання суб'єктами певних операцій над об'єктами, тобто функції моніторингу, виконується достовірної обчислювальної базою. При кожному зверненні користувача до програм або даних, монітор перевіряє допустимість даного звернення (узгодженість дії конкретного користувача зі списком дозволених для нього дій). Реалізація монітора звернень називається ядром безпеки, на базі якої будуються всі захисні механізми системи. Ядро безпеки має гарантувати власну незмінність.

Поняття бази даних та основні методи захисту інформації в ній

База даних (БД) - упорядкований набір логічно взаємопов'язаних даних, що використовується спільно, та призначений для задоволення інформаційних потреб користувачів. У технічному розумінні включно й система управління БД.

Система управління базами даних (СУБД) - це комплекс програмних і мовних засобів, необхідних для створення баз даних, підтримання їх в актуальному стані та організації пошуку в них необхідної інформації.

Головним завданням бази даних (БД) є збереження значних обсягів інформації (даних). Дані в базах даних повинні зберігатися з гарантування безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденої. Загрози втрати конфіденційної інформації стали звичайним явищем у сучасному комп’ютерному світі. Якщо в системі захисту є недоліки, то даним може бути завдано шкоди, наприклад, такої як:

- порушення цілісності даних;

- втрата важливої інформації;
- попадання важливих даних стороннім особам і т.д.

Кожен збій роботи бази даних може паралізувати роботу цілих корпорацій, фірм, що призведе до великих матеріальних втрат.

Методи захисту баз даних в СУБД умовно можна поділити на дві групи: основні та додаткові.

До додаткових засобів захисту БД можна віднести:

- вбудовані засоби контролю даних;
- забезпечення цілісності зв'язків таблиць;
- організація спільного використання об'єктів БД в мережі.
- До основних методів захисту відносять:
- захист паролем;
- шифрування;
- розділення прав доступу до об'єктів БД;
- захист полів і записів таблиць БД.

Захист паролем – є самим простим способом захисту БД від несанкціонованого доступу.

Паролі можуть бути встановленні користувачами або адміністраторами. Їх облік і зберігання виконується СУБД. Паролі зберігаються в спеціальних файлах СУБД в зашифрованому вигляді. Після введення пароля користувачу надається доступ до необхідної інформації.

Не дивлячись на простоту парольного захисту, він має ряд недоліків. По-перше, пароль є вразливим, особливо якщо він не шифрується при зберіганні в СУБД. По-друге, користувачу потрібно запам'ятати або записати пароль, а при недбалому відношенні до запису пароль може стати надбанням інших.

Більш сильнішим методом захисту є шифрування. Шифрування – це процес обробки інформації за певним алгоритмом в вигляд непридатний для читання, в цілях захисту від несанкціонованого перегляду або використання. Важливою особливістю будь-якого алгоритму шифрування є використання ключа, який стверджує вибір якогось конкретного методу кодування із всіх можливих. Розрізняють два основні методи шифрування: симетричне й асиметричне. В симетричному шифрування один і той же ключ використовується і для шифрування, і для дешифрування. В асиметричних методах застосовуються два ключі. Один з них, несекретний, використовується для шифрування і може публікуватися разом з адресою користувача, другий, секретний, застосовується для дешифрування і відомий тільки одержувачу.

Шифрування забезпечує всі три аспекти безпеки даних: конфіденційність, цілісність і доступність.

В цілях контролю використання основних ресурсів СУБД в багатьох системах є засоби розділення прав доступу до об'єктів БД. Права доступу визначають можливі дії над об'єктами. Власник об'єкта, а також адміністратор БД мають всі права. Решта користувачів мають ті права і рівні доступу до об'єктів, якими їх наділили.

Дозвіл на доступ до конкретних об'єктів бази даних зберігається в файлі робочої групи. Файл робочої групи містить дані про користувачів групи і зчитується під час запуску. Файл зберігає наступну інформацію:

- імена облікових записів користувачів;
- паролі користувачів;
- імена груп, в які входять користувачі.

Всі вище описані методи є основними, але їх не використання не гарантує повного зберігання даних. Для підвищення рівня безпеки інформації в БД рекомендується використання комплексних заходів.

Моделі безпеки БД

Управління доступом в БД включає такі питання, як доступ до таблиць і її полів. Для організації цього доступу використовуються моделі безпеки, які включають дискреційну, мандатну і рольову моделі.

Способом формалізованого представлення дискреційного доступу є матриця доступу або списки управління доступом, що встановлюють перелік користувачів і перелік дозволених операцій відносно кожного об'єкта БД. Можливі декілька підходів до побудови дискреційного управління доступом: децентралізована, централізована та змішана моделі безпеки. Саме змішаний варіант реалізований у більшості СУБД.

Мандатна модель поєднує захист і обмеження прав, що використовуються відносно комп'ютерних процесів, даних і системних пристроїв, та призначена для запобігання їх небажаному

використовуванню. Для СУБД мандатна модель безпеки може розширювати або замінювати дискреційний контроль доступу і концепцію користувачів і груп.

Права доступу кожного суб'єкта і характеристики конфіденційності кожного об'єкта відображаються у вигляді сукупності рівня конфіденційності і набору категорій конфіденційності. Для реалізації безпеки за допомогою мандатної моделі рядкам і стовпцям таблиці БД приписуються мітки, які потім надаються користувачам. Ефективно застосовуватися мандатна модель може тільки разом з дискреційною.

Рольова модель – розвиток політики виборного управління доступом, при цьому права доступу суб'єктів системи на об'єкти групуються з урахуванням специфіки їх використання, утворюючи ролі. Управління правами доступу здійснюється як на основі матриці доступу, так і на основі правил, що регламентують поведінку (ролі) користувача та їх активацію під час сеансів.

Рольове розмежування доступу дозволяє реалізувати гнучкі, динамічні правила розмежування доступу. Безпека в цій моделі забезпечується чіткими визначеннями ролей адміністратора БД і користувача БД на права доступу до об'єктів БД і прав на читання, модифікацію, запис і видалення об’єктів. Технологія управління доступом на основі ролей є достатньо гнучкою і потужною, щоб змоделювати як виборне, так і мандатне управління доступом.

Процедури ідентифікації, аутентифікації і авторизації в СУБД

Для будь-якої захищеної бази даних обов’язковими є процедури ідентифікації, аутентифікації та авторизації.

Сутність процедури ідентифікації полягає в призначенні користувачу БД – імені. Ім’я користувача – це деяка унікальна мітка, що відповідає прийнятим угодам і забезпечує однозначну ідентифікацію об’єкта реального світу в просторі об’єктів, що відображаються.

Сутність процедури аутентифікації полягає в підтвердженні автентичності користувача, що представив ідентифікатор. У ряді сучасних СУБД використовується:

- біометрична аутентифікація – це процес доведення і перевірки автентичності заявленого користувачем імені через пред’явлення користувачем своїх біометричних характеристик (наприклад, відбитки пальців і долоні, звуки голосу, обличчя, відбиток сітківки ока, особливості роботи на клавіатурі, електронний цифровий підпис);
- парольна аутентифікація – це процес доведення і перевірки автентичності заявленого користувачем імені шляхом введення ним пароля або парольної фрази. Парольні фрази забезпечують більшу безпеку, ніж короткі паролі, але вимагають більшого часу для введення. Заходами, що дають змогу підвищити надійність парольного захисту є: накладання технічних обмежень, управління терміном дії паролів, обмеження доступу до файлу паролів, обмеження кількості невдалих спроб входу в систему, використання програмних генераторів паролів;
- аутентифікація із застосуванням токенів. Токен – це предмет або пристрій, володіння яким підтверджує автентичність користувача.

Ефективність процедур ідентифікації та аутентифікації істотним чином впливає на ефективність системи безпеки в цілому. В процесі авторизації встановлюється набір можливих операцій з даними, які може здійснювати користувач.

Висновки

Отже, в даній статті проаналізовано основні моделі безпеки для організації доступу до бази даних. Тому, можна зробити висновок, що з усіх існуючих моделей безпеки найзручнішою для користувачів є рольова модель, проте вона найскладніша для адміністрування; за допомогою мандатної моделі можна створювати багаторівневі системи захисту, а найпростішою моделлю є дискреційна, але вона може виявитися надмірно детальною.

Також був проведений огляд основних методів захисту інформації в базах даних, виявлено їх переваги та недоліки. Проаналізувавши всі існуючі методи захисту інформації в БД, можна зробити висновок, що використання лише якогось певного методу не може гарантувати повного зберігання даних. Тому для підвищення рівня безпеки інформації в БД рекомендовано використання комплексних заходів.

Підсумовуючи, можна зробити висновок, що розробки в даній галузі є досить актуальними та вартими подальшої розробки. Бази даних мають досить високий попит у сучасному світі, саме тому їх захист потребуватиме постійного вдосконалення.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Корнеев В.В. Базы данных. Интеллектуальная обработка информации / Корнеев В.В, Гареев А.Ф., Васютин С.В., Райх В.В.– М.: Нолидж, 2001. – 496 с.

2. Домарев В.В. Безопасность информационных технологий. Системный подход / Домарев В.В. – К.: ООО «ТИД «ДС», 2004. – 992 с.

3. Азарова А.О. Методичні вказівки до проведення практичних занять та до виконання самостійної індивідуальної роботи з дисципліни «Основи науково-дослідної роботи» для студентів напрямів підготовки 6.030601 – «Менеджмент» та 6.170103 – «Управління інформаційною безпекою» / Азарова А.О., Карпінець В.В. – Вінниця: ВНТУ, 2013. – 44 с.

4. Дейт К. Введение в системы баз данных. 6-е изд / Дейт К. – К.; М., СПб.: «Вильямс», 2000. – 848 с.

5. Анализ концептуальных подходов к обеспечению защиты баз данных [Електронний ресурс] // Мир компьютеров. – Режим доступа: http://compsmir.ru/?p=112

6. Галатенко В. Информационная безопасность [Електронний ресурс] / В. Галатенко // Открытые системы. СУБД. – 1996. – № 04. – Режим доступа: http://www.osp.ru/os/1996/04/178931/

7. Шифрование данных в СУБД [Электронный ресурс] // Мир компьютеров. – Режим доступа: http://compsmir.ru/?p=118

8. Dorothy E. Denning and Peter J. Denning Data Security // Computer Science Department, Purdue Unwersity, West Lafayette, Indiana 47907

9. A Method of Protecting Relational Databases Copyright with Cloud Watermark // Proceedings of Academy of Science, Engineering and Technology Volume 3 January 2005 ISSN 1307-6884

10. Комаров А. Базу данных не стащить! Правильные способы защитить данные в таблицах БД [Електронний ресурс] / А. Комаров // Хакер. – № 04/09 (124). – Режим доступа: http://www.xakep.ru/magazine/xa/124/ 032/1.asp

Наталія Володимирівна Касянчук – студентка групи УБ-18м, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця, e-mail: natali109788@gmail.com

Людмила Миколаївна Ткачук – канд. економічних наук, доцент кафедри МБІС, Вінницький національний технічний університет, м. Вінниця, e-mail: ludatkachuk2017@gmail.com

Nataliia Kasianchuk - student of UB-18m group, faculty of Management and Information Security, Vinnitsa National Technical University, Vinnitsa, e-mail: natali109788@gmail.com

Liudmyla Tkachuk – cand. economic sciences, Assistant Professor of Building MBIS, Vinnitsa National Technical University, Vinnitsa, e-mail: ludatkachuk2017@gmail.com