УДК 004.01

Шманов Я.К., студент 2 курсу
спеціальності 122 «Комп'ютерні науки»
Зелінська. О.В., к.т.н., доцент,
заст. декана з наукової роботи

МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В БАЗАХ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Вступ

Інформаційні технології розвиваються [3], а разом з ними збільшується кількість загроз інформації, невизначеність їх виникнення та реалізація в певному середовищі, стає досить актуальним і важливим питання про шляхи захисту інформації.

Захист інформації – це сукупність систем чи методів, які можуть забезпечити цілісність, неушкодженість, конфіденційність і доступність інформації за деяких умов, коли виникають загрози природного або штучного характеру, наслідок яких може стати причиною шкоди власникам і користувачам інформації. Зазвичай методи захисту інформації проголошувалися і розроблялися державними органами. Однак, останніми роками з розвитком підприємництва і комерції число спроб несанкціонованого доступу до конфіденційної інформації значно зросло, і, звісно ж, ці проблеми стали в центрі уваги багатьох спеціалістів всіх країн світу. Наслідок цього – зріст потреби у захисті інформації.

На теперішній час у світі існує стільки інформації, що найбільш оптимальним шляхом користування з нею є база даних. База даних – це організована структура, що призначена для взаємодії із взаємозалежною інформацією, переважно великих обсягів. Її захист є однією із найважливіших задач у науковому світі на сьогоднішній день.

Результати дослідження

Ідея захисту інформації

Захист інформації [1] – це сукупність заходів, що спрямовані на попередження порушенню конфіденційності, неушкодженості, доступності та здійсненню несанкціонованої модифікації інформації. Захист інформації підлягає підтримці таких властивостей:

1) Цілісність – неможливість модифікації інформації стороннім користувачем
2) Конфіденційність – інформація не може бути використана стороннім користувачем
3) Доступність – користувач може використовувати інформацію у відповідності до правил, установлених політикою безпеки

У відповідності до властивостей, виділяють такі загрози в її безпеці:

1) Загрози цілісності: знищення чи модифікація інформації.
2) Загрози конфіденційності: неправомірний доступ, витік чи розголошення інформації.
3) Загрози доступності: блокування чи знищення інформації.

Система є безпечною тільки тоді, коли вона управляє доступом до інформації так, що тільки авторизовані користувачі можуть отримати право читати, писати, створювати і видаляти інформацію. Для цього системі необхідно включати в себе відповідні апаратні та програмні засоби. Однак, повністю безпечних систем не існує, тому необхідна надійна система. Система вважається надійною, якщо вона забезпечує користувачам непорушність прав доступу. Оцінити надійність можна двома шляхами: політикою безпеки та гарантованістю.

Політика безпеки – це набір правил і законів, яким підпорядковується конкретна організація при взаємодії із інформацією.

Гарантованість відображає певну довіру, яка може бути надана системі.

У надійній системі повинні бути зафіксовані всі події, що реалізуються та стосуються безпеки. Оцінюючи ступінь гарантованості, коли система може вважатись надійною, перше місце займає достовірна обчислювальна база (ДОБ). ДОБ складається із захисних механізмів комп'ютерної системи. Надійність ДОБ значною мірою залежить від її реалізації та правильності введених даних (наприклад, данні про довіру до користувачів, уведені адміністрацією). Межа ДОБ утворює периметр безпеки. Компоненти ДОБ, що знаходяться всередині цієї межі, повинні бути благонадійними. Компоненти, що знаходяться поза межею безпеки, не потребують надійності, і це не впливає на безпеку системи.

Розуміння бази даних та методи захисту інформації

База даних (БД) [2] – сукупність даних, які організовані відповідно до концепції, яка описує характеристику цих даних і зв'язки між їх елементами.

Система управління базами даних (СУБД) – це база даних і програма доступу до цих даних. СУБД надає можливість контролювати доступ до цих даних і взаємодіяти з ними.

Головною метою бази даних є збереження великих обсягів інформації. Дані в базі даних мають зберігатися у відповідності до надійної системи з гарантуванням безпеки. Якщо у такій системі є недоліки, то вони можуть проявитися в порушенні цілісності, втраті інформації чи доступу до неї сторонніми особами.

Будь-який збій бази даних може призвести до призупинення роботи підприємництва чи організації, що стане наслідком чималих матеріальних втрат.

Існують основні і додаткові методи захисту інформації в базах даних.

До основних належать: захист паролем – найпростіший спосіб захистити БД від неправомірного доступу, шифрування – спосіб приховання інформації, захист таблиць БД та розподіл прав доступу над базою даних.

Додаткові методи захисту бувають: вбудований засіб королю даних, забезпечення цілісності таблиць, організація спільного користування БД в мережі.

Як згадано вище, пароль – найпростіший засіб захисту. Він може бути встановлений як користувачем, так і адміністратором. Їхнє зберігання виконується СУБД. Паролі зберігаються в зашифрованому вигляді. Увівши пароль, користувач може отримати доступ до інформації.

Шифрування є сильнішим способом захисту інформації, адже це спеціальний алгоритм, який переводить інформацію у вигляд непридатний для читання. Існує два методи шифрування: симетричне й асиметричне. У симетричному один і той самий ключ використовується для шифрування і дешифрування. У асиметричному існує вже два ключі. Перший не секретний, який використовується для шифрування, а інший – секретний, який відомий одержувачу і використовується для дешифрування.

Висновки

Отже, в даній статті було досліджено основні методи захисту інформації в базі даних, а також виявлено їх плюси і мінуси. Провівши детальний аналіз існуючих методів захисту, зроблено висновок, що гарантування повної безпеки даних неможливе. Однак, краще використовувати комплекс заходів для підвищення безпеки інформації, а не лише якийсь один метод.

У підсумок можна додати, що бази даних є актуальними і залишаться такими й далі. Саме тому вчені всього світу приділятимуть увагу інформаційній безпеці та постійно вдосконалюватимуть систему захисту БД.

Список літературних джерел.

1) *«Data Security» Dorothy E. Denning and Peter J. Denning Data Security*
2) *«Database Systems: A Practical Approach to Design, Implementation, and Management» Thomas Connolly, Carolyn Begg*
3) *«High Performance MySQL: Proven Strategies for Operating at Scale 4th Edition» Silvia Botros, Jeremy Tinley*

УДК 004.65

Семенюк А. М.,
студент гр. Б21-д/122Б2-ІІ
Зелінська О.В., доцент
кафедри інформаційних технологій

ОБРОБКА ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ РЕЛЯЦІЙНИХ БАЗ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Плин часу вимагає зменшення паперового обігу документів і перехід до обробки інформації в електронному вигляді. Структурування цих даних, та їх виділення в окремі групи дозволить зменшити дублювання запитів і повторне введення однотипних відомостей.

Дана процедура є не що іншим як формуванням інформаційних масивів відібраних по певних критеріях, що по своїй суті є моделлю реляційної бази