Секція 1

ЗАХИСТ ЦІЛІСНОСТІ ДАНИХ У БАЗАХ ДАНИХ

Жарий І. І.
Національний аерокосмічний університет ім. М. Є. Жуковського
«Харківський авіаційний інститут»
Науковий керівник Морозова О. І.

Актуальність. В умовах розвитку інформаційних технологій, збільшення кількості інформації, права на зберігання якої передані користувачем третій особі, значно підвищується попит на якісні інструменти захисту цілісності, конфіденційності та доступності даних. Також віртуалізація юридичних та економічних процесів у локальних і глобальних системах додає актуальності завданню побудови системи захисту інформації (ЗІ), яка здатна якісно блокувати широкий спектр атак. Наразі об’єми інформації для зберігання та обробки збільшуються щодня, і потужним інструментом управління даними є бази даних (БД).

Цілісність є однією із основних характеристик інформаційної безпеки, а отже дослідження методів захисту цілісності інформації у БД є актуальним і необхідним для подальшого розвитку інформаційних технологій.

Метою даної роботи є аналіз методів забезпечення захисту цілісності даних у БД.

Основні положення. База даних (БД) являє собою упорядкований набір даних, які логічно взаємопов'язані. Головним завданням БД є збереження значних обсягів інформації. Дані в БД повинні зберігатися з гарантуванням безпеки та конфіденційності. Інформація не повинна бути загубленою або викраденою [1].

Якщо в системі захисту є недоліки, то даним може бути завдано шкоди, наприклад такої, як: порушення цілісності даних, викрадення (витік) даних, розсекречення даних з обмеженим доступом.

Система управління БД (СУБД) – це сукупність програм і мовних засобів, призначених для створення, ведення і використання БД [2].

Нижче наведено аналіз основних методів захисту інформації, що забезпечать надійний захист інформації від несанкціонованого втручання:

- захист паролем. Пароль має бути складною комбінацією літер, цифр та символів, зберігатися в СУБД у зашифрованому вигляді. Проте він має вразливість людського фактору;
- шифрування даних – це надійний метод, що забезпечує

неможливість прочитати інформацію, не знаючи ключа для дешифрування;

- права доступу дають контроль над спектром можливостей редагування даних у БД кожного з авторизованих користувачів;
- резервне копіювання – інструмент запобігання втрати цілісності всієї БД, або її частини. Копії зазвичай зберігають останній коректний образ БД, але можуть використовуватись для пошуку причини деякого інциденту безпеки БД [3];
- захист полів та записів – особливості БД, а саме як вона реалізована програмно та які модифікатори доступу мають її складові;
- аудит – це допоміжна процедура, яка призначена для перевірки повноти залучення передбачених засобів керування й відповідності рівня захищеності БД встановленим вимогам [3];
- забезпечення цілісності зв'язків таблиць БД;
- організація спільного використання об'єктів БД в мережі.

Висновки. Якість впровадження розглянутих методів захисту цілісності даних у БД та самої БД у цілому буде пропорційною стійкості системи. Однак, неможливо створити ідеально захищену систему, зловмисники все одно і надалі шукатимуть і використовуватимуть програмні і фізичні вразливості СУБД. Однак, при використанні методів захисту інформації, можливо створити систему, якій можна буде довіряти дані БД.

Список літератури

1. Захист інформації в базах даних. *IRlib*. URL: https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/24448/Касянчук%20Н.1.pdf?sequence=1&isAllowed=y (дата звернення 23.11.2022);
2. Системи управління базами даних. *Rodak*. URL: http://rodak.if.ua/komptech/lection4.htm (дата звернення 23.11.2022);
3. Захист БД від несанкціонованого доступу. *RDP*. URL: https://rdb.dp.ua/uk/chapter_11 (дата звернення 23.11.2022).

Відомості про авторів

Жарий Іван Ігорович, студент кафедри комп'ютерних систем, мереж і кібербезпеки, м.т. 0937232779, i.zharyi@student.csn.khai.edu
Морозова Ольга Ігорівна, професор кафедри комп'ютерних систем, мереж і кібербезпеки. д.т.н., професор, м.т. 0503001758, o.morozova@khai.edu