2. Пастернак В.В. Особливості моделювання методами StarUML. / В.В.Пастернак // Математичні методи та моделі технічних і економічних систем*:* тези доп. Міжнар. наук.-техн. конф. (22-23 лист. 2022 р.). – Тернопіль, 2022. – с. 146-147.

3. Пастернак В.В. Еволюція розвитку інформаційних систем та технологій. В.В.Пастернак // Комплексне забезпечення якості технологічних процесів та систем: тези доп. XII Міжнар. наук.-практ. конф. (26-27 травн. 2022 р.). – Чернігів, 2022. – с. 180-181.

*УДК: 004.056.6*

**Рзаєва С. Л., канд. техн. наук, доцент**
Державний торговельно-економічний університет, м. Київ, rzaevasl@knute.edu.ua
**Рзаєв Д. О., старший викладач**
Київський національний економічний університет імені Вадима Гетьмана, ditomas@ukr.net
**Ковальова Л. І., спеціаліст**
Державний торговельно-економічний університет, м. Київ, l.kovalova@knute.edu.ua

## ОСНОВНІ СКЛАДОВІ БЕЗПЕКИ СХОВИЩА ДАНИХ ТА МЕТОДИ ЗАХИСТУ

Проблеми безпеки сховища даних, пов’язані з процесом забезпечення безпеки всіх даних, незважаючи на те, що зберігається маса/велика інформація. Безпека даних пов’язана зі стійкістю та надійністю інформації.

На етапі сховища, доступ до даних зазвичай матимуть більше груп користувачів, ніж у базах даних. Необхідно застосовувати керування даними, щоб захистити певні фрагменти конфіденційної інформації від доступу не тих користувачів організації. Незалежно від того, чи йдеться про особисту інформацію (PII), чи фінансову інформацію, забезпечення конфіденційності даних має бути протягом усього «шляху» від БД до сховища даних. Запобігання оприлюдненню такої інформації є ключовим, і до нього можна підходити різними способами.

Кожна компанія зберігає інформацію, яка не може бути відкритою для всіх, хто працює в компанії. При переході від БД до Data Warehouse більше людей отримають доступ до даних. Адміністратору потрібно переконатися в узгодженості конфіденційної інформації, її збереження та обмеження у сховищі даних, і як до неї можна отримати доступ за допомогою інструментів бізнес-аналітики (BI).

Є кілька способів вирішення цього питання та кілька запитань, на які потрібно відповісти.

1) Де зараз обробляються конфіденційні дані (ідентифікаційна та фінансова інформація)?

2) Чи будуть ці конфіденційні дані все ще присутні в сховищі даних, а потім очищені?

3) Як цю інформацію буде видалено або обмежено з відкритих наборів даних - сценаріїв на шляху до сховища, вітрин даних, створених зі сховища?

На ці запитання потрібно відповісти, перш ніж підключати ці джерела до інструментів BI. У великих компаніях часто всі внутрішні дані вважаються конфіденційними. Навіть у внутрішньому плані департаментам необхідно знати дані інших департаментів. Проблеми виникають, коли компанія підключає своє сховище даних до своєї платформи BI або загалом надає доступ для запитів різним відділам. Це призводить до потенційного доступу до конфіденційних даних неавторизованими користувачами.

*Як захистити конфіденційні дані в сховищі даних.* Найпряміший спосіб обмежити доступ належним людям - це застосувати правила на рівні бази даних (сховище даних використовуються як реляційна база). Це можна зробити шляхом створення дозволів нарівні «лише для читання», створення спеціальних груп користувачів і шифрування конфіденційних даних.

*Лише для читання.* Налаштування сховище «лише для читання» за замовчуванням – запобігає виконанню будь-яких небезпечних інструкцій SQL-запису для даних.

*Спеціальні групи користувачів.* Незалежно від того, чи створюється сховище лише для читання, необхідно створити нову групу користувачів із доступом «лише для читання». Можна виключити доступ до певних таблиць або стовпців даних для цієї нової групи користувачів. Крім того, можна обмежити доступ до даних у розрізі окремих рядків. Дозволи на рівні рядків дозволяють надавати повний доступ до таблиць, що містять конфіденційну інформацію, але при цьому обмежують конкретні рядки та значення, що може бачити особа, яка здійснює запит.

*Шифрування стовпців.* Якщо потрібно згрупувати або агрегувати конфіденційні дані, можна створити зашифровані версії даних. Потім користувачі можуть створювати зведені таблиці, у яких конфіденційні показники, як-от фінансові дані, можна агрегувати до рівня, який підходить для перегляду та аналізу різними відділами. Рівень безпеки, який ви запроваджуєте, обмежує тип аналізу даних, але забезпечує захист конфіденційних даних.

*Як захистити конфіденційні дані в інструменті BI.* Після захищення базової структури даних у сховищі, необхідно переконатися, що в інструменті BI немає лазівок. Навіть встановлення правильних дозволів для сховища даних не гарантує, що конфіденційні дані не будуть неналежним чином передані через інформаційну панель або звіт інструменту BI. Цьому типу проблеми важко запобігти, тому загальною стратегією є встановлення політик для користувачів інструменту BI та регулярний контроль користувачів, з перевіркою прав доступ до даних, яких даний користувач може переглядати.

*Послідовний аудит/очищення облікового запису.* Змінюються проекти, змінюються ролі та сценарії використання. Будь-яка з цих змін може вплинути на дозволи співробітників компаії. Застарілі дозволи можуть призвести до проблем із відповідністю та конфіденційністю. Періодична перевірка та оновлення дозволів є найкращою практикою для захисту конфіденційних даних. Під час аудиту необхідно виконати перевірку та дати відповіді на питання:

Хто має доступ до яких джерел даних?

Хто має доступ до конфіденційної інформації на рівні рядка?

Хто входить до команди адміністратора чи має доступ адміністратора?

Хто має доступ або переглядає інформаційні панелі та звіти, що містять конфіденційні дані?

Періодична перевірка та оновлення дозволів є найкращою практикою для захисту конфіденційних даних. Всі сучасні інструменти BI пропонують відповіді на ці запитання за допомогою різних рівнів інформації про використання додатку, яку адміністратори можуть контролювати та переглядати.

Отже, захист даних є важливою темою в наш час. Інформація, яка зберігається в сховищах даних, може бути дуже цінною, тому її захист є ключовим завданням для бізнесу та інших організацій. Важливо пам'ятати, що при переході від бази даних до сукупних даних більше людей підтримують доступ до даних, тому необхідно забезпечити високий рівень конфіденційності та обмежити доступ до інформації.

При використанні інструментів бізнес-аналітики (BI) необхідно пам’ятати про те, що доступ до даних повинен бути обмежений лише до необхідного кола користувачів, а також необхідно включити заходи безпеки для захисту від несанкціонованого доступу до даних.

Тому захист даних є складною та важливою задачею, яка потребує поточного планування та виконання заходів безпеки, щоб забезпечити конфіденційність та надійність інформації.

**Список посилань**

1. Al-Fedaghi, S. (2020). Protecting Data Privacy and Security in Cloud Computing. Journal of Information Privacy and Security, 16(1), 28-39. Doi: 10.1080/15536548.2019.1703446

2. Huang, C., Li, M., Li, Y., Li, X., & Li, F. (2019). Data security and privacy protection in cloud computing. Future Generation Computer Systems, 93, 237-246. Doi: 10.1016/j.future.2018.10.048

3. Yaqoob, I., Hashem, I. A. T., Ahmed, E., Ahmed, A. I. A., Gani, A., & Imran, M. (2017). Big data: from analytics to learning. Big Data and Cognitive Computing, 1(1), 4. Doi: 10.3390/bdcc1010004.