ної схеми алгоритму багатоступеневого стиснення. Прикладом цього є формат даних TIFF, де алгоритм Хаффмана є лише одним із декількох кроків [4].

Отже, ефективне управління та обробка даних є важливим питанням у сучасному суспільстві, де різноманітної інформації багато і її обсяг постійно зростає. Технологія стиснення даних є важливим інструментом для оптимізації обробки великих масивів інформації та зменшення обсягу інформації без втрати її важливості. Було розглянуто кілька методів стиснення, зокрема RLE, групи KWE та алгоритм Хаффмана, кожен з яких має свої переваги та обмеження залежно від застосування.

Список використаних джерел

1. Salomon D. Data Compression: The Complete Reference. Springer London. 2007. DOI: 10.1007/978-1-84628-603-2.

2. Compression Algorithm. URL: https://www.sciencedirect.com/topics/ computer-science/compression-algorithm (дата звернення: 20.10.2023).

3. Основи інформаційних технологій. URL: https://informatics6.webnode.com.ua/zanyattya-10/ (дата звернення: 20.10.2023).

4. Олашин О. О. Інтелектуальна система покращення алгоритмів стиску зображення. URL: https://ela.kpi.ua/server/api/core/bitstreams/d2665c09-73e8-4319-8dc6-82bca5d989c8/content (дата звернення: 20.10.2023).

УДК 004.056.5:004.65

Коновалюк І. Л., здобувач 2 курсу спеціальності 122 Комп'ютерні науки,

Зелінська О. В., канд. техн. наук, доцент, в. о. завідувача кафедри інформаційних технологій

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БАЗ ДАНИХ

Донецький національний університет імені Василя Стуса, м. Вінниця

Кожен бізнес, корпорація чи державна установа має інформаційну базу, яка включає дані про клієнтів, нормативні акти, продукти та фінансову звітність. Великі об'єми інформації зазвичай містять конфіденційні, корпоративні та особисті дані. Несанкціонований доступ до цих даних може призвести до серйозних наслідків у фінансовій і репутаційній сферах.

Існують дві ключові причини, які зумовлюють необхідність для приватних компаній та державних установ вкладати значні ресурси у захист баз даних.

По-перше, це кіберзлочинність. Зловмисники постійно удосконалюють свої методи, використовують нові види програм-вимагачів та безфайлові методи

проникнення, що ставить під загрозу конфіденційність інформації. Тільки у 2019 р. було розкрито понад 9 мільярдів облікових записів із персональною інформацією. Спільно з розвитком злочинних технологій розробляються рішення для захисту конфіденційної інформації, як-от налаштування конфігурації брандмауера для обмеження доступу до підозрілого трафіка та впровадження процедур у разі порушення безпеки [1].

По-друге, існує проблема відповідності. Міжнародне законодавство щодо захисту персональної інформації стає дедалі суворішим, і відповідальність за дотримання конфіденційності даних покладається на організації. Нормативні вимоги можуть значно відрізнятися залежно від галузі та типу інформаційних активів. Забезпечення конкурентоспроможності вимагає від українських компаній великих витрат на захист баз даних [2].

Аспект безпеки даних є важливою частиною загальної стратегії захисту, яка включає в себе виявлення загроз, оцінку ризиків та їх зменшення для захисту конфіденційної інформації. Важливо відрізняти захист даних від безпеки баз даних, оскільки вони обидва вимагають активних та пасивних заходів відповідно. Захист баз даних включає в себе різноманітні методи, програмні засоби, процеси та технології, спрямовані на запобігання несанкціонованого доступу, модифікацій, випадкового розкриття та інших загроз. Політика конфіденційності стосується обробки та управління конфіденційною інформацією, зокрема особистою інформацією, даними кредитних карт та ін. конфіденційними даними.

Фундаментальна тріада, відома як конфіденційність, цілісність і доступність (CIA), є ключовими аспектами. Конфіденційність базується на принципі найменших привілеїв для запобігання несанкціонованого доступу. Цілісність спрямована на захист від неправомірного видалення чи зміни даних, а використання цифрових підписів є одним із методів гарантування цілісності. Доступність є ключовим елементом, який вимагає правильної роботи контролю, систем і програм для забезпечення доступності послуг та інформаційних систем за потреби [3].

Шифрування або криптографічний захист бази даних є одним з найбільш ефективних методів забезпечення безпеки БД. Алгоритм шифрування перетворює інформацію в незрозумілі символи з допомогою математичного процесу. Саме тоді, як інші інструменти безпеки захищають систему від вторгнень або атак, шифрування є фундаментальною формою, яка стосується безпеки самих даних. Навіть у разі злому системи інформація буде доступна для читання тільки авторизованим користувачам, які мають ключі шифрування.

Процес захисту бази даних неможливий без управління паролями, що має визначальне значення для підтримки безпеки. За цією стороною стратегії безпеки зазвичай стежать співробітники IT-підрозділу. Практика безпеки БД також

включає управління привілеями. Організації можуть зробити безліч різних кроків для управління паролями, наприклад, використовувати актуальні методи дво- або багатофакторної автентифікації, надавати користувачам обмежений час для введення облікових даних.

Розробка та забезпечення систем зберігання корпоративних даних є складним завданням, вирішення якого вимагає знаходження балансу між продуктивністю, доступністю і вартістю (рис. 1).

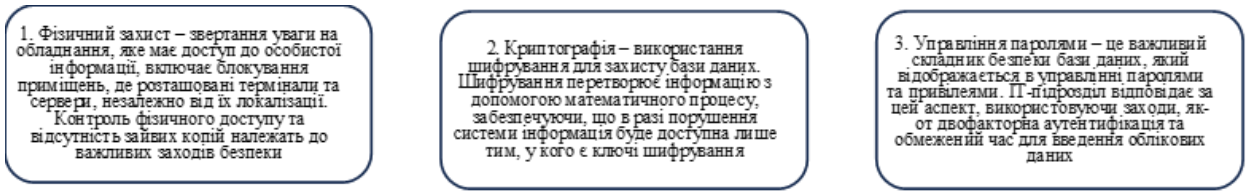

Рисунок 1. Системи зберігання корпоративних даних [4]

Можна зробити висновок, що використання лише одного методу не може гарантувати повного збереження даних. Тому для підвищення рівня безпеки інформації в базі даних рекомендується впровадження комплексних заходів. Розвиток у сфері безпеки баз даних є дуже важливим і потребує постійного вдосконалення. Проблема стала особливо актуальною під час російсько-української війни, коли для забезпечення державної безпеки були вжиті максимальні заходи, як-от закриття повного доступу до всіх державних реєстрів шляхом відокремлення їх від глобальної мережі.

Список використаних джерел

1. Касянчук Н. В., Ткачук Л. М. Захист інформації в базах даних. 2019. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/7001/5715.

2. Системи управління базами даних. URL: http://rodak.if.ua/komptech/lection4.htm. (дата звернення: 28.11.2023).

3. Шифрування та захист баз даних. URL: https://iitd.com.ua/shifruvannj a-ta-zahistbaz-danih/ (дата звернення: 28.11.2023).

4. Як створити надійний пароль – рекомендації спеціалістів ESET. URL: https://eset.ua/ua/news/view/649/nadezhnyy-parol-sposoby-sozdaniya-parolya-otspetsialistov-eset