Одна з основних переваг Splunk User Behaviour Analysis - виявлення невідомих загроз і аномального поведінки за допомогою машинного навчання.

– Micro Focus Security ArcSight UBA.

Продукт ArcSight User Behavior Analytics надає компаніям детальну інформацію про своїх користувачів, що значно спрощує формування даних про моделі поведінки, що допомагають пом'якшувати загрози. Він допомагає виявляти і розслідувати зловмисне поведінка користувачів, внутрішні загрози та зловживання обліковими записами. [4]

Підсумовуючи, можна стверджувати, що UEBA / UBA-системи - це наступний крок у визначенні невідомих типів загроз, цілеспрямованих атак і внутрішніх порушників. грунтуючись виключно на поведінковому аналізі, ці системи здатні виявляти аномалії і неочевидні взаємодії користувачів з корпоративними системами, що в кінцевому підсумку дозволяє адміністраторам безпеки бачити розширену картину безпеки підприємства та оперативно реагувати на інциденти ІБ.

Список використаних джерел

1.Обзор решений UBA, SIEM, SOAR: в чем различие? /[Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Technology_Analysis/UBA-SIEM-SOAR

2. UBA, или щем пользователей с «отклонениями» /[Електронний ресурс] – Режим доступу: https://habr.com/ru/company/inline_tech/blog/303240

Как UEBA помогает повышать уровень кибербезопасности /[Електронний ресурс] – Режим доступу: https://habr.com/ru/company/roi4cio/blog/436082/

3. Обзор рынка систем поведенческого анализа – User and Entity Behavioral Analytics(UBA/UEBA) /[Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/analytics/Market_Analysis/user-and-entity-behavioral-analytics-ubaueba

---

УДК 004.65

СУЧАСНІ ВИМОГИ ДО СИСТЕМ УПРАВЛІННЯ БАЗАМИ ДАНИХ

Бондар В., студ. гр. КБ-171, **Кулініч Р.,** студ. гр. КБ-171
Мехед Д.Б., кандидат педагогічних наук,
доцент кафедри кібербезпеки та математичного моделювання
Чернігівський національний технологічний університет

Актуальність. Кожне сучасне підприємство працює з великою кількістю інформації. В більшості випадків актуальність та доступність цих даних як для працівників, так і для клієнтів відіграють важливу роль в конкурентоспроможності та ефективній діяльності компанії. Зберігання актуальних даних є ключовим завданням для кожної сучасної організації. Зростає потреба в нових, надійніших засобах безпеки БД, здатних задовольнити вимоги до їх продуктивності та масштабованості. На сьогодні існує значна кількість різноманітних СУБД. Відповідно, актуальною постає необхідність комплексного розгляду та систематизації питань вибору оптимальних систем управління базами даних.

Метою дослідження виступає аналіз критеріїв та визначення сучасних вимог до систем управління базами даних.

Питання аналізу особливостей систем управління базами даних висвітлено в багатьох публікаціях закордонних і вітчизняних авторів. Зокрема, основні підходи до оцінки критеріїв та проблем вибору СУБД для побудови інформаційних систем розкриваються в працях: А. А. Аносова [1], М. Т. Фісуна, Є. О. Давиденка [2] та ін.

Завдання аналізу вимог до систем управління базами даних полягає в дослідженні потреб користувачів в зберіганні та оперуванні даними. Важливо враховувати вимоги до функціональності, надійності та доступності, зручність інтерфейсу та усвідомлення очікуваних результатів [3].

Визначення вимог до СУБД, що задовольнятимуть актуальні запити користувачів, ґрунтується на основних критеріях систем управління. При визначенні особливостей СУБД найчастіше використовують наступні групи критеріїв: моделювання даних; особливості архітектури та функціональні можливості; контроль роботи системи; особливості розробки додатків; продуктивність; надійність; вимоги до робочого середовища та змішані критерії.

Щодо *моделювання даних*, серед безлічі моделей найпоширеніші – ієрархічна, мережева, реляційна, об'єктно-реляційна і об'єктна. Вибір моделі залежить від вимог, що визначаються призначенням та галуззю використання баз даних.

Важливою є наявність та властивості тригерів – програм, що викликаються кожного разу при вставці, зміні або видаленні рядка таблиці. Тригери забезпечують перевірку будь-яких змін на коректність, перш ніж ці зміни будуть прийняті.

Деякі сучасні системи мають вбудовані додаткові засоби контекстного пошуку.

Слід також врахувати два фактично незалежних критерії: базові типи даних, закладені в систему, і наявність можливості розширення типів. Якщо відхилення базових наборів типів даних в сучасних

системах від якогось стандартного значення зазвичай невеликі, то механізми розширення типів даних у системах того чи іншого виробника істотно рызняться.

Мова запитів. Всі сучасні системи сумісні зі стандартною мовою доступу до даних SQL:2011, проте багато з них використовують різні розширення даного стандарту.

Особливості архітектури та функціональні можливості.

На сьогодні важливою умовою ефективності функціонування будь-якої системи є мобільність – це незалежність системи від середовища, в якому вона працює. Середовищем в даному випадку є як апаратура, так і програмне забезпечення (операційна система).

При виборі СУБД необхідно враховувати - чи зможе дана система відповідати зростанню інформаційної системи, до того ж зростання може виявлятися в збільшенні числа користувачів, обсязі збережених даних та оброблюваної інформації.

Розподіленість. Основною причиною застосування інформаційних систем на основі баз даних є прагнення об'єднати управління всією інформацією організації. Простий та надійний підхід – централізація зберігання та обробки даних на одному сервері. На жаль, це не завжди можливо і доводиться застосовувати розподілені бази даних. А отже, актуальність вибору залежить від різних можливостей управління розподіленими базами даних.

Мережеві можливості. В умовах сьогодення багато систем дозволяють використовувати широкий діапазон мережевих протоколів і служб для роботи та адміністрування.

Контроль використання пам'яті комп'ютера. Система може мати можливість управління використанням як оперативної пам'яті, так і дискового простору, стискання баз даних, або видалення надлишкових файлів.

Перевагою багатьох виробників СУБД є випуск *засобів розробки додатків* для своїх систем, зокрема: засоби проектування (деякі системи мають засоби автоматичного проектування як баз даних, так і прикладних програм), багатомовна підтримка, можливості розробки Web-додатків, підтримувані мови програмування (підвищують доступність системи для розробників, а також можуть істотно вплинути на швидкодію і функціональність створюваних додатків).

В умовах стрімкого розвитку інформаційних технологій на перший план виступають вимоги до *продуктивності* СУБД, що переважно визначається: рейтингом TPC (Transactions per Cent - TPC аналіз розглядає композицію СУБД і апаратури, на якій ця вона працює. Показник TPC – це відношення кількості запитів оброблюваних за якийсь проміжок часу до вартості всієї системи); можливостями паралельної архітектури (розподілення обробки послідовності запитів на кілька процесорів, або використання декількох комп'ютерів-клієнтів, що працюють з однієї БД, які об'єднують у так званий паралельний сервер), можливостями оптимізації запитів (за початковим поданням запиту шляхом його синтаксичних і семантичних перетворень розробляється процедурний план виконання запиту, найбільш оптимальний за наявних у базі даних елементів управління).

Однією з найважливіших вимог є *надійність* (передбачає збереження інформації незалежно від будь-яких збоїв, безвідмовність роботи системи в будь-яких умовах, забезпечення захисту даних від несанкціонованого доступу). Включає наявність функцій відновлення після збоїв, резервного копіювання, відкату змін, багаторівневої системи захисту.

Вимоги до робочого середовища визначаються: підтримуваними апаратними платформами, мінімальністю вимог до обладнання, максимальним розмір адресної пам'яті, операційними системами, під управлінням яких здатна працювати СУБД.

Звертають на себе увагу такі корисні характеристики СУБД, як: якість і повнота документації, локалізованість, модель формування вартості (наприклад, вартість одного і того самого продукту може істотно змінюватися в залежності від того, скільки користувачів буде з ним працювати), стабільність виробника, поширеність СУБД.

Висновки. Детальний порівняльний аналіз перерахованих вище вимог до СУБД на основі тенденцій розвитку інформаційних систем допоможе споживачу раціонально вибрати відповідну систему для конкретного проекту, а розробнику – визначити шляхи подальшого вдосконалення власного продукту.

Список використаних джерел

1. Аносов А. Критерії вибору СКБД при створенні інформаційних систем URL: http://easy-code.com.ua/2011/02/kriterii-viboru-subd-pri-stvorenni-informacijnix-sistem/.

2. Фісун М. Аналіз та вибір моделей даних при створенні систем автоматизованого проектування / М. Т. Фісун, Є. О. Давиденко // Збірник наукових праць Національного університету кораблебудування. 2013. №2. С.89-94.URL: http://nbuv.gov.ua/UJRN/znpnuk_2013_2_17

3. Ying Wang, Design and realization of rock salt gas storage database management system based on SQL Server. December 2018, 466-472 URL:
https://reader.elsevier.com/reader/sd/pii/S2405656117301001?token=E5CF6B5C8FC955B95BD63D5FE5654CDE433B0BE8CC9587B4FF79433FDFB6A185E56FBF33C84C403556726D62BF9C60D5