УДК 681.518:658.51

В. Є. Сокол[1], М. В. Ткачук[2], М. О. Кузнецов[3],
[1] НТУ «ХПІ», м.Харків, Україна, vladyslav.sokol@gmail.com
[2] НТУ «ХПІ», м.Харків, Україна, tka@kpi.kharkov.ua
[3] НТУ «ХПІ», м.Харків, Україна, mshakuznetsov@gmail.com

МОДЕЛІ ТА АЛГОРИТМИ ОПРАЦЮВАННЯ ІНЦИДЕНТІВ В СИСТЕМАХ АВТОМАТИЗАЦІЇ КОРПОРАТИВНИХ IT-ПОСЛУГ НА ОСНОВІ ВИКОРИСТАННЯ БАЗИ ДАНИХ УПРАВЛІННЯ КОНФІГУРАЦІЯМИ

Проаналізовані деякі сучасні проблеми розробки та використання баз даних управління конфігураціями в системах автоматизації корпоративних IT-послуг. З метою удосконалення цієї технології запропонована розширена модель даних та досліджена ефективність використання різних пошукових алгоритмів.

БАЗА ДАНИХ, УПРАВЛІННЯ КОНФІГУРАЦІЯМИ, КОРПОРАТИВНІ IT-ПОСЛУГИ, ПОШУКОВИЙ АЛГОРИТМ

Вступ

Створення та подальший супровід корпоративної інфраструктури інформаційних послуг (або IT-інфраструктури) є необхідною умовою ефективного функціонування та розвитку практично всіх сучасних організацій та підприємств. Вона поєднує в собі різноманітні програмно-апаратні засоби, бази даних, канали зв'язку, периферійне обладнання, а також технічний персонал, що обслуговує різні групи користувачів IT-послуг. Для ефективного формування та використання такої IT-інфраструктури з'явився новий клас автоматизованих систем управління, а саме: системи управління інформаційно-технологічними послугами (СУІТП), використання яких має на меті забезпечити корпоративним користувачам надання певних IT-послуг із заданим рівнем якості [1-2]. Однією із основних функціональних підсистем типової СУІТП є модуль управління інцидентами (Incident Management) [1], який забезпечує підтримку персоналу СУІТП при вирішенні проблемних ситуацій, що виникають в роботі користувачів IT-послуг. В свою чергу, однією із найбільш важливих компонентів підсистеми управління інцидентами є база даних управління конфігураціями (configuration management database – CMDB). У контексті рекомендацій стандарту ITIL (IT-Infrastructure Library) [1] CMDB представляє собою репозиторій, що зберігає дані про всі суттєві компоненти та ресурси корпоративної IT-інфраструктури та має відповідні програмні засоби для встановлення взаємозв'язків між цими компонентами (тобто їх конфігураціями), а також відстеження змін, що відбуваються з часом в цих конфігураціях. Таким чином, CMDB є основним компонентом процесу управління конфігураціями в СУІТП, який в свою чергу є необхідною складовою процесів управління інцидентами, що виникають в процесі функціонування корпоративної IT-інфраструктури.

Тому метою дослідження, результати якого представлено в цій роботі, є аналіз основних особливостей використання бази даних управління конфігураціями для задач управління інцидентами, а також дослідження моделей та алгоритмів, що мають на меті забезпечити підвищення ефективності цих процесів при використанні сучасних та перспективних СУІТП.

1. Критичний огляд існуючих підходів до побудови та застосування баз даних управління конфігураціями

Основними функціональними компонентами CMDB, які визначені на рівні її логічної моделі, а також які мають бути реалізовані за допомогою відповідних структур зберігання даних, є наступні [3]:

конфігураційна одиниця (configuration item) – це будь-який компонент або інший сервісний ресурс корпоративної IT-інфраструктури, яким необхідно управляти, для того аби надати відповідну IT-послугу користувачеві СУІТП. Інформація про кожну конфігураційну одиницю (КО) реєструється у формі запису в CMDB і підтримується актуальною протягом всього життєвого циклу процесу управління конфігураціями;

конфігурація (configuration) – узагальнений термін, що використовується для опису певної групи конфігураційних одиниць, які функціонують разом для забезпечення певної IT-послуги або деякої її частини.

Термін "конфігурація" також використовується в стандарті ITIL [1] для позначення налаштувань параметрів однієї чи декількох КО у складі CMDB. Управління конфігураціями (КФ) має забезпечувати вирішення наступних задач [4-6]:

– облік всіх КО в IT-інфрастуктурі організації, в якій функціонує відповідна СУІТП;

– надання точної інформації про існуючі КФ та документації для підтримки всіх інших процесів управління IT-послугами;

– створення інформаційного базису для поточного управління інцидентами, що виникають в роботі користувачів IT-послуг.

Досягнення цих цілей дозволяє організації більш ефективно здійснювати управління, інтеграцію і підтримку прийняття рішень щодо ІТ-послуг, а перевірка і коректування конфігураційних записів CMDB забезпечують більш високий рівень контролю корпоративної ІТ-інфраструктури. Процеси управління КФ та інцидентами можна інтегрувати, наприклад, двома способами [6]:

1) якщо для усунення інциденту необхідно внесення змін до даних щодо відповідних КО, модуль управління інцидентами може автоматично створити запит на модифікацію відповідних записів в CMDB;

2) модуль управління інцидентами може використовувати модель даних CMDB для виявлення змін у відповідних КФ, які могли стати причиною виникнення цього інциденту.

Наявність повних і точних даних щодо КО та КФ, які накопичені в CMDB і застосовуються в процесах управління ІТ-послугами, дозволяє персоналу СУІТП приймати вірні рішення і більш точно оцінити ресурси і продуктивність наявних ІТ-ресурсів. Згідно з визначенням [3], кожна КО – це окрема сутність, яка є частиною ІТ-інфраструктури організації і яка має певний набір відповідних атрибутів. Всі КО повинні бути безпосередньою частиною реально існуючої ІТ-інфраструктури відповідної організації, а не тільки інформацією про цю частину.

Для побудови концептуальної моделі даних CMDB можуть бути використані наступні альтернативні підходи [7]:

– розробка за схемою «зверху-вниз» (top-down approach), яка передбачає необхідність ідентифікації спочатку всіх основних бізнес-процесів в організації, а вже потім, на підставі цього, і визначення ключових елементів ІТ-інфраструктури (тобто відповідних КО та КФ), які їх забезпечують;

– розробка із застосуванням схеми «знизу-вверх» (bottom-up approach), що забезпечує формування моделі даних шляхом послідовного додавання до неї кожного нового КО, тобто додавання даних про кожний новий програмний сервіс або апаратний компонент ІТ-інфраструктури організації;

– ітеративний підхід (iterative approach), який означає те, що модель даних CMDB формується у досить вільному форматі, який визначається (та може неодноразово змінюватися) в процесі накопичення проектного досвіду.

Але, незважаючи на наявність різних підходів щодо побудови CMDB, її типова функціональність, як правило, містить наступні операції

(a) створення (create) та маніпулювання (select / delete / insert / update) таблицями, що містять різні типи КО;

(b) встановлення та підтримка логічних зв'язків (тобто КФ) між різними таблицями КО за допомогою механізму зовнішніх ключів (foreign key);

(c) моделювання ієрархічних структур КО (або ієрархічних КФ) шляхом побудови відношення "суперклас (superclass) – підклас (subclass)";

(d) відстеження в режимі реального часу стану змін та запитів на зміни в КО та у відповідних КФ.

На підставі цього аналізу можливо зробити наступні висновки щодо недоліків у наявній функціональності існуючих CMDB в процесі їх використання для управління інцидентами, які в основному збігаються із висновками, представленими в [6], а саме:

1. Типова функціональність CMDB не передбачає можливостей розширеного пошуку даних у запитах користувачів щодо інцидентів, які містять певні ключові слова (key words).

2. В існуючих процедурах пошуку в CMDB, як правило, не задіяні механізми індексації таблиць зберігання даних щодо КО.

3. При зберіганні даних щодо КО в структурі CMDB не враховуються різні вагові коефіцієнти для відповідних семантичних зв'язків, таких, як наприклад, проста асоціативна залежність (association) або наслідування / узагальнення (inheritance / generalization).

Таким чином, для подолання недоліків (1)-(3), що має на меті підвищення ефективності застосування технології CMDB у процесі управління інцидентами, необхідно розширити відповідну модель даних та розробити алгоритми, що доповнюють функціональність типових операцій (a)-(d) над даними, які накопичуються в CMDB.

2. Застосування CMDB для пошуку елементів конфігурації в процесах опрацювання інцидентів (Incident Management)

Запропонований вище загальний підхід до розширення функціональних можливостей застосування бази даних управління конфігураціями в процесі опрацювання інцидентів при застосуванні відповідної системи СУІТП може бути реалізований у спосіб, який більш детально представлений у цьому підрозділі даної статті.

2.1. Функціональна схема управління інцидентами із застосуванням CMDB

На рис. 1 представлена загальна схема процесу опрацювання інцидентів із використанням технології CMDB, основні етапи якого стисло можна викласти наступним чином.

Процес опрацювання інцидентів починається з моменту його виникнення (це блок (1) на рис. 1). Інцидентом (incident) називається будь-яке незаплановане переривання чи зниження якості ІТ-послуг [6], що надаються корпоративним користувачам. При цьому помилка в роботі окремої КО, яка ще не вплинув на певну послугу, також є

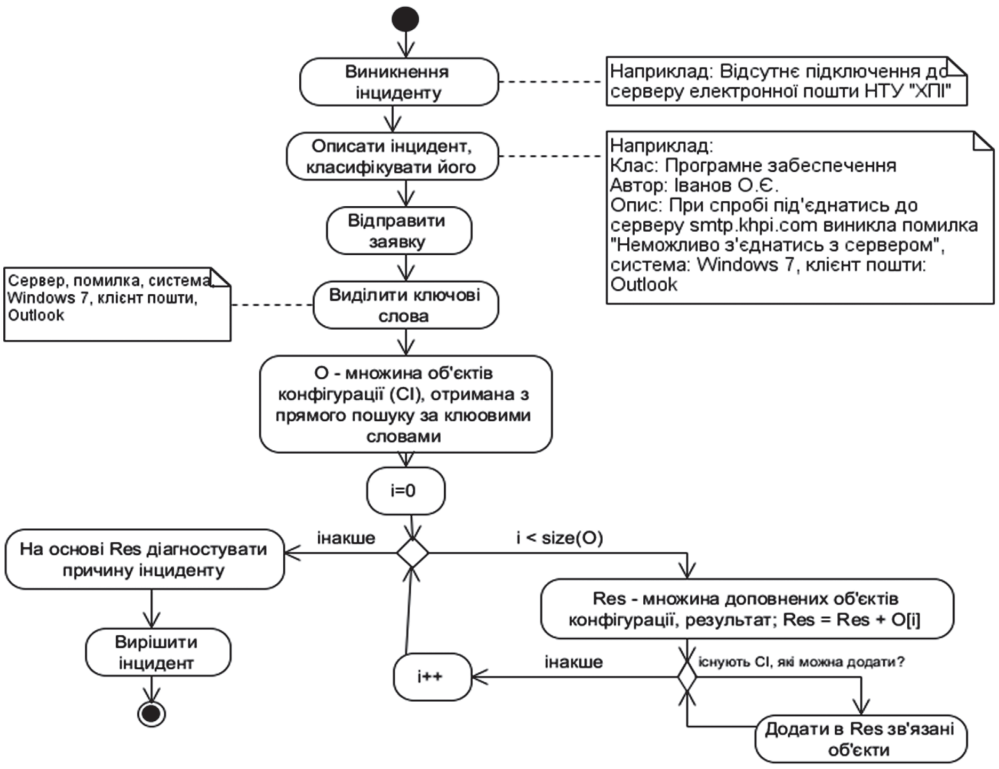

Рис. 1. Загальна схема застосування CMDB в процесі управління інцидентами

інцидентом. Кожному інциденту відповідає текстовий запит (або заявка), що складається відповідним користувачем ІТ-послуг у певному форматі, який він потім надсилає до системи СУІТП через її web-інтерфейс, або електронною поштою (блок (2) на рис. 1). Умовний приклад такої заявки надано на рис. 2.

Користувач	Наливайко М.П.
Тема	Не працює електронна пошта
Клас інциденту	Програмне забезпечення
Опис	При спробі підключення до серверу smtp.khpi.com виникла помилка «Неможливо з'єднатись з сервером». Операційна система: Windows 7, поштовий клієнт: Outlook 2007.

Рис. 2. Приклад текстового опису інциденту, який направлено в СУІТП

Наступним етапом є опис інциденту та його класифікація (це блок (3) на рис. 1). Після занесення запиту в систему із застосуванням методів обробки природної мови, наприклад, із використання онтологій, з його тексту виділяються ключові слова (це блок (4) на рис. 1). Цей список ключових слів далі передається до блоку пошуку релевантних КО, який має на меті розширити множину причин інциденту, спираючись на знання щодо КФ, по відношенню до яких був зафіксований поточний інцидент. Виконується пошук КО, що описуються цими ключовими словами. Далі цей список передається на вхід до алгоритму пошуку релевантних КО, в результаті роботи якого ми отримуємо новий, розширений список КО. На основі цього списку експерт може робити більш точний висновок відносно того, що могло бути причиною інциденту, провести додаткову діагностику, або ж список передається у якості ключових слів для CBR-системи.

2.2 Розширення типової схеми даних CMDB

На рис. 3 представлена підсхема даних, яка розширює модель даних типової CMDB, у якості якої може бути розглянута, наприклад, схема даних СУІТП Open-source Ticket Request System (OTRS), а саме її розширення OTRS::ITSM 3.3.3 [8]. Особливістю даної підсхеми є наявність таблиці ключових слів *keywords*, в яку заносяться ключові поняття про дану конфігураційну одиницю, а також наявність поля ваги (*weight*) для відображення семантичної значимості взаємозв'язків (link_type) між різними КО, інформація про які міститься в таблиці *link_relation*.

Необхідність модифікації існуючої схеми обумовлена необхідністю реалізації пошуку за ключовими словами. В роботі [6] проаналізовані декілька алгоритмів пошуку за ключовими словами та зроблені висновки щодо можливостей їх використання. Були також розглянуті недоліки існуючих можливостей використання типової схеми бази даних управління конфігураціями в процесі управління інцидентами та висунуті пропозиції щодо їх вирішення.

Запропонована схема надає можливість виконувати пошук КО більш ефективно, як показано в роботі [6], ціллю введення таблиці ключових слів

є індексація опису КО у вигляді списку тегів, які описують дану КО, адже у випадку відсутності такої таблиці для виконання пошуку за ключовими словами потрібно було б виконати пошук за полем повнотекстового опису КО. Поле ваги (weight) уможливлює врахування нерівноцінності зв'язків як з точки зору направлення (наприклад у відношенні наслідування, сторона-предок має більшу вагу по відношенню до потомків, ніж навпаки), так і з точки зору семантики (наприклад відношення наслідування є більш вагомим типом зв'язку, аніж асоціація).

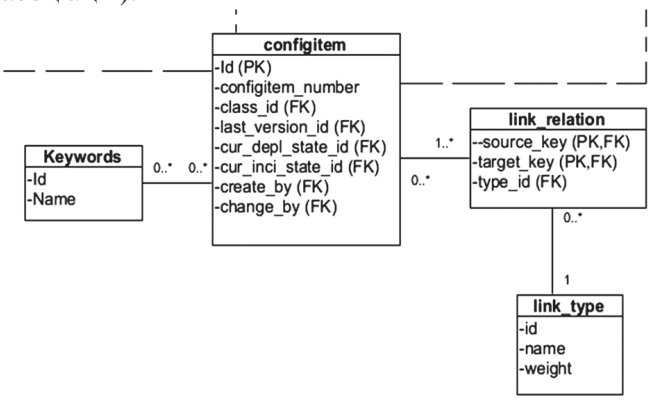

Рис. 3. Підсхема даних для розширення функціональності типової CMDB

2.3 Узагальнена схема пошукових алгоритмів

Як показано в [6], для пошуку КО може бути використано декілька алгоритмів: алгоритм всенаправленого (omni-directional) та направленого (directed) пошуків. На вхід кожного з алгоритмів подається список ключових слів, виділених попередньо з опису інциденту. Кожен з цих слів оцінюється з точки зору релевантності, ця оцінка *r*, з інтервалу [0;1] може бути отримана на етапі аналізу повідомлення про інцидент (див. рис. 1). Загальна схема цього процесу показана на рис. 4. При цьому вибирається глибина пошуку на графі опису КО, що є, в свою чергу, певною конфігурацією КФ, а також максимально можлива кількість КО, тобто величина *nmax*. Також, в залежності від алгоритму, може бути використаний коефіцієнт α, що задається на інтервалі [0;1] та вибирається таким чином, аби значення добутку значення релевантності ключового слова та відповідних вагових коефіцієнтів, належало до інтервалу [0;1].

Визначена таким чином оцінка релевантності *RR* для кожної КО може бути отримана за наступною формулою

$$RR = r * \prod_{0 \le i \le rd} \frac{w_i(rel\_type)}{a}. \qquad (1)$$

Пошук на графі реалізовано за допомогою рекурсивної функції, яка виконує пошук на графі з параметром глибини пошуку, а отримані таким чином результати потім складаються. Тоді для кожної конфігураційної одиниці знаходиться релевантність. $w_i(rel\_type)$ – це нормована вага зв'язку, що знаходиться на інтервалі [0;1]. Також може бути введене обмеження на величину *RR* деяким пороговим значенням c_n / β, де c_n – значення релевантності деякої КО, і тоді відповідне значення *RR* визначається формулою

$$RR = c_j * \prod_{0 \le i \le rd} \frac{w_i(rel\_type)}{a} > \frac{c_n}{\beta}. \qquad (2)$$

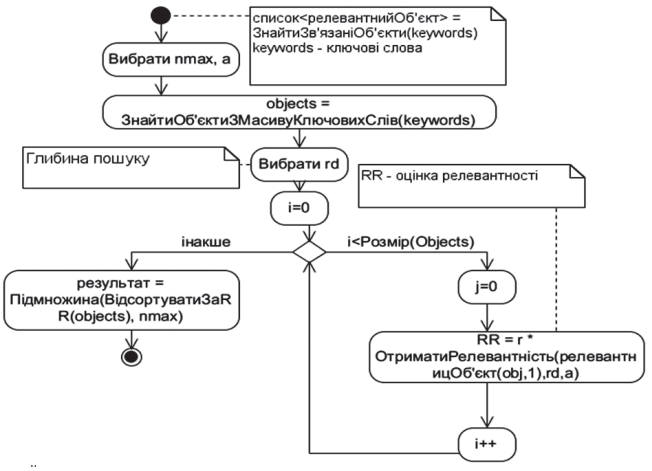

Рис. 4. Узагальнена схема пошукових алгоритмів

Якщо ж об'єкт КО пов'язаний з багатьма ключовими словами, його значення релевантності є сумою окремо порахованих для кожного ключового слова релевантностей за формулами (1)-(2). При цьому коефіцієнти α та β, а також максимальний розмір кількості об'єктів визначаються дослідним шляхом.

3. Програмна реалізація та тестування альтернативних алгоритмів пошуку в CMDB

3.1 Вибір технологій та проектування програмного компонента тестування CMDB

В якості програмного засобу для тестування алгоритмів було використано СКБД MS SQL Server 2008 [8], яка надає широкі можливості для відпрацьовування SQL-запитів і дозволяє використовувати інструменти відстеження часу виконання запитів з боку інших програм. Відповідний програмний компонент був спроектований таким чином, аби мати можливість задавати параметри окремих алгоритмів і тестувати їх ефективність.

3.2 Інтерфейс користувача та тестовий приклад

Для дослідження ефективності розглянутих вище алгоритмів використовувались тестові дані, які утворюють граф КФ, який наведено на рис. 5. Вузлами на цьому графі є окремі КО, а відповідними дугами вказані зв'язки, їх напрямок та тип. Для кожної КО також вказуються ключові слова, так, наприклад, для КО Windows 7 можна записати такі ключові слова, як «OS, Windows» та ін.

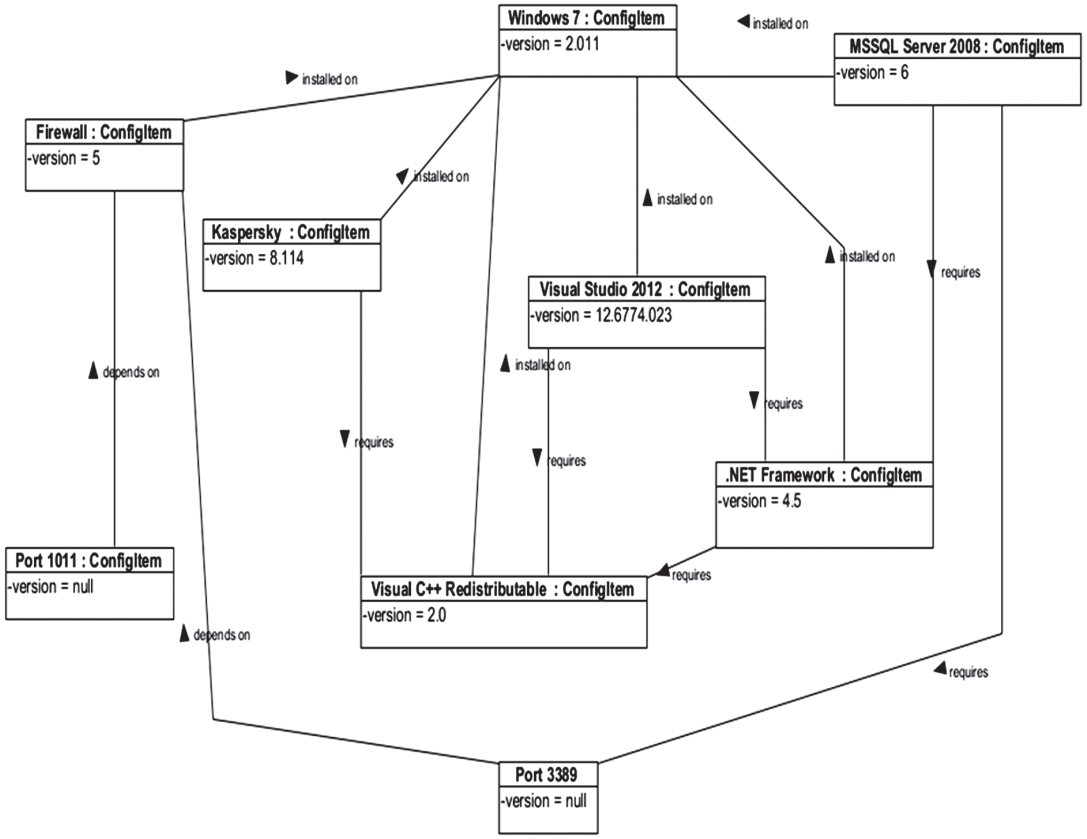

Рис. 5. Граф конфігурації для тестового прикладу

Інтерфейс користувача компонента тестування дозволяє інтерактивно задавати глибину пошуку *nmax* та вводити різні ключові слова. В результаті виконання алгоритму формується список КО, які відсортовані за спаданням значення оцінки їх релевантності *RR*., і приклад такого списку для всенаправленого пошуку наведено на рис. 6.

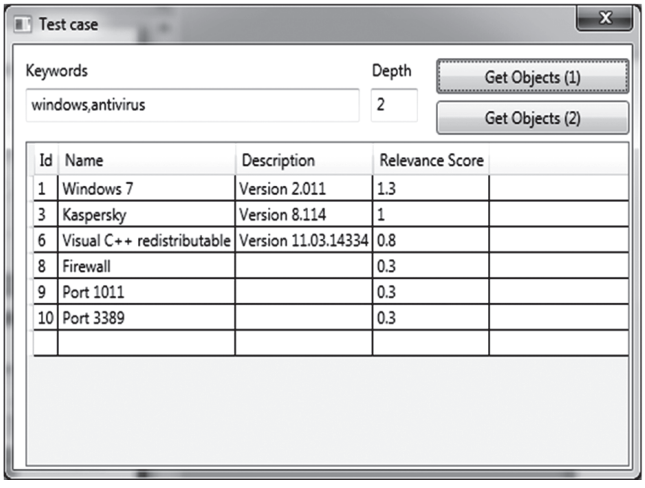

Рис. 6. Інтерфейс компоненту для тестування алгоритмів

Для реалізації роботи алгоритму направленого пошуку спочатку формується шаблон пошуку. Це граф, вузли котрого складають певні класи КО, такі, як, наприклад, «операційна система», «антивірус», «порт локальної мережі» та ін. Такі шаблони складаються експертами на основі аналізу прецедентів і один з можливих прикладів представлено на рис. 7.

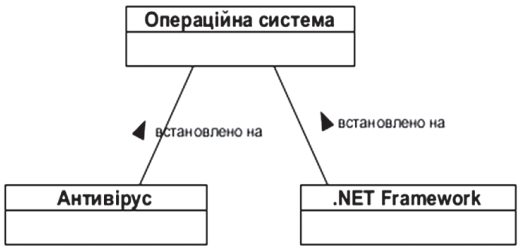

Рис. 7. Шаблон пошуку в базі даних

В подальшому розглянуті вище альтернативні були протестовані з метою оцінки їх ефективності.

3.3 Аналіз отриманих результатів

На основі аналізу тестових пошукових запитів до CMDB були отримали статистичні дані, що доводять вищу ефективність алгоритму направленого пошуку. Відповідні результати обчислювального експерименту наведені в табл. 1. В ній параметр *Depth* визначає глибину пошуку, тобто вказує на кількість рівнів на графі конфігурацій (див. рис. 4), які належать до області цього пошуку. При цьому кількість відповідних елементарних SQL-запитів, що є необхідними для виконання відповідних тестових пошукових запитів, була розрахована на основі аналізу процесу обробки CMDB за допомогою стандартного засобу SQL Server Profiler [8]. Фрагмент даних результатів цих тестів наведено в табл. 1.

Таблиця 1

Кількість запитів до бази даних
при різній глибині пошуку

Алгоритм	Depth=1	Depth=2	Depth=3
Всенаправленого пошуку	9	18	23
Направленого пошуку	9	11	15

З аналізу результатів цього експерименту видно, що із зростанням глибини пошуку на графі конфігурацій використання алгоритму направленого пошуку стає більш ефективним приблизно на 35-40%. В той же час необхідно відмітити, що для повного аналізу цієї проблеми необхідно враховувати також і деякі інші фактори, такі, як, наприклад, кількість ключових слів та їх релевантність (див. формули (1)-(2)).

Висновки

В даній статті розглянуто деякі актуальні питання підвищення ефективності використання баз даних управління конфігураціями (CMDB) в системах автоматизації надання корпоративних ІТ-послуг і, зокрема, побудована узагальнена схема застосування пошукових алгоритмів для опрацювання інцидентів, що виникають в таких системах. Експериментально досліджена порівняльна ефективність застосування двох альтернативних пошукових алгоритмів і зроблено висновки щодо доцільності їх використання в різних пошукових конфігураціях. У подальших дослідженнях заплановано розширити кількість параметрів пошукових алгоритмів, які мають вплив на їх ефективність, та розробити більш зручний програмний засіб для проведення таких експериментів.

Список літератури: 1. ISO/IEC 20000-1,2. Information Technology-Service Management, Part 1, 2: Geneva, Switzerland: ISO/IEC (2005). **2.** *Ткачук М. В.* Розробка методики комплексної оцінки ефективності впровадження систем управління ІТ – інфраструктурою організацій / М. В. Ткачук, В. Є. Сокол, О. В. Черкашенко // Вісник Національного технічного університету "ХПІ". – Харків: НТУ "ХПІ". – 2012. – № 30. – С. 94-104. **3.** Глоссарий стандарта ITIL v3 [Електронний ресурс] - Режим доступу : www/ URL: http://itsmforum.ru/ZAM-test/Russian_2011_Glossary_v2.0.pdf - 5.01.2014 р. **4.** The CMDB the central IT – repository [Електронний ресурс] - Режим доступу : www/ URL: http://doc.otrs.org/itsm/1.2/en/html/ch06.html 5.01.2014 р. **5.** *Александров* А. Конкретно о CMDB / А. *Александров* // Открытые системы. – 2007. – №6. – С. 45–51. **6.** *Gupta R.* Automating itsm incident management process / R. Gupta, K. Prasad, and M. Mohani // Autonomic Computing, 2008. ICAC '08. International Conference on, pp. 141-150, June 2008. **7.** *Ayat M.* CMDB Implementation Approaches and Considaration in SME/SITU's Companies / M. Ayat, M. Sharifi, S. Sahibudin // 2009 Third Asia International Conference on Modeling & Simulation, pp. 381-385, May 2009. **8.** OTRS IT Service Management Software Возможности [Електронний ресурс]. – Режим доступу : www/ URL: http://www.otrs.com/software/otrsitsm-features/?lang=ru 6.01.2014. **9.** SQL Server Profiler [Електронний ресурс] - Режим доступу: www/URL: http://technet.microsoft.com/ru-ru/library/ms181091.aspx 5.05.2014

Надійшла до редколегії 19.03.2014

УДК 681.518:658.51

Модели и алгоритмы обработки инцидентов в системах автоматизации корпоративных IT-услуг на основе использования базы данных управления конфигурациями / В. Е. Сокол, Н. В. Ткачук, М. А. Кузнецов // Бионика интеллекта: научн.-техн. журнал. – 2014. – № 1 (82). – С. 74–79.

В статье рассмотрены подходы к применению баз данных управления конфигурациями для решения задач обработки проблемных ситуаций в работе пользователей корпоративных ИТ-услуг. Предложен обобщенный алгоритм и расширенная модель данных для повышения эффективности применения этой технологии.

Ил. 6. Библиогр.: 9 назв.

UDK 681.518:658.51

Models and tools for incidents handling in corporative IT-Services automating systems based on configuration management database / V. Y. Sokol, N. V. Tkachuk, M. A. Kuznetsov // Bionics of Intelligence: Sci. Mag. – 2014. – № 1 (82). – P. 74–79.

In this article some approaches to usage of configuration management databases to handle problem situations by users of corporative IT-services are considered. The generalized algorithm and extended data model are proposed, which increase an efficiency to apply this technology.

Fig. 6. Ref.: 9 items.