Міністерство освіти і науки України
НТУ «Дніпровська політехніка»
Ройтлінгенський університет техніки та економіки (Німеччина)
Еслінгенський університет прикладних наук (Німеччина)
Технічний університет Фрайберзька гірнича академія (Німеччина)
Краківська гірничо-металургійна академія (Польща)
Вроцлавський технічний університет (Польща)
Дніпропетровський національний університет імені Олеся Гончара
ДКХ «Дніпровський машинобудівний завод»
Міжнародна науково-промислова корпорація «ВЕСТА»
ДАТ «КБ Дніпровське»

ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ, НАУЦІ ТА ПРОМИСЛОВОСТІ

XIV МІЖНАРОДНА КОНФЕРЕНЦІЯ

м. Дніпро
28 –29 листопада 2019 року

Збірник наукових праць
№ 4

Дніпро
НТУ «ДП»
2020

УДК 622 (06)
П 78

П 78 **Проблеми** використання інформаційних технологій в освіті, науці та промисловості : XIV міжнар. конф. (28–29 листоп. 2019 р.) : зб. наук. пр. / ред. кол.: Г.Г. Півняк та ін.; М-во освіти і науки України, Нац. техн. ун-т "Дніпровська політехніка". – Дніпро : НТУ «ДП», 2020. – № 4. – 115 с.

ISBN 978-966-350-733-0

Подано результати теоретичних та експериментальних досліджень з різних аспектів використання інформаційних технологій в освіті, науці та управлінні промисловістю. У публікаціях розглянуто питання створення та вдосконалення програмних засобів обробки та передачі інформації, математичного моделювання, дистанційної освіти, інформаційної безпеки та телекомунікації.

Для наукових, інженерно-технічних співробітників і студентів, які спеціалізуються в галузі обчислювальної техніки та інформаційних технологій.

УДК 622 (06)

ISBN 978-966-350-733-0

РОЗДІЛ 1

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ОСВІТИ, НАУКИ І УПРАВЛІННЯ ВИРОБНИЦТВОМ

UDC 651.3:518.5

DEVELOPMENT AND RESEARCH OF INFORMATION TECHNOLOGY WHICH ALLOWS ANALYSING PERFORMANCE OF RETAIL ENTERPRISE

V.V. Chashchyn, B.I. Moroz, K. Rodna
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Problem statement. Every business including retail is changing uninterruptedly. Therefore, to guarantee progress and success of this business permanent monitoring is needed. It is possible to do such monitoring by special numeric values called Key Performance Indicators. [1] Moreover, analysis of these values has to be automated.

This problem consists of such sub problems:

- which key performance indicators have to be analyzed;
- which data has to be stored for analysis;
- which format of data storage is the most suitable;
- how to analyze stored data.

For retail enterprises such key performance indicators are applicable [2]: conversion, gain (in monetary and natural units), average check, gain per square meter, quantity of returns, salary capacity. Besides main key performance indicators useful are average number of articles in every check and gain per seller. In addition, money equivalent of gain should store not only in national currency but in foreign too.

To calculate aforementioned indicators next values are needed: amount of checks, number of visitors, paid-up salary and area of the shop. They also have to be stored. Furthermore, developed technology suggests storing information about factors which can affect the key performance indicators. These factors are: assortment, manufacturers, suppliers, markup, prices, discount, availability of articles, advertisements, trainings for sellers, staff, shops, modernizations and loyalties.

In authors' opinion, OLAP-cube is the right data structure for analytical purposes. [3] In this case good solution is to create two cubes. Measures and facts of these cubes are listed in table 1.

Table 1

The structure of the OLAP - cubes

Cube	Measures	Facts
Cube №1	Assortment, markup, prices, discount, article availability, advertisements, trainings for sellers, staff, shops, modernizations, area of the shop, loyalties, date.	Quantity of checks, amount of visitors, conversion, gain (in national and foreign currencies, in natural units), average check, gain per square meter, paid-up salary, salary capacity, average number of articles in each check, gain per seller.
Cube №2	Article, manufacturer, supplier, seller, date.	Gain (in national and foreign currencies, in natural units), number of returns.

Number of returns located in separate cube, because measures needed to analyze it are different. Moreover, the first cube stores total gain all day while the second cube allows detailed analysis of this indicator.

Conclusion. An information technology which allows analyzing performance of retail enterprise was developed according to foregoing thesis. It stores, accumulates and analyzes statistical data of the retail enterprise. To provide advanced analysis the Deductor analytical platform was used. [4]

REFERENCES:

1. The IT-Enterprise official website (2019), "KPI – key performance indicators", available at: https://www.it.ua/knowledge-base/technology-innovation/key-performance-indicators-kpi, (accessed 23.10.2019).

2. The Marketing blog (2013), "6 indicators of retail shop performance", available at: https://www.buslergroup.com/slovar-terminov/6-pokazatelej-effektivnosti-raboty-roznichnogo-magazina.html, (accessed 21.10.2019).

3. Barsegjan, A.A. (2009), *Analiz dannyh i processov* [The analysis of data and processes], 3rd ed, BHV-Petersburg, St. Petersburg, Russia.

4. The Deductor official website (2019), "Deductor – analytical platform for effective business solutions", available at: http://deductor.com.ua/, (accessed 23.10.2019).

5. The national platform of small and medium business (2019), "Mathematics for retail. What indicators an independent shop has to calculate", available at: https://platforma-msb.org/matematyka-dlya-rozdribnoyi-torgivli-abo-yaki-pokaznyky-rahuvaty-nezalezhnij-kramnytsi/, (accessed 21.10.2019).

6. The Bizconsulting website (2017), "The main formula of sales and how it may help your shop to increase profit", available at: https://bizconsulting.com.ua/glavnaya-formula-prodazh/, (accessed 21.10.2019).

УДК 004.415

ПРОЕКТУВАННЯ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ПРОМИСЛОВИХ КОНТРОЛЕРІВ НА БАЗІ ГРАФІВ СТАНІВ

В.В. Ткачов, С.М. Проценко, О.О. Бойко, І.О. Погрібняк
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

В роботі запропоновано формальний підхід до проектування та розробки програмного забезпечення системи керування, що складається з трьох етапів: складання словесного опису алгоритму функціонування технологічного процесу, проектування програмного забезпечення системи керування у вигляді графу станів та розробки програмного забезпечення. Крім того наведено розроблений формальний підхід для переходу від графів станів до програмного забезпечення на мові Ladder Diagram. Отриманий підхід дозволяє виконувати перехід від графів станів до їх програмної реалізації використовуючи лише типові структурні елементи та потребує тільки їх налаштування відповідно до умов та дій дуг переходів.

Ключові слова: система керування, технологічний процес, об'єкт керування, промисловий контролер, проектування програмного забезпечення, розробка програмного забезпечення, автомат Мілі, граф стану, Ladder Diagram

The article proposes a formal approach to the design and development of control system software, which consists of three stages: compiling a verbal description of the process flow algorithm, designing the control system software as a state graph and software development. In addition, a formal approach to the transition from state graphs to Ladder Diagram software is presented. The resulting approach allows the transition from state graphs to their program implementation using conventional structural elements, and requires only adjusting them according to the conditions and actions of the transition arcs.

Keywords: control system, technological process, control object, industrial controller, software design, software development, Mealy machine, state graph, Ladder Diagram

В работе предложено формальный подход к проектированию и разработке программного обеспечения системы управления, состоящий из трех этапов: составление словесного описания алгоритма функционирования технологического процесса, проектирование программного обеспечения системы управления в виде графа состояний и разработки программного обеспечения. Кроме того приведен разработанный формальный подход перехода от графов состояний к программному обеспечению на языке Ladder Diagram. Полученный подход позволяет выполнять переход от графов состояний к их программной реализации, используя обычные структурные элементы, и требует только их настройки в соответствии с условиями и действиями дуг переходов.

Ключевые слова: система управления, технологический процесс, объект управления, промышленный контроллер, проектирования программного

обеспечения, разработка программного обеспечения, автомат Мили, граф состояний, Ladder Diagram

Постановка проблеми. У сучасній промисловості всюди використовуються системи автоматизованого керування технологічними процесами та об'єктами, що забезпечує підвищення якості продукції, зменшення витрат ресурсів, виконання вимог охорони праці в зонах підвищеної небезпеки, за рахунок прибирання людини або значного зменшення її участі в процесах отримання, перетворення, передачі та використання енергії, матеріалів, виробів, інформації. На сьогоднішній день для керування в таких системах використовуються електронно-обчислювальні пристрої, які називаються промисловими контролерами, до яких відносяться: програмовані логічні контролери, розподілені системи керування та промислові комп'ютери [2]. При цьому основною проблемою на сьогоднішній час є відсутність базових та надійних принципів розробки та налагодження програмного забезпечення систем керування. Виробники промислових контролерів пропонують курси та допоміжні матеріали, що описують реалізацію типових операцій всіх рівнів складності, але в цих рішеннях відсутній системний підхід, кожне з них є індивідуальним та потребує суттєвого доопрацювання. В процесі навчання інженери по автоматизації вивчають середовище розробки, особливості реалізації мов програмування та функціональні можливості бібліотек, але питання представлення алгоритмів керування та переходу від них до програмного забезпечення залишається не розглянутими. Таким чином, присутній розрив між чітким та детермінованим підходом до проектування і обранням апаратного забезпечення систем керування на базі промислових контролерів та відсутністю такого при проектуванні та розробці їх програмного забезпечення. З цього випливає, що завдання створення формального підходу до проектування та розробки програмного забезпечення промислових контролерів є актуальним.

Аналіз існуючих матеріалів показав, що на ранніх етапах розвитку автоматизації технологічних процесів перед системами окремо ставилися завдання дискретного та безперервного керування. Завдання дискретного керування вирішувалися з використанням теорії цифрових автоматів на базі релейно контактної логіки [1]. Розвиток напівпровідникової техніки дозволив перейти до реалізації цифрових автоматів за допомогою цифрової схемотехніки, що істотно підвищило надійність функціонування систем за рахунок видалення механічних контактів. При цьому процес модернізації існуючих систем торкався тільки апаратної частини, логічна структура залишалася незмінною. Початок використання в промисловості електронно-обчислювальних машин призвів до переходу від апаратної реалізації цифрових автоматів до програмної. Для спрощення цього процесу була розроблена мова програмування релейних діаграм, яка дозволяє за рахунок простого повторення релейно контактних схем отримувати графічне програмне забезпечення. Подальший розвиток електронно-обчислювальних машин призвів до появи програмованих логічних контролерів, а в подальшому промислових контролерів, однак це не призвело до розвитку проектування та розробки програмного забезпечення систем керування на базі цифрових автоматів.

При автоматизації використовуються два типи цифрових автоматів: комбінаційні та кінцеві. Комбінаційні автомати є логічними ланцюгами, що мають кілька входів та кілька виходів, в яких значення вихідних сигналів в кожен момент часу однозначно визначаються комбінаціями вхідних сигналів в той же момент часу. При проектуванні комбінаційних автоматів розробляється таблиці істинності, на підставі яких синтезуються логічні рівняння, що використовуються для обчислення функцій керування. Кінцеві автомати є математичними моделями, що мають кілька входів та кілька виходів, в яких значення вихідних сигналів, в кожен момент часу визначаються комбінаціями вхідних сигналів та поточним станом. Проектування кінцевих автоматів виконується на підставі таблиць переходів або графів станів.

Основна маса завдань які розв'язуються сучасними системами автоматизації вимагає реалізації алгоритмів керування на основі кінцевих автоматів, у свою чергу комбінаційні автомати здебільшого використовуються для обчислення допоміжних значень або окремих керуючих сигналів. Існують кінцеві автомати двох типів Мілі та Мура. Значення вихідних сигналів автомата Мілі залежать від стану автомата та вхідних сигналів, а автомата Мура лише від його стану. З урахуванням циклічності функціонування програмного забезпечення промислових контролерів, зміна вихідних сигналів в автоматі Мілі виконується одноразово при переході з одного стану в інший, а в автоматі Мура циклічно для поточного стану. Таким чином, в автоматі Мура при описі стану враховуються зміни вихідних сигналів для всіх варіантів переходів в даний стан, що робить реалізацію алгоритму керування непрозорою та істотно ускладнює налагодження та модифікацію програмного забезпечення в порівнянні з автоматом Мілі. Виходячи з цього, при вирішенні завдань керування використання автомата Мілі є переважним.

При розробці програмного забезпечення систем керування доцільним є графічне представлення алгоритмів керування, так як їх проектування, аналіз та експлуатація зрозумілі консультантам (інженерам-технологам), які не є фахівцями в обчислювальній техніці [6]. Крім того розробка програмного забезпечення систем керування не передбачає мінімізацію автоматів, так як це призводить до порушення сприйняття логіки функціонування системи, за рахунок усунення станів та переходів обумовлених технологічним процесом [4]. Виходячи з цього проектування програмного забезпечення на базі кінцевих автоматів необхідно виконувати на базі графів станів.

Дослідження показали, що процес проектування програмного забезпечення системи керування можливо розділити на три етапи: розробка словесного опису алгоритму функціонування технологічного процесу на підставі опису інженера-технолога, виділення станів системи керування та розробка графа станів.

В процесі розробки словесного опису алгоритму виділяються режими функціонування системи керування: ручний, автоматичний, пуск, стоп, аварійний [5]. Для кожного з режимів описуються допустимі технологічні операції та можливості переходів між ними. При описі технологічних операцій вказується їх послідовність, умови включення та виключення виконавчих пристроїв та

контрольовані параметри. До умов відносяться: виконувана технологічна операція, стан блокувань, необхідний стан датчиків та виконавчих пристроїв, необхідна послідовність дій, для включення або виключення пристрою. До контрольованих параметрів належать величини, які використовуються тільки для аналізу функціонування технологічного процесу або об'єкта керування. За результатами розробки алгоритму складаються таблиці вхідних, вихідних та контрольованих параметрів.

На підставі словесного алгоритму функціонування технологічного процесу або об'єкта керування виділяються стани, в яких може перебувати система керування. Спочатку визначаються загальні стани, що відповідають режимам роботи системи керування. Далі для кожного режиму виділяються стани які забезпечують виконання необхідної послідовності технологічних операцій. Стани зазвичай іменуються як SX, де S – скорочення від State (стан), а X – номер стану. Нумерація станів починається з нуля. Важливим є те, що стани та їх описи відносяться до системи керування, а не до технологічного процесу.

Відповідно до алгоритму функціонування технологічного процесу, виділеним станам та таблицям вхідних і вихідних параметрів розробляється граф станів. Спочатку на графі розміщують початковий стан та стани які відповідають режимам роботи системи керування, таким чином, що б між ними було якомога більше вільного простору. Стани позначаються колами, в яких зазначаються їх назви (рис. 1). Пари станів з'єднуються між собою дугами дій які виконуються при переході в новий стан, напрямок переходу між станами задається стрілкою, що розміщується на одному з кінців дуги. Над кожною дугою вказується умова переходу та виконувані дії, що розділяються між собою символом "/". Дії, що виконуються при знаходженні в стані, позначаються дугами дій сталого стану, що виходять та повертаються в цей же стан. Зазвичай такі дуги використовуються для паралельної перевірки значень параметрів та змінних, визначення моменту завершення роботи таймерів або зміни значення лічильників. Таке рішення значно спрощує структуру графа, за рахунок зменшення кількості станів та переходів між ними.

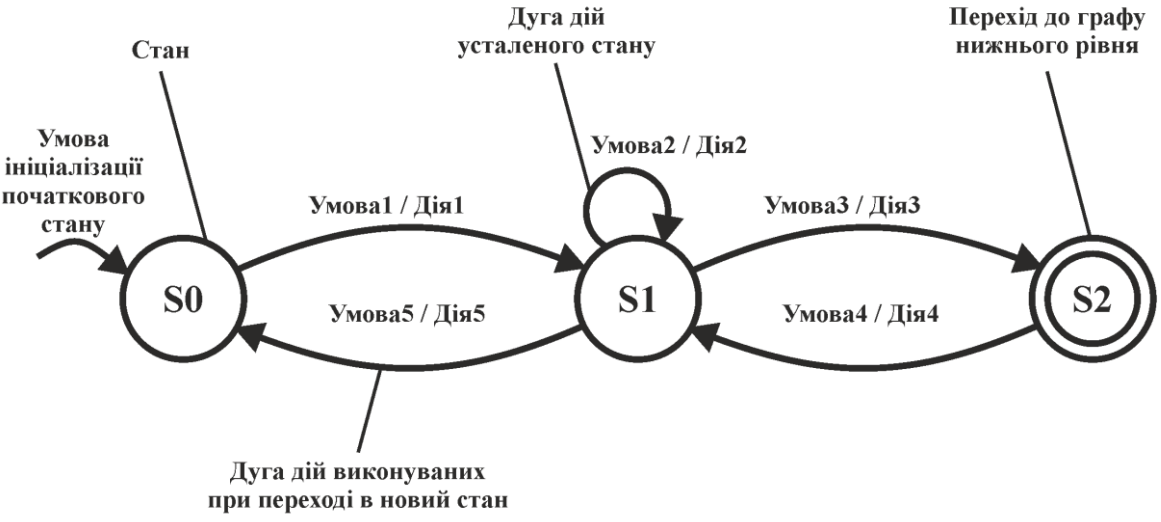


Рис. 1. Приклад графа станів

При проектуванні графів станів для розробки програмного забезпечення під умовами та діями мається на увазі більш широкі поняття, ніж використовувані в теорії цифрових автоматів. Це пов’язано з тим, що програмна реалізація не обмежена виконанням логічних операцій. Таким чином, умови включають перевірку бітових значень, обчислення логічних та математичних виразів, операції порівняння, інші типи операцій, що призводять до отримання логічного результату. У свою чергу дії включають в себе зміни бітових значень, запуск/зупинку таймерів, збільшення та зменшення значень лічильників, обчислення керуючих впливів, зміну налаштувань регуляторів, інші типи операцій.

Після розміщення станів режимів роботи системи керування, додаються стани необхідні для реалізації послідовностей технологічних операцій. З метою спрощення графа станів його незалежні гілки можуть бути винесені в окремі графи. При переході між такими графами функціонування графа верхнього рівня припиняється, до моменту повернення з графа нижнього рівня. Перехід позначається двома колами, в яких вказується назва графа або початковий стан при наявності наскрізної нумерації. Для позначення початкового стану використовується дуга з вільним вихідним кінцем.

Головною вимогою до проектування графів станів є максимально близьке відображення алгоритму функціонування системи керування, так як по ним розробляється програмне забезпечення яке є їх повною програмної копією.

На підставі запропонованого процесу проектування розроблено формальний підхід до у сього процесу розробки програмного забезпечення системи керування, який складається з трьох етапів:

– написання словесного опису алгоритму функціонування технологічного процесу;

– проектування програмного забезпечення, що включає складання таблиць вхідних, вихідних та контрольованих параметрів, виділення станів системи керування та розробку графів станів на основі кінцевого автомата Мілі;

– розробки програмного забезпечення на мові стандарту IEC 61131-3 Ladder Diagram.

Використання мови програмування Ladder Diagram обумовлено тим, що вона забезпечує легкість сприйняття логіки функціонування систем керування, простоту розробки та налагодження програмного забезпечення, швидкий пошук порушення функціонування датчиків та виконавчих пристроїв, що забезпечуються за рахунок її наочності та інтуїтивної зрозумілості для інженерів усіх електричних спеціальностей [3].

Розробка програмного забезпечення на базі графа станів який описується автоматом Мілі в першу чергу вимагає реалізації дуг дій виконуваних при переході в новий стан. Дані дуги описуються умовами переходу в нові стани та діями, виконуваними при переході. Дослідження показали, що найбільш повна реалізація дуги дій виконуваних при переході в новий стан передбачає три етапи: перевірку умови переходу, виконання дій відповідних переходу та завершення

переходу в новий стан. З огляду на особливості розробки на мові програмування Ladder Diagram кожен етап зручно представити у вигляді окремого ланцюга. У першому ланцюгу перевіряється знаходження системи керування в поточному стані та умова переходу в новий стан. Другий ланцюг на підставі поточного стану та нового стану виконує дії відповідні дузі переходу. Третій ланцюг завершує перехід в новий стан. Як видно з описаних функцій ланцюгів для їх реалізації необхідно зберігати поточний та новий стан системи керування.

Стан системи керування можна зберігати у вигляді цілого числа або бітових значень. Реалізація перевірок, установок та скидань бітових значень на мові програмування Ladder Diagram вимагає меншої кількості блоків в порівнянні з використанням цілих значень, крім того використовуючи бітові значення одночасно можна оперувати декількома станами системи керування (поточним та попереднім). Виходячи з цього, для зберігання станів системи керування доцільно використовувати при малій кількості станів окремі бітові змінні, а при великій масив бітових значень, логічного типу даних BOOL.

На підставі обраних рішень розроблена структура першого ланцюга, яка реалізує дугу дій виконуваних при переході в новий стан, в ланцюзі перевіряється знаходження системи керування в поточному стані та умова переходу в новий стан. При виконанні всіх умов встановлюється новий стан, в іншому випадку значення нового стану залишається незмінним (рис. 2). Під умовою переходу тут мається на увазі значення логічного результату виразу умови.

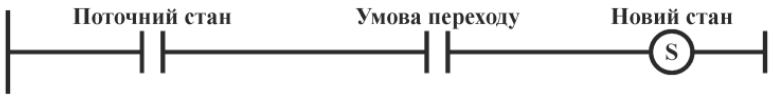


Рис. 2. Ланцюг установки нового стану

Другий ланцюг реалізує дії, що виконуються при зміні стану системи керування, в ньому перевіряється значення поточного та нового станів. При виконанні цієї умови вчиняються дії які відповідають переходу в новий стан (рис. 3).

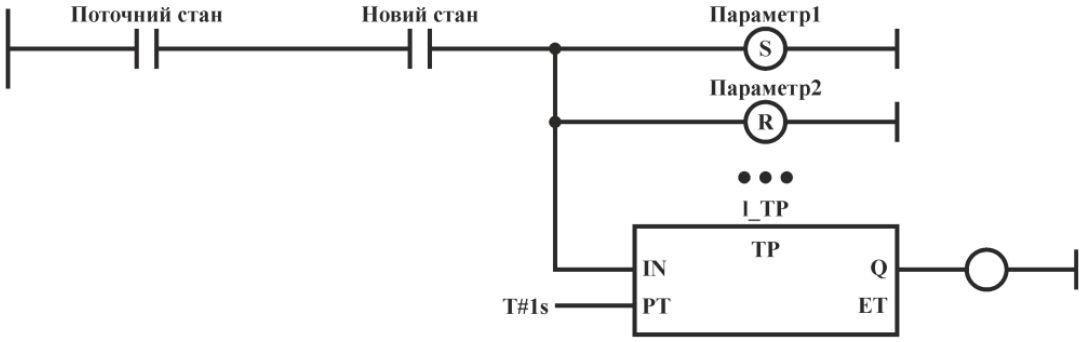


Рис. 3. Ланцюг дій

Третій ланцюг реалізує завершення переходу в новий стан, в ньому перевіряється значення поточного та нового станів. При виконанні цієї умови поточний стан скидається, а відпрацювання дуги дій виконуваних при переході в новий стан завершується (рис. 4).

Рис. 4. Ланцюг скидання поточного стану

При розробці програмного забезпечення яке реалізує граф станів на мові програмування Ladder Diagram основною вимогою є послідовне розміщення ланцюгів. Таким чином, усі три ланцюги, які реалізують одну дугу дій виконуваних при переході в новий стан повинні йти одна за одною зверху вниз. Таке жорстке обмеження пов’язане з тим, що на проміжку виконання програми між ланцюгом установки нового стану та ланцюгом скидання поточного стану активними є два стани. Дана вимога не накладає ніяких обмежень на реалізацію графа станів.

Відповідно до загальної структури реалізації графа станів на мові Ladder Diagram при задоволенні умов декількох дуг дій виконуваних при переході в новий стан, перехід буде виконаний по самій верхній. Таким чином, пріоритет дуги дій можна підвищити за рахунок переміщення її ланцюгів вгору або вниз.

Виходячи з опису функціонування промислових контролерів після перепрограмування ними виконується холодний перезапуску при цьому усі динамічні змінні стають рівними нулю або початковому значенню. Реалізація універсального завдання початкового стану системи керування вимагає створення окремого ланцюга на початку програмної реалізації графу стану. Даний ланцюг виконує перевірку значень всіх станів системи керування і в разі відсутності поточного стану встановлює початковий стан (рис. 5).

Рис. 5. Ланцюг встановлення початкового стану

Реалізація дуги дій сталого стану вимагає додавання окремо ланцюга, в якому виконується перевірка поточного стану та умов дій. Таких ланцюгів може бути декілька, при цьому дії для кожної дуги будуть виконуватися незалежно один від одного (рис. 6).

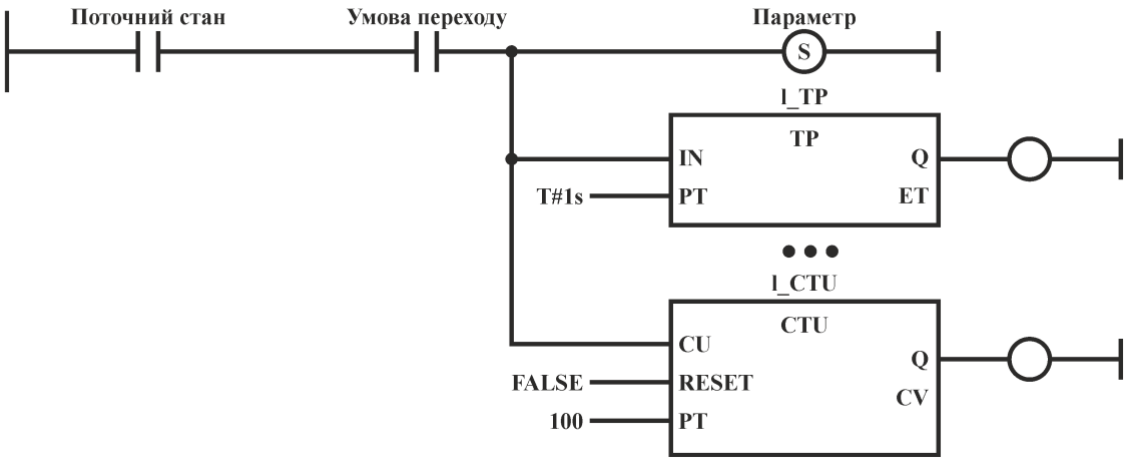


Рис. 6. Ланцюг дій сталого стану

Використовуючи отримані структури ланцюгів розроблено формалізацію переходу від графа станів до програмного забезпечення на мові програмування Ladder Diagram. В рамках даного підходу стан системи керування зберігаються в двійковому масиві, кожній дузі дій виконуваних при переході в новий стан відповідає ланцюг установки нового стану, ланцюг дій та ланцюг скидання поточного стану, кожній дузі дій сталого стану відповідає свій ланцюг який перевіряє знаходження у даному стані та умову переходу, для встановлення початкового стану системи керування використовується відповідний ланцюг який розміщується на початку програмної реалізації графу стану.

Висновки. В роботі проаналізовано сучасний стан питання проектування та розробки програмного забезпечення систем керування на базі промислових контролерів. На підставі чого встановлено, що на даний час відсутній системний підхід до цього питання, у технічній документації та літературі, а так само в навчальних курсах які надаються компаніями виробниками апаратного та програмного забезпечення промислових контролерів розглядаються тільки загальні питання пов’язані з використанням їх середовищ розробки та стандартних бібліотек. Виходячи з цього встановлено актуальність створення формального підходу до розробки програмного забезпечення промислових контролерів.

Аналіз питання розробки систем керування показав, що поява промислових контролерів розмила кордон між системами керування дискретними та безперервними об’єктами, що вимагає використання комплексного підходу до проектування та розробки програмного забезпечення таких систем. Основним способом вирішення даного типу питань є використання алгоритмів керування на базі кінцевих автоматів Мілі у вигляді графів стані.

Запропоновано формальний підхід до проектування та розробки програмного забезпечення системи керування, що складається з трьох етапів: складання словесного опису алгоритму функціонування технологічного процесу, проектування програмного забезпечення системи керування у вигляді графу станів та розробки програмного забезпечення. На підставі проведених досліджень

розроблено формальний підхід для переходу від графів станів до програмного забезпечення на мові Ladder Diagram. Даний підхід дозволяє виконувати перехід від графів станів до їх програмної реалізації використовуючи лише типові структурні елементи та потребує тільки їх налаштування відповідно до умов та дій дуг переходів.

Подальший розвиток дослідження передбачає дослідження складних питань проектування та розробки програмного забезпечення промислових контролерів на базі графів станів з метою їх формалізації. До таких питань відносяться:

– початкова ініціалізація системи керування після теплого перезапуску;

– реалізація ієрархічної структури програмного забезпечення;

– проектування та розробка програмного забезпечення при розпаралелюванні задач;

– проектування та розробка програмного забезпечення з урахуванням високопріоритетних завдань.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Динесенко В.В. Компьютерное управление технологическим процессом, экспериментом, оборудованием / В.В. Динесенко. – М.: Горячая линия-Телеком, 2009. – 608 с.

2. Парр Э. Програмируемые контролеры: руководство для инженера / Э. Парр. – М.: БИНОМ. Лаборатория знаний, 2007. – 516 с.

3. Петров И.В. Программируемые контроллеры. Стандартные языки и инструменты / И.В. Петров. – М.: СОЛОН-Пресс, 2003. – 256 с.

4. Пушкарь М.С. Проектування систем автоматизації: навч. посібник / М.С. Пушкарь, С.М. Проценко. –Д.: Національний гірничий університет,2013.–268 с.

5. Ткачев В.В., Формальные методы разработки программного обеспечения для систем дискретного управления / В.В. Ткачев, С.Н. Проценко, Н.В. Козарь // Гірнича електро-механіка та автоматика: науково технічний збірник. – Дніпропетровськ, 2009. – С. 115-123.

6. Федоров Ю.Н. Справочник инженера по АСУТП: проектирование и разработка. Комплект в двух томах. Том 2 / Ю.Н. Федоров. – М.: Инфра-Инженерия, 2016. – 484 с.

УДК 004.93

РОЗРОБКА МОДУЛЮ ІНФОРМАЦІЙНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ОСОБИСТОСТІ

В.В. Гнатушенко, Д.О. Літвінов, Г.Ю. Станчиць
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Розробка та теоретичне обґрунтування методів та алгоритмів, призначених для розпізнавання цифрових зображень у печатних документах, які отримані при скануванні, при ідентифікації особи.

Встановлення особи людини - одна з найважливіших завдань правоохоронної діяльності. Встановити особу людини в більшості випадків означає визначити його прізвище, ім'я, по батькові, рік народження, місце народження та інші установчі дані. Для встановлення особи розроблені і використовуються безліч методів. Найбільш поширеним є метод встановлення особистості за особистими документами людини, які покликані підтверджувати основні установчі дані людини [1]. Основний документ, що засвідчує особу, в нашій країні - паспорт. Якщо людина демонструє його або при ньому виявлено паспорт (або аналогічний йому документ), то вважається, що ця людина той, чиї дані вказані в паспорті. Для підтвердження цього в паспорт поміщена фотографія, яка дозволяє методом порівняння зовнішності підтвердити або спростувати особу власника паспорта. Таким чином, актуальною є задача зіставлення фотографій людини з самою особою. Для вирішення поставленої задачі необхідно реалізувати модуль, який розпізнає скановані паспортні дані для ідентифікації особи.

Були виявлені наступні вимоги до системи: програма повинна забезпечувати розпізнавання особи і паспортних даних з паспорта; зберігання паспортних даних в зручному форматі; підтримувати побудова звітів за допомогою шаблону; мати інтуїтивно зрозумілий інтерфейс.

Незважаючи на велику різноманітність алгоритмів, можна виділити загальну структуру процесу розпізнавання осіб: локалізація особи на зображенні; вирівнювання зображення особи (геометричне і яркісне); виявлення ознак; розпізнавання - порівняння обчислених ознак з закладеними в базу даних еталонами [2-4].

При аналізі алгоритмів розпізнавання осіб були виявлені наступні способи: метод головних компонент (Principal Component Analysis), метод гнучкого порівняння на графах (Elastic Graph Matching), активні моделі зовнішнього вигляду нейронні мережі.

При використанні систем еластичного порівняння на графах вказується висока ефективність розпізнавання навіть при наявності різних емоційних станів і зміненні ракурсу особи до 15 градусів. Однак розробники посилаються на високу обчислювальну вартість даного підходу. Наприклад, для порівняння вхідного зображення особи з 87 еталонними витрачалося приблизно 25 секунд. Недоліки: висока обчислювальна складність процедури розпізнавання. Низька технологічність при запам'ятовуванні нових еталонів. Лінійна залежність часу роботи від розміру бази даних осіб.

Таким чином, для вирішення поставленого завдання найбільш підходящим представляється метод головних компонент, так як він володіє більш низькою обчислювальною складністю, при цьому забезпечує більш швидке розпізнавання. Недолік у вигляді поганої стійкості до зміни освітлення не є критичним, так як в рамках поставленого завдання необхідно розпізнавати обличчя на зображенні яке скановане.

Висновки. Розроблено модуль інформаційної системи ідентифікації особистості на основі фотографії, яка вклеєна в паспорт, з використанням методу

головних компонент. При проектуванні представлена діаграма варіантів використання, діаграма класів, діаграма компонентів, діаграма бази даних.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Трущенков, И. В. Использование цифровой фотографии в криминалистических экспертизах: дис. ... канд. юрид. наук / И. В. Трущенков. – М., 2011. – 185 с.

2. Гонсалес Р., Вудс Р. Цифровая обработка изображений // Москва.: Техносфера, 2005. – 1072 с.

3. Прэтт У. Цифровая обработка изображений. Кн.1.- М.: Мир, 1982. – 874 с.

4. Гнатушенко Вік. В., Сердюк В.В. Методика розпізнавання напівтонових цифрових зображень тексту// Матеріали ІІ-ої всеукраїнської науково-практичної конференції «Прикладна геометрія та інформаційні технології в моделюванні об'єктів, явищ і процесів» – Миколаїв, 2017. – С. 83-84

УДК 006.015.8

ANALYSIS OF THESES OF THE ISO 27032 FOR THEIR IMPLEMENTATION INTO THE BANKING INFORMATION SYSTEMS

O.V. Lifshyts, S.I. Voitsekh
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Formulation of the problem. Adaptation of international standard recommendations for their implementation in banking information systems to ensure information security in cyberspace.

At present, the use of digital tools for solving various tasks is actively spreading in the world. These processes occur in cyberspace. According to ISO 27032, the term "cybersecurity" is defined as: "the complex environment that results from the interaction of people, software and services on the Internet through technological devices and networks associated with it that does not exist in any physical form.

The primary goal of cybersecurity is to ensure the confidentiality, integrity and accessibility of information in cyberspace. The main purpose of ISO 27032 is to be a guide that will help ensure a much safer interaction with the cyberspace environment.

It should be singled out for international security standards, as it contains recommendations for enhancing cybersecurity, addressing various aspects of the issue and linking cybersecurity to other types of security, including:

- information security;
- network security;
- Internet security;
- protecting the information infrastructure.

The standard discusses basic methods for protecting stakeholder information in cyberspace.

The standard contains:

– cybersecurity review;
– explaining the links between cybersecurity and other security;
– identifying stakeholders and their role in cyberspace;
– Guidelines for addressing major cybersecurity issues;
– Stakeholder engagement methods to address major cybersecurity issues.

Recently, the banking system in Ukraine is developing rapidly. Much attention is paid to remote work with clients using mobile applications, remote communication channels, various self-service methods and more. This is done using the global Internet, so the information that banks transmit and receive in cyberspace should be protected from unauthorized access.

In case, when bank provides cyberspace services to other organizations or clients for personal use, there is a need to develop guidelines that will provide additional explanations or examples necessary to fully understand how international standards should be acted upon.

To ensure cybersecurity at the bank, you need to create your own banking guidelines for all employees. Given the large amount of information circulating in cyberspace, a banking institution will be more profitable for individuals and businesses, as well as current and future partners, if it relies on an international standard in security matters.

Conclusions. There is an urgent need to create internal banking guidelines, based on international standards, which will allow the banking institution to increase the level of cybersecurity and information security, as well as to reduce the level of potential risks.

REFERENCES:

1. Richard Bejtlich. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. - 2013 — 376 с.
2. https://advisera.com/27001academy/blog/2015/08/25/iso-27001-vs-iso-27032-cybersecurity-standard/
3. https://www.iso.org/ru/standard/44375.html

УДК 681.5.011(075.8)

РЕАЛІЗАЦІЯ ЦИФРОВОЇ СИСТЕМИ АВТОМАТИЧНОГО КЕРУВАННЯ БЕЗПЕРЕРВНИМ ОБ'ЄКТОМ, НА ОСНОВІ ФІЗИЧНОЇ МОДЕЛІ ТЕПЛОВОГО ОБ'ЄКТА З ВИКОРИСТАННЯМ SCADA СИСТЕМИ ZENON

Є. К. Воскобойник, О. О. Бойко, Д. В. Славінський, В. В. Загорудько
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

У статті наведена методика поетапної реалізації системи цифрового керування безперервним об'єктом, реалізованої на персональному комп'ютері, що

дозволила максимально наблизити модель до реальної системи керування й виконати ефективне тестування її функціонування в невиробничих умовах.

Ключові слова: ZENON, MATLAB, SCADA, ПЛК, САК, тепловий об'єкт.

E. Voskoboynik, O. Boyko, V. Zagorudko, D. Slavinskyi. The implementation of a digital system for automatic continuous control object, based on a physical model of the object using a thermal scada Zenon system. The article describes a method of phased implementation of digital control system continuous object, realized on the personal computer, that made it possible to maximally draw nearer model the real system for control and to carry out the effective testing of its functioning under the non-production conditions.

Keywords: ZENON, MATLAB, SCADA, PLC, automation, thermal object.

Е. К. Воскобойник, О. А. Бойко, В. В. Загорудько, Д. В. Славинский. Реализация цифровой системы автоматического управления непрерывным объектом, на основе физической модели теплового объекта с использованием scada системы Zenon. В статье приведена методика поэтапной реализации системы цифрового управления непрерывным объектом, реализуемой на персональном компьютере, позволившая максимально приблизить модель к реальной системе управления и выполнить эффективное тестирование ее функционирования в непроизводственных условиях.

Ключевые слова: ZENON, MATLAB, SCADA, ПЛК, САУ, тепловой объект.

Вступ. Процес розробки системи автоматизованого керування тепловим об'єктом розглядається на базі лабораторного стенду для дослідження теплового об'єкта, який є частиною "Навчального центру компанії СВ Альтера при кафедрі Автоматизації та приладобудування Національного ТУ «Дніпровська політехніка». Пристрій стенда приведено на рис. 1.

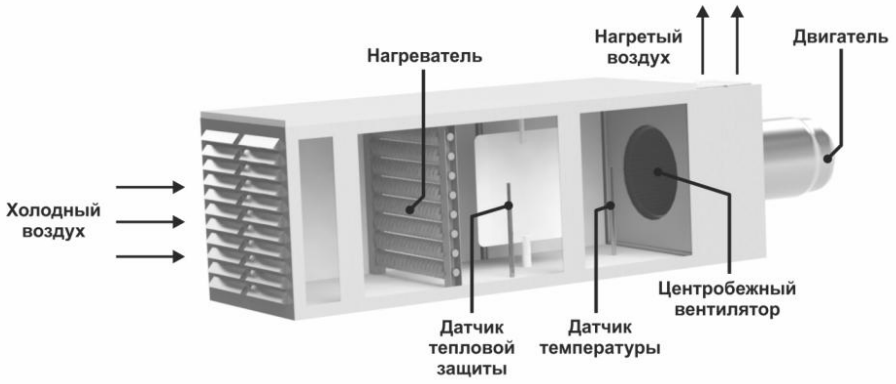


Рис. 1. Пристрій лабораторного стенду для дослідження теплового об'єкта.

Тепловий об'єкт являє собою квадратну трубу перетином 0,16 м2 і довжиною 1 м. У трубі послідовно розташовані нагрівач потужністю 1 кВт, датчик теплового захисту від перегріву нагрівача, що відключає нагрівач при досягненні температури вище 100 ° С, датчик температури з діапазоном вимірювання від 0 до 400 ° С і постійною часу 30 секунд, вентилятор, що обертається асинхронним двигуном зі швидкістю 1400 об / хв при частоті 50 Гц.

Вентилятор забезпечує необхідну витрату повітря для системи. Він керується за допомогою частотного перетворювача. Зміна частоти, що виробляється

перетворювачем призводить до зміни кількості повітря, що проходить через нагрівач. Зміна кількості повітря є збурюючим впливом для контуру управління нагрівача.

Під час роботи теплового об'єкта вентилятор створює розрядження, холодне повітря надходить в трубу, через нагрівач, де відбувається його нагрівання, потім в камеру, де вимірюється температура нагрітого повітря, після чого нагріте повітря викидається в навколишнє середовище. За рахунок великого розміру приміщення, в якому розташований стенд теплового об'єкта вплив нагрітого повітря на навколишнє середовище незначний, тому будемо вважати, що холодне повітря на вході в трубу має постійну температуру.

У системах автоматизованого керування людина бере участь в ухваленні рішень і їх реалізації [1]. Існує три автоматизованих режиму управління:

– ручний режим, при якому комплекс технічних засобів надає оперативному персоналу контрольно-вимірювальну інформацію про стан технологічного об'єкта керування, а вибір і здійснення управляючих впливів виробляє людина-оператор;

– режим "порадника", при якому комплекс технічних засобів виробляє рекомендації з керування, а рішення про їх використання приймається і реалізується оперативним персоналом;

– діалоговий режим, при якому оперативний персонал має можливість коригувати постановку і умови задачі, розв'язувані комплексом технічних засобів системи при виробленні рекомендацій з керування об'єктом.

Мета. У зв'язку з цим метою цієї роботи є розробка системи автоматичного керування, яка повинна забезпечувати:

– доведення температури в камері до заданого значення при заданому діапазоні витрати повітря в системі;

– підтримання температури в камері на заданому рівні при заданому діапазоні витрати повітря в системі;

– візуалізацію і контроль функціонування стенду теплового об'єкта;

– управління швидкістю обертання вентилятори з метою створення збурюючого впливу;

– реєстрацію параметрів процесів в тепловому об'єкт.

Основна частина. Розглянемо створення цифрової системи автоматичного керування об'єктом другого порядку з передавальної функцією:

$$W(p) = \frac{K}{(T_1 p + 1)(T_2 p + 1)},$$

де K - коефіцієнт підсилення;

T_1, T_2 - постійні часу об’єкта керування;

p - оператор Лапласа.

$$p = j\omega,$$

де $j = \sqrt{-1}$; ω - кругова частота.

На першому етапі в безперервній формі синтезований регулятор, який реалізує пропорційно-інтегрально-диференціальний (ПІД) закон керування. Структурна схема системи приведена на рис. 2. Моделювання отриманої системи виконано в математичному пакеті MATLAB [2, 3].

ПІД-регулятор з безперервної форми перетворений в цифрову для чого виконано z - перетворення передавальних функцій його ланок. Структурна схема САК з цифровим регулятором приведена на рис. 3. Система змодельована в математичному пакеті MATLAB і перевірена відповідність її реакцій на набір тестових впливів реакцій моделі системи з безперервним регулятором.

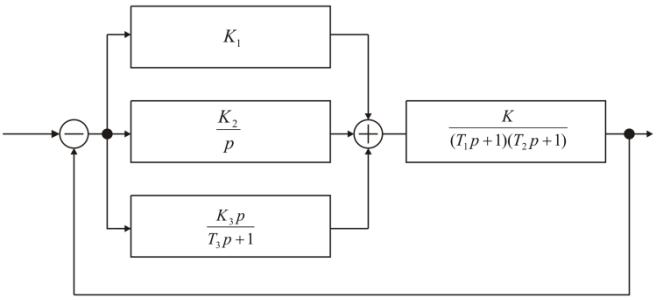


Рис. 2. Структурна схема аналогової САК

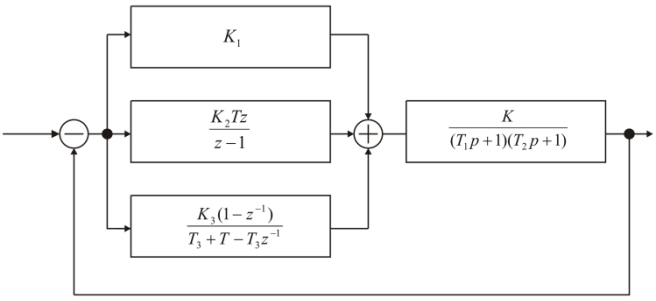


Рис. 3. Структурна схема цифрової САК

На другому етапі на персональному комп'ютері виконана програмна реалізація синтезованого цифрового регулятора. Крім того, виконана програмна реалізація цифрової моделі об'єкта керування, що дозволило отримати програмну реалізацію цифрової системи керування в цілому.

Коректність функціонування розроблених програмних модулів перевірена відповідністю реакцій на набір тестових впливів цифрової моделі системи реакції відповідної моделі в математичному пакеті MATLAB.

На третьому етапі розроблені та реалізовані апаратні елементи системи керування.

Лабораторний стенд може функціонувати в двох режимах автоматизованого керування: ручному і діалоговому. За замовчуванням після подачі електроживлення на стенд, він знаходиться в ручному режимі керувааня рис.4. В цьому режимі завдання значень уставок потужності і частоти виконується за

допомогою потенціометрів. Спостереження за температурою в камері виконується за допомогою блоку індикації.

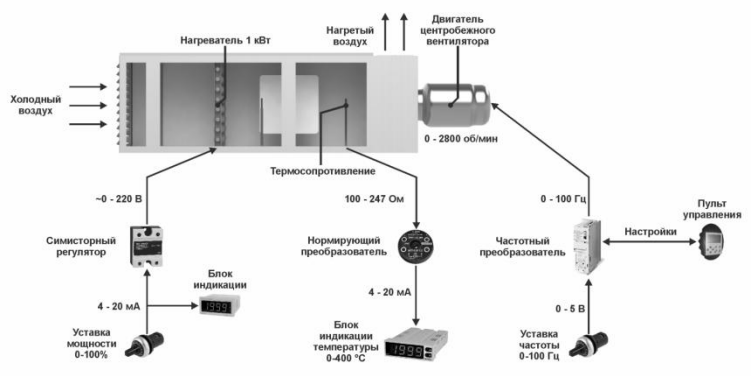


Рис. 4. Структура стенду теплового об'єкта при роботі в ручному режимі

Перемикання в діалоговий режим керування виконується з персонального комп'ютера з програми, розробленої для SCADA системи zenon. Програмований логічний контролер підключає ланцюг завдання уставок потужності і частоти до виходів модуля аналогового вводу / виводу, а до входу модуля - ланцюг вимірювання температури рис. 5.

Розробка системи керування починається з дослідження об'єкта. При цьому знімаються динамічні і статичні характеристики об'єкта, після чого виконується ідентифікація. Дослідження теплового об'єкта виконується в ручному режимі керування.

Для виключення впливу попереднього дослідження необхідно забезпечити початкову температуру в камері відповідну до навколишнього середовища, що досягається продувкою стенду. Продування виконується при вимкненому нагрівачі (потужність нагрівача 0%) і на швидкості обертання вентилятора відповідної швидкості необхідної для наступного дослідження. Продування триває до тих пір поки зміна температури в камері буде більше ніж 0.1 ° С / хв. Отримана температура в камері є початковою температурою при знятті динамічної характеристики.

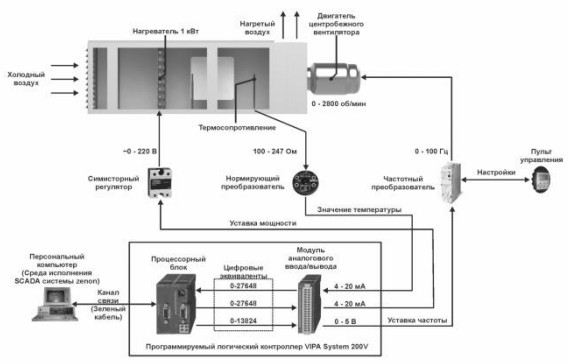


Рис. 5. Структура стенду теплового об'єкта при роботі в діалоговому режимі

Зняття динамічної характеристики проводиться методом ступеневого впливу. Поетапно вплив формується ступінчастою зміною потужності нагрівача від 0 до

100%. Зняття показань приладів проводиться при стабільній швидкості потоку повітря тому, що швидкість потоку впливає на динамічні характеристики. Для теплового об'єкта зняття динамічної характеристики полягає в реєстрації температури в камері через фіксовані інтервали часу.

Значення динамічної характеристики теплового об'єкта зняті при постійній швидкості потоку відповідної частоті 50 Гц наведені в таблиці 1, а сама характеристика на рис. 6.

Таблиця 1

Значення температури динамічної характеристики

Час, сек	0	30	60	90	120	150	180	210	240
Температура, °С	27.6	27.7	28.7	30.4	32.5	34.6	36.5	38.2	39.8
Час, сек	270	300	330	360	390	420	450	480	510
Температура, °С	41.1	42.3	43.2	44.1	44.7	45.3	45.7	46.1	46.4
Час, сек	540	570	600	630	660	690	720	750	780
Температура, °С	46.7	46.9	47.1	47.3	47.6	47.6	47.7	47.7	47.7

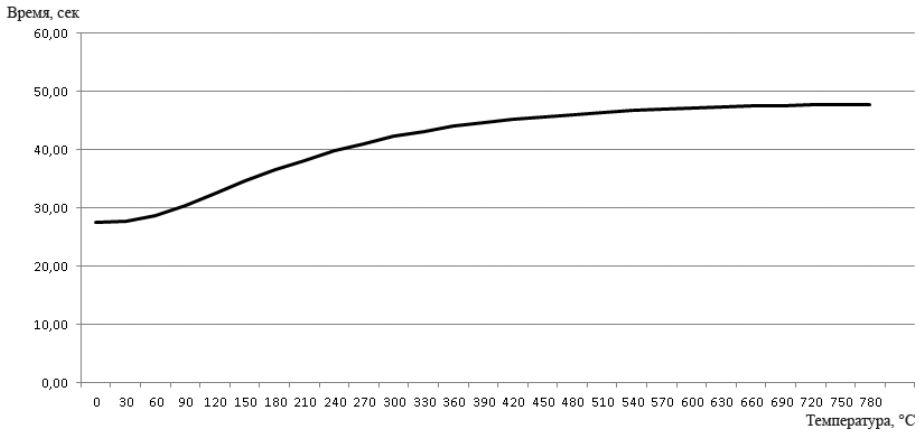


Рис. 6. Динамічна характеристика теплового об’єкта

Розглянемо зняття статичної характеристики на стенді теплового об'єкта. Для побудови статичної характеристики необхідно отримати не менше двох сталих значень, беручи до уваги початкове значення. Уставка потужності нагрівача теплового об'єкта може змінюватися в діапазоні від 0 до 100%, що б підвищити точність зняття статичної характеристики виберемо п'ять значень уставки, для яких буде визначатися усталене значення температури в камері: 20%, 40%, 60%, 80%, 100 %.

Перед початком зняття статичної характеристики необхідно виконати урівноваження температури в камері з температурою навколишнього середовища. Отримана температура в камері є початковою температурою при знятті статичної характеристики.

Далі формується поетапний вплив шляхом установки уставки потужності нагрівача, яка дорівнює 20%. По досягненню температурою в камері сталого

значення, дане значення температури реєструється, після чого формується поетапний вплив шляхом установки уставки потужності нагрівача на рівні 40%. Процес триває до тих пір, поки не будуть отримані всі п'ять значень.

Значення статичної характеристики зняті при постійній швидкості потоку відповідної частоті 50 Гц наведені в таблиці 2, а сама характеристика на рис. 7.

Таблиця 2

Значення температури статичної характеристики

Потужність, %	0	20	40	60	80	100
Температура, °С	28.4	32.28	36.10	40.01	43.89	47.7

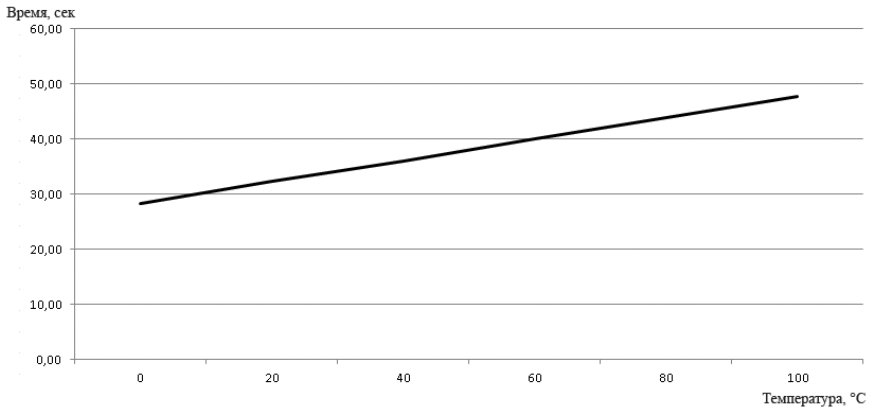


Рис. 7. Статична характеристика теплового об’єкта

На підставі отриманих динамічних і статичних характеристик виконується ідентифікація об'єкта керування, вибирається відповідний тип регулятора, його структура і виконується розрахунок його параметрів. Як регулятор використовуємо пропорційно-інтегрально-диференціальний регулятор.

Після розробки апаратного забезпечення системи автоматизованого керування починається розробка програмного забезпечення. Програмне забезпечення буде складатися з програми програмованого логічного контролера, який реалізує керування тепловим об'єктом і програми візуалізації стану об'єкта керування для SCADA системи zenon.

Основним завданням програмного забезпечення програмованого логічного контролера є реалізація ПІД регулятора призначеного для підтримки температури в камері теплового об'єкта, а також забезпечення доступу до параметрів ПІД регулятора, температури в камері, швидкості обертання вентилятора і потужності нагрівача з SCADA системи zenon.

Спрощена структура взаємодії між SCADA системою zenon і програмованим логічним контролером VIPA System 200V, керуючим стендом теплового об'єкта наведена на рис. 8.

На екрані оператора відображається людино-машинний інтерфейс. Оператор може задавати значення уставки температури, параметри ПІД регулятора, уставку

швидкості обертання вентилятор, а також спостерігати за зміною потужності нагрівача і значення температури в камері.

Середовище виконання SCADA системи zenon обмінюється даними з програмованим логічним контролером VIPA System 200V. На контролер передається уставка температури, параметри ПІД регулятора, уставка швидкості обертання вентилятора. Від контролера виходить значення потужності нагрівача і значення температури в камері.

Програмований логічний контролер на підставі уставки температури, поточного значення температури в камері і параметрів ПІД регулятора визначає відповідне значення керуючого впливу семісторного регулятора, який управляє потужністю нагрівача.

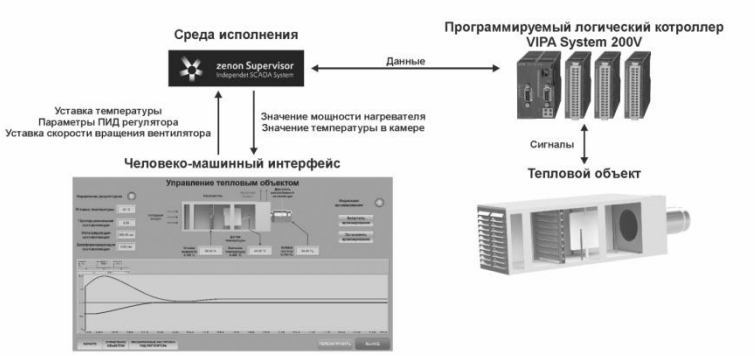


Рис. 8. Спрощена структура взаємодії між SCADA системою zenon.

Після налаштування всіх змінних, виконується розробка людино-машинного інтерфейсу. Розроблений людино-машинний інтерфейс наведено на рис. 9.

Рис. 9. Розроблений людино-машинний інтерфейс

Висновки. Використання даного підходу при розробці системи автоматичного керування безперервним об'єктом на базі теплового об'єкта дозволяє ефективно створювати завершену апаратно-програмну частину цифрових САК з використанням Scada системи Zenon. Це дає можливість істотно скоротити тривалість і вартість пусконалагоджувальних робіт САУ в виробничих умовах на реальному об'єкті управління.

ПЕРЕЛІК ПОСИЛАНЬ:

1. В.А. Втюрин, Основы АСУТП. Учебное пособие для студентов специальности 220301 “Автоматизация технологических процессов и производств” (по отрослям), Санк-Петербург, Санкт-Петербургская государственная лесотехническая академия имени С.М. Кирова, 2006, – с.154.

2. Дьяконов В.П., MATLAB 6.5 SP1/7 + Simulink 5/6. Обработка сигналов и проектирование фильтров. – М.: СОЛОН-Пресс, 2005. – 576 с.

3. Сергиенко А.Б., Цифровая обработка сигналов – СПб.: Питер, 2007. –751 с.

УДК 004.056.5: 004.414.22

ДОСЛІДЖЕННЯ АКТУАЛЬНИХ ВЕКТОРІВ АТАК У ІНТЕРНЕТІ РЕЧЕЙ ТА ОСНОВНИХ МЕХАНІЗМІВ ЗАХИСТУ

Ж.В. Гула, Д.С. Тимофєєв
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Інтернет речей (англ. Internet of Things - IoT) швидко зростає через розповсюдження інформаційно-телекомунікаційних технологій, наявності пристроїв та обчислювальних систем. Безпека IoT викликає занепокоєння для захисту апаратних засобів та мереж системи IoT. Проте, оскільки ідея мережевих приладів все ще відносно нова, безпека при виробництві цих приладів майже не розглядається.

Прикладами існуючих систем IoT є транспортні засоби із самостійним керуванням (англ. self-driving vehicles - SDV) для автоматизованих автомобільних систем, мікросітки для розподілених систем енергоресурсів та Smart City Drones для систем спостереження. Кіберфізичною системою є мікросітка, що пов'язує всі розподілені енергетичні ресурси (англ. distributed energy resources - DER) разом, щоб забезпечити комплексне енергетичне рішення для місцевого географічного регіону. Система мікрорешітки IoT використовує систему диспетчерського управління та збору даних (англ. Supervisory Control and Data Acquisition - SCADA). Інтеграція фізичного та кібер-домену збільшує можливість реалізації атак: кібер-атаки можуть націлювати на контроль SCADA і паралізувати фізичний домен, або фізичні пристрої можуть бути підроблені або скомпрометовані, впливаючи на систему контролю. Наразі ринок безпілотників рухається до впровадження методик автоматизації і може бути інтегрований у боротьбу з пожежами, поліцію, розумне спостереження міста та реагування на надзвичайні ситуації. Оскільки муніципалітети та громадяни почнуть розраховувати на таку систему, стане критично важливим зберегти систему надійною та достовірною.

Останнім часом академічні дослідження з вирішення питань конфіденційності та безпеки систем IoT досягли позитивних зрушень. На сьогодні найпоширеніші методи безпеки, засновані на звичайних методах мережевої безпеки. Проте застосування механізмів захисту в системі IoT є більш складною задачею, ніж у традиційній мережі, через неоднорідність пристроїв та протоколів, а також масштаб і кількість вузлів у системі. Проблеми поліпшення безпеки IoT,

які пов'язані з фізичним зв'язком, неоднорідністю, обмеженням ресурсів, конфіденційністю, великим масштабом, управлінням довірою та непідготовленістю до безпеки, детально пояснюються в [4].

Дослідження [1], [5], [7], оцінюють можливі загрози системам IoT відповідно до рівнів стека протоколів TCP/IP та наявних контрзаходів. Ключовим фактором швидкого прогресу наукових досліджень безпеки IoT є наявність інструменту для моделювання мереж IoT. Вичерпний перелік симуляторів, використовуваних у сучасних дослідженнях, представлений Чернишевим у [5]. Саме завдяки застосуванню симуляції мереж IoT та механізмів безпеки є можливою адекватна оцінка безпеки в IoT та визначення та вивчення основних векторів атак.

Проблеми безпеки IoT актуальні на всіх основних рівнях стека протоколів TCP/IP. Наприклад, відсутність «транспортного» шифрування стосується незахищеного зв’язку між пристроєм та Хмарним сховищем, пристроєм та шлюзом, пристроєм та мобільними додатками, одним пристроєм та іншим пристроєм.

Популярний вектор для отримання доступу до пристроїв IoT виникає через неадекватні процедури автентифікації та авторизації. У нинішніх системах IoT протоколами, що підтримують автентифікацію, є MQTT, DDS, Zigbee та Zwave. Проте, навіть якщо розробник надав інструменти автентифікації, необхідні для спілкування в Інтернеті, можливості для викрадення зв'язку все одно існують. Небезпечні мережеві сервіси можуть спричинити загрозу розвідування мережі та поширюватись через неї.

Недостатня конфігурація безпеки пояснюється вбудованними повноваженнями, які часто використовуються на пристроях IoT. Завдяки цьому облікові дані легко піддаються компроментуванню через використання одного і того ж пароля на багатьох пристроях. Погана фізична безпека - ще один вектор атаки, викликаний вразливістю апаратних засобів. Основна перешкода в шифруванні пристроїв пояснюється простотою датчиків.

Небезпечні веб- та хмарні інтерфейси - це вразливості, які можуть бути вектором атаки в системі IoT на програмному рівні. Тому, хмарні шлюзи повинні бути обладнані механізмами безпеки, щоб обмежити можливість несанкціонованих користувачів (порушників) від зміни конфігурацій. Застосування біометрії та багаторівневої автентифікації для контролю доступу є одним з найкращих механізмів захисту на програмному рівні. Через зміни тенденцій загроз безпеці [7] запропонував розгляд поточних проблем безпеки відповідно до рівня та можливих контрзаходів. Деякі поточні проблеми та запропоновані контрзаходи розглянуті у [1].

Розробка діючих механізмів безпеки IoT на разі перебуває у постійному розвитку. Основними механізмами захисту є:

– Автентифікація - процес ідентифікації користувачів та пристроїв у мережі та надання доступу уповноваженим особам. Це один із способів пом’якшення атак на системи IoT (атака «Людина в середині», атака Sybil). Автентифікація на даний час залишається найпопулярнішим методом надання доступу користувачеві на рівні додатків, а також надання доступу до пристрою в мережі IoT.

– Шифрування. Досягаючи цільової безпеки, вузли шифруються. Оскільки метою шифрування IoT є досягнення ефективної взаємодії з низьким споживанням енергії, симетричні та асиметричні алгоритми для IoT розроблені таким чином, щоб відповідати вимогам [6].

– Довірче управління. Мета управління довірою IoT - виявити та усунути шкідливі вузли та забезпечити безпечний контроль доступу. Автоматизовані та динамічні обчислення довіри для перевірки довірчих значень вузлів-учасників мережі IoT є найсучаснішими у дослідженні управління довірою. Проте, на сьогодні більшість досліджень зосереджена саме на виявленні шкідливих вузлів.

– Безпечна маршрутизація. Масштабованість, автономність та енергоефективність є важливими для будь-якого рішення маршрутизації. Завдяки великому масштабу мереж IoT, IP-адреси цих пристроїв базуються на IPv6 (англ. Internet Protocol version 6), що дозволяє забезпечити більш надійну та покращену модель маршрутизації пакетів.

– Нові технології. Існують два базових типи нових технологій. Програмно визначена мережа (англ. software defined network – SDN) та блокчейн (англ. blockchain) є одними з найпопулярніших нових технологій, що поєднуються з вирішеннями безпеки IoT. Основна ідея SDN - розділити мережевий контроль та управління даними (можливе як централізоване управління, так і динамічне управління мережею для вирішення проблем в середовищі IoT, таких як, наприклад, розподіл ресурсів в пристроях IoT). Блокчейн є основою криптовалюти. Програми на базі IoT користуються захищеними та приватними транзакціями, а також децентралізацією комунікацій та процесів. Застосування блокчейну досягло значних успіхів у фінансових додатках.

Результатом цієї роботи є огляд сучасних тенденцій дослідження безпеки IoT. Різні інформаційні джерела з питань захисту IoT було переглянуто з метою визначення основних векторів атак та проблем безпеки IoT. Було встановлено основні механізми захисту безпеки IoT, їх підґрунтя та особливості функціонування. Мета цієї роботи була досягнута шляхом надання адекватного огляду тенденцій дослідження в галузі безпеки IoT за період останніх років.

ПЕРЕЛІК ПОСИЛАНЬ:

1. А. Теварі, Б. Б. Гупта. Безпека, конфіденційність та довіра різних рівнів в рамках Інтернету речей (IoT) // Наступ. Генер. Обчислення. Сист. – 2018 1–13 с.

2. Дж. Камінья, А. Перкусич, М. Перкусич. Інтелектуальний метод управління довірою для виявлення атак, що підключаються в Інтернеті речей // Секур. Комун. Мереж. – 2018.

3. Ж.А. Гутьєррес, С. Кумар. SecTrust - RPL: безпечний протокол маршрутизації RPL для Інтернету речей, комп'ютерних систем майбутнього покоління.

4. К. Ша, У. Вей, Т. Ендрю Янг, З. Ванг, У. Ши. Про проблеми безпеки та відкриті проблеми в Інтернеті речей // Наступ. Генер. Обчислення. Сист. – 2018 – №83.

5. М. Чернишев, З. Байг, О. Белло, С. Зеадалі. Інтернет речей (IoT): Дослідження // IEEE Інтернет речей, журнал – 2018 – №5. 1637–1647.
6. С. Сінгх. Розширені легкі алгоритми шифрування пристроїв IoT: опитування, виклики та рішення // Інтел. Гуманіз. Обчислення – 2017.
7. Х.З. Ячень Ян, Лонгфей Ву, Гуйчен Інь, Ліє Лі. Огляд з питань безпеки та конфіденційності в Інтернеті речей // Інт. Конф. Інтернет Технол. Зах. – 2015. – 202–207 с.

УДК 004.056.53

КЛАСИФІКАЦІЯ ВИДІВ АВТЕНТИФІКАЦІЇ

К.О. Діденко, Ю.А. Мілінчук
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Атаки на системи автентифікації, на жаль, не рідкісне явище в наш час і багато статей присвячені різноманітним методам, видам та способам автентифікації. Для легшого розуміння кожного з видів, потрібно знати, які методи та способи можна використовувати і які типи протоколів при цьому застосовуються.

Саме автентифікація являє собою процедуру перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту. [1] Ця процедура може виконуватись за допомогою наступних методів:

– парольні, в яких може використовуватись одноразові або багаторазові паролі;

– Public Key Infrastructure (PKI), заснований на асиметричній криптографії, де закритий ключ користувача може бути на смарт карті, криптографічному токені або знімному накопичувачі;

– мобільна автентифікація, де, за допомогою спеціальної програми, на смартфоні генерується одноразовий пароль (one time password, OTP). Таким чином, смартфон виступає OTP токеном; [2]

– біометричні, де перевірка проходить за фізіологічними характеристиками користувача;

– інформація користувача, до якої відноситься номер телефону, дівоче прізвище матері, дата реєстрації та інше, що може використовуватись для відновлення логіна і пароля або для двофакторної автентифікації;

– користувацькі дані, де використовуються інформація про точки доступу бездротового зв'язку та геодані про місце знаходження користувача. [3]

Способи можна класифікувати наступним чином [4]:

– базова автентифікація, при застосуванні якої логін і пароль користувача входять до складу веб-запиту. Будь-який зловмисник, що перехоплює пакети інформації легко впізнає засекречені дані;

– дайджест-автентифікація. Вид автентифікації, який має на увазі передачу призначених для користувача паролів в хешованому стані. Постійне

оновлення хешу не дає зловмиснику можливості розшифрувати пакет даних - кожне нове підключення утворює інше значення пароля;

– HTTPS дає можливість шифрування не тільки логіна і пароля користувача, але і всіх інших даних, що передаються між інтернет-клієнтом і сервером;

– автентифікація з пред'явленням цифрового сертифікату, що має на увазі використання протоколів із запитом і відповіддю на нього;

– автентифікація з використанням Cookies. Браузер, при кожній спробі підключення до ресурсу, посилає Cookies як одну із складових частин HTTP-запиту;

– децентралізована автентифікація, за принципом якої працюють такі протоколи, як OpenID, OpenAuth та OAuth.

В залежності від кількості методів, що використовуються, автентифікація поділяється на однофакторну та багатофакторну, де використовується декілька методів.

Залежно від можливостей засобів автентифікації і рівня інформаційної безпеки, можна виділити наступні види автентифікації:

– статична автентифікація. Захищає від несанкціонованого доступу зловмисників, які можуть заволодіти даними про ідентифікатор користувача під час його роботи з інформаційним ресурсом або сайтом. Найпоширенішим методом, що забезпечує даний вид, є використання багаторазових паролів;

– стійка, механізм якої заснований на використанні динамічних ідентифікаторів, які змінюються перед кожним сеансом. Даний вид не захищає від активний атак;

– постійна, що захищає суб'єкта від несанкціонованої крадіжки і модифікації його ідентифікатора на будь-якому етапі роботи з інформацією. Цей вид забезпечує захист від атак навіть після автентифікації.

В залежності від політики безпеки систем та рівня довіри існує:

– одностороння автентифікація. Користувач доводить право доступу до ресурсу його власнику;

– взаємна. Перевіряється автентичність прав доступу і користувача і власника. Для цього використовують криптографічні способи. [5]

Також, слід розуміти, що автентифікація представляє собою процес порівняння інформації, наданої користувачем, з тією, що знає система. І залежно від типу інформації, її можна віднести до одного з наступних факторів [6]:

– фактор знання – щось, що користувач знає. Це може бути пароль або відповідь на секретне питання;

– речовий фактор – щось, чим користувач володіє. Це можуть бути смарт-картки, токени та інше;

– біофактор – щось, що є частиною користувача. Біометричні сканери розпізнають відбитки пальців, геометрію руки, почерк, голос користувача.

Тож, поєднавши наведену вище інформацію, можна скласти таблицю класифікації видів автентифікації.

Таблиця 1

Класифікація видів автентифікації

Метод	Фактор	Тип інформації	Вид
парольний	знання	багаторазовий пароль	статична
інформація користувача	знання	інформація, що знає тільки користувач	статична
парольний	знання	одноразовий пароль	стійка
мобільна автентифікація	речовий	одноразовий пароль, що генерується на смартфоні, який виступає OTP токеном	стійка
користувацькі дані	знання	геодані, інформація про точки доступу бездротової мережі	стійка
біометричний	біофактор	фізіологічні характеристики	стійка
PKI	речовий	ключ в смарт-карті, токені, знімному накопичувачі	стійка

Потрібно зауважити, що:

– залежно від виду автентифікації, дані методи можна реалізувати різними способами, описаними вище;

– до постійної автентифікації, з найбільш високим рівнем інформаційної безпеки, можна віднести багатофакторну автентифікацію, з використанням декількох методів;

– найбільш оптимальним варіантом можна вважати двофакторну автентифікацію з використанням статичного та стійкого видів, наприклад багаторазового та одноразового паролів, або багаторазового паролю та біометричного методу.

Висновки. Таким чином, запропонована класифікація може допомогти визначити вид автентифікації за методами, факторами та необхідною для автентифікації інформацією, та обрати необхідні методи багатофакторної автентифікації для забезпечення оптимального рівня інформаційної безпеки. Також, дану класифікацію можна використовувати для подальших досліджень, пов’язаних з процедурою автентифікації.

ПЕРЕЛІК ПОСИЛАНЬ:

1. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу».

2. Методы аутентификации [Електронний ресурс]. – Режим доступу: https://powersecurity.org/ru/blog/authentication-methods/

3. Что такое Аутентификация – Значение [Електронний ресурс]. – Режим доступу: https://sendpulse.ua/support/glossary/authentication

4. Что такое аутентификация [Електронний ресурс]. – Режим доступу: https://www.unisender.com/ru/support/about/glossary/chto-takoe-email-autentifikaciya/

5. Аутентификация [Електронний ресурс]. – Режим доступу: https://promopult.ru/library/Аутентификация

6. Классификация механизмов аутентификации пользователей и их обзор [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/177551/

УДК 004.94

ПРОЕКТУВАННЯ ТА ОПТИМІЗАЦІЯ КОМП'ЮТЕРНОЇ МОДЕЛІ ШТАМПОВИХ ПЛИТ

І.С. Дмитрієва, О.А. Зеленський, Г.Ю. Станчиц
(Україна, Дніпро, Національна металургійна академія України)

Актуальність роботи. В наші дні штампування - це один з прогресивних способів для отримання виробів. Показники економіки операцій штампування визначаються, в більшій мірі, вартістю самого штампового остраху, що припадає на одиницю виробу. У свою чергу вартість самого штампа складається з безлічі факторів: самої конструкції і її технологічності, геометрично-конструктивних параметрів, а також матеріалу, з якого виготовлений, власне, сам штамп. Одним з важливих показників якості штампа є його стійкість, від якої потерпають на кінцевій вартості оснащення, тому, для підвищення рентабельності обладнання, необхідно звернути увагу на цей показник. У процесі підготовки виробництва нових виробів трудомісткість проектування може становити до 50%. Скоротити цей відсоток допомагають САПР. Щоб мінімізувати всі витрати на етапі конструювання вже закладається вибір найбільш раціональної конструкції деталі, зокрема і штампових плит.

Геометрична оптимізація в середовищі чисельного моделювання. Системи автоматизованого проектування (САПР) міцно увійшли в промисловість, так як завдяки їм створення процесів, проектування оснащення помітно прискорюється, дозволяючи спроектувати модель об'єкта і його поведінку в середовищі чисельного моделювання, ще задовго до того, як це буде матеріалізовано.

Алгоритм роботи в системах САПР за умови, що використовується інженерний аналіз починається з параметризації, здійснення якої відбувається в середовищі CAD системи шляхом завдання певних параметрів, що визначають геометрію сплайнів, що надалі сформує геометрію конструкції. Далі проводиться експорт моделі з CAD в CAE, де відбувається етап створення сітки кінцевих елементів для моделі, рішення задач механіки, що включають обчислення цільового функціоналу і обмежень.

Це означає, що будь-яка зміна геометрії моделі CAD системі, спричиняє за собою перерахунок в системі CAE, так як доводиться знову перебудовувати звичайно елементну сітку, складати схему навантажень, задавати обмеження. Так відбувається по циклічній схемі поки конструктор не доб'ється потрібного йому результату. На практиці на створення і перевірку кінцево-елементної сітки йде помітна частина часу, як і на створення схеми навантаження.

Підготовчим етапом перед процесом геометричній оптимізації є робота в середовищі CAD для безпосереднього проектування штампового плити.

Таким чином нами була розглянута методика побудови штампового плити, але проводити CAE аналіз ми будемо на прикладі штампової плити з великою кількістю кишень

Після чого у вкладці «Поставити мету» в якості типу цільової функції вкажемо «Вага» і виберемо в якості його параметра пункт «Мінімізувати», так як наша цільова функція (вага) повинна прагнути до мінімуму.

Для того щоб оптімайзер міг вибрати змінні, які потрібні для розрахунку, зазначимо йому посилання на виконаний раніше розрахунок. У такому випадку при вирішенні оптімайзер буде здійснювати розрахунки виходячи з уже наявного рішення, тим самим скоротивши час розрахунку можливість допущення помилки.

Як завершеного результату буде створений файл формату «excel», в якому будуть відображені результати рішення. У таблиці відображено кількість отриманих рішень, власне, сам результат цільової функції і значення параметрів, які відповідаю певного рішення.

Результатом геометричній оптимізації буде вже готова параметрезованих математична модель штампового плити. Щоб оцінити параметризацію проведемо порівняння штампова плит. Для цього на панелі інструментів у вкладці «Аналіз» виберемо опцію «Додатково» і в списку, що випадає знайдемо функцію «Вимірювання тел». Після чого в діалоговому вікні вибрати тіло, яке необхідно виміряти, і вибрати необхідну фізичну величину

Висновок. В результаті виконання даної роботи:

1. Було проведено аналіз типових штампова конструкцій в цілому і проаналізовано значимість штампового плити. Була встановлена залежність конструкції штампового плити від певних технологічних параметрів.

2. Був проведений аналіз методу планованого експерименту. Були дані основні визначення і була встановлена залежність цільової функції від параметрів оптимізації.

3. Було розглянуто питання конструкції штампова плит з застосуванням методу планованого експерименту. Була встановлена цільова функція експерименту та визначено основні фактори, що впливають на конструкцію плити. Встановлено зв'язок між ними.

4. Була спроектована модель штампового плити в CAD системі, проведена геометрична оптимізація в системі CAE.

5. Здійснено аналіз конструкції штампового плити, отриманої після оптимізації.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Юсипов, З.И. Обработка металлов давлением и конструкция штампов: Учебник для машиностроительных техникумов. 2-е изд., перераб. / З.И. Юсипов, Ю.И. Каплин. – М.: Машиностроение, Москва, 1981. – 272 с.

2. Любченко, Е.А., Чуднова, О.А. Планирование и организация эксперимента: учебное пособие. Часть 1 / Е.А Любченко, О.А. Чуднова. – Владивосток: Изд-во ТГЭУ, 2010. – 156 с.

3. Ma, Y., Koˇseck´a, J., and Sastry, S. Optimization Criteria and Geometric Algorithms for Motion and Structure Estimation / Y. Ma, J. Koˇseck´a, and S. Sastry // International Journal of Computer Vision – 2001. – Vol. 44, № 3. Pp. 219–249.

УДК 651.3:518.5

АВТОМАТИЗАЦІЯ ПРОЦЕСУ ВСТАНОВЛЕННЯ МЕДИЧНОГО ДІАГНОЗУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ DATA MINING

І.А. Левдик, Л.В. Кабак, П.О. Іщук
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

На сьогоднішній час все більш актуальною стає технологія Data Mining (технологія глибинного аналізу), що являє собою інтелектуальну обробку, напівавтоматичний аналіз великих об'ємів даних з метою пошуку корисних фактів; Data Mining використовує методи машинного навчання, математичної статистики та теорії баз даних. Вищезгадана технологія є частиною великої сукупності інструментів, підходів та методів обробки структурованих та неструктурованих даних, що носить назву Big Data.

Фундаментально Data Mining базується на трьох поняттях: математична статистика, штучний інтелект, машинне навчання.

Загалом, технологія є дуже популярною в різноманітних бізнес-сферах: сфері роздрібної торгівлі - покращення якості реклами, розробка стратегії створення запасів товарів, дослідження часових шаблонів, створення прогнозуючих моделей; банківської справи - виявлення шахрайських злодіянь, сегментація клієнтів, прогнозування зміни клієнтури; телекомунікації - виявлення лояльності клієнтів; страхування - виявлення шахрайства, аналіз ризику; а також в інших спеціальних сферах, як-то медицина, молекулярна генетика та генна інженерія, прикладна хімія.[2]

На теперешній момент глибинний аналіз даних був імплементований в широку множину проектів. Наприклад, в лідуючій консалтінговій компанії "Argonauten360°" технологією Data Mining було підкріплено низку аналітичних процесів, що відбувалися в межах роботи організації. Звичайно, що це лише один приклад з багатьох, оскільки актуальність технології набирає обертів.

Зокрема, заслуговує уваги медична сфера застосування технології, а саме: вставновлення медичних діагнозів. Вони побудовані, головним чином, на основі правил, що описують поєднання окремих симптомів різних захворювань. За допомогою таких правил дізнаються не тільки, на що хворий пацієнт, але і як потрібно його лікувати. Правила допомагають обирати засоби медикаментозного впливу, визначати показання - протипоказання, орієнтуватися в лікувальних процедурах, створювати умови найбільш ефективного лікування, прогнозувати результати призначеного курсу лікування і т. д. Технології Data Mining дозволяють виявляти в медичних даних шаблони, що становлять основу зазначених правил. [1,4]

Пропонується створити програмний додаток, що реалізував би вищеописані функції за допомогою технології глибинного аналізу. Для цього визначається набір методів аналізу Data Mining, які використовуватимуться в програмному

продукті, а також вказується набір алгоритмів, які будуть використовуватися надалі.

Якщо розглянути методи, що відносяться до Data Mining, то можна виділити ряд тих, що будуть актуальними для вирішення наданої задачі:

1. Дерево рішень.
2. Метод асоціативних правил.
3. Нейронні мережі.
4. Лінійна регресія.

Вищевказані методи дозволять, по-перше, раціонально зберігати дані, відносячи їх до класів, по-друге, будуть слугувати інструментами для встановлення залежностей між симптомами та діагнозом.[1,3]

На рисунку 1 відображена контекстна діаграма встановлення діагнозу, яка описує процес в цілому.

Рис. 1. Контекстна діаграма встановлення діагнозу

На рисунку 2 відображена діаграмма декомпозиції процесу зображеного на рисунку 1, для більшої деталізації та чіткості. Для реалізації процесу встановлення діагнозу виконуються наступні функції:

– Пошук пацієнта в БД – задіяні засоби СУБД для пошуку конкретної людини та історії захворювань, пов’язаної з людиною.

– Перегляд пов’язаних історій захворювань – задіяні засоби СУБД та, власне, Data Mining; відбувається перебір та глибинний аналіз інформації.

– Встановлення діагнозу – задіяні засоби Data Mining, відбувається зважування результатів попереднього процессу та видача остаточного результату.

–

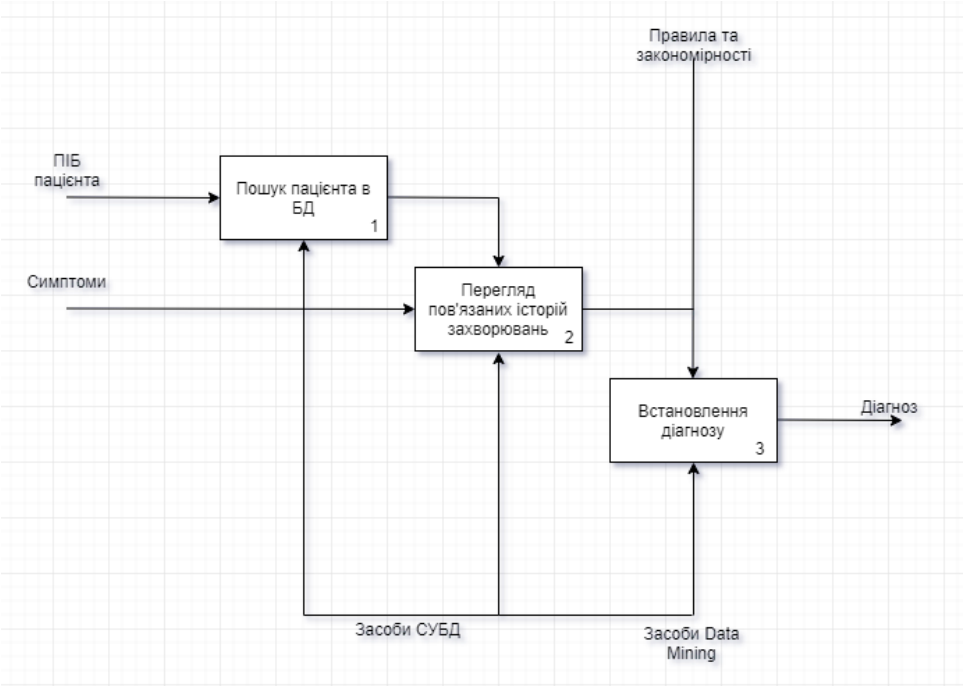


Рис. 2. Декомпозиція A0 процесу встановлення діагнозу

За допомогою технології Oracle Data Mining будуємо модель обёєктів експертної системи і отримуємо модель, зображену на рис. 3.

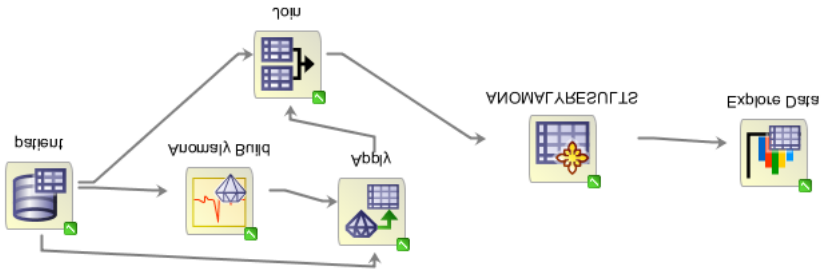


Рис. 3. Модель даних системи аналізу даних

Приклад роботи системи, що відображає кількість звернень пацієнтів до лікарні в залежності від віку.

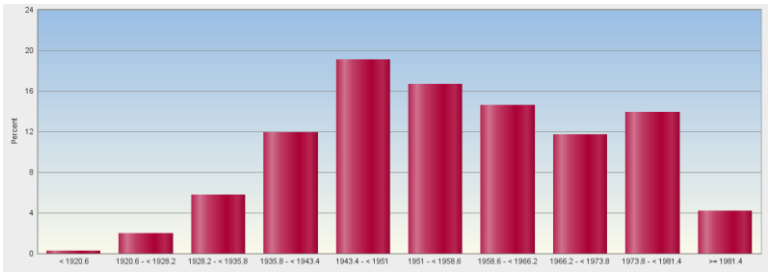


Рис. 4. Кількість звернень пацієнтів до лікарні, залежно від віку

Висновки: таким чином, пропонується створити програмне забезпечення, що забезпечувало би полегшення виконавчих процесів в медичній сфері.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Top 33 Data Mining software [Electronic resource] – Access mode: https://www.predictiveanalyticstoday.com/top-data-mining-software/
2. 50 top free data mining software [Electronic resource] - Access mode: https://www.predictiveanalyticstoday.com/top-free-data-mining-software/#
3. Brendan Tierney Predictive Analytics Using Oracle Data Miner: Develop & Use Data Mining Models in Oracle Data Miner, SQL & PL/SQL: - Oracle Press, 2014. – 429 - ISBN: 978-0-07-182175-9
4. Oracle Advanced Analytics Customer Success Stories [Electronic resource] – Access mode: https://www.oracle.com/technetwork/database/options/advanced-analytics/odm/odm-customers-086483.html

УДК 004.048

СХОВИЩА ДАНИХ СИСТЕМИ ПІДТРИМКИ ПРИЙНЯТТЯ РІШЕНЬ ІДЕНТИФІКАЦІЇ КУЛЬТУРНИХ ЦІННОСТЕЙ

А.А. Мартиненко, Б.І. Мороз, І.Г. Гуліна
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Дослідження та розробка методів і моделей організації та обробки даних і знань в інтелектуальній системі підтримки прийняття рішень ідентифікації культурних цінностей є важливою та актуальною задачею [1].

Проведення ідентифікації культурних цінностей, як один з етапів експертизи – складна справа, що не піддається чітко зафіксованому формальному опису, а часто має евристичний характер і залежить від професійного рівня та професійної інтуїції експерта. Важливим напрямком розвитку інформаційних технологій є розробка систем, призначених для підтримки процесів прийняття рішення.

Конкретне застосування даних систем актуально під час вирішення широкого кола завдань, пов’язаних із творами мистецтва. Велику практичну допомогу у вирішенні цієї проблеми надало б створення інтелектуальна система підтримки прийняття рішень, яка б містила в собі не тільки базу даних з відмітною атрибутикою предметів мистецтва, але й могла б робити висновки про ступінь культурної й історичної цінності досліджуваного об’єкта.[3]

В процесі ідентифікації культурних цінностей користувач інтелектуальної системи підтримки прийняття рішень через відповідний інтерфейс (блок формування запитів та відповідей) звертається до баз даних, де і знаходиться опис відповідного об’єкту (рис. 1). Таким чином, від якості інформації баз даних напряму залежить і якість відповідного звіту/відповіді.

Рис.1 Загальна схема роботи з інтелектуальною системою підтримки прийняття рішень ідентифікації культурних цінностей

Будь-який процес прийняття рішення здійснюється в декілька основних етапів:

– постановки задачі;
– формування рішень;
– вибору рішення.

Процес прийняття рішення складається з таких кроків:

– визначення цілей, критеріїв оптимальності;
– формування множини допустимих альтернатив;
– вибір методів розв’язання задачі;
– порівняння та упорядкування множини альтернатив за обраними критеріями;
– добір кращих варіантів за критерієм оптимальності та вибір рішення.

Необхідно зазначити, що будь-яке рішення, має сенс лише тоді, коли воно ефективне.

Виділяють два основних фактори, що впливають на ефективність рішень: фактор якості рішення Q та фактор прийняття рішення людиною A. Ефективність рішення E може бути виражена формулою:

$$E = Q \times A$$

За умов, що один із зазначених факторів прямує до мінімуму, ефективність рішення падає. Фактор якості рішення Q пов’язаний із вибором кращої альтернативи з тих, що зумовлює проблемна ситуація з урахуванням умов прийняття рішень та можливостей виконавців рішення.

Підвищення ефективності рішення головним чином слід спрямовувати на покращення фактору якості, а саме на вірний добір обмежень і критеріїв рішення, правильне формування множини допустимих альтернатив та на коректний вибір найкращого для умов задачі варіанту.

Отже, для підвищення ефективності роботи системи в цілому, на думку авторів, слід підвищити якість даних, та помістити їх у відповідне сховище, при цьому доопрацювати схему інтелектуальної системи підтримки прийняття рішень ідентифікації культурних цінностей (рис. 2).

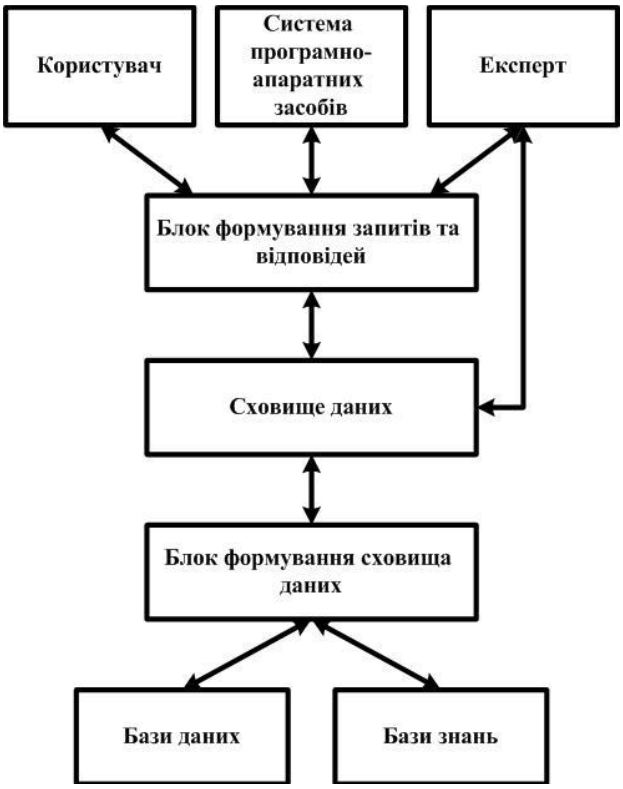


Рис. 2. Доопрацьована схема інтелектуальної системи підтримки прийняття рішень ідентифікації культурних цінностей

Відповідно до наведеної схеми, доступ та наповнення сховища даних мають експерт, та «блок формування сховища даних». Також слід зазначити, що «блок формування сховища даних» може використовувати дані з різних джерел та різних форматів та виконує консолідацію даних.

Консолідація - комплекс методів і процедур, спрямованих на вилучення даних з різних джерел, забезпечення необхідного рівня їх інформативності та якості, перетворення в єдиний формат, в якому вони можуть бути завантажені в сховище даних.

Цінність і достовірність знань, отриманих в результаті інтелектуального аналізу даних, залежить не тільки від ефективності використовуваних аналітичних методів і алгоритмів, але і від того, наскільки правильно підібрані і підготовлені вихідні дані для аналізу.

Тому, перш ніж приступати до аналізу даних, необхідно виконати ряд процедур, мета яких - доведення даних до прийнятного рівня якості та інформативності, а також організувати їх інтегроване зберігання в структурах, що забезпечують їх цілісність, несуперечність, високу швидкість і гнучкість виконання аналітичних запитів.

В основі консолідації лежить процес збору та організації зберігання даних у вигляді, оптимальному з точки зору їх обробки на конкретній аналітичної платформі або вирішення конкретної аналітичної задачі. Супутніми завданнями консолідації є оцінка якості даних і їх збагачення.

Основні критерії оптимальності з точки зору консолідації даних:

- забезпечення високої швидкості доступу до даних;
- компактність зберігання;
- автоматична підтримка цілісності структури даних;
- контроль несуперечності даних;
- джерела даних.

Ключовим поняттям консолідації є джерело даних - об'єкт, що містить структуровані дані, які можуть виявитися корисними для вирішення аналітичної задачі. Необхідно, щоб використовувана аналітична платформа могла здійснювати доступ до даних з цього об'єкта безпосередньо або після їх перетворення в інший формат. В іншому випадку очевидно, що об'єкт не може вважатися джерелом даних.

У процесі консолідації даних вирішуються наступні завдання:

- вибір джерел даних;
- розробка стратегії консолідації;
- оцінка якості даних;
- збагачення;
- очищення;
- перенесення в сховище даних.

Спочатку здійснюється вибір джерел, що містять дані, які можуть мати відношення до розв'язуваної задачі, потім визначаються тип джерел і методика організації доступу до них [5].

Висновки. Таким чином, пропонується при розробці інтелектуальної системи підтримки прийняття рішень ідентифікації культурних цінностей особливу увагу приділити питанням обґрунтування критеріїв формування сховища даних та консолідації даних. Також слід приділити увагу розробці методів і моделей оцінки якості даних із сторонніх джерел при наповненні сховища даних.

ПЕРЕЛІК ПОСИЛАНЬ:

1. А.А. Мартиненко, Б.І. Мороз, І.Г. Гуліна «Інтелектуальна система підтримки прийняття рішень ідентифікації культурних цінностей». IV Всеукраїнська науково-практична конференція «Перспективні напрямки сучасної електроніки, інформаційних і комп'ютерних систем (MEICS-2019)». Дніпро, 27–29 листопада 2019 р.

2. Ульяновська Юлія Вікторівна, «Моделі та методи обробки даних в єдиній автоматизованій інформаційній системі митної служби», автореферат дисертації на здобуття наукового ступеня кандидата технічних наук, 05.13.06 – автоматизовані системи управління та прогресивні інформаційні технології, Харків – 2005

3. Мазурець О.В. «Методи та системи штучного інтелекту», режим доступу https://msn.khnu.km.ua/course/view.php?id=4237

4. Орешков В.И. Паклин Н.Б. «Консолидация данных - ключевые понятия» режим доступу https://www.cfin.ru/itm/olap/cons.shtml

УДК 004.056.52

ВДОСКАНАЛЕННЯ РОЗМЕЖУВАННЯ ДОСТУПУ ДО ІНФОРМАЦІЇ У ЕЛЕКТРОННОЇ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я «eHealth»

А.В.Овєчкін, О.В.Кручінін
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Згідно до світових тенденцій, критичні вразливості від дій зловмисників щодо витоку великої кількості інформації з обмеженим доступом зазнає сфера медичного обслуговування. Вразливості медичних систем, які використовуються у лікарнях, в купі зі зухвалими діями співробітників призводять до викрадення цілих баз з персональними даними пацієнтів, лікарів, аптек, лікарень та інших суб'єктів медичних відношень. Витрати, пов'язані з порушенням конфіденційності інформації, становлять 3,92 мільйона доларів станом на 2019 рік, а сама галузь охорони здоров'я зазнає збитки у розмірі більш ніж 400 доларів за один медичний запис пацієнта [1]. Експерти прогнозують на 2026 рік, що ринок кібербезпеки у сфері охорони здоров'я буде оцінюватися майже у 27 млрд. доларів.[2].

Це питання актуальне і для України, у зв'язку з активним впровадженням електронної системи охорони здоров'я «eHealth». Сутність системи складається в тому, що вона забезпечує обмін конфіденційною медичною інформацією, з записом та подальшим зберіганням її у центральній базі даних (ЦБД) [3].

Доступ до даних ЦБД надається користувачам через спеціально розроблені медичні інформаційні системи (МІС) – інтерфейси, які поєднують лікарні або інші медичні заклади зі сховищем даних про пацієнтів, з можливостями отримання інформації, її модифікації або наповнення новими записами [4]. Ці нововведення у діяльності медичних установ, при недбалому використані їх, можуть спровокувати створення вразливостей, які можуть бути використані кіберзлочинцями.

У медичних системах найчастіше використовують рольову модель. Вона дуже проста в початковій імплементації за рахунок того, що в медичному середовищі чітко регламентована роль кожного лікаря та співробітника лікарні, з чітко встановленими дозволами на виконанні тих чи інших операцій.

Завдання розмежування доступу за рахунок розподілу ролей лише частково вирішена у «eHealth» – існуючі ролі дуже загальні та не відповідають усім сучасним потребам щодо розмежування доступом у лікарських закладах [5]. Розширення цієї моделі зі сторони «eHealth» не гарантує гнучкості та адаптивності для кількох різних за структурою та призначенням закладів, а також

у надзвичайних випадках. Наприклад, підписуючи декларацію про вибір лікаря, що надає первину медичну допомогу, пацієнт дає згоду на обробку своєї персональної інформації не тільки обраному лікарю, але ще й будь-якім лікарям, які можуть надавати допомогу.

Тому є необхідність в розширені існуючої моделі. Вона може зініціюватися зі сторони медичного закладу та бути складовою МІС, але це збільшує вартість та складність її розробки.

Універсальним варіантом є застосування додаткової програмної системи – системи управління основними даними (УОД), з доданням рольової моделі розподілу доступом. Розробка моделі має виконуватися представниками служб безпеки та керівниками кожного закладу, що використовують ті МІС, що планують підключення її до своїх систем, разом з представниками компанії-розробника системи УОД.

Саме варіант створення уніфікованої системи, з врахуванням потреб кількох МІС та з передбаченням можливості масштабування такої системи ще на стадії її проектування є більш ефективним рішенням. Треба розуміти, що проектування однієї тільки рольової моделі розподілу доступом потребує багатограного та поглибленого вивчення принципів роботи медичного закладу, дотримання норм законодавчого права, гарантування безпеки та надійності у функціонуванні такої системи, що пов’яже великі ключові ланки одного ланцюга обміну медичною інформацією між пацієнтами, лікарями, підприємцями та іншими можливими суб’єктами медичних процесів.

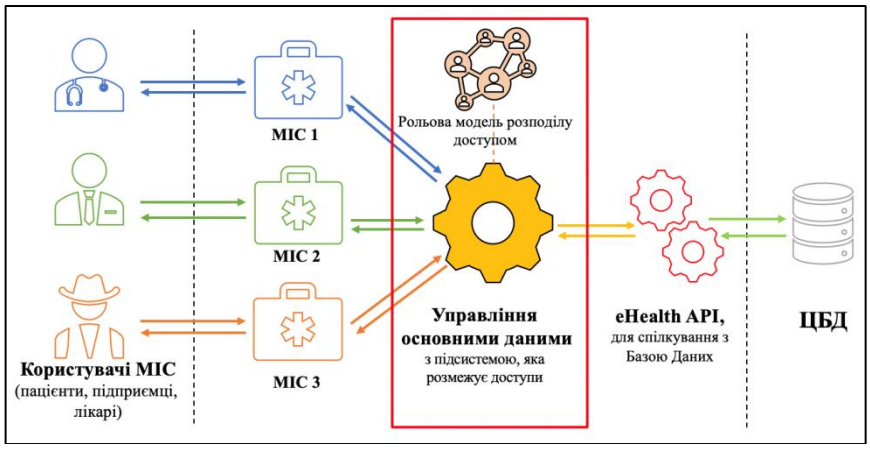


Рис 1. Структурна схема потоків даних від користувачів МІС до ЦБД з додатковою проміжною системою УОД

Механізм УОД це така сукупність інструментів та процесів обробки, яка займається збиранням та групуванням даних, як у випадках створення даних, так і в випадку запитів на їх отримання. Також вона призначена для узгодження бідь-яких систем між собою, які будуть підключені до неї [6]. У запропонованому підході головною метою такої системи є надання інформації користувачам за запитами до МІС, яка точно потребується для виконання його обов’язків відповідно до наданої йому ролі та дозволів.

Розроблятися така система може незалежно від МІС, на будь-якій мові програмування з використанням різноманітних додаткових технологій, незалежно ні від бази даних та «eHealth API», що надає інтерфейси для роботи з базою, ні від МІС, яка розроблялася сторонніми розробниками. Її вплив на загальний процес роботи користувачів МІС з базою даних складається в тому, що наприклад, по запиту лікаря на отримання даних про пацієнта, УОД отримує увесь набір даних, потім зіставляє її з роллю користувача, що передається при запиті частіше всього через так звані «HTTP заголовки». Встановлюючи відповідності між нею та її дозволами, система відфільтровує ті дані, до яких немає дозволів у конкретній ролі, та сформовану відповідь надсилає до МІС, яка в свою чергу вже інтерпретує її для користувача.

Висновки. Таким чином, використання додаткової системи дозволяє запобігти випадкам несанкціонованого доступу до інформації. Але водночас зобов'язує її забезпечувати відповідний рівень захисту інформації, яка циркулює через УОД. Запропонована системи повинна запобігти несанкціонованому копіюванні, та спотворенню інформації, що передається через неї. Основним завданням УОД є обмеження потрапляння до МІС даних с порушенням встановлених правил розмежування доступу. В такому випадку, можна забезпечити більш високий рівень захисту інформації, та контролювати її потоки, контролюючи хто, та в якому обсязі, отримує медичні дані.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Американський університет вирішує проблеми з кібербезпекою в галузі охорони здоров'я за допомогою першої національної програми «The Daily Swig – новини кібербезпеки» : веб-сайт. URL: https://portswigger.net/daily-swig/us-university-tackles-healthcare-cybersecurity-woes-with-first-national-program (дата звернення 12.11.2019).

2. Тенденції кіберзахисту у сфері охорони здоров'я «Reports And Data» : веб-сайт. URL: https://www.globenewswire.com/news-release/2019/08/26/1906602/0/en/Healthcare-Cybersecurity-Market-To-Reach-USD-27-10-Billion-By-2026-Reports-And-Data.html (дата звернення 12.11.2019).

3. «Електрона система охорони здоров'я» : веб-сайт. URL: https://ehealth.gov.ua

4. https://ain.ua/2017/11/21/kak-razrabatyvalas-ehealth/ (дата звернення 12.11.2019).

5. Технічна документація eHealth : веб-сайт. URL: https://edenlab.atlassian.net/wiki/spaces/EH/pages/2004415/Scopes+model (дата звернення 12.11.2019).

6. Управління майстер даними. «База знань в області корпоративних сховищ даних» : веб-сайт. URL: prj-exp.ru/integration/about_mdm.php (дата звернення 12.11.2019).

УДК 004.3

ДОСЛІДЖЕННЯ ПАРАЛЕЛЬНИХ АЛГОРИТМІВ ПОШУКУ ХАРАКТЕРНИХ НАБОРІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ПРОГРАММИРОВАНИЯ GPU

К.Ю. Островська, І.А. Бєлих
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Інтелектуальний аналіз даних є актуальною проблемою в області інформаційних технологій, оскільки ставить найбільш важкі завдання алгоритмічного характеру, які пов'язані з необхідністю забезпечення обчислювальної ефективності, точності, стійкості обробки накопичених знань.

Як правило, завданням інтелектуального аналізу даних є виявлення в сирих даних раніше невідомих, нетривіальних, практично корисних, доступних інтерпретації знань, необхідних для прийняття рішень в різних сферах людської діяльності. При цьому найбільш перевагу надають алгоритми, що використовують мінімальну кількість атрибутів, що безпосередньо пов'язано з їх обчислювальної ефективністю.

Серед найбільш перспективних підходів до вирішення даного завдання є підхід з виявлення асоціативних правил в даних, які відображають не просто статистичні залежності деяких атрибутів, але і причинно - наслідкові зв'язки, що існують в даних. Це дозволяє скоротити розмірність даних, зберігаючи найбільш інформативні атрибути.

Асоціативний аналіз спочатку був спрямований на задоволення потреб маркетингу: аналіз купівельної корзини, прогнозування попиту на товари. В даний час зростає інтерес до його використання в системах ухваленнях рішень для прогнозування громадської думки в соціології, в задачах медичної діагностики, ідентифікації шахрайських операцій на фінансових ринках і в багатьох інших прикладних напрямках.

Пошук асоціативних зв'язків умовно ділиться на два етапи, представлених на рисунку 1.

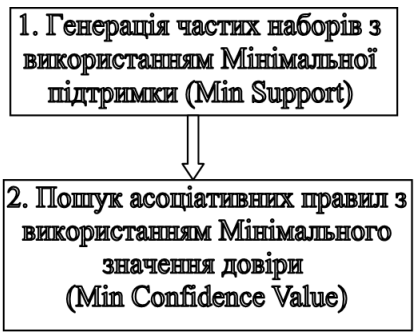


Рис. 1. Схема пошуку асоціативних правил

На першому етапі генеруються часті набори (frequent item sets), які задовольняють деякій мінімальній підтримки. На другому етапі, на основі частих наборів, здійснюється пошук асоціативних правил в відповідно до мінімального рівня довіри. На думку авторів [1] етап пошуку частих наборів є найбільш трудомістким, тому що вимагає звернення до бази транзакцій, перебору комбінацій значного числа елементів, з метою знаходження задовольняючих заданій підтримці. Рішення, забезпечують ефективне використання обчислювальних ресурсів систем при генерації частих наборів, безсумнівно, є актуальним напрямком досліджень при розробці алгоритмів пошуку асоціативних зв'язків.

В роботі [2] зазначається, що використання паралельної обробки даних на відеочіпах (GPU) дає істотний приріст продуктивності математичних розрахунків. Технологія програмування на відкритих (GPGPU) надає розробнику інструментарій для перенесення неграфічних обчислень на GPU, що дозволяє організовувати паралельне завантаження виконавчих блоків.

Аналіз стану досліджень і розробок алгоритмів пошуку характерних наборів, розроблених з використанням технології GPGPU показав, що існуючі популярні алгоритми, такі як Eclat, FP-Growth мають реалізації для виконання тільки на багатопроцесорних CPU [3].

Дана обставина вимагає проведення досліджень для пошуку альтернативних рішень, що забезпечують паралельне виконання пошуку частих наборів на GPU.

Метою даної роботи є дослідження і розробка паралельних алгоритмів пошуку частих (характерних) наборів даних, що використовуються в завданнях пошуку асоціативних правил, проведення експериментальної оцінки знайдених рішень за критеріями обчислювальної ефективності.

Висновки. У роботі вирішена актуальна задача підвищення ефективності інструментів асоціативного аналізу – досліджені популярні алгоритми пошуку характерних наборів Eclat і FPG і розроблені їх паралельні версії з використанням крос-апаратного і платформного сердовища програмування GPU OpenCL, а також вирішені наступні завдання:

1. Розроблено структуру зберігання транзакцій, що забезпечує перенос алгоритму FPG для виконання на GPU, а також процедури, забезпечують пошук і витяг частих наборів.

2. Досліджено ефективні рішення підрахунку підтримки для алгоритму Eclat з використанням підрахунку в циклі і підрахунку на основі функцій робочих груп, що реалізують паралельно алгоритми scan і reduce.

Аналіз розроблених алгоритмів з використанням реальної бази транзакцій показав наступний результат:

1. Алгоритм Eclat в цілому демонструє кращу тимчасову продуктивність, споживання оперативної пам'яті і завантаження CPU в порівняно з алгоритмом FPG на наборах даних з великою кількістю різнорідних атрибутів, зростання кількості яких призводить до експоненціального підвищення часу генерації наборів для алгоритму FPG проти лінійного росту для алгоритму Eclat. Однак, при збільшенні числа транзакцій відбувається збільшення кількості бітового

уявлення, підрахунок підтримки на якому призводить до лінійного зростання тимчасової продуктивності алгоритму Eclat, тоді як алгоритм FPG залишається нечутливим до даного параметру.

2. Паралельні алгоритми Eclat показали ефективне споживання ресурсів оперативної пам'яті, CPU, а також високу тимчасову продуктивність в порівнянні з послідовним алгоритмом на CPU при числі транзакцій більше 5000, при меншому значенні алгоритми на GPU неефективні через витрати на перемикання контексту host-> device-> host.

3. Підрахунок підтримки для алгоритму Eclat на основі функцій робочих груп, які наявні в стандарті OpenCl 2.0, показав кращу тимчасову ефективність в порівнянні з підрахунком в циклі, що пояснюється оптимізацією операцій додавання всередині робочої групи і відсутності витратних операцій завантаження і вивантаження результатів складання.

4. Паралельні алгоритми FPG показали також ефективне споживання ресурсів оперативної пам'яті, CPU, а також високу тимчасову продуктивність в порівнянні з послідовним алгоритмом на CPU навіть на невеликих наборах даних (починаючи від десятків транзакцій), тому що перемикання контексту, на відміну від алгоритму Eclat, який рекурсивно формує дерево частих наборів і для кожного вузла викликає kernel - функцію, проводиться лише двічі - під час передачі префіксного дерева в kernel-функцію і при вивантаженні результатів з вихідного буфера.

Варто відзначити, що паралельний алгоритм FPG має точку підвищення ефективності використання пам'яті GPU, яка полягає в розробці способів псевдодінамічного виділення пам'яті в kernel - функції. Як відомо, виділення пам'яті для обчислення на GPU пристрої виробляється на стороні host, що не завжди враховує реальну потребу процедур, що виконуються побудова структур, розмір яких заздалегідь не відомий. Одним із способів реалізіації динамічного управління пам'яттю на стороні GPU - пристрою є створення єдиного буфера значного розміру, переданого в kernel - функцію і визначення функцій, аналогічних malloc і free в стандартній бібліотеці C. Однак, визначення не надлишкових розмірів згаданого буфера вимагає проведення додаткових досліджень алгоритму FPG.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Guizhen Yang, The Complexity of Mining Maximal Frequent Item sets and –Maximal Frequent Patterns: [Электронный документ]. (https://www.semanticscholar.org/paper/The-complexity-of-mining-maximal-frequent-itemsets-Yang/6b92231d9815544d9c78891f94d246096b1393c8).

2. С.А. Полетаев, Параллельные вычисления на графических процессорах: [Электронный документ]. // Параллельное программирование. – 2012. – 300 с. (https://www.iis.nsk.su/files/articles/sbor_kas_16_poletaev.pdf).

3. Tianyuan Jiang & Prepost: A GPU Accelerated–Xin Lv, Zhihong Deng, GPU Frequent Pattern Mining Algorithm Based on PrePost: [Электронный документ]. (https://jtyuan.github.io/files/gpu-prepost.pdf).

УДК 004.77

ПРОЕКТУВАННЯ VPN МЕРЕЖІ ДЛЯ ОРГАНІЗАЦІЇ З ВИКОРИСТАННЯМ CISCO PACKET TRACER

Т.В. Селівьорстова, О.Ю. Юхименко
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. На сьогоднішній день майже кожне підприємство так чи інакше пов’язане з обчислювальними мережами. Це зумовлено тим, що обчислювальна техніка полегшує роботу в різних сферах і тим самим підвищує продуктивність підприємств. Але щоб отримати цю продуктивність, треба правильно реалізувати її можливості. Наприклад об’єднати комп’ютери в локальну обчислювальну мережу, що дасть можливість поєднати між собою підрозділи підприємства і тим самим полегшити обмін файлами між робітниками, або ж об’єднати філії одного підприємства, які розташовані на великій відстані один від одного, між собою через VPN канал і тим самим надати можливість обмінюватися даними між локальними мережами.

Аналіз останніх публікацій та досліджень. VPN – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Постановка завдання. Метою роботи є розробка та реалізація методичних і технологічних рекомендацій при створенні VPN мережі для організації та їхня реалізація засобами Cisco Packet Tracer.

Матеріали дослідження. Cisco Packet Tracer – це симулятор мережі розроблений компанією Cisco і рекомендований при вивченні телекомунікаційних мереж і мережевого устаткування. Цей додаток дозволяє будувати мережі на різноманітному обладнанні в довільних топологіях з підтримкою різних протоколів. Програмне рішення Cisco Packet Tracer дозволяє імітувати роботу різних мережевих пристроїв: маршрутизаторів, комутаторів, точок бездротового доступу, персональних комп'ютерів, мережевих принтерів, IP-телефонів і т.д. Універсальна інкапсуляція при маршрутизації (GRE) – це протокол тунелювання, здатний інкапсулювати різні протоколи мережевого рівня між двома об'єктами по загальнодоступній мережі, наприклад, в інтернеті.

Топологія складається з трьох маршрутизаторів Cisco 1941 двох комутаторів Cisco 2960 і двох вузлів, які використовують тільки порти Ethernet. Розглянуті питання побудови та налаштування VPN мережі розподіленої корпорації.

Висновки. В ході виконання роботи розроблені та реалізовані методичні і технологічні рекомендацій при створенні VPN мережі для організації із застосуванням Cisco Packet Tracer.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Cisco Packet Tracer [электронный ресурс] // Режим доступа свободный: http://www.cisco.com/c/dam/en_us/trainingevents/netacad/course_catalog/docs/Cisco_PacketTracer_DS.pdf

2. Frame Relay в Cisco [электронный ресурс] // Режим доступа свободный: http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/vpnmi_wp.htm

3. GNS3/Dynamips [электронный ресурс] // Режим доступа свободный: https://www.gns3.com/

4. VPN [электронный ресурс] // Режим доступа свободный: https://tools.ietf.org/html/rfc4026

5. Пакет К. Создание сетей удаленного доступа Cisco – М: "Вильямс", 2003. – 672 стр.

РОЗДІЛ 2

ПРОГРАМНІ ЗАСОБИ УПРАВЛІННЯ, ЗБОРУ, ОБРОБКИ І ПЕРЕДАЧІ ІНФОРМАЦІЇ

UDC 656.078.1

DEVELOPMENT OF AN INFORMATION SYSTEM TO JUSTIFY THE CHOICE OF DATABASES WHEN USING CRM SYSTEMS

M. Alekseev, S. Ochkur, I. Hnennyi
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Introduction. This paper is about the development and research of a method for evaluating the performance of databases that are used in CRM systems. The development of a separate CRM system for each organization is determined by the inability to solve the tasks on the basis of ready-made existing platforms. Finished products are designed to solve typical problems, not suitable for all companies. While individual development allows us to solve the main issues of the company related to internal document management and customer relations.

The main goal is to develop an information system for the method of evaluating and justifying the choice of a database model for CRM systems.

The main problem is that any database model can be used for each CRM system, which can adversely affect the performance of the system as a whole.

The aim of this paper is to develop an information system to justify the choice of databases when using CRM systems.

Ready-made solutions. While NoSQL databases have the speed and scalability advantage, there have a number of drawbacks compared to traditional relational databases. Leavitt lists these challenges [1]. He notes that NoSQL databases, even though fast for simple tasks, are time-consuming for complex operations. Besides queries for complex operations can be hard to form. The other drawback is the lack of native support for consistency. Leavitt also notes that NoSQL is a technology that many organizations are yet to learn and there is a lack of support and management tools to help.

Bartholomew gives a tutorial introduction to the history of and differences between SQL and NoSQL databases [2]. Sakr et al. discuss data management solutions, including NoSQL, for cloud-based platforms [3]. They discuss the challenges data management solutions face in the light of the cloud.

Hecht and Jablonski provide a use-case oriented survey of NoSQL databases [4]. They identify the difficulties in choosing a NoSQL database to fit a particular use-case, and therefore focus their paper to address this. They use as the basis for their comparison the data model, support for queries, partitioning, replication, and concurrency controls. They compare in this light fourteen NoSQL databases, including MongoDB, CouchDB, Cassandra and HBase.

Boicea et al. compare a NoSQL database against a SQL database. They choose Oracle for the SQL implementation and MongoDB for the NoSQL implementation [5]. They report that, with a large number of records, insertion time is a factor more in Oracle and update and delete times are several factors more in Oracle.

Yahoo! Cloud Serving Benchmark is an open-source work-load generator tool for comparing key-value stores [6].

Solve. In the study of performance of database management systems, the following criteria will be the benchmarking criteria: adding, finding, modifying, and deleting from a single table. All listed operations are present in MySQL and MongoDB.

Several tests were compiled for the study. You must create two tables before you start testing. The first table will consist of 30,000 entries with identical text and a random foreign key in the range from 1 to 100,000. The second table will consist of 100,000 entries, the keyCol and valueCol fields of each row will be equal to each other and take values from 1 to 100,000.

The text in the first table is only needed to increase the amount of data recorded. The keyCol attribute of the second table is named to emphasize that it is not a primary key. It is not the primary key for the reason that it will slow down the speed of MySQL operations through additional integrity checks. The keyCol and valueCol fields accept the same values just to simplify perception, conceptually it does not affect anything.

It should be noted that the second table is larger than the first table. This is done for several reasons. First, it should make searching for keyCol a little more complicated. Secondly, due to the first fact, it will make it somewhat difficult to join the two tables.

The first test will be adding up to 100,000 rows to the keyCol_valueCol table. The time commit is 1000 entries. The second test is to link two tables. In MySQL is used LEFT JOIN, in MongoDB - $ lookup. In this test, the size of the textCol_outsideKeyCol table will vary from 10,000 to 30,000 records.

The third test is to search up to 10,000 records in the keyCol_valueCol table.

The fourth test changes the value of the valueCol column by keyCol to 10,000 rows. The last test is to delete entries in the keyCol_valueCol table with keyCol for up to 10,000 rows.

Since all tests, except the first, require a keyCol attribute search, the tests are performed twice: with indexing of the attribute and without indexing.

For ease of testing, a Python program is written in three parts: the main program, the module with the MySQL test function, the module with the MongoDB test function.

Linux Ubuntu 18.04.3 LTS distribution was used as the server operating system. MySQL 8.0.17 and MongoDB 4.2.0 are installed as local databases and can be accessed through the computer's internal address. A computer with the following configuration was used as the server:

- processor: Intel Pentium CPU B950 clocked at 2.10 GHz 2 cores;
- RAM: DDR3 6 Gb;
- Video Adapter: GeForce GT 540M 1 Gb.

Test results. The first test (using indexes) is to perform line insertion. Line insertion runs in stages from 10,000 to 100,000 records. The test results are shown in Figure 1.

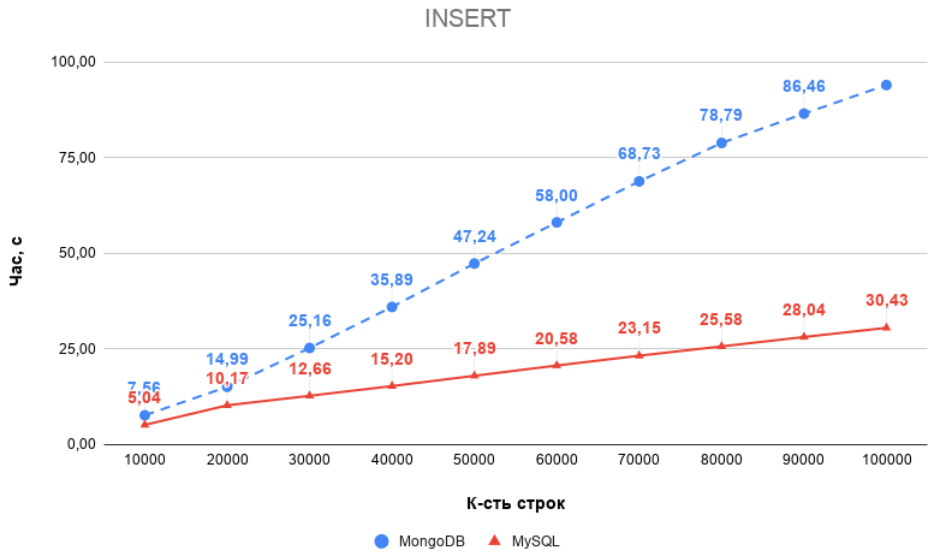


Fig. 1. Chart of time of operation of INSERT operation on number of records

Based on the results above, we can conclude that the insertion operation runs faster in MySQL almost 2 times than in MongoDB. It is also worth noting that as the number of MySQL product lines increased, it declined less rapidly than MongoDB.

The second test (using indexes) is the binding operation. The test uses the left link in stages from 10,000 to 30,000 rows. MySQL DBMS is a great time-consuming bind operation.

In other tests, MySQL was also better than MongoDB. But when tested without using indexes in a relational model, MongoDB showed an advantage in search, update, and delete operations.

The result of the search operation test is shown in Figure 2.

Fig. 2. Diagram of the execution time of a SELECT operation (not index) on the number of entries

According to the results of this test, we can conclude that the search time without indexing is almost the same in the two DBMSs, but MongoDB showed the best time for this test.

The result of the upgrade operation test is shown in Figure 3.

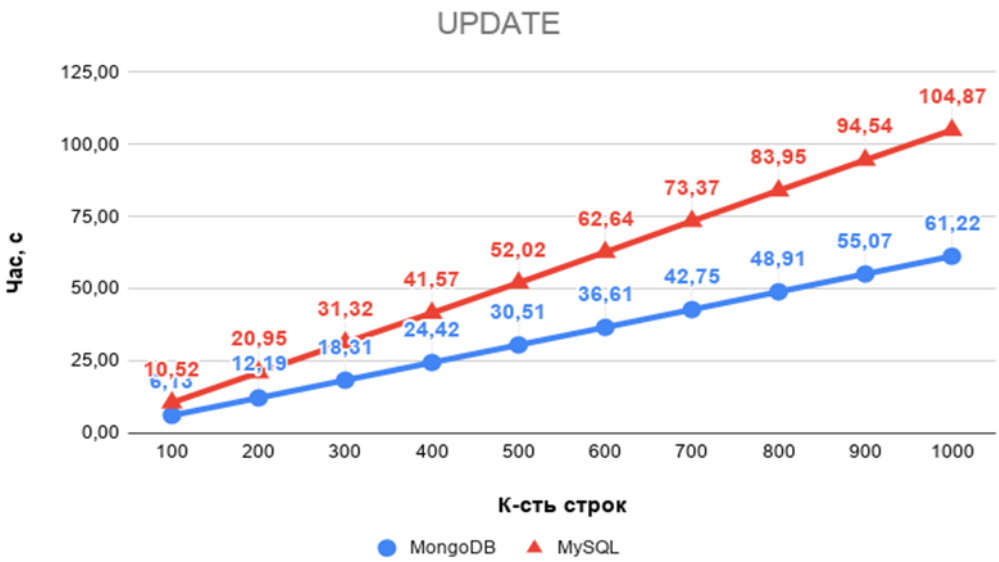


Fig. 3. UPDATE (not index) operation time chart versus number of records

According to the results of the fourth test, MongoDB showed the best time. It should be noted that with the increase in the number of records, the execution time of the operation in MySQL increased more intensively than in MongoDB.

The result of the removal test is shown in Figure 4.

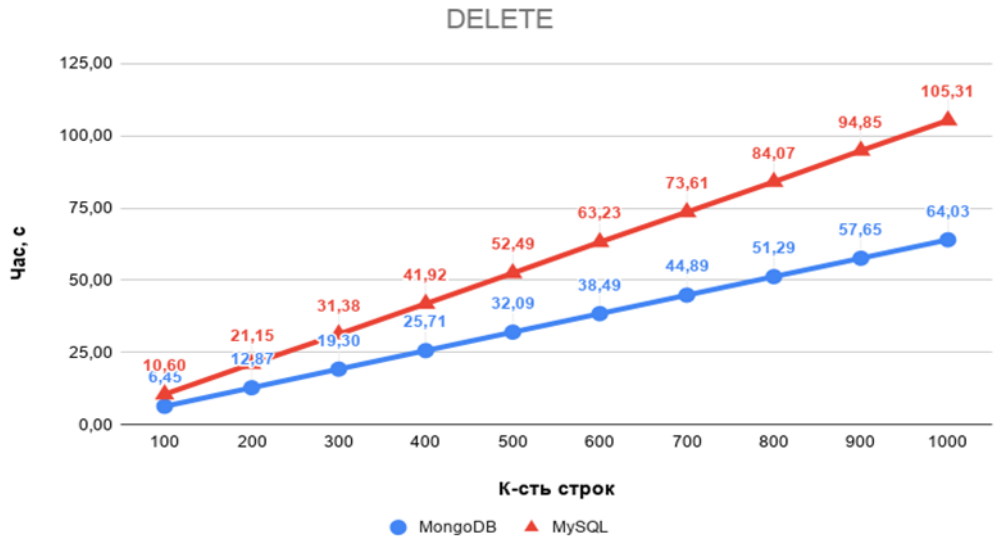


Fig. 4. Chart of DELETE operation time (not index) on the number of entries

In the operation of deleting records without using indexes, MongoDB obtained a time advantage.

Conclusions. MySQL is more suitable for CRM systems where the database must be rigorously structured without the dynamic appearance of tables or schemas. A prerequisite is to use indexes in tables. MongoDB is more suitable for CRM systems where the database is dynamic in terms of data change, flexible, performs a large number of searches and has no rigid structure. In this case, the indexes do not play a big role.

REFERENCES:

1. N. Leavitt, “Will NoSQL databases live up to their promise?” [Text], Journal Computer, - IEEE Computer Society Press Los Alamitos, CA, USA, vol. 43, no. 2, pp. 12 –14, feb. 2010.
2. D. Bartholomew, “SQL vs. NoSQL,” [Text], Linux Journal, - Department of Computer Science, Maharaja Surajmal Institute of Technology, Janakpuri, N.delhi 110058, Indiano. 195, July 2010.
3. S. Sakr, A. Liu, D. Batista, and M. Alomari, “A survey of large scale data management approaches in cloud environments,” [Text] Communications Surveys Tutorials - IEEE, vol. 13, no. 3, pp. 311–336, 2011.
4. R. Hecht and S. Jablonski, “NoSQL evaluation: A use case oriented survey” [Text], in Cloud and Service Computing (CSC), - 2011 International Conference on, dec. 2011, pp. 336 –341.
5. A. Boicea, F. Radulescu, and L. I. Agapin, “MongoDB vs Oracle – database comparison” [Text], in Emerging Intelligent Data and Web Technologies (EIDWT), - 2012 Third International Conference on, sept. 2012, pp. 330 –335.
6. B. F. Cooper, A. Silberstein, E. Tam, R. Ramakrishnan, and R. Sears, “Benchmarking cloud serving systems with ycsb” [Text], in Proceedings of the 1st ACM symposium on Cloud computing, - ser. SoCC ’10. ACM, 2010, pp. 143–154.

УДК 004.056.5: 004.414.22

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЕФЕКТИВНОСТІ МЕТОДІВ ВИЯВЛЕННЯ ШКІДЛИВИХ ПРОГРАМНИХ ЗАСОБІВ

М.Д. Даценко, С.В. Машурка
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Щороку в світі створюється величезна кількість комп'ютерних програм. Разом з цим зростає кількість комп'ютерних вірусів. Згідно зі звітом McAfee Labs [1] за перший квартал 2019 року в світі з'явилося понад 65 млн одиниць шкідливого програмного забезпечення (далі ШПЗ). Дані приведені на Рис. 1. Це на 18% більше, ніж за останній квартал 2018 року. При цьому загальна кількість ШПЗ практично досягло 1 млрд. Однією з причин цього явища є можливість автоматизованої розробки шкідливих програм. Про це свідчить і дані Data Breach Investigation Report за 2016 рік [2]. У звіті сказано, що більше 99% шкідливих програм існують у незмінному вигляді протягом 58 секунд

і менше. При цьому більшість програм виявляються лише одного разу. Ці дані свідчить про те, наскільки швидко зловмисники змінюють ШПЗ. Основним вектором атаки на даний момент є ШПЗ. При цьому, більшість зловмисників використовують більше одного вектора атаки [3]. Згідно з підрахунками міжнародних експертів, кожні 14 секунд у світі відбувається одна кібератака. У 2016 році цей час був 40 секунд. А прогноз на 2021 рік - 11 секунд. Однією з причин такого зростання фахівці вважають технологічні тренди. Згідно зі звітом компанії Cisco за 2018 рік [4], злочинці під час веб-атак в період 2014-2017 років широко використовували виконавчі файли а також шкідливий веб-контент.

Таким чином, необхідним і актуальним завданням в боротьбі з ШПЗ є визначення сильних та слабких сторін методів виявлення ШПЗ, а також систем, для яких той чи інший метод буде давати кращі результати.

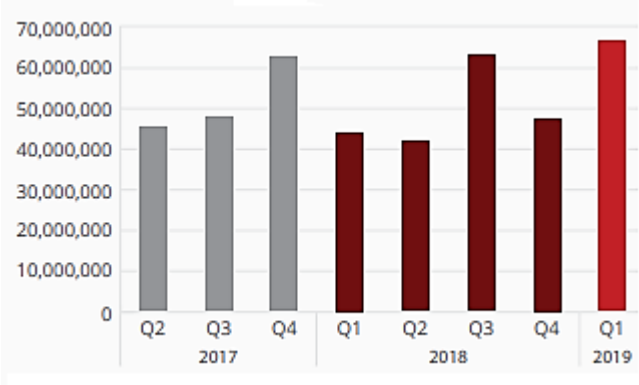


Рис.1. Графік росту кількості шкідливого програмного забезпечення

Основними методами виявлення ШПЗ є сканування, евристичний аналіз, виявлення змін та використання резидентних сторожів [5].

Сканування – це історично один із перших методів виявлення ШПЗ. При скануванні, програма-сканер проглядає вміст файлів на жорсткому диску, а також оперативну пам’ять пристрою. Класичне сканування передбачає пошук ШПЗ за їх сигнатурами. Сигнатура – це певна послідовність байтів, характерна для даного ШПЗ .

Основною перевагою даного способу є те, що він здатен виявляти широкий спектр ШПЗ а також висока швидкість роботи, яка зумовлена невеликою обчислювальною складністю.

До недоліків варто віднести те, що:

– сканування дозволяє виявити лише те ШПЗ, яке не використовує шифрування власного коду та поліморфізм;
– постійне використання ресурсів обчислювальної системи;
– необхідність постійного оновлення бази сигнатур;
– неможливо виявити ШПЗ, сигнатури якого немає в базі.

Евристичний аналіз. Суть цього методу полягає в контролі усіх дій, які може виконати програма, що перевіряється. При цьому відстежуються потенційно небезпечні дії, характерні для ШПЗ. Контролюючи дії програм, що перевіряються, аналізатор здатен виявляти нове ШПЗ ще до початку його виконання.

До недоліків даного методу слід віднести те, що

– евристичний аналізатор не дає повної гарантії виявлення будь-яких нових вірусів;

– постійне використання ресурсів обчислювальної системи;

– можлива помилкова тривога, коли аналізатор приймає безпечну програму за ШПЗ.

Метод виявлення змін. Базується на використанні програм ревізорів. Ці програми визначають і запам'ятовують характеристики всіх областей на дисках, в яких зазвичай розміщуються віруси. Під час періодичного виконання, програма-ревізор визначає нові характеристики контрольованих областей і порівнює їх з даними в пам’яті. У результаті порівняння, програма дає відповідь про можливу наявність ШПЗ.

Зазвичай програми-ревізори запам'ятовують наступні параметри:

– образи головного завантажувального запису;

– образи завантажувальних секторів логічних дисків;

– характеристики всіх контрольованих файлів і каталогів;

– номера дефектних кластерів;

– обсяг встановленої оперативної пам'яті;

– кількість підключених до комп'ютера дисків і їх параметри.

Перевагами методу є можливість виявлення ШПЗ усіх типів, в тому числі і так званих «стелс-вірусів», а також нове невідоме ШПЗ. Окрім цього використання даного способу може прискорити роботу інших методів виявлення ШПЗ. Наприклад, можна сканувати лише ті файли, які зазнали змін.

Метод виявлення змін має один суттєвий недолік: за допомогою програм-ревізорів неможливо визначити ШПЗ у файлах, які надходять в систему вже зараженими. ШПЗ буде виявлено лише після розмноження.

Метод використання резидентних сторожів. Заснований на застосуванні програм, які постійно перебувають в ОП ЕОМ і відстежують дії інших програм. Метод дозволяє виявити виконання підозрілих дій , таких як звернення для запису в завантажувальні сектора, розміщення в ОП резидентних модулів, спроби перехоплення переривань і т.п. До переваг методу можна віднести теоретичну можливість виявляти ШПЗ будь-якого типу, а також виявлення ШПЗ в момент виконання небезпечної дії.

Недоліком є практична неможливість реалізації повного контролю, а також значний відсоток помилкових тривог.

Висновки. Розглянувши основні методи виявлення шкідливого програмного забезпечення можна зробити висновки про те, що метод сканування гарно підходить для систем, які мають постійну можливість оновлення своїх баз вірусних сигнатур. Якщо дана вимога не виконується – втрачає сенс використання даного методу в будь-якій системі.

Метод евристичного аналіз ідеально підходить для систем, в яких циркулює велика кількість шифрованого трафіку та в системах, в яких немає жорстких вимог до кількості помилок другого роду.

Метод виявлення змін підходить для будь-яких систем в якості методу, який пришвидшує роботу інших методів. Не підходить для встановлення на вже запущену систему, адже вразливий до атаки першого дня.

Метод використання резидентних сторожів підходить для систем, які постійно стикаються з великою кількістю нових вірусів. Не підходить для систем з малою кількістю обчислювальних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Mcafee labs threats report.: веб-сайт. URL:https://www.mcafee.com/ enterprise/en-us /assets/reports /rp-quarterly-threats-aug-2019.pdf (дата звернення: 14.11.2019)

2. Data Breach Investigation Report.: веб-сайт. URL: https://regmedia.co.uk/ 2016/05/12/ dbir_2016.pdf (дата звернення: 10.11.2019)

3. Data Breach Investigation Report.: веб-сайт. URL: https://www.cisecurity.org/ blog/top-10-malware-september-2019/ (дата звернення: 12.11.2019)

4. Data Breach Investigation Report.: веб-сайт. URL: https://www.cisco.com/ c/dam/global/ ru_ru/assets/offers/assets/cisco_2018_acr_ru.pdf (дата звернення: 13.11.2019)

5. Ахметов І.Г. Молодой ученый. Международный научный журнал. 2016. № 125. С. 758.

UDC 004.048

DEVELOPMENT AND STUDY OF INTERACTION TRADING PLATFORM WITH CONSUMERS

D. Slipko, A.T. Khar
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Introduction. This article is about website development and analysis. Allow to show the full cycle of sales of goods from the very beginning.

The aim of this work is to develop a website and analyze the effectiveness of the trading platform.

Relevance and implementation methods. The rapid development of the Internet, the use of the latest technology and communications in business and everyday life has led to the emergence of new economic phenomena, such as electronic commerce. Currently, trading electronic platforms of various types and purposes are widespread [1,2].

E-commerce in Ukraine is one of the newest and most promising forms of innovation in the field of trade [3]. With the help of electronic commerce, most business processes are accelerated due to their electronic implementation, since information is transmitted directly to the recipient, bypassing the stage of creating a paper copy at each stage.

All online stores provide a potential buyer with a similar set of features that differ from each other in their extensive range and design. The main advantage is the high-quality implementation of the functions of the online store, as focused on the convenience of the potential buyer.

Thus, in order to surpass similar online stores based on the requirements of customers, the main attention in the development should be given to the convenience of the interface with which the potential buyer interacts, providing extensive information about the product and the availability of convenient payment methods.

To create the next tool has been used a web-site:

1. Markup languages:. HTML, CSS, etc.
2. Built-in raster graphics. Modern browsers accept images in JPG, GIF, and PNG.
3. Language development and frameworks: JS, Node-JS, jQuerry, SASS, Bootstrap.
4. Stripe payment system.
5. Firebase database.

Analysis of the trading platform shows that there are various ways to improve their effectiveness [4].

The calculation of the effectiveness of the online store and selection criteria [5,6].

1) Total attendance.
2) Conversion.
3) Payback (ROI - return on investment).
4) Failures.

– ,

where I is income and C is expense.

Analysis and solution of the problem. With the help of all used systems and services, we can conduct a visual analysis of the trading platform and determine the effectiveness of this store. Using these tools, we have detailed information about transitions through advertising services and the number of purchases made after the transition, which will give there information on the effectiveness of advertising and find out which products are popular and which require better promotion and improvement of advertising, we also have information about regions from which the purchase and rating of these regions was made, with the help of this information we can determine where to advertise most effectively, thereby reducing costs, also, given the scheme of trading through dropshipping [7], it is better to look for suppliers in the popular areas of sales and thus reduce the delivery time. We also get information using UTM tags [8], which makes it clear where the transition was made from.

Conclusion. The cost of e-commerce can be different - it all depends on the nature of the proposed trade. One of the main issues is the creation of the necessary infrastructure. The underlying network infrastructure must be sufficiently developed to meet the stringent requirements of e-commerce. Thanks to these tools and services, a detailed analysis of the trading platform was demonstrated and ways to improve the

efficiency of the online store were revealed, which will increase the conversion and number of visits, as well as reduce costs.

REFERENCES:

1. Trading platforms [Electronic resource] /. - The electron. journal –Access mode: https://www.investopedia.com/terms/t/trading-platform.asp
2. Types of trading platforms [Electronic resource] /. - The electron. journal – Access mode: https://bestforexbroker.online/types-of-forex-trading-platforms/
3. Ecommerce system [Electronic resource] /. - The electron. journal - Access mode: https://www.cs-cart.com/ecommerce-system.html
4. Online store performance [Electronic resource] /. - The electron. journal - Access mode: https://www.theselfemployed.com/ecommerce/10-ways-optimize-online-store-performance/
5. Sales Conversion [Electronic resource]. - The electron. journal - Access mode: https://www.klipfolio.com/resources/kpi-examples/sales/sales-conversion-rate
6. Calculation of the effectiveness [Electronic resource]. - The electron. journal - Access mode: https://www.investopedia.com/articles/fundamental-analysis/10/strategy-performance-reports.asp
7. Dropshipping [Electronic resource]. - The electron. journal - Access mode: https://www.shopify.com/guides/dropshipping/understanding-dropshipping
8. UTM tags [Electronic resource]. - The electron. journal - Access mode: https://www.opentracker.net/article/UTM-tags

УДК 004.056.55

ЗБЕРІГАННЯ КВАЛІФІКОВАНОГО ЕЛЕКТРОННОГО ПІДПИСУ

Р.С. Алексєєв, С. І. Войцех
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Розвиток глобальних комунікацій в діловому і повсякденному житті обумолює поширення взаємовідносин, пов’заних з електронним обміном даними. В обміні можуть приймати участь органи державної влади, комерційні і некомерційні організації, а також громадяни на офіційному та особистому рівнях.

Проблема зберігання електронних документів від копіювання, модифікації і підробки вимагає застосування спеціальних засобів і методів захисту. Важливу роль серед них відіграє електронний цифровий підпис (ЕЦП), який забезпечує підтвердження цілісності інформації документа, його реквізитів і факту підписання конкретною особою.

Цифровий підпис дозволяє здійснити:

1. Аутентифікацію особи - автора електронного документа.
2. Контроль цілісності переданого документа: при будь-якій випадковій або навмисній зміні документа підпис стане недійсним, тому що він обчислений на підставі вихідного стану документа і відповідає лише йому.

3. Захист від модифікації документа через наявність можливості контролю цілісності. Гарантія виявлення підробки при контролі цілісності робить підробку недоцільною у більшості випадків.

4. Неможливість відмови від авторства. ЕЦП створюється із використанням закритого ключа, який повинен бути відомим тільки підписанту, що не дає змоги відмовитися від свого підпису під документом.

5. Доказове підтвердження авторства документа. Створити коректний підпис можливо, лише знаючи закритий ключ, а він повинен бути відомим тільки власнику, через що власник пари ключів може довести своє авторство під документом. В документі можуть бути підписані такі поля як «автор», «внесені зміни», «мітка часу» і т.п.

На даний час порядок та організація електронного документообігу, а також правовий статус електронного цифрового підпису визначаються Законом України «Про електронні довірчі послуги» (далі – Закон). Він запроваджує поняття «кваліфікований електронний підпис»(КЕП) на зміну поняття «електронний цифровий підпис». Згідно Закону кваліфікований електронний підпис – це удосконалений електронний підпис, який створюється із використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. Для того, щоб мати можливість підписувати електронні документи, подавати електронну звітність або електронні декларації, особа повинна отримати КЕП. Видача останнього згідно Закону є довірчою послугою, що здійснюється лише в центрах сертифікації ключів, акредитованих Центральним засвідчувальним органом (АЦСК).

Згідно Закону для кваліфікованих постачальників електронних довірчих послуг кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки.

Це означає, що усі КЕП повинні генеруватися та зберігатися на захищеному носієві ключової інформації(НКІ).

Застосування апаратних НКІ (смарт-карт, токенів) має такі недоліки:

1. Висока ціна носіїв.
2. Необхідність завжди мати пристрій при собі (у разі утрати пристрою КЕП потрібно перевипускати)
3. Один захищений носій може зберігати лише один секретний ключ.
4. Електронний підпис неможливо використовувати на веб-ресурсах без установки на комп’ютер необхідних бібліотек (драйверів) для роботи з носієм.
5. Недостатня рівень забезпеченості носіями.

Усунення наведених недоліків може бути досягнуто шляхом створення програмно-апаратного комплексу “хмарного” КЕП на базі існуючого АЦСК. Такий підхід до надання електронних довірчих послуг також забезпечить такі переваги, як:

1. Одне централізоване сховище ключів, доступ до якого можливий лише при наявності інтернет-підключення.
2. Відповідальність за збереження і захист ключів приймає на себе АЦСК.
3. Відпадає необхідність використання бібліотек (драйверів).
4. Можливість інтеграції комплексу зі сторонніми сервісами.
5. Низька ціна аренди місця в криптомодулі.
6. Спрощення процедури отримання КЕП.

ПЕРЕЛІК ПОСИЛАНЬ:

1. https://zakon.rada.gov.ua/laws/show/2155-19#n534
2. https://www.pfu.gov.ua/kr/327258-pro-kvalifikovanyj-elektronnyj-pidpys/
3. Семь безопасных информационных технологий / под ред. А. С. Маркова. - М.: ДМК Пресс, 2017. — 224 с.: ил
4. https://medoc.ua/uk/blog/kep-na-zahishhenih-nosijah-roztlumachumo-shho-do-chogo

УДК 004.056

РОЗРОБКА ІНФОРМАЦІЙНОЇ СИСТЕМИ РИЗИК-БЕЗПЕКИ ПЕРСОНАЛЬНИХ ДАНИХ

В.В. Гнатушенко, В.О. Бура, Т.М. Фененко
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Створення інформаційної системи (ІС) ризик-безпеки персональних даних, яка б дозволила знизити невизначеність при виборі альтернатив, тим самим зменшити можливість прийняття неефективного рішення.

Сучасні інформаційні системи найчастіше представляють собою складні комплекси взаємопов'язаних компонентів. Завдання аналізу безпеки, оцінки ризиків у таких системах ускладнюється тим, що експерту невідомі точні значення характеристик системи яка аналізується. Більшість існуючих методик припускають завдання наближених точкових оцінок, що знижує достовірність отриманих, також точкових, результуючих показників.

При експертному оцінюванні, ми стикаємося з різними видами невизначеності, і основним завданням є її спільне моделювання. Аналогічна проблема виникає і при виборі найбільш ефективного комплексу засобів протидії загрозам інформаційної безпеки. Для її вирішення використовується методика рандомізації оцінок факторів з подальшим відбором результатів, що задовольняють вихідними даними.

В умовах реального світу інформація слабо визначена - має нечислової характер, неточна, погано структурована. Фактично, первинні дані являють собою випадкові величини. Поряд з невизначеністю оцінок можлива і структурна невизначеність, тобто неповнота знань про наявність чи відсутність відносин між факторами. З урахуванням структурної невизначеності, а також узгодження думки

кількох експертів, завдання моделювання факторів ризику ускладнюється, а час рандомізації значно зростає. Для вирішення завдань оцінки і аналізу ризиків застосовуються експертні системи, які, на жаль, мають не дуже велику методологічну різноманітність.

Виходячи з означених вище параметрів інформаційних систем та їх недоліків, була розроблена система ризик-аналізу, в якої оцінки факторів ризику представляють не точкові значення показників, а розподіл їх ймовірностей. Розроблена методика стохастичного ризик-аналізу, дозволяє більш достовірно оцінити загрози для конкретної ІС і розробити ефективну систему захисту. При необхідності можливе додавання факторів, або їх угруповання (об'єднання). Оскільки методика працює не з числовими значеннями, а з розподілами, то вона дозволяє описати різноманітні типи інформації, які одержані в результаті експертного оцінювання.

В рамках роботи розроблено модуль системи ризик-аналізу, що дозволяє вирішити задачу статистичної обробки даних, які отримані на етапі стохастичного моделювання, і подальшого їх відображення у вигляді профілів ризиків. В якості інформаційного об'єкта для аналізу та оцінки ризиків було використано ІСПД медичного закладу.

Висновки. Розроблена ризик-модель містить відмінності від вихідної базової моделі безпеки інформаційної системиа персональних даних (ІСПД). Перш за все, фактори ризику в ній об'єднані в зв'язну причинно-обумовлену структуру. Однак, для збереження несуперечності з базовою моделлю, в набір чинників ризик-моделі були включені всі загрози базової моделі. Створено перелік ризик-факторів, який містить джерела загроз, загрози, події ризику, інформаційні компоненти об'єкта захисту. Для дотримання методологічної строгості і логічної повноти ризик-моделі деякі вихідні чинники зазнали змін: змінено формулювання, вироблено розбиття на кілька факторів для зниження складності. Крім того, додані фактори, які явно не вказуються в базовій моделі, але включені в неї контекстуально. Подібні модифікації не створюють протиріч з базовою моделлю.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков Учеб. пособие для студ. высш. учеб. заведений. - 2-е изд., испр. - М. : Академия, 2008. - 368 с

2. Малкин В.С. Надежность технических систем и техногенный риск Учебное пособие. - Ростов-на-Дону: Феникс, 2010. - 432 с.

3. Хованов Н.В. Анализ и синтез показателей при информационном дефиците - СПб.: Изд-во СПб ун-та, 1996. - 196 с.

УДК 004.9

ПРОЕКТУВАННЯ ТА ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЛОКАЛЬНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПРИ ПЕРЕДАЧІ ТРАФІКА

В.В. Гнатушенко, О.М.Хоменко
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Створення структури локальної комп'ютерної мережі для бізнес-центру, який не має в даний час розвинених внутрішніх комунікацій, та оцінка якості передачі трафіка.

Більшість комп'ютерних мереж створювалося з розрахунком на передачу даних в основному традиційних видів трафіка, наприклад, файлів й електронної пошти [1]. Потреби сучасного суспільства в мультимедийной інформації диктують необхідність побудови нових мереж, що відповідають вимогам мультимедійних технологій, а також модернізації вже існуючих мереж [2]. Розроблене вже достатня кількість мережних технологій, що дозволяють поліпшити характеристики комп'ютерних мереж, що як уже існують, так і знову створюваних, в області передачі мультимедійного трафіка. Комплексний підхід реалізації мережної інфраструктури починається від побудови структурованої кабельної системи й закінчується уведенням в експлуатацію мультимедійних додатків.

Для рішення поставленого завдання було:

– проведено огляд методів формалізації комп'ютерних мереж і способів побудови моделей мереж і потоків трафіку;

– проведено аналіз існуючих технології проектування та розроблено логічну схему організації мережі;

– здійснено вибір програмних та апаратних засобів мережі і обладнання безперебійного електропостачання;

– спроектована локальна інформаційно-обчислювальна мережа з фізичної прив'язкою комп'ютерів і активного обладнання;

– проведено імітаційне моделювання функціонування мережі;

– створено методику тестування комп'ютерної мережі на придатність до передачі інформації.

У ході використання методики два хоста, що знаходяться в різних ділянках мережі, обмінюються тестовим трафіком. Параметри трафіку заміряються і аналізуються, після чого робиться висновок про здатність мережі передавати заданий обсяг мультимедійної інформації без спотворень в сприйнятті. Серед параметрів, які оцінює методика, розглядаються:

– частка втрат пакетів під час вимірювання, усереднена за час 5 с (характеризує сплески втрат);

– частка втрат пакетів, усереднена за часом всього виміру (характеризує загальний рівень втрат);

– довжина інтерквантільного проміжку для вибірки інтервалів між надходженнями послідовних пакетів (є оцінкою "тремтіння" (jitter) і побічно характеризує завантаженість мережі);

– бітова швидкість вузького місця мережі (визначається з аналізу інтервалів між надходженнями послідовних пакетів);

До цього списку слід додати час повного обороту (RTT) , методику вимірювання якого через технічні проблеми не вдалося реалізувати , що належить зробити в майбутньому. Також в числі подальших напрямків роботи можна назвати поліпшення методики визначення бітової швидкості вузького місця мережі та автоматизацію аналізу даних, зібраних протягом великих періодів часу.

ПЕРЕЛІК ПОСИЛАНЬ:

1. В.Г.Олифер, Н.А.Олифер. Компьютерные сети. Принципы, технологии, протоколы. СПб: Питер, 2001. - 672 с., ил.

2. Таненбаум Э.С. Компьютерные сети[пер. с англ.]. - СПб.: Издательский дом «Питер» 2012. - 960 с.

УДК: 004.657

ДОСЛІДЖЕННЯ ДАНИХ З РЕЄСТРАЦІЇ ТРАНСПОРТНИХ ЗАСОБІВ МОБІЛЬНОГО ЦЕНТРУ ОБЛІКУ ТА РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

О.А. Камишов, Н.Л. Дорош
(Україна, Дніпро, Національна металургійна академія України)

Кожного дня в Україні стає все більше та більше водіїв. При покупці або продажу авто, воно повинно бути поставлено на облік, або знято з нього. Раніше це робили у МРЕО зараз для цього існують спеціальні Сервісні центри, але основа задача їх залишається такою ж.

На першому етапі роботи розроблено програмне забезпечення для реєстрації транспортних засобів, на другому етапі проведено дослідження даних, які були перетворені у часові ряди. Результати досліджень представляють практичний інтерес[1].

Склад програмного засобу містить реляційну базу даних, структуру якої було розроблено. Інструментом розробки обрано СУБД SQL. Передбачено захист інформації та реалізовано доступ з використанням паролей. Визначені обов’язки адміністратора та співробітників[2].

База даних містить дані з властивостей автомобілів (марка, номер кузова, модель і т.д.), паспортні дані власника та дані про працівників.

Однією з важливих функцій програмного засобу є реєстрація порушення. Можливо обрати будь-яке авто (або його власника) внести його дані, а так само місце порушення і статтю яку він порушив, суму штрафу і що з його автомобілем

(наприклад в угоні або відправлений на штраф-стоянку). Була додана довідка, інструкція до програми, таблиця звітів порушень[3].

Основним завданням з використання баз даних є формування різнобічних запитів. Основною потребою є якнайшвидше виконання цих самих запитів. Для цього використовується оптимізація запитів. В реляційній СУБД оптимальний план виконання запиту — це така послідовність застосування операторів реляційної алгебри до перетворення відношень, яка для конкретного поточного стану БД може бути виконана з мінімальним використанням обчислювальних ресурсів [4].

Інформація, яка отримана в результаті виконання запитів, перетворена у часові ряди.

Виконано дослідження даних з використанням методів аналізу часових рядів. Проведено розрахунок описових статистик, перегляд даних. Реалізовані функції згладжування методами експонеційного згладжування та лінійної фільтрації цифровим фільтром з кінцевою імпульсною характеристикою[5].

Тепер можна підвести підсумки і вирахувати у яких областях України частіше купують автомобілі а також яких країн виробників. Можна також підрахувати середній вік водіїв які купували автомобілі, або якого кольору авто частіше купують. Дані внесені за Січень 2019 року і являються актуальними і зараз. За результатами, які отримані: частіше всього у січні-лютому 2019 автомобілі купували у Дніпропетровській та Київській областях. Виробника частіше всього обирали: Китай, або Корея. Середній вік водіїв, які купували автомобілі на початку року: 30-35р., колір у пріоритеті був чорний та трохи менше - білий.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Bootstrap from Twitter. [Електронний ресурс] – Режим доступу. — URL: http://getbootstrap.com (дата звернення 20.09.2019).

2. Люк Веллинг, Лора Томсон. Разработка веб-приложений с помощью PHP и MySQL. 5-е издание. Пер. с англ. – М. – Диалектика-Вильямс, 2017. – 768с.

3. BazaGai [Електронний ресурс] – Режим доступу. - URL: https://baza-gai.com.ua (дата звернення 15.09.2019).

4. Оптимізація SQL-запитів. [Електронний ресурс] – Режим доступу. - URL: http://ts-soft.ru/blog/sql-optimization-1 (дата звернення 22.10.2019).

5. BOOKLAND. [Електронний ресурс] – Режим доступу. - URL: https://bookland.com/ukr (дата звернення 02.10.2019).

УДК 651.3:518.5

ХМАРНІ ТЕХНОЛОГІЇ У ІНДУСТРІЇ ВІДЕОІГОР

М.С. Нападайло, Л.В. Кабак, О.А. Сподинець
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми: Десятиліттями у відеоіграх є ціла череда проблем, які розробники не раз намагались вирішити самими різними способами та засобами, але їм це не як не вдавалося, серед них такі як:

– “піратство” (Незаконне використання програмних засобів без купівлі ліцензії);

– “читери” (Незаконна зміна ігрового ПЗ/додавання до нього нових компонентів, які дають гравцю переваги над іншими гравцями);

– розповсюдження та встановлення користувацьких модифікацій без дозволу власників ПЗ;

– мультиплатформені збереження ігрового процесу (дозволяють на іншому девайсі продовжити гру, де зупинився користувач на попередньому пристрої).

– мультиплатформена розробка відеоігор.

Для захисту від “піратсва” створювались цілі технології захисту від несанкціонованого злому (Наприклад Denuvo Anti-Tamper), деякі проекти вимагали навідь для однокористувацької гри постійного підключення до інтернету, щоб гра у “real time” робила перевірку на ліцензування гри. Видавництва відеоігор та студії розробників погрожували подати позови до суду, а у деяких випадках і подавали їх для того, щоб заборонити деяким “аматорським” студіям випускати свої модифікації для їх ігор. Різні студії створювали свою хмарні сервіси для реалізації мультиплатформових збережень, але вони зазвичай просто зберігали рівень, на якому зупинився гравець та параметри його героя/аккаунту. Ще у далекі часи компанія Nintendo намагалася впровадити подібне рішення для своїх ігрових консолей і випускала окремий аксесуар Nintendo Transfer Pak для передачи збережень між консолями Nintendo 64 та Nintendo GameBoy. Але цей аксесуар не знайшов тоді популярності і його підтримує лише 16 ігор[1]. Для спрощення розробки ігор на різні пристрої, навіть консолі восьмого покоління перевели на архітектуру X64 (хоча всі попередні консолі мали архітектуру, яка різнилася від архітектури звичайних ПК, і навіть ще у сьомого покоління були свої архітектури - PowerPC та Cell (повна назва Cell Broadband Engine Architecture)[3][4]).[2]

Але вже сьогодні з’явились інструменти які в змозі вирішити ці проблеми, і це саме Хмарні технології.

Основна частина: Як взагалі працює хмарний ґеймінг?

Користувач використовує на своєму комп'ютері пристрій введення інформації, будь то клавіатура з маніпулятором миші, чи ґеймпад, ігровий руль, джойстик тощо. Після цього введена інформація передається через мережу на

віддалені сервери, на яких і розташована запущена гра. Після цього цей сервіс віддає відеопотік, який транслюється нам на екран.

Тобто простими словами, це можна порівняти з трансляцією відео з відеохостингу, але за умови того, що ми контролюємо події цього відео, тим самим від нас залежить, яка інформація наступною буде транслюватися на наш екран (рис. 1).

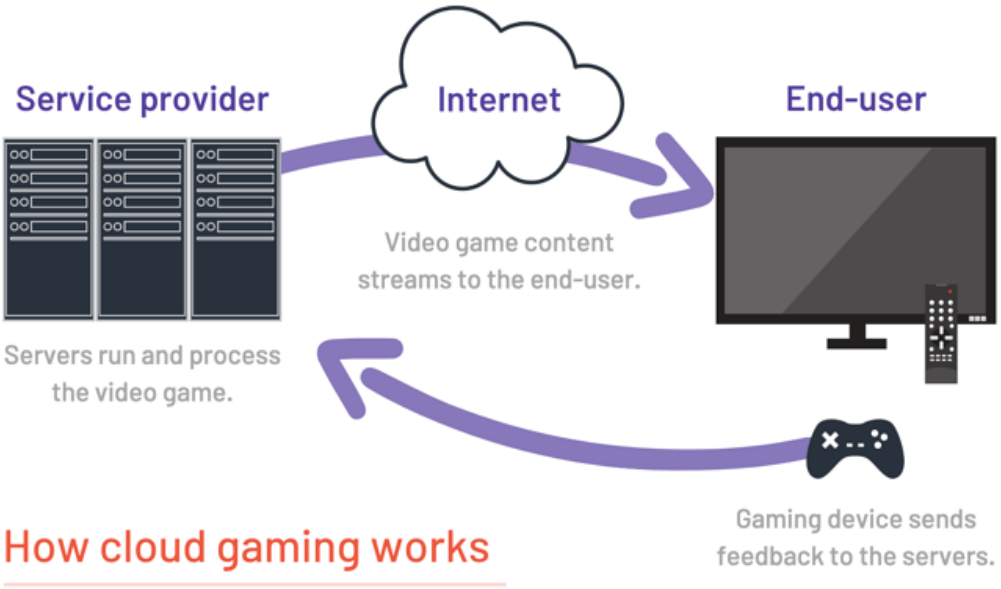


Рис. 1. Схема зв’язку

Сервери зазвичай встановлює та налаштовує таж сама компанія, що і створює клієнт-серверний додаток та і в загалом розробляє всю систему. Зазвичай такі компанії вже мають свої сервери, які використовують у інших цілях.

Яким чином хмарні технології вирішують вищепоставлені проблеми?

1. Гра знаходиться на віддалених серверах і тому її модифікація неможлива. На сервери неможливо встановити неліцензійне ПЗ, яке зламає програмний ключ гри, або підмінить його, неможливо також встановити ПЗ, яке буде давати перевагу над іншими гравцями. Крім цього в таком випадку власники гри отримують можливість контролювати усі користувацьки модифікації для своєї гри, можно буде створювати окремі системи, в які користувачи зможуть викладати свої модифікації і тільки після проходження модерації від розробників, ці модифікації можуть ставати доступними для завантаження іншими гравцями.

2. Є можливість створити лаунчери для різних платформ (windows, linux, android, ios, webOS, Tizen OS), що дозволить одну і ту ж саму гру запускати на різних пристроях. Так як гра знаходиться на віддалених серверах і весь процес у реальному часі зберігається там, то проблематика “мультиплатформених збережень прогресу” також вирішена.

Чи є подібні системи, які вже реалізовані, так на даний момент вже є ряд систем, які вже працюють, проходять бетатестування чи тільки анансовані:

– Playstation Now;

– Geforce Now;
– Google Stadia;
– Microsoft Project xCloud (робоча назва);
– Drova;
– Shadow;
– Vortex.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Nintendo Famdom, Transfer Pak //URL: https://nintendo. fandom.com/wiki/Transfer_Pak .
2. Wikipedia, Сьоме покоління ігрових систем //URL: https://uk.wikipedia.org/wiki/Сьоме_покоління_ігрових_систем (або https://uk.wikipedia.org/wiki/%D0%A1%D1%8C%D0%BE%D0%BC%D0%B5_%D0%BF%D0%BE%D0%BA%D0%BE%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D1%96%D0%B3%D1%80%D0%BE%D0%B2%D0%B8%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC).
3. Wikipedia, PowerPC //URL: https://uk.wikipedia.org/wiki/PowerPC
4. Wikipedia, Cell //URL: https://uk.wikipedia.org/wiki/Cell_(процесор) (або https://uk.wikipedia.org/wiki/Cell_(%D0%BF%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%BE%D1%80))

УДК 004.3

DEPENDENCY INJECTION КОНТЕЙНЕР ТА ВПРОВАДЖЕННЯ ЙОГО В СУЧАСНІ WEB-ДОДАТКИ

К.Ю. Островська, О.В. Захарченко
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Впровадження залежності (Dependency injection, DI) - процес надання зовнішньої залежності програмного компоненту. Є специфічною формою «інверсії управління» (Inversion of control, IoC), коли вона застосовується до управління залежностями. У повній відповідності з принципом єдиних обов'язків об'єкт віддає піклуватися про побудову необхідних йому залежностей зовнішньому, спеціально призначеному для цього спільного механізму.

При цьому впровадження залежностей об'єкт пасивний і не вживає взагалі ніяких кроків для з'ясування залежностей, а надає для цього сеттери і / або приймає своїм конструктором аргументи, за допомогою яких впроваджуються залежності.

Принцип роботи. Робота фреймворка, що забезпечує впровадження залежності, описується наступним чином. Додаток, незалежно від оформлення, виповнюється всередині контейнера IoC, що надається фреймворком. Частина об'єктів в програмі як і раніше створюється звичайним способом мови програмування, частина створюється контейнером на основі наданої йому конфігурації.

Умовно, якщо об'єкту потрібно отримати доступ до певного сервісу, об'єкт бере на себе обов'язок щодо доступу до цього сервісу: він або отримує пряме посилання на місцезнаходження сервісу, або звертається до відомого «сервіс-локатор» і запитує посилання на реалізацію певного типу сервісу. Використовуючи ж впровадження залежності, об'єкт просто надає властивість, яке в змозі зберігати посилання на потрібний тип сервісу; і коли об'єкт створюється, посилання на реалізацію потрібного типу сервісу автоматично вставляється в це властивість (поле), використовуючи кошти середовища.

Впровадження залежності більш гнучко, тому що стає легше створювати альтернативні реалізації даного типу сервісу, а потім вказувати, яка саме реалізація повинна бути використана, наприклад, файли конфігурації, без змін в об'єктах, які цей сервіс використовують. Це особливо корисно в юніт-тестуванні, тому що вставити реалізацію «заглушки» сервісу в тестований об'єкт дуже просто.

З іншого боку, зайве використання впровадження залежностей може зробити програми більш складними і важкими в супроводі: так як для розуміння поведінки програми програмісту необхідно дивитися не тільки в вихідний код, а ще й в конфігурацію, а конфігурація, як правило, невидима для IDE, які підтримують аналіз посилань і рефакторинг, якщо явно не зазначена підтримка фреймворків з впровадженнями залежностей.

У web-додатках JavaScript практично безальтернативно займає своє місце на фронті, в браузері. На серверній стороні щільно окопалися Java, PHP, .Net, Ruby, Python. Але з появою nodejs JavaScript також проник і на сервер. А технології, які використовуються в інших мовах, в тому числі і DI, почали проникати в серверний JavaScript.

Розвиток JavaScript обумовлено асинхронні роботи коду в браузері. Асинхронність не є винятковою особливістю JavaScript, швидше за вродженої. Зараз наявність JavaScript і на сервері, і на фронті вже нікого не дивує, а скоріше, стимулює до використання одних і тих же підходів на обох "кінцях" web-додатку. І одного і того ж коду.

Висновки. Обробка залежностей без DI можлива, але це може привести до збоїв роботи програми. DI - це просто ефективна ідея, згідно з якою можливо обробляти залежності поза залежного класу. Найефективніше використовувати DI в певних частинах програми. Багато фреймворків цьому сприяють. Фреймворки і бібліотеки не потрібні для DI, але можуть багато в чому допомогти.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Inversion of Control Containers and the Dependency Injection pattern (https://www.martinfowler.com/articles/injection.html).

2. Java for fun: Что такое Dependency injection, Inversion of Control и почему это возникло. Часть #1(http://www.apofig.com/2010/08/dependency-injection-inversion-of.html).

УДК 004.94

ПРОЕКТУВАННЯ ІНФОРМАЦІЙНОЇ СИСТЕМИ З ВИКОРИСТАННЯМ VREALIZE AUTOMATION

С.О. Смолянов, І.С. Дмитрієва
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Хмарні рішення пропонують компаніям ряд переваг, такі як: безпека, гнучкість на рівні ПО і апаратного забезпечення, надійність, автоматизація роботи IT персоналу, легкість доступу. vRealize Suite, платформа управління VMWare - це абсолютно новий спосіб розширення центру обробки даних до хмарного сховища за допомогою уніфікованих засобів управління:

1. Automation - автоматичне управління життєвим циклом інфраструктури, послуг і сервісів;
2. Orchestrator - це інструмент для управління IT інфраструктурою, її адміністрування;
3. Operations - попереджуюче управління продуктивністю, використання ресурсів і журналами подій;
4. Business insight - узгодження витрат на IT, забезпечення повної прозорості витрат;
5. Unified management - використання єдиної платформи для надання та управління додатками та інфраструктурою.

Мета роботи полягала у вирішенні таких IT завдань:

1. Автоматизація процесу створення, налаштування і реконфігурації віртуальних машин під потреби різних додатків;
2. Надання більшості хмарних сервісів і рішень за заниженою вартістю (в порівнянні з AWS і Microsoft Azure).

Було розгорнуто кластер vRealize Automation, реалізовано підключення декількох vCenter як endpoint, налагодження процесу створення і кастомізації ОС. Були створені сервіси по розвороту готових додатків і баз даних. Автоматизований процес реєстрації віртуальних машин в Identity Manager і створення політик доступів за допомогою API. Так само було створено ряд сервісів по реконфігурації і донастройки віртуальних хостів. Підключений VMware vRealize Business for Cloud для розрахунку вартості обчислювальних ресурсів. Розгорнуто і підключений Operations Manager для збору статистики з віртуальних машин гіпервізора і СЗД. Автоматизований процес реєстрації нових віртуальних машин в базі CMDB.

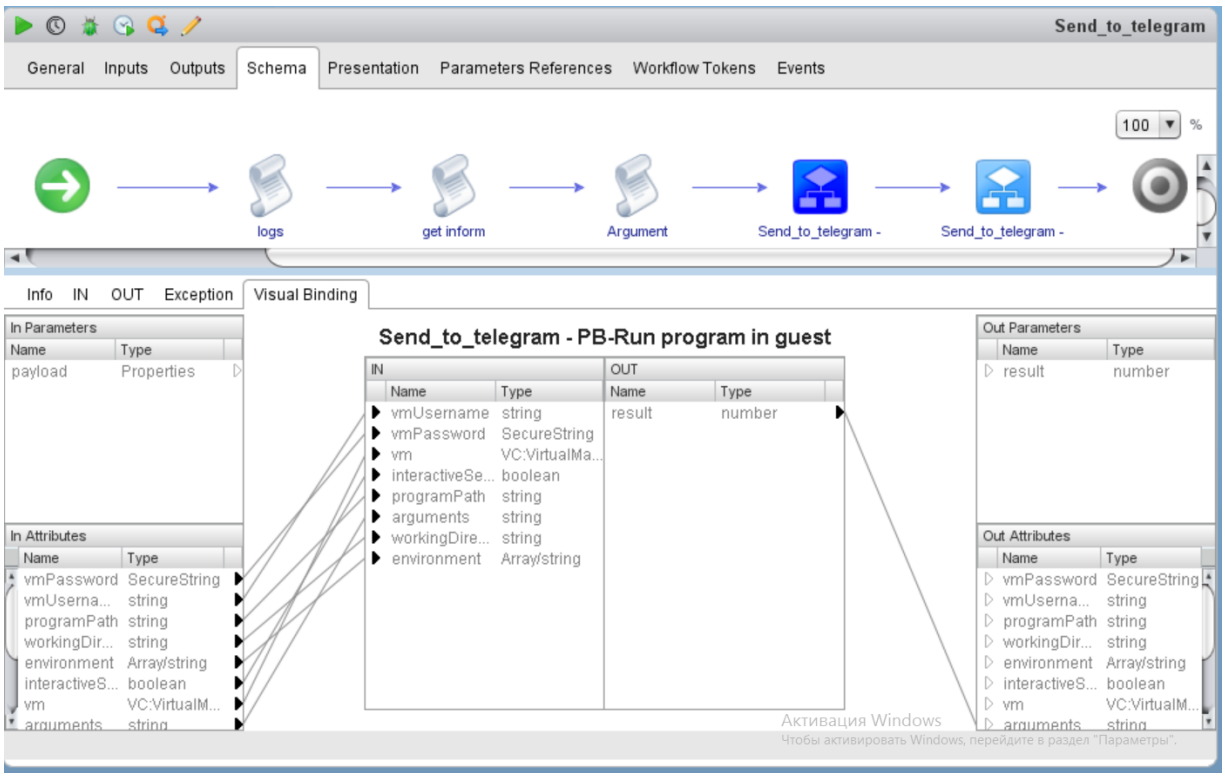


Рис. 1. "Рукописний" сервіс в vRealize Orchestrator, який відправляє в Telegram інформацію про замовлений сервісі, характеристики віртуальних машин і результат виконання деяких скриптів

Висновки. За допомогою даного програмного рішення можна вирішувати будь-які IT завдання на рівні інфраструктури і додатків. Впровадження продуктів vRealize Suite допомагає скоротити витрати компанії на IT в цілому.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Информация о vR Automation https://docs.vmware.com/en/vRealize-Automation/index.html

2. Использование подключаемого модуля vRealize Orchestrator для vSphere Replication 6.5 https://docs.vmware.com/en/vSphere-Replication/6.5/using-vr-plugin-65-guide.pdf

РОЗДІЛ 3

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ТА ОПТИМІЗАЦІЯ СИСТЕМ ОБРОБКИ ІНФОРМАЦІЇ ДЛЯ ВИРІШЕННЯ ЗАВДАНЬ ОСВІТИ, НАУКИ І УПРАВЛІННЯ ВИРОБНИЦТВОМ

UDC 656.078.1

DEVELOPMENT AND RESEARCH OF A TRAFFIC CONTROL SYSTEM AT THE INTERSECTION

B. Moroz, L. Mesheryakov, T. Shaptala
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Introduction. This paper is about development and research of traffic management system at intersections. Every year, the number of cars on the roads is increasing, and therefore issues such as optimizing or adjusting traffic lights are still relevant and until a solution is found that can overcome all the problems.

The main objective is to try to reduce the downtime of cars at traffic lights by improving the traffic lights and turning it into a standalone system that can evaluate the situation on the road, and recalculate the allotted time for all directions it manages.

A lot of the problem in this matter lies at the intersections. As it is the main place where two or more traffic flows need to be synchronized.

The aim of this paper is development smart traffic control system at the intersection with function evaluate the situation on the road.

Ready-made solutions. This problem is already being considered by many leading countries in the world, and Japan in this task has taken steps to solve this problem:

1. A road section with a fully automated traffic light or a group of traffic lights connected to each other that are monitored using special sensors for traffic on the road and reconfigures the time allocated to the streams in real time.
2. A section of the road that is under the control of a special group of people - who monitor traffic, and manually reconfigures traffic lights.

Traffic lights are configuring in Ukraine according to the principle of statistical calculation of the flow on a section of road at different times of the day, and on the basis of these data the time allocated for a particular flow for that section is calculated. The duration of the regulatory cycle is calculated using the Webster formula [1]:

_____. 1)

where - duration of the regulatory cycle, s;

– lost time at intermediate tact (yellow traffic light signal) on *i* cycle, s;

– phase coefficient, the largest value is determined by the formula [2]:

—.

2)

where – traffic intensity in one of the directions regulated by the traffic light, car/hour;

– saturation flow, car/hour.

The main problem with this method is that the measurements are made only a few times and adjust the traffic light statically based on these measurements [3].

Solve. Instead, it is suggested to modify the entire system so that it can predict flows based on sensor data and reconfigure itself.

To ensure that the necessary flow of traffic values for traffic lights are obtained, we will use on the term "sensor". Schematically, a map of sensors and links with traffic lights for two intersections is presented in figure 1.

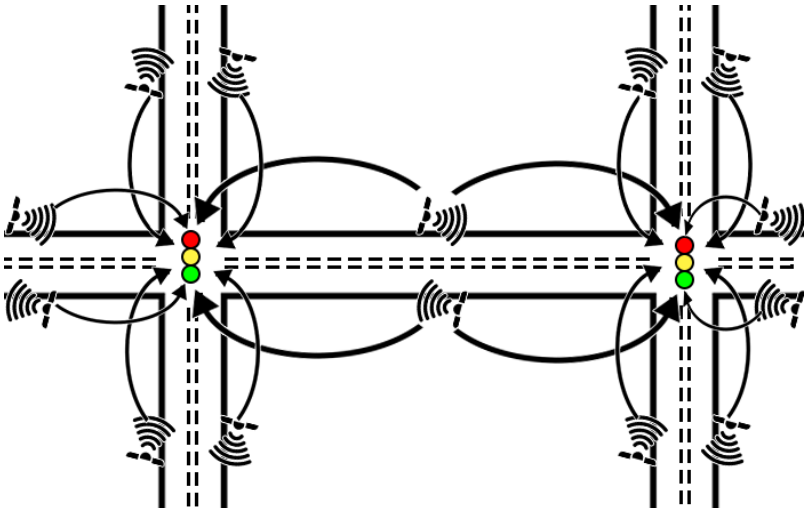


Fig. 1. Map of sensors and links with traffic lights for two intersections

Since the development of sensors for this system is not the topic of this report, we abstract from this issue. The sensors will be placed in such a way that each traffic light in the system has a complete picture of the situation at the road for which it is responsible.

On the basis of the data obtained stand out more time for travel for a flow of traffic with a higher density is allocated. Traffic lights that are connected in one system in the form of a double-link graph reconfigure a route with a large stream to the road with a green wave.

1. Modification the formula (2) that way that it calculated flow in minute and not in hour:

———
——— .

3)

where - traffic intensity on one of the counters regulated by the light data received from the sensors in the last minute, car/minute;

– flow prediction coefficient relative to traffic flow.

2. Modification the formula (1) that way that it calculation regulatory cycle at the crossroad by average between previous and current flow of traffic values:

. 4)

where – sum of phase coefficient that have been calculate now;

– sum of phase coefficient that had calculated previous.

3. And modification last formula for green signal traffic light:

. 5)

Next, you need to check the conditions for allocating sufficient time for pedestrians to pass the road [1]. This is provided in the rules for setting up regulated intersections. This is done according to the formula:

. 6)

where – time for pedestrians to pass the road;

– the width of the road;

– average speed of pedestrians.

Conclusions. When applying this method, we get a decrease in queues at intersections. In different situations, this numeric is different, but the increase in efficiency reaches 10%.

The main advantage this approach is that in the morning and evening peak of traffic the number of cars is the same, but their direction is opposite, this approach allows you to very effectively solve this situation. And also this method will solve temporary problems that are not typical for a given time of day on the roads, such as an accident that will change the flow characteristics.

REFERENCES:

1. Methodological recommendations for the design of traffic lights on roads [Text] / Federal Highway Agency (Rosavtodor) - Moscow, 2013. - 30 p.

2. Vlasov A.A., Orlov N.A., Portov D.V., Skripkin P.B., “Calculation of the operating modes of a traffic light object in conditions of saturated traffic” [Electroniy Resource], “Electronic Scientific Journal”, “Modern problems of science and education" https://www.science-education.ru/en/article/view?id=13145

3. Vlasov A.A., Orlov N.A., Chushkina K.A. “Methodology for calculating the operating modes of traffic lights in saturated traffic conditions” [Electroniy Resource], Internet journal “НАУКОВЕДЕНИЕ”, issue 2, birch - quarter 2014.

UDC 533.72

ANALYSIS OF SIR MODEL FOR PREDICTING THE SPREAD OF MEASLES

Z. Shulha, O.S. Shevtsova
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Introduction. The main task of the health care system in any country is to control the spread of infectious diseases. The social consequences, as well as the material losses, strongly demonstrate the need to predict the occurrence of epidemics. Measles is one of the most contagious diseases. In Ukraine, according to the Public Health Center of the Ministry of Health of Ukraine, more than 115,000 people have contracted measles since summer 2017, 41 of whom have died [1]. Simulation of the measles spreading allows to predict new outbreaks of measles and evaluate the strategy to prevent them.

The aim of this paper is to analyze the SIR epidemic model for simulation of the spread of infectious diseases and to select the appropriate model extension for modeling the spread of measles.

Epidemiology of measles. Measles is a viral infectious disease that starts in the respiratory system. Symptoms of measles generally first appear within 10 to 12 days of exposure to the virus. They include cough, fever, runny nose, red eyes, sore throat white spots inside the mouth. A widespread skin rash is a classic sign of measles. This rash lasts up to 7 days.

Measles can be spread through the air. An infected person release the virus into the air through coughing or sneezing. A susceptible person that is exposed to the measles virus has a 90 percent chance of becoming infected. An infected person is contagious for 4 days before the characteristic rash appears and for another four days after the rash.

Getting vaccinated is the best way to prevent measles. Two doses of the vaccine are approximately 97% effective at preventing measles, while one dose is about 93% effective. When rates of vaccination within a population are greater than 92% outbreaks of measles typically no longer occur. During 2000 – 2017, measles vaccination prevented an estimated 21.1 million deaths throughout the world [2].

The classical SIR model. A significant contribution to the mathematical modeling of epidemics has been made by W. O. Kermack and A. G. McKendrick in their scientific work “A Contribution to the Mathematical Theory of Epidemics” [3],

published in 1927. The SIR model, which was described in their scientific work, is now one the most popular models for modeling the spread of infectious diseases. The authors divided the whole population into three groups:

– S (t) – susceptible individuals who are not yet infected;

– I (t) - infected individuals capable of transmitting infection to susceptible people;

– R (t) - individuals who have been cured and immune to the disease therefore unable to contract the disease or transmit the infection.

This model is named SIR (Susceptible – Infected – Recovered), where the first letters of every group name had been used.

The transition of individuals from one group to another in this model is shown in Figure 1:

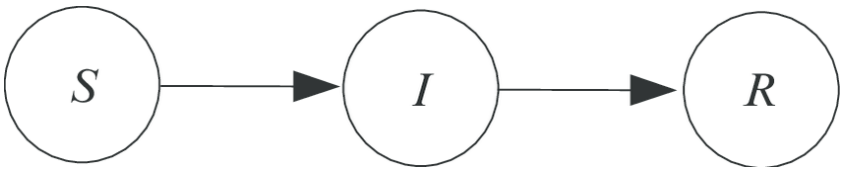


Fig. 1. The transition of individuals from one group to another in the SIR model

Assuming that population number is constant and equal to N = S (t) + I (t) + R (t), Kermak and McKendrick obtained the following equations to describe the epidemic:

$$\frac{dS}{dt} = -\beta I \frac{S}{N}, \quad (1)$$

$$\frac{dI}{dt} = \beta I \frac{S}{N} - \gamma I, \quad (2)$$

$$\frac{dR}{dt} = \gamma I, \quad (3)$$

where β - transmission probability;

1/γ - the average duration of the infectious period.

The SIR model assumes that all individuals in the population may equally be infected with the rate β. The first equation describes the dynamics of the number of individuals who are susceptible to the disease: an infected individual at a certain rate infects the susceptible individual. The second equation describes the dynamics of the number of infected individuals: the difference between the number of infected and the number of recovered individuals. The third equation describes the dynamics of recovery of the infected individual: at some speed the infected individual recovers.

Many modifications to the SIR model have been developed: SI model, which is successfully used to for modelling life-threatening epidemics of diseases (for example, herpes), SEIR model with an additional, "incubation" stage of the disease (for example, tuberculosis, measles), SIS model that is suitable for diseases without incubation period

and without lifelong immunity (for example, rhinoviruses or venereal diseases such as gonorrhea or chlamydia).

SEIR model. The SEIR model divides the whole population into four groups: Susceptible (S), Exposed (E), Infected (I), Recovered (R). Exposed group is a number of individuals who are already infected with the disease but not able to transmit it.

The transition of individuals from one group to another in this model is shown in Figure 1:

Fig. 1. The transition of individuals from one group to another in the SEIR model

The SEIR model system is made of four differential equations:

$$\frac{dS}{dt} = -\beta I \frac{S}{N}, \tag{4}$$

$$\frac{dE}{dt} = \beta I \frac{S}{N} - \alpha E, \tag{5}$$

$$\frac{dI}{dt} = \alpha E - \gamma I, \tag{6}$$

$$\frac{dR}{dt} = \gamma I, \tag{7}$$

where β - transmission probability;

α - the average duration of the infectious period ;

1/γ - the average duration of the infectious period.

This model has a disadvantage as it does not consider the possibility of being vaccinated. Our modification of the SEIR model contains both vaccination rate and vaccine efficacy as a way to decrease the number of susceptible and infected individuals:

$$\frac{dS}{dt} = -\beta I \frac{S}{N} - evS, \tag{8}$$

$$\frac{dE}{dt} = \beta I \frac{S}{N} - \alpha E, \tag{9}$$

$$\frac{dI}{dt} = \alpha E - \gamma I, \tag{10}$$

$$\frac{dR}{dt} = \gamma I + evS, \tag{11}$$

where e - vaccine efficacy;
v - vaccination rate.

A certain amount of susceptible will be vaccinated and move into the recovered class without becoming infected.

Conclusions. An analysis of SIR mathematical model of the spread of infectious diseases and its modifications is made in this article. In particular, SEIR model is considered and its features are described. An epidemiological characteristics of measles are studied. An appropriate model for modeling the spread of measles is selected and improved by adding two parameters: vaccination and vaccine efficacy.

REFERENCES:

1. Official site of the Public Institution of the Center of Public Health of the Ministry of Health of Ukraine [Electronic resource] https://phc.org.ua/news/dani-zakhvoryuvanosti-na-kir-10-16-zhovtnya-2019

2. World Health Organization [Electronic resource] https://www.who.int/news-room/fact-sheets/detail/measles

3. Kermack W.O., McKendrick A.G., A Contribution to the Mathematical Theory of Epidemics [Text] // Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character, 115 (772), 1927.

УДК 004.9

ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ДАНИХ ДЛЯ ДОСЛІДЖЕННЯ МОДЕЛІ ВИБОРЧОЇ КОМПАНІЇ

В.В. Гнатушенко, О.Г. Гончаров
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Дослідження аналітичних методів Microsoft SQL в галузі інтелектуального аналізу даних для створення моделі виборчої компанії. Для цього необхідно виділити підмножини вирішуваних завдань, провести порівняльний аналіз методів інтелектуального аналізу даних для вибраних типів завдань і на практичному прикладі визначити випадки, для яких більш привабливим є той чи інший метод.

Різноманіття методів для вирішення цього завдання ставить перед аналітиком питання вибору алгоритму, який найкращим чином придатний підходить під поставлені вимоги задачі [1, 2]. Так, у разі кластеризації, рекомендується використовувати ієрархічні методи, якщо заздалегідь невідомо число кластерів і потрібно отримати детальне уявлення про структуру даних. У свою чергу, ітеративні методи характеризуються більш високою стійкістю по відношенню до шумів і викидів, некоректного вибору метрики, включенню в аналіз незначущих атрибутів, але вимагають апріорної вказівки числа кластерів. У разі вибору методу класифікації необхідно брати до

уваги такі параметри, як точність, интерпретуємість результатів і, в залежності від випадку, масштабованість.

В рамках даної роботи було реалізовано практичне застосування методів ІАД в середовище MS SQL Server. Як об'єкт дослідження були взяті президентські праймеріз США 2016 року. Після проведення аналізу та формалізації предметної області визначені завдання дослідження (кластеризація та класифікація) і зроблена їх формальна постановка.

Проведена кластеризація громадян, які голосували на демократичних і республіканських праймеріз, тобто тих, хто в переважній більшості випадків відносить себе до відповідної партії. Кластеризація проводилася на двох незалежних вибірках: серед тих регіонів, де встигли пройти республіканські праймеріз, і тих, де пройшли демократичні. Для республіканців був складений портрет «типового» виборця, що віддає свій голос за Дональда Трампа. Однак, якщо поглянути на середні значення виділених ознак по всіх округах, можна встановити, що отриманий портрет збігається з портретом «середнього американця. Це говорить про те, що використані алгоритми не змогли виявити демографічних особливостей груп виборців, які віддають перевагу Дональду Трампу та могли б пояснити його успіх.

Проведено порівняльний аналіз двох алгоритмів, які засновані на методі максимізації очікувань і методі К-середніх. Було встановлено, що алгоритм максимізації очікувань в нашому випадку показує кращі результати, ніж алгоритм К-середніх. Отриманий результат можна пояснити тим, що алгоритм К-середніх має перевагу при роботі з відокремленими кластерами, але значно поступається алгоритму максимізації очікування при наявності їх перекриття, а саме цей випадок характеризує початковий набір даних.

Побудовано моделі класифікації. Досліджено вплив параметрів, що настроюються на чутливість одержуваних моделей і точність прогнозування. Завданням було підібрати найкращий алгоритм, який визначає ймовірність перемоги одного з демократів на своїх праймеріз. Були розглянуті методи дерева рішень, нейронна мережа і байесовский. Найвищу точність показала модель на основі нейронної мережі. Крім цього, вдалося підібрати такі параметри алгоритму, які підвищили її якість в порівнянні з настройками за замовчуванням. Отримана модель була використана для прогнозування результату демократичних праймеріз в штатах, де попередні голосування проходили з квітня по червень включно.

Висновки. Виконані всі етапи інтелектуального аналізу даних починаючи від аналізу предметної області і закінчуючи застосуванням моделі для реальної задачі прогнозування виборчої компанії.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Н.Б. Паклин, В.И.Орешков. Бизнес-аналитика: от данных к знаниям.– СПб: Питер, 2009.– 624с.

2. Замятин А.В. Интеллектуальный анализ данных Учебное пособие. - Томск: Издательский Дом Томского государственного университета, 2016. - 120 с. - ISBN 978-5-94621-531-2

УДК 004.491.22

БЕЗПЕКА ВИКОРИСТАННЯ ТЕХНОЛОГІЇ NFC

А.О. Кабанов, Ю.В. Ковальова
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Активне використання технології NFC вже стало повсякденною справою при оплаті товарів та послуг. Зі сторони маркетингу – це полегшення процедури оплати і зменшення витрат часу на цей процес, зі сторони фінансів – універсальний платіжний засіб, не потребуючий введення паролю, зі сторони технологій – використання новітніх розробок в повсякденному житті. А як щодо безпеки використання? Саме це питання є ключовим у розгляді розповсюдженої технології NFC.

NFC (Near Field Communication, «комунікація ближнього поля») – система бездротового високочастотного зв'язку малого радіусу дії, що дозволяє обмінюватися даними між пристроями, які перебувають на відстані близько 10 см. Це означає, що за допомогою NFC-гаджетів можна оплачувати покупки та послуги безконтактним способом, отримувати додаткову інформацію про товари і т.п.

За принципом дії NFC схожий з Bluetooth, але при підключенні до іншого пристрою NFC не потрібно витрачати багато часу на ідентифікацію, зв'язок встановлюється майже миттєво (за десяті частки секунди). Для передачі даних NFC використовує кодування з різним коефіцієнтом модуляції в залежності від швидкості передачі даних. При цьому пристрої NFC в змозі одночасно і отримувати, і передавати дані. Таким чином, вони можуть контролювати радіочастотне поле і виявляти невідповідність, якщо отриманий сигнал не відповідає переданому [1].

Технологія NFC в Україні використовується в трьох виглядах:

1. У вигляді мітки (коли до мітки підносять активний NFC-зчитувач, вона активується й передає інформацію зчитувачу. Здебільшого мітки доступні лише для зчитування).
2. У вигляді картки (дана технологія використовується в банківських платіжних картках та в проїзних у метрополітені).
3. У вигляді мобільного пристрою:
   - передавання даних з використанням NFC-чипа та Bluetooth або Wi-Fi модулів;
   - зчитування NFC міток для отримання додаткової інформації;
   - емуляція віртуальних карток для оплати товарів та послуг [2].

На сьогоднішній день в Україні функціонують дві системи електронних платежів з мобільних пристроїв: Google Pay (для мобільних пристроїв під керуванням операційною системою Android) та Apple Pay (для мобільних пристроїв під керуванням операційною системою iOS/iPadOS/WatchOS).

Успішне використання технології NFC призводить до її широкого застосування, наприклад:

– для контролю доступу в приміщення або на територію (великі об'єкти - заводи, готелі, готелі, аквапарки, публічні заходи - концерти, виставки, саміти, заходи з інформаційної безпеки, гірськолижні курорти, олімпіади та інші спортивні заходи);
– для доступу в автомобіль і його подальшого керування;
– для управління розумним будинком;
– для оплати транспорту (транспортні карти, електронні квитки);
– для відстеження переміщення товарів;
– для посвідчення особи.

Широке використання технології NFC передбачає широкий спектр можливостей для скоєння злочинів. З точки зору інформаційної безпеки основні слабкості і недоліки NFC пов'язані з тим, що стек протоколів NFC не передбачає криптографії при передачі. Стандарти зберігання даних в мітках і картах, а також їх емуляції - не передбачають криптографічного захисту при зберіганні. В реалізаціях багатьох карт, смарт-карт і їх емуляції застосовуються слабкі криптографічні алгоритми.

В NFC сервісах традиційно закладається надмірна довіра до інформації, що зберігається на картах і мітках, і в результаті чого фактично не виконується фільтрація даних. Раніше, коли пристрої для зчитування і запису інформації на карти були не так поширені, це можна було зрозуміти. Зараз в смартфонах з підтримкою NFC можна легко створити емуляцію карти і записати туди довільні дані (SQL-ін'єкції, виконання команд на стороні сервісу і т.п.).

Серед найбільш розповсюджених атак на NFC є:

– Прослуховування інформації при передачі по NFC;
– Несанкціоноване зчитування інформації з NFC пристроїв;
– Lock Attack (переведення емульованої карти (мітки) в режим тільки читання і блокування запису інформації зчитувачем);
– Time Attack (в разі якщо термін дії карти або послуг прописаний на самій карті, то можна замінити цю дату);
– Reply Attack (перехоплення інформації і багаторазове її повторення або застосування - дозволяє отримувати доступ до послуг, товарів від імені іншої особи);
– Clone attack (клонування NFC пристроїв);
– Relay attack (зловмисник використовує два NFC пристрої, одне з яких зчитує дані з пристрою жертви, передає дані на другий пристрій, а другий пристрій видає отримані дані зчитувачу і отримуємо послугу від імені жертви);
– Класичні атаки на серверну та інфраструктурну частину NFC сервісів [3].

Висновки. Використання технології NFC стало повсякденною справою в житті сучасної людини. Однак, з розвитком технологій та їх використання в мережі IoT (інтернет речей), розробники NFC-пристроїв та сервісів відкладають питання забезпечення безпеки даних сервісів на останній план, а згодом і взагалі не повертаються до нього. Перелічені типи атак на NFC-модуль стануть в нагоді розробникам NFC-пристроям для усунення вразливостей, а організаціям, які використовують такі прилади, нададуть освіченість в цьому питанні.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Near Field Communication (NFC) Ближняя бесконтактная связь – 2018 – [Електронний ресурс]. – Режим доступу https://bit.ly/2NcCv5C

2. Near Field Communication – 2019 – [Електронний ресурс]. – Режим доступу https://uk.wikipedia.org/wiki/Near_Field_Communication

3. NFC – 2016 – [Електронний ресурс]. – Режим доступу https://www.securitylab.ru /news/tags/NFC/

УДК 514.18

ПРОБЛЕМА АВТОМАТИЗАЦІЇ СТВОРЕННЯ ГРАФУ ДОРІГ ДЛЯ ГЕОМЕТРИЧНОГО МОДЕЛЮВАННЯ

С.Я. Кравців, О.М. Соболь
(Україна, Харків, Національний університет цивільного захисту України)

Робота присвячена автоматизації графу доріг для використання їх у комп’ютерних програмах для визначення областей покриття.

Ключові слова: граф доріг, геометричне моделювання, дискретні області, пожежно-рятувальний підрозділ.

S. Kravtsiv, O. Sobol. Problem of automation of the creation a graph of roads for geometric modeling. The work is devoted to the automation of the graph of roads for use in computer programs to determine the coverage areas/

Keywords: graph of roads, geometric modeling, discrete areas, fire and rescue unit.

С.Я. Кравцив, О.Н. Соболь. Проблема автоматизации создания графу дорог геометрического моделирования. Работа посвящена автоматизации графу дорог для использования в компьютерных программах для определения областей покрытия.

Ключевые слова: граф дорог, геометрическое моделирование, дискретные области, пожарно-спасательное подразделение.

Постановка проблеми. Одною із проблем для геометричного моделювання є збір необхідної інформації (масштаб карти, геолокації доріг та всіх елементів на карті, відомості про аварійні ділянки тощо), що необхідна для покриття області з дискретними елементами.

Для автоматичної побудови області покриття території в геометричному моделюванні досить важливим є те, що навігаційні карти необхідно будувати за допомогою графів доріг, що представляють собою цифрову векторну карту, що складаються з топологічно пов'язаних дуг і вузлів, розташування і властивості яких з заданою точністю та повнотою передають маршрути і організацію руху наземного транспорту.

Для розрахунку матриці відстані необхідно вибрати метрику або метод обчислення відстані між об'єктами в багатовимірному просторі. Найбільш часто використовуються такі метрики:

– Евкліда;
– сіті-блок (Манхеттен);
– Мінковського;
– метрика на основі кореляції Пірсона;
– метрика на основі кореляції Спірмена.

Елементи графа доріг призначені для використання в задачах з автоматизованої прокладці маршрутів між будь-якими заданими точками на графі або використання даних карт у програмних забезпечення для побудови області покриття (наприклад, зони виїзду пожежних рятувальних підрозділів).

Найчастіше використання навігаційних карт необхідне для побудови найкоротших маршрутів між точкою А та Б. Найкоротший маршрут можна знайти або за мінімальною довжиною шляху або за мінімальним часом проходження маршруту. При знаходженні мінімального шляху є можливість виключення деяких дуг, наприклад аварійних ділянок, з пошуку. Результати пошуку відображаються на карті у вигляді об'єкта – маршруту.

Використання графу доріг покажемо на прикладі покриття виїзду пожежно-рятувальних підрозділів в області їх обслуговування (рис. 1).

На рис. 1 наведено комп’ютерну реалізацію розробленого покриття опуклими багатокутниками заданої області з дискретними елементами [1], а саме, здійснено покриття Близнюківського району Харківської області районами обслуговування пожежно-яртувальних підрозділів (далі – ПРП), причому задачу було розв’язано з урахуванням існуючих ПРП.

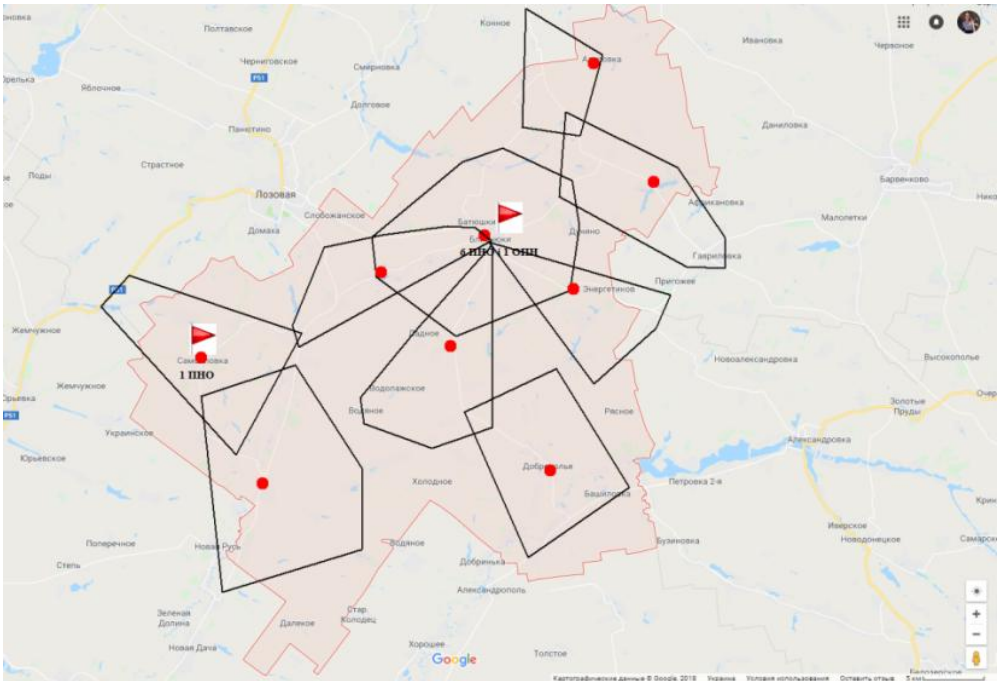


Рис. 1. Покриття Близнюківського району Харківської області районами обслуговування пожежно-рятувальних підрозділів

Кожен район обслуговування визначався виходячи з умови, що час реагування ПРП має не перевищувати 20 хв. [2, 3], причому розрахункова швидкість пожежно-рятувального автомобіля становила 30 км/год. Очевидно, що всі об'єкти підвищеної небезпеки та потенційно небезпечні об'єкти знаходяться в районах обслуговування центрів безпеки.

Висновки. Таким чином, маючи в доступі автоматизовані карти графу доріг з точними геоданими, можливо з меншою похибкою вирішувати задачі геометричного моделювання для покриття заданої області.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Комяк В.М. Моделювання покриття опуклими багатокутниками заданої області з дискретними елементами / В.М. Комяк, О.М. Соболь, С.Я. Кравців, І.А. Чуб // Вісник Херсонського національного технічного університету. – Херсон: ХНТУ, 2018. – № 3(66). – Т. 2. – С. 147–152.

2. ДБН 360-92**. Містобудування планування і забудова міських і сільських поселень [Електронний ресурс]. – Режим доступу: https://dnaop.com/html/29810/doc-%D0%94%D0%91%D0%9D_360-92__.

3. Постанова Кабінету Міністрів України від 27.11.2013 р. № 874 «Про затвердження критеріїв утворення державних пожежно-рятувальних підрозділів (частин) Оперативно-рятувальної служби цивільного захисту в адміністративно-територіальних одиницях та переліку суб'єктів господарювання, де утворюються такі підрозділи (частини)» [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/874-2013-%D0%BF#n10.

УДК 004.056.53

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ РОБОТИ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ

М.А. Лоян, С.І. Войцех
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. У сучасному цифровому світі безпека інформації стала надзвичайно важливою частиною процеса обробки, передачі та зберігання даних. В основі концепції безпеки інформації лежить безпека персональних комп'ютерів та мереж зв'язку між ними. В останні роки системи виявлення вторгнень (IDS) та системи профілактики вторгнень (IPS) життєво важливі для комп'ютерних мереж малих та середніх масштабів, в яких існує потреба в захисті конфіденційних даних. Для того, щоб забезпечити безпеку мережі, потрібно контролювати та аналізувати рух трафіку в ній.

Забезпечення безпеки інформації, особливо в комп'ютерних мережах малих масштабів, потребує суттєвих фінансових витрат. Тому актуальною задачею є розробка недорогих та практичних рішень.

Для реалізації поставленої задачі можуть бути використані малоенергетичні мікропроцесорні системи, які мають повноцінні безпекові характеристики і інструменти. Таким комплексом може стати одноплатний мікрокомп’ютер Raspberry Pi у зв'язці з програмним забезпеченням Snort IDS. Цей комплекс може бути розміщений в мережі і працювати як повноцінна система безпеки.

Raspberry Pi - одноплатний мікрокомп’ютер який має характеристики повноцінного комп'ютера при мінімальних розмірах.

IDS Snort є вільним програмним забезпеченням. Snort - це система, яка використовується для виявлення та запобігання вторгнень і може виконувати аналіз протоколів та аномалій в мережі на основі правил. Правила - основа Snort. Вони являються послідовність байтів, сигнатури нападів і даних інших типів, при виявленні яких, генерується попередження. Також, особливістю цієї системи є те, що користувачі можуть вільно додавати свої власні правила безпеки. За допомогою комплексу побудованого на базі Raspberry Pi і Snort можна зробити мережу більш безпечною аналізуючи мережевий трафік.

Snort працює наступним чином :

1. Відбувається прослуховування мережевого трафіку та прийняття пакетів.
2. Пакети аналізуються, із застосування правил до прийнятих даних. Процес застосування правил зводиться до пошуку в пакеті певних сигнатур, послідовностей, які вказані в правилах. Самі правила складаються з опису трафіку, сигнатури, яка шукається, опису загрози і опису реакції на виявлення.
3. При виявлення атаки до журналу подій заноситься попередження щодо загрози та дані сеансу зв’язку.

При побудові та проведенні дослідження ефективності системи виявлення вторгнень,використовувались наступня програмні та аппаратні засоби:

– коммутатор Cisco 2960x,
– мікрокомпьютер Raspberry Pi 3,
– ноутбук,
– серверний комп’ютер,
– операційні системи Debian, Ubuntu та Windows,
– програмний комплекс виявлення вторгнень IDS Snort,
– программа для роботи з мережевим трафіком hping3,
– програмні засоби для логування подій до журналу.

Дослідження продуктивності комплекса проводилося в локальній мережі. Згідно сценарію користувач атакував сервер у мережі пакетами даних за технологією SYN-flood. SYN-flood - один з різновидів мережевих атак типу "відмова від обслуговування", які полягають у відправці великої кількості SYN-запитів (запитів на підключення по протоколу TCP) в досить короткий термін. В процесі експерименту було проведено вимірювання продуктивності комплексу для різної кількості правил безпеки. В процесі експерименту вимірювалась кількість успішно прийнятих пакетів даних в системі для правил, використаних на момент нападу.

Було задіяно від 500 до 12500 правил при кожній атаці. Проведено 1 мільйон пакетних атак. Результати наведені на рисунку 1.

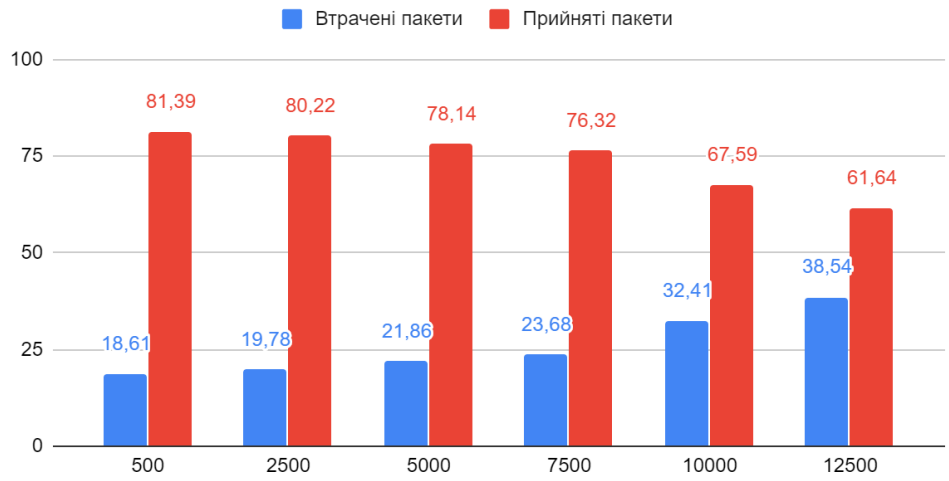


Рис. 1. Відносна кількість успішно прийнятих пакетів даних в системі від кількості правил задіяних на момент нападу

На момент атаки IDS почала працювати з 500 встановленими правилами, при цьому відносна кількість успішно прийнятих пакетів даних була на рівні 82%. При підвищенні кількості правил до 2500 і 5000 продуктивність знизилася на 1% та 3% відповідно. При задіянні 7500 правил продуктивність знизилася на 5%. Нарешті, з реалізацією 12500 правил продуктивність прийняття пакетів знизилась до 61%.

Висновки. Для комплекса, який досліджувався, кількість правил, які задіяні під час роботи, впливає на його продуктивність. При збільшенні кількості правил збільшується час обробки одного пакету даних, що призводить до втрати корисних робочих можливостей прийняття даних та зниження ефективності визначення можливих атак на мережу. Тому для конкретної конфігурації мережі потрібно оцінювати і визначати найвірогідніші атаки і формувати правила для системи на основі цієї оцінки. Намагання захиститися від всіх атак призводить до втрати значної кількості інформації, в тому числі і корисної.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Nabi Z., A $35 Firewall for the Developing World [Електронний ресурс] / Z. Nabi // arXiv. – 2014. – Режим доступу до ресурсу: https://arxiv.org /abs/1405.2517.
2. Ferdoush S. Wireless Sensor Network System Design using Raspberry Pi and Arduino for Environmental Monitoring Applications. The 9th International Conference on Future Networks and Communications / S. Ferdoush, X. Li. // Procedia Computer Science. – 2014. – №34. – С. 103–110.
3. Rolbin M. Early detection of network threats using Software Defined Network (SDN) and virtualization / M. Rolbin. – Ottawa, Canada: Carleton University, 2013. – 43 с.

УДК 004.056.53

СИСТЕМИ ВИЯВЛЕННЯ DOS-АТАК В ІНТЕРНЕТІ РЕЧЕЙ НА ОСНОВІ НЕЧІТКОЇ ЛОГІКИ

О.І.Луньова, О.В. Кручінін
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. Інтернет речей - це концепція комунікації об’єктів, які використовують технології для взаємодії між собою та з навколишнім середовищем. Також ця концепція передбачає виконання пристроями певних дій без втручання людини[1]. Ідея самостійної взаємодії фізичних об’єктів отримала стрімкий розвиток – вже сьогодні принципи Інтернету речей активно використовуються в медицині, промисловості, збройних силах. Разом із розвитком «розумних» систем значно погіршився стан інформаційної безпеки у сфері Інтернету речей.

Сьогодні крім небезпечних конфігурацій і стандартних налаштувань, гострою проблемою безпеки є DoS-атаки[2]. DoS-атака (Denial of Service) - вид зловмисної діяльності, що ставить собі за мету довести комп'ютерну систему до стану, коли обслуговування правомірних користувачів і коректне виконання функцій неможливе. Зловмисниками була продемонстрована можливість дистанційного керування кардіостимуляторами, дефібриляторами та інсуліновими помпами.

У результаті аналізу десяти популярних пристроїв Інтернету речей було виявлено вразливості, які спрощують реалізацію атак на відмову в обслуговуванні. Так, у 2016 році було здійснено масштабну атаку на інфраструктуру Dyn DNS, через що багато популярних сервісів, включаючи Amazon, CNN, Github, Netflix, Paypal, стали недоступними протягом декількох годин. У 2017 році вихідний код атаки було опубліковано, що дало змогу зловмисникам модифікувати його та вдосконалювати. Ця зростаюча загроза повинна мотивувати до розробки нових методів та систем виявлення та блокування трафіку атак.

У системах Інтернету речей, які побудовані за принципом «видавець - підписник», найбільшу критичність має брокер - компонент, що відповідає за прийом всіх повідомлень, їх фільтрацію, прийняття рішення про те, кому цікаві ці повідомлення, і, в кінцевому підсумку, за пересилку повідомлень всім підписаним клієнтам[3]. Саме на брокер здійснюються DoS-атаки задля неможливості обробки корисних запитів.

Аналіз досліджень. Дослідженням проблеми DoS-атак на Інтернет речей займалися такі компанії як Avast - «Avast Threat Landscape Report»[4], IBM - «The weaponization of IoT devices»[5], Google - «Security of IoT devices»[6]. Зазначені роботи створюють теоретичну базу результатів вивчення питання безпеки в Інтернеті речей, але не повністю розкривають всі аспекти даної проблеми. Більш детального аналізу потребують причини виникнення вразливості та можливостей для здійснення атак.

Постановка завдання. Актуальною задачею у сфері безпеки Інтернету речей є створення нових методів виявлення аномалій у мережі задля запобігання атак на відмову в обслуговуванні. Методи, що вже існують, схильні помилково класифікувати нормальний трафік, приймаючи його за аномальний, і не можуть адаптуватися до природи атак, що постійно розвивається. Варто також брати до уваги обмеженість ресурсів моделювання системи, наприклад: кількість робочих машин, з яких здійснюється атака; можливості операційної системи та швидкість роботи системи.

Для вирішення цієї задачі необхідно:

- проаналізувати наявні ресурси та елементну базу для оцінки можливостей системи;
- виконати аналіз методів виявлення мережевих аномалій, що існують;
- розробити систему виявлення DoS-атак з використанням принципів нечіткої логіки;
- створити базу здійснених атак для подальшого використання при моделюванні;
- виконати аналіз отриманих результатів та ефективності роботи даної моделі.

Матеріали дослідження. Одним із найбільш розповсюджених протоколів, за яким здійснюється взаємодія складових частин Інтернету речей, у тому числі і з брокером, є протокол MQTT. На сьогоднішній день саме особливості цього протоколу надають зловмисникам можливості для реалізації атак на відмову в

обслуговуванні. У новій версії протоколу, MQTT 5.0, що була опублікована на початку 2019 року, наведено перелік змін, які також варто розглядати у контексті можливості реалізації атак. Наприклад, надання ширших прав користувачам і можливість контролювати параметри та налаштування окремих пакетів клієнтськими додатками. Ці характеристики не тільки спрощують використання системи правомірними користувачами, а і створюють більш сприятливе середовище для здійснення атак, і саме вони стали ключовим об'єктом дослідження даної роботи.

Висновки. В ході роботи було проаналізовано слабкі сторони одного із найбільш розповсюджених протоколів, що використовується у сфері Інтернету речей. Також будо запропоновано основні етапи роботи. Кінцевою метою дослідження є створення системи аналізу активності в мережі Інтернету речей, з врахуванням нових стандартів протоколу, яка буде здатна відрізняти звичайний мережевий трафік від атаки на відмову в обслуговуванні.

ПЕРЕЛІК ПОСИЛАНЬ:

1. https://techno.nv.ua/popscience/chto-takoe-internet-veshchej-1326653.html
2. https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%D0%B0_%D0%B2%D0%B5%D1%89%D0%B5%D0%B9
3. https://h20195.www2.hpe.com/V2/getpdf.aspx/4AA6-3316ENW.pdf?
4. https://cdn2.hubspot.net/hubfs/486579/Avast_Threat_Landscape_Report_2019.pdf
5. https://www.ibm.com/downloads/cas/6MLEALKV
6. https://cloud.google.com/iot/docs/concepts/device-security

УДК 651.3:518.6

ВИКОРИСТАННЯ ТРИФАКТОРНОЇ АБО ДВОФАКТОРНОЇ АУТЕНТИФІКАЦІЇ: ПЕРЕВАГИ І НЕДОЛІКИ, ВИБІР ОПТИМАЛЬНОГО ВАРІАНТУ

М.В. Маркіна
(Україна, Дніпро, Національний ТУ «Дніпровська політехніка»)

Постановка проблеми. З розвитком технологій дедалі частіше виникають загрози, які використовують вразливості двофакторної аутентифікації для доступу до критичної інформації. Тому, необхідно зрозуміти, які нові рішення можуть бути використані для захисту від подібних загроз (у тому числі перехід до трифакторної аутентифікації) та у яких випадках яке рішення є найбільш оптимальним.

Двофакторна аутентифікація. Метод 2FA (Two-Factor authentication) був придуманий як додатковий спосіб підтвердження власника аккаунта. Він заснований на двох з трьох способах аутентифікації:

– користувач щось знає (наприклад, пароль);

– користувач володіє унікальними рисами, які можна оцифрувати і порівняти (біометрична аутентифікація, наприклад, відбиток пальця);

– користувач щось має (наприклад якийсь девайс з унікальним ідентифікатором, ключ-карту, флешку з ключовим файлом, тощо).

За думкою експертів у галузі інформаційної безпеки, двофакторна аутентифікація різко знижує можливість крадіжки особистих даних онлайн, так як знання пароля жертви недостатньо для здійснення шахрайства. Тим не менш, двофакторні підходи аутентифікації залишаються уразливими для атак типу «фішинг» та «людина посередині».

На сьогоднішній день, найпопулярнішим методом 2FA є пароль користувача (користувач щось знає) та SMS з перевірочними кодами, що генеруються за технологією OTP (one time password) та відправляється на смартфон (користувач щось має). Код приходить кожен раз різний, тому вгадати його практично неможливо.

Однак чим складніше подолати захист технічними методами, тим легше буває це зробити за допомогою соціальної інженерії. Всі настільки впевнені в надійності 2FA, що використовують її для найвідповідальніших операцій - від авторизації в Google (що дозволяє доступ до пошти, хмарного сховища, контактів і всієї інформації, що зберігається в історії) до систем клієнт-банк.

Національний Інститут стандартів і технологій США (The National Institute of Standards and Technology, NIST) оприлюднив влітку 2016 року попередню версію майбутнього Digital Authentication Guideline (документа, який встановлює нові норми і правила щодо цифрових методів аутентифікації), у якому говориться, що механізм SMS OTP спочатку для аутентифікації не призначався і що використання SMS-повідомлень для двофакторної аутентифікації може бути «неприпустимим» і «небезпечним».

Повністю даний параграф виглядає так: «Якщо верифікація по зовнішньому каналу здійснюється за допомогою SMS-повідомлення в публічній мережі мобільного телефонного зв'язку, верифікатор повинен переконатися, що використовуваний попередньо зареєстрований телефонний номер дійсно асоціюється з бездротовою локальною мережею, а не з VoIP або іншим програмним сервісом. Після можлива відправка SMS-повідомлення на попередньо зареєстрований телефонний номер. Зміна попередньо зареєстрованого номера не повинна бути можливою без двофакторної аутентифікації в ході зміни. Використання SMS-повідомлень в аутентифікації по зовнішньому каналу неприпустимо, і не буде дозволятися в майбутніх версіях цього посібника».

Основні побоювання експертів Національного інституту стандартів і технологій зводяться до того, що номер телефону може бути прив'язаний до VoIP-сервісу, крім того, зловмисники можуть спробувати переконати постачальника

послуг в тому, що номер телефону змінився, і подібні махінації потрібно зробити неможливими.

Хоча документ рекомендує виробникам використовувати в своїх додатках токени і криптографічні ідентифікатори, автори поправок також відзначають, що «смартфон або інший мобільний пристрій завжди можуть бути вкрадені, або можуть тимчасово перебувати в руках іншої людини» – йдеться в документі NIST.

Вчені з Амстердамського університету Радхеш Крішнан Конотом (Radhesh Krishnan Konoth), Віктор ван дер Вен (Victor van der Veen) і Герберт Бос (Herbert Bos) продемонстрували атаку з використанням установки уразливого додатку через Google Play. Їм вдалося успішно обійти перевірку Google Bouncer і активувати додаток для перехоплення одноразових паролів.

Трифакторна аутентифікація. При використанні трифакторної аутентифікації використовуються усі три методи аутентифікації: користувач щось знає, користувач володіє унікальними рисами та користувач щось має. Таким чином, як правило, до методів, що найчастіше використовуються у двофакторній аутентифікації, додаються технології біометричної аутентифікації.

При цьому застосовується відповідне обладнання та програмне забезпечення, а витрати на його придбання і підтримку можуть відрізнятися в рази від витрат на забезпечення двофакторної аутентифікації.

Однак, варто розуміти - біометричні аутентифікатори не є абсолютно точними даними. Відбитки одного пальця можуть мати відмінності під впливом зовнішнього середовища, фізіологічного стану організму людини і т.п. Для успішного підтвердження цього аутентифікатора достатньо неповної відповідності відбитка еталону. Методи біометричної аутентифікації містять визначення ступеня ймовірності відповідності чинного аутентифікатора еталону, таким чином біометрія лише із заданою вірогідністю, завжди відмінної від 100%, визначає користувача, що передбачає як помилкові спрацьовування на порушника, так і можливість відмови в доступі реальному власнику. Що стосується біометричної аутентифікації і віддаленого доступу до ІС, то поки у сучасних технологій немає можливості передати по незахищених каналах достовірні дані - відбиток пальця або результат сканування сітківки ока, тобто ці технології більше підходять для використання в корпоративних мережах.

Висновки. Таким чином, можна сказати, що недолік двофакторної аутентифікації полягає в тому, шо зловмисник може підібрати пароль користувача і перехопити SMS-повідомлення зі згенерованим кодом (механізми, що зазвичай використовуються при двофакторній аутентифікації). Тобто для захисту від відповідних атак, офіцер безпеки (або відповідальна за інформаційну безпеку компанії особа) має контролювати додатки на відповідних пристроях, на які користувачі отримують SMS-повідомлення, перевіряти чи телефонний номер дійсно належить пристрою користувача і чи має доступ до пристрою тільки сам користувач. Альтернативним варіантом є уникнення зазначеного метода аутентифікації і змінення його на більш надійний (що теж треба довести). Плюси двофакторної аутентифікації полягають у більш простій реалізації (порівнюючи із трифакторною), меншою ціною реалізації та меншою ймовірністю помилки

першого роду. Відповідно, трифакторна аутентифікація є більш надійною з точки зору забезпечення конфіденційності інформації, але це рішення є більш складним і дорогим; при біометричній аутентифікації можливі помилки першого і другого роду, тому є деякий ризик для доступності. Крім того, біометричну аутентифікацію можна використовувати лише для аутентифікації користувачів на локальних пристроях або в корпоративній мережі – вона не підійде для авторизації користувачів на віддалених ресурсах. Отже, загалом двофакторна аутентифікація підійде для ресурсів, на яких зберігається менш чутлива, з точки зору конфіденційності, інформація та для віддалених ресурсів, а трифакторна – для локальних ресурсів, на яких знаходиться інформація з високим ступенем конфіденційності.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Левашов А. Многофакторная (двухфакторная) аутентификация [Електронний ресурс] / Александр Левашов – Режим доступу до ресурсу: http://www.tadviser.ru/a/144161.

2. Афанасьев А. Безопасность корпоративной сети: защита изнутри [Електронний ресурс] / Алексей Афанасьев // Intelligent Enterprise. – 2003. – Режим доступу до ресурсу: https://www.aladdin-rd.ru/company/pressroom/articles/bezopasnost_korporativnoj_seti_zasita_iznutri.

3. Обходим двухфакторную аутентификацию с помощью Modlishka [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://xakep.ru/2019/05/28/ .

4. Пилипенко О. Взуття, жувальна гумка або недопалки — тепер ваш додатковий пароль [Електронний ресурс] / Олег Пилипенко. – 2017. – Режим доступу до ресурсу: https://www.imena.ua/blog/new-verification-ways/.

УДК 004.94

ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ РОЗВ'ЯЗКУ ЗАДАЧІ КОМІВОЯЖЕРА

Т.В. Селівьорстова, В.М. Пеліпака
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Як відомо задача комівояжера є відомою у такому формулюванні. Дано кількість міст і вказано відстані між ними. Комівояжер повинен вийти з першого міста, відвідати по одному разу в певному порядку всі міста і повернутися в перше місто. Необхідно знайти такий порядок відвідування міст, щоб довжина замкнутого маршруту комівояжера була мінімальною.

Аналіз останніх публікацій та досліджень. Для розв'язку задачі комівояжера було розроблено ряд методів, зокрема метод Літтла (точний метод) та наближений метод розв'язання задачі комівояжера (метод найближчого міста). Проте, при збільшенні кількості міст, точний алгоритм демонструє дуже великий

час обчислень, а наближений надмірну похибку. Тому для розв'язання даної задачі доцільно використовувати методи обчислювального інтелекту, зокрема генетичний алгоритм.

Постановка завдання. Метою роботи є програмна реалізація та дослідження генетичного алгоритму для розв'язку задачі комівояжера. Вивчення особливостей реалізації кросовера при реалізації генетичного алгоритму для розв'язання задачі комівояжера.

Матеріали дослідження. Значення функції пристосованості повинне відповідати відстані, що проходить комівояжер відповідно до шляху, що представляє хромосома. Оскільки це значення повинне бути мінімальним, то кінцева формула функції пристосованості j-й хромосоми часто виглядає в такий спосіб:

$$f_j = d_{\max} \cdot 1{,}1 - d_j ,$$

де $d_{\max}$ – довжина максимального маршруту в поточній популяції;

d_j – довжина маршруту, що представляє j-у хромосому.

Значення цієї функції чим більше, тим краще. Існує чотири основних варіанти подання маршруту комівояжера у вигляді хромосоми: сусідське, порядкове, шляхове й матричне. Оскільки класичні оператори схрещування й мутації для них, як правило, незастосовні, кожне із цих уявлень мають власні «генетичні» оператори, всі вони дуже сильно розрізняються. Що порядкове представлення маршруту дозволяє безперешкодно використовувати класичний оператор кросоверу, не проджуючі при цьому не валідні маршрути та петлі.Будь-які два маршрути в порядковому поданні, розрізані в будь-якій позиції й склеєні разом, породять два нащадки, кожний з яких буде валідним маршрутом.

Висновки. В ході виконання роботи виконано програмну реалізацію та дослідження генетичного алгоритму для розв'язку задачі комівояжера. Вивченні особливості реалізації оператора кросовера та мутації при реалізації генетичного алгоритму для розв'язання задачі комівояжера.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Белоусов А. И., Ткачев С. Б. «Дискретная математика». – М.: Изд-во МГТУ им.
Н. Э. Баумана, 2002. – 744 стр.

2. Кормен Т., Лейзерсон Ч., Ривест «Алгоритмы: построение и анализ». – М.: МЦНМО, 2000. – 960 стр.

3. Гладков Л.А. Генетические алгоритмы / Л.А. Гладков, В.В. Курейчик, В.М. Курейчик. – М : Физматлит, 2006 г. – 402 с.

4. Емельянов В.В. Теория и практика эволюционного моделирования/ В.В. Емельянов, В.В. Курейчик, В.М. Курейчик. – М : Физматлит, 2003 г. –431 с.

5. Батищев Д.И. Генетические алгоритмы решения экстремальных задач: учеб. пособие / Д.И. Батищев. – Воронеж: ВГТУ, 1995. – 69 с.

УДК 004.921

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ WEBGL ДЛЯ СТВОРЕННЯ ПРОТОТИПУ КОНСТРУКТОРА ГРАФІЧНИХ ВЕБСАЙТІВ

Т.В. Селівьорстова, А.В. Рєзнік
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Наявність яскравого та функціонального сайту підприємства або проекта вже стає стандартом функціонування сучасної економіки, які характеризується гострою конкуренцією. Яка в свою чергу вимагає від керівництва компаній постійної модернізації бізнес-процесів підприємства, використання інноваційних технологій. Отже використання новітніх технологій Інтернет-маркетингу сприяє підвищенню конкурентоспроможності підприємства, а для деяких ринків з часом може стати бар'єром виходу на ринок.

Аналіз останніх публікацій та досліджень. Серйозні веб-проекти краще створювати на CMS, що зарекомендовали себе, або движках, заточених під конкретні завдання. Це так, але в деяких ситуаціях такий підхід занадто довгий, дорогий та і трудовитратний. У противному випадку можна скористатися візуальними конструкторами. Це не панацея, є проекти, які неможливо реалізувати без участі дизайнерів і програмістів. Такі сервіси доцільно використати для: візуалізації ідеї, щоб згодом передати її розроблювачам; швидкого запуску невеликих і нескладних проектів; створення одностраничних сайтів під трафик з контекстної й таргетованої реклами; тестування ідеї, щоб зрозуміти чи варто витрачати час і гроші на розробку; некомерційних сайтів «для душі». Вибирати конструктор слід виходячи з конкретних завдань. Деякі відмінно справляються з Landing Page, інші – підходять для створення багатостраничних сайтів, треті добре просуваються в пошуку. Проте загальним недоліком конструкторів вебсайтів є досить скромні дизайнерські та графічні можливості, тому питання включення до конструктору вебсайтів WebGL є актуальними.

Постановка завдання. Провести дослідження можливостей WebGL для створення прототипу конструктора графічних вебсайтів.

Матеріали дослідження. WebGL (Web-based Graphics Library) – відкритий веб-стандарт, який використовується для візуалізації графіки в будь-якому підтримуваному веб-браузері і без необхідності підключення додаткових модулів. WebGL повністю інтегрований в усі веб-стандарти браузерів, що дозволяє використовувати апаратне прискорення для обробки зображень і ефектів на полотні веб-сторінки. Елементи WebGL можна вбудовувати разом з іншими елементами HTML. Вони можуть використовуватися в комбінації з іншими елементами сторінки. WebGL – це бібліотека для ПО, яка розширює функціональність мови JavaScript, і дозволяє йому створювати інтерактивну 3D графіку всередині сумісного з нею браузера. Даний код запускається за допомогою відеокарти. WebGL – це контекст елемента canvas HTML, що забезпечує API3D графіком без застосування плагінів. Даний стадарт

підтримується Google Chrome, Mozilla Firefox, Safari, Opera, Internet Explorer. По суті WebGL – це API або програмний інтерфейс, який заснований на архітектурі широко популярної відкритої бібліотеки OpenGL.

Висновки. В роботі виконано розробку прототипу конструктора графічних вебсайтів, який використовує WebGL. Показані переваги застосування WebGL при розробці дизайну графічних вебсайтів.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Мозгова Г. В. Сайт як інструмент інтернет-маркетингу / Г. В. Мозгова, Ю. А. Бойко. // Економіка і суспільство. – 2017. – №9. – С. 523–528.

2. Рудь А. WebGL – открытый веб-стандарт для визуализации графики [Електронний ресурс] / Алла Рудь // HyperHost. – 2016. – Режим доступу до ресурсу: https://hyperhost.ua/info/webgl-otkryityiy-veb-standart-dlya-vizualiza/.

УДК 004.921

ПРОГРАМНА РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ МОДЕЛЕЙ ЕПІДЕМІЇ ТА КЛІТИННОГО АВТОМАТА ДЛЯ МОДЕЛЮВАННЯ ПРОЦЕСУ ПОШИРЕННЯ ІНФОРМАЦІЇ

Т.В. Селівьорстова, А.А. Сазоновський, В.С. Жучков
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. Вивчення мереж поширення інформації є перспективним науковим напрямком. В економічному аспекті це цікаво маркетологам і бізнес-аналітикам. Інструменти аналізу дозволяють оцінити індивідуальні та групові переваги клієнтів, виявити тренди інтересів і надалі вирішувати важливі стратегічні завдання фірми.

Аналіз останніх публікацій та досліджень. Існує два типи моделей для моделювання процесу поширення інформації: моделі епідемії і моделі клітинного автомата. Моделі епідемії були сформульовані ще в 1921 р. а в 1965 році була сформульована модель Дале-Кендалла для опису поширення чуток. Даний клас моделей до сих пір застосовується при моделюванні процесу поширення інформації. Тому данні моделі не втрачають актуальність і їхня реалізація має методичну цінність.

Постановка завдання. Мета роботи полягає у програмній реалізації та дослідженні моделей епідемії та клітинного автомата для моделювання процесу поширення інформації.

Матеріали дослідження. Процес поширення інформації можна порівняти з епідемією. У зв'язку з відсутністю відстані між агентами, швидкості поширення інформації дуже високі (за умови, що інформація нова і викликає інтерес), поширення починається з малих груп і переходить на все більші групи, поки не досягне піку і не піде на спад. Але моделі епідемії мають недоліком: вони

відображають кількісне поширення інформації і не дозволяють отримати уявлення про канали розповсюдження.

Щоб більш точно відобразити реальний процес, була розглянута модель клітинного автомата. Клітинний автомат – це дискретна динамічна система, що включає однорідні клітини, з'єднані одна з одною. Інформаційне поле являє собою сітку довільної розмірності, кожна клітина якої в кожен момент часу може приймати одне значення із кінцевої множини станів, при цьому визначено правило переходу клітин з одного стану в інший. Автомат приймає рішення про прийняття новини, орієнтуючись на думку найближчих сусідів: якщо серед сусідів m підтримали інновацію і p – ймовірність прийняття новини (генерується в ході роботи моделі), тоді якщо $pm > R$, де R – фіксоване порогове значення, клітина приймає інновацію. Правила поширення новини: (1) спочатку кожна клітина зафарбована білим кольором, крім однієї чорної клітини (яка отримала новину); (2) біла клітина може змінити колір на чорний або залишитися білою (це означає прийняла новину чи залишилася в невіданні); (3) біла клітка змінює свій колір, якщо умова (1) виконується в моделі поширення дифузії (m – число чорних клітин, якщо $m < 3$, то p збільшується в 1,5 рази); (4) якщо осередок чорний і все осередки навколо тільки чорні або сірі, він змінює свій колір на сірий (новина застаріває); (5) якщо осередок сірий і осередки навколо тільки чорні або сірі, то він змінює свій колір на білий (інформація забута). Таке визначення не суперечить інформаційній мережі. Виходячи з цього можна вважати, що модель придатна для побудови соціального графа і моделювання соціальних процесів.

Висновки. В роботі проведено програмну реалізацію та дослідженні моделей епідемії та клітинного автомата для моделювання процесу поширення інформації. Визначені переваги та недоліки обраних підходів.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Емельянов В.В., Курейчик В.В., Курейчик В.М. Теория и практика эволюционного моделирования. М.: Физматлит, 2003. 432 с.

2. Робертс Ф.С. Дискретные математические модели с приложениями к социальным, биологическим и экологическим задачам. М.: Наука, 1986.

УДК 004.942

ДОСЛІДЖЕННЯ ТА ПРОГРАМНА РЕАЛІЗАЦІЯ ЕВОЛЮЦІЙНИХ ПРОЦЕСІВ

Т.В. Селівьорстова, Р.О. Хобот
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми. У сучасному економічному просторі чітко виражений міждисциплінарний аспект досліджень. В останні десятиліття економісти активно використовують методи і підходи, розроблені в інших науках. Математика, статистика, психологія, політологія, філософія, юриспруденція,

соціологія, об'єднані в єдиний комплекс, і в цій множині економіка виконує функцію інтегратора. Наприклад, одним із напрямів, що бурхливо розвивається, є економофізіка, яка використовує інструменти теоретичної фізики для вирішення економічних завдань. Перші роботи з економічної фізики з'явилися ще на початку XX століття, коли економісти почали застосовувати рівняння статистичної фізики для аналізу динаміки фінансових ринків, а також процесів, що відбуваються в суспільстві.

Аналіз останніх публікацій та досліджень.

Постановка завдання. Метою роботи є дослідження та програмна реалізація еволюційних процесів на прикладі економічної стратегічної гри «El Farol bar problem».

Матеріали дослідження. Еволюційна теорія ігор з'явилася як додаток математичної теорії ігор, яка не враховувала зміни в поведінці членів суспільства і не розглядала повторювані гри. Тому на допомогу економістам з еволюційної біології прийшла еволюційна теорія ігор, переваги якої пояснюються трьома фактами:

1) Еволюція, яка вивчається в даній теорії, необов'язково повинна бути біологічною еволюцією. Вона також може бути і культурною, тобто відображати зміни в нормах і переконаннях в часі.

2) Раціональні припущення, що лежать в основі еволюційної теорії ігор, у багатьох випадках більш підходять для моделювання соціальних систем, ніж припущення, що лежать в традиційній теорії ігор.

3) Еволюційна теорія ігор є динамічною теорією ігор, що знову ж таки вигідно відрізняє її від традиційної теорії ігор.

Однією і найпростіших моделей еволюційної теорії ігор є гра «El Farol bar problem», що часто застосовується при моделюванні економічних процесів і відноситься до підкласу ігор «Minority games». Найпростіший випадок такої гри складається з N непарного числа гравців, які вибирають один з двох варіантів можливих рішень протягом кожного раунду гри. Таким рішенням може бути, наприклад, покупка або продаж акцій, або інших активів. Гравець вважається виграв, якщо виявляється в меншості. І таким шляхом в результаті такої гри формується меншість гравців, яка завдяки своїй стратегії, вдаліше інших передбачає результат гри. Така гра також отримала назву задача бару «El Farol bar problem» і була вперше описана Вільямом Артуром в 1994 році. Різні моделі, засновані на іграх меншини, активно використовуються для аналізу фінансових ринків. Крім цього такі ігри дозволяють моделювати макроекономічні процеси.

Висновки. В ході виконання роботи було проведено дослідження динаміки еволюційних процесів на прикладі економічної стратегічної гри «El Farol bar problem».

ПЕРЕЛІК ПОСИЛАНЬ:

1. Alexander, J. McKenzie, Evolutionary Game Theory // The Stanford Encyclopedia of Philosophy. – 2009. [Электронный ресурс]. URL: http://plato.stanford.edu/entries/game-evolutionary/

2. Диксит А. Стратегические игры / А. Диксит, С. Скит, Д. Рейли., 2017. – 880 с.

УДК 004.9

ПРОЕКТУВАННЯ ТА ОПТИМІЗАЦІЯ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ ВХІДНОГО ТРАФІКУ СЕРВЕРА

Д.Е. Чернорот, І.С. Дмитрієва
(Україна, Дніпро, Національна металургійна академія України)

Постановка проблеми: У наш час, коли інтернет займає більшу частину сфер життя, неможливо уявити собі будь-яке діло (компанію, бізнес), яке не буде використовувати для виконання частини роботи інтернет. Зберігання даних, віддалена робота або, що зараз найбільше використовується у більшості різноманітної промисловості, сайти використовують певні ресурси, а саме сервери. За рахунок нашого темпу життя ми не маємо часу на те, щоб очікувати, доки ми отримаємо відповідь на наш запит на файл, чи доки відкриється веб-сторінка. Саме тому з технічного боку постає питання про те, як саме забезпечити швидкий відклик від сервера, при цьому зекономивши кошти на масштабуванні обчислювальних ресурсів?

Аналіз досліджень: Для найбільш вдалого розділення запитів до сервера найкраще використовувати балансування трафіку. Буває декілька видів балансування вхідного трафіку на сервер. Але спочатку необхідно розуміти, що балансування має задовольняти певні умови[1]:

– балансування повинно задовольняти вимогам справедливості - будь-який запит, що прийшов на сервер у нашому кластері, повинен бути обслужений, а не кинутий без відповіді;

– балансування повинно задовольняти вимогам передбачуваності - ми повинні заздалегідь чітко розуміти, який з алгоритмів балансування в певній ситуації ми зможемо використовувати;

– балансування повинно бути здатним до масштабування - при виявленні різкого збільшення трафіку (а, відповідно, і навантаження) система повинна забезпечувати стабільну роботу нашого сервісу;

– скорочення часу відповіді - при використанні балансування ми повинні в підсумку отримати скорочення часу виконання запиту до сервера, тобто, як тільки запит приходить в нашу систему, ми повинні якомога швидше його обслужити, дати на нього відповідь;

– ефективність - ми повинні забезпечити таку роботу балансування, при якій всі сервера, що знаходяться в нашому кластері, працювали б приблизно однаково, навантаження було рівномірним.

За географічною ознакою балансування умовно можемо розділити на два види:

– локальна - якщо наші сервери розміщені всередині одного дата-центру;

– глобальна - наші сервера розкидані по різних дата-центрам.

Локальне балансування можна застосовувати на канальному рівні (з використанням окремого балансувальника і без нього), на мережевому рівні або на транспортному рівні. Дані способи найбільш поширені при локальної балансуванню.

Балансування на канальному рівні виконується за рахунок наступного: ми беремо і навішуємо на якийсь спеціалізований інтерфейс всіх наших серверів однуй ту ж IP-адресу нашого ресурсу, на який будуть приходити запити, і з якого будуть йти відповіді. Але на ARP-запит з цієї IP-адреси сервера не повинні відповідати. І ми навішуємо таку ж IP-адресу на наш балансувальник, відповідно, на нього будуть приходити запити, і відправлятися відповіді з нього, і він же буде відповідати на ARP запити. Таким чином, отримуючи запит від клієнта, наш балансувальник вибирає за певним алгоритмом той чи інший сервер, який буде обробляти цей запит, підміняє destination MAC і відправляє його на обробку на даний сервер. Сервер його у себе обробляє, і, так як ми не робили підміну заголовків на мережевому рівні, то безпосередньо, минаючи балансувальник, сервер відразу відповідає клієнту через наш шлюз [2].

Реалізувати подібне балансування без окремого балансувальника (і в підсумку скоротити витрати) можна наступним чином: нам необхідно перетворити вхідний unicast запит в broadcast, або в multicast. Робиться це в такий спосіб: всі сервера повинні на ARP запит відповідати однією і тою самою MAC-адресою, тобто, це може бути або неіснуючий MAC-адресу, або якийсь мультикастового. Або ми можемо навісити цей мультикастового MAC-адресу на наш шлюз. Відповідно, запит приходить на наш ресурс, і шлюз його просто розмножує до всіх серверів, таким чином запити надходять на всі сервери одночасно, і кожен сервер повинен сам розуміти, чи повинен він відповідати на запит чи ні.

Балансування на мережевому рівні має досить схожий механізм з балансуванням на канальному рівні. Єдина відмінність в тому, що в даному випадку при отриманні вхідного запиту наш балансувальник підміняє destination IP, переправляючи його на той сервер, який буде обробляти запит. Сервер отримує його, обробляє і повинен передати його назад балансувальник, щоб той виконав зворотну заміну[3].

Балансування на транспортному рівні. Тут дуже тонка грань, яка відрізняє балансування на мережевому від балансування на транспортному рівні. Для простоти скажемо, що в даному виді балансування використовуються при балансуванні навантаження вхідні порти джерела і адресата.

В балансуванні DNS часто застосовують так званий алгоритм Round Robin. Це найпростіший механізм балансування, за допомогою якого можна балансувати будь-які системи, в яких доступ до сервісу відбувається по імені. Саме цей метод у зв’язці з іншими видами балансування буде розглянуто в рамках дипломної роботи, виходячи з наявних ресурсів. Суть даного методу в наступному: на DNS сервер додається кілька A-записів з різними IP-адресами всіх наших серверів, і сервер сам буде в циклічному порядку видавати ці адреси. Тобто, перший запит

отримає перший сервер, другий запит - другий сервер, третій запит - третій сервер і так далі.

Наступний алгоритм – це алгоритм проксіювання. Суть даного алгоритму полягає в тому, що в якості балансувальника застосовується так званий «розумний» проксі. Тобто якщо балансувальник отримує запит до нашого ресурсу, він аналізує заголовки прикладного рівня і, відповідно, він може розуміти до якого ресурсу прийшов запит на наш балансувальник, і направити запит на той чи інший сервер, на якому цей ресурс міститься. Також при отриманні даного запиту балансувальник може додавати в заголовки HTTP, наприклад, інформацію про те, з якого IP прийшов клієнт. Корисно це для того, щоб сервер знав, куди його потім згодом відправляти, і з ким він працює. Виконавши запит сервер передає його назад на балансувальник, балансувальник виконує необхідні маніпуляції з новими заголовками або третього рівня, або сьомого рівня і віддає його клієнту [1].

Redirect запитів. Redirect запитів має досить обмежене застосування – застосовується, в основному, для глобального балансування, і, зокрема, для HTTP він добре застосується. Суть його полягає в тому, що ми отримуємо запит від клієнта на наш балансувальник, балансувальник відповідає йому редіректом на наш сервер, на якому містяться ресурси. Наприклад, отримуючи запит по HTTP, балансувальник відповідає йому у відповідь кодом 302 move temporary із зазначенням адреси того сервера, на який далі буде ходити наш клієнт.

Балансування на базі Anycast. Цей алгоритм балансування не вимагає ніякого налаштування з боку клієнта, і суть його полягає в наступному: ми з різних географічних ділянок анонсуємо один і той же префікс мережі. Таким чином, кожен запит клієнта маршрутизується на найближчий до нього сервер, який буде його обробляти.

Цілі: Необхідно, використовуючи методи балансування, розробити систему, що буде з найменшими вкладеннями балансувати трафік и витримувати велике навантаження з боку запитів клієнтів.

Висновки: З найменшими витратами можливо балансувати трафік за допомогою алгоритму RoundRobin, що використовується при балансуванні DNS. Цей алгоритм є найбільш вдалим з огляду на масштабування. За допомогою налаштування параметрів ми зможемо досягти оптимального відклику від серверів при отриманні запиту. При цьому для масштабування не буде необхідності правити повторно конфігурації на серверах, буде досить додати новий запис з IP адресою додаткового сервера и таким чином ми зможемо збільшити ресурси нашого кластеру у самий короткий термін без простою усього кластера. Таким чином ми досягнемо також зменшення ризику відмови нашого кластеру, тобто відмовостійкість наших обчислювальних потужностей збільшиться на певний відсоток.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Y. Hu, R. Blake, D. Emerson. An optimal migration algorithm for dynamic load balancing. Concurrency: Practice and Experience. – V.10(6). – 1998. P. 467–483.

2. E.G. Ignatenko, V.I. Bessarab, V.V. Turupalov, The algorithm of adaptive load balancing in cluster systems, Modeling and information technologies, Kyiv: IPME G.E. Puhova NAN of Ukraine, № 58, 2010, pp. 142-150.

3. Hisao Kameda, Lie Li, Chonggun Kim, Yongbing Zhang. Optimal Load Balancing in Distributed Computer Systems. Springer, Verlag London Limited.- London. - 1997. - P. 238

УДК 004.942

ПОРІВНЯЛЬНИЙ АНАЛІЗ ФРАКТАЛЬНОСТІ МІНЛИВОСТІ СТОКУ ДНІПРА ПО ГІДРОМЕТРИЧНИМ ДАНИМ ТА КЕРНАМ

А.Г. Станчиц, О.І. Михальов, Т.В. Селівьорстова
(Україна, Дніпро, Національна металургійна академія України)

Відновлення багатовікових рядів гідрологічних відомостей по річці Дніпро представляє складну задачу і особливо в формі хронологічно безперервного ряду з інтервалами часу не більше року. Існують різні способи відновлення даних, наприклад, по даним гідрометеостанцій, відкладанням у водоймам, за письмових джерелтощо. Але найбільш реальним шляхом відновлення відомостей за минулі століття можуть служити природні пам'ятки, створені природою в органічному світі, мінеральних відкладеннях, льодовиках. Процес накопичення опадів у водоймах залежить від багатьох факторів, але провідними є кліматичні. Під впливом періодичності їх змін формуються сезонні різновиди відкладень, які характеризують річні цикли накопичення опадів (досліджуються по кернам) і дають можливість датувати з річними інтервалами часу.[1]

Дані стоку Дніпра відновлювались за відомостями про відкладення солі в Сакському озері. У цих відкладах помічається сезонна закономірність: взимку відкладаються світлі мули, а влітку - більш темні, насичені продуктами водної та вітрової ерозії. Розглянуто дані за період з 1818 року по 1872, так як з 1873 року через видобуток солі, споруди додаткових каналів тощо, явно знизилося надходження в озеро продуктів водної ерозії.[1]

Таблиця 1

Фрагмент даних відкладення солей у Сакському озері за 10 років[1]

Рік	Відкладення (мм)
1818	1,3
1819	3,0
1820	3,0
1821	2,0
1822	1,6
1823	1,5
1824	1,6
1825	1,6
1826	0,9
1827	1,8
1828	1,4

Розрахунок показника проводився відповідно формули (1):

$$\frac{\overline{\quad}}{\quad\quad\quad} \qquad (1)$$

У якості величини R(n) виступає розмах накопичених відхилень n значень від середнього значення ряду даних. Стандартне відхилення ряду представлено величиною S(n). Показник Херста розраховується як відношення різниці натуральних логарифмів математичного сподівання і константи, в нашому випадку = 0,33, до натурального логарифму проміжку часу ряду. Так як показник Херста рахується для проміжку 1818 – 1872, величина проміжку часу становитиме 55.

Використавши R/S-метод для знаходження показника Херста[2], був проведений фрактальний аналіз даних по відкладенню солей у Сакському озері (див. фрагмент у табл.1) за період з 1818 р. по 1872 р., в результаті якого було отримано значення показника Херста H=0.7894, яке підтверджує фрактальність (природну самоподібність) стоку Дніпра. При цьому закономірність отриманого результату полягає у практично повному збігу значень показників Херста щодо розливу р. Нил (H≈0.73), що отримано ще самим Гарольдом Ервіном Херстом[2], а також з результатом, враховуючи усі похибки, отриманим при обробці даних стоку Дніпра, які встановлені завдяки водоміру H=0.7227.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Швец Г.И. Многовековая изменчивость стока Днепра. – Л.: Гидрометиоиздат, 1978. – 84 с.

2. ХерстГ. Нил: Общееописаниерекииииспользованияеевод = Hurst H. The Nile: A General Account of the River and the Utilization of Its Waters. London, 1952 / Гарольд

РОЗДІЛ 4

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ОСВІТИ, НАУКИ І ВИРОБНИЦТВА

UDC 651.3:518.5

ANALYSIS AND RESEARCH OF EXISTING ERASMUS + PROJECTS FOR STUDENTS

M. Tytarenko, L. Kabak, O.A. Yakunin
(Ukraine, Dnipro, NTU «Dnipro Polytechnic»)

Nowadays, the analysis of existing exchange programs is an important task for students. The importance of this work is that it makes it possible to find the necessary program for students, based on their knowledge and capabilities. There are a huge number of exchange programs, but it is very important to find the program on which student will be the best candidate and where student have the right to participate.

Erasmus+ stands for European Community Action Scheme for the Mobility of University Students. It's a Higher Education exchange program for students, teachers and institutions, run in the UK by the British Council. Basically, it's a chance for universities and students across 33 countries to mingle, learn new skills, expand their horizons, study for 1-2 semesters or doing an internship abroad in another country for a period of at least 2 months and maximum 12 months per cycle of studies.

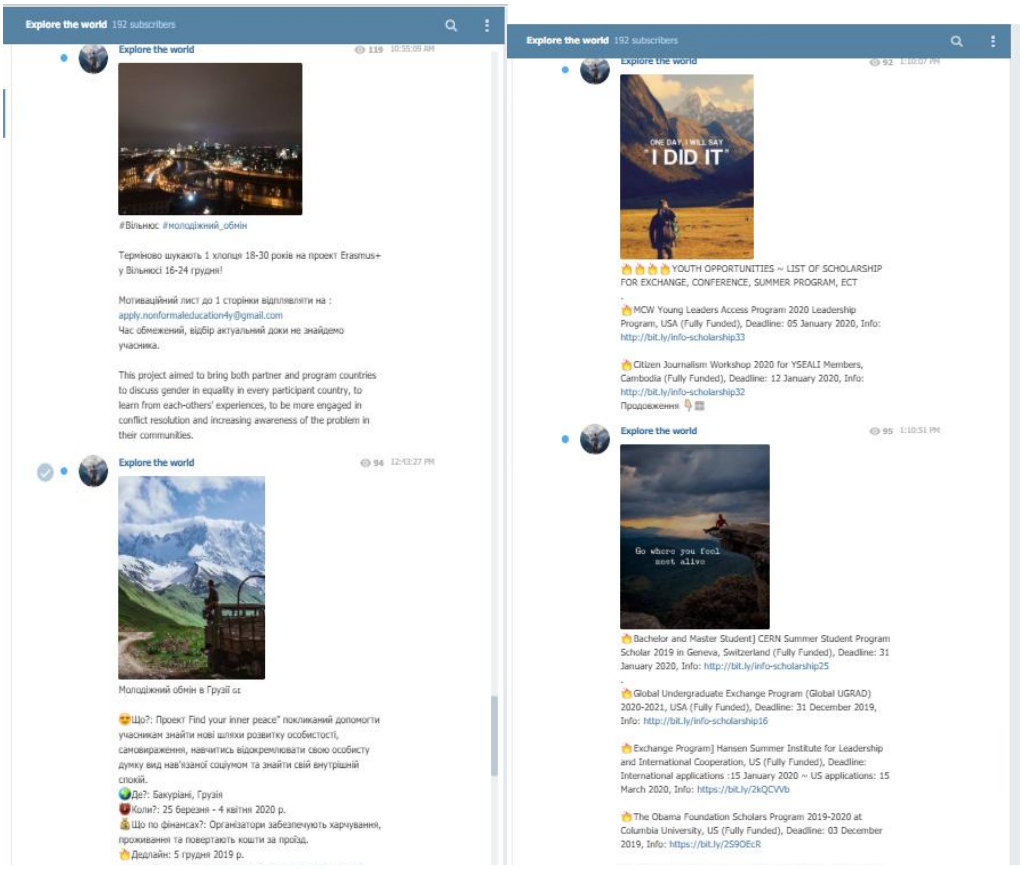
Erasmus+ has opportunities for people of all ages, helping them develop and share knowledge and experience at institutions and organizations in different countries.

There are 5 types of programs:

– Study abroad with Erasmus+
– Erasmus Mundus Joint Master Degrees
– Youth Exchanges
– Teach abroad with Erasmus+
– Traineeships with Erasmus+

I am currently working on a channel to collect and release the latest student programs. The goal is to release posts with different terms and conditions for the programs. This allows students with various knowledge, specialties, and skills to find a suitable program. Moreover, this creates the conditions for the most effective selection of programs for the student.

Every day I post the latest information and opportunities for students. Here is an example of my channel, which in the future will be in the form of an automated web application with a database of new programs.



In this example, only the prospect of the development of this topic is indicated.

The following is an example of a web application that is planned to be developed in the future. In order to select an individual program for each student.

There will be 5 main tabs with categories of basic student search: Scholarship, Country, Online course, Intership-job, Short course. This will speed up the search and help the work of both the international department and students. Herein lies the basic concept.

УПРАВЛІННЯ КЛЮЧОВИМИ ПРОЦЕДУРАМИ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ВИЩОЇ ОСВІТИ

Нєнно І. М.
(Україна, Одеса, Одеський національний університет ім. І.І. Мечникова)

Забезпечення якості в системі вищої освіти в Україні, починаючи з підписання у Вірменії угоди щодо впровадження Керівництв European Standards and Guidelines, (тут і надалі, - ESG [1]) відбувається шляхом оновлення системи управління освітою. Європейські процедури забезпечення якості спираються на експертний підхід та прагнення досконалості. Зміст цих процедур не є перманентним. Він зароджується Керівництвами ESG , проте набуває постійної трансформації у прикладному аспекті. Такий еволюційний підхід повністю відповідає концепції Life Long Learning. Метою цього дослідження є формування прикладних засад дотримання та забезпечення якості вищої освіти відповідно до кращих європейських практик та Керівництв ESG.

Ключові процедури забезпечення якості вищої освіти. Відповідно до закону попиту та пропозиції на ринку, досягнення точки рівноваги відбувається у разі відповідності якості та ціни товару, що пропонується для платоспроможного споживання. В інших випадках створюється дефіцит та залишок. Неможливо уявити якісну освіту, яка не сформована якісними дослідженнями, новими науковими результатами, апробованим інструментарієм прогнозування. Таким чином, необхідність інституційної акредитації є цілком обґрунтованою та необхідною. Її наявність підтверджує статус закладу вищої освіти (тут і надалі, - ЗВО) з позицій відповідальності, професіоналізму, наявності науково-педагогічної синергії та сталості розвитку закладу. Другою ключовою процедурою, відповідно до практики роботи міжнародних акредитаційних агенцій, зокрема німецької агенції ASIIN [2] є програмна акредитація. В програмній акредитації існує формат рецензування. Основні критерії забезпечення якості наведені у таблиці 1.

Змістовна частина управління в контексті реалізації процедур забезпечення якості вищої освіти. Управління якістю вищої освіти розглянемо із використання функціонального підходу, а саме реалізації базових функцій менеджменту: планування, організація, регулювання і контроль. У випадку імплементації програми вищої освіти в Україні прийняття рішень та делегування відбувається відповідно Міністерством освіти і науки України (тут і надалі, - МОН), Національним Агентством із забезпечення якості вищої освіти (тут і надалі Національне Агентство), ЗВО, кафедрою менеджменту та інновацій (тут і надалі, - КМІ)

Таблиця 1

Базові функції менеджменту в управління освітою

Критерій	Планування	Організація	Регулювання	Контроль
Легальне право на акредитацію	МОН ЗВО	ЗВО КМІ	Національне Агентство ЗВО	Національне Агентство
Створення програми та формування кваліфікаційного профілю	МОН	ЗВО КМІ	ЗВО	ЗВО
Структура навчального плану, робоче навантаження та мобільність	МОН	ЗВО КМІ	ЗВО	ЗВО
Вимоги до вступу	МОН	ЗВО	-	МОН
Навчальна та учбова підтримка	КМІ	КМІ	КМІ	КМІ
Екзаменування	КМІ	КМІ	КМІ	КМІ
Управління персоналом	ЗВО	КМІ	КМІ	ЗВО
Матеріальне забезпечення	МОН ЗВО	ЗВО	МОН	МОН
Фінансові ресурси	МОН	КМІ	ЗВО	ЗВО
Управління якістю	МОН	ЗВО КМІ	-	МОН
Прозорість	ЗВО	ЗВО	ЗВО	-

**розроблено авторкою.*

Програмна акредитація включає спілкування з основними групами стейкхолдерів системи вищої освіти - студентами, персоналом, роботодавцями та керівництвом університету з метою отримання відповідних висновків та рекомендацій. Поряд із спостереженнями по кожному з критеріїв оцінки програми застосовується наступна шкала оцінки: не досягнуто (-1 бал); частково досягнуто (1 бал); значною мірою досягнуто (2 бали); повністю досягнуто (3 бали); не застосовується на цій стадії вирівнювання (0 балів).

Експерти ставили під сумнів, що можливе виконання програми на рівні магістра для студентів з інших спеціальностей бакалаврату, не загрожуючи рівню освіти. Водночас небажаним є відштовхувати студентів різнорідними вимогами до вступу. Вони рекомендують уважно стежити за ситуацією та у разі необхідності запропонувати курси відновлення.

У технічному плані правила зарахування студентів є чіткими і прозорими. Існує система визнання академічних кваліфікацій за межами університету. Шляхом опитування студентів виявляється поточний рівень викладання та навчання в університеті. Враховується новизна літератури, стилі навчання, наявність модулів на іноземній мові. Рекомендовано залучати до викладання іноземних запрошених лекторів.

Важливе існування прозорої системи експертизи, яка містить можливості для відшкодування та компенсаційних заходів для студентів-інвалідів. Під час аудиту

були згадані «тести з множинним вибором», які повинні використовуватися виключно на курсі магістрів за думкою однолітків.

Після закінчення навчальної програми студенти спочатку захищають дипломну роботу на кафедрі, а потім - на другому етапі до екзаменаційної комісії. Оскільки програма тільки почалася, рівень дипломної роботи не може бути вивчений. Кафедра забезпечує наукового керівника студентам за магістерську роботу.

Відповідно до Звіту про самооцінку, персонал та академічні консультанти відповідають за перевірку та запобігання плагіату та інших форм неетичної поведінки. Використовується університетський програмний інструментарій плагіату. Вся відповідна інформація про курс подається на початку семестру.

Рекомендовано використання довідника для персоналу, для того, щоб колеги мали особисте враження щодо кваліфікаційного профілю / напрямів досліджень. Цінним є, що під час засідань Вченої ради факультету та кафедри співробітники регулярно збираються для обговорення структури програми та її необхідності в модернізації. Фінансові ресурси частково надходять з державного фінансування (надаються протягом кожного фінансового року), а також з оплати за навчання та інших доходів університету. Неефективним є те, що плата за навчання переходить до центрального університетського фонду. Отже, факультет не зацікавлений у збільшенні кількості студентів.

Рекомендовано систематизувати інструменти забезпечення якості, такі як опитування задоволеності студентів / викладачів (тощо), які на сьогоднішній день здійснюються на індивідуальній та добровільній основі. Експерти наголошують на необхідності не тільки збирати дані, а й систематично аналізувати їх для покращення програми, що розглядається. З точки зору закриття циклу забезпечення якості, надзвичайно важливо не тільки контактувати із зацікавленими сторонами за їхні думки та пропозиції, але й дати їм детальну відповідь про те, як їх зворотній зв'язок вписується в модернізацію програми. Виявляється доступність документації під час аудиту та можливість знайти відповідну інформацію на веб-сайті університету.

Напрямки запровадження проактивного підходу у надання якісних послуг вищої освіти. На думку авторки, запровадження проактивного підходу можливе через використання “bottom-up approach”. Бо, як видно з таблиці 1, найвища оцінка по критеріях втілюється у разі наявності можливостей делегування базових функцій менеджменту кафедрі менеджменту та інновацій. Тобто, ефективність підвищується, якщо рівень делегування повноважень зростає. На рівні кафедри відбувається формування профілю компетенцій та результатів навчання.

Практика роботи авторки експертом Національного агентства з забезпечення якості вищої освіти дає можливість розповсюдження кращих практик по критеріях акредитації освітніх програм (вибірково), які вже впроваджені в акредитованих Національним Агентством ЗВО України.

1. Критерій «Проектування та цілі освітньої програми». Зв’язок цілей освітньої програми із місією та стратегією ЗВО. Визначення того наскільки вони

привабливі для студентів, чи можуть бути реалізовані при опануванні ними навчального плану та досягненні програмних результатів навчання. Стратегія може спиратися на цілі сталого розвитку ООН, за взірцем багатьох європейських ЗВО.

2. Критерій «Доступ до освітньої програми та визнання результатів навчання». Орієнтація на стейкхолдерів. Чітке визначення того, хто є цільовою аудиторією в Україні та за кордоном. Для цього для набору студентів активно використовувати SMM, власне телебачення, прес-служби та медіа служби. На youtube-каналі університету представити презентації та відеоматеріали програми, українською та англійською.

3. Критерій «Людські ресурси». Запрошення роботодавців у якості штатних викладачів та залучення бізнес-спікерів, практиків. Введення дуальної освіти. Стимулювання розвитку викладацької майстерності. Впровадження положення про стимулювання публікаційної активності учасників наукового і освітнього процесу, яким забезпечується «Премія за публікаційну активність» за наявність публікацій в журналах, що індексуються в міжнародних наукометричних базах Scopus та Web of Science.

4. Критерій «Навчання і викладання за освітньою програмою». З точки зору інтернаціоналізації ОП. необхідні угоди про наявність погодження навчальних планів та програм, що дає можливість визнання результатів навчання, отриманих під час академічної мобільності в Європейському просторі по програмах подвійного диплому.

5. Критерій «Прозорість та публічність». Використання електронного архіву відкритого доступу, електронного журналу успішності студентів, що дає можливість оперативного доступу до даних успішності. Розробка і використання мобільного додатку розкладу.

6. Критерій «Освітнє середовище та матеріальні ресурси». Взаємодія з науковою бібліотекою з точки зору наявності інформаційних ресурсів за програмою, а саме надання можливості електронного доступу до фондів і електронних ресурсів 27 бібліотек ЗВО Francofoni, доступу до спеціалізованих іншомовних баз даних ECONLIT та Wilson Business Abstracts, Statista. Заснування науково-технологічного парку по прикладу «Синергія», співзасновником якого є ХНУРЕ.

ПЕРЕЛІК ПОСИЛАНЬ:

1. Стандарти і рекомендації щодо забезпечення якості в Європейському просторі вищої освіти (ESG). – К.: ТОВ “ЦС”, 2015. – 32 с.

2. Система забезпечення якості вищої освіти в Україні: розвиток на засадах європейських стандартів та рекомендацій : посібник / В. Кухарський, О. Осередчук, М. Мазуркевич та ін.; за ред. В. Кухарського, О. Осередчук. – Львів : ЛНУ імені Івана Франка, 2018. – 408с.

УДК 378.014.6(477)

ПРОДОВЖЕННЯ НАПРАЦЮВАНЬ QUAERE ПІСЛЯ ОФІЦІЙНОГО ЗАВЕРШЕННЯ ПРОЕКТУ: ПЕРСОНАЛЬНИЙ ВИМІР

Лиман Ігор Ігорович
(Україна, Бердянськ, Бердянський державний педагогічний університет)

Впродовж 2016-2018 рр. у рамках проекту Еразмус+ КА2 «QUAERE: Система забезпечення якості освіти в Україні: розвиток на основі європейських стандартів та рекомендацій» було напрацьовано багато того, що має бути продовжене і стає у нагоді при забезпеченні якості вищої освіти в Україні.

Саме керуючись цими міркуваннями, у жовтні 2018 – червні 2019 р. я взяв участь у Міжнародному проекті «Формування мережі експертів із забезпечення якості вищої освіти» (Інститут вищої освіти Національної академії педагогічних наук України, Центр досліджень вищої освіти (Чеська Республіка), МОН України). В рамках цього проекту пройшов тренінг для тренерів (жовтень 2018 р.), он-лайн тестування, провів тренінги для експертів у Вінницькому національному медичному університеті ім. М.І. Пирогова (21.03.2019 р.) і Бердянському державному педагогічному університеті (27.03.2019 р.). В рамках обох тренінгів окремий пункт програми формулювався як «Досвід проекту QUAERE». Як мінімум 21 учасник тренінгу у Бердянському державному педагогічному університеті згодом успішно пройшов он-лайн тестування ІВО НАПН України.

Одним із співорганізаторів і лекторів проекту «Формування мережі експертів із забезпечення якості вищої освіти» був Тарас Фініков, який кілька разів виступав із доповідями і на проекті QUAERE. На початку червня 2019 р. від запрошених Тарасом Фініковим для презентації представниць Національного агентства із забезпечення якості вищої освіти – учасниць попередніх фаз проекту «Інноваційний університет та лідерство» в рамках фінальної, звітної зустрічі IV фази цього проекту пролунала пропозиція подавати документи на конкурс з відбору членів галузевих експертних рад Національного агентства із забезпечення якості вищої освіти.

Це була можливість продовжити попередні активності щодо участі в процесах реформування системи забезпечення якості вищої освіти в Україні і на практиці застосовувати досвід, набутий в рамках QUAERE. Тож я подав заяву-анкету. Хоча на той момент нормативними документами не були чітко визначені ні статус галузевих експертних рад, ні повноваження їх членів.

Будучи відібраним до складу членів галузевої експертної ради, рішенням Національного агентства від 1.10.2019 р. я став головою ГЕР 03 («Гуманітарні науки»). Відтоді значна, якщо не більша, частина робочого (і не тільки) часу стала уходити саме на організацію роботи ГЕР. Впродовж 7 місяців ГЕР 03 має розглянути 127 справ, тобто в середньому приймати 2 рішення кожні 3 дні.

Ні члени галузевих експертних рад, ні керівництво Національного агентства на початку роботи не усвідомлювали обсягів організаційних та інших викликів, з

якими довелось зіткнутись. Значущість цих викликів стала всім зрозуміла вже в грудні 2019 року. Тож Тарас Фініков із його Міжнародним фондом досліджень освітньої політики виступив ініціатором організації разом із Національним агентством низки тренінгів «Акредитація освітніх програм за новою моделлю: сутність, перші уроки, шляхи вдосконалення» для представники ректоратів, керівників структурних підрозділів закладів вищої освіти, ґарантів освітніх програм і експертів Національного агентства. Для проведення цих тренінгів були запрошені екс-заступник міністра освіти та науки України Юрій Рашкевич, заступник голови Національного агентства забезпечення якості вищої освіти Наталія Стукало, член Національного агентства, провідний експерт з питань академічної доброчесності Артем Артюхов, голова ГЕР 07 Артем Бардась і голова ГЕР 03. Таким чином, коло учасників тренінгів включало фактично всі щаблі, задіяні в процесі акредитації освітніх програм. У грудні 2019 р. такі тренінги були проведенні на базі Національного технічного університету «Дніпровська політехніка» (м. Дніпро) і Прикарпатського національного університету імені Василя Стефаника (м. Івано-Франківськ) – в останньому ми з Артемом Бардасем брали участь дистанційно, спілкуючись завдяки використанню відеоконференцзв'язку сервера Cisco WebEx. У січні 2020 р. тренінг вже очно був проведений на базі Черкаського національного університету імені Богдана Хмельницького.

Цілком логічно, що на тих тренінгах я та Артем Бадась розповідали саме про роботу галузевих експертних рад. Втім, неузгодженості у регламентації цієї роботи, складності комунікації галузевих експертних рад з іншими учасниками акредитаційного процесу зробили актуальною організацію семінарів вже виключно для голів галузевих експертних рад та їхніх заступників. Організацію цих семінарів наприкінці зими – на початку весни 2020 р. знов взяли на себе Тарас Фініков із його Міжнародним фондом досліджень освітньої політики та Національне агентство. Тут вже заявлене в програмі коло спікерів від галузевих експертних рад включило голову ГЕР 07 Артема Бардася, голову ГЕР 12 Ірину Удовик і голову ГЕР 03.

Наскільки ефективною буде подальша робота у сфері забезпечення якості вищої освіти, наскільки її реалії будуть відповідати задекларованій високій меті – покаже час.

В рамках же проблематики продовження напрацювань QUAERE після офіційного завершення проекту надзвичайно важливо і показово, що на кожному з перелічених вище етапів я мав щастя співпрацювати з іншими учасниками команди QUAERE, які були широко представлені і серед лекторів і учасників проекту «Формування мережі експертів із забезпечення якості вищої освіти», і увійшли до складу членів Національного агентства із забезпечення якості вищої освіти, голів і членів галузевих експертних рад, експертів Національного агентства. Такий персональний вимір є запорукою того, що досвід QUAERE використовується і продовжить використовуватись при забезпеченні якості вищої освіти в Україні.

ВІДОМОСТІ ПРО АВТОРІВ

Алексєєв Ростислав Сергійович – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Алексєєв Михайло Олександрович – д.т.н., професор, декан факультету інформаційних технологій, НТУ «Дніпровська політехніка», м. Дніпро

Бєлих Ігор Анатолійович – магістр кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Бойко Олег Олександрович – асистент кафедри автоматизації та приладобудування НТУ «Дніпровська політехніка», м. Дніпро

Бура Владислав Олександрович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Войцех Сергій Іванович – старший викладач кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Воскобойник Євген Костянтинович – асистент кафедри автоматизації та приладобудування НТУ «Дніпровська політехніка», м. Дніпро

Гнатушенко Вікторія Володимирівна – д.т.н., професор, завідувач кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Гненний Ігор Алексійович – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Гончаров Олександр Геннадійович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Гула Жанна Володимирівна – студентка кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Гуліна Ірина Григорівна – к.т.н., доцент, доцент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Даценко Максим Дмитрович – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Діденко Катерина Олександрівна – студентка кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Дмитрієва Ірина Сергіївна – к.т.н., доцент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Дорош Наталія Леонідівна – к.т.н., доцент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Жучков Владислав – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Захарченко Олексій Володимирович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Зеленський Олексій Андрійович – магістр кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Іщук Павло Олександрович – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Кабак Леонід Віталійович – к.т.н., доцент, доцент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Кабанов Артем Олександрович – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Камишов Олег Андріович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Ковальова Юлія Вікторівна – асистент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Кравців Світлана Ярославівна – викладач-методист Науково-методичного центру навчальних закладів сфери цивільного захисту, Національний університет цивільного захисту України, м. Харків
Кручінін Олександр Володимирович – старший викладач кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Левдик Ірина Андріївна – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Літвінов Дмитро Олександрович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Ліфшиц Олексій – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Лиман Ігор Ігорович – д. іст. н., професор, координатор міжнародної діяльності Бердянського державного педагогічного університету, м. Бердянськ
Лоян Максим Анатолійович – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Луньова Олена Ігорівна – студентка кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Маркіна Марія Володимирівна – студентка кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Мартиненко Андрій Анатолійович – старший викладач кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Машурка Сергый Володимирович – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Мещеряков Леонід Іванович – д.т.н., професор кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Мілінчук Юлія Анатоліївна – асистент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро
Михальов Олександр Ілліч – д.т.н., професор, завідувач кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Мороз Борис Іванович – д.т.н., професор кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Нападайло Максим – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Нєнно Ірина Михайлівна – д.е.н., професор кафедри менеджменту та інновацій

Одеського національного університету ім. І.І. Мечникова, експерт Національного Агентства з забезпечення якості вищої освіти, м. Одеса

Овєчкін Артем Вадимович – студент кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Островська Катерина Юріївна – к.т.н., доцент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Очкур Сергій Олегович – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Пеліпака Владіслав студент – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Погрібняк Ірина Олегівна – студентка спеціальності автоматизації та комп'ютерно-інтегровані технології, кафедри Автоматизації та приладобудування, група 151-19м-1 НТУ «Дніпровська політехніка», м. Дніпро

Проценко Станіслав Миколайович – старший викладач кафедри автоматизації та приладобудування НТУ «Дніпровська політехніка», м. Дніпро

Рєзнік Артур – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Родна Катерина Станіславівна – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Сазоновський Андрій – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Селівьорстова Тетяна Віталіївна – к.т.н., доцент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Славінський Дмитро Вячеславович – асистент кафедри автоматизації та приладобудування НТУ «Дніпровська політехніка», м. Дніпро

Сліпко Денис – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Смолянов Сергій Олександрович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Соболь Олександр Миколайович – д. т. н., старший науковий співробітник, професор кафедри управління та організація діяльності у сфері цивільного захисту Національного університетк цивільного захисту України, м. Харків

Сподинець Олексій Анатолійович – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Станчиц Антон Георгійович – асистент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Станчиц Георгій Юрійович – старший викладач кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро

Титаренко Марія – студентка кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

Тимофєєв Дмитро Сергійович – старший викладач кафедри безпеки інформації та телекомунікацій НТУ «Дніпровська політехніка», м. Дніпро

Ткачов Віктор Васильович – д.т.н., професор, завідувач кафедри автоматизації та приладобудування НТУ «Дніпровська політехніка», м. Дніпро

Фененко Тетяна Михайлівна – старший викладач кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Харь Альона Тарасівна – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Хобот Руслан – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Хоменко Олександр Михайлович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Чащин Владислав – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Чернорот Данило Едуардович – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Шаптала Тарас – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Шевцова Ольга Сергіївна – асистент кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Шульга Жанна – магістр кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро
Юхименко Олександр – студент кафедри інформаційних технологій і систем Національної металургійної академії України, м. Дніпро
Якунін Анатолій Олександрович – д.т.н., професор кафедри програмного забезпечення комп'ютерних систем НТУ «Дніпровська політехніка», м. Дніпро

ЗМІСТ

Наукове видання

ПРОБЛЕМИ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ОСВІТІ, НАУЦІ ТА ПРОМИСЛОВОСТІ

XIV міжнародна конференція

Збірник наукових праць
№ 4

Відповідальний за випуск І.М. Удовик

Видано в редакції авторів публікацій.

Підписано до друку 03.10.2020. Формат 30х42/4.
Папір офсетний. Ризографія. Ум. друк. арк. 8,4.
Обл.-вид. арк. 8,4. Тираж 20 пр. Зам. №

Підготовлено до друку та видрукувано
в НТУ «Дніпровська політехніка»
Свідоцтво про внесення до Державного реєстру ДК № 1842 від 11.06.2004.

49005, м. Дніпро, просп. Д. Яворницького, 19.