

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ**

**МАТЕРІАЛИ
XXVI МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ
РАДІОЕЛЕКТРОНІКА
ТА МОЛОДЬ
У ХХІ СТОЛІТТІ**



Том 5

Харків 2022

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
РАДІОЕЛЕКТРОНІКИ

МАТЕРІАЛИ 26-го МІЖНАРОДНОГО
МОЛОДІЖНОГО ФОРУМУ

**«РАДІОЕЛЕКТРОНІКА ТА МОЛОДЬ
У ХХІ СТОЛІТТІ»**

20 – 22 квітня 2022 р.

Том 5

КОНФЕРЕНЦІЯ

«Комп'ютерні системи і мережі управління та обробки даних»

Харків 2021

УДК 004.032.2+004.7.032.2](06)

26-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. матеріалів форуму. Т. 5. – Харків: ХНУРЕ. 2022. – 46с.

В збірник включені матеріали 26-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Видання підготовлено факультетом комп'ютерної інженерії та управління
Харківського національного університету радіоелектроніки

61166 Україна, Харків, просп. Науки, 14

тел./факс: (057) 7021397

E-mail: mref21@nure.ua

© Харківський
національний університет
радіоелектроніки (ХНУРЕ), 2022

Програмний комітет конференції

Ляшенко О.С.	к.т.н., декан факультету КІУ
Чумаченко С.В.	д.т.н., зав. каф. АПОТ
Литвинова С.І.	д.т.н., проф. каф. АПОТ
Халімов Г.З.	д.т.н, зав. каф. БІТ
Северінов О.В.	к.т.н., доц. каф. БІТ
Коваленко А.А.	д.т.н., зав. каф. ЕОМ
Вовк М.О.	д.т.н., проф. каф. ЕОМ
Руденко О.Г.	д.т.н, зав. каф. КІТС

УДК 004.3+004.4]:519.713:007.52

ФІЗИЧНИЙ КОМП'ЮТІНГ

УДК 681.326

МІКРОКОНТРОЛЕРНА СИСТЕМА ДЛЯ ПІДРАХУНКУ КІЛЬКОСТІ ЛЮДЕЙ У ПРИМІЩЕННІ НА БАЗІ ARDUINO UNO

Братищенко М.Р.

Науковий керівник – к.т.н., доц. Кулак Е. М.

Харківський національний університет радіоелектроніки, каф. АПОТ,
м. Харків, Україна

тел. +38(099) 791-07-25, e-mail: mykyta.bratyshchenko@nure.ua.

The store visitor counter (counter of people, traffic, flow, attendance, etc.) is a device that can automatically count the number of visitors entering / exiting. This technology is used to determine the number of visitors, the dynamics of visits, frequency. The role of these technologies is focused around measuring visitor behaviour, allowing you to define and analyze behavioural metrics, calculate conversion rates, evaluate/plan marketing activities. The counting system is installed at the entrance to the premises usually. Various technologies are used in people counting devices, such as infrared rays, computer vision and thermal imaging.

Так склалося, що пандемія Covid-19 тільки набирає оберти. На сьогоднішній день дотримання соціальної дистанції має особливу роль у протиепідемічних заходах (так само як і дезінфекція шкіри рук або носіння масок). Задля того, щоб у громадських закладах було можливо дотримуватись соціальної дистанції та не допустити розповсюдження вірусу, можна відстежувати кількість людей, які перебувають у приміщенні, а також ураховувати такі події, як вхід та вихід людини з приміщення.

Також варто розуміти, що у кожного приміщення є своя площа, а отже і допустима кількість відвідувачів закладу буде різною. Тому для мікроконтролерної системи необхідно встановити ліміт відвідувачів, і якщо його буде перевищено, то система повинна повідомити про це, подавши звуковий сигнал. Таку систему доцільно розмістити на вході у такі приміщення, як: кафе, магазин, зал кінотеатру, музей, театр тощо. Це дасть змогу як і запобігти накопичуванню великої кількості людей у громадському закладі, так і мінімізувати розповсюдження вірусу.

За основу пристрою було вирішено обрати мікроконтролер Arduino Uno R3, який заснований на чіпі Atmel ATmega328. Також буде використано 2 інфрачервоні датчики руху, LCD дисплей та активний п'єзоелектричний зумер (спрацює у тому випадку, коли буде переповнення приміщення людьми).

Що стосується принципу роботи пристрою, то його можна описати наступним чином. Коли буде подано живлення на пристрій спочатку спрацює зумер, подавши короткий звук. На дисплеї з'явиться привітальне повідомлення. Це все свідчить про те, що наш пристрій готовий до роботи. Якщо людина буде входити до приміщення, то вона перетне спочатку перший інфрачервоний датчик, а потім другий. В результаті цієї події на

выводах цих двох датчиків буде сформовано високий рівень сигналу та збільшиться програмний лічильник відвідувачів, після чого на дисплеї можна буде побачити повідомлення з оновленою кількістю людей у кімнаті. При перетині людиною спочатку другого інфрачервоного датчику, а потім першого, програмний лічильник зменшиться, та на дисплеї буде відображено кількість людей у кімнаті, враховуючи нещодавній вихід однієї людини з неї.

Може трапитись така ситуація, коли після чергового входу людини кількість відвідувачів досягне максимально допустимого значення для цього приміщення (варто зауважити, що це значення встановлюється у процесі прошивки плати, тому якщо виникне необхідність змінити це число, плату потрібно перепрограмувати, під'єднавши до комп'ютера за допомогою USB кабелю). В такому разі на дисплеї відобразиться кількість людей та повідомлення про те, що досягнуто ліміт відвідувачів та кімната заповнена достатньою кількістю людей. Але якщо до кімнати зайде ще одна людина (перетнувши інфрачервоні датчики), то це спричинить таку послідовність подій: в результаті перевірки на те, що оновлена кількість людей перевищує максимальне допустиме значення, буде подано високий рівень сигналу на вивід п'єзоелектричного зумера, що приведе до його спрацювання. Звуковий сигнал буде лунає до тих пір, поки кількість відвідувачів не стане меншою ніж максимальне значення або дорівнюватиме йому. На LCD дисплеї буде виведено актуальну кількість людей та попереджувальне повідомлення про те, що кімната переповнена.

Для пристрою передбачено два режими роботи: живлення від електромережі та від акумуляторів.

Серед переваг пристрою можна відокремити невелику вартість компонентів та їх доступність, простоту у збірці та налаштування. Якщо порівнювати пристрій з іншими лічильниками відвідувачів, то він буде значно дешевший.

Щодо недоліків, то розроблений лічильник повинен бути розміщений десь на рівні поясу людини. З цього випливає те, що зона чутливості інфрачервоних датчиків та спрацювання пристрою при вході чи виході людини обмежена. Також готовий пристрій потребує постійне та безперебійне живлення. Проте незважаючи на все це, пристрій можна вдосконалити у майбутньому.

Список використаної літератури:

1. Порівняння систем підрахунку людей у закладі: огляд технологій та їх оцінка [Електронний ресурс] / Режим доступу: https://www.watcom.ru/blog/tekhnologii/obzor_sistem_podscheta_posetitelej_vidy_i_sravnenie_oczenka/

2. Arduino и Raspberry Pi в проектах Internet of Things. - СПб.: БХВ-Петербург, 2016. – 320 с.

3. Arduino Uno: схема, опис та підключення пристрою [Електронний ресурс] / Режим доступу: <https://arduinomaster.ru/platy-arduino/plata-arduino-uno/>

УДК:004.7.032.2

СИСТЕМА КЕРУВАННЯ ЖИВЛЕННЯМ ЕЛЕКТРОПРИЛАДІВ

Михальчук М.О.

Науковий керівник – к. т. н., доцент Рахліс Д.Ю.

Харківський національний університет радіоелектроніки, каф. АПОТ,

м. Харків, Україна

тел. +38(067) 122-79-28, e-mail: maksym.mykhalchuk@nure.ua.

The Internet of Things is a variety of devices, ranging from the simplest, for example, devices to control lighting in the house, “smart” household sockets that can be controlled using a phone application, ending with more complex ones – a soil monitoring system. In this article the appliance power control system were proposed based on microcontroller ESP. For the data exchange in the proposed system the MQTT Protocol was proposed to use.

На сьогодні систем, за допомогою яких можна керувати живленням електроприладів, або, інакше кажучи, «розумних» розеток дуже велика кількість. Спочатку це були пристрої, за допомогою, яких можна було вмикати та вимикати електроживлення підключеного об'єкта через смартфон. Але, дуже швидко, в гонитві за покупцями, виробники почали розширювати функціонал. З простої системи розетка перетворилась на багатофункціональний пристрій, за допомогою якого можна встановлювати таймер роботи, вимірювати споживання електроенергії, зберігати його історію, а також встановлювати графік роботи підключеного пристрою [1].

Основним компонентом кожної системи, з світу Internet of Things, є мікроконтролер. Він виконує функцію мозку, тобто обробляє отримані дані та всі команди користувача. Для розумної розетки можна використати будь який мікроконтролер. Наприклад, ESP8266, який підтримує стандарт IEEE 802.11 b/g/n Wi-Fi, має до 4 МБайт пам'яті, та над мале енергоспоживання, або його вдосконалену версію – ESP32, яка отримала більше вбудованої пам'яті (32 МБайт), а також Bluetooth v4.2 [2].

Другий важливий компонент таких систем – це реле напруги, яке контролює подачу напруги на прилад. Також воно слідкує за напругою і в разі виходу її за встановлені межі (160-260 Вольт), спрацює захист, який знеструмить підключений пристрій. За допомогою цих двох компонентів вже можна зробити найпростішу розумну розетку, якою можна буде керувати за допомогою телефону, але щоб збільшити можливості та безпечність системи, треба додати ще декілька компонентів.

По-перше, додаймо датчик сили струму, щоб реалізувати захист від перевищення сили струму, при короткому замиканні, а також його показники будуть використані для розрахунку потужності, яку споживає електроприлад. По-друге, треба додати датчик температури. Адже всі електронні компоненти нагріваються при роботі і цей датчик буде

повідомляти контролер про перегрів розетки. По-третє, для реалізації таймера та розкладу роботи підключеного приладу, використаємо датчик реального часу, який буде відправляти дані на контролер.

На рисунку 1 проказано принцип передачі даних в запропонованій системі керування живленням електроприладів на основі використання протоколу MQTT (Message Queue Telemetry Transport).

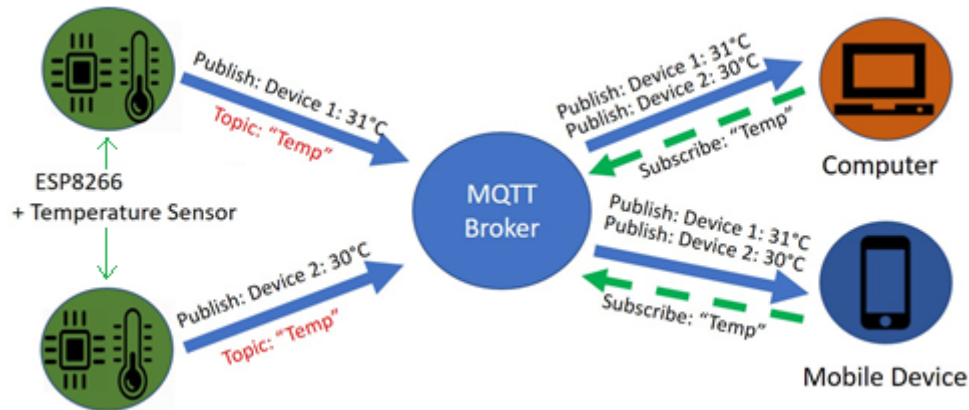


Рисунок 1 – Принцип передачі даних в системі «розумна» розетка

MQTT – це легкий, компактний та відкритий протокол обміну даними, створений для передачі даних на віддалених локаціях, де потрібен невеликий розмір коду та є обмеження щодо пропускної спроможності каналу [3]. При цьому контролер розумної розетки виступає в ролі видавця (Publisher), він отримує дані з датчиків, які до нього підключені, обробляє та відправляє їх через MQTT протокол на сервер (Broker). У свою чергу, сервер відправляє дані своєму передплатнику (Subscribe), у ролі якого зазвичай виступає телефон чи комп'ютер.

Отже, у цій статті запропоновано систему керування живленням електроприладів та розглянуто принцип взаємодії всіх компонентів на базі протоколу MQTT. Варто зауважити, що компоненти такої системи є цілком доступні, а функціонал можна легко розшири шляхом додавання будь-яких датчиків, тощо.

Список використаних джерел:

1. Karanchery S. Smart Power Socket using Internet of Things / S. Karanchery, N. Rakesh // 2020 International Conference on Inventive Computation Technologies (ICICT), Coimbatore, India, 26-28 Feb. 2020. – с. 1060-1064.

2. Babiuch M. Using the ESP32 Microcontroller for Data Processing / Marek Babiuch, Petr Foltyněk, Pavel Smutný // 20th International Carpathian Control Conference (ICCC), Poland, 26-29 May 2019. – с.88-93.

3. MQTT: відкритий мережевий протокол та його значення в IoT. – Режим доступу: https://www.hwlibre.com/uk/MQTT/#_Todo_sobre_MQTT. – Дата доступу: 23.02.22.

УДК 004.946:[004.6+004.7]

ВІРТУАЛЬНИЙ КОМП'ЮТІНГ

УДК 004.8

СИСТЕМА КЕРУВАННЯ АУДІО ТА МУЛЬТИМЕДІА «РОЗУМНОГО» БУДИНКУ НА ОСНОВІ ПЛАТИ ARDUINO

Соколова В. К.

Науковий керівник – к.т.н., доц. Хаханова Г. В.

Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. АПОТ, тел. (057) 702-13-26)
тел. +38(097) 886-94-40, e-mail: viktoriiia.sokolova1@nure.ua

"Smart home" is a modern tool to increase the level of comfort and human life, and because most processes are controlled by electronics and occur automatically, it makes it important to study and improve such technologies. In solving the problem, a functional scheme of automation has been developed, software for the microcontroller has been developed, economic calculations have been carried out for expediency of the system implementation.

«Розумний» будинок – це житловий будинок, у якому присутня система домашніх пристроїв, здатних виконувати дії та вирішувати певні повсякденні завдання без участі людини, з можливістю керування цими пристроями.

Всі прилади під'єднуються до комп'ютерної мережі, що дозволяє керувати ними за допомогою ПК або смартфона, маючи віддалений доступ до них через Інтернет. Завдяки інтеграції інформаційних технологій у домашні умови, усі системи та прилади узгоджують виконання функцій між собою, порівнюючи показники та задані значення програми.

З кожним роком зростає тенденція, що більшість повсякденних завдань спрощені або автоматизовані. У побут сучасної людини щільно увійшли електроніка та технології віддаленого керування. Популярність автоматизованих систем, таких як «розумний» будинок, обумовлена прагненням людини до комфорту та зручності. «Розумний» будинок є сучасним інструментом підвищення рівня комфорту та життя, так як частина процесів відбувається автоматично, а решту можна керувати віддалено.

«Розумний» будинок складається з набору підсистем, що відповідають за виконання функцій енергопостачання та теплозбереження, контролю клімату, безпеки. З часом відбулось вдосконалення цих підсистем і збільшення кількості виконуваних ними функцій, тому керувати системою «розумним» будинком стало легше. Існує безліч засобів автоматизації, яка сама справляється з покладеними на неї завданнями, такими, як наприклад підтримка мікроклімату, опалення, вентиляція будинку, освітлення, охоронна сигналізація, контроль входу та виходу, але керування та обслуговування цих систем вимагає наявності людини.

У «розумному» будинку достатньо одним натисканням на настінній клавіші або пульті дистанційного керування, вибрати один зі сценаріїв, то

будинок сам налаштує роботу всіх систем, відповідно до побажань користувача, часу доби, погоди, зовнішньої освітленості.

Концепція «розумного» будинку містить в собі такі положення:

- створення інтегрованої системи управління будівлею – системи з можливістю забезпечення комплексної роботи всіх інженерних систем будівлі: освітлення, опалення, вентиляції, водопостачання, контролю доступу;

- відсутність обслуговуючого персоналу та передача функцій контролю і прийняття рішень підсистемам інтегрованої системи управління будівлею;

- реалізація механізму миттєвого відключення та передачі, при необхідності, управління людині будь-якою підсистемою «розумного» будинку;

- забезпечення коректної роботи окремих підсистем в разі відмови загальної керуючої системи або інших частин системи;

- мінімізація вартості обслуговування та модернізації систем будівлі, що має забезпечуватися застосуванням загальних стандартів у побудові підсистем, автоматичне конфігурування і виявлення нових пристроїв і модулів при їх додаванні в систему;

- наявність в будівлі прокладеного комунікаційного середовища для підключення до неї пристроїв і модулів.

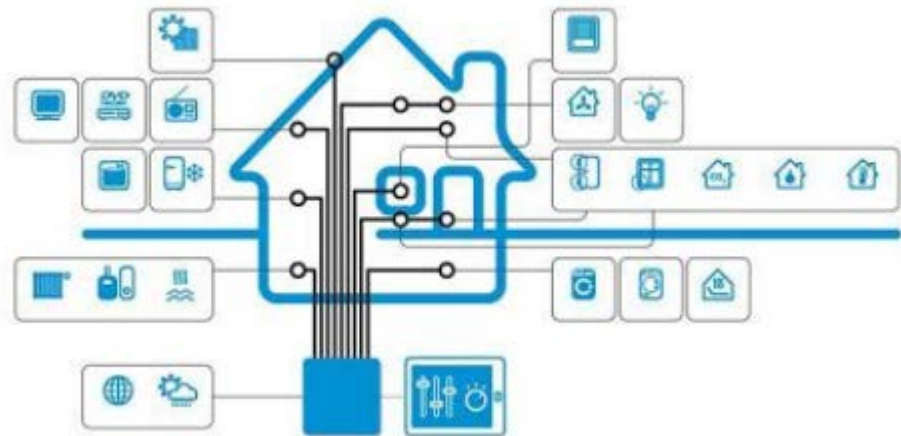


Рисунок 1– Концептуальне зображення системи «розумний» будинок

Список використаних джерел:

1. Моніт, Я. В. (2016). Система «Розумний будинок» з відкритим програмним забезпеченням. Політехніка.
2. Емельянов, Г. С., & Крапивный, Ю. Н. (2018). Модель адаптивного контролера на основі нечіткої логіки для управління системою «Розумний Дім».

УДК 004.056:004.7

**ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ
РЕСУРСІВ В ІКС**

УДК 004.056.55:004.021

СИНТЕЗ КРИПТОГРАФІЧНИХ СИСТЕМ НА ПРИКЛАДІ DES І RSA АЛГОРИТМІВ

Марініч К. Ю.

Науковий керівник – професор катедри ПІ, к.т.н. Бондарєв В. М.
Харківський національний університет радіоелектроніки, каф. ПІ,
м. Харків, Україна

тел. +38-(099)-788-18-24, e-mail: kseniia.marinich@nure.ua.

The purpose of this work is to identify types of cryptographic systems, analyse and compare them. Determine the difference between symmetric and asymmetric cryptographic systems on examples of DES and RSA algorithms. In thesis were considered principles of working both of these methods.

З кожним роком питання безпеки та секретності стає все більш і більш актуальним. Потужності комп'ютерів посилюються, швидкість обробки даних зростає, тож і можливості дешифрування стають ширше. Тому задля забезпечення секретності повідомлень користувачів використовують різні системи та алгоритми шифрування.

Яким чином взагалі відбувається шифрування і дешифрування інформації? Шифрування передбачає перетворення даних у зашифровану форму так, що будь-яка сторона, яка перехоплює, не може прочитати та зрозуміти їх, крім отримувача, якому вони призначені. Процес шифрування стає можливим завдяки криптографічним ключам в поєднанні з різними математичними алгоритмами. На наш час існує дві системи шифрування: симетрична (symmetric cryptographic system) та асиметрична (asymmetric cryptographic system). Розглянемо кожну окремо.

Симетрична криптосистема, що містить алгоритми, які виконуються на одному наборі параметрів. Симетричний шифр, тобто шифр, що є симетричною криптографічною системою, використовує один й той самий ключ як для шифрування, так і для розшифровки, або ж різні, але такі, що з одного легко можна знайти інший. Найбільш розповсюдженим алгоритмом з закритим ключом є DES (Data Encryption Standard) алгоритм.

Принцип його заснований на мережі Фейстля, і має таку структуру: шифрує текст 64-бітними блоками, з одного кінця алгоритму вводиться 64-бітний блок відкритого тексту, з іншого виводиться 64-бітний блок шифротексту. Ключ – 56-бітне число, що псевдорандомно генерується і може бути змінене в будь-який момент часу. На першому рівні алгоритм – це лише комбінація двох основних методів шифрування: зміщення та перестановки. Фундаментальною частиною DES є застосування до тексту одиначної комбінації цих методів (спочатку зміщення, потім – дифузія), що залежить від ключа. Такий блок називається раундом, DES складається з 16 таких раундів. В алгоритмі використовується лише стандартна арифметика 64-бітових чисел та булеві операції, а достаток

повторень робить його ідеальним для реалізації в спеціалізованій мікросхемі.

Асиметрична криптосистема – це така система, що містить алгоритми, набори параметрів яких різняться і є такими, що по одному з них неможливо обчислювально знайти інші. RSA (аббревіатура від прізвищ Rivest, Shamir й Adleman) є найбільш популярним шифруванням з відкритим ключом.

Ці криптосистеми використовують односторонні функції, що мають такі властивості:

- якщо x відомо, то $f(x)$ знайти досить просто;
- якщо відомо $y = f(x)$, то для знаходження x немає ефективного шляху.

В основу RSA покладено складність задачі факторизації добутку двох простих великих чисел. Для шифрування використовується піднесення до степеню за модулем великого числа. Для дешифрування необхідно за реальний час вирахувати функцію Ейлера від даного великого числа.

Генерація простого та секретного ключів виконується за таким алгоритмом:

1. Оберемо два простих великих числа p й q ;
2. Нехай n – результат їх множення, $n=p*q$;
3. Оберемо довільне число d , d є взаємно простим до $(p-1)*(q-1)$;
4. Визначимо таке число e , для якого є правдивим співвідношення $(e*d) \bmod ((p-1)*(q-1))=1$.
5. Тоді відкритим ключом буде пара (e, n) , а секретним (d, n)

Аби зашифрувати текст ми маємо розбити його на блоки, кожний з яких може бути представлений у вигляді числа $M(i) = 1, 2, \dots, n-1$ і зашифрувати за формулою $c = m^e \bmod n$.

У 2010 році група вчених зуміла дешифрувати RSA шифротекст довжиною в 768 біт, тож зараз в якості надійної системи шифрування розглядається лише RSA-ключі довжиною від 1024 біт. Деякі компанії не підтримують шифрування менше ніж 2048 біт.

RSA шифрування, як і будь який інший алгоритм з відкритим ключом, є в рази повільнішим, аніж будь-який із симетричним шифруванням. Також системи з відкритим ключом потребують меншу довжину ключа для забезпечення потрібної стійкості шифру, що спрощує реалізацію алгоритму. Але асиметричні системи можуть використовуватись у E2EE методі – шифрування і дешифрування відбувається на сторонах, через що сервер не має доступу до даних, що передаються.

Список використаних джерел:

1. Акопов Д. О. (2014). Криптографія - історія, методи та стандарти. *Вісник Київського інституту бізнесу та технологій*.
2. Zubov A. Y. (2008). Authentication encryption based on authentication code with secrecy. *Prikladnaya diskretnaya matematika*.

УДК 004.6:004.032.2]:[004.272.26+004.7]

**МЕТОДИ І ЗАСОБИ ОБРОБКИ ДАНИХ В
ГЕТЕРОКОМПОНЕНТНИХ КОМП'ЮТЕРНИХ
СИСТЕМАХ І МЕРЕЖАХ**

MONTE CARLO TREE SEARCH METHOD – FUTURE OF NEURAL NETWORK DEVELOPMENT

Berdnyk M.I.

Scientific Supervisor– Candidate of Technical Science, S.L. Babii A.S.

Kharkiv National University of Radio Electronics, department SE

Kharkiv, Ukraine

ph. +38(099)-085-27-87, email: mariia.berdnyk@nure.ua

Today neural network developing is one of the most progressive and promising field. That is why looking for better algorithms to speed up their work is very important. For this purpose Remi Coulin described in 2006 a heuristic search algorithm Monte Carlo tree search (MCTS) based on Monte Carlo method of random sampling for deterministic problems [1]. It was successfully applied to board games such as Go, Chess and Shogi [2], high-level AI in computer strategy games such as Civilization II [3] and so on. So, the aim of the study is to discuss Monte Carlo tree search method benefits and offer ways of using this algorithm in other fields.

In comparison with other game algorithms of neural networks, which mostly base their strength on the brute force computational power, MCTS works differently. Its operations are based on many roll-outs, in which the game is played out till the end by random selection moves. Each round of game playing of MCTS is based on four steps (Figure 1) [4]:

- 1) Selection: Select successive child nodes after root (R) until a leaf node (L) is reached. We mean by “root of game” its current state and by “leaf of game” its any node, that has a potential child from which no roll-outs exist yet.
- 2) Expansion: Unless the leaf (L) somehow ends the game (win/loss/draw) for either side, then it creates one (or more) child nodes and chooses node (C) from one of them. We mean by “child nodes of game” its possible moves from the game position.
- 3) Simulation: End one rollout (no matter which) from node C.
- 4) Backpropagation: Update information in the nodes on the path from C to R by according to the result of the rollout.

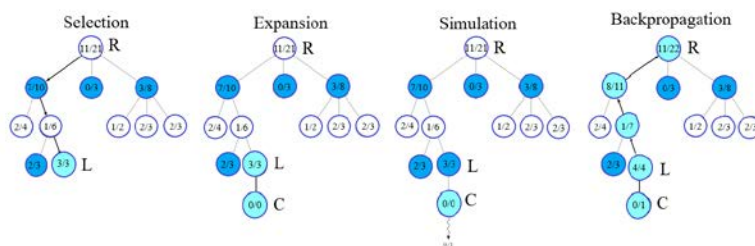


Figure 1 – Work of MCTS

So, MCTS analyses the most promising moves/ways, expanding the search tree based on random sampling of the search space.

As an example we can compare work of AlphaZero chess program, which is based on MCTS method, with simple chess program Stockfish in their match in 2018 [5]. The particular point of comparison is the number of positions searched per second by the two programs. Stockfish searches 70 million of positions per second compared with 80,000 by AlphaZero [5], that is why we can conclude, that simple program has much bigger search deep. Despite this fact, AlphaZero convincingly won that match of 100 games with 28 wins and draws in the rest. This ability was achieved by work of MCTS method. Like a human it gets experience from numerous played games with itself and like a human it analyses at first the most promising moves. So, we can conclude, that neural networks based on MCTS method work different versus their predecessors.

We can conclude, that Monte Carlo Tree Search (MCTS) method combined with neural network is very perspective way of developing artificial intelligence in different fields. Because of its algorithm, which analyse the most promising moves/ways, expanding the search tree based on random sampling of the search space, it is able to to work much faster in comparison with algorithms-ancestors. The latest successful method usage in complex board games like go and chess means, that this algorithm can be used in such specific fields like medicine or physics and lead to more important law discoveries. This topic needs more researchers in future.

References:

1. Coulom R. (May 29–31, 2006). Efficient Selectivity and Backup Operators in Monte-Carlo Tree Search. Computers and Games, 5th International Conference, CG (pp. 72–83). Turin (Italy).
2. Silver D., Hubert T., Schrittwieser J., Antonoglou I., Lai M., Guez A., Lanctot M., Sifre L., Kumaran D., Graepel T., Lillicrap T., Simonyan K., & Hassabis D. (2017). Mastering Chess and Shogi by Self-Play with a General Reinforcement Learning Algorithm. Google Deepmind (19 p.). London (Great Britain).
3. Branavan S.R.K., Silver D., & Barzilay R. (2011). Non-Linear Monte-Carlo Search in Civilization II. International Joint Conference on Artificial Intelligence, #22 (17 p). Barselona (Spain).
4. Chaslot G.M.J.B., Winands M.H.M., Uiterwijk J.W.H.M., & van den Herik H.J., Bouzy B. (2008). Progressive Strategies for Monte-Carlo Tree Search. New Mathematics and Natural Computation (pp. 343–359).
5. Bratko I. (2018) AlphaZero – What’s Missing? Informatica, Vol.42. (pp. 7-11 – page 8).

ВИКОРИСТАННЯ МЕТОДІВ АДАПТИВНОГО НЕЧІТКОГО КЛАСТЕРУВАННЯ ДЛЯ ВИРІШЕННЯ ЗАВДАННЯ ОПРАЦЮВАННЯ МАТРИЧНИХ ДАНИХ

Анісімов В.Е.

Науковий керівник – к.т.н., проф. Кулішова Н.Є.

Харківський національний університет радіоелектроніки

61166, Харків, просп. Науки, 14, каф. Штучного Інтелекту, тел. (057) 702-13-37

email: vladyslav.anisimov@nure.ua

Проблема кластерування багатовимірних даних часто зустрічається в багатьох задачах, які пов'язані з інтелектуальним аналізом даних. Традиційний підхід до вирішення таких завдань дозволяє припущення відносно того, що кожне спостереження може відноситись до одного кластеру [1], хоча більш природньою є ситуація, коли вектор ознак з різними рівнями належності або ймовірності може належати одразу декільком класам.

Для випадку, коли вхідна інформація надходить на опрацювання не у векторному, а в матричному вигляді. Така ситуація є характерною, наприклад, при обробці зображень [2], коли вхідна $(N_1 \times N_2)$ -матриця розбивається на $N = N_1 \cdot N_2 \cdot (n_1 \cdot n_2)^{-1}$ $(n_1 \times n_2)$ -матриць-фрагментів, які необхідно кластерувати, в результаті формуються одномірні в деякому сенсі сегменти зображення. Традиційно ця задача вирішується шляхом попередньої векторизації фрагментів та у використанні вже відомих процедур, найбільш популярною з яких є метод кластерування нечітких С-середніх [1, 2].

Нехай задана вибірка спостережень $x(k) = \{x_{i_1, i_2}(k)\} \in R^{n_1 \times n_2}$, $k = 1, 2, \dots, N$, а в якості цільової функції кластерування використовується ймовірнісний критерій

$$\begin{aligned}
 E(u_j(k), c_j) &= \sum_{k=1}^N \sum_{j=1}^m u_j^\beta(k) D^2(x(k), c_j) = \\
 &= \sum_{k=1}^N \sum_{j=1}^m u_j^\beta(k) \text{Tr}(x(k) - c_j)(x(k) - c_j)^T
 \end{aligned} \tag{1}$$

за наявності обмежень:

$$\sum_{j=1}^m u_j(k) = 1, \text{ та } \sum_{j=1}^m u_j(k) - 1 = 0, \tag{2}$$

де $k = 1, 2, \dots, N$, $0 < \sum_{j=1}^m u_j(k) < N$, $j = 1, 2, \dots, m$, $u_j(k) \in [1, 2]$ – рівень належності $x(k)$ до j -го кластеру, c_j – центроїд j -го кластеру, β – параметр фаззифікації, $D^2(x(k), c_j)$ – міра відстані між $x(k)$ та c_j .

Результатом кластерування є $(N \times m)$ -матриця $U = \{u_j(k)\}$, яка має назву матриці нечіткого розбиття. Фінальний результат матричних операцій до класичного методу кластерування нечітких С-середніх має вигляд:

$$\left\{ \begin{array}{l} u_j(k) = \frac{\left(D^2(x(k), c_j)\right)^{1/1-\beta}}{\sum_{l=1}^m \left(D^2(x(k), c_l)\right)^{1/1-\beta}}, \\ \lambda(k) = -\left(\sum_{l=1}^m \left(\beta D^2(x(k), c_l)\right)^{1/1-\beta}\right)^{1-\beta}, \\ c_j = \frac{\sum_{k=1}^N u_j^\beta(k)x(k)}{\sum_{k=1}^N u_j^\beta(k)}. \end{array} \right. \quad (3)$$

Отримана система породжує клас процедур кластерування. Так, обираючи $\beta = 2$, отримуємо простий та ефективний алгоритм матричного кластерування, який є узагальненням популярної процедури Дж. Бездека [2]:

$$\left\{ \begin{array}{l} u_j(k) = \frac{\left(\text{Tr}(x(k) - c_j)(x(k) - c_j)^T\right)^{-1}}{\sum_{l=1}^m \left(\text{Tr}(x(k) - c_l)(x(k) - c_l)^T\right)^{-1}}, \\ c_j = \frac{\sum_{k=1}^N u_j^2(k)x(k)}{\sum_{k=1}^N u_j^2(k)}. \end{array} \right. \quad (4)$$

Функціонування алгоритму кластерування починається із задання початкової (зазвичай випадкової) матриці нечіткого розбиття U^0 . На основі її розраховується початковий набір центроїдів c_j^0 , які далі використовуються для обчислення нової матриці U^1 . Спостереження в пакетному режимі перераховуються $c_j^1, U^2, \dots, c_j^{t-1}, U^t$, поки різниця $\|U^t - U^{t-1}\|$ не стане меншою за деякий апріорі заданий поріг ε . Таким чином весь масив спостережень опрацьовується декілька разів.

Описаний в роботі метод нечіткого кластерування матричних даних, є модифікацією класичного методу нечіткої самоорганізації даних, який було запропоновано Дж. Бездеком. Цей метод дозволяє опрацьовувати як дані у векторній формі, так і матричній. На відміну від класичного методу нечітких С-середніх знімається суворе обмеження на функцію належності і пропонується використовувати більш адаптивний підхід для розрахунку, замість рівнів належності використовуються рівні можливості.

Список літератури

1. Bezdek, J. C. Fuzzy Models and Algorithms for Pattern Recognition and Image Processing: Springer [Text] / J.C. Bezdek, J. Keller, R. Krisnaparum, N. Pal. – 1999. – P. 777.

2. Bezdek, J. C. Pattern Recognition with Fuzzy Objective Function Algorithms [Текст] / J. C. Bezdek. – New York: Plenum Press, 1981. – P. 272.

УДК 004.725

ОГЛЯД ТЕХНОЛОГІЇ АНОНІМІЗАЦІЇ ТРАФІКУ З ВИКОРИСТАННЯМ CLOUD DISCOVERY

Артьоменко А.О.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: artomenko.andrii@gmail.com.

One such solution is Microsoft Cloud Cloud Vendor's traffic anonymization technology. Solutions based on this technology help protect the privacy of users. The purpose of the report is to review the main benefits of this solution and the risks that may arise. Such benefits include personal data are not stored or displayed. All data is encrypted; closed data is encrypted using the AES-128 standard; the definition of the user name is performed only for a specific case by decrypting the encrypted user name. It is concluded that this is possible only in the case of corporate use of software solutions based on this technology.

На сьогоднішній день анонімізація мережного трафіку є важливим механізмом для запобігання ідентифікації джерела даних та місця призначення запитів від користувача мережі [1]. У мінливому інфокомунікаційному полі мережі Інтернет застосування такої стратегії поведінки дозволяє безпечно використовувати мережні сервіси, не задумуючись про ймовірність стеження за запитом та відповідями з мережних вузлів, особливо в мобільних або супутникових мережах [2-5].

Одним із таких рішень є технологія анонімізації трафіку вендора хмарних послуг Microsoft – Cloud Discovery. Рішення на базі цієї технології дозволяє захищати конфіденційність користувачів. Метою доповіді є огляд основних переваг даного рішення та ризиків, які можуть виникати.

Розглянемо особливості функціонування такого програмного забезпечення. Після передачі журналу даних на порталі Microsoft Defender для хмарних додатків журнал відвідувань очищається, і всі відомості про ім'я користувача замінюються зашифрованими іменами користувачів. Таким чином, всі дії в області зонації доступу до ресурсів залишаються анонімними. При використанні корпоративного варіанту використання, де безпека мережі є запорукою її успішної роботи, за необхідності, адміністратори зможуть розкрити ім'я користувача для службового дослідження (наприклад, порушення цілісності системи безпеки або при аномальних діях із сторін користувача). Якщо у адміністратора є підстави розглянути конкретного користувача, він також може використовувати у разі дослідження трафіку зашифроване ім'я користувача. Для перетворення імені користувача виконується аудит в журналі управління (рисунок 1).

Отже, враховуючі ці особливості, варто розглянути такі основні моменти:

Action type	Target	Initiator	App	Initiated time	Status	Actions
Resolve Cloud Discovery username	User_X6I9IvnRhgF...	admin1	Micro...	Oct 15, 2021. 2:57 PM	Successful	Justification: Investigation

Рисунок 1 – Журнал аудиту адміністратора

- персональні дані не зберігаються і не відображаються. Всі дані зашифровані;
- закриті дані шифруються за допомогою стандарту AES-128. Для клієнта кожного – свій ключ;
- визначення імені користувача виконується тільки для конкретного випадку шляхом розшифровки вказано зашифрованого імені користувача. Це можливо лише у разі корпоративного використання програмного рішення на базі розглянутої технології.

Список використаних джерел:

1. Tkachov V. M. Enabling IOT Solutions for Smart Cities / V. M. Tkachov, O. A. Yeroshenko, A. S. Nuk // Дев'ята міжнародна науково-технічна конференція «Проблеми інформатизації». Т.2. – Черкаси - Харків - Баку - Бельсько-Бяла. – 18-19 листопада 2021 р. – С. 80.
2. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.
3. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.
4. Саваневич В.Е. Метод передачи данных с промежуточным хранением / В.Е. Саваневич, В.Н. Ткачев // Системы обработки информации: сборник научных трудов. - Х.: ХУВС им.Ивана Кожедуба, 2014. - Вып. 7 (123). - С. 99-105.
5. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies». – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

УДК 004.725

МЕТОД БАЛАНСУВАННЯ НА БАЗІ ЗВОРОТНИХ ПРОКСІ-ВУЗЛІВ

Задорожний А.Ю.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: antonzadoroznyi20@gmail.com.

The aim of the work is to develop a method of balancing internal network segments on the platform of reverse proxy nodes. Load balancing actions often differ in the level of OSI on which they operate. This method involves the integration of existing load balancing technology into the type of network in which it will be implemented, as it depends on the overall deployment architecture. The paper considers load balancers of level 3/4 and 7. Thus, the proposed method allows to choose, depending on the needs of the network, adapted algorithms with known software implementations of them on the nodes.

Зворотний проксі-сервер – це вузол, який зазвичай розгортається в межах прикордонного сегменту мережі (демілітаризованої зони або проміжної підмережі), який обробляє запити з Інтернету та перенаправляє їх на обчислювальні мережі внутрішньої мережі. Перенаправляючи запити, зворотний проксі-сервер маскує ідентичність комп'ютерів, що знаходяться за брандмауером організації, таким чином захищаючи внутрішні комп'ютери від прямих атак з боку користувачів інтернету [1-3].

Метою роботи є розробка методу балансування внутрішніх сегментів мереж на платформі зворотних проксі-вузлів. Додатковою вимогою є можливість застосування методу у високомобільних мережах [4].

При використанні зворотних проксі-серверів з функцією перевірки працездатності, необхідно використовувати точку доступу перевірки працездатності, щоб визначити, чи може вузол внутрішньої мережі отримувати запити. Це використовується для швидкого визначення наявності на вузлі апаратного або програмного збою. Зворотні проксі-сервери іноді називають балансувальниками навантаження, але зазвичай вони пропонують більше, ніж простий розподіл вхідних повідомлень за внутрішніми цілями. Багато реалізації зворотного проксі-сервера можуть працювати з будь-якою ємністю вузлів та обсягів трафіку, залежно від конфігурації [5].

Дії балансування навантаження часто відрізняються рівнем моделі взаємодії відкритих систем (OSI), на якому вони працюють. Даний метод передбачає інтеграцію існуючої технології балансування навантаження до типу мережі, в якій він реалізовуватиметься, оскільки від цього залежить загальна архітектура розгортання.

Балансувальники навантаження рівня 3/4 іноді називають балансувальниками навантаження на рівні мережі чи пакетів. Ці

балансувальники навантаження зазвичай не перевіряють вхідний трафік, а натомість направляють вхідні пакети TCP/UDP до внутрішніх цілей. Нові реалізації допускають SSL-термінацію на балансувальнику навантаження, але клієнтський сеанс SSL зазвичай встановлюється із внутрішнім цільовим сервером або серверами.

Балансувальники навантаження рівня 7 іноді називають балансувальниками навантаження за допомогою додатків. Ці балансувальники навантаження перевіряють вхідні повідомлення та можуть приймати рішення, пов'язані з маршрутизацією, враховуючи кілька факторів, а також змінювати зміст цих повідомлень перед їх проксюванням на кінцеву ціль або кінцеві об'єкти. Балансувальники навантаження рівня 7, що використовують HTTPS, перервуть SSL-з'єднання з клієнтом і повторно зашифрують цей трафік перед проксюванням запитів до внутрішніх HTTPS-цілей.

Таким чином, запропонований метод дозволяє обирати в залежності від потреб мережі адаптовані алгоритми з відомими програмними реалізаціям їх на вузлах.

Список використаних джерел:

1. Ткачов В.М. Огляд методів забезпечення кібербезпеки індустріальної полігрової мережі / В. М. Ткачов, О. І. Морозова, А. Г. Тецький, А. О. Нічепорук // Дев'ята міжнародна науково-технічна конференція «Проблеми інформатизації». Т.1. – Черкаси - Харків - Баку - Бельсько-Бяла. – 18-19 листопада 2021 р. – С. 60.

2. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

3. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies». – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

4. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.

5. Саваневич В.Е. Метод передачи данных с промежуточным хранением / В.Е. Саваневич, В.Н. Ткачев // Системы обработки информации: сборник научных трудов. - Х.: ХУВС им.Ивана Кожедуба, 2014. - Вып. 7 (123). - С. 99-105.

УДК 004.725

ОЦІНКА ПРОПУСКНОЇ ЗДАТНОСТІ БАЛАНСУВАЛЬНИКІВ ВІРТУАЛЬНОЇ МЕРЕЖНОЇ ІНФРАСТРУКТУРИ

Кульков Б.І.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: bogdann.kulkovv@gmail.com

The purpose of the report is to assess the capacity of balancers of a special class of network infrastructures to obtain a qualitative description of the benefits of this method of organizing access to virtual network resources. Load balancers used in virtual cloud infrastructures are typically HAProxy (High-Availability Proxy) virtual machines, that is, high-availability traffic proxies. The paper presents a list of functions performed by such a balancer. It is shown that under all conditions, the bandwidth of load balancers is 1-1,5 Gb/s, with an RPS value of ~10000 requests per second.

Віртуальні мережні інфраструктури останнім часом все частіше використовуються у якості платформи для побудови віртуальних брандмауерів [1-2], систем високої доступності трафіку у сегментах Глобальної мережі з обмеженою присутністю вендорів останньої милі [3-4], нестационарних мереж передачі даних [5] тощо.

Метою доповіді є оцінка пропускної здатності балансувальників такого класу мережних інфраструктур для отримання якісної характеристики переваг такого способу організації доступу до віртуальних ресурсів мережі.

Балансувальники навантаження, що використовуються в віртуальних хмарних інфраструктурах – це, як правило, віртуальні машини з HAProxy (High-Availability Proxy), тобто з сервісом проксування трафіку високої доступності. Список функцій, що виконуються таким балансувальником включає:

- користувальницькі балансувальники, створені спеціально під інфраструктуру програми. Трафік у таких балансувальниках приходить із зовнішньої мережі та перенаправляється до компонентів користувача програми;

- HA (High availability) балансувальники – створюються для управління баз даних. HA-балансиувальники створюються за замовчуванням, підключаючи базу даних до користувача додатку;

- Ingress-Controller. У маніфесті такого балансувальника вказуються правила підключення між додатками користувача, відкриття портів і маршрутизації трафіку до відповідних додатків. Основна функціональність – розвантаження мережі для додатків у подах Kubernetes.

Для забезпечення найкращої пропускної спроможності балансувальника навантажень необхідно виконання наступних умов:

- програмне та апаратне забезпечення гіпервізора – балансувальники повинні мати багатоядерні процесори (не менше 4-х ядер) і останні оновлення ядер Linux;
- завантаженість робочого часу CPU гіпервізора має перевищувати 80 %;
- версія підключення клієнтського сервісу повинна відповідати стандарту HTTP1.1 із підтримкою протоколу keep-alive;
- розмір пакетів, що передаються через балансувальник, об'ємом не менше 1500 мс.

Таким чином результати оцінки вказують на те, що при виконанні всіх умов пропускна здатність балансувальників навантаження становить 1-1,5 Гб/с, зі значенням RPS ~10000 запитів в секунду, що задовольняє більшість вимог сучасних вендорів розподілених послуг.

Список використаних джерел:

1. Tkachov V. Method to Determine Fault-Tolerant Performance Probability of High-Survivability Computer Network based on Mobile Platform / V. Tkachov, M. Hunko, O. Morozova, A. Tetskyi, A. Nicheporuk // 2021 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), 2021. Pp. 1-6.

2. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.

3. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

4. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies». – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

5. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.

ОГЛЯД ТИПІВ МІГРАЦІЇ ІСНУЮЧИХ ІНФРАСТРУКТУР В ХМАРУ

Садовська А.О.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: anastasia.sadovskaya.student@gmail.com.

Cloud migration is the process of moving programs and data from one location to the servers of public cloud service providers, as well as between different clouds. The paper considers the main advantages of migration to the cloud. This reduces IT costs and increases productivity. But there are other advantages, such as high security and convenience. Two technical factors are also considered for most migration scenarios: the type of portable resource (or workload); the location where the migration is performed. These arguments allow us to more fully describe the benefits of migrating existing infrastructures to the cloud environment.

Більшість сучасного ІТ-ринку використовує хмарні технології, тоді як державний сектор доволі кволо переходить до використання хмарних технологій. Це пов'язано з вимогами до їх безпеки [1], застарілістю використовуваних технологій або їх специфікою [2-4], використанням гетерогенного середовища зберігання, обробки та передачі даних [5] тощо. Метою роботи є огляд основних типів міграції інформаційних структур в хмару.

Міграція в хмару – це процес переміщення програм та даних з одного розташування на сервери постачальників загальнодоступних служб хмар, а також між різними хмарами. Основні переваги міграції у хмару – це скорочення витрат на ІТ та підвищення продуктивності. Але є й інші переваги, такі як високий рівень безпеки та зручність.

Два ключові технічні фактори для більшості сценаріїв міграції:

- тип переносного ресурсу (або робочого навантаження).
- розташування, у якому виконується міграція.

Як правило, задача зводиться до вирішення задачі переносів центрів даних та міграції у гібридну хмару.

Перенесення центру обробки даних – це процес переміщення інформації з локальних серверів та мейнфреймів (які часто розміщені в серверній) на сервери постачальника хмарних служб, які зазвичай знаходяться у дуже великих, високобезпечних та професійно обслуговуваних точках. Мережі з великою ємністю – це найпоширеніший спосіб переміщення ресурсів центру обробки даних у хмару. Але якщо потужна мережа недоступна, ресурси можна перенести спочатку перемістивши їх на диски великої ємності та

пристрої Data Box, а потім фізично доставивши постачальнику хмарних служб, який відправить їх на сервери.

Багато державних організацій вирішують залишити деякі зі своїх ресурсів у локальному центрі обробки даних і перемістити в хмару тільки їхню частину, створивши гібридну хмару. Переваги гібридної хмари: підвищення рентабельності існуючого локального обладнання у центрі обробки даних, а також забезпечення відповідності галузевим та державним вимогам для організацій у певних галузях. Гібридні хмари також корисні для резервного копіювання з хмари в хмару, при якому резервні копії локальних даних створюються в загальнодоступній хмарі як рішення аварійного відновлення на той випадок, якщо локальний центр обробки даних стане непрацездатним, наприклад, при пожежі, повені або злочинних діях (у цьому випадку у виразі «з хмари в хмару» маються на увазі локальні центри обробки даних, які іноді називають «приватними хмарами»).

Таким чином, такі доводи дозволяють більш повно описати переваги міграції існуючих інфраструктур до хмарного середовища.

Список використаних джерел:

1. Morozova O.I. Methods and technologies of ensuring cybersecurity of industrial and web-oriented systems and networks / O.I. Morozova, A.O. Nicheporuk, A.G. Tetskyi, V.M. Tkachov // *Radioelectronic and Computer Systems*. 2021. № 4 (100). Pp. 145-156. doi: 10.32620/reks.2021.4.12.

2. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // *Системи управління, навігації та зв'язку*. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.

3. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

4. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // *Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies»*. – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

5. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // *Системи управління, навігації та зв'язку*. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.

ОГЛЯД МЕТОДІВ ПІДВИЩЕННЯ ВІДМОВОСТІЙКОСТІ ВІРТУАЛЬНИХ КЛАСТЕРІВ VM MANAGER CLOUD

Тарасенко В.С.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: vladyslav.tarasenko.studies@gmail.com.

The purpose of the report is to review the methods that increase the resilience of virtual clusters built on the VMmanager platform Cloud version. The following methods are considered: quorum of cluster nodes; network storage of virtual disks; cluster node availability diagnostics system; control panel fault tolerance system. It is stated that the main feature is that if the cluster node on which VMmanager Cloud is installed fails, the control panel will be automatically launched on one of the working nodes. This will allow you to use any of these methods.

Відмовостійкість кластера – відмінна риса VMmanager версії Cloud [1-4]. Хмарні функції можна ввімкнути за наявності щонайменше трьох вузлів кластера. Проте відмовостійкість досягається лише за наявності функціонуючих чотирьох і більше вузлів кластера. Цей підхід заснований на принципах, які використовуються у мобільних мережах [5].

Метою доповіді є огляд методів, які дозволяють підвищити відмовостійкість віртуальних кластерів, що будуються на платформі VMmanager версії Cloud. Отже, розглянемо наступні методи:

- кворум вузлів кластера;
- мережеве сховище віртуальних дисків;
- система діагностики доступності вузлів кластеру;
- система відмовостійкості панелі керування.

Вузол вважається працездатним, якщо він знаходиться у кворумі. Кластер вважається працездатним, якщо працездатна хоча б мінімально необхідна кворуму кількість вузлів. Якщо вузол втрачає зв'язок з іншими вузлами або має зв'язок тільки з частиною кластера, що знаходиться в меншості, він (і вся менша частина кластера) відзначаються як не в кворумі, а всі хмарні послуги на них призупиняють роботу. Наприклад, у кластері 8 серверів, причому значення кворуму дорівнює 5. Це означає, що сервер знаходиться в кворумі, якщо він крім себе має зв'язок ще з 4-ма або більше серверами. Якщо сервер має зв'язок з менш ніж 3 серверами, то вважається, що вузол кластера не в кворумі.

У разі відмови вузла кластера віртуальні машини, що працюють на цьому вузлі, відновлюються на іншому працездатному вузлі кластера. Для цього необхідно, щоб віртуальні диски віртуальних машин розташовувалися в мережних сховищах.

Система діагностики перевіряє доступність вузлів кластера та при відмові відновлює віртуальні машини на доступних вузлах кластера. Вузол кластера вважається таким, що відмовив і від'єднується від кластера, якщо він не відповідає більше 1 секунди.

При виході з ладу вузла кластера, на якому встановлений VMmanager Cloud, панель управління буде автоматично запущена на одному із працездатних вузлів.

Відмовостійкість VMmanager Cloud досягається за рахунок реплікації бази даних VMmanager та необхідних файлів. За реплікацію файлів VMmanager відповідає завдання cron. Для синхронізації файлів використовується утиліта rsync. Файли синхронізуються на усіх вузлах кластера. Для реплікації бази даних використовується стандартна реплікація mysql. Реплікація бази даних виконується на вузлі кластера, для яких відзначено роль Реплікація mysql в Вузлі кластера→Ролі.

Таким чином, виконаний огляд дозволяє застосовувати ці методи для підвищення відмовостійкості віртуального кластеру.

Список використаних джерел:

1. Morozova O., Tetskyi A., Nicheporuk A., Krivak D., Tkachov V. Smart Home System Security Risk Assessment // International Scientific Journal «Computer Systems and Information Technologies». 2021. № 3. Pp. 81-88. doi: 10.31891/CSIT-2021-5-11.

2. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.

3. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

4. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies». – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

5. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.

**ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ХМАРНИХ ТЕХНОЛОГІЙ В
ГАЛУЗІ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ
ВАНТАЖОПЕРЕВЕЗЕНЬ НА ЗАЛІЗНИЦІ**

Шкіренко Д.В.

Науковий керівник – к.т.н., доц. Ткачов В.М.

Український державний університет залізничного транспорту, каф. ІТ,
м. Харків, Україна

тел. +38(057)730-19-84, e-mail: shkirenkov.dmitriy@gmail.com.

Optimizing the loading of transport units and transport routes, real-time tracking of goods throughout the journey - such tasks require speed of processing, high accuracy and consistency in logistics operations. The advantages of cloud technologies on the railway can be a reliable transportation management system, the ability to store and exchange documents for transportation, tracking the location of goods. The purpose of the report is to reveal the features of the application of modern cloud technologies in the field of information support of rail freight.

Метою доповіді є розкриття особливостей застосування сучасних ІТ-технологій [1-5], зокрема таких як хмарні, в галузі інформаційного забезпечення вантажоперевезень на залізниці.

Вантажоперевезення на залізниці – це ринок, де існує моментальний попит та пропозиція. В «хмарах» є можливість створити єдину платформу для вантажовласників (тих, кому треба везти вантажі) та перевізників. Віртуальні платформи дозволяють розміщувати заявки на перевезення і бачити найкращі пропозиції від контрагентів – учасників хмарної платформи.

Оптимізація завантаження транспортних одиниць та маршрутів перевезення, відстеження вантажів в реальному часі протягом усього шляху – такі завдання потребують швидкості обробки, високої точності та узгодженості у логістичних операціях. У якості переваги хмарних технологій на залізниці можуть служити надійна система управління перевезеннями, можливість зберігання та обміну документацією на перевезення, відстеження розташування вантажу.

Зберігання документації на перевезення – велика проблема. В «хмарі» є можливість автоматизувати цей процес: по-перше, відпадає потреба встановлювати, а потім оновлювати програмне забезпечення. По-друге, зобов'язання щодо внесення даних у систему можна перекласти на перевізника, вивільнивши цим власний людський ресурс.

Відстеження пересування вантажу маршрутом допомагає компанії розрахувати точний час прибуття потягу в точку доставки. За допомогою цих даних можна планувати постачання та вирішити проблему порожніх полиць та зайвих запасів.

Проте, хмарні технології можуть виявитися корисними не лише у сфері транспортного планування, а також як фактор розвитку приміської залізничної інфраструктури. Хмарні технології у цій сфері можуть застосовуватись для зберігання та збору геоінформаційних даних. Під геоданими в даному випадку маються на увазі інформацію про приміську або міжобласну мережу, адресну базу, статистику з вимушених зупинок тощо. Наприклад, тільки можливість перемикання режиму semaфорів залежно від поточного навантаження суміжних маршрутів здатна значно знизити затримки.

Реалізація хмарних технологій в Укрзалізниці до 2025 року дозволить суттєво перетворити модель надання послуг підрозділам. Гнучкість віртуального середовища буде реалізована за рахунок рішення щодо динамічного розподілу навантаження на фізичне обладнання, що передбачає автоматичне перенесення систем без їх зупинки на менш завантажене обладнання. Дані можливості також дозволять підвищити доступність та надійність систем за рахунок ремонту та обслуговування обладнання без зупинки функціонування інформаційних систем.

Список використаних джерел:

1. Коваленко А.А. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання / А.А. Коваленко, Г.А. Кучук, В.М. Ткачов // Системи управління, навігації та зв'язку. – Полтава: Полтавський національний технічний університет ім. Ю. Кондратюка, 2021. – № 1 (63). – С. 90-95.

2. Tkachov V. Technology of Load Balancing in Anonymous Network Based on Proxy Nodes Cascade Platform / V. Tkachov, M. Hunko, M. Bondarenko, S. Artyomov // Четверта міжнародна науково-технічна конференція «Комп'ютерні та інформаційні системи і технології». Збірка наукових праць. Харків: ХНУРЕ. – 2020. – С. 82.

3. Kuchuk N. Predicting traffic anomalies in container virtualization / N. Kuchuk, A. Kovalenko, V. Tkachov, H. Kuchuk, D. Rosinskiy // Proceedings of Fifth International Scientific and Technical Conference on «Computer And Information Systems And Technologies». – April 22-23, 2021. – Kharkiv-Riga-Kyiv-Lviv-Baku. – С. 25-26.

4. Ткачов В.М. Критерії вибору стандарту безпроводної передачі даних у високомобільних комп'ютерних мережах / В.М. Ткачов, К.Р. Гальченко, А.А. Коваленко, О.А. Єрошенко // Системи управління, навігації та зв'язку. Збірник наукових праць. – Полтава: ПНТУ, 2021. – Т. 4 (66). – С. 63-68. – doi: <https://doi.org/10.26906/SUNZ.2021.4.063>.

5. Саваневич В.Е. Метод передачи данных с промежуточным хранением / В.Е. Саваневич, В.Н. Ткачев // Системы обработки информации: сборник научных трудов. - Х.: ХУВС им.Ивана Кожедуба, 2014. - Вып. 7 (123). - С. 99-105.

УДК 004.6:004.032.2]:[004.272.26+004.7]

**МЕТОДИ І СПОСОБИ ОБЧИСЛЮВАЛЬНОГО
ІНТЕЛЕКТУ**

УДК 004.9:519.876]:004.382.4.04

РОЗРОБКА ПРИСТРОЮ КЕРУВАННЯ ПОБУТОВИМИ ПРИЛАДАМИ ЗА ДОПОМОГОЮ WI-FI

Чапарин І.М.

Науковий керівник – к.т.н., доц. Сердюк Н.М.

Харківський національний університет радіоелектроніки, каф. КІТС
м. Харків, Україна

тел. +38 (097) 533-60-53, e-mail: ilia.chaparyn@nure.ua

There are many household appliances that can be controlled using an IR remote control; however, this method is no longer entirely relevant at the present time. As in the modern world the quantity of the devices is controlled with a smartphone grows, which allows, in addition to simple control, to come up with various automation scenarios. Above mentioned solution allows you to achieve this goal performing the process with the Arduino microcontroller and some additional modules for it. The proposed solution is can be called universal and offers management options via a web interface, which eliminates the need to install additional mobile applications.

Технології швидко змінюють одна одну і якщо 10 років тому управління пристроями за допомогою пульта дистанційного керування було зручним способом взаємодії з технікою, зараз зростає кількість пристроїв, які контролюються за допомогою смартфона, що дозволяє, окрім простого керування, створювати різноманітні сценарії автоматизації. Проте не всі побутові прилади підтримують цю опцію. Деякі з них досі керуються пультом з інфрачервоним випромінювачем, що стає вагомою перешкодою у процесі організації системи розумного будинку. Викладене рішення допоможе адаптувати застарілі пристрої до сучасних реалій. Наведений нижче спосіб дозволяє досягти цієї мети за допомогою використання мікроконтролера Arduino. Цей спосіб можна віднести до універсальних, тому що він передбачає можливості керування за допомогою веб-інтерфейсу, а це позбавляє необхідності встановлення додаткових мобільних застосунків.

Ідея полягає у використанні мікроконтролера Arduino як пристрою для трансляції команд, що передаються у межах зони покриття Wi-Fi задля перетворення у світлові імпульси в інфрачервоному діапазоні. Такі імпульси випромінює більшість пультів дистанційного керування для побутової техніки. Для реалізації такого проекту буде раціонально обрати Arduino UNO.

Arduino UNO є стандартною платою Arduino, і вірогідно, що найпоширенішою. Вона заснована на чіпі ATmega328, що має на борту 32 Кб флеш-пам'яті, 2 Кб SRAM та 1 Кб EEPROM. На периферії має 14 дискретних (цифрових) каналів введення/виведення та 6 аналогових

каналів введення/виведення. Arduino UNO є дуже багатофункціональними девайсами, що дозволяють покрити більшість аматорських завдань у галузі мікроконтролерної техніки. Ця плата контролера є однією з найдешевших та найчастіше використовуваних [1].

Як передавачі використовуються звичайні інфрачервоні світлодіоди. Зазвичай таких датчиків необхідно встановити декілька, до того ж спрямованих у різні сторони, щоб забезпечити трансляцію сигналу усім пристроям в діапазоні дії.

Відстань, на якій можна безпроблемно приймати сигнал залежить від потужності джерела та чутливості приймача, тож слід встановити на платі передавачі з релевантними показниками потужності [2].

На платі буде розгорнутий невеликий веб-сервер. Передбачається використання модулю ESP8266 для Arduino. Одна з найважливіших функцій, яку забезпечує ESP8266 полягає у тому, що він може не тільки підключатися до існуючої мережі Wi-Fi та працювати як веб-сервер, а ще й встановлювати власну мережу, що дозволяє іншим пристроям підключатися безпосередньо до нього та отримувати доступ до веб-сторінок. Це можливо тому, що ESP8266 може працювати у трьох різних режимах: режим станції, режим точки доступу та обидва режими одночасно. Інтерфейс керування передбачено зробити в браузері або розробити відповідний застосунок для мобільних платформ [3]. Однак, як було зазначено вище, варіант розробки застосунку створює низку проблем, а саме: додаткові ресурси на розробку, необхідність адаптації під кожну окрему платформу та необхідність інсталяції на цільовий пристрій.

Список використаних джерел:

1. Ampermarket. (2022, 19 лютого). Сравнение плат Arduino. https://ampermarket.kz/base/arduino_family/
2. Горрес, А. (2007). Инфракрасное дистанционное управление. Нетания.
3. Radioprogram. (2022, 19 лютого). Создание простого веб-сервера на ESP8266 NodeMCU в Arduino IDE. <https://radioprogram.ru/post/866>

УДК 004.8:61

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В МЕДИЦИНІ

Омельченко С. О.

Науковий керівник – д.т.н., проф. Аксак Н. Г.

Харківський національний університет радіоелектроніки, каф. КІТС

м. Харків, Україна

тел. +38(096) 69-07-089, email: serhii.omelchenko1@nure.ua.

This work is devoted to the study of the use of artificial intelligence in medicine. It is considered what artificial intelligence is in medicine, how artificial intelligence is trained and how it processes the received data, in what areas of medicine it is used and what it can be suitable for, what diseases it can diagnose at an early stage, how it can simplify the work of doctors and life the patients themselves. The main advantages and disadvantages of using artificial intelligence in medicine, as well as its further development and future opportunities in medicine were also considered.

Штучний інтелект у медицині – це використання моделей машинного навчання для пошуку медичних даних та отримання інформації, яка допоможе покращити стан здоров'я та досвід пацієнтів. Завдяки останнім досягненням комп'ютерних наук та інформатики штучний інтелект (ШІ) швидко стає невід'ємною частиною сучасної охорони здоров'я. Алгоритми штучного інтелекту та інші додатки на основі ШІ використовуються для підтримки медичних працівників у клінічних умовах та в поточних дослідженнях [1].

Щоб створити ефективний алгоритм ШІ, комп'ютерним системам спочатку надходять дані, які зазвичай структуровані, яку алгоритм розпізнає. Після того, як алгоритм отримає достатню кількість точок даних та їх міток, ефективність аналізується, щоб забезпечити точність. На основі результатів тестування алгоритм можна змінити, надати більше даних або розгорнути, щоб допомогти людині приймати рішення.

Більшість застосунків штучного інтелекту в медицині зчитують дані певного типу, чи то числові, наприклад, частота серцевих скорочень або кров'яний тиск, так і на основі зображень, наприклад, МРТ або зображення зразків біопсійної тканини, як вхідні дані. Потім алгоритми вивчаються на даних і виробляють або ймовірність, або класифікацію. Наприклад, можливим результатом може бути ймовірність утворення артеріального згустку з урахуванням даних про частоту серцевих скорочень і кров'яного тиску, або позначення зразка тканини як ракового чи неракового [2].

Штучний інтелект застосовується в таких областях медицини як: кардіологія (для виявлення таких захворювань як миготлива аритмія та серцево-судинного ризику), пульмонологічна медицина (служить інструментом для прийняття рішень у випадку інтерпретації результатів тестів легеневої функції), ендокринологія (безперервний моніторинг рівня

глюкози в реальному часі та надання інформації про напрямок і швидкість зміни рівня глюкози в крові).

Також ШІ застосовується у гастроентерології (для виявлення поліпів товстої кишки), неврології (для виявлення епілепсії, оцінки ходи, постави та тремору), комп'ютерній діагностиці раку в гістопатології. ШІ знайшов своє застосування в медичній візуалізації – для виявлення ознак раку молочної залози, пневмонії та інших захворювань, а також для розпізнавання таких медичних зображень як знімків МРТ, висновків УЗВ, кардіограм, результатів комп'ютерної томографії.

До основних переваг використання ШІ в медицині можна віднести: більшу точність, поліпшення результатів лікування пацієнта, зменшення витрат на догляд, збільшення взаємодії лікаря і пацієнта, рання діагностика, ефективна та унікальна допомога в хірургії.

Застосування систем штучного інтелекту в будь-якій галузі, включаючи охорону здоров'я, пов'язане з певними обмеженнями та проблемами [3]. До таких можна віднести: доступність даних, упередженість даних, навчання штучного інтелекту (якщо система спроектована погано, вона може поставити неправильний діагноз), помилки в роботі ШІ, проблеми конфіденційності, можливість безробіття.

За результатами досліджень було виявлено, що штучний інтелект, який почав своє існування ще в 1950 роках минулого століття, здійснив значний прорив у сфері медицини. ШІ використовує складні алгоритми машинного навчання для обробки великої кількості даних, навчання та згодом – створення корисного результату для вирішення чітко визначеної проблеми в медичній системі. Навчившись, системи штучного інтелекту можуть звільнити час зайнятим лікарям, переписуючи нотатки, вводячи та впорядковуючи дані пацієнтів, персоналізувати лікування, надавати дистанційно діагностику пацієнтам, відповідаючи на їх основні запитання та надсилати необхідні ресурси. Але найголовніше, що такі системи ШІ є точними, дозволяють розроблювати ліки, допомагають проводити операції та можуть заздалегідь більш ефективно діагностувати небезпечне захворювання у пацієнта ще на ранній його стадії і тим самим врятувати життя людини.

Список використаних джерел:

1. Ramesh A. N. et al. Artificial intelligence in medicine //Annals of the Royal College of Surgeons of England. – 2004. – Т. 86. – №. 5. – С. 334.
2. Greenfield D. Artificial intelligence in medicine: Applications, implications and limitations //Retrieved from Harvard University at <http://sitn.hms.harvard.edu/flash/2019/artificial-intelligence-inmedicine-applications-implications-andlimitations>. – 2019.
3. Hamid S. The opportunities and risks of artificial intelligence in medicine and healthcare. – 2016.

УДК 004.85

МУЛЬТИАГЕНТНІ СИСТЕМИ ДЛЯ ВИРІШЕННЯ СТАТИЧНИХ І ДИНАМІЧНИХ ЗАДАЧ ПЛАНУВАННЯ РОБІТ

Андрющенко Д.Д

Науковий керівник – д.т.н., проф. Аксак Н.Г.

Харківський національний університет радіоелектроніки

(61166, Харків, просп. Науки, 14, каф. Комп'ютерних інтелектуальних технологій та систем, тел. (057) 702-02-45)

e-mail: dmytro.andriushchenko@nure.ua.

The article provides an overview of multi-agent systems and technologies. Multi-agent systems are a subfield of distributed artificial intelligence that is growing rapidly due to the flexibility and intelligence available to solve distributed problems. This chapter provides a brief overview of multi-agent systems. They cover various attributes such as architecture, communication, coordination strategies, decision making, and learning abilities. In the work it is offered to use the distributed system of planning of several agents on the basis of the cooperative approach for the decision of static and dynamic problems of planning of works.

Мультиагентні системи (MAS) є окремим випадком розподіленої системи, і її особливість полягає в тому, що компоненти системи автономні та егоїстичні, прагнучи задовольнити свої власні цілі. Крім того, ці системи також виділяються тим, що є відкритими системами без централізованої конструкції. Однією з головних причин великого інтересу та уваги до мультиагентних систем є те, що вони розглядаються як технологія для складних додатків, які вимагають розподіленої та паралельної обробки даних і працюють автономно в складних і динамічних областях. Дослідження з дисципліни мультиагентних систем (MAS) базуються на результатах розподілених обчислень, які ставлять нові запитання про те, як агенти повинні взаємодіяти один з одним, щоб координувати свою діяльність і вирішувати складні проблеми[1].

Навчання в MAS є парадигмою великого значення, оскільки система, здатна навчатися і динамічно змінювати свій спосіб дій, має великий потенціал для вирішення багатьох проблем, щодо яких ми не знаємо поведінки інших агентів у навколишньому середовищі.

У мультиагентному середовищі навчання є і важливішим, і складнішим, оскільки вибір дій має здійснюватися в присутності інших агентів, які не обов'язково повинні дотримуватися правил середовища і можуть приймати недетерміновані рішення. Ці агенти, у свою чергу, адаптують свої дії до тих, які раніше виконували інші агенти[2].

Протягом останніх кількох років MAS використовувався як інструмент для розробки багатьох фреймворків AmI(AmbientIntelligence). Як приклад можна виділити iGendaframework, основною метою якого є

забезпечення інтелектуального керування подіями, що складається з платформи, яка отримує події від інших користувачів і намагається планувати їх відповідно до своєї важливості, маючи можливість створювати, переміщувати та видаляти події [3].

Агентне моделювання — це підхід до моделювання систем, який зосереджується на моделюванні складних технічних систем, які розподілені та передбачають складну взаємодію між людьми та машинами [4]. Моделі моделюють одночасні операції кількох сутностей (агентів) у спробі відтворити та передбачати дії складних явищ. Це аварійний процес від самого елементарного рівня (мікро) до найвищого рівня (макро).

Концепція розумного міста виникає через необхідність знайти рішення для швидкого зростання населення та ризиків, які це несе для міста, економічних ризиків, таких як безробіття, або фізичних ризиків, таких як надмірне забруднення. Для вирішення цих проблем, серед багатьох інших, були застосовані різні технології, щоб знайти рішення в цій області. Розумне місто — це великий взаємозв'язаний організм, який разом із розумним урядом прагне покращити якість життя своїх громадян [5].

У роботі були досліджені мультиагентні системи, що є багатообіцяючим підходом до використання нових технологій з метою покращення ефективності планування та контролю. Побудова MAS інтегрує технології з різних галузей знань, методи програмної інженерії для структурування процесу розробки методів штучного інтелекту, а також одночасне програмування для вирішення координації завдань, що виконується на різних машинах за різними політиками планування. Пропонується використовувати розподілену систему планування кількох агентів на основі кооперативного підходу для вирішення статичних і динамічних задач планування робіт.

Список використаних джерел:

1. Baldoni, M., Baroglio, C., May, K. M., Micalizio, R., & Tedeschi, S. (2018). Computational accountability in MAS organizations with ADOPT. *Applied Sciences*, 8(4), 489.
2. Duan, K., Fong, S., Zhuang, Y., & Song, W. (2018). Artificial neural networks in coordinated control of multiple hovercrafts with unmodeled terms. *Applied Sciences*, 8(6), 862.
3. Barriuso, A. L., De la Prieta, F., Villarrubia González, G., De La Iglesia, D. H., & Lozano, Á. (2018). MOVICLOUD: Agent-based 3D platform for the labor integration of disabled people. *Applied Sciences*, 8(3), 337.
4. Miyashita, K. (2017). Incremental design of perishable goods markets through multi-agent simulations. *Applied Sciences*, 7(12), 1300.
5. Lozano, Á., De Paz, J. F., Villarrubia González, G., Iglesia, D. H., & Bajo, J. (2018). Multi-agent system for demand prediction and trip visualization in bike sharing systems. *Applied Sciences*, 8(1), 67.

МЕТОДИ ПОШУКУ КЛЮЧОВИХ СЛІВ

Лебідь В.М.

Науковий керівник – к.т.н., доц., доц. каф. КІТС Сердюк Н. М.
Харківський національний університет радіоелектроніки, каф. КІТС,
м. Харків, Україна
тел. +38(095) 515-37-39, e-mail: vadym.lebid@nure.ua.

This work is devoted to methods for extracting keywords. Often in scientific papers and publications there is a large amount of text that is very difficult to read quickly and at the same time not to lose important information. In this case, it becomes necessary to reduce the volume of the document by highlighting the most significant parts of the text, called the abstract. Compiling keywords is a complex and time-consuming job. This task requires additional staff and therefore it is more expedient to use systems for automatically extracting keywords from text.

Ключові слова – це ідеї та теми, які визначають зміст контенту. З погляду SEO, це слова та фрази, які користувачі вводять у пошукові системи, також звані пошуковими запитамі. Якщо звести все на своїй сторінці – всі зображення, відео, текст тощо – до простих слів та фраз, це будуть основні ключові слова. За допомогою ключових фраз кінцевий користувач може отримати максимально повну інформацію про основні думки або теми конкретного тексту. Це завдання постійно повинні вирішувати пошукові системи, агрегатори новин і ресурсів, які аналізують думку користувачів соціальних мереж [1].

Основні види методів і моделей автоматичного вилучення ключових слів можна розділити на лінгвістичні, статистичні, спектральні, та гібридні.

Етапи вилучення ключових слів з тексту практично ідентична всім використовуваним методам з чотирьох етапів:

1. Етап попередньої обробки текстів. Видалення слів із тексту з метою його спрощення, виключення елементів маркування, приведення слів до словникової форми та видалення стоп-слів, що не несуть смислового навантаження.

2. На основі цих даних складається список кандидатів в ключові слова, за якими проводитиметься пошук.

3. Виявлення найважливіших ознак кожного з кандидата.

4. Відбір ключових слів з-поміж кандидатів для подальшого використання.

Лінгвістичні методи базуються на значеннях слів, використовують онтології та семантичні дані про слово. З цим методом пов'язана низка проблем. По-перше, це трудомісткість виконання операцій аналізу текстів, що виконуються вручну. Крім того, цей метод вимагає від дослідника

великої кількості вільного часу для проведення досліджень, а також може виникнути значна кількість помилок та неточностей.

На основі чисельних даних про зустрічальність слова будується статистичний метод дослідження тексту. Головною перевагою статистичних методів є універсальність алгоритмів вилучення ключових фраз, відсутність необхідності у трудомістких процедурах побудови лінгвістичних баз знань, простота реалізації [2].

При використанні гібридних методик статистичні методи обробки доповнюються однією-двома лінгвістичними процедурами та лінгвістичною базою знань різної глибини. Цей підхід є комбінованим, оскільки він поєднує лінгвістичний та статичний методи.

Для того, щоб отримати спектральний аналіз, використовується перетворення Фур'є та карти усереднення – подібно до частотно-часового представлення сигналу від джерела, отриманого за допомогою вейвлет-перетворення. А це означає, що цей метод може працювати зі спектрограмою тексту, що містить новий якісний вигляд вмісту текстового файлу. У цьому методі відсутній ряд недоліків, властивих іншим методам. Наприклад нема потреби проводити складні процедури лексичного та морфолого-лінгвістичного дослідження, а також можна визначити місце ключового слова в тексті [3].

Отже, розглянуто чотири метода які мають як переваги, так і недоліки. Ключові слова є одним із найважливіших етапів у процесі класифікації та кластеризації документів, а також виявлення загальної теми документа. В останні роки розроблено різні підходи автоматизованого вилучення ключових слів та фраз, в основі яких лежать лінгвістичні чи статистичні методи. У їхньому аналізі зазначається, що створення ефективних екстракторів стане й надалі одним із ключових трендів комп'ютерної обробки текстів.

Список використаних джерел:

1. Лебідь В.М. Основні проблеми пошуку необхідного контенту при виборі сайтів (2021, 5 листопада) <https://ojs.ukrlogos.in.ua/index.php/liga/issue/view/inter-05.11.2021/629>

2. Мазурець О. В. Інформаційна технологія автоматизованого визначення семантичних термінів в елементах навчальних матеріалів / О. В. Мазурець // Вісник Хмельницького національного університету. Серія: Технічні науки. – 2018. – № 3. – С. 223–230.

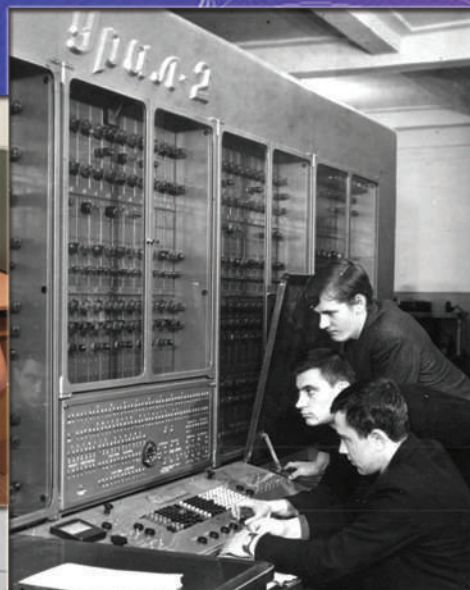
3. Современные методы автоматизированного извлечения ключевых слов из текста (б.д.). Взято 23 лютого 2022 з <https://www.academia.edu/30459750>

АЛФАВІТНИЙ ПОКАЗЧИК

В		Ш	
Verdnyk M.I.	16	Шкіренко Д.В.	30
А			
Андрющенко Д.Д	37		
Анісімов В.Е.	18		
Артьоменко А.О.	20		
Б			
Братищенко М.Р.	5		
З			
Задорожний А.Ю.	22		
К			
Кульков Б.І.	24		
Л			
Лебідь В.М.	39		
М			
Марініч К. Ю.	13		
Михальчук М.О.	7		
О			
Омельченко С. О.	35		
С			
Садовська А.О.	26		
Соколова В. К.	10		
Т			
Тарасенко В.С.	28		
Ч			
Чапарин І.М.	33		

ЗМІСТ

ФІЗИЧНИЙ КОМП'ЮТІНГ	4
ВІРТУАЛЬНИЙ КОМП'ЮТІНГ	9
ЗАХИСТ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІКС.....	12
МЕТОДИ І ЗАСОБИ ОБРОБКИ ДАНИХ У ГЕТЕРОКОМПОНЕНТ- НИХ КОМП'ЮТЕРНИХ СИСТЕМАХ І МЕРЕЖАХ.....	15
МЕТОДИ І СПОСОБИ ОБЧИСЛЮВАЛЬНОГО ІНТЕЛЕКТУ.....	33
АЛФАВІТНИЙ ПОКАЗЧИК	42



NURE