www.konferenciaonline.org.ua

Міжнародна наукова інтернет-конференція

"Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення" (випуск 29)

12 червня 2018 р.

Частина 1

Тернопіль – 2018

Міжнародна наукова інтернет-конференція "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 29)" / Збірник тез доповідей: випуск 29 (м. Тернопіль, 12 червня 2018 р.). Частина 1. – Тернопіль. – 2018. – 118 с.

УДК 001 (063)
ББК 72я431

ISSN 2522-932X

Збірник тез доповідей підготовлено за матеріалами Міжнародної наукової інтернет-конференції (випуск 29) від 12 червня 2018 р.

Збірник матеріалів науково-практичної інтернет-конференції включаються до наукометричної бази даних "РІНЦ/RSCI".

Наша адреса: Оргкомітет МНІК "Конференція онлайн"
а/с 1079, м. Тернопіль 46010
тел. моб. 068 366 0 525
e-mail: inetkonf@gmail.com

URL Інтернет-конференції: http://www.konferenciaonline.org.ua/

Архипова С.А., канд. техн. наук, доцент
Национальный технический университет Украины "Киевский политехнический институт им. Игоря Сикорского", г. Киев
Факультет социологии и права, кафедра философии, доцент

ПОСТРОЕНИЕ РЕГРЕССИОННЫХ МОДЕЛЕЙ ПРИ НЕПОЛНОЙ ИНФОРМАЦИИ О ПОГРЕШНОСТЯХ ИЗМЕРЕНИЙ

Рассматривается задача построения наилучшей модели $y = \mu(x_1, x_2, ...)$ в классе линейных регрессионных моделей по экспериментально полученным данным: матрице плана $[x_{ij}]$ и вектору $[z_i]=[y_i]+[e_i]$ результатов измерения значений зависимой переменной *Y*, наблюдаемой в присутствии аддитивного случайного шума *E*. Исследования выполняются на двухфакторном x_1, x_2 тестовом примере, объем выборки n=200 значений.

Последовательность значений $x_{i1}, i = \overline{1,n}$, задается программным генератором псевдослучайных чисел. Вектор точных значений переменной рассчитывается в соответствии с истинным уравнением регрессии

$$y = x_1 + x_2 + 0{,}04x_1^2 + 0{,}05x_2^2 + 0{,}003x_1x_2^2. \qquad (1)$$

Для селекции наилучшей модели применим один из вариантов процедуры регрессионного анализа, описанный в [1]. Оценивание параметров моделей производится методом наименьших квадратов (МНК). Процедуры селекции [3] сводятся к следующему:

(1) Модели регрессии, в зависимости от количества m_j входящих в них элементов, разбиваются на девять классов: А, Б, В, Г, Д, Е, Ж, З, И. Класс А представлен моделью среднего $y = a_0$. Класс Б включает модели, состоящие из одного регрессора, класс В – из двух регрессоров и т.д. Всего в девяти классах было отобрано и исследовано 29 моделей.

(2) Для каждой из 29-ти моделей рассчитывается средний квадрат ошибки аппроксимации $S^2 = 1/n \sum_{i=1}^{n} (z_i - \tilde{y}_i)^2$, где $\tilde{y}_i$ – модельное значение зависимой переменной.

(3) В каждом классе отбираются одна или несколько моделей, имеющих минимальные для этого класса значения S_j^2.

(4) Производится сопоставление моделей, проверка адекватности моделей исходным данным, проверка необходимости усложнения этих моделей. Конечная цель этого анализа – выбор структуры аппроксимативной модели.

В результате получен ряд минимальных в классах Б–И значений S_j^2:

257,41; 191,96; 142,92; 132,79; 121,49; 121,06; 120,24; 120,19.

Очевидно, с введением новых переменных в модель скорость уменьшения показателя S_j^2 замедляется. С этих позиций (согласно [1,2]) можно полагать адекватными модели в классах Г с тремя регрессорами ($S_Г^2$ =142,92) или Д с четырьмя регрессорами ($S_Д^2$ =132,79).

Эмпиризм подобного подхода обычно побуждает исследователя к поиску других способов селекции модели. При этом прибегают к априорному постулированию нормальности распределения погрешностей измерения E значения зависимой переменной Y, что позволяет сразу решить две проблемы: обосновать оптимальность применения МНК для оценивания параметров модели и использовать наработки классического регрессионного анализа по оценке качества линейной регрессии для селекции структуры модели.

Для проверки значимости уравнений регрессии применяют статистику

$$\tilde{F}_j = \frac{S_1^2/(n-1)}{S_j^2/(n-m_j)}, \qquad (2)$$

которая определяет во сколько раз исследуемая j-тая модель лучше предсказывает результаты эксперимента, чем среднее $\bar{y}$, т.е. модель $y(1) = a_0$ из класса А .

Расчет [3] значений $\tilde{F}_j$ для всех 29-ти моделей определяет максимальное значение $\tilde{F}_{27}$=4,58, что соответствует семиэлементной модели μ_{27} из класса З, что подтверждает только статистическую значимость этой модели по отношению к модели среднего, а не ее оптимальность.

Дальнейший подбор модели [1] основан на применении более сложного попарного сопоставительного анализа моделей j и r при поэлементном введении регрессоров в структуру модели по статистике

$$\tilde{F}_{j\to r} = \frac{S_j^2 - S_r^2}{S_r^2}\,\frac{n-m_r}{m_r-m_j}. \qquad (3)$$

Если теоретическое значение меньше $\tilde{F}_{j\to r}$ следует признать, что усложнение модели приводит к значимому росту ее качества.

По результатам исследований [3] можно предположить, что наиболее адекватны исходным данным шестиэлементные модели класса Ж.

Если сопоставить итог селекции моделей по показателю $\tilde{F}_{j\to r}$ с моделями, отобранными по показателю S^2, очевидно наличие существенных различий в сложности отобранных групп моделей: область возможных решений перекрывает четыре класса Г, Д, Е, Ж. Признать удовлетворительным подобный результат нельзя из-за содержащейся в нем значительной неопределенности. Необходимо проведение дополнительных исследований, позволяющих радикально сузить эту область.

Один из возможных способов уточнения вида модели состоит в проверке значимости найденных оценок коэффициентов моделей [2,4], целиком базирующейся на гипотезе нормальности погрешности.

Поэтому актуальным представляется вопрос о возможности проверки гипотезы нормальности распределения погрешности значений зависимой переменной. В частности, для этого в [2] рекомендуется проверка нормальности остатков (невязок) $\varepsilon_i = z_i - \tilde{y}_i$. Однако, как показали исследования, описанные в статье [3], если для параметрической идентификации параметров модели (1) использовался МНК, в подавляющем большинстве случаев, независимо от вида исходного закона распределения погрешности e_i, распределения невязки ε_i как правило оказывается нормальным. Другими словами, применение МНК обуславливает эффект нормализации невязки.

Таким образом, если следовать рекомендациям [2], то практически всегда будет принята гипотеза нормального распределения погрешностей в значениях зависимой переменной, из чего очевидно будет следовать нормальность распределения оценок параметров исследуемой модели.

Результаты исследований позволяют сделать следующие выводы:

– процедура классического регрессионного анализа не содержит способов надежной селекции структуры модели при отсутствии априорных сведений о нормальности погрешности E;

– апостериорное утверждение о принятии гипотезы нормальности остатков регрессии не гарантирует нормальности исходной погрешности E и, следовательно, не может служить обоснованием принятия положений регрессионного анализа, опирающихся на нормальность распределения E, в частности, гипотезы о нормальности распределения оценок параметров и базирующихся на ней методов проверки значимости оценок и модели регрессии;

– при отсутствии априорной информации о виде распределения погрешности измерений следует применять методы структурной идентификации свободные от вида распределения.

Литература

1.Себер Дж. Линейный регрессионный анализ. - М.: Мир, 1980.- 456с.

2.Львовский Е.Н. Статистические методы построения эмпирических формул. - М.: Высш. школа, 1982. - 224с.

3.Архипов А.Е., Архипова С.А. О некорректности параметризации распределений оценок при решении задачи идентификации. //Адаптивні системи автоматичного управління. Межвідом. науково-техн. зб. - Дніпропетровськ: Системні технології, 1999. - Вип.2(22). - с. 114-121.

Балалаева Е.Ю., к.т.н.,
ГВУЗ «Приазовский государственный технический университет»,
г. Мариуполь,
Кафедра информатики, доцент
Вакуленко Т.В. ,
ГВУЗ «Приазовский государственный технический университет»,
г. Мариуполь,
Кафедра информатики, студентка группы ВТ-17-М

ПРИМЕНЕНИЕ АЛГОРИТМОВ НЕЧЕТКОЙ ЛОГИКИ ДЛЯ СОЗДАНИЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ МЕДИЦИНСКОЙ ДИАГНОСТИКИ

Особенностью медицинской предметной области является наличие нечетких информационных составляющих, таких как субъективные сведения, сообщаемые больным; данные объективно-субъективного обследования врачом; результаты заключений по результатам исследований; образные визуальные представления и гипотезы и т.д. Исходя из этого для реализации информационных систем медицинской диагностики целесообразно использовать методы нечеткой логики.

Формальное представление понятий и данных осуществляется с помощью нечетких множеств и функций принадлежности к данному нечеткому множеству. При формальном представлении клинических признаков используются нечеткие порядковые шкалы, называемые лингвистическими. Они представляют собой дескриптивную, иерархическую модель триады, включающую понятие, его значение и смысл.

Нечеткая логико-лингвистическая система включает в себя набор значений входных и выходных лингвистических переменных, которые связаны между собой эвристическими правилами. Нечеткие логические выводы представляют собой способ обработки информации на базе экспертных правил, задаваемых в нечетком виде, и создают модель приближенных рассуждений человека. Нечеткий классификатор является базой нечетких правил, его настройка сводится к решению задач оптимизации. Настройка функции принадлежности осуществляется с помощью генетических и иммунных алгоритмов.

Обозначим множество всех болезней через $X = \{X_i, 1\ldots m\}$, а множество всех симптомов $Y = \{Y_j, 1\ldots n\}$. Пусть X_i – наличие болезни; Y_j – наблюдается симптом; R_{ij} – соответствие болезни X_i симптому Y_j.

Получим следующие утверждения:

$P_j\Delta''Y_j \rightarrow OR(R_{ij}\&X_i)$ – «Если есть симптом Y_j, то на основании взаимосвязи R_{ij} между болезнями и симптомами проявляется по крайней мере болезнь X_i.»;

$P_{jj}\Delta''(R_{ij}\&X_i) \rightarrow Y_j$ – «Если на основании взаимосвязи R_{ij} между болезнями и симптомами проявляется болезнь X_i, то есть симптом Y_j.».

Достоверности R_{ij}, P_j, P_{jj} выражены в форме лингвистических значений истинности (от «очень правдивое» до «очень ложное»).

Преимуществами использования нечетких систем в медицинской диагностике являются возможность использования нечетких входных данных, нечеткой формализации критериев оценки, а также возможность быстрого моделирования динамических систем с заданной точностью.

Литература

1. Кореневский Н.А. Использование нечеткой логики принятия решений для медицинских экспертных систем / Н.А. Кореневский // Медицинская техника, 2015. – № 1. – С. 33-35.
2. Пурський О.І. Особливості застосування інформаційних систем в медицині: експертні системи / О.І. Пурський // І Міжнар. наук.-техн.конф. «Обчислювальний інтелект», м. Черкаси, 10-13 травня 2011 р. – Черкаси: ЧДТУ, 2011. – С. 364
3. Абдулаева З.И. Применение нечётких множеств и мягких вычислений в медицинской статистике / З.И. Абдулаева // Медицинские науки, 2016. – № 51-1. – С. 237-238.
4. Кобринский Б.А. Нечеткость в клинической медицине и необходимость ее отражения в медицинских системах / Б.А. Кобринский // Врач и информационные технологии, 2016. – № 5. – С. 6-14.
5. Nieto J.J. Fuzzy logic in medicine and bioinformatics / J.J. Nieto, A. Torres. – Journal of biomedicine & biotechnology, 2006. – http://www.biomedsearch.com/nih/Fuzzy-logic-in-medicinebioinformatics/16883057.html.

Бондаренко В.А., студент
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»
Кафедра біомедичної кібернетики

ДЕРЖАВНА ПОЛІТИКА ВПРОВАДЖЕННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ГАЛУЗЬ МЕДИЦИНИ УКРАЇНИ

Згідно закону «Про державні фінансові гарантії надання медичних послуг та лікарських засобів» (реєстраційний номер 6327) з 1 січня 2018 року в Україні почала діяти медична реформа. В рамках цієї реформи в дію була впроваджена електронна система охорони здоров'я eHealth, яка забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією в електронному вигляді.

Система eHealth складається з центрального компонента (ЦБД), що відповідає за централізоване зберігання та обробку інформації, та медичних інформаційних систем (МІС), які лікарні та поліклініки можуть обирати на ринку і встановлювати в себе.

Центральний компонент, що був розроблений Проектним офісом, з лютого 2018 року контролюється державою. Адміністратором eHealth системи є створене з цією метою державне підприємство «Електронне здоров'я». Адміністратор вимагає від розробників МІС строго дотримуватися вимог до надійності, безпеки та конфіденційності даних, якими їхні системи обмінюватимуться з центральним компонентом [1].

На сьогодні eHealth пропонує 13 МІС, що пройшли перевірку та задовольняють необхідні вимоги, щоб бути під'єднаними до центрального компонента [2].

Ці рішення забезпечують можливість реєстрації медичних закладів, лікарів та декларацій у ЦБД, можливість через електронні кабінети створювати, вносити, переглядати рецепти, напрямки, медичні записи та інші документи. Системи перевіряються на належний рівень захисту інформації, збереження, автоматичне резервування і відновлення даних, які передавалися до ЦБД, облік операцій з інформацією і документами в ній, а також змін, які відбуваються в системі і стосуються її безпеки. Система має бути сумісна з деякими іншими інформаційними ресурсами, зокрема з єдиним державними демографічним реєстром, ЄДР юридичних осіб, фізичних осіб підприємців та громадських формувань, а також реєстром актів цивільного стану громадян[3].

eHealth почала працювати в тестовому режимі ще з вересня 2017 року, коли стало технічно можливо зареєструвати у системі медичний заклад, лікарів, а також ввести дані декларацій пацієнтів. Цей етап тривав до квітня 2018 року.

Її впровадження поділено на 4 етапи:

Перший етап:

- Запуск в тестовому режимі функціоналу «капітація».
- Затвердження необхідної нормативної бази для тестового режиму.
- Підготовка довгострокової стратегії розвитку eHealth.
- Підготовка ТЗ для отримання сертифікату КСЗІ,

Другий етап:

- Запуск в пілотному режимі підтримки програми «Доступні ліки».
- Створення ДП, яке стане адміністратором системи.
- Проведення міграції готових компонентів системи в український центр обробки даних
- Передача системи на ДП
- Узгодження бізнес-моделі для розробників МІС

Третій етап:

- Отримання сертифікату КСЗІ
- Забезпечення нормативно-правовою базою для функціонування системи.
- Проведення навчання лікарів щодо переходу на нову систему фінансування.

Четвертий етап:

- Капітаційні виплати на основі даних з системи.

На сьогоднішній день триває другий етап впровадження eHealth в дію. Вже 1233 медичних заклади, 21656 лікарів та 7821327 пацієнтів приєдналися до eHealth (станом на 10 червня 2018 року)[4]. З 1 липня 2018 року оплата послуг лікарів буде здійснюватися згідно з кількістю декларацій, зареєстрованих у системі.

Зміна моделі фінансування первинної ланки медицини, яка реалізується в ході медичної реформи, є в даний час головним стимулятором для впровадження медичних інформаційних систем у медицині. Це стосується не тільки державних, але й приватних медичних закладів, тому що вони також можуть претендувати на державні гроші для оплати обслуговування пацієнтів.

Використання медичних інформаційних систем, окрім надання можливості створення єдиних реєстрів при їх під'єднанні до центрального компоненту системи, допомагає значно оптимізувати всі процеси в медичних закладах. eHealth допоможе пацієнтам отримувати, а лікарям – надавати якісні медичні послуги, зробити медицину в Україні ефективною та прозорою.

Література

1. Нова система фінансування первинної ланки охорони здоров'я та електронна система eHealth [Електронний ресурс] // Юридична Газета Online. – 2018. – Режим доступу до ресурсу: http://yur-gazeta.com/publications/practice/medichne-pravo-farmacevtika/stavka-na-yakist.html.
2. eHealth.Долучитися [Електронний ресурс] // – Режим доступу до ресурсу: https://portal.ehealth.gov.ua/providers.html
3. Проект постанови КМУ «Про затвердження порядку функціонування електронної системи охорони здоров'я» [Електронний ресурс] // Аптека.ua. – 2018. – Режим доступу до ресурсу: https://www.apteka.ua/article/450829.
4. eHealth.Статистика [Електронний ресурс] // – Режим доступу до ресурсу: https://portal.ehealth.gov.ua/#statistic.

Гораш М.А.
Вінницький національний технічний університет, м. Вінниця
Кафедра системного аналізу, комп'ютерного моніторингу та інженерної графіки

РОЗРОБКА ІНФОРМАЦІЙНО-АНАЛІТИЧНОЇ СИСТЕМИ МОНІТОРИНГУ СТАНУ АРХІТЕКТУРНИХ ОБ'ЄКТІВ

Використання сучасних інформаційних технологій, раціональна організація функціонування інформаційно-аналітичних систем – важливий напрям удосконалення роботи підприємств та установ.

Питання створення інформаційно-аналітичних систем моніторингу стану архітектурних об'єктів розроблялися такими видатними вітчизняними та зарубіжними науковцями. Були визначені принципи та напрями використання сучасних інформаційних технологій для раціоналізації документообігу, проте питання вибору критеріїв та моделей для управління процесами документообігу висвітлені недостатньо і потребують подальшої розробки.

Розв'язання задач розробки моделей та інформаційної технології, що здійснюють управління процесами моніторингу стану архітектурних об'єктів з метою зниження витрат часу та трудомісткості їхнього виконання, пов'язане з підвищенням ефективності функціонування органів державної влади, місцевого самоврядування та інших державних інститутів та установ України. Необхідність формування концепції управління процесами створення інформаційно-аналітичних систем визначає актуальність дослідження цієї теми.

Математично форму заповнення ІАС можна зобразити у вигляді формули (1):

$$F = W_1 \pm W_2 \pm W_3 \pm W_4 \pm W_5 + W_6, \quad (1)$$

де W_1 – вкладка «Загальні відомості»; W_2 – вкладка «Майнове право»; W_3 – вкладка «Земельна ділянка»; W_4 – вкладка «Балансоутримувач»; W_5 – вкладка «Технічні характеристики»; W_6 – вкладка «Карта».

Кожну вкладку ІАС можна подати за допомогою математичної моделі. Кожна вкладка – множина полів, а рівнянням записано – відношення полів. І вони подаються такими рівняннями (2-7).

$$W_1 = T + N + S \pm H \pm G \pm P \pm C \pm V + K + Z \quad (2)$$

$$W_2 = \pm Q \pm P \pm L \pm J \pm U \quad (3)$$

$$W_3 = \pm S \pm N \pm D \pm T \pm R \pm M \pm K \pm Y \pm K \pm Z \quad (4)$$

$$W_4 = \pm M \pm N \pm B \pm C \pm F \pm H \pm J \pm K \pm L \pm U \pm Y \quad (5)$$

$$W_5 = \pm H \pm S \pm A \pm Z \pm E \pm W \pm Q \pm G \quad (6)$$

$$W_6 = X + Y \pm D_x \pm D_y \quad (7)$$

Інформаційно-аналітична система, яка була розроблена за даною моделлю використовується для моніторингу стану архітектурних об'єктів у місті Вінниці, а також для збереження даних про об'єкти в електронному вигляді на серверах.

Список використаної літератури

1. Перевозчикова О. Л. Сучасні інформаційні технології / О. Л. Перевозчикова. – Київ, 2002. – 121 с.

2. Білова Т. Г. Інформаційна технологія управління процесами документообігу / Т. Г. Білова // Новітні інформаційні технології в освіті : матеріали міжвузівської наук. конф. –Харків : ХДАК, 2008. – С. 52-55.

Доброштан Мирослав Володимирович
Освітній ступінь - магістр
Національна академія Служби безпеки України
Навчально-науковий інститут інформаційної безпеки

ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ЛЮДИНИ

Анотація: У статті розглядаються питання сутності, ролі та значення інформаційних прав людини, їх види, особливості правового механізму захисту інформаційних прав людини.

Ключові слова: інформація, право на інформацію, інформаційні права, види інформаційних прав, інформаційна безпека, інформаційні правовідносини.

Аннотация: В статье рассматриваются вопросы сущности, роли и значения информационных прав человека, их виды, особенности правового механизма защиты информационных прав человека.

Ключевые слова: информация, право на информацию, информационные

права, виды информационных прав, информационная безопасность, информационные правоотношения.

Summary: The article deals with the issues of the essence, role and meaning of information rights of people, their types, features of the legal mechanism of protection of information rights of people.

Key words: information, right to information, information rights, types of information rights, information security, information legal relations.

Постановка проблеми. У сучасному суспільстві інформація займає провідне місце та вважається визначним стратегічним ресурсом. Сьогодні Україна переходить від індустріального суспільства до інформаційного, тому зростання ролі інформації, її вільний кругообіг в державі, а також поза її межами стає важливим питанням.

Становлення та розвиток інформаційних засад соціуму припускає наявність сукупності передумов, що забезпечують його оновлення і розвиток. Основною умовою зазначеного процесу є юридично оформлений захист інформаційних прав людини. У зв'язку з цим дослідження питань правового механізму захисту інформаційних прав людини є досить актуальним.

Метою статті є удосконалення науково-методичних підходів і розробка практичних рекомендацій щодо правового механізму захисту інформаційних прав людини.

Дослідження проблеми. Проблемам інформаційних прав людини присвячено багато наукових робіт, зокрема таких вчених, як Н.Г. Александрова, С.С. Алексєєва, А.І. Арістової, М.І. Байтіна, О.О. Баранова, К.І. Бєлякова, В.М. Брижко, О.П. Дзьобань, А.В. Малько, Н.І. Матузова, В.С. Нерсесянц, В.Г. Пилипчука, Ю.С. Решетова, Н.А. Савінової, А.Ф. Черданцева, В.М. Фурашева та інших.

Проте, віддаючи належне теоретичній та практичній цінності попередніх наукових здобутків, існує досить багато невирішених питань, особливо щодо правового механізму захисту інформаційних прав людини.

Виклад основного матеріалу.

Згідно Закону України «Про інформацію» від 02.10.1992 № 2657-XII інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [2].

Вперше поняття «право на інформацію» було визначено також у Законі України «Про інформацію», а саме: «Кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів. Реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб» [2].

Закон України «Про інформацію» – це перший в державі закон, який заклав правові основи інформаційної діяльності, визначив головні напрями державної інформаційної політики, закріпив право громадян України на інформацію і визначив правові форми міжнародного співробітництва в галузі

інформації.

Основою національного законодавства є Конституція України, в нормах якої відображені основні права, свободи та інтереси людини.

У Конституції України зазначено, що право людини на інформацію - самостійне конституційне право, яке дозволяє людині вільно збирати, зберігати, використовувати і поширювати інформацію будь-яким способом, що гарантується ч. 2 ст. 34 Конституції України [1].

Існує два шляхи виникнення інформаційних прав і свобод людини у правовій системі української держави:

1) шляхом ухвалення нових нормативно-правових актів внутрішньо державного характеру, що закріплюють нові інформаційні права людини і громадянина;

2) шляхом ратифікації міжнародних угод, що містять нові інформаційні права людини і громадянина [5, с. 22].

Виділяють наступні види інформаційних прав людини, що закріплюються конституційними нормами.

1. Свобода особистого і сімейного життя (ст. 32);

2. Таємниця листування, телефонних переговорів, телеграфної й іншої кореспонденції (ст. 31);

3. Право громадянина не зазнавати втручання в його особисте та сімейне життя, шляхом збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, знайомитися в органах державної влади, органах місцевого самоврядування, установах та організаціях із відомостями про себе (ст. 32);

4. Право громадянина направляти індивідуальні або колективні письмові звернення або особисто звертатися в органи державної влади, органи місцевого самоврядування та до посадових і службових осіб цих органів (ст. 40);

5. Право кожного громадянина на сприятливе навколишнє середовище, достовірну інформацію про її стан (ст. 50);

6. Право кожного на свободу творчості і право доступу до культурних цінностей (ст. 54);

7. Право кожного громадянина на одержання кваліфікованої правової допомоги (ст. 59) [4, с.200].

Правовий механізм захисту інформаційних прав людини поділяється на нормативно-правовий та організаційно-правовий.

Нормативно-правова форма виражається в ухваленні нормативно-правових актів або у внесенні до існуючих нормативно-правових актів таких змін, які можуть сприяти здійсненню захисту інформаційних прав людини і громадянина [5, с. 22].

Елементами нормативно – правового механізму захисту інформаційних прав є: нормативне закріплення здійснення правового захисту інформаційних прав людини і громадянина; юридичний факт, який дозволяє почати процес правового захисту інформаційних прав людини і громадянина; правовідносини, в яких є права та відповідні ним обов’язки; суб’єкти правового механізму

захисту інформаційних прав людини і громадянина; об'єкти правового механізму захисту інформаційних прав людини і громадянина [5, с. 23].

Організаційно-правова форма виражається в діяльності державних органів, що беруть участь у процесі захисту прав інформаційної людини і громадянина на території України.

Основна роль належить Президентові України, Верховній Раді України, органам виконавчої влади, правоохоронним органам, а також інститутам громадського суспільства. Роль Президента України в організаційно-правовому механізмі захисту інформаційних прав і свобод людини і громадянина в Україні обумовлена тим, що він є гарантом прав і свобод людини в українській державі. Роль органів виконавчої влади в організаційно - правовому механізмі захисту інформаційних прав і свобод людини і громадянина визначається в організації виконання норм Конституції України і законів, також вона реалізується через аналітичну роботу [1].

Особливе місце в організаційно-правовому механізмі захисту інформаційних прав людини відводиться правоохоронним органам (судам, прокуратурі, органам МВС, адвокатурі, нотаріату), які відіграють найактивнішу роль у захисті інформаційних прав і свобод людини і громадянина [5, с. 23].

Існує ціла низка проблемних питань, які виникають під час судового захисту інформаційних прав людини, серед яких: складність розмежування підсудності справ щодо захисту прав особи на звернення та доступ до публічної інформації; застосування судами не передбачених чинним законодавством способів судового захисту права на повагу до честі, гідності та ділової репутації особи; відсутність у чинному законодавстві засобів доказування поширення інформації в мережі Інтернет; відсутність у законодавстві визначення меж інформації, що становить суспільний інтерес; юридична невизначеність у частині можливостей втручання держави в приватне життя особи та використання її персональних даних тощо [3, с. 30].

Висновки. Отже, для подальшого удосконалення та підвищення ефективності правового механізму захисту інформаційних прав людини пропонуємо:

– ухвалити закон, яким регулюватимуться умови і порядок реалізації права на інформацію, що, у свою чергу, дозволить скоротити обсяг підзаконного правового регулювання;

– створити інститут спеціалізованого Уповноваженого із захисту інформаційних прав людини;

– створити спеціалізовані суди, діяльність яких буде пов'язана із захистом інформаційних прав і свобод людини і громадянина (інформаційних судів);

– провести уніфікацію переліку підстав для обмежень інформаційних прав і свобод людини і громадянина та створити перелік випадків їх прямого обмеження з подальшим закріпленням в законодавстві.

Список використаних джерел:

1. Конституція України від 28.06.1996 № 254к/96-ВР
2. Про інформацію: Закон України від 02.10.1992 № 2657-XII

3. Куруц В. М. Деякі особливості судового захисту інформаційних прав людини / //Судова апеляція. – 2014. - №2(35). - С. 25-32
4. Ліпкан В.А., Максименко Ю.Є., Желіховський В.М. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. – К.: КНТ, 2006. – 280 с.
5. Настюк В.Я., Бєлєвцева В.В. Правовий захист інформаційних прав і свобод людини в Україні: проблеми та перспективи / В.Я. Настюк, В.В. Бєлєвцева // Інформація і право. – 2015. – № 2(14). – С. 20-25

Драбинко В.П.
Національний технічний університет України «КПІ ім. І. Сікорського», м. Київ
Кафедра автоматики і управління в технічних системах, студент

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ У ПРОЦЕСІ ОСВІТИ У ВИЩИХ НАВЧАЛЬНИХ ЗАКЛАДАХ

В нинішніх реаліях інформаційно-комунікаційні технології (ІКТ) впливають на всі сфери життя людини. Особливо вплив відчувається у вищих навчальних закладах. ІКТ надають нові можливість для студентів та викладачів, такі як покращення якості подачі матеріалу чи індивідуальний розвиток особистості. Зважаючи на те, що Україна ще молода країна, що розвивається потенціал ІКТ розкритий лиш трохи.

Існує декілька способів, як ІКТ інтегруються в освітній процес. Одним з найбільш популярних є так зване електронне навчання: - це навчальна програма, яка використовує інформаційну мережу – таку як Інтернет, інтранет (LAN) або екстранет (WAN) повністю або частково для доставки знань та взаємодії з викладачем. Веб-навчання є підмножиною електронного навчання і відноситься до навчання, що використовує різні веб-засоби для досягнення кінцевої цілі.

Інший вид це - змішане навчання, що складається з двох частин – практика в класі, коли ти обличчя-до-обличчя з викладачем та електронне навчання. Наприклад, вчитель може сприяти навчанню студентів у класовому контакті і використовує певне модульне динамічне навчальне середовище для самостійного опрацювання матеріалу.

І два останніх способи це конструктивізм та навчальне середовище. Конструктивізм - це парадигма навчання, яка передбачає навчання як процес навчання на основі попередніх знань та досвіду. Навчально-орієнтоване навчальне середовище - це середовище, яке приділяє увагу до знань, навичок і поглядів, з якими студенти прийшли до навчального закладу, це означає, що студенти самостійно залучаються до навчального процесу, використовуючи комп'ютер та підключення до Інтернету.

Використання ІКТ надає великі переваги у навчанні для студентів та викладачів. Інститути в західному світі зробили багато інвестицій в інфраструктуру ІКТ в останні 20 років. Тому там студенти використовують комп'ютери частіше і мають ширший спектр можливостей, ніж студенти з України. Кілька досліджень показують, що студенти, які використовують ІКТ у

навчальному процесі, отримують більше якісних знань, ніж ті, хто не ними не користується.

Наприклад, проведені дослідження у Сполучених Штатах показали наступні результати. Студенти, які використовували комп'ютерні підручники з математики, природничих та соціальних наук, мали значно вищі бали з тестів в цих темах. Студенти, які використовували програмне забезпечення для моделювання, при вивчені певних матеріалів, також мали кращі бали. Також слід зазначити, що студенти, які використовують текстові процесори для написання текстів, мають вищий рівень письмової майстерності.

Таким чином, використання ІКТ у сфері освіти надихнуло на появу нове покоління інформаційно-освітніх технологій, що дозволило поліпшити якість навчання, створювати нові засоби впливу та ефективніше взаємодіяти з учнями. Як вважає більшість науковців, нові інформаційні технології, засновані на комп'ютерних засобах, дозволяють значно підвищити ефективність навчання. Тому Україні необхідно і надалі рухатися в даному напрямку.

Список використаних джерел

1. Биков В.Ю. Моделі організаційних систем відкритої освіти : монографія / В.Ю. Биков. – К. : Атіка, 2009. – 684 с.
2. Заболотний В.Ф. Дидактичні засади застосування мультимедіа у формуванні методичної компетентності майбутніх учителів фізики : автореф. дис. на здобуття наук. ступеня докт. пед. наук : спец. 13.00.02 “Теорія та методика навчання (фізика)”/В.Ф. Заболотний . – Київ. – 2010. – 38 с.

Дрегало Л.В.
Національний технічний університет України «КПІ» ім. І. Сікорського, м. Київ
Кафедра автоматизованих систем обробки інформації та управління, студент

ОПТИМІЗАЦІЯ ВИКОРИСТАННЯ РЕСУРСІВ СХОВИЩ ДАНИХ

Одним із найяскравіших новітніх трендів у галузі інформаційних технологій є зберігання та обробка величезних масивів даних на віддалених серверах (у «хмарі»). Сучасні дослідження у галузі мережевих систем відкривають нові можливості для високошвидкісної передачі даних на великі відстані [1]. Це дозволяє серверам і клієнтам обмінюватись петабайтами корисної інформації. Водночас зростають і вимоги до швидкості обробки даних. Наприклад, у фінансовій індустрії отримання аналітики та прийняття рішення на мілісекунди раніше за конкурентів може означати прибуток у мільярди доларів [2].

У хмарних сховищах дані зберігають на фізичних носіях інформації, аналогічних за принципом роботи тим, що використовуються в персональних комп’ютерах. Це, як правило, жорсткі диски (HDD) – пристрої, на яких інформація записується і зчитується за допомогою механічних частин. Все більшого розповсюдження набувають швидкісні носії інформації, побудовані на NAND-елементах (SSD).

Перевагою SSD перед HDD:

– швидкодія: швидкості читання й запису можуть досягати 550 MB/s (для порівняння, до 120 MB/s на HDD);

– відсутність рухомих механічних і магнітних частин, що робить SSD набагато менш чутливим до дії магнітних полів, фізичного впливу, а також більш енергоефективними і безшумними.

Недоліки SSD відносно HDD:

– ціна (приблизно $0.20 за гігабайт, при ціні HDD близько $0.03 за гігабайт);

– обмежена кількість циклів запису: кожен заново записаний файл збільшує ймовірність відмови пристрою [3].

На сьогодні більш популярним рішенням для побудови сховищ даних є HDD, не в останню чергу через свою відносну дешевизну [4]. Проте розповсюдження високошвидкісних мереж та підвищення вимог до швидкості обробки даних вимагають пошуку нових рішень для зберігання інформації в сховищах даних.

Через названі вище недоліки SSD побудова сховища даних на їх основі є економічно недоцільною та технічно складною. Для конструювання високошвидкісного сховища даних необхідно використати комбінацію SSD та HDD. Це дозволить максимально використати переваги обох видів накопичувальних пристроїв.

Інструментом оптимізації ресурсів такого комбінованого сховища даних є алгоритми, що зменшують кількість записів на SSD, зберігаючи тимчасові дані на HDD. Лише постійні, архівні дані, або дані, до яких потрібен швидкий доступ, надходять на SSD. Втілення таких алгоритмів на рівні файлової системи дозволить серйозно оптимізувати швидкодію і зменшити вартість побудови сховищ даних.

Отже, оптимізація використання ресурсів сховищ даних – це перспективний напрямок досліджень, що має пряме прикладне значення.

Література

1. Chen Z. Use of polarization freedom beyond polarization-division multiplexing to support high-speed and spectral-efficient data transmission / Zhi-Yu Chen. // Light: Science & Applications. – 2017. – №6.

2. Menkveld A. J. Need for speed? Exchange latency and liquidity. / A. J. Menkveld, A. Z. Marius. // The Review of Financial Studies. – 2017. – №30. – с. 1188–1228.

3. Schroeder B. Reliability of NAND-based SSDs: What field studies tell us. / B. Schroeder, A. Merchant, R. Lagisetty. // Proceedings of the IEEE. – 2017. – №106. – с. 1751–1769.

4. Wah T. Building data warehouse / T. Wah, S. Ching, H. Ng. // Proceedings of the 24th South East Asia Regional Computer Conference. – 2007. – №15.

Елізаров Анатолій Борисович
Гасімов Фархад Мікель Огли
Національний авіаційний університет, студент
(Київ, Україна)

ЗАХИСТ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЕМСТВА ЗА РАХУНОК СТВОРЕННЯ VPN ТУНЕЛЮ

На даний час проблема забезпечення інформаційної безпеки постає дуже гостро. З поширенням і розвитком технологій почався процес відмови від традиційного укладу праці в офісі, який зробив роботу та передачу даних більш зручною, але більш схильною до витоку інформації. Для побудови будь-якої захищеної корпоративної інфраструктури потрібно вирішити ряд складних питань. Корпоративна інфраструктура базується у першу чергу на аналізі організаційно-штатної структури підприємства, функцій посадових осіб, топології корпоративної мережі, степені секретності інформаційних ресурсів, апаратного та програмного забезпечення.

Одночасно з сильним зростанням ролі Інтернету в житті підприємства, виникає серйозна небезпека витоку персональних даних працівників, комерційної таємниці, корпоративних ресурсів, баз даних клієнтів і т.д. На сьогоднішній день багато корпорацій та малих фірм користуються послугами хакерів для отримання переваги над своїми діловими конкурентами. Робота цих зловмисників з року в рік стає легшою. Цьому сприяють два основні чинники.

По-перше, це проникнення Інтернету в майже усі сфери людського життя. Сьогодні до мережі Інтернет підключені мільйони пристроїв, і ще більше пристроїв будуть підключено до нього в найближчому майбутньому, тому можливості доступу зловмисників до уразливих пристроїв стають біль широкими з кожним роком. Крім того, глобальна мережа Інтернет дозволяє хакерам обмінюватися інформацією один з одним в режимі реального часу, і створювати злочині групи.

По-друге, це щонайширше розповсюдження простих у використанні операційних систем і середовищ розробки. Даний чинник різко знижує рівень необхідних хакерові знань і навиків. Також потрібно мати на увазі що кожна програма має свої вразливі місця, і тому творці програм часто випускають нові версії, і люди, котрі не обновили своє програмне забезпечення безпосередньо підпадають під загрозу втратити свої дані. Щоб створювати і поширювати прості програми, хакер може і не володіти достатніми знаннями у сфері програмування. Через спеціальні форуми, де зловмисники здійснюють обмін шкідливими програмами, будь-який хакер може заволодіти програмою, за допомогою якої буде проводити незаконні дії. Щодня хакери здійснюють атаки на мало захищенні важливі ресурси, намагаючись дістати доступ до них за допомогою спеціалізованих програм.

При застосуванні таких класичних засобів управління інформаційною безпекою, як антивірусне програмне забезпечення, засоби шифрування інформації, міжмережеві екрани тощо, знижується ризик несанкціонованого

доступу до секретної інформації. В випадку створення корпоративної мережі існує проблема так званого Соціального чинника. Людина яка має доступ, або працює з секретною інформацією є найбільш уразливою ланкою в усій системі захисту корпоративної мережі, і зловмисники можуть використати це за допомогою так званої соціальної інженерії. Проблеми які виникають через робітників фірми можна розділити на випадкові та спеціальні. Випадкові проблеми виникають через помилки, які допускають працівники через свою необачність або халатність. Типовим прикладом такої проблеми може бути простий пароль, який хакер може зламати шляхом грубого перебору, або з використанням так званого словника, - файлу який вже містить список найбільш уживаніших паролів. Для того, щоб уникнути таких проблем, потрібен комплексний підхід до створення паролів для різних рівнів доступу до різних пристроїв на фірмі. Для цього в компаніях вводять систему централізованої видачі унікальних паролів, які відповідають потребам складності та кількості символів, а також установлюють жорсткі корпоративні правила для робітників фірми і адекватні заходи покарання за недотримання правил. Соціальна інженерія дає змогу зловмисникам вчинити злочин, при тому не боячись бути пійманими.

Основна доля витоку інформації з підприємств припадає на злочини, які були вчинені за допомогою використання схем соціальної інженерії. Інформацію не завжди необхідно красти, дуже поширені випадки, коли зловмисники не крали дані з серверів, але знищували їх, чи змінювали інформацію, тим самим завдаючи матеріальні збитки жертвам атаки, в результаті яких жертви ще й втрачали багато часу на відновлення інформації. На сьогоднішній день широке розповсюдження технології Інтернет дозволяє кіберзлочинцям обмінюватися інформацією в режимі реального часу. Вже давно існують потужні міжнаціональні форуми хакерів, де вони обмінюються інформацією про вразливі ресурси, і організують групи для атаки на них. Також потрібно розуміти, що мережа майже ніким не контролюється, і тому зловмисники мають повний спектр можливостей в Інтернеті.

Ще однією причиною уразливості сучасних мереж є використання застарілого програмного забезпечення. Для багатьох програмних продуктів, які мають діло з даними користувача постійно випускають нові версії продукту, де закривають знайденні раніше уразливі місця. Тому, якщо в людини стоїть не оновлене програмне забезпечення, вона дуже підвернена атаці з боку зловмисників, бо хакери вже знають уразливі місця в цій версії програми. Це дозволяє зловмисникам створювати універсальні інструменти для злому. Найбільш доцільним методом захисту є профілактика зломів, бо виявлення хакера після того, як він вже зламав систему і знищив дані, не дасть потрібного результату. Томі найбільш ефективним методом боротьби з зловмисниками буде не допустити їх проникнення в мережу. З розвитком систем зв’язку все більш значущим стає бездротовий зв'язок. Тому на даний момент багато фірм, які забезпечують інформаційну безпеку, уділяють все більше уваги стандартам бездротового зв’язку. Мережні атаки такі ж різноманітні, наскільки різноманітні системи, проти яких вони направлені. Атаки також розділяють за їх цілю,

найпростіші атаки такі як , наприклад, DDOS-атака можна перервати простим відключенням серверів, або за допомогою вбудованої утиліти, яка відмовляє в доступі новим користувачам, якщо бачить, що за короткий час на сервер поступає дуже багато запитів, і розуміє, що це так звана атака обмеження доступу.

Перед тим, як розпочати атаку, зловмисники звичайно проводять мережеву розвідку, під час якої шукають слабкі місця в системі інформаційного захисту. Для того, щоб перевірити систему на слабі місця, хакери проводять сканування портів, запити DNS, ехо-тестування розкритих за допомогою DNS адрес і т.д. За допомогою цих дій, зловмисники можуть з'ясувати, кому належить той або інший домен і які адреси цьому домену привласнені. За допомогою технології ехо-тестування адрес, розкритих за допомогою DNS, хакери можуть побачити, які хости реально працюють в даній мережі, а засоби сканування портів дозволяють скласти повний список послуг, підтримуваних цими хостами.

На думку фахівців основні тенденції розвитку галузі захисту корпоративних мереж найближчими роками будуть такі:

1. Основними загрозами для корпоративних мереж становляться саме “внутрішні” загрози, а не “зовнішні”.

2. Розвиватимуться і удосконалюватимуться апаратні засоби захисту від хакерських атак. На ринку з'явиться новий клас мережевого устаткування — "захисні сервісні комутатори". Вони зможуть забезпечувати комплексний захист комп'ютерних мереж, тоді як сучасні пристрої зазвичай виконують досить обмежений набір конкретних функцій, а основна тяжкість все одно лягає на спеціалізоване програмне забезпечення.

3. Інтернет-провайдери будуть надавати послуги комп’ютерної безпеки. Основними їх клієнтами стануть компанії - активні споживачі послуг web-хостингу, систем електронної комерції і т.д.

5. Капіталізація ринку послуг мережевої безпеки різко зросте в декілька раз. Це пов'язано з тим, що нові концепції захисту IT-систем від хакерів акцентують увагу не стільки на реагування на події/атаки, що вже відбулися, а на їх прогнозування, попередження і проведення попереджуючих і профілактичних заходів, бо кожен день зловмисники знаходять нові уразливості в програмних продуктах, які використовуються в корпоративних мережах.

Віртуальна приватна мережа (virtual private network, VPN) — це розширення приватної мережі, що містить інкапсульовані, зашифровані і аутентифіковані зв'язки усередині розділених (shared) або загальнодоступних (public) мереж. Віртуальні приватні мережі (VPN - Virtual Private Network) створюють на базі загальнодоступної Internet.

Найпростішим способом застосування VPN є використання цієї технології для анонімайзінга свого інтернет-серфінгу. Весь трафік буде проходити через сервери вашої локальної робочої мережі або сервери провайдера в якості зашифрованої інформації. З іншого боку, доступ до інтернет-ресурсів відбуватиметься через IP відповідного VPN-сервера. Оскільки

трафік в такому випадку робить свого роду гак, швидкість з'єднання знижується.

Для вирішення інших завдань за допомогою VPN організовується просте з'єднання типу "точка-точка", що об'єднує дві машини або в захищену внутрішню мережу для обміну шифрованими даними. Подібним чином можна об'єднати й цілі локальні мережі. Так, підключення типу "маршрутизатор-маршрутизатор" за допомогою VPN-з'єднання використовується компаніями для захищеного обміну внутрішніми даними між різними офісами і віддаленими співробітниками.

У разі VPN-підключення мережа підрозділу фізично сполучена з інтрамережою організації, але відокремлена від неї сервером VPN, який не підтримує пряме підключення мережі підрозділу і інтрамережі організації. Користувачі інтрамережі, маючи відповідні права, можуть встановити віддалене VPN-підключення до сервера VPN і працювати із захищеними ресурсами мережі. Крім того, для посилення захисту інформація, що передається по віртуальній приватній мережі, шифрується. Для користувачів, що не мають дозволів на установку VPN-підключення до мережі підрозділу, ця мережа недоступна (і не видна в мережному оточенні).

Правильно побудована VPN повинна забезпечувати:

- Аутентифікацію, тобто користувачі повинні ідентифікувати себе;
- Авторизацію - іншими словами, обмеження доступу до ресурсів (кожен користувач має доступ тільки до дозволених для нього ресурсів);
- Цілісність даних - тобто відправлені дані повинні бути прийняті одержувачем без змін.

Можна виділити чотири основні варіанти побудови мережі VPN, які використовуються у всьому світі.

Варіант "Intranet VPN". Дозволяє об'єднати в єдину захищену мережу декілька розподілених філій однієї організації, що взаємодіють по відкритих каналах зв'язку.

Варіант "Remote Access VPN" Реалізує захищену взаємодію між сегментом корпоративної мережі (центральним офісом або філією) і одиночним користувачем, який підключається до корпоративних ресурсів з будинку (домашній користувач) або через ноутбук (мобільний користувач).

Даний варіант відрізняється від першого тим, що віддалений користувач, як правило, не має статичної адреси, і він підключається до ресурсу, що захищається, не через виділений пристрій VPN, а прямо з свого власного комп'ютера, на якому і встановлюється програмне забезпечення, що реалізовує функції VPN. Компонент VPN для віддаленого користувача може бути виконаний як в програмному, так і в програмно-апаратному вигляді .

Варіант "Extranet VPN" призначений для тих мереж, до яких підключаються так звані користувачі "зі сторони" (партнери, замовники, клієнти і т.д.), рівень довіри до яких набагато нижчий, ніж до своїх співробітників. Хоча за статистикою найчастіше саме співробітники є причиною комп'ютерних злочинів і зловживань.

Для формування VPN в Windows 2000 і 2003 використовуються протоколи PPTP, L2TP, IPSEC і IP-IP. Вони можуть працювати як разом, так і незалежно один від одного.

Протокол PPTP.

Протокол PPTP (Point-to-Point Tunneling Protocol) — розширений протокол PPP, що інкапсулює кадри PPP в IP-дейтаграми для передачі їх через мережу IP, наприклад, Інтернет. PPTP можна використовувати при з'єднанні два приватних ЛВС.

В даний час найбільш поширеним протоколом VPN є протокол тунельного зв'язку або Point-to-Point Tunnelling Protocol - PPTP. Розроблений він компаніями 3Com і Microsoft з метою надання безпечного віддаленого доступу до корпоративних мереж через Інтернет. PPTP використовує існуючі відкриті стандарти TCP / IP і багато в чому покладається на застарілий протокол зв'язку PPP. На практиці PPP так і залишається комунікаційним протоколом сеансу з'єднання PPTP. PPTP створює тунель через мережу до NT-сервера одержувача і передає по ньому PPP-пакети віддаленого користувача. Сервер і робоча станція використовують віртуальну приватну мережу і не звертають уваги на те, наскільки безпечною або доступною є глобальна мережа між ними. Завершення сеансу з'єднання відбувається з ініціативи сервера, на відміну від спеціалізованих серверів віддаленого доступу цей протокол дозволяє адміністраторам локальної мережі не пропускати віддалених користувачів за межі системи безпеки Windows NT Server.

Хоча компетенція протоколу PPTP поширюється лише на пристрої, що працюють під управлінням Windows, він надає компаніям можливість взаємодіяти з існуючими мережевими інфраструктурами і не завдавати шкоди власній системі безпеки. Таким чином, віддалений користувач може підключитися до Інтернету за допомогою місцевого провайдера за допомогою аналогового або каналу ISDN і встановити з'єднання з сервером NT. При цьому компанії не доводиться витрачати великі суми на організацію і обслуговування пулу модемів, що надає послуги віддаленого доступу.

PPTP інкапсулює пакети IP для передачі по IP-мережі. Клієнти PPTP використовують порт призначення для створення керуючого тунелем з'єднання. Цей процес відбувається на транспортному рівні моделі OSI. Після створення тунелю комп'ютер-клієнт і сервер починають обмін службовими пакетами. На додаток до керуючого з'єднанню PPTP, що забезпечує працездатність каналу, створюється з'єднання для пересилання по тунелю даних. Інкапсуляція даних перед пересиланням через тунель відбувається дещо інакше, ніж при звичайній передачі. Інкапсуляція даних перед відправкою в тунель включає два етапи:

1. Спочатку створюється інформаційна частина PPP. Дані проходять зверху вниз, від прикладного рівня OSI до канального.

2. Потім отримані дані відправляються вгору по моделі OSI і інкапсулюються протоколами верхніх рівнів.

Таким чином, під час другого проходу дані досягають транспортного рівня. Однак інформація не може бути відправлена за призначенням, так як за це відповідає канальний рівень моделі OSI. Тому PPTP шифрує поле корисного

навантаження пакета і бере на себе функції другого рівня, зазвичай належать PPP, тобто додає до PPTP-пакету PPP-заголовок і закінчення. На цьому створення кадру канального рівня закінчується.

Далі, PPTP інкапсулює PPP-кадр в пакет GenericRoutingEncapsulation (GRE), який належить мережевого рівня. GRE инкапсулирует мережевий рівень, наприклад IPX, AppleTalk, DECnet, щоб забезпечити можливість їх передачі по IP-мереж. Однак GRE не має можливості встановлювати сесії і забезпечувати захист даних від зловмисників. Для цього використовується здатність PPTP створювати з'єднання для управління тунелем. Застосування GRE в якості методу інкапсуляції обмежує поле дії PPTP тільки мережами IP.

Після того як кадр PPP був інкапсульований в кадр з заголовком GRE, виконується інкапсуляція в кадр з IP-заголовком. IP-заголовок містить адреси відправника і одержувача пакету. На закінчення PPTP додає PPP заголовок і закінчення.

Система-відправник посилає дані через тунель. Система-одержувач видаляє всі службові заголовки, залишаючи тільки дані PPP.

Протокол L2TP.

L2TP з'явився в результаті об'єднання протоколів PPTP і L2F (Layer 2 Forwarding). PPTP дозволяє передавати через тунель пакети PPP, а L2F-пакети SLIP і PPP. Щоб уникнути плутанини і проблем взаємодії систем на ринку телекомунікацій, комітет Internet EngineeringTaskForce (IETF) рекомендував компанії CiscoSystems об'єднати PPTP і L2F. На загальну думку, протокол L2TP увібрав в себе кращі риси PPTP і L2F. Головне достоїнство L2TP в тому, що цей протокол дозволяє створювати тунель не тільки в мережах IP, але і в таких, як ATM, X.25 і Frame Relay. На жаль, реалізація L2TP в Windows 2000 підтримує тільки IP.

L2TP застосовує в якості транспорту протокол UDP і використовує однаковий формат повідомлень як для управління тунелем, так і для пересилання даних. L2TP в реалізації Microsoft використовує в якості контрольних повідомлень пакети UDP, що містять шифровані пакети PPP. Надійність доставки гарантує контроль послідовності пакетів.

Функціональні можливості PPTP і L2TP різні. L2TP можуть використовуватися не тільки в IP-мережах, службові повідомлення для створення тунелю і пересилання за нього даних використовують однаковий формат і протоколи. PPTP може застосовуватися тільки в IP-мережах, і цьому протоколу необхідно окреме з'єднання TCP для створення і використання тунелю. L2TP поверх IPSec пропонує більше рівнів безпеки, ніж PPTP, і може гарантувати майже 100-відсоткову безпеку важливих для організації даних. Особливості L2TP роблять його дуже перспективним протоколом для побудови віртуальних мереж.

Протоколи L2TP і PPTP відрізняються від протоколів тунелювання третього рівня рядом особливостей:

1. Надання корпораціям можливості самостійно обирати спосіб аутентифікації користувачів і перевірки їх повноважень - на власній «території» або у провайдера Інтернет-послуг. Обробляючи тунелюватись пакети PPP,

сервери корпоративної мережі отримують всю інформацію, необхідну для ідентифікації користувачів.

2. Підтримка комутації тунелів - завершення одного тунелю і ініціювання іншого до одного з декількох потенційних термінаторів. Комутація тунелів дозволяє, як би продовжити PPP - з'єднання до необхідної кінцевої точки.

3. Надання системним адміністраторам корпоративної мережі можливості реалізації стратегій призначення користувачам прав доступу безпосередньо на брандмауері і внутрішніх серверах. Оскільки оператори тунелю отримують пакети PPP з відомостями про користувачів, вони в змозі застосовувати сформульовані адміністраторами стратегії безпеки до трафіку окремих користувачів. (Туннелювання третього рівня не дозволяє розрізняти надходять від провайдера пакети, тому фільтри стратегії безпеки доводиться застосовувати на кінцевих робочих станціях і мережевих пристроях.) Крім того, в разі використання тунельного комутатора з'являється можливість організувати «продовження» тунелю другого рівня для безпосередньої трансляції трафіку окремих користувачів до відповідних внутрішніх серверів. На такі сервери може бути покладено завдання додаткової фільтрації пакетів.

Таким чином, запропоновано створення та налаштування VPN тунелю для підвищення захисту корпоративної мережі. Це призвело до підвищення рівня захисту інформації, що циркулює в корпоративній мережі.

Література

1. Оліфер В.К. Компьютерные сети. Принципы, технологии, протоколы. – С.-П.: КОМ, 2016. – 992 с.
2. Леонов А.В. Великі мережі. Підтримка мереж. – С-П.: СПГТУ, 2007. – 820 с.
3. Ватаманюк А.І. Створення та обслуговування корпоративних мереж – М.: ТОП, 2008. – 804 с.
4. Міронін В.Р. Основи етичного хакінгу. – В.: МИР, 2017. - 445 с.

Колесников В.А.
Київський національний університет імені Тараса Шевченка, м. Київ
Кафедра обчислювальної математики, студент

ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА СИМЕТРИЧНОГО ТА АСИМЕТРИЧНОГО ШИФРУВАННЯ

Основна відмінність між симетричним і асиметричним видами шифрування полягає в знаннях відправника та одержувача даних про ключі шифрування.

У випадку симетричного шифрування відправник та одержувач наперед домовляються про ключ і мають обидва тримати його в таємниці. Так, отримавши зашифровані за допомогою ключа повідомлення, можна тим же ключем і розшифрувати їх.

Асиметричне шифрування (або шифрування з відкритим ключем) використовує два ключі, один з яких одержувач має зберігати в таємниці, а інший може пересилати відправнику по незахищених каналах. Відправник шифрує свої дані за допомогою отриманого відкритого ключа і пересилає їх одержувачу. Той за допомогою закритого ключа може їх розшифрувати. При цьому мається на увазі, що третя особа, яка прагне перехопити дані, навіть маючи відкритий ключ та зашифроване повідомлення, не зможе достатньо швидко дешифрувати його.

Порівнюючи ці два види шифрування за різними параметрами, маємо такі результати:

- Швидкість:

шифрування-дешифрування у асиметричному випадку відбувається на декілька порядків повільніше, ніж за симетричного шифрування.

- Криптостійкість:

для досягнення однакового рівня криптостійкості, довжина ключів асиметричного шифрування повинна бути у сотні разів більша за довжину ключів симетричного шифрування.

- Секретність ключів:

під час симетричного шифрування закритий ключ має зберігатися одночасно у двох осіб, і щоб його узгодити, необхідно мати особливий захищений канал зв'язку. Асиметричне шифрування дає можливість зберігати закритий ключ лише в одержувача, що значно зменшую можливість його розкриття.

- Великі мережі:

керувати ключами симетричного шифрування, на відміну від асиметричного, значно складніше у великих мережах. До того ж, їх кількість набагато більша у симетричному випадку.

- Вивченість:

Симетричне шифрування відоме з давніх часів і досить гарно вивчене. Асиметричне з'явилося відносно нещодавно і багато аспектів ще підлягають доведенню та перевірці.

Література

1. Гатчин Ю.А., Коробейников А.Г. Основы криптографических алгоритмов. Учебное пособие. – СПб.: СПбГИТМО(ТУ), 2002;

2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. – М.: Триумф, 2002. – 816 с.

Корзун В.І., студент 4 курсу
НТУУ «Київський політехнічний інститут імені І.Сікорського», м. Київ
Кафедра програмного забезпечення комп'ютерних систем

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ РОЗПІЗНАВАННЯ ОБ'ЄКТІВ МІСЦЕВОСТІ НА ЗОБРАЖЕННЯХ

Пошук об'єктів на зображеннях є фундаментальною проблемою комп'ютерного зору - якщо надається зображення, то потрібно визначити чи є такий самий об'єкт на схожих зображеннях у великій базі даних. Це особливо важливо для зображень, що містять відомі об'єкти місцевості, пам'ятки, орієнтири (англ. - landmark), на які припадає велика частина того, що люди фотографують.

Найбільш популярними та ефективними в останні роки є методи, що базуються на виявленні ознак (англ. - feature detection) за допомогою штучних нейронних мереж.

Для вирішення задачі пропонується використовувати програмний засіб для виявлення локальних ознак - DELF (DEep Local Features), заснований на використанні згорткових штучних нейронних мереж.

Це новий (анонсований у жовтні 2017) модуль Tensorflow, відкритої програмної бібліотеки для машинного навчання, розробленої компанією Google.

Модуль включає в себе попередньо підготовлену модель машинного навчання, що була оптимізована для задач розпізнавання об'єктів місцевості, тому передбачається, що вона добре працюватиме у цій галузі.

DELF працює, витягуючи ключові ознаки з зображення та описи цих ключових моментів. Під час пошуку він буде знаходити зображення з подібними описами та геометрично узгоджуватиметься з їхніми ключовими точками, щоб переконатися, що зображення правильне.

Після того, як будуть вилучені локальні ознаки з усіх зображень в базі даних, можна надавати системі стороннє зображення та знаходити зображення зі схожими ознаками у первинній базі даних.

Цю пошукову систему пропонується реалізувати за допомогою алгоритмів пошуку найближчих сусідів (англ. - nearest neighbor search). Таким чином, з'являється можливість подавати до моделі ознаки стороннього зображення та визначати найближчі співпадіння кожної ознаки. Схожим визначається зображення, для якого буде знайдено найбільше співпадінь. Існує кілька реалізованих бібліотек для пошуку найближчих сусідів. У даному випадку використовувався Annoy - бібліотека зі зручним API, реалізована на мові програмування Python.

Нарешті, для двох зображень виконується геометрична перевірка за допомогою RANSAC. Це необхідно, щоб впевнитись у тому, що на двох зображеннях присутній один й той самий об'єкт. На рис. 1 зображено функціонування запропонованої моделі.

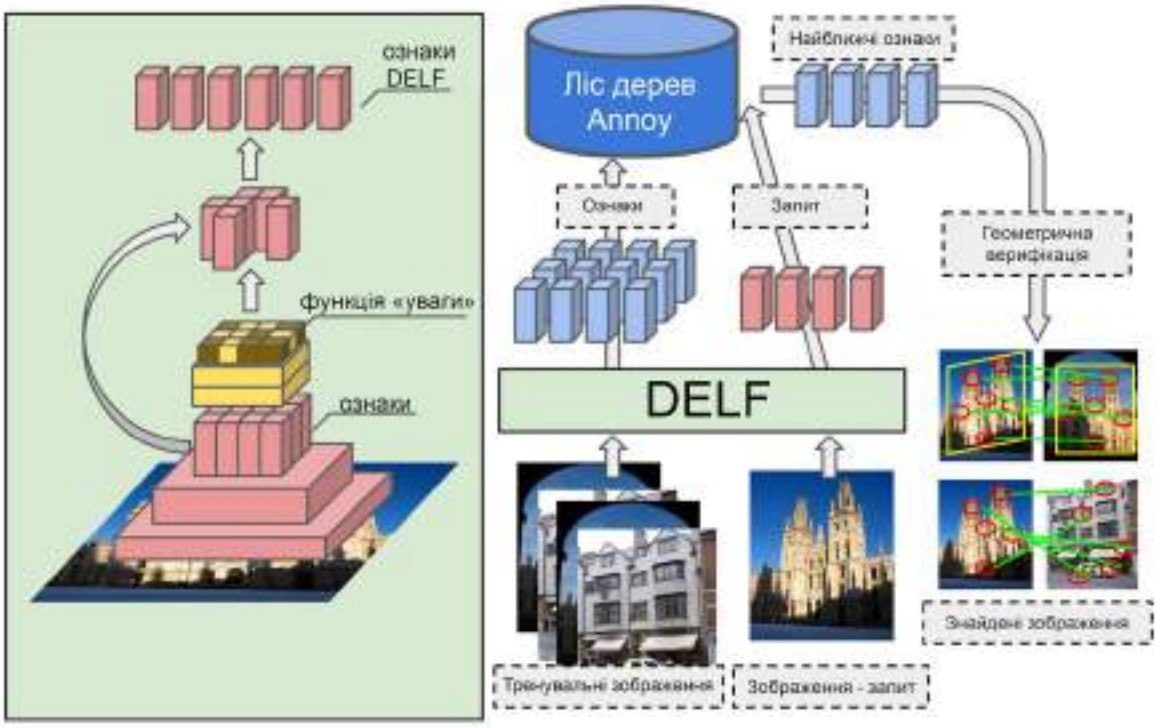
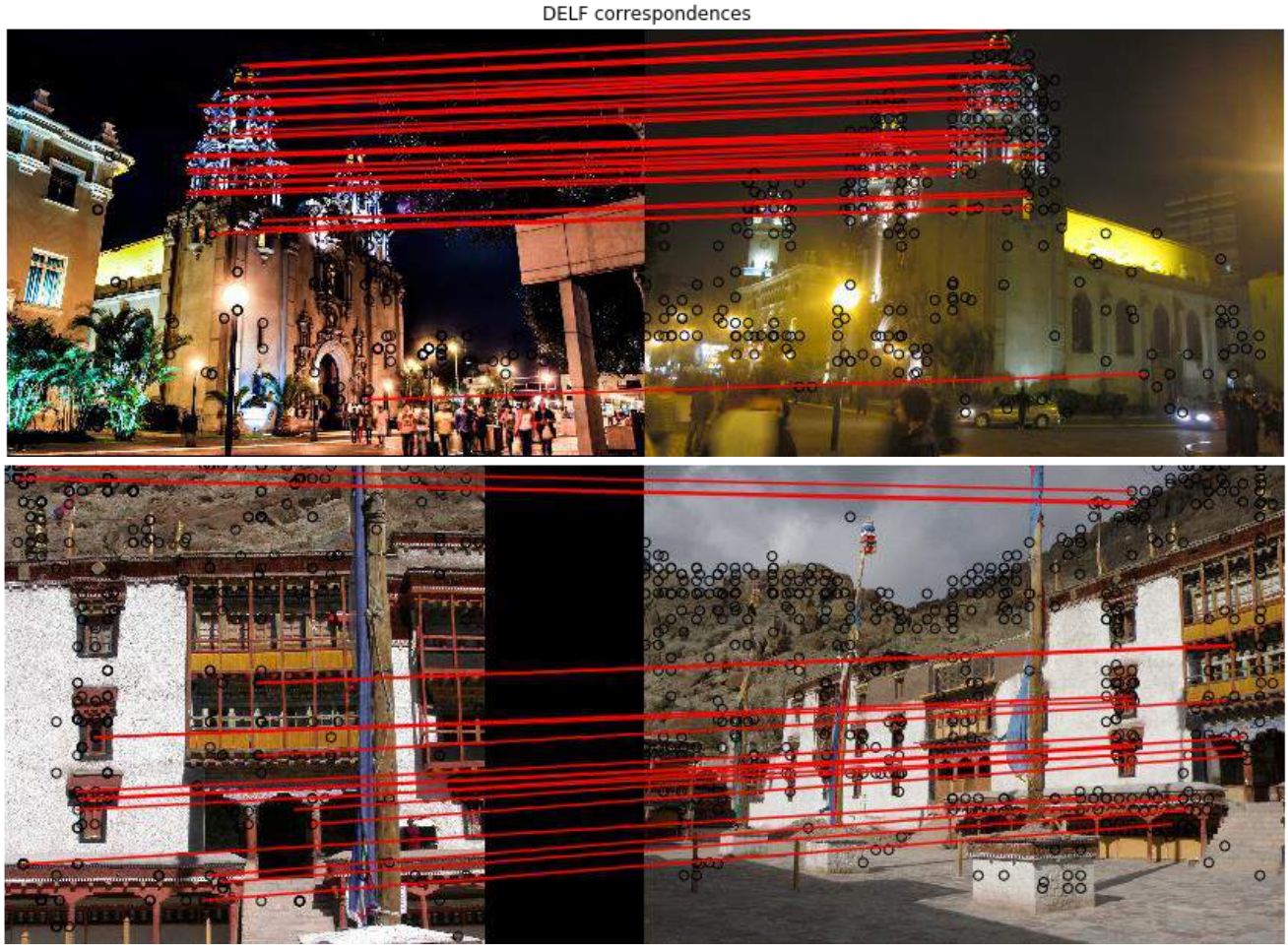


Рис. 1. Схема роботи запропонованої моделі

Приклад роботи моделі наведений на рис. 2, де для сторонніх зображень знайдені схожі зображення з первинної бази даних.

Рис. 2. Приклади знаходження однакового об’єкту на двох зображеннях



Література
1. DELF: DEep Local Features [Електронний ресурс]. - Режим доступу: https://github.com/tensorflow/models/tree/master/research/delf/
2. Visual Landmark Recognition from Internet Photo Collections: A Large-Scale Evaluation Features [Електронний ресурс]. - Режим доступу: https://arxiv.org/pdf/1409.5400.pdf
3. Landmark Matching in Images [Електронний ресурс]. - Режим доступу: https://modeldepot.io/mikeshi/delf

Котлерман І.В.
Отношенний І.О.
Одеський національний політехнічний університет, м. Одеса
Кафедра прикладної математики та інформаційних технологій, студент

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ СТЕГАНОСИСТЕМИ З СЕКРЕТНИМ КЛЮЧЕМ

Серед методів захисту інформації важливе місце займають стеганографічні методи. Основною особливістю методів є те, що приховуване повідомлення вбудовується в об'єкт, що не привертає уваги, результатом чого є стеганоповідомлення, що відкрито транспортується по каналу зв'язку або зберігається в поданому вигляді. Ефективність стеганографічного алгоритму визначається зокрема його стійкістю до різноманітних атак. Одною з найпоширеніших атак на даний час вважається атака стиском, що пов’язано з форматами зберігання цифрових зображень. У роботі [1,2] представлена модифікація стеганографічного перетворення для зображення, стійкого до стиску. Завдяки встановленим та врахованим при розробці властивостям, стеганографічний алгоритм дозволяє забезпечити високу стійкість до атак стиском, прийнятне співвідношення можливого об’єму інформації, що вбудовується, до розміру стеганографічного контейнера, залишаючи процес вбудовування інформації відносно простим та легким для реалізації.

У відповідності з принципом Керхгофса безключові стеганосистеми є недостатньо захищеними. У зв’язку з цим, доцільно на основі запропонованого алгоритму реалізувати роботу стеганосистеми із застосуванням секретного ключа. Замість вбудовування бітів прихованої інформації послідовно у кожний блок квантованих коефіцієнтів ДКП, блоки для вбудовування будуть обиратися за певним порядком, що задається секретним ключем. Для вирішення поставленої задачі в алгоритмі вбудовування прихованої інформації необхідно модифікувати вбудовування інформації в заданий квантований коефіцієнт.

Нехай r(n,k) – функція, що задає псевдовипадкову перестановку n елементів, яка залежить від параметра – ключа k. Псевдовипадкова перестановка може бути отримана, наприклад, за допомогою тасування Фішера-Йетса з використанням генератора псевдовипадкових чисел із заданням k у якості породжуючого елементу. Для конкретного зображення можна отримати кількість блоків для вбудовування інформації l_b. Позначимо

$s = r(l_b, k)$ – вектор, що задається псевдовипадковою перестановкою, індекси якого відповідають номеру біта секретного повідомлення, а значення – номеру блока для вбудовування. Тоді формула вбудовування бітів секретної інформації приймає такий вигляд:

$$F'_{s(i)}(u,v) = [(F^{Q}_{s(i)}(u,v))/2]\cdot 2 + m_i,$$

(1)

де m_i – і-й біт прихованої інформації; $F^{Q}_{s(i)}(u,v)$ – заданий квантований коефіцієнт блоку для вбудовування і-го біту інформації; $F'_i(u,v)$ – квантований коефіцієнт для вбудовування і-го біту інформації із прихованою інформацією.

Для вилучення з контейнера секретної інформації, необхідно, знаючи ключ k, отримати вектор s і визначити біти інформації за формулою:

$$m^*_i = F'_{s(i)}(u,v) - [(F'_{s(i)}(u,v))/2]\cdot 2,$$

(2)

де m^*_i – і-й біт прихованої інформації; $F'_{s(i)}(u,v)$ – заданий квантований коефіцієнт блоку для вбудовування і-го біту із прихованою інформацією.

Література

1. Котлерман, І.В. Розробка стеганографічного алгоритму для цифрових зображень, стійкого до стиску / І.В. Котлерман, І.О. Отношенний // Тези доповідей 15 Всеукраїнської конференції студентів і молодих науковців «Інформатика, інформаційні системи та технології». – Одеса. – 27 квітня 2018р. – С. 179–181.

2. Котлерман, І.В. Стеганоперетворення частотної області цифрового зображення, стійке до атаки стиском / Журнал «Актуальные научные исследования в современном мире» // І.В. Котлерман, І.О. Отношенний. – Переяслав-Хмельницький, 2018. – Вип. 4(36), ч.3. – С. 52–56.

Кравченко О.О., студент групи ІПЗм-16-1
Харківський Національний Університет Радіоелектроніки, м. Харків
Факультет комп'ютерних наук, Кафедра програмної інженерії

АНАЛІЗ МЕТОДІВ КЕШУВАННЯ ДАНИХ У ВЕБ-ЗАСТОСУВАННЯХ

Пришвидшення роботи будь-якого програмного забезпечення під великим навантаженням є завжди актуальною проблемою, котру та чи інша команда розробників намагається вирішити впродовж розробки продукту.

Існує багато методик пришвидшення роботи веб-застосувань, одною з яких є кешування, а саме кешування даних, наявних в базі даних. Кешування – це збереження результату операції, яка може бути використана пізніше, замість того, щоб повторювати операцію знову у майбутньому. Для кеша може використовуватися оперативна пам'ять. Таким чином, окрім заощадження часу на вирахування необхідного результату операції, ще й зчитування даних

відбувається значно швидше – дані будуть зчитуватися з оперативної пам'яті, а не з жорсткого диску.

У типовій архітектурі веб-застосування є декілька шарів, де можна виконувати кешування:

1. браузер;
2. Інтернет (мережі доправлення контенту);
3. зворотній проксі;
4. веб-застосування;
5. база даних.

Слід зазначити, що кешування у шарах на початку списку сильніше всього впливають на затримку повернення результатів веб-застосуванням, а кешування у останніх шарах забезпечує кращий контроль над деталізацією та способами очищення чи оновлення кеша.

Кешування у веб-застосуванні відрізняється від кешування у базі даних тим, що кеш зберігається зазвичай у найшвидших структурах пам'яті та дані можуть бути отримані дуже швидко. Таким чином нівелюється необхідність бази даних у зчитуванні даних з жорсткого диску, а також час на виконання самого запиту до бази даних.

Одним з методів кешування на рівні веб-застосування є локальний кеш. Локальний кеш зберігає часто використовувані дані в межах застосування. Це робить пошук даних швидшим, ніж інші методи кешування, оскільки цей метод видаляє мережевий трафік, який пов'язаний з отриманням даних. Основним недоліком цього методу є те, що застосування може мати декілька копій, де кожна копія має свою власну кеш-пам'ять, яка працює у несинхронізованому режимі. Інформація, що зберігається в окремому вузлі кешу, незалежно від того, чи є це кешована база даних, рядки, веб-вміст або дані сеансу, не синхронізується з кеш-пам'яттю інших вузлів. Це створює проблеми в розподіленному середовищі, де обмін інформацією є критичним для підтримки масштабованої динаміки.

Оскільки більшість застосувань використовують декілька серверів, координувати значення кешу поміж ними стає великою проблемою, коли кожен сервер має свою власну кеш-пам'ять. Крім того, при виникненні переривань, дані локального кешу втрачаються і мають бути відновленими. Більшість з цих недоліків нівелюються за допомогою віддалених кешів.

Віддалений кеш – це окремий сервер (або сервера), призначений для зберігання кешованих даних в пам'яті. Віддалений кеш зберігається на виділених серверах і зазвичай будується на основі сховищ формату ключ-значення (NoSQL), таких як Redis та Memcached. Вони можуть обробляти сотні тисяч і мільйони запитів в секунду.

Середня затримка запиту до віддаленого кешу визначається в частинах мілісекунд, що на порядок швидше, ніж запит до бази даних на диску. За таких швидкостей локальні кеші рідко потрібні. Віддалений кеш ідеально підходить для розподілених середовищ, оскільки він працює як з'єднаний кластер, який можуть використовувати всі системи. Проте, коли затримка мережі завдає проблем, можна застосувати дворівневу стратегію кешування, яка використовує локальний та віддалений кеш одночасно.

При використанні віддаленого кешу саме веб-застосування керує тим, як і коли дані кешуються, а також коли кеш перестає бути актуальним. Сам віддалений кеш не пов’язаний напряму з базою даних вею-застосування, а використовується разом із нею.

Для кешування даних із бази даних існують різні схеми кешування, які можна реалізувати, включаючи активні та реактивні підходи. Вибір шаблонів для реалізації кешування має відбуватися з урахуванням цілей кешування та конкретної реалізації. Два найбільш популярні підходи – це відкладене завантаження (реактивний підхід) та наскрізний запис (проактивний підхід). Кеш відкладеного завантаження оновлює данні під час зчитування, а кеш наскрізного запису оновлюється одночасно з оновленням основної бази даних. За допомогою обох підходів застосування, по суті, керує тим, які дані зберігаються в кеші та як довго.

Таким чином, можна зробити висновок, що найбільш ефективним методом кешування є кешування на рівні саме веб-застосувань з використанням віддаленого кешу. За допомогою використання віддаленого кешу його легко масштабувати разом із самим веб-застосуванням. Єдиним обмеженням цього методу є швидкість передачі даних у мережі. А найбільш ефективним підходом цього кешування є використання комбінації реактивного та проактивного підходів для найкращої ефективності витрати ресурсів веб-застосувань, як для операції запису, так і для операції зчитування даних із бази даних.

Література

1. Wessels D. Web Caching: Reducing Network Traffic 1st Edition – Newton, USA: O'Reilly Media, 2001. – 205 p.

2. Кеш – Вікіпедія URL: https://uk.wikipedia.org/wiki/Кеш (дата звернення: 09.04.2018).

3. Caching To Scale Web Applications URL: http://venkateshcm.com/2014/05/Caching-To-Scale-Web-Applications/ (дата звернення: 25.03.2018).

4. Database Caching URL: https://aws.amazon.com/caching/database-caching/ (дата звернення: 28.03.2018).

5. Caching | AWS URL: https://aws.amazon.com/caching/ (дата звернення: 20.03.2018).

Кузьмінох В.О., к.т.н., доцент
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ
АПЕПС, доцент

Осипенко М.В.
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м. Київ
АПЕПС, аспірант

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОШУКУ ІНФОРМАЦІЇ В ЕЛЕКТРОННИХ ДЖЕРЕЛАХ

За останні десятиліття кількість інформації [1], створеною людством стрімко зростає. Виникає необхідність її швидкої обробки, але це потребує значної кількості ресурсів. При цьому постає протиріччя між кількістю накопиченої інформації та можливістю її ефекти обробки для наступного використання. Тому задача створення засобів для пошуку інформації в електронних джерелах та її консолідації з метою подальшої обробки на сьогодні є актуальною.

Найпростіший спосіб пошуку документа по запиту – це врахувати частоту слів у тексті документа, що відображені у конкретному запиті. Це вкрай примітивний спосіб визначення відповідності документу відповідному запиту. Сучасні обчислювальні потужності дозволяють використовувати для цього нейронні мережі, які справляються з аналізом різною за типом інформації (текст, звук, зображення) краще, ніж будь-який інший метод машинного навчання. Нейронної мережі [2] дозволяють машині перейти від пошуку за словами до пошуку за змістом.

Використання нейронних мереж має свої обмеження, що зумовлено наступними проблемами:

1. По-перше, це потребує використання великої кількість пам'яті. Для пошуку по тексту під час виконання запиту необхідно мати цей текст в оперативній пам'яті. Це може бути припустимо для пошуку по заголовках, або невеликих текстах, але не з повними текстами документів.
2. По-друге, це потребує значної потужності CPU. Для звичайного пошуку перебором слів в тексті потрібно зробити один прохід по документу.

Фактично на даному етапі ми повинні виконати n * m дій, де n - кількість слів у документі, а m – кількість документів. Таким чином, кількість процесорного часу, лінійно залежить від довжини тексту та кількості документів.

Потрібно зрозуміти наскільки запит та текст документа відповідають один одному за змістом. Для цього текст запиту і текст документу, що оброблюється, представляється в вигляді таких векторів, скалярний добуток яких був б тим більше, чим більш релевантні запиту документ з цим заголовком. Інакше кажучи, нейрона мережа навчається таким чином, щоб для близьких за змістом

текстів вона генерувала схожі вектору, а для семантично незв'язаних запитів і документів вектори повинні відрізнятися.

Підхід, який отримав назву Deep Structured Semantic Model [3], був запропонований розробниками з Microsoft Research. В ньому на вхід моделі надаються тексти запитів і заголовків. Над ними проводиться операція хешування слова (word hashing) для зменшення розмірів даних. До тексту додаються маркери початку і кінця, а потів текст розбивається на літерні триграми. Під триграмами розуміються при цьому усі можливі комбінації з трьох літер відповідного алфавіту. Теоретична кількість різних триграм обмежена розміром алфавіту:

$$K_T = D^3 + D^2 + D, \quad (1)$$

де D – кількість літер у алфавіті мови, що розглядається.

Для англійського алфавіту кількість можливих триграм дорівнює 20306. Реальна кількість триграм, які мають розглядатися при аналізі текстової інформації, може бути значно зменшена за рахунок триграм, які не є характерними для англійської мови, тобто таких, які не зустрічаються в англійській мові. Таким чином, реальна кількість триграм значно менше теоретичної:

$$K_R << K_T \quad (2)$$

Для збільшення скорості обробки інформації та підвищення ефективності роботи програмних засобів обробки необхідно щоб таблиці, які містять перелік триграм, були б впорядженні відповідно до оцінок частоти появи триграм для певних типів текстів.

Таким чином модель використання триграм для пошукових запитів може складатися з набору (словника) трійок символів і приписаного їм ваги. Триграми впорядковані за вагою таким чином, що більша вага означає більшу частоту зустрічальності триграми в природній мові, точніше в деякому корпусі текстів природною мовою, до якого має відноситися певний запит.

В загальному випадку під вагою триграми розуміється ймовірність її народження в природній мові. Зрозуміло, на різних вибірках текстів природної мови ми можемо отримувати розрізняються ваги триграм.

При цьому текст запиту, як і текст, що аналізується на відповідність, розглядається у вигляді вектору розміром не більш ніж K_R елементів.

Відповідні триграмам запиту елементи вектору дорівнюватимуть 1, а решта дорівнює 0. Визначається таким чином входження триграм з тексту в словник, що складається з усіх відомих триграм. Якщо порівняти такі вектори, то можна дізнатися тільки про наявність однакових триграм в запиті і заголовку, що не повного результату. Тому тепер їх треба перетворити в інше представлення, яке вже буде мати необхідні для аналізу властивості семантичної близькості текстів, що аналізуються, конкретним запитам.

Замість того, щоб брати заголовок документа і під час виконання запиту обчислювати його семантичний вектор, можна обчислити цей вектор і зберегти його в пошуковій базі. Іншими словами, можна виконати значну частину роботи заздалегідь, а саме – перемножити матриці для документа і зберегти результат. Тоді під час виконання запиту буде потрібно тільки дістати вектор документа з

пошукового індексу і виконати скалярне множення з вектором запиту. Це істотно швидше, ніж динамічне обчислення вектору. Однак, при цьому буде потрібно виділити місце для зберігання попередньо обчислених векторів[4].

Але для значної кількості документів час пошуку все одно залишається достатньо тривалим, так як необхідно обробити всі наявні джерела. Для оптимізації часу пошуку по джерелах пропонується поетапне виконання пошуку тексту за запитами. На першому етапі слід відфільтрувати наявні документи за назвою, яка буде найбільш релевантна запиту. Таким чином запобігти втрачання часу на документи, які не можуть містити корисної інформації для конкретного запиту. На другому етапі повторити перший крок для анотації до роботи, так як зазвичай це невеликий об'єм тексту, але він містить основу тему роботи. На останньому етапі відбувається основний пошук в звуженій вибірці джерел, таким чином значно знизивши час та використання ресурсів для пошуку.

Література

1. 10 Key Marketing Trends for 2017 [electrinic resourse]. – Access mode: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=WRL12345USEN
2. Introduction to Deep Neural Networks (Deep Learning) [electrinic resourse]. – Access mode: https://deeplearning4j.org/neuralnet-overview
3. Learning Deep Structured Semantic Models for Web Search using Clickthrough Data [electrinic resourse]. – Access mode: https://www.microsoft.com/en-us/research/publication/learning-deep-structured-semantic-models-for-web-search-using-clickthrough-data/
4. Люгер Ф. Дж. Искусственный интеллект: стратегии и методы решения сложных проблем. 4-е издание. Пер. с англ. – М.: «Вильямс», 2003. – 864с. ISBN 5-8459-0437-49 (рус.)

Макута М.Ю.
Східноєвропейський Національний університет ім. Лесі Українки, м. Луцьк
Кафедра прикладної математики та інформатики, студент

ДОСЛІДЖЕННЯ ТА РОЗРОБКА ТЕЛЕГРАМ-БОТА СИСТЕМИ САМООБСЛУГОВУВАННЯ ІНТЕРНЕТ-ПРОВАЙДЕРА

В сучасному світі все більше відпадає потреба в SMS, адже за допомогою месенджерів можна безлімітно обмінюватися повідомленнями через Інтернет. Крім того, більшість месенджерів дозволяють створювати ботів – комп'ютерні програми, які розроблені на основі нейромереж та технологій машинного навчання, які ведуть розмову за допомогою слухових або текстових методів. Зазвичай їх використовують для досягнення якої-небудь мети (наприклад, для надання довідкової інформації) чи для розваг. Досить часто боти використовуються в різноманітних системах для різних практичних цілей, зокрема, деякі боти дозволять обслуговувати клієнтів та отримувати безкоштовні консультації.

Актуальність побудови чат-бота системи самообслуговування інтернет-провайдера полягає в тому, що впровадження чат-бота дозволяє значно автоматизувати надання консультацій для клієнтів інтернет-провайдера та збільшити кількість одночасно обслуговуваних клієнтів. Крім того, така система дозволяє значно спростити доступ до особистого кабінету, пришвидшити обмін інформацією про послугу Інтернет між провайдером та користувачем, а також дозволяє впровадити функцію сповіщення про технічні роботи чи про актуальний стан балансу.

Особливе значення чат-бот системи самообслуговування інтернет провайдера має для клієнта, адже за рахунок автоматизації значно скорочується час технічного обслуговування. Приміром, якщо раніше інформація про проблему в користувача проходила тривалий шлях від спеціаліста технічної підтримки до інженера, який обслуговує даний сегмент мережі, то завдяки впровадженню чат-бота інформація миттєво, в режимі реального часу, надсилається технічному інженеру, який на екрані свого гаджета зразу ж отримує інформацію від користувача про характер поломки, інформацію від біллінгу Інтернет-провайдера про те, чи наявне з'єднання з мережею Провайдера, та актуальні підключені послуги. Ця інформація дозволяє технічному інженеру якомога швидше відреагувати на проблему в користувача та прискорити усунення несправності.

Для досягнення найбільшої ефективності було обрано саме месенджер telegram, оскільки він має декілька переваг, зокрема досить велику аудиторію серед користувачів в Україні, використовує меншу кількість апаратних ресурсів, необхідних для його запуску та роботи, а також передача даних від пристрою користувача, на якому встановлено даний месенджер, до його серверів відбувається за допомогою надійного зашифрованого з'єднання.

Література

1. *Stuart J. Russell, Peter Norvig*. Artificial Intelligence: A Modern Approach. — 3. — Pearson, 2015

2. *Alan Bundy, Rod Burstall*. Artificial Intelligence: An Introductory Course. — Revised. — Edinburgh University Press, 1984.

3. Системи штучного інтелекту: навч. посіб. / Ю. В. Нікольський, В. В. Пасічник, Ю. М. Щербина ; за наук. ред. В. В. Пасічника ; М-во освіти і науки, молоді та спорту України. — 2-ге вид., виправл. та доповн. — Львів: Магнолія-2006, 2013. — 279 с.

4. Засоби штучного інтелекту: навч. посіб. / Р. О. Ткаченко, Н. О. Кустра, О. М. Павлюк, У. В. Поліщук ; М-во освіти і науки України, Нац. ун-т «Львів. політехніка». — Львів: Вид-во Львів. політехніки, 2014. — 204 с.

5. *Nils J. Nilsson*. The Quest for Artificial Intelligence. — 1. — Cambridge University Press, 2009. — 578 с.

Марочканич О.Р., студент
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислюваної техніки

ПРОБЛЕМИ ТА РИЗИКИ У ВЕБ-ЗАСТОСУВАННЯХ

Будь-яка система, що складається хоча б з двох компонентів (а якщо у вас є і PHP, і база даних, то це вже два компоненти), стикається з цілими класами ризиків у взаємодії між цими компонентами. Розглянемо основні ризики та проблеми при роботі з веб-платформами та способи боротьби з нештатними ситуаціями.

Рано чи пізно сервер, на якому розташований ваш сервіс, «впаде». Це точно трапиться, і ви не зможете від цього захиститися - тільки зменшити ймовірність. Вас може підвести залізо, мережа, код, невдалий деплой - що завгодно. І чим більше у вас серверів, тим частіше таке буде відбуватися. Як зробити так, щоб ваші сервіси виживали в світі, в якому постійно падають сервера? Загальний підхід до вирішення цього класу проблем - резервування. Резервування використовується повсюдно на різних рівнях: від заліза до цілих дата-центрів. Наприклад, RAID1 для захисту від відмови вінчестера або резервний блок живлення у вашого сервера, на випадок виходу з ладу першого. Також ця схема широко застосовується і до баз даних. Наприклад, для цього можна використовувати master-slave. Додаток спілкується виключно з мастером, при цьому в фоновому режимі, асинхронно, дані передаються в слейв. Коли мастер впаде, ми перемкнемося на слейв і продовжимо працювати. Після відновлення мастера ми просто зробимо з нього новий слейв, а старий перетвориться в мастер.

Припустимо, що один сервер з прикладу вище може витримати приблизно 100к RPS. Зараз навантаження становить 60К RPS, і все працює як годинник. Але з часом навантаження на додаток, а значить і навантаження на мастер, збільшується. Ви можете захотіти її балансувати, перевівши частину читання на слейв. Виглядає ніби непогано. Навантаження тримає, сервера більше не простоюють. Але це погана ідея. Важливо пам'ятати, навіщо ви спочатку підняли слейв - для перемикання на нього в разі проблем з основним. Якщо ви почали навантажувати обидва сервера, то коли ваш майстер впаде - а він рано чи пізно впаде, - вам доведеться перемкнути основний трафік з майстра на резервний сервер, а він і так уже навантажений. Подібна перевантаження або зробить вашу систему жахливо повільної, або повністю виведе її з ладу.

У якийсь момент ваш сервіс може почати дуже повільно працювати. Ця проблема може виникнути з безлічі причин: надмірне навантаження, проблеми мережі, проблеми з залізом або помилки в коді. Виглядає як не дуже страшна проблема, але насправді вона підступніша, ніж здається. Уявімо: користувач запитує якусь сторінку (рисунок 1). Ми синхронно і послідовно звертаємося до чотирьох компонент, щоб відобразити її. Вони швидко відповідають, все працює добре.

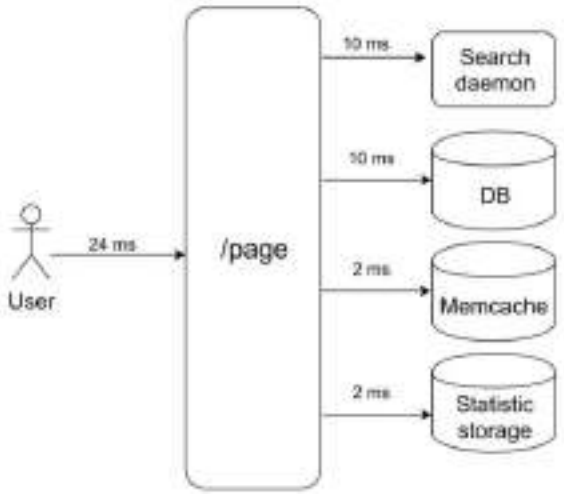


Рисунок 1. Структура зав’язків додатку

Припустимо, це обробляється за допомогою nginx з фіксованою кількістю PHP FPM Воркерів (з десятьма, наприклад). Якщо кожен запит обробляється приблизно 20 мс, то за допомогою нескладних обчислень можна зрозуміти, що наша система здатна обробити близько п'ятисот запитів в секунду.

Що трапиться, коли один з цих чотирьох сервісів почне гальмувати, і обробка запитів до нього зросте з 20 мс до таймауту в 1000 мс? Тут важливо пам'ятати, що коли ми працюємо з мережею, затримка може бути нескінченно великою. Тому необхідно завжди ставити таймаут (в даному випадку він дорівнює секунді). Виходить, що бекенд змушений чекати закінчення часу очікування, щоб отримати і обробити помилку від сервісу. А це означає, що користувач отримує сторінку через одну секунду замість десяти мілісекунд. Повільно, але не фатально.

Але в чому тут насправді проблема? Справа в тому, що коли у нас кожен запит обробляється секунду, пропускна здатність трагічно падає до десяти запитів в секунду. І одинадцятий за рахунком користувач вже не зможе отримати відповідь, навіть якщо він запитував сторінку, ніяк не пов'язану з гальмуючим сервісом. Просто тому що всі десять Воркерів зайняті очікуванням таймаута, і не можуть обробляти нові запити. При цьому важливо розуміти, що зі збільшенням кількості Воркерів ця проблема не вирішується. Адже кожен Воркер вимагає для своєї роботи певну кількість оперативної пам'яті, навіть якщо він не виконує реальну роботу, а просто висить в очікуванні таймаута. Тому якщо ви не обмежите кількість Воркерів відповідно до можливостей вашого сервера, то підняття все нових і нових Воркер покладе сервер цілком. Цей випадок - приклад каскадного відмови, коли падіння якогось одного, нехай навіть не критичного для користувача сервісу, викликає відмову всієї системи.

Для вирішення цієї проблеми існує патерн під назвою circuit breaker. Його завдання досить просте: він повинен в якийсь момент часу відмикати гальмуючий сервіс. Для цього між сервісом і Воркером ставиться проксі. Це може бути як PHP-код зі сховищем, так і окрема компонента на локальному хості. Важливо відзначити, що якщо ваш сервіс роздубльований, то це поксі повинне окремо відстежувати кожен з них. Є абстрактний сервіс Sphinx, перед яким стоїть circuit breaker. Circuit breaker зберігає кількість активних

підключень до конкретного сервісу. Як тільки це значення досягає порогу, який ми встановлюємо у відсотку від доступних FPM-Воркерів на машині, ми вважаємо, що сервіс почав пригальмовувати. При досягненні першого порога ми відправляємо повідомлення відповідальному за сервіс. Така ситуація - або ознака того, що потрібно переглянути ліміти, або вісник проблем з гальмуванням. Якщо ситуація погіршується, і кількість гальмуючих Воркерів досягає другого порогового значення - ми вирубуваємо цей хост повністю. Точніше, сервіс фактично продовжує працювати, але ми перестаємо висилати йому запити. Circuit breaker їх відкидає і відразу віддає Воркеру помилку, як ніби-то сервіс недоступний.

Час від часу ми автоматично пропускаємо запит від якогось Воркера, щоб подивитися, чи не запрацював все-таки сервіс. Якщо він відповідає адекватно, то ми знову включаємо його в роботу.

Все це робиться для того, щоб звести ситуацію до попередньої схеми з реплікацією. Замість того щоб чекати секунду, перед тим як зрозуміти, що хост недоступний, ми відразу отримуємо помилку і переходимо на резервний хост.

Висновок

У даній роботі було розглянуто основні проблеми та ризики пов’язані з розгортанням веб-сервісу, а також розглянули методи їх вирішення та запобігання. Враховуючи все вищесказане можна сформувати наступні поради:

- **Резервуйте**. Якщо важливі самі дані і доступність конкретного сервісу, то переконаєтеся, що ваш сервіс витримає падіння конкретної машини.
- **При розрахунку навантаження враховуйте падіння частини серверів.** Якщо у вашому кластері чотири сервера, переконайтеся, що коли один впаде, три інші витримають навантаження.
- **Не кладіть всі яйця в одну корзину.** Переконайтеся, що ви досить далеко розташували резервні сервера. Залежно від критичності доступності сервісу, ваші сервера можуть бути як в різних стійках в одному дата-центрі, так і в різних дата-центрах в різних країнах. Все залежить від того, наскільки глобальну катастрофу ви хочете і готові пережити.
- **Виставляйте таймаути.** Всі мережеві запити повинні мати таймаут, тому що мережа може відповідати нескінченно довго.
- **Попередьте каскадну відмову.** Використовуйте circuit breaker, якщо хочете уникнути каскадного відмови додатки через те, що гальмує один маленький сервіс.

Література

1. Безопасное взаимодействие в распределенных системах [Електронний ресурс] // habr.com. – 2018. – Режим доступу: https://habr.com/company/badoo/blog/413555/

2. CircuitBreaker [Електронний ресурс] // martinfowler.com. – 2014. – Режим доступу до ресурсу: https://martinfowler.com/bliki/CircuitBreaker.html.

3. Circuit breaker design pattern [Електронний ресурс] // wikipedia.org. – 2017.– Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Circuit_breaker_design_pattern.

Марочканич О.Р., студент
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислюваної техніки

ПОРІВНЯЛЬНИЙ АНАЛІЗ АЛГОРИТМІВ ШИФРУВАННЯ НА ПРИКЛАДІ ВЕБ-БРАУЗЕРІВ

На сьогоднішній день, інформація є легкодоступною для кожного завдяки мережі Інтернет. Деяка інформація є відкритою для всіх, інша призначена для певного кола користувачів та повинна бути закритою. Незахищеність даних в призводить до ризику потрапляння конфіденційної інформації до рук злодіїв. Саме для цього певним даним потрібно більший рівень захисту.

В цьому дослідженні описані заходи безпеки шляхом шифрування інформації. На основі аналізу чотирьох веб-браузерів буде запропоновано механізм шифрування даних.

В першу чергу, представимо одну з технік шифрування даних, що може бути використана, яка є XOR операцією та покажемо як текстові дані переводяться в шістнадцяткові. На основі різних тестових сценаріїв буде вибраний найкращий метод шифрування для веб-браузерів. В кінці дослідження буде підведено підсумки про різницю різних алгоритмів шифрування у різних браузерах, що дасть змогу визначити який алгоритм працює найкраще та найбільше підходить для того чи іншого веб-браузеру.

Існують різні заходи безпеки, які можуть бути введені для забезпечення безпеки збереженої інформації. Чим більше та якісніше розвиваються нові технології, тим більше можливостей знайти спосіб розриву, будь-які лазівки в межах системи, щоб проникнути в її серце через слабкі сторони. Це пов'язано з тим, що створені людиною конструкції можуть бути порушені іншою людиною. Таким чином, з часом заходи безпеки повинні постійно переглядатися та зміцнюватися, щоб боротися з хакерами.

Одним з засобів для захисту даних є застосування секретного коду шифрування. Якщо він зашифрований, відправник може передавати дані одержувачу, і лише одержувач або уповноважений персонал матимуть доступ до даних, якщо відправник надав ключ для розшифровки. З іншого боку, без правильної ключа ніхто не може прочитати отримані або збережені дані. Навіть якщо хакерам або несанкціонованій особі вдалося перехопити або вкрасти дані, це було б марним, оскільки текст неприйнятний для них.

Шифрування складається з різних типів, відомих як алгоритми, і вони розроблені або написані різними людьми. Оскільки багато людей розвивали їх, є і плюси і мінуси, які нам слід розглянути. Більш того, мова алгоритмів також може бути розроблена або написаний у багатьох формах, тобто на різних мовах програмування.

У цьому дослідженні запропоновано аналіз лише одного веб-сценарію мовного програмування з чотирма веб-браузерами, для визначення типу алгоритму, що підходить до типу веб-браузера з точки зору їхньої продуктивності та сумісності.

Вибрано Active Server Pages (ASP), і для аналізу їх ефективності було обрано п'ять різних типів алгоритмів шифрування. Вибрані алгоритми шифрування - Blowfish, International Data Encryption Algorithm (IDEA), Advanced Cryption Standard (AES), Tiny Encryption Algorithm (TEA) та Twofish. Як відомо, ці алгоритми шифрування можуть підтримувати 128-бітний розмір ключа [1]. Крім того, ці п'ять типів будуть спільно проаналізовані з чотирма вибраними веб-браузерами, які зможуть ефективно обробляти свої сценарії.

Є досить багато веб-браузерів, які доступні на ринку, але ці чотири, як відомо, є одними з найпопулярніших і найпопулярніших. Це Internet Explorer, Mozilla Firefox, Opera і Netscape Navigator [1]. З аналізу ми сподіваємося дізнатись веб-браузери, які найкращим чином можуть збігатися з алгоритмами шифрування ASP-скриптів.

Перш ніж реалізувати алгоритм шифрування, ми повинні розуміти принцип шифрування, тобто захистити дані, що зберігаються в повідомленні або файлі, і забезпечити нечитаність даних іншими. Нешифроване повідомлення або файл часто називають "звичайним текстом", а зашифроване повідомлення або файл називається "шифрованим текстом". Складність шифрування визначається довжини ключа в кількості бітів. Ключем є довга послідовність бітів, що використовуються алгоритмами шифрування. Таким чином, довжина ключа визначає ймовірність визначення ключа шляхом перебору всіх можливих значень, якщо треба розібрати всі її можливі ключові значення.

Процес шифрування починається після того, як було отримано дозвіл на використання системи, лише тоді, коли введена інформація буде подана. Щоб не бути перехопленим шахраями на цьому шляху, спочатку текст повинен бути зашифрований перед зберіганням, використовуючи секретні коди шифрування, а також його ключ, відомий лише відправнику та одержувачу. Щоб одержувач міг його прочитати, дані потрібно розшифрувати, просто повернувши процес, використовуючи даний ключ шифрування [2].

Щоб перевірити, який з п’яти алгоритмів шифрування краще підходить для чотирьох веб-браузерів, що згадувались раніше, проводився тест з використанням двох комп’ютерів, які були налаштовані та визначені як Клієнт та Сервер через маршрутизатор. Тестування шифрування – це тестування виконання п’яти алгоритмів шифрування в шифруванні тексту та ключа через веб-браузери для скриптів ASP. Таким чином довжина тексту, починаючи з 10, збільшиться в чотири рази відносно початкової, тоді як довжина ключа для кожного тексту залишиться незмінною.

Результат тестування продемонструє час відповіді, тобто процес шифрування та час, витрачений чотирьма веб-переглядачами, а саме Internet Explorer, Mozilla Firefox, Opera та Netscape Navigator після виконання сценаріїв шифрування, заукруглених до мілісекунди. З аналізу Internet Explorer випливає, що Twofish виконує краще в порівнянні з іншими і підтримує майже нижчий час відгуку. З аналізу роботи Mozilla Firefox, Twofish все ще відрізняється краще, ніж інші, і просто підтримує менший час відгуку. Він, однак, виконується повільніше при 20 і 40 довжинах тексту з парою алгоритмів, а саме Blowfish і

AES. З аналізу роботи Opera IDEA виконується трохи швидше, ніж Blowfish на початку. Тим не менш, він реалізується краще для інших текстових довжин, порівняно з іншими. З аналізу Netscape Navigator, TEA мав хороший старт і виконувався краще, ніж інші, до 30 довжини тексту. Але далі AES та IDEA перевищили ефективність TEA протягом останніх двох довжин тексту [3].

Висновок

У реальному спостереженні час відповіді іноді коливається, коли нам потрібно двічі запускати тест з алгоритмом шифрування на тому ж веб-браузері, використовуючи ту ж довжину тексту. Це може бути пов'язано з мережевим трафіком або навіть важким використанням Сервера.

Але в цьому випадку є лише один Клієнт та Сервер, отже, взагалі не повинно бути жодного трафіку, як тільки один Клієнт має доступ до Сервера. Таким чином, ми можемо сміливо зробити висновок, що це було пов'язано з тим, скільки часу потрібно для сервера обробляти сценарій ASP алгоритму в веб-браузері разом з багатьма іншими процесами, що працюють одночасно в межах Сервера. Це може призвести до високого використання центрального процесора (ЦП), що уповільнює процес шифрування. Тому, крім мережевих умов, які нам відомо про використання локальної мережі (LAN), широкосмугової мережі (WAN) та Інтернету, сервер також відіграє важливу роль для підвищення продуктивності.

Виходячи з результатів дослідження можна прийти до висновку, що для одноразового тестування симуляції алгоритму, який найкраще працює в веб-браузері, є наступні:

I. веб-браузер Internet Explorer, який підходить для алгоритмів шифрування Twofish.

II. веб-браузер Mozilla Firefox підходить для алгоритмів шифрування Twofish.

III. веб-браузер Opera, який підходить для алгоритмів шифрування IDEA.

IV. веб-браузер Netscape Navigator, що підходить для алгоритмів шифрування TEA.

Література

[1] Веб-браузер [Електронний ресурс] // wikipedia.org. – 2007.– Режим доступу до ресурсу: http://en.wikipedia.org/wiki/Web_browser.

[2] Encryption: Basic Concepts. [Електронний ресурс]] // Gandalf. – 2007.– Режим доступу до ресурсу: http://www.exegesis.uklinux.net/gandalf/encrypt/basic.htm.

[3] Syed Zulkarnain Syed Idrus, Syed Alwee Aljunid, Salina Mohd Asi, Suhizaz Sudin and R. Badlishah Ahmad (2008). Performance Analysis of Encryption Algorithms': Text Length Size on Web Browsers, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008

Марочканич О.Р., студент
НТУУ «Київський політехнічний інститут імені Ігоря Сікорського»
Факультет інформатики та обчислюваної техніки

ОСНОВНІ ЗАСАДИ ТА ПРИНЦИПИ ОПТИМАЛЬНОГО ПОШУКУ ІНФОРМАЦІЇ

На сьогоднішній день, у світі існує проблема переповнення інформацією. Серед мільярдів гігабайтів даних все важче швидко та якісно знайти потрібну інформацію. Виходячи з цього пошукові системи постійно вдосконалюються спрощуючи та оптимізуючи процес пошуку.

Якщо подивитися на деталі пошуку, то крім очевидної частини у вигляді пошукового рядка можна побачити ще багато чого:

- підказку (вона ж suggest);
- лічильник пошукової видачі (counter);
- різні види сортування (sort);
- фасета (facet) - згруповані характеристи документів;
- синоніми (synonyms);
- пагінація (pagination);
- сніппет (snippet) - невеликий опис документа у видачі;
- і т.д.

І все це служить для однієї мети - задовольнити потребу користувача в знаходженні потрібної інформації максимально швидко і доречно [1]. Наприклад, фільтрація важлива, щоб звузити пошукову видачу. Також важливо доповнювати запити і документи синонімами, щоб за запитом «розробник java» могли знайти документи «java developer».

Крім самого пошуку поруч завжди знаходиться багато компонентів, які полегшують користування сервісом: перевірка орфографії, що відповідає за виправлення помилок, або саджест, який підказує більш популярні запити, коли ви взаємодієте з рядком пошуку. У деяких випадках важливо вміти переформулювати запит. Наприклад, частину запиту перемістити в фільтри: із запиту «робота програміст київ» Київ можна винести в фільтр по місту. Пошук ділиться на дві великі стадії:

- індексація (обробка документів і розкладання їх за спеціальними структурам індексу, для того щоб потім можна було швидко здійснити сам пошук),
- пошук (застосування фільтрів, логічний пошук, ранжування і т. д.).

Розглянемо процес індексації. Для початку вхідні документи потрібно перетворити в набір термінів і відфільтрувати стоп-слова. Ними можуть бути як часто зустрічаються слова - прийменники, сполучники, вигуки, так і інші речі, наприклад, спецсимволи, за якими ми не хочемо шукати. Щоб пошук працював з різними словоформами, в процесі індексації ми зазвичай наводимо всі слова до якогось базового стану. Зазвичай використовується одна з двох процедур: або

стемінг - процес виділення основи слова (розробка-> розроб), або лематизації - процес приведення до нормального формі слова (навиками-> навик).

Найпопулярнішим способом подання індексу є інвертований індекс (inverted index). По суті це різновид хеш таблиці, де ключем є терм, а значенням список документів (а зазвичай список id документів, який називається postings list), в якому цей терм присутній. Зазвичай інвертований індекс складається з двох частин - словника (term dictionary) і списків документів по кожному терму (posting list). Крім того в індексі може міститися інформація про позиції термів в документі (position index), яка буде корисна при пошуку термів на певній відстані, зокрема при фразових запитах, про частотності термів, що допоможе в ранжуванні і при побудові плану запиту.

Словник зберігає в собі всі терми, які існують в індексі, і призначений для швидкого знаходження посилання на список документів. Є кілька варіантів зберігання словника:

- Хеш-таблиця, де терм - ключ, а значення - посилання на список документів цього терма.
- Упорядкований список, за яким можна шукати бінарним пошуком.
- Префіксне дерево.

Найоптимальнішим способом є останній варіант, тому що він має ряд переваг. По-перше на великій кількості термів префіксне дерево буде займати набагато менше пам'яті, тому що повторюються частини префіксів будуть зберігатися всього один раз. По-друге ми відразу отримуємо можливість робити префіксні запити. І по-третє таке дерево можна стискати, об'єднавши нерозділені частини [2].

Звичайно, префіксне дерево може бути не єдиною структурою для зберігання термів в індексі. Наприклад, поряд може перебувати також і суфіксне дерево, яке буде в свою чергу оптимальніше для запитів з джокерами.

Список документів являє собою упорядкований список з ідентифікаторів документів, що дозволяє виробляти з ним деякі оптимізації. Зазвичай він зберігає в собі не тільки список документів, в яких зустрічається терм, а й позиції (postings), на яких воно зустрілося. Це вирішує відразу кілька проблем: ми відразу знаємо скільки разів зустрілося слово в документі, ми можемо робити запити по фразам і запити з певним відстанню між термами, перетинаючи відразу кілька списків документів і дивлячись на позиції термів.

Для пошуку важлива швидкість роботи, тому зазвичай більшість операцій пошуку по індексу виробляються в оперативній пам'яті. Для цього дуже важливо застосувати ряд оптимізацій до індексу, які дозволять вмістити його в обмежений обсяг пам'яті. Крім цього зазвичай застосовується ряд оптимізацій, які дозволяють при пошуку переміщатися по індексу з більшою швидкістю, пропускаючи його непотрібні шматки. Є кілька способів оптимізації, ось деякі з них:

- Компресія дельтами
- VarByte і VarInt
- Skip list / Jump table

Розглянемо другу складову пошуку ранжування. Як ми пам'ятаємо, головне завдання пошуку - отримання максимально релевантної інформації за мінімальний час. І в цьому нам допоможе ранжування документів після того, як ми відфільтрували документи по текстовому запиті і застосували потрібні фільтри і права.

Найпростіший і найлегший спосіб зробити ранжування – це просто впорядкувати документи за датою. У деяких системах раніше так і робилося, наприклад, в новинах або в оголошеннях нерухомості, так користувачеві показувалися спочатку найновіші документи [3].

Іноді може використовуватися модель ранжирування за кількістю знайдених слів в документі, наприклад, коли документів не так багато, і ми хочемо знайти всі документи, в яких зустрічається хоча б одне зі слів запиту. В такому випадку релевантні будуть ті документи, в яких зустрічаються всі слова із запиту або більша їх кількість.

Звичайно, в даний час ці способи вже стали неактуальні, і їх швидше можна віднести до питання історії.

TF-IDF (term frequency - inverse document frequency) - одна з найбільш базових і найбільш використовуваних формул ранжирування. Суть формули в тому, щоб зробити меншою значимість терм, використовуваних повсюдно, наприклад, прийменників і вигуків, і зробити більш значущими терми, які зустрічаються рідко, тим самим показавши у видачі спочатку документи з рідкісними і більш значущими термами із запиту. Більшої ваги отримають документи, у яких терми зустрічаються частіше, але при цьому вони зустрічаються в меншій кількості інших документів. Це дозволяє правильно зважити запит, наприклад, слово developer зустрічатиметься у вакансіях програмістів набагато частіше, ніж назва конкретного мови програмування, і при запиті java developer це дозволить зробити правильне ранжування пошукової видачі.

Підсумовуючи все вищесказане можна зауважити, що поширення та збільшення доступної інформації вимагає строгої типізації та систематизації. Саме тому розробники пошукових систем досліджують все нові і нові способи фільтрування, індексування та ранжування даних. Проблема оптимального пошуку інформації все гостріше постає в наш час, а з розвитком технологій лише збільшить свою важливість.

Література

[1] Пошукова система [Електронний ресурс] // wikipedia.org. – 2014.– Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Web_search_engine.

[2] Ранжирование [Електронний ресурс] // wikipedia.org. – 2013.– Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/Ранжирование.

[3] Как устроен поиск [Електронний ресурс] // habr.com. – 2016.– Режим доступу до ресурсу: https://habr.com/company/hh/blog/413261.

Мерзлікін К.М., студент
Харківський національний університет радіоелектроніки, м. Харків
Факультет комп'ютерних наук, Кафедра програмної інженерії

АНАЛІЗ МЕТОДІВ КЛАСИФІКАЦІЇ ЧАСОВИХ РЯДІВ

На даний момент часові ряди лежать в основі багатьох бізнес активностей. Через це бізнес часто зацікавлений у аналізі та прогнозуванні змінних часових рядів. Часові ряди використовуються у статистиці, обробці сигналів, розпізнаванні шаблонів, економетриці, фінансовій математиці, метеорології, передбаченні землетрусів, електроенцефалографії, астрономії, інженерії комунікацій та в багатьох інших областях прикладної науки та інженерії, де використовуються часові вимірювання.

Часовий рядом називають послідовність точок даних, що зазвичай складається з успішних вимірювань чи спостережень деякої кількісної змінної (або змінних), що відбувалися на протязі часу. Типовими прикладами часових рядів є історичні дані про продажі, облік товарів, кількість клієнтів, курс акцій, витрати, тощо.

Зростаюча необхідність у застосуванні часових рядів для вирішення різноманітних задач спричинила різке підвищення інтересу до дослідження різних типів операцій з рядами. Серед цих операцій наступні: індексація, кластеризація, прогнозування, агрегація, сегментація, класифікація.

Класифікація це процес групування об'єктів у заздалегідь визначені категорії, класи. Зазвичай вона виконується на базі деякого обраного атрибуту (мітки класу), який може набувати кінцевої кількості значень. Завдяки цьому ми завжди знаємо загальну кількість класів. Ключова відмінність класифікації та кластеризації – те, що при кластеризації ми не знаємо заздалегідь загальну кількість груп, групи виявляються у процесі кластеризації. Ціль класифікації – знайти правила, які забезпечать точне відображення об'єктів (в нашому випадку часових рядів) на визначені класи.

У загальному випадку процес класифікації складається з наступних основних кроків:

а) тренування класифікатора: ми тренуємо класифікатор, базуючись на заздалегідь визначеному наборі об'єктів, з використанням тренувального алгоритму;

б) тестування класифікатора: після тренування, отриманий класифікатор має бути верифікований з використанням тестового набору даних. Точність класифікатору перевіряється шляхом його застосування до об'єктів тестового набору та перевірки результуючої і реальної міток класу для кожного об'єкта. Якщо точність класифікатора нижча за бажану, необхідно виконати крок тренування ще раз;

в) застосування класифікатора: якщо отриманий класифікатор має задовільну точність, він може бути використаний для класифікації некласифікованих об'єктів.

Існує декілька способів групування методів класифікації часових рядів. Найбільш зручним є класифікація алгоритмів за типом дискримінаційних властивостей які ці алгоритми намагаються виявити. Можна виділити наступні категорії:

а) методи, що працюють з цілими часовими рядами. Два часові ряди порівнюються або векторним способом або за допомогою метрики відстані, що використовує всі точки даних;

б) інтервальні методи – замість опрацювання цілих часових рядів, цей клас підходів вибирає один чи більше фазово незалежних інтервалів ряду;

в) методи засновані на використанні шейплетів. Це сімейство алгоритмів фокусується на пошуку коротких шаблонів, що визначають цілий клас, але можуть з'явитися будь-де у часовому ряді. Ці шаблони називаються шейплетами. Клас потім визначається за наявністю або відсутністю одного чи більше шейплетів у часовому ряді, що аналізується;

г) методи, що використовують словник. Деякі задачі класифікації вирізняються тим, що головну роль грає не наявність (відсутність) деякого шаблону у часовому ряді, а якого повторюваність. Словникові методи обчислюють частоту повторень сегментів, а потім будують класифікатори засновані на результуючих гістограмах;

д) методи, засновані на використанні моделей. Ці алгоритми намагаються знайти підходящу узагальнюючу модель, а потім визначають схожість часових рядів за схожістю моделей. Деякі з підходів включають використання авторегресивних моделей, прихований моделей Маркова, моделей ядра.

Найбільш поширеними є методи, що працюють з цілими часовими рядами. Більшість з них є комбінацією стандартного класифікаційного підходу k найближчих сусідів та деякої метрики подібності.

Метрикою подібності може виступати проста евклідова відстань, яка однак має вагомий недолік – при зміщенні одного з подібних рядів вдовж часової осі, величина подібності значно зменшується, не зважаючи на незмінну форму ряду. Виправити цей недолік покликана інша метрика подібності – метрика динамічного викривлення часу (dynamic time wrap або DTW). Вона припускає обчислення відстані не тільки між «паралельними» точками даних часового ряду, але й між точками з різними значеннями часу. Після обчислення відстані між всіма можливими (або деякими, залежно від обмежень) парами точок двох часових рядів, відстань між цими рядами (а звідси і показник схожості) знаходиться за допомогою пошуку мінімального сумарного шляху у матриці викривлення, яка містить всі обчислені відстані. DTW використовується у великій кількості областей, включаючи: аналіз супутникових зображень, розпізнавання рухів людини, діагноз несправності двигуна, дослідження шаблонів мобільності міських зон з використанням стільникових даних, розпізнавання голосових команд.

До іншої категорії методів, що знаходить широке застосування, відносяться методи, що використовують шейплети. Шейплет є підпослідовністю часового ряду, що може бути використана у якості примітиву для виконання класифікації, заснованої на локальній, незалежній від фази

схожості у формі. Класифікація з використанням шейплетів включає вимірювання схожості між шейплетом та кожним рядом, а потім використання цього показника схожості у якості дискримінаційної ознаки. Оригінальний класифікатор передбачає виконання пошуку шейплетів через дерево рішень, шейплет знаходиться для кожного вузла шляхом перебору. Вичерпний пошук шейплетів може займати багато часу. Тому більшість досліджень, пов'язаних із шейплетами, фокусуються на техніках прискорення пошуку.

Зазвичай вибір алгоритму класифікації залежить від характеру часових рядів, що аналізуються, та від поставленої задачі класифікації. В багатьох випадках найефективнішим підходом буде комбінований (наприклад, комбінація двох метрик подібності).

Література

1. Ye L., Keogh E. Time series shapelets: a new primitive for data mining – New York, 2009. – 947-956 с.

2. Mueen A., Keogh E., Young N. Logical-Shapelets: An Expressive Primitive for Time Series – New York, 2011. – 1154-1162 с.

3. Aßfalg J. Advanced Analysis on Temporal Data// LMU München, 2008

4. Keogh E., Ratanamahatana C.A. Exact indexing of dynamic time warping// Knowledge and Information Systems, 2005

5. Xi X., Keogh E., Shelton C., Wei L. Ratanamahatana C.A. Fast time series classification using numerosity reduction – New York, 2006 – 1033-1040 с

***Миколайчук Т.В.**, магістрант*
***Фоміченко І.П.**, к.е.н, доцент*
Донбаська державна машинобудівна академія, місто Краматорськ
Кафедра менеджменту

ВПРОВАДЖЕННЯ СУЧАСНИХ СИСТЕМ ФІЛЬТРАЦІЇ У ГАЛУЗЬ КОЛЬОРОВОЇ МЕТАЛУРГІЇ УКРАЇНИ

Кольорова металургія в Україні є потужним промисловим сектором. Галузь кольорової металургії охоплює понад 70 підприємств різних власників.

Можна визначити, що майже 80% видобутку кольорових металів в Україні експортується за кордон через низьке внутрішнє споживання. В даний момент кольорова металургія забезпечує металами галузі народного господарства країни, машинобудування, а також окремі галузі промисловості – радіотехніку, електроніку, електротехніку, авіаційну.

Кольорова металургія України має цілий ряд підгалузей: алюмінієву, електродну, титано-магнієву, рідкіснометалеве, твердосплавну, нікель-кобальтову, свинцево-цинкову, металообробну, вторинної кольорової металургії і напівпровідникових матеріалів.

Виробництво кольорових металів переважно енергоємне тому підприємства розташовують поблизу джерел дешевої електроенергії [1].

Щороку заводами кольорової металургії викидається в атмосферу до 2900 тис. тонн шкідливих речовин. Забруднення навколишнього середовища підприємствами кольорової металургії характеризується переважно викидами SO2, оксидів вуглецю та пилу.

На думку Войцицького А. П. жерелами утворення шкідливих викидів під час виробництва глинозему, алюмінію, купруму, плюмбуму, стануму, цинку, нікелю та дорогоцінних металів є різноманітні види печей [3].

Оскільки метал виділяється в процесі виплавки, величезна кількість сірки окислюється до SO2, що було токсичним для більшості рослинності. Аналогічним чином, алюмінієві установки випускали велику кількість фторидових сполук, які знищили рослинність і негативно вплинули на сільськогосподарських тварин.

Існуючі системи плавки за великі кошти запобігають неконтрольованому вивільненню SO 2 , але в багатьох областях відновлення екосистеми займе роки і, можливо, століття.

Гази з плавильних печей та повітря, що рухаються через вентиляційні системи, випускаються в циклони, скруббери, бачок та інші засоби контролю забруднення повітря для видалення. Таким чином, системи збору можуть бути важливим джерелом експозиції важких металів та інших мінеральних речовин, якщо вони не обробляються, не експлуатуються, не очищуються та не підтримуються належним чином.

Ранні алюмінієві заводи були відповідальні за забруднення повітря через викиди фтору від їх діяльності. Викиди фторидів можуть завдати серйозної шкоди рослинності та тваринам, які живляться такою рослинністю. Мідна руда може містити дуже високі концентрації сірчистих сполук [2].

Викиди летких мікроелементів з процесів випалу, плавлення та перетворення є небажаними як із забруднення повітря, так і з економічної точки зору. Кольорові метали меншого значення мають миш'як, кадмій та тугоплавкі метали, такі як цирконій та титан. Викиди забруднення повітря від виробництва цих металів не становлять серйозної проблеми, хоча біля об'єкта можуть існувати серйозні локальні проблеми. В аналогічному ступені відбувається забруднення атмосферного повітря на підприємствах кольорової металургії , із виготовлення міді, цинку, свинцю, нікелю та інших металів. Тип та ступінь викидів залежать від печі та сплаву.

Використання фільтрів GORE може забезпечити зменшення викидів. Він був першим у виробництві мембранних фільтрів на основі PTFE. З їх PTFE мембраною і міцною конструкцією, фільтрувальні мішки забезпечують високу продуктивність – і цінність - забезпечуючи при цьому ваш завод відповідає всім екологічним нормам. На всіх фільтрових продуктах надійність - стандарт Gore.

Хоча кожен з фільтрів забезпечує ці переваги металургійній промисловості, фільтровий мішок GORE LOW DRAG особливо ефективний. Чим нижче опору фільтра, тим менше енергії потрібно для переміщення повітря через сталевий завод. Завдяки використанню нової власної мембрани, Gore може досягти фільтраційної поверхні, яка залишається практично ідеально

"чистою" та розчищається після кожного циклу системи очищення, що дозволяє знизити падіння тиску та більше повітря.

Результати включають:

- підвищена енергоефективність вентилятора;
- підвищена пропускна здатність;
- збільшений запас мішка;
- потенціал для зменшення кількості фільтрових мішків;
- зниження викидів.

Пакети фільтрів надійно проводять контроль над викидами, що забезпечує гарну репутацію виробників сталі разом з EPA та іншими екологічними організаціями у всьому світі. Різниця в GORE полягає в тому, що він зменшує вартість, за рахунок економії енергії або покращення вилучення неповоротних речовин у печі та цеху через збільшену потужність їхньої газової системи. Така покращена продуктивність може забезпечити більшу гнучкість, щоб оптимізувати свої операції.

І так можна зробити висновок, що впровадження нових систем фільтрації на підприємствах кольорової металургії сприяє зменшенню викидів в атмосферу, зберігає кошти підприємства від сплати штрафів за руйнування екології.

Література:

1.Металургія кольорових металів: Навч. посібн. для вищих навч. закладів. Рабинович О. В., Садовник Ю. В., Ігнатьєв В. С., Трегубенко Г. М., Бубликов Ю. О., — НМетАУ. — Дніпропетровськ: Журфонд, 2009—154 с.

2.*Robert Noyes (1993).* Pollution Prevention Technology Handbook. *Noyes Publications.* ISBN 978-0815513117.

3.Войцицький А. П. Техноекологія : підручник / Войцицький А.П., Дубровський В.П., Боголюбов В.М. ; за ред. В. М. Боголюбова. − К. : Аграрна освіта, 2009. – 533 с.

Мискін Ю.І., Міщенко Р.О., Вальдовский В.І.

Університет державної фіскальної служби України

ХАРАКТЕРИСТИКА СУЧАСНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ АВТОМАТИЗАЦІЇ ОБЛІКОВО-ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ

Характеристику сучасного програмного забезпечення обліково-інформаційних технологій управління діяльністю підприємства доцільно здійснювати у розрізі програм, спрямованих на автоматизацію обліку (1С, Парус, Галактика, ІС ПРО, Фінанси без проблем, САР) та програмних продуктів, що супроводжують електронне звітування перед контролюючими органами (1С: Звіт, Medoc, Арт-звіт плюс, Соната, iFin, Taxer, OPZ, Єдине вікно надання електронної звітності, Електронний кабінет платника податків).

Програма «1С: Бухгалтерія» є лідером українського ринку (займає приблизно 43 %). Спеціалізується на вітчизняних стандартах бухгалтерського обліку. Основними споживачами є підприємства середнього та малого бізнесу.

Програма «Парус» - це вітчизняна комп'ютерна програма з автоматизації обліково-інформаційного забезпечення управління. На ринку України займає приблизно 15 %. Спеціалізується на підприємствах і організаціях державного сектору економіки.

Програма «Галактика» - система ERP, що дозволяє автоматизувати не лише облік, а й інші аспекти управління. Забезпечує можливість ведення обліку за міжнародними стандартами. Займає приблизно 8 % вітчизняного ринку. Основними споживачами є підприємства великого бізнесу.

Програма «ІС ПРО» - розробка корпорації «Інтелект-Сервіс» (розробник програми «Medoc»). Вона спеціалізується на забезпеченні автоматизації обліку на організаціях державного сектору. Використовується у Державній фіскальній службі України.

Програма «Фінанси без проблем» спрямована на автоматизацію обліково-аналітичного забезпечення управління діяльністю бюджетних організацій. Її особливістю є оптимізований розмір баз даних, що досягається за рахунок мінімізації технологічної платформи.

Програма «САР» - лідер світового ринку (використовується приблизно 50 % усіх підприємств у світі). Займає приблизно 10 % українського ринку. Є системою ERP. Забезпечує можливість обліку за міжнародними стандартами. Використовується переважно великим бізнесом та підприємствами з іноземними інвестиціями.

Особливого значення в сучасних умовах господарювання набувають системи електронної звітності. Їх використання дозволяє: зекономити ресурси (час, фінанси), вибрати зручний час для звітування (не обов'язково робочий), використати додаткові можливості (нагадування, консультації тощо), бути впевненим у актуальності форм документів (досягається за рахунок оновлення програм), оперативно контролювати стан та процес звітування, автоматично створювати архів (базу даних з використовуваних документів).

Зазначивши переваги електронного звітування, вважаємо за необхідне акцентувати увагу і на ризиках, які виникають при автоматизації звітування перед контролюючими органами. До них відносяться: можливість несвоєчасного звітування через проблеми з комп'ютерною програмою чи інтернетом, деякі програми потребують самостійного оновлення, робота з різними ключами АЦСК та необхідність захисту архіву – як підтверджуючих документів.

На сьогоднішній день існує достатньо значний вибір програмного забезпечення для електронного звітування перед контролюючими органами. Відтак, кожен суб'єкт господарювання стоїть перед вибором, яке саме програмне забезпечення для електронного звітування обрати. З метою вирішення даного завдання пропонуємо дотримуватися наступного алгоритму:

1) проаналізуйте, які програми працюють з Вашими ключами АЦСК;

2) вивчить, чи є можливість у програмі подавати звітність саме у потрібні для Вас контролюючі органи;

3) оцініть зручність підключення, установки та роботи (попрацюйте з демо версією програми);

4) зверніть увагу чи є технічна підтримка та автоматичне оновлення;

5) проаналізуйте цінову політика;

6) дізнайтесь чи є можливість інтеграції електронного архіву з іншими програмами.

Використання наведеного алгоритму дає можливість визначитися, яке саме програмне забезпечення буде оптимальним для суб'єкта господарювання у контексті електронного звітування перед контролюючими органами.

Псюк Н. М., студентка
ННІ іноземної філології
ЖДУ ім. Івана Франка

КЛАСИФІКАЦІЯ ФРАЗЕОЛОГІЗМІВ: ТЕОРЕТИКО-ПОНЯТІЙНИЙ АСПЕКТ

Фразеологія як наука продовжує розвиватися і привертати увагу все ширшого кола дослідників. При цьому з`являються нові проблеми, уточнюються або ж по-новому висвітлюються питання, досліджувалися до сьогодні.

Фразеологія як наука є досить молодою дисципліною (йдеться про самостійний розділ мовознавства). Стійкі вирази завжди приваблювали дослідників. Тому лексикографів по праву називають першовідкривачами фразеологізмів. Саме вони ставили перед собою мету зібрати і зберегти для майбутнього покоління всі народні перли такі, як прислів`я, приказки, влучні образні вирази тощо; чітко визначити й пояснити їхнє значення (зі стилістичних міркувань); вказати на джерело виникнення і т.д. У середні віки починають укладати словники в яких містяться стійкі сполуки слів. Серед авторів цих праць варто зазначити В. Корте, К. Зімрока, Г. Бюхмана, Й. Ейзелейна, Ф. Тетцнера, Ф. Ліппергайде.

Однією з найвизначніших праць першої половини XX століття є «Німецька фразеологія» Ф. Зайлера. Він вперше спробував диференціювати стійкі сполуки слів. Дослідник виділяє в окремі групи прислів`я, приказки (sprichtwörtliche Redenarten), куди він відносить і власне фразеологізми (Öl ins Feuer giesen), афоризми, крилаті слова, парні сполуки слів. Значну увагу Ф. Залер приділяє сферам виникнення фразеологізмів і тематичній характеристиці.

Через класифікацію фразеологізмів виникло багато дискусій між вченими. Наукові основи класифікації фразеологізмів виділяли такі вітчизняні та зарубіжні вчені, як В. Виноградов, Л. Бухановський, Б. Ларін, О. Кунін, Н. Амосова, Ш. Баллі тощо. В основу цих класифікацій покладено різні принципи,

проте зустрічаються класифікації з подібними рисами, а деякі є трансформаціями інших.

Вперше семантичну класифікацію фразеологізмів було розроблено швейцарським лінгвістом Шарлем де Баллі, який науково обґрунтував необхідність спеціального вивчення стійких словосполучень. З-поміж усіх словосполучень лінгвіст виділяє три групи фразеологізмів: звичайні словосполучення; фразеологічні ряди; фразеологічні єдності.

До звичайних словосполучень належать звороти, свобода вибору яких обмежена Фразеологічні ряди – це звороти, що виражають одне, але складає поняття. Фразеологічні єдності утворюють одне нерозривне ціле [2, с.7, 8, 99, 100].

Тривалий час класифікація В.Виноградова займала чільне місце у дослідженні фразеологічних одиниць. В основу його фразеологічної теорії покладено ступінь видозміни значення слова у різних синтаксичних і стилістичних умовах фразотворення. Він визначає такі три типи фразеологізмів: 1) фразеологічні зрощення; 2) фразеологічні єдності; 3) фразеологічні сполучення. А от прислів` я та приказки В. Виноградов взагалі не включає до класифікації фразеологізмів [1, с. 21].

Вдалою, на нашу думку, є структурно-семантична класифікація російського лінгвіста О. Куніна. Він поділяє фразеологічні одиниці на чотири структурно-семантичні класи:

1) номінативні ФО; 2) номінативно-комунікативні ФО; 3) вигукові і модальні ФО;

4) комунікативні ФО.

Саме класифікація О. Куніна набула наукового статусу класичної в сучасній фразеології.

Отже, наведені класифікації дають змогу виокремити спільні та відмінні риси серед фразеологічних одиниць, розподілених за певними критеріями.

Список використаних джерел

1. Виноградов В. В. Лексикология и лексикография / Виноградов В.В – М., 1977. – 254 с.
2. Фразеологія: знакові величини / [Баран Я. А., Зиморя М. І., Білоус О. М., Зиморя І. М.]. – В.: Нова Книга, 2008. – 256 с.

Рогоза А.В.
Національний технічний університет України
“Київський Політехнічний Інститут ім. Ігоря Сікорського”, м. Київ
Кафедра автоматизованих систем обробки інформації та управління, студент

ХМАРНІ ОБЧИСЛЕННЯ

Бачення комп'ютерних технологій 21-го століття це те, що користувачі матимуть доступ до Інтернет-послуги через легкий важіль портативного пристрою, а не через якийсь нащадок традиційного настільного ПК. Так як

користувачі не мають потужних машин, хто забезпечить обчислювальні потужності? Відповідь на це питання лежить у хмарних обчисленнях.

Хмарна обчислювальна техніка [1] – нещодавня тенденція в IT, що рухає обчислення та дані далеко від настільних і портативних ПК у великі центри обробки даних. Це стосується заявки, наданої як послуги Інтернет, а також фактично хмарна інфраструктура – а саме апаратне та системне програмне забезпечення в даних центрах, які надають ці послуги.

Обчислення є повсюдно широкосмуговим, падають витрати на зберігання та прогресивні покращення в комп'ютерному програмному забезпеченні. Cloud-сервісні клієнти зможуть, знизити витрати, експериментувати з новими послугами, і видаляти непотрібну ємність в той час як постачальники послуг збільшують інвестиції у програмне забезпечення та апаратне забезпечення.

В даний час основні технічні підвалини інфраструктури хмарних обчислень і послуги включають віртуалізацію, програмне забезпечення, орієнтоване на сервіс, обчислення сітки технології, управління великими об'єктами та енергоефективності. Споживачі придбають такі послуги у формі інфраструктури як послуги (IaaS), платформа-як-служба (PaaS), або програмне забезпечення-як-сервіс (SaaS) і продаватимуть додану вартість послуги (такі як комунальні послуги) для користувачів. У межах хмари, закони України надають послуги провайдерам чудово використовуючи статистичне мультиплексування різного навантаження і полегшення управління – єдине встановлення програмного забезпечення може охопити потреби багатьох користувачів.

Ми можемо розрізняти дві різні архітектурні моделі для хмар: перший призначений для масштабування забезпечуючи додаткові обчислення випадків на вимогу. Хмари можуть використовуватися із SaaS та PaaS. Другий архітектурний, модель призначена для надання даних та обчислення інтенсивних додатків через масштабовану здатність.

Хмарна інфраструктура може підтримувати будь-яку модель обчислень, сумісну з вільно пов'язаними кластерами процесора. Організація може забезпечити обладнання для хмар всередині (внутрішні хмари), яку може надати третя сторона – це зовні (розміщені хмари). Хмара може бути обмежена однією організацією або групою (приватні хмара), доступні широкій публіці Інтернет (загальнодоступні хмари), або розділений багатьма групами (гібридні хмари).

Хмара містить обробку, мережу та елементи зберігання. Хмарна архітектура складається з трьох абстрактних шарів: найнижчий рівень є засобом доставки базових можливостей зберігання та обчислення як стандартизовані послуги по мережі. Сервери системи зберігання, комутатори, маршрутизатори та інші системи обробляють певні типи робочих навантажень, від пакетної обробки до сервера або зберігання збільшення при пікових навантаженнях. Середина платформний шар забезпечує вищі абстракції і послуги з розробки, тестування, розгортання, хоста та підтримувати програми в тому ж інтегрованому середовищі розробки. Найвищий рівень має повний набір додатків, які пропонуються як сервіси.

Основні завдання

У 1961 році Джон МакКарті передбачав, що "обчислення" може коли-небудь бути організованою як громадська "утиліта". Ми можемо переглянути парадигму хмарних обчислень як великий крок до цієї мрії. Усвідомлювати це цілком, однак, ми повинні вирішувати кілька важливих проблеми та невикористані можливості щодо розгортання, ефективної роботи, та використання інфраструктури хмарних обчислень.

Архітектура програмного забезпечення / апаратного забезпечення

Про це свідчить виникнення служб хмарних обчислень, фундаментальні зміни програмного та апаратного забезпечення архітектури. Комп'ютерні архітектури повинні зміщувати фокус закону Мура від збільшення тактової частоти на чіп для збільшення числа ядер процесора і ниток на чіпі. Наукові установи повинні розробляти нові системи і послуги, які експлуатують високий ступінь паралелізму. Масові програмні архітектури паралельні, обчислювальні потужності даних, наприклад як MapReduce, буде зростати у популярності. В умовах зберігання технологій, ми, ймовірно, зміна від жорстких дисків (жорстких дисків) до твердотільних накопичувачі (SDD), такі як флеш-пам'ять або дані що повністю замінять жорсткі диски. Найбільші перешкоди для прийняття SSD в центрах обробки даних були ціна, ємність, і, певною мірою, відсутність складних методів обробки запитів. Однак це збирається змінюватися як операції вводу / виводу SSD. Другі (IOPS) переваги стають надто вражаючими для ігнорування, їхня потужність зростає швидко, і ми розробляємо нові алгоритми та структури даних пристосовані до них.

Управління даними, зсув комп'ютерної обробки, зберігання та доставка програмного забезпечення від настільних і локальних серверів, через Інтернет, і в наступну генерацію. Центри обробки даних призводять до обмежень, а також нові можливості щодо даних управління, дані реплікуються по великих географічних відстанях, де їх наявність і довговічність є найважливішою для хмарних постачальників послуг. Обчислення в хмарах повинні бути еластичними для зміна умов. Наприклад, провайдери можуть виділяти додаткові обчислювальні ресурси на льоту оброблячи підвищений попит. Вони повинні розгортати нові підходи управління даними, такі як аналітичне управління даними завдання, багатостадійні бази даних для SaaS, або гібридні конструкції серед управління базами даних, системи (СУБД) та системи MapReduce для того, щоб розглянути обмеження даних та можливості платформ використання зброї у хмарних обчисленнях.

Характеристика сумісності - це здатність клієнтів використовувати ті самі артефакти, як інструменти управління, зображення віртуальних серверів із різними постачальниками хмарних обчислень і платформи.

Хмара взаємодії дозволить хмарам інфраструктури перетворитися на всесвітню, прозору платформу, в якій немає додатків обмежених корпоративними хмарами та хмарним сервісом. Ми повинні будувати нові стандарти та інтерфейси, що дозволять підвищити портативність і гнучкість віртуалізованих додатків.

Безпека та конфіденційність

У хмарних обчисленнях центр даних містить інформацію, що кінцеві користувачі будуть більш традиційно зберігаються на своїх комп'ютерах. Це викликає занепокоєння щодо захисту конфіденційності користувачів, тому, що користувачі повинні передавати свої дані. Крім того, перехід на централізовані послуги може вплинути на конфіденційність та безпеку користувачів взаємодії загрози безпеки можуть статися у забезпеченні ресурсів та під час розподілу виконання заявки. Також, швидше за все, з'являться нові загрози. Наприклад, хакери можуть використовувати віртуалізовану інфраструктуру як майданчик для нових атак. Обласні сервіси повинні зберігати цілісність даних та конфіденційність користувачів. В той же час вони повинні покращувати сумісність через декілька постачальників послуг хмарної служби. У цьому контексті ми повинні вивчити нові захисти даних, механізми забезпечення конфіденційності даних, захист ресурсів та вміст авторських прав.

З точки зору економіки хмар, постачальнику слід запропонувати ресурсно-економічні послуги. Енергозберігаючі схеми для кешування, запит на обробку та термічне управління є обов'язковими через збільшення кількості відходів. Крім того, нове ціноутворення моделі, що базується на політиці pay-as-you-go необхідні для вирішення дуже змінних ресурсів хмари на попит.

Хмарна обчислювальна техніка є руйнівною технологією з глибокими наслідками не тільки для Інтернет-послуг, а також для IT-сектора в цілому. Його поява обіцяє оптимізувати забезпечення за замовчуванням програмного забезпечення, апаратне забезпечення та дані як послуги, досягнення економії масштабу при впровадженні IT-рішень і операцій.

Тим не менше, існують деякі вирішальні питання, зокрема пов'язані з SLA, безпекою, конфіденційністю і енергоефективністю. Інші відкриті питання включають право власності, вузькі місця передачі даних, продуктивність, непередбачуваність, надійність і питання ліцензування програмного забезпечення. І, нарешті, бізнес-моделі повинні показувати чіткий шлях до монетизації хмарних обчислень. Кілька компаній вже побудували Інтернет споживчі послуги, такі як пошук, соціальні мережі, веб-електронна пошта та Інтернет-комерція, що використовують інфраструктуру хмарних обчислень. Понад усе, невизначена "прихована програма" хмарних обчислень визначить багато проблем і рішень, які ми повинні розвинути, щоб зробити цю технологію працюючою.

Література

1. Хмарні обчислення [Електронний ресурс] / Режим доступу: https://en.wikipedia.org/wiki/Cloud_computing.

Рогоза А.В.
Національний технічний університет України
"Київський Політехнічний Інститут ім. Ігоря Сікорського", м. Київ
Кафедра автоматизованих систем обробки інформації та управління, студент

МОБІЛЬНА ХМАРНА МЕРЕЖА

Мобільна медіа-мережа була передбачена, щоб використовувати нові технології хмарних обчислень до підвищення мобільного медіа-досвіду.

На рисунку 1 ми ілюструємо схему кінцевого перегляду хмарної мобільної система масової інформації. Система складається з трьох учасників: зацікавлені сторони в ланцюжку вартості цифрових засобів масової інформації, включаючи постачальників контенту, постачальники мультимедійних сервісів та вміст споживачі. Крім того, унікальна для парадигми мобільного обласного середовища, крапка мобільної хмар, яка і включається в робочий процес, щоб підкреслити складний виклик управління радіоресурсами в цій цілісній архітектурі.

Провайдери вмісту несуть відповідальність за створення медіа-вмісту для розподілу та споживання. ЗМІ може бути вмістом сформованим професійними виробниками зі складної цифрової камери або звичайні користувачі Інтернету, які знімають відео та / або зображення з власними (мобільними) пристроями.

Зміст носіїв захопленими цими мобільними пристроями, є переважними технічні проблеми при обробці, передачі та аналізі вони, для традиційних систем масової інформації, вимагають нових рішень, що охоплюватиме останні досягнення в інформації та комунікації технології (ІКТ), зокрема хмарних обчислень технології. Посередники хмарних сервісних служб збирають пул спільного доступу ресурсу ІКТ, включаючи обчислення, зберігання та мережеві зв'язки і виділятють їх еластично для різних медіа-завдань у відповідь на вимоги до застосування в режимі реального часу. Обчислення місткості може бути отримане з різноманітного набору ресурсів, наприклад, центри обробки даних, в яких розташований парк універсальних стійок / блейд-серверів комерційного класу і масивів ЦП / ГПУ призначені для обробки зображень або відео. Ці об'єкти часто перебувають на стороні супермаркетів, які поширюються в різних місцях і можуть бути запитом на вимогу. Місця для зберігання можуть надходити з щільні резервування (наприклад, мережа пам'яті) або рідкісні (вбудовані диски з серверами). Ці ресурси зберігання пов'язані між собою мережевою тканиною для формулювання пулу системних ресурсів, як показано на рис. 1. Цей пул ресурсів ІКТ може бути динамічно змінено для виконання завдань у медіа-мережах, наприклад, обробки медіа (кодування / декодування / транскодування), розповсюдження медіа, рендеринг засобів масової інформації та аналітика засобів масової інформації, щоб назвати декілька. Порівняно до статичного розподілу ресурсів у традиційних системах масової інформації, обладнана медіа-мережа може збільшуватися і зменшуватися, щоб відповідати динамічному попиту, з меншою вартістю та кращою QoS для досвіду роботи з медіа. Наприклад, медіа-мережа на основі хмар може краще справлятися з

горезвісним феноменом флеш-натовпу в засобах масової інформації, коли багато користувачів цікавляться непередбачено конкретним фрагментом вмісту протягом дуже короткого часу.

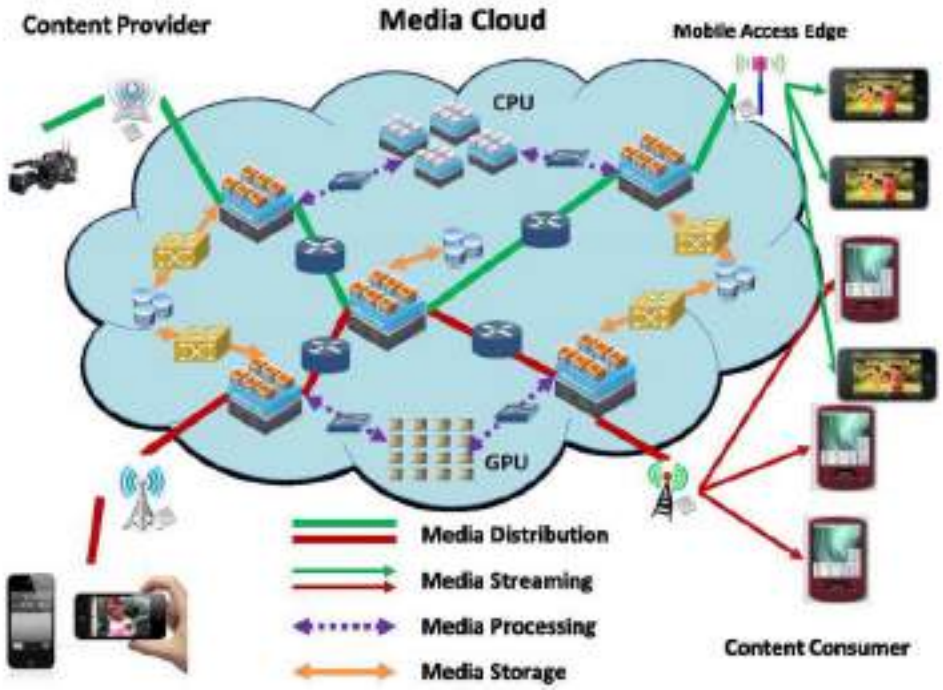


Рис. 1. Пул ресурсів

Споживачі вмісту дивляться відео на різні ЗМІ (наприклад, телевізор, ноутбук, смартфон і планшет) через безпровідний Інтернет. У дизайні цього випадку використовується перелік технічних проблем, в тому числі:

• Мобільні пристрої за своєю суттю обмежені ресурсами.

• З'єднання, що піддається мобільним пристроям, зазвичай і поступається їх настільним колегам.

• Очікування мобільних користувачів стають дедалі більшими, тому що такі функції, як підтримка мобільності, інтерактивна підтримка, природно, в прикладних програмах, що не стосуються засобів масової інформації.

Це обурення між обмеженими ресурсами та високим попитом мобільних засобів масової інформації з гідним QoS неперевершені. Ми бачимо все нові і нові рішення, використовуються нові технології хмарних обчислень для забезпечення додаткового джерела системи для покращення досвіду перегляду бездротового Інтернету.

Мобільне хмарне середовище відіграє важливу роль у з'єднанні обмежених ресурсів мобільного пристрою з багатими ресурсами інфраструктури хмари. Приклади мобільної хмари включають базу станції, точок доступу до Wi-Fi та інші бездротові пристрої. Ключовим компонентом для безперебійної взаємодії між хмарою та мобільним пристроєм – є схема доступу через різні бездротові шлюзи. Це через такі бездротові шлюзи, що мобільні пристрої можуть вивантажити обмеження в обчислення та зберігання в хмарі. Поточна хмара мобільної ЗМІ системи приймає різні протоколи зв'язку, як її бездротові шлюзи, включають Wi-Fi, Bluetooth, WiMAX і 3G / 4G LTE. Ці бездротові шлюзи часто використовуються в мобільній хмарні обчислень. Для обласних мобільних мультимедійних програм попит на широкосмуговий доступ

і постійне підключення, щоб забезпечити адекватну якість досвіду (QoE) для мобільних пристроїв споживачі медіа нав'язують значні виклики. Протягом деякої розширеної медіа-програми, на відміну від дротових мереж, мобільні користувачі можуть переходити через декілька локальних бездротових мереж: доступ до осередків і вимагає безперебійного перемикання носіїв шлюза (точка доступу) з однієї комірки до іншої.

Більш того, бездротові шлюзи до хмари часто складаються з гетерогенної мережі радіодоступу. Неоднорідність сьогоднішньої мережі бездротового доступу ставить додаткові виклики для ефективного доступу та керування ресурсами через декілька технології радіодоступу. Потрібен інтелектуальний підхід, щоб бути спроектованим, щоб завжди підтримувати високу якість широкосмугового мобільного зв'язку, використовуючи наявні мобільні пристрої конкретної інформації в місці, контексту та запиту користувачів послуги. Альтернативний підхід добре ілюструється а

Мережі та користувацький термінал використовуються як звичайні частотні смуги і, отже, повинні мати когнітивний спектр сенсорної функції, щоб знайти вакантні смуги частот для праці.

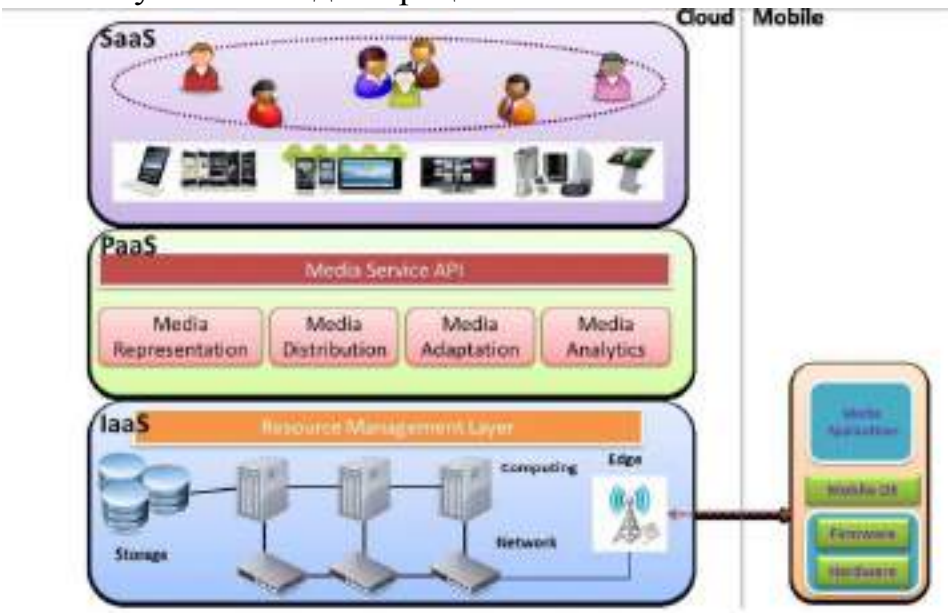


Рис. 2. Багатошарова модель служби

Система хмарних мобільних медіа, успадкована від визначення з Cloud Computing, також можна зрозуміти в багатошарову модель служби, як показано на малюнку 2. В цій багатошаровій моделі немає зв'язування між двома інтерфейсними шарами, в той час як в Інтернет-шаровій моделі зв'язування служб здійснюється між інтерфейсами шару, зокрема, медіа-послуги на рівні PaaS може перебувати як у хмарній інфраструктурі, так і в сирій інфраструктурі ІКТ або на гібриді обох ресурсів

Масштабований перегляд забезпечує лише концептуальна ієрархія під складністю хмарного мобільного медіа-архітектора:

- Infrastructure-as-a-Service: у IaaS, ресурси ІКТ об'єднані з гібридної хмарної інфраструктури увімкнено за технологією віртуалізації, постачальник хмарних послуг може виділити ці ресурси в тонкій формі. Ці ресурси можуть піддаватися впливу засобів масової інформації додатків та / або медіа-послуг у

неформальному форматі, зі спеціальною угодою про рівень обслуговування (SLA). В рамках цієї моделі ключовим компонентом є протокол управління розподіленим ресурсом, який здійснює нагляд за всіма наявними ресурсами у хмарній інфраструктурі. Інтелектуальні алгоритми повинні бути розроблені в дослідженнях, щоб розглянути список технічних проблем у хмарному ресурсі управління та у зв'язку з розширеним мобільним носієм;

- Platform-as-a-Service: у PaaS різні носії послуги інкапсулюються в шар проміжного програмного забезпечення, що працює над сирими ресурсами ІКТ або обласними ресурсами ІКТ;
- Software-as-a-Service: у SaaS - мобільний носій вмісту та програми споживаються глядачами в їх мобільні пристрої. Як правило, ці програми складаються з легкого клієнта працючого на мобільних пристроях.

Література

1. Мобільна хмарна мережа [Електронний ресурс] / Режим доступу: https://en.wikipedia.org/wiki/Mobile_cloud_computing.

Рогоза А.В.
Національний технічний університет України
"Київський Політехнічний Інститут ім. Ігоря Сікорського", м. Київ
Кафедра автоматизованих систем обробки інформації та управління, студент

ВРАЗЛИВІСТЬ ХМАРНИХ ОБЧИСЛЕНЬ

Кожен день, свіжі новини чи запис в блозі попереджає нас про ризики хмарних обчисленнях та загрози безпеці, в більшості випадків – безпека називається найбільш суттєвим блокуванням для поглинання хмарних обчислень. Але ця дискусія про проблеми з хмарними обчисленнями ускладнює роботу. По-перше, у багатьох в цій дискусії про ризик, основні терміни лексики - в тому числі ризик, загроза та вразливість взаємозамінно, незалежно від їх відповідних визначень. По-друге, не кожне підняте питання є специфічним до хмарних обчислень. Щоб досягти обґрунтованого розуміння, що додає хмарне обчислення щодо безпеки проблеми, ми повинні проаналізувати, як облаштовані обчислення впливають на встановлені проблеми безпеки. Ключовий фактор тут це вразливості системи безпеки: хмарне обчислення робить певну добре усвідомлену вразливість більш значущою а також додає нові в суміш. Перш ніж вивчати вразливості, пов'язані з хмарами, спочатку встановимо, що таке "вразливість" насправді.

Відповідно до таксономії ризику Open Group, Вразливість [1] - це ймовірність того, що буде не в змозі протистояти дії агента-загрози. Вразливість існує, коли є різниця між силою, яка застосовується агентом загрози та об'єктом, який здатний протистояти цій силі. Отже, вразливість завжди повинна бути описана в термінах стійкості до певного типу атаки. Реальний приклад – нездатність автомобіля захистити його водія проти травми, коли потрапляє в

фронт вантажівкою водіння 90 км / год – вразливість: опір автомобіля просто занадто слабкий порівняно з силою вантажівки. Проти "атаки" байкера, або навіть маленького автомобіля, що їздить на більш помірній швидкості – потужність опору автомобіля є абсолютно адекватною.

Вразливості в технології Core-Technology. Основні технології хмарних обчислень [2] – веб-додатки і сервіси, віртуалізація та криптографія – мають вразливості, які є невід'ємними для технологій або поширені в сучасній технології реалізацій. Два приклади таких вразливостей: викрадення віртуальної машини та небезпечна або застаріла криптографія.

По-перше, можливість того, що зловмисник може успішно втекти з віртуального середовища, такою є сама природа віртуалізації. Отже, ми повинні враховувати, що ця вразливість властива віртуалізації і дуже актуальна для хмарних обчислень. По-друге, технології веб-додатків повинні подолати проблему, яка за проектом HTTP-протоколу є протоколом без громадянства, тоді як веб-додаткам потрібно певне уявлення про стан сеансу.

Незалежно від того, чи є ураження сеансом, чи викраденням, воно є невід'ємною частиною технологій веб-додатків. У будь-якому випадку, такі вразливості, безумовно, є доречні для хмарних обчислень.

Нарешті, просування криптоаналізу може зробити будь-який Криптографічний механізм або алгоритм невпевненим як у виявлені нового методу так і його розбиття. Ще частіше зустрічаються критичні недоліки: алгоритм реалізацій, який може обернутися із сильного шифрування в слабке шифрування (або іноді немає шифрування взагалі). Оскільки широке поглинання хмари обчислень немислимі без використання криптографії для захисту конфіденційності даних та цілісності в хмарі, небезпечні або застарілі криптографічні вразливості дуже важливі для хмарних обчислень.

Характерні вразливості для хмари: попит на самообслуговування, всюдисущий доступ до мережі, пул ресурсів, швидка еластичність, і вимірюване обслуговування. Основні причини в однієї або декількох з цих характеристик:

• Несанкціонований доступ до інтерфейсу керування. Хмарна характеристика на вимогу самообслуговування вимагає інтерфейс керування, доступний для хмарного сервісу користувачів. Несанкціонований доступ до управління інтерфейсу, є особливо актуальною вразливістю для хмарних систем: ймовірність, що неавторизована доступ може мати місце набагато вище, ніж для традиційних системи, де функціонує управління доступне лише для декількох адміністраторів.

• Вразливості Інтернет-протоколу. Хмарі характерний повсюдний доступ до мережі, це означає, що хмарні сервіси доступні через мережу за допомогою стандартних протоколів. У більшості випадків ця мережа являє собою Інтернет, який слід вважати недовірливим.

• Вразливість відновлення даних. Хмарні характеристики: поєднання та еластичність передбачають, що при виділенні ресурсів одному користувачеві буде перерозподіл іншому користувачеві пізніше, для пам'яті або запам'ятовуючого ресурсу. Тому може бути можливим відновлення записаних даних попереднім користувачем.

Обчислювальні ресурси

Надзвичайно релевантний набір розрахункових вразливостей ресурсів стосується обробки зображень віртуальних машин: єдиний можливий спосіб надання майже ідентичного серверного зображення, що забезпечує послугу під замовлення для віртуальних серверів – це клонування образів шаблонів.

Вразливості ОС або програми для розповсюдження серед багатьох систем: зловмисник міг би проаналізувати конфігурацію і код докладно використовуючи адміністративні права на оренду віртуального сервера як служби клієнтом і, таким чином, отримуючи корисні знання атакувати зображення інших клієнтів. Пов'язана проблема це те, що зображення можна взяти з недостовірності джерела, нове явище, особливо з'являється на ринку віртуальних зображень для IaaS (Infrastructure as a service). У цьому випадку зображення може, наприклад, маніпулювали таким чином, щоб забезпечити доступ до дверей для зловмисника.

Витік даних за допомогою реплікації віртуальної машини – це вразливість, яка теж пов'язана з використанням клонування для надання послуг на замовлення. Клонування призводить до проблеми з витоком даних стосовно машинних секретів: певні елементи ОС, такі як ключі хостів і криптографічні цінності - призначені для приватного спілкування, хост клонування може порушувати таке припущення про конфіденційність.

Знову ж таки, з'являється ринок для віртуальної машини зображення, як в Amazon EC2, це все призводить до пов'язаної проблеми: користувачі можуть надавати зображення шаблонів для інших користувачів, перетворення робочого зображення у шаблон. Залежно від способу використання зображення перед створенням шаблону, він може містити дані, які користувач не бажає оприлюднити.

Існують також контрольні проблеми, в тому числі пов'язані з використанням криптографії. Криптографічні вразливості через слабке покоління випадкових чисел може існувати, якщо абстрактний шар між апаратним забезпеченням і ядром ОС, впроваджене шляхом віртуалізації, є проблематичним для генерації випадкових чисел.

Усі хмарні сервіси (і керування кожним хмарним сервісом) вимагають механізмів управління ідентифікацією, аутентифікацією, авторизацією та аудитом (IAAA). Певною мірою, можуть бути частинами цих механізмів враховуючи як окремий сервіс IAAA для використання в інших послугах. Два елементи IAAA, які повинні бути частиною кожнної реалізації служби є виконанням адекватної перевірки авторизації (що, зазвичай, використовує аутентифікацію та / або інформацію про авторизацію, отриману від служби IAAA) та перевірка хмарної інфраструктури.

Більшість вразливостей пов'язаних з IAAA: компонент повинен розглядатися як обласний характер, оскільки вони поширені в найсучасніших хмарних пропозиціях.

Приклад механізму аутентифікації користувача включає в себе:

• Відмову в обслуговуванні через блокування облікового запису. Один часто використовуваний контроль безпеки, особливо для аутентифікації з ім'ям

користувача та паролем - це блокування облікових записів, які отримали кілька невдалих аутентифікацій. Зловмисники можуть використовувати спроби запустити DoS-атаки на користувача.

• Недостатня або несправна перевірка авторизації. Відсутній дозвіл перевірки, наприклад, є основною причиною виникнення атаки URL-адреси. У таких атаках користувачі змінюють URL-адреси для відображення інформації інших облікових записів користувачів.

• Крупний контроль авторизації. Керування Cloud Services інтерфейсами особливо схильне пропонувати моделі керування авторизацією, які є надто грубими. Таким чином, стандартні заходи безпеки, такі як розподіл обов'язків, не може бути реалізованим, оскільки це неможливо надавати користувачам лише ті привілегії, які вони мають суворо вимагати виконуючи свою роботу.

• Недостатнє ведення журналу та можливості моніторингу. В наш час немає ніяких стандартів чи механізмів для надання реєстрації клієнтів хмари. Також провайдер моніторингу безпеки часто перешкоджає можливості моніторингу.

З усіх цих уразливостей IAAA, в досвіді постачальників хмарних сервісів, в даний час проблема аутентифікації є основною вразливістю, яка наражає на ризик інформацію користувача в хмарних сервісах.

Вразливості, які мають відношення до всіх хмарних компонентів обчислень, як правило, стосуються постачальника – або скоріше, нездатність користувачів контролювати хмарну інфраструктуру в той час як вони роблять свою власну інфраструктуру. Серед контрольних викликів – недостатні можливості аудиту безпеки, і той факт, що схеми сертифікації та показники безпеки не приймаються до хмарних обчислень. Далі стандартний контроль безпеки щодо аудиту, сертифікації, і безперервний моніторинг безпеки не може бути ефективно впровадженим.

Література

1. Вразливість [Електронний ресурс] / Режим доступу: https://en.wikipedia.org/wiki/Vulnerability;

2. Хмарні обчислення [Електронний ресурс] / Режим доступу: https://en.wikipedia.org/wiki/Cloud_computing.

Синельников Н.Д.
ГВУЗ «Приазовский государственный технический университет»,
г. Мариуполь,
Кафедра информатики, студент группы ВТ-17-М

ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ ДЛЯ ДЕЯТЕЛЬНОСТИ НЕКОММЕРЧЕСКОГО ПРЕДПРИЯТИЯ

Девять лет спустя системы, основанные на цифровой наличности, стали для Интернета таким же привычным явлением, как, например, безналичные

деньги для реального мира. И это притом, что электронные платежные системы, как правило, экстерриториальны, как и весь рынок интернет-торговли. То есть, скажем, француз может запросто совершить покупку в английском электронном магазине, оплатив товар деньгами английской же электронной платежной системы.

Система электронных платежей, или электронная платёжная система - это система расчётов между финансовыми организациями, бизнес-организациями и Интернет-пользователями при покупке-продаже товаров и за различные услуги через Интернет. Такие системы представляют собой электронные версии традиционных платёжных систем и по схеме оплаты делятся на:

1. дебетовые (работающие с электронными чеками и цифровой наличностью);
2. кредитные (работающие с кредитными карточками).

Любая Электронная Платежная Система обеспечивает ряд преимуществ своих электронных денег по сравнению с деньгами традиционными, ведь переводы и платежи внутри ЭПС обладают следующими свойствами:

1. Моментальностью (занимают считанные секунды);
2. Анонимностью (не во всех платежных системах);
3. Относительно небольшими комиссиями (сопоставимыми с комиссиями банков);
4. Экстерриториальностью;
5. Защищенностью (электронные деньги нельзя или крайне сложно подделать, в отличие от наличных);
6. Делимостью (любая сумма ЭД больше принятого в данной ЭПС минимума может быть без труда разделена на много более мелких частей).

Принципы использования электронных денег остались прежними:

Самостоятельное пополнение своего счет, когда необходимо идти в банк.

Используя электронный кошелек. Получая переводы как с другой карты, так и получая переводы с электронных внебанковских систем(PayPal, Webmoney, Qiwi и .т.д).

PayPal — крупнейшая дебетовая электронная платёжная система. Позволяет клиентам оплачивать счета и покупки, отправлять и принимать денежные переводы. С октября 2002 года является подразделением компании eBay. С 20 июля 2015 года акции PayPal и eBay продаются на рынке отдельно. В 2015 году стоимость отделившейся компании PayPal на фондовом рынке оценивалась выше, чем стоимость её прежней материнской компании[2].

По состоянию на 2017 год PayPal работает в 202 странах (хотя не во всех предоставляется полный набор услуг), имеет более 200 млн зарегистрированных пользователей, работает с 25 национальными валютами.

Недостатками системы PayPal можно считать:

- возможность блокировки счета без объяснения причин (разумеется, блокировку можно оспорить, но это потребует времени);
- невозможность проведения конвертации валют (например, из гривны – в доллары, из долларов – в фунты стерлингов и так далее);

- значительные ограничения для пользователей из стран бывшего СССР (правда, этот недостаток относится, скорее, к законодательству этих стран).

Преимуществами системы PayPal можно считать:

- превосходный уровень защиты финансов;
- рекордная распространенность – благодаря PayPal вы можете пользоваться собственным электронным счетом практически в любой стране мира;
- высокая скорость выполнения операций;
- простота и доступность русифицированного интерфейса, работать с которым может любой пользователь компьютера и интернета;
- возможность проведения операций со счетом при помощи мобильного;
- тщательная проверка продавцов как дополнительная защита от мошенничества.

Когда-то все расчеты происходили с помощью наличных денег. Это позволяло однозначно проводить идентификацию и аутентификацию. Потом пришло время банковских переводов через банковские счета, затем в ход пошли пластиковые карты. Очевидно, что сейчас намечается глобальная тенденция перехода от наличных, банковских счетов и пластиковых карт к инновационным платежным услугам: все активнее используются электронные и мобильные платежи и переводы. Если говорить об электронных деньгах, то сейчас это в основном предоплаченные карты или электронные кошельки, которые в торговом обороте вытесняют наличные деньги. Программы в области электронных денег функционируют во многих странах: Австралии, Бразилии, Китае, Франции, Германии, Индии, Японии, России и многих других. В качестве примеров областей успешного применения электронных денег можно назвать оплату общественного транспорта, стоянок, телефонной связи и т. д.

Литература

1. Электронные деньги и мобильные платежи. Энциклопедия. – М.: КноРус, 2009.
2. Афонина С. Электронные деньги. – СПб.: Питер, 2008.

Сініцин О.В.

Національний університет біоресурсів і природокористування Укроаїни
Кафедра комп'ютерних систем і мереж, аспірант

АЛГОРИТМІЧНІ ТА ПРОГРАМНІ ЗАСОБИ ФОРМУВАННЯ І ВІДОБРАЖЕННЯ ТРИВИМІРНОГО ЗОРОВОГО ОБРАЗУ ЗЕМЕЛЬНОЇ ДІЛЯНКИ ТА ОБ'ЄКТІВ НАЗЕМНОГО БАЗУВАННЯ В ГЕОІНФОРМАЦІЙНІЙ СИСТЕМІ ПРЕЦИЗІЙНОГО ЗЕМЛЕРОБСТВА

Системи прецизійного землеробства базуються на новому погляді на сільське господарство, при якому поле, неоднорідне за рельєфом, ґрунтовим покривом, агрохімічним вмістом потребує застосування на кожній ділянці окремих агротехнологій [1].

На сьогоднішній день для забезпечення технології прецизійного землеробства використовують дистанційні методи вимірювання стану ґрунтового покриву та посівів, системи глобального позиціонування, а також інструментарій геоінформаційних систем (ГІС) [2]. Інтегруючою основою технології прецизійного землеробства є геоінформаційні системи (ГІС), що дозволяють знімати, накопичувати і обробляти інформацію, що характеризує, наприклад посіви або ріллю, тощо [3].

Для формування і відображення зорового образу земельної ділянки та об'єктів наземного базування в геоінформаційній системі прецизійного землеробства необхідно вирішити ряд взаємопов'язаних задач, а саме:

- розробити алгоритм створення класифікатору складених умовних знаків об'єктів наземного базування використовуючи бібліотеку умовних знаків у ППП Digitals;
- розробити алгоритм формування тривимірного зорового образу земельної ділянки в геоінформаційній системі прецизійного землеробства.

Класифікація об'єктів наземного базування проводиться згідно з правилами позначення вихідної множини об'єктів на підмножини відповідно до певних правил кодування, кожному з яких надається унікальний код, який призначений для формалізованого опису різних характеристик даних.

Для ведення бібліотеки умовних знаків (УЗ) в ППП Digitals використовується «Менеджер умовних знаків». Переглядаючи каталог УЗ та помічаючи відповідну піктограму можливо побачити збільшене зображення знаку, та назву шарів яким даний знак належить.

Проведено розрахунок кількості елементів для формування УЗ на прикладі техніки озброєння згідно стандартів NATO

$$N_i = (n_1 * n_2 * \cdots * n_n) \quad (1)$$

$$N_j = (1 + n_1 + n_2 + \cdots + n_n) \quad (2)$$

де N_i - Множина умовних знаків в стандартній бібліотеці УЗ ППП Digitals

N_j - Множина умовних знаків в бібліотеці УЗ ППП Digitals при використанні запропонованої технології створення складеного УЗ

n_n - кількість складових елементів УЗ, що залежить від параметру n.

Для вирішення задачі розробки оптимальної схеми формування зорового образу окремої земельної ділянки, нами пропонується алгоритм, що забезпечує формування і візуалізацію двомірних і тримірних зорових образів окремої земельної ділянки, який містить наступні блоки:

растрова карта – блок відображає прив'язані та трансформовані картографічні зображення, перетворені в електронний вигляд, що зберігаються у вигляді, придатному для обробки;

векторна карта – блок відображає векторизовані растрові зображення, що зберігаються у вигляді, придатному для обробки;

семантичні дані – блок відображає масив атрибутивних даних та метаданих, що зберігаються у вигляді, придатному для обробки.

- проофіль автодороги, грунтовий профіль, профіль рівня грунтових вод – блоки, що відображають прив'язані та трансформовані растрові зображення, перетворені в електронний вигляд та векторні зображення, що зберігаються у вигляді, придатному для обробки;
- генерація тривимірного, шестигранного об'єкта – блок відображає зумовлений процес, що складається операцій, які визначені в підпрограмі, що створює тривимірний об'єкт, кожна грань якого відображає один, або декілька вхідних шарів;
- формування зорового образу окремої земельної ділянки – блок відображає зумовлений процес, що складається операцій, які визначені в програмі, що відображає тривимірний об'єкт.

Створений таким чином зоровий образ окремої земельної ділянки є основою для побудови програмного засобу, який формує і візуалізує двомірні і тримірні моделі окремої земельної ділянки в ГІС ПЗ (далі - геопорталу), у web - середовищі.

Висновки. Вперше запропоновано алгоритм побудови складених умовних знаків, що дозволяє створювати велике різноманіття знаків які здатні адаптуватись під умови їхнього використання (освітленість, носій, завантаженість карти), та кількість параметрів, що приймають участь у формуванні знаку.

Також в статті запропоновано алгоритми формування і відображення зорового образу окремої земельної ділянки, які є основою для побудови програмного засобу, який формує і відображає двомірні і тримірні моделі окремої земельної ділянки та об'єкти наземного базування в ГІС ПЗ.

Список літератури:

1. Ласло О. О. Впровадження технологій точного землеробства в Україні / О. О. Ласло // Вісн. Полтав. держ. аграр. акад. - 2011. - № 1. - С. 49-50.

2. Vasiukhin M. Methods and means for building a system of visual images forming in GIS of precision agriculture / M. Vasiukhin, O. Tkachenko, A. Kasim, I. Ivanyk // Збірник матеріалів Міжнародної наукової конференції "Біоресурси планети та біобезпека навколишнього середовища: проблеми та перспективи", 4 – 7 листопада 2013. – К., Аграр Медіа Груп, 2013. – С. 24 – 31.

3. Белавцева Т.М. Технологии точного земледелия, их перспективы и возможности использования на мелиорированных землях. М.: ФГНУ ЦНТИ «Мелиоводинформ», 2009. - 112 с.

Слабінога Мар'ян Остапович, канд. техн. наук, доц. кафедри КСМ
Семків Роман Юрійович, студент кафедри КСМ
Івано-Франківський національний технічний університет нафти і газу

СИСТЕМА ПРОПУСКНОГО КОНТРОЛЮ НА БАЗІ ESP8266 ТА ПЛАТФОРМИ ARDUINO

Автоматизований облік відвідуваності установ та організацій є надзвичайно важливою прикладною задачею в галузі інформаційних технологій, оскільки цей процес допомагає ефективно визначати дисципліну чи вести необхідні статистичні дані. Система допомагає виявляти порушення дисципліни (запізнення чи пропуски), а також здійснює підтримку керування доступом до об'єктів та визначає всі спроби отримання доступу до них.

Для реалізації апаратного забезпечення системи автоматизованого обліку відвідуваності було вибрано модуль, який складається з плати ESP8266 (12 серії) та мікропроцесорної плати Arduino Nano, яка відповідає за відправку даних. Програмне забезпечення було реалізоване як веб-додаток на основі платформи NodeJS та з використанням VueJS, та відповідає за збір, обробку і показ даних. Переваги даного апаратного та програмного забезпечення системи полягають у його вартості та універсальності. Вартість системи набагато нижча ніж у комерційних аналогів (вартість одного модуля становить 8-10$). Універсальність полягає в тому, що систему можна сконфігурувати під будь-які потреби і завдання, без змін в апаратній частині.

Мікроконтролер ESP8266 (12 серії), який має базову підтримку Wi-Fi та має власну файлову систему SPIFF розміром 4 Мб, 1 аналоговий вхід, 10 цифрових вводів/виводів (8 з підтримкою ШІМ) та UART інтерфейс, використовується для зв'язку з Arduino або з іншими пристроями вводу/виводу провідним шляхом.

Платформа Arduino Nano в собі містить 14 цифрових вводів/виводів (6 з яких з підтримкою ШІМ) та 8 аналогових входів.

Зв'язок між робочим модулем та веб-додатком може здійснюватись як і безпровідно за допомогою Wi-Fi, так і через Ethernet, обох випадках через протокол MQTT. Підтримка протоколу має бути реалізована на сервері обов'язково, тому, що вимагається брокер (посередник) для передачі даних, яким і є сервер. Спочатку повідомлення приходить до брокера потім з нього розсилається потрібним пристроям або в веб-застосунок. Налаштування пристроїв зберігаються в файлі конфігурації на вбудованій в ESP8266 SPIFF файловій системі. В системі передбачена можливість деякий час працювати автономно, використовуючи акумулятор, всі дані за цей час накопичуються, а при відновленні роботи брокера відправляються на нього.

Система дозволяє отримувати та показувати будь-які необхідні задані параметри про людину, яка хоче отримати доступ на об'єкт. Аутентифікацію можна здійснити за допомогою біометричних даних (відбиток пальця), RFID - карт (міток) з унікальним, незмінним номером або PIN – кодом.

Для аутентифікації потрібно прикласти RFID мітку/картку до робочого модуля, у випадку її відсутності можна ввести PIN чи сканувати поверхню пальця. Після цього можна виконати якусь запрограмовану дію, яка потрібна клієнту системи (почати/закінчити відлік часу, відмітити присутність людини в журналі або дату та час аутентифікації, відкрити двері/турнікет).

Веб-додаток написаний на мові Javascript, та розгортає власний MQTT сервер (брокер) на 1883 порті. Додаток побудований на платформі NodeJS з використанням технології REST API. Для відображення даних використовується front-end фреймворк VueJS.

В порівнянні з своїми промисловими конкурентами система має велику кількість переваг, а саме:

1) Низька вартість (біля 10$);

2) Маштабованість:

a) кількість модулів обмежена тільки Wi-Fi роутером;

b) функціонал можна сильно розширити користуючись вільними виводами мікроконтролерів, що дає змогу підключати нові периферійні модулі;

c) вивід нових даних, їх збір, додавання та обробку можна реалізувати на програмному рівні без втручання в апаратну частину;

3) Універсальність (один і той самий модуль можна використовувати для різних об’єктів господарювання додаючи чи змінюючи програмну частину);

Система володіє великою кількістю переваг, а її функціонал можна розширити без змін у апаратній частині, а тільки на стороні ПЗ. Також вагомою перевагою є те, що дані про працівників зберігаються в базах даних, і при потребі ці бази можна одразу імпортувати на нові підрозділи одного об'єкту господарювання, або зробити резервні копії цих баз.

Література

1. MQTT [Електронний ресурс] Режим доступу: http://mqtt.org/
2. Mosca [Електронний ресурс] Режим доступу: http://www.mosca.io/
3. Arduino [Електронний ресурс] Режим доступу: https://www.arduino.cc/
4. NodeMCU [Електронний ресурс] Режим доступу: http://nodemcu.com

Тєлишева Т.О., к.т.н., доцент
Курилко І.М., магістр
Національний технічний університет України «КПІ імені Ігоря Сікорського», Київ
Кафедра автоматизованих систем обробки інформації та управління, доцент

СЕРВІС З ПРИКЛАДНИМ ІНТЕРФЕЙСОМ ДЛЯ РОЗПІЗНАВАННЯ ОБЛИЧ

Задача розпізнавання обличчя полягає у локалізації обличчя та ідентифікації людини. Хоча комп’ютеру ще далеко до точності розпізнавання облич людей, зараз існує багато алгоритмів, що вирішують цю задачу. Серед

методів, що для цього використовуються можна виділити нейронні мережі, скриту модель Маркова, метод гнучкого порівняння на графах, статистичні моделі [2].

Наразі реалізовано багато інструментів для побудови моделей розпізнавання облич на різних мовах програмування і з використанням великого спектру бібліотек і фреймворків [1]. Найчастіше вони використовують моделі, побудовані на нейронних мережах з використанням машинного навчання. Серед таких інструментів можна виділити TensorFlow, Torch, Keras та інші. Більшість алгоритмів цього розділу інформатики потребують значних обчислювальних потужностей і детально продуманої архітектури для обслуговування програмних додатків.

Отже, проблемою у сучасній розробці програмних додатків для розпізнавання облич є складність розробки і підтримки архітектури додатків, що використовують алгоритми. Для вирішення цієї проблеми при розробці програмних додатків використовують сторонні API- сервіси, що займаються безпосередньо розпізнаванням облич, тим самим значно спрощуючи і здешевлюючи розробку продукту. Найвідомішими сервісами, що надають API для розпізнавання облич є Google Cloud Vision, Amazon Rekognition та Microsoft Face API. Використання подібних сервісів при розробці програмного додатку значно прискорює розробку, даючи змогу сконцентруватись на інтерфейсі, дизайні, UX та маркетингу, що додає продукту конкурентоспроможності на ринку.

Недоліком існуючих сервісів, що надають API для розпізнавання облич, є їхня закритість і отже неможливість розгорнути такий сервіс на своїх серверах, що не дає змогу гарантувати конфіденційність інформації. З цього випливає, що більшість цих сервісів є платними.

Тому тема даної роботи є актуальною.

Головна мета розробки - підвищити доступність використання технологій розпізнавання облич для розробників програмного забезпечення за рахунок створення масштабованого сервісу для надання функції розпізнавання облич.

Для досягнення поставленої мети мають бути вирішені задачі або реалізовані наступні функції:

- можливість масштабування сервісу, тобто створення більшої кількості серверів для витримування більшого навантаження;
- забезпечити конфіденційність інформації користувачів; реалізувати доступність використання ресурсу, якій створюється розробниками програмного забезпечення;
- забезпечити стороннім розробникам безкоштовний доступ до програмного коду за ідеологією open-source;
- можливість легко інтегруватися із засобами для розпізнання облич;
- надання стандартизованого REST API інтерфейсу, що є єдиною точкою входу для сервісу;
- збереження інформації користувача для її подальшого використання у класифікації;
- стандартизація REST API за специфікацією Open API/Swagger;

• розпізнання облич;

Оптимізація бізнес-процесів розробників програмного забезпечення, що використовують у своєму продукті технології розпізнавання облич, виконуються за допомогою проведення реінжинірингу бізнес процесів (див.рис.1).

Опис бізнес - процесів.

У бізнес-процесах розробника програмного забезпечення, що використовує технології розпізнавання облич акторами є Розробник, Система стороннього розробника та Система, яка створюється.

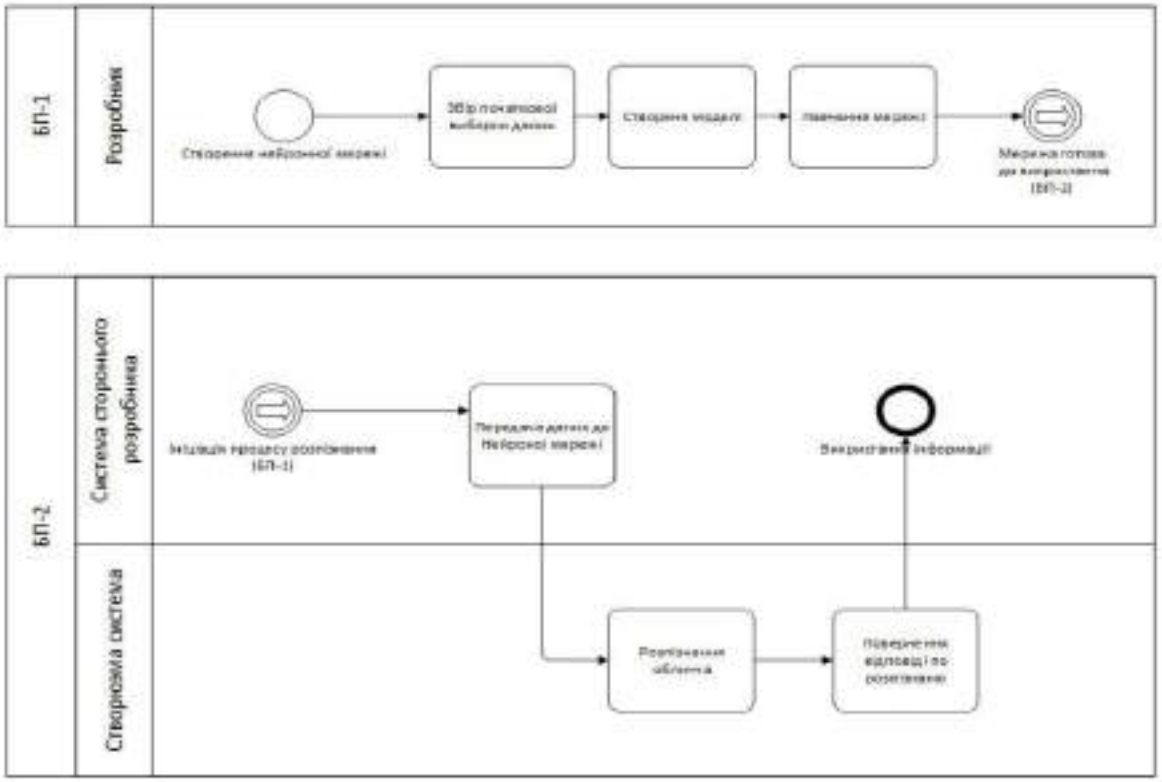


Рисунок 1 -Аналіз бізнес-процесів розробників програмного забезпечення

БП-1

Розробник розпочинає створення нейронної мережі, збирає дані для навчальної вибірки, сортує вибірку, розподіляючи її на навчальну вибірку і тестову вибірку, створює модель мережі, обирає алгоритми навчання, проводить навчання нейронної мережі і зберігає її. Мережа готова до використання.

БП-2

У створюваній системі сторонній розробник ініціює розпізнавання обличчя, надсилає дані збереженій моделі, модель розпізнає обличчя і надсилає результат створюваній системі розробника, яка використовує результат.

Пропозиції щодо реінжинірингу бізнес процесу.

Після аналізу процесу роботи системи стороннього розробника можна виявити деякі недоліки. Головним з них є необхідність самостійно створювати і навчати нейронну мережу, що вимагає додаткових ресурсів, як технічних так і

людських (кваліфікованих спеціалістів). Для усунення недоліків можна використати у бізнес - процесі стороннього розробника створювану систему в якості інструменту для розпізнавання облич.

Бізнес процес після реінжинірингу.

Суттєвих змін в бізнес процесі немає, але розпізнавання облич тепер виконується не самостійно створеною нейронною мережею, а створюваною системою, що дозволяє виключити етапи створення нейронної мережі, її навчання та збору навчальної вибірки (див.рис.2).

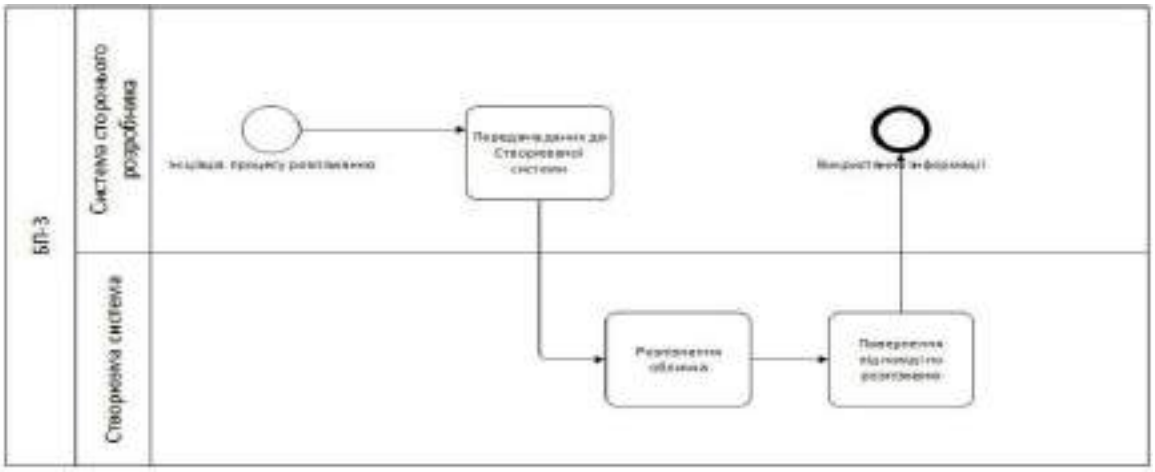


Рисунок 2 - Бізнес-процес розробників програмного забезпечення після реінжинірингу

БП-3

Система стороннього розробника ініціює розпізнавання обличчя та передає дані створюваній системи, яка проводить розпізнавання та надсилає результат системі стороннього розробника.

Як видно з діаграм бізнес-процесів новий бізнес-процес дозволяє сторонньому розробнику уникнути необхідності створювати та навчати власну нейронну мережу, збирати тестову вибірку для навчання, що дозволить ефективніше використати ресурси, які у старому бізнес-процесі були би витрачені на створення власної нейронної мережі.

Результати. Перевага системи, що розробляється в тому, що вона є самодостатньою і незалежною, її можна розгорнути локально для використання всередині компанії.

Тим самим ми отримуємо наступні переваги:

дані зберігаються локально і до них не мають доступ сторонні компанії;

можливість необмеженого користування системою, за неї немає необхідності платити, досить надати обчислювальну потужність;

можливість гнучко видавати права доступу до даних для внутрішніх користувачів компанії;

можливість гнучко масштабувати сервера в залежності від навантаження і використовувати рівно стільки обчислювальної потужності, скільки необхідно.

Література
1. F. Schroff, D. Kalenichenko, and J.Philbin. Facenet: A unified embedding for face recognition and clustering. In Proc. CVPR, 2015.
2. K. Q. Weinberger, J. Bützer, and L. K.Saul. Distance metric learning for large margin nearest neighbor classification. In NIPS. MIT Press, 2006. 2, 3

Ченька Мар'яна
студентка IV курсу
напряму «Міжнародна інформація»
Національного університету
«Львівська політехніка»

CAMBRIDGE ANALYTICA ТА ІНФОРМАЦІЙНА БЕЗПЕКА У СОЦІАЛЬНИХ МЕДІА

У статті проведено аналіз впливу Cambridge Analytica на інформаційну безпеку у соціальних мережах. Проведено дослідження, яке демонструє можливість викрадення персональних даних з метою використання у власних цілях, зокрема для маніпуляції цільовою аудиторією за допомогою таргетованої реклами. Cambridge Analytica використовувала персональні дані користувачів для того, щоб проводити рекламні кампанії, зокрема компанія була долучена до президентської кампанії Дональда Трампа. У статті описано принцип роботи API додатка, який збирав дані користувачів

Ключові слова: *інформаційна безпека, соціальні мережі, соціальні медіа, Facebook, Cambridge Analytica, персональні дані, інформаційні технології.*

Мета: дослідити діяльність компанії Cambridge Analytica та її вплив на інформаційну безпеку персональних даних у соціальних мережах.

Результати досліджень: визначено особливості діяльності компанії Cambridge Analytica і особливості технології збору персональних даних.

Нещодавно ЗМІ повнились гучними заголовками, пов'язаними із компанією Cambridge Analtica та Facebook і витоком даних. Коган зібрав 50 млн персональних даних, які формували профіль особи з інформацією про інтереси, релігійні, політичні погляди. Зібрати дані можна завдяки тестам, а також за допомогою цифрового сліду – лайки в мережі, геодані, пошукові запити тощо.

М. Косинські розробив систему, що складає психологічний портрет людини на основі опитувань, профілів у соціальних мережах. Тобто, Косинські отримав змогу «читати» особистість людини через аналіз активності особи в соціальних мережах. Дослідження проводились на основі даних, зібраних додатком у Facebook myPersonality. Опитування включало 100 запитань, які визначали характер людини. Респонденти дозволили додатку отримати доступ до своїх даних у профілі Facebook та інформацію про контакти. Це дозволило дослідникам будувати модель кореляції і схожості між користувачами. З цією моделлю дослідники створювали чітке уявлення про особистість користувача, використовуючи лише список контактів та інформацію про цифровий слід.[13]

Cambridge Analytica звернулась до Косинські з проханням використати дану систему, який відмовився. Основна мета дослідження – цифровий слід людини здатний замінити різноманітні тести. [18]. Згодом компанія скористалась послугами О. Когана, професора Кембріджського університету. У 2013 році Коган створив додаток тестів для особистості, який встановили близько 300 тис осіб. Він отримав доступ до мільйонів даних користувачів.[2]

Видання «The New York Times» провело розслідування у цій справі. Журналісти виявили, що О. Коган, за аналогом Косинські, налаштував модель збору даних. Він також використовував добровольців для проходження психологічного тесту. Крім того, учасникам цього експерименту платили гроші (приблизно 800 тис доларів). Ці тести збирали інформацію з профілів користувачів та їхніх контактів. Додаток This is your digital life отримав інформацію понад 50 млн користувачів. Саме ці дані дозволили проводити таргетування реклами з високою ефективністю.[13]

У 2014 році Facebook змінив політику щодо обмеження доступу до даних користувачів за допомогою додатків. Був проваджений новий інструмент, який вимагав погодження від користувача для отримання чи надсилання даних. Розробники Facebook заблокували додаток Когана, а компанія вимагала видалити всі дані, які були отримані незаконним чином. [2]

В супереч правилам Facebook, дані були передані третій стороні – Cambridge Analytica. Адміністрація мережі заявила, що кількість зібраних даних за допомогою додатка, може сягати 87 млн.[14] З 87 мільйонів користувачів понад 70 мільйонів людей перебувають у США. [12]

Крістофер Уайлі, колишній працівник Cambridge Analytica, стверджує, що компанії вдалося зібрати особисті дані мільйонів користувачів Facebook за допомогою API додатка This is your digital life [16]. Глобальна маніпуляція персональними даними перетворилася в реальність, і це вже більше, ніж попередження науковців, журналістів та юристів. Доступ величезної кількості користувачів в мережу дозволяє компаніям або зацікавленим особам все простіше отримувати і використовувати дані. Причому це змінює саме поняття конкуренції та ефективності, а клієнтам дає небувалі можливості.

О. Коган отримав доступ до даних користувачів, які вирішили пройти «тест». Люди свідомо надавали дані, а жодні системи не були пошкоджені [17]. Основна проблема соціальної мережі в тому, що Facebook занадто довіряє розробникам, які використовують особливості її програмного забезпечення.[10]

Facebook і Cambridge Analytica понесли економічні втрати. Вартість цінних паперів Facebook ще у березні знизилася на 7%.[3] Главу Cambridge Analytica, О. Нікса, відсторонили від посади після виходу на екран фільму-розслідування від телеканалу Channel 4.[7] В силу останніх подій, судових позовів Cambridge Analytica оголосила про закриття компанії. Цукерберга викликали до Європейського парламенту і в британську Палату громад для пояснень щодо витоку персональних даних. У США Федеральна комісія з торгівлі почала розслідування щодо Facebook.[4] Цукерберг приносив вибачення користувачам соціальної мережі. Однак це не сильно вплинуло на ситуацію. Користувачі запустили флешмоб #deletefacebook із закликом до

видалення облікового запису з соціальної мережі. У зв'язку з цим компанія прийняла ряд заходів, спрямованих на підвищення безпеки приватності даних. Соціальна мережа тепер попереджає всіх власників скомпрометованих акаунтів про те, якою саме персональною інформацією заволоділа Cambridge Analytica. [9]

На хвилі скандалу компанія Mozilla оголосила про запуск нового розширення для браузера Firefox. За допомогою нього користувачі можуть не турбуватися за збереження своїх даних. Розширення Facebook Container допомагає ізолювати персональні дані користувача після переходу на сторінку Facebook за посиланням з іншого сайту. Браузер відкриває соцмережу в спеціальній вкладці-контейнері, попередньо видаливши файли cookie. Mozilla переконує, що це ускладнить для Facebook збір даних для використання з метою показу таргетованої реклами та інших повідомлень.[6]

Тим не менше, вчені з Прінстона з'ясували, що існуються сторонні JavaScript-бібліотеки, які збирають інформацію про відвідувачів сайту через функцію аутентифікації «Увійти через Facebook». Більшість ресурсів навіть не підозрюють про те, що відбувається. Це засовується на сайтах, де можлива авторизація через Facebook. У процесі аутентифікації API соцмережі формує запит до її серверів, і ті повертають дані, до яких користувач дозволив доступ. Існує сторонній код JavaScript, який завантажується на сторінці авторизації, і може перехопити дані і виокремити інформацію про користувача. (рис.1) [15]

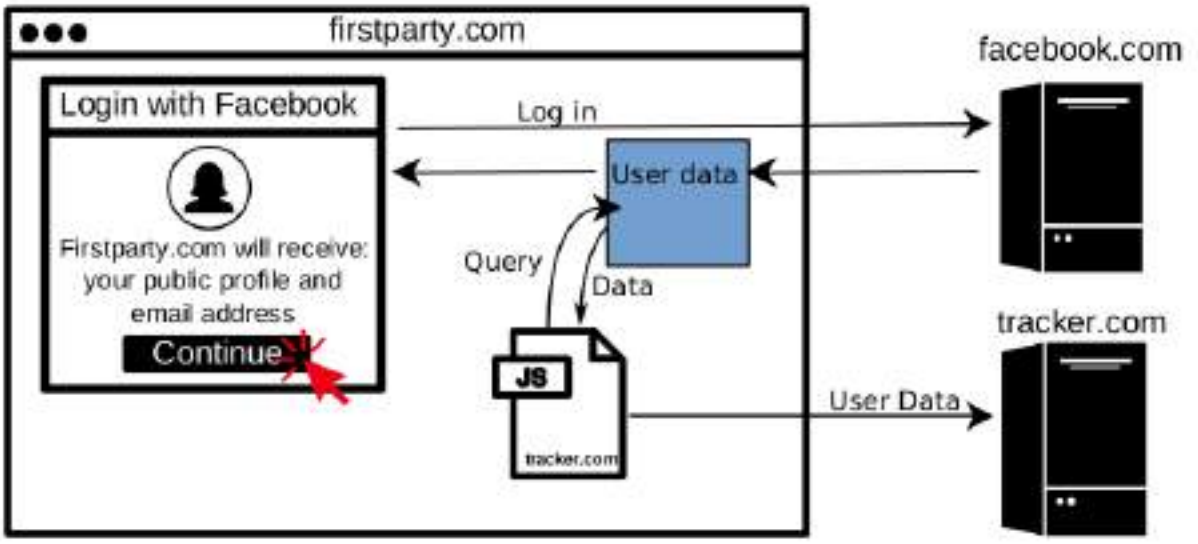


Рис. 1 Схема крадіжки персональних даних за допомогою стороннього коду JavaScrit

Дослідники вважають, що подібні витоки пов'язані не з помилками в авторизації через Facebook, а з відсутністю кордонів безпеки між ресурсами і сторонніми скриптами в Інтернеті.

Цікавим є те, що Cambridge Analytica не єдина компанія, яка займається, а точніше займалась, збором персональних даних. Видання CNBC виявило, що компанія CubeYou слідувала Cambridge Analytica і використовувала дані користувачів Facebook в рекламних цілях. Соціальна мережа закрила для неї доступ до персональної інформації людей і почала розслідування. CubeYou проводила опитування за допомогою яких дізнавалася дані про користувача.

Отримана інформація використовувалась для створення детальних профілів і продавалася маркетологам.Директор CubeYou повідомив, що опитування «You Are What You Like» попереджало про можливість передачі інформації третім особам. Він зазначив, що CubeYou не використовувала дані про друзів користувачів, як це робила Cambridge Analytica.[11]

Після гучного скандалу і падіння акцій компанії Facebook відмовився від партнерських відносин з брокерами даних, які допомагають рекламодавцям орієнтувати свою кампанію на конкретних користувачів. [8]. На сайті Facebook перераховані дев'ять компаній, з якими працювала компанія, включаючи Acxiom, Experian PLC, Oracle Data Cloud, TransUnion та WPP PLC.[5]

Загалом, основна цінність даних користувачів – можливість створювати більш ефективну таргетовну рекламу. Це рекламні оголошення, які спеціально налаштовані на певну аудиторію.Перш за все, визначається цільова аудиторія за допомогою різних параметрів (стать, вік, місце проживання, сфера діяльності, мова, хобі тощо). Згодом створюється оголошення, яке повинне привернути увагу користувачів. Особливістю цього типу реклами є те, що вона поширюєтьсяне на всіх користувачів соціальної мережі, а лише на обраних, які відповідають заданим параметрам. Така увага за допомогою вдало підібраного тексту та візуальної частини здатна не лише привернути увагу користувача, а й спонукати його до дій. Саме за таким принципо здійснювалась рекламна капанія Трампа у мережі Facebook.

"Важливість історії Cambridge Analytica, насправді, не в тому, що компанія допомогла Трампу в передвиборчій кампанії, - говорив Косинські в інтерв'ю Радіо Свобода в грудні 2016 року. - Це комерційна фірма, у них є технологія, вони хочуть заробляти гроші, тут все ясно. Важливим є те, що якщо раніше ви хотіли скласти чийсь психологічний профіль, ви повинні були попросити людину заповнити опитувальник, пройти тест - і людина розуміла, що саме зараз, в цей самий момент, хтось вимірює його психологічні характеристики. А тепер можна робити те ж саме, але людина не дізнається, що його особливості прямо зараз хтось оцінює і вимірює. Досить подивитися на цифровий слід: записи в соціальних мережах, лайки, історію перегляду сторінок в інтернеті, історію пошукових запитів ".[1]

Список використаної літератури та джерел

1. Сергій Добринін. «Мы не заметим, как мир захватит искусственный интеллект». Режим доступу: https://www.svoboda.org/a/28166040.html
2. Публікація Марка Цукерберга у Facebook. Режим доступу: https://www.facebook.com/zuck/posts/10104712037900071
3. Цукерберг: Facebook проаналізує всі додатки, які мають доступ до значної кількості даних. Режим доступу: https://www.radiosvoboda.org/a/news/29113921.html
4. Цукерберга викликають у британський парламент через скандал навколо Facebook, Режим доступу: https://bit.ly/2xtIazA

5. Acxiom shares tank after Facebook cuts ties with data brokers. Режим доступу: https://www.reuters.com/article/us-acxiom-stocks/acxiom-shares-tank-after-facebook-cuts-ties-with-data-brokers-idUSKBN1H520U
6. Being Open and Connected on Your Own Terms with our New Facebook Container Add-On. Режим доступу: https://blog.mozilla.org/blog/2018/03/27/facebook-container-add-on/
7. Cambridge Analytica: директора Нікса після його заяв журналістам відсторонили. Режим доступу: https://www.radiosvoboda.org/a/news/29111907.html
8. Facebook abandons Acxiom and other major data brokers over Cambridge Analytica affair. Режим доступу: https://www.v3.co.uk/v3-uk/news/3029387/facebook-abandons-acxiom-and-other-major-data-brokers-over-cambridge-analytica-affair
9. Facebook: Cambridge Analytica warning sent to users. Режим доступу: http://www.bbc.com/news/technology-43698733
10. Facebook security chief reportedly planning to leave company. Режим доступу: https://www.cnet.com/news/facebook-security-chief-reportedly-leaving-company/
11. Facebook suspends another data analytics firm after CNBC discovers it was using tactics like Cambridge Analytica. Режим доступу: https://www.cnbc.com/2018/04/08/cubeyou-cambridge-like-app-collected-data-on-millions-from-facebook.html
12. Facebook to notify users affected by Cambridge Analytica scandal/ Режим доступу: http://www.dw.com/en/facebook-to-notify-users-affected-by-cambridge-analytica-scandal/a-43302882
13. How Researchers Learned to Use Facebook ‘Likes’ to Sway Your Thinking. Режим доступу: - https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html
14. Mike Schroepfer. An Update on Our Plans to Restrict Data Access on Facebook. Режим доступу: https://newsroom.fb.com/news /2018/04/restricting-data-access/
15. No boundaries for Facebook data: third-party trackers abuse Facebook Login. Режим доступу: https://freedom-to-tinker.com/2018/04/18/no-boundaries-for-facebook-data-third-party-trackers-abuse-facebook-login/
16. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. Режим доступу: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
17. Suspending Cambridge Analytica and SCL Group From Facebook - Режим доступу: https://newsroom.fb.com/news/2018/03/ suspending-cambridge-analytica/
18. The Data That Turned the World Upside Down. Режим доступу: https://motherboard.vice.com/en_us/article/mg9vvn/how-our-likes-helped-trump-win

Черняк Б.Р.
ДВНЗ «Приазовський державний технічний університет», м. Маріуполь,
Кафедра інформатики, студент групи ВТ-17-М

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ДЛЯ ПІДТРИМКИ ДІЯЛЬНОСТІ НЕКОМЕРЦІЙНОГО ПІДПРИЄМСТВА

В умовах сучасної світової економіки важливим напрямом вдосконалення останньої виступає розвиток соціального підприємництва, яке надає можливість часткового й динамічного вирішення на місцевому рівні тих гострих соціальних проблем, які неспроможна вирішити держава, а також включення в економічну діяльність тих підприємств, які ставлять за мету не лише одержання прибутку, але й її спрямування на підтримку уразливих груп населення, створення нових робочих місць, пом'якшення та вирішення соціальних проблем країни.

Досить поширеним є розуміння соціального підприємства як підприємницької діяльності неприбуткових недержавних організацій (unprofitable private organization), які спрямовані передусім на реалізацію статутних цілей цих організацій. Сектор некомерційних організацій включає недержавні дослідницькі фонди, наукові та освітні установи, заклади охорони здоров’я і багато інших типів організацій. Всі вони, як і всі юридичні особи, якою би благородною не була мета їхнього існування, не можуть існувати самоплином, а отже потребують управління. Кожне підприємство є системою, має свій бюджет, який потребує планування та організації виконання і звітності.

Управління системою базується на інформації, яка реєструється, передається, зберігається, накопичується і обробляється. Для організації та реалізації цього інформаційного процесу необхідний персонал, здатний виконувати його процедури, а також відповідні засоби і методи обробки інформації. Все це в сукупності становить інформаційну систему.

У сучасному розумінні термін «інформаційні системи» (надалі ІС) має на увазі автоматизацію інформаційних процесів. Тому терміни «інформаційна система» і «автоматизована інформаційна система» часто використовуються як рівноправні.

ІС орієнтовані, переважно, на реалізацію управлінських рішень на базі широкого використання засобів обчислювальної техніки й економіко-математичного моделювання. Такі системи характеризуються також безпосередньою взаємодією з користувачами різних рангів, функціонуванням реального режиму часу отримання і використання інформації, можливістю задоволення інформаційного попиту споживачів.

Проте, при створенні сучасних ІС такі традиційні підходи вже не задовольняють дослідників. Цікавою видається інтерпретація ІС на основі виділення в них трьох так званих фільтрів: синтаксичного, семантичного і прагматичного.

Під синтаксичним фільтром розуміють засоби передачі та збереження даних, що не торкаються їх змістової обробки (реалізується лише первинна обробка, контроль, збереження і пошук). Такий фільтр може характеризувати

пропускну здатність інформаційної системи. Семантичний (змістовий) фільтр забезпечує розуміння змісту даних, які передаються, тобто в ньому відбувається змістова обробка. При цьому під семантичним шумом розуміють ті дані, в яких або відсутні елементи новизни, або вони «безглузді» для використання. В прагматичному фільтрі здійснюється оцінка міри корисності даних із позиції цілей користувача, визначається актуально корисна інформація для вирішення завдань управління. Відбувається також відтік непотрібних даних, які утворюють прагматичний шум (непотрібні знання). Отже, дані, що пройшли цей фільтр, становлять собою інформацію в тому вигляді, в якому вона потрібна для прийняття рішення.

У багатьох наукових роботах виділяють такі види інформаційних систем: інформаційно-пошукові, інформаційно-довідникові, інформаційно-консультативні. Основою для такої класифікації, як правило, служать комплекси використовуваних методів і засобів їх реалізації, технологічні процеси обробки даних, види і форми оброблюваної інформації, функціональна орієнтація системи.

Останнім часом набувають розвитку багатофункціональні інтегральні ІС, які призначені для роботи в будь-яких режимах, тобто об'єднують різні властивості й особливості різних систем. Найбільш розповсюджені програми - це 1С та MASTER:Бухгалтерія.

Отже, згідно з досвідом світової демократії, для здорового розвитку громадянського суспільства одною з необхідних умов є існування та розвиток некомерційних підприємств.

Управління підприємством передбачає наявність інформаційної системи, яка виконує функції накопичення, зберігання, передачі та обробки даних.

Вимоги до таких систем стрімко зростають. З'являються нові ІС, вдосконалюються вже існуючі.

Ефективність функціонування ІС визначає рівень успішності фільтрації даних, тобто перетворення їх на інформацію.

Для продуктивного розвитку діяльності певної організації необхідною умовою є підібрати ІС, що максимально задовольняє потребам цієї організації.

Література

1. Ігнатович, Н. Зарубіжний досвід розвитку соціального підприємництва/ Н. Ігнатович, В. Гура // Вісник КНУ ім. Тараса Шевченка. Економіка, 2014. – № 12 (165). – С. 22-25.
2. Охріменко В. М. Інформаційні системи і технології на підприємствах / В. М. Охріменко, Т. Б. Воронкова. – Харків: ХНАМГ, 2006. – 185 с.
3. Галушка З. Феномен соціального підприємництва: поняття та перспективи розвитку в Україні/ З. Галушка // Вісник КНУ ім. Тараса Шевченка. Економіка, 2013. – № 1 (148). – С. 15-17.
4. Герасим М.П. Необхідність інформаційних систем і технологій в управлінні підприємством / М.П. Герасим, Л.Я Сайко // Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку : [збірник наукових праць] – Львів : Видавництво Львівської політехніки, 2012. – С. 327-332.
5. Заєць І.В. Роль інформації в системі управління підприємством / І.В. Заєць // Вісник ЖДТУ. – 2010. – №2(52). – С. 97-98.

Шевелін Марія Сергіївна, студентка
Національний аерокосмічний університет ім. М.Є. Жуковського «ХАІ», м. Харків
Науковий керівник – Артьомова Аліна Вадимівна, доцент кафедри економіки та маркетингу

ПРОБЛЕМИ ПРОГНОЗУВАННЯ БАГАТОФАКТОРНИХ МОДЕЛЕЙ

Проблема багатофакторного прогнозування – надзвичайно складна і мало вивчена. Вона вимагає вирішення низки методологічних і теоретичних запитань (статистичного і динамічного прогнозу, вибору математичного апарату для опису зміни економічного явища за певний період часу). Багатофакторні моделі економічних явищ будуються за інформацією, що відноситься до різних періодів. Серед типів інформації можна виділити просторову, яка відображає вплив попередніх періодів часу. Вона впливає на формування інформації, яка характеризуватиме явища і в майбутньому. У цьому полягає динамічний характер просторової інформації. При її використанні для побудови рівнянь регресії важко з'ясувати зміну впливів чинників-аргументів в часі та врахувати їх запізнювання. У цьому полягає статичність просторової інформації.

Використання просторової інформації та інформації, що характеризує динаміку явища, дозволить побудувати моделі, придатні для практичного використання. При побудові подібних моделей виникають дві математичні проблеми – автокореляція і мультиколінеарність між факторами, що приводить до падіння точності оцінювання та високої чутливості оцінок коефіцієнтів до особливостей вибіркових даних. Для вирішення цієї проблеми необхідно виділити з багаточисельного набору діагностичних змінних такий набір, який має найбільшу вагу для прогнозування. На основі розрахованих коефіцієнтів кореляції необхідно провести розбиття множини ознак на підмножини з врахуванням основних властивостей: сильна кореляція ознак усередині кожної групи; некорельованість або слабка кореляція між ознаками, що входять до різних груп. Обираючи по одному елементу, можна отримати набір ознак з цінними властивостями для прогнозування. Далі здійснюється побудова моделі.

Якість прогнозу характеризують такі поширені в прогностичній літературі терміни, як точність і надійність. Проте зміст цих термінів часто тлумачать досить неоднозначно. Це пояснюється тим, що нині не знайдено ефективного підходу до оцінювання якості прогнозу, окрім його практичного підтвердження. Про точність прогнозу прийнято судити за розміром помилки прогнозу — різниці між прогнозним і фактичним значенням показника. Такий підхід можливий, якщо дослідник має інформацію стосовно справжніх значень часового ряду, який він оцінював під час розроблення прогнозів.

Серед сучасних дослідників немає єдиної думки щодо існування найкращого методу прогнозування. Досвід доводить, що кожен метод призводить до різних результатів. Отже, як правило, виходить кілька відмінних прогнозів одного економічного показника. Будь-який прогноз, відкинутий через його неоптимальність, майже завжди містить певну корисну незалежну

інформацію. Об’єднання незалежно одержаних прогнозів залучає обидва види додаткової інформації, і якщо припустити, що кожна з моделей описує лише один бік динаміки заданого процесу, то використання кількох моделей уможливить точніший і повніший опис і прогнозування динаміки.

Таким чином, при прогнозуванні багатофакторних моделей виникає достатня кількість проблем, пов'язаних з вихідною інформацією, способами і методами проведення самого прогнозу. Запропоновані підходи дозволяють отримувати комплексні моделі прогнозування динаміки економічних явищ.

Література

1. Березька К. М. Економетрія: основи теорії та комп’ютерний практикум / К. М. Березька. – Тернопіль : Тайп, 2007. – 137 с.
2. Іващук О. Т. Економетричні методи та моделі : навч. посібник / О. Т. Іващук. – Тернопіль : ТАНГ Економічна думка, 2002. – 348 с.
3. Лещинський О. Л. Економетрія : навчальний посібник / О. Л. Лещинський, В. В. Рязанцева, О. О. Юнькова. – К. : МАУП, 2003. – 208 с.
4. Науменко В., Панасюк Б. Впровадження методів прогнозування і планування в умовах ринкової економіки. — К.: Глобус, 1995.

Секція: Технічні науки

Божко К.М.
кандидат технічних наук,
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
м.Київ, Україна

ТЕЛЕВІЗІЙНІ ЗАСОБИ В НЕРУЙНІВНОМУ КОНТРОЛІ ЕЛЕКТРОЛЮМІНІСЦЕНТНИХ МІКРОДЕФЕКТІВ СОНЯЧНИХ ЕЛЕМЕНТІВ

Неруйнівний контроль фотоелектричних сонячних елементів (ФЕСЕ) і батарей посідає чільне місце в технології їх виготовлення і може бути впровадженим і при їх експлуатації. Наявність дефектів знижує експлуатаційні параметри сонячних батарей та призводить до їх передчасної деградації. Нами доведено в лабораторних умовах, що телевізійна інформаційно-вимірювальна система є ефективним засобом контролю електролюмінісцентних мікродефектів (Рис.1) та вимірювання їх геометричних і світлових параметрів. Дослідженню цих мікродефектів в Україні надано початок у роботі [1].

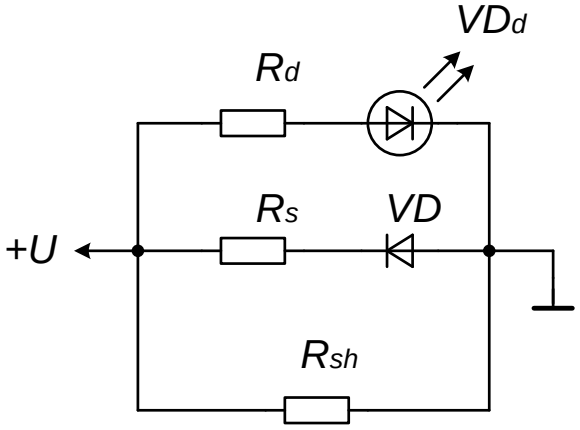


Рисунок 1 – Еквівалентна схема ФЕСЕ в режимі темнового струму за наявності електролюмінісцентного мікродефекту у вигляді світлодіоду: +U – зворотна напруга; VD – фотодіод; Rs – послідовний опір; Rsh – шунтовий опір; Rd – послідовний опір зони дефекту; VDd – дефект (паразитний світлодіод)

На схемі (Рис. 1) основний діод ФЕСЕ включено зворотно, а паразитний світлодіод, що символізує дефект – прямо. Оскільки область дефекту обмежена радіусом r = 10 мкм, то послідовний до світлодіоду VDd резистор Rd значно обмежить його струм і наявність дефекту призведе до локального нагрівання осередку дефекту на 5-20 ºС при протіканні темнового зворотного струму ФЕСЕ.

Телевізійний метод доповнено осцилографічними вимірюваннями сигналу від фотоелектричного підсилювача. Надано еквівалентну схему дефектного елементу та розраховано на її основі потужність та світлову віддачу

мікродефекту. Отримані результати можуть бути використані при виробництві та експлуатації фотоелектричних сонячних батарей.

Література
1. Попов В.М. Локальные свойства электрически активных дефектов в солнечных батареях на основе кремния [Текст] /В.М. Попов, А.С. Клименко, А.П. Поканевич и др. //ТКЭА, №4. – 2010. С. 43 – 48.

Бреус Д.М., студент IV курсу
НТУУ «КПІ» ім. Ігоря Сікорського, м.Київ
Кафедра акустики та акустоелектроніки, студент

РОЗРАХУНОК ДЛЯ ДОСЛІДЖЕННЯ ПРИНЦИПУ ДІЇ УЛЬТРАЗВУКОВОГО ДАТЧИКУ ДЛЯ ЕЛЕКТРОННОЇ СИСТЕМИ ВИЯВЛЕННЯ ПЕРЕШКОД

I.Вступ. Одним з головних завдань у мобільної рухомої робототехніки є проблема виявлення перешкод, як нерухомих, так і рухомих. Рішення такої задачі відкриває шляхи до розробки систем маршрутизації роботів. Як правило, для пересування по відомому маршруту використовуються системи глобального позиціонування. Однак такий спосіб не завжди достатньо надійний, оскільки має значну похибку по відношенню до розмірів самого робота, а в закритих приміщеннях і зовсім може не працювати. Для уточнення положення робота щодо інших об'єктів використовуються в основному системи технічного зору в оптичному діапазоні на основі стандартних відеокамер і відеокамер, що працюють в інфрачервоній частині спектра [1, 2]. Системи технічного зору дозволяють отримати більше інформації про оточуючі об'єкти, але в певних умовах цілком достатньо знати лише про присутність того чи іншого предмета на шляху руху робота. У таких ситуаціях способом вирішення проблеми відносного позиціонування є використання датчиків різної фізичної природи. Дані системи можуть бути застосовані як у рамках конструкцій сучасних роботів так і для допомозі руху людини, наприклад, не зрячої, система подаватиме звуковий сигнал, у разі виникнення на шляху перешкоди.

Актуальність дослідження.

На сьогоднішній день, питання впровадження робототехніки знаходить своє застосування у сфері послуг. По всьому світу сервісні роботи стали з'являтися в музеях, аеропортах, магазинах, лікарнях та інших в установах, де потрібні операції обслуговування. Такими операціями є переміщення предметів: товарів, ліків, тощо, патрулювання приміщення, рух з метою залучення уваги, надання інформаційних ресурсів, прибирання приміщень і т. д. В сегменті

роботів для населення будуть все більш популярними машини, які надають безпосередню підтримку людині. Робот дозволяє не тільки дистанційно переміщатися в просторі, але і взаємодіяти з об'єктами.

Існуючі сервісні роботи функціонують тільки за допомогою телекерування, при цьому даний режим мало автоматизований. Датчики на борту робота, наприклад, інфрачервоні та ультразвукові далекоміри, забезпечують безпеку руху в статичному середовищі через заборону наближення до перешкод при телеуправлінні.

Тому на сьогодні, актуальним питанням постає розробка електронної системи виявлення перешкод, що й посприяло при виборі теми дипломного проекту.

II. Основна частина

Розрахунок для дослідження принципу дії ультразвукового датчику для електронної системи виявлення перешкод.

В основі електронної системи виявлення перешкод, лежить ультразвуковий датчик, принцип дії якого наведено на рис. 2.1.

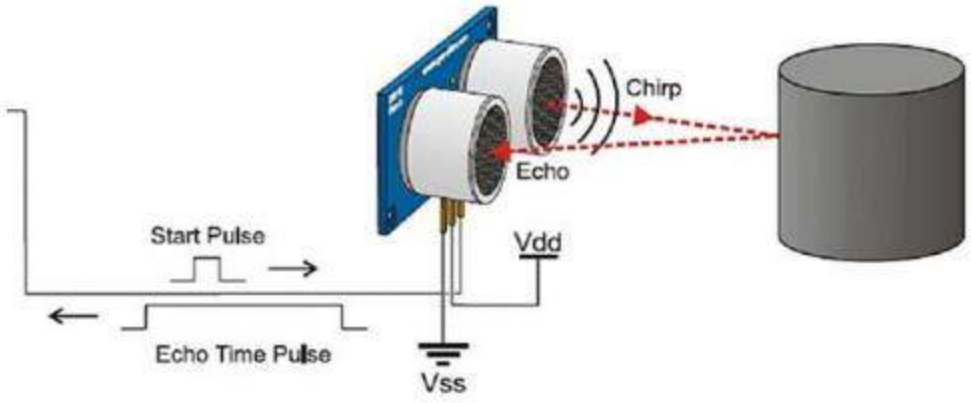


Рисунок 2.1 – Принцип дії ультразвукового датчику

В основі фізико-математичної моделі лежить наступне упередження: круглий перетворювач з площею

$$S_0 = \pi d^2 / 4 \qquad (2.1)$$

розбитий на елементарні випромінювачі площею

$$S = \lambda^2 / 4, \qquad (2.2)$$

кількість яких дорівнює

$$N = \pi d^2 / \lambda^2 = \pi n. \quad (2.3)$$

Кожен такий випромінювач має кругову діаграму спрямованості

$$\Phi(\varphi) = \cos\varphi. \quad (2.4)$$

Тому випромінювання імпульсів і прийом сигналів описані як щільності ймовірностей подій, що складаються в спільному випромінюванні-прийомі сигналів від πn незалежних джерел в різних напрямках. Розподіл цих щільності ймовірності інтерпретовані як сигнали перетворювача в режимі випромінювання-прийому:

$$\Phi^2(\varphi) = (\cos\varphi)^{2\pi n} = (1 + tg^2\varphi)^{-\pi n} = (1 + a^2 / r^2)^{-\pi n} = (1 + nS / \pi nr)^{-\pi n} \approx exp(-nS / r^2) = exp(- = y^2 / x^2) = exp(-v^2 / u^2). \quad (2.5)$$

За умови, що $\pi n \geq 10^2$, помилка заміни функцій не більше $0{,}1\%$.

Ультразвуковий датчик бере участь в:

– розпізнаванні місць і об'єктів;

– визначенні вільного простору і планування в ньому руху для того, щоб уникнути зіткнень з перешкодами;

– створення загального уявлення про навколишнє середовище.

Вимірювання, вироблені датчиком, залежать і від положення рухомого об’єкта $\mathbf{x}$ і від стану навколишнього його світу $\mathbf{y}$:

$$z_0 = z_0(x, y) \quad (2.6)$$

Описати стан зовнішнього світу можна, наприклад, за допомогою орієнтирів.

Стан може бути або невизначеним, або повністю відомим.

Розподіл моделювання ультразвукового датчика

Усі вимірювання які виробляють датчики, є невизначеними. Реальні датчики завжди видають деякий розкид значень, тобто вимірюють з певною точністю. У результатах вимірювань, зробленими тим чи іншим датчиком завжди присутня деяка похибка [12].

На сьогодні, можна охарактеризувати датчик, побудувавши його математичну модель. Зрозумівши невизначеність, яка присутня у вироблених сенсором вимірах, можна побудувати вірогідну модель вимірювань. Така

модель буде представляти із себе розподіл ймовірностей (функцію правдоподібності) виду:

$$p(z_0|x,y) \qquad (2.7)$$

Цей розподіл має вигляд колоколоподібної кривої (вид гауссіана).

Функція правдоподібності показує, наскільки ймовірним є еталонне значення $\mathbf{x}, \mathbf{y}$ при отриманні значення $\mathbf{z}_0$. Використовуючи функцію правдоподібності можна оцінити невідомий параметр при відомих результатах (коли використовується поняття ймовірність, навпаки використовуючи значення параметра можна передбачити результат) [13].

Функція правдоподібності повністю описує роботу датчика:

$$p(z|u) \qquad (2.8)$$

є функцією і змінних вимірювання z і еталона v і може бути побудована у вигляді ймовірнісної поверхні.

Імовірнісна модель електронної системи виявлення перешкод наведена на рис. 2.2

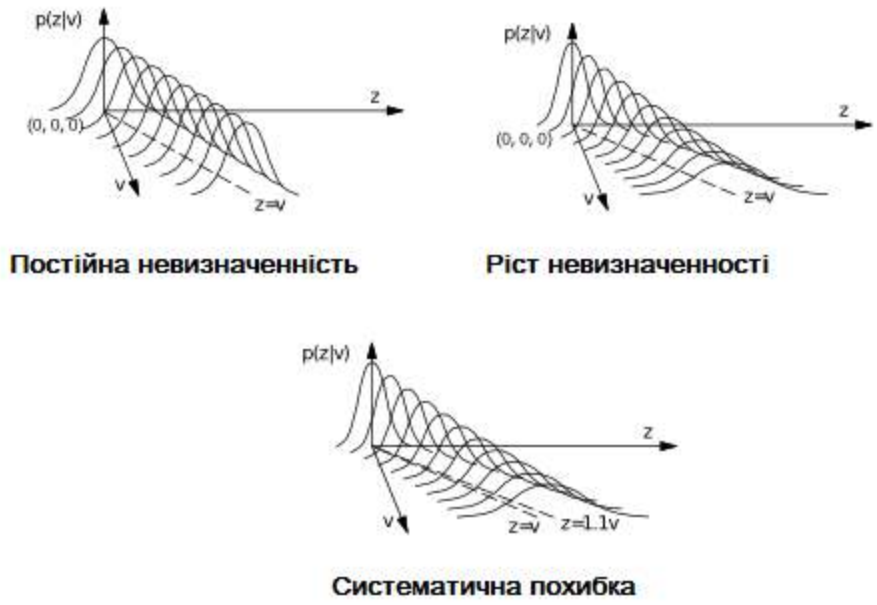


Рисунок 2.2 – Імовірнісна модель електронної системи виявлення перешкод

Чим більш похилою є функція правдоподібності, тим більше невизначеності вона містить. Тому, чим яскравіше виражені «пікові» вимірювання, тим менше невизначеності система містить в своїх даних.

Функція правдоподібності для ультразвукового датчика говорить нам, наскільки ймовірним є вимірювання z , отримане датчиком, з огляду на те, що справжнє очікуване значення m .

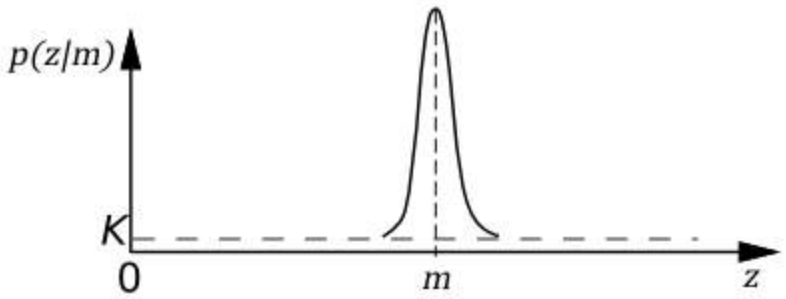


Рисунок 2.3 – Стійка модель ультразвукового датчика [14]

$$p(z|m) \propto e^{-(z-m)^2/2\sigma_g^2} + K \qquad (2.9)$$

Цей розподіл має форму вузької кривої Гаусса навколо очікуваного значення з деяким постійним рівнем K, який відображає фіксований відсоток «сміттєвих вимірювань».

Висновок: В результаті даного дослідження, ми розрахували та дослідили принцип дії ультразвукового датчику для електронної системи виявлення перешкод.

Література:

1. Кий К. И., Серединский М. В.. Система технического зрения робота «Амур» для движения на ориентиры // Труды международной научно-технической конференции «Экстремальная робототехника». – СПб: Изд-во «Политезника-сервис». – 416 с. Resources and Technology 10 (1): 1-10. – 2013 ISSN 2307-0048 http://rt.petrsu.ru 126

2. Александров В. А., Меркурьев И. В. Динамический оптический дальномер, применяемый для навигации мобильного робота. – ЦНИИ «Электроприбор»: Гироскопия и навигация, № 2. – 2006. – стр. 94.

Грудз В.Я.
доктор технічних наук, професор
Івано-Франківський національний технічний університет нафти і газу,
Івано-Франківськ
Кафедра спорудження та ремонту газонафтопроводів і газонафтосховищ, завідувач кафедри

Марущенко В.В.
АТ «Укргазвидобування», Київ
Департамент наземної інфраструктури, начальник

Братах М.І.
кандидат технічних наук, старший науковий співробітник
Український науково-дослідний інститут природних газів, Київ
АТ «Укргазвидобування», Київ
відділ транспортування газу, завідувач відділу

Савчук М.Т.
АТ «Укргазвидобування», Київ
Сектор промислових трубопроводів та електрохімічного захисту
Департамент наземної інфраструктури, начальник

Філіпчук О.О.
АТ «Укргазвидобування», Київ
Відділ збору, підготовки та транспортування вуглеводнів
Департамент наземної інфраструктури, менеджер проектів

ПИТАННЯ ЕКСПЛУАТАЦІЇ ГАЗОВИДОБУВНОЇ СИСТЕМИ НА ЗАВЕРШАЛЬНІЙ СТАДІЇ ЕКСПЛУАТАЦІЇ РОДОВИЩ

Безаварійна експлуатація газових свердловин є надзвичайно важливим питанням, яке постає перед інженерами у процесі видобування газу. Це зумовлено, зокрема, переходом більшості родовищ на завершальну стадію розробки. Тому саме вибір оптимального режиму експлуатації свердловин та системи збору, підготовки та транспортування газопромислової продукції може забезпечити стабільну роботу системи «пласт-свердловина-шлейф-установка підготовки газу». Найбільш значним фактором, який ускладнює експлуатацію свердловини в таких умовах, є скупчення рідини на вибої свердловини і в понижених ділянках трубопроводів. [1]

Ефективність роботи систем збору та транспортування газу з родовищ газовидобувних Компаній залежить від гідравлічного стану сукупних ділянок лінійної частини газопроводів. Тому необхідно проводити періодичний моніторинг гідравлічного стану з метою оцінки фактичних гідравлічних характеристик (визначення перепадів тиску, фактичних коефіцієнтів гідравлічного опору ділянки та гідравлічної ефективності, орієнтовний об`єм

забруднень), оскільки відхилення від номінального режиму роботи вказуватиме на утворення двофазних течій, що значно знижує ефективність та надійність експлуатації системи.

Процеси випадіння та формування рідинних скупчень в газозбірних мережах носять більш специфічних характер, оскільки такі забруднення є більш рухомими, ніж в нафтопроводах на початковому етапі розробки, коли основним забрудником буде газовий конденсат, і більш стійкими до локалізації на завершальному етапі розробки родовищ, коли формуватимуться виключно із водних фракцій лише із слідами конденсату. В будь-яких випадках і українські, і закордонні спеціалісти рекомендують проводити комплексне обстеження ділянок трубопроводів, де можливе накопичення рідини [2].

В роботі приведено результати дослідження стану системи збору, підготовки та транспортування газу Котелевської групи родовищ. Для дослідження динаміки коефіцієнту гідравлічної ефективності міжпромислових газопроводів було проведено вимірювання фактичних технологічних параметрів на окремих ділянках. З метою оцінки впливу зміни температури навколишнього середовища на показник коефіцієнту гідравлічної ефективності, вимірювання проводилось в зимовий та літній періоди експлуатації.

Проведене авторами дослідження ґрунтувалось на вимірюванні технологічних параметрів в контрольних точках наступних ділянок міжпромислових газопроводів: Високонапірні: 1 – «УКПГ Березівка – кр. № 6 т.п. УКПГ Котельва»; 2 – «кр. № 6 т.п. УКПГ Котельва – т.п. УКПГ Опішня»; 3 – «УКПГ Котельва – кран № 6 т.п. до газопроводу УКПГ Березівка – т.п. УКПГ Опішня»; 4 – «УКПГ Опішня – ГС Солоха». Низьконапірні: 5 – «УКПГ Опішня – УКПГ Котельва»; 6 – «УКПГ Березівка – УКПГ Котельва» [3].

На підставі аналізу результатів проведених досліджень в різні періоди експлуатації, слід відмітити, що в зимовий період (при понижених температурах навколишнього середовища) процес сепарації газу на установках попередньої підготовки газу здійснюється якісніше. Отже, газ, який поступає до трубопроводу, в зимовий період експлуатації є менш вологомістким і загальна кількість сконденсованої рідинної фази є меншою в порівнянні із літнім періодом експлуатації. Дана умова знайшла експериментальне підтвердження проведеними дослідженнями в даній роботі, оскільки коефіцієнт гідравлічної ефективності на ділянках даного газозбірного вузла та орієнтовні об’єми забруднень в порожнинні трубопроводів значно менші порівняно із літнім періодом роботи.

Відповідне зростання температури сепарації газу позначається на падінні коефіцієнтів гідравлічної ефективності і суттєвому зростанні обсягів забруднень в літній період. В послідуючому газ поступає в газопроводи, де відбувається зниження його температури, в результаті чого виникають сприятливі термодинамічні умови до фазових перетворень, результатом яких є накопичення рідинних забруднень у порожнинні трубопроводів. Дані забруднення накопичуються у понижених ділянках газопроводу у вигляді пробок, що може перерозподілятись при русі по висхідним ділянкам профілю траси трубопроводів, що призводить до створення надлишкових перепадів, а з

часом і повного перекриття перерізу трубопроводу в наступній за рухом газу природній пастці рідини. При накопиченні забруднень робочий тиск в газопроводі починає пульсувати із раптовим падінням нижче тиску конденсації або зростанням вище тиску випаровування рідинної фази, що за таких переходитиме у газоподібну фазу і навпаки. Враховуючи безперервні надходження рідинної фази до порожнини трубопроводів, накопичення критичного об'єму призводить до перерозподілу рідинної фази, результатом чого є залпові викиди до технологічного обладнання на виході із трубопроводу [4].

Такий сукупний вплив механічного надходження рідини в порожнину трубопроводів і фазових перетворень формує різноманітні структури руху газорідинної суміші по довжині трубопроводу залежно від швидкісного режиму роботи. Чітко відмічається, що на ділянках 1,6 в зимовий період експлуатації швидкість газового потоку сприяє накопиченню капель рідини в нижній частині газопроводу, «висхідні ділянки». Тоді як на ділянках 2,3,4,5, в зимовий період експлуатації, швидкість газового потоку сприяє тому, що більша частина рідини збирається в пониженій ділянці газопроводу із хвилеподібним розподілом фаз та наступним переміщенням до «висхідної ділянки» у вигляді пробки під час «залпового викиду». Ефективність системи в літній період експлуатації характеризується дещо іншими значеннями, оскільки на всіх ділянках системи швидкість газового потоку сприяє проходженню вищеприведеного процесу. Слід зазначити, що ефективність роботи газопроводів, в зимовий та літній період експлуатації коливається в межах 49 %, а швидкість газового потоку притаманна розшарованим структурам газорідинного потоку (нижче 3,5 м/с) або пробковим (до 8,2 м/с) для даного випадку, але не в змозі створити кільцеву структуру течії на жодній із різноорієнтованих в просторі ділянках [3].

Такий підхід до оцінки впливу швидкісного режиму роботи до формування структурних форм руху на ділянках системи дозволив розробити комплекс заходів по збільшенню завантаженню системи і зростанню лінійних швидкостей газу.

Наступним кроком авторами було проведено моделювання процесу пониження тисків на вході в ДКС Солоха. Симуляція процесу руху рідини і її перерозподілу між ділянками системи свідчить про можливість зменшення обсягу забруднень при зміні завантаження і робочого тиску в 3,5 рази, що фактично вдвічі зменшує перепади тиску на ділянках призводячи до зростання обсягів видобутку газу в середньому додатково на 5-20% залежно від поточного робочого тиску свердловин (див. рисунки 1,2).

В результаті даних досліджень авторами було експериментально підтверджено залежність впливу температури навколишнього середовища на якість підготовки газу, а також вплив швидкості газового потоку на утворення рідинних забруднень в порожнинні газопроводу.

Основним проявом економічної ефективності для газопроводів системи збору і міжпромислового транспортування газу родовищ, які знаходяться на завершальній стадії експлуатації, є зменшення величин надлишкових (або надмірних) втрат тиску, що виникають в цьому процесі. Нівелювання або

фактично повне усунення їх впливу досягається завдяки реалізації трьох основних заходів:

- очистка внутрішньої порожнини газопроводів на забруднених ділянках, що відбивається у зниженні робочого тиску на виході з УКПГ, зменшенні витрат паливного газу або збільшенні температурного перепаду на УКПГ, що подають газ до системи міжпромислових газопроводів;

- перепланування (зміна напрямку газових потоків) по системі міжпромислового збору і транспорту продукції, що характеризується зміною завантаження окремих ділянок;

- облаштування додаткових ниток газопроводів, нових газопроводів, що збільшує пропускну здатність еквівалентної системи і зменшує втрати тиску в процесі збору і транспортування газу між об'єктами газопромислового підприємства.

В результаті проведених робіт змодельовано процес самоочищення досліджуваних ділянок газопроводів, режими роботи яких суттєво впливають на розподіл тиску на УКПГ і роботу низьконапірних і середньонапірних свердловин за рахунок перепланування потоків газу в системі із обґрунтуванням їх доцільності в техніко-економічних розрахунках. Фактично, зміна завантаження системи і зниження робочого тиску в ній призведе до збільшення лінійних швидкостей, достатніх для переходу структурної форми потоку з розшарованої (хвильової) до пробкової і кільцевої, а отже надання руху забрудненням і самоочистці системи.

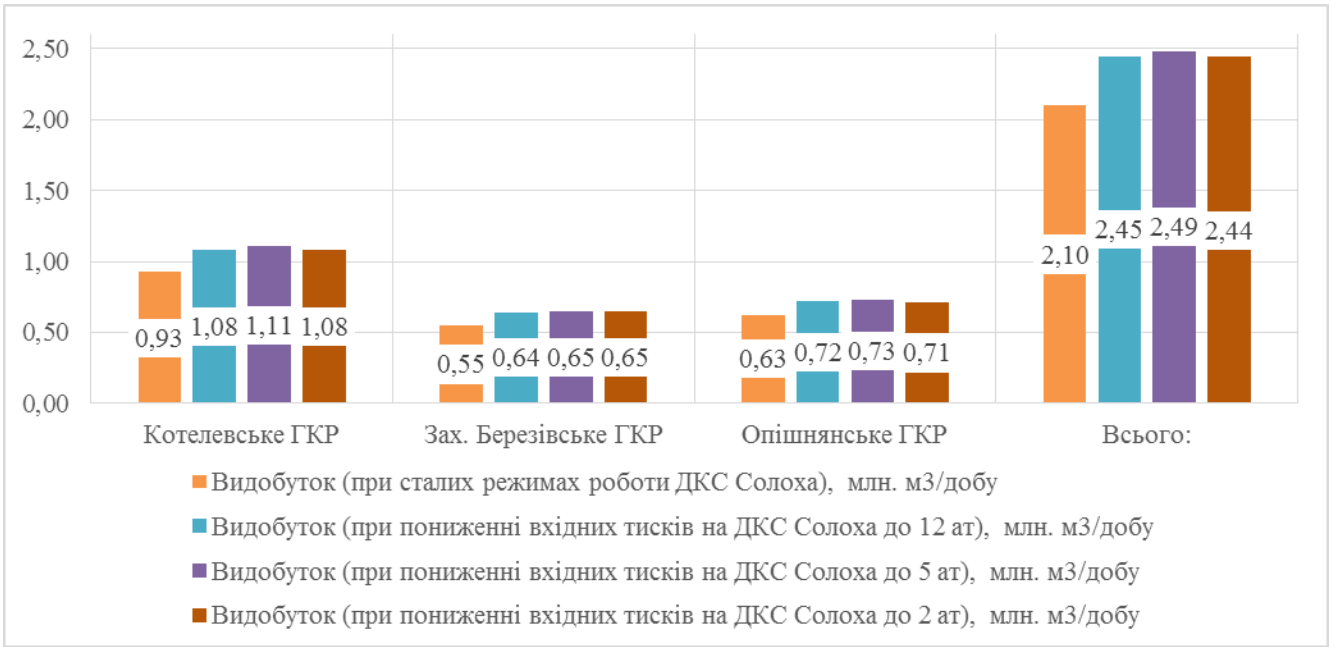


Рисунок 1 Результати симуляції розподілу робочого тиску на обсяги видобутку при зниження робочого тиску з 25 до 12, 5, 2 ат на вході в Солохівську ДКС відповідно (при поточному забрудені системи)

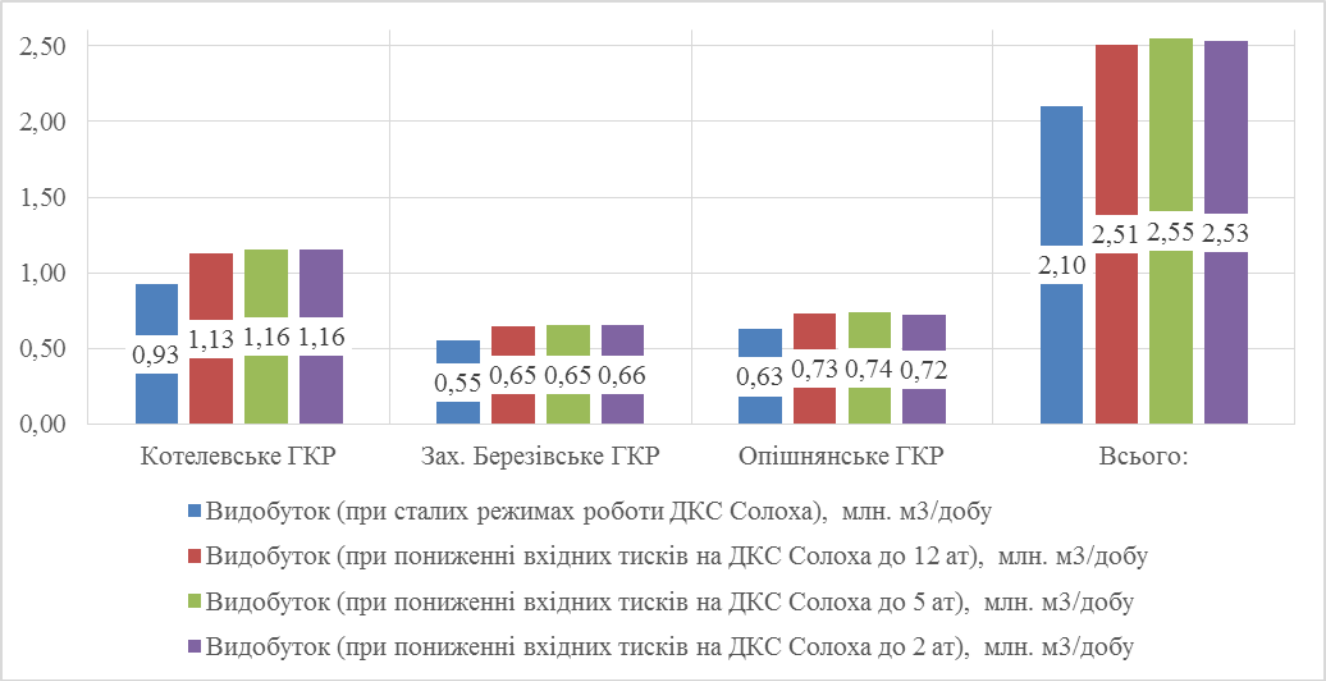


Рисунок 2 – Результати симуляції розподілу робочого тиску на обсяги видобутку при зниження робочого тиску з 25 до 12, 5, 2 ат на вході в Солохівську ДКС відповідно (при прогнозному самоочищенні системи)

Список використаних джерел

1. Кондрат О.Р. Підвищення ефективності експлуатації свердловин та роботи системи збору і підготовки свердловинної продукції зі значним вмістом рідини. // О.Р. Кондрат, Н.М. Гедзик. Розвідка та розробка нафтових і газових родовищ, № 4 (45), 2012 р.

2. Introduction to Pigging & a Case Study on Pigging of an Onshore Crude Oil Trunkline. Available from: ttps://www.researchgate.net/publication/307583466_Introduction_to_Pigging_a_Case_Study_on_Pigging_of_an_Onshore_Crude_Oil_Trunkline accessed Mar 16, 2018.

3. Шимановський Р.В. Звіт про науково-дослідну роботу «Аналіз гідравлічної ефективності роботи промислових газоконденсатопроводів, розроблення рекомендацій по покращенню їх роботи» // Р.В. Шимановський, С.М. Стецюк, М.І. Братах, О.І. Шапар - м. Харків, 2017 р. 218 стр.

4. Скоробагач М.А. Проблемы эксплуатации системы сбора газа на месторождении Медвежье / Научно-технологический журнал «Технологии нефти и газа» № 6.- Москва, 2011 г. – С. 42 – 47.

Запорожець Ю.А.
Національний технічний університет України «КПІ імені Ігоря Сікорського», м. Київ
Кафедра кібернетики хіміко-технологічних процесів, асистент

ВПЛИВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА НА ПЕРЕНЕСЕННЯ ЗАБРУДНЮЮЧИХ РЕЧОВИН В ПРИРОДНОМУ ДИСПЕРСНОМУ СЕРЕДОВИЩІ

Перенесення розчинних речовин в природному середовищі залежить від різних факторів навколишнього середовища та від внутрішніх процесів. Ступінь впливу процесів може відрізнятися для різних дисперсних середовищ, забруднюючих речовин, розглянутих моментів часу і простору.

На перенесення і сорбцію забруднюючих речовин в природних дисперсних середовищах істотно впливає динаміка розподілу вологи в середовищі. У свою чергу ця динаміка визначається інтенсивністю дощових опадів, коливаннями температури і відносної вологості повітря на поверхні ґрунту, топ то кліматичними факторами [1].

Інтенсивність дощових опадів є головним фактором у формуванні в середовищі потоку вологи, яким переносяться забруднюючі речовини [1]. Після випадання дощових опадів спочатку вода швидко поглинається середовищем, а потім потік вологи стабілізується. Початкову стадія швидкого проникнення води в ненасичену вологу середу називають інфільтрацією. Далі в міру насичення всього простору дисперсного середовища водою потік вологи стабілізується. Настає стадія руху води в насиченому дисперсному середовищі - фільтрація. Таким чином, швидкість потоку вологи, яким переносяться забруднюючі речовини, безпосередньо залежить від інтенсивності дощових опадів. Чим більше кількість опадів, що випали в одиницю часу, тим більше буде швидкість потоку вологи в середовищі і, отже, швидше буде відбуватися міграція забруднюючих речовин в глиб середовища.

Також на перенесення забруднюючих речовин в природному дисперсному середовищі, є температура і відносна вологість повітря на поверхні середовища [2]. Ці два фактори визначають інтенсивність випаровування вологи і підтік вологи до поверхні. Випаровування вологи з поверхні впливає на насиченість середовища водою, зміна якої, в свою чергу, впливає на сорбцію і перенесення забруднюючих речовин. Крім того, якщо насиченість середовища вологою стає менше максимальної гігроскопічності, то вода в ній буде знаходитися в зв'язаному стані, при цьому рух вологи буде відбуватися тільки у вигляді водяної пари, який не переносить водорозчинні забруднюючі речовини.

Як відомо, рух ґрунтової вологи, що переносить розчинні забруднюючі речовини, здійснюється під дією капілярно-сорбційного потенціалу [3]. У свою чергу капілярно-сорбційний потенціал залежить не тільки від насиченості дисперсного середовища вологою, а й від температури. Отже, вже тільки коливання температури на поверхні середовища впливатиме на капілярно-сорбційний потенціал і швидкість потоку вологи і в свою чергу - на швидкість

міграції забруднюючих речовин. При температурах нижче нуля в природних дисперсних середовищах знаходиться незамерзла волога, рух якої направлено з області з більш високою в область з більш низькою температурою.

Таким чином для моделювання перенесення забруднюючих речовин в природних дисперсних середовищах необхідно враховувати інтенсивність дощових опадів, коливання температури і відносної вологості повітря на поверхні ґрунту, топ то кліматичними факторами.

Література

1. Прохоров, В. М. Миграция радиоактивных загрязнений в почвах. Физико-химические механизмы и моделирование / В. М. Прохоров; под ред. Р. М. Алексахина. – М.: Энергоиздат, 1981. – 98 с.
2. Методы прогноза солевого режима грунтов и грунтовых вод / Н. Н. Веригин [и др.]; под общ. ред. Н. Н. Веригина. – М.: Колос, 1979. – 336 с.
3. Бровка, Г. П. Тепло- и массоперенос в природных дисперсных системах при промерзании / Г. П. Бровка. – Минск: Наука и техника, 1991. – 191 с.

Запорожець Ю.А.
Національний технічний університет України «КПІ імені Ігоря Сікорського», м. Київ
Кафедра кібернетики хіміко-технологічних процесів, асистент

ВИКОРИСТАННЯ ЕКСПЕРТНИХ СИСТЕМ ДЛЯ ПРОГНОЗУВАННЯ МІГРАЦІЇ РОЗЧИНЕНИХ РЕЧОВИН В ҐРУНТОВОМУ ШАРІ

В наш час використовують велику кількість концептуальних математичних моделей, які дозволяють прогнозувати міграцію рідин в пористих середовищах, поширення теплоти в ґрунтових системах і, в результаті, міграцію розчинених речовин. Але частина з них має в своєму розпорядженні достатньо великі припущення і наближення. Також існують більш повні феноменологічні моделі, що включають в себе досить глибокий опис хімічних і фізичних процесів, що протікають в ґрунті. Однак через складність і динамічності цих процесів основною проблемою при їх математичному описі є велика кількість параметрів, коефіцієнтів, граничних умов, необхідних для визначення, і, як наслідок, складність їх використання. Додатковим недоліком виступає і потреба у великих обчислювальних ресурсах для забезпечення виконання розрахункових операцій.

В цьому відношенні велику перспективу мають функціональні моделі ґрунтових процесів, експертні та географічні інформаційні системи. Наявність великих обсягів експериментальних даних як за розподілом (тимчасовому і просторовому) забруднюючих речовин в ґрунті, так і за фізико-хімічними властивостями ґрунтів, накопичених в науково-дослідних організаціях, створює передумови для використання експертних систем з метою їх ефективної обробки. Експертні системи обробки даних відрізняються від звичайних систем тим, що в них використовуються правило-орієнтований апарат представлення

знань, символьний висновок і евристичний пошук рішення (в якості альтернативи використання відомого алгоритму) [1]. Виходячи з цього, основним призначенням експертних систем є рішення неформалізованих задач, що робить їх застосування для вирішення завдань в області екології, зокрема для прогнозування міграції домішок в ґрунтах, досить ефективним.

При цьому експертні системи не відкидають і не замінюють традиційного підходу до розробки програм, орієнтованих на рішення формалізованих задач, а гармонійно їх доповнюють. Тому з метою вдосконалення рішень таких завдань широке поширення набувають інструменти, побудовані на базі гібридизації окремих елементів експертних систем і нейронних мереж, що дозволяє використовувати їх основні переваги та уникнути в ряді випадків окремих недоліків.

Таким чином, складність формалізації задач в аналізованій предметній області, різноманіття процесів що впливають, а також різнорідність експериментальних даних по міграції хімічних речовин в ґрунті робить застосування експертних систем актуальним завданням.

Література

1. Люгер, Дж. Ф. Искусственный интеллект: стратегии и методы решения сложных проблем / Дж. Ф. Люгер. – М.: Вильямс, 2003. – 864 с.

Защепкіна Н.М.[1)], Божко К.М.[2)]
[1)]доктор технічних наук, професор, [2)]кандидат технічних наук,
[1,2)]Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського»
м. Київ, Україна

ВИМІРЮВАННЯ ЕНЕРГЕТИЧНОЇ ОСВІТЛЕНОСТІ ІМІТАТОРА СОНЯЧНОГО ВИПРОМІНЮВАННЯ МОНОХРОМНИМ ПРИЙМАЧЕМ

Спектр сонячного випромінювання є важливою характеристикою для розробки та впровадження технологій фотоелектричної енергетики. При створенні різних типів імітаторів сонячного випромінювання важливою задачею є вимірювання інтегральної величини – енергетичної освітленості, яку створює імітатор в площині сонячної батареї. Нами досліджена можливість вимірювання енергетичної освітленості за величиною фотоструму монохромного приймача, який сприймає світловий потік у вузькому діапазоні ближнього ультрафіолету, а саме 365 ±3 нм.

Попередній аналіз сонячного спектру показав, що відповідно до міжнародних стандартів ASTM E891-92 та IEC 60904-3-2013 для атмосферної маси AM1 (при глобальному випромінюванні 1000 Вт·м$^{-2}$ пряма інтегральна питома потужність дорівнює 793 Вт·м$^{-2}$) на довжині хвилі 365 нм спектральна щільність енергетичної освітленості складає 593 Вт·м$^{-2}$·мкм$^{-1}$. Для порівняння, максимальна щільність дорівнює 1628 Вт·м$^{-2}$·мкм$^{-1}$ на довжині хвилі 480 нм [1].

На Рис. 1 наведено спектр сонячного випромінювання за версіями обох зазначених вище стандартів. Нами зроблено припущення, що вимірювання спектральної щільності на довжині хвилі 365 нм надає інформацію про інтегральну енергетичну освітленість в межах лінійності датчика ультрафіолету.

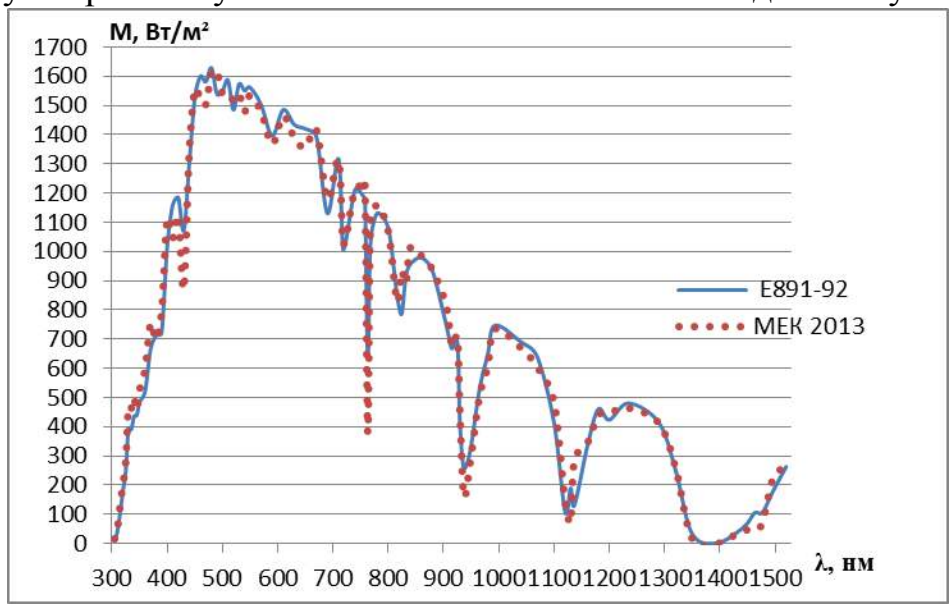


Рисунок 1.1 – Залежності сонячної світимості від довжини хвиль за стандартом ASTM E891-92 та IEC 60904-3-2013

Проведені досліди з одночасного вимірювання інтегральної освітленості цифровим люксметром та спектральної щільності ультрафіолетовим датчиком виявили експоненціальну залежність вихідного струму датчика від інтегральної освітленості (Рис. 2).

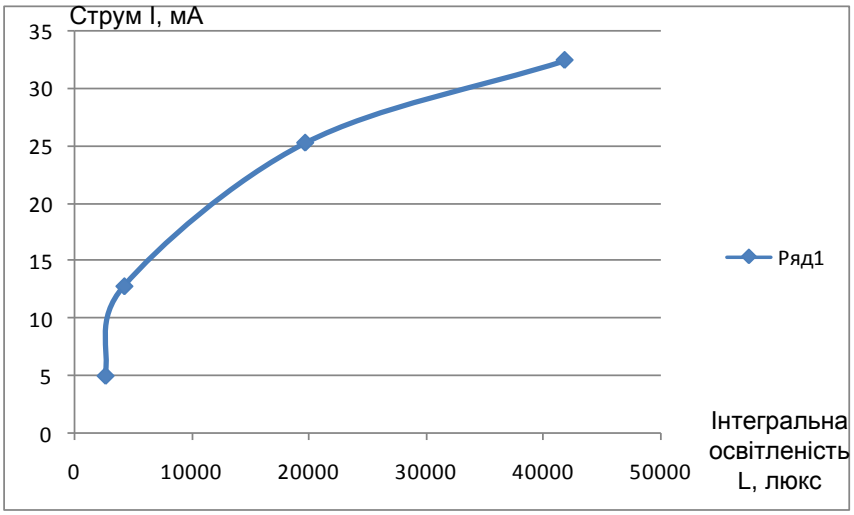


Рисунок 2 – Залежність струму УФ-датчика I від інтегральної освітленості L, створеної імітатором на лампах розжарення

Результати дослідів свідчать про перспективність використання ультрафіолетового датчика для вимірювання інтегральної енергетичної сонячної батареї.

Література.

1. Luque A. Handbook of Photovoltaic Science and Engineering [Текст] /A. Luque, S. Hegedus . – New York.: Wiley. – 2003. – 1180 p.

*[1]**Касько А.Р.**, [2]**ШтаєрЛ.О.**, канд.техн.наук, доцент*
Івано-Франківський національний технічний університет нафти і газу,
м. Івано-Франківськ
Кафедра інформаційно-телекомунікаційних технологій та систем, [1]студент,
[2]доцент

АНАЛІЗ РЕЗУЛЬТАТІВ ПОЛЬОВИХ ДОСЛІДЖЕНЬ ПРИ ЗАСТОСУВАННІ АКУСТИЧНОГО МЕТОДУ КОНТРОЛЮ ВИТОКІВ З ТРУБОПРОВОДІВ

Вирішення проблеми забезпечення безаварійного функціонування газотранспортних систем передбачає підвищення надійності трубопроводів. Методи, які найчастіше застосовуються в системах виявлення витоків розглянуто в [1]. Як спосіб зменшення впливу сторонніх завад при виявленні та визначенні місця витоку з трубопроводу запропоновано використовувати підхід, який полягає у поширенні збуджених в середовищі транспортування акустичних хвиль (область плоских хвиль), які мають властивість розповсюдження на значні відстані і відбивання від місць зміни конфігурації трубопроводу (в т.ч. витоків). Математичні основи методу, методика та результати експериментальних досліджень представлено в [1].

Актуальною задачею при застосуванні тестових методів контролю є вибір величини порогового значення діагностичної характеристики, перевищення якого свідчить про появу витоку з трубопроводу.

Обладнання для проведення польових досліджень: польовий трубопровід ∅ 150 мм довжиною 172 м; модуль випромінювача коливань, змонтований в патрубку довжиною $l_g = 1$ м і ∅ 150 мм; модуль імітації витоку, змонтований в трубі довжиною $l_v = 6$ м і ∅ 150 мм (насадки для крана-імітатора витоку діаметрами 1, 3 ,5 та 10 мм); модуль генерування та реєстрації сигналів – ЕОМ (24 бітова звукова карта ESI Juli@ з частотою дискретизації 192 кГц); підсилювач; повітряно-компресорна пересувна станція ЗИФ-55В з гвинтовим компресором.

Аналіз результатів проведених серій досліджень показав, що пороговим значенням при виявленні витоку ∅ 1 мм є зменшення амплітуди максимуму різницевої характеристики, який ідентифікує місце витоку, на $\approx 30\%$, на $\approx 40\%$ для діаметру витоку 3 мм та на $\approx 20\%$ для діаметру витоку 5 мм. При цьому враховано запас стійкості виявлення витоку за рахунок аналізу мінімальних значень амплітуди ідентифікації витоку за серію експерименту та максимального значення рівня шуму. Підвищення загального рівня шуму при реєструванні витоку ∅ 5 мм зумовлено впливом шуму виривання середовища з отвору в стінці трубопроводу. Отже, при віднесенні до "малих витоків" ті, шум виривання середовища з яких не створює відчутного додаткового шуму довкола трубопроводу (витоки ∅ 1 та 3 мм), умовою виявлення координати витоку є перевищення локальним максимумом різницевої імпульсної характеристики рівня шуму не менше ніж на 30 %.

Ймовірність контролю (виявлення витоку) P в загальному випадку визначається співвідношенням [2]:

$$P = N_v / N_\Sigma,$$

де N_v – кількість успішно проведених процедур виявлених витоків за алгоритмом; N_Σ – загальна кількість проведених досліджень.

В результаті польових досліджень при контролі появи витоку на відстані ≈ 65 м для серії вимірювань (77 шт.) одержано 5 хибних результатів. Визначена ймовірність виявлення витоку становить $(77-5)/77 \approx 0,94$.

Отже, проведений аналіз результатів польових досліджень дозволив встановити поріг виявлення факту наявності витоку за різницевою діагностичною характеристикою та ймовірність контролю.

Література

1. Заміховський Л. М. Контроль витоків з магістральних та технологічних трубопроводів: монографія / Л. М. Заміховський, Л. О. Штаєр. – Івано-Франківськ : ІФНТУНГ, 2013. – 224 с.
2. Чумаков Н. М. Оценка эффективности сложных технических устройств / Н. М. Чумаков, Е. И. Серебряный. – М. : Сов. радио, 1980. – 192 с.

Кондрашов К.В.
Херсонская государственная морская академия, г. Херсон
Кафедра эксплуатации судовых энергетических установок и общеинженерной подготовки, аспирант

АНАЛИЗ СОВРЕМЕННЫХ СИСТЕМ АВАРИЙНО-ПРЕДУПРЕДИТЕЛЬНОЙ СИГНАЛИЗАЦИИ СУДОВ

Начало автоматизации судов относят к эпохе перехода от парусного флота к паровому флоту, и с той поры, все больше функций контроля и управления судовыми механизмами осуществляют приборы.

Постепенно происходил переход от автоматизации отдельных процессов к созданию комплексных систем автоматизации. На современных судах количество процессов, находящихся в автоматических режимах работы, насчитывает несколько сотен. Но, для надёжной работы автоматизированных судовых устройств и механизмов, необходимо было осуществлять непрерывный контроль над самими этими механизмами. Эту функцию взяла на себя система аварийно-предупредительной сигнализации (САПС) судна. Системы АПС являются неотъемлемой частью любого современного судна [1,2].

Первые системы АПС выполняли только одну основную задачу - предупреждение обслуживающего персонала о достижении предельных значений некоторых параметров судовых установок.

По мере развития технологического прогресса, мир судовой автоматики претерпевал постоянные модернизации: появлялись всё новые и новые устройства и механизмы, которые дополняли судовой комплекс систем. Также ширился спектр возможностей и задач судовых САПС.

Система АПС судов прошла путь модернизации от элементарных жёстких контактных связей, потом через релейно-контакторные комплексы, и в наши дни, сигналы от аналоговых и цифровых датчиков обрабатывают высокоскоростные многофункциональные контроллеры. Появилось большое количество вспомогательных задач, которые стала выполнять система аварийно-предупредительной сигнализации [3].

Но, основная функция систем АПС судов, как во времена парового флота, так и в наши дни осталась неизменна – это контроль над работой судового оборудования и подаче сигнала оператору, при появлении неисправности.

Все современные системы АПС имеют абсолютно одинаковую иерархическую структуру (рис.1). Разница будет лишь в производителе электронных карт, модулей и протоколах взаимодействия.

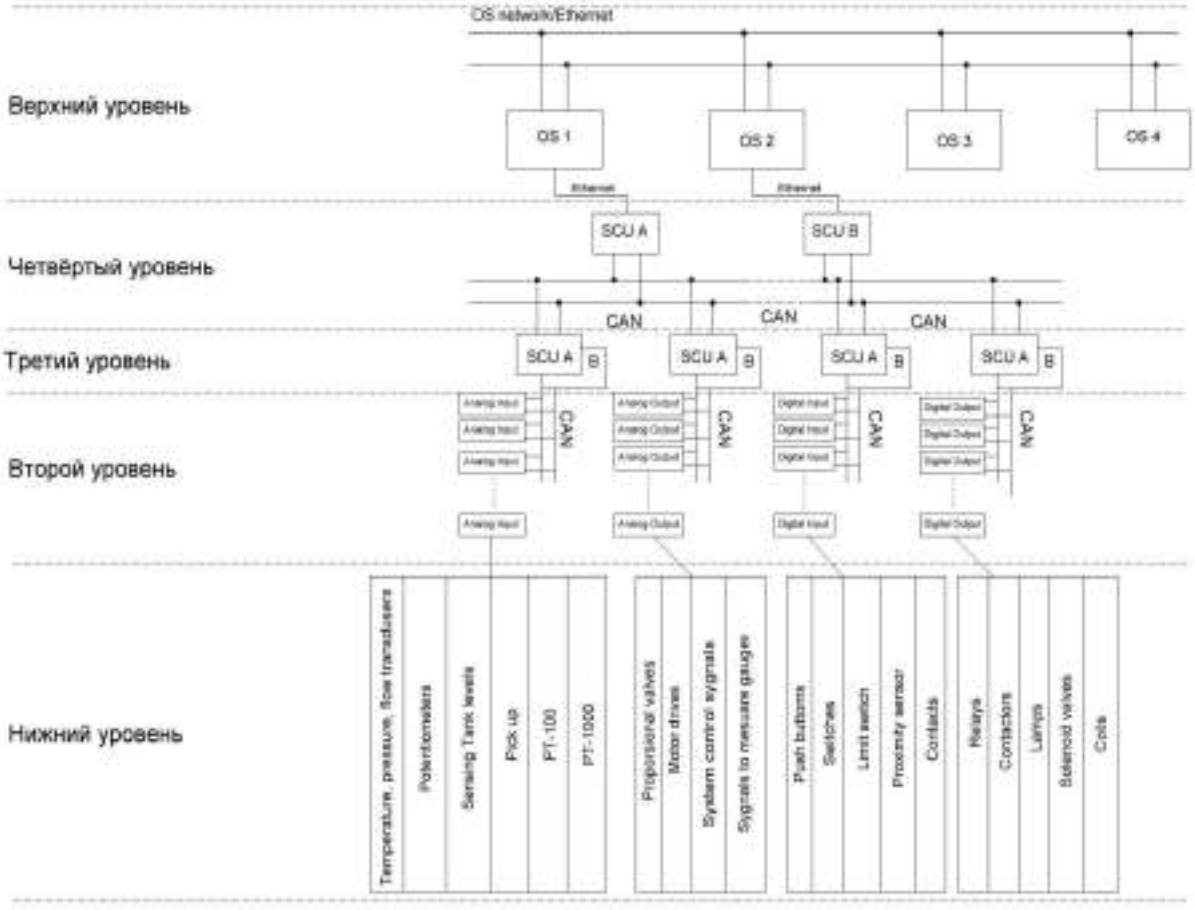


Рис. 1 Иерархическая структура САПС.

Суть процесса работы любой современной АПС состоит из двух этапов:

1. Восприятие информации (источники информации – датчики) о состоянии объекта и внешних условиях и преобразование ее в электрические сигналы для последующей обработки;

2. Обнаружение в поступающей информации признаков отклонения параметров и формирование предупредительного или аварийного сигнала о наступлении этого события.

То есть происходит следующее: сигналы от аналоговых/цифровых датчиков поступают на модули ввода/вывода, аналоговые или цифровые, соответственно. Далее сигналы обрабатываются и переводятся в бинарный код,

который, к примеру, по CAN шине через маршрутизатор поступает в блок главного процессора. Процессор обрабатывает поступившие данные и сравнивает их с допустимыми значениями для каждого конкретного параметра. Любое нарушение в состоянии агрегатов автоматических энергетических установок, от которых поступил отклоненный от нормы сигнал, сопровождается световой и звуковой сигнализацией, а также регистрацией данного события. [2].

Таким образом, принципиального отличия между существующими современными системами АПС судов – нет.

Любая современная САПС – это комплексы электронных модулей, объединённых в локальную сеть сетевым интерфейсом с выводом сигналов в общий, главный контроллер с программируемой конфигурацией.

Основное отличие будет в конфигурации элементов системы, в интерфейсе доступа и функций оператора, в дополнительных возможностях системы, и, конечно же, в производителе основных модулей системы АПС.

Во всех системах АПС, независимо в какой период эпохи автоматизации они были использованы и какими бы функциональными возможностями не обладали, действует один и тот же алгоритм. При возникновении неисправности – система АПС выводит на дисплей параметр, в котором было зарегистрировано отклонение, посылает сигнал для запуска резервного механизма, если предусмотрена данная функция, и запускает световую и звуковую сигнализацию для предупреждения оператора.

На этом основная задача САПС заканчивается.

Дальнейшее развитие событий, и какие меры будут предприняты для устранения поломки, целиком и полностью зависит только от действий обслуживающего персонала.

Чем сложнее оборудование, контролируемое системой АПС, тем труднее быстро выявить и устранить причину неисправности в случае её возникновения.

Список литературы

1. Калявин В. П. Надежность и техническая диагностика судового электрооборудования и автоматики / В. П. Калявин, А. В. Мозгалевский, В. Л. Галка. — СПб.: Элмор, 1996. — 296 с.
2. Тимофеев Ю. К. Системы управления судовыми энергетическими процессами / Ю. К. Тимофеев. — СПб.: Судостроение, 1994. — 312 с.
3. Афромеев Э. А. Критерии технического совершенства судов/ Э. А. Афромеев // Судостроение. — 2005. — № 6. — С. 14–17.
4. KONSBERG. Standard K-Chief 600 Alarm and Monitoring System/ 354760/ Rev.D March 2013 © Kongsberg Maritime AS
5. KONSBERG. Kongsberg K-Chief 500/600 Marine Automation System Installation Manual /311956/F March 2013 © Kongsberg Maritime AS

Левченко К.А., *студентка*
Сабадаш Н.І.,
доцент кафедри ХТХДКЗ,
Національного університету харчових технологій
кандидат технічних наук

Е 160А – ХАРЧОВА ДОБАВКА ПОЛІФУНКЦІОНАЛЬНОЇ ДІЇ

Відомо, що β-каротин дуже цінний і корисний для організму людини. Натуральний каротин був визначений як виняткова поживна харчова добавка [1]. Його широко використовують як натуральний барвник (харчова добавка Е 160а), вводять в продукти лікувально-профілактичного призначення. Застосовують як функціональний інгредієнт [2]. Властивості β-каротину зумовлені його перетворенням в організмі на вітамін А, що необхідно для нормального функціонування органів зору, шкіри. На відміну від вітаміну А в β-каротину відсутня гіпервітамінна активність. Він є сильним антиоксидантом, може захищати від вільних радикалів також β-каротин захищає тканини і клітини від ушкоджень, має імуностимулюючу дію, захищає від УФ-випромінювання. Каротини також захищають клітини організму людини від патогенних мікроорганізмів.

Використання β-каротину в продуктах харчування дозволяє поліпшити їх зовнішній вигляд, органолептичні властивості, підвищити харчову цінність, зберегти якість при тривалому зберіганні, розширити асортимент виробів з β-каротином, в тому числі спецпризначення.

Уже протягом багатьох років каротиноїди використовують в якості барвників в харчовій галузі. Їх наявність в багатьох природних продуктах харчування робить їх цілком доступними для цієї мети. В харчові жири, особливо у маргарин, вершкове масло, додають β-каротин, завдяки чому організм отримує додаткову кількість необхідного для нього вітаміну А. Водорозчинні у воді похідні β-каротину, кантаксантин і апокаротиноїди, застосовуються для підфарбовування напоїв та інших продуктів харчування [3].

Забарвлення β-каротину різниться від світло-жовтого до помаранчевого. Більш того, відтінки каротиноїдів можна регулювати, змінюючи співвідношення подвійних зв'язків в цис- і транс-конфігурації. Однак в чистому вигляді його використовувати не можна, оскільки β-каротин розчиняється в воді, помірно розчиняється в маслах і до того ж швидко окислюється киснем повітря [4].

Список літератури

1. Pat. CN103642266A China. Method for extraction of carrot pigment from carrots [text]: Ni Haiping, CN103642266A. - Application: 19.03.2014.
2. Ковальчук, В. П. Екологічно чистий натуральний барвник: / В. П. Ковальчук, С. І. Олійник, Т. І. Опанасюк, Л. Резвіна // – Харчова і Переробна промисловість. – 2001. - № 239. – 453-454.
3. Сімахіна, Г. О. Технологія природних вітамінів / Г. О. Сімахіна, В. Д. Іванова //. – Київ : НУХТ, 2015 . – 343 с.

4. Курамшин, А. И. Страшная буква Е: Пятьдесят оттенков натуральных пищевых красителей / А. И. Курамшин // Химия и жизнь. – 2017. - № 1. – с. 10-14.

***Морозова Ірина Володимирівна*[1]**
***Богданов Володимир Володимирович*[2]**
Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», м.Київ, кафедра наукових, аналітичних та екологічних приладів і систем, [1]старший викладач, аспірант, [2]студент 4 курсу

ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ПАРАМЕТРІВ І ХАРАКТЕРИСТИК ІМІТАТОРА СОНЦЯ У НЕПЕРЕРВНОМУ РЕЖИМІ

Для визначення довготривалості та ефективності роботи сонячних батарей, а також їх ціни, головними параметрами являються їх експлуатаційні характеристики. Контроль їх параметрів стає все більш і більш актуальним через зростання кожного року числа сонячних батарей в світі.

Імітатор сонячного випромінювання [1] – це пристрій який забезпечує максимально наближене до природного сонячного випромінювання. Його метою є забезпечення контрольованому об’єкту відповідний закритий тест в лабораторних умовах.

У спеціально відведеній лабораторії було проведено дослідження параметрів та характеристик стенда, який включає в себе імітатор сонячного випромінювання з комбінацією двох галогенних вольфрамових ламп розжарення, які по характеристиками практично являються аналогом до світлодіодів та сонячну батарею з дванадцятьма «комірками» (плоскими фотоелектричними елементами). Метою цього дослідження є визначення нерівномірного розподілення неперервного освітлення на сонячну батарею за допомогою люксметру для оптимального налаштування стенда.

Рисунок 1. Установка в не робочому і робочому стані та один з її прожекторів

Досліджувана сонячна батарея має довжину 450 мм та ширина 540 мм. На ній розташовані дванадцять «комірок» (плоских фотоелектричних перетворювачів). Кожна «комірка» досягає 127 мм у ширину, та 124 мм у довжину.

Галогенна вольфрамова лампа розжарення в кожному з прожекторів має такі характеристики: довжина 218 мм; потужність 1000 Вт; світовий потік 13000 люменів. Спектральний склад лампи наближений до абсолютного чорного тіла, а також до спектрального складу сонячного випромінювання. З

розповсюджених імітаторів сонячного випромінювання ця лампа найбільш точно відповідає характеристикам сонячного випромінювання.

Лабораторний стенд працює при неповній освітленості під напругою в 150В. За цих умов струм короткого замикання сонячної батареї дорівнює 0,3А, а температура на поверхні плоских фотоелектричних елементів сягає приблизно 89 °С.

На лабораторному стенді за допомогою люксметра було проведено сорок вимірювань рівня освітленості на кожній з дванадцяти «комірок» сонячної батареї. Приблизне положення плоских фотоелектричних елементів та імітаторів сонячного випромінювання, їх положення над батареєю виділено сірою зоною (рис. 2).

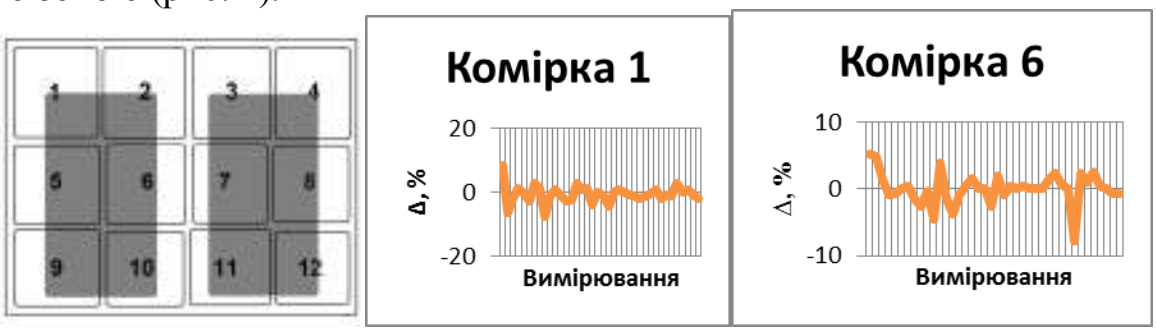


Рисунок 2. Приблизне положення комірок та імітаторів над ними, та графічне зображення дисперсії в 2-х точках

За результатами досліджень було зроблено висновок, чим ближче знаходився фотоелектричний елемент до прожектора з галогенно-вольфрамовими лампами, тим менша у нього спостерігалась дисперсія світла.

Література:

1. Solar Simulator (Continuous Type) [Electronic resource]. - Access mode: http://www.wacomele.co.jp/en/products/solar/normal/. – 8.11.2014

[1]Петрова Ж.О., докт. техн. наук, ст.наук. співр.,
[2]Дмитренко Н.В., канд. техн. наук,
Слободянюк К.С., аспірант
Інститут технічної теплофізики НАН України, м. Київ
Відділ Тепломасопереносу в теплотехнологіях, [1]гол. наук. співр., [2] ст.наук.співр.

ВИЗНАЧЕННЯ ТЕПЛОТИ ВИПАРОВУВАННЯ СОЄВО-ШПИНАТНОЇ СУМІШІ

Труднощі при сушінні рослинної сировини пов’язані з тим, що під впливом теплової обробки світла, кисню, відбуваються втрати біологічно активних речовин. Основною проблемою при переробці сої шляхом сушіння, є максимальне збереження фітоестрогенів та запобігання окисленню ліпідів. Для інактивації антихарчових компонентів сої, поліпшення якості проводять попередню гігротермічну обробку сировини. Сою замочують, промивають, проварюють, та знову промивають, в результаті чого підвищується

перетравлюваність білків та руйнування анти харчових компонентів, що містять боби [1].

Також, в процесі сушіння рослинної сировини багато енергії витрачається на випаровування вологи. Практика сушіння цілого ряду складних рослинних матеріалів вказує на істотну відмінність реальних значень витрат теплоти на випаровування з них вологи від теплоти випаровування чистої води [2]. Оскільки зростання енергетичних витрат при сушінні рослинних матеріалів пов'язують з утрудненою проникністю клітинних оболонок для води та складністю видалення води, яка взаємодіє з розчинними компонентами клітинного соку і молекулами скелету матеріалу, важливо було дослідити вплив створення функціональних композицій з рослинної сировини на питому теплоту її випаровування. Для визначення витрат теплоти на випаровування вологи з запропонованих функціональних сумішей було проведено визначення питомої теплоти випаровування води з них та їх компонентів.

Було використано калориметричний метод, заснований на безперервному одночасному вимірюванні зменшення маси зразка та кількості теплоти, що витрачена на випаровування вологи в процесі ізотермічного сушіння. Експерименті проводили за допомогою удосконаленого варіанту створеної в ІТТФ НАНУ установки синхронного термічного аналізу ДМКИ-01[3], де використано калориметричну платформу з глибокими комірками циліндричної форми, що дозволяють досліджувати дисперсні матеріалі. Для проведення досліджень використовували подрібнені гігротермічно оброблену сою, шпинат, та їх функціональні суміші. Рослинні тканини подрібнювали до приблизного розміру 4х2х3 мм. Кондуктивне сушіння зразків масою 0,3 г відбувалося в робочій камері калориметричного блоку, при температурі 60ºС, в умовах, наближених до ізотермічних, до моменту досягнення зразками рівноважної вологості. Температуру сушіння 60С було визначено як оптимальну для попередньо обробленої білкововмісної сировини, що запобігає втратам біологічно активних речовин. Масу сухої речовини в зразку визначали методом досушування всередині робочої камери при 105 °С.

Поточні значення питомої теплоти випаровування води зі зразку визначали, починаючи з часу встановлення термодинамічної рівноваги всередині калориметричної камери, за формулою:

$$r_i = \frac{\int_{\tau_{i-1}}^{\tau_{i+1}} q(\tau) d\tau}{m(\tau_{i-1}) - m(\tau_{i+1})}$$

де r_i – питомі витрати теплоти на випаровування за час від $\tau_{i\text{-}1}$ до τ_{i+1}, кДж/кг;

$\tau_{i\text{-}1}$ та τ_{i+1} – значення поточного моменту часу, с;

$q(\tau)$ – тепловий потік всередині робочої камери як функція часу, Дж /с;

$m(\tau_{i\text{-}1})$ та $m(\tau_{i+1})$ – маса зразка в моменти часу $\tau_{i\text{-}1}$ та τ_{i+1}, кг.

Результати вимірювання наведено на рисунку 1. З рисунка 1 бачимо, що на початку сушіння теплота випаровування вологи зі шпинату та соєво-шпинатної суміші приблизно на 4…5% більша від теплоти випаровування чистої води. Змішування компонентів, призвело до того, що в процесі сушіння,

починаючи з вологості 65%, в суміші відбувається екзотермічна реакція, яка супроводжується додатковим виділенням теплоти. Можна припустити, що це реакція взаємодії жирів сої з жиророзчинними каротиноїдами шпинату, але більш точне встановлення характеру цієї реакції потребує додаткових досліджень.

Попередня підготовка рослинної сировини методом створення функціональних композицій зі спеціально підібраним співвідношенням дозволяє запобігти окисленню ліпідів та продовжити термін зберігання переробленої сої та шпинату.

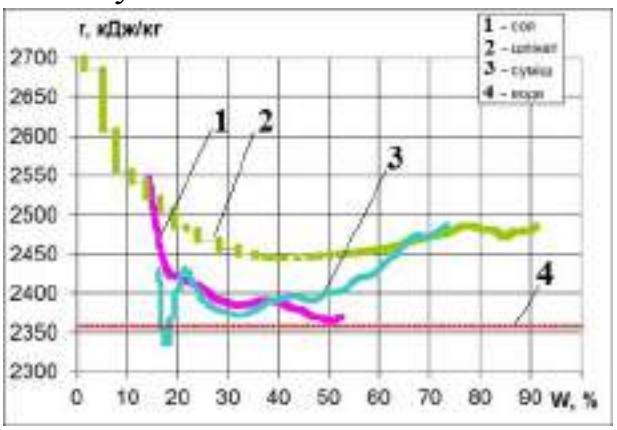


Рис. 1 Залежність приведеної теплоти випаровування води зі зразків від їх відносної вологості під час сушіння.

Встановлено, що питомі витрати теплоти на випаровування води з розробленої рослинної композицій на основі сої з додаванням шпинату на 4…5% більше від теплоти випаровування чистої води вже на початку процесу сушіння. Виявлено, що при сушінні запропонованої композиції відбувається реакція поміж компонентами суміші, яка супроводжується екзотермічним ефектом.

Література

1. PetrovaZh.O., Slobodianiuk K.S. Energy effective drying modes of soy-vegetable compositions. Ukrainian Journal of Food Science. 2017. Volume 5, Issue 1, p. 150 – 160.

2. Дмитренко Н.В., Дубовикова Н.С., Снежкин Ю.Ф. Изучение влияния состояния воды в пищевых растительных материалах на теплоту испарения // Научные труды Одесской национальной академии пищевых технологий. – 2011. – Вып. 40, Т.2. – С. 71-75.

3. Патент України № 84075 МПК G01 N25/26, G01 N25/28. Калориметричний пристрій для визначення питомої теплоти випаровування вологи і органічних рідин з матеріалів / Снєжкін Ю.Ф., Декуша Л.В., Дубовікова Н.С., Грищенко Т.Г., Воробйов Л.Й., Боряк Л.А. – Заявка № a200613266; заявл. 15.12.06; видано 10.09.08; опубл. 10.09.08; Бюл. №17. – 10 с.

Харченко Т.П., студентка
Київський політехнічний інститут ім. Сікорського, м. Київ
Кафедра інформаційно-телекомунікаційних мереж

МЕХАНІЗМ ЗБЕРЕЖЕННЯ ЕНЕРГІЇ DISCONTINUOUS RECEPTION (DRX) В LTE ADVANCED

LTE Advanced - стандарт мобільного зв'язку. LTE Advanced стандартизований 3GPP як головне поліпшення стандарту Long Term Evolution (LTE). LTE-Advanced передбачає розширення смуги частот, агрегацію (декількох смуг, в тому числі не сусідніх) спектра, має розширені можливості багатоантенної передачі даних MIMO, підтримує функції ретрансляції сигналу LTE, а також розгортання гетерогенних мереж (HetNet).

Так як мобільні пристрої мають обмежений запас енергії (який визначається ємністю акумуляторних батарей), то для збільшення часу роботи без підзарядки акумуляторів стандартом LTE визначається спеціальний режим функціонування, який дозволяє знизити енергоспоживання мобільних станцій. Такий режим називається Discontinuous Reception (DRX).

Принцип роботи режиму DRX полягає в тому, що мобільний пристрій здійснює прийом даних від базової станції (БС) не весь час, а періодично. Тобто, в певні моменти часу мобільна станція (МС) відключає свій радіоприймач, тим самим знижуючи свої енерговитрати. На малюнку 1.1 представлений приклад роботи МС в режимі DRX, а також наведені параметри даного режиму. Значення параметрів задаються в підкадрах (TTI).

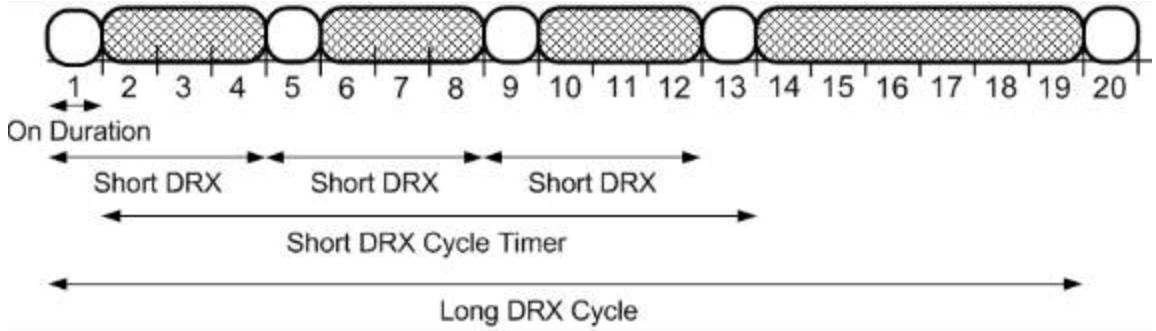


Рис. 1.1 Робота мобільної станції в режимі DRX

Весь час функціонування системи розбивається на цикли. Кожен цикл починається з періоду "on Duration".

Під час періоду on Duration - МС прослуховує радіоканал і здійснює прийом даних від БС (прийом каналу PDCCH) з метою дізнатись чи з’явились на БС дані для передачі цієї МС. Якщо протягом цього часу eNB не повідомив про наявність даних для передачі, то МС відключає свій радіо приймач до закінчення циклу, тривалість якого визначається як Short DRX – on Duration. Де Short DRX визначає загальну тривалість циклу.

Крім циклу Short DRX, може бути заданий цикл Long DRX (як випливає з назви, тривалість другого циклу має більшу тривалість першого). Використання циклів Long DRX дозволяє ще більше знизити енерговитрати МС (але при цьому також збільшується затримка передачі даних). МС переходить до

використання Long DRX циклу, якщо протягом таймера Short DRX Cycle Timer не було передач даних від БС. Після кожного прийому даних від БС цей таймер перезапускається.

Відзначимо, що на малюнку 1.1 тривалість циклу LongDRX більше, ніж тривалість ShortDRXCycleTimer.

Як вже зазначалося вище, використання DRX режиму не тільки знижує енерговитрати МС, але і збільшує затримку при передачі даних. Відповідно, при завданні параметрів цього режиму необхідно враховувати вимоги до якості обслуговування (Quality of Service, QoS), які пред'являються переданим потоком даних

Література

1. LTE advanced [Електронний ресурс] – Режим доступу: https://ru.wikipedia.org/wiki/LTE_Advanced.

2. Описание механизма сбережения энергии - Discontinuous Reception (DRX). [Електронний ресурс] – Режим доступу: http://anisimoff.org/lte/drx.html.

3. C.-J. Tsai, T.-H. Lee, Quality of service support in LTE advanced systems with DRX mechanism, Digital Communications and Networks (2018), doi: 10.1016/j.dcan.2018.04.001.

Харченко Т.П., студентка
Київський політехнічний інститут ім. Сікорського, м. Київ
Кафедра інформаційно-телекомунікаційних мереж

ФІЗИЧНИЙ РІВЕНЬ LTE: АНАЛІЗ ТА ОЦІНКА ЕФЕКТИВНОСТІ

Забезпечення високошвидкісної передачі даних було найважливішою метою 4-го покоління стандартів мобільного зв'язку. На відміну від стандартів третього покоління, що використовують технологію CDMA, LTE використовує мультиплексування з ортогональним частотним розділенням (OFDM) та частотним розподіленням (SC-FDMA). Також наявний гнучкий радіо інтерфейс, а його основна мережа називається System Architecture Evolution (SAE) або Evolved Packed Core (EPC).

Архітектура SAE складається з двох основних частин: EPC та E-UTRAN . Ці дві частини разом утворюють систему Evolved Packet System (EPS). EPS маршрутизує IP-пакети з заданим QoS, від мережевого шлюзу пакетної передачі даних (P-GW) до User Equipment (UE). EUTRAN керує радіоресурсами та забезпечує безпеку переданих даних . E-UTRAN складається з базових станцій, які підключені до UE. Архітектура E-UTRAN є плоскою, таким чином відсутня централізована керованість в E-UTRAN. EPC дозволяє комутувати пакети даних як з Інтернетом, так і з UE, з підтриманням QoS. EPC включає Home Subscriber Service (HSS), Policy Control and Charging Rules Function (PCRF), елемент управління мобільністю (MME), пакетний P-GW та серверний шлюз (S-GW).

Інтерфейс складається з трьох рівнів, з назвами 1, 2 і 3. Транзитні канали рівня Medium Access Control (MAC) з'єднані з логічними каналами, які зв'язують MAC-рівень з RLC-рівнем. Логічні канали на рівні MAC характеризуються типом переданих через них даних.

Архітектура протоколу фізичного рівня LTE представлена на рис.1

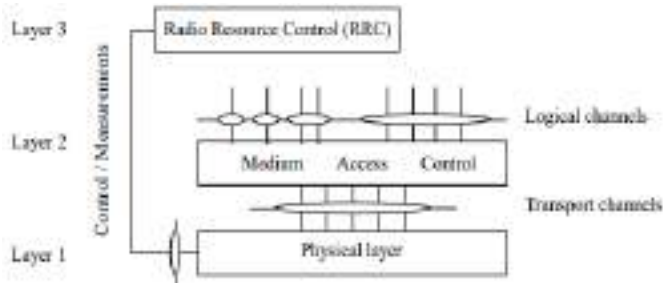


Рис. 1.1 Архітектура протоколу фізичного рівня між мережею LTE та UE

Фізичний рівень LTE підтримує два режими передачі даних: FDD, TDD

TDD: Зв'язок здійснюється завдяки тимчасовому ущільненню каналів передачі і прийому даних на одній частоті. Завдяки такому режиму досягається найбільш оптимальний перерозподіл ресурсів ліній радіозв'язку. При цьому виділяється різна кількість тимчасових інтервалів в низхідних (download) і висхідних (upload) каналах зв'язку.

FDD: Сигнал розділяється на дві різні частоти. Одна частота для прийому даних (download), інша - для передачі (upload). Це дозволяє поліпшити якість зв'язку та зменшити затримки при передачі даних. В даному режимі кількість каналів в обох напрямках (висхідні і низхідні канали зв'язку), як правило, однакові.

На фізичному рівні LTE застосовуються технології для забезпечення високої швидкості передачі даних і ефективного використання спектра. OFDMA і MIMO дозволяють досягати в низхідному каналі швидкість передачі 100 Мбіт / с, а технологія SC-FDMA допомагає зменшити відношення пікової потужності до середньої і дозволяє спростити схему абонентських терміналів. Різні методи модуляції і кодування дозволяють збільшити пропускну здатність і ємність мережі.

Література

1. C.-C. Yang, J.-Y. Chen, Y.-T. Mai, and C.-H. Liang, "Adaptive load-based and channel-aware power saving for nonreal-time traffic in LTE," EURASIP Journal on Wireless Communications and Networking, vol. 2015, p. 1, 2015.

2. Физический уровень LTE [Електронний ресурс] – Режим доступу: http://www.russianelectronics.ru/leader-r/review/2187/doc/53411/.

3. Режимы связи LTE FDD и TDD [Електронний ресурс] – Режим доступу: http://www.techno-guide.ru/informatsionnye-tekhnologii/mobilnaya-svyaz.

Швець Л.В., кандидат технічних наук, доцент
Труханська О.О., кандидат технічних наук, ст. викладач
Вінницький національний аграрний університет, м. Вінниця

УДОСКОНАЛЕННЯ МАШИННИХ ТЕХНОЛОГІЙ ТА ВІДПОВІДНОГО ОБЛАДНАННЯ НА ОПЕРАЦІЇ ЗРІЗУ ГИЧКИ

Основною сировиною для виробництва цукру в Україні та багатьох європейських країн є цукрові буряки. Вирощування і збирання даної культури потребує високих матеріальних і трудових затрат. Розвиток науково – технічного прогресу в буряківництві дає можливість здійснювати біологічний контроль за продуктивністю рослин, впроваджувати інтенсивні технології їх вирощування.

Ряд відомих Європейських фірм випускають потужні бурякозбиральні комбайни, виготовлені за типовою схемою: спочатку зрізується гичка, потім викопуються коренеплоди і транспортуються в бункер, звідки навантажуються в транспортний засіб.

Постійний розвиток рівня механізованих технологій і коренезбиральних машин дає можливість поліпшити якість очистки цукрових буряків від гички перед їх транспортуванням на цукровий завод шляхом розширення величини зрізу головки коренеплоду та підвищення допуску (до 5%) на відходи цукроносної маси із зрізаними головками до нижньої межі «сплячих вічок».

В західноєвропейських країнах, переважно, прийняті більш жорсткі вимоги до чистоти сировини, а саме при використанні пониженого зрізу, коли некондиційними вважаються корені, у яких площина зрізу проходить на рівні, або вище основи листкових черешків на головці коренеплоду.

Удосконалення машинних технологій та відповідного обладнання на операції зрізу гички дасть можливість підвищити урожайність коренеплодів, продуктивність гичкозбиральних машин шляхом підвищення якості (плаский зріз, відсутність сколів і косого зрізу), точності роботи, підвищення швидкої дії приводів гичкозрізальних апаратів, що є актуальним і може суттєво зменшити втрати сировини.

Для зменшення втрат врожаю при зрізанні гички під час збирання коренеплодів представлено модернізований зрізувальний пристрій з механічною системою копіювання окремо для кожного рядка (рис.1).

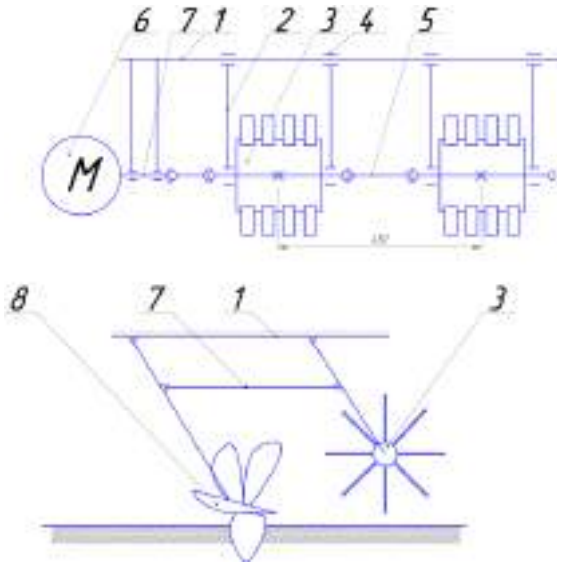


Рисунок 1 – Схема пристрою для зрізання гички: 1 – рама; 2 – кріплення приводу; 3 – обрізчик гички роторний; 4 – шарнір; 5 – карданний вал; 6 – гідропривід; 7 – паралелограмна підвіска; 8 – копір.

Пристрій для зрізання гички складається з рами 1, на якій змонтовано робочі органи обрізчика, ротора 3, закріпленого шарніром 4, який разом із копіром 8 утворює паралелограм. Кожен ротор на окремий рядок має своє кріплення. Привід здійснюється від гідродвигуна 6, на кожний ротор передача крутного моменту проходить через карданну передачу 5.

Робота роторного подрібнювача гички коренеплодів полягає в копіюванні кожного рядка коренеплодів окремо. При цьому привод подрібнювачів на кожний рядок може здійснюватись одним гідродвигуном на шість рядків, або на чотири рядки з встановленими гідромоторами з боків подрібнювачів. Рух подрібнювачів окремо по рядкам здійснюється завдяки шарнірному паралелограмному кріпленню роторів, окремо один від одного, і карданної передачі крутного моменту від гідродвигуна на подрібнювачі.

Використання роторного копіювального подрібнювача дасть змогу зменшити втрати цукрового буряка при зрізанні гички та поліпшити якість зрізу.

Щедролосєв Олександр Вікторович
Доктор технічних наук, професор,
завідувач кафедри Будівництва та ремонту суден
Кораблебудівного навчально-наукового інституту
Національного університету кораблебудування імені адмірала Макарова,

Коннов Володимир Миколайович
Головний конструктор ХГЗ «Паллада»,

Узлов Олександр Миколайович
Старший викладач кафедри Будівництва та ремонту суден
Кораблебудівного навчально-наукового інституту
Національного університету кораблебудування імені адмірала Макарова,

Кириченко Костянтин Володимирович
Аспірант кафедри Будівництва та ремонту суден
Кораблебудівного навчально-наукового інституту
Національного університету кораблебудування імені адмірала Макарова,

ТЕХНОЛОГІЧНІ ОСОБЛИВОСТІ ПОБУДОВИ КОМПОЗИТНИХ ДОКІВ ЗІ ЗМЕНШЕНОЮ КІЛЬКІСТЮ НАБОРУ У ПОНТОНІ

Залізобетонні споруди в порівнянні з аналогічними типами, які виготовлені з металу, мають ряд вагомих переваг: витрати металу в 2-3 рази менше, вартість споруди на 30-50% дешевше, безремонтний термін експлуатації в 2-3 рази довше [1].

Сучасні композитні плавучі доки вітчизняної побудови, у яких понтон залізобетонний, а вежі - сталеві, мають істотні відмінності від зарубіжних. Ці відмінності виявляються в особливостях конструкції понтонів, плоскі елементи яких мають значно меншу товщину [2-4].

Вежі дока, включаючи зовнішній борт понтона і днище понтона під вежами, набрані по поздовжній системі, а понтон між внутрішніми бортами по поперечній системі. Таке рішення дозволяє виконати весь залізобетонний корпус понтона із плоских секцій. Пропуск дорівнює 750мм. Відстань між поперечними перегородками понтона прийнято рівним 4 шпації, тобто 3000мм. Вежі дока - сталеві.

При постановці судна в док, кільблоки ставляться на повздовжню перебірку доку, навантаження від якої передаються на рідко розставлені поперечні перебірки доку, завдяки чому забезпечується загальна поперечна міцність.

При побудові понтону - очищення арматури від жирних плям і слідів фарби проводиться за допомогою хімічних розчинників, потім ці місця витираються насухо. Гнучка арматурної сталі виконується на згинальних верстатах або вручну. Виготовлення арматурних сіток проводиться на

автоматичної зварювальної машині або зварюванням перетині в шаховому порядку в середовищі CO_2.

Перед установкою на стенди арматурних сіток для збірки в об’єм, стенди повинні бути очищені від бетону і бруду. Стенди для формування залізобетонних секцій повинні забезпечувати виготовлення секцій з гладкими поверхнями рівномірної товщини і забезпечувати швидке знімання відформованих секцій.

Монтаж секцій веж на понтон допускається тільки після бетонування і досягнення міцності стиків заставних вузлів з'єднання веж з понтоном, а також всіх стиків зовнішнього і внутрішнього борту не менше 21 МПа (210 кг/см^2) на відстані не менше 6 шпацій в ніс і корму від кінців встановлюваних секцій.

Формування веж виконується від міделя в ніс і корму. Послідовність формування веж:

- навантаження секцій,
- прикреслення і прирізка по стиках і пазах,
- кріплення на гребінках по пазах і прихватках по стиках секцій.

При установці і стикування секцій між собою повинна бути забезпечена система контролю за точністю стикування по висоті і горизонталі. Заключний монтаж механізмів, пристроїв і трубопроводів виконується після закінчення складально-зварювальних робіт по корпусу дока, фундаментів і підкріпленням в районі їх штатної установки.

Перед установкою опалубки арматура стику повинна бути очищена від бруду, масел, фарби, іржі. Кромки секцій всіх елементів понтона і весь бетон конструкцій, що потрапляють в стик, повинні бути звільнені від цементної плівки шляхом насічки пневмоінструментом. Після очищення стиків та установки всіх закладних конструкцій проводиться установка деревометалевої опалубки, яка повинна відповідати наступним вимогам:

- забезпечувати правильність форм і розмірів бетонованого стику;
- мати достатню міцність і твердість;
- не допускати витікання цементного молока при ущільненні бетонної суміші;
- вільно розбиратися з мінімальними пошкодженнями.

У всіх випадках бетон міжсекційних з'єднань повинен мати міцність, водонепроникність і морозостійкість не менше необхідної для бетону сполучних елементів понтона. Укладання бетону в форми проводиться не пізніше 45 хвилин після його виготовлення (в літній період). Укладання бетону в вертикальні стики повинно проводитися на всю висоту стика. Після укладання бетону виконують його ущільнення шляхом вібрації за допомогою пневмовібраторів.

Перерви при укладанні бетону в одну конструкцію не повинні перевищувати 1 годину при температурі зовнішнього повітря більше 25 ° С, в інших випадках не більше 2-х годин. При більш тривалих перервах бетонування повинно бути припинено і відновлено після закінчення твердіння бетону і насічки (поновлення) штраби. Розпалубку стиків виробляти після досягнення бетоном вертикальних стиків 35% і горизонтальних 50% проектної міцності.

Усунення дефектів бетонування повинно здійснюватись за допомогою повного видалення всього нетривкого бетону і наступним закладенням дефектного місця бетоном такої ж якості, який вживався для бетонування міжсекційних з'єднань. Дефекти у вигляді тріщин або невеликих отворів повинні бути попередньо оброблені по кромках на величину, достатню для якісного заповнення їх бетоном на всю глибину.

Випробування на водонепроникність залізобетонного корпусу понтона проводиться після усунення дефектів, виявлених зовнішнім оглядом і закінчення монтажу закладного і приварного насичення.

Висновки. Наведено технологію побудови залізобетонного понтона зі зменшеною кількістю набору у понтоні. Конструкція бетонних перекриттів сприймає в декілька разів більший момент спротиву ніж сталь, що дозволяє збільшити проліт перекриття і рідше розставляти опори-переборки. Внаслідок цього знижуються витрати пов'язані з вартістю матеріалів, а також зменшується трудомісткість робіт при побудові доку.

Література

1. Мишутин А.В. Железобетонные плавучие сооружения и перспективы их использования [Текст] / А.В. Мишутин.: Вісник ОДАБА. – Одесса – 2002, - Вып. 6, – с. 181-187.

2. Рашковський О.С. Проектування, технологія і організація побудови композитних плавучих доків [Текст] / О.С. Рашковський, О.В. Щедролосєв, Д.В. Єрмаков, О.М. Узлов.: Навчальний посібник. – Миколаїв: НУК: РАЛ Поліграфія, 2015 – 254 с.

3. Патент на корисну модель 7809 Україна, МПК В 63 В 9/00. Спосіб стикування підводних частин залізобетонної плавучої споруди / Слуцький М.Г., Маломан В.Ф. (Україна). Заявл. 17.11.04; Опубл. 15.07.05. – К.: Промислова власність, 2005. – № 7, кн. 1. – С. 5.85.

4. Патент на корисну модель МПК B63B 9/00 B63C 5/00 Стапель для спорудження залізобетонних суден / Щедролосєв О.В., Узлов О.М., Кириченко К.В. № 113891 Бюлетень №4 від 27.02.2017.

Зміст

Частина 1

Секція: Інформаційні системи і технології

Архипова С.А.
Построение регрессионных моделей при неполной информации о погрешностях измерений……..……7

Балалаева Е.Ю., Вакуленко Т.В.
Применение алгоритмов нечеткой логики для создания информационной системы медицинской диагностики……..…...……6

Бондаренко В.А.
Державна політика впровадження інформаційних технологій в галузь медицини України……..……..……..……7

Гораш М.А.
Розробка інформаційно-аналітичної системи моніторингу стану архітектурних об'єктів……..……..…….9

Доброштан М.В.
Правові механізми захисту інформаційних прав людини……..……10

Драбинко В.П.
Інформаційно-комунікаційні технології у процесі освіти у вищих навчальних закладах……14

Дрегало Л.В.
Оптимізація використання ресурсів сховищ даних……..……15

Елізаров А.Б., Гасімов Ф.М.О.
Захист корпоративної мережі підприємства за рахунок створення VPN тунелю……..……17

Колесников В.А.
Порівняльна характеристика симетричного та асиметричного шифрування….23

Корзун В.І.
Використання штучного інтелекту для розпізнавання об'єктів місцевості на зображеннях……..……25

Котлерман І.В., Отношенний І.О.
Особливості реалізації стеганосистеми з секретним ключем……27

Кравченко О.О.
Аналіз методів кешування даних у веб-застосуваннях……..……28

Кузьміних В.О., Осипенко М.В.
Використання штучного інтелекту для пошуку інформації в електронних джерелах……..……31

Макута М.Ю.
Дослідження та розробка телеграм-бота системи самообслуговування Інтернет-провайдера……..……33

Марочканич О.Р.
Проблеми та ризики у веб-застосуваннях……..……35

Марочканич О.Р.
Порівняльний аналіз алгоритмів шифрування на прикладі веб-браузерів…..…38

Марочканич О.Р.
Основні засади та принципи оптимального пошуку інформації……41

Мерзлікін К.М.
Аналіз методів класифікації часових рядів……..……44

Миколайчук Т.В., Фоміченко І.П.
Впровадження сучасних систем фільтрації у галузь кольорової металургії України……..……46

Мискін Ю.І., Міщенко Р.О., Вальдовский В.І.
Характеристика сучасного програмного забезпечення автоматизації обліково-інформаційних систем управління……..……48

Псюк Н.М.
Класифікація фразеологізмів: теоретико-понятійний аспект……..……50

Рогоза А.В.
Хмарні обчислення……..……51

Рогоза А.В.
Мобільна хмарна мережа……..……55

Рогоза А.В.
Вразливість хмарних обчислень……..……58

Синельников Н.Д.
Электронные платежные системы для деятельности некоммерческого предприятия……..……61

Сініцин О.В.
Алгоритмічні та програмні засоби формування і відображення тривимірного зорового образу земельної ділянки та об'єктів наземного базування в геоінформаційній системі прецизійного землеробства……63

Слабінога М.О., Семків Р.Ю.
Система пропускного контролю на базі ESP8266 та платформи Arduino…..…66

Тєлишева Т.О., Курилко І.М.
Сервіс з прикладним інтерфейсом для розпізнавання облич……..……67

Ченька М.В.
Cambridge Analytica та інформаційна безпека у соціальних медіа……..……71

Черняк Б.Р.
Використання інформаційних систем для підтримки діяльності некомерційного підприємства……..……76

Шевелін М.С.
Проблеми прогнозування багатофакторних моделей……..……78

Секція: Технічні науки

Божко К.М.
Телевізійні засоби в неруйнівному контролі електролюмінісцентних мікродефектів сонячних елементів……80

Бреус Д.М.
Розрахунок для дослідження принципу дії ультразвукового датчику для електронної системи виявлення перешкод……81

Грудз В.Я., Марущенко В.В., Братах М.І., Савчук М.Т., Філіпчук О.О.
Питання експлуатації газовидобувної системи на завершальній стадії експлуатації родовищ……86

Запорожець Ю.А.
Вплив навколишнього середовища на перенесення забруднюючих речовин в природному дисперсному середовищі……91

Запорожець Ю.А.
Використання експертних систем для прогнозування міграції розчинених речовин в ґрунтовому шарі……92

Защепкіна Н.М., Божко К.М.
Вимірювання енергетичної освітленості імітатора сонячного випромінювання монохромним приймачем……93

Касько А.Р., Штаєр Л.О.
Аналіз результатів польових досліджень при застосуванні акустичного методу контролю витоків з трубопроводів……95

Кондрашов К.В.
Анализ современных систем аварийно-предупредительной сигнализации судов……96

Левченко К.А., Сабадаш Н.І.
Е 160а – харчова добавка поліфункціональної дії……99

Морозова І.В., Богданов В.В.
Експериментальні дослідження параметрів і характеристик імітатора сонця у неперервному режимі……100

Петрова Ж.О., Дмитренко Н.В., Слободянюк К.С.
Визначення теплоти випаровування соєво-шпинатної суміші……101

Харченко Т.П.
Механізм збереження енергії Discontinuous Reception (DRX) в LTE Advanced……104

Харченко Т.П.
Фізичний рівень LTE: аналіз та оцінка ефективності……105

Швець Л.В., Труханська О.О.
Удосконалення машинних технологій та відповідного обладнання на операції зрізу гички……107

Щедролосєв О.В., Коннов В.М., Узлов О.М., Кириченко К.В.
Технологічні особливості побудови композитних доків зі зменшеною кількістю набору у понтоні……109

Частина 2

Секція: Економічні науки

Аль-Газу Алі
Напрямки зменшення собівартості послуг авіатранспорту……3

Балагур Ю.А.
Проблеми безпеки електронної комерції в мережі інтернет……5

Балагур Ю.А.
Проблеми розвитку ринку інновацій в процесі інституціоналізації української економіки……7

Божок Є.М.
Формування портфелю банківських послуг……8

Бондаренко В.В.
Інноваційна діяльність аграрних підприємств……10

Босак А.О., Пенгрин С.М.
Світовий ринок риби: загальні тенденції і місце України……12

Буркова Л.А., Бабіна К.О.
Загальнодержавні податки та збори: сутність та значення……14

Буртник С.Р., Яременко М.І.
Удосконалення обліку нематеріальних активів……16

Бусарєва Т.Г.
Характеристика етапів управління знаннями ТНК……19

Буштаков С.В., Джур О.Є.
Вплив цифрових технологій на формування систем менеджменту підприємств……22

Галушко О.І.
Перспективи розвитку форензік послуг в Україні……25

Губиш Н.О.
Шляхи підвищення ліквідності підприємства в межах антикризового управління……27

Добра М.В.
Контроль процесу управління інвестиційним проектом та його фінансові елементи……..…28

Дуганець Н.В., Кучер І.Т.
Інвентаризація грошових коштів……..…31

Закіров Р.Р.
Продуктивність праці в Україні……..…34

Захаренко Ю.С.
Особливості відображення уцінки основних засобів з метою податкових розрахунків……..…36

Іванова В.С.
Аналітичні аспекти оцінки результативності реалізації інвестиційних проектів на основі збалансованої системи показників……..…38

Іващенко О.В., Клименко С.Є.
Ділова розвідка як складова фінансово-економічної безпеки підприємства.…40

Клеймьонова А.О.
Технологія блокчейну в обліку «потрійного запису»……..42

Колосенко К.О.
Проблеми формування ресурсного потенціалу підприємства……..…44

Кримінець О.Я.
Інвестиції в основний капітал в Україні……..…45

Лакуста Н.Ю.
Особливості ліцензування торговельної діяльності……..…47

Личак О.О.
Вдосконалення принципів управління операційними ризиками в банках України……..…51

Нашкерська Г.В., Лемешко С.Я.
Удосконалення організації обліку готівкових операцій на підприємстві……52

Пастух Х.Р., Машлій Г.Б.
Роль стратегічного планування у розвитку територіальних громад……..…54

Петрушко Я.Р.
Конкурентна розвідка як елемент системи безпеки кредитної діяльності банків……56

Прудкий В.В., Малик І.П.
Мотивація як фактор підвищення продуктивності праці……58

Рибалка Ю.А.
Заходи вдосконалення системи управління фінансовими результатами від операційної діяльності підприємства……60

Савчук Л.О.
Інфляція в Україні та її прогнози……64

Саидова Д.Н., Мусаева Н.Н., Мустафаев С.А.
Вопросы совершенствования профессиональной подготовки предпринимательских кадров в условиях инновационного развития……66

Саидова Д.Н., Мусаева Н.Н., Худойбердиева Ф.М.
Инновационные технологии в аграрном секторе Узбекистана для повышения производства растениеводства……68

Соколенко Л.Ф.
Інформаційне забезпечення системи обліку альтернативних форм обслуговування житлового фонду……72

Талоєв Д.Р.
Інструментарій вирішення конфліктних ситуацій в організації……74

Танчик О.І., Дятлов Є.В.
Інформаційне забезпечення як складова управління національною економікою……76

Фрайт О.В.
Перспективні напрямки застосування Інтернет технологій в маркетинговій діяльності підприємства……79

Ширяєва Л.В., Шахова О.А.
Проблеми та шляхи вдосконалення страхового ринку в Україні……81

Kryshtal G.
Situation of the institutional and evolutionary concept of interaction of the state regulator, banking institutions and real sectors of the economy in modern conditions……82

Підписано до друку 20.06.2018
Формат 60х84/16. Папір офсетний. Друк на дублікаторі.
Умов.-друк. арк. 4,5. Обл.-вид. Арк 4,95.
Тираж 100 прим.

Віддруковано ФО-П Шпак В.Б.
Свідоцтво про державну реєстрацію № 073743
СПП № 465644
Тел. 097 299 38 99, 063 300 86 72
E-mail: tooums@ukr.net