

Міністерство освіти і науки України

Прикарпатський національний університет імені Василя Стефаника
AGH науково-технологічний університет імені Станіслава Сташіца
в Кракові

**КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА СИСТЕМИ УПРАВЛІННЯ**

**Матеріали
міжнародної науково-технічної конференції
молодих вчених, аспірантів та студентів**

**10–12 квітня 2017 року
Івано-Франківськ, Україна**

**COMPUTER SCIENCE, INFORMATION TECHNOLOGIES
AND MANAGEMENT SYSTEMS**

**Proceedings
of the International Scientific Young Scientists Conference**

**2017, April, 10th to 12th
Ivano-Frankivsk, Ukraine**

Івано-Франківськ
Прикарпатський національний університет імені Василя Стефаника
2017

Електронне видання комбінованого
використовування на CD-ROM

УДК 004+005

Наукові редактори: докт. техн. наук, проф. **Л.Б. Петришин** (ПНУ, АГН);
докт. техн. наук, проф. **П. Лебковський** (АГН).

Рецензенти:

д.т.н., проф. **І.Т. Когут**;

д.т.н. **Д. Саля**;

д.т.н., проф. **В. Кубіньски**.

Комп'ютерні науки, інформаційні технології та системи управління : матеріали Міжнародної науково-технічної конференції студентів, аспірантів та молодих вчених, м. Івано-Франківськ, 10–12 квітня 2017 року / наук. ред. Л. Б. Петришин, П. Лебковський. – Електрон. дані. – Івано-Франківськ : Прикарпатський національний університет імені Василя Стефаника, 2017. – 1 електрон. опт. диск (CD-ROM); 12 см. – Назва з тит. екрана.

ISBN 978-966-640-435-3

Збірник містить матеріали статей Міжнародної науково-технічної конференції з проблем комп'ютерних наук, інформаційних технологій, систем управління та ігрового програмного забезпечення.

УДК 004+005

ISBN 978-966-640-435-3

© ПНУ ім. В. Стефаника та автори, 2017

Передмова

Ігор Цепенда¹, Любомир Петришин^{1,2}, Петро Лебковський²

¹Прикарпатський національний університет, Івано-Франківськ, Україна

²AGH University of Science and Technology, Krakow, Poland

l.b.petryshyn@gmail.com

plebkows@zarz.agh.edu.pl

Впровадження інформаційних технологій є ключовим чинником підвищення техніко-економічної ефективності систем управління об'єктами народного господарства. При цьому методи формування, перетворення форми та цифрової обробки повідомлень визначають інтегральну динаміку систем, що зумовлює актуальність здійснення наукових досліджень у вказаному напрямку.

Метою проведення науково-технічної конференції молодих науковців «Комп'ютерні науки, інформаційні технології та системи управління» є обмін передовим досвідом розробки та застосування сучасних інформаційних технологій в системах управління, встановлення міжнародної співпраці між молоддю різних країн, ознайомлення із культурним та національним надбаннями. Конференція організована партнерськими вищими навчальними закладами України – Прикарпатським національним університетом імені Василя Стефаника та Польщі – Науково-технологічним університетом «Гірничо-металургійна академія» імені Станіслава Сташца в Кракові, співпраця між якими здійснюється у рамках міжнародних міжуніверситетських угод, а також угод про спільне навчання студентів рівня магістра. У напрямку наукової співпраці навчальні заклади співпрацюють за проектом Erasmus+ GameHub (561728-EPP-1-2015-1-ES-EPPKA2-SBHE-JP), метою якого є забезпечення зайнятості та самодостатності університетів і випускників коледжів, безробітних інженерів, а також ветеранів АТО в Україні, пропонуючи їм набір знань і навичок, затребуваних в цифровій ігровій індустрії.

Робота конференції організована за чотирма напрямками:

- комп'ютерних наук, в якому представлено результати досліджень безпеки інформаційних технологій, моделювання та цифрової обробки даних;
- інформаційних технологій, в якому запрезентовано мережні технології інфообміну, перетворення форми інформації, алгоритмічного та програмного забезпечення комп'ютеризованих систем;
- систем управління технологічними, організаційними, господарчими об'єктами, а також їх економіко-математичного моделювання;
- ігрового програмного забезпечення, методів розробки та алгоритмізації ігрових аплікацій.

За результатами роботи науково-технічної конференції молодих науковців «Комп'ютерні науки, інформаційні технології та системи управління» прийнято наступні пропозиції:

- відзначено високий науковий рівень презентованих доповідей;
- вирішено продовжити наукові дослідження у визначених напрямках та започаткувати співпрацю науковців, які працюють у суміжних напрямках;
- рекомендовано кращі доповіді до друку у наукових фахових виданнях;
- висловлено подяку організаторам конференції за належний рівень організації;
- рекомендовано проведення конференції в наступні роки з метою продовження співпраці молодих науковців та обміну досвідом.

СЕКЦІЯ 1

Комп'ютерні науки

Computer Science

Wstęp do Kryptografii

Klasyczne techniki kryptograficzne

Algorytmy podstawieniowe

Marek Lewiński

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
lewinski.marek@protonmail.ch

Abstract. Klasyczne techniki kryptograficzne takie jak algorytmy podstawieniowe stanowią podstawę i punkt wyjścia do poznawania nowoczesnych algorytmów kryptograficznych i mechanizmów zabezpieczeń opartych na rozwiązaniach kryptograficznych. Referat ten stanowi przegląd podstawowych algorytmów szyfrujących i pojęć kryptografii klasycznej.

Keywords: Kryptografia, Kryptografia Klasyczna, Szyfrowanie Monoalfabetyczne, Szyfrowanie Polialfabetyczne, Szyfrowanie Podstawieniowe

1 Wstęp

Potrzeba zabezpieczenia przekazywanych i przechowywanych informacji istnieje od momentu opracowania technik jej transmisji – korespondencja dyplomatyczna, raporty wywiadowcze oraz rozkazy dla wojska są przykładami informacji, których ochrona jest kluczowa dla bezpieczeństwa regionów oraz całych krajów. Obecnie rola kryptografii ma jeszcze większe znaczenie – w erze bankowości elektronicznej, tajemnic handlowych, wojny elektronicznej i tym podobnych, kwestia zabezpieczenia danych przybiera na sile. Nasze fundusze nie mogą zostać skradzione przez niepowołaną osobę, a dane medyczne nie powinny trafić do osób trzecich. Projekty tworzone gigantycznymi nakładami wieloletniej pracy nie powinny zostać wykradzione przez konkurencję, a poufne dane i tajne dokumenty związane z bezpieczeństwem narodowym nie mogą trafić w niepowołane ręce. Kryptografia jest obecna w każdej dziedzinie związanej z telekomunikacją i techniką komputerową, ale jej zastosowania nie ograniczają się do ochrony danych w systemach komputerowych – odnoszą się one do ogółu przetwarzanej informacji. Zgodnie z tzw. Kostką McCumbera istnieje potrzeba zapewnienia bezpieczeństwa danych w trakcie ich przesyłania, przetwarzania i przechowywania – głównym środkiem technicznym (który nie powinien być stosowany samodzielnie) jest tutaj zastosowanie algorytmów i technik kryptograficznych. Algorytmy te mają zastosowanie w uwierzytelnianiu

użytkowników, weryfikowaniu autentyczności dokumentów, potwierdzaniu integralności transmisji danych, ukrywaniu faktu istnienia kanału transmisyjnego (steganografia) oraz w zabezpieczeniu wymiany danych.

Referat ten stanowi wprowadzenie do podzbioru klasycznych technik kryptograficznych, czyli do algorytmów podstawieniowych stanowiących jedne z najbardziej elementarnych technik szyfrujących, ale które mogą być wykorzystane do zapewnienia bezpieczeństwa absolutnego.

2 Początki kryptografii

Jednym z pierwszych narzędzi służących do ochrony informacji było tzw. skytale używane przez Spartan – była to laska o określonej grubości, na którą nawijano pasek skóry lub pergaminu. Na tak przygotowanym podłożu nadawca pisał swoją wiadomość, a następnie odwijał pergamin i przekazywał posłańcowi – tylko osoba posiadająca laskę o takiej samej grubości mogła bez większego nakładu pracy odczytać wiadomość. Kluczem szyfrującym w przypadku tego narzędzia była średnica użytej do stworzenia wiadomości laski. Poziom bezpieczeństwa tego mechanizmu pozostawia wiele do życzenia – w celu odczytania wiadomości bez znajomości średnicy wystarczy używać kijów o coraz większych średnicach do momentu odczytania sensownego komunikatu. Znaczącym czynnikiem osłabiającym bezpieczeństwo tego mechanizmu jest również długość wiadomości – w przypadku komunikatu o długości jednej linii wystarczy odczytać kolejne litery z paska.

Pierwszym znanym zastosowaniem techniki podstawieniowej datuje się na czasy Juliusza Cezara – tak zwany Szyfr Cezara jest najprostszym z szyfrów podstawieniowych – każda litera wiadomości jest przesuwana cyklicznie o 3 pozycje do przodu w używanym alfabecie (ostatnie pozycje przechodzą na pierwsze). Używając zapisu arytmetyki modularnej:

$$c_i = (p_i + 3) \bmod 26 . \quad (1)$$

Liczba 26 jest liczbą liter w alfabecie łacińskim, p_i oznacza i -ty znak tekstu jawnego, a c_i – i -ty znak szyfrogramu. Algorytm deszyfrujący otrzymujemy zmieniając znak + na – w powyższym wzorze:

$$p_i = (c_i - 3) \bmod 26 . \quad (2)$$

Szyfr Cezara można uogólnić zamieniając stałą równą 3 dowolną liczbą z zakresu 0-25 (wyższe liczby nie mają sensu, ponieważ w wyniku działania mod 26 redukują się one do zakresu 0-25)

$$c_i = (p_i + k) \bmod 26 . \quad (3)$$

Głównymi wadami szyfru Cezara są:

- bardzo mała przestrzeń dostępnych kluczy (26), która umożliwia efektywne przeprowadzenie ataku siłowego
- brak ukrycia charakterystyki tekstu jawnego – częstotliwość występowania liter zostaje zachowana w szyfrogramie ponieważ każde wystąpienie litery po zaszyfrowaniu tym samym kluczem daje takie samo wystąpienie (innej) litery w szyfrogramie
- brak ukrycia cech językowych – dwuznaków i trójznaków (np. „th” i „the” dla języka angielskiego) – w połączeniu ze statystyką występowania liter w danym języku (znając charakter tekstu jawnego np. język, w którym został on napisany) możemy dzięki temu dedukować kolejne znaki i słowa w szyfrogramie

Przykład tekstu zaszyfrowanego uogólnionym szyfrem Cezara :

Tekst jawny: attack from the north

Klucz: 5

Szyfrogram: fzzfhp kxtr zmj stxzm

W przykładzie widoczna jest możliwość przeprowadzenia kryptoanalizy – poszukujemy w słowniku słowa, które składa się z 4 różnych liter, na pozycji 1 i 4 posiada te same litery, podobnie na pozycji 2 i 3, a następnie na 5 i 6 pozycji ma różne litery – technicznie można takie wyszukiwanie zautomatyzować przy użyciu wyrażeń regularnych.

3 Szyfrowanie monoalfabetyczne

Szyfrowanie monoalfabetyczne polega na zastosowaniu pojedynczego alfabetu kodowego dla całego tekstu jawnego – jednej literze tekstu jawnego odpowiada jedna litera alfabetu kodowego (lub wiele wartości w przypadku stosowania homofonów – na przykład literze „a” mogą odpowiadać wartości 10, 20 oraz 30 w alfabecie kodowym).

Technika szyfrowania monoalfabetycznego drastycznie zwiększa przestrzeń kluczy w stosunku do przestrzeni kluczy Szyfru Cezara. Polega ona na zamianie stałego alfabetu kodowego (przesunięcia liter o stałą będącą kluczem) na dowolną permutację tego alfabetu. Przykładowo:

Tekst jawny : a b c d e f g h i j k l m n o p q r s t u v w x y z

Szyfrogram : e c b a g z u t y w v n m r o s k l d i f h x z j q

Szyfrowanie odbywa się poprzez zamianę litery alfabetu tekstu jawnego odpowiadającą jej literą alfabetu kodowego (przykładowo h zamieniamy na t). Daje nam to $n(n-1)(n-2)\dots(2)(1) = n!$ możliwych kluczy (około 4×10^{26} dla alfabetu łacińskiego).

Specyficzną odmianą tej techniki jest Szyfr Cezara – jest to permutacja cyklicznie przesuwająca alfabet kodowy.

Pomimo dużej przestrzeni kluczy, szyfrowanie to nie jest odporne na ataki wykorzystujące charakterystykę języka – jeśli znamy charakterystykę tekstu jawnego i statystykę występowania liter w danym języku możemy wytypować w szyfrogramie kandydatów do bycia najczęściej występującymi znakami – im dłuższy przechwycony

szyfrogram, tym większe prawdopodobieństwo poprawnego wytypowania. Dodatkowo szyfr ten nie rozprasza dwu- i trójznaków – analogicznie możemy wytypować najczęściej występujące dwu- i trójznaki w danym języku (na przykład „th” i „the”) oraz inne cechy charakterystyczne języka (duplikowanie liter w słowie np. „meet”). Analizując pod tym kątem szyfrogram otrzymujemy zarys wiadomości, który umożliwia dalszą kryptoanalizę przypominającą rozwiązywanie krzyżówki („Jakie słowo zaczyna się na ‘bu’ i kończy na ‘nek’ – budynek).

4 Szyfrowanie polialfabetyczne

Szyfrowanie polialfabetyczne polega na stosowaniu zbioru podstawień monoalfabetycznych. Podstawienia monoalfabetyczne zmieniają się w miarę szyfrowania tekstu jawnego (np. każdy znak szyfrowany jest przy użyciu innego podstawienia), a wybór podstawienia determinowany jest przez klucz wykorzystywany do szyfrowania.

Najbardziej znanym szyfrem polialfabetycznym jest szyfr Vigenere’a, który opiera się na stosowaniu szyfru Cezara dla kolejnych znaków tekstu jawnego przy użyciu kolejnych znaków klucza w oparciu o tzw. tabula recta (tablica utworzona przez Johanna Trithemiusa w 1508 roku). Szyfr ten został opublikowany w 1553 roku.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Rys. 1. Tabula recta

Zakładając, że tekst jawny składa się ze znaków $p_0, p_1, p_2, \dots, p_{n-1}$, a klucz ze znaków $k_0, k_1, k_2, \dots, k_{n-1}$, to ciąg kolejnych znaków szyfrogramu wyrażony jest wzorem:

$$c = c_0 c_1 c_2 \dots c_{n-1} = (p_0 + k_0) \bmod 26 \parallel (p_1 + k_1) \bmod 26 \parallel \dots \parallel (p_{n-1} + k_{n-1}) \bmod 26, \quad (4)$$

gdzie \parallel oznacza konkatencję ciągów.

Proces deszyfracji przebiega w sposób analogiczny do deszyfracji szyfru Cezara poprzez zamianę operacji dodawania znaków klucza na ich odejmowanie.

W przypadku gdy długość klucza jest mniejsza od długości tekstu jawnego stosujemy cykliczne powtórzenie klucza – klucz powtarzamy aż do otrzymania klucza długości równej długości tekstu jawnego (nadmiarową część klucza pomijamy).

Przykładowo :

Tekst jawny :	abcdefghijklmn
Klucz (bez powtórzeń) :	abc
Klucz (z powtórzeniem) :	abcabcabcabc

Przy spełnieniu następujących założeń:

- Długość klucza jest równa długości wiadomości (brak konieczności powtarzania klucza)
- Klucz jest generowany w sposób całkowicie losowy (brak możliwości odgadnięcia klucza)
- Klucz jest używany do zaszyfrowania tylko jednej wiadomości (brak możliwości porównywania kilku różnych szyfrogramów)

otrzymujemy szyfr typu One-Time-Pad (szyfr z kluczem jednorazowym) czyli szyfr nie do złamania (atak siłowy może prowadzić do niejednoznacznych wyników ponieważ pełny przegląd kluczy jest równoważny z pełnym przeglądem zbioru możliwych wiadomości – atakujący może uzyskać zupełnie inny komunikat sprawiający wrażenie poprawnego, ale całkowicie różny od tekstu jawnego). Zostało to udowodnione przez Claude'a Elwooda Shannona 1949.

W przypadku niespełnienia wymogów szyfru OTP, szyfr Vigenere'a posiada podatność umożliwiającą potencjalne złamanie szyfru – jeśli klucz jest wykorzystywany cyklicznie, to dedukując jego długość (znajdujemy w szyfrogramie 2 takie same ciągi – mogą to być te same ciągi zaszyfrowane tym samym kawałkiem klucza w tekście jawnym) można rozłożyć szyfr na ciągi znaków szyfrowanych tym samym kluczem – otrzymujemy n podstawień monoalfabetycznych.

Szyfrów z kluczem jednorazowym jest więcej – przykładowo szyfr Vernamaa ulepszony przez Josepha Mauborgne'a (ulepszenie to wprowadza warunki dla klucza).

Szyfr Vernamaa został opracowany w 1918 roku przez Gilberta Vernama w firmie AT&T. W przeciwieństwie do poprzednich algorytmów nie operuje on na znakach tekstu jawnego, ale na pojedynczych bitach tekstu jawnego oraz klucza. Wyraża się on wzorem

$$c_i = p_i \dot{\wedge} k_i. \quad (5)$$

Różni się on od szyfru Vigenere'a zastosowaniem operacji bitowej XOR w miejscu dodawania znaków.

Szyfry z kluczami jednorazowymi pomimo absolutnego bezpieczeństwa posiadają wady blokujące ich zastosowanie praktyczne :

- Klucz musi być długości wiadomości – przykładowo jeżeli chcemy zaszyfrować dysk o pojemności 1 TB zawierający poufne dane, potrzebujemy do tego celu klucza o rozmiarze 1 TB – problemem staje się przechowywanie go m.in. z powodu konieczności ochrony tego klucza (zwykle jest to ochrona pozakryptograficzna – do zaszyfrowania klucza potrzeba innego klucza)
- Klucze nie mogą się powtarzać i muszą być całkowicie losowe - wykorzystywane w komputerach generatory liczb pseudolosowych nie gwarantują zadanego poziomu losowości – istnieje potencjalna możliwość odtworzenia generatora przez atakującego i wygenerowania odpowiedniego klucza
- Kolejnym problemem jest dystrybucja kluczy – klucz musi zostać dostarczony do odbiorcy transmisji. Dystrybucję kluczy utrudnia w tym przypadku rozmiar klucza oraz konieczność ochrony tego klucza w trakcie transmisji – do przesłania go przez medium transmisyjne potrzebujemy odpowiedniego zabezpieczenia tego medium (np. specjalnie chroniony wojskowy kabel telekomunikacyjny) przykładowo poprzez szyfrowanie transmisji.... ale jak zaszyfrować transmisję klucza? Kolejnym kluczem... i tu powstaje błędne koło.

Metodą dystrybucji klucza dla szyfru OTP jest jego fizyczne dostarczenie do odbiorcy przykładowo przez zaufanego kuriera. Z oczywistych przyczyn szyfr OTP nie nadaje się w takim wypadku do zastosowania w komunikacji rozproszonej, w której systemy łączą się ze sobą dynamicznie. Zastosowaniem szyfru OTP są łącza komunikacyjne o krytycznym stopniu poufności przykładowo linie komunikacyjne pomiędzy głowami państw (tzw. czerwona linia), gdzie dystrybucja klucza odbywa się na drodze dyplomatycznej, a kontakt wymagający pełnego szyfrowania danych jest sporadyczny.

Metodą dystrybucji klucza na potrzeby szyfru OTP (lub szyfrów wymagających kluczy o dużej długości), która może sprawdzić się w praktyce jest kwantowa dystrybucja klucza (wykorzystująca mechanikę kwantową) i technika SKQ (Secret-Key Distillation) wykorzystywana m.in. w algorytmie BB84 (Bennett and Brassard 1984 – Quantum Key Distribution).

Literatura (References)

1. <http://gva.noekeon.org/QCandSKD/QCandSKD-introduction.html>, dostęp 04.03.17
2. „Kryptografia i bezpieczeństwo sieci komputerowych. Matematyka szyfrów i techniki kryptologii. Wydanie V”, William Stallings, wyd. Helion 2012
3. „Kryptografia i bezpieczeństwo sieci komputerowych. Koncepcje i metody bezpiecznej komunikacji. Wydanie V”, William Stallings, wyd. Helion 2012
4. „Podstawy kryptografii. Wydanie III”, Marcin Karbowski, wyd. Helion 2014
5. „Bezpieczeństwo informacyjne”, Krzysztof Liderman, Wydawnictwo Naukowe PWN, Warszawa 2012

Analiza Bezpieczeństwa Routerów

Wojciech Reguła

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
wojciechregula@yahoo.pl

Abstract. Bezpieczeństwo łączącego się z niezaufaną siecią jest zagrożone. Nadal większa część ruchu sieciowego przesyłana jest w postaci nieszyfrowanej z wykorzystaniem przestarzałych protokołów. Ta praca pokazuje jak łatwo atakujący może przejąć kontrolę nad routerem z perspektywy sieci wewnętrznej, czego skutkiem może być np. podsłuchiwanie całego ruchu sieciowego.

Keywords: IT Security, hacking, routers, penetration tests, network security

1 Analiza problemu

1.1 Routery jako pełnoprawne komputery

Routery są obecnie powszechnie stosowanym urządzeniem sieciowym. Z badań przeprowadzonych przez Główny Urząd Statystyczny wynika, że ponad 76% gospodarstw domowych w Polsce ma dostęp do Internetu. Taka statystyka jasno określa ogromną liczbę routerów w Polsce i pokazuje, jak ważnym jest dbanie o bezpieczeństwo urządzenia łączącego z Internetem.

Routery działają zazwyczaj w oparciu o systemy z rodziny BSD (FreeBSD, OpenBSD, NetBSD) lub systemy dedykowane, takie jak np. OpenWRT, Mikrotik RouterOS czy Freesco. Sprawia to, że te urządzenia stają się pełnoprawnymi komputerami narażonymi na różnego typu ataki hakerskie.

1.2 Cel pracy

Celem pracy jest przedstawienie bezpieczeństwa routerów – tj. analiza ich usług sieciowych, panelu administracyjnego oraz powierzchowna analiza ich systemu operacyjnego. W oparciu o te badanie, zostaną sformułowane rady pozwalające użytkownikom sieci zwiększyć swoje bezpieczeństwo.

1.3 Standardowe metody hakowania routerów

Standardową metodą rozpoczynającą analizę routera jest jego rozkręcenie i znalezienie portów debugowania. Następnie, połączenie się poprzez układ scalony UART i skopiowanie całego oprogramowania.

Autor tej pracy nie wykorzysta jednak tego podejścia ze względu na chęć pokazania, że w zdecydowanej większości przypadków wystarczającymi metodami są:

- skanowanie portów za pomocą narzędzia Nmap,
- wykonanie ataku typu brute-force z użyciem oprogramowania Routersploit,
- analiza ruchu sieciowego z wykorzystaniem proxy BURP Suite.

1.4 Spis routerów poddanych analizie

Analizie z wykorzystaniem wyżej opisanych metod zostaną routery:

- Sagem Livebox F@st 3202 TP,
- BlackBox BB54G v2 PoE,
- Netgear JNR1010v2
- TP-Link TL-WR340G,
- Pentagram Cerberus P6351,
- Netgear WN2000RPT.

2 Sagem Livebox F@st 3202 TP

2.1 Panel administracyjny

Urządzenie posiada bardzo ograniczony panel administracyjny pozwalający jedynie na modyfikację parametrów dostępu do Internetu oraz funkcję odłączenia się od sieci (rys. 1).



Rys. 1. Panel administracyjny routera Livebox F@st 3202

2.2 Usługi sieciowe

Wykryto następujące usługi sieciowe:

- Telnet na porcie 23,
- HTTP na porcie 80 (panel administracyjny)

2.3 Próba ataku

Za pomocą narzędzia Routersploit wykonano atak typu brute-force na usługę Telnet. Poniższy rys. 2 zawiera konta uzyskane za pomocą tej metody.

Target	Port	Login	Password
192.168.1.1	23	1234	1234
192.168.1.1	23	1502	1502
192.168.1.1	23	266344	266344
192.168.1.1	23	ADMINISTRATOR	ADMINISTRATOR
192.168.1.1	23	1111	1111
192.168.1.1	23	3comcso	RIP000
192.168.1.1	23	ADMN	admn
192.168.1.1	23	ADVMAIL	HP

Rys. 2. Loginy i hasła do usługi telnet

Po połączeniu za pomocą konta 1234 uzyskano dostęp do wewnętrznego systemu zarządzania routerem. Za jego pomocą można dokonać pełnej kompromitacji routera.

3 BlackBox BB54G v2 PoE

3.1 Panel administracyjny

Urządzenie posiada prosty panel administracyjny z funkcjonalnościami przedstawionymi na rys. 3.

3.2 Usługi sieciowe

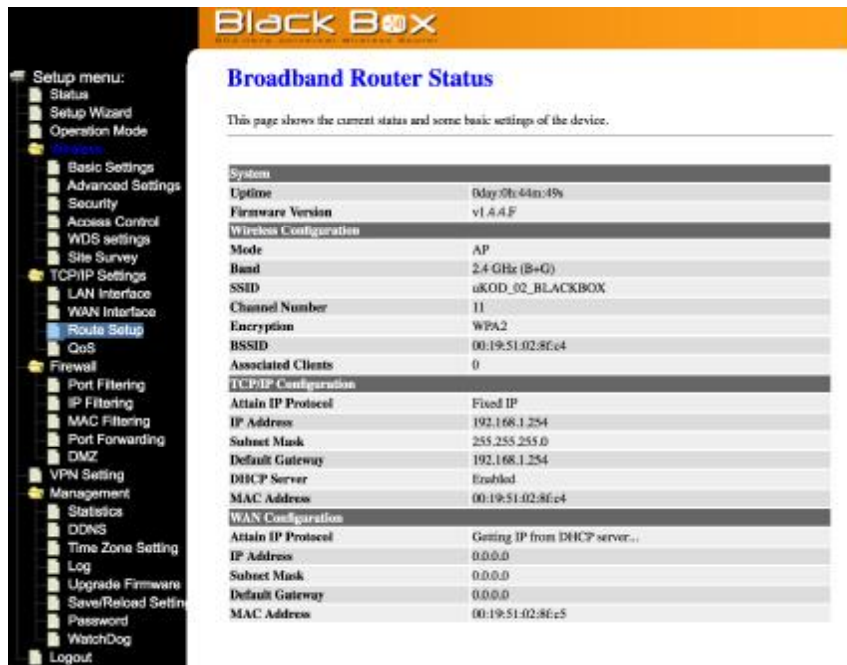
Wykryto następujące usługi sieciowe:

- HTTP na porcie 80 (panel administracyjny).

3.3 Próba ataku

Panel administracyjny działa w oparciu o stary serwer GoAhead posiadający publicznie znane podatności typu Remote Code Execution czy Denial of Service.

Dodatkowo, analiza plików na routerze wykazała obecność interfejsu umożliwiającego wykonywanie dowolnego kodu po stronie powłoki systemowej urządzenia. Na rys. 4 przedstawiono przykład wykorzystania opisywanego interfejsu.



Rys. 3. Panel administracyjny routera BlackBox BB54G v2 PoE

System Command

This page can be used to run target system command.

System Command:

```
root:abSQTpC!skFGc:0:0:root:;/bin/sh
nobody:x:99:99:Nobody:;
```

Rys. 4. Publicznie dostępny interfejs routera

4 Netgear JNR1010v2

4.1 Panel administracyjny

Urządzenie posiada panel administracyjny o funkcjonalnościach przedstawionych na rys. 5.



Rys. 5. Panel administracyjny routera Netgear JNR1010v2

4.2 Usługi sieciowe

Wykryto następujące usługi sieciowe:

- Telnet na porcie 23 (port filtrowany – brak możliwości połączenia),
- Domain na porcie 53,
- HTTP na porcie 80 (panel administracyjny),
- HTTP na porcie 5000,
- UPnP na porcie 56688.

4.3 Próba ataku

Atak rozpoczęto od próby zalogowania do usługi telnet. Niestety, urządzenie nie zezwoliło na takie połączenie. Dzięki opracowaniu przedstawionemu na stronie <https://wiki.openwrt.org/toh/netgear/telnet.console>, pozyskano wiedzę o możliwości

odblokowania atakowanej usługi. Wykorzystując program Telnetable (<http://www.myopenrouter.com/downloads/file/3032/telnetenable-0.4-2.tar.gz>) skutecznie odblokowano dostęp do usługi Telnet. Dzięki temu możliwe było zalogowanie przez Telnet i pełne skompromitowanie urządzenia (rys. 6).

```
MacBook-Pro:telnetenable-0.4 2 r3$ ./telnetenable.osx 10.0.0.1 00C002123588 Gearguy Geardog
MacBook-Pro:telnetenable-0.4 2 r3$ telnet 10.0.0.1
Trying 10.0.0.1...
Connected to www.routerlogin.com.
Escape character is '^]'.
# /bin/busybox
BusyBox v1.12.1 (2015-08-30 13:20:41 CST) multi-call binary
Copyright (C) 1998-2008 Erik Andersen, Rob Landley, Denys Vlasenko
and others. Licensed under GPLv2.
See source distribution for full notice.

Usage: busybox [function] [arguments]...
or: function [arguments]...

BusyBox is a multi-call binary that combines many common Unix
utilities into a single executable. Most people will create a
link to busybox for each function they wish to use and BusyBox
will act like whatever it was invoked as!

Currently defined functions:
[, [[, arp, ash, basename, bunzip2, bzip, cat, chmod, chpasswd,
cp, cut, date, dd, df, dmesg, echo, expr, false, fdisk, free, ftpget,
grep, halt, head, hexdump, hostname, ifconfig, init, init, insmod,
kill, killall, ln, login, ls, lsmod, md5sum, mdev, mkdir, mknod,
more, mount, mv, passwd, pidof, ping, poweroff, ps, pwd, reboot,
renice, rm, rmdir, route, sed, seq, sh, sleep, sync, tail, telnetd,
test, tftp, time, top, touch, tr, traceroute, true, umount, uname,
unzip, vconfig, wc, wget

#
```

Rys. 6. Odblokowywanie usługi Telnet routera za pomocą narzędzia Telnetable

5 TP-Link TL-WR340G

5.1 Panel administracyjny

Urządzenie posiada panel administracyjny o funkcjonalnościach przedstawionych na poniższym rys. 7.

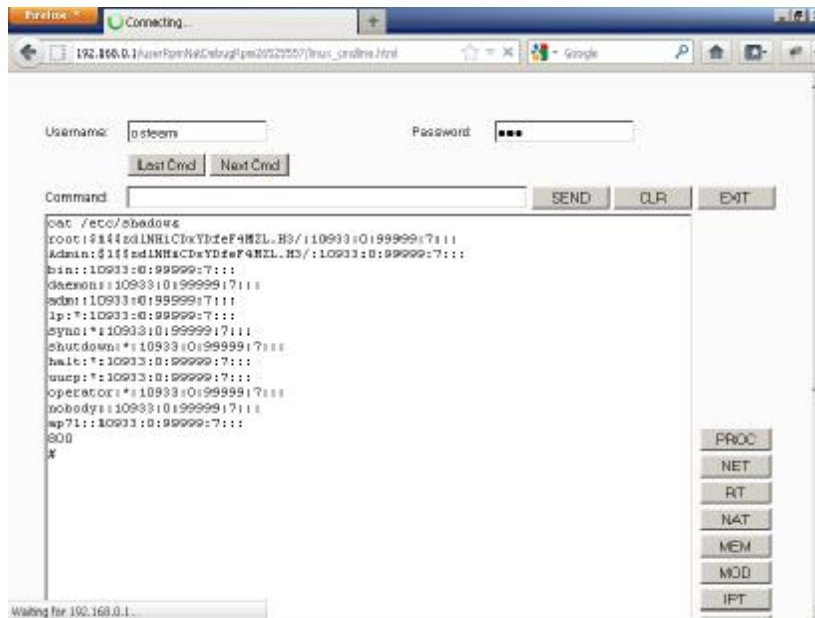


Rys. 7. Panel administracyjny routera TP-Link TL-WR340G

5.2 Usługi sieciowe

Wykryto następujące usługi sieciowe:
HTTP na porcie 80 (panel administracyjny).

5.3 Próba ataku



Rys. 8. Publicznie dostępny interfejs routera TP-Link TL-WR340G. (Źródło: <http://websec.ca/advisories/view/root-shell-tplink-wdr740>)

6 Pentagram Cerberus P6351

6.1 Panel administracyjny

Urządzenie posiada panel administracyjny o funkcjonalnościach przedstawionych na rys. 9.

PENTAGRAM Cerberus P 6351

Status

This page shows the current status and some basic settings of the device.

System	
Alias Name	PENTAGRAM Cerberus P 6351
Uptime	7 min
Firmware Version	2.3.0
Customer Version	RNR4-AD-4X32H_uc2660409_PEN_02_101122
DSP Version	2.9.0.72
Name Servers	
Default Gateway	

WAN	
Operational Status	ACTIVATING
Upstream Speed	0 kbps
Downstream Speed	0 kbps

LAN Configuration	
IP Address	192.168.1.100
Subnet Mask	255.255.255.0
DHCP Server	Enabled
MAC Address	0513339c7eb5

WAN Configuration						
Interface	VPI/VCI	Encap	Protocol	IP Address	Gateway	Status
ppp0_vcd	0/35	LLC	PPPoE			down / Disc / Disc

Refresh

Rys. 9. Panel administracyjny routera Pentagram Cerberus P 6351

6.2 Usługi sieciowe

Wykryto następujące usługi sieciowe:

- FTP na porcie 21,
- Telnet na porcie 23,
- HTTP na porcie 80 (panel administracyjny),
- HTTP na porcie 18182,
- UPnP na porcie 54616.

6.3 Próba ataku

Analiza plików znajdujących się na serwerze wystawionym przez router na porcie 80 wykazała, że pod adresem <http://192.168.1.100/syscmd.asp> znajduje się interfejs pozwalający na wykonanie dowolnej komendy po stronie routera. Poniżej przedstawiono zdjęcie (rys. 10) zawierające wykorzystanie strony do wyciągnięcia zawartości pliku /etc/passwd.



Rys. 10. Interfejs routera dostępny po zalogowaniu za pomocą konta administratora

Następnie złamano hasze zawarte w pliku otrzymując następujące rezultaty (rys. 11).

	User	Password	Hash
1	<input checked="" type="checkbox"/> admin	ukod	\$1\$\$IGZO8p7gtv8Z...
2	<input checked="" type="checkbox"/> adsl	realtek	\$1\$\$m9g7v7tSyWPY...
3	<input checked="" type="checkbox"/> user	user	\$1\$\$ex9cQFo.PV11e...

Rys. 11. Konta użytkowników i ich złamane hasze

Konto admin posiada hasło zmienione w panelu administracyjnym. Pozostali użytkownicy nie są widoczni w panelu administracyjnym – są wgrani na sztywno i mogą posłużyć jako tzw. „tylna furka”.

Wszyscy użytkownicy jako domyślną powłokę mają ustawioną /bin/cli. Z tego powodu, połączenie przez telnet nie umożliwi w dalszym ciągu pełnej kontroli routera. Zdecydowano się więc na wgranie przez FTP (wykorzystując konto adsl:realtek) zmodyfikowanego pliku /etc/passwd.

Następnie zalogowano się przez telnet doprowadzając do pełnej kompromitacji routera (rys. 13).

```
BusyBox Built-in shell (msh)
Enter 'help' for a list of built-in commands.

#
```

Rys. 13. Poprawne zalogowanie do routera przez usługę Telnet

7 Netgear WN2000RPT

7.1 Panel administracyjny

Urządzenie posiada panel administracyjny z funkcjonalnościami przedstawionymi na rys. 14.



Rys. 14. Panel administracyjny routera Netgear WN2000RPT

7.2 Usługi sieciowe

Wykryto następujące usługi sieciowe:

- HTTP na porcie 80 (panel administracyjny),
- Niezidentyfikowana usługa na porcie 3333.

7.3 Próba ataku

Podczas analizy plików natrafiono na logi routera, które zawierają między innymi login i hasło do panelu administracyjnego (rys. 15).



```
Request
Raw Headers Hex
GET /cgi-bin/WNR2000KT_log HTTP/1.1
Host: www.mywifi.net
Connection: close

Response
Raw Headers Hex
HTTP/1.0 200 OK
Date: Sat, 01 Jan 2006 00:57:27 GMT
Server: BSA/0.94.11
Cache-Control: no-cache
Pragma: no-cache
Expires: 0
Connection: close
Content-type: application/download

Admin login name      admin
Admin password       password
Country Europe
Wireless network name (SSID)  uE0C_04_SetgearRepeater
Wireless channel      11
Security type         WPA-PSK(TKIP) + WPA2-PSK(AES)
Wireless passphrase   h6ckwa1!
```

Rys. 15. Żądanie i odpowiedź HTTP prezentujące pobranie logów routera

Za ich pomocą możemy zalogować się do panelu administracyjnego urządzenia i przejąć nad nim kontrolę.

8 Podsumowanie wyników analizy

8.1 Porównanie zabezpieczeń routerów

Na podstawie przeanalizowanej próbki stwierdzono, że bezpieczeństwo routerów z perspektywy sieci wewnętrznej jest niewystarczające. Każde z opisywanych urządzeń posiadało przynajmniej jedną lukę bezpieczeństwa, mogącą skutkować jego kompromitacją. Routery miały wystawione do sieci wewnętrznej różne usługi, które stawały się jednocześnie kolejnymi wektorami ataku. Wniosek płynący z porównania zabezpieczeń może być następujący – im więcej wystawionych usług, tym więcej potencjalnych podatności.

8.2 Zwiększenie bezpieczeństwa routerów

W punkcie 3.1 został przedstawiony wniosek, z którego jednoznacznie wynika, że należy wyłączyć wszystkie niepotrzebne usługi uruchomione na urządzeniach. Jak

pokazał przykład routera TP-Link TL-WR340G – aktualizacja oprogramowania przyczyniła się do zwiększenia bezpieczeństwa (autorowi nie udało się odnaleźć żadnych podatności krytycznych po aktualizacji urządzenia). Należy więc stale aktualizować oprogramowanie routerów.

8.3 Bezpieczne połączenie z niezaufaną siecią

Na podstawie powyższej analizy można stwierdzić, że bezpieczeństwo routerów pozostawia wiele do życzenia. Kompromitacja routera może skutkować np. przejęciem poufnych informacji czy atakami hakerskimi na inne urządzenia. Z tego powodu należy sprawdzać czy sieć, z którą się łączymy jest bezpieczna. Jeśli nie mamy takiej pewności, autor tej analizy zaleca łączenie się poprzez Wirtualną Prywatną Sieć (VPN).

Watch Out! – Mobile Application Threats

Paweł Kuryłowicz

AGH University of Science and Technology, Cracow, Poland
pawel.kurylowicz95@gmail.com

Abstract. Firstly, I want to tell an anecdote from my life as a student. It is about a flashlight android application, which demands too many privileges. This story will shine some light on that problem of how malware and unsecured applications affect all of us in everyday life. People have to understand how big the problem is and to be aware. From that point I will move to aspects like who wants to break into mobile applications and why they do that. Subsequently I will show the methodology of android application penetration testing.

Keywords: Application, Security, Vulnerability, Threats, Aware, Penetration test, Methodology, Malware, Tinder, Facebook

1 Why we should be aware

1.1 Defining the problem

Nowadays people are extremely dependent on mobile applications. Mobile phones can provide a single point of access to their personal information like financial data, medical records, photos as well as work-related email, documents or professional resources. They do not pay attention to what they are downloading to their devices. A great example here will be Facebook which was recording us anonymously through phone microphone for about month before someone discovered it. Slowly most of us are getting used to sharing privacy, but today's problem is with whom we are sharing it.

1.2 Who is threatening us - “Black Hats”

There is a huge amount of applications with malware and even more of those which are unsecured. We need to realize that using mobile applications without caution is a real threat. Who wants our data? Who can get some benefits from that? Those people in our industry are called "Black Hats". There are three types of “Black Hats”. The first are people who have no idea what they are doing but as long as they get some benefits they won't stop. The second type is popularly named "Script Kiddie". This type just knows the basics. They are using prepared tools for massive blind attacks. As a result, they rarely get what they want. The third and the most dangerous type is a sophisticated hacker. This guy has deep knowledge and understanding in IT Security and they know exactly what to do to take control over your phone and data which is

hidden inside. Why do they do that? Most of them are doing this for money, but there are a bunch of people who are doing this for satisfaction, getting information, some kind of influence or just for fun.

1.3 Who protects us - “White Hats”

But it is not as bad as it looks like. Opposite of "black hats" there are the "white hats". Ethical hackers with great responsibility for keeping all of us safe. They are doing almost the same things but in good faith. I am one of them and I want to show how process of mobile application testing looks like. It will expose places where people are making mistakes and maybe will help to prevent from future vulnerabilities.

2 Methodology of Mobile Application Testing

2.1 Information gathering

Firstly, we have to get to know with the application. By checking basic functionalities, we have got a great view for a tested environment. After that part, we are able to start thinking about threats which can result from used functions. Again, we have to ask ourselves questions; Who? Why? How? Applications used in banking will have different potential threats than in social media. In the first case, critical risk would be a waste of money and for application like Facebook a greater threat would be waste of data.

2.2 Static analysis

When we passed through the first step and we know what the potential risks are we can move to static analysis. Basically, it starts from getting apk package. We can find it at www.apkpure.com if application is available at Google Play store or pull it from phone by command `adb pull /data/app/NameOfApplication`. When we have got the package, we need to decode and unpack it. In this step, there is a helpful tool called “APK TOOL”, which will do it all for us. Afterwards we will convert .dex files into .jar by “dex2jar” to get java archives and finally thanks to “JD GUI” we will get the java source code. It will help to understand application functionalities and perhaps identify implementation mistakes or find comments left by the developers. From more interesting things for attacker there are also often tokens, keys or passwords.

2.3 Dynamic analysis

After static analysis, we move to dynamic. In this part, we are checking what is stored inside application logs and how it communicates with the server or how it interacts with other active processes. By setting a proxy we are able to see the whole traffic between mobile application and the server. We are looking at requests through differ-

ent functionalities and we are trying to modify them in an unplanned way to get unexpected results.

2.4 Real example – Tinder

A lot of people use Tinder. It is android mobile application dedicated for singles to find a partner or a friend. There are three basic functionalities “Like”, “Dislike” and “Super Like”. After matching we are able to chat with potential friend. Through Tinder by default we are sharing information’s such as school/job, age from Facebook profile and distance between us and our matched partner. Normally it should be safe because even if we have this information, we do not know where the person is exactly without the specified direction. Unfortunately, there is a way to get around that. If we will look closer at the communication between the server and the mobile application, we will find a HTTP request which sends our geographical coordinates. Server based on that creates a response with an information of how far is our partner. As an attacker, someone can modify his request and then he will know how far is someone from another location. If he will do that at least two times there will be a possibility to track down the victim. How? By creating three circles with victim’s distance as radius from various places. These circles intersect exactly at one point Going further by continuously sending requests he can even track her live without her knowledge.

3 Stay aware

Attackers can use this information for example to rob our homes when we are far away and it is not the only one possible case of the use. Everyone is trying to stay safe through life and nobody wants to share his privacy with criminals. But if we look closer to how we treat things stored on our mobiles like correspondence, files or photos, then the problem is really easy to discover. Even applications that seem to be useful but demand a lot privileges, we should reconsider if we really need them. These applications do not have to have malware. It can just be unsecured and dangerous by default. So if we don't want to be robbed, or lose privacy, we have to check application or at least its source before installing it.

References

1. Florian Stahl, Johannes Ströher.: Security Testing Guidelines for mobile Apps. https://www.owasp.org/images/0/04/Security_Testing_Guidelines_for_mobile_Apps_-_Florian_Stahl%2BJohannes_Stroeher.pdf
2. OWASP Mobile Security Project. https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
3. Łukasz Bobrek.: Testowanie bezpieczeństwa aplikacji dedykowanych na platformę Android. <https://www.slideshare.net/wojtwo/testowanie-bezpieczestwa-aplikacji-dedykowanych-na-platform-android>
4. Sławomir Jasek.: Testowanie bezpieczeństwa aplikacji mobilnych. <https://www.slideshare.net/wojtwo/testowanie-bezpieczestwa-aplikacji-mobilnych>

Firewalls in Contemporary Networks

Michał Ogorzałek

AGH University of Science and Technology, Cracow, Poland
michalogorzalek5@gmail.com

Abstract. Nowadays, every organization is connected to the Internet and thereby is exposed to various threats. For years, people have been creating different devices that can protect networks. However with every change in defense, a new way of attack emerges. This paper is an introduction to various devices and approaches to network security. It considers the evolution of the Internet, web applications and securing devices, trying to find the best way of protecting networks.

Keywords: Firewalls, Network security, Next-Generation Firewall

1 Introduction

By being connected the Internet, network becomes vulnerable to hackers who try to access your financial and personal information. If you have a web application, it is likely that it has flaws. If you have workers in your company, you can be sure at least one of them will connect to a malicious website. Sometimes, a small flaw can make you lose a lot of money, so it is important to secure from various threats as well as possible.

There is a solution for our concerns, called a firewall. The firewall is a network security system that uses rules to control incoming and outgoing network traffic. It acts as a barrier between a trusted (internal) network and an untrusted network – the Internet.

Firewalls occur either as hardware devices – physical box with multiple ports, or as software that can be installed on a single computer.

2 Types of devices

Looking into the history of firewalls, we can observe different generations of firewalls.

2.1 Static Packet Filtering Firewalls

The network security began with packet filtering firewalls which have functionalities that all contemporary routers have. They allow to make a decision if a packet should be dropped or forwarded basing on protocol, port numbers and IP addresses.

2.2 Stateful Packet Filtering Firewalls

The next type of firewall is called stateful firewall. These devices are called so, because they monitor and maintain the state of active connections to, and from the network. Decision of forwarding a packet is based not only on rules regarding content of packets, but also on the fact whether the packet is part of an existing session. Obviously, packets of connected users (and packets to help initiate a new authorized sessions) are trusted as opposed to others [4].

2.3 Application Firewall

Application firewall is the next type of firewall and as the name says, it operates at the application layer of protocol stack. It acts as a proxy server and can inspect not only headers but also the contents of traffic. Working on the highest layer of OSI model means that firewall processes the whole traffic like end-user. It reads every header, decompresses, decodes and decrypts data if needed to get to know what this data is about to do. After that, firewall does it in reverse sequence and sends to end-user. It is a lot to do, however, this is the only way to ensure that device understands applications and protocols (such as HTTP, FTP, DNS). For example, we can set a rule to deny request on port 80 where one of the parameters contains words like 'select' or 'from'. Such situation indicates an SQL attack and even if the web application is vulnerable, the attack will not succeed. This kind of traffic (HTTP) can be handled by a special and very popular version of application layer firewall – WAF (Web Application Firewall).

2.4 Intrusion Detection/Prevention System

Another useful device is IDS/IPS (Intrusion Detection/Prevention System) that detects attacks focused on vulnerabilities that exist in systems and applications. IDS only alerts us about detection, whereas IPS actively blocks detected attacks. These devices monitor network traffic and compares byte sequences with pre-determined attack patterns known as signatures – similarly to anti-virus software. They also check if the traffic is "normal". It means IDS/IPS inspects the current traffic and protocols and compares them to the generally used ones. If they differ significantly, it can raise an alarm [3].

3 The place of firewalls in the network

The placement of a firewall depends on several subjective factors and there is no single strategy perfect for every organization. Nevertheless, there are general rules that should be followed. Firstly, we need to understand the structure of our network. As was mentioned at the beginning, firewall separate our internal network from the insecure Internet. However, in most cases, there is a need for creating an additional area called DMZ (Demilitarized Zone). This zone is placed between aforementioned areas

and its purpose is to add an extra layer of security to the internal network. It is useful when an organization provides services to users from an external network and they should access only what is exposed in the DMZ (for instance web, mail, ftp servers). These services can communicate with the internal network. For example, a web application to access a database server. However, traffic generated from DMZ can not be trusted. If our application has flaws, it can be compromised and thereby attacker can have control over it.

There are many complex ways to design a network with a DMZ. Two simplest examples of them are shown in fig. 1 and 2. The network from figure 2 is more expensive. However, it is considered more secure since two devices need to be compromised to get to the internal network. We can also purchase firewalls provided by two different vendors to increase security even more, since it is less likely that both devices suffer from the same vulnerabilities. Firewalls often work beside IPS/IDS. Since Intrusion Detection System only detects attacks and does not ensure real-time protection, we place it out-of-band. It means that the system works separately and data is sent to the device over an independent path. Intrusion Prevention Systems should be implemented inline instead, which means that all the traffic goes over the same path. This solution ensures real-time protection, however, causes additional delay and in case of failure the whole network is down [2, 3].

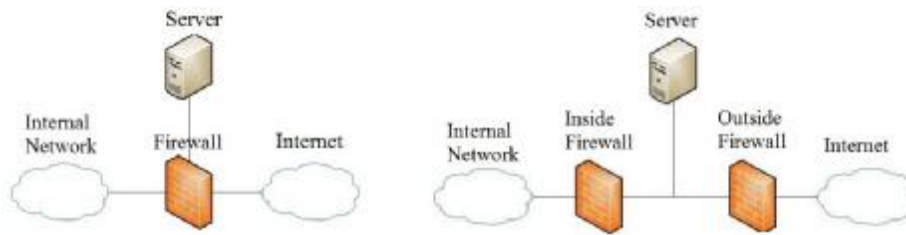


Fig. 1. Network with a single firewall DMZ

Fig. 2. Network with a dual firewall DMZ

4 The contemporary Internet

A part of currently deployed firewalls are still packet filter or stateful inspection firewalls. These devices are popular since they are low-cost and simple to operate. However, they inspect only a few bytes of headers to determine what is application protocol. This is one of the reasons why the Internet is nowadays full of 'new generation applications'. Because most of basic firewalls allow to forward traffic at least on port 80 or 443, these applications use various techniques to "be allowed" by rules and enhance their accessibility. For instance, they are designed to use nonstandard ports or tunnel data within other services (this method is also used during attacks). There are also protective technique such as port hopping which enforce random port changes during transmission or using encrypted connections on port 443. It all makes the internet unpredictable and causes that firewalls from the last century, are not even able to identify what kind of data is transmitted [1].

Over time, network security has been refined. At first, companies were adding more various devices to networks, trying to compensate deficiencies in firewalls. This approach however, results in latency and necessity to monitor and manage every single appliance separately. Packets passed from device to device are examined several times to determine whether they should be allowed into the network. We are living in times when performance is so important that we do not want to accept that.

The next step was combining these all devices into a single platform called unified threat management (UTM). Having all helpers in one physical package allows us to manage only one device examining packets in many ways. However, this approach still does not resolve the problem of additional latency. UTMs are like putting many devices in one box. They use separate internal engines to perform individual security functions and packets are tested several times anyway [6].

5 Next-Generation Firewall

The solution for our concerns is a next-generation firewall. It is a network security system combining a traditional firewall with other network devices filtering functionalities such as an application firewall using deep packet inspection, an IPS or other techniques.

Similarly to an UTM device, the lack of necessity for numerous stand-alone products results in reducing complexity of the network and administration as well as lower capital cost. However, by contrast to UTM, NGFW not only combine, but also integrate these functionalities. It means that repetitive handling of packets is eliminated and the performance problem is minimized [1, 6].

Enumerating features of next-generation firewall we begin with identifying applications that device runs, regardless of port, protocol and IP address. If, for example, there is a tunnel to hide the actual application, it will be detected and a real one will be identified anyway. If an administrator do not want user to use Facebook video conversation, he can block it, still allowing the use of Facebook chat [5]. This advanced platform understands the logic of application, which allows to provide protection against various threats and not only that. He can manage bandwidth and limit the use of application that we defined as less important (e.g. Youtube, Facebook). NGFW also gives control of network activity by its user identification technology that links an IP address to specific user and regularly verifies these relationships. Communicating with LDAP directories, gives visibility into who specifically is responsible for particular traffic. It gathers important user information, such as roles and groups and in that way, allows to better control the use of applications. The next technology is content identification which enables to analyze content that users try to download from or sent to the Internet. It is very dependent upon functionalities that particular platform provides such as IPS, antivirus, anti-spam or anti-bot. Part of NGFWs is even able to provide detection and prevention of zero-day malware. They can place downloaded file in a sandbox, analyze it and if it is malicious, generate new signatures that become available for other firewalls via cloud. NGFWs have many features and thus, can provide comprehensive protection [1, 8].

After identifications, the device makes decisions. However, they are more detailed than simply forwarding or dropping. We can apply more appropriate policies for various types of traffic. For example, all the data to one particular user scan for exploits and prevent transferring some types of files to another ones [1].

6 Security devices market

Contemporary networks are protected by different devices, however, next-generation firewalls are believed to be efficient and effective and thus become more and more popular. They are created to do everything what traditional firewalls do with the addition of advanced capabilities. By enhancing visibility and control, they allow organizations to focus on more business-relevant elements and it could seem that it is a matter of time when they displace other devices. Nevertheless, vendors of these devices try to convince consumers that general NGFW is not able to work as good as their dedicated products.

It is a truth that NGFWs allow us to create detailed web application rules, it is also not a lie that they have web gateway features. However, we should remember that NGFWs are not intended to be a replacement for neither WAFs nor Web Secure Gateways. Vendors of dedicated devices constantly indicate why their appliances are worth deploying with NGWF solutions and listening to their arguments it is hard to deny them [5, 8].

Disregarding all the features, NGFWs owe their popularity and opinion to vendors, that create many materials, articles and books to pitch their products. Part of analysts claimed even that they are basically UTMs and vendors simply created new definition. Anyway, the marketing has been extremely effective and nowadays, the world market is filled with devices called Next-Generation Firewalls [7,8].

7 Conclusions

Next-Generation Firewalls undoubtedly have significant meaning for enterprises and organizations, though the choice of devices that secure our network is not a trivial task. It seems that it is a good idea to apply NGFW to our network, however, we need to consider various scenarios and decide whether we want it to be replacement for our IPS, firewall or all other devices. Still, there is no one, perfect solution and as always, the decision belongs to people who need to strike a balance between convenience, performance, price and security.

References

1. J. Michael Stewart, *Network Security, Firewalls, and VPNs*, Jones & Barlett Learning, 2010
2. Robert J. Shimonski, *The Best Damn Firewall Book Period*, Syngress Publishing, 2003
3. Hira Sathu, *Free and open source intrusion detection systems: a study*, IEEE, 2015

4. Lawrence C. Miller, *Next-Generation Firewalls for dummies*, 2nd. ed., John Wiley & Sons, Inc., 2016
5. *Why you need more than a Next Generation or Application Aware Firewall to protect your applications*, Fortinet 2014
6. Troy McMillan, *CompTIA Advanced Security Practitioner (CASP) CAS-002 Cert Guide*, Pearson Education, 2015
7. Brandan Blevins, *Next-generation firewall comparisons show no product is perfect*, techtarget.com, 2014
8. Diana Kelley, *NGFW: Getting clarity on next-gen firewall features*, techtarget.com, 2012

Maglev, czyli Najszybsza Kolej Świata

Konrad Marszałek

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
konradmarszalek10@interia.pl

Abstract. „Maglev, czyli najszybsza kolej świata” to krótka praca, mająca na celu przybliżenie idei kolei magnetycznej, ukazanie tego jak działa i dlaczego nie podbiła jeszcze świata. Pomysł, który narodził się w głowach ludzi już w latach 30. XX w. przeszedł długą drogę by uformować się w obecnie nam znaną koncepcję. Staram się pokazać jak to wszystko zmieniało się przez lata oraz jak wygląda teraz, pokazuję różnice między niemiecką technologią Transrapid a tradycyjną Maglev oraz prezentuję imponujące dokonania inżynierów z Japonii, jakimi niewątpliwie są plany stworzenia superszybkiej linii Chuo Shinkansen na odcinku Tokio- Osaka.

Keywords: Maglev; Kolej magnetyczna; Technologia; Pociąg; Transport; Transrapid; Lewitacja;

1 Czym jest Maglev?

Maglev, czyli inaczej kolej magnetyczna to nowoczesna technologia transportowa, wykorzystująca elektromagnesy do przemieszczania się pociągu bez styku z torowiskiem (pociąg unosi się nad nim). Dzięki temu jedyny opór jaki maszyna musi pokonać to opór powietrza (tarcie powierzchniowe jest wyeliminowane) co z kolei pozwala na rozwinięcie bardzo dużych prędkości, sięgających nawet 500 km/h. W pojeździe nie ma żadnego silnika, przemieszcza się on tylko i wyłącznie poprzez powstałe pole magnetyczne. Technologia ta jest obecnie rozwijana jedynie na Dalekim Wschodzie- w Chinach i Japonii.

2 Krótka historia

Pierwsze plany budowy kolei magnetycznej powstały już w latach 30. XX w. w Niemczech. Nie zostały jednak zrealizowane przez brak odpowiednich technologii i wybuch II wojny światowej. Po niemieckich naukowcach ideę przejął brytyjski profesor Eric Laithwaite, który w latach 60. opracował projekt o nazwie Tracked Hovercraft. Zakładał on połączenie technologii silnika liniowego indukcyjnego z poduszkowcem. Równoległe we Francji rozwijano bardzo podobny system, zwany Aerotrain. Na początku wyniki były bardzo obiecujące, Francuzi wybudowali nawet 18-kilometrowy odcinek trasy Aerotrain, na którym pojazd rozpedził się do 417 km/h. Laithwaite zaś opracował nowatorski układ magnesów umożliwiający pojedynczemu

silnikowi unoszenie i przemieszczanie pojazdu. Ostatecznie oba projekty uznano za zbyt kosztowne i nieperspektywiczne i zaniechano w latach 70.

W 1984 r. nastąpiło pierwsze komercyjne wykorzystanie technologii Magleva, przy lotnisku w Birmingham uruchomiono 600-metrową trasę, na której pociągi nie osiągały jednak dużych prędkości i unosiły się ok. 15 mm nad prowadnicą. W Niemczech z kolei rozwinięto nieco inną technologię- Transrapid, którą zastosowano pierwszy raz na 31- kilometrowym torze próbnym w Emsland. Podczas jazd testowych rozpędzano pociąg nawet do 420 km/h. Zaczęto również przeprowadzać kursy demonstracyjne dla turystów. Wszystko skończyło się w roku 2006, kiedy to z winy operatora maszyna rozbiła się, a śmierć poniosły 23 osoby. W 2011 roku tor zamknięto i rozebrano. Ponadto w Berlinie przez 2 lata (1989-1991) działała magnetyczna kolej miejska M-Bahn, której trasa wynosiła 1,6 km. Po reunifikacji miasta połączenie uznano za zbędne i zlikwidowano.

Technologię kolei magnetycznej rozwijano jednak nie tylko w Europie. Od końca lat 60. również Japończycy zaczęli ją wdrażać w swoim kraju. W latach 70. w prefekturze Miyazaki powstał 7-kilometrowy odcinek testowy, będący załącznikiem wielkiego projektu, jakim bez wątpienia jest Chuo Shinkansen.

3 Chuo Shinkansen, czyli szybciej już się nie da

W 1997 r. w prefekturze Yamanashi do użytku mieszkańców został oddany 18-kilometrowy odcinek kolei maglev, na którym pociągi mogły rozpędzać się do 500 km/h. W 2013 roku rozbudowano go do prawie 43 km. Obecnie trasa ta jest zamknięta, gdyż trwają prace nad największym projektem w historii kolei magnetycznych, jakim jest Chuo Shinkansen, którego ma być częścią. Jest to trasa mająca łączyć Tokio z Nagoją, a w dalszej przyszłości planuje się również dołączenie Osaki. 286- kilometrowa trasa, w budowie od 2014 roku, ma być pokonywana w 40 minut z maksymalną prędkością 505 km/h (obecnie czas podróży „tradycyjnym” Shinkansenem to 88 minut). Ponad 86% trasy ma znajdować się pod ziemią, co generuje olbrzymie koszty, obecnie szacowane na 40 mld Euro. 20 grudnia 2015 roku ruszyła budowa 25 km tunelu przebiegającego pod Japońskimi Alpami, a jej planowane zakończenie jest przewidziane na 2025 rok. Cały odcinek Tokio-Nagoja ma być otwarty w 2027 roku, zaś odcinek Nagoja-Osaka w 2045 roku.



Rys. 1. Planowany przebieg trasy Chuo Shinkansen (źródło: Wikipedia).

Ciekawostką jest fakt, że w roku 2015 na rozbudowanym odcinku testowym w prefekturze Yamanashi (na mapie oznaczony kolorem czerwonym) osiągnięto światowy rekord prędkości pociągu- 603 km/h.

4 Obecnie funkcjonujące linie kolei magnetycznych

Na chwilę obecną, na całym świecie działają 4 otwarte linie komercyjne kolei magnetycznych:

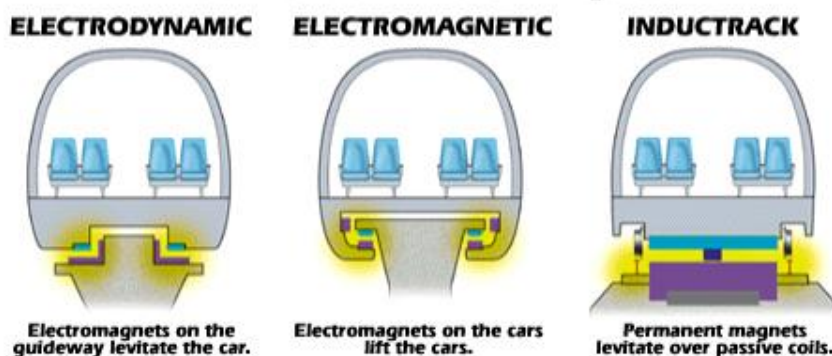
- Linimo, 9-kilometrowa trasa w Japonii w prefekturze Aichi, powstała na potrzeby Expo w 2005 roku; była to pierwsza w pełni automatyczna i bezobsługowa kolej magnetyczna na świecie; pojazdy służą lokalnej społeczności, przewożąc rocznie ok. 9 milionów pasażerów; pociąg nie należy do najszybszych, porusza się z maks. prędkością 105 km/h;
- Shanghai Maglev Train, 30,5- kilometrowa trasa zbudowana w Szanghaju przez niemieckie przedsiębiorstwo Transrapid International z zastosowaniem rodzimej technologii Transrapid; jest obecnie jedyną linią kolei magnetycznych dużych prędkości na świecie- pociągi poruszają się na niej z prędkością nawet 431 km/h, a czas przejazdu wynosi 8 minut;
- Maglev w Incheon w Korei Południowej, jest to bezobsługowy system otwarty w 2016 roku na lotnisku w Incheon; linia ma długość 6,1 km, jednak w planach jest jej rozbudowa o kolejne 2 odcinki, łączące port lotniczy z resztą miasta;
- Maglev w Changsha w Chinach; odcinek o długości 18,55 km łączy dworzec kolei dużych prędkości z lotniskiem i został otwarty w 2016 roku.

5 Maglev a Transrapid, czyli nie do końca to samo

Właściwie określenie „Maglev” nie jest zbyt precyzyjne, dotyczy bowiem tak naprawdę tylko jednej z 2 obecnie używanych technologii w kolei magnetycznej. Maglev to zwyczajowe określenie pociągów, w których stosuje się technologię EDS (technologia unoszenia elektrodynamicznego), którą w obecnej formie stworzyli i zastosowali po raz pierwszy Japończycy. Zakłada ona unoszenie się pojazdu na wysokości do kilkunastu centymetrów poprzez wzajemne odpychanie się elektromagnesów. Jednakże podczas rozpędzania i hamowania, gdy pociąg nie osiąga zbyt dużych prędkości konieczne jest zastosowanie dodatkowych kół, na których maszyna może oprzeć część swojego ciężaru. Jest to spowodowane zbyt małą siłą indukującą się przez pole elektromagnetyczne, która nie mogłaby utrzymać pociągu w torze. Elektromagnesy wykonywane są z nadprzewodników.

Transrapid to opracowana w Niemczech technologia unoszenia przez przyciąganie magnetyczne (EMS). Podwozie pociągu jest ukształtowane w taki sposób, by sięgać pod tor i jest do niego przyciągane, co unosi cały pociąg. Odległość między maszyną a torem jest tutaj bardzo mała i wymaga stałej kontroli podczas jazdy. W przeciwieństwie do EDS nie trzeba jednak instalować dodatkowych kół podtrzymujących.

Levitation Techniques



Rys. 2. Schemat działania technologii EDS, EMS i Inductrack, rozwijanej z myślą o statkach kosmicznych (źródło: www.propelsteps.wordpress.com)

6 Krytyka

Skoro więc mamy do czynienia z tak dobrą i niezawodną technologią, dlaczego nie możemy poruszać się Maglevami po całym świecie?

Pierwszą podstawową kwestią są ogromne koszty budowy infrastruktury i eksploatacji (francuskie linie TGV czy japońskie Shinkanseny są kilkukrotnie tańsze w budowie niż Maglevy, a również bardzo szybkie i nowoczesne). Koleje magnetyczne po prostu nie mają aż tak miażdżącej przewagi nad kolejami tradycyjnymi, by opłacalne było ich wprowadzenie. Analizy fachowców wykazują, że dochody uzyskiwane ze sprzedaży biletów po akceptowalnych cenach nie pozwalają na zwrot inwestycji nawet przez cały cykl życia produktu (ok. 40 lat). Niestety przy obecnie niewielkim zainteresowaniu budową nowych linii kolei magnetycznych na świecie (na ten moment powstaje jedynie Chuo Shinkansen w Japonii oraz jedna linia w Chinach) nie należy się spodziewać by w następnych kilkunastu latach technologia ta staniała. A szkoda, bo pociągi te są niezwykle przyjazne dla środowiska, ich bezemisyjność oraz niewytwarzanie hałasu podczas jazdy są ogromnym atutem. Poza tym, kto nie chciał by się przejechać lewitującym pociągiem?

Bibliografia (References)

1. Długa historia Magleva, www.transport-publiczny.pl
2. Lewitujące pociągi. Jak działa maglev? www.gadzetomania.pl
3. Maglev, ww.wikipedia.org
4. Japan's magnetic levitation train | Linimo, www.youtube.com
5. Tanel F.: Historia kolei. Od lokomotyw parowych do kolei magnetycznej, Carta Blanca (2012)

Моделювання Процесів Надання Інтелектуальних Сервісів у Системі NS-2

Богдан Пустовий

Інститут холоду, кріотехнологій і екоенергетики
Одеської національної академії харчових технологій, Одеса, Україна
b.pustoviy@gmail.com

Abstract. Розроблено загальний алгоритм сценарію моделювання інтелектуальної надбудови з централізованим принципом управління в системі NS-2. При створенні імітаційної моделі враховувався експоненційний, самоподібний і змішаний характер мережевого трафіку.

Keywords: інтелектуальна надбудова, централізований принцип управління, самоподібний трафік, експоненційний трафік, NS-2.

1 Вступ

Одним з найважливіших питань при проектуванні мереж наступного покоління (NGN) є прогнозування можливих навантажень на систему. При прогнозуванні необхідно брати до уваги всі параметри, які можуть вплинути на ефективність системи управління. Сучасними дослідженнями природи мережевого трафіку [3-5] виявлено, що він має самоподібну структуру. Особливість самоподібного трафіку полягає в тому, що в різні моменти часу відбуваються великі викиди трафіку, які при масштабуванні за шкалою часу мають повторювану структуру. В результаті цих викидів відбувається різке навантаження на мережу, в зв'язку з чим неконтрольовано зростають черги на лініях, через що в підсумку може бути перевищена довжина черги на обслуговування. Результатом цього буде вимушене скидання нових пакетів, які абонент повинен буде знову відправити, що призведе до нераціонального використання ресурсів мережі. Урахування самоподібної структури мережевого трафіку дає можливість більш точного виявлення можливих навантажень на систему управління.

Таким чином, задача прогнозування поведінки мережевого трафіку з урахуванням само подібності його структури є актуальною. Одним з методів прогнозування поведінки мережевого трафіку є імітаційне моделювання. За допомогою імітаційного моделювання можливо відтворити поведінку досліджуваної мережі і визначити її характеристики.

Одним з найбільш популярних інструментів імітаційного моделювання є мережевий симулятор «Network Simulator-2» (NS-2). NS-2 має широкі можливості і велику бібліотеку готових компонентів [1], що в сукупності з

відкритим початковим кодом і безкоштовною моделлю поширення вигідно виділяє його на тлі інших систем моделювання.

2 Загальний опис архітектури імітаційної моделі ІНЦПУ

На даному етапі розвитку концепції NGN використовується інтелектуальна надбудова з централізованим принципом управління (ІНЦПУ). Саме така мережа буде розглядатися в даній роботі. У загальному випадку ІНЦПУ містить лише один керуючий центр (сервер послуг). На сервері знаходяться всі необхідні дані для надання інтелектуальних сервісів (ІС).

В загальному вигляді блок-схема алгоритму створення імітаційної моделі ІНЦПУ в системі NS-2 наведена на рис. 1.

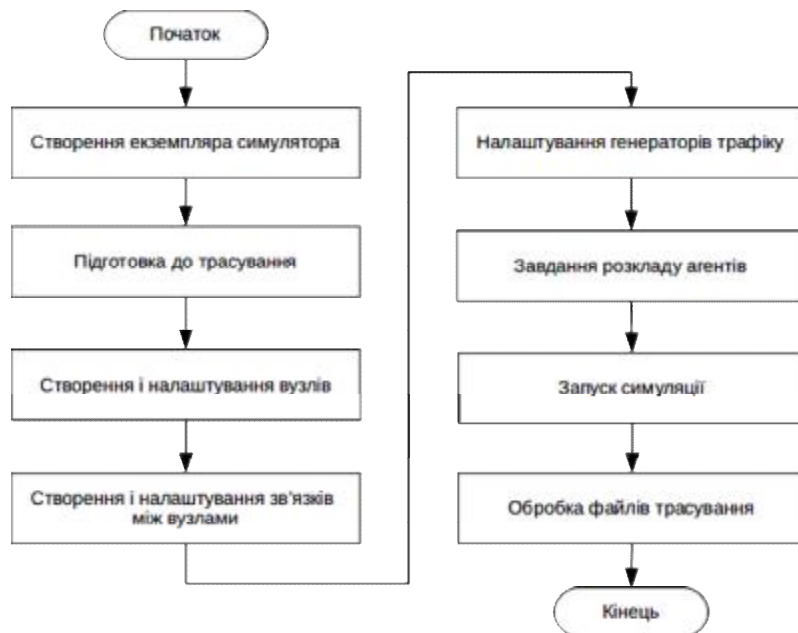


Рис. 1. Загальний алгоритм сценарію моделювання ІНЦПУ в системі NS-2.

У розробленій імітаційній моделі ІНЦПУ представлена структура з декількох абонентів, які генерують заявки на ІС і відправляють їх на програмний комутатор Softswitch, який переадресовує їх на сервер обслуговування.

Надсилання заявок відбувається через протокол TCP. В імітаційній моделі допущено, що мережа має необмежену пропускну здатність. Абоненти можуть генерувати як експоненціальний, так і самоподібний трафік.

При генеруванні заявок на ІС вказується розмір пакетів даних, інтервал їх відправки та розмір вікна TCP.

3 Реалізація імітаційної моделі в системі NS-2

NS-2 генерує трафік згідно з розподілом Парето використовуючи модель ON / OFF періодів [2]. Проста ON / OFF модель передбачає, що джерела перемикаються між двома станами: ON-стан, в якому джерела генерують трафік з постійною швидкістю, OFF-стан, в якому вони простоюють.

Розподіл Парето має функцію розподілу:

$$F(x) = 1 - \left(\frac{b}{x}\right)^a, \quad (1)$$

де α – параметр форми, β – мінімальне значення випадкової величини x .

Щільність розподілу Парето задається функцією:

$$f(x) = \frac{a}{b} \left(\frac{b}{x}\right)^{a+1}, \quad (2)$$

де $x > \beta$ та $a > 0$,

$$f(x) = F(x) = 0, \quad (3)$$

де $x \leq \beta$.

Середнє значення випадкової величини визначається як:

$$m(x) = \frac{ab}{a-1}. \quad (4)$$

Параметр α визначає середнє і дисперсію випадкової величини:

- якщо $\alpha \leq 1$, розподілення має нескінченне середнє;
- якщо $1 \leq \alpha \leq 2$, розподілення має кінцеве середнє і нескінченну дисперсію;
- якщо $\alpha \leq 2$, розподілення має нескінченну дисперсію.

Існує відношення між параметром α та параметром Херста (H):

$$H = \frac{b - a}{2}. \quad (5)$$

Тривалість ON і OFF періодів є випадковими величинами з розподілом Парето, які задаються усередненими значеннями.

Сервер обслуговування здатний обробляти тільки одну заявку в одиницю часу. Час обслуговування заявки змінюється в залежності від її розміру. На сервері обслуговування для формування черги на обслуговування використовується звичайна структура FIFO (First In, First Out). Якщо сервер

обслуговування зайнятий, заявки стають в чергу. Максимальна довжина черги задається вручну; якщо довжина перевищується, відбувається втрата заявок.

Отриманий в результаті моделювання trace-файл дозволяє розрахувати час перебування заявки в мережі, середню довжину черги на обслуговування, поточну довжину черги, ймовірність блокування заявки в мережі, а також кількість втрачених та доставлених пакетів. Розроблена модель дозволяє проводити дослідження при різних часових проміжках.

4 Організація модельних експериментів в системі NS-2

За допомогою описаної вище моделі в системі NS-2 було організовано кілька експериментів. Ці експерименти відрізнялися інтенсивністю надходження потоку і типом трафіку, що генерується – експоненційний, самоподібний і змішаний. Трафік формується заявками від 100 абонентів, які відправляються групами з 3÷8 пакетів. У моделі задані параметри трафіку, які приблизно відповідають параметрам реального трафіку телеголосування: ON період – 0,5 с, OFF період – 1,5 с, rate = 40 Мбіт/с, розмір пакету = 1000 байт, $\alpha = 1,2$.

У процесі аналізу trace-файлів були отримані характеристики модельованої системи: інтенсивність потоку заявок на обслуговування, поточна і середня довжина черги на сервері для заявок від абонентів, середній час очікування заявок в черзі, а також середній час існування заявки в системі. Нижче наведені графіки зміни цих характеристик в часі.

Наведені графіки дозволяють оцінити навантаження на систему обслуговування заявок.

На рис. 2 показані графіки зміни в часі довжини L черги заявок від абонентів, яка накопичується на сервері обслуговування.

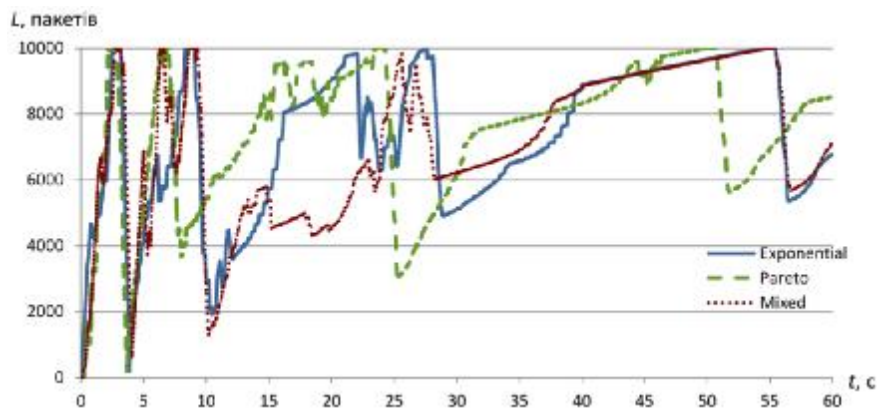


Рис. 2. Поточна довжина черги заявок від 100 абонентів, яка накопичується на сервері обслуговування, при експоненційному, самоподібному (Pareto) і змішаному трафіку.

Довжина черги у всіх варіантах моделі обмежена величиною в 10000 пакетів. Якщо чергу переповнюється, нові заявки губляться.

Рис. 3 демонструє графіки зміни середньої довжини LC черги заявок на сервері.

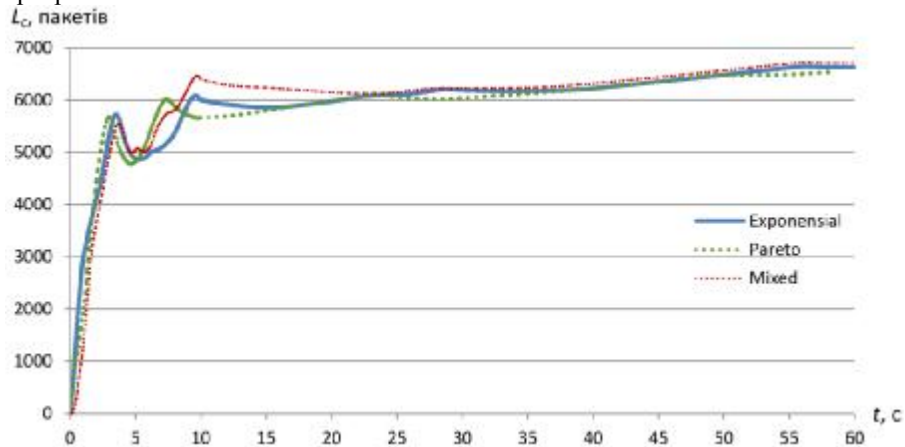


Рис. 3. Середня довжина черги заявок від 100 абонентів, яка накопичується на сервері обслуговування, при експоненційному, самоподібному (Pareto) і змішаному трафіку.

На рис. 4 і 5 показані графіки зміни середнього часу знаходження абонентських заявок в системі (t_s) і очікування в черзі сервера обслуговування (t_q).

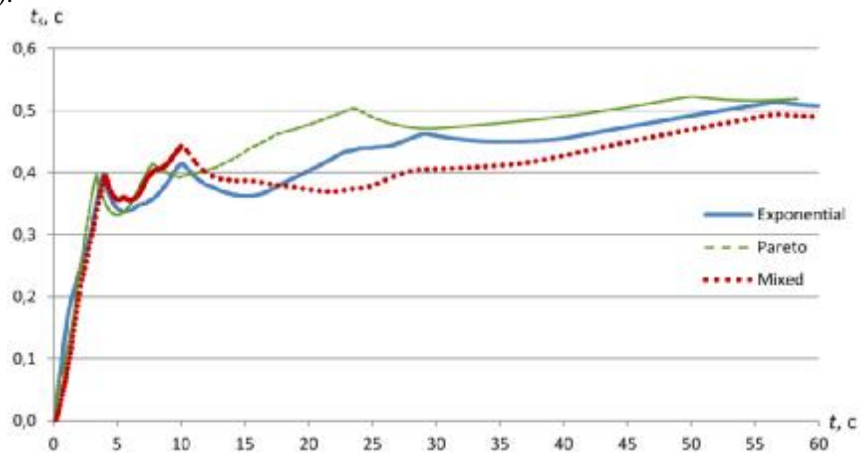


Рис. 4. Середній час перебування заявок в системі при експоненційному, самоподібному (Pareto) і змішаному трафіку в моделі з 100 абонентами.

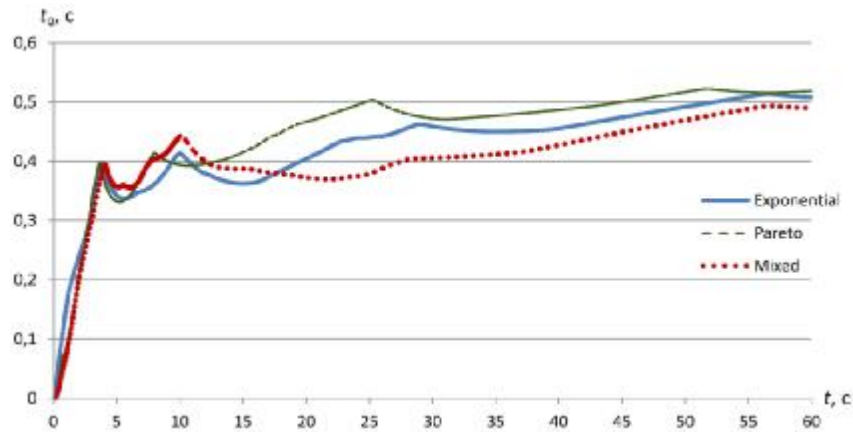


Рис. 5. Середній час очікування заявок на обслуговування при експоненційному, самоподібному (Pareto) і змішаному трафіку в моделі з 100 абонентами.

5 Висновок

Аналіз результатів, отриманих в ході імітаційного моделювання, дозволяє стверджувати, що врахування самоподібності потоку заявок на ІС призводить до «погіршення» значень мережевих показників.

Практичне застосування аналітичних та імітаційних моделей інтелектуальних надбудов централізованого принципу управління дозволить проектувальникам мереж наступного покоління ще на перших етапах проекту визначитися з характеристиками системи управління наданням інтелектуальних сервісів з урахуванням прогнозованого на них попиту.

Литература (References)

1. Кучерявый Е.А. NS-2 как универсальное средство имитационного моделирования сетей связи. – Режим доступа: <http://www.cs.tut.fi/~yk/ns2ru/ns2.pdf> (дата обращения 29.10.2016).
2. Моргайлов, Д.Д. Моделирование самоподобного входного трафика сетевых процессоров в системе NS-2. Д.Д. Моргайлов, Ю.В. Ладыженский, Моатаз Юнис // Информационные управляющие системы и компьютерный мониторинг. - Донецк : ДонНТУ, 2012. - С. 826 - 832.
3. Цыбаков Б.С. Модель телетрафика на основе самоподобного случайного процесса // Радиотехника. 1999. - № 5. - С. 24-31.
4. Чупахина Л. Р., Киреева Н. В. Исследование самоподобного трафика в мультисервисной сети // Т-Comm. 2013. №8.
5. Шелухин О.И. Самоподобие и фракталы / О.И. Шелухин , А.В. Осин, С.М. Смольский // Под ред. О.И. Шелухина. – М.: ФИЗМАТЛИТ 2008. – 368 с.

Wizualizacja Pracy na Tablicy Scrumowej

Lukasz Pstrong

Akademia Górniczo-Hutnicza, Kraków, Polska
lukasz.pstrong@mescomp.pl

Abstract. Celem poniższej pracy jest przedstawienie działania przykładowej Tablicy Workflow w zwinnym podejściu wytwarzania oprogramowania (Agile) implementowanym za pomocą metodyki Scrum.

Keywords: Scrum, tablica Scrum, workflow, issue tracker, Agile.

1 Wstęp

Publikacja ta ma na celu przedstawienie sposobu wizualizacji przepływu pracy (eng. workflow) w podejściu zwinnym wytwarzania oprogramowania – Agile. Zaprezentowana zostanie przykładowa implementacja Tablicy Scrumowej, na której zostanie przeprowadzona jedna iteracja, w ramach której widoczny będzie przepływ pracy w Scrumie, czyli metodyce będącej praktyczną implementacją podejścia Agile. W pracy zostanie też pokazane, że tablica ta, mimo iż w Scrumie nie jest obligatoryjna, stanowi stały element znaczącej liczby projektów rozwoju oprogramowania na całym świecie.

Poniższa praca skupia się na wąskim zagadnieniu Tablicy Scrumowej, jednakże w celu lepszego zarysowania kontekstu, w którym owa tablica funkcjonuje. W tekście przedstawione zostaną również podstawowe pojęcia związane z ideą podejścia Agile oraz metodyką Scrum, z pominięciem jednak założeń nieistotnych w kontekście Tablicy Scrumowej. W związku z tym niniejsza praca nie jest kompletnym przewodnikiem po metodyce Scrum, a zawiera jedynie opisy wybranych zagadnień, jednocześnie rozszerzając wymagania metodyki o komplementarne, nieobligatoryjne elementy, które są w praktyce stosowane w Tablicach Scrumowych.

2 Agile & Scrum – wstęp teoretyczny

2.1 Agile

Agile to tzw. zwinne wytwarzanie oprogramowania, którego założenia zostały opisane w manifestie podpisanym przez czołowe postacie nurtu nowoczesnego podejścia wytwarzania oprogramowania w 2001 roku:

“Odkrywamy nowe metody programowania dzięki praktyce w programowaniu i wspieraniu w nim innych.

W wyniku naszej pracy, zaczęliśmy bardziej cenić:

Ludzi i interakcje od procesów i narzędzi
Działające oprogramowanie od szczegółowej dokumentacji
Współpracę z klientem od negocjacji umów
Reagowanie na zmiany od realizacji założonego planu.

Oznacza to, że elementy wypisane po prawej są wartościowe, ale większą wartość mają dla nas te, które wypisano po lewej [1].

Mimo że manifest można interpretować na wiele sposobów, to bezsprzecznie nawołuje on do większego skupienia się na potrzebach ludzi w czasie tworzenia oprogramowania: klientów, zespołów wdrożeniowych oraz wszystkich innych. Wzywa on również do wytwarzania oprogramowania aktualnego w odniesieniu do dynamicznych zmian, które zachodzą w branży w sposób bardziej przystępny dla człowieka. W manifeście “działające oprogramowanie” oznacza przede wszystkim podzielenie produktu na małe fragmenty, z czego każdy posiada dodaną wartość biznesową dla klienta. Pozwala to szybciej i częściej dostarczać klientowi efekty pracy, tym samym zwiększając częstotliwość jego feedbacku. Dzięki temu produkt staje się bardziej aktualny i odzwierciedla potrzeby rynku.

2.2 Scrum

Scrum jest to metodyka - praktyczna implementacja podejścia Agile i, zgodnie z jego założeniami, zakłada pracę iteracyjno – przyrostową. Zasady Scruma określa The Scrum Guide™ [2]. Scrum składa się z: roli, artefaktów, wydarzeń i zasad. Ostatnie pojęcie opisuje jedynie zależności między pierwszymi trzema składowymi. Pojawiać się będzie ono więc za każdym razem, gdy pozostałe będą opisywane, bez nadmieniania, że mamy do czynienia właśnie z daną zasadą.

Trzy role scrumowe, składające się na Scrum Team (Zespół Scrumowy) to: Product Owner (Właściciel Produktu), Development Team (Zespół Deweloperski) oraz Scrum Master. Product Owner to osoba odpowiedzialna za maksymalizację wartości produktu oraz jego dobre zrozumienie przez Scrum Team oraz całą organizację. Oznacza, że jego drugą odpowiedzialnością jest zwiększanie efektywności samej pracy. To on kreuje wymagania dla Development Teamu – czyli zespołu inżynierów implementujących technicznie założenia biznesowe przedstawiane przez PO (skrót od: Product Owner). Development Team powinien być cross funkcjonalny i samoorganizujący się tak, aby móc każdy problem rozwiązać tylko we własnym zakresie. Nad całym procesem Scruma, czuwa ostatni, ale równie ważny członek Scrum Teamu – Scrum Master. Jego zadaniem jest wdrażanie oraz nauczanie Scruma oraz zgodnych z nim interakcji w Scrum Teamie oraz w organizacji, a także dostosowywanie metodyki na potrzeby swojego zespołu. Pochodną tych działań, tak jak w przypadku Product Ownera, jest maksymalizacja wartości produktu, ale tylko poprzez optymalizację samej pracy (większa efektywność pracy, to większa wartość wypracowana).

Artefakty w Scrumie także wyróżniamy trzy: Product Backlog, Sprint Backlog oraz Przyrost. W Scrumie tradycyjna specyfikacja produktu ukryta jest pod pojęciem

Product Backlogu (Backlog Produktu) i to tam spisane są wszystkie założenia produktu. Są one podzielone na jak mniejsze elementy, które na Scrum Guide określa-jako elementy Backloga Produktu. Dany produkt może posiadać tylko jeden Backlog Produktu i wszystko, co ma zostać wdrożone, musi się w nim znaleźć.

Scrum Team pracuje w stałych, zamkniętych odstępach czasu, zwanych Sprintami lub też Iteracjami. W każdym Sprincie z Backlogu Produktu Scrum Team wybiera zbiór wymagań, zwany Sprint Backlogiem (Backlogiem Sprintu), które będzie wdrażał w najbliższym czasie, określając jednocześnie Sprint Goal (Cel Sprintu) oraz plan dostarczenia Przyrostu. W tym okresie implementowane przez Development Team będą jedynie zagadnienia zawarte w Backlogu Sprintu, ale sam Backlog Produktu powinien być równolegle rozwijany przez PO. Zmiany te jednak nie dotyczą Development Teamu, który zajmuje się aktualnie tylko tym, co ma miejsce w Sprincie. W przypadku, gdy w czasie trwania Sprintu pojawi się konieczność wykonania dodatkowej pracy, jest ona umieszczana w Backlogu Produktu. Co ważne, Backlog Sprintu jest wyłączną własnością Development Teamu i nikt poza jego członkami nie może go edytować. Ostatnim artefaktem jest Przyrost, którego definicja jest dość prosta: jest to suma elementów Backloga Produktu, które zostały skończone w ostatnim Sprincie oraz we wszystkich poprzednich Sprintach. Tylko Development Team tworzy Przyrost.

W czasie Sprintu nie można zmniejszać wymagań jakościowych, np. usuwając elementy z Backloga Sprintu. Analogicznie nie można też dodawać tam nowych elementów, zgodnie z opisanymi wcześniej założeniami dotyczącymi kierowania dodatkowej pracy powstałej w czasie Sprintu do Backloga Produktu. Wymieniony wcześniej Cel Sprintu powinien przy tym zostać niezmienny przez cały Sprint, mimo że same elementy Backloga Sprintu mogą być renegotjowane między Development Teamem, a Product Ownerem. Przykładowo, jeśli dany element jest zbyt duży, możliwe jest rozbitcie go na mniejsze fragmenty lub też, na życzenie zespołu, jego opis może być doprecyzowany, jeśli wcześniej był niejasny. Obszar renegotjacji może być oczywiście dużo szerszy i ma on skutkować lepszym zrozumieniem produktu przez Development Team, a co za tym idzie efektywniejszą pracą. W praktyce każdy zespół nieco inaczej organizuje pracę nad elementami Backloga Produktu, ponieważ ich kształt ani forma nie są w Scrum Guidzie dookreślone. Stanowi on jedynie, że każdy element powinien posiadać swój opis, kolejność, estymację i wartość, które to określa się na poziomie właśnie Product Backloga.

Sam opis danego elementu jest rzeczą w Scrumie dość dowolną i jest on implementowany na różne sposoby. Kolejność elementów decyduje o tym, co Development Team powinien wykonać najpierw, a co potem. Za ustalenie kolejności (priorytetyzację) elementów w Product Backlogu odpowiada Product Owner. Estymacja jest z kolei odpowiedzialnością Development Teamu i pokazuje ona, jak dużo pracy obejmuje dany element. Informacja, ile jesteśmy w stanie zrobić w jednym Sprincie, może być cenna przy planowaniu kolejnych Iteracji. Wartość elementu jest to przyrost biznesowy, jaki element ten oferuje i to właśnie sumaryczne wartości poszczególnych elementów składają się na Przyrost danego Sprintu. Fizycznie - wartość jest zawarta zazwyczaj w opisie elementu, ale sam Scrum Guide nie określa dokładnie ani jej definicji, ani jej miejsca w samym Product Backlogu.

Wyróżnia się pięć głównych wydarzeń w Scrumie, w tym wydarzenie główne – Sprint, zawierając w sobie cztery kolejne wydarzenia: Sprint Planning (Planowanie Sprintu), Daily Scrum (Codzienny Scrum), Sprint Review (Przegląd Sprintu) oraz Sprint Retrospective (Retrospektywa). Kolejne wydarzenie, które trzeba bez wątpienia wymienić to Backlog Refinement (Doskonalenie Backloga), polegające na pielęgnowaniu Backloga Produktu przez Scrum Team. Product Owner może także samodzielnie, dowolnie edytować Product Backlog poza owym spotkaniem. Planowanie Sprintu polega na określeniu, które elementy Product Backloga będziemy realizować w najbliższym Sprincie, toteż co będzie składać się na jego Przyrost. W czasie tego spotkania definiuje się także Sprint Goal (Cel Sprintu) oraz zarysowuje plan jego dostarczenia (w języku branżowym: dowiezienia). Codzienny Scrum to krótkie, codzienne spotkanie, na którym każdy z członków Development Teamu odpowiada na pytania: “Co udało mi się dotąd zrobić?”, “Co robię obecnie?”, “Czy coś blokuje mnie w wykonywaniu moich zadań?” Przegląd Sprintu odbywa się tuż po jego zakończeniu i omawia się na nim przebieg Sprintu. Przyrost jest także prezentowany przed interesariuszami. Retrospektywa też odbywa się zaraz po zakończeniu Sprintu i ma na celu optymalizację swojej pracy przez Scrum Team na podstawie doświadczeń z poprzednich Sprintów. To ostatnie spotkanie jest szczególnie ważne, ponieważ jest bezpośrednią realizacją założenia Scruma o samoorganizujących się zespołach. Może ono doprowadzić nawet do zmiany samej metodyki. Sprint trwać może maksymalnie miesiąc, a w jego czasie Scrum Team stara się dowieźć biznesową wartość dodaną dla produktu. Scrum Team stara się monitorować Przyrost codziennie, określając przy na bieżąco tym prawdopodobieństwo dostarczenia Celu Sprintu.

Ostatnim ważnym zagadnieniem, niezdefiniowanym co prawda w Scrum Guidzie, jednakże wyjątkowo istotnym z punktu widzenia Tablicy Scrumowej jest Velocity (Prędkość Zespołu). To na jej podstawie określa się limit pracy, który zespół jest w stanie wykonać w najbliższym Sprincie. Jednym z popularnych sposobów estymacji elementów Product Backloga jest używanie jednostki Story Points – określającej, jak duży jest dany element w porównaniu z innym. Jeżeli dany element ma dwa Story Pointsy, a inny osiem, oznacza to, że pierwszy element kosztuje zespół cztery razy mniej pracy, niż drugi. Na tej podstawie, można więc w każdym Sprincie wyliczać Velocity, czyli sumę Story Points wszystkich elementów Sprint Backloga, które udało się dowieźć w ostatnim Sprincie.

3 Tablica Scrumowa

3.1 Wstęp faktograficzny

W Scrumie Tablica nie jest obowiązkowa, ale jest mimo to stosowana w znaczącej liczbie projektów. Wskazuje na to chociażby popularność oprogramowania służącego do jej implementacji z poziomu chmury, jak np. JIRA [3]. Z jej tablic (w tym w dużej części ze scrumowych) korzysta ponad 35.000 użytkowników, a warto zaznaczyć, że każdy z użytkowników (często są to organizacje) ma skonfigurowanych kilkanaście projektów oraz zarejestrowanych od kilku do 2.000 członków tychże projektów. Tego rodzaju rozwiązań podobnej wielkości można znaleźć jeszcze przynajmniej kilka.

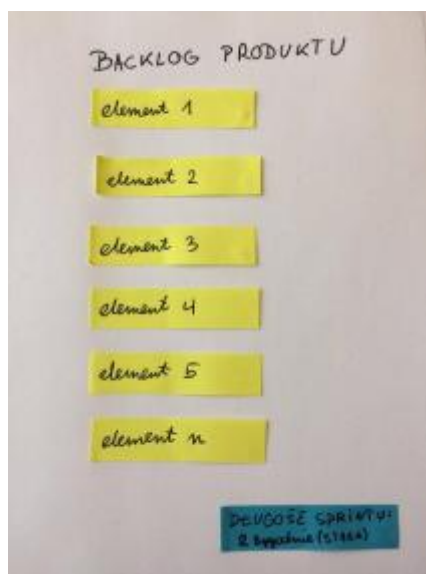
Wiele zespołów do dziś korzysta też z tradycyjnych tablic umieszczonych fizycznie w biurach.

W dalszej części pracy zostanie przedstawiony workflow podstawowej Tablicy Scrumowej, czyli takiej, która spełnia wszystkie założenia zawarte w The Scrum Guide™. Warto jednak zaznaczyć, że może być ona implementowana na wiele innych sposobów, w tym takich, które Scruma nie spełniają – wówczas jednak, nie będziemy mówić już o Tablicach Scrumowych, a jedynie o tablicach workflow, czy inaczej boardach.

3.2 Przykład implementacji tablicy

Tablicę Scrumową tworzymy na podstawie Backlogu Produktu, który w czasie trwania poprzednich Sprintów był przygotowywany w tym celu przez Scrum Team, m.in. w trakcie Backlog Refinement. Elementy Backloga Produktu ułożone są (według priorytetyzacji) od najbardziej do najmniej ważnego z punktu widzenia produktu. W momencie Planowania Sprintu powinny one już posiadać: wspomniany wcześniej priorytet nadany przez PO, być wyestymowane przez Development Team oraz mieć klarowne i jasne opisy, które zawierają wartość danego elementu.

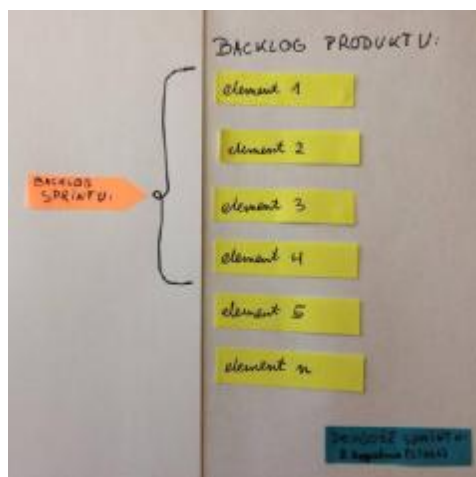
Poniższy rys. 1 to przykład Backlogu Produktu w formie uproszczonej, stworzonej na potrzeby symulacji (bez opisów i estymacji):



Rys. 1. Przykładowy Backlog Produktu (opracowanie własne)

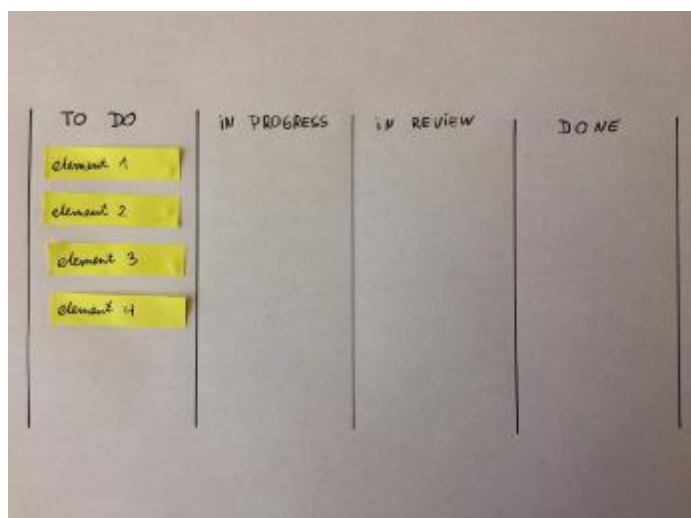
Podczas Planowania Sprintu wybierana jest pewna ilość elementów Backlogu Produktu możliwa do dowiezienia przez Development Team zgodnie z jego Velocity z poprzednich Sprintów. Ustalany jest także Cel Sprintu oraz plan dostarczenia Przyrostu.

W wyniku Planowania tegoż Sprintu wybrane zostały cztery elementy, które przeniesione zostaną do Backlogu Sprintu, co ukazuje rys. 2:



Rys. 2. Przykładowy Backlog Sprintu (opracowanie własne)

Elementy Backloga Sprintu przenoszone są na Tablicę Scrumową, co widać na rys. 3:

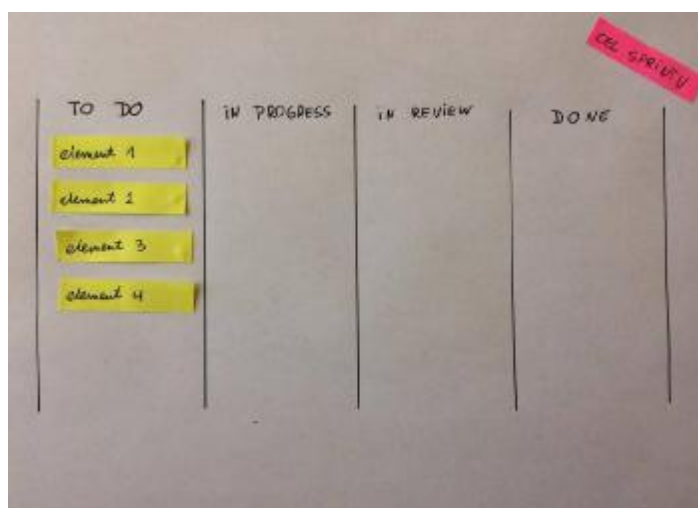


Rys. 3. Tablica Scrumowa – stworzenie tablicy (opracowanie własne).

Jak widać, wszystkie nowe elementy tablicy wstawiane są do kolumny “to do”, reprezentującej to, co jest do zrobienia (nazewnictwo kolumn zostało celowo utrzymane w języku angielskim w związku z brakiem polskich odpowiedników w języku branżowym). Dwie kolejne kolumny: “in progress” oraz “in review” reprezentują tzw. WIP – work in progress (pracę w toku). W pierwszej znajdują się elementy, nad któ-

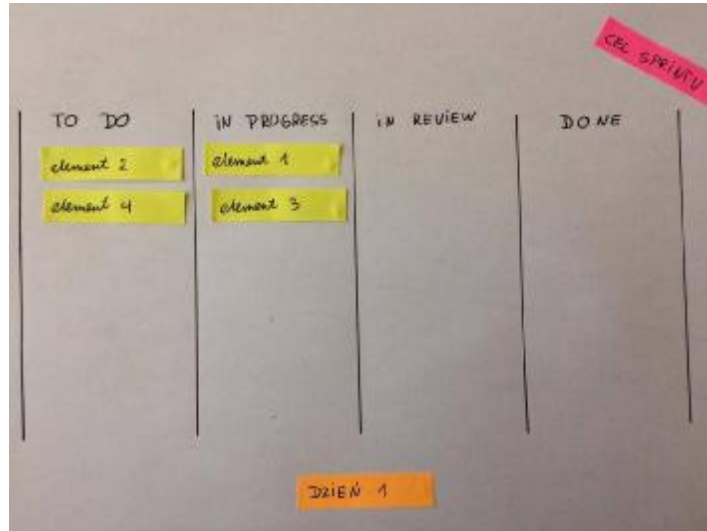
rzymi obecnie trwają prace, w drugiej natomiast te do zatwierdzenia. W praktyce w części projektów (zwłaszcza w mniejszych organizacjach lub w bardziej doświadczonych zespołach) rezygnuje się z kolumny “in review”, a pracę związaną z testowaniem czy akceptacją kodu, zawiera się kolumnie “in progress”. Ostatnią kolumną jest kolumna “done”, czyli elementy ukończone. Kolejne elementy w tej kolumnie są jednocześnie składowymi przyrostu Sprintu. Każdy element tablicy, który wykroczy poza kolumnę „to do”, powinien być przypisany do konkretnego członka Development Teamu. W myśl podejścia Agile, gdzie to zespoły organizują się samodzielnie, wskazanym jest, aby członkowie zespołu sami wybierali sobie zadania z kolumny „to do”, a nie, żeby były im one narzucane.

Dobłą praktyką jest także oznaczenie Celu Sprintu na tablicy, tak, aby był on wyraźnie widoczny na Tablicy, co przedstawia rys. 4:



Rys. 4. Tablica Scrumowa – Cel Sprintu (opracowanie własne)

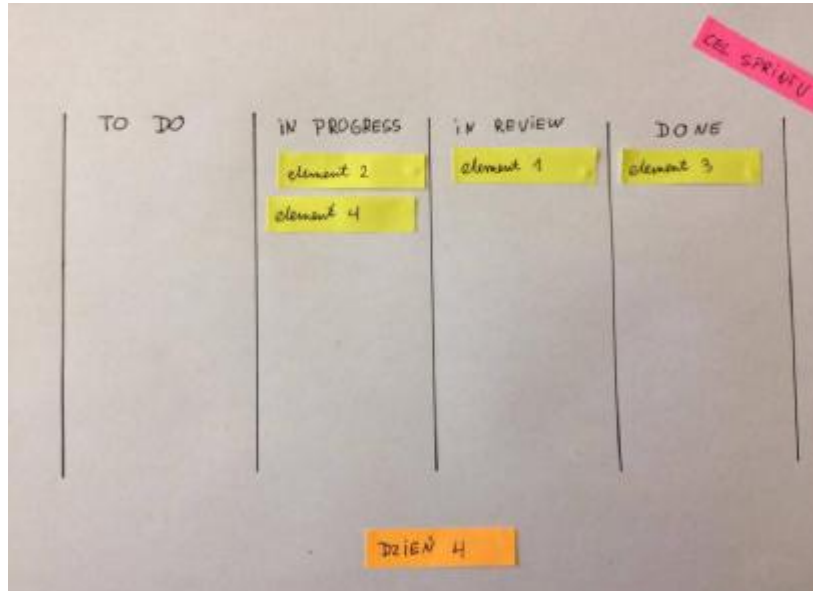
Sprint rozpoczyna się, toteż rozpoczyna się praca nad jego elementami. Rys. 5 obrazuje stan tablicy po pierwszym dniu Sprintu. Zespół pracuje nad elementami 1 oraz 3, pozostawiając elementy 2 i 4 w kolumnie “to do”.



Rys. 5. Tablica Scrumowa – dzień 1 (opracowanie własne).

Na koniec każdego dnia Sprintu (może odbywać się to także następnego dnia rano - najważniejsze, aby miało miejsce o stałej godzinie) Development spotyka się w ramach Codziennego Scruma, gdzie to omawiany jest Przyrost każdego dnia Sprintu.

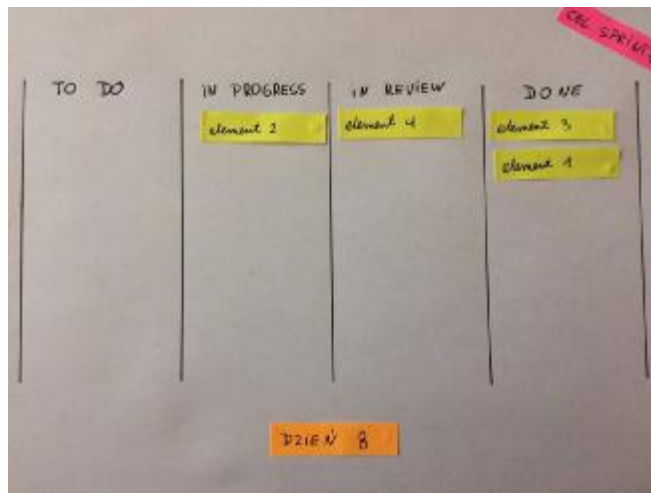
Rys. 6 przedstawia Tablicę po upływie kolejnych trzech dni prac nad Sprintem, przy czym warto zaznaczyć, że elementy na Tablicy powinny być przesuwane równoległe z pracą – każdego dnia. Na koniec czwartego dnia Tablica Scrumowa prezentuje się następująco:



Rys. 6. Tablica Scrumowa – dzień 4 (opracowanie własne)

Jak widać powyżej, element 3 został ukończony, a element 1 znajduje się w fazie testów. Obecnie prowadzone są prace tylko nad elementami: 2 i 4. Na koniec tego dnia, jak i każdego poprzedniego ma miejsce Codzienny Scrum.

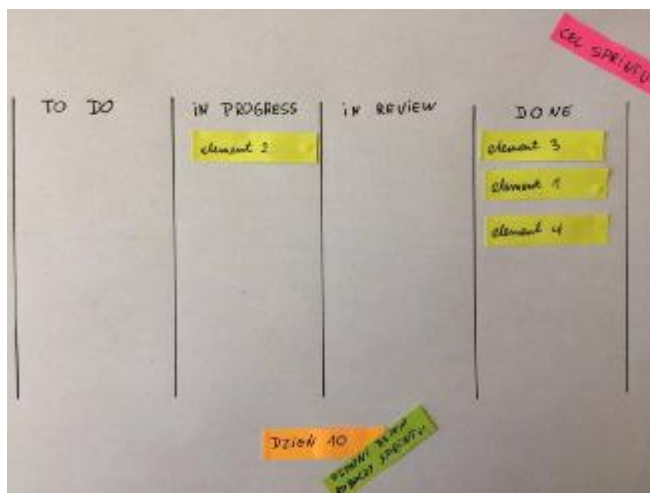
Po kilku kolejnych dniach, w ósmym dniu prac, Tablica osiągnęła następujący stan, widoczny na rys. 7:



Rys. 7. Tablica Scrumowa – dzień 8 (opracowanie własne)

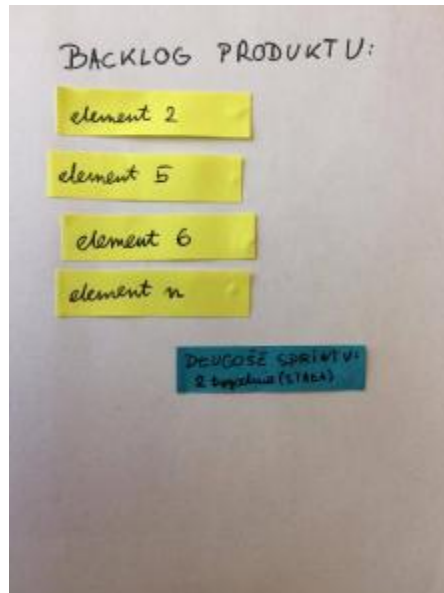
Widoczne jest, że elementy 1 oraz 3 zostały już ukończone, a element 4 jest w fazie testów. Prace trwają już tylko nad elementem 2. Development Team jest bardzo bliski dowiezienia wszystkich elementów. Na koniec dnia odbywa się Codzienny Scrum.

Nadszedł ostatni dzień Sprintu, co przedstawia rys. 8:



Rys. 8. Tablica Scrumowa – dzień 10 (opracowanie własne)

Development Team w czasie Przeglądu Sprintu prezentuje i ocenia wyniki swojej pracy w ostatnich dwóch tygodniach. Wyliczone jest też nowe Velocity zespołu. Niestety, nie udało się dowieźć elementu 2. Dlaczego? Tego Scrum Team spróbuje dowiedzieć się w czasie Retrospekcji, na której to spróbuje zoptymalizować swoją pracę, na podstawie wcześniejszych doświadczeń. Na tablicy widać, że elementy: 1, 3 i 4 są wykonane i po akceptacji Product Ownera następuje ich release (wydanie). To właśnie one stanowią Przyrost Sprintu. Element 2 wraca z powrotem do Backloga Produktu z najwyższym priorytetem, co obrazuje następny rys. 9:



Rys. 9. Zaktualizowany Backlog Produktu (opracowanie własne)

Można zaobserwować, że niewykonany element w poprzednim Sprincie znajduje się najwyżej w zaktualizowanym Backlogu Produktu (ma automatycznie najwyższy priorytet). Doszedł także nowy element 6, który mógł zostać dodany przez Product Owenera lub wspólnie przez Scrum Team podczas Backlog Refinement, lub na wniosek Development Teamu, jeśli w czasie Sprintu pojawiła się jakaś dodatkowa praca, którą trzeba wykonać (tą automatycznie przenosimy do Product Backloga).

Po przejściu całego Procesu, zaczynamy go od nowa, planując Sprint zaraz po wyciążeniu wniosków z poprzedniego w czasie Retrospektywy.

Warto zaznaczyć też, które z ról Scrumowych biorą udział w poszczególnych etapach prac przedstawionych wyżej. Product Owner koncentruje się przede wszystkim na dobrym sprecyzowaniu i spriorytetyzowaniu wymagań w okresie poprzedzającym Sprint oraz w czasie Doskonalenia Backlogu. Następnie bierze on udział w jego estymowaniu przez zespół i finalnie w planowaniu. Jest on obecny przez cały Sprint, jednakże nie ingeruje on ani w Tablicę Scrumową, ani w Codzienny Scrum. Powinien być on jednakże dostępny dla Development Teamu przez cały okres jego trwania tak, aby móc rozwiązać wszelkie wątpliwości dotyczące produktu powstałe w trakcie Sprintu. Na koniec Product Owner bierze również aktywny udział w Przeglądzie Sprintu oraz w Retrospekcji. Development Team bierze udział właściwie we wszystkich etapach procesu od momentu zamieszczenia przez PO spriorytetyzowanych wymagań w Backlogu Productu, łącznie z Codziennym Scrumem – to spotkanie jest dedykowane właśnie dla nich. Development Team, z racji, że tylko on tworzy Przyrost, jako jedyny może używać Tablicy Scrumowej. W końcu Scrum Master – bierze udział we wszystkich spotkaniach, w których proces nie jest wciąż zoptymalizowany. W idealnym świecie nie musi on robić nic, ponieważ Scrum Team działa w sposób perfek-

cyjny, a proces przebiega w sposób wzorcowy. W praktyce jednak Scrum Master w sposób ciągły doskonali proces, powinien być obecny na każdym z jego etapów i wszystko bacznie obserwować. W przypadku, kiedy Scrum jest źle rozumiany, implementowany bądź też interakcje między jego uczestnikami przebiegają inaczej niż zakłada metodyka, on interweniuje.

3.3 Podsumowanie symulacji

Tablica Scrumowa, to podstawowa forma wizualizacji pracy w zwinnym podejściu wytwarzania oprogramowania. Jej użyteczność powinna być jednakże zrewidowana osobno przez każdy zespół, tak aby była w jego rękach użytecznym narzędziem, a nie niepotrzebnym balastem. Tak samo powinno być w przypadku samego Scruma oraz Agile.

Bibliografia (References)

1. Manifest Agile, <http://agilemanifesto.org/iso/pl/manifesto.html>
2. The Scrum Guide™, <http://www.scrumguides.org/docs/scrumguide/v1/scrum-guide-us.pdf>
3. Atlassian, <https://www.atlassian.com/software/jira>
Odnosiniki na dzień 19.03.2017r.

Мікроконтролерна Обробка Даних Сенсора на Основі Поруватого Кремнію

Л.С. Монастирський¹, Р.Я. Яремик², О.І. Петришин³

¹проф., каф. РКС, ф-тет електроніки та комп'ютерних технологій, ЛНУ ім. Івана Франка,
м.Львів, Україна

²наук. с., каф. ФБЕ, ф-тет електроніки та комп'ютерних технологій, ЛНУ ім. Івана
Франка, м.Львів, Україна

³ас., каф. РКС, ф-тет електроніки та комп'ютерних технологій, ЛНУ ім. Івана Франка,
м.Львів, Україна

liu_mon@yahoo.com
yaremyk@yahoo.com
oleg.lpml@gmail.com

Abstract. The work deals with the problem of detecting the combustible and toxic gases, as well as their pairwise recognition on the basis of measuring the changes in technical parameters of PS, particularly investigating the concentration dependences of resistance, capacitance and frequency dependence of impedance of PS sensors. For gas detection, it is proposed to process the sensor's data by means of microcomputer systems.

Keywords: gas sensors, porous silicon (PS), microcomputer analysis of data, gas detection, pelargonic morpholide acid, ammonia, propane, volatile organic compounds.

1 Вступ

На сьогодні важливою роботою в області розумних рішень і систем є пошук нових видів сенсорів, в основі яких є показники змін характеристик кристалічних напівпровідників, зокрема, поруватого кремнію [1-3]. Поруватий кремній (ПК) — це наноматеріал, виготовлений з моно або полікристалічного кремнію шляхом електрохімічного травлення. Використовуючи такий тип сенсорів, необхідно знати залежності їх провідності від типу газового середовища, його концентрації, від властивостей поверхні поруватого кремнію – геометрії пор, радіуса пор і середньої відстані між ними. Поруватий кремній має властивість адсорбції молекул газу, що призводить до зміни провідності та ємності ПК і забезпечує чутливість поруватого кремнію як до типу газу, так і до його концентрації.

2 Постановка завдання

В основі роботи покладено ціль використання сенсора поруватого кремнію у житлових умовах. За допомогою обв'язки схеми ПК, можна знімати воль-амперну характеристику одного із зрізів. Проведення калібрування показів ВАХ зрізця відповідно до еталонного датчика вологості та температури DHT22(AM2302).

2.1 Опис макету

Запропоновано макет, що складається з двох частин: обв'язки сенсора ПК (рис. 1); також використано датчик вологості та температури — DHT22(AM2302); додатковий дисплей Nokia LCD5110, для показу поточних характеристик сенсора ПК. У мікроконтролерній системі використано програмний комплекс Arduino IDE, запропоновано програмний код, що написаний на мові С із використанням допоміжних бібліотек. За допомогою стандартних бібліотек Arduino, здійснена передача оброблених даних на персональний комп'ютер.



Рис. 1. Блок схема роботи мікроконтролерної системи з сенсором ПК.

Схема обв'язки складається із компонентів операційного підсилювача типу MCP604, цифрового потенціометра MCP4010 та цифро-аналогового перетворювача типу DAC7611 (рис. 2).

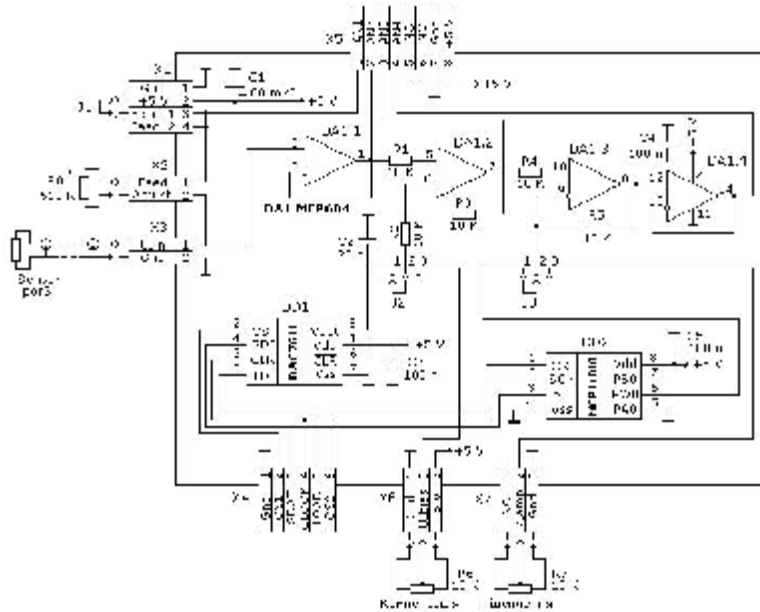


Рис. 2. Схема об'язки сенсора ПК

2.2 Вимірювання

Вимірювання проводиться у житловому приміщенні у місці віддаленому від джерела опалення, а також безпосередньо біля нього. Як джерело опалення встановлено газовий конвектор типу АКОГ-2М-СП. За середній показник температури і вологості взято виміри у центрі приміщення. Зняття показів біля джерела опалення показало відмінний результат від показів у центрі приміщення, що свідчить про чутливість сенсора ПК у житлових умовах (рис. 3).

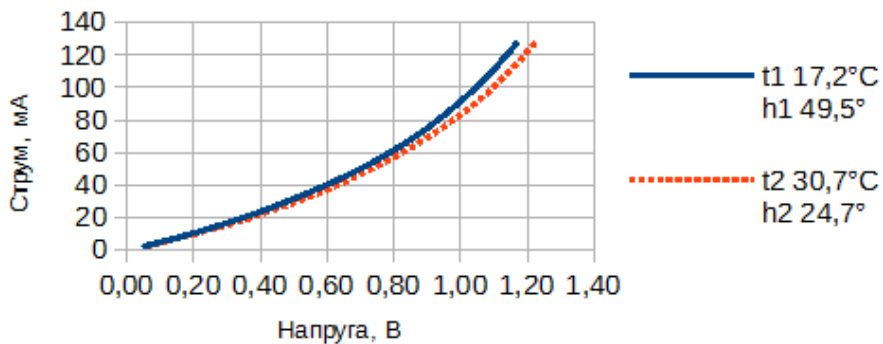


Рис. 3. Графіки вольт-амперних характеристик сенсора ПК у різних точках вимірювання

3 Висновок

Запропонований макет роботи з сенсором ПК є робочим прикладом, що можна використовувати у подальших цілях. На основі вимірних даних можна провести калібрування макету, як системи для сенсора вологості та температури. Також пропонується розширення макету для роботи набору сенсорів із ПК.

Література (References)

1. Оленіч І.Б., Монастирський Л.С., Аксіментьєва О.І., Соколовський Б.С., “Адсорбційне легування наноструктур поруватого кремнію.”, Фізика і хімія твердого тіла, Т.136 № 4 (2012) С.1011-1014
2. Skryshevskiy V. A. Fizychni osnovy napivprovidnykovykh fizychnykh sensoriv / V. A. Skryshevskiy. - K:VPTs «Kyivskiy universytet», 2006. - 190 p. (in Ukrainian)
3. Humidity sensors using porous silicon layer with mesa structure / S.-J. Kim, J.-Y. Park, S.-H. Lee, S.-H. Yi // Journal of Physics D: Applied Physics. - 2000. - V.33, No 15. P. - P. 1781-1784.

Трійкові Симетричні Функції та їх Застосування для Цифрової Обробки Інформації на Основі Ортогональних Перетворень

Артем Ізмайлов

Аспірант, Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
aiartefact@gmail.com

Abstract. Обґрунтовано актуальність дослідження застосування трійкових симетричних функцій для цифрової обробки інформації на основі ортогональних перетворень. Запропоновано побудову систем функцій на основі трійкових симетричних функцій за допомогою логічних операцій в межах трійкової симетричної логіки та обґрунтовано необхідність аналізу властивостей відповідних матриць значень.

Keywords: Цифрова обробка інформації, Трійкові симетричні функції, Ортогональне перетворення.

1 Вступ

У більшості сучасних систем цифрової обробки інформації використовується двійкова логіка. У той же час використання трійкових симетричних функцій та відповідної їм логіки є обмеженим, незважаючи на доведену більшу ефективність описаної логіки у порівнянні із двійковою [1]. Метою дослідження є побудова системи функцій на основі трійкових симетричних функцій, яка може бути використана для цифрової обробки інформації на основі ортогональних перетворень.

2 Трійкові симетричні функції

Трійкові симетричні функції задаються аналітичним виразом (1) [2]. Однак у вигляді (1) ці функції непридатні для цифрової обробки інформації на основі ортогональних чи вейвлет-перетворень, у зв'язку з неповнотою даної системи та її неортогональністю [2].

$$Ter_n(x) = \begin{cases} 0, & \text{якщо } 0 \notin \text{modh}(x + \frac{3^n - 1}{2}, 3^{n+1}) < 3^n, \\ 1, & \text{якщо } 3^n \notin \text{modh}(x + \frac{3^n - 1}{2}, 3^{n+1}) < 2 \times 3^n, \\ -1, & \text{якщо } 2 \times 3^n \notin \text{modh}(x + \frac{3^n - 1}{2}, 3^{n+1}) < 3^{n+1}, \end{cases} \quad (1)$$

де n – порядковий номер функції, x – цілочисельний аргумент, $\text{modh}(x,p)$ – допоміжна функція, задана аналітичним виразом (2).

$$\text{modh}(x, p) = \begin{cases} \text{mod}(x, p) + p, & \text{якщо } x < 0, \\ \text{mod}(x, p), & \text{якщо } x \geq 0, \end{cases} \quad (2)$$

де $\text{mod}(x,p)$ – функція залишку від ділення числа x на число p .

Для подолання проблеми неможливості застосування системи (1) трійкових симетричних функцій для цифрової обробки інформації на основі ортогональних перетворень необхідно побудувати нову систему функцій на основі існуючої системи (1).

3 Система функцій на основі добутоків трійкових симетричних функцій

Одним з найочевидніших варіантів утворення нової системи функцій є утворення системи добутоків трійкових симетричних функцій подібно до утворення

функціями Радемахера системи функцій Уолша [3]. Однак, у зв'язку з тим, що при утворенні системи добутоків на основі принаймні двох трійкових симетричних функцій утвориться лише $2^2 = 4$ функції і отримана система буде неповною. Неповнота даної системи пояснюється тим, що максимальна кількість змін функціями своїх значень у випадку використання трійкових симетричних функцій перших двох порядків буде рівна 9, тобто для досягнення повноти даної системи необхідно, щоб вона складалась з 9 функцій (на противагу чотирьом отриманим).

Один із варіантів вирішення описаної проблеми полягає у використанні піднесення до другого степеня (на противагу першому степеню, який використовується при формуванні добутоків функцій Радемахера) при формуванні добутоків трійкових симетричних функцій.

У випадку побудови системи добутоків на основі трійкових симетричних функцій з використанням піднесення до другого степеня можна отримати систему функцій, яка після процедури ортогоналізації Грама-Шмідта породить матрицю значень (рис. 1), яка може бути використана у якості матриці ортогонального перетворення.

\mathbb{R}	1	1	1	1	1	1	1	1	$1 \div$
\mathbb{C}	-1	-1	-1	0	0	0	1	1	$1 \div$
\mathbb{C}	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{2}{3}$	$-\frac{2}{3}$	$-\frac{2}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{3} \div$
\mathbb{C}	-1	0	1	0	0	0	-1	0	$1 \div$
\mathbb{C}	1	0	-1	0	0	0	-1	0	$1 \div$
\mathbb{C}	0	0	0	-1	0	1	0	0	$0 \div$
\mathbb{C}	$\frac{1}{3}$	$-\frac{2}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{2}{3}$	$\frac{1}{3}$	$\frac{1}{3}$	$-\frac{2}{3}$	$\frac{1}{3} \div$
\mathbb{C}	$-\frac{1}{3}$	$\frac{2}{3}$	$-\frac{1}{3}$	0	0	0	$\frac{1}{3}$	$-\frac{2}{3}$	$\frac{1}{3} \div$
\mathbb{C}	$\frac{1}{3}$	$\frac{2}{3}$	$\frac{1}{3}$	0	0	0	$\frac{1}{3}$	$-\frac{2}{3}$	$\frac{1}{3} \div$
\mathbb{C}	$\frac{1}{9}$	$-\frac{2}{9}$	$\frac{1}{9}$	$-\frac{2}{9}$	$\frac{4}{9}$	$-\frac{2}{9}$	$\frac{1}{9}$	$-\frac{2}{9}$	$\frac{1}{9} \div$

Рис. 1. Матриця значень системи ортогоналізованих добутоків трійкових симетричних функцій

Отримана матриця, однак, у 2-му, 6-му, 7-му та 8-му рядках містить дробові значення, які ускладнюють процедуру перетворення. У такому випадку доцільно перевірити можливість отримання матриці, яка буде містити меншу кількість дробових значень і, відповідно, буде у меншій мірі ускладнювати процедуру перетворення. Отримати таку матрицю можна шляхом заміни добутоків трійкових симетричних функцій на результати інших логічних операцій в межах трійкової симетричної логіки.

4 Висновки

Проаналізовані властивості отриманої на основі системи добутоків трійкових симетричних матриці значень вказали, що дана матриця може розглядатися у якості матриці ортогонального перетворення, але водночас ускладнить саму процедуру перетворення. Відповідно, перспективним напрямом досліджень є пошук більш придатної для ортогональних перетворень системи функцій як результату використання логічних операцій симетричної трійкової логіки.

Література (References)

1. В. Hayes, Computing science. Third base. A reprint from American Scientist, the magazine of Sigma Xi, the Scientific Research Society, vol. 89, Nr. 6. November–December 2001, pp. 490-494
2. Измайлов А. В. Трійкові симетричні функції та їх застосування у цифровій обробці інформації / А. В. Измайлов, Л. Б. Петришин // Системи обробки інформації. — 2016. — № 4. — С. 41-44.
3. Залманзон Л. А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. – М.: Наука, 1989. – 496 с.

Властивості Методів Частотного Аналізу Цифрових Сигналів

Ігор Голуб¹, Артем Ізмайлов²

¹Студент, Прикарпатський Національний Університет імені Василя Стефаника, Івано-Франківськ, Україна

²Аспірант, Прикарпатський Національний Університет імені Василя Стефаника, Івано-Франківськ, Україна
igorjokg@gmail.com
aiartefact@gmail.com

Abstract. Проаналізовано класифікацію сигналів за ознакою стаціонарності. Проаналізовано переваги та недоліки методів частотного аналізу цифрових сигналів (перетворення Фур'є, віконне перетворення Фур'є, вейвлет-перетворення). Визначено актуальність та перспективність розробки нових материнських вейвлетів.

Keywords: Цифрова обробка інформації, Стаціонарність сигналу, Перетворення Фур'є, Віконне перетворення Фур'є, Вейвлет-перетворення, Материнський вейвлет.

1 Вступ

Частотний аналіз є одним із ключових розділів цифрової обробки сигналів, перелік галузей застосування якої постійно розширюється. Відповідно, аналіз властивостей методів частотного аналізу цифрових сигналів є актуальним та перспективним науковим завданням. Метою дослідження є аналіз переваг та недоліків методів частотного аналізу цифрових сигналів.

2 Стаціонарні та нестаціонарні сигнали

Сигнали класифікують за багатьма характеристиками. Однією з найістотніших характеристик сигналу є його стаціонарність [1, 2]. Стаціонарними називаються сигнали, частотне наповнення яких не змінюється протягом часу [1]. Відповідно, при частотному аналізі даного типу сигналів відсутня потреба у часовій інформації: всі частоти присутні в сигналі протягом усього проміжку часу. Графік типового стаціонарного сигналу зображений на рис. 1.

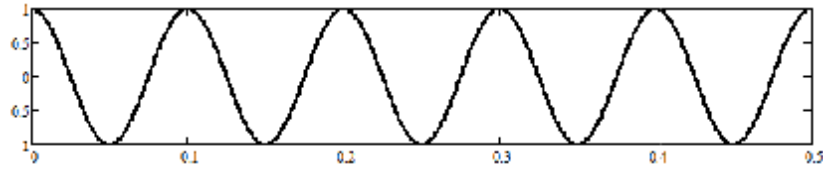


Рис. 1. Графік типового стаціонарного сигналу

Нестаціонарним сигналом називають сигнал, частота якого змінюється на проміжку часу [1]. Графік типового нестаціонарного сигналу зображений на рис. 2.

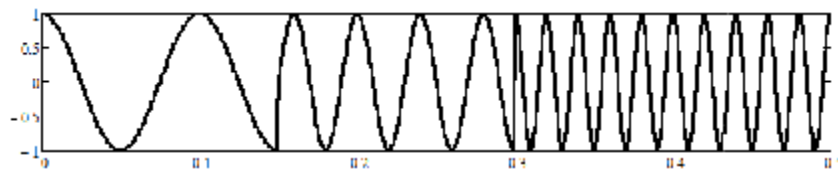


Рис. 2. Графік типового нестаціонарного сигналу

3 Перетворення Фур'є

Перетворення Фур'є (ПФ) є одним з найбільш поширених методів частотного аналізу цифрових сигналів [1]. Результатом ПФ сигналу, заданого в часовій області, є його спектральне подання. Іншими словами, замість значень параметра часу на осі абсцис графіка сигналу відкладаються значення частоти, у результаті чого на осі ординат відображається амплітуда тієї чи іншої частоти в сигналі. ПФ деякого сигналу обчислюється за формулою (1).

$$F(kW) = \sum_{n=0}^{N-1} f(nT)e^{-iWnT}, \quad (1)$$

де $F(kW)$ – спектр перетворення Фур'є, $0 \leq k \leq N - 1$, $W = \frac{2\pi}{NT}$ – вибрана відстань між двома відліками у частотній області, $f(nT)$ – послідовність з N відліків сигналу, $0 \leq n \leq N - 1$, T – інтервал дискретизації у часовій області.

Однак, дане перетворення може бути використаним для частотного аналізу лише стаціонарних сигналів. При перетворенні нестаціонарних сигналів виділення чіткої частотної характеристики сигналу є неможливим, оскільки неможливо зафіксувати момент часу, в який виникає та чи інша частота.

4 Віконне перетворення Фур'є

З метою застосування переваг ПФ у частотному аналізі нестаціонарних сигналів, ПФ було модифіковано, у результаті чого було розроблено віконне

перетворення Фур'є (ВПФ) [1]. Суть ВПФ полягає у тому, що нестационарний сигнал розділяють на частини у яких даний сигнал можна із деяким наближенням розглядати у якості стаціонарного.

У результаті застосування ВПФ для сигналу будується тривимірний графік, на осях якого позначаються частота, амплітуда і параметр часу. Однак, незважаючи на можливість частотного аналізу нестационарного сигналу, ВПФ не дозволяє однаково добре характеризувати сигнал за часом і частотою. При виборі вузького вікна більш деталізується часова характеристика, а при виборі широкого – частотна. Іншими словами, значним недоліком ВПФ є більша деталізація однієї характеристики сигналу за рахунок меншої деталізації іншої.

5 Вейвлет-перетворення

Алгоритм вейвлет-перетворення (ВП) подібний до алгоритму ВПФ [1]. У ВП в якості базисних використовуються відмінні від гармонічних функції, які називаються материнськими вейвлетами [3]. ВП дозволяє у однаковій мірі деталізувати часову та частотну характеристики нестационарного сигналу, тобто позбавлене недоліку ВПФ.

Однак, успішно застосований для аналізу одного сигналу материнський вейвлет, може дати неприйнятні результати для іншого. Відповідно, для частотного аналізу кожного окремо взятого сигналу необхідно підбирати такий материнський вейвлет, який дасть прийнятний (для вирішення конкретної задачі) рівень деталізації характеристик даного сигналу. У зв'язку з цим актуальною і перспективною задачею є пошук та розробка функцій, які можуть бути використані у якості материнського вейвлету, що суттєво розширить можливості застосування ВП для частотного аналізу нестационарних цифрових сигналів.

6 Висновки

В результаті даного дослідження проаналізовано переваги і недоліки перетворення Фур'є, віконного перетворення Фур'є та вейвлет перетворення. На основі отриманих результатів подальшою перспективою розвитку методів частотного аналізу цифрових сигналів є пошук функцій, які можуть бути використані у якості нових материнських вейвлетів.

Література (References)

1. Polikar R. The Wavelet Tutorial. – Iowa State University of Science and Technology, 1996. – 79 с.
2. Ізмайлов А. В. Трійкові симетричні функції та їх застосування у цифровій обробці інформації / А. В. Ізмайлов, Л. Б. Петришин // Системи обробки інформації. — 2016. — № 4. — С. 41-44.

3. Добеши И. Десять лекций по вейвлетам: Пер. с англ. – Ижевск: НИЦ «Регулярная и хаотическая динамика», 2001. – 464 с.

Дослідження Методів Розв'язку Задачі про Призначення із Обмеженнями з Неоднорідними Параметрами при Складанні Розкладу Навчального Закладу

Михайло Ільчук

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
misha.ilchuk95@gmail.com

Abstract. Розглянуто задачу складання розкладу занять навчального закладу. Проаналізовано методи вирішення задачі призначення.

Keywords: Задача про призначення Розклад навчального закладу
· Генетичний алгоритм

1 Вступ

Складання розкладу занять студентів навчального закладу є однією із важливих задач, якісне вирішення якої оптимізує використання аудиторного фонду, сприяє засвоєнню студентами навчального матеріалу, створює комфортні умови праці для викладацького персоналу.

Комплексне вирішення задачі у ручному режимі вимагає значних затрат часу і не завжди є оптимальним. Урахування великої кількості обмежень ускладнює отримання швидкого результату, а потреба в оперативному внесенні змін робить ручне складання розкладу неефективним.

Існує ряд методів вирішення задачі складання розкладу. Від вибору методу залежить складність реалізації та універсальність застосування. Відповідність результатів вирішення задачі планування розкладу занять поставленим обмеженням визначає методичну складову перебігу навчального процесу.

Дослідження виконано як частину дипломної роботи магістра.

2 Постановка задачі

Задача складання розкладу навчального закладу є задачею про призначення, котра належить до базису задач комбінаторної оптимізації, а також лінійного програмування.

Розклад навчального закладу повинен:

- забезпечувати рівномірне навантаження на учасників навчального процесу;

- відповідати вимогам вищої школи до обсягу тижневого навчального навантаження;
- сприяти ефективному завантаженню аудиторного фонду тощо.

Обмеження, котрі накладають на задачу призначення, можуть визначатися специфікою використання аудиторного фонду, ступенем завантаженості викладацького складу, графіком роботи викладачів, сезонними особливостями навчального процесу, вихідними та святковими днями тощо. Аналізуючи наведене, можна виділити жорсткі та відносно жорсткі обмеження.

Вихідними даними до складання розкладу є:

- структуру навчального закладу чи підрозділу;
- інформація про академічні групи, що включає дані про аудиторне навантаження;
- індивідуальне навантаження викладачів;
- інформація про предмети з прив'язкою до груп та викладачів тощо.

Розклад занять повинен забезпечувати при заданих вихідних умовах та накладених обмеженнях вирішення цільової функції, котра полягає у задоволенні потреб учасників навчального процесу.

3 Розв'язок задачі про призначення

Існує ряд методів розв'язку задачі про призначення. Серед них: метод імітації відпалу, метод розмальовування графу, метод імітаційного моделювання, метод логічного програмування, генетичні алгоритми.

Метод імітації відпалу реалізує розв'язок задачі глобальної оптимізації, при цьому пошук оптимального результату імітує процедуру відпалу.

Метод розмальовування графу базується на знаходженні мінімальної кількості кольорів, котра може бути використана для розмальовування вершин графу таким чином, щоб сусідні вершини завжди були зафарбовані різними кольорами.

Метод імітаційного моделювання імітує дії диспетчера при складанні розкладу занять. При цьому використовують логіко-математичну модель розкладу.

Згадані методи знаходять локальні екстремуми, при цьому знаходження оптимального розв'язку не гарантовано.

У роботі використано генетичний алгоритм [1, 2], котрий вирішує задачу оптимізації шляхом варіації параметрів підбору.

Література (References)

1. Poli, R., Langdon, W. B., McPhee, N. F. (2008). A Field Guide to Genetic Programming. Lulu.com, freely available from the internet. ISBN 978-1-4092-0073-4

2. Субботін С.О., Олійник А.О., Олійник О.О. Ітеративні, еволюційні та мультиагентні методи синтезу нечіткологічних і нейромережних моделей: Монографія // Під заг. ред. С. О. Субботіна. – Запоріжжя: ЗНТУ, 2009. – 375 с.

Дослідження Методів Детектування Рис Обличчя для Автомобільної Системи Безпеки Руху

Орест Фуфалько

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
orestfufalko95@gmail.com

Abstract. У роботі проаналізовано методи детектування очей для системи моніторингу втомленості водія автомобіля. Розроблено архітектуру тестової системи та проведено її дослідження з використанням бібліотеки Open CV на базі ОС Android.

Keywords: Детектування очей · Моніторинг втомлюваності водія · Open CV

1 Вступ

Автоматизований моніторинг втоми водія – один із перспективних напрямків розвитку систем забезпечення безпеки автомобільного руху. Такі системи контролюють положення голови водія, класифікують його міміку та дозволяють визначити, відкриті чи закриті очі у водія і куди скеровано його погляд.

Детектування очей може бути використано як складову алгоритму для визначення положення голови водія.

Автомобільні виробники приділяють значну увагу системам моніторингу втомлюваності водія.

Дослідження виконано як частину дипломної роботи магістра.

2 Аналіз предметної області

Методи детектування очей поділяють на активні та пасивні [1]. Активні використовують підсвітку у той час як пасивні не вносять локальних змін в оточуюче водія середовищі. Підсвітка обличчя зазвичай — інфрачервона [2, 3]. Активні методи забезпечують більшу точність та демонструють гнучкість у роботі, проте для них характерна більша кількість помилкових спрацювань в умовах поза приміщеннями.

Ранні дослідження оперували поняттями градієнта [4] зображення, проекції [5] та шаблонів. Для зменшення кількості помилкових спрацювань такі алгоритми потребували значного рівня евристики та постобробки зображень.

Також для детектування очей можуть бути застосовані вейвлети.

У деяких пасивних методах задачу детектування очей розглядають як задачу розпізнавання з двома шаблонами.

3 Постановка задачі

Завданням даного дослідження є розробка архітектури тестової системи для моніторингу втомлюваності водія на базі ОС Android з використанням бібліотеки Open CV. Базовим елементом такої системи є детектування очей у режимі реального часу. За відомим положенням очей робиться висновок про нахил голови. Також у процесі детектування моніториться процес кліпання, що також є одним із індикаторів стомленості.

4 Детектування очей за допомогою Open CV

Бібліотека Open CV використовує для детектування об'єктів каскадні класифікатори. В основі такого підходу лежить машинне навчання, за якого каскадна функція тренується на наборові позитивних та негативних зображень. Позитивними зображеннями називають такі, котрі містять об'єкти детектування, негативними – такі, що не містять їх.

Ідея каскаду класифікаторів полягає у побудові ієрархії об'єктів, котрі повинні бути класифіковані і, відповідно, створенні каскаду їхніх класифікаторів. Наприклад, якщо алгоритм повинен визначити, закриті чи відкриті очі, доцільно спочатку знайти, чи містить зображення обличчя чи – ні. Якщо зображення не містить об'єкту вищого рівня ієрархії, то немає сенсу шукати об'єкт, котрий знаходиться далі від вершини.

У роботі здійснено практичну реалізацію детектування очей у відеопотоці, що може бути використано при моніторингові втомленості водія автомобіля.

Література (References)

1. Qiang Ji, Harry Wechsler, Andrew Duchowski, and Myron Flickner, Special issue: eye detection and tracking, *Computer Vision and Image Understanding* (2005), 1–3.
2. A. Haro, M. Flickner, and I. Essa, Detecting and tracking eyes by using their physiological properties, dynamics, and appearance, *IEEE International Conference on Computer Vision and Pattern Recognition*, vol. 1, 2000, pp. 163–168.
3. Zhiwei Zhu, Qiang Ji, and Kikuo Fujimura, Combining kalman filtering and mean shift for real time eye tracking under active ir illumination, *International Conference on Pattern Recognition*, 2002, pp. 318–321.
4. R. Kothari and J.L. Mitchell, Detection of eye locations in unconstrained visual images, *ICIP*, vol. 3, 1996, pp. 519–522
5. Z.H. Zhou and X. Geng, Projection functions for eye detection, *Pattern Recognition* 37 (2004), no. 5, 1049–1056.

СЕКЦІЯ 2

Інформаційні технології

Information Technologies

Programy Bug Bounty jako Podejście do Zapewnienia Bezpieczeństwa Aplikacji Internetowych

Michał Szymański

Akademia Górniczo-Hutnicza w Krakowie, Kraków, Polska
michalszyman1@gmail.com

Abstract. Zapewnienie bezpieczeństwa aplikacji internetowych stało się istotną kwestią w obliczu usług, jakie oferowane są za ich pośrednictwem. Autor przedstawia programy Bug Bounty, jako sposób zwiększania bezpieczeństwa poprzez weryfikację i poprawę istniejących zabezpieczeń. Jednocześnie na przykładzie pokazuje istotność odpowiedniego zarządzania takimi programami.

Keywords: Security · Penetration testing · Bug bounty ·

1 Bezpieczeństwo aplikacji webowych, a testy penetracyjne

Rozwój połączonych ze sobą za pośrednictwem sieci Internet systemów oraz ich dynamiczne powiększanie się umożliwiły oferowanie przy ich użyciu zaawansowanych usług. Przy użyciu aplikacji internetowych możliwe jest obecnie robienie zakupów, czy dokonywanie operacji bankowych. W konsekwencji zapewnienie bezpieczeństwa systemów oferujących usługi webowe stało się wyzwaniem znacznie istotniejszym, niż miało to miejsce dotychczas [1].

Jednym ze sposobów weryfikacji bezpieczeństwa danej aplikacji są testy penetracyjne, które często prowadzone są w ramach procesu certyfikacji systemu [2]. Działania prowadzone w ramach testu penetracyjnego są symulacją rzeczywistego ataku, podczas którego podejmowane są próby ominięcia istniejących zabezpieczeń w celu uzyskania nieautoryzowanego dostępu do systemu. Jedną z cech, która wyróżnia testy penetracyjne na tle innych sposobów sprawdzania bezpieczeństwa aplikacji jest rzeczywiste potwierdzanie zidentyfikowanych luk przez wskazywanie potencjalnych sposobów ich wykorzystania [3].

W zależności od przyjętego podejścia można wyróżnić następujące typy testów penetracyjnych:

- a) ze względu na posiadaną wiedzę:
 - metoda białej skrzynki – tester posiada pełny dostęp do informacji o badanym systemie (specyfikacja, kod źródłowy),
 - metoda czarnej skrzynki – tester całą wiedzę nabywa w trakcie prowadzenia prac z powszechnie dostępnych źródeł informacji,

- metoda szarej skrzynki – tester posiada częściową wiedzę o systemie – jest to podejście pośrednie łączące elementy dwóch poprzednich [1],

b) ze względu na sposób prowadzenia testów:

- testy manualne – wykonywane ręcznie przez testujących,
- testy automatyczne - wykonywane za pomocą narzędzi automatyzujących pracę,
- testy mieszane - połączenie dwóch powyższych metod [4].

Wynikiem testu penetracyjnego jest raport opisujący przeprowadzone prace, wskazujący występujące w aplikacji podatności oraz zawierający rekomendacje dotyczące sposobów zmniejszenia ryzyka. Nie ma jednak gwarancji, że w ramach testu znalezione zostały wszystkie luki bezpieczeństwa. Stale ewoluujące sposoby prowadzenia ataków stwarzają potrzebę cyklicznego testowania w celu weryfikacji zabezpieczeń.

2 Programy Bug Bounty

Ciekawym podejściem do sprawdzania bezpieczeństwa, które wyewoluowało z klasycznych testów penetracyjnych są programy Bug Bounty. Organizator takiego programu zezwala wybranej grupie (programy na zaproszenie) lub dowolnym osobom (programy publiczne) na prowadzenie testów bezpieczeństwa. Warunkiem jest przestrzeganie określonych przez organizatora reguł odnoszących się np. do wykorzystywanych narzędzi czy zakresu działań. Konieczne jest również zgłaszanie znalezionych podatności. Wiedza o znalezionych przez testujących lukach bezpieczeństwa daje właścicielowi aplikacji możliwość ich poprawy. Z kolei dla osób testujących programy Bug Bounty są możliwością podniesienia lub weryfikacji swoich umiejętności, a za zgłoszenie błędów są oni nagradzani w zależności od programu przez umieszczenie w galerii sław, nagrodami lub pieniędzmi.[5] Programy Bug Bounty cieszą się rosnącą popularnością o czym świadczyć może np. uruchomienie ich przez firmy takie jak Google [6] czy Facebook [7].

3 Poprawność zarządzania programem Bug Bounty

W celu lepszego poznania realiów programów Bug Bounty autor przeprowadził szeroki zakres działań mających na celu weryfikację zabezpieczeń aplikacji posiadającej program publiczny. Organizator programu nie określił ścisłych sposobów, jakimi należy prowadzić testy. Jednak ze względu na brak udostępnienia dodatkowych informacji, jak również na charakterystykę aplikacji przyjęte podejście można określić jako testy manualne metodą czarnej skrzynki. Korzystając jedynie z darmowych narzędzi takich jak np. Burp Suite Free Edition zidentyfikowano 24 luki bezpieczeństwa. Obszary oraz ilość znalezionych podatności zestawione zostały poniżej:

- niepoprawna walidacja danych wprowadzanych przez użytkowników – 12 podatności,
- słabości w zarządzaniu sesją – 4 podatności,
- podatności związane z logiką aplikacji – 4 podatności,
- wykorzystywanie oprogramowania z powszechnie znanymi podatnościami – 1 podatność,
- brak dodatkowych zabezpieczeń – 3 podatności.

Najczęściej występującą luką była podatność na ataki typu Stored Cross-Site Scripting, która umożliwia przy użyciu dostępnych w aplikacji formularzy na trwałe wprowadzenie do jej kodu elementów, które wykonywane będą przy każdym jej ładowaniu. Najczęściej jest to wykorzystywane przez atakujących do wprowadzania nieautoryzowanych skryptów, które atakują użytkowników aplikacji. Może to pozwolić na przejęcie tożsamości użytkownika oraz na przeprowadzenie szeregu innych działań, takich jak np. przekierowanie ofiary ataku na stronę propagującą złośliwe oprogramowanie [8].

Autor kilkakrotnie skontaktował się z organizatorami programu Bug Bounty w celu przekazania informacji o zidentyfikowanych podatnościach, jednak nie otrzymał odpowiedzi. Brak reakcji ze strony osób odpowiedzialnych za aplikację na zgłaszane w ramach programu kwestie stwarza wysokie ryzyko wykorzystania tych słabości. Podczas prowadzonych prac autor wielokrotnie obserwował wyniki testów innych osób biorących udział w programie, w szczególności na nieautoryzowane skrypty umieszczone w kodzie stron. Stwarza to wysokie ryzyko wykorzystania systemów aplikacji do prowadzenia rzeczywistych ataków. Obecność programu Bug Bounty sprawia, że testujący wykonują działania, które w przypadku braku takiego programu mogą być łatwo zaobserwowane jako nietypowe i podejrzane. Duża ilość takich działań oraz ich efektów obecnych na stronie sprawia, że rzeczywisty atak staje się trudny do wykrycia. Stwarza to wysokie zagrożenie dla użytkowników aplikacji jak również dla samych testujących. W konsekwencji aplikacja może posłużyć jako narzędzie do prowadzenia ataków, co negatywnie wpływa na reputację jej właścicieli.

4 Podsumowanie

Programy Bug Bounty są ciekawą alternatywą dla tradycyjnych form weryfikacji zabezpieczeń. Umożliwienie testowania aplikacji może przynieść korzyści zarówno jej właścicielom jak i testującym. Istotne jest jednak odpowiednie zarządzanie i monitorowanie uruchomionego programu. W przeciwnym przypadku Bug Bonty może przyczynić się nie do poprawy, ale do zwiększenia ryzyka występującego w aplikacji. Decyzja o uruchomieniu takiego programu powinna być poprzedzona odpowiednią analizą możliwości organizacji dotyczących nadzoru i reagowania na działania testujących.

Literatura (Reference)

1. Bacudio A., Yuan X., Bill Chu B., Jones M., *An overview of penetration testing*, International Journal of Network Security & Its Applications, Vol. 3, No. 6, listopad 2016
2. RFC 4949 *Internet Security Glossary, Version 2*, sierpień 2007
3. Patkowski A., *Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych*, Biuletyn Instytutu Automatyki i Robotyki, nr 24, Warszawa 2007
4. Antczak M., Świerczewski Z., *Metodyki testowania bezpieczeństwa aplikacji internetowych*, Przegląd Teleinformatyczny, nr 2, 2013
5. Schulz P., *Penetration Testing of Web Applications in a Bug Bounty Program*, 2014
6. Google Security Reward Programs, www.google.com/about/appsecurity/programs-home/ [dostęp 09.03.2017]
7. Facebook Bug Bounty Program, www.facebook.com/whitehat/ [dostęp 09.03.2017]
8. Cross-site Scripting (XSS), [www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](http://www.owasp.org/index.php/Cross-site_Scripting_(XSS)) [dostęp 09.03.2017]

Характеристики Протоколів Маршрутизації з Урахуванням Якості Обслуговування в Ad-Нос Мережах

Юлія Казак (ORCID 0000-0002-1055-7537)

Одеська національна академія харчових технологій, Одеса, Україна
flyger11@bigmir.net

Abstract. У даній роботі проведений огляд основних рішень для маршрутизації з урахуванням QoS в мережі MANET. Поточні дослідження протоколів маршрутизації для мобільних Ad-нос мереж (MANET) об'єдналися в кілька домінуючих протоколів маршрутизації, які включають оптимізований Link State Routing Protocol (OLSR), спеціальний вектор відстані за вимогою (AODV) і динамічну маршрутизацію від джерела (DSR). У той же час, класичні протоколи маршрутизації, такі як відкритий протокол маршрутизації, що базується на алгоритмі пошуку найкоротшого шляху (OSPF) і протокол, що використовує дистанційно векторний алгоритм (DSDV), покращені для мереж MANET. На основі проведеного аналізу існуючих протоколів сформована таблиця, дані якої можуть бути застосовані при обґрунтуванні вибору протоколу маршрутизації в мережах MANET.

Keywords: Ad-нос мережі, протоколи маршрутизації, якість обслуговування.

1 Вступ

Одним з найбільш перспективних напрямків мережних технологій є мережі MANET (mobile Ad hoc networks) завдяки унікальній можливості розгортання цих мереж в будь-якому місці і в будь-який час. Мережі MANET – це безпроводові самоорганізуючі мережі, які призначені для зв'язку між рухомими об'єктами. Характерною особливістю цих мереж є динамічна змінна топологія, яка формується на базі автономних вузлів, що функціонують як маршрутизатори і які об'єднані в комунікаційну самоорганізуючу мережу.

Мережі MANET володіють певними унікальними характеристиками, які створюють ряд труднощів у забезпеченні якості обслуговування (QoS). До таких характеристик можна віднести динамічну топологію мережі, відсутність точної інформації про стан маршруту, відсутність централізованого управління, схильні до помилок радіоканали, що спільно використовуються, обмежена доступність ресурсів, а також приховані проблеми терміналів [1]. Більшість протоколів маршрутизації для мобільних Ad hoc мереж, таких як OLSR, DSDV,

DSR, AODV і ZRP, розроблено без явного врахування QoS. Маршрутизація з урахуванням QoS вимагає знаходження не тільки маршруту від джерела до пункту призначення, а й маршруту, який задовольняє вимоги QoS, такі як пропускна здатність, затримка, тремтіння або ймовірність втрати пакетів.

Незважаючи на те, що QoS в мережі MANET широко досліджувалась, це – швидко зростаюча область дослідницького інтересу через зростаючу популярність і необхідність мультимедійних додатків. Це пов'язано з тим, що мультимедійні додатки часто мають строгі вимоги до часу і надійності, які повинні задовольняти мережу. Як наслідок, особливо в останні п'ять років, фокус змістився з послуг з кращими результатами на забезпечення більш високого і більш певного QoS в дослідженнях мережі MANET. Протоколи маршрутизації з урахуванням якості обслуговування грають важливу роль в механізмі QoS, оскільки їх завдання – визначити, які вузли, якщо такі є, можуть обслуговувати додатки з необхідною якістю. Таким чином, протоколи маршрутизації з урахуванням QoS також грають важливу роль в управлінні доступом до сеансу зв'язку, оскільки це залежить від виявлення маршруту, який може підтримувати запитувана QoS.

Таким чином, на сьогоднішній день існує безліч проблем в області створення безпроводових самоорганізуючих мереж зі змінною топологією. Однією з головних є проблема маршрутизації, яка забезпечує необхідну якість обслуговування.

Отже розробка нових і вдосконалення існуючих алгоритмів маршрутизації з метою підвищення ефективності передачі даних, є актуальним завданням.

2 Проблеми, пов'язані з наданням якості в мережі MANET

Основні проблеми в забезпеченні механізмів маршрутизації з урахування QoS для мереж MANET наведено в роботі [2].

Динамічна топологія. Зміни в топології мережі MANET обумовлені постійними змінами положення рухливих вузлів, довжиною життя вузла, а також входу і виходу мобільних вузлів в мережу. Проте, часті обміни інформацією про топологію можуть привести до значного перевантаження обмеженої пропускної здатності безпроводових ліній зв'язку, а також можливе виснаження обмеженого часу автономної роботи вузлів, що беруть участь у маршрутизації. Ці ускладнення, що накладаються на рухливість в мережі MANET, можуть серйозно погіршити якість мережі. Часті поломки маршрутів є природним наслідком мобільності, що ускладнює маршрутизацію. Застосування управління топологією може бути рішенням для зниження великого обсягу службового трафіку, що виникає в результаті безперервних змін в параметрах мережі.

Ненадійність безпроводового каналу. Безпроводові канали можуть бути ненадійними через перешкоди з боку інших передач, теплових перешкод, затінення і ефекту багатопроменевого завмирання. Все з даних причин впливають або на коефіцієнт доставки пакетів або ж на гарантію довговічності лінії зв'язку.

Мобільність вузла. Інформація про топологію повинна часто оновлюватися, для того щоб вузли знали про пакети даних, які будуть направлятися в пункти призначення.

Канал з'єднання. Для реалізації топології мережі, вузли в мережі MANET повинні спілкуватися по загальному каналу. Проте, це призводить до проблем перешкод і з'єднання каналу. Цю проблему каналного з'єднання можна уникнути, вдаючись до таких протоколів як CDMA (Code Division Multiple Access) і TDMA (Time Division Multiple Access) і їх поліпшеним варіантам.

Відсутність централізованого управління. Основною перевагою мережі MANET є те, що вона може бути створена на спеціальній основі та її вузли можуть динамічно змінюватися. Відсутність централізованого управління є невід'ємною умовою мереж MANET.

Неоднорідність. Мережі MANET, як правило, гетерогенні і мають різні типи мобільних вузлів, що використовують різні комунікаційні технології. Вузли відрізняються в своїх енергетичних потужностях і обчислювальних здібностях. Отже, мобільні вузли будуть мати різні швидкості генерації пакетів, мережеву активність і показники витрати енергії. Робота з вузлами гетерогенності є найважливішим фактором для успішної роботи мереж MANET.

Небезпечна середу. Безпека є серйозною проблемою в мережах MANET, особливо для військових і тактичних застосувань. Мережі MANET уразливі для атак, таких як підміна, підслуховування, відмова в обслуговуванні, спотворення повідомлення і імперсонації.

Неточний стан інформація. Вузли в мережі MANET передають інформацію про стан лінії зв'язку і потоку конкретної інформації. Інформація про стан лінії зв'язку включає в себе затримку, пропускну здатність, частоту помилок, швидкість втрати, вартість, стабільність і значення відстані для кожного з'єднання. Потік конкретної інформації включає в себе адресу джерела, ідентифікатор сеансу, адресу одержувача і QoS вимоги потоку, такі як максимальна вимога до смуги пропускання, вимога мінімальної смуги пропускання, максимальна затримка і максимальна затримка джитера. Інформація про стан мережі часто буває неточною через мобільності вузлів і характеристик каналу.

Енергетичні обмеження. Частина або всі вузли мережі MANET можуть працювати від батарей або інших джерел з обмеженою ємністю. Для таких вузлів важливу роль відіграють питання економії енергії.

3 Базові підходи QoS

Загальновідомі три базових підходи QoS [3]:

1. Best Effort – абсолютна відсутність механізмів QoS. Використовуються всі доступні ресурси мережі без будь-якого виділення окремих класів трафіку і регулювання. Забезпечується автоматичне мінімальне управління параметрами мережі і відсутність гарантії доставки даних. Прикладом забезпечення QoS на цьому рівні є черги FIFO (First in First out – першим увійшов, першим вийшов).

2. Soft QoS (Differentiated service) – модель диференційованого обслуговування. Розділяє трафік на класи, вводячи кілька рівнів QoS, і

забезпечує пріоритизацію трафіку і використання різних механізмів організації черг. Архітектура DiffServ припускає наявність класифікаторів і формувачів трафіку на межі мережі, а також підтримку функції розподілу ресурсів в ядрі мережі.

3. Hard QoS (Guaranteed service) – модель інтегрованого обслуговування. Забезпечує якість обслуговування, гарантуючи необхідну пропускну здатність за рахунок абсолютного резервування мережних ресурсів і використання спеціального протоколу сигналізації RSVP і більш ефективних алгоритмів управління розподілом трафіку.

Якщо вимоги QoS до з'єднання гарантовано виконуються протягом усього сеансу, QoS підхід називається жорстким (Hard QoS). У мережі MANET дуже складно забезпечити жорсткі гарантії QoS для призначених додатків. Деякі з протоколів NSR і SIRCCR (SIR і Channel Capacity based Routing). Якщо вимоги QoS не гарантовано для всього сеансу, QoS підхід називається підходом з м'яким QoS (Soft QoS). Таким чином, QoS гарантії можуть надаватися лише в певних статистичних межах. Більшість протоколів забезпечують м'які гарантії QoS. Тверде QoS, що надається мережним технологіями, такими як ATM, є чудовим способом поділу мережних ресурсів для регулювання трафіку. Основною перевагою QoS жорсткого підходу над м'яким QoS є гарантована пропускну здатність. Soft QoS виявилося життєздатним і надійним конкурентом Hard QoS, але, тим не менш, за нижчою ціною.

4 Метрики QoS

Метрики, що зазвичай використовуються додатками для вказівки вимог QoS до протоколу маршрутизації [4]:

- мінімальна необхідна пропускну здатність або ємність (b/s) – необхідна пропускну здатність додатків;
- максимальна допустима затримка (s) – зазвичай визначається як максимально допустима наскрізна (від джерела до пункту призначення) затримка для пакетів даних;
- максимальний допустимий дрейф затримки – одне загальноприйняте визначення цього показника – це різниця між верхньою межею наскрізної затримки (ВМНЗ) і абсолютною мінімальною затримкою (АМЗ). ВМНЗ включає в себе затримку черг на кожному вузлі, а АМЗ визначається затримкою поширення і часом передачі пакета. Час передачі між двома вузлами – це просто розмір пакета в бітах / пропускну здатності каналу. Ця метрика також може бути виражена як дисперсія затримки;
- максимальне припустиме співвідношення втрат пакетів – допустимий відсоток від загальної кількості відправлених пакетів, які не приймаються транспортним агентом або агентом більш високого рівня на кінцевому вузлі пакета.

5 Протоколи маршрутизації, що забезпечують QoS

На основі аналізу в даній роботі запропоновано класифікувати усі протоколи маршрутизації з урахуванням QoS за такими характеристиками:

- метод побудови мережі або топології мережі (плоска, ієрархічна або локальна);
- підхід до виявлення маршруту (проактивний, реактивний, гібридний або географічний);
- тип гарантії якості (Best Effort, Soft, Hard);
- тип метрики, що використовується (Single, Multi).

На основі використовуваного механізму оновлення інформації про маршрутизацію підходи для визначення маршруту з урахуванням QoS можна розділити на три категорії: проактивні, реактивні і гібридні. Проактивні протоколи – це протоколи, що підтримують маршрутизацію на кожному вузлі. Реактивний протокол також називається протоколом «за запитом». Інформація про стан надається за необхідністю. Гібридний протокол є комбінацією проактивних і реактивних стратегій.

У більшості протоколів основна увага приділялася забезпеченню гарантованої пропускної здатності, оскільки пропускна здатність вважається найбільш важливою вимогою. Протоколи маршрутизації, що використовують тип метрики Single є більш успішними, однак, вони не завжди працюють краще за все. Так, у алгоритмі CEDAR пропускна здатність використовується як єдиний параметр забезпечення якості. Більшість мультимедійних додатків вимагають, щоб зв'язок відповідав суворим вимогам щодо затримки, затримки джитера, вартості та інших показників QoS. За цих обставин тенденція полягає в переході від маршрутизації з типом метрики Single до Multi. Основна функція маршрутизації з типом метрики Multi – знайти правильний шлях, який одночасно відповідає деяким обмеженням, що є великою проблемою для мереж MANET, де топологія може постійно змінюватися.

У даній роботі запропонована класифікаційна таблиця протоколів маршрутизації (табл. 1), які враховують якість обслуговування. Перераховані та інші протоколи оптимізують ті параметри маршрутизації, які представляють значимість для конкретного мультимедійного додатка, тому вибір протоколу залежить в кінцевому підсумку від вимог користувача.

Таблиця 1. Порівняння протоколів маршрутизації, що підтримують QoS

Протокол	Метод побудови маршруту	Мережна архітектура	Тип гарантії якості	QoS	
				Метрика	Тип метрики
CEDAR	Ієрархічний	Проактивний / реактивний	Soft	Пропускна здатність	Single
MRP	Ієрархічний	Реактивний	Soft	Пропускна здатність	Single
AQOR	Плоский	Реактивний	Soft	Пропускна здатність, затримка	Multi
QMRPD	Ієрархічний	Реактивний	Hard	Пропускна здатність, затримка, затримка усунення тремтіння, вартість	Multi
BEQR	Плоский	Реактивний	Soft	Пропускна здатність	Single
QOLSR	Ієрархічний	Проактивний	Soft	Пропускна здатність, затримка	Multi
PLBQR	Прогнозування розташування	Проактивний / реактивний	Soft	Затримка, пропускна здатність	Multi
QAODV	Плоский	Реактивний	Soft	Пропускна здатність, затримка	Multi
Ticket-based	Плоский	Реактивний	Soft	Пропускна здатність, затримка	Multi
GAMAN	Ієрархічний	Реактивний	Soft	Обмеженість затримки, коефіцієнт втрати пакетів	Multi

6 Висновок

Мобільні Ad hoc мережі – це самоорганізуючі мережі, що швидко розгортаються і не вимагають постійної інфраструктури. Підтримка QoS – складний, але життєво важливий компонент для досягнення того, щоб мережі MANET стали ефективним доповненням до інфраструктурних провідних та безпроводових локальних мереж.

У роботі представлено широке уявлення про поточні проблеми, пов'язані із забезпеченням QoS в безпроводових мобільних мережах Ad hoc. Окрім цього, наведена класифікація деяких протоколів маршрутизації з різними функціями для

забезпечення необхідної якості обслуговування. Кожен з цих протоколів унікальним чином вирішує проблеми оцінки пропускної здатності, затримки, виявлення маршрутів і обслуговування маршрутів, надаючи різні переваги і недоліки для кожного протоколу. У таблиці 1 наведено класифікацію цих протоколів маршрутизації з точки зору підтримки мобільності вузлів, підтримки масштабування мережі, мереженої архітектури, гарантії якості. Також відзначено невідомі проблеми, які необхідно вирішувати для маршрутизації з урахуванням якості обслуговування з точки зору оцінки пропускної здатності/затримки, виявлення маршруту, резервування ресурсів і обслуговування маршруту. Дані таблиці можуть бути застосовані при обґрунтуванні вибору протоколу маршрутизації в мережах MANET.

Література (References)

1. S. Chakrabarti and A. Mishra, "QoS Issues in Ad-Hoc Wireless Networks," IEEE Communications Magazine, Vol. 39, No. 2, February 2001, pp. 142-148.
2. J. Abdullah, "QoS Routing Solutions for Mobile Ad Hoc Network," Mobile Ad-Hoc Networks: Protocol Design, pp. 417-454, 2011.
3. Seema, Yudhvir Singh, Vikas Siwach. Quality of Service in MANET. International Journal of Innovations in Engineering and Technology (IJET). Vol. 1 Issue 3 Oct 2012
4. A. Abdrabou and W. Zhuang, "A Position-Based QoS Routing Scheme for UWB Mobile Ad Hoc Networks," IEEE JSAC, vol. 24, Apr. 2006, pp. 850-856.

Використання SaaS Технологій при Проектуванні Систем Управління Навчанням

Олег Дашкевич

Харківський національний університет радіоелектроніки, Харків, Україна
oleg.daskevych@gmail.com

Abstract. Система управління навчанням – основа системи управління навчальною діяльністю, використовується для розробки, управління та поширення навчальних онлайн-матеріалів із забезпеченням спільного доступу. Метою даного дослідження є розглянути питання про необхідність вивчити цілий ряд методів аналізу даних і їх осмисленого застосування до складного набору зібраної інформації в процесі побудови інформаційної системи дистанційного навчання студентів.

Keywords: LMS Big Data; SaaS; система; метод; аналіз.

1 Вступ

Системи управління навчанням (англ. системи управління навчанням, LMS) мають важливе значення для забезпечення високої якості і найбільш ефективного навчання студентів – особливо коли мова йде про підвищення дотримання і розвитку навичок.

LMS є інфраструктурою, яка забезпечує і керує навчальним контентом, ідентифікує і оцінює індивідуальні та групове навчання або підготовку цілей. Також вона відстежує прогрес на шляху досягнення цих цілей, а також збирає і представляє дані для контролю за процесом навчання групи в цілому [1].

Важливими аспектами системи управління навчанням є виконання студентом базових дій для роботи, розуміння робочого процесу, надання онлайн контенту, ведення системи оцінок, управління неперервної професійної освіти, спільного навчання та управління ресурсами навчання [1].

Дані платформи надають великі набори даних (англ. Big Data) в процесі навчання, що дає можливість розвивати дослідження в області аналітичних інструментів, відомих як навчально-інтелектуальний аналіз даних (Data Mining Освітніх), академічної та освітньої аналітики [2]. Вони допомагають краще зрозуміти процес навчання студентів та поліпшити освітній досвід. Аналіз великих даних дозволяє прискорити рішення наукових, дослідницьких і педагогічних проблем. Вивчаючи статистику, можна працювати і з індивідуальними траєкторіями, і з глобальними освітніми системами.

LMS автоматично зберігає онлайн-взаємодія інструктора і учня, зібрані як частина природного навчальної діяльності. Підвищення доступності цих

наборів даних в поєднанні з «великих даних» і методами освітнього інтелектуального аналізу даних (англ. Освітніх Data Mining, EDM) пропонують унікальні можливості для досліджень в області вивчення розуміння і навчання в системі вищої освіти.

2 Робота з Big Data

EDM широко використовується в педагогічних дослідженнях: прогнозування, кластеризація, встановлення зв'язків і асоціацій, трансформація даних від людського судження і знаходження серед них математичних моделей.

Однією з моделей роботи з великими даними є прогноз, де комбінація відомих даних дозволяє прогнозувати шукане невідоме. Прогнозоване може бути числом: наприклад, це час, витрачений на рішення, кількість використаних підказок, відсоток переглянутого відео або результат тесту в балах. Для таких випадків використовують метод класифікації і різні алгоритми, наприклад, дерево рішень або кластеризацію.

Інший метод, мережевий аналіз, розглядає всіх учасників навчального процесу як «вузли», з'єднані зв'язками, які можуть бути сильніше або слабкіше в залежності від інтенсивності і частоти спілкування. Система передбачає різні типи взаємодії: колективна робота з одним ресурсом, лідерство, допомога, критика чи навіть образу. Дані про взаємодію визначаються важливими параметрами: щільність, доступність, відстань, потік, центричність, взаємність і власний вектор.

Кластеризація являє собою метод, щоб знайти точки даних, які, мають загальні характеристики і групує їх за даними ознаками на підгрупи [2]. Завдання кластеризації відноситься до статистичної обробки, а також до широкого класу задач навчання без учителя.

Перегонка даних для судження відноситься до зображення даних, включаючи візуалізацію даних, щоб дозволити людям швидко зрозуміти матеріал. На мікрорівні можуть бути використані методи візуалізації, такі як теплові карти, графіки та діаграми розкиду. На макрорівні, результати EDM були використані для розробки систем моніторингу студентів і надання гнучкою контрольної панелі, такі як система сигналів курсу і активності контекстно-залежних систем оповіщення [2].

Проте, EDM, як нової дисципліни, запозичив прийоми з інших областей, і до сих пір відсутня стандартний набір інструментів, моделей і процесів або аналізу великого набору даних. Виявлено відсутність стандартів або як корисні дані слід аналізувати, змодельовані і оброблені.

3 Формування SAAS інфраструктури

Хмарні обчислення ґрунтуються на обміні даними в мережі Internet, в результаті чого загальні ресурси, програмне забезпечення та інформація надаються на комп'ютери і інші пристрої на вимогу [3]. В результаті це передбачає існування

центрів обробки даних, які в змозі забезпечити послуги. Хмара можна розглядати як єдину точку доступу для всіх запитів, що надходять від можливих клієнтів.

Програмне забезпечення як послуга (SaaS) — надання додатків в браузері користувача або клієнта з хмари. Це допомагає організаціям працювати з обмеженими ІТ-ресурсами навчитися розгортати і підтримувати необхідне програмне забезпечення своєчасно, і в той же час, знизити енергоспоживання і витрати. Все більше число академічних інститутів звертаються до моделі SaaS для своїх настільних додатків.

Компоненти пропонованої моделі: (1) Web 2.0 технології, (2) окремі види послуг і додатків, (3) Web 2.0 на основі діяльності, (4) процеси навчання (5) Хмарні обчислення.

(1) Web 2.0 Технології: Перший шар включає в себе технології, які роблять веб-сервіси і додатки більш зручними, такі як AJAX, JavaScript, XSL T / XML, XHTML, каскадні таблиці стилів (CSS), REST, RSS, Atom, тощо. Ці технології дозволяють користувачам створювати, ділитися, співпрацювати і спілкуватися, підвищити продуктивність системи і зробити користувацький інтерфейс більш привабливим. З цього шару ми будемо використовувати тільки ті інструменти, які сумісні з хмарних обчислень.

(2) Web 2.0 Служби і додатки: Другий шар складається з Web 2.0 сервісів і додатків, побудованих на технології Web 2.0 шару, які демонструють основи її концепції, і вони вже використовуються в певній мірі в галузі освіти, ці додатки включають веб-блоги, вікі, соціальні інструменти листи, соціальні закладки та теги, подкасти, інструменти обміну медіа, соціальні мережі тощо. Це насправді не технології як такої, але сервіси, побудовані з використанням будівельних блоків технологій і відкритих стандартів, що лежать в основі Інтернету і веб-сторінок. Університети можуть використовувати ці додатки, щоб спілкуватися і взаємодіяти з учнями, персоналом і більш широкого наукового співтовариства. З цього шару ми будемо використовувати тільки ті інструменти, які сумісні з хмарних обчислень.

(3) Web 2.0 на основі діяльності. Третій шар містить конкретні заходи в залежності від сервісів і додатків. Це включає спільне написання контенту, обмін, спілкування, обмін повідомленнями, інформацію, яка б пов'язала, подання інформації тощо.

(4) Процеси навчання організовані в ряд процесів навчання визначаються його завданнями. Кожне із завдань навчання можна керувати за допомогою одного або навіть декількох навчальних заходів. Такі заходи можуть бути надані через сервіси і додатки за допомогою діяльності Web 2.0 на основі.

(5) Хмарні обчислення в якості платформи нової ери хмарних обчислень пропонують академічній організації знайомий досвід розробки, на вимогу масштабованості, що дає змогу розширювати чи оптимізувати використання задля економії коштів, а також скоротити час виходу на ринок для додатків в захищеному середовищі [4]. Це новий інструмент для розміщення і розгортання електронного навчання екосистеми більш ефективним способом.

LMS можуть використовувати вигоду від хмарних обчислень за допомогою:

- Інфраструктури: використання електронного навчання як екосистеми провайдера інфраструктури.
- Платформи: використання і розвиток електронного навчання, заснованого на екосистемі інтерфейса розробки провайдера.
- Послуги: використання екосистеми електронного навчання від провайдера.

Одним з головних принципів при проектуванні архітектури являється мультитенантність - це можливість ізольовано обслуговувати користувачів з різних організацій (тобто незалежних передплатників SaaS) в рамках одного сервісу (однієї інсталяції або розгортання). Основним тут є дотримання ізольованості передплатників один від одного.

4 Висновки

Таким чином, побудова архітектури інформаційної системи управління навчанням будується на застосуванні основних принципів роботи з описаними вище аналізом і обробкою даних. Висновки з цього дослідження сприяють просуванню області EDM шляхом вивчення методів аналізу, розуміння і моделювання зростаючої кількості даних про використання LMS в процесі освіти користувачів. З величезним зростанням числа користувачів, змісту освітніх послуг і ресурсів, електронного навчання екосистеми стикається з проблемами оптимізації розподілу ресурсів, маючи справу з динамічними вимогами паралелізму, обробки швидких вимог зростання зберігання і контролінгу витрат. Таким чином, найкращим рішенням для цього є використання нових технологій (інтеграція між хмарних обчислень і веб 2.0).

Література (References)

1. Learning management system//Wikipedia. Дата оновлення: 09.10.2016. Режим доступу: https://en.wikipedia.org/wiki/Learning_management_system (дата звернення: 26.01.2017).
2. Бейкер, Р. Educational data mining and learning analytics/Р. Бейкер, Г. Сіменс – The Cambridge handbook of the learning sciences, 2014. — 274 с.
3. Тьорнер, Н. Cloud Computing: A Brief Summary/ Н. Тьорнер. — Lucid Communications Limited, 2009.
4. Software as a service//Wikipedia. Дата оновлення: 10.03.2017. Режим доступу: https://en.wikipedia.org/wiki/Software_as_a_service (дата звернення: 13.03.2017).

Особливості Давачів для Визначення Параметрів Вібραції

О. Лещенко¹, Е. Притуляк², К. Лещенко³

¹к.т.н., доцент, Одеська державна академія технічного регулювання та якості,
Одеса, Україна

²Одеська державна академія технічного регулювання та якості, Одеса, Україна

³Одеській національній політехнічний університет, Одеса, Україна

¹olegleshchenko@gmail.com

Abstract. Актуальність роботи полягає в тому, що сучасні технології вимагають безперервного контролю за багатьма параметрами технологічного процесу і контролю стану обладнання. Робота присвячена дослідженням параметрів багатовекторних датчиків вібрації для їх використання в інформаційно-вимірювальних системах.

Keywords: Багатовекторні датчики, Вібрація.

1 Вступ

Зменшення вібрації машин і виробничого обладнання, оздоровлення праці і побуту людей набувають все більшого значення. Проблеми, пов'язані з оцінками вібрації, стосуються як встановлення їх допустимих рівнів при впливі на людину, так і характеристик вібрації, випромінюваних джерелами (гігієнічне та технічне нормування). Питання гігієнічного нормування в даний час розроблені досить добре. На відміну від цього, до останнього часу розробники і виробники машин і устаткування проблем технічного нормування віробезпечних машин, на наш погляд, приділяли недостатньо уваги. Значним кроком вперед в цьому напрямку є введення ряду державних стандартів системи безпеки праці, які регламентують вібраційні характеристики машин безпосередньо як джерела вібрації і зобов'язують вносити цю характеристику в технічні умови, стандарти і паспорти машин.

Дослідження процесів налагодження механічних приладів свідчить про необхідність визначення параметрів вібрації. При цьому найчастіше досліджувалися амплітуда та частота вібраційних коливань. Однак, не найменшим параметром є вектор напрямку коливання, або вектор максимальної амплітуди.

2 Основна частина

Раніше нами вже було розглянуто контактні методи дослідження вібраторів з застосуванням найбільш простого методу реєстрації вібрацій за допомогою п'єзоелектричних датчиків [1]. Реєстрацію переміщень при малих амплітудах вібрацій проводять амплітудним методом по зміні вихідної потужності в разі прохідний схеми включення резонатора або відображеної потужності, у випадку застосування кінцевого включення. Недоліками цього методу вимірювання є високі вимоги до сталості потужності, що підводиться до резонатора та необхідність високої стабільності частоти збудження. В цьому способі реєструється зсув резонансної частоти, що можна зробити з дуже високою точністю. Але такий спосіб стає ефективним тільки у разі великих амплітуд вібрацій.

В публікаціях [2] було запропоновано використання тензодатчиків. Крім того розташування тензодатчиків на первинному перетворювачі – балці виконувалося так, що давало змогу визначити вектор напрямку вібраційних хвиль найбільшої амплітуди. Так розташування на балці, як найменш двох тензодатчиків дозволяє виконувати стежити за амплітудою (та/або частотою) коливань в двох взаємо перпендикулярних напрямках. Для збільшення напрямів, отримання багатовекторного контролю запропоновано конструкцію з більшим числом датчиків. В тому числі запропоновано датчик, в якому безпосередньо тензоперетворювач закріплюється на балці у спеціальний спосіб, що дозволяє отримувати та визначати максимум амплітуди практично з будь якого напрямку.

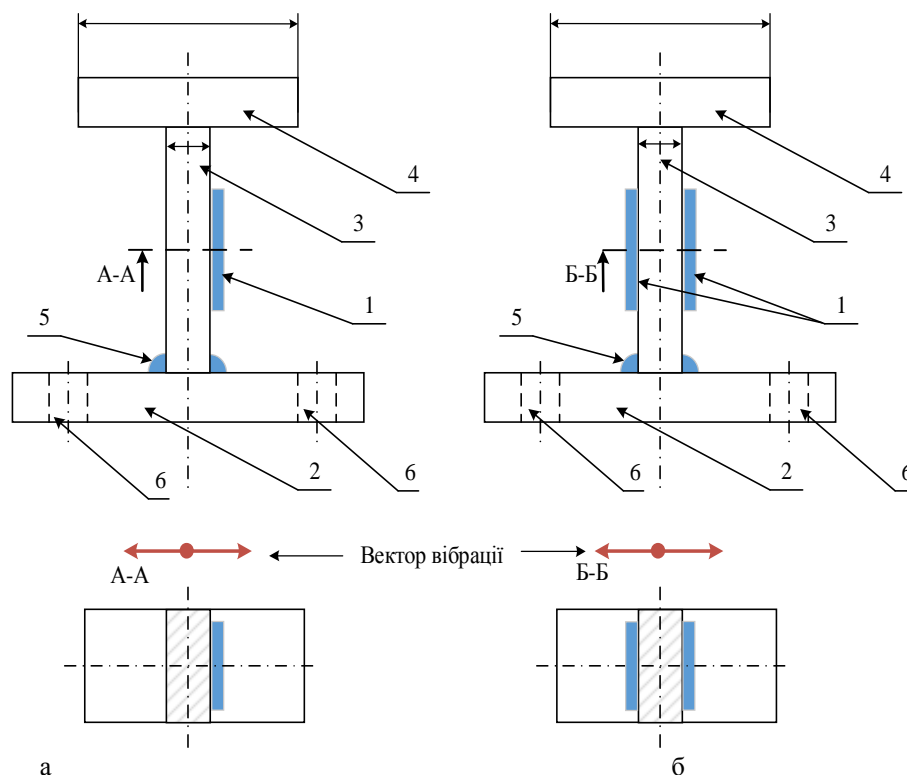
Такий спосіб застосування вимірювального перетворювача можна визначити як диференційний, тому як використовується тільки узагальнена інформація від датчика. Такий спосіб вирішує ще одну важливу задачу. Це лінеаризація характеристики датчика практично у всьому його робочому діапазоні. Для цього в конструкції датчика чутливі елементи виконуються попарно симетрично. Для лінеаризації характеристики береться середньо квадратичне значення кожної пари перетворювачів.

Раніше для цього пропонувалося використання додаткових приладів або схемних рішень. Тут же з'являється можливість отримання лінійної характеристики після першого перетворення. Такий спосіб дозволить значно спростити подальші схеми обробки інформації, і, завдяки цьому, зменшити методичні похибки. Також цікаво використання випадку, коли балка може бути створена у вигляді перекрученого шестикутника на кожну грань якого закріплений тензоперетворювач, що дозволяє більш точно проводити вимірювання. При цьому, крок скрутки повинен дорівнювати ширині однієї грані. При такому розташуванні тензоперетворювача і системному підході до знімання з них інформації, отримана можливість з однаковою точністю зняття показань вібродатчика практично з будь-якого напрямку – тобто багатовекторно. Обробка інформації проводиться в програмованому контролері.

Тензодатчики є найбільш уразливими компонентами ваговимірювальної системи. У процесі експлуатації на вагові тензодатчики впливають: агресивне навколишнє середовище, ударні динамічні навантаження, температурні дії,

електростатичний вплив (зварювання), вібрації і т.д. Тому в періоди технічного обслуговування, перед установкою в устаткування, а також в аварійних випадках, існує необхідність діагностики вагових тензодатчиків - перевірка та калібрування.

На основі принципу роботи вагових датчиків, знайшли своє застосування віброметри, тобто пристрій для визначення параметрів вібрації. Такими параметрами виступають в першу чергу амплітуда і частота вібрації. У найпростішому вигляді, пристрій для отримання цих двох параметрів показано на рис.1, а..



а
 1 – тензоперетворювач; 2 – кріплення; 3 – балка вібратора; 4 – балансир; 5 – місце зварювання; 6 – отвір для кріплення

Рис. 1. Вібродатчик з тензометричним перетворювачем: а – з одним тензоперетворювачем; б – з двома симетричними тензоперетворювачами

Особливістю цього пристрою є зняття характеристики вібрації в одному напрямку. Для зміни напрямку необхідно переміщення всього датчика в місці кріплення підстави 2. Для цього часто застосовують прорізи 6 для кріпильних болтів в підставі у вигляді сектора кільця. Недоліком такого пристрою виступає досить велика помилка для точного вибору інсталяційні напрямки - вектора.

Іншим недоліком таких систем є складність отримання лінійної характеристики тензоелемента для різних амплітуд коливань [9].

Для отримання сигналу в якості первинного перетворювача використовується балка 3, жорстко закріплена на підставі вібродатчика 2, наприклад за допомогою зварювання 5. Товщина балки вибирається з розрахунку передбачуваних амплітуди і частоти вібрації. На вільному кінці балки жорстко закріплений балансір 4. Розміри і маса балансира вибираються так само з розрахунку передбачуваних характеристик вібрації, причому, маючи набір балансірів з'являється можливість управління діапазоном характеристик вібратора. На балку прикріплений тензоперетворювач 1 для вимірювання змін геометричних параметрів у результаті коливання балки.

Для лінеаризації характеристики перетворювача запропоновано пристрій для балансування механічних пристроїв з лінеаризацією вихідної характеристики, рис.1, б. Відмінною рисою цього пристрою є те, що два тензодатчика 1 закріплюються симетрично, по різні сторони балки 3.

Обидва пристрої, показані на рис.1 мають можливість реагувати на вібрацію тільки в одному напрямку, тобто в нашому випадку уздовж горизонтальної осі симетрії (див. розріз А-А і Б-Б рис. 1).

Часто є необхідність отримання характеристики вібрації в різних (багатовекторних) напрямках. Для отримання сигналів про вібрації в перпендикулярному (поперечному) напрямку досить вибрати перетин балки у вигляді квадрата і прикріпити симетричні тензоперетворювачі на протилежні грані, як показано на рис. 2. Так само для отримання однакових сигналів про вібрації необхідно застосування симетричного балансира 4 (див. рис.1).

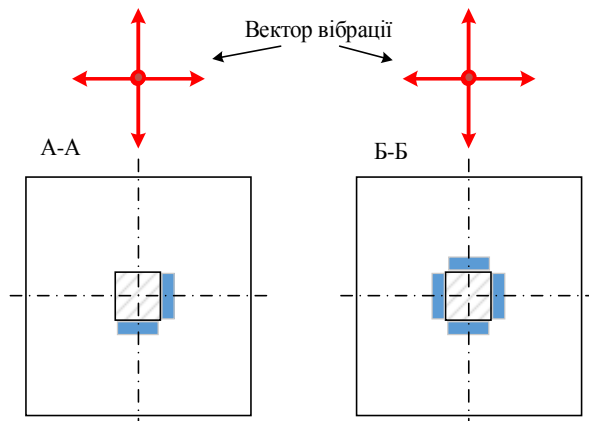


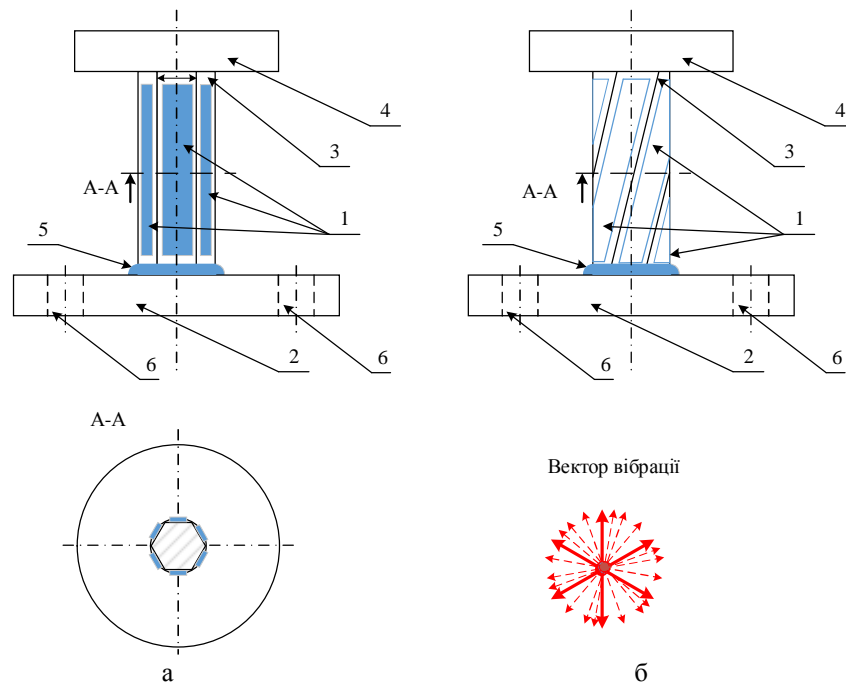
Рис. 2. – Перетин вібродатчика (рис.1) з симетричним тензометричним перетворювачем:
а – з двома тензоперетворювачами; б - з чотирма попарно симетричними тензоперетворювачами

Такий спосіб вимірювання можна назвати диференціальним, тому як надалі слід постійно використовувати тільки узагальнену інформацію від

запропонованого датчика. Такий спосіб вирішує ще одну немаловажну задачу. Це лінеаризація характеристики датчика практично во всьому його робочому діапазоні.

Раніше запропоновувалися для цього додаткові прилади або схемні рішення. Тут же з'являється можливість отримання лінійної характеристики опісля першого перетворення. Такий спосіб дозволить значно спростити подальші схеми обробки інформації, та завдяки цьому зменшити методичні похибки.

Також балка може бути у вигляді перекрученого шестикутника на кожен грань якого закріплені тензоперетворювачі, що дозволяє більш точно проводити вимірювання. Крок скрутки має дорівнювати ширині однієї грані. При цьому розташуванні тензоперетворювачі і системному підході до знімання з них інформації, отримано можливість з однаковою точністю зняття показань вібродатчика практично з будь-якого напрямку – багатовекторно (див. рис. 4.3).



1-тензоперетворювач; 2-кріплення; 3-шестигранна балка вібратора;
4 - балансир; 5 - місце зварювання; 6 - отвір для кріплення

Рис. 3. Вібродатчик з тензометричним перетворювачем на балці шестигранного типу:
а - з одним тензоперетворювачем; б - з двома симетричними тензоперетворювачами

Попередні дослідження, що були проведені у середовищі MatLAB, надали результати, які наведено на рис. 4. Математичні функції перетворення описані у попередніх виданнях [1, 2]. Дослідження напряму максимальної амплітуди вібрації датчика з чотиригранною балкою прямого типу з двома тензодатчиками дало надто звичайні результати, крім того похибка визначення кута (напряму)

максимальної амплітуди складала майже $8,5^\circ$, при заданому куті 220° . (На рис. 4 не наведено). Результати більшої точності показали дослідження багатовекторного тензодатчика. Тут було визначено напрям максимальної амплітуди датчика з вісім граню балкою прямого типу (рис. 1,а) та датчика з вісім граню балкою зі зарученими гранями (рис. 4,б) [2].

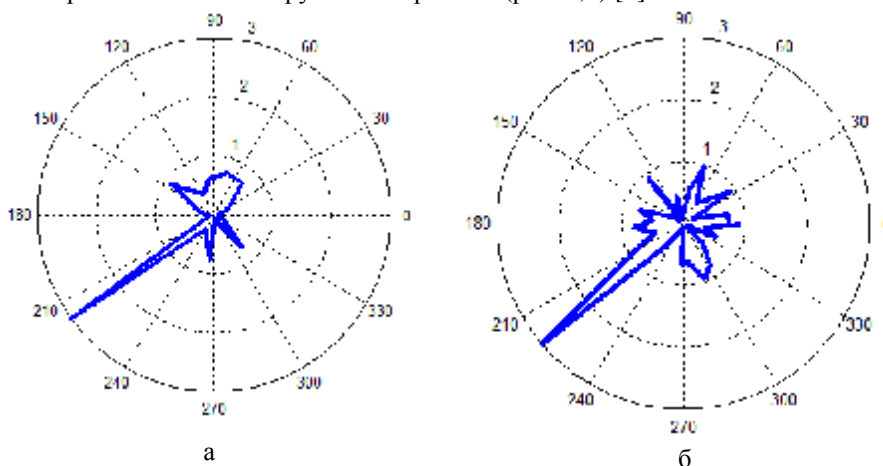


Рис. 4. Моделювання роботи багатовекторного тензодатчика: а – діаграма визначення напрямку максимальної амплітуди датчика з вісім граню балкою прямого типу та б – датчика з вісім граню балкою зі зарученими гранями

3 Висновки

Запропоновані багатовекторні тензодатчики дозволяють додати до звичайних параметрів вібрації вектор (напрямок) максимальних пульсацій. В такий спосіб багатовекторні датчики вібрації дозволяють з високою точністю визначити причину виникнення (збільшення) вібрації приладу, що досліджується. Визначення вектору вібрації корисно впливає до налагодження механізмів та приладів, а простота конструкції дозволяє бути таким засобам більш доступними.

Література (References)

1. Лещенко О.И. Исследование вибрационных характеристик поверхностного вибратора / О.И. Лещенко, И.И. Садковская // Тези доповідей ІХ Міжнародної науково-практичної конференції “Військова освіта і наука: сьогодення та майбутнє” / за заг. редакцією В.В. Балабіна. – К.: – ВІКНУ, 2013. – 378 с.
2. Multivectorial differential transformers of vibration of the informative measuring system / Лещенко О.І., Банзак О.В., Зборовська І.А., Садковська І.І. Збірник наукових праць Одеської державної академії технічного регулювання та якості 2(5). Одеса, 2014. С. 84 - 88.
3. Лещенко О.І. Методи вимірювання параметрів вібрацій / О.І. Лещенко, І.І. Садковська, І.А. Зборовська // Технічне регулювання та якість: сучасний стан,

проблеми і перспективи: матеріали П'ятої Всеукраїнської науково-практичної конференції молодих вчених і студентів. Одеса, 20-21 травня 2014 р. – Одеса: ОДАТРА, 2014. – С. 162-163.

4. Фрайден Дж. Современные датчики: справочник / Дж. Фрайден. – М.: Техносфера, 2005. – 152 с.

Застосування Системи Підтримки Прийняття Рішень при Проведенні Лікарсько-Діагностичних Заходів

Георгій Мумладзе¹, Анатолій Поворознюк²

¹НТУ"ХП", Харків, Україна

²д.т.н., професор, НТУ"ХП", Харків, Україна

gr.mumladze@gmail.com

ai.povoroznjuk@gmail.com

Abstract. Розглянуте поняття фармакологічних дій, та його зв'язок із діагностичними станами. Був запропонований механізм для переведення діагнозів із простору діагностичних ознак в простір фармакологічних дій. Розроблена структурна схема системи підтримки прийняття рішень, що повинна надавати підтримку на протязі всього лікувально-діагностичного процесу.

Keywords: комп'ютерна система, прийняття рішення, діагностика, лікування, лікарське дія, лікарська помилка, діагностична ознака, вирішальне правило.

На теперішній час спостерігається перехід від традиційних медичних інформаційно-пошукових систем до інтелектуальних комп'ютерних систем підтримки прийняття рішень в медицині із розвиненим математичним апаратом та елементами експертних систем.

Процес реабілітації пацієнтів складається з двох пов'язаних етапів: діагностики захворювання та лікування виявлених патологій. Дані етапи не мають чіткої границі, тому що після постановки діагнозу та призначення лікувального комплексу необхідно проводити постійний моніторинг процесу, для оцінки ефективності лікування та, при необхідності, його корегування.

Існує широкий спектр комп'ютерних систем, які застосовуються на етапі постановки діагнозу, проте на етапі медикаментозної реабілітації підтримка зазвичай обмежується довідником фармацевта. При цьому прийняття неправильного рішення, як на етапі діагностики, так і на етапі медикаментозної реабілітації, може призвести до трагічних наслідків для здоров'я пацієнта.

В таких системах діагностика захворювань зводиться до задачі класифікації стану пацієнта при аналізі вектора діагностичних ознак X_i (симптомокомплексу), при чому результатом діагностики i -го пацієнту D_i може бути деяка кількість альтернативних захворювань.

При такому підході мінімізується ризик неправильного визначення діагнозу, але ризики, що виникають під час лікувальних заходів, не враховуються. Тому

задача мінімізації ризиків при комплексній оцінці всіх етапів лікувально-діагностичного процесу на сьогоднішній день являється актуальною.

Метою роботи є розробка системи підтримки прийняття рішень на етапах діагностики і лікування, в якій реалізовано синтез бінарного дерева рішень по критерію мінімуму помилок в призначенні комплексу лікарських препаратів.

Для диференційної діагностики в заданій предметній галузі необхідно синтезувати бінарне дерево рішень в кожній вершині якого реалізовано ймовірнісне вирішальне правило, за допомогою якого визначається один з альтернативних потомків на основі аналізу діагностичних ознак.

Синтез дерева рішень зазвичай виконується по критерію мінімізації помилок першого та другого роду, які залежать від розташування еліпсоїдів розсіювання в просторі ознак.

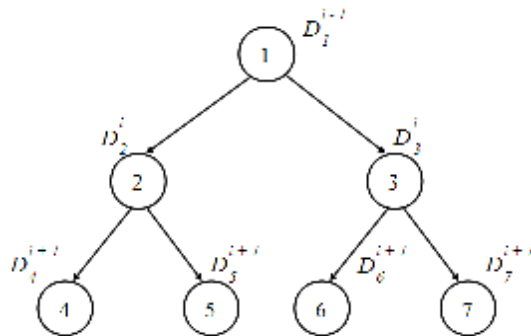


Рис. 1. Бінарне дерево рішень для постановки діагнозу

При комплексній оцінці необхідно використовувати критерій мінімізації помилок в призначенні комплексу лікарських препаратів.

Враховуючи те, що кожний діагноз характеризується вектором необхідних фармакологічних дій, які повинні бути покриті комплексом лікарських препаратів з урахуванням їх несумісності та індивідуальної непереносимості, в роботі пропонується перехід з традиційного простору діагностичних ознак у простір фармакологічних дій.

На даному етапі виконується вибір необхідної предметної області медицини, її аналіз та формування множини вхідних даних для подальшої обробки.

Література (References)

1. Поворознюк А.І. Інформаційні технології підтримки прийняття рішень в медичній діагностиці на основі синтезу структурованих моделей : автореф. дис. на здобуття наук. ступеня доктора техн. наук: спец. 05.13.06 "Інформаційні технології" / Поворознюк Анатолій Іванович. – Харків, 2011. – 39 с.
2. Поворознюк А.И. Системы поддержки принятия решений в медицинской диагностике. Синтез структурированных моделей и решающих правил / А.И. Поворознюк – Saarbrücken Germany: LAP LAMBERT Academic Publishing GmbH & Co. KG, 2011. – 314 с.

Проблеми Впровадження Інформаційних Технологій у Навчальний Процес

Ігор Михайлюк

Прикарпатський національний університет імені Василя Стефаника, Україна
igor.mihailyuk1994@gmail.com

Abstract. Відзначено необхідність реформування освіти в Україні шляхом проведення її інформатизації. Розглянуто завдання інформатизації освіти з врахуванням реалій сьогодення.

Keywords: Інформатизація освіти; Інформаційні технології; Реформування освіти.

1 Вступ

Аналіз сьогоденної української системи освіти вказує на потребу проведення модернізації змісту освіти для приведення її у відповідність до сучасних потреб суспільства. Особливу увагу слід приділити середній освіті, яка є центральною ланкою в освітній системі країни та основою для успішного здобуття освіти наступних рівнів й самоосвіти протягом усього життя. Саме тому першочергово важливим є проведення реформи освіти, що буде готувати всебічно розвинену, здатну до критичного мислення цілісну особистість, патріота з активною позицією, інноватора, здатного змінювати навколишній світ та вчитися впродовж життя. Одне з головних завдань освіти в умовах розвитку інформаційного суспільства — навчити учнів і студентів використовувати сучасні інформаційні та комунікаційні технології.

За останні роки вимоги, що висуваються до освіти, змінилися: крім базових знань і постійного оволодіння новими навиками сучасний працівник повинен вміти продуктивно використовувати інформаційні ресурси. Тому забезпечення дітей можливістю використовувати сучасні інформаційні технології в навчальному процесі є одним із важливих факторів, що суттєво впливають на можливість одержання якісної освіти.

Аналіз напрямків реформування освіти і можливостей застосування інформаційних технологій під час їх здійснення, дає підстави стверджувати, що вирішальним чинником досягнення основних цілей реформування освіти є її інформатизація. Ефективні системи інформатизації освіти можуть бути створені, якщо вони базуються на дослідженні видів діяльності, що здійснюються в системі освіти, і враховують як сучасний стан, так і можливі трансформації освіти у процесі її реформування, перспективи розвитку галузі

інформаційних технологій, останні досягнення педагогіки, психології та інформаційних технологій.

2 Інформатизація освіти як основа впровадження інформаційних технологій в процес підготовки фахівця

Інформатизація освіти визнана одним із пріоритетних державних завдань і повинна здійснюватися згідно з єдиними державними нормативами, враховуючи при цьому особливості наявної системи освіти в Україні.

Виділимо основні завдання інформатизації освіти:

1). достатнє фінансування освіти, забезпеченість та постійне вдосконалення програмних і технічних засобів з урахуванням досягнень педагогічних, психологічних і технічних наук, спрямованих на спрощення пошуку необхідних знань, їх засвоєння і практичне застосування;

Упродовж останніх років Україна витрачає на освіту з бюджету різних рівнів, включно із спеціальними фондами приблизно 5,3% валового внутрішнього продукту (ВВП), а видатки на освіту з Державного бюджету не перевищують 3% ВВП. Для порівняння, країни Європи, які мають якісну освіту, зокрема Фінляндія і Швеція, витрачають на освіту до 7,5% свого ВВП. У 2013 році бюджетна забезпеченість одного учня школи склала 8123 гривні, що у доларовому еквіваленті складало близько 1000 дол. У 2016 році бюджетна забезпеченість 1 учня в Україні складає близько 10 тисяч гривень, що у доларовому еквіваленті складає приблизно 400 дол., тоді як у Європі – 6,8 тис. євро.

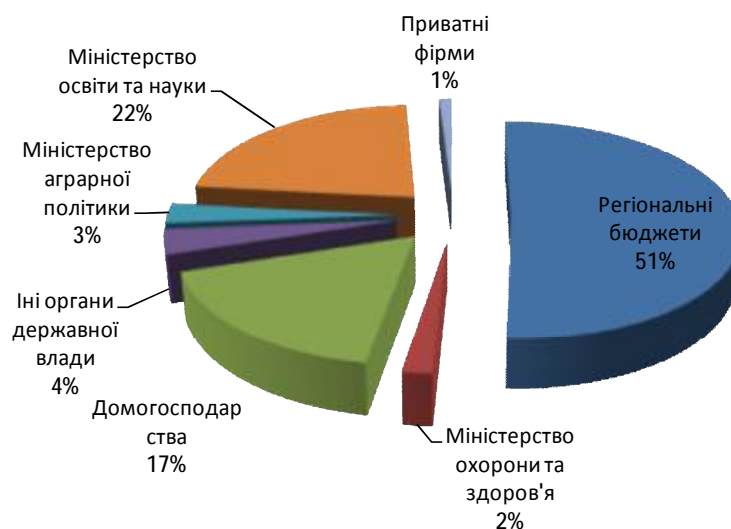


Рис. 1. Структура загальних витрат на освіту за фінансуючими організаціями в Україні

2). підвищення рівня комп'ютерної та інформаційної грамотності населення;

Констатувальний експеримент виявив низький рівень мотивації вчителів щодо використання комп'ютерів, невдоволеність відсутністю достатнього рівня теоретичної та практичної готовності до використання комп'ютера як об'єкта вивчення і як засобу навчання. Високим і достатнім рівнем загальної і професійної комп'ютерної грамотності володіє тільки 13% вчителів, 62% респондентів зовсім не вміють користуватися комп'ютером. Серед причин такого стану – відсутність стійкої мотивації, а також потреби використовувати інформаційно-комунікаційні технології (ІКТ) у професійній діяльності, недостатня увага навчальних закладів до даного аспекту підготовки, відсутність вільного доступу до комп'ютерної техніки.

3). впровадження нових методів навчання із застосуванням сучасних ІКТ;

Основою зміни стилю мислення і ціннісних орієнтацій особистості майбутнього вчителя повинні стати підходи використання ІКТ в навчанні, системне застосування педагогічних програмних засобів, мультимедійних технологій, веб-ресурсів, Інтернет-ресурсів, що розроблені в системі освіти.

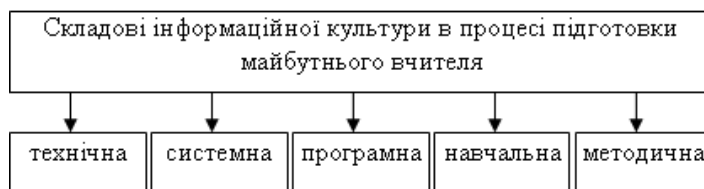


Рис. 2. Складові інформаційної культури

4). забезпечення можливості доступу населення до комп'ютерних і телекомунікаційних засобів, викорінення «інформаційної нерівності» між окремими регіонами, галузями економіки та різними верствами населення;

Згідно додатку 1 до наказу МОН від 29.06.2010 р. № 637 необхідна кількість комп'ютерів для оснащення навчального закладу ($\Pi_{\text{ІЗ}}$) визначається за наступною формулою:

$$\Pi_{\text{ІЗ}} = \sum (P_{\text{обов}} \times K_{\text{уч}}) + \sum (P_{\text{дод}} \times K_{\text{уч}}) / \text{Ч} \times K_{\text{роб}}, \text{ од.} \quad (1)$$

де

$P_{\text{обов}}$ – ресурс комп'ютерного забезпечення, необхідний для вивчення інформатики одним учнем/студентом протягом тижня відповідно до навчальної програми з інформатики, год.;

$K_{\text{уч}}$ – кількість учнів/студентів відповідної категорії, осіб.

$P_{\text{дод}}$ – ресурс комп'ютерного забезпечення, необхідний для проведення додаткових занять учнем/студентом відповідної вікової категорії протягом тижня відповідно до дозволених санітарно-гігієнічних норм (факультативні заняття, можливість доступу до мережі Інтернет у позаурочний час та інші), год.;

Ч – можливий час роботи комп'ютера на день, год.;

$K_{\text{роб}}$ – кількість робочих днів навчального закладу протягом тижня, днів.

Але реалії показують, що, якщо 97% шкіл України мають комп'ютерні класи, то на 40% вони вже морально й фізично застаріли, 13% з них взагалі несправні. Інший оптимістичний, на перший погляд, показник стосується Інтернету. Здавалось би, 87% шкіл мають доступ до всесвітньої мережі, але, як правило, користування шкільними комп'ютерами з підключеним Інтернетом обмежується уроками інформатики, а в ряді випадків ним може скористатись тільки керівництво школи.

5). створення єдиного інформаційного освітнього простору, який забезпечує доступність якісної інформації;

Створення єдиного інформаційно-освітнього простору, який включає сукупність технічних, програмних, телекомунікаційних і методичних засобів, дозволить застосовувати в освітньому процесі нові інформаційні технології і здійснювати збір, зберігання і обробку даних системи освіти. Даний простір здійснить підтримку освітнього процесу і автоматизацію управлінської діяльності, забезпечить підвищення якості освіти і будується на основі розвитку ІКТ компетенцій адміністрації, учителів і учнів.

Основними учасниками і користувачами єдиного інформаційно-освітнього простору мають бути: педагоги, учні, адміністрація школи, батьки.

6). підвищення рівня підготовки фахівців за рахунок покращення технологій навчання (впровадження в учбовий процес інформаційних, телекомунікаційних засобів, зокрема можливостей мережі Інтернет);

Загалом на підготовку кадрів та підвищення кваліфікації у 2017 р. припадає 24,34 млрд грн, з них лише 18,27 млрд грн – у віданні Міносвіти (МОН). На рис. 3. подано дані для порівняння рівня фінансування за останні 5 років.

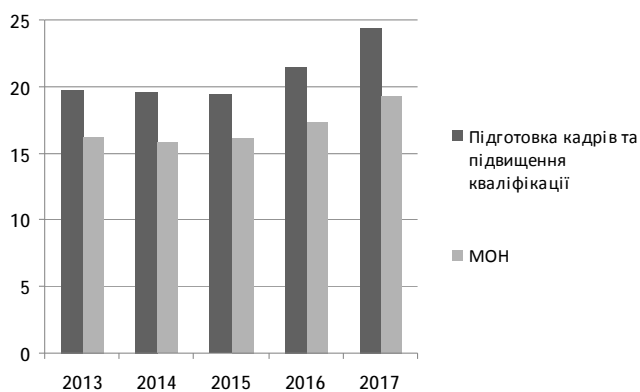


Рис. 3. Фінансування підвищення кваліфікації з бюджету освіти

7). адаптація інформаційних технологій навчання цілям та умовам навчального процесу;

8). розробка програмно-методичної основи застосування інформаційних технологій навчання, які сприяють активізації пізнавальної діяльності студентів та підвищенню їх мотивації;

При розробці прикладного програмного забезпечення для базової школи слід враховувати, що перш за все необхідно створити педагогічний програмний засіб для забезпечення навчання з врахуванням індивідуальним особливостей учнів та специфіки формування навиків.

9). формування навичок обробки, аналізу та перерозподілу інформації за допомогою інформаційних технологій з метою їх подальшого ефективного використання в самостійній професійній діяльності.

Слід згадати про старшу школу, де згідно реформи освіти очікується найбільше змін. Тут планується запровадити профільне навчання, яке передбачає чітку та реальну спеціалізацію навчання. Вже у 2015/16 навчальному році майже 200 навчальних закладів були профільними, що складало 38% від загальної кількості загальноосвітніх навчальних закладів. Із них 135 навчальних закладів (70%) є однопрофільними; 43 (22,5%) – реалізують профільне навчання за двома профілями, і лише 14 навчальних закладів (7,5%) забезпечують своїм учням вибір між трьома та більше профільними спрямуваннями.

Отже, проблема ефективного використання вчителями та викладачами сучасних інформаційних технологій особливо актуальна в наш час.

Ще одним із завдань інформатизації освіти є розробка спеціального програмного забезпечення, що враховуватиме досягнення психології щодо формування особистості, а також врахування під час розробки програм з інших навчальних предметів фактору впливу їх майбутнього використання на формування особистості.

Також важливим аспектом є організація навчально-виховного процесу за принципом дитиноцентризму і важливу роль тут повинні відігравати інформаційні технології. Уже сьогодні створені навчальні комп'ютерні програми і системи, які певною мірою спроможні адаптуватися до здібностей учня. Завданням інформатизації освіти у вирішенні цієї проблеми є створення спільно з педагогами і психологами навчальних комп'ютерних систем, які дозволять максимально наблизити навчання і виховання кожної дитини до її сутності, здібностей та особливостей. Особлива увага повинна бути приділена створенню навчальних комп'ютерних систем для дітей з особливими потребами. Природно, що в таких навчальних системах учитель (викладач) повинен бути не ментором, а партнером учня (студента) в навчанні та розвитку.

Проблеми, що постали на сьогоднішній день – це підготовка висококваліфікованих викладачів та фахівців у сфері ІКТ, оснащення закладів освіти сучасною комп'ютерною технікою, педагогічними програмними засобами, електронними підручниками тощо. Адже забезпеченість загальноосвітніх навчальних закладів комп'ютерною технікою в середньому по Україні становить дуже низка. Україна посідає одне з останніх місць за кількістю комп'ютерів у загальноосвітніх навчальних закладах (1,3 комп'ютера на 100 учнів). За індексом «готовності інформаційної інфраструктури» Україна посідає 82-ге місце серед 104 країн світу.

Вище наведені завдання свідчать, що інформатизація освіти є важливим засобом і складовою реформування освіти. Перехід системи освіти на якісно

новий рівень без її інформатизації просто неможливий. Водночас необхідно зауважити, що використання інформаційних технологій необхідне і корисне не лише у реформованій, але й у нинішній освіті.

3 Висновки

Система освіти є складною ієрархічною системою, цілі й правила функціонування якої встановлюються Законами та іншими нормативно-правовими актами України у сфері освіти. Досягнення поставлених цілей і реалізація встановлених правил забезпечується шляхом побудови відповідної організаційної структури системи освіти і здійснення в ній певних видів діяльності. Сьогоднішній стан освіти в Україні вказує на необхідність проведення її реформування, що включає інформатизацію освіти і відповідні зміни в структурі та діяльності в сфері освіти.

Для успішного вирішення проблем інформатизації освіти України доцільно комплексно проводити дослідження за вище зазначеними напрямками з широким залученням до виконання цієї роботи наукових установ академії педагогічних наук України, вищих навчальних закладів та виробників засобів ІКТ, потрібно визначити науково обґрунтовані вимоги до засобів інформатизації, які необхідні й достатні для вивчення навчальних предметів в обсягах, передбачених державними стандартами загальної освіти, а державі забезпечити такими засобами всі навчальні заклади, що надають загальну середню освіту, згідно з єдиними нормативами.

Література (References)

1. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року № 537. <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi>.
2. Кремень В.Г. Суспільство знань і якісна освіта. Всеукраїнський громадсько-політичний тижневик «Освіта». № 13 – 14 (21–27 березня 2007 р.)
3. Богатырь Б.Н. Система образования России как объект информатизации. Школа-семинар «Создание единого информационного пространства системы образования» (г. Москва, 3–5 нояб. 1998 г.). М.: Исследовательский центр проблем качества подготовки специалистов (1998).
4. Гончаренко С.У. Український педагогічний словник. К.: Либідь (1997).
5. Жук Ю.О. Системні особливості освітнього середовища як об'єкту інформатизації. Післядипломна освіта в Україні. № 2. (2002).
6. Бюджет освіти та науки 2016: що пропонує уряд. Аналітичний центр CEDOS. <https://www.cedos.org.ua/uk/osvita/biudzheth-osvity-ta-nauky-2016-shcho-proponuie-uriad>

Розробка Алгоритмічного та Програмного Забезпечення для Прогнозування Зміни Кількості Населення на Заданій Території

Мар'яна Бурак

Прикарпатський національний університет імені Василя Стефаника,
м.Івано-Франківськ, Україна
maryana613@ukr.net

Abstract. Запропонований спосіб прогнозування показників трудової міграції в Україні методом МНК.

Keywords: багатофакторна регресія , міграція, МНК.

1 Вступ

Різке скорочення чисельності населення України на тлі зростання чисельності населення всього світу породжує інтерес українського суспільства до сучасних проблем демографічного розвитку та його перспектив. На сьогоднішній момент в Україні спостерігається відтік молодого населення, так звана трудова міграція.

Розробка методів прогнозування міграції населення в Україні, що враховували б специфіку цього явища, перебуває на стадії становлення.

У даній роботі йтиме мова про використання методу найменших квадратів для прогнозування зміни кількості міграції населення на території України.

2 Постановка проблеми

На сьогодні існує багато статистичних методів дослідження, але не всі вони можуть якісно та достовірно відображати інформацію про досліджувані об'єкти. Для якісної оцінки прогнозування досліджуваних даних необхідно перевірити передумови методу, і в разі їх не виконання – змінювати на інший метод. На практиці ми спрогнозуємо міграційний рух населення України в залежності від зміни окремих параметрів (заробітної платні населення, індексу споживчих цін, безробіттю молодого населення, курсу національної валюти по відношенню до долара) та перевіримо передумови по правильності вибору МНК.

Для оцінки кількості трудових мігрантів за межами України, було використано дані з різних країн світу, оскільки державна статистика охоплює лише міграції, пов'язані зі зміною офіційного місця проживання. До того ж, статистика зареєстрованих міграцій показує рік реєстрації, а не рік фактичного

прибуття. Прогнозування майбутніх параметрів міграційних процесів також ускладнене тим, що не має 100 % достовірних даних.

3 Пропонований підхід

Для реалізації програмного коду було розглянуто незалежні випадкові величини X_1, X_2, \dots, X_m (заробітна платня населення, індекс споживчих цін, безробіття, курс національної валюти по відношенню до долара) і залежну величину Y (кількість мігрантів).

Багатофакторна лінійна регресія виглядає так: $Y = b_0 + b_1X_1 + \dots + b_mX_m + \epsilon$, b_0, \dots, b_m – параметри моделі, які потрібно оцінити, ϵ – не спостережувана випадкова величина. Отже, $Y = \{Y_1, \dots, Y_n\}$ – ряд спостережень за залежною змінною та за незалежними змінними, або факторами: $X_1 = (X_{11}, \dots, X_{1n}), \dots, X_m = (X_{m1}, \dots, X_{mn})$.

На підставі цих спостережень було побудовано лінійну багатофакторну модель за допомогою функції `summary.lm()` на мові програмування R (рис.1).

```
Residuals:
    Min       1Q   Median       3Q      Max
-4567.3 -650.7  161.6  1235.4  2084.2

Coefficients:
            Estimate Std. Error t value Pr(>|t|)
(Intercept) 5328.9836  7613.7663   0.700   0.4985
ISZ         -70.0870   70.9588  -0.988   0.3445
Ur          -556.0091  413.3793  -1.345   0.2057
Zplata       2.4374    0.8062   3.023   0.0116 *
kurs         0.7583    2.9926   0.253   0.8047
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1987 on 11 degrees of freedom
Multiple R-squared:  0.6221,    Adjusted R-squared:  0.4847
F-statistic: 4.527 on 4 and 11 DF,  p-value: 0.02095
```

Рис. 1. Таблиця лінійної багатофакторної моделі

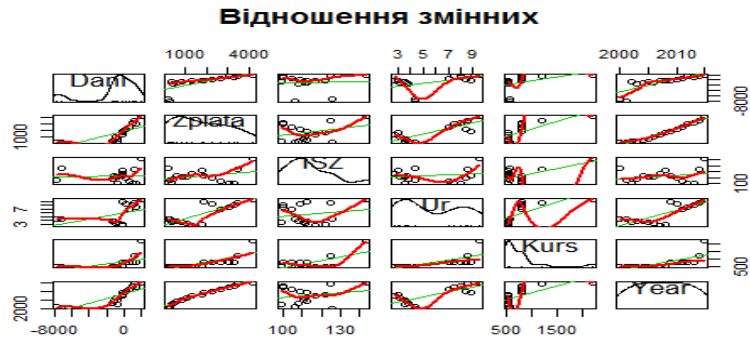


Рис. 2. Графіки відношення змінних

На рис. 1-2 зображено таблиці та графіки з отриманою моделлю. Для аналізу даних використано коефіцієнти R^2 . Чим ближче величина цих значень до 1, тим краще модель описує дані. У нашому випадку число $R^2 = 0,62$, а це означає, що отримана модель на 62% описує дані.

Також було проведено діагностику отриманої моделі. Введено початкові передумови МНК і перевірено модель (рис. 3-6). Передумови моделі: ненульова дисперсія, відсутність мультиколінеарності, незалежність Y , відсутність автокореляції, стабільність дисперсії помилок, нормальність.

lag	Autocorrelation	D-w	Statistic	p-value
1	0.3193581	1.240067	0.016	

Alternative hypothesis: rho != 0

Рис. 3. Таблиця автокореляції

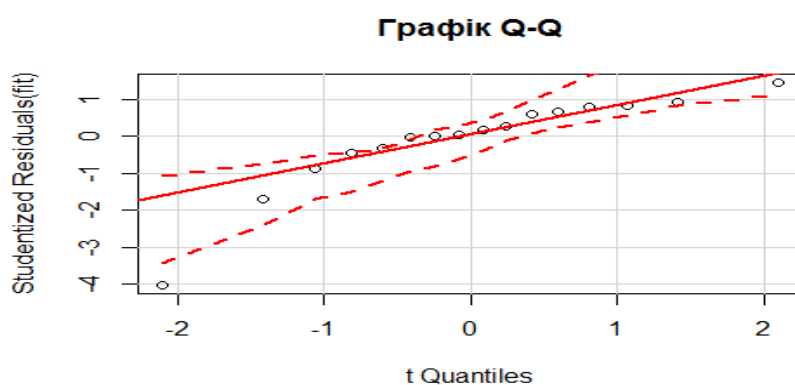


Рис. 4. Графік нормальності

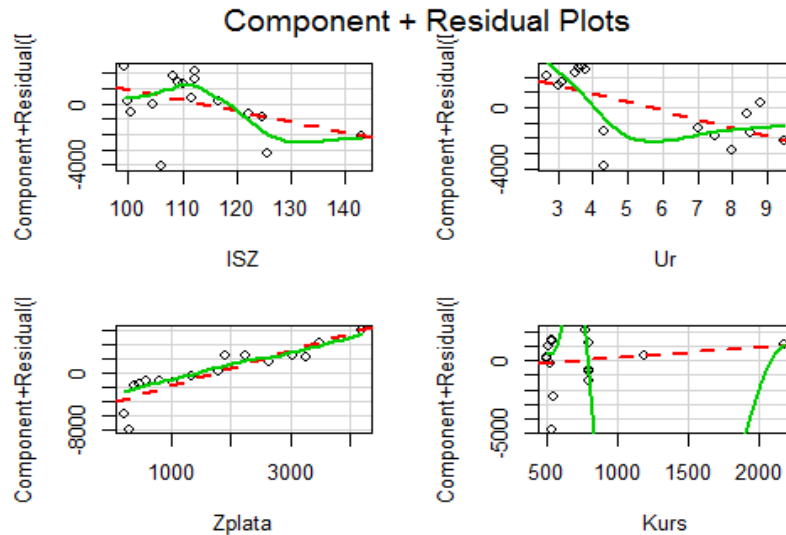


Рис. 5. Графік лінійності

ISZ	Ur	Zplata	Kurs
FALSE	TRUE	TRUE	TRUE

Рис. 6. Таблиця мультиколінеарності функції

4 Висновки

Розроблено програмне забезпечення для розв'язання проблеми міграційних процесів в Україні. Проаналізовано метод найменших квадратів, його доцільність застосування в досліджуваній роботі. Подальші дослідження будуть пов'язані із удосконаленням методів статистичного аналізу та удосконалення програмного пакету для вирішення поставлених задач.

Література (References)

1. Державне служба статистики України - Режим доступу: <http://www.ukrstat.gov.ua>
2. Malynovska O. : MIGRATION IN UKRAINE: FACTS AND FIGURES, Kyiv(2016) http://www.iom.org.ua/sites/default/files/ff_eng_10_10_press.pdf (дата звернення: 15.03.20017).
3. Світовий банк даних - Режим доступу: <http://data.worldbank.org/indicator/SM.POP.NETM?end=2012&locations=Z7UA&start=1962>

Прогнозування Відмов Відновлюваних Об'єктів з Ієрархічною Конструктивною Структурою

Я.М. Проценко¹, Т.В. Бондаренко²

¹Військовий інститут Київського національного університету імені Тараса Шевченка,
Київ, Україна

²Військовий інститут телекомунікацій та інформатизації, Київ, Україна
procenko_yarik@ukr.net
lenkov_s@ulr.net

Abstract. У статті аналізуються особливості моделювання процесів відмов-відновлень складного технічного об'єкта з ієрархічною конструктивною структурою. Для моделювання використовується імітаційна статистична модель (ІСМ), мета моделювання - прогнозування показників надійності (ПН) і вартості експлуатації (ВЕ) об'єкта. Вводяться поняття відмовляючих і відновлюваних елементів, пропонуються алгоритми і методика їх визначення. Показується, що достовірність прогнозування ПН і ВЕ із застосуванням ІСМ істотно залежить від правильності (оптимальності) визначення цих множин. Їх оптимальність розуміється в сенсі їх відповідності параметрам ремонтпридатності об'єкта. Наводиться приклад моделювання, на якому показується, як визначаються оптимальні множини відмовляючих і відновлюваних елементів, і як від них залежать прогнозовані оцінки ПН і ВЕ об'єкта.

Keywords: Відновлюваний технічний об'єкт, ієрархічна конструктивна структура, середнє напрацювання на відмову, питома вартість експлуатації, імітаційне статистичне моделювання.

Для складних об'єктів з ієрархічною структурою ефективність їх застосування за призначенням істотно залежить від показників надійності (ПН) і вартості їх експлуатації (ВЕ). Тому достовірне прогнозування ПН і ВЕ вельми важливо на всіх стадіях життєвого циклу таких об'єктів, крім того, ці об'єкти в перебігу періоду їх життєвого циклу, як при розробці, так і при експлуатації, постійно піддаються модернізації і, отже, вимагають постійних уточнень прогнозу ПН і ВЕ.

Питання впливу параметрів конструктивної структури технічного об'єкта на його ПН і ВЕ є недостатньо дослідженим і в той же час важливим. Хоча вплив очевидний, проте, не зовсім зрозумілий механізми і кількісні оцінки ступеня цього впливу. Для розробника складного технічного об'єкта важливо мати інструменти (методики) оцінки цього впливу і використовувати їх при прийнятті тих чи інших конструктивних рішень, а розробнику математичних

моделей, призначених для прогнозування ПН і ВЕ, необхідно розуміти механізми цього впливу щоб забезпечити адекватність розроблених моделей.

Для об'єктів, що мають ієрархічну конструктивну структуру, при моделюванні відмов виникає питання, відмови яких конструктивних елементів повинні імітуватися в імітаційній статистичній моделі (ИСМ). Моделювати відмови всіх простих елементів не доцільно, так як їх кількість дуже велика. Для будь-якого складового елемента при відомій конструктивній структурі завжди можна розрахувати необхідні для моделювання показники безвідмовності і потім використовувати їх в якості вихідних даних для ИСМ. Тому при застосуванні ИСМ вирішується завдання визначення вихідної множини конструктивних елементів, для яких повинно здійснюватися моделювання відмов.

Множина відмовляючих елементів E_0 – це підмножини конструктивних елементів, відмови яких повинні моделюватися (імітуватися) в ИСМ при прогнозуванні ПН і ВЕ об'єкта. Склад множини E_0 визначається користувачем і може їм регулюватися. Для забезпечення коректності обчислень множина E_0 має задовольняти вимогам повноти і ненадлишковості, суть яких полягає в наступному. Вимога повноти полягає в тому, що в множині E_0 повинні бути включені всі елементи, відмови яких можуть привести до відмови об'єкта. Вимога ненадлишковості полягає в тому, що будь-який шлях між коренем дерева і будь-якою його висячою вершиною повинен містити не більше одного елемента, що належить множині E_0 .

При відмовах об'єкта відновлення його працездатності здійснюється шляхом заміни елемента, що відмовив і при цьому не обов'язково замінюється конструктивний елемент, що відмовив - на практиці замінюється, як правило, елемент старшого конструктивного рівня, що вимагає найменших витрат часу на його заміну.

Множиною відновлюваних елементів E_0 є сукупність елементів, які підлягають заміні в процесі експлуатації об'єкта в разі виникнення відмов. На практиці завжди відновлюється (замінюється) або безпосередньо сам елемент, що відмовив, або елемент старшого конструктивного рівня, що його включає, якщо час заміни істотно менше, ніж час заміни елемента, що відмовив.

Множини E_0 і E_v є модельними поняттями і правильний їх вибір дуже важливий для адекватного моделювання процесів відмов-відновлень в ИСМ.

Відношення W встановлює відповідність між відмовляючими і відновлюваними елементами.

З метою формування оптимальних множин E_0 і E_v пропонується методика, що включає три наступних етапи:

На першому етапі проводиться попереднє формування множини E_0 та відношення W . Для кожного простого елемента формується шлях, що з'єднує висячу вершину з кореневою вершиною. Серед елементів відшукується і додається в множину E_0 елемент e , для якого час заміни має найменше значення і одночасно формується пара, яка додається в множину W . Сформована таким чином множина E_0 може бути надлишковою, в ній в можуть міститися елементи, що належать одному і тому ж шляху.

На другому етапі проводиться усунення надлишковості множини E_o . З цією метою формується допоміжна множина для перебору елементів вихідної множини (отриманої в результаті виконання алгоритму 1), і допоміжна ознака p , призначення якої буде пояснено нижче. Оператор 2 вибирає довільним чином з множини елемент (і відразу видаляє його з). Якщо елемент був єдиним, робота алгоритму на цьому завершується якщо ні, то повторюється доки не буде усунено надлишковості вихідної множини.

На третьому етапі відбувається остаточне формування множини (відношення) W . Раніше створена множина W перетворюється з урахуванням отриманої на другому етапі множини E_o . Проводиться перебір всіх простих елементів і для кожного елемента будується шлях, на якому знаходиться елемент, що належить одночасно E_o (такий елемент завжди є і він єдиний).

Розглянуті три етапи спільно реалізують методику формування оптимальних множин E_o і E_b , множина E_b в даному випадку існує неявно через множини (відношення) W .

Отримувані множини E_o і E_b є оптимальними для використання їх при моделюванні процесу відмов-відновлень, що в найбільшій мірі відповідає реальним властивостям ремонтпридатності об'єкта. Використання отриманих множин і в ІСМ забезпечує найкраще наближення процесу, що моделюється до реального.

Крім того, отримані за даною методикою множини E_o і E_b є оптимальними з точки зору мінімізації витрат машинного часу на моделювання, так як містить найменше число елементів і при цьому є повним.

Розглянуті алгоритми реалізовані в програмі ISMPN.

З метою забезпечення адекватності процесу моделювання відмов-відновлень об'єкта з ієрархічною конструктивною структурою та його відповідності реальним діям обслуговуючого персоналу під час проведення ремонтів, множини E_o і E_b повинні розраховуватися з урахуванням параметрів РП, за запропонованою методикою.

Вплив параметрів РП об'єкта на прогнозовані оцінки ПН і ВЕ об'єкта стає очевидним, так при поліпшенні якості РП відбувається відповідне поліпшення прогнозованих значень показників середнього напрацювання на відмову, середнього часу відновлення та питомої вартості експлуатації.

Представлена методика дозволяє забезпечити достовірне прогнозування ПН і ВЕ об'єкта, здійснюване із застосуванням ІСМ.

Література (References)

1. Прогнозирование надежности сложных объектов радиоэлектронной техники и оптимизация параметров их технической эксплуатации с использованием имитационных статистических моделей. Монография / С.В. Ленков, К.Ф. Борjak, Г.В.Банзак, В.О. Браун [и др.] : под ред. С.В.Ленкова. – Одесса : Изд-во «ВМВ», 2014. – 256 с.
2. Р. Фор, А. Кофман, М. Дени-Папен. Современная математика. М.: Изд. «Мир», 1966. – 272 с.

3. ГОСТ 27.005-97. Надежность в технике. Модели отказов. Основные положения. – Введ. 01.01.99. – 45 с.

Хмарні Обчислення в Мобільному Математичному Середовищі Sage

Ірина Абрамова

Прикарпатський національний університет імені Василя Стефаника,
м.Івано-Франківськ, Україна
ira_abramova_95@mail.ru

Abstract. Проаналізовано особливості мобільного математичного середовища на основі хмарних технологій, Web-систем комп'ютерної математики SageMathCloud та Sage. Систематизовано та узагальнено команди виконання обчислень, автоматизованого розв'язування задач з основних розділів математики та розподілених обчислень.

Keywords: хмарні обчислення, система комп'ютерної математики, обчислення, розподілені обчислення, Sage, SageMathCloud

1 Вступ

Хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, які можуть бути оперативно надані та забезпечені з мінімальними управлінськими затратами та зверненнями до провайдера послуг (за означенням Національного інституту стандартів і технологій NIST у США). Пристрій із підключенням до Інтернету може виконувати складні обчислення, використовуючи потужності віддаленого сервера та опрацьовувати дані, які зберігаються на ньому.

Значна ефективність застосування концепції мережецентричних обчислень може бути досягнута в математичних програмних засобах, які вимогливі до швидкодії комп'ютерної системи та інших характеристик. Прикладами програмних засобів математичного призначення, розроблених на основі хмарних технологій, є мобільні математичні середовища [1, 2], зокрема системи комп'ютерної математики (СКМ) Web-СКМ Sage, система Wolfram|Alpha, система динамічної геометрії GeoGebra, wxMaxima тощо.

Мобільне математичне середовище (ММС) – відкрите мережне програмне забезпечення, за допомогою якого надається можливість доступу до інформаційних ресурсів математичного і навчального призначення [1].

Основними характеристиками мережних систем комп'ютерної математики (СКМ) є [1]:

- відсутність необхідності встановлення обчислювального ядра СКМ на клієнтській машині;

- виконання обчислень на Web-сервері СКМ;
- відображення результатів у Web-браузері;
- індиферентність до використовуваного браузера;
- мобільний доступ до навчальних ресурсів, програм, даних та ін.

СКМ Sage – відкрите мобільне математичне середовище, яке є інтегратором різних математичних пакетів із забезпеченням спільного Web-інтерфейсу.

Різновидом такого типу систем, хмаро орієнтованих Web-СКМ, є SageMathCloud, хмаро орієнтована версія Web-СКМ Sage.

SageMathCloud - це онлайн сервіс, в якому виконуються математичні обчислення та розробка додатків в Sage або IPython Notebook.

Метою роботи є аналіз основних характеристик мобільного математичного середовища, базових конструкцій та обчислень в системі SageMathCloud (Sage).

2 Основна частина

Засоби Sage забезпечують виконання [3]:

- арифметичних операцій над числами та обчислення значень функцій, наближені обчислення із заданою точністю;
- операцій перетворення виразів;
- обчислення границь послідовностей і функцій;
- диференціювання та інтегрування функцій;
- розв’язування алгебраїчних та трансцендентних рівнянь аналітично, графічно та чисельно;
- розв’язування диференціальних рівнянь;
- операцій лінійної алгебри, зокрема дії з векторами і матрицями;
- обчислення комбінаторних виразів;
- побудови графіків функцій на площині та у просторі;
- створення інтерактивних інтерфейсів та розробку моделей з інтерактивними інтерфейсами для моделювання складних систем;
- виконання паралельних обчислень.

2.1 Арифметичні операції і команди присвоювання

Кожна команда Sage та SageMathCloud в діалоговому режимі вводиться з нового рядка або команди в межах рядка розділяються знаком “;”. Для виконання команд використовується комбінація клавіш Shift + Enter або кнопка Run.

У математичному середовищі Sage виконуються арифметичні операції і команди присвоювання, наприклад

```
sage: 2+2*2; a = 5; b = a + 2; c = b^2; c
```

Середовище забезпечує можливість використання вбудованих функцій:

```
sage: sqrt(3.4); sin(3.14); numerical_approx(exp(2))
```


Означення функцій користувача здійснюється за допомогою конструкції `def f(x): return <вираз>`.

2.2 Символьні вирази

З метою виконання перетворень символьних виразів попередньо необхідно оголошити символьні змінні. Оголошення символьних змінних здійснюється за допомогою функції `var`. Аргументом функції є рядок, що містить спеціальні змінні, вираз, наприклад `x=var('x')`.

До команд перетворення виразів належать: `expand (f)` - розкривання дужок у виразі `f`; `factor (f)` - розкладання на множники; `simplify (f)` – спрощення виразу `f`.

Диференціювання в символьному вигляді здійснюється із використанням функцій:

- `diff(f)` диференціює символьний вираз `f` по вільній змінній;
- `diff(f, v)` диференціює символьний вираз `f` по `v`;
- `diff(f, n)` і `diff(f, v, n)` диференціює `n` разів символьний вираз `f`;
- Символьне інтегрування здійснюється командою `int`:
- `int (f)` – інтегрування виразу `f` по незалежним змінним;
- `int (f, v)` – інтегрування виразу `f` по змінній `v`;
- `int (f, a, b)` – обчислення визначеного інтеграла на проміжку `[a; b]`;
- `int (f, v, a, b)` – обчислення визначеного інтеграла по зазначеній змінній.

При роботі з матрицями, векторами, многочленами і т. ін. існують засоби задання кільця, простору, алгебри, в якому відбувається робота: цілі числа, раціональні, дійсні, комплексні та ін.

2.3 Розв'язування рівнянь

Рівняння розв'язуються за допомогою функції `solve`. Для її використання спочатку означаються символьні змінні. Аргументами для `solve` будуть рівняння (або система рівнянь, розділених комою і записаних в квадратних дужках) і змінні, відносно яких потрібно знайти розв'язок.

Для чисельного розв'язування рівнянь використовується функція `find_root`.

`Sage` може використовуватися для розв'язання диференціальних рівнянь, за допомогою команди `desolve`.

2.4 Лінійна алгебра і алгебраїчні структури

У системі `Sage` підтримуються стандартні конструкції з лінійної алгебри. Для створення матриці використовується функція `matrix`. Об'єкти подаються у вигляді матриць (`matrix() objects`) і векторів (`vector() objects`).

З матрицями в середовищі `Sage` можна проводити наступні операції: додавання, віднімання, множення, піднесення до степеня, транспонування. Для виконання арифметичних операцій з матрицями достатньо поставити між ідентифікаторами матриць відповідний знак операції.

Обчислення визначника здійснюється командою `det(M)`, де M – ідентифікатор матриці. Транспонування матриці виконується за допомогою команди `transpose(A)`.

Системи лінійних рівнянь розв'язуються, знаходженням оберненої матриці і множенням оберненої матриці на вектор-стовпець вільних членів за допомогою функції `inverse()` або запису $A \setminus v$.

2.5 Розподілені обчислення

ММС Sage містить засоби реалізації паралельних і розподілених обчислень. Модуль для розподілених обчислень дозволяє будувати ефективні розподілені системи різного призначення [4].

Організація паралельних обчислень у Sage можлива на трьох рівнях:

- 1) рівень комунікаційної бібліотеки (MPI);
- 2) рівень бібліотек Sage (pynex, python);
- 3) рівень користувача (DSage, Ipython).

Розподілені обчислення реалізуються за клієнт-серверною технологією за допомогою пакету DSage (Distributed Sage).

Для паралельних обчислень використовуються декоратори інтерфейсу `@fork` та `@parallel` [4]. Декоратор `@fork` при виклику створює підпроцеси і розділяє на паралельні підпроцеси. Декоратор `@parallel` є функцією паралельного інтерфейсу і викликається зі списком входів, значення яких обчислюються паралельно.

Таким чином, в роботі проаналізовано основні можливості мобільного математичного середовища на основі хмарних технологій SageMathCloud та Sage. Здійснено систематизацію та узагальнено команди виконання обчислень та розв'язування задач з основних розділів математики. Проаналізовано засоби реалізації та використання розподілених обчислень.

Література (References)

1. Інноваційні інформаційно-комунікаційні технології навчання математики: навчальний посібник / В. В. Корольський, Т. Г. Крамаренко, С. О. Семеріков, С. В. Шокалюк; науковий редактор академік АПН України, д.пед.н., проф. М. І. Жалдак. – Кривий Ріг: Книжкове видавництво Киреєвського, 2009. – 2009. – 316 с.
2. Словак К. І. Мобільні математичні середовища як засіб хмарних технологій / К. І. Словак // Хмарні технології в освіті : матеріали Всеукраїнського науково-методичного Інтернет-семінару (Кривий Ріг – Київ – Черкаси – Харків, 21 грудня 2012 р.). – Кривий Ріг : Видавничий відділ КМІ, 2012. – С. 131–132.
3. Sage Tutorial in Russian. Выпуск 7.5. янв, 12, 2017. Режим доступу http://doc.sagemath.org/pdf/ru/tutorial/SageTutorial_ru.pdf.
4. Sage Reference Manual: Parallel Computing Release 7.6. Mar 25, 2017. Режим доступу <http://doc.sagemath.org/pdf/en/reference/parallel/parallel.pdf>.

Сервіс для Створення Інтерактивних Завдань LearningApps

Андрій Маринець

Прикарпатський національний університет імені Василя Стефаника,
м.Івано-Франківськ, Україна
andrii.marynets@gmail.com

Abstract. Проаналізовано систему для підтримки навчального процесу LearningApps, яка дозволяє створювати інтерактивні завдання, електронні наочні посібники. Наведено шаблони інтерактивних завдань та засоби дистанційного спілкування. Розроблено тестові завдання в данному сервісі.

Keywords: Інтерактивний додаток, інтерактивне навчання, LearningApps.

1 Вступ

На сучасному етапі розвитку інформаційно-комунікаційних технологій розроблені і широко використовуються спеціалізовані програми для підтримки інтерактивного навчання. Сервіси пропонують інтерактивні програми, які не потрібно завантажувати та встановлювати.

Інтерактивне навчання – це спеціальна форма організації пізнавальної діяльності, діалогове навчання [1]. Інтерактивне навчання має багато переваг перед класичним.

Інтерактивний додаток – додаток який взаємодіє з користувачем в режимі реального часу. Може використовуватись в різних галузях, від навчання до виробництва.

LearningApps – це сервіс Web 2.0 для підтримки процесів навчання та викладання за допомогою інтерактивних модулів. Ці модулі можуть використовуватись безпосередньо як навчальні ресурси або для самостійної роботи [2]. Даний сервіс або система являє собою конструктор для розробки інтерактивних завдань з різних дисциплін.

Сервіс LearningApps має простий у використанні інтерфейс, підтримує багатомовність і можливість проходити курси без попередньої реєстрації. Ресурси з подібним функціоналом для створення завдань різними мовами відсутні.

Сервіс має 20 готових базових шаблонів та 5 додаткових інструментів.

2 Основна частина

Для створення вправ потрібно зареєструвати нового користувача. Після цього надається можливість як переглядати існуючі модулі, так і розробити вправу самостійно обравши відповідний пункт меню та існуючий шаблон.

В сервісі є можливість створювати додатки різні за складністю, такі як вікторина (запитання з можливістю дати кілька правильних відповідей та вставки мультимедійного контенту: зображення, аудіоматеріалів та відеоматеріалів); знайди на картці (у цій вправі на мапі розташовуються мітки-питання у вигляді тексту, зображення, аудіо-або відеоелементів); pinboard («пробкова дошка») – інструмент запису текстових заміток і завантаження файлів з імітацією прикріплення канцелярськими кнопками до пробкової дошки; etherpad – онлайн редактор, в якому може спільно працювати кілька інтернет-користувачів; аудіо / відеоконтент – інструмент, що дозволяє не тільки завантажувати аудіо / відеофайли, але вбудовувати їх у додатки; класифікація; пазли; упорядкування; заповнити пропуски; тестові відповіді; кросворди тощо.

Із використанням сервісу розроблено декілька вправ для ознайомлення з системою. Розроблений модуль для закріплення знань з інформатики з теми “Будова та програмне забезпечення комп’ютера” містить 15 вправ (рис. 1). Результатом роботи є аплікація доступна в Інтернеті або викладена на сайт.



Рис. 1. Приклад інтерактивної вправи

При розробці завдань використано шаблони наступних типів: колекція вправ, знайти пару, фрагменти зображення, скачки, пазл, вікторина, заповнити пропуски, числова пряма. Дану аплікацію можна зробити загальнодоступною або захистити паролем.

Також розроблено 6 вправ для закріплення навичок з теми “Бази даних”, які можуть бути використані при вивченні інформаційних технологій.

Література (References)

1. Інтерактивні методи навчання – запорука розвитку творчої особистості: метод. посіб. / [упоряд. М. Трачук]. – Чернівці, 2013.
2. LearningApps.org – создание мультимедийных интерактивных упражнений. <http://learningapps.org/about.php>.

Побудова Векторно-Розгалужуючих Діаграм на Основі Чисел Фібоначчі

Михайло Петришин

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
m.l.petryshyn@gmail.com

Abstract. В роботі здійснено аналіз властивостей перетворення форми інформації на основі чисел Фібоначчі. Визначено можливі алгоритми перебігу процесу ПФІ. За допомогою векторно-розгалужуючих моделей виконано графічне моделювання процесу перетворення форми інформації на основі визначених алгоритмів.

Keywords: векторно-розгалужуючі діаграми; перетворення форми інформації, числа Фібоначчі.

1 Вступ

Вибір способу кодування повідомлень, який би враховував специфіку джерела інформації, задовольняв вимоги користувача і мінімально навантажував засоби інформаційного обміну та цифрової обробки є актуальним завданням на стадії розробки, проектування та впровадження розосереджених інформаційних систем. Метою проведених досліджень було моделювання процесів ПФІ на основі класичної системи Фібоначчі та їх методів кодування повідомлень.

2 Побудова векторно-розгалужуючих діаграм

Метод векторно-розгалужуючих діаграм (ВРД) в своїй основі застосовує індикаторне моделювання. Практика моделювання процесів ПФІ ґрунтується на здійсненні визначених процедур порівняння, що реалізуються за допомогою компараторів, які дозволяють визначити співвідношення невідомої величини з визначеною системою «еталонних величин» або «мір», чи то «шкалою», сформованою в «системі одиниць перетворення». Процес ПФІ зводиться до послідовних порівнянь невідомого значення величини з заданими визначеним чином значеннями системи «мір», що формуються як сумарне значення на кожному ітераційному кроці процесу перетворення. За результатами процесу ітераційних порівнянь формується кінцевий результат кількісної оцінки невідомої величини вхідного параметру перетворення [1].

3 Аналіз властивостей класичної системи Фібоначчі

Система числення Фібоначчі належить до класу позиційних систем, в якій значення ваг F_i розрядних коефіцієнтів визначаються рекурентним співвідношенням

$$F_i = F_{i-1} + F_{i-2}. \quad (1)$$

Довільне число N представляється сумою

$$N = a_n F_n + a_{n-1} F_{n-1} + \dots + a_i F_i + \dots + a_1 F_1, \quad (2)$$

де $a_i = \{0, 1\}$ – бінарні значення коефіцієнтів ваг розрядних позицій F_i , що формують наступну мережу значень ваг, n -розрядність коду (1)

.....	F_{13}	F_{12}	F_{11}	F_{10}	F_9	F_8	F_7	F_6	F_5	F_4	F_3	F_2	F_1
.....	233	144	89	55	34	21	13	8	5	3	2	1	1

Проаналізуємо моделі основних методів ПФІ з адитивним зрівноваженням на базі Фібоначчі алгоритму. Початкове перетворення невідомого значення вхідної величини x як наслідок прикладання ІЕ до i -го моменту перевищення значення суми позиційних мір $\sum F_i$ можливе (визначити місце i -го ітераційного кроку в діапазоні):

- від молодших розрядних значень F_1 до старших F_n ;
- від старших значень мір F_n до молодших F_i ;

зворотне перетворення після перевищення значення суми мір $\sum q_i$ значення невідомої вхідної величини x можливе:

- від молодших значень мір F_1 до старших значень F_{n-1} ;
- від старших значень мір F_{n-1} до молодших значень F_n .

Узагальнюючи існує 4 методи адитивного порівняння значення вхідної невідомої величини x з набором значень еталонних величин $\sum F_i$, значення яких становлять ряд, що формується сумою за формулою (1) [2].

4 Висновки

В даній роботі проаналізовано властивості Фібоначчі системи числення, яку доцільно використовувати в пристроях ПФІ через простоту формування рекурсивних чисел. Побудовано ВРД для 4 методів адитивного формування суми мір (1) визначено переваги та недоліки котрі унеможливають їх реалізації. Проте важливим відмінністю системи Фібоначчі є неоднозначне представлення чисел, що доведено в теоремі Цекенфорда.

Література (References)

1. Петришин М.Л. Застосування векторно-розгалужуючих схем в моделюванні процесів ПФІ/ П Міжнародна конференція “Комп’ютерна алгебра та інформаційні технології”, 21-26 серпня 2016.:Одеса, Україна. Тези доповідей / Одеський національний університет імені І.І. Мечникова.- Одеса, 2016. –С. 60.
2. Стахов А.П. Принцип асимметрии логики измерения. Проблемы передачи информации, №3, 1976 г.

Порівняння Фронтального Зображення Лиця із Двома Профілями

Ігор Голуб'як

Прикарпатський національний університет імені Василя Стефаника, Івано-Франківськ,
Україна
i.holubiak@gmail.com

Abstract. Наведено оглядовий алгоритм роботи системи. Проведено порівняння профільних зображень між собою та профільних із фронтальним. Запропоновано використання більшої кількості характерних ознак для порівняння.

Keywords: розпізнавання облич; характерні ознаки; коефіцієнт кореляції; каскадний детектор об'єкта.

1 Вступ

Теперішній час диктує вимоги до захисту інформації як особистою, так і інформації, яка є під грифом секретно. Великий внесок в захист інформації вносять біометричні системи ідентифікації особи, зокрема особливого поширення набувають системи розпізнавання особи за обличчям.

Зазвичай такі системи можна зустріти у великих організаціях з певною обмеженістю доступу. Простим прикладом є система безпеки вокзалу, в якій уже розпізнавання здійснюється при обробці масиву зображень облич отриманого з відеопотоку. Варто відмітити, що нові мобільні пристрої такі як телефони і ноутбуки та ін. все частіше використовують для введення доступу до користування системи ідентифікації за біометричними ознаками. Враховуючи той факт, що велика кількість людей має мету захистити свою інформацію, є інша сторона, яка шукає шляхи для обходу та викрадення даних в певних цілях. Оглянувши велику кількість методів, що застосовуються для ідентифікації особи за обличчям можна зауважити, що вони акцентовані на роботу «пропустити свого», проте рівень захисту від несанкціонованого доступу залишається не досить високим. Взявши до уваги те, що у системі, яка працює за відбитком пальця можна використати скопійований відбиток пальця на теплій поверхні, чи у системі з ідентифікацією по голосу можна записати голос носія, так і у системі, яка працює за ідентифікацією за обличчям достатньо буде скористатись гарним макетом обличчя, а саме якісною фотографією чи зображенням на смартфоні для того щоб отримати доступ.

Відтак актуальною тематикою дослідження буде створення нового алгоритму роботи методу, яка дозволить зробити систему більш захищеною від обману, а

також покращить саму роботи системи використовуючи більшу кількість характерних ознак та типів порівняння даних.

Варто відмітити, що обличчя людини не є симетричним, тобто права та ліва частина має певні відмінності форм. Звернувши увагу на цей факт можна припустити, що використання двох профілей зображення обличчя дасть змогу обробити більшу кількість характерних ознак для порівняння з еталонним зображенням. Більша кількість ознак дозволить покращити точність роботи системи.

2 Виділення характерних ознак

Для виділення характерних ознак зручно буде використати уже відомий метод Віоли Джонса. **Метод Віоли-Джонса**, запропоновано в [1] та дозволяє виявляти об'єкти на зображеннях в реальному часі. Метод добре працює при спостереженні об'єкта під невеликим кутом, приблизно до 30°. Точність розпізнавання з використанням даного методу частково досягає понад 90%, що є хорошим результатом. Слід відмітити велику кількість реалізацій даного методу, в тому числі у складі бібліотеки комп'ютерного зору OpenCV. У роботі [2] пропонується застосування даного алгоритму на новій технології GPU, яка може стати найшвидшою в обробці.

На даний час даний метод реалізований у програмі MATLAB. Розробник використав тулбокс, який дозволяє виділяти на зображенні обличчя очі, рот, ніс, губи. Даний тулбокс має назву - vision.CascadeObjectDetector [3].

Приклад виділення характерних ознак обличчя зображено на рис. 1 [4].

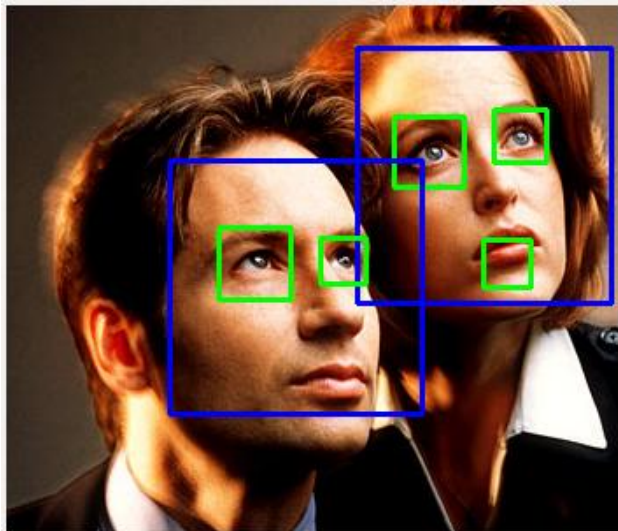


Рис. 1. Виділення характерних ознак обличчя за допомогою CascadeObjectDetector [4]

Оцифрувавши кожну характерну ознаку, тобто ніс, око, очі разом, губи та інші можна створити окремі порівнювальні елементи в базі даних, що дозволить порівнювати отримані зображення з еталонними як в цілому так і окремо один з одним, що дає можливість краще працювати при різному освітленні, тобто коли одна половина обличчя затінена, можливо здійснити часткове порівняння, по видимих областях рисунок 2 [5].

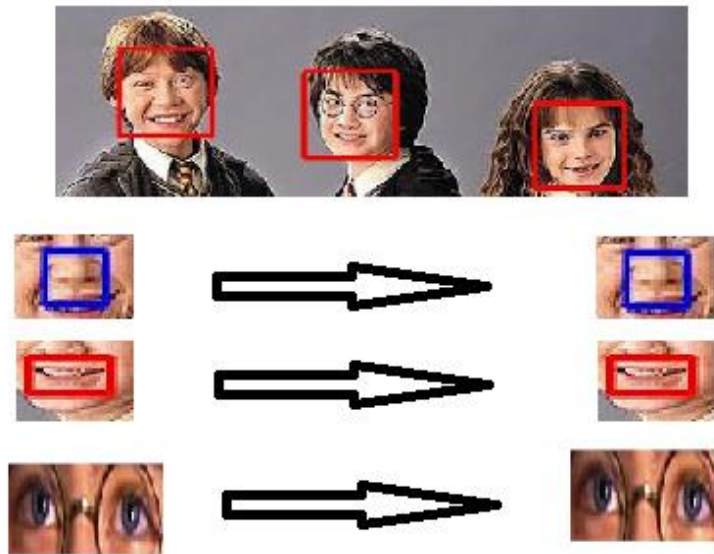


Рис. 2. Порівняння частин обличчя [5]

3 Порівняння реальних зображень

Для отримання зображень можна скористатись веб камерою. В даному випадку потрібно дві веб камери розташовані під певним кутом до обличчям для отримання профільних зображень.

Код програми:

```
% take an image
clc;
clear all;
close all;
[fname path]=uigetfile('.tif','Open a Face');
fname=strcat(path,fname);
im1=imread(fname);
a=im1;
% take an second image
[fname path]=uigetfile('.tif','Open a Face');
fname=strcat(path,fname);
```

```

im2=imread(fname);
b=im2;
a= imresize(im1,[118 118]);
a=imadjust(a);
b= imresize(im2,[118 118]);
b=imadjust(b);
a = gray2ind(a,16);
b = gray2ind(b,16);
c = corr2(a,b);
%finding the correlation
subplot(2,2,1);subimage(im1)
subplot(2,2,2);subimage(im2)
title (c)
if c==1
    disp('same') % display
else
    disp('not same')
end;
disp (c)

```

Провівши кореляцію між двома профільними зображеннями можна побачити що вони сильно різняться, також на це впливає різниця освітлення, відображено на рис. 3.

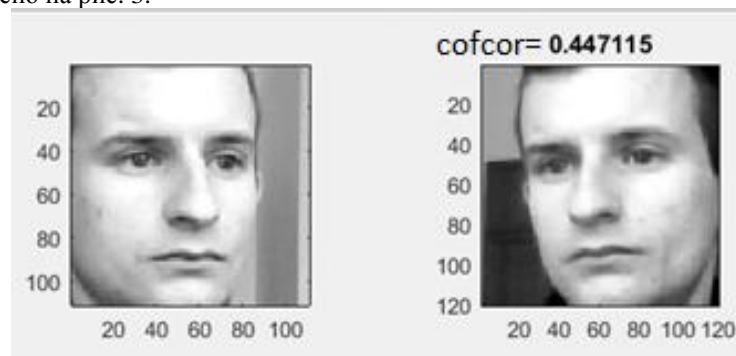


Рис. 3. Коефіцієнт кореляції двох профілей 0.44

Обернувши один із профілей дзеркально отримаємо кращий коефіцієнт кореляції, але все ж таки не рівний 1 в зв'язку з різним освітленням та важкістю добитись ідеальних умов зйомки рис. 4.

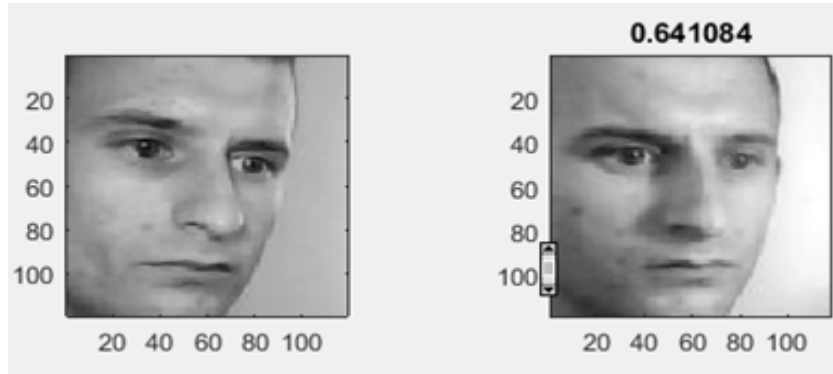


Рис. 4. Порівняння нормально та дзеркального профіля

Для покращення результатів, доцільно застосувати попередню обробку зображення.

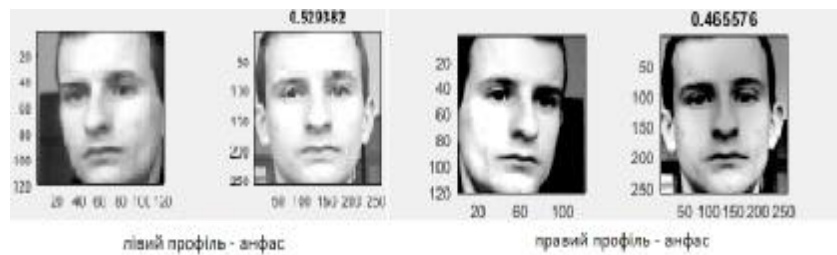


Рис. 5. Попередня обробка зображень, порівняння лівого та правого профілей з акцентом обличчя, коефіцієнт кореляції 0.46-0.52.

4 Висновки

Наведено оглядовий алгоритм порівняння зображень з використанням співставлення еталонному акценту двох профілей по чергово. Запропоновано в якості підвищення точності розпізнавання застосувати більшу кількість характерних ознак. Враховуючи використання профільних зображень отриманих із двох камер можна припустити, що така система не дозволить пропустити чужого з використанням в якості ключа фотографії особи.

Література (References)

1. Метод Виолы-Джонса (Viola-Jones) как основа для распознавания лиц, <https://habrahabr.ru/post/133826/>
2. Hefenbrock D.; Oberg J.; Thanh N.T.N. and oth. Accelerating Viola-Jones Face Detection to FPGA-Level Using GPUs, Field-Programmable Custom Computing Machines (FCCM),

- 18th IEEE Annual International Symposium (2010),
<http://ieeexplore.ieee.org/abstract/document/5474075/>
3. Train a Cascade Object Detector, <https://www.mathworks.com/help/vision/ug/train-a-cascade-object-detector.html>
 4. Hong K., Object detection: face detection using haar cascade classifiers, http://www.bogotobogo.com/python/OpenCV_Python/python_opencv3_Image_Object_Detection_Face_Detection_Haar_Cascade_Classifiers.php
 5. Face Detection - Matlab Code, <http://angeljohnsy.blogspot.com/2013/07/face-detection-matlab-code.html>

Технології Створення Інтерактивних Мультимедійних Електронних Книг

Анна Дранчук

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
dranchuk94@gmail.com

Abstract. У статті розглянуто питання актуальності використання електронних книг у сучасному інформаційному суспільстві та в освітньому процесі, зокрема; наведено огляд інформаційних технологій, які використовуються для створення інтерактивних мультимедійних електронних книг; описано основні принципи функціонування відповідних програмних продуктів, їх переваги та недоліки; окреслено перспективи їх використання та вдосконалення.

Keywords: Електронна книга, Програмне забезпечення, Інтерактивність, Мультимедійність.

1 Вступ

На сучасному етапі розвитку інформаційного суспільства значне місце у всіх сферах людської діяльності зайняли інформаційні та комунікаційні технології, які продовжують і надалі швидко розвиватися. В свою чергу, використання сучасних інформаційних технологій стало невід'ємною складовою організації освітнього процесу, що значним чином сприяє створенню передумов для творчого розвитку як педагогів, так і учнів. Дедалі більшої актуальності набуває питання можливості використання електронних підручників та посібників, які вже давно перестали асоціюватися із просто електронними копіями паперових відповідників [1, 2]. Взагалі кажучи, до поняття електронної книги різні автори підходять по різному [2, 3], однак безперечним залишається той факт, що електронна книга як інтерактивний мультимедійний продукт міцно вкорінюється у життєдіяльності людини і відкриває нові можливості для способів пізнання [4]. Оскільки розроблення електронної книги здійснюється шляхом поєднання тексту, графіки, аудіо та інтерактивних елементів, то процес створення такої книги вимагає фахових знань у галузі ІТ-технологій та володіння відповідними ІТ-компетентностями. У зв'язку з цим актуальним є питання аналізу наявних на ринку програм для розроблення інтерактивних мультимедійних електронних книг.

2 Огляд програмного забезпечення

EBooksWriter – зручний професійний інструмент для підготовки різнопланових електронних публікацій: книг, брошур, посібників користувача, каталогів. Пакет є повнофункціональним редактором, що забезпечує підготовку публікацій на візуальному рівні. У ньому є всі основні можливості текстового редактора: форматування символів і абзаців, застосування стилів (допускається створення нових стилів), робота з таблицями, вставка гіперпосилань тощо. Однак, на відміну від текстового редактора, EBooksWriter працює не з автономними сторінками, а з набором сторінок, що забезпечує ефективне управління гіпертекстовими зв'язками між сторінками [5].

Переваги: версія EBooksWriter Lite є безкоштовною, програма проста в освоєнні. Пакет забезпечує можливість використання широкого спектру матеріалів: тексту, зображень, музики, відео, кнопок, спливаючих вікон і т.п. Вбудовані в EBooksWriter потужні інструменти безпеки дозволяють виключити можливість читання публікацій для користувачів, які не мають ліцензії.

Недоліки: платні версії (ліцензія shareware) Standard, Pro і Gold мають набагато більше можливостей, зокрема версія Gold додатково підтримує flash-анімації та форми, має вбудовану галерею зображень, має розширені можливості пошуку, використання гіперпосилань, дозволяє застосовувати скрипти, а також дані версії не мають обмежень на об'єм публікації. Кількість опублікований сторінок у EBooksWriter Lite сягає тільки 20, що є суттєвим обмеженням, якщо є потреба створення великої е-книги. Не достатньо цікавий інтерфейс для використання даної програми учнями в школі.

Kotobee Publisher – програмне забезпечення, що дозволяє користувачам створювати інтерактивні електронні книги, які включають корисні інструменти, що працюють на декількох платформах. Готові електронні книги можуть бути експортовані як додаток для Android і IOS, або перетворені в веб чи настільні додатки. Зміст книги може бути розроблений з нуля або імпортований з PDF. Kotobee Publisher підтримує безліч інтерактивних об'єктів в межах сторінок, серед яких особливо цікавими є: In-page video, Audio regions, 3D interactive objects, Augmented reality, Interactive animations, Mathematical formulas, Interactive motion, Galleries and slideshows, Multiresolution images [6].

Переваги: мультиплатформенність, багато можливостей широкий спектр інтерактивних додатків, зручний та зрозумілий інтерфейс, можливість використання 3D технологій.

Недоліки: безкоштовна тільки пробна 30-денна версія, ліцензія shareware.

NeoBook – пакет, який володіє широкими можливостями для візуального створення публікацій і розрахований в першу чергу на професіоналів. Інтерактивність забезпечується за рахунок застосування різноманітних навігаційних елементів, з якими можуть бути співставлені певні дії, що виконуються при настанні деяких подій (наведенні курсору або клацання миші, вибору певного варіанту відповіді зі списку та ін.). Можливе застосування скриптів, що дозволяє застосовувати умовні переходи, цикли, файлові операції введення-виведення і інші мовні конструкції – формувати скриптові конструкції можна як на рівні програмного коду, так і у візуальному редакторі за допомогою вибору потрібних функцій зі списку.

Переваги: досить легко створювати інтерактивні багатосторінкові документи з зображеннями, текстовими блоками і навігаційними елементами у вигляді кнопок, check-боксів, полів для введення тексту, списків. Підтримує програвання звукових та відеофайлів, запуск анімаційних роликів (Animated GIF і Flash), відкриття Web-сторінок або діалогових вікон.

Недоліки: потрібен час, щоб освоїти інтерфейс програми. Програма розповсюджується за ліцензією shareware, безкоштовна тільки 30-денна пробна версія; для старіших версій Windows.

FlipSnack – безкоштовний сервіс для створення та публікації електронних книг, презентацій, журналів, каталогів онлайн. Створення публікації відбувається по кроках за допомогою майстра і не потребує спеціальних знань та великих затрат часу [2].

Переваги: Створена книга відображається у вигляді книги із розробленою обкладинкою з ефектом перегортання сторінок, як у паперовому носії, швидкою навігацією, можливістю масштабування.

Недоліки: Сервіс підтримує завантаження файлів лише у форматах PDF та JPG. Підтримки аудіо- та відеофайлів не розроблено. Сервіс не дає можливостей захисту вмісту книги. В безкоштовній версії сервісу книга зберігається на сайті компанії, її не можна завантажити на комп'ютер.

HTML Executable – потужний і універсальний HTML-компілятор, який конвертує веб-сайти (або будь-яку групу HTML сторінок) у EXE-файл. Сторінки можуть містити графіку, DHTML, JavaScript, Java аплети, CSS файли, текстові документи, анімаційні GIF файли, Flash анімацію, SWF, файли PDF, файли презентації PPT відео та звукові файли [4]. Програма дозволяє вибирати між трьома типами електронних книг: такі, що самі відкриваються; такі, що базуються на Internet Explorer; такі, що мають вбудований автономний HTML-переглядач (компілюються у EXE-файли та не потребують додаткового програмного забезпечення для перегляду).

Переваги: можна встановити пароль на запуск публікації, задати параметр відключення контекстного меню, захистити від копіювання, виділення, друку, а також створити обмежену, пробну і апаратно заблоковану публікацію.

Недоліки: можливість перегляду вихідного коду HTML, що може призвести до несанкціонованого копіювання. Для відображення PDF-документів, які містяться в електронній книзі, потрібно встановити Adobe Reader. Електронна книга з вбудованим автономним HTML-переглядачем не підтримує JavaScript. Для відкриття Flash-анімації та SWF-файлів, вбудованих в сторінки електронної книги, потрібний Adobe Player.

iBooks Author – програма, розроблена компанією Apple для створення продуктів електронного навчання. Як основу книги можна використати один з шаблонів та внести свої зміни. Шаблон має обкладинку книги, яка відображається в iBooks Store і на книжковій полиці читачів у програмі iBooks, зображення чи відео, яке відображається при відкритті книги, зміст, який генерується автоматично, глосарій, частини та розділи. Кожний шаблон містить кілька макетів частин і розділів, які можна налаштувати [7].

Переваги: програма є безкоштовною, в книгу можна імпортувати як глави чи розділ текстовий документ з редакторів Pages або Microsoft Word. Зміст книги генерується автоматично. Також можна сформувати Глосарій з посиланнями на

текст книги. Зміст створюється зі стилів змісту. У книгу можна вставити діаграми, таблиці, інтерактивні зображення, використовувати вбудовані шрифти, математичні формули з використанням розмітки LaTeX і MathML. Програма підтримує всі формати мультимедіа, які можуть відтворюватися в QuickTime, напр., mov, MPEG-4, MPEG-2, 3GPP, AVI (лише Motion JPEG) для відео та iTunes Audio (.m4a, .m4b, .m4p), MP3, WAV для аудіо фрагментів та ін.

Недоліки: програма працює тільки на платформі Mac OS X. Для відкриття файлу повинна бути встановлена програма iBooks Author. Публікацію можна захистити паролем на відкриття, проте немає інших параметрів захисту.

3 Висновки

Більшість сучасних програмних засобів для створення електронних книг розповсюджуються за ліцензією shareware, проте наявність безкоштовних версій надає широкий спектр можливостей, забезпечуючи інтерактивність та мультимедійність, що є важливою характеристикою сучасної електронної книги. Володіння технологіями створення електронних книг повинно бути однією із ключових компетентностей сучасного фахівця з IT-технологій.

Література (References)

1. Богданова И.Ф., Богданова Н.Ф. Технологии электронных книг. Сборник научных статей XVIII Объединенной конференции «Интернет и современное общество» IMS-2015, Санкт-Петербург, 23-25 июня 2015 г.
2. Гриценко С.С. Сучасні технології створення електронних підручників. Особливості розробки й використання електронних освітніх ресурсів. (2015). С. 185-188.
3. Женченко М. Типологічна класифікація електронних видань як науково-практична проблема. Вісник Книжкової палати (2016), № 8, С. 17-20.
4. Нестеренко О. А. Лонгрид як мультимедійний формат промоції книги. Лонгрид як мультимедійний формат промоції книги. Вісник Донецького національного університету Серія Б. Гуманітарні науки, [S.l.], n. 1-2, p. 178-183, arg. 2015. ISSN 1817-2253. <http://jvestnik-b.donnu.edu.ua/article/view/2571/2605>.
5. Ющик А. Обзор программного обеспечения для создания электронных книг <http://dspace.nuft.edu.ua/jspui/bitstream/123456789/16918/1/315.pdf>.
6. Interactive Ebook Creation. <https://www.kotobee.com>
7. Назаркевич М. А., Сторож О. В., Ключник І. І. Особливості розроблення інтерактивних електронних книг. Вісник Національного університету “Львівська політехніка”. С. 332-347. (2015).

Спільноти Google як Середовище Навчально-Виховного Процесу

Людмила Рішко

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
liudmyla_rishko@comp-sc.if.ua

Abstract. Розглянуто питання доцільності, ефективності та можливості використання спільнот Google в навчально-виховного процесі, що передбачає перетворення учнів з пасивних суб'єктів процесу навчання на його активних учасників.

Keywords: Спільноти Google; навчально-виховний процес; середовище; професійна діяльність.

1 Вступ

1.1 Аналіз попередніх досліджень

Проблеми й особливості використання Інтернет мережі у навчально-виховному процесі вищої школи для обміну знаннями розглядали в своїх роботах українські науковці: В. Биков, В. Кухаренко, Н. Морзе та ін. Серед робіт російських науковців із даного напрямку слід відзначити праці Д. Патаракіна, Ю. Еельма та ін. Провідні науковці, котрі працюють над цією проблемою зазначають, що соціальні сервіси дають можливість спільно створювати та редагувати навчальні ресурси не зважаючи на відстань і кордони. Використання спільнот у сфері освіти досліджують американські педагоги Л. Куркела та П. Сміт.

1.2 Мета цієї статті

Розглянути ефективність використання спільнот Google та їх можливості в навчально-виховному процесі.

2 Виклад основного матеріалу

В нинішніх умовах мережа Інтернет перестає бути засобом, що дозволяє лише одержати доступ до віддаленого ресурсу. Вона сама стає ресурсом, який вирішує нові педагогічні завдання: здійснювати навчальну діяльність,

знаходити навчальні матеріали в Інтернет тощо. Застосування Інтернету лише для пошуку інформації, зазначає Є. Патаракін, засвідчує, що його можливості використовуються тільки на 40%, решта 60% – це комунікаційні можливості Інтернет (мережеві комунікації). Використання технологій мережевих комунікацій у педагогічній практиці забезпечує якість навчального процесу, суть якого полягає в неформальній комунікації на основі повного доступу до аудіо-, відео-, графічної і текстової інформації всіх учасників навчального процесу [5, с. 45]. Спільноти Google змінюють звичні стереотипи використання глобальної мережі, що перестала бути середовищем передавання інформації і транспортним каналом постачання знань. Пасивна позиція «читача» (споживача інформації) змінюється на інтерактивну позицію «письменника» (коментатора, співучасника дискурсу, виробника інформації) [4].

Метою створення навчальної спільноти Google є досягнення певних дидактичних цілей, виконання педагогічних завдань, об'єднання суб'єктів та об'єктів навчального процесу для ефективної співпраці, орієнтованої на підвищення якості навчальних результатів учнів. Фактично вчитель може проектувати навчальне середовище під певний логічно завершений фрагмент навчання та з урахуванням пізнавальних можливостей, здібностей, інтересів і рівня попередньої навчальної підготовки конкретного учня.

До характеристик навчання за допомогою спільнот Google треба віднести: гнучкість, структурованість, інтерактивність, персоналізацію, вмотивованість, нову роль вчителя, інноваційну діяльність учня.

Гнучкість – учень може взаємодіяти з вчителем індивідуально, займатися у зручному для себе місці у своєму власному темпі і ритмі, приділяти кожній темі (уроку) стільки часу, скільки потрібно для засвоєння навчального матеріалу.

Структурованість – систематизація навчальних матеріалів, відповідно до навчальних планів і програм.

Інтерактивність – використання ЗК-технологій (комунікації, співпраці, кооперації) для обміну та опрацювання різноманітних даних.

Персоналізація – все навчання зорієнтоване на розвиток індивідуальних особливостей та потреб учня.

Вмотивованість – учень має бути мотивований, працьовитий, мати вміння і бажання працювати самостійно.

Нова роль вчителя – координатора персоналізованого розвитку учня та неперервного особистого розвитку.

Інноваційна діяльність учня – активна, динамічна, розумова і емоційна діяльність учня з використанням хмарних технологій як під час навчання, так і під час виконання домашніх робіт.

Ефективність використання соціальних сервісів полягає:

- у вмінні спілкуватися;
- здійснювати самостійний творчий пошук у розв'язанні навчальних проблем;
- розвивати успішну міжособистісну взаємодію у професійній діяльності та спілкуванні;

- проектувати навчальні й виховні заходи з використанням можливостей спільнот Google.

Використання спільнот є необхідним під час бурхливого розвитку цифрових технологій. Перехід учнів на рівень активних учасників навчально-виховного процесу надає можливості не тільки ефективно впроваджувати цифрові технології у професійну діяльність вчителя, а й розширити світогляд дітей. Учні з пасивних суб'єктів навчального процесу стають його активними учасниками. Бути членом навчальної спільноти, означає брати участь у взаємній навчальній діяльності, озвучувати нові ідеї та обмінюватися здобутими в процесі знаннями й досвідом. Навчання відбувається в процесі обговорення, роздумів, спільної роботи в команді. Таким чином, учні отримують підвищену відповідальність за своє навчання поза межами класної кімнати, в той час як викладачі - ширші можливості для організації навчання [1].

Використання соціальних сервісів у навчально-виховному процесі вищих навчальних закладів (середніх загальноосвітніх шкіл) визначається різними напрямками, а саме:

- як джерело навчального матеріалу;
- для планування й організації навчальної діяльності;
- для спільного написання творчих робіт, статей;
- як середовище для обговорення навчальних і методичних матеріалів, статей, підручників (посібників);
- для ознайомлення мережевої спільноти з авторськими методиками і технологіями.

Варто також зазначити психологічний аспект такого навчання. В інтровертних учнів є час подумати і поміркувати про матеріали і коментарі своїх однокласників до початку побудови своїх власних відповідей в Інтернеті. Вони можуть редагувати свої зауваження до публікації, на відміну від усної відповіді в класі. Ідеальна навчальна спільнота є безпечним місцем для прийняття ризику, вразливості і обміну різноманітних ідей. Всі учасники розділяють відповідальність за створення і підтримання цього середовища навчання [2; 3].

Спільнота відображає модель побудови людського товариства з характерними для нього атрибутами: соціокультурними цінностями, нормами спілкування, правилами соціальної поведінки. І головне завдання вчителя - не бути "головним", а допомагати кожному учневі проявити себе в новому середовищі, підштовхнути до групової роботи заради єдиної освітньої мети.

3 Висновок

Соціальні спільноти як нова форма навчальної та позаурочної праці і спосіб взаємодії з учнями швидкими темпами входять в життя педагогів, розширюючи виховний простір освітньої установи. Тому актуальними є дослідження спільнот

Google, можливості їх використання для навчання, соціального виховання та комунікативного розвитку учнів, підготовку молоді до життя в інформаційному суспільстві.

Література (References)

1. Caverly, D.C., & MacDonald, L. (2002). Online learning communities. *Journal of Developmental Education*, 25 (3), 36-37.
2. Брескіна Л. В. Професійна підготовка майбутніх вчителів інформатики на основі сучасних мережових інформаційних технологій. Дис. канд. пед. наук: 13.00.02 / Л. В. Брескіна // ПДПУ імені К.Д. Ушинського. –Одеса, 2003. – 178 с.
3. Smith, P.: Google+: First Thoughts and Potential Use in Education, *edSocial Media* (2011), <http://www.edsocialmedia.com/2011/07/google-first-thoughts-and-potential-use-in-education/>
4. Патаракин Е. Д. Сетевые сообщества и обучение / Е. Д. Патаракин. – М. : ПЕР-СЭ, 2006. – 112 с. 7. Ресурси мережі Інтернет [Електронний ресурс] – Режим доступу:–
<http://www.google.com.ua/url?sa=t&rct=&q=&esrc=s&source=Веб&cd=5&ved>.
5. Venosdale, K.: Google Plus: What does it mean for education, *Missouri State Teachers Association* (2011),
http://mostateteachers.typepad.com/missouri_state_teachers_a/2011/07/googleplus-what-does-it-mean-for-education.html

Особливості Застосування 3D-моделей в Навчальному Процесі

Ігор Колісник

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
kolisnyk_igor@comp-sc.if.ua

Abstract. У роботі обґрунтовано можливості використання 3D-моделей у навчальному процесі, зокрема у вивченні природничо-математичних дисциплін. Розглянуто ефективність та особливості упровадження 3D-моделей для унаочнення навчальної інформації з метою підвищення мотивації навчання та пізнавальної активності студентів.

Keywords: 3D-графіка; 3D-модель; мультимедіа; цифрові технології.

1 Вступ

Одним із напрямів підвищення якості освіти є інформатизація. Цей напрям полягає в широкому впровадженні в навчальний процес цифрових технологій і наукових досягнень, зокрема, мультимедійних технологій. Це дозволяє інтенсифікувати навчання, активізувати цікавість, підвищити інтерес до вивчення матеріалу.

Сучасні електронні освітні ресурси містять текст, графіку, фото, відео, аудіо, 3D-моделі тощо. Кожний із цих засобів володіє власним потенціалом, що виражається в термінах викладання та навчання, якому вони можуть ефективно сприяти. Тривимірна графіка (3D-графіка) та анімація займають особливе місце серед цифрових технологій. Актуальність обраної теми обумовлена широким використанням 3D-графіки та 3D-моделей в різних сферах людської діяльності. Застосування 3D графіки, у поданні навчального матеріалу, дозволить не лише швидше та якісніше засвоювати знання, але й збільшить зацікавлення до його поглибленого вивчення.

2 Постановка задачі

Метою статті є обґрунтування дидактичних можливостей використання 3D-моделей у вивченні природничо-математичних дисциплін, розкрити переваги їх порівняно із традиційними засобами та особливості застосування 3D-моделей у навчальному процесі.

3 Основна частина

Мультимедіа є новою інформаційною технологією, є сукупністю прийомів, методів, способів продукування, оброблення, зберігання, передачі аудіовізуальної інформації. Це дає нам змогу поєднати в одному програмному продукті текст, графіку, аудіо- та відеоінформацію, анімацію [1, с. 217]. Мультимедійні засоби розкривають нові можливості навчального процесу, вони характеризуються інтерактивністю й новизною та є одним із перспективних напрямів інформатизації навчального процесу.

Дослідження в різних країнах світу показують, що застосування звукових пристроїв збільшує обсяг засвоєної інформації на 15%, візуальних на 25%, а спільне їх використання вже на цілих 65% [5], під час використання технологій мультимедіа частка засвоєння навчального матеріалу підвищується до 75% [1].

Інтеграція сучасних цифрових технологій з природничо-математичними дисциплінами сприяє виникненню проблемних ситуацій, підвищенню ефективності проведення занять, розв'язання задач і вправ. Широке застосування мультимедійних засобів у навчанні доцільне для проведення експериментів, практичних занять, візуального інтерпретування діяльності, проведення досліджень з природничо-математичних дисциплін.

Мультимедійні засоби використовують на різних етапах навчання природничо-математичних дисциплін: під час пояснення нового матеріалу як ілюстрації, у процесі узагальнення й систематизації знань, повторення навчального матеріалу, контролю засвоєного матеріалу, в процесі підготовки до семінарів, позаурочних заходів. Основною перевагою цифрових технологій є те, що існують такі фізичні, хімічні й біологічні процеси або явища, які неможливо продемонструвати візуально в лабораторних умовах, тому використовують 3D-графіку, що імітує реальні процеси. Однією з безперечних переваг засобів мультимедіа є можливість проектування, створення й використання 3D-моделей. У освітньому аспекті 3D-модель може розглядатися як складова електронних освітніх ресурсів, що призначена допомогти користувачеві візуалізувати (наочно представити) об'єкт вивчення.

Основною перевагою 3D-графіки, є можливість взаємодії із моделями, тобто можна розглянути об'єкт з будь-якого ракурсу, видозмінити його, приховати деякі його частини тощо. Візуалізуючи деякий фізичний процес, можна змінювати вхідні дані, цим самим змінюючи результат експерименту [2]. Подання матеріалу у такій формі проходить досить наочно та живо, що збільшує зацікавлення у студентів (учнів). 3D-демонстрації дозволяють викладачу сфокусувати увагу студентів на темі заняття і допомогти їм отримати набагато більше знань, на відміну від традиційних методів викладання [3].

В порівнянні зі традиційними засобами відображення інформації, такими як схеми чи плакати, 3D-модель набагато краща для сприйняття, адже дозволяє роздивитися окремі частини об'єкту, його вигляд в цілому або в розрізі, заглянути у його середину.

Недоліками окремих традиційних засобів відображення інформації є: складні схеми, які містять кілька вузлів, зазвичай є дуже важкими для зрозуміння, тому

потребують достатньо багато часу на детальне вивчення. Фотографії, на відміну від схем, дозволяють зрозуміти апарат в цілому, але на фотографіях не зрозумілий вміст елементів і зв'язок між ними. Найкращим засобом відображення інформації є повномасштабний стенд, проте його вартість є досить високою. За допомогою стенду не можна вивчити принцип роботи об'єкта і, як правило, стенди займають досить-таки багато місця. У випадку вивчення будови волосини людини (без мікроскопа), чи вивчення якихось фізичних або хімічних процесів, які відбуваються на протязі багатьох років, такі стенди є непридатними до застосування. Саме тому 3D модель як найкраще підходить для вивчення будь-яких об'єктів і процесів. Для створення таких моделей найчастіше користуються програмою компанії Autodesk 3Ds Studio MAX, яка для навчання є безкоштовною [4].

Отже, освітні 3D-моделі, без всяких сумнівів – найкраще підходять для представлення різного роду інформації: моделей автомобілів, двигунів, архітектурних об'єктів, будови людського тіла, атома чи сонячної системи. За допомогою засобів мультимедіа можна побачити те, що у реальному житті ніколи б не побачив (наприклад, демонстрування роботи адронного колайдера, розкладання пластику чи зіткнення якогось небесного тіла з астероїдом). Застосування в навчальному процесі електронних мультимедійних освітніх ресурсів, що містять 3D-моделі, збільшить інтенсивність навчання, зробить його більш цікавим та ефективним. І все це завдяки 3D графіці, яка візуалізує не тільки об'єкти, а й процеси пов'язані із їх функціями. Також дозволяє вивчати внутрішню будову об'єкта та його властивості, а також дозволяє активно взаємодіяти із ним. Використання мультимедійних технологій та перехід від традиційної дошки до сучасних тривимірних технологій сприяє кращому сприйняттю і більш якісному засвоєнню навчального матеріалу молодими людьми і відповідно підвищує їхню майбутню конкурентоспроможність [5].

4 Висновки

Одна з важливих особливостей і переваг цифрових технологій порівняно з іншими навчальними засобами полягає саме в тому, що засоби мультимедіа надають можливість проектувати, створювати та використовувати 3D-моделі, які здебільшого розраховані на самостійне активне сприймання та засвоєння студентами знань, умінь і навичок, створюють ситуації здивування, емоційного підйому, підвищують навчальну мотивацію та пізнавальну активність. Використання цифрових технологій у процесі вивчення природничо-математичних дисциплін є ефективним засобом формування професійної компетентності, сприяє розширенню інформаційного простору, підвищенню якості освіти, розвитку комунікативних здібностей та пізнавальної активності.

Література (References)

1. Гуревич Р.С. Теорія і практика навчання в професійно-технічних закладах : монографія / Р.С. Гуревич. – Вінниця : ТОВ «Планер», Вінниця, 2009. – 410 с.
2. Селезнев В.А. Компьютерные технологии и образное представление информации в учебном процессе образовательных организаций // Теория и практика общественного развития – 2012. – № 1. – С. 134-137.
3. Сучасні технології електронних мультимедійних видань: Монографія / Під ред. О.І.Пушкаря. – Харків: «ІНЖЕК», 2011. – 296 с.
4. Мелешко М.А., Денисенко С.М., Пясківський М.І. Застосування 3d-моделей в мультимедійних електронних освітніх ресурсах // Проблеми інформатизації та управління - НАУ - Том 3, № 51 (2015) [Електронний ресурс] // Режим доступу: <http://jrn1.nau.edu.ua/index.php/PIU/article/view/10322/13596>
5. Знання в 3D-форматі // Учительская газета [Електронний ресурс] // Режим доступу: <http://www.ug.ru/appreciator/29>

Інтернет-Технології як Засіб Організації Групових Форм Роботи

Іван Мельник

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
jmc.johnmelnyk@gmail.com

Abstract. Розкрито особливості групової форми навчання за допомогою сучасних цифрових технологій. Запропоновано використання інтернет-технологій для організації онлайн конкурсів.

Keywords: цифрові технології, інтернет-технології, групова робота, онлайн конкурси.

1 Вступ

Одним із пріоритетних напрямів, який визначено Національною доктриною розвитку освіти, є запровадження сучасних цифрових технологій, які забезпечують підготовку молодого покоління до життєдіяльності в інформаційному суспільстві [1]. Зокрема, однією з найактуальніших проблем є інтеграція освітнього мультимедійного матеріалу в навчальний процес. Наявність комп'ютерної техніки в загальноосвітніх навчальних закладах є необхідною, але не достатньою умовою її широкого й ефективного використання в освітньому процесі. Матеріальні, технічні та організаційні труднощі створення працездатних взаємодіючих груп техніків і педагогів часто стають перешкодою для реалізації освітніх ідей в комп'ютерних розробках [1, 2]. Тому актуальним є питання пошуку таких форм, методів та засобів організації навчання, які б ґрунтувалися на активній взаємодії як учнів між собою, так і педагога та учнів. На нашу думку, однією із таких форм роботи є групова, організована за допомогою сучасних мережових технологій.

2 гра як особлива форма групової роботи

Досвід праці в школі підказує, що саме групова і парна робота найкраще допомагає розвитку комунікативних здібностей учнів. Групова робота – це перш за все гра, гра в організацію, гра в навчання. Гра допомагає учням зрозуміти навчальну тему. Головна мета групової і парної роботи – розвиток мислення учнів. Як в кожній грі, тут існують свої правила, які можна виводити в залежності від конкретних ситуацій. Організація групової

форми роботи в колективі є важким завданням, адже сучасного учня важко зацікавити до роботи. Вирішенням даного питання є проведення інтерактивних занять типу “Брейн-ринг” та “Що? Де? Коли?”. Дані види занять проводяться у вигляді змагання, що стимулює мислення, увагу, концентрацію та командний дух. Організація таких занять важка та клопітка робота, що потребує багато часу. На даний час є багато ресурсів, які дозволяють розробити цікаві та інтересні конкурси, завдання та квести. При використанні таких ресурсів виникають проблеми їх реалізації, оскільки деякі прив’язані до певної операційної системи, інші не мають широкого функціоналу для створення цікавих завдань [3].

3 Роль мережевих технологій в організації групових форм роботи

3.1 Розробка інтреактивнихмодулів в LearningApps

Перспективним напрямком організації групової діяльності учнів є використання систем спільної навчальної діяльності (Computer Supported Collaborative Learning – CSCL). Одним з найцікавіших на даний час є сервіс LearningApps для підтримки процесів навчання за допомогою невеликих інтерактивних модулів. Ці модулі можуть використовуватись безпосередньо як навчальні ресурси, так і для самостійної роботи. Вони не розглядаються як цілісні уроки чи завдання, їх можна використати у будь-якому доречному методичному сценарії. Сервіс надає велику кількість заготовок для створення завдань різного характеру. Це конструктор для розробки інтерактивних завдань за різними предметними дисциплінами. LearningApps.org розробляється як науково-дослідний проект Центру Педагогічного коледжу інформатики освіти РН Берн у співпраці з університетом м.Майнц та Університетом міста Циттау / Герліц (Німеччина). Основним недоліком є неможливість автоматичного оцінювання завдань. Великою перевагою є наявність україномовної версії сервісу. Для роботи на сайті треба зареєструватись, створити свій аккаунт та розпочати творчий процес. Існуючі модулі можуть бути безпосередньо включені у зміст навчання, а також їх можна змінювати чи створювати в оперативному режимі. Вправи на сайті подаються у зручному візуальному режимі сітки зображень, навівши на які вказівник миші можна побачити тип вправи та її рейтинг на сайті (залежить від кількості переглядів та оцінок користувачів). Усі вправи поділено на категорії, які відповідають виду завдання, яке потрібно буде виконати учням: вибір, розподіл, послідовність, заповнення, онлайн-ігри, інструменти. У кожній групі доступно кілька шаблонів вправ, опис та зразки яких можна попередньо переглянути перед тим, як створити власний навчальний ресурс. Дуже важливо, що користуватися створеними продуктами може кожний. Є можливість співпрацювати з колегами не тільки свого навчального закладу, але і всього світу, використовуючи Інтернет. Вчитель може працювати з групами учнів, швидко створювати вправи на уроці, задавати домашнє завдання, отримувати гіперпосилання від учнів та перевіряти виконання завдань. Сервіс відкриває

великі можливості для різноманітності дидактичних завдань. Кожний учасник процесу може використовувати розробки своїх колег, використовуючи величезний банк розробок користувачів сервісу та ділитися своїми авторськими продуктами. Є також можливість використовувати ілюстративні, відео- та аудіо-матеріали. Створені завдання образні, барвисті і легко запам'ятовуються. Автори завжди мають можливість використовувати функцію «повернутись та виправити» [4].

3.2 Використання Інтернет-технологій для організації онлайн конкурсів

Сервіс LearningApps дає можливість вбудовувати створені завдання в веб-сайти в якості html-коду, який відобразиться як готова вправа. Можливість вбудовування вправи надає можливість створювати повноцінні курси, які можна відвідувати просто маючи одне посилання на веб-ресурс. Доцільно використовувати безплатний сервіс компанії Google Sites (класична версія) в якому є можливість редагування html коду. Для цього потрібно просто відкрити сторінку для редагування та розмістити посилання на вправу в режимі відображення коду html.

Для прикладу, розроблено сайт для проведення конкурсів, присвячених дню числа π . На сайт були вбудовані інтерактивні завдання створені за допомогою LearningApps.

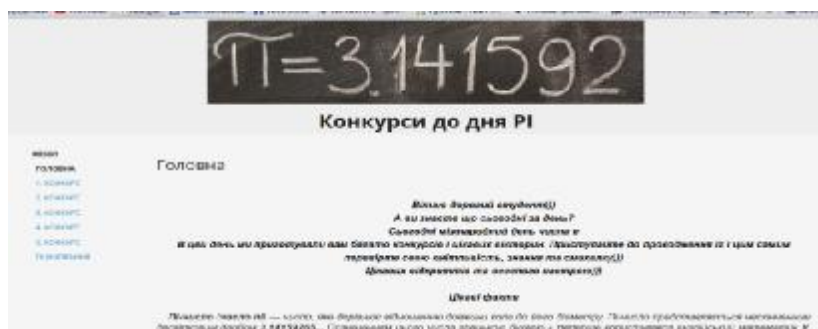


Рис. 1. Зразок використання сайту для проведення конкурсів до “Дня числа π ”.



Рис. 2. Зразок вмонтованої вправи LearningApps.

Даний сайт можна використовувати, наприклад, для організації онлайн брейн-рингу. Оскільки з допомогою LearningApps не можна зробити перевірку на швидкість виконання завдань, вирішити дану проблему допоможе сервіс Google Gmail, за допомогою якого можна надсилати електронні листи. Метод реалізації оцінювання доволі простий – учасники повинні при завершенні виконання певного завдання надіслати “Print screen” на електронну пошту судді, що підтверджує завершення завдання. Суддею проводиться оцінювання виконаних завдань, при якому критерієм може бути, наприклад, швидкість виконання, що дуже добре відобразить час надсилання листа. При такій формі оцінювання конкурсів розвивається вміння учнів вести електронне листування.

4 Висновки

Наявність широкого вибору інтернет-ресурсів, які можна використати в освітньому процесі, відкриває широкі можливості для реалізації освітніх ідей в комп’ютерних розробках. Використання Інтернет-технологій є не тільки одним із засобів реалізації групових форм роботи учнів, а й способом активізації пізнавальної діяльності та формування цифрових компетентностей учнів. В статті як приклад наведено можливість використання Інтернет-технологій (LearningApps, Google Sites, Gmail) для організації онлайн брейн-рингу.

Література (References)

1. Царенко В.О. Сучасні інтернет-технології як засіб забезпечення групового навчання учнів старшої школи. <https://goo.gl/domfoi>
2. Мультимедійні системи як засоби інтерактивного навчання. ав.: Жалдак М. І., Шут М. І., Жук Ю. О., Дементієвська Н. П., Пінчук О. П., Соколюк О. М., Соколов П. К. / За редакцією: Жука Ю. О. – К.: Педагогічна думка, 2012р.
3. Групова робота http://pidruchniki.com/1975030635003/pedagogika/frontalna_robota
4. Що таке LearningApps.org? <https://learningapps.org/about.php>

Virtual Library Architecture Using Cloud Computing

Liubomyr Pohreliuk

Karpenko Physico-Mechanical Institute of NAS of Ukraine, Lviv, Ukraine
liubomyrpohreliuk@gmail.com

Abstract. In this paper the problem of construction and development of virtual library with distributed databases using cloud technologies is presented. Analyzed advantages and disadvantages of existing popular virtual libraries. Criteria of suggested approach are meeting modern requirements for speed and performance are stated and detailed approach is shown.

Keywords: virtual library; cloud technology; performance; accessibility; distributed databases.

1 Introduction

A good example of virtual library based on cloud technologies is Google Scholar. The given virtual library is mostly oriented for scientists and it gives the access to research articles and documents. In this system the following three approaches to gather the required information are used: 1) its own internal algorithm to automatically identify documents on the Internet, which are scientific; 2) the usage of data from scientific journals, public and private databases, academic institutions; 3) based on data which was gathered with the help of the methods described above, you get algorithms for the links' investigation in these articles to collect other articles.

Thus, Google Scholar as one of the web search engines has raised academic search papers to a whole new level. Other web search engines such as Microsoft Academic Search and Citeseer [2] also contributed - in contrast to the classical digital libraries (ieACM Digital Library, PubMed, IEEE Xplore), they index the PDF files of various scientific articles from any publisher, that exist on the Internet. This approach is very efficient because it provides free access to millions of scientific articles at the same time it allows scientists to share their articles so that they are available for the entire scientific community. Furthermore, the process is very easy since all you need is to post the articles and they will be automatically index-linked. This is not possible with classical and digital libraries. So, it is very important for researchers because if their articles are indexed, their visibility in the scientific community will be much higher.

It is important to point out that the need for cloud technologies [3] is essential in this case. Their use will provide the desired flexibility in the use of resources, reducing costs for maintaining servers and other necessary equipment. Nowadays there are many virtual libraries constructed, which are based on cloud technologies, including both successful and not. An example of such successful library is Z. Smith Reynolds

Library at the University of Wake Forest, NC. All IT services of this library were transferred to the cloud. When using Amazon's EC2 service, they also migrated all of its vital services. They claim that the cost of these transitions was similar, but they gained significant operational benefits such as the decrease of hardware failures.

Amazon Elastic Compute Cloud (Amazon EC2) provides the computing power in the cloud, making it easier for developers, provides the ability to manage the web scale of cloud computing. This reduces the time required to get new duplicates of services and allows the user to pay only for capacity that is actually used. Amazon EC2 provides tools, which developers need to avoid frequent failures by constructing resilient applications.

Existing solutions in the field of virtual libraries based on cloud technologies usually cover a niche (as in the case of Google Scholar) and have specificity in architectural solutions, such as in CiteSeer (virtualization) [5]. Most of these decisions do not take into account the case when there is the necessity to save not only scientific articles and data in general, but art articles as well.

Taking into the consideration the advantages and disadvantages of the above systems, there is a need to create a new virtual library, which is going to include important shortcomings, namely, will improve the overall level of service, making the performance and the system of performance in general better, with the opportunity to work easily with large Extent data by creating a new architecture and the development of lossless compression algorithms.

2 Solution

Due to the fact that the existing systems does not fully satisfy our requirements and needs, it was decided to develop advanced architecture of the virtual library using cloud technologies and distributed databases [6]. The new architecture will grade up the working pace of the system for large number of data, which will include various kinds of digital medium.

In Figure 1 general system structure is shown and the interrelationships between the individual blocks. The given solution is implemented using the Azure Cloud and uses the already existing applications to store digital media and graphic resources (Azure Blob Storage), automated services that run in the cloud and in the regular mode gather information, graphic resources, construction of book shelves and book-cases. The data in the system are stored in distributed databases, relational and document based one.

The system architecture provides distributed database, namely the existence of a parallel relational database (MSSQL) and non-relational document based (MongoDB), the last in turn works closely with REDIS system that is designed to store relevant information in memory for fast access and searching. As a result, the relational database contains all the information that exists in the system when the non-relational database contains sample data that is used for accelerated search. Redis database is used for instant search queries, which the system knows how to handle

and store (with improved search elements AI). Standard Azure Cache database used to improve search algorithms using existing cloud solutions.

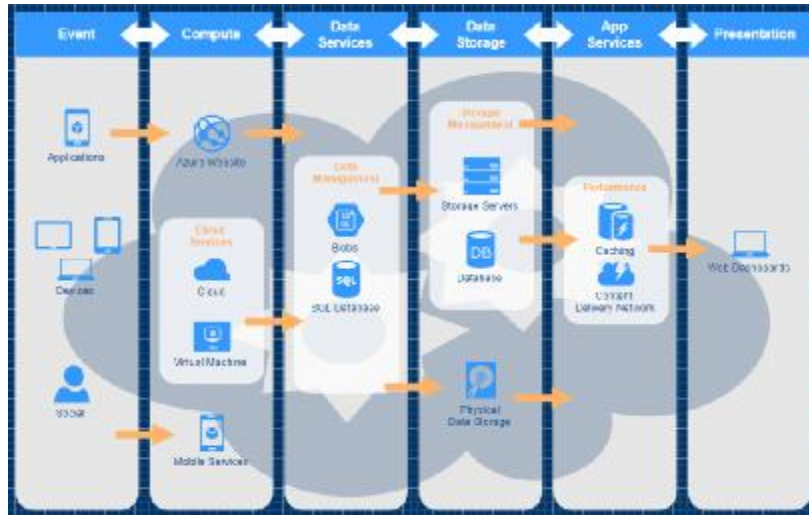


Fig. 1. Azure based architecture design

In order to allow system to display library in the way of shelves and stacks, we developed algorithms that are gathering needed graphical metadata on the internet. Main approach here is to get all needed images of books, like spines and covers, to be able to build a virtual shelf and then stack of shelves for particular library. To implement such process we have used Azure Web jobs and Scheduled Jobs/Services, these mechanisms allows easily run a lot of work in parallel.

Next main parallel processed [4] were developed: process of gathering graphic data on the internet from different sources and relating found images to books; process of building shelves of books using found spines and making resolution of the image on proper level so users will be able to see book metadata easily; process of building stacks based on shelves and then making needed resolution adjustments to optimize load of the images to users web browser; process of building missing images for books if such are needed, this is case when auto search process found only cover but not spine and vice versa. Image related automatic web jobs are using Bitmaps and last ones requires a lot of RAM to do needed actions. Here cloud computing is taking place and providing its benefits – we are able to allocate as much resources as needed for only period of time when we are running heavy operations. In case if we had this architecture not in the cloud – we were supposed to have a very powerful servers and even farms of servers to support that, which is very costly and requires a lot of maintenance.

To search for book covers Amazon Store and Google Books were selected, mentioned above resources are providing clear and usable API that is easy to integrate with. These resources allows user to find needed graphical representation of a book cover or spine by knowing the appropriate book metadata and author. The system

supports cases when automatic search will find only the cover or the spine of the book - in this case a separate automatic service which is responsible for the generation of a graphic element that is missing, will take place. This service itself, mentioned above, will be able to detect the main color schema of found book spine or cover and generate missing part based on color palette. It's important to keep consistency of graphic book representation because our main aim is to make user feel like this is the real graphic data tool from library. Such relation and feeling will make system the best from usability and functionality point of view.

When library has its physical library and wants to have virtual one – it's essential to provide users of this virtual/physical library feeling the connection between them. To support such user experience in the system the display of the library will be done in the special graphical approach. Using such approach, we are allowing users to basically view library as it is in real life.

Using zoom functionality users will be able to make picture bigger and make transition to shelf display and view books in a better resolution. In shelf view, user will be able to see books so closely that he will be able to recognize book he is looking for or find the one that he want. By selecting a book user will have an ability to view bibliographic details of particular book and start reading digital resource related to this book if such exists.

3 Conclusions

In this paper we have compared existing virtual libraries and their implementation approaches; we have investigated their advantages and disadvantages. It has been found that current situation can be improved and needed essential features can be implemented in new system that provides better connection between virtual and real libraries. Furthermore, new approach was stated and shown in the paper; new architecture allows to work with big data (over 10 millions of books) and provides good speed performance and metrics for accessing digital resource. Therefore, we need a specific improvement on search algorithms to be able to efficiently search on big data.

References

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, M. Zaharia, Above the Clouds: A Berkeley View of Cloud Computing, Technical Report No. UCB/EECS-2009-28, University of California at Berkeley, 2009.
2. I.G. Councill, C. L. Giles, E. Di Iorio, M. Gori, M. Maggini, A. Pucci, Towards Next Generation CiteSeer: A Flexible Architecture for Digital Library Deployment, ECDL, 2006.
3. N.B. Ruparelia, Cloud computing, The MIT Press Essential Knowledge series, 2016.
4. T.Erl, R. Puttini, Z. Mahmood, Cloud Computing: Concepts, Technology & Architecture, The Prentice Hall Service Technology Series from Thomas Erl, 2013.
5. C.L. Giles, K. Bollacker, S. Lawrence, CiteSeer: An automatic citation indexing system, ACM Conference on Digital Libraries, 1998.
6. M.T. Ozsü, P. Valduriez, Principles of Distributed Database Systems, Springer, 2011.

Safety of Usage Typical Hash-Functions in Modern Information Systems

Andriy Byalyk

Vasyl Stefanyk Precarpathian National University,
Ivano-Frankivsk, Ukraine
rewrite.andriy@gmail.com

Abstract. This article analyzes some basis aspects of hash-function that are used nowadays and that were used during this decade; also it shows some types and examples of collisions and what it is; the security of hash-functions. The SHA-256 is used as a part of Amazon security service and we will consider it in this article.

Keywords: hash-functions; collisions; security.

1 Introduction

A password hash is the very last line of defense. Its only purpose is to prevent an attacker from gaining total control of a user when all other measures of security have been broken [3].

It is extremely important that a good hashing algorithm will resist all attempts of cracking it, at least for a long time.

Good hash algorithm means that the password must **always** be stored with a cryptographic one-way function. When a password has been encrypted with an algorithm which allows decryption then there is no guarantee that an attacker has not already gained access to the secret key and immediately by passed all borders of security [3].

The aim of the report is the analysis of modern one-way hash-function algorithms, their durability, worst-case scenarios, collisions and usage in enterprise software and systems.

2 Description of basic material

A hash function is any function that can be used to map data of arbitrary size to data of fixed size. The values returned by a hash function are called hash values, hash codes or simply hashes. One-time use is a data structure called a hash table, widely used in computer software for quick search [5].

Hash functions are widely used in cryptography. A cryptographic hash function allows us to easily verify that some input data maps shows a given hash value, but if the

input data is unknown, it is deliberately difficult to reconstruct it (or equivalent alternatives) by knowing the stored hash value. This is used for assuring integrity of transmitted data, and for the building block for hash-based message authentication codes, which provide message authentication [3].

Hash functions are related to checksums, check digits, fingerprints, lossy compression, randomization functions, error-correcting codes, and ciphers. Although these concepts overlap to some extent, each has its own uses and requirements and is designed and optimized differently [5].

Collision resistance is a property of cryptographic hash functions: a hash function H is a collision resistant if it is difficult to find two inputs for which hash function will have the same output; that is, two inputs a and b for which $H(a) = H(b)$, and $a \neq b$ [1].

3 Hash-Functions collision

Cryptographic hash functions are usually designed to be collision resistant. But many hash functions that firstly were collision resistant were later broken. MD5 and SHA-1 in particular both have published techniques more efficient than brute force for finding collisions. Let's have a look, why they are dangerous.

Here we have two different messages, but their MD5 hashes are equal to 008ee33a9d58b51cfcb425b0959121c9.

- 4Dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783e7b9518afbfa200a8284bf36e8e4b55b35f427593d849676da0d1555d8360fb5f07fea2
- 4dc968ff0ee35c209572d4777b721587d36fa7b21bdc56b74a3dc0783e7b9518afbfa202a8284bf36e8e4b55b35f427593d849676da0d1d55d8360fb5f07fea2.

When you compute the hash, message divides by blocks and for each block applies the compress function, that is dependent on some, that is called the initialization vector. The result of this function is the initialization vector for the next block. The result of the execution function on last block is called the hash of given message.

Let's define initialization vector as $s_{i+1}=f(s_i, M_i)$.

Collisions also can have worse consequences, than just the same hash for different messages. Vlastimil Klíma's method allows us to pick up for any defined value s_i two same 128-bytes blocks M, M' and N, N' such as $f(f(s, M), M') = f(f(s, N), N')$.

Using this methodology we can construct two files with the same MD5 hash sum, but these files will have different 128 bytes in the center.

$M_0, M_1, \dots, M_{i-1}, M_i, M_{i+1}, M_{i+2}, \dots, M_n$ and $M_0, M_1, \dots, M_{i-1}, N_i, N_{i+1}, M_{i+2}, \dots, M_n$.

But MD5 hashes of this functions will be the same, because blocks M_i, M_{i+1} and N_i, N_{i+1} will return as s_{i+2} the same value, because $f(f(s, M_i), M_{i+1}) = f(f(s, N_i), N_{i+1})$.

Let's consider that we have the file with given blocks: $M_0, M_1, X, X, \dots, M_n$. We can make two files which are based on those: $M_0, M_1, N_1, N_1, \dots, M_n$ and $M_0, M_1, N_2, N_1, \dots, M_n$. If N_1 and N_2 are collisions then the MD5 sum will be the same for them.

So we can have the next situation:

if $(X = X)$ then { good_program } else { evil_program }[4].

4 Amazon

SHA-256 signatures are widely used in Amazon services. For example, let's have a look on Amazon Glacier. If we want to upload an archive, we have two ways of doing it. First one: uploading entire chive, second one: uploading archive by parts. But in both scenarios we should use SHA-256 signatures in headers.

SHA-256 signatures are widely used in Amazon services. For example, let's have a look on Amazon Glacier. If we want to upload an archive, we have two ways of doing it. First one: uploading entire chive, second one: uploading archive by parts. But in both scenarios we should use SHA-256 signatures in headings.

Computing SHA-256 signatures is done by several rules: For every 1 MB chunk of pay load data, compute the SHA-256 hash. The last chunk of data can be smaller than 1 MB. For example, if you are up loading a 3.2 MB archive, you compute the SHA-256 hash values for each of the first three 1 MB chunks of data, and then compute the SHA-256 hash of the remaining 0.2 MB data. These hash values form the leaf nodes of the tree.

1. Build the next level of the tree.
 - (a) Concatenate two consecutive child node hash-values and calculation the SHA-256 hash of the concatenated hash values. This concatenation and generation of the SHA-256 hash produce a parentnode for the two child nodes.
 - (b) When only one childnode remains, you promote that hash value to the next level in the tree.
2. Repeat step 2 until the resulting tree has a root. The root of the tree provides a hash of the entire archive and a root of the appropriate subtree provides the hash for the part in a multipart upload.

Basically it looks like a tree of calculated hashes, as on following image [2]:

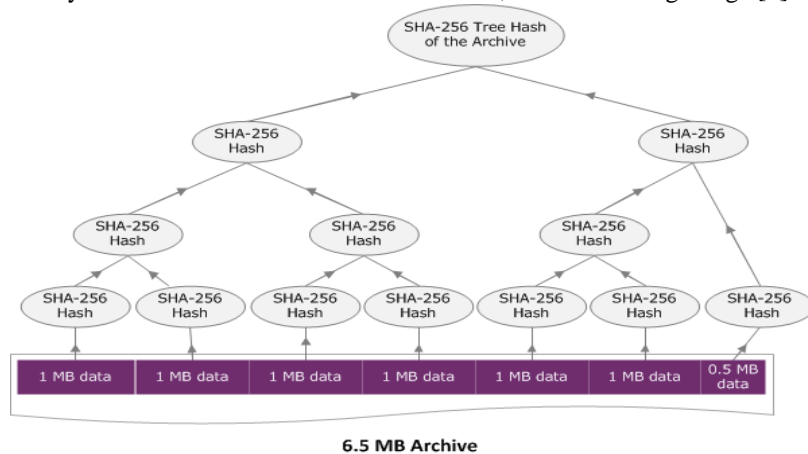


Fig. 1. SHA-256 Tree Hash

5 Summary

Nowadays there are a lot of hash-functions, but they are created for different purposes. But pure SHA-256/SHA-512 is not secure for storing passwords and MD family is deprecated to use as a hash-sum functions, because of possibility of collisions.

It is better to use SHA-256 Tree Hash to compute the hash-sum of archive, because it is more efficient in big data.

References

1. "Collision Resistance | Wikiwand". Wikiwand. http://www.wikiwand.com/en/Collision_resistance
2. "Computing Checksums - Amazon Glacier". Docs.aws.amazon.com. N.p., 2017. <http://docs.aws.amazon.com/amazonglacier/latest/dev/checksum-calculations.html>
3. "SHA-256 Is Not A Secure Password Hashing Algorithm". Dusted Codes. N.p., 2016. <https://dusted.codes/sha-256-is-not-a-secure-password-hashing-algorithm>
4. "Забавляемся С Хешами". Habrahabr.ru. N.p., 2012. <https://habrahabr.ru/post/113127/>
5. "Hash Function". Wikipedia. https://en.wikipedia.org/wiki/Hash_function

Особливості Програмної та Апаратної Реалізації Алгоритму Симетричного Блокового Перетворення ДСТУ 7624:2014 (шифр Калина)

Василь Петреній

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
vasylpetreniy@gmail.com

Abstract. В статті проведено аналіз особливостей реалізації програмними та апаратними засобами нового національного стандарту України, симетричного блокового перетворення ДСТУ 7624:2014 (шифр Калина), який прийнятий 1 липня 2015 року. Сформульовано вимоги до національного стандарту шифрування і також конструктивні рішення, які використані для їх забезпечення.

Keywords: ДСТУ 7624:2014 , блоковий шифр, криптоаналіз, S-перетворення, національний стандарт, швидкодія шифрування.

1 Вступ

Блокові шифри є одним із найбільш розповсюджених криптографічних примітивів. Крім забезпечення конфіденційності, вони використовуються як конструктивний елемент в ході побудови функцій хешування, кодів автентифікації повідомлення тощо.

З практичної точки зору, у сучасних інформаційно-комунікаційних системах основний потік інформації, що передається відкритими каналами зв'язку, захищається за допомогою саме симетричних перетворень із залученням блокового шифру. Засоби криптографічного захисту інформації (КЗІ), які існують зараз, у ряді випадків не можуть забезпечити рівень пропускну здатності, який повністю відповідає актуальним вимогам.

Блоковий шифр, визначений ДСТУ ГОСТ 28147-89 [1] був введений в дію 27 років тому. Хоча він все ще забезпечує практичну стійкість, та з точки зору швидкодії, на сучасних обчислювальних архітектурах загального призначення ДСТУ ГОСТ 28147:2009 (остання версія стандарту шифрування) суттєво поступається іноземними аналогам.

Вимоги до надійного криптографічного перетворення

Нове криптографічне перетворення повинно відповідати наступним загальним вимогам:

1. Захищеність алгоритму від криптоаналітичних атак.
2. Статистична безпека криптографічного алгоритму в плані нерозрізнюваності гам шифрування та шифротекстів від істинно випадкових.
3. Криптоалгоритм повинен мати зрозумілу, легку для аналізу структуру й ґрунтуватися на надійному математичному апараті.
4. Стійкість до модифікації.
5. Обчислювальна складність шифрування/розшифрування.
6. Універсальність криптографічного алгоритму: можливість роботи з різними довжинами початкових ключів та інформаційних блоків.
7. Параметри криптоалгоритму:
 - криптоалгоритм повинен будуватись на основі блокового симетричного перетворення (БСП);
 - обов'язкові розміри блока даних – 128, 256 та 512 бітів;
 - обов'язкові розміри разового (сеансу) ключа – 128, 256, 512 бітів.
8. Реалізація криптоалгоритму:
 - криптоалгоритм повинен бути орієнтованим для можливості реалізації на 32- або 64-розрядних процесорах;
 - зазначені в криптоалгоритмі операції повинні мати ефективну програмну та апаратну реалізацію;
 - необхідний для роботи обсяг пам'яті має враховувати можливість реалізації криптоалгоритму у мікропристроях;
 - давати змогу паралельного виконання декількох операцій.

2 Конструктивні рішення обрані при розробці стандарту

При розробці було вирішено забезпечити прозорість проектування і використовувати консервативний підхід із залученням відомих і добре досліджених конструкцій, а також наявність достатнього запасу стійкості для безпечного використання алгоритму в умовах значного прогресу криптоаналітичних технік та засобів обробки даних.

У результаті як високорівнева конструкція шифру обрана Substitution Permutation Network (SPN-структура). Для підвищення складності атак лінійного, диференційного і алгебраїчного криптоаналізу додатково застосовується попереднє і прикінцеве забілювання (pre- and postwhitening) із використанням модульного додавання. В рамках консервативного і прозорого підходу до проектування блокового шифру, шар нелінійного перетворення циклової функції реалізований на базі S-блоків.

Для реалізації блоку лінійного розсіювання було обране множення на МДВ-матрицю як найбільш ефективний метод реалізації впливу кожного вхідного символу на кожний вихідний завдяки отриманню найбільшого індексу галуження відображення.

Для блокового шифру «Калина» використовується МДВ-матриця розміром 64x64 біта (8x8 над полем $GF(2^8)$) як така, що забезпечує необхідні криптографічні властивості і вимоги щодо швидкодії на сучасних програмних 64-бітових архітектурах. Зокрема, розмір табличного перетворення для найшвидшої реалізації дорівнює 16 кБ, що дозволяє ефективно використовувати можливості сучасних процесорів з розміром кешу даних L1 у 32 кБ або 64 кБ.

Розмір блоку і довжина ключа визначають зовнішні параметри алгоритму та його галузь використання (за умови забезпечення внутрішніх компонентів стійкості до відповідних видів атак). Довжина ключа повинна забезпечувати практичне унеможливлення здійснення перебірних атак та методів аналізу, що засновані на таблицях передобчислень, із суттєвим запасом стійкості. Для забезпечення достатнього рівня криптографічної стійкості національний стандарт шифрування підтримує конфігурації ключа і блоку, які наведені у табл. 1.

Таблиця 1. Комбінації довжини ключа і розміру блоку шифру «Калина»

Розмір блоку	Довжина ключа
128	128, 256
256	256, 512
512	512

Відповідно кількість циклів (ітерацій) криптографічного алгоритму було обрано на основі достатнього запасу стійкості до різних видів криптоаналізу. Кількість циклів перетворення для різних конфігурацій наведено у табл. 2.

Таблиця 2. Кількість циклів шифрування блокового шифру «Калина»

Блок	Ключ	128	256	512
128		10	14	-
256		-	14	18
512		-	-	18

3 Висновки

- Блокові шифри є одним із найбільш поширених криптографічних примітивів, які використовуються як для забезпечення конфіденційності основного потоку інформації, що передається відкритими каналами зв'язку так і як основа хеш функцій.
- ДСТУ ГОСТ 28147:2009 вже не міг забезпечити достатній рівень криптографічної стійкості і не міг в повні мірі використати переваги сучасних архітектур. Проте його заміна на AES не є вирішенням проблеми нового національного стандарту для України, бо світові тенденції вже свідчать про поступову відмову від AES
- У якості високорівневої конструкції шифру на основі аналітичного порівняння обрана SPN-структура як більш ефективна порівняно з ланцюгом Фейстеля і схемою Лей-Мессі. Шар нелінійного перетворення циклової функції реалізований на базі S-блоків. Розмір S-блоку був обраний виходячи з можливості ефективної реалізації на процесорах загального призначення.
- Для реалізації блоку лінійного розсіювання було обране множення на МДВ-матрицю як найбільш ефективний метод реалізації впливу кожного вхідного символу на кожний вихідний. Для блокового шифра «Калина» задана МДВ-матриця розміром 64x64 біта
- Блоковий шифр «Калина», визначений ДСТУ 7624:2014, забезпечує нормальний, високий і надвисокий рівень стійкості, із довжинами блока і ключа 128, 256 і 512 бітів.

Література (References)

1. ГОСТ 28147–89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования [Текст]. – Введ. 01–07–1990. – М. : Изд-во стандартов, 1989. – 28 с.
2. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. [Текст]. – Введ. 01–07–2015. – К.: Мінекономрозвитку України, 2015.
3. О.О. Кузнецов, Р. В. Олійников, Ю. І. Горбенко, А. І. Пушкарьов, О. В. Дирда, І. Д. Горбенко. Обґрунтування вимог, побудування та аналіз перспективних симетричних криптоперетворень на основі блочних шифрів. Вісник Національного університету "Львівська політехніка". Комп'ютерні системи та мережі. - 2014. - № 806. - с. 124-141.

СЕКЦІЯ 3

Системи управління

Management Systems

Analiza Działań Logistycznych Przedsiębiorstwa Handlowego przy Przygotowaniach do Światowych Dni Młodzieży 2016 w Krakowie

Anna Ostrowska

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
anna.ostrowska1994@gmail.com

Abstract. W lipcu 2016 r. w Krakowie odbyły się Światowe Dni Młodzieży. W Internecie pojawiło się wiele artykułów dotyczących przebiegu wydarzeń lub podsumowań przygotowań miasta do obchodów. Natomiast nie pojawiły się żadne publikacje dotyczące wpływu ŚDM Kraków 2016 na przedsiębiorstwa z branży FMCG.

Keywords: Światowe Dni Młodzieży 2016 w Krakowie, handel detaliczny, branża FMCG

1 Wprowadzenie

Organizacja imprez masowych generuje wiele ograniczeń i problemów logistycznych, związanych z przesyłem informacji, komunikacją i transportem. Światowe Dni Młodzieży 2016, które odbyły się w Krakowie, są dokładnym odzwierciedleniem tego typu problemów.

W jaki sposób Światowe Dni Młodzieży 2016 wpłynęły na organizację pracy oraz przygotowania jednego z największych przedsiębiorstw handlowych w Polsce? Jakie środki zostały podjęte w celu zabezpieczenia regularności dostaw oraz dostępności asortymentu? Jak podjęte działania wpłynęły na organizację pracy centrum logistycznego oraz placówek handlowych?

W poniższej pracy będzie można odnaleźć odpowiedzi na powyższe pytania. Zostaną one również poddane analizie i ocenie, które ukażą czy zaplanowane działania oraz wdrożone rozwiązania były potrzebne.

2 Opis przedsiębiorstwa

Opisywane przedsiębiorstwo to prężnie działająca spółka, na krajowym rynku produktów szybkozbywalnych, obsługująca blisko 2700 placówek handlowych od ponad 20 lat. Ze względu na rozbudowaną strukturę przedsiębiorstwa, towar trafia do punktów sprzedaży z 15 centrów dystrybucyjnych, które rozlokowane są w całej Polsce. Jedno centrum średnio zaopatruje 150 – 200 sklepów.

Centra logistyczne wraz z biurem regionu tworzą tzw. dystrykt, który nosi nazwę miasta w którym się znajduje. W strukturze firmy można wyodrębnić 15 dystryktów, które dodatkowo można podzielić na 4 makrodystrykty: południe, wschód, zachód i Warszawa. Ich najważniejszym zadaniem jest zamawianie towaru od dostawców, który trafi do placówek detalicznych. Natomiast najważniejszym filarem firmy jest pion operacyjny odpowiadający za sprzedaż.

3 Opis branży

Analizowane przedsiębiorstwo funkcjonuje w branży handlu detalicznego, ściślej rzecz ujmując – w sektorze produktów szybkozbywalnych.

Handel detaliczny (ang. retail) obejmuje transakcje polegające na:

- zakupie asortymentu od producentów krajowych lub zagranicznych;
- odsprzedaży niewielkiej ilości towaru dokonywanej w punkcie handlowym.

W ten sposób przedsiębiorstwo kształtuje oferowany asortyment dla potrzeb konsumentów, by móc zapewnić im wymagany towar w najdogodniejszych warunkach, miejscu i czasie.

Podstawowymi funkcjami handlu detalicznego są:

- zakup towaru;
- sprzedaż produktów;
- gospodarka zapasami.

Sektor FMCG (ang. FastMoving Consumer Goods) - sektor dóbr szybkozbywalnych, inaczej szybkorotujących. Są to produkty często kupowane przez konsumentów, które oferowane są w relatywnie niskich cenach. W tej branży sprzedawane są produkty tj.: artykuły spożywcze, chemia gospodarcza itp.

4 Analiza przygotowań przedsiębiorstwa

Przy analizie i ocenie przygotowań przedsiębiorstwa do ŚDM Kraków 2016, przeprowadzono analizę SWOT krakowskiego centrum dystrybucyjnego (tab. 1.).

Krakowskie centrum logistyczne, na co dzień zaopatruje blisko 130 punktów handlowych. Jednak na okres Światowych Dni Młodzieży, kierownictwo najwyższego szczebla, podjęło decyzję o ograniczeniu liczby sklepów do 50 placówek znajdujących się na terenie Krakowa. Pozostałe 80 sklepów, tymczasowo umieszczono pod kierownictwem trzech sąsiadujących dystryktów. Dzięki takiemu rozwiązaniu, menedżerowie mogli skoncentrować się na obmyśleniu strategii logistycznych, dostosowanych do panujących warunków.

Kadra zarządzająca centrum dystrybucyjnego, napotkała również następujące problemy wewnątrzorganizacyjne:

- zmiana struktury przedsiębiorstwa, polegająca na utworzeniu, wyżej wspomnianych, makrodystryktów oraz scentralizowaniu łańcucha dostaw na ich poziomie. W wyniku czego zaszła również konieczność dobrania i przeszkolenia nowego kierownictwa, personelu oraz opracowanie nowych strategii zarządzania procesami: zamawiania, dystrybucji i transportu;
- tworzenie i weryfikacja nowych narzędzi, których nadrzędnym celem jest ulepszenie procesów: zamawiania towaru oraz gospodarki magazynowej;

Tabela 1. Analiza SWOT przedsiębiorstwa w kontekście przygotowań do ŚDM Kraków 2016.
Źródło: [4].

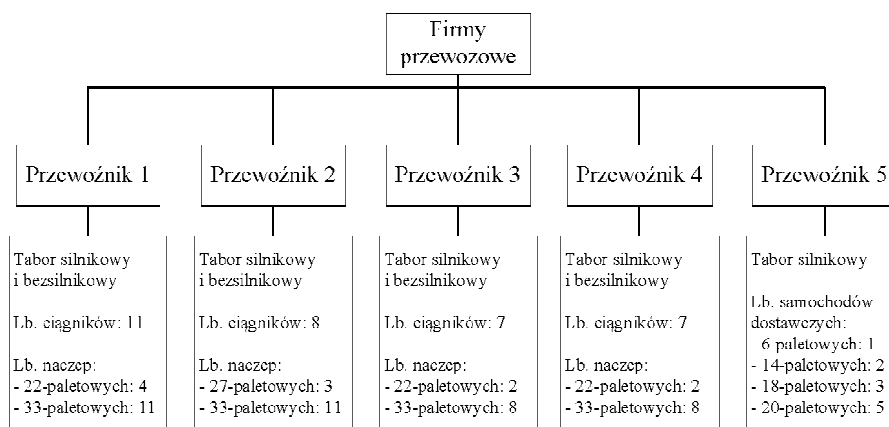
Mocne strony	Słabe strony
<ul style="list-style-type: none"> • dobra znajomość rynku; • szeroki zakres asortymentu; • duży udział w runku krajowym; • dobry wizerunek marki; • relatywnie niskie ceny towarów; • wysoki poziom obsługi klienta; • doświadczona kadra; • szeroka gama środków transportu; • wysoki poziom procesów logistycznych; • korzystne położenie geograficzne centrum dystrybucyjnego. 	<ul style="list-style-type: none"> • zachodzące zmiany w strukturze przedsiębiorstwa; • testowanie nowych rozwiązań dotyczących systemu zamawiania towarów; • stosunkowo krótki okres funkcjonowania centrum logistycznego w Krakowie (3lata); • spora ilość nowych, wdrażających się pracowników; • punkty sprzedaży znajdowały się stosunkowo daleko wydarzeń centralnych ŚDM.
Szanse	Zagrożenia
<ul style="list-style-type: none"> • napływ dużej ilości potencjalnych klientów; • zwiększenie rozpoznawalności marki dla klientów zagranicznych (z państw graniczących z Polską); • zdobycie doświadczenia w obsłudze procesów logistycznych w niecodziennych warunkach. 	<ul style="list-style-type: none"> • duża konkurencja rynkowa; • zmiana organizacji ruchu w Krakowie; • wprowadzone regulacje prawne dotyczące tonażu oraz godzin wjazdu do miasta przez samochody ciężarowe; • migracje mieszkańców Krakowa na okres ŚDM; • brak lub nadmiar towaru w sklepowym magazynie lub centrum dystrybucyjnym; • problemy z przesyłem zamówień sklepowych; • powstawanie długich kolejek w placówkach detalicznych; • chaos w pracy centrum dystrybucyjnego ze względu na zmianę godzin pracy magazynu.

- modyfikacja harmonogramu funkcjonowania centrum dystrybucyjnego na okres Świątowych Dni Młodzieży - godziny przyjęcia dostaw zmodyfikowano z porannych na popołudniowe. W wyniku czego nastąpiła zmiana: godzin pracy magazynu, głównie pracowników kontroli jakości oraz sekcji przyjęć, które odpowiadają za odbiór asortymentu od producentów.

Dodatkowe utrudnienia, zwłaszcza w logistyce transportu, wywołało *Obwieszczenie wojewody małopolskiego z dnia 22.07.2016r.*¹, które dotyczyło ograniczeń w ruchu na okres ŚDM Kraków 2016. Zatwierdzono zakaz przemieszczania się dla pojazdów i zespołów pojazdów o masie całkowitej przekraczającej 12 ton, we wskazanych w obwieszczeniu dniach i godzinach. Opisywana regulacja, nakładała również ograniczenia dla pojazdów przewożących artykuły szybko psujące się, tj.: owoce, warzywa, mięso, itd., co skutkowało zmianą harmonogramu transportów i odbioru dostaw.

Znaczącym utrudnieniem okazała się również zmiana organizacji ruchu na okres ŚDM. Większość głównych ulic zostało tymczasowo zablokowanych, ze względu na kwestię bezpieczeństwa. Oprócz zamknięcia kluczowych tras, przez służby porządkowe, wiele dróg w Krakowie okazało się nieprzystępnych dla samochodów ciężarowych, z uwagi na ograniczenia tonażowe lub zbyt dużą wysokość pojazdu. Wyznaczenie tras objazdowych stało się bardzo istotnym i trudnym elementem planowania transportu towarów.

W ramach przygotowań do Świątowych Dni Młodzieży i przewidywane trudności z przewozem produktów do punktów sprzedaży, menedżerowie podjęli decyzję o stworzeniu zapasów w magazynach przy punktach sprzedaży. Krakowskie placówki handlowe, w okresie poprzedzającym wydarzenie, zaopatrzone zostały w zwiększone ilości towarów o długim terminie przydatności, nie wymagających szczególnych warunków do przechowywania. Zapasy gromadzone były w sklepowych magazynach lub w specjalnie przygotowanych namiotach.



Rys. 1. Flota działająca na rzecz centrum dystrybucyjnego w Krakowie. Źródło: [4].

¹ *Obwieszczenie wojewody małopolskiego z dnia 22.07.2016 r.*, bip.malopolska.pl [07.01.2017r.]

5 Wnioski

Analizowane przedsiębiorstwo działa w bardzo specyficznej i trudnej branży jaką jest handel detaliczny oraz sektor FMCG. Konsumenci wymagają ciągłej dostępności towarów bardzo dobrej jakości, oferowanych im w wygodnych dla nich warunkach, miejscu i czasie.

Światowe Dni Młodości w Krakowie były bezspornie ogromnym wyzwaniem logistycznym dla menedżerów oraz pracowników badanego przedsiębiorstwa. Także stanowiły dogodną okazję do:

- uzyskania dużej liczby klientów, a co się z tym wiąże – zwiększenia obrotów firmy;
- pozyskania nowych nabywców zza granicy oraz tym samym zwiększenie rozpoznawalności marki;
- zdobycia doświadczenia przez kadrę zarządzającą i pracowników, przy pracy w niecodziennych warunkach.

Menedżerowie podjęli szereg czynności, mających zapewnić jak najlepsze funkcjonowanie łańcucha logistycznego. Kluczowymi decyzjami okazały się:

- przekazanie 80 punktów sprzedaży pod kierownictwo sąsiadujących centrów dystrybucyjnych, by móc skoncentrować się na obsłudze krakowskich placówek;
- zaplanowanie oraz dostarczenie do placówek handlowych produktów o długim terminie przydatności, w okresie poprzedzającym wydarzenia ŚDM, by zapewnić dostępność asortymentu dla klientów;
- zmiana godzin pracy centrum logistycznego, a co z tym związane - zmiana godzin przyjęcia asortymentu od producentów. Realizacja dostaw do placówek handlowych przeprowadzona była według zaleceń opisanych we wprowadzonych regulacjach prawnych;
- zagwarantowanie dostępności i elastyczności floty przewozowej.

Przedsiębiorstwo napotkało problemy:

- zmiana organizacji ruchu ulicznego w Krakowie, która wymusiła modyfikacje dotychczasowych tras dostaw;
- wprowadzone regulacje prawne dotyczące m.in.: ograniczeń tonażowych oraz związanych z poruszaniem się samochodów dostawczych na terenie Krakowa, w wyniku czego nastąpiły zmiany w harmonogramie dostaw;
- zmiany wewnątrzorganizacyjne, obejmujące restrukturyzację firmy oraz scentralizowanie procesu zamawiania towaru na poziomie makrodystryktów;
- testowanie nowych narzędzi zamawiania towaru i gospodarki magazynowej;

Podsumowując przedsiębiorstwo handlowe było dobrze przygotowane do ŚDM Kraków 2016. Kadra zarządzająca wypracowała możliwe działania w różnych sytuacjach, wprowadziła zabiegi prewencyjne, mające zapewnić ciągłość łańcucha dostaw i dostępności asortymentu dla klientów. Wprowadzane zmiany

wewnątrzorganizacyjne w firmie nie wpłynęły na jakość realizowanych procesów logistycznych.

Ze względu na migracje mieszkańców Krakowa oraz dobre przygotowania Komitetu Organizacyjnego ŚDM Kraków 2016, firmie nie udało się polepszyć ani zrealizować zakładanego budżetu sprzedaży. Jednak wiele parametrów funkcjonowania centrum, tj.: punktualność realizacji dostaw, okres oczekiwania na rozładunek oraz procesy magazynowania, uległy znacznej poprawie.

Zdobyta wiedza i doświadczenie przez pracowników przedsiębiorstwa, przy obsłudze placówek detalicznych w warunkach, jakie panowały podczas Światowych Dni Młodzieży, zdecydowanie zapoczątkuje na korzyść przedsiębiorstwa, zwłaszcza przy opracowywaniu nowych strategii zarządzania łańcuchem dostaw i sterowania zapasami.

Literatura (References)

1. Dobrzyński M. *Logistyka*, Politechnika Białostocka, Białystok 1999
2. Niziński S., Żurek J. *Logistyka ogólna*, Wydawnictwa Komunikacji i Łączności, Warszawa 2011
3. *Obwieszczenie wojewody małopolskiego z dnia 22.07.2016 r.*, bip.malopolska.pl [07.01.2017 r.]
4. Ostrowska A., *Analiza działań logistycznych przedsiębiorstwa z branży handlu detalicznego przy przygotowaniach do Światowych Dni Młodzieży 2016 w Krakowie*, Praca dyplomowa (niepublikowana) 2017

Projekt Linii Produkcyjnej Gipsu Budowlanego

Agata Frątczak

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
agatafratczak31@gmail.com

Abstract. Poniższa praca przedstawia gips budowlany jako powietrzne spoiwo wiążące, jego charakterystykę, zastosowanie oraz surowce do produkcji. W dalszej części znajduje się opis operacji technologicznych stosowanych w procesie produkcyjnym: eksploatacja złóż, załadunek i transport surowca, rozdrabnianie, mielenie oraz prażenie.

Keywords: gips, surowce gipsowe, gips budowlany, prażenie, kalcynacja

1 Wprowadzenie

Gipsy budowlane stanowią jedną z podgrup spoiw gipsowych, w skład których wchodzi gipsy sztukatorskie, tynkarskie i mieszane. Gips budowlany to powietrzny materiał wiążący, co oznacza, że po zarobieniu jego sproszkowanej postaci z wodą albo roztworami wodnymi powstaje plastyczna masa, ulegająca formowaniu, wiążąca i twardniejąca na powietrzu. Wytrzymałość mechaniczna zapraw gipsowych może ulec obniżeniu w obecności środowiska wodnego.

Gips budowlany powstaje w wyniku zmielenia i wysuszenia kamienia gipsowego oraz jego wyprażenia w kalcynatorze obrotowym. Wówczas w procesie częściowej dehydratacji tworzy się gips budowlany, czyli półwodny siarczan wapnia $\text{CaSO}_4 \cdot 1/2\text{H}_2\text{O}$. W zależności od warunków prażenia (wysokość temperatury, obecność pary wodnej lub jej brak) uzyskujemy różne jego odmiany: α lub β , różniące się od siebie rozpuszczalnością, czasem wiązania i wytrzymałością. Gips budowlany jest to niepalne, szybko wiążące, czyste spoiwo powietrzne. Gipsy te - sztukatorski, tynkarski, mieszany - są szeroko stosowane w przemyśle budowlanym: do produkcji prefabrykatów gipsowych, jako spoiwo do sporządzania zapraw, do powierzchni ścian i sufitów – wypełnianie ubytków, renowacje i wykończenia oraz do montażu instalacji elektrycznych.

2 Surowce gipsowe

Do wytwarzania siarczanowych materiałów wiążących najczęściej stosowane są skały gipsowe i anhydrotowe, zwane potocznie kamieniem gipsowym. Posiada on twardość 2 w skali Mohsa, przez co może być uznany za skałę dość miękką – da się ją zarysować nawet paznokciem. Produkcja spoiw siarczanowych może opierać się również na

wykorzystaniu odpadów przemysłowych, wytwarzanych w różnorodnych procesach chemicznych. Są to zazwyczaj fosfogipsy i borogipsy, jednak ten sposób produkcji stosowany jest jedynie w sytuacji braku dostępu do złóż skał naturalnych o zadowalającej jakości

Gips jest pospolitym minerałem, stanowiącym podstawowy składnik skał gipsowych. Jest to naturalny, dwuwodny siarczan wapniowy określany wzorem chemicznym $\text{CaSO}_4 \cdot 2\text{H}_2\text{O}$.

Anhydryt CaSO_4 jest to bezwodny siarczan wapnia, będący znaczącym składnikiem skał solnych oraz osadowych.

3 Operacje technologiczne w produkcji gipsu budowlanego

3.1 Eksploatacja surowców gipsowych

Metoda eksploatacji kamienia gipsowego zależy głównie od budowy złoża, głębokości zalegania oraz miąższości. Przy doborze sposobu eksploatacji na uwagę zasługują również rodzaj i grubość nadkładu, lokalne warunki topograficzne i hydrogeologiczne oraz twardość i urabialność skał.

Początkowym etapem prac jest udostępnienie złoża. Polega ono na wykonaniu odpowiednich wykopów górniczych tak, by umożliwić eksploatację surowca ze ścian wyrobiska, transport i usuwanie zalegających skał płonnych. Wykonanie takich wyrobisk oraz ich wielkość zależą od wielu czynników, m. in. od warunków zalegania złoża, rzeźby terenu i granicznej głębokości wyrobiska [2].

Kolejny etap to usuwanie nadkładu zalegającego nad złożem. Nadkładem mogą być warstwy gleby, piasku, gliny bądź skał płonnych o wysokiej twardości. Przed przystąpieniem do eksploatacji warstwy te muszą zostać usunięte.

Stosowanie odkrywkowej metody wydobywania kamienia gipsowego wiąże się z wykorzystaniem techniki strzelniczej. Polega ona na odstrzeliwaniu skał surowca za pomocą materiałów wybuchowych. Proces ten składa się z następujących po sobie kroków:

- wykonanie otworów strzelniczych o odpowiednich rozmiarach i ilości,
- usunięcie zwiercin,
- załadunek materiałów wybuchowych, ładunku inicjującego i materiału zamykającego otwór do wydrążenia,
- odpalenie ładunku.

Wszelkie parametry wykonywanych otworów, takie jak ich liczba, usytuowanie, głębokość, średnica, odległość między poszczególnymi otworami oraz ilość materiału wybuchowego zależą od charakterystyki złoża. Obecnie powszechnie stosowaną metodą jest strzelanie otworami wiertniczymi, polegające na wywoływaniu eksplozji materiału wybuchowego w otworach. Następujące po sobie w niewielkich odstępach czasowych eksplozje powodują odspojenie skały na całej wysokości ściany eksploatacyjnej i w znacznej części frontu wydobywczego. Materiałem wybuchowym jest zazwyczaj pochodna saletry amonowej [2].

3.2 Załadunek i transport surowców

Po wydobyciu surowca następuje etap jego załadunku i transportu do zakładu przetwórczego. Do ładowania urobku na samochody technologiczne stosowane są koparki łyżkowe o dużych pojemnościach łyżek załadowniczych, dochodzących do 8 m³, bądź ładowarki. Koparki to maszyny samojezdne, posiadające mocne podwozie gąsienicowe oraz wielosilnikowy napęd elektryczny. Ładowarki są z kolei napędzane przez silniki spalinowe, a ich podwozie jest kołowe. Pojemność ich łyżek załadowniczych wynosi do 5 m³.

Do transportu najczęściej stosuje się samochody samowyładowcze, zwane też wywrotkami. Ich ładowność różni się w zależności od producenta, modelu pojazdu technologicznego i stawianych mu wymagań, jednak wahają się one w granicach 15-60 ton.

3.3 Rozdrabnianie kamienia gipsowego

Kamień gipsowy przewieziony z kamieniołomu do zakładu przetwórczego poddawany jest rozdrabnianiu jako operacji przygotowawczej, nie głównej, ponieważ na tym etapie materiał podlega przygotowaniu do wypalania.

Rozdrabnianie dużych brył materiału wymaga poddania ich działaniu sił udarowych, natomiast rozdrabnianiu drobnemu (mieleniu) towarzyszą siły działające głównie ścierająco. Biorąc pod uwagę granulację rozdrobnionego materiału wyróżnia się:

- kruszenie wstępne – uzyskujemy bryły o wielkości do 300 mm,
- kruszenie średnie – bryły o wielkości do 20 mm,
- kruszenie drobne – bryły o wielkości ok. 3 mm.

Parametrem charakteryzującym każde rozdrabnianie, niezależnie od rodzaju użytej maszyny, jest stopień rozdrobnienia n . Jest on określany jako stosunek rozmiaru ziaren nadawy do wymiarów ziaren produktu po rozdrobnieniu:

$$n=D/d \quad (1)$$

gdzie: n – stopień rozdrobnienia, D – wymiar ziaren nadawy, mm, d – wymiar ziaren produktu, mm.

Najczęściej stosowane maszyny do rozdrabniania kamienia gipsowego to kruszarki szczękowe, kruszarki stożkowe i kruszarki walcowe. Ich dobór zależy od rodzaju skały, jej twardości, rozmiaru oraz żądanej wielkości produktu [2].

3.4 Mielenie

Kolejnym etapem, któremu poddawany jest kamień gipsowy, jest jego mielenie. Odbywa się ono w agregatach susząco-mielących, spośród których najbardziej rozpowszechnione to młyny aeracyjno-bijakowe, młyny walcowe oraz młyny szybowe. Wówczas przemiał surowca prowadzony jest jednocześnie z jego suszeniem i częściową dehydratacją.

Dla procesu mielenia obowiązuje podobny podział jak w przypadku kruszenia i zależy on od wielkości produktu:

- mielenie grube – średnica ziaren produktu 3-0,8 mm,
- mielenie średnie – średnica ziaren produktu 0,8-0,2 mm,
- mielenie drobne – średnica ziaren produktu poniżej 0,2 mm.

3.5 Prażenie

Obróbka cieplna gipsu przeprowadzana jest zazwyczaj w urządzeniach zwanych prażarkami bądź w piecach obrotowych (kalcynatorach). Prażenie zmielonego surowca odbywa się w temperaturze od 135°C do nawet 230°C, w zależności od tego, jaki produkt chcemy uzyskać. W celu uzyskania gipsu budowlanego najczęściej stosuje się temperatury z zakresu 150-180°C.

Podczas prażenia zachodzi najważniejszy z procesów w produkcji gipsu budowlanego, mianowicie dehydratacja. Polega ona na odłączeniu się cząsteczek wody od gipsu, czyli dwuwodnego siarczanu wapnia $\text{CaSO}_4 \cdot 2\text{H}_2\text{O}$. W trakcie ogrzewania woda krystalizacyjna stopniowo wyparowuje z gipsu, przechodząc w gips półwodny $\text{CaSO}_4 \cdot 1/2\text{H}_2\text{O}$.

Proces dehydratacji oraz przejścia gipsu w siarczan półwodny wiąże się ze zmianą sieci krystalicznej – następuje przebudowa sieci o symetrii jednoskośnej w sieć rombową. Odmiana $\alpha\text{CaSO}_4 \cdot 1/2\text{H}_2\text{O}$ powstaje w przypadku prowadzenia dehydratacji gipsu w obecności nasyconej pary wodnej, podczas gdy odmiana β uzyskiwana jest w procesie z usunięciem tej pary.

Dehydratacja gipsu zachodzi zgodnie z równaniem:



Ogrzewanie gipsu w celu przeprowadzenia go w półhydrat wiąże się z ubytkiem masy reagentów, wywołanych wydzielaniem się wody, a w dalszych etapach również wydzielaniem SO_2 oraz tlenu [2].

Spośród urządzeń stosowanych do kalcynacji gipsu wyróżniamy prażarki gipsu pracujące okresowo, pracujące w ruchu ciągłym oraz różne typy pieców obrotowych. W niektórych przypadkach stosowane są urządzenia mieląco-prażące, w których wstępnie rozdrobniony kamień gipsowy poddawany jest jednoczesnemu mieleniu, suszeniu i dehydratacji.

Literatura (References)

1. Bolewski A., Budkiewicz M., Wyszomirski P., 1991: *Surowce ceramiczne*, Wyd. 1, Wyd. Geologiczne, Warszawa, s. 59-71.
2. Brylicki W., Derdacka-Grzymek A., Gawlicki M., Małolepszy J., Olejarz J., 1979: *Technologia budowlanych materiałów wiążących cz.1 Wapno Gips*, WSiP, Warszawa.
3. Frątczak A., Projekt linii produkcji gipsu budowlanego o granulacji poniżej 0,2mm. Wydajność linii prażącej – 20t/h produkt.
4. Kurdowski W., 1981: *PORADNIK technologia przemysłu cementowego*, Wyd. 1, Wyd. Arkady, Warszawa, s. 142-156.

Przemysł Rybny

Weronika Mikurda

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
weronika.mi@poczta.fm

Abstract. Obecnie technologia jest już zauważalna we wszystkich gałęziach przemysłu, nawet rybnego. Ważnym czynnikiem pomagającym osiągnąć sukces jest redukcja kosztów, która zaczyna się już na morzu. Obecnie prezentowane są dwa nowe typy statków rybackich, którym warto się przyjrzeć ze względów ekonomicznych oraz technologicznych. Na lądzie wdrażane są, lub zostały już wdrożone, systemy informatyczne pozwalające na kontrolę kutrów znajdujących się na morzu. W przetwórnictwie dominują systemy teleinformatyczne pozwalające łatwo i szybko rozemnić się w zakresie dyspozycji i planowania zasobów, zaopatrzenia, zarządzania produkcją oraz sprzedażą.

Keywords: • Statki rybackie • NP.-24 • TR-80 • SFIS • VMS • Oprogramowanie wspierające • Przetwórstwo ryb •

1 Wstęp

Obecnie głównym czynnikiem decydującym o tym, czy klient zechce zakupić konkretny produkt jest jego jakość, która zaraz obok marketingu i ceny decyduje o sukcesie producenta na rynku. Aby jakość produktu była jak najlepsza należy wdrożyć i stosować odpowiednie systemy zarządzania, które jednocześnie będą pomagać w spełnieniu wymogów państwowych oraz unijnych. Poza samymi systemami w utrzymaniu dobrego wizerunku firmy i zaistnieniu na rynku pomocne są najnowsze technologie oraz maszyny. Szczególnie ciekawym tematem jest rybołówstwo oraz przemysł rybny, ponieważ wydawać by się mogło, że całość kończy się na morzu. Jednak większość pracy, związanej z przetwórstwem złowionych na kutrach ryb, odbywa się w zakładach. Wymaga to sprzętu oraz technologii, które pozwolą w efektywny sposób sprostać wymogom sanepidu, normom jakościowym oraz pomogą w generowaniu zysków.

2 Statki rybackie

Nowoczesne rozwiązanie, które pozwala na redukcję kosztów już na samym początku łańcucha produkcyjnego, zaproponowała firma NED Project z siedzibą w Gdańsku. Mowa tu o trzech nowych modelach statków rybackich: NP-24, TR-80 oraz TR-123. Charakteryzują się gruszkowym typem dzioba, który poprzez swoją budowę powoduje korzystny przepływ strug wody i tym samym w efektywny sposób zmniejsza zuży-

cie paliwa. Jest to szczególnie opłacalne przy dużych jednostkach pływających. NED Project przedstawiła na swojej stronie internetowej specyfikację dwóch z trzech jednostek: NP-24 oraz TR-80.

NP-24 to specjalnie zaprojektowany, do połowów na północnych morzach, statek o masie 339 GT osiągający prędkość maksymalną 12 węzłów. Wyposażony w hybrydowy silnik potrzebuje 7 osób załogi i może spędzić na morzu 12 dni. Pod pokładem znajduje się miejsce do przetwarzania ryb oraz maszyna obładzająca z wydajnością 5t/24h. Łódź jest wykorzystywana w ładowni ryb.

TR-80 również przeznaczona na północne morza jednostka prawie czterokrotnie większa od NP-24. Osiąga prędkość do 15 węzłów i wymaga aż 92 osób załogi. Z dala od portu może spędzić 40 dni.

Tabela 1. Parametry NP-24 i TR-80. Źródło: Opracowanie własne na podstawie informacji NED Project

	NP-24	TR-80
Maksymalna prędkość	12 węzłów	15 węzłów
Długość	28,60 m	80,7 m
szerokość	9 m	17 m
Głębokość pokładu	7,15 m	9,2 m
Zanurzenie	5,48 m	6,05 m
Liczebność załogi	7 osób	92 osoby
Maksymalny czas na morzu	12 dni	40 dni

Każdy statek został wyposażony w szereg urządzeń mających na celu poprawienie jakości połowów oraz wstępnego przetwórstwa złowionych ryb. Na mostku zainstalowano urządzenie, które dzięki połączeniu systemów sterowania, nawigacji oraz komunikacji, ogranicza pracę człowieka do minimum. Na włokach umieszczono sonary mające za zadanie wykrywanie ryb w okolicach statku. W pomieszczeniu przetwórczym umieszczono między innymi przenośniki taśmowe, parowniki o ruchu ciągłym oraz autoklawy. Parownik stanowi część linii produkcyjnej i służy do wyparowania ryb w puszkach w temperaturze do 92°C. Ryby umieszcza się w ramie załadowniczej skąd trafiają do komory parowej. Następnie przekazywane są do ramy wyładowniczej, gdzie są chłodzone, skąd trafiają na transportery. Transportery najczęściej przekazują puszki do odsączarki. Z kolei autoklaw to urządzenie, które służy do sterylizacji konserw rybnych w puszkach stalowych.

3 Technologie informatyczne

Kilka lat temu zaproponowano komputerowe rozwiązanie, które ma za zadanie pomagać w zarządzaniu i kontroli kutrów rybackich. Mowa tu o SFIS, czyli Zintegro-

wanym Systemie Zarządzania Rybołówstwem, na który składają się cztery moduły zwiększające funkcjonalność połowów. Pierwszy z nich, czyli moduł Rejestru Statków pozwala na przechowywanie oraz systematyzowanie wszelkich danych dotyczących właściciela, załogi i wyposażenia statku. Kolejny nazwany VMS, czyli Vessel Monitoring System, ma za zadanie monitorować położenie jednostek łowiących na wodach terytorialnych RP. System wyposażono również w moduł mający za zadanie weryfikowanie ilości złowionych ryb, zapisanej w dziennikach pokładowych, z ilością podaną na kartach wyładunkowych. Czwarty podzespół – Statystyczno-Raportujący – ma na celu zebranie w całość wszelkich informacji, przekazanych przez pozostałe elementy, w raporty, w których zamieszcza takie informacje, jak stan floty rybackiej lub ilość obcych jednostek w 200 milowej strefie.

Obecnie na rynku reklamuje się wiele firm, które oferują swoim klientom rozwiązania IT. Oferowane są systemy wspierające przedsiębiorców w zakresie dyspozycji i planowania zasobów, zaopatrzenia, zarządzania produkcją oraz sprzedażą. Niektóre firmy realizują każde z tych zadań w osobnych produktach, jednak są dostępne takie programy, które wszystkie te zadania opracowują jednocześnie. Największa wydajność przedsiębiorstwa jest wtedy, gdy pracuje w nim jeden system oparty na jednolitej i automatycznie aktualizowanej bazie danych. Redukuje to zbędne nakłady pracy spowodowane np. podwójną rejestracją w systemie. Najbardziej pożądane cechy oprogramowania dla przemysłu rybnego to:

- jeden system automatycznie aktualizowany na bieżąco;
- planowanie i dyspozycja zapasami oraz mocą produkcyjną;
- kontrolowanie pochodzenia surowców;
- kontrolowanie jakości;
- kontrola pracownicza, rejestracja oraz higiena pracy;
- elektroniczna wymiana danych z klientami;
- sprzedaż wielokanałowa;
- system zarządzania maszynami produkcyjnymi wraz z serwisowaniem;
- prowadzenie statystyk: przychody, dochody, rozchody, itp.

Literatura (References)

1. <http://www.ned-project.eu/products/fishing-vessels/>
2. M. Marciniak, *Zastosowanie technologii teleinformatycznych w zarządzaniu surowcem rybnym*

Lean Management – Nowoczesna Filozofia Zarządzania

Katarzyna Majka

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
katarzynamajka2@gmail.com

Abstract. Istnieje wiele metod i technik służących doskonaleniu zarządzania przedsiębiorstwem. Jedną z nich jest tzw. wyszczuplanie organizacji – Lean Management – jednoczesne i ciągle obniżane kosztów, podwyższanie jakości, skracanie cykli realizacji produkcji, zdobywanie nowych klientów. Jest to nowatorska koncepcja zarządzania przedsiębiorstwem, wykorzystywana szczególnie w procesie restrukturyzacji.

Keywords: Lean Management; Lean production; Szczupła produkcja; Zarządzanie; Marnotrawstwo.

1 Krótka historia

Twórcą pojęcia *lean* był John Krafcik, który po raz pierwszy użył go w 1988 roku w swoim artykule opublikowanym w „Sloan Management Review”. Pojęcie zostało następnie spopularyzowane przez grupę naukowców z Massachusetts Institute of Technology Jamesa Womacka, Daniela T. Jonesa i Daniela Roosa, którzy w 1990 roku opublikowali słynną pracę „**The Machine That Changed the World**” (dosłownie: „*Maszyna, która zmieniła świat*”), w której przedstawili wyniki międzynarodowego programu badawczego IMVP (ang. *International Motor Vehicle Program*) realizowanego w latach 1984-1990 w sektorze motoryzacyjnym. W badaniu porównywali parametry nakładów i wyników w przedsiębiorstwach japońskich, amerykańskich i europejskich. Za lidera uznali japońską firmę Toyota Motor Corporation z systemem Toyota Production System. Autorzy uznali ten system za pierwszy odchudzony system wytwórczy i nazywając go *lean manufacturing*. Według autorów odchudzona produkcja: „*daje możliwość, aby produkować coraz więcej wykorzystując coraz mniej – mniej ludzkiego wysiłku, urządzeń, czasu i miejsca – przy jednoczesnym zbliżaniu się do osiągnięcia celu jakim jest dostarczenie klientom dokładnie tego czego chcą*”. Stąd też korzeni *lean* należy poszukiwać w Toyocie.

Jednak zanim pojawiła się Toyota, w 1913 roku Henry Ford stworzył produkcję płynną (ang. *flow production*), czyli wprowadził taśmowy montaż samochodu. Model T zrewolucjonizował system wytwarzania, jednak Ford stanął przed problemem niemożności dostarczania różnorodności, wymaganej przez klienta i konkurencję. Model T był ograniczony do jednego koloru, ale i specyfikacji. Pierwszy Model T wyprodukowany w 1908 w rzeczywistości niczym nie różnił się od ostatniego, który zjechał z

taśmy w 1926 roku. Kilka lat później Ki'ichirō Toyoda i Taiichi Ohno postanowili wykorzystać oryginalny pomysł Forda i stworzyli Toyota Production System.

W 1937 roku Sakichi Toyoda założył Toyota Motor Company, którego pierwszym prezesem był najstarszy syn założyciela Kiichiro Toyoda. Sformułowali oni dwie podstawowe koncepcje odchudzania produkcji:

1. Jidoka – gdy tylko popełniony jest błąd automatycznie zatrzymywane są maszyny i linie, w celu uniknięcia produkowania bubli i niezakłócenia przepływu w dalszej części strumienia;
2. Just In Time – produkcja części, które są akurat potrzebne przy wykorzystaniu systemu ssącego.

Obie koncepcje zostały zastosowane w praktyce przez jednego z dyrektorów Toyoty, Taiichi Ohno. Oprócz tego w Toyocie, jako pierwszej na świecie, rozpoczęto prace nad rozwojem produktów, zarządzanie łańcuchem dostaw oraz przyjmowaniem zamówień od klientów. Kiedy w latach 50. XX wieku w Japonii zauważalny był kryzys powojenny Eiji Toyoda (syn Sakichi Toyoda) odwiedził fabrykę Forda Rouge w Detroit. Dziennie powstawało tam 7000 samochodów, podczas gdy Toyota wyprodukowała 2685 w przeciągu 13 lat. Na podstawie tej wizyty i wspólnych spostrzeżeń z Taiichi Ohno doszli do wniosku, że chociaż masowa produkcja nie sprawdzi się w Japonii to można usprawnić system. Toyota Production System oparty został przede wszystkim na eliminacji wszelkiego marnotrawstwa.

2 Struktura systemu

Struktura systemu Lean opiera się na trzech podstawowych filarach:

- Planowanie strategiczne;
- Struktura organizacyjna; Zdolność zasobów ludzkich.
- Zrozumienie zależności pomiędzy tymi kluczowymi czynnikami umożliwia maksymalne wykorzystanie zasobów firmy.

Planowanie strategiczne jest sformalizowanym procesem długofalowego planowania stosowanego do określania i realizacji celów organizacji. Na nim oparte będą długoterminowe zadania dla kadry menedżerskiej.

Struktura organizacyjna to pewien wzór relacji między pozycjami i człowiekiem w danej organizacji. Musi być podporządkowana strategii poprzez dostosowanie rozwoju produktu, produkcji i dystrybucji oraz systemu informacyjnego czyli Lean Production.

Ostatnim składnikiem kluczowym jest zdolność zasobów ludzkich. Obejmuje on tworzenie nowej kultury organizacji polegającej na ciągłym doskonaleniu, usprawnieniu produkcji, kształceniu kadry kierowniczej i sprawny przepływ informacji ze sprzężeniem zwrotnym włącznie.

Gdy te trzy filary nabiorą właściwych kształtów ważne staje się skupienie na elementach wyjściowych każdego z obszarów. W obszarze rozwoju strategii najważniejszym (krytycznym) elementem jest jedynomyślność kierownictwa naczelnego. Walki

wewnętrzne czy konkurencja pomiędzy działami powodują marnotrawienie energii i zagrażają procesom niezbędnym do realizacji strategii.

Następnym elementem tego obszaru jest satysfakcja klienta. Oznacza to ciągłą kontrolę rynku, ocenę rynku, projektowanie produktu i określenie wymagań jakościowych. Kierownictwo naczelne tworzy politykę, strukturę organizacyjną. Kierownicy niższego szczebla są odpowiedzialni za realizację wyznaczonych celów. Dla pełnej realizacji celów struktura organizacyjna musi być pozbawiona zbędnych elementów biurokracji, lenistwa i apatii. Struktura organizacyjna musi być czuła na zmiany otoczenia, rynku i samej organizacji, musi utrzymywać wytworzone drogi komunikacji (system informacyjny) dbając o informacje pochodzące od pracowników i dostawców.

3 Zastosowanie

Spory nacisk Lean Management kładzie na kształtowanie długotrwałych i bezpośrednich kontaktów z dostawcami oraz odbiorcami, wówczas zastosowanie znajduje metoda „Just In Time” - metoda stosowana w celu usprawnienia zwrotu inwestycji poprzez redukcję poziomu zapasów. Tymczasem dla odciążenia przedsiębiorstwa ze zbędnych kosztów stosuje się „Outsourcing”, który równocześnie upraszcza i usprawnia system zarządzania poprzez zlecenie na zewnątrz niektórych funkcji.

4 Marnotrawstwo według filozofii Lean

Istotą szczupłego zarządzania jest „odchudzenie” przedsiębiorstwa poprzez wprowadzenie znaczących zmian w zakresie działalności, w strukturze majątku firmy, sposobie organizacji oraz w dziedzinie zarządzania personelem, jak też kształtowanie zachowań i postaw pracowników firmy.

Marnotrawstwem według filozofii Lean Management jest każda działalność, która absorbuje zasoby, pochłania czas, a nie dodaje wartości produktom. Według prekursora Lean pana Taiichi Ohno do podstawowych źródeł marnotrawstwa zaliczamy powszechnie występujące w przemyśle nieproduktywne straty takie jak:

- Nadprodukcja – czyli produkowanie więcej niż trzeba lub zbyt wcześnie, jest to wytwarzanie produktów bez zamówienia klienta, co prowadzi do wzrostu zapasów wyrobów gotowych;
- Zła organizacja stanowisk pracy, bezczynne oczekiwanie ludzi i maszyn na opóźnione dostawy lub następne kroki w procesie;
- Za duże czasy wykonania operacji ze względu na złe zaprojektowanie produktów i narzędzi,;
- Niepotrzebny transport materiałów między funkcyjnymi obszarami – przemieszczanie elementów, części, półwyrobów, wyrobów częściej niż to jest konieczne;
- Zbyt wiele materiałów w procesie produkcji, zbyt wiele wyrobów gotowych, a także zapasy materiałowe większe niż absolutne minimum;

- Błędy lub braki wymagające naprawy lub korekty, dotyczą one zarówno wyrobów, jak i dokumentacji, dostaw, informacji;
- Wykonywanie zbędnych kroków w procesie obróbki, przemieszczanie się ludzi w czasie pracy (szukając części, narzędzi, instrukcji czy pomocy).

Uniknąć marnotrawstwa można jedynie drogą ciągłego procesu racjonalizacji całej firmy oraz jej relacji z otoczeniem, co pozwala na ograniczenie funkcji wewnętrznych do działań absolutnie niezbędnych.

5 Elementy, które składają się na koncepcję Lean Management

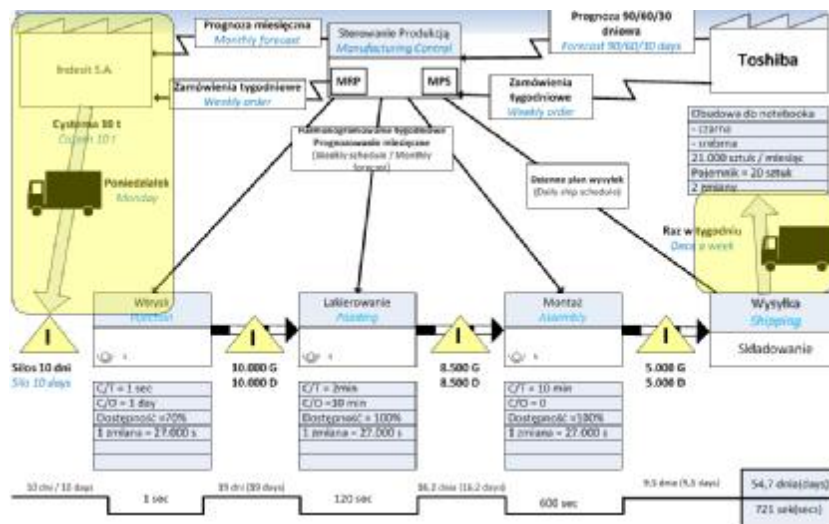
- Praca zespołowa;
- Totalny „Quality Control”, czyli usuwanie błędów już w trakcie produkcji;
- Rynkowy charakter produkcji, czyli delegowanie pracowników do punktów sprzedaży;
- Bezpośredni kontakt z dostawcami;
- Symultaniczny engineering, czyli równoległe przeprojektowywanie;
- Zarządzanie zasobami ludzkimi.

6 Podstawowe narzędzia Lean Management

- **VSM – Value Stream Mapping** – technika polegająca na mapowaniu (czyli opisywaniu w sposób graficzny) jak wygląda przepływ wartości z perspektywy klienta w procesach organizacyjnych przedsiębiorstwa. Celem zastosowania **mapowania strumienia wartości** jest takie połączenie wszystkich podejmowanych działań i realizowanych procesów produkowania i dostarczenia wyrobów i usług aby zobrazować i zrozumieć, w jaki sposób przez firmę przepływa strumień wartości dla klientów.
- **5S** – odnosi się do pięciu japońskich słów, które opisują standaryzację utrzymywania porządku w miejscu pracy:
 - **Seiri**: *sort*, selekcja; dotyczy praktyki sortowania wszystkich narzędzi, materiałów itp. na miejscu pracy i posiadanie tylko tego co niezbędne. Rzeczy zbędne należy magazynować lub wyrzucić, gdyż stwarzają niebezpieczeństwo na stanowisku pracy oraz powodują bałagan, co zakłóca wydajnej pracy.
 - **Seiton**: *storage*, systematyka; skupienie na potrzebę uporządkowanego miejsca pracy. Narzędzia, urządzenia i materiały muszą być systematycznie układane dla łatwiejszego i skutecznego dostępu. Każda rzecz musi mieć swoje, wydzielone i oznaczone miejsce. Musi być miejsce dla wszystkiego i wszystko musi być na swoim miejscu.
 - **Seiso**: *shine*, sprzątanie; wskazuje na potrzebę utrzymywania miejsca pracy zarówno uporządkowanego jak i czystego. W japońskich firmach sprzątanie jest codzienną czynnością. Po zakończeniu zmiany, przestrzeń pracy jest sprzątana a wszystkie elementy wracają na swoje miejsce.

- **Seiketsu**: *standardise*, standaryzacja; pozwala na kontrolę i konsekwencję. Wykonywane czynności należy standaryzować, aby stosowane były z dużą większą łatwością. Każdy musi wiedzieć za co jest odpowiedzialny. Obowiązek utrzymywania czystości staje się częścią regularnie wykonywanych działań.
- **Shitsuke**: *sustain*, samodyscyplina; dotyczy utrzymywania standardów. Wczesniejsze 4S musza być przestrzegane za ścisłą dyscypliną dzień po dniu. Należy przestrzegać wcześniej ustalonych zasad i uczynić je przyzwyczajeniem.
- **TPM** – *Total Productive Maintenance* – Optymalne Utrzymanie Ruchu; celem jest zapewnienie maksymalnej dostępności krytycznych urządzeń. Jest to system który umożliwia minimalizację awarii oraz poprawę jakości dzięki zaangażowaniu wszystkich pracowników. Głównym celem TPM jest osiągnięcie poziomu trzech zer: zero awarii, zero braków, zero wypadków przy pracy.
- **SMED** – *Single Minute Exchange of Die* – szybkie przebrojenie. Jest to zespołowy proces redukujący czas przebrojenia maszyny, co zwiększa czas przeznaczony na produkcję i jednocześnie umożliwia zmniejszenie wielkości partii produkcyjnych, ilości zapasów, „Lead Time”, i w efekcie powoduje obniżenie kosztów produkcji. Nominalnym celem czasu trwania przebrojenia jest maksimum 10 minut.

Wszystkie te narzędzia powinny być wdrażane jako kompleksowy system współzależnych i wzajemnie się wspierających praktyk. Można się jednak spotkać z niezależnymi wdrożeniami narzędzi wspierających lub pozbawionymi elementami Lean w przypadku tych rodzajów produkcji, gdzie typowe rozwiązania Lean nie mają zastosowania.



Rys. 1. Przykładowa mapa strumienia wartości (Źródło: <http://www.bgc.com.pl>)

7 Zalety i wady

7.1 Zalety:

- Zwiększenie zdolności konkurencyjnej – dzięki redukcji kosztów, zmniejszenie rozrzutności i wyższa jakość;
- Zwiększenie wydajności pracy, spłaszczenie hierarchii, skrócenie czasu podejmowania decyzji;
- Zwrócenie większej uwagi na potrzeby i życzenia klientów;
- Zwiększenie zadowolenia pracowników dzięki lepszej komunikacji między kierownikami a podwładnymi.

7.2 Wady:

- Przekształcenie się koncepcji w prostą racjonalizację, z groźbą obniżenia płynności, spadkiem jakości i zaniedbywaniem usług;
- Stres pracowników i spadek motywacji;
- Powierzchnowa redukcja pracowników;
- Wzrost zapotrzebowania na siły fachowe, przy równoczesnym zaniedbywaniu problemów pracowników o niższych kwalifikacjach.

8 Podsumowanie

W tej strategii zmian i transformacji, założenia Lean Management muszą znaleźć swoje odbicie w faktycznej produkcji. Oznacza to budowę zespołów zadaniowych i zespołów ds. realizacji celów, zarządzania zasobami, ustanowienie kultury umacniania, udoskonalania i uczenia się. Opisana powyżej strategia wymaga niezwykle dokładnego przygotowania by możliwe było osiągnięcie jak najlepszego efektu. Konieczne jest stworzenie dokumentacji określającej: stan obecny, metody kontroli i pomiaru postępu, okresową kontrolę celów i ich korektę. Transformacja Lean ma za zadanie stworzyć organizację otwartą, czułą, nie bojącą się zmian, elastyczną, zaangażowaną, ufną w stosunku do zasobów materialnych.

Literatura (References)

1. Lisiński, M., Ostrowski, B.: Lean Management w restrukturyzacji przedsiębiorstwa, Kraków (2006)
2. Lean Management – Sposobem na zarządzanie przedsiębiorstwem, <http://www.lean-management.pl>
3. Codzienne informacje do rozwoju firmy – portal nowoczesna firma, <http://www.nf.pl>
4. Polskie centrum Lean, <http://www.leancenter.pl>
5. Aspekty zarządzania organizacjami, <https://www.governica.com>

Wizja Kolonizacji Marsa – SpaceX

Maciej Gacek

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
mafej791@gmail.com

Abstract. Ziemi w odległej przyszłości grozi zagłada. Nikt nie wie w jaki sposób może do tego dojść, jednak Elon Musk wraz ze swoim SpaceX postanowił przedsięwziąć kroki, mające w takim przypadku zapewnić ludzkości bezpieczeństwo. Kolonizacja Marsa – to wizja, która wydaje się być tylko marzeniem. Jednak SpaceX ma zamiar wysłać na „Czerwoną Planetę” ludzi w przeciągu najbliższych kilku lat. Pod koniec zeszłego roku Elon Musk przedstawił wiele szczegółów tego jak ma wyglądać podróż oraz sam transporter. Niespotykany dotychczas rozmiarów statek kosmiczy. Nowe silniki Raptor, ponad 70m „booster” oraz tankowanie na orbicie to tylko kilka z nowoczesnych rozwiązań SpaceX. Naukowcy zapewniają, że na planecie tej znajdują się wszystkie potrzebne pierwiastki do uprawiania roślin, a samą temperaturę Marsa można podnieść. Już w latach 20` XXI w. na „Czerwoną Planetę” ma polecieć około 100 ludzi oraz 450t ładunku.

Keywords: Booster, Tanker, Międzyplanetarny Statek Kosmiczny, SpaceX, Elon Musk, Interplanetary Transport System, Raptor

1 Dlaczego Mars?

Zaludnienie innej planety niż Ziemia w wypadku kataklizmu zapewni ludzkości przetrwanie. To właśnie główny cel SpaceX – kolonizacja innej planety. Dlaczego więc Mars? Wenus odpada ze względu na zbyt wysokie ciśnienie atmosferyczne oraz temperaturę na powierzchni tej planety. Podobnie z Merkurem – znajduje się zbyt blisko Słońca. Księżycy Jowisza i Saturna? Mimo tego, że Dyrektor Generalny I Techniczny SpaceX Elon Musk zapewnia, że możliwy jest lot, na niektóre z nich to jednak znajdują się one znacznie dalej od Słońca i ciężko się na nie dostać. Nasz Księżyc natomiast jest zdecydowanie mniejszy od planet, nie posiada atmosfery, a dzień trwa tam około 28 dni ziemskich. Jedyna możliwość dla ludzkości żeby zostać „międzyplanetarną” cywilizacją to zasiedlenie Marsa. Mimo, że średnia temperatura wynosi tam -63°C to Elon Musk uważa, że planetę tą można „podgrzać”. Mars jest bardzo bogaty w surowce mineralne, a głównymi składnikami atmosfery są dwutlenek węgla, argon oraz azot, które umożliwią rozwój roślin na tej planecie. Dzień trwa tam 24h i 40min czyli bardzo podobnie jak na Ziemi. Grawitacja na Marsie jest o ponad 62% mniejsza niż na Ziemi, co umożliwi dźwiganie przez ludzi cięższych przedmiotów, co będzie dla nich niezłą zabawą – podsumował Musk.

2 Interplanetary Transport System

2.1 Raptor

Silniki Raptor pod każdym względem mają zdominować wszystkie napędy raketowe wykorzystywane do tej pory. SpaceX zdecydowało się na użycie rewolucyjnego paliwa – „methalox” czyli kombinację metanu z ciekłym tlenem. Temperatura ciekłego metanu to około $-180\text{ }^{\circ}\text{C}$. Podobnie do ciekłego tlenu. Dodatkowo metan jest tani i prosty do uzyskania nawet na Marsie. Komora ciśnieniowa silnika jest trzy razy większa niż w produkowanych przez SpaceX silnikach Merlin, które zabierają raketę Falcon 9 na Międzynarodową Stację Kosmiczną. Impuls właściwy Raptora będzie osiągał wartość 382, zaś ciąg wyniesie ponad 3 MN, ponad trzy razy więcej niż osiągają Merliny. Ciśnienie w komorze spalania Raptora wyniesie ma 296 atmosfer, więcej niż w jakimkolwiek innym silniku raketowym.

2.2 „Booster”

„Booster” to rakieta, która ma wynieść statek kosmiczny oraz „tanker” na orbitę okołoziemską. Ma to na celu zmniejszenie rozmiarów oraz wagi statku kosmicznego co zdecydowanie zmniejszy koszty lotu. „Booster” ma mieć 77,5 m wysokości oraz 12 m średnicy. Jego masa to 275 t, zaś masa paliwa napędowego to aż 6 700 t. Będzie on napędzany przez 42 silniki Raptor. Ma on rozpędzić statek kosmiczny aż do prędkości 8 650 km/h – w momencie separacji, a następnie powrócić na miejsce lądowania w około 20 min. Szacuje się, że „Booster” będzie można wykorzystać przy około 1000 startach.

2.3 Interplanetary Spaceship

„Międzyplanetarny Statek Kosmiczny” to konstrukcja, która mierzyć będzie 49,5 m, jej maksymalna średnica wyniesie 17 m. Statek napędzany będzie przez 9 silników Raptor. Masa samego statku to 150 t. Masa paliwa napędowego wewnątrz statku wyniesie 1 950 t. SpaceX chce aby jednorazowo „Międzyplanetarny Statek Kosmiczny” mógł zabrać na Marsa około 100 osób oraz 450 t ładunku. Szacuje się, że statek kosmiczny będzie można wykorzystać przy 12 startach.

2.4 Tanker

„Tanker” właściwie niczym nie będzie się różnił od statku kosmicznego. Ma on być jego kopia z powiększoną pojemnością na paliwo. Sam „Tanker” ważył będzie 90 t i pomieści 2 500 t paliwa. Podobnie jak w „Międzyplanetarnym Statku Kosmicznym” za napęd posłuży mu 9 silników Raptor i będzie wynoszony na orbitę przez „Booster”. „Tanker” ma być gotowy na 100 startów z Ziemi.

3 „Międzyplanetarny Statek Kosmiczny”, a Saturn V

Saturn V to wielostopniowa rakiet kosmiczna wykorzystywana przez NASA. Podczas Misji „Apollo11” pierwszy raz dzięki tej rakiecie człowiek wylądował na Księżycu. Warto pokazać jaką przewagę nad tą rakieta ma projekt SpaceX. Ogromną różnicę widać już patrząc na masę całkowitą obu rakiet. W przypadku Saturna V jest to 3 039 t, kiedy rakiet SpaceX może poszczycić się masą na poziomie 10 500 t – jest to aż 3,5 raza więcej. Co ciekawe w wysokości możemy zaobserwować różnice jedynie o 11 m na korzyść rakiety SpaceX, 122 m oraz 111 m. Dominacja „Międzyplanetarnego Systemu Transportowego” staje się jeszcze większa kiedy spojrzymy jaki ciąg wytwarza przy starcie – to aż 128 MN. W przypadku Saturna V to jedynie 35 MN czyli 3,6 raza mniej. Bardziej obrazowe będzie przeliczenie tego na masę jaką mogłyby unieść te rakiety z powierzchni Ziemi. W przypadku Saturna V to około 3 579 t, podczas gdy jego młodszy „kolega” byłby w stanie unieść ponad 13 000 t. Projekt SpaceX jest zdecydowanie wydajniejszy jeżeli chodzi o wyniki, a nie rozmiary. Zbiornik na paliwo w „marsjańskiej rakiecie” ma 12 m średnicy kiedy ten w Saturnie V ma zaledwie 2 m mniej. Dodatkowo rakiet wyprodukowana przez NASA jest jednokrotnego użytku, podczas gdy i „Booster” i „Międzyplanetarny Statek Kosmiczny” mają później bezpiecznie wylądować na Ziemi i być gotowe do następnego startu.

4 Koszt

Bardzo ważnym elementem minimalizacji kosztów jednego lotu na Marsa jest możliwość ponownego użycia komponentów transportera. Skonstruowanie „Booster’a” to koszt rzędu 230 milionów dolarów. Inaczej to jednak wygląda kiedy dodamy, że ma on wystartować aż 1000 razy, 5-6 razy przy każdym wylocie ludzi na Marsa. Średnie koszty utrzymania na jeden start SpaceX szacuje na 0,2 miliona dolarów. Dodając do tego koszt amortyzacji oraz paliwa wychodzi około 11 milionów dolarów na jedną podróż na Marsa. Weźmy teraz pod lupę „Tanker”. Koszt produkcji to 130 milionów dolarów. Jego żywotność liczy się na 100 startów, w tym 4-5 na jedną podróż. Średni koszt utrzymania na jeden start to 0,5 miliona dolarów. Ponownie dodając koszt amortyzacji oraz paliwa wychodzi około 8 milionów dolarów na jedną podróż na „Czerwoną Planetę”. Pozostaje statek kosmiczny – 200 milionów dolarów pochłona koszty produkcji. Koszty utrzymania to około 10 milionów dolarów. Zakładają, że statek będziemy mogli użyć 12 razy i dodając do tego wszystkie inne koszty wychodzi około 43 milionów dolarów na jeden start. Podsumowując wszystko jeden start będzie kosztował około 62 milionów dolarów. Jeżeli weźmiemy pod uwagę to, że przetransportowane ma być w tej cenie 450 t ładunku to na jedną tonę wychodzi niecałe 140 000 dolarów. Co ciekawe analitycy SpaceX wyliczyli, że koszt tony paliwa będzie ich kosztował jedynie 168 dolarów amerykańskich. Jednak Elon Musk i jego korporacja mogą liczyć na około 20 milionów zwrotu na każdym starcie. Statek ma zabierać na pokład 100 osób, a bilet kosztować ma 200 000 dolarów.

5 Podróż

Jak ma wyglądać podróż na Marsa? Bardzo „prosto”. „Booster” wynosi statek na niską orbitę okołozemską z prędkością 8 650 km/h gdzie dochodzi do rozłączenia się obu obiektów. „Booster” wraca na Ziemię aby wystartować pierwszy „Tanker”. Później wraca na Ziemię kiedy statek jest tankowany na orbicie. Oczywiście po wykonanym zadaniu „Tanker” również bezpiecznie wraca. Cała operacja powtarzać się będzie 4-5 razy do momentu pełnego załadowania „Międzyplanetarnego Statku Kosmicznego”. Statek będzie czekał na orbicie do momentu kiedy Ziemia i Mars maksymalnie się do siebie zbliżą. Zjawisko takie obserwujemy co 26 miesięcy. Energię w statku zapewniać mają panele słoneczne o mocy aż 200 kW. W trakcie lotu statek ma osiągnąć zawrotną prędkość 100 800 km/h. Warto zaznaczyć, że największa prędkość z jaką kiedykolwiek podróżował człowiek to 39 986 km/h. Ile więc ma trwać lot? Elon Musk twierdzi, że około 80 dni jednak przy takich prędkościach wydaje się to do osiągnięcia znacznie szybciej. Wlatując w atmosferę Marsa statek ma wytrzymać temperaturę około 1700 °C. Do tej pory wszystkie obiekty lądujące na Marsie spowalniane były poprzez spadochron. Tym razem jednak wszystko ma odbyć się poprzez działanie silników. Po wylądowaniu najważniejsza będzie produkcja paliwa, która jak już wspomniałem będzie na Marsie możliwa. Biorąc pod uwagę to, że grawitacja na Marsie jest prawie 63% słabsza niż na Ziemi, a atmosfera znacznie rzadsza statek nie będzie miał problemu z wystartowaniem w drogę powrotną bez pomocy „Boostera”.

6 Przyszłość

SpaceX planuje na 2018 rok bezzałogową misję na Marsa pod nazwą „Red Dragon”. Misja ta ma na celu sprawdzenie systemu lądowania na „Czerwonej Planecie” przy użyciu silników, zidentyfikowania miejsc, w których znajdują się niezbędne surowce takie jak woda oraz znalezienie potencjalnego miejsca lądowania dla misji załogowej, która miałaby się na Marsie pojawić kilka lat później. W połowie 2018 roku planują również rozpoczęcie testów. Statku, „Boostera” oraz wszystkich działań, które mają być prowadzone na orbicie. Testy te mają trwać około 4 lata. Start pierwszej misji załogowej na Marsa planowany jest na końcówkę roku 2022, a w podróż ma się udać 12 osób. Do tego czasu misja „Red Dragon” ma już być zakończona.

Litatura (References)

1. National Aeronautics and Space Administration. <https://www.nasa.gov/>
2. Space Exploration Technologies Corporation. <http://www.spacex.com/>

Pewność Siebie w Karierze Zawodowej i Wykorzystywanie Wiedzy w Praktyce

Piotr Matera

Akademia Górniczo-Hutnicza im. Stanisława Staszica, Kraków, Polska
matera12@gmail.com

Abstract. Pewność siebie w karierze zawodowej jest niezwykle ważna w życiu, to ona definiuje nas samych i określa nasze miejsce w otoczeniu. Jednak pewność siebie determinuje przede wszystkim wiedza, a raczej wykorzystywanie jej w praktyce.

Keywords: Pewność siebie, nauka, wiedza, praktyka, personalna marka

1 Wprowadzenie

Studia to wspaniały okres zdobywania wiedzy i poznawania wielu wspaniałych ludzi. W większości przypadków w tym właśnie okresie sporo rozmyślamy o naszej przyszłości. Począwszy od idealizacji własnych marzeń, skończywszy na konkretnych planach popartych już rozpoczętymi działaniami.

Jedną z kluczowych spraw przy rozpoczynaniu kariery zawodowej niezależnie w jakiej branży będzie to czy będziemy pewni siebie, czy będziemy atrakcyjni pod względem efektywności dla pracodawców.

Kluczem do tego jest efektywne wykorzystywanie swojej wiedzy i to nie tylko w zawodzie ale także w wielu obszarach życia. To pozwoli nam zbudować „personalną markę” co prowadzi do nieograniczonego wzrastania własnego podkreślę zdrowego ego.

Właśnie dlatego połączyłem te dwa na pierwszy rzut oka niezależne aspekty, ponieważ by być pewnym siebie musimy znać swoją wartość, a by znać swoją wartość musimy być świadomi co wiemy, a co nie i jak najefektywniej wykorzystywać swoją wiedzę.

2 Wykorzystywanie wiedzy w praktyce

Może na początek dosyć banalny, ale myślę potrzebny wstęp. Naturalnym synonimem nauki jest naukowiec jego doświadczenia, badania, tezy poparte doświadczeniami itd.

Wiec bardzo możliwe, że w przyszłości także i my coś do tej dziedziny wniesiemy. Jednak co potrzebne nam jest do inaugurowania takich działań?

Wiedza – bez wątpienia jako opoka podstawa i trzon naszych wywodów, nie tylko na tle naukowym, ale teŝ ȳciowym...

Wiadomo im więcej wiemy, im mamy więszą wiedzę, tym lepiej postrzegani jesteŝmy w otoczeniu, tu pojawiają się juŝ załączki autorytetu. Ale czy sama wiedza wystarczy?

Oczywiŝcie to pytanie retoryczne, poniewaŝ nie poruszałbym tego tematu, gdyby moja odpowiedz brzmiała- ”wystarczy”. Sama wiedza nie wystarczy ale poparta efektywnym i owocnym jej wykorzystywaniem juŝ tak.

Efektywnoŝć wykorzystywania wiedzy jest kluczowa w rozwoju nauki.

To juŝ kolejny waŝny aspekt tego elementu w tym referacie. Tutaj skupię się jednak na traktowaniu wiedzy jako narzędzia do powięszania własnego powaŝania, do budowania wcześnieŝ wspomnianej „personalnej marki”, a przecieŝ to międy innymi to jest bardzo istotne w kontekŝcie kariery.

Umiejętnoŝć wykorzystywania wiedzy asertywnoŝć i błyskotliwoŝć w operowaniu wiedzą, a takŝe pewnoŝć siebie w jej wykorzystywaniu.

Ŗwiat nieustannie się rozwija i to my musimy za nim podąŝać, a jeśli chcemy osiągnąć sukces musimy te elementy traktować jako podstawy. Posunę się do prostego, aleŝ jak bardzo nam studentom bliskiego przykłądu- kolokwia.

Ile razy nam się zdarzało, ŝe zasadniczo znaleŝmy odpowiedź na zadane pytanie, ale z drugiej strony nie wiedzieliŝmy jak ten temat ugryŝć itd.

Mnie osobiŝcie bardzo to męczyło i od kiedy zacząłem interesować się takimi zagadnieniami jak sposobnoŝci wykorzystywania wiedzy (sztuką prezentacji naszych dziełań czy to w pracy, na uczelni, czy na różnego rodzaju konferencjach, technikami przemówień publicznych) zacząłem dostrzegać jak waŝny ma to wpływ na to co juŝ umiemy, a co nie do końca umiemy przekazać.

W nawiązaniu do wspomnianych kolokwiów zacząłem stosować metodę, w której przy nauce kaŝdego jednego nowego zagadnienia wyobraŝam sobie, ŝe komuŝ tłumaczę to zagadnienie mając kartkę przed sobą. Jednocześnie sam się go szybko i efektywnie uczę, polecam.

Najczęszszym zarzutem studentów do uczenia się czegoŝ jest to ŝe nigdy tej wiedzy w ŝyciu nie wykorzystamy. Wgłębiając się we wcześnieŝ wspomniane elementy dotyczące wiedzy zaczynam dostrzegać, ŝe to od nas zależy czy my tą wiedzę wykorzystamy czy nie.

Posłuŝę się znów doŝyć prostym, ale wymownym przykłądem: dziadek całe ŝycie uczył Antka szyc buty, kuć podkowy i rzeŝbić...

Po pewnym okresie, gdy dziadek zmarł Antek musiał szybko znaleźć pracę. Nie wiedział jak dysponować swoją wiedzą wiec znalazł zatrudnienie u pierwszego lepszego szewca. Antek zamiast narzekać, ŝe do końca ŝycia albo przez więszą jego połówę będzie szyl buty, a reszta umiejętności mu się na nic nie przyda zaczął po godzinach dla relaksu szyc i rzeŝbić na zamówienie co przynosiło mu zysk w wielkoŝci drugiej pensji zarabianej u szewca. Głupie? Ok troszkę prymitywne ale tylko na pierwszy rzut oka.

3 Pewność siebie w karierze zawodowej

Rozważania na temat pewności siebie w karierze zawodowej chciałbym rozpocząć tym czym tak naprawdę zaczyna się ta kariera zawodowa. Rozmowa kwalifikacyjna przyprawia niektórych o dreszcze, paraliżuje nas co w efekcie nie pozwala nam się pokazać z dobrej strony. Musimy sobie jednak wtedy wmówić, że to my tu jesteśmy dla niego a nie on dla nas, a wcześniejsze przygotowanie sobie ewentualnych równie atrakcyjnych dla nas alternatyw pomaga nam stanąć przed potencjalnym pracodawcą z podniesioną głową, musimy więc mieć świadomość ile jesteśmy warci.

Kiedyś pewna bardzo mądra osoba powiedziała, że największym sukcesem dla nas było by to by tak umieć się przedstawić i zaprezentować przed pracodawcą by nie poprosił cię on o CV, by sama osoba była reprezentatywnym dowodem na to, że taki pracownik jest pani/panu potrzebny.

No dobrze, zostaliśmy zatrudnieni ale co dalej? Nowe otoczenie nowe obowiązki stres i ponoszona na każdym kroku odpowiedzialność wprowadzają mnóstwo osób na początku kariery w ogromne zakłopotanie, a nawet depresję. Budowanie pewności siebie to na pewno nie złoty środek dla tych problemów, ale bez wątpienia jeden z kluczowych elementów do ich rozwiązania. Pewność siebie można wyćwiczyć, nie trzeba się z tym urodzić ani zostać tak a nie inaczej wychowany. Psychologiczną podstawą, takimi podwalinami, by być pewnym siebie jest świadomość swoich mocnych i słabych stron.

Kolejnym elementem na tej drodze jest docenianie własnych sukcesów nawet, a może przede wszystkim tych najmniejszych. Człowiek niezwykle szybko przyzwyczaja się do sytuacji w jakiej jest, czasem jest to zaleta, ale w tym przypadku niestety wada. Bardzo szybko po osiągnięciu jakiegoś sukcesu przestajemy go doceniać i stajemy się neutralni wobec niego. Chcemy jak najszybciej czegoś więcej, co nie zawsze jest takie łatwe i znów wpadamy w takie błędne, zgubne koło tracąc przy tym pewność siebie, bo oczywiście nie wszystko się udaje.

Trzeci element jest nawiązaniem do poprzedniego, a mianowicie nie wolno bać się porażek ponieważ ,nie dość że pracujemy mniej efektywnie ale także tracimy to jakże kluczowe nastawienie.

Wiadomo, że czasem jest trudno a słowa krytyki od pracodawcy brzmiały w uszach godzinami ale to jest ćwiczenie jak każde inne by osiągać lepsze rezultaty stań się bardziej neutralnym a porażkę traktuj jako element rozwoju. Następny element to przyjęcie odpowiedniej postawy, postawy pewnej siebie osoby nawet jeśli na początku będzie inaczej, jesteś w nowym środowisku wśród ludzi którzy może nie za bardzo będą za Tobą przepadać, ponieważ wszędzie są jednostki, które traktują partnerów zawodowych jako konkurencje itd.

Sprawianie pozorów pozwoli uniknąć stłamszenia przez nich, a w dłuższej perspektywie pomoże nabrać wspomnianej już wielokrotnie pewności siebie. Wykorzystywanie wiedzy, którą posiadamy w jak najlepszy sposób pomoże nam w budowaniu tej swojej pozycji, własnej pewności siebie, własnej personalnej marki nie tylko w zawodzie ale i w życiu. I tak właśnie łączą się nam w tym momencie te dwa jakże przydatne w życiu elementy. By być pewnym siebie nie tylko w zawodzie ale i w życiu- trzeba wiedzieć co się wie.

Zarzucając, że brzmi to banalnie powinniśmy jednocześnie zapytać się dlaczego tak wiele osób o tym zapomina, nie doceniając siebie dając się stłamsić przez pracodawców, którzy niejednokrotnie nie pozwalają wykorzystywać potencjału i w żaden sposób nie umożliwiają rozwoju.

To my sami musimy wiedzieć jak wykorzystać własne możliwości, podążać za marzeniami, w spełnianiu których pomoże nam nasza pewność siebie i wykorzystywanie wszystkich nabytych umiejętności a także całej poznanej wiedzy w przyszłości. To wcale nie takie trudne.

Na koniec kończąc motywacyjną puentę, chciałbym podkreślić, że warto walczyć o to o czym marzymy, wiadomo, że nie zawsze się udaje i w życiu bardzo często przychodzi taki moment, że należy odpuścić ale w myśl tego, że kieruję ten wywód do osób, które zaczynają swoją karierę i budowanie wiele razy wspomnianej marki- słuchajcie jesteście młodzi więc co nam szkodzi?

4 Podsumowanie

Reasumując można narzekać i załamywać się, że nie jesteśmy usatysfakcjonowani pracą lub studiami, że uczymy się a następnie i tak wszystko zapominamy, że większość z poznanych rzeczy i tak w późniejszej pracy nie wykorzystamy ale nic nie zmieni faktu że to tylko nasza psychika.

Tu nie ma filozofii, wszystko można wyćwiczyć i na każdej płaszczyźnie można się realizować, aby tak było potrzebna nam jest bardzo szeroko pojęta wiedza którą wykorzystując stajemy się pewni siebie w życiu w zawodzie co prowadzi do tego, że będziemy spełnieni życiowo i zawodowo.

Literatura (References)

1. Alan Loy McGinnis „Sztuka pewności siebie: jak odkryć swoją wartość i pokonać nieśmiałość”
2. Kate Burton, Brinley Platts „Budowanie pewności siebie dla bystrzaków”
3. Alexandre Havard „Etyka przywódcy. Trening doskonalenia osobowości”
4. Wawer Rafał, Wawer Monika „Trwałość wiedzy w procesie kształcenia”

Arkusz 8D jako Narzędzie Doskonalenia Jakości w Przedsiębiorstwie

Katarzyna Szczepara

Akademia Górniczo-Hutnicza im. S.Staszica, Kraków, Polska
katarzyna.szczepara@gmail.com

Abstract. W referacie został omówiony arkusz analizy 8D. Wprowadzony początkowo w branży motoryzacyjnej, może być z powodzeniem stosowany w przedsiębiorstwach usługowych. Jego budowa umożliwia stosowanie narzędzia w całości bądź dopasowanie go do własnych potrzeb. W referacie przedstawiono przebieg analizy za pomocą arkusza 8D na prostym przykładzie z życia codziennego.

Keywords: Lean Management · Szczupłe zarządzanie · Toyota Production System · Arkusz 8D · Zarządzanie jakością · 5 WHY

1 Wstęp

Zapewnienie odpowiedniego poziomu jakości produkowanych wyrobów jest istotne dla każdego przedsiębiorstwa, które chce utrzymać konkurencyjną pozycję na rynku lub ma aspiracje do bycia branżowym liderem. Odpowiedni poziom jakości nie oznacza, że wyroby muszą być doskonałe, ponieważ ich wysoka cena może sprawiać, że klienci nie będą skłonni ich kupić. Z tego powodu podczas planowania produkcji istotne jest, żeby dopasować poziom jakości wyrobów gotowych do oczekiwań klientów.

2 Arkusz 8D – case study

Szczupłe Zarządzanie jest koncepcją pracy w taki sposób, żeby straty ograniczyć do minimum. Likwidacja takich muda jak nadprodukcja, nadmierny transport, oczekiwanie czy zbędny ruch pozwala ograniczyć wydatki przedsiębiorstwa. Likwidacja czynności niedodających wartości dla klienta sprawia, że więcej czasu można poświęcić na doskonalenie procesu i wyrobu. Tym samym pozwala osiągnąć wyższą jakość bez ponoszenia dodatkowych kosztów. Jedną z metod rozwiązywania problemów, stosowanych podczas szczupłego zarządzania, jest analiza wykonywana przy użyciu arkusza 8D.

Arkusz 8D to zaawansowane narzędzie stworzone dla potrzeb przemysłu samochodowego. Pozwala na bardzo dokładną analizę przyczyn powstania danego problemu i odnalezienie przyczyn źródłowych. Dzięki temu wprowadzane działania

zaradczę są słuszne i rozwiązują problem zamiast maskować go lub odkładać jego skutki w czasie. Dokładna analiza przyczyn jest pracochłonna, co stanowi główną wadę arkusza.

Zespół 8D musi składać się z co najmniej 3 osób. Ważne jest również, żeby był możliwie najbardziej interdyscyplinarny. W przypadku pojawienia się wadliwego wyrobu na stanowisku montażu końcowego, do zespołu powinni być zaproszeni również pracownicy poprzednich etapów obróbki, zarówno operatorzy jak i wyższe kierownictwo. Zapewni to szerokie spojrzenie na analizowany problem, dzięki czemu stawiane przypuszczenia będą bardziej trafne.

Budowa arkusza sprawia, że konieczna jest dogłębna analiza problemu. Nie można od razu przejść do wprowadzania długotrwałych usprawnień, które mają trwale wyeliminować zaistniały problem. W przypadku problemu, jakim jest brak wody w czajniku, od razu przychodzi nam na myśl oczywiste rozwiązanie - wystarczy dolać wody i problem zostanie rozwiązany. Często przechodzimy do wprowadzania usprawnień bez dokładnej analizy przyczyn powstania problemu. Uzupełnienie wody pomoże, jednak w przypadku dziurawego dna czajnika, problem będzie stale powracał do czasu, aż zostanie zlikwidowana przyczyna źródłowa. Z tego samego powodu w przypadku rozwiązywania problemów produkcyjnych, a także każdego innego problemu, istotne jest spojrzenie na problem z dystansu, chłodna ocena i dociekanie przyczyn źródłowych.

Ponieważ analiza trudnych problemów, takich jak wady powstałe w procesie spawania czy wulkanizacji, wymaga znajomości przebiegu tych procesów, zdecydowałam się na prostszy przykład. Problemem, który chcę rozwiązać, pokazując krok po kroku przebieg rozumowania w analizie 8D, będzie problem fusów w kawie. Każdemu z nas zdarzyło się pić kawę parzoną, więc problem jest zrozumiały dla szerokiego grona odbiorców. Przebieg analizy został zilustrowany w tabeli zamieszczonej poniżej (rys. 1).

Dzięki przeprowadzeniu dogłębnej analizy przyczyn powstania problemu odkryto przyczyny źródłowe. Wprowadzone działania pozwoliły zlikwidować przyczyny źródłowe. Z tego powodu ponowny problem nie wystąpił ponownie.

3 Podsumowanie i wnioski

Gdyby w analizie ograniczono się do typowego toku myślenia, w którym od razu wprowadzane są działania naprawcze, końcowy efekt prawdopodobnie byłby inny. Poświęcenie zaledwie minuty na rozwiązanie problemu (a przecież tyle myślimy o zepsutej prasie do kawy) sprawiłoby, że alternatywne rozwiązania problemu, takie jak wprowadzenie oznaczeń na zmywarkę, zostałyby przeoczone. Szerokie spojrzenie na analizowany problem sprawiło, że zmniejszono ryzyko wystąpienia innych problemów związanych z brudnymi naczyniami. Poziomą jakość pożywienia przyrządzanego w danym miejscu podniósł się. Jednocześnie obniżyło się ryzyko „awarii”, takiej jak fusy w kawie. Co ważne, wprowadzone rozwiązania nie wymagają dużych nakładów finansowych.

Arkusz 8D																	
Data:	2018/07/04 Tłuszcz: Kawa ekspozycja w procesie francuskiej, ma fusy																
Opis problemu:	Wzrost fusów w kawie, zmiana koloru, zmiana smaku																
Opis celu problemu:	Redukcja zawartości fusów w kawy w ilości 20,000 tona, zmniejszenie wad, zapewnienie jakości i zgodności z wymaganiami klienta. Skonkretyzowanie celu i wykonanie i monitorowanie. Podjęcie działań korekcyjnych i zapobiegawczych, aby uniknąć powtórzenia błędów. Wykonanie działań korekcyjnych i zapobiegawczych, aby uniknąć powtórzenia błędów.																
Opis efektów:	Przebieg choroby kawy w kawa, zmiana koloru, zmiana smaku, zmiana smaku, zmiana smaku. W celu zapewnienia jakości produktu, podjęcie działań korekcyjnych i zapobiegawczych, aby uniknąć powtórzenia błędów. Wykonanie działań korekcyjnych i zapobiegawczych, aby uniknąć powtórzenia błędów.																
Opis sposobu postępowania:	<p>PLANOWANIE</p> <p>Wniosek:</p> <p>Tępy w kawałki -> kawałki w kawałki, np. fusy -> kawałki w kawałki -> zmniejszenie zawartości fusów</p> <p>Tępy w kawałki -> kawałki w kawałki, np. fusy -> kawałki w kawałki -> zmniejszenie zawartości fusów</p> <p>Tępy w kawałki -> kawałki w kawałki, np. fusy -> kawałki w kawałki -> zmniejszenie zawartości fusów</p> <p>Tępy w kawałki -> kawałki w kawałki, np. fusy -> kawałki w kawałki -> zmniejszenie zawartości fusów</p> <table border="1"> <thead> <tr> <th>Przyczyna</th> <th>Opis</th> <th>Wpływ</th> <th>Wpływ</th> </tr> </thead> <tbody> <tr> <td>Przyczyna</td> <td>Opis</td> <td>Wpływ</td> <td>Wpływ</td> </tr> <tr> <td>Przyczyna</td> <td>Opis</td> <td>Wpływ</td> <td>Wpływ</td> </tr> <tr> <td>Przyczyna</td> <td>Opis</td> <td>Wpływ</td> <td>Wpływ</td> </tr> </tbody> </table>	Przyczyna	Opis	Wpływ	Wpływ	Przyczyna	Opis	Wpływ	Wpływ	Przyczyna	Opis	Wpływ	Wpływ	Przyczyna	Opis	Wpływ	Wpływ
Przyczyna	Opis	Wpływ	Wpływ														
Przyczyna	Opis	Wpływ	Wpływ														
Przyczyna	Opis	Wpływ	Wpływ														
Przyczyna	Opis	Wpływ	Wpływ														
Opis efektów:	Wzrost fusów w kawie, zmiana koloru, zmiana smaku																
Opis efektów:	Wzrost fusów w kawie, zmiana koloru, zmiana smaku																
Opis efektów:	Wzrost fusów w kawie, zmiana koloru, zmiana smaku																

Rys. 1. Arkusz analizy 8D (opracowanie własne)

W przypadku problemu fusów w kawie skutki wystąpienia wady nie są znaczące. Jest to jednak prosty przykład, umożliwiające zrozumienie przebiegu analizy przyczyn powstania wad za pomocą arkusza 8D. Jak łatwo się domyślić, arkusz jest stosowany do poważnych problemów występujących w procesach produkcyjnych. Może być z powodzeniem stosowany również w przedsiębiorstwach usługowych. Jego budowa umożliwia dopasowanie arkusza do własnych potrzeb, poszerzenie niektórych elementów analizy i zrezygnowanie z innych. Z tego powodu jest niezwykle interesującym narzędziem, z którym bez wątpienia warto się zapoznać.

Literatura (References)

1. Referat powstał w oparciu o moją pracę inżynierską. Praca nosi tytuł: „Zastosowanie analizy 8D jako elementu doskonalenia jakości na przykładzie firmy produkcyjnej z branży motoryzacyjnej”. Promotorem pracy był dr inż. Jan Sas, natomiast recenzentem dr hab. inż. Piotr Saługa. Praca inżynierska została obroniona 27.01.2017 roku w Akademii Górniczo-Hutniczej w Krakowie.

Zmiany w Klasyfikacji Odporności Ogniowej Kabli i Przewodów

Magdalena Muszyńska

Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, Polska
mgd.muszynska@gmail.com

Abstract. Na terenie Państw Unii Europejskiej, z dniem 1 lipca 2016, rozporządzenie CPR zastąpiło dotychczasową działającą Dyrektywę CPD (z ang. Construction Products Directive). CPR wprowadziło szereg zmian w produkcji i dystrybucji wyrobów budowlanych na terenie państw Unii Europejskiej. Została zwrócona jeszcze większa uwaga na zachowanie bezpieczeństwa pożarowego.

Keywords: kabel, przewód, odporność ogniowa, klasyfikacja kabli

1 Wstęp

Instalacje elektryczne są nieodłącznym elementem budynków. Ludzie przyzwyczaili się do prądu i ciężko wyobrazić sobie jego brak podczas codziennego funkcjonowania. Jednak tam gdzie znajdują się instalacje elektryczne, zwiększa się ryzyko pożaru, ponieważ są one ich nierzadką przyczyną. Bagatelizowanie przyczyn pożarów i nie dbanie o ich odpowiednie zabezpieczenie, może skutkować poważnymi konsekwencjami dla stanu budynku, obiektów, które się w nim znajdowały, jak również ludzi.

Wraz z dyrektywą dotyczącą wyrobów budowlanych CPR (ang. *Construction Products Regulation*), uregulowano przepis odnoszący się do bezpieczeństwa pożarowego wyrobów budowlanych, które będą podlegać temu rozporządzeniu, a co za tym idzie, ich definicję i klasyfikację. Trafnie przypisano kable i przewody, które mają być na stałe wbudowane w obiekt do wyrobów budowlanych.

Podczas każdej z faz pożaru, zagrożeniami stają się inne negatywne skutki spalania się kabli i przewodów. Wprowadzenie zaostrzonych zasad nadawania im klasy odporności ogniowej nie jest więc bezpodstawne, lecz kierowane potrzebą rynku.

2 Rozporządzenie CPR

Klasyfikacja kabli i przewodów do wyrobów budowlanych, a więc podlegających pod nowe rozporządzenie, zmusiło ich producentów do uregulowania procesów kontroli jakości, którym wyroby zostają poddawane. Zwiększono ilość badań mającą na celu zakwalifikowanie ich do odpowiednich klas odporności ogniowej i nadania im, oprócz głównej, dodatkowych klas, określających ich zachowanie podczas spalania.

Oprócz pomiaru rozprzestrzeniania się płomienia, dołączono także cztery inne parametry: wydzielania się ciepła, dymu i toksycznych gazów jako produktów spalania się materii, oraz pojawienie się płonących kropli. Obecne wymagania normowe dają możliwość szeroko pojętej analizy zachowania się produktu podczas pożaru. Potrzeba utrzymania wysokich europejskich standardów, niejako narzuca projektantom, aby kryterium priorytetowe stanowiła klasyfikacja odporności ogniowej wyrobów budowlanych, w tym kabli i przewodów. Uregulowano obowiązek przekazywania pełnej informacji na temat stanu i klasy wyrobu do użytkownika ostatecznego. Jest to zdecydowane ułatwienie dla inwestorów, którzy już na początku podejmowania decyzji o wyrobie użytym w ich inwestycji, będą posiadać pełen zakres informacji o nim. CPR ukazuje metody przekazywania tych informacji, z których najważniejsza jest Deklaracja Właściwości Użytkowych. Dodatkowo rozporządzenie określa, iż w obowiązku wytwórcy, którym jest bezpośredni producent, lub, jeżeli produkcja prowadzona jest poza granicami Unii Europejskiej, importer, jest oznakowanie CE i przedstawienie niezbędnej dokumentacji gwarantującej przeprowadzenie badań.

3 Analiza zagrożenia pożarowego, wywołanego przez kable i przewody

Podczas analizy zagrożenia pożarowego, wywoływanego przez kable i przewody, istotą jest rozróżnienie zagrożeń wynikających z materiałów, z których się składają, jak i cech funkcjonowania, czy zagrożeń powstałych w wyniku ich niepoprawnego eksploataowania, wad konstrukcyjnych budynku. Dopiero takie podejście, pozwala obiektywnie spojrzeć na kable i przewody od strony ich odporności na ogień, albo przyczyniania się do jego powstania. Kluczowym aspektem bezpieczeństwa pożarowego, jest bowiem życie i zdrowie osób, znajdujących się w budynku. Ponieważ często osoby te nie mają wiele czasu na ewakuację, wielokrotnie dochodzi do sytuacji, gdzie na stan ich zdrowia wpływają minuty, czy sekundy.

Podstawowym pojęciem omawianym w rozporządzeniu CPR jest odporność ogniowa, definiowana jako „*zdolność elementu budynku do spełnienia określonych wymagań podczas pożaru*”. W trakcie pożaru nierzadko dochodzi do sytuacji niebezpiecznych, zagrażających życiu i zdrowiu osób, najważniejsza jest więc ich szybka i bezpieczna ewakuacja.

4 Klasyfikacja odporności ogniowej kabli i przewodów

Izolacje to ważny czynnik podczas analizowania bezpieczeństwa pożarowego. To właśnie tworzywa sztuczne zapalają się podczas pożaru. Dąży się do tworzenia izolacji samogasnących, które nie podtrzymują płomienia, a co za tym idzie - ogień nie może się rozprzestrzeniać a szkodliwe gazy nie zostałyby uwalniane podczas spalania. CPR narzuca standardy, które ograniczają użycie szczególnie polwinitu, jako materiału termoplastycznego użytego do wykonania izolacji. Gdy jest on ułożony w wiązce, bardzo szybko rozprzestrzenia ogień, a ponadto podczas spalania uwalniany

jest chlor, który po połączeniu z wodorem tworzy szkodliwy gaz - chlorowodór. Już w małym stężeniu oddziałuje on szkodliwie na zdrowie człowieka, a jego obecność może uniemożliwić oddychanie. Obecność toksycznych gazów powoduje więc w niektórych sytuacjach szkody gorsze od tych wywołanych samym pożarem. Kable, których materiał izolacyjny zawiera polimery na bazie czystych węglowodorów – tzw. kable bezhalogenowe - podczas spalania nie wytwarzają niczego prócz pary wodnej oraz dwutlenku węgla, są więc o wiele bezpieczniejsze dla zdrowia. Niestety ich wadą jest łatwopalność. By sprostać wymaganiom CPR, kable bezhalogenowe, muszą być wytworzone dodatkowo z mieszanką specjalnych polimerów, zawierających znaczący procent środków chroniących przed płomieniami.

Do tej pory, przepisy gwarantowały jedynie testy na rozprzestrzenianie się ognia, jednak wraz z CPR wprowadzono cztery inne, dodatkowe parametry:

- wydzielanie ciepła,
- wydzielanie dymu, który zaburza zmysł orientacji, przez co dotarcie do wyjść ewakuacyjnych, jak i przeprowadzenie akcji ratunkowej jest utrudnione,
- wydzielanie korozyjnych gazów,
- występowanie płonących kropli, które w krótkim czasie umożliwiają zwiększenie terytorium objętego przez ogień.

Wprowadzenie nowego rozporządzenia wymusiło zmiany w produkcji, klasyfikacji i kontroli jakości kabli i przewodów. Powstały nowe klasy odporności ogniowej kabli i przewodów a także dodatkowe oznaczenia. By uzyskać najwyższe klasy, możliwość stosowania niektórych dotychczasowych materiałów izolacyjnych kabli została mocno ograniczona. Kolejną konsekwencją CPR jest wymóg wystawiania Deklaracji Właściwości Użytkowych oraz znakowanie wyrobów znakiem CE. DoP to dokument wystawiany wyrobom, które są objęte zharmonizowaną normą europejską lub są tożsame z wydaną dla nich Europejską Oceną Techniczną. Znak CE gwarantuje użytkownikowi danego wyrobu, że producent spełnił wysokie kryteria w obszarze bezpieczeństwa pożarowego dla danego produktu, zakwalifikował go do odpowiedniej euroklasy, co zostało prawidłowo udokumentowane. Zmiany w oznakowaniu oznaczają zmianę etykiet wyrobów, na których muszą znaleźć się dodatkowe informacje, które wcześniej nie były wymagane. Zakłady produkujące kable i przewody, by sprostać nowym wymaganiom, musiały doposażyć swoje laboratoria. Dotychczas, wybór kabli bazował na ich zastosowaniu. W tym momencie staje się to drugorzędną sprawą, a priorytetem jest typ budynku, do którego dobierane są kable i przewody, zgodne z klasą dla niego obowiązującą.

Wdrożenie CPR poskutkowało wprowadzeniem nowej klasyfikacji odporności ogniowej kabli i przewodów, która wzbogacona jest o dodatkowe oznaczenia, jak i nowe główne klasy. Aktualnie rozróżnia się siedem głównych klas, kolejno: A, B1, B2, C, D, E oraz F. Na dzień dzisiejszy nie jest możliwe wyprodukowanie przewodu o klasie A, ponieważ oznaczałoby to, że jest on niepalny. Główna klasa określa wydzielanie się ciepła, oraz rozprzestrzenianie ognia podczas spalania.

Dodatkowymi oznaczeniami, które dopełniają całości są:

- gęstość dymu, oznaczona odpowiednio klasami: s1, s1a, s1b, s2, s3;
- występowanie płonących kropeł, oznaczone odpowiednio klasami: d0, d1, d2;
- wydzielanie trujących gazów podczas spalania, tzw. korozyjność: a1, a2, a3.

Całość oznaczeń tworzy pełną klasę odporności ogniowej, przypisaną dla danego wyrobu, które spełnia odpowiednie wymagania.

5 Podsumowanie

Podsumowując kable i przewody, podczas pożaru, mogą zarówno przyczynić się do jego rozprzestrzeniania się, jak i zwiększyć szkody nim spowodowane. Rozporządzenie CPR nakreśla zmiany przede wszystkim w polityce kontroli jakości kabli i przewodów. Materiały dotychczas używane do produkcji kabli, stopniowo będą ustępować nowym, które oprócz mniejszego wydzielania ciepła i rozprzestrzeniania się płomienia, spełniać będą pozostałe normy bezpieczeństwa pożarowego. Wprowadzenie nowych klas odporności ogniowej kabli i przewodów usystematyzowało ich podział ze względu na zastosowanie w budynkach, w których bezpieczeństwo pożarowe wymaga wysokich standardów. Nie tylko zbyt niska klasa główna, ale także niskie parametry dodatkowe parametrów, wpływają na niemożliwość stosowania kabli i przewodów w budynkach o wysokich wymaganiach bezpieczeństwa pożarowego, o utrudnionej ewakuacji w przypadku zagrożeń takich jak: hotele, sale konferencyjne i widowiskowe, szpitale, magazyny składujące materiały o podwyższonym ryzyku pożaru czy galeriach handlowych.

Literatura (References)

1. Germata M, Grobicki J., *Przewody i kable elektroenergetyczne*, Wydawnictwo WNT, Warszawa 2012.
2. Jaskółowski W., *Zagrożenia powstające przy spalaniu izolacji, kabli lub przewodów elektrycznych*, Elektro.info, nr 05/2015, str 24-27.
3. https://pl.wikipedia.org/wiki/Odporno%C5%9B%C4%87_ogniowa [dostęp 12.01.2017]
4. Piechulek M., *Klasyfikacja kabli pod względem pożarowym (część 1)*, Zabezpieczenia, nr 04/2016, str 40-43
5. Muszyńska M. Analiza jakości kabli uwzględniająca klasyfikację odporności ogniowej kabli i przewodów, Praca dyplomowa.

Аналіз Точності Методів Контролю Складу Бінарної Вугільної Суміші

Галина Матіко, Степан Мисак

Національний університет “Львівська політехніка”, Львів, Україна
halynamatiko@gmail.com
s.mysak750@gmail.com

Abstract. В роботі виконана оцінка точності двох методів контролю складу бінарної суміші, що надходить до пилосистеми котла. За першим методом склад вугільної суміші визначають за значеннями вмісту летких речовин на горючу масу вугільної суміші та кожної із марок вугілля, з яких складається суміш. У другому методі частки двох марок вугілля знаходять за нижчою теплотою згоряння вугільної суміші та нижчою теплотою згоряння вугілля двох марок, що входять до складу суміші. Отримані залежності для оцінки невизначеності результату обчислення часток складових вугільної суміші, які дають змогу прогнозувати точність реалізації цих методів для вугільної суміші різного складу

Keywords: Вугільна суміш; Метод; Склад суміші; Точність; Невизначеність

1 Вступ

Для забезпечення ефективного спалювання непроектного палива на теплових електричних станціях слід контролювати вміст складових вугільної суміші. Для цього застосовують методи визначення часток складових двох видів палива за результатами хімічного аналізу вугільної проби, яку відбирають безпосередньо з потоку вугілля перед млином [1-3]. В методі [1] склад вугільної суміші знаходять за відомими значеннями вмісту летких речовин на горючу масу вугільної суміші та вмісту летких речовин на горючу масу кожної із марок вугілля. Відповідно частку r_1 та r_2 вугілля першої та другої марки у суміші визначають як:

$$r_1 = \frac{V_C - V_2}{V_1 - V_2}, \quad r_2 = 1 - r_1 \quad (1)$$

де V_1 і V_2 – вміст летких речовин на горючу масу кожної із марок вугілля, з яких складається вугільна суміш; V_C – вміст летких речовин на горючу масу вугільної суміші.

Другий метод [2] контролю часток складових суміші двох марок вугілля

полягає у застосуванні залежності, яка пов'язує склад вугільної суміші із нижчою теплотою згоряння суміші палива на робочу масу та нижчою теплотою згоряння вугілля двох марок палива.

2 Оцінка точності методів контролю складу суміші вугілля двох марок

Авторами виконана оцінка точності описаних вище методів контролю часток складових суміші двох марок вугілля, що поступає в кульові барабанні млини пилосистеми котла. Зокрема, сумарну стандартну невизначеність u_{r_1} результату непрямих вимірювань частки r_1 першої марки вугілля визначають за залежністю

$$u_{r_1} = \sqrt{a_1^2 \times u_{V_C}^2 + a_2^2 \times u_{V_1}^2 + a_3^2 \times u_{V_2}^2}, \quad (2)$$

де u_{V_C} - стандартна невизначеність результату обчислення вмісту легких речовин на горючу масу вугільної суміші; u_{V_1} - стандартна невизначеність результату обчислення вмісту легких речовин на горючу масу першої марки вугілля; u_{V_2} - стандартна невизначеність результату обчислення вмісту легких речовин на горючу масу другої марки вугілля; a_i - відповідні вагові коефіцієнти, які враховують вплив кожної складової залежності (2) на результат непрямого вимірювання частки r_1 вугілля першої марки:

$$a_1 = \frac{\partial r_1}{\partial V_C} = \frac{1}{V_1 - V_2}; \quad a_2 = \frac{\partial r_1}{\partial V_1} = \frac{V_2 - V_C}{(V_1 - V_2)^2}; \quad a_3 = \frac{\partial r_1}{\partial V_2} = \frac{V_C - V_1}{(V_1 - V_2)^2}.$$

Якщо $u_{V_C} = u_{V_1} = u_{V_2} = u_V$, то сумарну стандартну невизначеність результату обчислення частки r_1 вугілля першої марки у вугільній суміші знаходимо за формулою

$$u_{r_1} = \frac{u_V}{(V_1 - V_2)^2} \sqrt{(V_1 - V_2)^2 + (V_2 - V_C)^2 + (V_C - V_1)^2}. \quad (3)$$

Відносну стандартну невизначеність результату обчислення частки r_1 вугілля першої марки у вугільній суміші знаходимо за залежністю [4]:

$$u'_{r_1} = \frac{u_{r_1}}{r_1} \times 100\% = \frac{u_v \times 100\%}{(V_1 - V_2)(V_c - V_1)} \sqrt{(V_1 - V_2)^2 + (V_2 - V_c)^2 + (V_c - V_1)^2}. \quad (4)$$

Оскільки у другому методі [2] залежність для визначення частки вугілля у суміші аналогічна за виглядом до залежності (1), то для оцінки можливої невизначеності результату обчислення часток складових суміші двох марок вугілля цим методом можна також скористатися залежностями (2-4).

За даними лабораторії електростанції проаналізовано, як змінюється склад вугільної суміші та його відносна стандартна невизначеність u'_{r_1} при зміні значення вмісту V_c летких речовин на горючу масу вугільної суміші. На рисунку 1 наведено зміну складу вугільної суміші (частки r_1), яка складається із пісного вугілля марки «П» ($V_1 = 12\%$) та антрациту марки «А» ($V_2 = 3,5\%$) залежно від значення вмісту летких речовин V_c на горючу масу вугільної суміші.

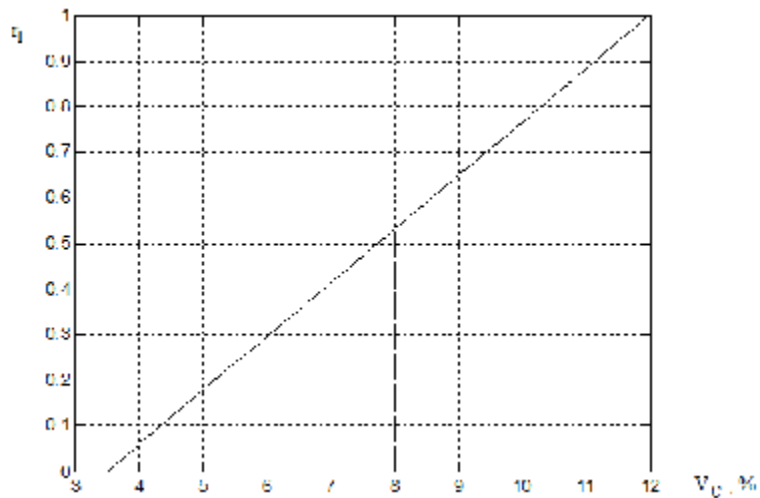


Рис. 1. Залежність частки r_1 пісного вугілля марки «П» у вугільній суміші від значення вмісту летких речовин V_c на горючу масу вугільної суміші

Так, наприклад, вміст летких речовин $V_c = 8\%$ відповідає значенню частки пісного вугілля марки «П» $r_1 = 0,53$ та частки вугілля марки «А» $r_2 = 1 - r_1 = 0,47$.

На рисунку 2 показано зміну відносної стандартної невизначеності u'_{r_1}

результату обчислення частки r_1 вугілля марки «П» у вугільній суміші в залежності від значення вмісту V_C летких речовин на горючу масу вугільної суміші. Так, наприклад, при значенні вмісту летких речовин $V_C = 8\%$ та частці вугілля марки «П» у вугільній суміші $r_1 = 0,53$ відносна стандартна невизначеність u'_{r_1} результату $u'_{r_1} = 5,4\%$. При збільшенні частки вугілля марки «А» у вугільній суміші відносна стандартна невизначеність результату обчислення складу суміші зростає і при $V_C \text{ ® } V_1$ відносна стандартна невизначеність $u'_{r_1} \text{ ® } \text{¥}$.

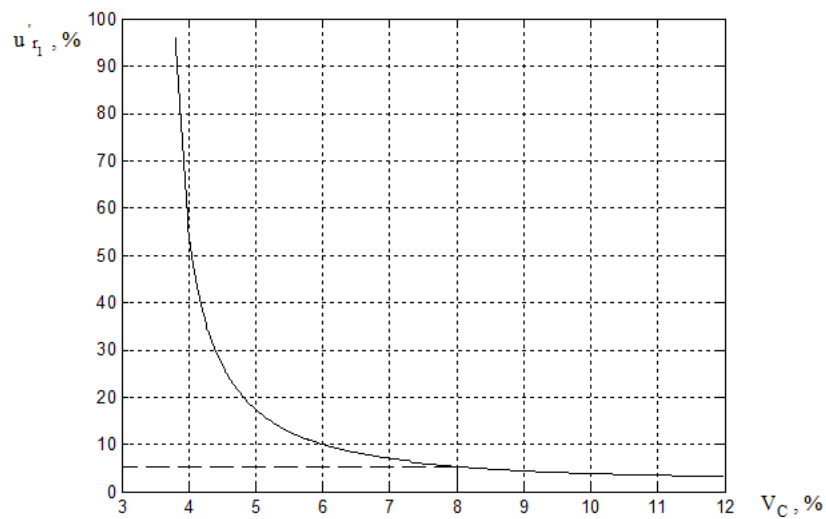


Рис. 2. Залежність відносної стандартної невизначеності u'_{r_1} результату обчислення частки r_1 пісного вугілля марки «П» у вугільній суміші від значення вмісту летких речовин V_C на горючу масу вугільної суміші

3 Висновки

В роботі виконана оцінка невизначеності результату обчислення складу суміші двох марок вугілля, що надходить у пилосистему котла. Отримані залежності для оцінки невизначеності результату обчислення часток складових вугільної суміші за методами [1, 2], які дають можливість прогнозувати точність реалізації цих методів для вугільної суміші різного складу.

Література (References)

1. Спосіб визначення часток складових суміші двох марок вугілля пилосистеми котла. Патент України на винахід , № 90343, автори: Омеляновський П.Й., Голишев Л.В., Мисак Й.С., Мисак І.В. Бюл. № 8 від 26.04.2010 р. F 23 K 1/00, G 01 N 25/00.
2. Спосіб визначення часток складових суміші марок вугілля пилосистеми котла. Патент України на винахід № 104223, автори: Мисак С.Й. Бюл. №1 від 10.01.2014. F 23K 1/00 , G 01N 33/22 (2006.01), G 01 N 25/00.
3. Дєдов В. Г. Досвід експериментального спалювання вугілля Г/А на Трипільській ТЕС / В. Г. Дєдов, О. М. Коземко, м.в. Чернявський та ін. // Енергетика та електрифікація. – 2010. – №6. – С. 21–25.
4. Дорожовець М. М. Опрацювання результатів вимірювань: навч. посібник / М. М. Дорожовець – Л.: Вид-во Львівської політехніки, 2007. – 624 с.

Wykorzystanie Standardu XBRL w Sprawozdawczości Zintegrowanej

Bartosz Rymkiewicz, Iwona Matuszyk

Akademia Górniczo-Hutnicza im. S.Staszica, Kraków, Polska

bartosz.rymkiewicz@wp.pl

matuszykiwona@gmail.com

Abstract. Współcześnie można zaobserwować znaczący wzrost zainteresowania interesariuszy informacjami na temat działalności przedsiębiorstw, a w szczególności jego wpływu na otoczenie. W związku ze wzrostem potrzeb informacyjnych interesariuszy tradycyjna sprawozdawczość zawierająca wyłącznie dane finansowe przestaje spełniać swoje cele. Doskonałym rozwiązaniem tego problemu, a jednocześnie efektywnym narzędziem komunikacji z interesariuszami wydaje się sprawozdawczość zintegrowana. Sprawozdanie zintegrowane integruje w postaci jednego dokumentu zarówno dane finansowe, jak i pozafinansowe, zapewniając ich wzajemne powiązanie. Jednakże wielość metod sporządzania raportów zintegrowanych i form ich prezentacji utrudnia komunikację z interesariuszami. Zdaniem autorów rozwiązaniem wskazanego problemu mogłoby być wprowadzenie standardu XBRL w sprawozdawczości zintegrowanej. W niniejszym artykule autorzy podejmują próbę przedstawienia możliwości wykorzystania języka XBRL w tworzeniu raportów zintegrowanych. W tym celu wykorzystano metody badawcze takie jak: analiza literatury przedmiotu oraz analiza treści publikacji korporacyjnych.

Keywords: XBRL, sprawozdawczość zintegrowana, komunikacja z interesariuszami

1 Wprowadzenie

We współczesnym świecie, dostęp do informacji stanowi podstawę funkcjonowania nie tylko działalności gospodarczej, ale również całego społeczeństwa. W ostatnich dziesięcioleciach znacząco wzrosła liczba podmiotów zainteresowana danymi na temat wpływu przedsiębiorstwa na jego otoczenie. Jednakże powstaje pytanie, w jaki sposób organizacja powinna się komunikować z interesariuszami, aby umożliwić maksymalizację korzyści zarówno dla nich, jak i samej organizacji. W dobie szybkiego rozwoju technologicznego organizacja może wybierać z szerokiego katalogu kanałów komunikacyjnych tj. kontakty bezpośrednie, media tradycyjne, media społecznościowe, publikacje korporacyjne itp. Niewątpliwie jednym z najważniejszych kanałów komunikacji jest sprawozdawczość przedsiębiorstwa. Jednakże tradycyjna sprawozdawczość zawierająca wyłącznie dane finansowe przestała spełniać swoją rolę,

jaką jest przedstawienie rzetelnego obrazu przedsiębiorstwa, interesariusze oczekują od organizacji również informacji pozafinansowej dotyczącej jej wpływu ekonomicznego, społecznego i środowiskowego na otoczenie wewnętrzne i zewnętrzne. Współczesna sprawozdawczość przedsiębiorstwa wychodzi na przeciw potrzebom interesariuszy ewoluując z prostego sprawozdania finansowego zawierającego wyłącznie dane finansowe w rozbudowane zestawy raportów korporacyjnych zawierających raporty roczne, raporty społeczne, raporty środowiskowe i inne raporty obejmujące zarówno dane finansowe, jak i pozafinansowe [15]. Jednakże wielość raportów odnoszących się do różnych aspektów działalności przedsiębiorstwa, rozmywa obraz organizacji i utrudnia odbiór informacji przez interesariuszy. Interesariusze oczekują zaś informacji istotnych zarówno z perspektywy ich samych, jak i organizacji, a także rzetelnych, wiarygodnych, porównywalnych i wzajemnie ze sobą powiązanych. Rozwiązaniem wypełniającym wszystkie powyższe cechy jest sprawozdawczość zintegrowana, która stanowi nowoczesne narzędzie komunikacji z interesariuszami.

W niniejszym artykule autorzy podejmują próbę przedstawienia możliwości wykorzystania języka XBRL w tworzeniu raportów zintegrowanych. W tym celu wykorzystano metody badawcze takie jak: analiza literatury przedmiotu oraz analiza treści publikacji korporacyjnych.

2 Raportowanie zintegrowane jako nowoczesne narzędzie komunikacji z interesariuszami

Współczesne przedsiębiorstwa prowadzą bardzo rozbudowaną sprawozdawczość. Publikują zarówno raporty o charakterze obligatoryjnym (sprawozdanie finansowe, sprawozdanie z działalności jednostki), jak i raporty dobrowolne tj. raporty roczne o charakterze marketingowym lub biznesowym, raporty środowiskowe, raporty społeczne, raporty zrównoważonego rozwoju, raporty z przestrzegania zasad ładu korporacyjnego i wiele innych. Wielość publikacji nie przekłada się jednak na jakość komunikacji z interesariuszami. Duże rozproszenie danych pomiędzy raportami, odnośnienie się tylko do wybranych aspektów działalności oraz znaczne rozmiary publikacji dla wielu interesariuszy stanowią znaczące bariery w komunikacji z organizacją. Odpowiedź na potrzeby interesariuszy w zakresie transparentności i jakości publikowanych informacji stanowić może nowoczesna koncepcja sprawozdawczości jaką jest raportowanie zintegrowane [14]. Koncepcja ta jest obecnie szeroko dyskutowana w literaturze przedmiotu¹. Zakłada ona zintegrowanie i powiązanie danych finansowych i pozafinansowych (np. dotyczących strategii, wyników działalności oraz zarządzania), w jednym kompleksowym raporcie. W literaturze przedmiotu wskazuje się również na kluczowe znaczenie wartości jaką kreuje organizacja [15, 10]. W związku z powyższym raport zintegrowany określa się niekiedy sprawozdaniem z wartości [15].

¹ Tematykę sprawozdawczości zintegrowanej poruszali m.in. R.G. Eccles, M.P. Krzus, S. Ribot [4], C. Churet, R.G. Eccles [3], B.Bek-Gaik, B.Rymkiewicz [1], G.K.Świdarska, B.Bek-Gaik [12], B.Bek-Gaik [2] i inni.

W celu zapewnienia uniwersalności publikowanych raportów zintegrowanych International Integrated Reporting Council (IIRC) opracowało wytyczne [10], ujednoliciące proces ich sporządzania i publikowania. Zawarto w nich podstawowe zasady sporządzania raportu (strategiczny nacisk i orientacja na przyszłość, powiązania informacji, relacji z interesariuszami, istotności, zwięzłości, wiarygodności i kompletności oraz spójności i porównywalności) oraz podstawową strukturę raportu (profil organizacji oraz środowiska zewnętrznego, ład korporacyjny, model biznesu, szanse i zagrożenia, strategia i alokacja zasobów, dokonania, podsumowanie wyników, podstawy prezentacji i przygotowania raportu).

3 Zastosowanie języka XBRL w sprawozdawczości przedsiębiorstwa

Język XBRL (ang. Extensible Business Reporting Language, rozszerzalny język sprawozdawczości biznesowej)¹ jest ogólnodostępnym standardem międzynarodowym przeznaczonym do cyfrowego sporządzania sprawozdań biznesowych wykorzystywanych przez organizacje pochodzące z ponad 50 państw. Umożliwia on sporządzanie nowoczesnych raportów biznesowych w wersji cyfrowej, zapewniającej większą użyteczność, efektywność i dokładność niż tradycyjne raporty papierowe [7].

Standard umożliwia raportowanie zarówno informacji finansowych, jak i informacji na temat sytuacji przedsiębiorstwa, ryzyka oraz zgodności z przepisami.

Podstawową funkcją XBRL jest sporządzanie sprawozdań finansowych z wykorzystaniem gotowych szablonów. Należy, jednakże zaznaczyć, iż każdy szablon może być dostosowywany do potrzeb organizacji [7].

Standard XBRL oparty jest obecnie o specyfikację XBRL 2.1 określającą podstawowe bloki faktów, przykładowych dokumentów i, pojęć oraz taksonomii. Poszczególne pojęcia zostały omówione w tabeli 1.

Podstawowym elementem standardu XBRL stanowią taksonomie zawierające definicje kategorii ekonomicznych oraz pozycji sprawozdania. Poszczególne pozycje powinny być szczegółowo opisane poprzez wskazanie ich typu, wymiaru czasowego oraz charakteru [11].

Do najczęściej wykorzystywanych na świecie taksonomii zalicza się m.in. IFRS, US GAAP, COREP oraz FINREP [11].

Najważniejszą zaletą standardu XBRL jest automatyzacja procesów raportowania umożliwiająca proste analizowanie i przetwarzanie danych [11].

Standard XBRL umożliwia sporządzanie sprawozdania biznesowego w nowoczesnej cyfrowej wersji. Nie wyklucza to jednak możliwości sporządzenia sprawozdania w najczęściej używanych formatach takich jak PDF, XLS lub HTML, a nawet wydruk w formie papierowej.

¹ Język XBRL został opracowany przez konsorcjum non profit - XBRL International. Więcej: [7]

Tabela 1. Podstawowe pojęcia związane ze standardem XBRL 2.1. Źródło: opracowanie własne na podstawie [7]

Pojęcie	Omówienie	Przykład
Przykładowy dokument	Określa zbiór faktów, które łącznie składają się na raport biznesowy.	Spółka X osiągnęła zysk w wysokości 2 mln złotych. Spółka osiągnęła przychody ze sprzedaży w wysokości 30 mln złotych.
Fakt	Jest to pojedynczy fragment informacji.	Spółka X osiągnęła zysk w wysokości 2 mln złotych.
Pojęcie	Jest definicją nadającą znaczenie faktom.	Zysk, przychody.
Taksonomia	Jest to zbiór definicji związanych z pojęciem.	Stanowi definicje zysku, przychodu.

W Polsce standard XBRL rozpowszechniony jest głównie w sprawozdawczości bankowej, dzięki wprowadzonemu w 2007 roku przez Narodowy Bank Polski Systemie Informacji Sprawozdawczej (SIS) [13].

W literaturze przedmiotu do najważniejszych korzyści z wynikających z wykorzystania standardu XBRL zalicza się: usprawnienie przepływu informacji, wzrost jakości przesyłanych informacji, wzrost efektywności kontroli, redukcję obciążeń administracyjnych, porównywalność, wzrost możliwości analitycznych [11].

Standard XBRL ma również olbrzymie znaczenie ze względu na komunikację z interesariuszami. Automatyzacja procesów sprawozdawczych umożliwia minimalizację kosztów pozyskiwania informacji. Cyfryzacja sprawozdań przynosi wiele korzyści. W szczególności istotna jest możliwość uzyskiwania danych w każdym miejscu i czasie. Elektroniczny dostęp do sprawozdań pozwala również na łatwiejszy dostęp dla szerokiego grona interesariuszy. Standard XBRL zapewnia interesariuszom ciągłość danych, a ich ujednoczenie daje możliwość szybkiego ich przetwarzania [11]. Wprowadzenie jednolitego standardu raportowania pozwala również na wzrost porównywalności danych zarówno w czasie, jak i względem podmiotów zewnętrznych.

4 Możliwość aplikacji języka XBRL w sprawozdawczości zintegrowanej

Stosowanie standardu XBRL w sprawozdawczości organizacji przynosi bardzo wiele korzyści. Jednakże obecnie nie są w pełni wykorzystywane jego możliwości, gdyż służy głównie sporządzaniu sprawozdań finansowych, czyli sprawozdań wyłącznie o charakterze finansowym. Należy zaznaczyć, iż możliwości stosowania standardu nie ograniczają się wyłącznie do tego typu raportów. Nic nie stoi na przeszkodzie, aby wykorzystać XBRL w nowoczesnej formie raportowania jaką jest sprawozdawczość zintegrowana. W tym celu należałoby opracować odpowiednią taksonomię określającą definicje poszczególnych pozycji sprawozdania zintegrowanego. Niewątpliwie pomocne w jej sporządzaniu byłoby wykorzystanie istniejących już wytycznych opracowanych przez IIRC, które wyraźnie określają poszczególne elementy raportu zinte-

growanego tj. profil organizacji oraz środowiska zewnętrznego, ład korporacyjny, model biznesu, szanse i zagrożenia, strategia i alokacja zasobów, dokonania, podsumowanie wyników, podstawy prezentacji i przygotowania raportu. Wskazane wytyczne obejmują jedynie podstawowe informacje na temat zawartości informacyjnej raportu, w związku z czym należałoby dookreślić definicje niektórych pozycji. W tym celu przydatne mogą być również inne dokumenty opracowane na potrzeby sprawozdawczości zintegrowanej takie jak *Capitals, Background paper for <IR>* [9] (omawiający szczegółowo tematykę kapitałów występujących w przedsiębiorstwie - finansowego, produkcyjnego, ludzkiego, intelektualnego, naturalnego oraz społecznego i relacyjnego) oraz *Business Model Background paper for <IR>* [8] (określający sposób przedstawiania modelu biznesowego organizacji) i inne. Możliwe do wykorzystania są również wytyczne raportowania zrównoważonego rozwoju opracowane przez Global Reporting Initiative¹ w standardzie GRI G4², który dość dokładnie określa kwestie zrównoważonego rozwoju z podziałem na aspekty ekonomiczny, społeczny i środowiskowy.

Reasumując, należy wskazać, iż w świecie w coraz większym stopniu zdominowanym przez nowoczesne technologie, w szczególności w zakresie komunikowania się na odległość, wprowadzenie standardu XBRL do sprawozdawczości zintegrowanej wydaje się konieczne, a jego wykorzystanie w praktyce stanowi jedynie kwestię czasu.

5 Podsumowanie

Współcześnie sprawozdawczość organizacji staje przed wieloma nowymi wyzwaniami. Interesariusze coraz częściej domaga się informacji na temat działalności organizacji. Tradycyjna sprawozdawczość obejmująca jedynie informacje finansowe nie potrafi sprostać oczekiwaniom interesariuszy. Kluczowe staje się ujawnianie informacji pozafinansowych dotyczących wpływu organizacji na społeczeństwo i środowisko, warunków pracy, ładu korporacyjnego oraz modelu biznesu. Doskonałym rozwiązaniem umożliwiającym zaspokojenie tych potrzeb jest sprawozdanie zintegrowane. Stanowi ono nowoczesne i uniwersalne narzędzie komunikacji z interesariuszami.

Sprawozdawczość zintegrowana jest koncepcją stosunkowo nową, wytyczne IIRC zostały opublikowane w grudniu 2013 roku, jednakże z roku na rok wzrasta zainteresowanie nią wśród przedsiębiorców. Należy jednakże zaznaczyć, iż sprawozdawczość zintegrowana znajduje się dopiero w początkowej fazie rozwoju. Zdaniem autorów wykorzystanie standardu XBRL mogłoby przynieść wiele korzyści dla dalszej ewolucji sprawozdawczości. Jednakże w celu umożliwienia sporządzania sprawozdań zintegrowanych z wykorzystaniem nowoczesnego standardu XBRL należałoby opracować odpowiednią taksonomię definiującą pojęcia poszczególnych pozycji raportu.

¹ Global Reporting Initiative jest międzynarodową organizacją non profit mającą na celu pomoc biznesowi, organom państwa oraz innym organizacjom w zrozumieniu i komunikowaniu informacji na temat wpływu biznesu na kluczowe problemy zrównoważonego rozwoju tj. zmiany klimatu, prawa człowieka, korupcja itp. Więcej: [6]

² Przewodnik na temat zasad raportowania i standardów ujawnień: G4 Sustainability Reporting Guidelines. Reporting Principles and Standard Disclosures [5]

Zdaniem autorów w tym celu można wykorzystać istniejące już wytyczne IIRC oraz inne dokumenty określone przez tą organizację, a także wytyczne dotyczące raportowania kwestii zrównoważonego rozwoju GRI G4.

Reasumując, wykorzystanie standardu XBRL w opracowywaniu i publikacji sprawozdań zintegrowanych wydaje się kwestią czasu. W szybko zmieniającym się świecie wykorzystanie nowoczesnych technologii informatycznych staje się niezbędne.

Literatura (References)

1. Bek-Gaik B., Rymkiewicz B.: Tendencje rozwoju sprawozdawczości zintegrowanej w praktyce polskich spółek giełdowych. Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse. Rynki Finansowe. Ubezpieczenia. nr 1 (79). 2016. s. 767-783;
2. Bek-Gaik B.: Sprawozdawczość zintegrowana - wybrane problemy. Zeszyty naukowe Uniwersytetu Szczecińskiego nr 873. Finanse. Rynki Finansowe. Ubezpieczenia. nr 77. 2015. s. 479-491
3. Churet C., Eccles R.G.: Integrated reporting. quality of management and financial performance. „Journal of Applied Corporate Finance”. vol. 26. no. 1. 2014. s. 56–64.
4. Eccles R.G., Krzus M.P., Ribot S.: The Integrated Reporting Movement: Meaning, Momentum, Motives, and Materiality. Wiley & Sons, New Jersey. 2015
5. GRI: G4 Sustainability Reporting Guidelines. Reporting Principles and Standard Disclosures. 2013. <https://www.globalreporting.org/resource/library/GRIG4-Part1-Reporting-Principles-and-Standard-Disclosures.pdf> (19.03.2017)
6. <https://www.globalreporting.org> (19.03.2017)
7. <https://www.xbrl.org> (17.03.2017)
8. IIRC: Business Model Background paper for <IR>. 2013. http://integratedreporting.org/wp-content/uploads/2013/03/Business_Model.pdf (19.03.2017)
9. IIRC: Capitals Background paper for <IR>. 2013. <http://integratedreporting.org/wp-content/uploads/2013/03/IR-Background-Paper-Capitals.pdf> (19.03.2017)
10. IIRC: The International <IR> Framework. 2013. <http://integratedreporting.org/wp-content/uploads/2013/12/13-12-08-THE-INTERNATIONAL-IR-FRAMEWORK-2-1.pdf>. 05.03.2017
11. Klimczak K.: Standard XBRL jako koncepcja wspomagająca raportowanie finansowe. Studia Prawno-Ekonomiczne. tom XCI/2. 2014. s. 175-192
12. Świdarska G.K., Bek-Gaik B.: Dokąd zmierza raportowanie biznesowe?. Studia Ekonomiczne : Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach. no 274. 2016. no 5. s. 7–15.
13. Walaszek A.: XBRL - standard lepszej sprawozdawczości finansowej. http://www.xbrl-pl.org/files/agata.milo/Standard_XBRL.pdf (17.03.2017)
14. Walińska E., Bek-Gaik B., Gad J., Rymkiewicz B.: Sprawozdawczość przedsiębiorstwa jako narzędzie komunikacji z otoczeniem: wymiar finansowy i niefinansowy. Wydawnictwo Uniwersytetu Łódzkiego. 2015. s. 111
15. Walińska E.: Zintegrowany raport - początek końca sprawozdania finansowego?. "Zeszyty Teoretyczne Rachunkowości". tom 82 (138). 2015. s. 151-165

Method For Determining the Structural Survivability of Intelligent Superstructure with Decentralized Control Principle

Liliya Zimenko (ORCID 0000-002-1866-8370)

Odessa National Academy of Food Technologies, Odessa, Ukraine
zimenko.liliya@gmail.com

Abstract. This work is devoted to developing the method for determining structural survivability of intelligent superstructure (IS) with decentralized control principle (DCP) in providing intelligent services in Next Generation Network. To evaluate structural survivability here is proposed a middle-weighted value of the upper and lower limits of the structural survivability.

Keywords: Structural survivability, intelligent superstructure, the upper limit of survivability, the lower limit of survivability, decentralized control principle.

1 Introduction

Providing intelligent services (800 service, service VAS – Value Added Services, services of added value, Freephone – the call paid by those who make a call, Rate Service – calls with added payment, checking outcoming calls, etc.) is actual. To control intelligent services (IS) are used intelligent superstructures (IS) with centralized control principle. But this architecture has some significant drawbacks, so there should be used decentralized control principle. Due to the necessity to ensure continuous processing of IS applications in various conditions including the cases of adverse effects (AE) at IS with DCP, definition and ensuring the structural survivability of such system is an important task.

2 Definition and ensuring structural survivability of intelligent superstructure

According to [1] the survivability of the system – is the system's ability to save and restore its basic functions at a set volume and during a set time in case of changes in the structure of the system and / or algorithms and conditions of its operation because of external adverse.

The intelligent superstructure – is the device that controls the intelligent services – are additional services of telecommunications network, while providing them there happens change of the service call process.

In DCP for serving the applications of IS can be used universal servers for servicing all kinds of applications, and specialized servers – for servicing a certain class of applications.

General view of DCP, in which specialized servers are used, each of which serves a certain class of applications for IS is shown in fig. 1 [4]:

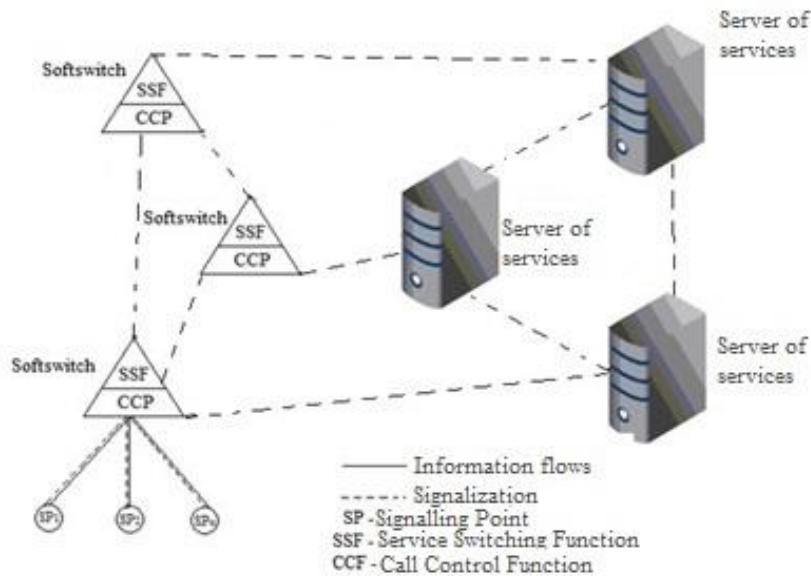


Fig. 1. Intelligent superstructure with Decentralized Control Principle

When servicing the application of IS, the application from the Softswitch comes to servicing server which directly connected with it. If the server is free and serves this class of applications, it serves the application. If the server does not serve this class of IS applications, then the application is sent to the Softswitch, which is connected with server.

Fig. 1 shows the Softswitches, which are interconnected. At one level between Softswitches are equal links while when they are used there can be formed set of routes of service of applications for IS $M_{st} = \{m_{st}^k\}$ where $k = \overline{1, K}$, K – a number of several routes between points s (users) and t (servers of services).

The presented in this work method of providing structural survivability of IS with DCP realizes a current approach with usage of the proposed indicator of structural survivability, which is determined on the basis of the upper and lower limits of structural survivability, the achievement of which is provided by the introduction of structural redundancy.

The indicator of structural survivability of IS (P_{IS}) is defined as the average weighted of the upper and lower limits of structural survivability. The upper limit of a structural survivability is based on the use of set of routes to service IS applications – P_{ULSS} . While calculating P_{ULSS} the routes are considered to be independent and form a parallel structure. The lower limit of a structural survivability is determined on the basis of a set of sections which are formed for determining set of routes – P_{LLSS} . While calculating P_{LLSS} all the sections form a consequent structure. Indicator of P_{IS} is calculated according to the formula (1):

$$P_{IS} = \frac{P_{ULSS}w_{ULSS} + P_{LLSS}w_{LLSS}}{w_{ULSS} + w_{LLSS}}, \quad (1)$$

where w_{ULSS} and w_{LLSS} – are significant coefficients which determine the importance for calculation of P_{IS} indicators P_{ULSS} and P_{LLSS} , respectively.

The method of determination of P_{IS} consists of the following parts:

1. Let's determine the upper limit of a structural survivability in the case of intact at least of one k -th path m_{st}^k from set of routes M_{st} for servicing IS applications (2):

$$P_{ULSS} = 1 - \prod_{m_{st}^k \in M_{st}} \tilde{O} (1 - \prod_{b_{xy} \in m_{st}^k} \tilde{O} p_{xy}), \quad (2)$$

where b_{xy} – is section of the route m_{st}^k , $k = \overline{1, K}$, K – is the number of set of routs; p_{xy} –probability of intact the section b_{xy} , which belongs to the rout m_{st}^k at adverse effect.

2. Let's determine the lower limit of a structural survivability (3) as the probability of intact of set of cuts d_{st}^l which divide a set of routs M_{st} of servicing application on IS:

$$P_{LLSS} = \prod_{d_{st}^l \in M_{st}} \tilde{O} (1 - \prod_{b_{xy} \in d_{st}^l} \tilde{O} (1 - p_{xy})), \quad (3)$$

where b_{xy} – the section of the cut d_{st}^l ($l = \overline{1, L}$, L – is number of cuts which divide a set of routes M_{st}).

Next, a method of ensuring the structural survivability is as follows:

I. The indicator of structural survivability (formula 1) we compare with the required indicator P_{REQ} :

$$P_{IS} \geq P_{REQ}, \quad (4)$$

P_{REQ} – is the required indicator of structural survivability of IS.

If the condition (4) is completed, it means that the required indicator of structural survivability have been reached, the system IS services satisfies the requirement for structural survivability. If condition (4) is not done there is a removal to the procedures of ensuring the necessary indicator of structural survivability.

II. The task of ensuring structural survivability of IS is formulated as a linear programming problem, when having solved it the optimal structure reserved route sections (cuts) is formed: to minimize the objective function (5) in the performance of limits (4):

$$C_{SYS} = \sum_{i=1}^n c_i m_i \rightarrow \min, \quad (5)$$

where C_{SYS} – is the cost of the system of reserve sections;

i – is the number of the section in the system;

n – is the number of sections in the system;

c_i – is the cost of i -th reserved section of the system;

m_i – is the frequency of reservation of the i -th section of the system.

The solution of the presented optimization problem is as follows.

Find the optimal structure vector of reserve $M(m_1, m_2, \dots, m_n)$ which provides minimum functions (5) under the limit (4).

III. The optimal system that is reserved will be shown as follows. First, we find the one section which provides the most significant growth of structural survivability value in the whole when you add a reserved element to it. The evaluation of the effectiveness of reserve section is performed by using a gradient method based on indicator (6), which is calculated for each i -th section when the frequency of its reservation is increased on one figure [3]:

$$g(m_i + 1) = \frac{p_i(m_i + 1) - p_i m_i}{c_i \times p_i(m_i)}. \quad (6)$$

where $p_i(m_i + 1)$, $p_i(m_i)$ – is the indicator value of the i -th undestroyed sections when its frequency of reservation $(m_i + 1)$ and m_i respective.

The need for reservation for each section is determined by taking into account its impact on the change of values P_{ULSS} and P_{LLSS} , by using indicators $g_{ULSS}(m_i + 1)$ and $g_{LLSS}(m_i + 1)$ which are calculated according to the formula (7) for set of routs (indicator $g_{ULSS}(m_i + 1)$) and for the sets of sections (indicator $g_{LLSS}(m_i + 1)$). As a result, for each i -th section is formed an average weighted value (7), the maximum meaning of which amongst all derived average weighted values determines the number of the section for increasing it on one figure in the frequency of it reservation at this step:

$$g_{av} = \frac{w_{ULSS} g_{ULSS} + w_{LLSS} g_{LLSS}}{2}, \quad (7)$$

where g_{ULSS} and g_{LLSS} – are for values of the upper and lower limits of structural survivability.

At the second and each next step is searched such section (including the one to which there has just been attached a reserved element), when adding to it another reserved element again gives the greatest relative growth of indicator value of structural survivability of the system in the whole. The process of reservation continues until you reach the condition (4).

Thus, the presented method allows determining and providing structural survivability of IS with DCP.

3 Conclusions

The method for determining structural survivability of intelligent superstructure with decentralized control principle for providing intelligent services on the basis of using the upper and lower limits of structural survivability of IS, has been proposed here and it allows to obtain data about the maximum possible values of the system survivability. Also there has been represented the method of providing structural survivability on the basis of using structural redundancy.

References

1. Dodonov A.G., Lande D.V. The survivability of information systems. - K.: Science Dumka, 2011. – 256 p.
2. Dodonov A.G. To the problem of survivability of corporate information systems / A.G. Dodonov, D.V Flaytman – Kiev, 2004, 130 p.
3. Knyazeva N.O. Theory of the Project of Computer systems and networks. Part 2. Methods of Analysis and Synthesis of Computational Measurements / N.O. Knyazeva. — Odessa: СПД Бровкін О.В., 2012. – 240 p.
4. Shestopalov S.V. Otsnka zagal'nogo hour obdesgovuvannya application for dodatkovu sledu systems management / S.V. Shestopalov. – Problems інформатизації та управління, 3 (27) '2009. – 166 p.

Аналіз Математичних Моделей Технічного Обслуговування Складних Технічних Об'єктів

Геннадій Жиров¹, Євгеній Ленков²

¹Військовий інститут Київського національного університету імені Тараса Шевченка,
Київ, Україна

²Військовий інститут телекомунікацій та інформатизації, Київ, Україна
zhirov93@gmail.com
torwer007@gmail.com

Abstract. В статті проводиться аналіз найбільш розповсюджених математичних моделей технічного обслуговування. Визначення переваг та недоліків відомих моделей необхідно для створення нових моделей технічного обслуговування, які будуть взяті за основу при створенні загальної інформаційної технології ТОiP. Встановлено, що відомі на теперішній час математичні моделі і методики розрахунку оптимальних параметрів процесів ТО мало придатні для застосування до реальних технічних об'єктів. Основний недолік цих моделей полягає в тому, що в них не враховується складна структура об'єкта, або є можливість враховувати тільки деякі найпростіші структури.

Keywords: Технічне обслуговування, Математична модель, Технічний стан.

Складні технічні об'єкти в сучасному суспільстві мають виключно важливе значення. У першу чергу йдеться про різноманітні радіоелектронні комплекси, радіолокаційні станції, автоматизовані системи управління (повітряним рухом, об'єктами енергетики і т.п.). Від рівня безвідмовності таких об'єктів залежить обороноздатність держави, економічна безпека та життя людей.

Складні технічні об'єкти відносяться до класу відновлюваних об'єктів тривалого багаторазового застосування. Вони, як правило, є дорогими і вимагають значних витрат на їх експлуатацію. Для забезпечення необхідного рівня безвідмовності в процесі їх експлуатації зазвичай проводиться технічне обслуговування (ТО).

Характерною особливістю складних технічних об'єктів є наявність в їх складі великої кількості різноманітних комплектуючих елементів, які мають різний рівень надійності, різні закономірності процесів їх зносу, старіння та деградації. Ця особливість вимагає більш тонкого підходу до організації і планування ТО в процесі їх експлуатації.

Проблема полягає в тому, що при розробці таких об'єктів всі питання, що пов'язані з ремонтпридатністю і технічним обслуговуванням повинні вирішуватися вже на ранніх етапах проектування об'єкта. Якщо не передбачити

заздалегідь необхідні апаратні і програмні засоби вбудованого контролю технічного стану (ТС) об'єкта, або не створити автоматичну (автоматизовану) систему технічного діагностування, не розробити і не "вбудувати" в об'єкт технологію проведення ТО, то реалізувати в майбутньому можливий вигреш в безвідмовності об'єкта за рахунок проведення ТО у повній мірі не вдасться. Оскільки всі ці питання повинні вирішуватися на етапі створення об'єкта, то виникають задачі щодо створення математичних моделей процесу ТО, за допомогою яких можна було б прорахувати можливий вигреш в рівні безвідмовності об'єкта за рахунок проведення ТО, оцінити необхідні для цього вартісні витрати. Потім на підставі таких розрахунків, необхідно прийняти рішення щодо проведення ТО для даного типу об'єктів і, якщо таке рішення прийнято, розробити структуру системи ТО, вибрати найбільш прийнятну стратегію ТО, визначити її оптимальні параметри.

У доповіді проводиться аналіз математичних моделей технічного обслуговування, які найбільш часто цитуються у науковій літературі. Визначення переваг та недоліків відомих моделей необхідно для створення нових моделей ТО, які будуть взяті за основу при створенні загальної інформаційної технології ТОiP.

На жаль, відомі в даний час математичні моделі і методики розрахунку оптимальних параметрів процесів ТО мало придатні для застосування до реальних технічних об'єктів. Основний недолік цих моделей полягає в тому, що в них або взагалі не враховується складна структура об'єкта, або є можливість враховувати тільки деякі найпростіші структури.

Наведені твердження цілком обґрунтовують висновок про необхідність визначення основних характеристик системи ТО на ранніх стадіях його проектування, коли ще є можливість внесення змін в конструкцію об'єкта.

Визначення та оптимізація параметрів системи ТО можливі тільки на основі застосування математичних моделей процесів ТО. Такі моделі повинні застосовуватися в процесі проектування на всіх етапах по мірі уточнення складу, структури і конструкції об'єкта. Відомі аналітичні моделі ТО, на жаль, мало придатні для застосування до реальних складних технічних об'єктів. Одним з виходів є розробка моделі ТО на основі методу імітаційного статистичного моделювання.

Література (References)

1. Барзилович Е.Ю. Модели технического обслуживания сложных систем. – М.: Высш. школа, 1982. – 231 с.
2. Каштанов В.А. Оптимальные задачи технического обслуживания. – М.: Знание, 1981.
3. Barlow R.E., Yfntel L.G. Mathematical models for system reliability. Part 1. – Sylvan: Technol., 1980/ – 217 p.
4. Модели технического обслуживания систем с избыточностью / Б.П. Креденцер.С.В., Ленков, М.И.Резников, В.В. Зубарев. – К.:Феникс, 2002. – 192 с.

Особливості Економіко-Математичного Моделювання Промислового Підприємства

Анна Лінник¹, Юлія Синиціна²

¹студентка, Національна металургійна академія України, Дніпро, Україна

²доцент, Національна металургійна академія України, Дніпро, Україна

ysynytsina@mail.ru

oksana22oksana@gmail.com

Abstract. У роботі розглянуті особливості застосування економіко-математичного моделювання в управлінні промисловим підприємством. Визначені правила розробки економіко-математичної моделі в умовах промислового підприємства. Запропоновано використання процесного, системного, ситуаційного, цільового, синергетичного та кумулятивного підходів комплексно.

Keywords: промислове підприємство, економіко-математичне моделювання, функціональна система, процес управління. Система обмежень

Динаміка ринку промислової продукції України, а також показників господарської діяльності промислових підприємств свідчить про наявність негативних тенденцій. Сировинна спрямованість структури виробництва, розрахована переважно на потреби експорту, зробила промисловість і економіку України в цілому залежними від кон'юнктури зовнішніх ринків, стримуючи при цьому розвиток внутрішнього ринку.

Особливостям управління промисловим підприємством присвятили свої дослідження О.І. Амоша, І.В. Алексеев, Я.Г. Берсуцький, А.Я. Берсуцький, І.П. Булеев, В.П. Вишневський, А.Е. Воронкова, В.М. Забродський, М.І. Иванов, М.О. Кизим, М.М. Лепа, Р.М. Лепа, О.І. Пушкар, О.В. Раєвнева, О.М. Тридід, Ю.І. Яковець.

Відаючи належне науковому та практичному значенню праць названих авторів, необхідно підкреслити, що певне коло завдань залишилось недостатньо розвинутим. Так, потребують подальшого дослідження методологія управління розвитком підприємства, що повинна передбачати особливості діяльності суб'єктів господарювання в умовах кризи, врахування нестабільності зовнішнього середовища, зміна парадигми розвитку промислових підприємств відповідно до світових процесів.

Метою досліджень є застосування оптимізаційного економіко-математичного моделювання для підвищення ефективності роботи промислового підприємства шляхом управління прибутком та витратами операційної діяльності.

Об'єктом дослідження є процеси управління розвитком промислового підприємства.

Предметом дослідження є теоретичні, методологічні та методичні засади побудови механізму управління розвитком підприємства на основі методів економіко-математичного моделювання.

Для досягнення означеної мети використано систему оптимізаційних економіко-математичних моделей – для визначення реальних можливостей підприємства з урахуванням тенденцій їх розвитку.

С.Л. Чернишов під економічною системою розуміє будь-яку систему, в якій діють натуральні товарні змінні [1]. На думку Л. фон Бертоланфі, система – це комплекс елементів, що перебувають у взаємодії [3], за А. Холлом, система є множиною об'єктів разом з відносинами між об'єктами і між їх атрибутами [3].

Найближчим до економічних систем є визначення К. Уотта, який вважає, що система – це взаємодіючий інформаційний механізм економічної діяльності підприємства, що характеризується багатьма причинно-наслідковими взаємодіями [4]. Система управління підприємством являє собою комплекс цілей, задач і основних напрямків діяльності, а також різних видів, методів і відповідного механізму управління, спрямованих на підвищення продуктивності праці і якості роботи.

Цілями функціонування системи управління підприємства є: підвищення конкурентоспроможності підприємства; підвищення ефективності діяльності підприємства, зокрема, досягнення максимального прибутку.

Параметри c_k ($k = 1, 2, \dots, l$) є кількісними характеристиками системи. Наприклад, якщо йдеться про таку економічну систему, як промислове металургійне підприємство, то його параметрами є наявні ресурси (сировина, робоча сила, промислова техніка та складські приміщення), рівень сировини, продуктивності обладнання, норми витрат ресурсів, ціни та собівартість проміжної і кінцевої продукції, норми податків, проценти за кредит, ціни на куповані ресурси тощо.

Частина параметрів c_k для певної системи може бути сталими величинами, наприклад, норми витрат сировини відносно продукції, норми споживання сировини тощо, а частина – змінними, тобто залежатиме від певних умов, як, скажімо, якість сировини, собівартість продукції, реалізаційні ціни на металургійну продукцію.

Розрізняють наступні змінні величини: незалежними чи залежними, дискретними чи неперервними, детермінованими або випадковими. Наприклад, залежною змінною є собівартість продукції, незалежною від процесу функціонування підприємства величиною є початковий розмір статутного фонду, дискретною – кількість обладнання, неперервною – об'єм випуску чавуну або сталі, детермінованою – норма витрат сировини на одиницю продукції, випадковою – кількість ремонтів, які народяться у плановому періоді.

Вхідні змінні економічної системи поділяються на два види: керовані x_j ($j=1,2,\dots,n$), значення яких можна змінювати в деякому інтервалі; і некеровані змінні y_i ($i=1,2, \dots, m$), значення яких не залежать від волі людей і визначаються зовнішнім середовищем. Наприклад, обсяг придбаного пального – керована, а

температура повітря – некерована змінна. Залежно від реальної ситуації керовані змінні можуть переходити у групу некерованих і навпаки. Наприклад, у разі насиченого ринку обсяги придбання дизельного палива є керованою змінною величиною, а за умов дефіциту цього ресурсу – некерованою.

У загальному вигляді задача економіко-математичного моделювання формулюється наступно: знайти такі значення керованих змінних x_j , щоб цільова функція набувала екстремального (максимального чи мінімального значення).

Отже, потрібно відшукати значення

$$\max_{x_j} (\min) F^* = f(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_m; c_1, c_2, \dots, c_l). \quad (1)$$

Можливості вибору x_j завжди обмежені зовнішніми щодо системи умовами, параметрами виробничо-економічної системи тощо.

Наприклад, об'єм випуску чавуну або сталі обмежена наявністю сировини та інших ресурсів, можливістю реалізації продукції, необхідністю виконання договірних зобов'язань тощо. Ці процеси можна описати системою математичних рівностей та нерівностей виду:

$$q_i(x_1, x_2, \dots, x_n; y_1, y_2, \dots, y_m; c_1, c_2, \dots, c_l) \{ \leq, =, \geq \} 0; \quad (2)$$

$$(i = 1, 2, \dots, S).$$

Набір символів ($\leq, =, \geq$) означає, що для деяких значень поточного індексу i виконуються нерівності типу \leq , для інших – рівності ($=$), а для решти – нерівності типу \geq .

Система (3) називається системою обмежень, або системою умов задачі. Вона описує внутрішні технологічні та економічні процеси функціонування й розвитку виробничо-економічної системи, а також процеси зовнішнього середовища, які впливають на результат діяльності системи. Для економічних систем змінні x_j мають бути невід'ємними:

$$x_j \geq 0 \quad (j = 1, 2, \dots, n). \quad (3)$$

Залежності (1) – (3) утворюють економіко-математичну модель економічної системи. Розробляючи модель, слід дотримуватись певних правил:

1. Модель має адекватно описувати реальні технологічні та економічні процеси.
2. У моделі потрібно враховувати все істотне, суттєве в досліджуваному явищі чи процесі, нехтуючи всім другорядним, неістотним у ньому. Математичне моделювання — це мистецтво, вузька стежка між переспрошенням та переускладненням. Справді, прості моделі не забезпечують відповідної точності, і «оптимальні» розв'язання за такими моделями, як правило, не відповідають реальним ситуаціям, дезорієнтують користувача, а переускладнені моделі важко реалізувати на ЕОМ як з огляду на

неможливість їх інформаційного забезпечення, так і через відсутність відповідних методів оптимізації.

3. Модель має бути зрозумілою для користувача, зручною для реалізації на ЕОМ.
4. Необхідно, щоб множина змінних x_j була не порожньою. З цією метою в економіко-математичних моделях за змоги слід уникати обмежень типу «=», а також суперечливих обмежень. Наприклад, ставиться обмеження щодо виконання контрактів, але ресурсів недостатньо, аби їх виконати. Якщо система (1), (2) має єдине розв'язання, то не існує набору різних планів, а отже, й задачі вибору оптимального з них.

Будь-який набір змінних x_1, x_2, \dots, x_n , що задовольняє умови (1) і (2), називають допустимим планом, або планом. Очевидно, що кожний допустимий план є відповідною стратегією економічної системи, програмою дій. Кожному допустимому плану відповідає певне значення цільової функції, яке обчислюється за формулою (1).

Сукупність усіх розв'язань системи обмежень (2) і (3), тобто множина всіх допустимих планів утворює область існування планів.

План, за якого цільова функція набуває екстремального значення, називається оптимальним. Оптимальний план є розв'язанням задачі економіко-математичного моделювання (1) – (2).

Складність економічних систем (явищ, процесів) як об'єктів досліджень вимагає їх ретельного вивчення з метою з'ясування найважливіших функціональних залежностей, внутрішніх взаємозв'язків між їх елементами. В результаті здійснюються можливі спрощення та допущення, що, вочевидь, погіршує адекватність побудованих математичних моделей і є чудовим приводом для критики. Однак лише прийняття певних допущень уможливорює формалізацію будь-якої економічної ситуації.

Не існує загальних рекомендацій щодо процесу моделювання, тому в кожному конкретному разі вимоги до побудови математичної моделі залежать від цілей та умов досліджуваної системи.

У процесі застосування математичного моделювання в економіці чітка постановка задачі та її формалізація є найскладнішим етапом дослідження, вимагає ґрунтовних знань передусім економічної суті процесів, які моделюються. Однак, вдало створена математична модель може надалі застосовуватись для розв'язування інших задач, які не мають відношення до ситуації, що початково моделювалася.

Література (References)

1. Чернышев С.Л. Моделирование экономических систем и прогнозирование их развития / С.Л. Чернышев. – М.: МГТУ им. Баумана, 2003. – 231 с.
2. Bertalanfy L. von. General system theory. Foundations, development applications. – N.Y.: Braziller, 1969. – 483 p.
3. Hall A.D. A methodology for systems engineering / A.D. Hall. –Princeton. 1962. – 346 p.

4. Systems analysis in ecology / Ed.By Kenneth E.F., Watt. – N.Y, London: Accad. Press, 1996. – 710 p.

СЕКЦІЯ 4

Ігрове програмне забезпечення

Game Development

Розробка Комп'ютерної гри на Прикладі Створення Scratch-проекту

Людмила Рішко

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
liudmyla_rishko@comp-sc.if.ua

Abstract. Розглянуто особливості процесу створення комп'ютерних ігор. Запропоновано вивчення розробки ігрового програмного забезпечення на прикладі створення ігрових проектів у середовищі візуального програмування Scratch.

Keywords: комп'ютерна гра, розробка програмного забезпечення, Scratch-проект

1 Вступ

Ігрова індустрія розвивається надзвичайно швидкими темпами і розглядається як одна із найбільш перспективних галузей для працевлаштування. Процес розробки ігрового програмного забезпечення (ІПЗ) має свої особливості та вимагає співпраці фахівців з різних галузей - письменники, дизайнери, художники, програмісти, композитори, економісти і т.д. Індустрія створення комп'ютерних ігор вимагає від розробників, зокрема, широкого спектру ІТ-компетенцій, пов'язаних з цілим рядом напрямків розвитку комп'ютерних наук та інформаційних технологій: машинна графіка, людино-машинна взаємодія, безпека, дизайн, програмування, моделювання і т.п. [1]. Тому питання вивчення процесу розробки комп'ютерних ігор та можливості підготовки фахівців в даній галузі є актуальним. В даній статті розкрито можливості середовища візуального програмування Scratch для вивчення основних етапів процесу розробки комп'ютерної гри, що обґрунтовує доцільність використання Scratch як початкової ланки у вивченні процесу розробки ІПЗ.

2 Можливості Scratch для реалізації комп'ютерних ігор

Візуальна мова програмування Scratch, хоча розглядається як мова програмування для дітей та підлітків, має широкі можливості для реалізації прототипів повноцінних ігрових програм [2]. Scratch дає можливість легко поєднувати графіку, зображення, звук, а саме такі елементи поєднує в собі будь-

яка комп'ютерна гра [3]. Процес розробки ігрового проекту в середовищі Scratch включає найважливіші характерні етапи створення комп'ютерної гри: від ідеї та пошуку жанру до публікації та документування. Наведемо лише кілька аналогій: вмонтований графічний редактор дає можливість розробляти графічні образи героїв та створювати дизайн сцен; в свою чергу, розробка образів спрайтів ознайомлює із основами класичної анімації; послідовне виконання скриптів, організоване на основі передачі повідомлень, дає поняття про механізми передачі параметрів; паралельне виконання скриптів дає уявлення про паралельні процеси; можливість використання датчиків підводить до розуміння інтерактивності; можливість прив'язки змінних та скриптів до спрайтів – до поняття об'єктно-орієнтованого програмування. Авторами було розроблено ігровий проект Earth for Peace та реалізовано за допомогою Scratch. Основна ідея проекту - демонстрація можливості використання в мирних цілях так званого «бойового жанру». На початку гри гравець отримує повідомлення з проханням про захист від ворожої армії та про допомогу у відновленні миру. Головним героєм є голубка, яка тримає в дзьобі гілку миру. Метою гри є перетворення за допомогою гілки миру усіх об'єктів воєнного характеру на мирні. Людмила Рішко представила даний Scratch-проект на Європейських змаганнях «eSkills for Jobs 2016 competition» і стала призером в номінації «Young digital talent» (http://eskills4jobs.ec.europa.eu/2016_winners).

3 Висновки

Візуальна мова програмування Scratch має всі можливості для розробки ІПЗ. Простий і доступний інструментарій роботи в середовищі Scratch робить процес створення ігрового проекту цікавим та зрозумілим і водночас дає можливість в повній мірі відчувати особливості технологій розробки комп'ютерних ігор. На нашу думку, Scratch можна розглядати як першу ланку в підготовці майбутніх фахівців ігрової індустрії. Планується подальше вдосконалення розробленого ІПЗ та реалізація його ідеї на платформі Cocos3dx в рамках проекту «GameHub, University-enterprises cooperation in game industry in Ukraine», який реалізується в ДВНЗ «Прикарпатський національний університет імені Василя Стефаника».

Література (References)

1. Alf Inge Wang, Bian Wu. The Use of Game Development In Computer Science and Software Engeneering Education. <https://goo.gl/GZ40xJ>
2. Scratch: Programming for All. <https://goo.gl/kJ0uJ>
3. Shall We Learn. Scratch Programming by Jessica Chiang. <https://goo.gl/7ySB9M>

Алгоритмізація Пошуку Розв'язку ри Судоку

Стефанія Таран

Прикарпатський національний університет імені Василя Стефаника,
Івано-Франківськ, Україна
stefania.taran@pnu.edu.ua

Abstract. У роботі проаналізовано алгоритми розв'язку пазлів Судоку. Розглянуто алгоритми з поверненням, алгоритми, побудовані на правилах та алгоритми, побудовані на основі машини Больцмана. Автором реалізовано програмну імплементацію Судоку з використанням ігрового рушія Unity 3D.

Keywords: Судоку Пошук з поверненням Машина Больцмана
· Алгоритми, побудовані на правилах Unity 3D

1 Вступ

Попередникові гри Судоку – латинському квадратові – більше тисячі років. У свій час Ейлер використовував для своїх задач схожий підхід із латинськими літерами. Автор сучасного варіанту гри – Howard Garns.

Існує значна кількість методів розв'язку гри. Найпростіші варіанти полягають в обході поля гри і заповненні тих клітинок, де напевне можна проставити тільки один символ. Складніші варіанти передбачають висунення припущення і наступне підтвердження або заперечення його.

Метою даної роботи є дослідження алгоритмів розв'язку гри Судоку.

Дослідження виконано у рамках проекту «GameHub, University-enterprises cooperation in game industry in Ukraine» (<http://gamehub-cbhe.eu/gamehub-in-ukraine/gamehub-pnu/>), до складу консорціуму якого входять ряд університетів та провідних компаній Іспанії, Австрії, Польщі та України. Метою проекту є забезпечення зайнятості та самодостатності університетів і випускників коледжів, безробітних інженерів а також ветеранів АТО, пропонуючи їм навички, затребувані у цифровій ігровій індустрії.

2 Аналіз предметної області

Сітка розміром 9x9, комірки котрої заповнені числами, утворює ігрове поле. Поле поділяють на квадрати розміром 3x3 комірки. Кожен рядок, стовпчик чи квадрат пазла повинен містити цифри від 1 до 9 без повторів. Також повинен існувати унікальний розв'язок пазла.

Залежно від того, скільки клітинок заповнено, розв'язок можна класифікувати як простий чи складний. Зазвичай блоки мають прямокутну форму, проте форма може бути і довільною.

Вірно складена головоломка повинна давати можливість знайти розв'язок, використовуючи логічні побудови.

3 Постановка задачі

Серед алгоритмів розв'язку Судоку можна виділити наступні групи: алгоритми пошуку з поверненням, алгоритми, побудовані на правилах, алгоритми на основі машини Больцмана (стохастичної рекурентної нейронної мережі) [1-3] тощо.

Алгоритми пошуку із поверненням формують кандидата на розв'язок і приймають його або відкидають (повернення), якщо кандидат не може бути ланкою у послідовності до вірного розв'язку. Алгоритми, що базуються на правилах, перевіряють пазл на відповідність наборові правил, зменшуючи набір кандидатів. Машина Больцмана, у свою чергу, використовує алгоритм імітації відпалу, призначений для розв'язку задачі глобальної оптимізації.

У роботі досліджено залежність часу вирішення задачі від використаного алгоритму.

4 Реалізація алгоритмів з використанням Unity 3D

Unity 3D – кросплатформний ігровий рушій, розроблений Unity Technologies [4]. Програмне забезпечення, написане з його використанням, може виконуватися на широкому діапазоні пристроїв: від персональних комп'ютерів до ігрових консолей.

Генерування поля гри, інтерфейс користувача та імплементацію розглянутих алгоритмів виконано за допомогою мови C# та ігрового рушія Unity 3D.

Література (References)

1. Кнут Д. Э. Искусство программирования. Том 1. Основные алгоритмы = The Art of Computer Programming. Volume 1. Fundamental Algorithms / под ред. С. Г. Тригуб (гл. 1), Ю. Г. Гордиенко (гл. 2) и И. В. Красикова (разд. 2.5 и 2.6). — 3. — Москва: Вильямс, 2002. — Т. 1. — 720 с. — ISBN 5-8459-0080-8
2. Ackley, David H.; Hinton, Geoffrey E.; Sejnowski, Terrence J. A Learning Algorithm for Boltzmann Machines. — Cognitive Science 9 (1), 1985. — С. 147–169.
3. Hinton, G. E. (2002). "Training Products of Experts by Minimizing Contrastive Divergence" (PDF). *Neural Computation*. 14 (8): 1771–1800.
4. Greg Lukosek. *Learning C# by Developing Games with Unity 5.x – Second Edition*. — Packt, 2016. — 230 p.
5. Jere Miles. *Unity 3D and PlayMaker Essentials: Game Development from Concept to Publishing (Focal Press Game Design Workshops)*. — A K Peters/CRC Press, 2016. — 506 p.

З М І С Т

<i>Передмова</i>	3
I. Цепенда, Л. Петришин, П. Лебковський	
СЕКЦІЯ 1	5
КОМП'ЮТЕРНІ НАУКИ	
COMPUTER SCIENCE	
<i>Wstęp do kryptografii</i>	6
M. Lewiński	
<i>Analiza bezpieczeństwa routerów</i>	12
W. Reguła	
<i>Watch out! – Mobile Application Threats</i>	25
P. Kuryłowicz	
<i>Firewalls in contemporary networks</i>	28
M. Ogorzałek	
<i>Maglev, czyli najszybsza kolej świata</i>	34
K. Marszałek	
<i>Моделювання процесів надання інтелектуальних сервісів у системі NS-2</i>	38
Б. Пустовий	
<i>Wizualizacja pracy na Tablicy Scrutowej</i>	44
L. Pstrong	
<i>Мікропроцесорна обробка даних сенсора на основі поруватого кремнію</i>	56
Л. Монастирський, Р. Яремик, О. Петришин	
<i>Трійкові симетричні функції та їх застосування для цифрової обробки інформації на основі ортогональних перетворень</i>	60
А. Ізмайлов	
<i>Властивості методів частотного аналізу цифрових сигналів</i>	63
І. Голуб, А. Ізмайлов	
<i>Дослідження методів розв'язку задачі про призначення із обмеженнями з неоднорідними параметрами при складанні розкладу навчального закладу</i>	67
М. Ільчук	
<i>Дослідження методів детектування рис обличчя для автомобільної системи безпеки руху</i>	70
О. Фуфалько	

СЕКЦІЯ 2..... 72

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
INFORMATION TECHNOLOGIES

<i>Programy Bug Bounty jako podejście do zapewniania bezpieczeństwa aplikacji internetowych.....</i>	<i>73</i>
М. Szymański	
<i>Характеристики протоколів маршрутизації з урахуванням якості обслуговування в ad-hoc мережах.....</i>	<i>77</i>
Ю. Казак	
<i>Використання SaaS технологій при проектуванні систем управління навчанням.....</i>	<i>84</i>
О. Дашкевич	
<i>Особливості датчиків для визначення параметрів вібрації.....</i>	<i>88</i>
О. Лещенко, Е. Притуляк, К. Лещенко	
<i>Розробка системи підтримки прийняття рішень при проведенні лікарсько-діагностичних заходів.....</i>	<i>95</i>
Г. Мумладзе, А. Поворознюк	
<i>Проблеми впровадження інформаційних технологій у навчальний процес.....</i>	<i>97</i>
І. Михайлюк	
<i>Розробка алгоритмічного та програмного забезпечення для прогнозування кількості населення на заданій території.....</i>	<i>103</i>
М. Бурак	
<i>Прогнозування відмов відновлюваних об'єктів з ієрархічною конструктивною структурою.....</i>	<i>107</i>
Я. Проценко, Т. Бондаренко	
<i>Хмарні обчислення в мобільному математичному середовищі Sage.....</i>	<i>111</i>
І. Абрамова	
<i>Сервіс для створення інтерактивних завдань LearningApps.....</i>	<i>115</i>
А. Маринець	
<i>Побудова векторно-розгалужуючих діаграм на основі числення Фібоначчі.....</i>	<i>117</i>
М. Петришин	
<i>Порівняння фронтального зображення лиця із двома профілями.....</i>	<i>120</i>
І. Голуб'як	
<i>Технології створення електронних книг.....</i>	<i>126</i>
А. Дранчук	
<i>Спільноти Google як середовище навчально-виховного процесу.....</i>	<i>130</i>
Л. Рішко	
<i>Особливості застосування 3D-моделей в навчальному процесі.....</i>	<i>134</i>
І. Колісник	

<i>Інтернет-технології як засіб організації групових форм роботи</i>	138
I. Мельник	
<i>Virtual library architecture using cloud computing</i>	142
L. Pohreliuk	
<i>Safety of usage typical hash-functions in modern information systems</i>	146
A. Byalyk	
<i>Особливості програмної та апаратної реалізації алгоритму симетричного блокового перетворення ДСТУ 7624:2014 (шифр Калина)</i>	150
B. Петреній	

СЕКЦІЯ 3..... 154

СИСТЕМИ УПРАВЛІННЯ

MANAGEMENT SYSTEMS

<i>Analiza działań logistycznych przedsiębiorstwa handlowego przy przygotowaniach do Światowych Dni Młodzieży 2016 w Krakowie</i>	155
A. Ostrowska	
<i>Projekt linii produkcyjnej gipsu budowlanego</i>	161
A. Frątczak	
<i>Przemysł rybny</i>	165
W. Mikurda	
<i>Lean Management – nowoczesna filozofia zarządzania</i>	168
K. Majka	
<i>Wizja Kolonizacji Marsa – SpaceX</i>	174
M. Gacek	
<i>Pewność siebie w karierze zawodowej i wykorzystywanie wiedzy w praktyce</i>	178
P. Matera	
<i>Arkusz 8D jako narzędzie doskonalenia jakości w przedsiębiorstwie</i>	182
K. Szczepara	
<i>Zmiany w klasyfikacji odporności ogniowej kabli i przewodów</i>	185
M. Muszyńska	
<i>Аналіз точності методів контролю складу бінарної вугільної суміші</i>	189
Г. Матіко, С. Мисак	
<i>Wykorzystanie standardu XBRL w sprawozdawczości zintegrowanej</i>	194
B. Rymkiewicz, I. Matuszyk	
<i>Method for determining the structural survivability</i>	200
L. Zimenko	

<i>Аналіз математичних моделей технічного обслуговування складних технічних об'єктів</i>	<i>205</i>
<i>Г. Жиров, Є. Ленков</i>	
<i>Особливості економіко-математичного моделювання промислового підприємства</i>	<i>207</i>
<i>А. Лінник, Ю. Синиціна</i>	
СЕКЦІЯ 4.....	212
ІГРОВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ	
GAME DEVELOPMENT	
<i>Розробка комп'ютерної гри на прикладі створення Scratch-проекту</i>	<i>213</i>
<i>Л. Рішко</i>	
<i>Алгоритмізація пошуку розв'язку гри Судоку.....</i>	<i>215</i>
<i>С. Таран</i>	
ЗМІСТ.....	218

Наукове електронне видання
комбінованого використання
Можна використовувати в локальному та мережному режимах

**КОМП'ЮТЕРНІ НАУКИ, ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ
ТА СИСТЕМИ УПРАВЛІННЯ**

**Матеріали
міжнародної науково-технічної конференції
студентів, аспірантів та молодих вчених
10–12 квітня 2017 року
Івано-Франківськ, Україна**

Матеріали статей опубліковані в авторській редакції

**COMPUTER SCIENCE, INFORMATION TECHNOLOGIES
AND MANAGEMENT SYSTEMS**

**Proceedings
of the International Scientific Young Scientists Conference
2017, April, 10th to 28th
Ivano-Frankivsk**

Materials are published in author's edition

Технічний редактор магістр А.В. Ізмайлов (ПНУ)

Видавець

Прикарпатський національний університет
імені Василя Стефаника
вул. С. Бандери, 1, м. Івано-Франківськ, 76025,
тел.: 71-56-22

E-mail: vdvcit@pu.if.ua

Свідоцтво суб'єкта видавничої справи
ДК № 2718 від 12. 12. 2006

ISBN 978-966-640-435-3