МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Матеріали XXVIII Міжнародного молодіжного форуму

«Радіоелектроніка та молодь у XXI столітті»

ТОМ 4

«Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій»

Харків 2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЛЕКТРОНІКИ

МАТЕРІАЛИ 28-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

16 – 18 квітня 2024 р.

Том 4

КОНФЕРЕНЦІЯ

«ПЕРСПЕКТИВИ РОЗВИТКУ ІНФОКОМУНІКАЦІЙ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ ТЕХНОЛОГІЙ»

Харків 2024

28-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2024. – 238 с.

У збірнику представлені матеріали доповідей учасників 28-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті».

Для науковців, викладачів, практичних працівників, студентів, а також широкого кола читачів, які цікавляться цією проблематикою.

Відповідальність за зміст поданого матеріалу несе його автор.

61166 Україна, Харків, прос. Науки, 14
тел./факс.: (057) 7021397

E-mail: mref21@nure.ua

ISBN 978-966-659-394-1
DOI 10.30837/IYF.PDICIMT.2024

Програмний комітет конференції

Снігуров А.В.	к.т.н., декан факультету ІК
Захаров І.П.	д.т.н., зав. каф. ІВТ
Безрук В.М.	д.т.н, зав. каф. ІМІ
Лемешко О.В.	д.т.н., зав. каф. ІКІ

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ, МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ

ПРОБЛЕМИ ІНФОКОМУНІКАЦІЙ

УДК 004.8:621.396.6 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.005

СТВОРЕННЯ МОДЕЛІ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ВИЯВЛЕННЯ БПЛА

Білик О.С., Мартинчук О.О.
Науковий керівник - к.т.н., доц. Мартинчук О.О.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
e-mail: oleksandr.bilyk@nure.ua

This presentation outlines the development of an artificial intelligence (AI) model for processing, analyzing, and classifying Unmanned Aerial Vehicles (UAVs) based on signal characteristics. The report details a multi-stage approach, utilizing machine learning techniques. Initial stages involve data collection and preparation, including gathering signal data from various UAV types and preprocessing to enhance data quality.

Створення моделі штучного інтелекту (ШІ) для обробки, аналізу та класифікації безпілотних літальних апаратів (БПЛА) на основі характеристик отриманих сигналів може бути здійснено з використанням кількох етапів з використанням методів машинного навчання. Нижче наведено етапи створення такої моделі.

1. Збір та підготовка даних

- збір даних сигналів з різних типів БПЛА, включаючи частоту, амплітуду, фазу, поляризацію та інші характеристики;
- класифікація зібраних даних за типами БПЛА або за характером використання (наприклад: ударний, розвідувальний ін.);
- попередня обробка: фільтрація, нормалізація та інші методи попередньої обробки для поліпшення якості даних перед подачею їх до моделі ШІ.

2. Вибір моделі машинного навчання

- класифікаційні алгоритми: використання алгоритмів навчання з вчителем, таких як опорні векторні машини (SVM), випадкові ліси (Random Forest), або глибокі нейронні мережі для класифікації сигналів;
- вибір моделі може залежати від кількості та різноманітності даних, а також від потрібної точності та швидкості обробки.

3. Тренування моделі

- розділення даних на тренувальний та тестувальний набори;
- підготовка моделі з використанням тренувального набору даних;
- перевірка та валідація: використання тестового набору для перевірки ефективності моделі.

4. Оцінка та оптимізація

- аналіз точності, повноти, F1-оцінки та інших метрик.
- оптимізація: тонке налаштування параметрів моделі та структури для покращення результатів.

5. Впровадження та використання

Створення програми математичного моделювання в MATLAB для виявлення малопомітних цілей типу БПЛА та придушення каналів керування за допомогою ортогонально-поляризованих шумоподібних радіосигналів вимагає глибоких знань в області радіоелектроніки, сигнальної обробки та програмування MATLAB.

```
% Параметри сигналу
Fs = 1000;          % Частота дискретизації
T = 1/Fs;           % Час дискретизації
L = 1500;           % Довжина сигналу
t = (0:L-1)*T;      % Часовий вектор
% Створення шумоподібного сигналу
S = randn(size(t));
% Моделювання відбитого сигналу від БПЛА
delay = 300;        % Затримка сигналу
alpha = 0.5;        % Коефіцієнт затухання
Reflected = alpha * [zeros(1, delay), S(1:end-delay)];
% Візуалізація сигналів
subplot(2,1,1);
plot(Fs*t(1:100), S(1:100))
title('Оригінальний шумоподібний сигнал')
subplot(2,1,2);
plot(Fs*t(1:100), Reflected(1:100))
title('Відбитий сигнал від БПЛА')
```

Даний код демонструє базове створення шумоподібного сигналу та моделювання його відбиття від БПЛА. Подальший аналіз, такий як ідентифікація характеристик сигналу БПЛА, вимагає більш складних методів, які залежать від конкретного сценарію та доступних даних.

Моделювання взаємодії з малопомітними цілями у радіолокаційній системі, особливо з використанням ортогонально-поляризованих шумоподібних сигналів, можна реалізувати за допомогою простого сценарію в MATLAB.

```
% Визначення параметрів
fc = 2.4e9;          % Центральна частота (Гц)
fs = 10e6;           % Частота дискретизації (Гц)
pulseWidth = 1e-6;   % Тривалість імпульса (с)
prf = 1e3;           % Частота повторення імпульсів (Гц)
targetRange = 500;   % Відстань до малопомітної цілі (м)
targetRCS = 1e-4;    % РКС (радіолокаційний переріз) малопомітної цілі (м^2)
% Створення двохполяризаційної фазованої антенної решітки та сигналу
array = phased.URA('Size', [4, 2], 'ElementSpacing', [0.5, 0.5]);
waveform = phased.RectangularWaveform('PulseWidth', pulseWidth, 'PRF', prf);
% Генерація двохполяризаційного радарного сигналу
returnSignalH = radar(array, waveform, 'Polarization', 'H');
% Моделювання відбиття від малопомітної цілі
targetReturn = phased.RadarTarget('Model', 'Nonfluctuating', 'MeanRCS', targetRCS);
targetSignal = targetReturn(returnSignalH, targetRange);
% Відображення сигналу до і після взаємодії з малопомітною ціллю
figure;
```

```
subplot(2, 1, 1);
plot(abs(returnSignalH));
title('Сигнал до взаємодії з малопомітною ціллю');
subplot(2, 1, 2);
plot(abs(targetSignal));
title('Сигнал після взаємодії з малопомітною ціллю');
```

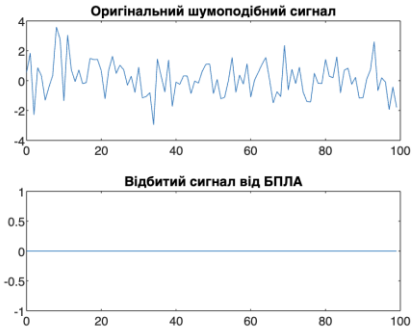


Рисунок 1. Демонстрація роботи моделі

У цьому прикладі ми створюємо двохполяризаційний сигнал, а потім моделюємо взаємодію з малопомітною ціллю за допомогою об'єкта `phased.RadarTarget`. Графіки демонструють сигнал перед взаємодією з ціллю та сигнал після взаємодії.

Таким чином, ортогонально-поляризовані шумоподібні радіосигнали представляють собою новаторський підхід у виявленні малопомітних цілей, таких як БПЛА. Цей метод відрізняється високою ефективністю у виявленні цілей, що традиційно важко виявити.

Список використаних джерел:

1. Білик О.С., ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDR В МЕТОДАХ ПАСИВНОЇ РАДІОЛОКАЦІЇ ТА РАДІОРОЗВІДКИ // 27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – С. 37-38.

2. Білик О. С. Огляд методів виявлення бпла з використанням ортогонально-поляризованих шумоподібних радіосигналів та технології SDR / О. С. Білик, О. О. Мартинчук // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023) : матеріали дев’ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 52-56.

УДК 621.396.6 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.008

ВИКОРИСТАННЯ ОРТОГОНАЛЬНО-ПОЛЯРИЗОВАНИХ ШУМОПОДІБНИХ РАДІОСИГНАЛІВ ДЛЯ ПРИДУШЕННЯ СИГНАЛІВ УПРАВЛІННЯ ТА НАВІГАЦІЇ БПЛА

Білик О.С., Мартинчук О.О.
Науковий керівник - к.т.н., доц. Мартинчук О.О.
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
e-mail: oleksandr.bilyk@nure.ua

This report presents a detailed analysis of using orthogonally-polarized noise-like radio signals for effectively jamming the radio-frequency signals that control Unmanned Aerial Vehicles (UAVs). These signals, characterized by a broad frequency spectrum, are difficult to detect and suppress. Orthogonal polarization allows targeted impact on UAV receiving antennas regardless of their orientation, disrupting UAV-operator communication, stabilization, satellite links, and video data transmission. The report discusses the adaptability of Electronic Warfare (EW) systems to different UAV types and control methods, highlighting the use of Software Defined Radio (SDR) technology.

Ортогонально-поляризовані шумоподібні радіосигнали можуть бути використані для створення специфічних перешкод, які змушують БПЛА втратити зв'язок з оператором, вплинути на стабілізацію БПЛА, зв’язок зі супутниками та передачу відеоданих. Шумоподібні сигнали характеризуються широким спектром частот, що ускладнює їх виявлення та придушення. Використання ортогональної поляризації дозволяє цілеспрямовано впливати на приймальні антени БПЛА, незалежно від їхньої орієнтації.

Системи РЕБ повинні бути гнучкими, щоб адаптуватися до різних типів БПЛА та їхніх методів управління. Для даних цілей може бути використана технологія Software Definition Radio (SDR), дані отримані попередньо під час виявлення БПЛА, програмне забезпечення, яке може генерувати необхідні сигнали-завади на основі виявлених даних та набір антен відповідно до діапазону використовуваних частот та різних типів поляризації.

У випадку використанні ортогонально-поляризованих шумоподібних радіосигналів існують певні виклики:

- точність націлювання: необхідно точно націлювати сигнали на БПЛА, що може бути складно при їх високій мобільності;
- побічний вплив на власні системи зв'язку та БПЛА. У випадку використання направлених антен та резервних засобів зв’язку - мінімізується вплив на власні засоби;
- для великої потужності випромінювання потребуються більш складні та дороговартісні пристрої, потужні та ємнісні джерела живлення.

В той же час розвиток технологій РЕБ в контексті ортогонально-поляризованих шумоподібних радіосигналів, відкриває нові можливості для захисту від БПЛА:

- комбінація з іншими засобами РЕБ та протиповітряною обороною;
- вдосконалення алгоритмів для більш точного виявлення та придушення сигналів БПЛА.

Ортогонально-поляризовані шумоподібні радіосигнали є одним із методів радіоелектронної боротьби та виявлення. Для зрозумілості переваг та недоліків цього методу, корисно порівняти його з іншими підходами.

Через ортогональну поляризацію, ці сигнали ефективніше взаємодіють з різними типами приймачів, забезпечуючи більш ефективне придушення сигналів управління БПЛА.

Шумоподібні сигнали з широким спектром ускладнюють їх виявлення та придушення ворожими системами. Ортогонально-поляризовані сигнали можна адаптувати під різні сценарії, забезпечуючи більшу універсальність у використанні. Також дані сигнали можуть бути налаштовані таким чином, щоб мінімізувати вплив на неворожі комунікаційні системи.

До недоліків ортогонально-поляризованих шумоподібних сигналів слід віднести складну реалізацію засобів РЕБ з даними сигналами, необхідність високотехнологічного обладнання та спеціалізованих знань. Розробка та втілення ортогонально-поляризованих систем може бути коштовнішою порівняно з традиційними методами РЕБ.

Таким чином, використання ортогональної поляризації та шумоподібних радіосигналів забезпечує значні переваги у радіоелектронній боротьбі, включаючи покращене придушення сигналів, складність для виявлення противником та гнучкість застосування. В той же час використання таких систем супроводжується технічними та оперативними викликами, включаючи необхідність високотехнологічного обладнання, високу вартість імплементації, а також потенційний вплив на цивільні комунікаційні системи. Нижче наведено приклад простої програми на мові Python, яка може використовуватись для генерування шумоподібних сигналів за допомогою SDR HackRF:

```
from gnuradio import analog, blocks, gr, osmosdr
import time
class NoiseSignalGenerator(gr.top_block):
    def __init__(self, sample_rate=1e6, frequency=2.4e9, gain=10):
        gr.top_block.__init__(self, "Noise Signal Generator")
        # Parameters
        self.sample_rate = sample_rate
        self.frequency = frequency
        self.gain = gain
        # Blocks
        self.sdr_sink = osmosdr.sink(args="hackrf=0")
        self.noise_source = analog.noise_source_c(analog.GR_GAUSSIAN, amplitude=1.0)
```

```
            self.throttle = blocks.throttle(gr.sizeof_gr_complex, self.sample_rate, True)
            # Set SDR parameters
            self.sdr_sink.set_sample_rate(self.sample_rate)
            self.sdr_sink.set_center_freq(self.frequency)
            self.sdr_sink.set_gain(self.gain)
            # Connect blocks
            self.connect(self.noise_source, self.throttle, self.sdr_sink)
        def start(self):
            gr.top_block.start(self)
            print(f"Generating noise-like signal at {self.frequency} Hz with gain {self.gain}")
        def stop(self):
            gr.top_block.stop(self)
            gr.top_block.wait(self)
            print("Stopped noise signal generation")
    # Parameters for the noise signal
    SAMPLE_RATE = 1e6 # 1 MHz
    FREQUENCY = 2.4e9 # 2.4 GHz, common for WiFi signals/pilot channels
    GAIN = 10 # Gain for the transmission
    # Create a noise signal generator and start it
    generator = NoiseSignalGenerator(sample_rate=SAMPLE_RATE,
frequency=FREQUENCY, gain=GAIN)
    generator.start()
    # Run the generator for a specified time
    RUN_TIME = 10 # seconds
    time.sleep(RUN_TIME)
    # Stop the generator
    generator.stop()
```

Список використаних джерел:

1. Martynchuk A. Research the efficiency and feasibility of circular polarization in the tropospheric radio link / Valery Loshakov, Alexander Martynchuk, Alex Nazmutdinov, Alex Skorohod, Abdenour Drif // 2016 Third International Scientific-Practical Conference "Problems of Infocommunications. Science and Technology". PIC S&T 2016. – Харьков: ХНУРЭ, 2016, с. 99-102
2. Білик О.С., ВИКОРИСТАННЯ ТЕХНОЛОГІЇ SDR В МЕТОДАХ ПАСИВНОЇ РАДІОЛОКАЦІЇ ТА РАДІОРОЗВІДКИ // 27-й Міжнародний молодіжний форум «Радіоелектроніка та молодь у XXI столітті». Зб. Матеріалів форуму. Т.4. – Харків: ХНУРЕ. 2023. – С. 37-38.
3. Білик О. С. Огляд методів виявлення БПЛА з використанням ортогонально-поляризованих шумоподібних радіосигналів та технології SDR / О. С. Білик, О. О. Мартинчук // Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023) : матеріали дев’ятої Міжнародної науково-технічної конференції, 7 грудня 2023 р. – Харків : ХНУРЕ, 2023. – С. 52-56.

УДК 621.396:004.738.5

ОСОБЛИВОСТІ ПОБУДОВИ ГЕТЕРОГЕННИХ МЕРЕЖ

Гонтар І.Ю.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: iryna.hontar@nure.ua

It is shown that the development of the concept of heterogeneous networks is due to an increase in bandwidth due to the mechanisms of spatial compaction and spectral aggregation. The architecture and basic properties of the HetNet network are analysed. It is proved that the efficient simultaneous use of several RATs is one of the key tasks of HetNet. The main approaches to coordinating the joint work of different RATs are presented. It is shown that the network optimisation is possible due to more advanced methods of radio resource allocation between the RATs.

Для досягнення високої пропускної здатності в сучасних стільникових мережах використовуються механізми просторового ущільнення та спектральної агрегації [1]. Просторове ущільнення включає розгортання макростільників великої площі, які додатково перекривають дрібніші стільники для підвищення пропускної здатності, що створює концепцію гетерогенної мережі Heterogenic Networks (HetNet). Архітектуру мережі HetNet зображена на рис.1.

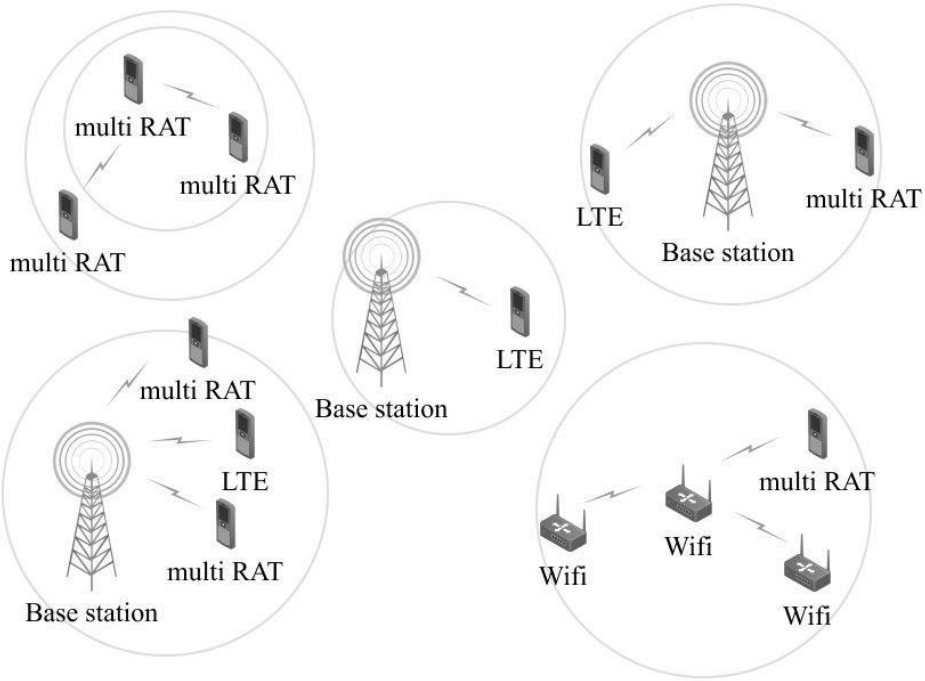


Рисунок 1 – Архітектура HetNet

За рахунок використання концепції HetNet мережі в рамках стільникових мереж п’ятого покоління 5G можна домогтися значно вищої пропускної здатності мережі, ефективного покриття та кращого користувацького доступу. Необхідними вимогами для оптимізації мережі HetNet слід зазначити [2, 3]:

– підвищення швидкості передачі даних, яка залежить від сукупної швидкості передачі даних. При цьому велика увага приділяється наступним складовим: граничній та піковій швидкостям. Гранична швидкість або швидкість 5% вважається найгіршою швидкістю передачі даних, яку користувач може очікувати, перебуваючи в зоні дії мережі. Але ж піковою є найкраща швидкість передачі даних, яку користувач може досягти за будь-якої конфігурації мережі;

– зниження затримки в обидва боки до однієї мілісекунди, що критично для нових додатків, таких як: двосторонні ігри, нові хмарні технології, а також віртуальної й доповненої реальності;

– зниження енергоспоживання обладнання й витрат.

Основні властивості, які притаманні мережі HetNet, обумовлені неоднорідністю типів Radio Access Technology (RAT). Ефективне одночасне використання декількох RAT є одним з ключових завдань HetNet. Для координації сумісної роботи різних RAT існують два підходи: керування за допомогою централізованого координуючого органу та використання децентралізованого підходу всередині окремих RAT.

Зважаючи на те, що HetNet характеризуються неоднорідністю додатків, окремі компоненти RAT різняться за очікуваним використанням. Плаский розподіл площини керування та площини користувача стає фундаментальним завданням для реалізації HetNet. Координуючий вузол, що керує гетерогенною системою, збирає всю необхідну інформацію про поточний попит на користувацький трафік, а також відстежує доступність певного покриття RAT у цільовій зоні обслуговування.

Таким чином, гетерогенна мережа HetNet, що включає стільники різних масштабів, що керовані різними RAT, потребує оптимізації мережі як за рахунок досконаліших методів розподілу радіоресурсів між RAT, так і за рахунок основних показників мережі.

Список використаних джерел:

1. Andrews J., Buzzi S. and et. What will 5G be? *IEEE Journal on Selected Areas in Communications*. 2014. Vol. 32. P. 1065–1082.

2. Baldemair R., Dahlman E. and et. Evolving Wireless Communications: Addressing the Challenges and Expectations of the Future. *IEEE Vehicular Technology Magazine.* 2013.Vol. 8. P. 24–30.

3. Li Q., Niu H., Papathanassiou A. and Wu G. 5G Network Capacity: Key Elements and Technologies. *IEEE Vehicular Technology Magazine*. 2014. Vol. 9. P. 71–78.

УДК 621.396.49 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.013

АНАЛІЗ ЕФЕКТИВНОСТІ АЛГОРИТМІВ КОМПЕНСАЦІЇ КАНАЛЬНИХ СПОТВОРЕНЬ У SDR

Жуга Ю.С.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
e-mail: yurii.zhuha@nure.ua.

This paper examines the effectiveness of channel compensation algorithms in SDR systems using QPSK modulation. SDR's adaptability makes it integral to modern telecom. The study employs GNU Radio simulations to analyze noise impact on QPSK signals. Results highlight the necessity for robust compensation methods, especially under high noise conditions, to maintain SDR system integrity.

Сучасні телекомунікаційні системи неухильно розвиваються, забезпечуючи широкий спектр послуг від голосового зв'язку до високошвидкісного інтернету. Одним з визначних нововведень у цій галузі є технології програмованого радіо (Software Defined Radio - SDR), які надають можливість гнучкої та швидкої адаптації до змінних умов передачі даних та стандартів зв'язку. SDR відкриває нові перспективи для інноваційних підходів у дизайні та впровадженні телекомунікаційних систем завдяки своїй високій конфігурувальності та масштабованості.

Вибір квадратурної фазової модуляції (QPSK) для аналізу обумовлений її широким використанням у сучасних бездротових комунікаціях. QPSK дозволяє ефективно використовувати смугу частот та відповідає високим вимогам до швидкості передачі даних та надійності зв'язку. Особлива увага в цьому дослідженні приділяється вивченню впливу шуму на якість передачі сигналу QPSK у SDR системах та методам компенсації канальних спотворень.

Квадратурна фазова модуляція (QPSK) є однією з основних цифрових модуляційних схем, яка дозволяє передавати два біт інформації за один символьний період. Ця ефективність досягається за рахунок кодування інформації в чотири різні фазові зсуви, кожен з яких відповідає унікальному комбінації двох бітів. Математично, QPSK сигнал можна виразити як суму двох ортогональних несучих сигналів, модульованих відповідно до відібраних бітів інформації. Дана модуляція є оптимальним вибором для SDR систем через свою стійкість до шуму та здатність ефективно використовувати радіочастотний спектр.

Використовуючи програмне середовище GNU Radio, було створено симуляційну модель для вивчення поведінки QPSK модульованих сигналів в різних умовах. Симуляція включала генерацію випадкових бітів даних, їх модуляцію за допомогою QPSK, передачу через канал з доданим шумом, та демодуляцію отриманих сигналів. Експериментальна установка була

налаштована для варіювання рівнів шуму, щоб визначити його вплив на якість прийняття сигналу.

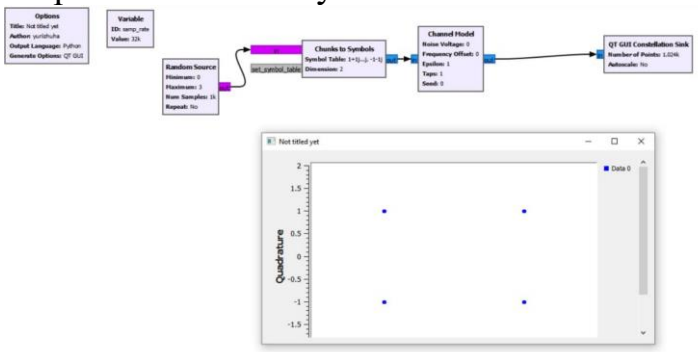


Рисунок 1 – Фазова діаграма QPSK без шумового впливу

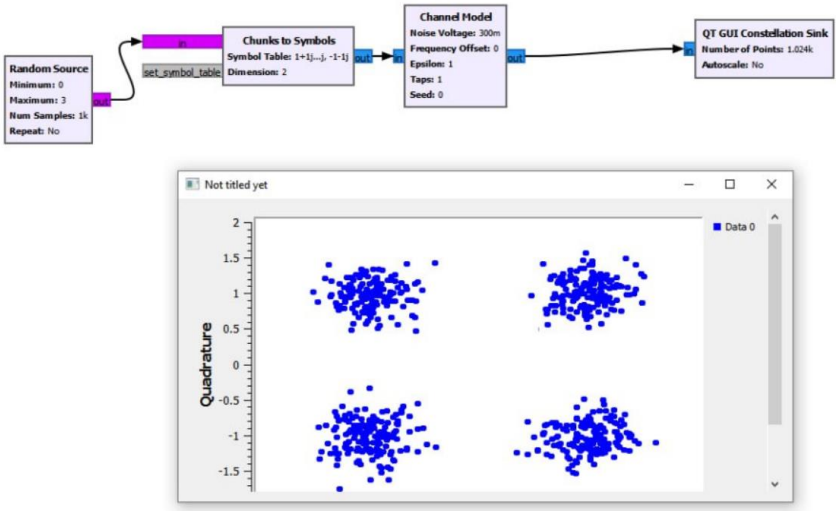


Рисунок 2 – Фазова діаграма QPSK з доданим шумом 0.3

Результати симуляції показали, що при відсутності шуму QPSK сигнали демодулюються з високою точністю, підтверджуючи передбачувану надійність цієї модуляційної схеми. Однак, зі збільшенням рівня шуму спостерігалося погіршення точності демодуляції, що проявлялося у зростанні кількості помилок. Таке зниження якості прийому сигналу підкреслює важливість розробки ефективних алгоритмів для компенсації канальних спотворень.

Дослідження показало, що при низьких рівнях шуму QPSK демонструє високу надійність, однак при високих рівнях шуму якість сигналу значно знижується. Ці висновки підкреслюють важливість використання розширених методів компенсації, наприклад, алгоритмів адаптивного фільтрування та кодування з перевіркою помилок, щоб забезпечити високу точність прийому даних. Зокрема, алгоритми, такі як Least Mean Squares (LMS) та Recursive Least Squares (RLS), виявилися ефективними у мінімізації помилок, викликаних шумом, та можуть бути інтегровані у SDR системи для покращення якості бездротової передачі даних.

Дослідження підтвердило важливість QPSK як модуляційної схеми для SDR систем та виявило критичний вплив шуму на якість сигналу. Розробка та оптимізація алгоритмів компенсації спотворень є ключовим для підвищення ефективності та надійності сучасних телекомунікаційних систем. За результатами цього дослідження можна зробити висновок, що подальші розробки в галузі SDR відкривають широкі перспективи для інновацій у бездротовому зв'язку.

Список використаних джерел:

1. Лошаков В.А., Москалець М.В., Велліо А., Al-Vandavi Saif Ahmed Iskandar Ismael, Хвостик І.О.: “Комплекс лабораторних робіт з дослідження систем зв’язку та радіомоніторингу на базі SDR технології”, 2019.

2. Коляденко Ю.Ю. Аналіз технології когнітивного радіо в телекомунікаціях / Ю.Ю. Коляденко, А.М. Ткаченко // Матеріали 26-го міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Харків, ХНУРЕ, 2022. С. 25-26.

3. Коляденко Ю.Ю. Управління радіочастотним спектром в когнітивних мережах зв’язку / Ю.Ю. Коляденко, А.М. Ткаченко // Матеріали 24-го міжнародного молодіжного форуму «Радіоелектроніка та молодь у XXI столітті». Харків, ХНУРЕ, 2020. С. 13-15.

УДК 621.391.8 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.016

МОДЕЛІ ТА МЕТОДИ РОЗРІЗНЕННЯ RZ–СИГНАЛІВ НА ФОНІ АСИМЕТРИЧНО–ЕКСЦЕСНИХ НЕГАУСОВИХ ЗАВАД

Зорін О.С.
Науковий керівник – д.т.н., проф. Палагін В.В.
Черкаський державний технологічний університет, каф. РТСК,
м. Черкаси, Україна
e-mail: snjzrin@gmail.com.

The proposed new method of processing an additive mixture of bipolar discrete RZ signals against the background of asymmetric-excessive non-Gaussian interference when receiving data in telecommunication systems demonstrates its effectiveness in comparison with known results due to nonlinear statistical processing of signals and taking into account the fine structure of the studied random processes. The conducted studies demonstrate a decrease in erroneous decisions when receiving RZ signals, taking into account the coefficient of asymmetry and the excess of non-Gaussian interference, which indicates an increase in the efficiency of the data reception system.

Системи передачі і прийому даних є невід'ємною і, в багатьох випадках визначальною частиною сучасних систем спостереження, діагностики, контролю, управління, розвиток яких характеризується підвищеними вимогами до обробки прийнятих даних. При побудові таких систем застосовують один із типів лінійного кодування повідомлення, наприклад RZ–кодування [1].

На функціонування таких систем при передачі даних, як правило, впливають різноманітні дестабілізуючі завади, що в свою чергу впливає на якість та ефективність їх роботи. Завади виникають при багатопроменевому поширенні радіосигналів, при проходженні їх через неоднорідні середовища, флуктуації параметрів каналів зв'язку та ін., які характеризуються як негаусові випадкові процеси.

Дослідження останніх років свідчать про те, що при розв'язанні задач обробки негаусових процесів перспективним є підхід, який для опису статистичних властивостей випадкових величин використовує моменти і кумулянти, та дозволяє з прийнятним наближенням характеризувати статистичні властивості негаусових процесів [1-3]. Такий підхід дозволяє підвищити точність обробки негаусових сигналів порівняно з традиційним кореляційним підходом при заданих обмеженнях на їх складність, зменшити складність алгоритмів виявлення і розрізнення сигналів, реалізувати обробку сигналів при адитивно-мультиплікативній взаємодії з негаусовими завадами, врахувати кореляційні зв'язки негаусових випадкових величин.

Мета роботи – підвищення ефективності систем прийому даних при розрізненні RZ–сигналів на фоні негаусових завад при застосуванні моментно-кумулянтного представлення випадкових величин з

формуванням моментного критерію якості перевірки статистичних гіпотез та поліноміальних розв'язувальних правил (РП).

Постановка задачі: нехай на інтервалі спостереження $(0-T)$ спостерігаються випадкові сигнали $\xi_i(t)$, $i=0,1,2$ які являють собою адитивну суміш постійних корисних сигналів a_1 та a_2 з $\eta(t)$ – асиметрично-ексцесної негаусової завади з нульовим математичним сподіванням та дисперсією χ_2: $\xi_0(t)=\eta(t)$, $\xi_1(t)=a_i+\eta(t)$, $\xi_2(t)=-a_i+\eta(t)$, $i=1,2$. З випадкових сигналів $\xi_i(t)$, $i=0,1,2$ отримуємо вектор вибіркових значень $X=\{x_1,x_2,...x_n\}$, за результатами обробки якого необхідно прийняти рішення про реалізацію гіпотези H_1 або H_2, що відповідає прийому постійного корисного сигналу a_1 або $(-a_2)$ відповідно, або рішення про реалізацію гіпотези H_0, що характеризує наявність адитивної негаусової завади. Кожному сигналу, який приймається, відповідає моментно-кумулянтний опис, представлений у вигляді кінцевої послідовності моментів $m_i[\{0,\chi_{i2},\gamma_{i3},...\gamma_{ij}\}]$, де $\gamma_{i3},...\gamma_{ij}$ – кумулянтні коефіцієнти, які описують ознаки негаусової завади $\eta(t)$. Для обробки вектора вибіркових значень $X=\{x_1,x_2,\cdots,x_n\}$ пропонується використовувати РП, які представлено у вигляді стохастичних поліномів на основі розкладання логарифма відношення правдоподібності. Синтезовані РП при степені полінома $S=1$, являють собою систему рівнянь перевірки гіпотез H_{10},H_{20},H_{21}, які не враховують негаусовий розподіл досліджуваних випадкових процесів. При збільшенні степені полінома до $S=2$ використовуються початкові моменти 3-го та 4-го порядків, що дає можливість врахувати негаусові параметри досліджуваних випадкових процесів, зокрема для даної постановки задачі у вигляді коефіцієнту асиметрії так ексцесу γ_3,γ_4 відповідно.

Аналіз отриманих результатів: Для оцінки ефективності отриманих результатів скористаємося виразом[5], який характеризує ймовірність помилок першого та другого роду отриманих РП, або величиною, яка є зворотна даному функціоналу – кількість добутої інформації про розрізнення гіпотез. На рис.1. наведена залежність відношення кількості добутої інформації I_1 про розрізнення трьох гіпотез РП для гаусової моделі завади $(S=1)$ до кількості добутої інформації I_2 $(S=2)$ про розрізнення гіпотез РП для негаусової асиметрично-ексцесної моделі завади від коефіцієнта асиметрії γ_3. З отриманих графіків видно, що для гаусової моделі завад ($\gamma_4=\gamma_3=0$) нелінійна обробка РП при степені полінома $S=2$ не дає виграша у зменшенні ймовірності помилкових рішень (відношення $I_{1n}/I_{2n}=1$). Разом з тим, врахування негаусової характеристики досліджуваних процесів у вигляді коефіцієнтів асиметрії та ексцесу

($\gamma_3 \neq 0, \gamma_4 \neq 0$) дозволяє збільшити кількість добутої інформації при нелінійній обробці вибіркових значень ($S = 2$) у порівнянні з добре відомими результатами для гаусових моделей ($S = 1$). Так, наприклад, для кривої (3) $\gamma_3 = 1.55, \gamma_4 = 1$ ефективність в зменшенні ймовірності помилкових рішень для нелінійної обробки виявлення RZ сигналів збільшиться в 2 рази у порівнянні з відомими результатами для гаусових моделей досліджуваних випадкових процесів.

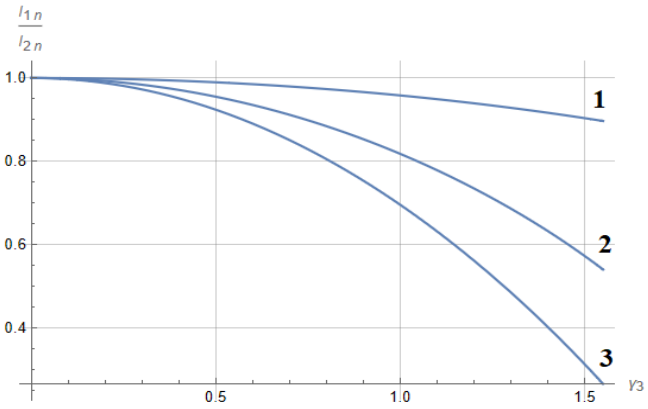


Рис. 1 Залежність кількості добутої інформації про розрізнення гіпотез від коефіцієнта асиметрії γ_3 при наступних параметрах: $\gamma_4 = 1$, 1) $p_1 = p_2 = 10$; 2) $p_1 = p_2 = 1$; 3) $p_1 = p_2 = 0{,}1$. Де $p_i = a_i^2 / \chi_2, i = 1,2$ – відношення потужності корисного сигналу a_i до дисперсії адитивної негаусової завади χ_2.

Висновки: Запропонований метод обробки адитивної суміші біполярних дискретних RZ сигналів на фоні асиметрично-ексцесних негаусових завад є більш ефективним у порівнянні з відомими алгоритмами, які не враховують тонкої структури досліджуваних випадкових процесів. Проведені дослідження демонструють збільшення кількості добутої інформації про розрізнення гіпотез при врахуванні коефіцієнта асиметрії негаусової завади, що свідчить про зменшення ймовірностей помилок таких РП і підвищення ефективності функціонування системи розрізнення сигналів в цілому.

Список використаних джерел:

1. Mahmoud M. A., Ahmed Nabih Zaki Rashed. Hybrid NRZ/RZ line coding scheme based hybrid FSO/FO dual, Indonesian Journal of Electrical Engineering and Computer Vol. 22, No. 2, May 2021 p. 866-873.

2. S.L.Miller, D.Childers, Probability and random processes: With Applications to Signal Processing and Communications, 2-d ed., 2004, Amsterdam; Boston: Elsevier Academic Press, ISBN: 978-0-12-386981-4.

3. Y.Kunchenko: Polynomial Parameter Estimations of Close to Gaussian Random Variables, Aachen: Shaker Verlag, 2002.

4. Палагін В.В, Палагіна О.А., Зорін О.С. Комп'ютерне моделювання системи обробки шумових сигналів на фоні негаусових завад / В.В. Палагін, Палагіна О.А., Зорін О.С., // Математичне та комп’ютерне моделювання. Серія: Технічні науки: зб. наук. праць – Кам.-Подільський: Кам.-Подільський нац. ун-т ім. Івана Огієнка, 2017. – Вип. 16. – С. 104-113.

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.019

ОГЛЯД МЕТОДІВ КЕРУВАННЯ ТРАФІКОМ ТА СУЧАСНОГО СТАНУ РОЗВИТКУ МЕРЕЖ SDN

Колтаков О.А., Москалець М.В.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
email: oleksandr.koltakov@nure.ua

In modern networks, heterogeneous traffic is transmitted, which consists of data packets, control packets, voice, video data, which require special priority during transmission. The problem is exacerbated by the transition of users to a remote form of employment, the active use of mobile devices and IoT devices. Today, network providers and numerous IT organizations use software-defined networking (SDN) to optimize network infrastructure management and ensure a high level of service quality. In this work, a study of SDN network functioning methods, its current state of development and future forecasts of use was conducted.

Основною ідеєю програмно-конфігурованої мережі (SDN – Software-defined Networking) є розділення функцій передачі трафіку і функцій керування. SDN надає спосіб централізованого налаштування та управління мережами та мережевими службами, такими як комутація, маршрутизація та балансування навантаження в центрі обробки даних. В концепції SDN контролер виконує логістичну функцію, аналізуючи трафік та розподіляючи його. Це дозволяє керувати мережею як єдиним цілим.

Архітектура мереж SDN поділяється на три рівні [1]:

- Рівень програм: програми та служби, що працюють у мережі.
- Рівень контролю: контролер SDN.
- Рівень інфраструктури: комутатори, маршрутизатори та інше мережеве обладнання.

В SND широко використовуються наступні методи керування трафіком:

- Конструювання трафіку.
- Моніторинг та аналіз трафіку.
- Сегментація трафіку.
- Балансування навантаження.
- Якість обслуговування (QoS).
- Маршрутизація на основі політики.

Дані методи дозволяють ефективно використовувати мережеві ресурси та проводити маршрутизацію [1]; контролювати розподіл смуги пропускання, пріоритет пакетів та затримку; сегментувати трафік на окремі віртуальні машини; динамічно балансувати трафік між шляхами; збирати статистику про актуальний стан каналів та вузлів; маршрутизувати трафік на основі політик.

В еволюції концепції мережі SDN можна виділити три етапи:

1. Етап ранньої концептуалізації. Характеризується представленням ідеї відокремленні керуючого вузла та першими проектами даної ідеї.

2. Впровадження протоколу OpenFlow та створення ONF. Відкрилися можливості динамічно керувати потоками трафіку та поведінкою мережі, а створення організації Open Networking Foundation (ONF) дало просування та стандартизації технологій SDN. OpenFlow був успішно запущений в мережі у 2008 році, перемістивши управління з комутаторів, що містили тільки площину даних, на мережевий контролер. Пізніше цей протокол був використаний Googley своїй магістральній мережі в 2011-2012 роках.

3. Розширення в SD-WAN та інтеграція з NFV. Характерною ознакою є інтеграція з глобальною мережею та віртуалізація мережевих функцій.

В останні роки концепція SDN мереж продовжує активно розвиватися та набирати розповсюдження у різних галузях, включаючи телекомунікації, центри обробки даних, корпоративні мережі та хмарну інфраструктуру. Проаналізувавши зміни та нововведення за останні роки, можна виділити наступні тенденції розвитку мереж SDN:

1. Вдосконалення стандартів. Органи стандартизації, такі як ONF і Open Networking User Group (ONUG), продовжують розробляти та вдосконалювати стандарти SDN. Ці стандарти допомагають забезпечити взаємодію та спрощують інтеграцію рішень SDN у існуючу мережеву інфраструктуру.

2. Зростання SD-WAN. Програмно-визначена глобальна мережа (SD-WAN) набула значного імпульсу. Технологія SD-WAN дозволяє організаціям динамічно керувати глобальними мережевими з’єднаннями та оптимізувати їх, що веде до підвищення продуктивності, економії коштів і кращого зв’язку між додатками. За прогнозами Gartner доля ринку SD-WAN, яка складала 5,3 мільярда доларів США на 2023 рік, зросте до понад 8 мільярдів доларів США до 2026 року. Dell'Oro Group очікує, що SD-WAN подвоїться з 2022 по 2027 рік і досягне 6 мільярдів доларів.

3. Інтеграція з хмарними технологіями. SDN все більше інтегрується з платформами хмарних обчислень для створення більш гнучких і масштабованих хмарних мереж. Хмарні постачальники пропонують рішення на основі SDN, які дозволяють користувачам ефективно керувати мережевими ресурсами та розгортати програми в хмарі [4].

4. Штучний інтелект. Також слід відмітити зростаючу тенденцію до включення штучного інтелекту (AI) і машинного навчання (ML) у рішення SDN. Ці технології забезпечують автономне керування мережею, прогнозну аналітику та проактивне усунення несправностей, що сприяє підвищенню продуктивності та надійності мережі [4].

5. Мережі 5G. SDN відіграє вирішальну роль у підтримці мереж 5G і розгортання периферійних обчислень. SDN забезпечує ефективний поділ

мережі, розподіл ресурсів і надання послуг у середовищах 5G [4]. Планується активне використання у мережах 6G.

6. Покращення безпеки. Функції безпеки інтегруються в рішення SDN для вирішення нових загроз і вразливостей. Платформи SDN пропонують централізовану видимість і контроль, забезпечуючи більш ефективний моніторинг мережі, контроль доступу та реагування на загрози. Наприклад, за останні роки значного розвитку набула Detection and Prevention Systems (IDPS) система, що запобігає вторгненням.

За прогнозами дослідження Market Research Report доля світового ринку SDN зросте з 24.5 мільярдів доларів (2023 рік) до 60.2 мільярдів доларів (2028 рік). Загальний вклад в використання та розвиток SDN збільшиться на 19.7% [3]. Це показує високий інтерес до використання даного підходу адміністрування мережі у недалекому майбутньому. Збільшення фінансування відкриє нові можливості в інтеграції SDN з іншими телекомунікаційними та цифровими сферами, дослідження нових та вдосконалення існуючих методів керування.

За словами аналітика Gartner Ендрю Лернера, який вивчає ринок SD-WAN, привабливими перевагами цієї технології є простота впровадження, централізована керованість та економія витрат. За його оцінками, впровадження SD-WAN може коштувати приблизно в два з половиною рази менше, ніж традиційна архітектура глобальної мереж [2].

Таким чином, аналіз сучасного стану використання SDN показав, що даний тип мереж широко інтегрований та використовується як в існуючих телекомунікаційних сферах, так в нових, котрі тільки починають розвиватися.

Список використаних джерел:

1. Єременко О.С., Плєханова Г.А. Дослідження моделей безпечної маршрутизації на основі базових метрик уразливостей у мережах SDN // Проблеми телекомунікацій. 2022. №2. С. 34-50.

2. Савицька Л., Коробейнікова Т., Леонтьєв І., Богомолов С. Методи та засоби захисту ресурсів в комп’ютерній SDN-мережі // Інформаційні технології та комп’ютерна інженерія. 2023. №53. С. 41–52.

3. The Software-Defined Networking (SDN) Market in 2022 | Enterprise Storage Forum. Enterprise Storage Forum. URL: https://www.enterprisestorageforum.com/networking/software-defined-networking-market/ (дата звернення: 29.02.2024).

4.The evolution of Software Defined Networking. URL: https://www.redhat.com/en/blog/evolution-software-defined-networking (дата звернення: 29.02.2024).

УДК 621.396:004.7

РІШЕННЯ ДЛЯ ЗМЕНШЕННЯ ЕНЕРГОСПОЖИВАННЯ БАЗОВИМИ СТАНЦІЯМИ В БЕЗПРОВОДОВИХ МЕРЕЖАХ

Котолупенко Б.О.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: bohdan.kotolupenko@nure.ua

It is proved that the existence of the problem of growing energy consumption caused by the need to increase capacity is important for telecommunication networks. It is analysed that the BS is considered to be the main element of the network that consumes the largest part of energy. Possible solutions aimed at energy saving of the BS are presented. It is shown that to solve the problems of energy saving, approaches should be used both at the architectural level and by increasing the efficiency of individual network components.

Підвищення пропускної здатності безпроводового широкосмугового доступу призводить до зростання енергоспоживання та збільшення витрат за електроенергію. Тому перед операторами постає завдання зниження енергоспоживання базовими станціями (БС), що й обумовлює актуальність даної роботи.

Доведено, що 10% усієї світової електроенергії споживається телекомунікаційними мережами. За оцінками, до 2030 споживання енергії збільшиться до 51% [1]. Взагалі у мережі БС вважається основним елементом, що споживає найбільшу частину енергії (рис.1) [2].

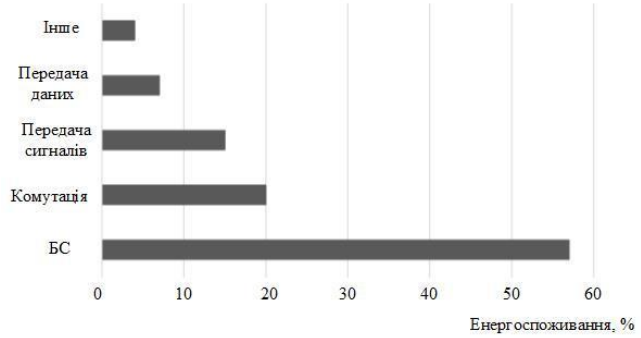


Рисунок 1 – Енергоспоживання мобільного оператора

Енергія, що споживається БС, складається з трьох чинників [3]:

$$E_{BS} = P_0 T_F + E_{DATA} + E_{SIGN}, \quad (1)$$

де $P_0 T_F$ - фіксований коефіцієнт, що відповідає енергії, що необхідна для роботи БС; P_0 - потужність, яка необхідна для включення БС; E_{DATA} - енергія, яка необхідна для передачі даних; E_{SIGN} - енергія, яка необхідна для передачі сигналів.

Останні фактори залежать від навантаження на трафік та є змінними. Таким чином, рівняння (1) дозволяє зробити розрахунок необхідної енергії БС для передачі N каналів N користувачам, що випадково розподілені по заданій області.

Для енергозбереження БС використовуються декілька рішень:

− енергоефективне проєктування БС – ефективне апаратне забезпечення БС з погляду енергоспоживання;

− стратегії проєктування БС, що враховують системи кондиціювання повітря Air Conditioning (A/C).

− зниження споживаної потужності при радіопередачах - зменшення переданої потужності з точки зору потужності пілот-сигналу і потужності, що виділяється на передачу даних користувача;

− оптимізація кількості діючих БС - мінімізація кількості діючих БС (або модулів у складі БС) шляхом вимикання та включення їх залежно від стану мережі;

− одним із цікавих рішень є розгортання широкосмугової мережі, відповідно до вимог до трафіку, з використанням малопотужних мікросот та мікро-БС, спеціально призначених для зменшення енергоспоживання порівняно із сучасними схемами макро-БС високої потужності.

Таким чином, для вирішення проблем енергозбереження мають бути використані підходи як на архітектурному рівні, так і за рахунок підвищення ефективності окремих компонентів мережі, наприклад, таких як: використання комбінацій нових можливостей спектру, енергоефективних рівнів Physical Layer (PHY) та стратегій розгортання та транзиту, спрямованих на загальну мінімізацію вартості системи.

Список використаних джерел:

1. Piovesan N., Fernandez Gambin A., Miozzo M., Rossi M. Dini P. Energy sustainable paradigms and methods for future mobile networks. *Computer Communications*. 2018. Vol. 119. P. 101–117.

2. Han C. et al Green radio: radio techniques to enable energy-efficient wireless networks. *IEEE Communications Magazine*. 2011. Vol. 49. P. 46 – 54.

3. Giuliano R., Mazzenga, F. & Petracca M. Power Consumption Analysis and Dimensioning of UMTS-LTE with Relays. *Procedia Computer Science*. 2014. Vol. 40. P. 74–83.

УДК 621.391:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.024

ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ БЕЗПЕЧНОЇ МАРШРУТИЗАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Лемешко В.О., Персіков М.А.
Науковий керівник – д.т.н., проф. Єременко О.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: valentyn.lemeshko@nure.ua, mykhailo.persikov@nure.ua

This work is devoted to determining the features of implementing secure routing in information and communication systems. The importance of ensuring information security at all seven OSI model layers is noted. At the Network Layer, an increasingly important role in ensuring network security indicators will be assigned to routing protocols, which should adapt to the realities of today and, when forming routing metrics, take into account, along with the Quality of Service indicators, network security metrics. In addition, when configuring routers and routing protocols, it is also necessary to use existing tools to increase network security.

Забезпечення інформаційної безпеки – це складна та багатоаспектна проблема, яка для успішного рішення вимагає скоординованої роботи щодо використання наявних організаційних та технічних ресурсів на всіх етапах її проходження та обробки. Важливе місце у передачі інформації відводиться інформаційно-комунікаційним системам (ІКС), основою яких останнім часом є програмно-конфігуровані мережі (Software-defined Networking, SDN). Тому в SDN для забезпечення безпеки інформації намагаються задіяти функціонал всіх семи рівнів моделі OSI (Open Systems Interconnection) [1].

На мережному рівні все більша роль у забезпеченні показників мережної безпеки буде відводитись протоколам маршрутизації, які повинні адаптуватись до реалій сьогодення та при формуванні маршрутних метрик враховувати поруч з показниками якості обслуговування (Quality of service, QoS) додатково й мережні показники, які пов’язані з інформаційною безпекою – ймовірність компрометації маршрутизатора, каналу, маршруту, ризики інформаційної безпеки тощо [2, 3]. Прикладом подібного вдосконалення з адаптацією до стану мережі є пропрієтарний протокол EIGRP (Enhanced Interior Gateway Routing Protocol), запропонований компанією Cisco [2]. Саме цей протокол дозволяє формувати у реальному часі композитні метрики, які зважено враховують різноманітні мережні показники – від пропускної здатності інтерфейсів та їхньої завантаженості, до затримок та рівня втрат пакетів на цих інтерфейсах. Опосередковано при розрахунку маршрутної метрики також враховується й кількість хопів (переприйомів пакетів) вздовж маршруту. У оновленій версії протоколу

EIGRP з’явився шостий показник, який за необхідністю адміністратор може прив’язати до того чи іншого показника мережної безпеки. Варіюючи ваговими коефіцієнтами $k_1 \div k_6$ адміністратор зможе встановлювати ієрархію впливу QoS-показників та/або показників мережної безпеки на процес визначення оптимального маршруту.

Сформовані подібним чином маршрутні метрики можуть бути використані як в уже класичних алгоритмах розрахунку шляхів DUAL, Дійкстри та Беллмана-Форда, так і у більш перспективних потокових моделях та методах безпечної маршрутизації, в яких, крім мережних показників, додатково враховуються ще й характеристики мережного трафіка [2, 3]. Це є дуже важливим з погляду того, що вимоги до рівня конфіденційності різних повідомлень, пакетів чи потоків можуть суттєво відрізнятись.

З іншого боку, не варто забувати, що процес маршрутизації сам по собі є досить цікавим для зловмисників об’єктом для компрометації у результаті успішно організованих атак і вторгнень. На жаль, і маршрутизатори, як елемент апаратного забезпечення ІКС, і самі протоколи маршрутизації, як елемент програмного забезпечення ІКС, мають вразливості та відмінні від нуля ймовірності їхньої реалізації (використання) з боку зловмисників. Тому адміністратору мережі при налаштуванні маршрутизаторів та протоколів маршрутизації також не варто нехтувати використанням традиційних засобів підвищення рівня мережної безпеки – налаштування авторизованого доступу з використанням безпечних протоколів віддаленого налаштування пристроїв (наприклад, SSH), а також криптографічної автентифікації при передачі повідомлень щодо оновлень стану ІКС, використання надійних паролів і коректних політик фільтрації трафіка.

Список використаних джерел:

1. Liu Y., Zhao B., Zhao P., Fan P., Liu H. A survey: Typical security issues of software-defined networking. *China Communications*. 2019. Vol. 16, No 7. P. 13-31. DOI: https://doi.org/10.23919/JCC.2019.07.002.

2. Лемешко О. В., Єременко О. С., Невзорова О. С. Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість : моногр. Харків : ХНУРЕ, 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1.

3. Лемешко О. В., Єременко О .С., Євдокименко М. О., Шаповалова А. С., Слейман Б. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : моногр. М-во освіти і науки України, Харків. нац. ун-т радіоелектроніки. Харків : ХНУРЕ, 2022. 198 с. DOI: https://doi.org/10.30837/978-966-659-378-1.

УДК 621.396.946

МЕТОДИ ФОРМУВАННЯ ПРОМЕНЮ У ЗАДАЧАХ ПРОСТОРОВОГО ДОСТУПУ В МЕРЕЖАХ МОБІЛЬНОГО ЗВ'ЯЗКУ НАСТУПНИХ ПОКОЛІНЬ

Літвінов І.О.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: ivan.litvinov@nure.ua,
mykola.moskalets@nure.ua

An analysis of the beamforming method of base station antennas in 5G mobile communication systems, which implements spatial access of mobile users, was carried out. Problematic tasks related to the active use of spatial parameters in the group of mobile users of the 5G mobile communication system are outlined. The main aspects of the implementation of beamforming technology of base station antennas in the tasks of spatial access for next-generation mobile communication networks are considered.

1. Технологія формування променя антенною базової станції мережі мобільного зв'язку «Beamforming»

Beamforming (формування променів) – технологія, що використовується в безпроводових інфокомунікаційних системах, включаючи мережі 5G, з метою покращення якості зв'язку та ефективності використання радіочастотних ресурсів. Основна ідея beamforming полягає в управлінні сигналами, що передаються і приймаються з декількох антен, таким чином, щоб вони взаємодіяли один з одним і створювали вузькоспрямовані просторові промені. Принцип роботи «beamforming» заснований на явищі інтерференції хвиль. Коли сигнали від різних антен збігаються у певній точці у просторі, їх хвилі можуть посилювати чи послаблювати одне одного залежно від фазових співвідношень між ними. Використовуючи цей ефект, система може формувати просторові промені, спрямовані до певних користувачів, і мінімізувати інтерференцію з іншими пристроями (рис.1).

Надширокополосні частоти 5G працюють на міліметровій довжині хвиль (mmWave) радіоспектра, що є частиною того, що дозволяє надширокополосним мережам 5G передавати так багато даних на революційних швидкостях. Оскільки міліметрові хвилі можуть бути більш вражені загасанням із-за змішуваних об'єктів, а міліметрові хвилі не проникають через стени та інші перешкоди так само легко, як спектр низьких і середніх частот, який використовується для додатків 4G і DSS, то формування променя може допомогти створити більш надійну динаміку підключення.

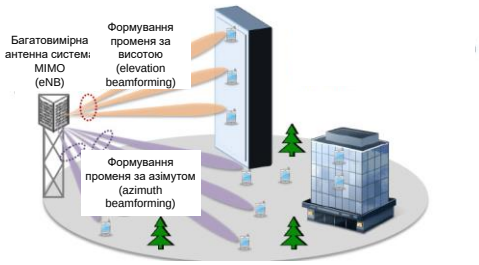


Рисунок 1 – Модель формування променя «Beamforming» на основі багатовимірної антенної ситеми Massive MIMO [1]

Ще одним рішенням проблеми поширення з mmWave є наша можливість використовувати переваги рознесення та мультиплексування, що отримуються від передачі на основі MIMO, для забезпечення більш високої пропускної здатності та більш надійного прийому сигналу на приймальній стороні, що призводить до загального покращення досвіду користувача. Для реалізації технології формування променя «beamforming» використовуються алгоритми, які визначають вагові коефіцієнти і фазові здвиги для кожної антени, таким чином, щоб сигнали від різних антен сумувалися конструктивно в напрямку інтересу користувача і деструктивно в інших напрямках. Це дозволяє підвищити якість зв'язку, збільшити пропускну здатність і підвищити енергоефективність системи.

Для розрахунку оптимальних вагових коефіцієнтів, що задовольняють декількома критеріями або обмеженнями, різні адаптивні алгоритми вже розроблені. Після обчислення вагового вектора w, що відповідає за формування ДС, фільтр просторових частот для всіх напрямків представляється діаграмою випромінювання антени (діаграмою спрямованості) за допомогою виразу

$$P(\theta) = \left| w^H(\theta) a(\theta) \right|^2. \quad (1)$$

У виразі (1) $P(\theta)$ є середня вихідна потужність просторового фільтра при надходженні окремого сигналу одиничної потужності під кутом θ [2]. За наявності відповідного контролю величини і фази w головний лепесток ДС буде спрямований на джерело корисного сигналу, а нулі (в ідеальному випадку) - у напрямку завадових сигналів.

Цифрова технологія формування променя «beamforming» обробляє сигнали на рівні базової смуги, використовуючи цифрові процесори і перетворювачі аналогового сигналу в цифровий і навкпаки (ADC і DAC). Цифровий «beamforming» дозволяє більш гнучко керувати формуванням променів і працювати з декількома частотами одночасно, що забезпечує більш високу продуктивність та ефективність, однак, вимагає великих обчислювальних потужностей і складності обладнання [1,2].

Технологія «Beamforming» також тісно пов'язана з іншими ключовими технологіями у мережах 5G, такими як Massive MIMO та міліметрові

хвилі. У системах Massive MIMO, що використовують велику кількість антен, «beamforming» є основним інструментом для управління просторовими ресурсами та забезпечення високої пропускної здатності. Міліметрові хвилі, з їх короткою довжиною хвилі і високою пропускною здатністю, можуть забезпечити дуже вузькоспрямовані промені, що дозволяє ефективно використовувати «beamforming» для покращення зв'язку та боротьби з загасанням сигналу.

2. Задачі та етапи реалізації технології формування променя «Beamforming»

Схема організаціїї формування променя «Beamforming» включає ряд етапів, а саме:

- виявлення викличного сигналу мобільної станції (МС), прийнятого по широкому променю діаграми спрямованості антени базової станції (БС);
- процедура ідентифікації, автентифікації і прийом запиту від МС на використання радіоресурсу,
- визначення кількості запитів випромінювань, які надійшли від інших МС і знаходяться в межах поточного променю;
- визначення напряму приходу викличного сигналу МС;
- формування вузького променя за необхідним напрямом;
- вирішення колізії, якщо буде виявлено два або більше викличних сигналів МС в межах одного променю діаграми спрямованості антенної решітки базової станції.

Ідея просторово доступу полягає в тому, що весь фізичний простір, в якому може поширюватися корисний сигнал, ділиться на досить вузькі сектори (при 2-мірному просторі) або стерадіани (у 3-мірному), в межах кожного з яких можлива незалежна одночасна передача сигналів від базової станції мобільним користувачам в тому самому спектрі частот. Таким чином, при утворенні таких секторів або стерадіанів можна в N разів використати радіочастотний ресурс. Все це реалізується з використанням N-елементної багатопроменевої антени, що дозволяє паралельно в тому самому спектрі обслуговувати N -абонентських станцій.

Список використаних джерел:

1. Оцінка продуктивності алгоритмів адаптивного формування променю smart-антени для систем мобільного зв’язку 5G / О.В. Андрущенко, І.М. Шумков, М.В. Москалець // Матеріали восьмої Міжнародної науково-технічної конференції «Проблеми електромагнітної сумісності перспективних безпроводових мереж зв’язку (ЕМС-2022)». Харків, ХНУРЕ, 2022. С. 01-04.

2. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. Method Radio Resource Allocation in Cognitive Radio Network. Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham.

УДК 621.396.946

МОДЕЛЬ ОПТИМАЛЬНОГО РОЗМІЩЕННЯ БАЗОВИХ СТАНЦІЙ НА ОСНОВІ ВИКОРИСТАННЯ ГЕНЕТИЧНОГО АЛГОРИТМУ ДЛЯ МЕРЕЖІ МОБІЛЬНОГО ЗВ`ЯЗКУ 5G

Літвінов О.О.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: oleksii.litvinov1@nure.ua,

The purpose of the work is to study the genetic approach to solving the problem of optimal placement of base stations in the fifth generation (5G) mobile communication network. An algorithm for optimizing the placement of base stations has been developed based on a genetic approach, as an example of a search procedure, which uses an element of randomness as a means of carrying out the process of finding a solution among many chromosomes. The developed algorithm is implemented as software, which will allow solving large-scale tasks.

1. Постановка задачі дослідження оптимального розміщення базових станцій у мережі 5G.

На етапі запобіжного планування безпроводової мережі мобільного зв’язку вирішується завдання оптимального розміщення. Завдання стоїть у тому, щоб на заданій території розмістити мінімально можливу кількість базових станцій при підключенні до них з відповідним рівнем якості послуг. Оптимальність розміщення базових станцій і підключення до них абонентів визначається за критерієм мінімальної вартості при наявності ряду обмежень.

Для вирішення даної задачі будемо використовувати сучасний оптимізаційний апарат на основі генетичного підходу. Генетичні алгоритми широко застосовуються для вирішення завдань оптимізації в різних областях науки і техніки [1,2]. На основі генетичного підходу відповідно до отриманої математичної моделі розроблено алгоритм оптимізації розміщення базових станцій. Структурна схема розробленого алгоритму представлено на рис.1. Розглянемо послідовність дій при вирішенні задачі оптимального розміщення базових станцій, що визначається даним алгоритмом.

2. Застосування генетичного алгоритму.

Перший крок генетичного алгоритму полягає у визначенні відповідної вихідної популяції хромосом. Замість звичайного бінарного подання у вигляді множини [0,1], що вимагає двійкових рядків довжиною $m \times k$ і в той же час не гарантує виконання умов (4) і (5), обрано уявлення, в якому кожна хромосома є k -мірним вектором цілих чисел на множині $[1, \mathrm{m}]$.

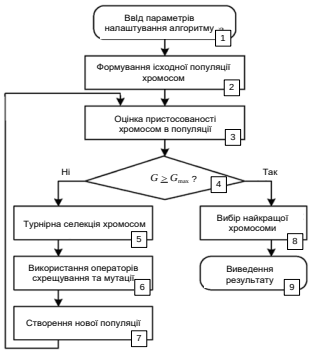


Рисунок 3.1 – Блок-схема генетичного алгоритму

Цілочисленне значення k-й позиції вказує базову станцію, розміщену на m-ому місці кандидата, до якої прикріплений k-й абонент. Якщо, наприклад, $\mathrm{m} = 3$ і $k = 4$, то запис хромосоми у вигляді [1,2,1,3] означає, що: абоненти з номерами 1 і 3 підключені до базової станції, встановленої на місці кандидата 1; абонент 2 підключений до базової станції, встановленої на місці кандидата 2; користувач 4 підключено до базової станції, встановленої на місці кандидата 3. Далі формується вихідна населення особин випадковим вибором заданої кількості хромосом. При цьому популяція є кінцевим безліччю розмірністю N_{pop}. Число особин у популяції залишається постійним протягом усієї роботи генетичного алгоритму.

Після визначення відповідної вихідної популяції хромосом обчислюються функції пристосованості для кожної зі знайдених хромосом. При цьому функції пристосованості завжди набувають невід'ємних значень.

Потім здійснюється перевірка умови завершення завдання. Розв'язання задачі вважається отриманим під час виконання умови

$$G \geq G_{\max}, \tag{1}$$

де G - номер поточного покоління; $G_{\max}$ - максимальна кількість поколінь, задане на початку роботи алгоритму.

Відповідно до (1) пошук мінімального значення цільової функції припиняється після того, як номер поточного покоління особин, створеного в ході роботи алгоритму, досягає значення, що дорівнює заданому максимальному числу поколінь. Після досягнення заданого числа поколінь здійснюється висновок результатів оптимізації розташування базових станцій.

По розрахованим значенням функції пристосування проводиться вибір тих хромосом, які братимуть участь у створенні наступної популяції, тобто нового покоління. За заданою кількістю батьків N_{par} відбирається

певне число хромосом, яким дозволено створювати особин наступного покоління. Якщо всім особинам у популяції дозволено створювати нащадків, то $N_{par} = N_{pop}$, інакше $N_{par} < N_{pop}$. Половина батькивських хромосом вибирається на основі турнірної селекції, при якій особини популяції випадковим чином розбиваються на підгрупи чисельністю по 2 хромосоми в кожній. Потім здійснюється вибір у кожній з підгруп найкращої особини, що має найменшу функцію пристосованості. Хромосоми, що у турнірі, вибираються у складі найкращих особин, впорядкованих за рівнем погіршення функції пристосованості. Половина батьківських хромосом, що залишилася, вибирається випадковим чином з числа хромосом, не задіяних у турнірі.

Така стратегія дає можливість створювати нащадків всіма видами особин, включаючи найкращих і найгірших. Це покращує генетичне розмаїття популяції, підвищує швидкість збіжності на початкових ітераціях алгоритму і дозволяє у випадках уникнути локальних мінімумів. Процес селекції закінчується створенням батьківської популяції.

До заключної стадії роботи алгоритм переходить при виконанні умови визначення найкращої хромосоми, що має найменше значення функції пристосованості серед усіх хромосом, що становлять останнє покоління, і виводиться результат розв'язання задачі. Ця хромосома, отримана в результаті виконання завдання, дозволяє обчислити сумарну вартість комплексу.

Розроблений алгоритм оптимізації розміщення базових станцій на основі генетичного підходу є прикладом пошукової процедури, в якій використовується елемент випадковості як засіб проведення процесу пошуку рішення серед безлічі хромосом.

Розроблений алгоритм реалізований як програмне забезпечення, дозволить вирішувати завдання великої розмірності.

Список використаних джерел:

1. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. Method Radio Resource Allocation in Cognitive Radio Network. Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham.

2. Muliar B, Koliadenko YU., Moskalets M., Loshakov V., Martynchuk O., Ageyev D. Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network. 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022, pp. 1-7.

УДК 004.738.5:004.722 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.032

ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ ПРОТОКОЛУ MATTER ЯК ЗАСОБУ УНІФІКАЦІЇ ПРИСТРОЇВ INTERNET OF THINGS

Муха Р.В.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
e-mail: rostyslav.mukha@nure.ua

It has been proven that smart home devices need to be unified. This helps to simplify the development of devices and enable their use in Matter-compatible IoT devices. The features and functionality of the Matter protocol are presented. It is shown that creating a network based on the Matter standard is a reliable and stable solution. An extended network based on the Matter topology is presented and its components are characterized.

Уніфікація пристроїв «розумного будинку» та підвищення їх сумісності з різними системами є основними завданнями, спрямованими на спрощення розробки пристроїв Internet of Things **(**IoT). Одним з рішень є впровадження протоколу Matter, а також виявлення можливостей його використання в сумісних із Matter пристроях IoT. За підтримки великих технологічних компаній, таких як Apple, Google, Amazon, і Zigbee Alliance, протокол Matter спрощує розробку пристроїв IoT, надаючи єдиний підхід до підключення. Особливості та функціональні можливості Matter наступні [1]:

– уніфікація та інтероперабельність. Технологія має на меті уніфікувати фрагментований ринок пристроїв «розумного будинку», і надає загальний стандарт для спрощення кінцевого рішення для користувача;

– чітка специфікація дозволяє налаштувати спільний зв'язок між будь-якими пристроями, сертифікованими Matter, за умови дозволу користувача;

– використовує сучасні методи та протоколи безпеки, забезпечуючи надійне з'єднання. Здійснює стабільне та швидке локальне з'єднання. Пристрої працюють локально, але стандарт також призначений і для зв'язку з хмарою, коли це необхідно;

– підтримує широкий спектр пристроїв, визначає конкретний набір мережних технологій на основі IP для сертифікації пристроїв.

Створення мережі на базі Matter потребує обрання пристрою або декількох пристроїв за стандартом Matter, та налаштувати граничний роутер для підключення пристроїв [2].

Загальний приклад розширеної топології Matter показано на рис.1.

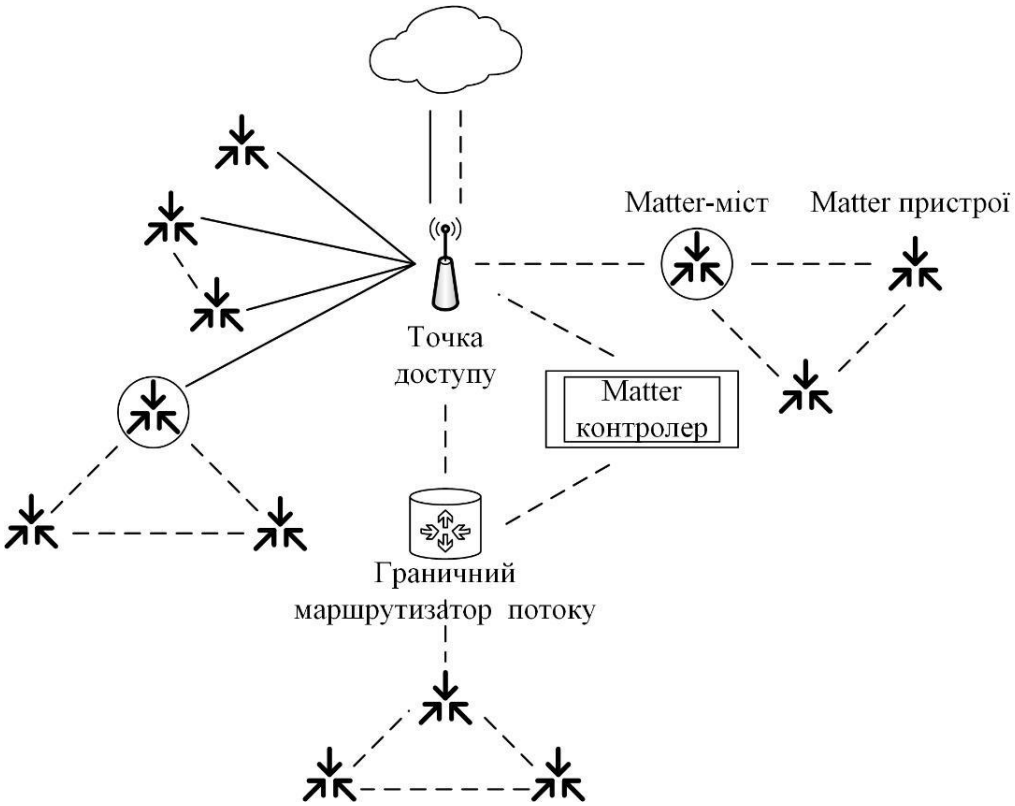


Рисунок 1 – Приклад топології мережі

Основними елементами мережі є:

– міст – пристрій для з'єднання з мережею Matter несумісних пристроїв. Гарантує безпечну і правильну взаємодію з пристроями Matter;

– контролер – вузол в мережі Matter, що використовується для віддаленого керування пристроями через Bluetooth LE та IPv6. контролер Matter використовує Bluetooth LE для налаштування і IPv6 для регулярного обміну даними в мережі Thread або Wi-Fi з іншими пристроями Matter, для зменшення електроспоживання;

– граничний маршрутизатор – мережний пристрій, який координує взаємодію різних мереж IPv6 у системі Matter.

Таким чином, Matter характеризується своєю універсальністю, надійністю та здатністю інтегруватися з різноманітними технологіями, визначаючи себе як передовий стандарт для розумних пристроїв та їх взаємодії в системі Internet of Things.

Список використаних джерел:

1. Belli D., Barsocchi P., Palumbo F. Connectivity Standards Alliance Matter: State of the art and opportunities. *Internet of Things*. 2024. Vol. 25. P. 1–27.

2. Matter’s plan to save the smart home. URL: https://www.theverge.com/22787729/matter-smart-home-standard-apple-amazon (дата звернення: 01.03.2024).

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.034

ЦЕНТРАЛІЗОВАНЕ ЗОНДУВАННЯ ДЛЯ КООРДИНАЦІЇ ТА МОНІТОРИНГУ ВИКОРИСТАННЯ СПЕКТРУ В КОГНІТИВНІЙ МЕРЕЖІ

Оголюк В.В.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім В.В. Поповського,
м. Харків, Україна
e-mail: vadym.oholiuk@nure.ua

A method of centralized spectrum sensing in a cognitive network is proposed, using antennas to detect spectral holes in local regions. This improves the efficiency of frequency utilization by optimizing their distribution in real time. Antenna scanning allows you to accurately determine the available spectrum resources, increasing network performance and facilitating the management of radio frequency resources. This approach facilitates the development of future networks by increasing their efficiency and scalability.

При когнітивному розподілі ресурсів кожна АС мережі повинна безперервно виконувати моніторинг спектра на наявність вільних каналів. Результати аналізу передаються БС, і вона приймає остаточне рішення щодо придатності каналу. При прийнятті рішення БС спирається на результати аналізу спектра, інформацію про місцезнаходження, а також на допоміжну інформацію [1,2]. Необхідно відзначити, що дані задачі повинні бути вирішені в режимі реального часу. Працездатність таких радіомереж в значній мірі залежить від ефективності роботи алгоритмів виявлення незайнятих частотних каналів, при радіомоніторингу [2].

Основною проблемою спектрального зондування є виявлення первинного користувача в зашумленому середовищі. Це складне завдання особливо при низьких значеннях відношення сигнал/шум (SNR) через загасання сигналу та затінення (рис.1) [1].

Рис. 1 – Прихований термінал

Задачу зондування можна охарактеризувати як перевірку гіпотези [2]:

$H_0: y(t) = n(t)$ - первинний користувач відсутній,

$H_1: y(t) = h(t)s(t) + n(t)$ - первинний користувач працює зі спектром.

де $y(t)$ - прийнятий сигнал, $n(t)$– шум в момент часу *t* з дисперсією δ, $s(t)$ - переданий сигнал, який є автокорельований $E[|s(t)|^2] \neq 0$, а $h(t)$ -

коефіцієнт підсилення або затухання каналу. H_0 та H_1 - це гіпотези про наявність шуму та сигналу відповідно. Класичні методи використовують виявлену енергію як індикатор присутності сигналу в каналі.

Процес прийняття рішення виглядає наступним чином [2]:

$$\text{Рішення}\{E[|s(t)|^2] \le V_T \quad H_0, E[|s(t)|^2] > V_T \quad H_1.$$

де V_T – потужність (дисперсія) шуму. Енергію часто оцінюють сумою, яка є неточною оцінкою особливо коли є невелика кількість відліків [2]:

$$E[|y(t)|^2] \approx \frac{1}{N}\sum_{k=1}^{N} \quad |y(t)^2|.$$

Спільні підходи до спектрального зондування використовують інформацію, зібрану всіма приймачами, для визначення наявності сигналу в каналі. Така кооперативна стратегія дозволяє уникнути прихованої термінальної проблеми, в якій передавач когнітивного радіо не в змозі виявити первинного передавача через затінення або затухання, але його передача спричиняє завади для первинної користувацької передачі в первинному приймачеві. Оскільки завади виникають у приймачах, можна уникнути завад від основного приймача. Цей метод виявився практичним лише для телевізійних приймачів.

Спільне зондування спектра потребує декількох датчиків, розподілених на великій площі. Його точність залежить від щільності розміщення сенсорів на площі, оскільки низька щільність призводить до того, що дані, отримані сенсорами, є дуже некорельованими.

На продуктивність схеми прийняття рішень впливає також техніка злиття, що використовується для об'єднання інформації з багатьох джерел.

Припустимо, що:

- є *K* базових станцій зондування когнітивного радіо, які розподілені по місцевості випадковим чином, але їх точні просторові координати відомі. Припустимо, що ці базові станції можуть спілкуватися через проводову мережу і підтримка мережі управління не викликає проблем;

- усі вони здатні використовувати одну і ту ж ділянку спектру.

Визначимо *S*, матрицю зондування розмірністю *K* × *N*, яка визначається *N* нещодавно зондованих зразків *K* базових станцій, $y_i(k)$ - k -й зразок, знятий *i*-ю антеною:

$$S = (y_1(1)\, y_1(2) \ldots y_2(1)\, y_2(2) \ldots\ldots\ldots\ldots\ldots)$$

У випадку H_0, коли присутній лише шум, внутрішній добуток всіх рядків буде оцінкою автокореляційної функції шуму. Оскільки припускається, що вибірки шуму є взаємно некорельованою, ця величина буде близькою до нуля.

У випадку H_1, внутрішній добуток рядів буде пропорційний автокореляції переданих сигналів. Визначимо постійний коефіцієнт підсилення каналу для періоду зондування. Оскільки шум є некорельованим з переданим сигналом, то матимемо:

$$S_m \cdot S_n = \sum_{i=1}^{N} y_m(i) \times y_n(i)$$

$$= \sum_{i=1}^{N} \left((h_m s(i) + N_m(i)) \times (h_n s(i) + N_n(i))\right) \approx$$

$$\approx h_m h_n \times N \times E[|s(t)|^2], \quad m \neq n.$$

Таким чином, використовуючи дану схему можливе спільне вимірювання спектру. В цій схемі використано просторову інформацію антен для знаходження спектральних дір в локальних регіонах.

Рис. 2 – Графіки залежності ймовірності помилки від ВСШ

Аналіз ефективності запропонованого методу проведено в середовищі Matlab за допомогою імітаційного моделювання. В якості критерію ефективності обрана ймовірність загальної помилки $p_{пом}$, яка за допомогою імітаційного моделювання розраховувалася як сума помилково прийнятих рішень поділена на кількість дослідів. На рис. 2 надано графіки залежності ймовірності помилки $p_{пом}$ від відношення сигнал/шум (ВСШ). З даних графіків видно, що при низьких значення ВСШ від -5 дБ до - 1 дБ ймовірність помилки практично однакові мають що метод децентралізованого зондування, що метод централізованого зондування. Зі збільшенням ВСШ (вище -1 дБ) ймовірність помилки при централізованому зондуванні різко зменшується, і при значеннях ВСШ вище 7 дБ становить менше 10^{-15}.

Список використаних джерел:

1. Cardoso L. S., Debbah M., Bianchi P., Najim J. Cooperative spectrum sensing using random matrix theory. IEEE ISWPC, May 2008. P. 334–338.

2. Поповский В. В., Коляденко А. В. Метод обнаружения сигналов первичных пользователей в когнитивных радиосетях. *Радіоелектроніка, інформатика, управління*. 2017. № 2. С. 7–15. DOI: 10.15588/1607-3274-2017-2-1.

УДК 621.391:004.77 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.037

ОЦІНКА ПРОДУКТИВНОСТІ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ У МОБІЛЬНИХ AD HOC МЕРЕЖАХ

Пастушенко І.Ю., Черненко Д.С.
Науковий керівник – к.т.н., доц. Мельнікова Л.І.
Харківський національний університет радіоелектроніки, каф.ІКІ
м. Харків, Україна
e-mail: ihor.pastushenko@nure.ua

This scientific report evaluates the performance of routing protocols in mobile Ad hoc networks (MANET), focusing on the challenges posed by the dynamic topology and limited bandwidth typical of these networks. It highlights the inefficiency of traditional wired network protocols in MANET and emphasizes the importance of addressing scalability, security, network lifetime, and the growing demands of applications. The study compares the performance of the multi-path Dijkstra algorithm in the MP-OLSR protocol with the OLSR protocol. The findings suggest that MP-OLSR outperforms OLSR in terms of packet delivery and average delay, especially at higher node speeds, by effectively distributing packets across multiple paths and eliminating unnecessary transmissions through a loop detection mechanism.

Специфіка мереж Ad hoc (MANET) полягає в тому, що їхня топологія постійно змінюється через переміщення вузлів мережі в просторі або зміни умов поширення радіосигналу. Крім цього, для Ad hoc-мереж, як і для будь-яких безпроводових систем, характерні обмежені смуга пропускання та зона радіовидимості. В результаті протоколи та технічні рішення, що використовуються в класичних провідних мережах передачі даних, наприклад, централізована маршрутизація з ієрархією заздалегідь призначених маршрутизаторів, в мережах Ad hoc виявляються неефективними та не забезпечують потрібну продуктивність [1].

У цьому контексті маршрутизація даних є великою дослідницькою задачею, оскільки має бути охоплений значний перелік питань: масштабованість, безпека, час життя мережі, бездротова передача, потреби додатків, що постійно зростають [2].

У літературі наводиться детальне порівняння протоколів маршрутизації у мережах Ad hoc шляхом імітаційного моделювання їхньої роботи у різних сценаріях роботи мережі [3, 4].

Підвищити продуктивність Ad-hoc мереж можна за рахунок використання алгоритмів багатошляхової маршрутизації, які, на відміну від алгоритмів маршрутизації найкоротшого маршруту, дозволяють балансувати завантаженість мережі, збільшуючи її продуктивність в 1,5-2 рази, додатково забезпечуючи відмовостійкість мережі.

Для підвищення якості обслуговування в мережах MANET у роботі запропоновано використання багатошляхового алгоритму Дейкстри в протоколі маршрутизації MP-OLSR.

Проведено порівняння продуктивності протоколів MP-OLSR та OLSR у різних у різних сценаріях роботи мережі. На рис.1 представлено відсоток успішної доставки даних за обома протоколам. OLSR має трохи кращий відсоток доставлених пакетів у порівнянні з MP-OLSR (близько 3%) лише на швидкості 1 м/с (3,6 км/год). Причиною тому збільшення кількості шляхів одночасної передачі, зростає ймовірність виникнення колізій на рівні MAC. Ці міжшляхові впливи можуть бути усунені шляхом використання багатоканальної апаратури, що гарантує різні смуги частот кожного з шляхів. У цьому випадку використовується тільки один частотний канал, тому протокол MP-OLSR має більше втрачених пакетів через колізію на рівні MAC.

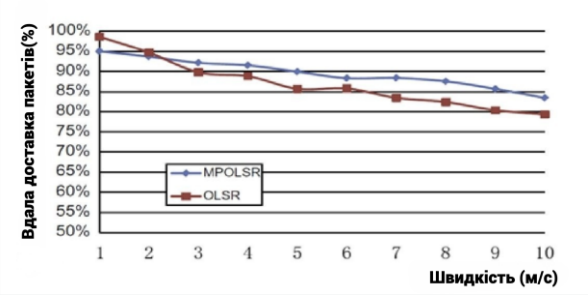


Рисунок 1 – Доставка пакетів протоколами MP-OLSR та OLSR у ситуації з 81 вузлом та 4 джерелами

Проте, зі збільшенням швидкості руху вузлів, зв'язки поміж них стають більш нестабільними, і в мережі з'являється більше «петель». Відсоток вдалої доставки протоколу OLSR швидко зменшується і він поступається MP-OLSR. У порівнянні з невеликим виграшом у відсотку вдалої доставки (близько 5% на високій швидкості), багатошляховий протокол працює набагато краще за показниками середньої затримки, ніж одношляховий протокол (як показано на рис.2). Затримка OLSR у 4 рази більша, ніж MP-OLSR, починаючи зі швидкості 4 м/с (14,4 км/год). Затримка з кінця в кінець включає затримку розповсюдження від відправника до одержувача і затримку в черзі в кожному транзитному вузлу. Багатошляховий протокол може мати більш тривалу затримку розповсюдження тому, що деякі пакети направляються більш довгими маршрутами.

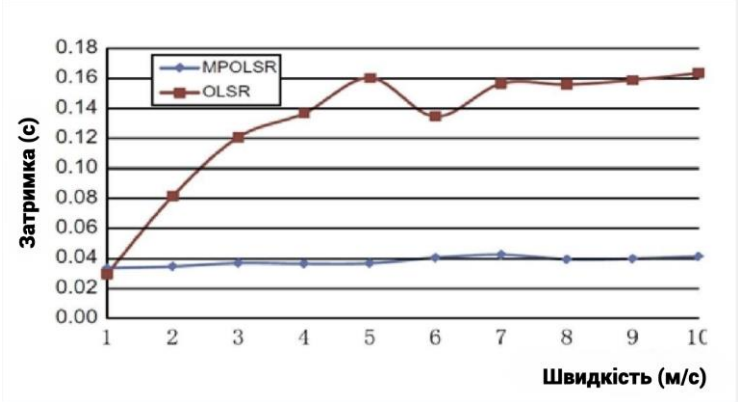


Рисунок 2 – Середня затримка від відправника до одержувача в ситуації з 81 вузлом та 4 джерелами

Однак, що важливіше те, що він (MP-OLSR) може ефективно зменшити затримку в черзі розподіляючи пакети різними шляхами. У доповненні пропонований механізм визначення "петель" також здатний зменшити непотрібні передачі, виключивши "петлі". Як показано, MP-OLSR має значно менший час затримки в черзі в порівнянні з OLSR.

Застосування багатошляхового алгоритму Дейкстри в протоколах багатошляхової маршрутизації може суттєво покращити продуктивність мережі, оскільки MP-OLSR вузли можуть виконувати багатошляхову маршрутизацію та визначення «петель».

Список використаних джерел:

1. Clausen, T. Generalized Mobile Ad Hoc Network (MANET) [Текст] / T. Clausen, C. Dearlove // Request for Comments. – 2009. – № 5444. – С. 28.

2. Badis, H. Qolsr multi-path routing for mobile ad hoc networks based on multiple metrics: bandwidth and delay [Текст] / H. Badis, K. A. Agha / Vehicular Technology Conference. – 2004. – № 15. – С. 64.

3. Abolhasan, M. A review of routing protocols for mobile ad hoc networks [Текст] / M. Abolhasan, T. Wysocki // Ad Hoc Networks. – 2004. – № 2 (1). – С. 22.

4. Tarique, K. E. Survey of multipath routing protocols for mobile ad hoc networks [Текст] / K. E. Tarique // Journal of Network and Computer Applications. – 2009. – № 32 – С. 43.

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.040

РЕЗУЛЬТАТИ ПОПЕРЕДНЬОЇ ОБРОБКИ ГОЛОСОВОГО СИГНАЛУ В СИСТЕМАХ АВТЕНТИФІКАЦІЇ

Пастушенко М.С., Петраченко М.О.
Науковий керівник – к.т.н., проф. Пастушенко М. С., каф. ІКІ
Харківський національний університет радіоелектроніки
м. Харків, Україна
e-mail: mykola.pastushenko@nure.ua, maksym.petrachenko@nure.ua

The report examines the current scientific problem of preprocessing a voice signal in authentication systems, which is currently implemented in the field of amplitude-frequency characteristics of the processed data. To increase the efficiency of voice signal preprocessing procedures, it is proposed to use its phase data. The phase data of a voice signal in the time domain is known to be in the form of sawtooth signals of unknown duration. It has been established that during the phase change period there are one or two harmonics. The selection of signals with one harmonic can be performed using linear approximation and the chi-square criterion. Further research will be focused on identifying the degree of the polynomial for phase signals with two harmonics.

В доповіді розглядається актуальна наукова задача попередньої обробки голосового сигналу в системах автентифікації, яка зараз виконується в області амплітудно-частотних характеристик даних, що обробляються. Для підвищення ефективності попередньої обробки запропоновано використовувати фазові дані голосового сигналу, які мають стійку апріорну інформацію щодо їх форми.

Відомо, що голосові дані це полігармонійний сигнал. Тому під час аналізу фазової інформації голосового сигналу було застосовано метод, що базується на розкладанні сигналу на гармоніки і подальшому вивченні їх фазових характеристик [1]. Виявлено, що сигнал може мати різні кількості частот на періоді зміни фази: одну частоту, дві частоти, або рідше - фазовий сигнал може бути руйнований.

Мета дослідження полягала в аналізі одночастотних і двохчастотних сигналів, тому увага була зосереджена на цих типах. У випадку одночастотного сигналу можна провести пряму апроксимацію частоти. Однак у випадку двохчастотного сигналу спостерігається плавна зміна частоти, і гармоніка апроксимується поліномом більш високого ступеня.

Для експериментального аналізу були створені штучні сигнали - як одночастотний, так і двохчастотний, з метою розробки методу ідентифікації цих типів сигналів. Для оцінки відповідності використовувався критерій хі-квадрат [2].

Наступним кроком був аналіз для однієї гармоніки. При апроксимації частоти прямою лінією виявилися значні похибки, що внесли відхилення в

результати. Проте, за критерієм хі-квадрат, апроксимація однієї гармоніки все ж пройшла, хоч і з помітною похибкою.

Під час оцінки використовувався критерій хі-квадрат для аналізу відповідності результатів експерименту очікуваним значенням. Параметри цього критерію були застосовані як до різниці між фазовим та апроксимованим сигналом. В якості розподілу аналізу використовувався рівномірний розподіл. Результати моделювання свідчать, що з ймовірністю 0.92 критерій хі-квадрат дозволяє виявити одночастотний фазовий сигнал.

В подальшому були виконані дослідження сигналу з двома гармоніками. При обробці за допомогою критерію хі-квадрат з використанням апроксимації прямої лінії було виявлено, що результати не відповідають аналізованому критерію. Це значить що з використанням лінійної апроксимації з високою імовірністю можливо виявити двохчастотний фазовий сигнал.

Однак на цей час не визначена ступень поліному, який з високою імовірністю дозволяв би здійснювати апроксимацію двохчастотного сигналу. Це складає завдання подальших наукових досліджень в галузі попередньої обробки голосових сигналів.

Список використаних джерел:

1. M.Pastushenko, Ya.Krasnozheniuk, M. Zaika (2020) "Investigation of Informativeness and Stability of Mel-Frequency Cepstral Coefficients Estimates based on Voice Signal Phase Data of Authentication System User" International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkiv, Ukraine, pp. 1-5.

2. Проакіс Дж. Г., Манолакіс Д. Г. Цифрова обробка сигналів: принципи, алгоритми та застосування. Видавництво Пірсона, 2018.

УДК 004.722:004.8 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.042

ХМАРНІ ОБЧИСЛЕННЯ ТА ШТУЧНИЙ ІНТЕЛЕКТ

Подлісний Г.С
Науковий керівник – доц. Штангей С.В
Харківський національний університет радіоелектроніки
61166, Харків, пр. Науки, 14,
кафедра Інфокомунікаційної інженерії ім. В.В. Поповського,
e-mail hlib.podlisnyi@nure.ua.

Recent advancements in cloud computing have revolutionized the landscape of artificial intelligence (AI) by providing scalable infrastructure and resources for AI development and deployment. Usage of AI with cloud computing is developing rapidly. Cloud services play a huge role in facilitating the integration of AI algorithms, enabling efficient model training, inference, and deployment at scale. Moreover, cloud-based AI solutions offer flexibility, accessibility, and cost-effectiveness, driving innovation and integration across various industries. The synergistic relationship between cloud computing and AI is reshaping technological landscapes and fueling progress in diverse domains.

У сучасному світі все більше використовують штучний інтелект. Вже понад 77% компаній використовують або планують впровадити цю технологію [1]. Зі зростанням попиту, з’являється потреба у великій потужності обчислень, зберіганні даних та гнучкості. Все це можуть надати хмарні сервіси та обчислення.

Хмарні обчислення в сфері штучного інтелекту (ШІ) представляють собою важливу парадигму, яка змінює спосіб, яким розробляються, впроваджуються та використовуються інтелектуальні системи. Платформи хмарного обчислення забезпечують інфраструктуру для розгортання інтелектуальних додатків та сервісів, спрощуючи процес розробки та забезпечення доступності для широкого кола користувачів. Популярні хмарні платформи, такі як Amazon Web Services, Microsoft Azure та Google Cloud Platform, пропонують набір інструментів та сервісів для розробки та рогортання інтелектуальних застосунків, що враховує в себе машинне навчання, обробку природної мови та комп'ютерний зір. До головних переваг застовування хмарних сервісів для ШІ відноситься: економність, висока продуктивність та маштабованість. Економність полягає у можливості підприємств знизити витрати на інфраструктуру, оскільки хмарні сервіси не потребують значних вкладень у власне обладнання та обслуговування. Це дозволяє компаніям сконцентруватися на розвитку своїх інноваційних проектів, замість витрат на інфраструктуру. Висока продуктивність визначається доступом до високоефективних обчислювальних ресурсів, які дозволяють ефективно тренувати та виконувати складні моделі штучного інтелекту [2]. Це особливо важливо в умовах швидкозмінних вимог ринку та потреби в оперативній реакції на

нові тенденції. Масштабованість означає, що хмарні сервіси легко можуть змінювати обсяги ресурсів відповідно до зростання потреб користувача або підприємства, забезпечуючи гнучкість і швидку адаптацію до змін у вимогах. Окрім цього, організації, які використовують один сервіс хмарних послуг, за потреби можуть обирати інших провайдерів. Таким чином, понад 39% керівників компаній обирають додаткові платформи, через потребу у додатковій потужності [4]. Такий підхід дозволяє підприємствам оптимізувати витрати та забезпечує високий рівень продуктивності.

Синергічна взаємодія хмарних технологій та моделей ШІ використовується у багатьох галузях, таких як: медицина, фінанси, маркетинг, транспорт. У медицині є застосування у прогнозі захворювань, розробки нових лікарських засобів та персоналізованого лікування. Фінансова сфера використовує прогнозування ринкових тенденцій та виявлення шахрайства. У сфері маркетингу, ШІ генерує персоналізовану рекламу для споживачів та оптимізує маркетингові компанії. В сфері транспорту, синергія хмарних технологій та моделей штучного інтелекту відіграє роль у вдосконаленні логістики та маршрутного планування. Також слід згадати великі мовні моделі, які використовує вже понад 60% бізнесів, для покращення взаємодії із користувачами [3]. Але такі моделі , як (Generative Pre-trained Transformer) та BERT (Bidirectional Encoder Representations from Transformers), а також їхні варіації потребують значних обчислювальних ресурсів для своєї роботи, що зазвичай перевищує можливості окремих компаній. Рішенням є використання хмарних сервісів для забезпечення необхідної потужності та інфраструктури для цілодобової роботи цих моделей. Такий підхід дозволяє підприємствам інтегрувати великі мовні моделі у свої продукти та сервіси, поліпшивши взаємодію з користувачами.

Список використаних джерел:

1. Статистика ШІ за 2024 рік: зростання, використання та впровадження. *MSPoweruser*. URL: https://mspoweruser.com/uk/ai-statistics/ (дата звернення: 11.03.2024).
2. AI cloud platforms: A comprehensive guide to AI and cloud platform integration | octavius.ai. *Octavius AI*. URL: https://octavius.ai/ai-cloud-platforms/ (date of access: 11.03.2024).
3. AI in customer service statistics for 2023. *businessolution.org*. URL: https://businessolution.org/ai-in-customer-service-automation-statistics/ (date of access: 11.03.2024).
4. Franklin B. 40 cloud computing stats and trends to know in 2023 | Google Cloud Blog. *Google Cloud Blog*. URL: https://cloud.google.com/blog/transform/top-cloud-computing-trends-facts-statistics-2023 (date of access: 11.03.2024).

УДК 621.391:621.396.946 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.044

СИНТЕЗ МЕТОДІВ ПОЛЯРИЗАЦІЙНО-ЧАСОВОЇ ОБРОБКИ СИГНАЛІВ В СИСТЕМАХ МОБІЛЬНОГО ЗВ'ЯЗКУ НАСТУПНИХ ПОКОЛІНЬ

Савченко Р.О., Москалець М.В.
Науковий керівник – д.т.н., проф. Москалець М.В.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: roman.savchenko1@nure.ua, mykola.moskalets@nure.ua

Algorithms similar to spatial-temporal processing can be used for polarization-temporal processing of mobile station signals. The solution to the problem of synthesis of polarization-time signal processing methods from the standpoint of optimal stochastic control is considered. Procedures for observation, status and evaluation of the vector of weighting coefficients for adaptive antenna arrays are presented. On the basis of AAR, if necessary, it is possible to implement a spatially-polarization separated reception, which will minimize losses due to multibeam.

Боротьба з завадами шляхом поляризації є перспективним методом обробки, особливо в тих випадках, коли завади діють у межах головної пелюстки діаграми спрямованості приймальної антени. Задачі поляризаційно-часової обробки, так само як і просторово-часової, можуть бути вирішені різними способами. Так, оцінюючи поляризацію сигналів і завад, можна побудувати систему управління поляризаційним базисом приймання антени, що забезпечує безперервну ортогоналізацію, того базису по відношенню до завади. Рішення цієї задачі може бути складним, особливо при нелінійній ситуації, коли умови теореми про поділ не виконуються [1].

Більш конструктивним у даному випадку виявляється підхід, коли оцінці підлягають не самі параметри поляризації спостережуваних сигналів і завад, а значення оптимальних вагових коефіцієнтів $w_i(t)$ при $i=1,2$ для антенної системи, що складається з двох взаємно ортогональних антенних елементів, включених між антенними елементами і загальним суматором і забезпечують, наприклад, мінімум середньоквадратичного відхилення (МСКВ) прийнятого сигналу $y(t)$ від еталонного y_E. Очевидно, вибір тих чи інших значень вагових коефіцієнтів $\mathrm{w}_i(t)$ призводить до відповідних перетворень поляризаційного базису антеною системи, що, в свою чергу, визначає рівень частково поляризованих сигналів і завад на виході загального суматора, але не чинить впливу на рівень безполяризованого «білого» шуму, що потрапляє в смугу частот прийому.

Рівняння стану вектору вагових коефіцієнтів (ВВК), спостереження і оцінки $\hat{\mathrm{w}}(k)$ в даному випадку аналогічні відповідним рівнянням для адаптивних антенних решіток (ААР), [2,3]:

$$d\hat{w}_i(t)/dt = -a_i(t)\hat{w}_i(t) + \sum_{j=1}^{N} 2K_{ij}(t)V_H^{-1}\left[\mathrm{y}_{\Э}(\mathrm{t}) - y(t)\right]x_i(t) =$$

$$= -a_i(t)\hat{w}_i(t) + 2V_H^{-1}\mathrm{v}(\mathrm{t})\sum_{j=1}^{N} K_{ij}(t)x_i(t), \qquad (1)$$

Структурна схема пристрою оцінки вагових коефіцієнтів, що згідно з (1) здійснює поляризаційно-часову обробку, представлена на рис.1.

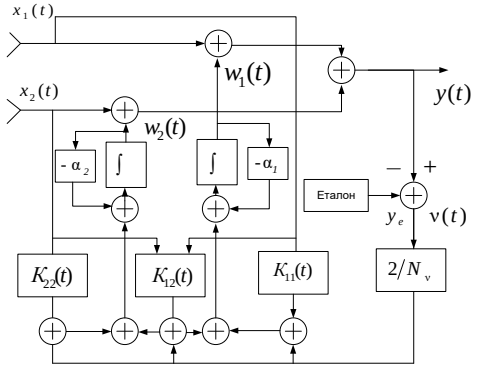


Рисунок 1 – Схема пристрою оцінки вагових коефіцієнтів, що здійснює поляризаційно-часову обробку сигналів

Проаналізуємо ефективність розглянутих задач для різних значень кута δ, що є половиною центрального кута сфери Пуанкаре і точки з'єднання, які відповідають значенням поляризації сигналу і завади. Для аналізу виберемо коефіцієнт, що показує, наскільки рівень сигналу по відношенню до завади на виході системи більший, ніж на вході:

$$\eta = (d_{свих}/(d_{з\_вих} + d_{швих}))/(d_{с\_вих}/(d_{звх} + d_{швх})), \qquad (2)$$

де $d_{с\_вих} = W^T R_c W$, $d_{з\_вих} = W^T R_з W$, $d_{швых} = W^T W$ – нормовані по одиничному значенню спектральної щільності потужності неполяризованого "білого" шуму рівні сигналу, завади і самого шуму відповідно. Значення оптимальних вагових коефіцієнтів визначимо з матричного рівняння Вінера-Хопфа $W = R_{xx}^{-1} r_{xy}$, де $R_{xx} = R_c + R_n + R_ш$, а $R_c, R_n, R_ш$ – кореляційні матриці сигналу, завади і шуму відповідно; r_{xy} – матриця взаємної кореляції між векторами прийнятого і еталонного сигналів.

Незважаючи на те, що процедура аналізу заснована на рівнянні фільтра Вінера, вона для даного випадку може застосовуватися, оскільки фільтр Калмана володіє тією ж ефективністю. Залежність η від d_n

представлена на рис.2, звідки видно, що із зменшенням рівня шуму ступінь придушення завади зростає.

Ефективність зростає також при збільшенні відмінності поляризації сигналу та завади (зі збільшенням δ).

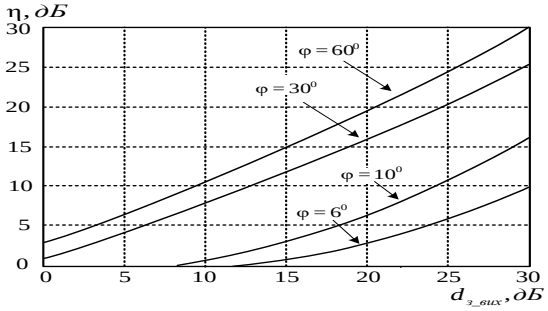


Рисунок 2 – Графіки залежностей коефіцієнта завадозахисту η від значення відмінності кута приходу сигналу і завади $\Delta\theta$

Характерно, що навіть при малій відмінності в поляризаціях сигналу і завади (при $\delta \le 30^0$) можна досягти рівня придушення 20 дБ і більше, що відповідно підвищує якість електромагнітної доступності.

Список використаних джерел:

1. Koliadenko, Y., Moskalets, M., Badieiev, V., Savchenko, R. Method Radio Resource Allocation in Cognitive Radio Network. In: Dovgyi, S., Trofymchuk, O., Ustimenko, V., Globa, L. (eds) Information and Communication Technologies and Sustainable Development. ICT&SD 2022. Lecture Notes in Networks and Systems, vol 809. Springer, Cham, pp 102–115. DOI: https://doi.org/10.1007/978-3-031-46880-3_7

2. Loshakov, V., Moskalets, M., Ageyev, D., Drif, A., Sielivanov, K. Adaptive space-time and polarisation-time signal processing in mobile communication systems of next generations. Lecture Notes on Data Engineering and Communications Technologies, 2021, 48, P.469-488. DOI: 10.1007/978-3-030-43070-2_21

3. Muliar B, Koliadenko YU., Moskalets M., Loshakov V., Martynchuk O., Ageyev D. Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network. 2022 IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T), 2022, pp. 1-7.

УДК 621.391:004.7 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.047

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЇ 5G НА ПЛАТФОРМИ IoT

Сазонов Б.О.
Науковий керівник - доц. каф. ІКІ Сабурова С.О.
Харківський національний університет радіоелектроніки, каф. ІКІ
М. Харків, Україна
e-mail: bohdan.sazonov@nure.ua

The article explores the potential of 5G technology in the context of the Internet of Things (IoT). It examines the impact of high-speed, low-latency and low-power (HL-LP) 5G communication on the development of smart systems in the home environment. The use of 5G in Broad Band - IoT (BB-IoT) tssechnology's opens up new perspectives for expanding the functionality and efficiency of intelligent systems. The article examines the benefits and challenges of implementing 5G in smart homes, such as high bandwidth, low latency, improved scalability, and network security.

В інтелектуальних IoT системах (індустрії, бізнес-структурах, приватних смартбудинках і т.д) питання якості відіграє ключову роль. Це стосується якісної реалізації окремих компонентів (наприклад, датчики, пристрої автоматизації, мережне обладнання і т.д.), загальної архітектури та інтеграції IoT системи. Існують вимоги QoS системи до параметрів якості в технологіях нових поколінь, які є важливі також на платформи BB-IoT.

1. Надійність: Система повинна працювати надійно без відмов. Нестабільність може призвести до втрати функціональності та зниження зручності для користувачів.
2. Безпека: Забезпечення захисту від несанкціонованого доступу до системи та даних користувачів є критично важливим.
3. Енергоефективність: Для пристроїв, які працюють в режимі постійного підключення до мережі (наприклад, датчики), важливо, щоб вони ефективно використовували енергію та могли працювати на довготривалій батареї.
4. Масштабованість: Система повинна бути здатною впоратися з ростом кількості підключених пристроїв та зміною вимог користувачів.
5. Сумісність: Важливо, щоб пристрої та системи були сумісними між собою, щоб уникнути проблем з інтеграцією та взаємодією.
6. Легкість у використанні: Інтерфейс користувача повинен бути інтуїтивно зрозумілим та легким у використанні, щоб користувачі могли легко керувати своїм інтелектуальним домом.
7. Загальна продуктивність: Система повинна працювати ефективно та без затримок у відповіді на команди користувача.
8. Приватність даних: Збір та обробка даних користувачів

повинна відбуватися відповідно до правил конфіденційності та захисту особистих даних.

Ці параметри якості допомагають забезпечити ефективну працездатність та безпеку для користувача інтелектуального дому.

Якщо швидкість 4G сягає в середньому 10 Мб/с, а максимум — до 1 Гб/с, то 5G має середню швидкість від 50 Мб/с, а максимальну — в межах 1-10 Гб/с. За параметрами якості 5G має меншу затримку, тобто період часу між відправкою та отриманням інформації. У 4G затримка — 200 мс, а у 5G — 1 мс. Це дозволяє охоплювати більшу кількість пристроїв Інтернет речей.

На рисунку 1 показано схема функціонування системи 4G/5G на платформи IoT.

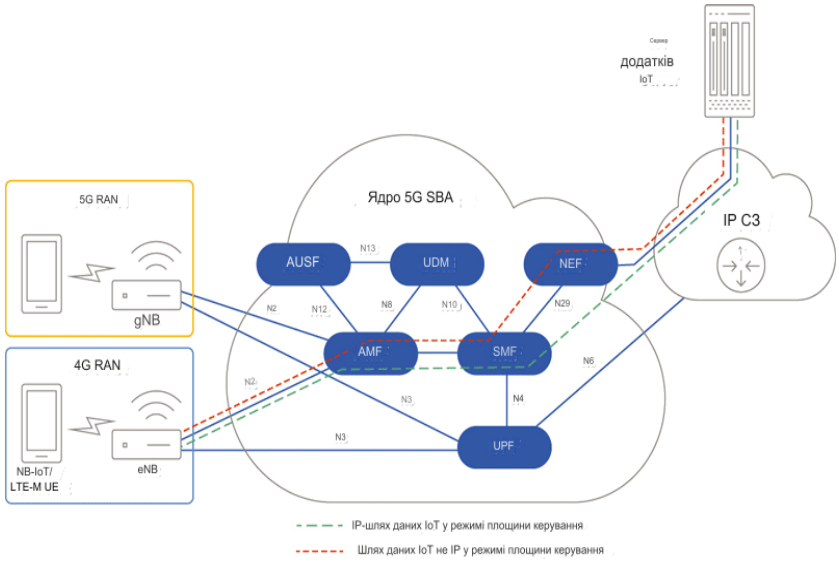


Рисунок 1 – Схема функціонування систем 4G /5G на платформи IoT

Висновки:

1. Впровадження технології 5G системи на платформи IoT дозволяє збільшити спектр пристроїв, а також значно зробити це доступнішим для споживачів та суспільства.

2. Мобільна 5G мережа здатна розвивати швидкість у десять разів швидше ніж 4G з найбільш стійким та надійним забезпеченням параметрів якості BB-IoT послуг.

Список використаних джерел:

1. Інтернет речей: мережна архітектура та архітектура безпеки URL: https://www.bizmaster.xyz/2020/12/internet-rechei-merezheva-arkhitektura-ta-arkhitektura-bezpeky.html.

Як розвивається 5G у світі: кейси та перспективи. URL: https://hub.kyivstar.ua/articles/yak-rozvivayetsya-5-g-u-sviti-kejsi-ta-perspektivihttps://hub.kyivstar.ua/articles/yak-rozvivayetsya-5-g-u-sviti-kejsi-ta-perspektivi.

УДК 621.396.946

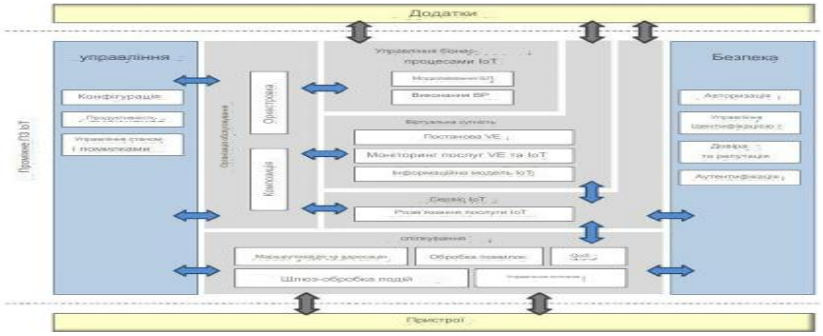
ДОСЛІДЖЕННЯ МЕТОДІВ УПРАВЛІННЯ ПАРАМЕТРАМИ ЯКОСТІ NB-IoT 4G ПОСЛУГ

Сізов Я.А.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: yaroslav.sizov@nure.ua

In addition, research was carried out on methods for managing services, which is an important warehouse for any IoT system. It has been noted that there are a number of functional models for managing IoT services, one of which is IoT-A. The IoT-A model was chosen, which is an expanded version of the IoT MCE model and consists of seven horizontal levels, supplemented by two vertical ones (control and security). An analysis of methods for ensuring effective control of NB-IoT4G services, measurements and development, and an assessment of the parameters of the capacity of NB-IoT 4G services with the help of schedules was carried out.

Internet of Things (IoT) є мережею фізичних об'єктів, або "речей", вбудованих з електронікою, програмним забезпеченням, датчиками та з'єднаннями, які дозволяють цим об'єктам збирати та обмінюватися даними. Технологія IoT забезпечує об'єкти можливостями бути контрольованими віддалено через фіксовані або мобільні мережі створюючи нові перспективи для автоматизації управління та контролю [1].

Дослідження методів управління послугами показали, що на цей час впроваджені важливи складови будь-якої IoT системи. Для ефективного управління послугами необхідно мати чітку функціональну модель. Існують кілька функціональних моделей управління IoT послугами, одна з яких - IoT-A. Вибрана модель IoT-A є розширеною версією моделі IoT MCE та складається з семи горизонтальних рівнів, які доповнюються двома



вертикальними (управління і безпека) [1].

Рисунок 1 – Функціональна модель IoT-A управління послугами [1]

Прикладом застосування IoT є Web-речі (WEBofThings - WoT), які забезпечують взаємодію та контроль різних інтелектуальних об'єктів

("речей") з використанням стандартів і механізмів Інтернет мережі. WoT передбачає реалізацію концепції IoT на прикладному рівні з використанням вже існуючого архітектурного рішення, орієнтованого на розробку web-застосування. Велика кількість різних типів мереж та даних призвела до необхідності перенесення 4G мережею різного виду трафіку з високими вимогами що о якості обслуговування. При цьому задачами управління головними параметрами якості для трафіку Інтернет-речей є забезпечення контролю та моніторингу за параметрами якістю: кругової затримки, коливанням та втратами пакетів.

Параметри якості кругової затримки включають в себе затримку поширення, затримку в черзі на маршрутизаторі та затримку, яку вносить активний елемент. Нормований параметр якості - час затримки на маршрутизаторах завжди менше 1 мс, коли середня довжина пакету - 800 байт при швидкості до 100 Мбіт/с з оцінкою - 4 бали, якщо канали не перевантажені в ЧНН (час найбільшого навантаження). Рівень показника втрати пакетів у ЧНН визначається кількістю пакетів, які відкидаються мережею під час передачі. Коефіцієнт втрати пакетів залежить від кількості втрачених пакетів та кількості пакетів, отриманих успішно. Наприклад, якщо кількість переданих пакетів – 300000, втрачених (або пошкоджених) – 407, при цьому кількість доставлених пакетів – 299593, то коефіцієнт втрати пакетів буде дорівнювати: 0.013% - 4 бали.

Згідно вимогами Рекомендацій MCE-T, G.1020 коефіцієнт втрачених IP-пакетів за нормою, $К_{PER}$ – 0,001% – 5 балів, $К_{PER}$ = 0,01% – 4 бали, $К_{PER}$ = 0,1% – 3 бали, $К_{PER}$ – більше 0,1% – 2 бали.

Для підвищення якості обслуговування зі забезпеченням виконання нормативних рівнів в час найбільш навантаження (ЧНН) система управління фіксує причини зниження якісних характеристик та приймає рішення в необхідності збільшення станційних та транспортних ресурсів в межах виконання класів обслуговування за вимогами системи якості QoS (Quality of Service).

Висновки: Проведено аналіз методів забезпечення ефективного контролю послуг NB-IoT4G мережі на прикладному рівні та розглянуто схематично рішення задачі управління параметрами якості на основі моделі IoT-A послуг. Представлено розрахунки та оцінка параметрів якості NB-IoT 4G мережі з побудуванням графіків.

Список використаних джерел:

1. Кухарчук М.М., науковий керівник доц. Сабурова С.О., Моніторинг послуг NB IoT (LTE)//Матеріали 25-го Міжнародного молодіжного форуму «Радіоелектроніка та молодь в XXI столітті». – Харків: ХНУРЕ, – 2021. – С.30-31.

УДК 004.738.5:004.272]:656.13

КЛАСТЕРИЗАЦІЯ В МЕРЕЖАХ VEHICULAR AD-HOC NETWORKS

Соловйов П.В.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки
кафедра ІКІ ім В.В. Поповського
м. Харків, Україна
e-mail: pavlo.soloviov@nure.ua

The article analyzes the VANET technology and shows the problems that arise in the network. It is proved that the need to introduce a hierarchical network structure is aimed at effective network management. The basic and modified structures of the VANET network are analyzed. The influence of clustering on the effectiveness of collision prevention in a VANET is studied. The analysis showed that the use of clustering can significantly affect the number of potential collisions compared to the baseline scenario, which in turn will reduce the emergency situation on the roads and increase the efficiency of road traffic.

Дослідження в галузі автомобільного зв'язку для інтелектуальних транспортних систем активно розвиваються, що підкреслює важливість і актуальність технології VANET (Vehicular Ad-Hoc Networks), як основи для створення ефективних і безпечних транспортних систем.

Технологія VANET стикається з низкою викликів: затримками в передаванні критично важливих повідомлень, захистом даних, проблемами масового розсилання, якістю обслуговування, керуванням потоками даних, перевантаженням мережі та розподілом ресурсів [1].

Ці проблеми підкреслюють необхідність впровадження ієрархічної структури, де транспортні засоби з подібними характеристиками об'єднуються в кластери, що дасть змогу розділити велику мережу на кластери для ефективного керування [2]. Кожен автомобіль виступає в ролі портативного роутера, використовуючи бортові пристрої On Board Units (OBU) для комунікації, що підкреслює потребу в ефективній організації мережної інфраструктури через кластеризацію.

Базову структуру кластера у VANET представлено автомобілями, об'єднаними в кластери з виділеним лідером кластера, що координує комунікацію всередині кластера та з іншими кластерами (рис. 1).

Голову кластера становить автомобіль, який позначено як Cluster Head (CH), об’єкт кластеру позначено Cluster Member (CM), шлюз кластеру позначено Cluster Gateways (CG).

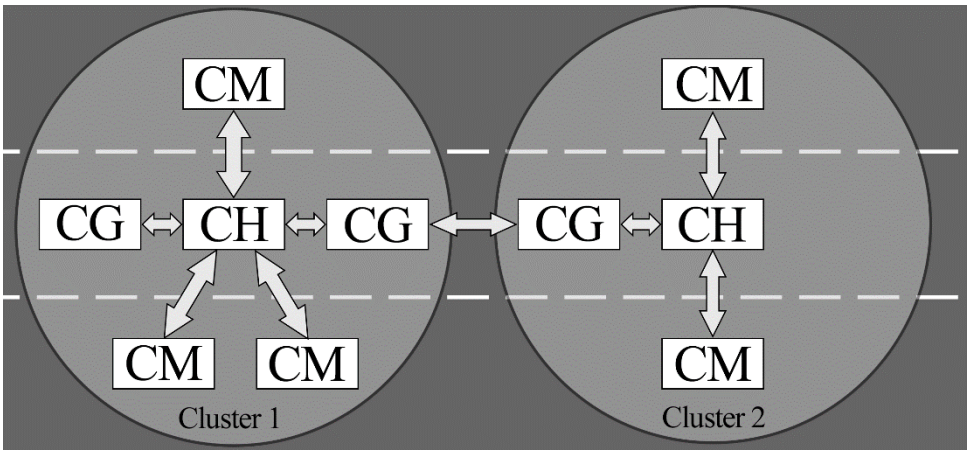


Рисунок 1 – Базова структура кластера в VANET

У базовому сценарії розгортання автомобілі випадковим чином розміщуються на дорозі і рухаються з індивідуальними швидкостями, обраними випадково в діапазоні від 60 до 100 км/год. На кожному часовому кроці автомобілі оновлюють свої позиції на основі поточної швидкості. Якщо відстань між двома автомобілями стає меншою за критичну, вони зменшують свою швидкість на 20%, щоб запобігти зіткнення.

У роботі проведено дослідження впливу кластеризації на ефективність запобігання зіткненням у мережі VANET. Симуляцію реалізовано з метою порівняння двох сценаріїв: базового - без застосування кластеризації, і модифікованого, де автомобілі об'єднуються в кластери на основі їх географічного положення та швидкості. В обох сценаріях проаналізовано динаміку попереджених зіткнень протягом 100 часових кроків.

Результати продемонстровано у вигляді кумулятивних графіків (рис. 2), що відображають загальну кількість попереджених зіткнень залежно від часу.

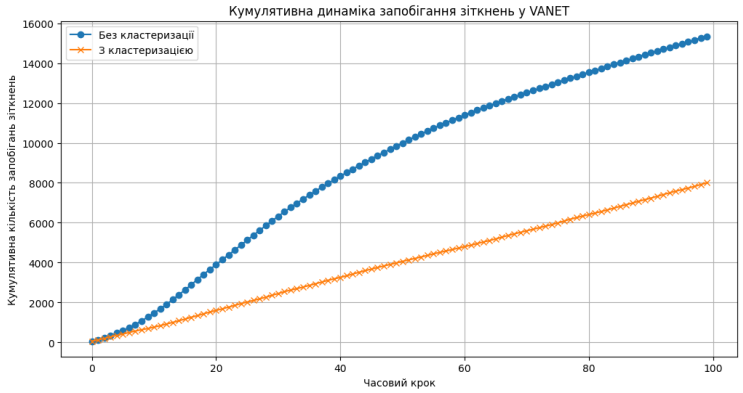


Рисунок 2 – Результати симуляції транспортного руху з кластеризацією та без кластеризації

Ефективність кожного сценарію оцінюється за кількістю потенційних зіткнень, яким вдалося запобігти за час симуляції.

Основний напрям дослідження спрямовано на оцінку потенційного зниження ризику зіткнень завдяки координованому керуванню швидкістю і положенням автомобілів у рамках кластерів. Вихідні дані для дослідження: кількість машин 250; довжина дороги – 10 км; радіус – 100 м; критична відстань – 10 м; максимальний розмір кластеру 25 м.

На початковому етапі автомобілі аналізують навколишній простір у радіусі дії та формують кластери, розмір яких не перевищує заданий максимум. У кожному кластері обирається лідер. Усередині кластера автомобілі рухаються з усередненою швидкістю всіх його учасників, що сприяє зниженню ризику зіткнень між ними. Зв'язок між автомобілями дає змогу оперативно реагувати на зміни в динаміці руху.

Результати симуляції показують, що застосування кластеризації у VANET може істотно знизити кількість потенційних зіткнень порівняно з базовим сценарієм. Це свідчить про те, що кластеризація сприяє ефективному та безпечному керуванню дорожнім рухом завдяки оптимізації взаємодії між об'єктами мережі.

Таким чином в дослідженні показано, що кластеризація у мережах VANET є ефективним інструментом для підвищення безпеки дорожнього руху. Розробка і впровадження алгоритмів кластеризації в системі керування транспортними потоками відкриває нові перспективи для зниження аварійності на дорогах і підвищення загальної ефективності дорожнього руху.

Список використаних джерел:

1. El Mouna Zhioua G., Tabbane N., Labiod H., Tabbane S. A fuzzy multi-metric QoS-balancing gateway selection algorithm in a clustered VANET to LTE advanced hybrid cellular network. *IEEE Transactions on Vehicular Technology*. 2015. Vol. 64(2). P. 804–817.

2. Wang Z., Liu L., Zhou M., Ansari N. A position based clustering technique for ad hoc inter vehicle communication. *IEEE Transactions on Systems, Man, and Cybernetics*.2008. Vol. 38.є P. 201–208.

УДК 621.396:004.738

АНАЛІЗ FRONTHAUL У ЦЕНТРАЛІЗОВАНІЙ АРХІТЕКТУРІ МОБІЛЬНОЇ МЕРЕЖІ

Солоділов В.В.
Науковий керівник – к.т.н., доц. Токар Л.О.
Харківський національний університет радіоелектроніки, кафедра ІКІ ім В.В. Поповського,
м. Харків, Україна
e-mail: viktor.solodilov@nure.ua

It is proven that the construction of a mobile network based on a centralized architecture causes the organization of a more demanding and expensive transport network FH. The data transfer rate was analyzed to evaluate the centralized architecture of the mobile network. 4G and 5G networks are used. The difference between the maximum possible transfer rate and the actual rate at which the 5G network will increase the existing high FH requirements is shown. It has been proven that the requirements for networks will increase due to the increase in bandwidth.

Побудова мобільної мережі, заснованої на централізованій архітектурі, спрямована на зниження експлуатаційних та капітальних витрат; централізацію BBU (Battery Backup Unit), що значно полегшує реалізацію способів спільної обробки; досягнення в галузі процесорних технологій та віртуалізації, що дозволило реалізувати обробку основної смуги частот на процесорах загального призначення GPP (Green Power Processor) [1]. Однак такий підхід спричиняє організацію більш вимогливої та дорогої транспортної мережі FH (fronthaul).

Архітектура такої мобільної мережі передбачає обробку основної смуги частот на рівні PHY (Physical Layer) та MAC (Medium Access Control). Конвергенція пакетних даних виконується у хмарному центрі обробки, підключеному до ядра через BH (backhaul). Центр хмарної обробки обмінюється цифровими даними із BS (Base Station) FH з використанням стандарту CPRI (Common Public Radio Interface) [2]. FH поділено на мережу агрегації, яка збирає і розподіляє дані по багатьох BS, і так звану "останню милю", яка є кінцевим каналом зв'язку з BS [3].

Однак, переваги хмарної мережі досягаються ціною вимогливої транспортної мережі FH до пропускної здатності, низької затримки та джитера. Таким чином, дані обмінюються у FH та відповідають оцифрованому набору вибірок комплексного сигналу I/Q. Швидкість передачі даних, необхідну для такого централізованого варіанту побудови, розраховано за формулою:

$$R = 2 \cdot N_A \cdot N_Q \cdot f_s \cdot \gamma \ , \qquad (1)$$

де N_A – кількість антен, f_s – частота дискретизації, N_Q – роздільна здатність квантувача в бітах. Коефіцієнт 2 враховує I і Q фази сигналу, а γ являє собою службові дані, що вносяться FH, або додаткові сигнали керування. У роботі проаналізовано швидкість передачі даних для оцінки централізованої архітектури мобільної мережі (табл. 1). Використовуються максимальні та робочі параметри мобільних мереж [4].

Таблиця 1 – Аналіз швидкостей передачі даних

Швидкість передачі даних	Мережа $5G_{max}$	Мережа $5G_{real}$	Мережа $4G_{max}$	Мережа $4G_{real}$
R, біт/с	$7\,182 \cdot 10^9$	$7\,182 \cdot 10^9$	$4\,902 \cdot 10^6$	$2\,451 \cdot 10^6$

У дослідженні показано мережу 4G та мережу 5G з використанням максимально можливих параметрів з робочими характеристиками.

Аналіз показав різницю між максимально можливою швидкістю передачі і реальною швидкістю, у якій мережа 5G підвищить існуючі високі вимоги до FH. Зокрема, використання масивних методів MIMO (Multiple Input Multiple Output) з великою кількістю антенних елементів лінійно збільшить швидкість передачі даних FH, при цьому фактична швидкість передачі даних збільшиться більш ніж на три порядки. Крім того, частота дискретизації залежить від загальної пропускної здатності і роздільна здатність квантувача повинна бути досить високою з урахуванням високої динаміки сигналу в часовій області 5G [5].

Таким чином, очікується, що вимоги до мереж збільшаться в основному за рахунок трьох покращень: впровадження масивної технології MIMO, використання більш високих носіїв та збільшення пропускної здатності.

Список використаних джерел

1. Aldhaibani O., AL-Jumaili M. H., Raschella A., Kolivand H, Preethi A. Peace a centralized architecture for autonomic quality of experience oriented handover in dense networks. *Computers & Electrical Engineering*. 2021. Vol. 94. P. 1–12.

2. Oliva A., Hernández J. A., Larrabeiti D., Azcorra A. An overview of the CPRI specification and its application to C-RAN based LTE scenarios. *IEEE Communications Magazine*. 2016. Vol. 54 (2). P. 152–159.

3. Do H. M., Gregory M. A., Li S. SDN-based wireless mobile backhaul architecture: Review and challenges, *Journal of Network and Computer Applications*. 2021. Vol. 189. P. 1–24.

4. Mohammed S. H. K., Rodriguez J. Backhauling/Fronthauling for future. Wireless systems: John Wiley & Sons Ltd, 2017. 218 p.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

УДК 004.056

ІННОВАЦІЙНІ ПІДХОДИ ДО ЗАХИСТУ БЕЗПЕКИ ІНФОРМАЦІЙНИХ КАНАЛІВ КЕРУВАННЯ В КОНТЕКСТІ РОЗВИТКУ АВТОНОМНИХ СИСТЕМ

Вельма І.Ю.,
Науковий керівник – д. т. н., проф. Мартинчук О. О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: ihor.velma@nure.ua

In the modern world, the importance of autonomous systems such as unmanned aerial vehicles (UAVs), autonomous vehicles, and robots is growing. These systems require reliable and secure management, but they also become targets for potential cyberattacks. As a result, there is a need for innovative approaches to protecting the information channels of these systems.

На сьогоднішній день інформаційні канали керування автономними системами стають дедалі більш вразливими перед кіберзагрозами через низку факторів. Перш за все, зростаюча кількість підключених пристроїв і збільшення обсягу передаваних даних створюють більше можливостей для зловмисників здійснювати атаки. Відкритість інтернету дещо ускладнює захист каналів передачі даних, оскільки це може створювати можливості для зловмисників перехоплювати інформацію, що передається через мережу. Зловмисники можуть використовувати різноманітні методи для атак на інформаційні канали керування. Наприклад, вони можуть перехоплювати передані дані, щоб отримати доступ до конфіденційної інформації або внести зміни до команд, що керують автономною системою. Можливість модифікувати або блокувати передачу даних може призвести до серйозних наслідків, таких як аварії або порушення безпеки, зокрема в областях, де автономні системи залежать від неперервного зв'язку з операторами або іншими системами для нормальної роботи. Загрози для інформаційних каналів керування автономними системами наголошують на необхідності постійного вдосконалення заходів безпеки та використання передових технологій для захисту цих каналів від кібератак.

Одним із перспективних напрямків є застосування штучного інтелекту та машинного навчання для виявлення та запобігання кібератак на інформаційні канали керування. Це означає застосування алгоритмів та моделей, які навчаються на основі великої кількості даних, щоб автоматично виявляти аномальну або підозрілу активність у мережі та реагувати на неї. Наприклад, системи машинного навчання можуть аналізувати трафік мережі для виявлення незвичайних патернів або атак, а потім надавати відповідні заходи безпеки, такі як блокування підозрілих джерел або виявлення зламаної аутентифікації. Ці методи дозволяють

покращити ефективність захисту інформаційних каналів керування та забезпечити вчасну реакцію на потенційні загрози кібербезпеки.

Додатковим інноваційним підходом є використання блокчейн-технологій для створення безпечних та недоступних до модифікації інформаційних каналів керування. Блокчейн може забезпечити захист від фальсифікації та змін даних, що передаються між автономними системами та їхніми контролерами.

Блокчейн - це розподілена база даних, яка зберігається на кожному пристрої в мережі, і що містить набір записів, які називаються блоками. Кожен блок містить інформацію, час та дату, а також посилання на попередній блок у ланцюжку, що робить його неможливим для зміни без зміни всіх попередніх блоків у ланцюжку. Це робить блокчейн особливо відповідним для створення безпечних інформаційних каналів. [1]

Коли мова йде про інформаційні канали керування в автономних системах, блокчейн може забезпечити безпеку від фальсифікації та несанкціонованого доступу. Наприклад, дані, що передаються між автономними пристроями та їхніми контролерами, можуть бути записані у блокчейні. Це робить їх неспроможними до модифікації або видалення без відома всіх учасників мережі. Крім того, блокчейн може забезпечити захист від зловмисників, оскільки будь-яка спроба змінити дані буде легко виявлена завдяки системі реєстрації та підтвердження транзакцій.

Використання блокчейн-технологій для створення безпечних та недоступних до модифікації інформаційних каналів керування є потужним інноваційним рішенням, яке може допомогти забезпечити безпеку та надійність в управлінні автономними системами.

Застосування інноваційних підходів до захисту інформаційних каналів керування вже має практичні застосування. Наприклад, деякі компанії вже використовують системи аналізу великих даних для виявлення загроз та аналізу поведінки систем.

У сучасному світі захист інформаційних каналів керування автономних систем стає все більш важливою проблемою. Інноваційні підходи, такі як застосування штучного інтелекту та машинного навчання, а також використання блокчейн-технологій, можуть допомогти підвищити ефективність захисту та забезпечити безпеку та надійність управління автономними системами.

Список використаних джерел:

1. Блокчейн (blockchain, ланцюжок блоків). URL: https://alpari.com/ru/beginner/glossary/blockchain/ (дата звернення: 01.03.2024)

УДК 004.032.26:004.056]:004.773.3

ВИКОРИСТАННЯ НЕЙРОННИХ МЕРЕЖ ДЛЯ ВИЯВЛЕННЯ ТА КЛАСИФІКАЦІЇ ШАХРАЙСЬКИХ ПОВІДОМЛЕНЬ У ЕЛЕКТРОННІЙ ПОШТІ

Вельма І.Ю.
Науковий керівник – д. т. н., проф. Мартинчук О. О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: ihor.velma@nure.ua

In today's digital world, email phishing has become a serious threat to users and organizations. Malicious actors employ various methods and techniques to deliver fraudulent messages, attempting to deceive recipients and gain access to their confidential data or financial resources. Consequently, there is a need for effective methods of detecting and classifying phishing emails.

Використання нейронних мереж є одним з перспективних напрямків у розв'язанні проблеми виявлення та класифікації шахрайських повідомлень у електронній пошті. Нейронні мережі, зокрема глибокі нейронні мережі, є потужним інструментом у сфері кібербезпеки завдяки їх здатності аналізувати великі обсяги даних та виявляти складні зв'язки та патерни. Глибокі нейронні мережі складаються з багатьох шарів нейронів, які обробляють вхідні дані на різних рівнях абстракції. Це дозволяє їм автоматично виявляти навіть тонкі та складні закономірності в даних, які можуть бути важко виявити за допомогою традиційних методів. Наприклад, глибокі нейронні мережі можуть аналізувати текстові повідомлення у електронних листах та виявляти підозрілі ключові слова, фрази або шаблони, що вказують на можливість шахрайства. Однією з переваг використання нейронних мереж є їх здатність до самонавчання. Це означає, що мережа може вдосконалювати свої навички на основі нових даних, які вона отримує, що дозволяє підтримувати високий рівень точності та ефективності виявлення шахрайських повідомлень навіть у змінному середовищі. Таким чином, використання нейронних мереж, зокрема глибоких нейронних мереж, є потужним інструментом для виявлення та класифікації шахрайських повідомлень у електронній пошті, і цей підхід може значно полегшити роботу при боротьбі з кіберзагрозами в цій сфері.

Для виявлення та класифікації шахрайських повідомлень застосовуються різноманітні архітектури нейронних мереж, такі як згорткові нейронні мережі (CNN), рекурентні нейронні мережі (RNN) та їхні комбінації. Методи передбачення на основі нейронних мереж можуть використовувати як текстові дані повідомлень, так і додаткові характеристики, такі як адреси електронної пошти, метадані повідомлень та інші атрибути.

Основна ідея згорткових нейронних мереж (CNN) полягає у тому, щоб вони могли автоматично вивчати корисні функції (ознаки) з вхідних даних. Це відбувається за рахунок використання фільтрів (які також називають ядром або маскою), які згортаються по всій вхідній матриці даних для виділення особливостей. У процесі навчання мережі ваги цих фільтрів автоматично оптимізуються таким чином, щоб вони могли ефективно розпізнавати корисні ознаки. Однією з ключових переваг згорткових нейронних мереж є їхній потенціал для автоматичного виявлення локальних шаблонів у вхідних даних [1].

Основна ідея рекурентних нейронних мереж полягає у використанні зворотного зв'язку, що дозволяє інформації передаватися з одного кроку до наступного. Кожен часовий крок рекурентної мережі обчислює вихід на основі введених даних та попереднього стану. Це дозволяє їм враховувати контекст та історію даних при роботі з послідовностями. Однією з ключових переваг рекурентних нейронних мереж є їх здатність до моделювання довгострокових залежностей у послідовностях даних [1].

Дослідження використання нейронних мереж для виявлення та класифікації шахрайських повідомлень показали високу ефективність цих методів. Нейронні мережі здатні автоматично виявляти характерні ознаки шахрайських повідомлень та відокремлювати їх від легітимних. Застосування нейронних мереж дозволяє знизити кількість фальшивих позитивів та підвищити точність виявлення шахрайських повідомлень.

Додатковою перевагою використання нейронних мереж є їхня здатність до адаптації до нових видів шахрайства та змін у технологіях шахрайства. Це робить їх ефективним інструментом для захисту від постійно змінюючихся загроз у сфері електронної пошти.

Використання нейронних мереж для виявлення та класифікації шахрайських повідомлень у електронній пошті виявляється як обіцяний підхід, що дозволяє підвищити ефективність захисту користувачів та організацій від кіберзлочинності. Результати досліджень свідчать про високу ефективність цих методів та їхню здатність адаптуватися до нових загроз, що робить їх важливим інструментом у боротьбі з електронним шахрайством.

Список використаних джерел:

1. McMillan C. The Connectionist Scientist Game: Rule Extraction and Refinement in a Neural Network / C. McMillan, M.C. Mozer, P. Smolensky // Proc. XIII Annual Conf of the Cognitive Science Society, Hillsdale, NJ,
USA. – 2001.

УДК 004.85:004.056

РОЛЬ НАВЧАННЯ З ПІДКРІПЛЕННЯМ У ПІДВИЩЕННІ ЕФЕКТИВНОСТІ СИСТЕМ ЗАХИСТУ ВІД ЕЛЕКТРОННОГО ШАХРАЙСТВА

Вельма І.Ю.,
Науковий керівник – д. т. н., проф. Мартинчук О. О.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: ihor.velma@nure.ua

In today's digital age, where technology permeates every aspect of our lives, cybersecurity has emerged as a paramount concern. With the exponential growth of online transactions, communication, and data storage, the threat of electronic fraud, commonly known as cybercrime, has become more pervasive and sophisticated than ever before. In response to this evolving landscape, organizations worldwide are continuously striving to fortify their defense mechanisms against cyber threats.

Навчання з підкріпленням (reinforcement learning) є методом машинного навчання, який базується на використанні системи нагород та покарань для навчання агента. У контексті кібербезпеки, цей підхід може бути дуже корисним, оскільки дозволяє створювати адаптивні та ефективні системи захисту, які вчаться на власних помилках та уникають їх у майбутньому. У сфері кібербезпеки, навчання з підкріпленням може бути використане для навчання систем виявлення загроз або іншого програмного забезпечення взаємодіяти з ними. Наприклад, агент може отримувати позитивну нагороду за виявлення підозрілого трафіку та відповідне реагування на нього, або негативну нагороду за пропуск потенційно шкідливих дій. Один з головних переваг навчання з підкріпленням в кібербезпеці є можливість адаптувати систему захисту до змінюючихся умов і загроз. Система може навчитися реагувати на нові види атак або змінювати свою стратегію захисту відповідно до нових обставин. Це дозволяє забезпечити більш ефективний захист від кібератак та зменшити ймовірність успішних атак. Крім того, навчання з підкріпленням допомагає зрозуміти, які дії є найбільш ефективними в конкретних ситуаціях. Аналізуючи реакції системи на різні види загроз, можна виявити слабкі місця та вдосконалити стратегії захисту [1].

Проведення симуляцій та тренувань дозволяє нейромережі отримати практичний досвід виявлення та реагування на потенційні загрози електронного шахрайства в контрольованих обставинах. Під час симуляцій відтворюються ситуації, що можуть виникнути в реальному житті, проте в контрольованому середовищі. Наприклад, можна використовувати програмне забезпечення для моделювання атак на комп'ютерні мережі або імітацію спам-атак на електронну пошту. Спеціалістам з кібербезпеки

дається можливість взаємодіяти з цими сценаріями, аналізувати їх і реагувати на них, не ризикуючи безпекою реальних систем. Тренування включає в себе систематичну практику та навчання нейромережі засобам виявлення та протидії електронному шахрайству. Це може бути проведено у формі рольових ігор, симуляційних вправ або інтерактивних тренажерів. Під час тренувань нейромережа отримує можливість працювати з реальними інцидентами, навчаючись розпізнавати загрози та вживати необхідні заходи для їх подолання.

Навчання нейромережі на реальних прикладах є дієвим методом для покращення розуміння конкретних загроз електронного шахрайства та їх реальних наслідків. Використання реальних прикладів електронного шахрайства дозволяє персоналу отримати практичний досвід у роботі з нейромережами. Це допомагає їм краще зрозуміти як нейромережі можуть застосовуватися для виявлення та протидії кіберзагрозам. Робота з реальними випадками електронного шахрайства дозволяє персоналу аналізувати реальні наслідки кібератак. Це допомагає їм краще зрозуміти масштаб та серйозність потенційних загроз та прийняти відповідні заходи захисту. Робота з реальними прикладами надає персоналу можливість навчитися практичним навичкам розробки та налаштування нейромереж для виявлення та запобігання кіберзагрозам.

Оновлення навчальних програм у сфері кібербезпеки є критично важливим процесом для забезпечення ефективної підготовки персоналу до боротьби зі сучасними кіберзагрозами. Швидкі технологічні зміни в кіберпросторі вимагають постійного оновлення навчальних програм, щоб вони відповідали сучасним методам та інструментам захисту. Наприклад, із зростанням використання штучного інтелекту та машинного навчання в кібератаках, навчальні програми повинні включати в себе вивчення цих технологій для розпізнавання та протидії їхнім використанням в атаках. Нові методи атак вимагають розробки та вдосконалення стратегій оборони. Оновлені навчальні програми повинні враховувати ці стратегії та навички для ефективного запобігання та виявлення кіберзагроз.

Навчання з підкріпленням може стати потужним інструментом в підвищенні ефективності систем захисту від електронного шахрайства. Використання випереджаючих стратегій та урахування практичних аспектів навчання може допомогти створити адаптивні та надійні системи захисту, які здатні ефективно протистояти сучасним кіберзагрозам.

Список використаних джерел:

1. Навчання з підкріпленням у машинному навчанні. URL: https://evergreens.com.ua/ua/articles/reinforcement-learning.html (дата звернення: 28.02.2024)

УДК 621.391:004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.063

ВИРІШЕННЯ ЗАВДАННЯ ОПТИМАЛЬНОГО ВИБОРУ ЗАСОБІВ ЗАХИСТУ ДЛЯ КОРПОРАТИВНОЇ КОМП'ЮТЕРНОЇ МЕРЕЖІ НА ОСНОВІ МЕТОДУ АНАЛІЗУ ІЄРАРХІЙ

Гонтар Д.Ю., Пшеничних С.В.
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В., каф. ІКІ
Харківський національний університет радіоелектроніки
м. Харків, Україна
e-mail: daria.hontar@nure.ua

This document presents a variant of solving the problem of optimal selection of security tools to create an effective integrated information security system for a small computer network of an enterprise using the T. Saaty hierarchy analysis method. The main optimality criteria are the residual risk and the level of implementation costs. In the course of the work, a hierarchical system was built, the priorities of each of the criteria were calculated, and the global priorities of the proposed security measures were determined. Based on the data obtained, the optimal complex for a given computer network of an enterprise was proposed.

Велике різноманіття технічних і програмних засобів захисту інформації ставить завдання оптимального їх вибору для створення ефективної комплексної системи захисту інформації (КСЗІ). При розробці звертається увага на такі параметри, як залишковий ризик після її впровадження та рівень витрат на реалізацію. Метою даної роботи є використання методу аналізу ієрархій (МАІ) Т. Сааті, задля визначення оптимального комплекту програмно-технічних засобів забезпечення захисту від кіберзагроз для невеликої комп'ютерної мережі підприємства, яка складається зі 100 персональних комп'ютерів та двох файлових серверів. В таблиці 1 представлено перелік найпоширеніших кіберзагроз на комп'ютерну мережу та ризики їх реалізації, параметри для обрахування яких було визначено методом експертних оцінок.

Таблиця 1 – Можливі загрози безпеці та можливі збитки від їхньої реалізації на інтервалі часу один рік

Загроза	Ймовірність реалізації	Можливі збитки від реалізації, грн.	Ризик від реалізації, грн.
Витік конфіденційної інформації (загроза 1)	0,8	1800000	1440000
Несанкціоноване вторгнення в мережу (загроза 2)	0,6	500000	300000
Вірусна атака (загроза 3)	0,9	2900000	2610000

В таблиці 2 відображено перелік запропонованих засобів захисту, їх вартість та можливості запобігання обраним загрозам впродовж одного року, які також були визначені на основі експертних оцінок.

Таблиця 2 – Засоби захисту від загроз безпеки, вартості їхньої реалізації та можливості запобігання загрозам на інтервалі часу один рік

Засіб захисту	Вартість реалізації, грн.	Витрати на експлуатацію, грн.	Можливість запобігання загрозі		
			витоку конфіденційної інформації	несанкціонованого вторгнення в мережу	вірусної атаки
Logpoint SIEM (засіб 1)	138453	36000	0,5	0,8	0
ESET NOD32 Antivirus (засіб 2)	20088	0	0	0	0,9
ActivTrack Professional (засіб 3)	890712	34000	0,8	0	0
Quantum Rugged 1595R (засіб 4)	71857	44400	0,5	0,7	0,3

На рисунку 1 наведено розроблену ієрархічну систему, де на кожному рівні представлено критерії, які використовуються для оцінки альтернативних варіантів відповідно до головної мети [1]. Для зручності розрахунків для кожного елементу було визначено умовне позначення та індекси: перший визначає рівень у ієрархії, а другий – порядковий номер показника на певному рівні.

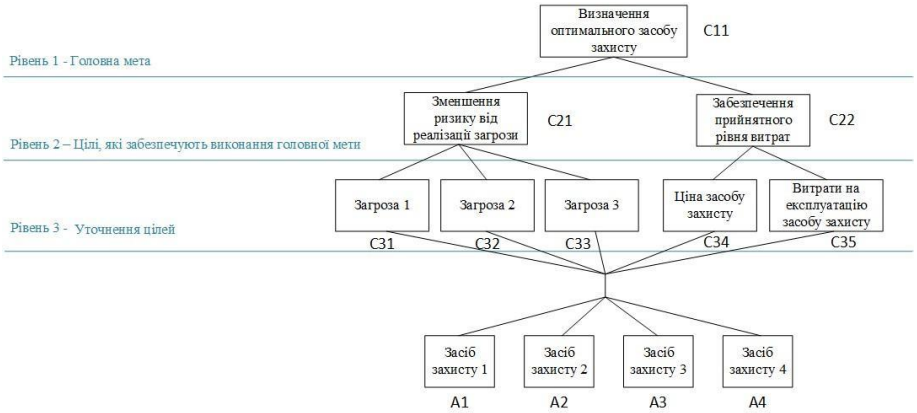
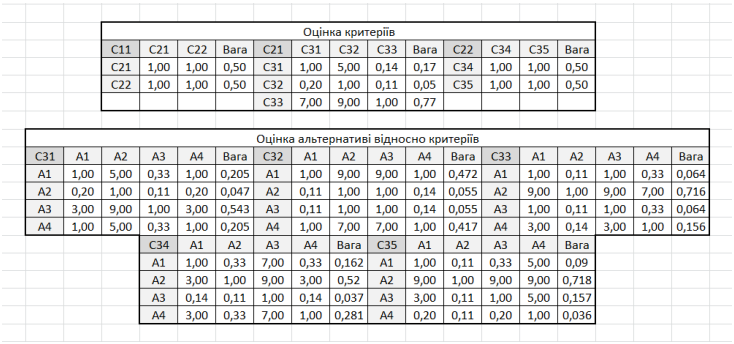


Рисунок 1 – Ієрархія для визначення оптимального засобу захисту

Наступним кроком є оцінка критеріїв за допомогою попарного порівняння за шкалою від 1 до 9 для визначення їх відносної значущості до критерію вищого за рівнем. Після цього було обчислено вагу кожного

критерію, яка знаходиться як нормоване середнє геометричне елементів матриці [2]. Результат проведених обчислень представлено на рисунку 3.



Оцінка критеріїв

C11	C21	C22	Вага	C21	C31	C32	C33	Вага	C22	C34	C35	Вага
C21	1,00	1,00	0,50	C31	1,00	5,00	0,14	0,17	C34	1,00	1,00	0,50
C22	1,00	1,00	0,50	C32	0,20	1,00	0,11	0,05	C35	1,00	1,00	0,50
				C33	7,00	9,00	1,00	0,77				

Оцінка альтернативі відносно критеріїв

C31	A1	A2	A3	A4	Вага	C32	A1	A2	A3	A4	Вага	C33	A1	A2	A3	A4	Вага
A1	1,00	5,00	0,33	1,00	0,205	A1	1,00	9,00	9,00	1,00	0,472	A1	1,00	0,11	1,00	0,33	0,064
A2	0,20	1,00	0,11	0,20	0,047	A2	0,11	1,00	1,00	0,14	0,055	A2	9,00	1,00	9,00	7,00	0,716
A3	3,00	9,00	1,00	3,00	0,543	A3	0,11	1,00	1,00	0,14	0,055	A3	1,00	0,11	1,00	0,33	0,064
A4	1,00	5,00	0,33	1,00	0,205	A4	1,00	7,00	7,00	1,00	0,417	A4	3,00	0,14	3,00	1,00	0,156

C34	A1	A2	A3	A4	Вага	C35	A1	A2	A3	A4	Вага
A1	1,00	0,33	7,00	0,33	0,162	A1	1,00	0,11	0,33	5,00	0,09
A2	3,00	1,00	9,00	3,00	0,52	A2	9,00	1,00	9,00	9,00	0,718
A3	0,14	0,11	1,00	0,14	0,037	A3	3,00	0,11	1,00	5,00	0,157
A4	3,00	0,33	7,00	1,00	0,281	A4	0,20	0,11	0,20	1,00	0,036

Рисунок 3 – Результати обчислення ваг елементів ієрархії

На основі отриманих результатів було розраховано підсумкову вагу для кожного із запропонованих засобів захисту за допомогою адитивної згортки локальних ваг альтернатив за окремими критеріями з урахуванням ваг цих критеріїв [2]. Результати проведених обчислень представлено у таблиці 3.

Таблиця 3 – Результати обчислень підсумкових ваг для кожного із засобів захисту

Засіб захисту	Logpoint SIEM	ESET NOD32 Antivirus	ActivTrack Professional	Quantum Rugged 1595R
Підсумкова вага	0,10689	0,59217	0,122128	0,16829

Аналіз результатів розрахунків (табл. 3) показує, що для запобігання вірусної атаки оптимальним є засіб захисту 2. Засіб 4 забезпечує захист відразу від трьох загроз. Цей засіб є оптимальним за критерієм «ефективність-вартість» і забезпечує розумний баланс між вартістю реалізації засобу та ефективністю протидії загрозам. Тобто, для даного випадку оптимальний комплект засобів захисту складають засоби ESET NOD32 Antivirus та Quantum Rugged 1595R.

Таким чином, метод аналізу ієрархій може бути застосований для вирішення завдання оптимального вибору засобів захисту від загроз безпеки на об'єкті інформатизації.

Список використаних джерел:

1. Васильєв О. Б., Васильєва Н. С., Кічмаренко О. Д. Методи розв’язування задач багатокритеріальної оптимізації : метод. вказівки. Одеса, 2017. 48 с.

2. Файнзільберг Л. С., Жуковська О. А., Якимчук В. С. Теорія прийняття рішень : підручник. Київ, 2018. 246 с.

УДК 004.7:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.066

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ВІД ВИТОКІВ ІНФОРМАЦІЇ ЧЕРЕЗ МЕТАДАНІ РЕСУРСІВ WEB-ДОДАТКІВ

Качан В.Є.
Науковий керівник – к.т.н., ст. викл. каф. Марчук А.В.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, кафедра ІКІ імені В.В. Поповського, тел. +38(050) 702-55-92)
email: vadym.kachan@nure.ua, artem.marchuk@nure.ua

The work is aimed at considering the criticality of information leakage in files metadata. A vulnerable web application OWASP Juice Shop has been analyzed and a possible solution has been developed that removes this critical vulnerability.

У сучасному світі безпека веб-додатків постає одним з найвизначніших викликів безпеки, адже вони обслуговують значну кількість користувачів, що зростає щодня. Організація OWASP визначає 10 найрозповсюдженіших вразливостей веб-безпеки, що наявні в сучасних веб-додатках (OWASP Top 10) [1]. Ресурси OWASP, що пов’язані із OWASP Top 10 надають чіткий опис того, як використовується вразливість, із наданням прикладів та рекомендацій по її усуненню.

Однією із вразливостей, що впливають на конфіденційність у веб-додатках є витік інформації з метаданих файлів, особливо файлів, що завантажуються користувачами. Для проведення дослідження, яке показало б чіткий приклад та наслідки такого витоку, використовується тренувальний вразливий додаток OWASP Juice Shop, метою якого є навчання спеціалістів з кібербезпеки на прикладі різних вразливостей, що впроваджені в цей веб-додаток. Як зазначається на офіційній сторінці OWASP [2], даний вразливий додаток має в сумі 106 завдань, що стосується наступних категорій вразливостей:

- порушений контроль доступу;
- порушена автоматизація;
- порушена аутентифікація;
- вразливості в криптографії;
- неправильна обробка вхідних даних;
- ін’єкції;
- ненадійна десеріалізація;
- різні некласифіковані помилки (miscellaneous);
- неправильні налаштування безпеки;
- безпека за допомогою «затьмарення» (obscurity);
- розкриття конфіденційних даних;
- неперевірені переадресації;
- вразливі компоненти;

−міжсайтовий скриптинг;

−атака на зовнішню сутність XML.

В ході роботи було проаналізовано кожну вразливість в додатку, окрім тих, що визначені як жартівливі та тих, що стосуються розвідки OSINT. В категорії що стосується розкриття конфіденційних даних було виявлено вразливість, яка стосується витоку інформації через картинки, що завантажені користувачами. В конкретному прикладі додатка картинка користувача містила GPS-дані щодо місця, де було зроблено фото і це місце являло собою відповідь на секретне питання користувача, що дозволило отримати доступ до його акаунту шляхом скидання його паролю. Далі, за допомогою документації OWASP Top 10 та суміжних ресурсів OWASP, було визначено, що така документація не надає жодних пояснень або згадувань того, як виявляти та захищатись від подібного роду атак. Окремим чином було визначено, що документація інструменту OWASP ZAP [3], який є проксі-додатком для роботи з запитами, надає список оповіщень безпеки, до якого входить оповіщення «Зображення викриває локацію або приватні дані». Опис даного оповіщення визначає, що перед завантаженням або передачею картинок необхідно видалити з них критичну інформацію, що міститься в метаданих. Це передбачає повне видалення метаданих або лише GPS компоненти, та інших даних, таких як серійні номери.

Як було визначено, опис захисту від витоку інформації з метаданих ресурсів, що завантажуються в додаток, не чітко визначений в основних ресурсах, що надаються OWASP, лише наявний в документації їхнього програмного продукту. Незважаючи на це, такий витік становить критичну необхідність його усунення, адже зловмисник таким чином може без значних затрат скомпрометувати обліковий запис користувача. Через це, в рамках даної роботи запропоновано програмне рішення, яке є прикладом можливого впровадження відповідного функціоналу в реальний веб-додаток, в тому числі Juice Shop, який, однак, є комплексним та динамічним, і був створений командою OWASP та їхньою спільнотою, через що зазначений механізм обробки метаданих впроваджено локально в окремому вигляді.

Спочатку було створено локально сайт тільки із функціоналом завантаження файлів формату jpg/png та pdf, файли того ж формату можна завантажити і у додаток OWASP Juice Shop. На рисунку 1 зображено видалення метаданих картинки, після того як вона була завантажена. Було видалено конфіденційні дані GPS, а також переіменовано картинку випадковим чином, щоб у випадку, якщо зловмисник отримає до неї доступ, він не міг зробити висновок про те, чия це картинка/фотографія і ким вона була завантажена.

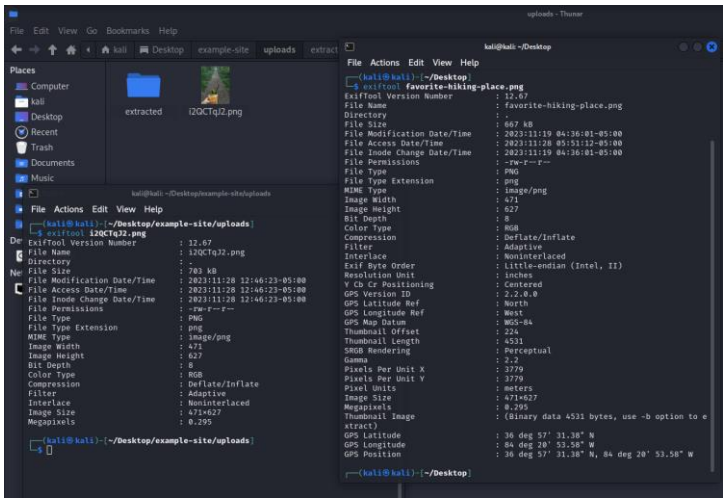


Рисунок 1 - Результат видалення метаданих картинки

Аналогічним чином виконується обробка файлу pdf – усі критичні метадані (наприклад, автор файлу і програма, де було створено файл) видаляються і файл зберігається із випадковим іменем.

Висновок.

В роботі виконано аналіз загальнодоступних ресурсів OWASP та вразливостей в OWASP Juice Shop і запропоновано впровадження можливого рішення для усунення витоку інформації користувача з веб-додатку із використанням метаданих файлів.

Критичність атаки, що досліджувалась, за шкалою оцінки CVSS [4] становить 7.3 і визначається як «висока» («high»). Таким чином, впровадження запропонованого рішення усуває високо критичну атаку.

Список використаних джерел:

1. Top 10 Web Application Security Risks. URL: https://owasp.org/www-project-top-ten/ (дата звернення 03.03.2024).

2. OWASP Juice Shop. URL: https://owasp.org/www-project-juice-shop/mage Expo.ses Location or Privacy (дата звернення 03.03.2024).

3 ZAP. Image Exposes Location or Privacy Data. URL: https://www.zaproxy.org/docs/alerts/10103/ (дата звернення 03.03.2024).

4. NIST. Common Vulnerability Scoring System Calculator. URL: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator (дата звернення 03.03.2024).

УДК 004.056.523 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.069

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ МЕТОДИ ПІДВИЩЕННЯ ЯКОСТІ ЗАХИСТУ В СИСТЕМАХ ГОЛОСОВОЇ АВТЕНТИФІКАЦІЇ

Квашенко В. Р., Пастушенко М.С.
Науковий керівник – к.т.н., проф. Пастушенко М. С., каф. ІКІ
Харківський національний університет радіоелектроніки
м. Харків, Україна
e-mail: vladyslav.kvashenko@nure.ua, Mykola.Pastushenko@nure.ua

With the rapid development of artificial intelligence technologies, industries must quickly adapt to new challenges. It is known that 62% of IT executives expressed concerns about the security threats posed by AI and deepfakes, as there have been cases where large banks' authentication systems were bypassed using synthesized voices. Voice authentication systems are a convenient and effective method of user identity verification. However, the development of modern voice synthesis technologies creates significant security threats. Criminals can generate synthetic voices that precisely imitate another user's voice, leading to unauthorized access. To address this issue, organizational and technical measures can be implemented. For example, the use of a changeable vocabulary, issuing a one-time password on the screen, and limiting the time for password entry are steps towards strengthening the security of voice authentication systems.

Зі стрімким розвитком технологій штучного інтелекту, все більше галузей мають так само швидко адаптуватись до нових викликів. Так, згідно з [1], 62% IT-керівників повідомили про занепокоєння щодо загроз безпеці, які несуть штучний інтелект та deepfake, через випадки, коли в великих банках обходили системи автентифікації використовуючи синтезований голос.

Системи голосової автентифікації є зручним та ефективним методом підтвердження особи користувача. Однак, розвиток сучасних технологій синтезу голосу створює значні загрози для безпеки. Зловмисники можуть генерувати синтетичні голоси, які точно імітують голос іншого користувача, що призводить до неавторизованого доступу. Для вирішення цієї проблеми, окрім технічних заходів, можна впровадити організаційно-технічні заходи.

Зазвичай процес голосової автентифікації складається з наступних кроків [2]:

1. Реєстрація голосу – користувач записує зразок голосу, який система використовує для створення унікального шаблону.
2. Виділення ознак – система виокремлює характерні риси зі зразка голосу, такі як висота, тон і швидкість мовлення.
3. Навчання моделі – виділені ознаки зберігаються в базі даних, для подальших порівнянь.

4. Автентифікація – на етапі автентифікації користувач надає новий зразок свого голосу. Система ідентифікує ознаки з цього зразка і порівнює їх зі збереженим шаблоном голосу. Якщо збіг перевищує певний поріг, користувач проходить автентифікацію.

Організаційно-технічні методи застосовуються під час етапу автентифікації. Розглянемо випадок, коли зловмисники змогли дістати достатньо вхідних даних для створення правдоподібного зразку голосу особи. Можна вирізнити декілька методів запобігання атакам синтезу голосу.

Використання змінного словника – замість запровадження сталого секретного слова, використовується динамічна система словника, в якій фраза для автентифікації завжди змінюється. Це ускладнює зловмисникам підготовку синтезованого зразка голосу заздалегідь.

Виведення одноразового пароля (OTP) на екран – поєднання секретного слова з відображенням випадково згенерованого OTP на екрані користувача на короткий час. Користувач, потім, повинен прочитати цей OTP для голосової автентифікації. Оскільки OTP є непередбачуваним та швидкозмінюваним, це унеможливлює сценарій авторизації з попередньо синтезованим секретним словом та зменшує ризик успішних атак синтезу голосу.

Якщо автентифікація відбувається в якомусь контрольованому приміщенні – є сенс встановити камери відеонагляду, для унеможливлення використання будь яких сторонніх інструментів для синтезу голосу, або, якщо автентифікація відбувається віддалено – встановити часове обмеження на введення паролю.

Обмеження часу на введення пароля – встановлення чіткого часового ліміту для введення OTP після того, як він з’явиться на екрані. Таке обмеження часу додає додатковий рівень безпеки, оскільки зменшує вікно можливостей для зловмисників використовувати синтезований зразок голосу.

Наприклад, модель штучного інтелекту VALL-E від Microsoft може клонувати голос з трисекундного аудіокліпу і генерувати новий голос відносно швидко [3]. Хоча точний час, необхідний для синтезу речення, явно не вказаний, здатність моделі клонувати голос з такого короткого кліпу дозволяє припустити, що процес синтезу може бути досить швидким, потенційно протягом декількох секунд. Тому, потрібно визначити баланс між складністю OTP паролю та часом на його проголошення.

Згідно з [4], швидкість читання для дорослих становить близько 183 слів на хвилину при читанні вголос, а фактичний час, необхідний для синтезу, також залежатиме від таких факторів, як довжина OTP-пароля, обчислювальна потужність системи та ефективність механізму Text-to-Speech, тому можна обрати довжину паролю в 2 слова та ліміт в 5 секунд для проголошення паролю.

В доповіді наводяться чисельні характеристики, які показують ефективність запропонованих організаційно-технічних заходів.

Системи голосової автентифікації, хоча й ефективні, стають уразливими перед атаками синтезу голосу. Запровадження таких організаційно-технічних заходів безпеки як, змінний словник, використання одноразових паролів та обмеження часу на введення пароля є кроками до зміцнення безпеки голосових систем автентифікації.

Подальші наукові дослідження будуть орієнтовані на розробку заходів підвищення захисту систем голосової автентифікації.

Список використаних джерел:

1. Daon Unveils xSentinel to Combat Voice Deepfakes as Part of AI.X Family. 2023. URL: https://www.daon.com/resource/daon-unveils-xsentinel-to-combat-voice-deepfakes-as-part-of-ai-x-family/.

2. Pastushenko M. KrasnozheniukY, Lemeshko O. Analysis of voice signal phase data informativity of authentication system // Proceedings of The Third International Workshop on Computer Modeling and Intelligent Systems (CMIS-2020), Zaporizhzhia, Ukraine, April 27–May 1, 2020. P. 1040–1053.

3. Microsoft's new VALL-E AI can clone your voice from a three-second audio clip. 2023. URL: https://techmonitor.ai/technology/ai-and-automation/vall-e-synthetic-voice-ai-microsoft.

4. How many words do we read per minute? A review and meta-analysis of reading rate. 2019. URL: https://www.researchgate.net/publication/335174808_How_many_words_do_we_read_per_minute_A_review_and_meta-analysis_of_reading_rate.

УДК 004.7:004.9

ПОРІВНЯЛЬНИЙ АНАЛІЗ СЦЕНАРІЇВ РОЗГОРТАННЯ ІНФРАСТРУКТУРИ У ХМАРНОМУ СЕРЕДОВИЩІ

Красюкова В.В.
Науковий керівник – доц. Коваленко Т.М.
Харківский національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: valeriia.krasiukova@nure.ua

The use of cloud environments is an essential part of working with information technologies. The process of deploying infrastructure in a cloud environment is one of the key stages that ensures the efficiency of using this infrastructure in the future. The physical location and ownership structure of the cloud environment play a significant role in the effectiveness of cloud computing applications. According to their combination, four deployment scenarios are distinguished. To choose a scenario, it is necessary to analyze the advantages and disadvantages of each of them, as well as evaluate one's own needs, requirements, and capabilities.

Використання хмарних середовищ є важливою частиною роботи з інформаційними технологіями. Процес розгортання інфраструктури у хмарному середовищі є одним з ключових етапів, що забезпечує ефективність використання даної інфраструктури в подальшому.

Оцінити ефективність розгортання інфраструктури у хмарному середовищі можна за допомогою наступних аспектів:

– оцінивши загальні витрати на розгортання та управління інфраструктурою, порівнявши їх з потенційними вигодами;

– проаналізувавши адаптивність інфраструктури при зміні задач і масштабів бізнесу;

– визначивши продуктивність та стабільність у доступі до даних та сервісів;

– врахувавши вимоги до забезпечення безпеки даних та систем

– оцінивши зручність інструментів управління та моніторингу для відстеження роботи інфраструктури;

– визначивши час потрібний для розгортання [1].

Важливе значення в ефективності застосуванні хмарних обчислень відіграє фізичне розташування та форма власності хмарного середовища. Відповідно до їх комбінації виділяють чотири сценарії розгортання.

Приватний – обслуговує одну організацію. Інфраструктура розташовується на власній території користувача.

Спільний – обслуговує спільноту споживачів у складі організації що має спільні інтереси.

Публічний – передбачає відкритий публічний доступ до хмарних послуг.

Гібридний – утворюється поєднанням кількох платформ з різними сценаріями розгортання, які об’єднуються між собою технологіями які забезпечують сумісність обміну даних та застосунків.

Відповідно для вибору одного зі сценаріїв необхідно врахувати такі фактори як надійність мережі, складність у реалізації, розподіл навантаження, ризики спільного використання, та витрати на реалізацію.

Найбільший рівень надійності та контролю дає приватний сценарій розгортання інфраструктури, так як він передбачає використання власних ресурсів та персоналу. Також цей сценарій дозволяє налаштувати інфраструктуру точно відповідно до потреб та вимог бізнесу. Разом з тим даний сценарій є найскладнішим у реалізації та найдорожчим у використанні, і є важко масштабованим.

Натомість публічний сценарій значно економніший фінансово, але пропонує найменший контроль з боку користувача, що збільшує ризик безпеки. Основними перевагами даного сценарію можна назвати найбільшу адаптивність та швидке масштабування.

Сценарій спільного використання дозволяє кільком організаціям використовувати спільні ресурси. Хмарні рішення в такому разі можуть бути налаштовані відповідно до специфічних вимог спільного використання, що дозволяє зручно контролювати доступ до даних та ресурсів. Порівняно з публічними хмарними сервісами даний сценарій має менші можливості до масштабування, а також потребує враховувати залежність кожної організації від інших учасників.

Гібридний сценарій поєднує в собі переваги публічних та приватних хмар, створюючи при цьому додаткові складності в управлінні, необхідність забезпечення синхронізації даних, та потребуючи значних витрат на розгортання.

Кожний з даних сценаріїв має унікальні переваги та недоліки, які необхідно враховувати. Кожна організація при виборі стратегій повинна проаналізувати власні потреби, вимоги та можливості.

Список використаних джерел:

1. CloudBus. VMProvisionCloud: A Framework for Optimized VM Provisioning in Clouds // Доповідь на конференції International Conference on Parallel Processing (ICPP). URL : http://www.cloudbus.org/papers/VMProvisionCloud-ICPP2011.pdf. (2011).

2. Badger L., Grance T., Patt-Corner R. et al. Cloud Computing Synopsis and Recommendations. Recommendations of the National Institute of Standards and Technology. NIST Special Publication. SP 800–146. URL : https://csrc.nist.gov/publications/detail/sp/800-146/final

УДК 004.7:004.056

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ І МЕТОДІВ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФРАСТРУКТУРИ У ХМАРНОМУ СЕРЕДОВИЩІ

Красюкова В.В.
Науковий керівник – доц. Коваленко Т.М.
Харківский національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: valeriia.krasiukova@nure.ua

The use of cloud environments is an essential part of working with information technologies. The use of cloud technologies requires thorough security measures. Key methods include multifactor authentication, limiting user access to the necessary minimum, network protection, and data encryption. Recommendations include creating network tiers, securing networks, using certificates, and encrypting traffic. Traffic filtering and monitoring, automated response to threats, auditing, and adherence to standards such as ISO/IEC 27001 are crucial for ensuring a high level of security and trust in cloud environments.

Використання хмарних середовищ є важливою частиною роботи з інформаційними технологіями. Безпека інфраструктури в хмарному середовищі є ключовим аспектом в питанні довіри користувачів до сервісу.

Захист інфраструктури хмарного середовища включає в себе багатофакторну автентифікацію, захист мереж, журнали активності користувачів та шифрування даних.

Основоположним принципом забезпечення безпеки в хмарному середовищі є надання доступу користувачам до ресурсів та даних, зведених до необхідного мінімуму. Так завданням адміністратора є визначення потреб кожного конкретного користувача, або груп користувачів, та надання прав таким чином, щоб кожен користувач мав доступ до ресурсів які потрібні йому для роботи, але не більше. Облікові дані не повинні надаватись спільно жодному користувачу чи системі. Доступ користувачам слід надавати з найменшими привілеями, включаючи паролі та використання багатофакторної автентифікації. Програмний доступ має здійснюватись за допомогою тимчасових облікових даних з обмеженими привілеями [1]. Таким чином користувач не буде мати доступ до ресурсів та даних які не потрібні йому для роботи, а також у випадку компрометування певного користувача зловмисник не отримає доступ до всієї системи, а лише до певної її частини. Крім того варто встановити вимоги до паролів користувачів, періодичної їх заміни згідно з журналом паролів, та автоматично виявляти паролі з високим ризиком.

Для захисту мереж рекомендовано створювати мережеві рівні, де компоненти які мають спільні вимоги до чутливості будуть згруповані. Трафік при цьому має надходити лише від сусіднього наступного найменш чутливого рівня. Розробляючи топологію мережі необхідно вивчити

вимоги до підключення кожного компонента. Для ефективного захисту трафіку використовуються групи безпеки, мережеві списки дозволів, підмережі та таблиці маршрутів [2].

Для захисту даних під час передачі необхідно впровадити використання сертифікатів безпеки транспортного рівня. Крім того для захисту даних варто шифрувати ці дані при зберіганні та транспортуванні, що допоможе забезпечити їх конфіденційність і цілісність. Мережевий трафік між інфраструктурою хмари та Інтернетом має бути обов'язково зашифрований. Мережевий трафік у внутрішньому середовищі має шифруватись за допомогою TLS там де це можливо.

Для фільтрування трафіку що виходить за периметр приватної інфраструктури необхідно налаштувати брендмауер. Так трафік можна фільтрувати за певними критеріями, білими та чорними списками, чи налаштування тихих перевірок за допомогою CAPTCHA для зменшення трафіку ботів [1].

Для виявлення потенційних загроз та аномальних подій необхідно впроваджувати системи моніторингу інфраструктури, що дозволить оперативно виявляти та реагувати на виявлені загрози. Використання автоматизованих систем реагування на події дозволить масштабувати та прискорити можливості моніторингу та зменшить вплив людського фактору.

Крім описаних методів варто зауважити що важливе значення має також аудит та впровадження стандартів безпеки, таких як ISO/IEC 27001, SOC 2. Впровадження даних стандартів допомагає забезпечити високий рівень безпеки, відповідність законодавства у сфері забезпечення інформаційної безпеки та підвищить довіру партнерів та користувачів до організації. Регулярне проведення внутрішніх та зовнішніх аудитів є частиною вимог стандартів безпеки та дозволить виявити потенційні загрози та слабкі місця в захисті, підвищить ефективність впроваджених підходів до забезпечення безпеки а також перевірить інфраструктуру на відповідність стандартам безпеки.

Список використаних джерел:

1. Security Pillar - AWS Well-Architected Framework. URL : https://docs.aws.amazon.com/pdfs/wellarchitected/latest/framework/wellarchitected-framework.pdf

2. Data classification models and schemes. URL : https://docs.aws.amazon.com/whitepapers/latest/data-classification/data-classification-models-and-schemes.html

УДК 004.7:004.056

АНАЛІЗ ІСНУЮЧИХ ПІДХОДІВ І МЕТОДІВ ОЦІНКИ БЕЗПЕКИ ІНФРАСТРУКТУРИ У ХМАРНОМУ СЕРЕДОВИЩІ

Красюкова В.В.
Науковий керівник – доц. Коваленко Т.М.
Харківский національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: valeriia.krasiukova@nure.ua

The use of cloud environments is an integral part of working with information technologies. Analyzing modern methods of assessing infrastructure security in cloud environments is one of the key aspects to ensure a high level of data and resource protection. To assess security, methods such as security audits, penetration testing, risk assessment, and event log analysis can be utilized. These methods can be used separately, but to ensure maximum accuracy in security assessment, combining them is recommended. Security assessment of the infrastructure in the cloud environment needs to be conducted periodically to identify security threats and address them.

Використання хмарних середовищ є невід'ємною частиною роботи з інформаційними технологіями. Аналіз сучасних методів оцінки безпеки інфраструктури в хмарних середовищах є одним з ключових аспектів для забезпечення високого рівня захисту даних і ресурсів. Для оцінки безпеки можна використовувати такі методи як аудит безпеки, тест на проникнення, оцінка ризиків та аналіз журналів подій.

Перш за все для оцінки безпеки інфраструктури варто почати з оцінки ризиків. Для цього необхідно визначити потенційні загрози та вразливості, та оцінити потенційні наслідки від реалізації зловмисником цих загроз. Класифікація ризиків допомагає визначити пріоритети для розробки стратегії управління ризиками. Ці стратегії приймаються після оцінки ризиків, які можуть включати в себе технічні та організаційні заходи для зменшення вразливостей [1].

Ефективніше всього оцінювати захищеність інфраструктури можна за допомогою перевірки її на відповідність міжнародним стандартам безпеки, наприклад ISO/IEC 27001 [2]. Стандарт є по суті списком параметрів які мають бути втілені у системі. Внутрішній аудит власної організації означає що співробітник служби безпеки має перевірити чи втілені у компаній всі вимоги, та вказати всі відмінності у звіті. Таким чином власник організації отримає інформацію про оцінку захищеності інфраструктури. Зовнішній аудит проводиться консалтинговою компанією і відбувається аналогічним чином, проте зазвичай він може стати більш об'єктивним, тому що виключає можливість того що співробітник служби безпеки приховає певні недоліки через те що відповідальність за їх усунення може бути покладене на нього. Тож зовнішній аудит виключає

власну зацікавленість співробітника в певних результатах. Після усунення виявлених недоліків варто провести повторний аудит.

Крім аудиту організація може оцінити захищеність власної інфраструктури у хмарному середовищі за допомогою тесту на проникнення. Зазвичай для цього наймають консалдингову компанію, яка намагається проникнути в систему з метою виявити слабкі місця в захисті та оцінити рівень захисту інфраструктури. Перед початком проникнення укладається договір зі всіма умова проведення тесту, а після власне тесту компанія надає детальний звіт про виявлені вразливості.

Аналіз журналів подій включає в себе вивчення журналів подій з метою виявлення аномальних активностей та інцидентів у хмарному середовищі. Журнали подій можуть містити в собі інформацію про те хто та коли входив до інфраструктури, до яких ресурсів звертався чи намагався звернутись, які дії були зроблені (успішні та неуспішні). Зазвичай інформацію в цих журналах можна відфільтрувати для зручного вивчення, а також даний аналіз можна автоматизувати. На успішні дії варто звертати увагу для того щоб перевірити чи правильно налаштовано надання доступу користувачам, чи не отримують користувачі доступ до ресурсів, до яких вони не повинні мати доступ. Проте аналіз неуспішних спроб може показати які користувачі намагались отримати доступ до ресурсів яі для них закриті, що є підозрілою поведінкою. Також за допомогою аналізу неуспішних спроб входу в систему можна побачити чи не намагався хтось отримати несанкціонований доступ до облікових записів певних користувачів. Також підзрілою можна вважати якщо певний обліковий запис здійснює активність в неробочий час працівника. Це також може свідчити про потенційну компроментацію облікового запису.

Наведені методи можуть використовуватись окремо, проте для забезпечення максимальної точності в оцінці безпеки поєднувати їх. Також варто зауважити що оцінка рівня захисту інфраструктури повинна проводитись регулярно, для виявлення потенційних загроз та їх усунення.

Список використаних джерел:

1. Reconshell. Cloud Security Handbook. 2022. URL: https://reconshell.com/wp-content/uploads/2022/07/Cloud-Security-Handbook.pdf

2. ISO/IEC 27001:2022 "Information technology — Security techniques — Information security management systems — Requirements", International Organization for Standardization, Geneva, Switzerland. URL: https://www.iso.org/standard/27001

УДК 004.056

RELEVANCE OF HSRP SECURITY

Milanka I.Yu., Volotka V.S.
Scientific Supervisor - Senior Lecturer Volotka V.S.
Kharkiv National University of Radio Electronics, Faculty of Infocommunication,
Kharkiv, Ukraine
e-mail: ihor.milanka@nure.ua.

Currently, there are a lot of threats that can disrupt the proper functioning of information and communication systems and lead to their denial of service. If this happens, any company risks significant material and reputational losses. That is why it is so important to constantly develop new and more advanced methods of protecting information and communication systems, which can help increase the level of fault tolerance of corporate networks in relation to external influence from third parties and sources.

The FHRP (First Hop Redundancy Protocol) family of protocols is a crucial element in the topology of any organization's network and significantly impacts its security level [1]. In the context of security, the role of the FHRP family of protocols includes:

- Ensuring network continuity (fault tolerance);
- Performing load balancing to effectively distribute network resources and prevent equipment overload;
- Protection against attacks aimed at network service disruption (e.g., DoS and DDoS);
- Organizing the process of network traffic authentication and filtering.

The main advantage of the HSRP (Hot Standby Router Protocol) protocol (as well as all other protocols in the FHRP family) is that if the active router fails and the standby router takes its place, the network continues to serve subscribers during this process, and user devices do not disconnect from it. This is because all devices in the HSRP group are configured with identical virtual IP and MAC addresses. Despite being used for providing fault-tolerant routing within a corporate network, the HSRP protocol also has its own vulnerabilities [2].

These vulnerabilities can be exploited through the following types of attacks:

- Traffic interception attack;
- Spoofing attack;
- Denial of Service (DoS) attack targeting router overload with traffic;
- Password retrieval attack targeting router passwords compromise;
- Attack on HSRP v1 protocol.

Each of the mentioned attacks is utilized by malicious actors to exploit the most common vulnerabilities of the HSRP protocol. The "Traffic interception" attack aims to intercept HSRP packets transmitted between routers of the same group openly. The "Spoofing" attack allows attackers to forge HSRP packets in a way that they will transmit compromised virtual IP addresses and the desired priority values to routers. This attack can lead to destabilization of the corporate network operation and enable the attacker to designate a rogue router as "active" by altering priority values for all legitimate network devices. Through a DoS attack, the attacker can overload routers and disrupt the operation of the entire network. The DoS attack is executed by sending a large number of false HSRP packets to the network devices configured with the HSRP protocol.

The "Password retrieval" attack targets routers configured with the HSRP protocol to intercept authentication passwords and gain unauthorized access to the configuration of network devices.

The last type of attack is associated with vulnerabilities in the HSRP v1 protocol. In the first version of HSRP, it is possible to spoof HSRP packets and perform a DoS attack. As a rule, it is generally recommended not to use the first version of the HSRP protocol [3].

To ensure the necessary level of security for the HSRP, the following methods can be utilized:

1. Use of HSRP v2: deploying the second version of the HSRP protocol is recommended as it offers more advanced security mechanisms compared to HSRP v1.
2. Authentication of HSRP packets.
3. Filtering HSRP traffic: configure HSRP traffic filtering on network equipment to only allow HSRP traffic from trusted sources, thereby mitigating vulnerabilities associated with adding rogue routers to the HSRP group (e.g., "Traffic interception" and "Spoofing" attacks).
4. Restrict access to HSRP configuration: minimize unauthorized dissemination of HSRP technical information beyond the corporate network and among unauthorized individuals.
5. Encryption of traffic: organize encryption of HSRP traffic by creating and configuring a dedicated VPN topology utilizing the Internet Protocol Security (IPSec) protocol.
6. Monitoring: set up a monitoring system to track suspicious activity propagated through HSRP traffic and alert information security experts or system administrators about potential network attacks. Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) are often used for network monitoring.
7. Software updates.
8. Physical access control.
9. Employee training.

The aforementioned methods will significantly enhance the security level of the HSRP and the corporate network as a whole. It is important to remember, however, that all the described protection methods are not guarantees of complete network and HSRP protocol security. Security is an ongoing process that requires continuous monitoring, adaptation to emerging threats, and implementation of additional measures as needed.

References:

1. Barney N., Lutkevich B. What is Network Security? 2022. URL: https://www.techtarget.com/searchnetworking/definition/network-security.

2. HSRP MD5 Authentication. URL: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/15-s/fhp-15-s-book/fhp-hsrp-md5.pdf.

3. 10 Common Internet Security Threats and How to Avoid Them. URL: https://velecor.com/10-common-internet-security-threats-and-how-to-avoid-them/.

УДК 004.056:005.33 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.081

ПРОПОЗИЦІЇ ЩОДО ОЦІНЮВАННЯ КОМПЕТЕНТНОСТІ АУДИТОРІВ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЇНОЮ БЕЗПЕКОЮ

Пашкова А.В., Вакуленко Д.В.
Науковий керівник – доцент каф. ІКІ ім. В.В. Поповського Добринін І.С.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського, м. Харків, Україна
e-mail: anhelina.pashkova@nure.ua, danyil.vakulenko@nure.ua.

The work is devoted to the actual problem of assessing the consistency of experts' opinions in the field of information security. The work provides proposals for assessing the agreement of experts' opinions using the concordance coefficient, which takes into account the ranking of factors and provides a more accurate assessment of agreement than other methods.

Проведення аудитів – це важлива частина при побудові систем управління інформаційною безпекою (СУІБ). Відповідно до [1], для проведення аудитів організація повинна призначити групу аудиторів, на яких, серед інших задач, покладатиметься задача формування підсумкової оцінки стану інформаційної безпеки.

У роботі [2] надані пропозиції щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022. Зазначимо, що оцінювання відбувається на основі експертної інформації отриманої від аудиторів, які, у цьому випадку, виконують роль експертів.

Відповідно до теорії прийняття рішень [3] експертне оцінювання передбачає рішення п’яти основних задач.

1) Формування групи потенційних експертів.
2) Оцінювання компетентності кожного з експертів.
3) Розрахунок репрезентативності групи експертів.
4) Оцінювання узгодженості думок експертів.
5) Формування експертного висновку.

Проведений авторами аналіз основних етапів експертного оцінювання показує, що одним із найскладніших моментів є оцінювання компетентності кожного з експертів.

У літературі [1] надана формула, за допомогою якої можна оцінити компетентність експертів:

$$K_{K_i} = \frac{K_{a_i} + K_{o_i}}{K_{a_{max}} + K_{o_{max}}}, \quad (1)$$

де K_{a_i} – коефіцієнт аргументації і-го експерта;

K_{o_i} – коефіцієнт обізнаності і-го експерта;

$K_{a_{max}}$, $K_{o_{max}}$ – максимально можливі оцінки аргументації та обізнаності експертів.

Зазвичай, під час розрахунків приймають $K_{a_{max}} = 1, K_{o_{max}} = 1$.

Аналіз виразу (1) показує, що компетентність і-го експерту (K_{K_i}) є функцією двох величин: коефіцієнтів аргументації (K_{a_i}) та обізнаності (K_{o_i}). Причому, ці величини (K_{a_i} та K_{o_i}) мають однаковий вплив на підсумкову оцінку. Це, на нашу думку, призводить до викривлення підсумкової оцінки компетентності. Так, наприклад, якщо перший експерт максимально аргументований ($K_{a_1} \to max$) , але необізнаний ($K_{o_1} \to 0$), а другий експерт – не аргументований ($K_{a_2} \to 0$), але максимально обізнаний ($K_{o_1} \to max$), то в цьому випадку підсумкова оцінка компетенції є однаковою, що суперечить логіці.

Тому авторами даної роботи пропонується наступний підхід для вирішення зазначеної колізії. А саме:

– встановлення порогового рівня аргументації експертів, який дозволяє виконувати задачу з формування експертного оцінювання ($K_{a_{\text{порог}}}$);

– використання вагового коефіцієнту ω_j $(j = 1 \dots N)$, який враховує обізнаність і-го експерта за j-ю областю оцінювання (документація, мережна безпека, фізичний доступ тощо).

У цьому випадку, формула (1) матиме вигляд:

$$K_{K_i} = \sum_{j=1}^{N} \frac{K_{a_i} + \omega_j \cdot K_{o_i}}{K_{a_{max}} + K_{o_{max}}} \quad \forall\, K_{a_i} \geq K_{a_{\text{порог}}} \qquad (2)$$

Зазначимо, що визначення порогового рівня аргументації експертів та вагових коефіцієнтів ω_j покладається на особу, яка керує програмою аудиту.

Таким чином, завдяки запропонованому підходу, можна запобігти викривленій оцінці компетентності експертів (аудиторів) СУІБ на етапі формування групи з аудиту.

Список використаних джерел:

1. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements : вебсайт. URL: https://www.iso.org/standard/27001 (дата звернення: 28.02.2024).

2. Добринін І. С., Пашкова А. В. Розробка пропозицій щодо кількісного оцінювання рівня реалізації вимог стандарту ISO/IEC 27001:2022. *Міжнародна науково-технічна конференція «Інформаційно-комунікаційні технології та кібербезпека (ІКТК-2023)»*. Харків, 2023. URL: https://ice.nure.ua/wp-content/uploads/2024/01/43_Dobrynin-I.S.-Pashkova-A.V._Str.151-153.pdf (дата звернення 28.02.2024).

3. Файнзільберг Л. С., Жукова О. А., Якимчук В. С. Теорія прийняття рішень : навч. посіб. Київ : КПІ ім. Ігоря Сікорського, 2018. 250 с.

УДК 004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.083

КРИМІНАЛІСТИЧНЕ ДОСЛІДЖЕННЯ МЕСЕНДЖЕРА SIGNAL

Рєзніченко Д.Ю.
Науковий керівник – к.т.н., доцент Снігуров А.В.
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського,
м. Харків, Україна
e-mail: dymytrii.rieznichenko@nure.ua

This work is devoted to a forensic investigation of the Signal messenger developed by Open Whisper Systems. The internal structure of the messenger, as well as its mechanisms for protecting confidential user data, will be considered. In addition, the working directories of the Signal messenger in the Android and Windows operating systems will be investigated.

У сучасному світі питання захисту конфіденційних даних має найвищій пріоритет для будь-якої компанії, яка розробляє власну систему обміну мультимедіа та швидкими текстовими повідомленнями між користувачами. З цією метою, розробники мобільних додатків (зокрема месенджерів) намагаються реалізувати у власному програмному продукті найбільш сучасні та ефективні криптографічні рішення, а деякі компанії навіть створюють власні протоколи шифрування. Але, чи є ці рішення та протоколи настільки надійними та, чи дозволяють вони безпечно зберігати дані на кінцевому пристрої користувача – відповідь на ці питання можна знайти у даній роботі.

Останнім часом дуже швидко набирає популярність месенджер Signal від компанії Signal Technology Foundation. Даний месенджер надає користувачам можливість створювати зашифровані повідомлення, пересилати медіафайли, а також здійснювати безпечні голосові та відеодзвінки. Також, Signal Messenger надає користувачу велику кількість налаштувань безпеки: розблокування месенджера за відбитком пальця (або пароля), відключення можливості створення скриншотів у приватних чатах, захист IP-адреси під час голосових дзвінків та інше.

Крім вищезазначених механізмів безпеки, у месенджері Signal використовується власний криптографічний протокол Signal Protocol (раніше – TextSecure Protocol) від компанії Open Whisper Systems. Варто також додати, що Signal Protocol працює разом з наступними алгоритмами і протоколами: XEdDSA та VXEdDSA (створення та перевірка цифрових підписів), X3DH (встановлення спільного секретного ключа між сторонами спілкування), PQXDH (додатковий протокол встановлення спільного секретного ключа разом із можливістю його взаємної автентифікації), Double Ratchet (використовується для шифрування повідомлень на основі спільного секретного ключа) та Sesame (використовується для управління

сеансами шифрування повідомлень у асинхронному середовищі з різними типами пристроїв)[1].

Далі розглянемо, де месенджер зберігає дані користувача. Так, комп'ютерна версія месенджера Signal зберігає дані користувача (разом із артефактами) у локальній директорії «%AppData%\Signal\». У цій директорії можна знайти папку «\databases» із зашифрованим файлом, який має назву «Databases.db». Мобільна версія месенджера Signal зберігає аналогічну базу даних у закритій директорії «data\data\org.thoughtcrime.securesms\databases\signal.db» (потрібні root-права для доступу). Загалом, ці два файли містять у собі однакову інформацію (артефакти) про користувача та є зашифрованими криптографічним алгоритмом AES у режимі AES-GCM. Цікавим є той факт, що у випадку з комп'ютерною версією месенджера Signal, криптографічний ключ для розшифрування бази даних «Databases.db» зберігається у тій самій директорії (поряд із базою даних) у файлі «config.json» у відкритому вигляді.

У мобільній версії месенджера вищезазначений криптографічний ключ можна знайти у директорії «data\keystore\"username"\». Варто підмітити, що для розшифрування бази даних на мобільній версії месенджера Signal, окрім ключа, потрібно ще використати рядки «ciphertext» та «authTag», які можна знайти у директорії «\org.thoughtcrime.securesms\shared_prefs\»[2].

Розшифрування вищезазначених баз даних може проводитися з використанням інструмента «SQLCipher»[3], який є доповненням для програмного забезпечення SQLiteStudio, що дозволяє переглядати вміст баз MySQL. У директорії «%AppData%\Signal\» можна також знайти папку «Network», в якій знаходиться файл «Trust Tokens», що зберігає значення довірених токенів. Ці токени використовуються месенджером для автентифікації користувача на серверах додатку. Самі токени зберігаються у зашифрованому вигляді. Інший файл у тій же папці, який має назву «Network Persistent State», зберігає інформацію про налаштування HTTP-сервера та тип мережного з'єднання, які використовує додаток Signal.

Крім усього вищезазначеного, у директорії «%AppData%\Signal\» можна також знайти наступні корисні артефакти: папка «Session Storage» (інформація про сесії користувача), папка «logs» (зберігається інформація про всі запити, які здійснює додаток по відношенню до сервера, разом із посиланнями на конкретні ресурси), папка «attachments.noindex» (локальне сховище графічних зображень месенджера), папка «stickers.noindex» (локальне сховище стікерів, які використовує користувач у чатах), файл «ephemeral.json» (містить інформацію про розміри вікна месенджера та місце розташування цього вікна на робочому столі), файл «Local State» (містить значення криптографічного ключа, який використовується для шифрування локальних технічних файлів месенджера), файл «Preferences» (містить значення «солі», яка додається до ідентифікатора користувацького

пристрою, а також деякі дані про мови інтерфейсу, які використовує користувач).

Тепер розглянемо внутрішню будову бази даних «Databases.db». Загалом, у даному файлі можна знайти такі основні таблиці (артефакти): «groups» (містить ідентифікатор групи, перелік учасників, назву групи тощо), «mms» (архів текстових повідомлень користувача разом із часовими мітками), «one_time_prekeys» (перелік одноразових ключів, які використовуються для створення безпечних сесій у месенджері), «identities» (ідентифікатор користувача, персональний криптографічний ключ, ім'я користувача тощо), «sms» (схожа на «mms», але містить більше інформації про повідомлення), «storage_key» (ключ, який використовується для розшифрування файлів із локального сховища даних користувача) та інші. Наостанок необхідно розглянути, яким чином месенджер Signal зберігає медіафайли, які користувачі пересилають у чатах. Як вже було сказано раніше, комп'ютерна версія месенджера зберігає медіафайли (фото та відео) і ці дані знаходяться у директорії «%AppData%\Signal\attachments. noindex» (в Android взагалі створюється окреме ізольоване сховище). Усередині даної директорії знаходиться велика кількість папок, імена яких, як правило, складаються з двох символів (число та буква латинського алфавіту). Цікавим є те, що переслане через користувацький чат графічне зображення, месенджер зберігає у декількох папках одразу: в одній – повноцінне зображення (розмір, наприклад, 1152x2048 пікселів), а у другій – його обрізана копія (розмір 150x150 пікселів). Причому, кожен новий пересланий медіафайл зберігається в іншу папку (вибір папки відбувається випадковим чином). Крім усього вищезазначеного, якщо переглянути метадані цих зображень, то можна побачити, що їх розмір (простір, який вони займають на диску), а також значення параметра «Bit depth» (інформація про кольори зображення) теж відрізняються. Варто також додати, що месенджер автоматично видаляє практично всі корисні метадані зображень та інших медіафайлів. Загалом, варто зробити висновок, що месенджер Signal є доволі цікавим додатком з точки зору цифрової криміналістики, оскільки він надає велику кількість механізмів захисту, але паралельно самостійно створює слабкі місця у власній системі безпеки (наприклад, зберігає криптографічні ключі у відкритому вигляді).

Список використаних джерел:

1. Technical information [Електронний ресурс] // 2024. Режим доступу: https://signal.org/docs/. Decrypting Signal DB for Android [Електронний ресурс] // 2021. Режим доступу: https://rado0z.github.io/Decrypt_Android_Database.SQLCipher Community Edition [Електронний ресурс] // 2024. Режим доступу: https://www.zetetic.net/sqlcipher/open-source/.

УДК 621.396:004.7

ДОСЛІДЖЕННЯ ТЕХНОЛОГІЙ БЕЗПРОВІДНОГО ЗВ'ЯЗКУ В ІНТЕРНЕТІ РЕЧЕЙ: ПЕРЕВАГИ, ОБМЕЖЕННЯ ТА ПОТЕНЦІЙНІ ЗАГРОЗИ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14,
каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

The Internet of Things (IoT) plays an important role in our modern lives, facilitating automation and convenience in many aspects of our daily and professional lives. One of the key aspects of the IoT is wireless communication, which allows devices to communicate with each other and with central servers without the need for physical connection via cables. In this article, we will explore the benefits, limitations, and potential threats of wireless communication in the IoT.

Однією з найважливіших переваг безпровідного зв'язку в IoT є його зручність та мобільність. За допомогою безпровідних технологій можна підключити пристрої до мережі з будь-якого місця без необхідності проведення кабелів. Це особливо корисно у випадку розгортання IoT у великих просторах, таких як промислові об'єкти чи будівлі.

Другою важливою перевагою є масштабованість безпровідних мереж. Безпровідні технології дозволяють легко розширювати м ережі, додавати нові пристрої та розширювати покриття без значних витрат на інфраструктуру. Це робить безпровідний зв'язок ідеальним варіантом для масштабування IoT у великих містах чи інших густих населених пунктах.

Незважаючи на всі його переваги, безпровідний зв'язок в IoT має свої обмеження. Наприклад, деякі технології можуть мати обмежений діапазон дії та проблеми з проникненням сигналу через стіни або інші перешкоди. Це може обмежувати місце використання певних типів безпровідних пристроїв та технологій, особливо у великих будівлях чи спорудах з товстими стінами.

Додатковим обмеженням є витрата енергії. Деякі безпровідні протоколи можуть вимагати значних витрат енергії для передачі даних, що може стати проблемою для пристроїв з обмеженим живленням, таких як датчики або вбудовані системи.

Попри всі його переваги, безпровідний зв'язок в IoT також відкриває двері для різних потенційних загроз та вразливостей. Наприклад, безпровідні мережі IoT можуть стати об'єктом різних кібератак, серед яких особливо небезпечними є DDoS-атаки та атаки на викидання сервісу (DoS-атаки). Ці атаки відносяться до так званих "відмов у обслуговуванні"

(Denial of Service, DoS) або "розподіленого відмов у обслуговуванні" (Distributed Denial of Service, DDoS) атак.

Вони полягають у перевантаженні мережі чи сервера штучно створеним трафіком, що надходить з багатьох джерел одночасно. Зловмисники можуть використовувати масштабні ботнети (мережі комп'ютерів, що керуються зловмисниками без відома їх власників) для організації DDoS-атак. Це може призвести до перевантаження мережевого обладнання, відмови серверів або інших пристроїв у мережі, що призводить до тимчасової недоступності для легітимних користувачів та серйозних фінансових втрат для організацій. [1]

Ці типи атак можуть бути особливо небезпечними в контексті IoT, оскільки багато пристроїв у безпровідних мережах не мають достатнього рівня захисту, щоб відбити масштабні атаки. Крім того, зловмисники можуть використовувати вразливості в програмному забезпеченні або недоліки в конфігурації мережі для організації атак.

Також передача особистих даних через безпровідні мережі викликає серйозні питання щодо приватності та захисту цих даних. Оскільки безпровідні мережі передають дані через радіосигнали, вони можуть бути вразливі до перехоплення та несанкціонованого доступу. Наприклад, зловмисник, який має технічні знання та відповідне обладнання, може перехопити передані дані із безпровідної мережі, які можуть містити особисті інформаційні дані, такі як імена, адреси, номери телефонів, фінансові дані тощо.

Несанкціонований доступ до особистих даних може мати серйозні наслідки для користувачів та організацій. Це може призвести до крадіжки особистої ідентифікаційної інформації, фінансового шахрайства, витрат на відновлення даних та репутаційних втрат для організацій. Крім того, якщо конфіденційна інформація потрапить в руки зловмисника, це може вплинути на довіру користувачів до системи або послуг, що пропонуються через IoT.

Таким чином, забезпечення безпеки та захисту особистих даних у безпровідних мережах IoT важливо для підтримки приватності користувачів та довіри до систем IoT. Для цього можуть бути використані різноманітні заходи безпеки, такі як шифрування даних, аутентифікація користувачів, використання захищених протоколів зв'язку та систем управління доступом до мережі. Такі заходи допомагатимуть запобігти несанкціонованому доступу до особистих даних та зберегти конфіденційність інформації користувачів у безпровідних мережах IoT.

Список використаних джерел:

1. Горбань, А. В. Кібербезпека в інтернеті речей / А. В. Горбань, І. С. Постернак // Інформаційні технології та комп’ютерна інженерія. – 2018. – № 2 (46). – С. 35–40.

УДК 004.8:004.056

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА МАШИННОГО НАВЧАННЯ У ВИЯВЛЕННІ ТА ЗАПОБІГАННІ АТАКАМ НА БЕЗПРОВІДНІ МЕРЕЖІ ІНТЕРНЕТУ РЕЧЕЙ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

The modern world is becoming increasingly dependent on Internet of Things (IoT) technologies, which are implemented in various areas of life: from industry to home devices. However, as the IoT grows in popularity, so does the threat to cybersecurity, especially with wireless networks being more vulnerable to attack. We now consider the role of artificial intelligence (AI) and machine learning (ML) in detecting and preventing attacks on IoT wireless networks.

Штучний інтелект (ШІ) та машинне навчання (МН) відіграють важливу роль у забезпеченні кібербезпеки в контексті Інтернету речей (IoT). Вони дозволяють системам автоматично виявляти аномалії, атаки та інші загрози безпеки у безпровідних мережах та вчасно реагувати на них. Ось кілька способів, які використовуються у ролі ШІ та МН для захисту безпровідних мереж IoT:

- Виявлення аномалій. Системи на основі МН виявляють аномалії у безпровідних мережах IoT, аналізуючи трафік та виявляючи відхилення від типових патернів передачі даних. Це досягається за допомогою алгоритмів, які навчаються розпізнавати нормальну поведінку мережі на основі історичних даних. Наприклад, якщо система виявляє, що зазвичай певний пристрій відправляє дані з певною частотою або обсягом, але виявляється зміна у цих параметрах, це може вказувати на підозрілу активність, таку як атака або несанкціонований доступ. Системи виявлення аномалій можуть навіть автоматично навчатися адаптуватися до нових шаблонів поведінки мережі з часом, щоб покращити точність виявлення аномалій;
- прогнозування ризиків. Штучний інтелект (ШІ) використовується для аналізу даних про попередні атаки та аномальні події у безпровідних мережах IoT з метою прогнозування майбутніх ризиків. ШІ може аналізувати великі обсяги даних для виявлення шаблонів та ознак, що передують атакам або іншим загрозам кібербезпеки. Наприклад, якщо історичні дані показують, що певні типи атак зазвичай відбуваються після певних подій або мають певні характеристики трафіку, ШІ може використовувати цю інформацію для прогнозування майбутніх ризиків та розробки ефективних стратегій захисту;

- автоматизована відповідь. Системи на основі ШІ можуть автоматично реагувати на виявлені загрози у безпровідних мережах IoT, забезпечуючи швидку та ефективну відповідь. Це може включати автоматичне блокування атак, ізоляцію вразливих пристроїв або розробку власних стратегій оборони. Наприклад, якщо система виявляє атаку на певний пристрій, вона може автоматично відключити його від мережі, щоб запобігти подальшим атакам або поширенню інфекції.

На сьогоднішній день вже існують різні системи та продукти, які використовують ШІ та МН для захисту безпровідних мереж IoT. Наприклад, Cisco IoT Threat Defense або Darktrace Industrial.

Cisco IoT Threat Defense - це рішення, розроблене компанією Cisco для захисту безпровідних мереж Інтернету речей (IoT) від кіберзагроз. Це комплексна платформа, яка використовує розумний аналіз даних, машинне навчання та штучний інтелект для виявлення, моніторингу та запобігання різним видам кібератак. Ця платформа аналізує трафік у безпровідних мережах IoT з використанням розумних алгоритмів машинного навчання для виявлення аномальних або підозрілих активностей. Вона враховує різні параметри, такі як типова поведінка підключених пристроїв, характеристики трафіку та інші фактори, щоб виявити відхилення від норми, які можуть вказувати на потенційні загрози. Також вона легко інтегрується з іншими рішеннями безпеки Cisco, такими як Cisco Umbrella, Cisco Identity Services Engine та інші. Це дозволяє створити єдину систему безпеки для всієї інфраструктури організації, включаючи безпровідні мережі IoT.[1]

Darktrace Industrial - це рішення з кібербезпеки, призначене для захисту промислових систем та безпровідних мереж Інтернету речей (IoT) від кіберзагроз. Ця платформа використовує штучний інтелект та алгоритми машинного навчання для виявлення аномалій та вчасного реагування на потенційні загрози. Вона є потужним інструментом для захисту промислових систем та безпровідних мереж IoT від кіберзагроз. Її здатність виявляти аномалії, прогнозувати ризики та автоматично реагувати на загрози допомагає забезпечити надійний рівень безпеки в промислових середовищах.

Список використаних джерел:

1. Cisco IoT Threat Defense. (2022). Cisco IoT Threat Defense: Overview. Retrieved from URL: https://www.cisco.com/c/en/us/solutions/collateral/internet-of-things/iot-threat-defense-smart-building-aag.html

УДК 004.056.523:004.7

РОЗГЛЯД МЕТОДІВ ШИФРУВАННЯ ТА АУТЕНТИФІКАЦІЇ ДЛЯ БЕЗПЕЧНИХ БЕЗПРОВІДНИХ МЕРЕЖ ІНТЕРНЕТУ РЕЧЕЙ

Стрименешенко О.С.,
Науковий керівник – д. т. н., проф. Агеєв Д. В.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Науки, 14, каф. Інфокомунікаційної інженерії ім.Поповського В.В.,
e-mail: oleksandr.strymeneshenko@nure.ua

In recent decades, we have seen an exponential growth in the number of devices that connect to the Internet. From home devices and smart gadgets to industrial sensors and medical devices, the Internet of Things is becoming not only an integral part of our daily lives, but also a key foundation for innovation and development of modern society. However, along with this, the threat to the security and confidentiality of this data is also increasing. Each new connected device in the Internet of Things network opens up a new potential attack vector for attackers. From misuse of devices to leakage of personal information, the risks are growing as the number of connected devices grows. Therefore, the importance of ensuring data security and privacy in wireless Internet of Things networks is becoming more and more important.

Шифрування в безпровідних мережах Інтернету речей (IoT) відіграє ключову роль у забезпеченні конфіденційності даних, переданих через мережу. Призначенням шифрування є перетворення звичайного тексту у нерозбірливий шифрований текст за допомогою криптографічних алгоритмів. Це робить дані незрозумілими для будь-якого, хто не має відповідного ключа для розшифрування.[1]

Одним із найпоширеніших і найбільш ефективних методів шифрування для безпровідних мереж є протокол WPA2 (Wi-Fi Protected Access 2). WPA2 використовує стандартний криптографічний протокол AES (Advanced Encryption Standard), який вважається одним з найбільш безпечних методів шифрування. AES забезпечує високий рівень захисту, що робить його надійним і відповідним для захисту важливих даних в безпровідних мережах IoT.

Наступним важливим аспектом є питання обміну ключами. Під час встановлення безпровідного зв'язку, пристрої взаємодіють, щоб обмінятися ключами, необхідними для шифрування та розшифрування даних. Забезпечення безпеки обміну ключами є критичним, оскільки недостатня захищеність може призвести до компрометації всієї мережі. Також важливо регулярно змінювати ключі шифрування для запобігання можливим атакам на злам.

Загалом, шифрування є невід'ємною частиною забезпечення безпеки в безпровідних мережах IoT. Використання надійних методів шифрування, таких як WPA2 з AES, в поєднанні з правильним обміном ключами та регулярною зміною ключів, є важливими стратегіями для захисту конфіденційності даних у мережі IoT.

Іншими важливим елементом захисту є аутентифікація у безпровідних мережах Інтернету речей (IoT), оскільки вона визначає, чи може пристрій отримати доступ до мережі. Цей процес полягає в перевірці ідентичності користувача чи пристрою, що намагається підключитися до мережі, перш ніж надавати йому доступ до ресурсів.

Один із популярних методів аутентифікації у безпровідних мережах IoT - це використання протоколу EAP (Extensible Authentication Protocol). EAP дозволяє використовувати різні методи аутентифікації, що робить його дуже гнучким та адаптивним до різних потреб і сценаріїв застосування. Наприклад, метод EAP-TLS (Transport Layer Security) використовує сертифікати для аутентифікації, тоді як EAP-TTLS (Tunneled Transport Layer Security) створює захищений тунель для передачі аутентифікаційних даних.

Крім того, важливо враховувати різні фактори аутентифікації для підвищення рівня безпеки. Наприклад, використання біометричних даних, таких як відбиток пальця або розпізнавання обличчя, може забезпечити додатковий рівень впевненості у тому, що лише власник має доступ до пристрою. Одноразові паролі або токени також можуть бути використані для створення унікальних і тимчасових ідентифікаторів, які надаються користувачеві лише на певний час або за певних умов.

Загалом, використання надійних методів аутентифікації та врахування різних факторів аутентифікації є ключовими для забезпечення безпеки у безпровідних мережах IoT. Це дозволяє уникнути несанкціонованого доступу та забезпечити захист конфіденційності даних, які передаються через ці мережі.

Поза шифруванням та аутентифікацією, існують інші методи забезпечення безпеки в безпровідних мережах IoT. Наприклад, використання вогнепровідних стін та систем виявлення вторгнень може допомогти вчасно виявляти та відвертати загрози. Також важливо постійно оновлювати програмне забезпечення пристроїв та мережевого обладнання для закриття виявлених вразливостей.

Список використаних джерел:

1. Savelyev A. V., Кібербезпека в інтернеті речей. Безпека бізнесу. – 2019. – № 2 (46). – С. 45–51.

УДК 004.942:519.816 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.092

МОДЕЛЮВАННЯ БАГАТОКРИТЕРІАЛЬНОЇ ЗАДАЧІ ОПТИМІЗАЦІЇ ВИБОРУ МЕТОДИКИ ПОБУДОВИ СУІБ МЕТОДАМИ ТОМАСА САТІ

Фукс М.А.
Науковий керівник – к.т.н., доцент Добринін І.С.
Харківський національний університет радіоелектроніки, каф. ІКІ
м. Харків, Україна
e-mail: maksymillian.fuks@nure.ua

The aim of the work is to analyze the purpose of the multi-criteria optimization, which is gaining much more popularity during the last decades. Thomas L. Saaty took part in the development of two methods to solve this type of problem, namely the Analytic Network Process and the Analytic Hierarchy Process. When choosing a methodology for building an ISMS, a CISO seeks to determine the best of the available alternatives. This task has been modeled using both of the abovementioned methods taking into account the presence of potential internal relationships between the described criteria.

Метою багатокритеріальної задачі оптимізації є визначення найкращої альтернативи шляхом аналізу декількох критерій в процесі відбору єдиного рішення. При цьому, головну роль у процесі оптимізації грає особа, яка приймає рішення й бере на себе відповідальність, адже саме вона трактує цілі, інтереси та бажання, на основі яких й будується задача оптимальності. Тому процес вирішення таких задач пов'язаний з експертним оцінюванням критеріїв і взаємовідносин між ними.

Запропонований Analytic Hierarchy Process (AHP) Томасом Сааті [1] засновується на декомпозиції проблеми вибору на більш прості складники і поступовому наданні пріоритетів компонентам використовуючи парні порівняння.

Яскравим прикладом багатокритеріальної задачі оптимізації може слугувати вибір певної методики на основі якої будувати систему управління інформаційною безпекою (СУІБ) організації. При виборі методики побудови СУІБ адміністратор безпеки прагне визначити найкращу з наявних альтернатив, при тому, що складність полягає у неоднозначності вибору найкращого рішення [2, с. 17].

The Analytic Network Process (ANP) [3], тобто метод аналізу мереж, є узагальненням (AHP), аналітичного ієрархічного процесу, враховуючи залежність між елементами ієрархії. Тобто ANP доповнює концепцію AHP, але, використовуючи мережеву структуру, надає можливість моделювання наявних зв'язків та залежностей між елементами. Таким чином забезпечується вирішення проблеми неможливості опису задачі прийняття рішень ієрархічним шляхом через наявність взаємодії елементів сусідніх рівнів.

На рис. 1. зображена можлива декомпозиція проблеми вибору на основі AHP [2, с. 18] та ANP.

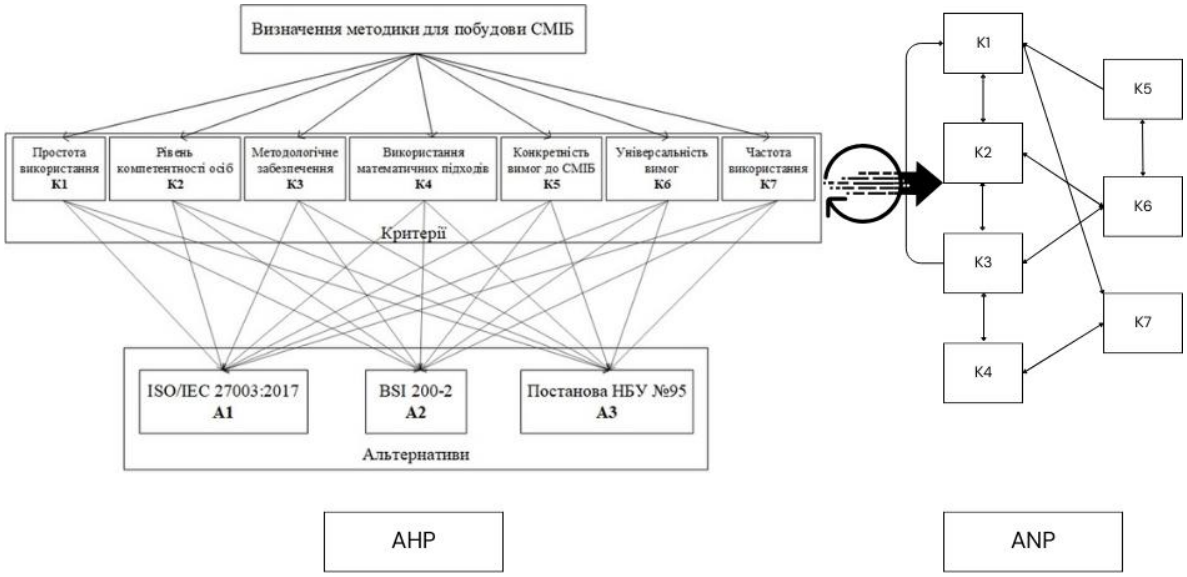


Рисунок 1 – Декомпозиція проблеми вибору методами AHP та ANP

Представлений приклад опису багатокритеріальної задачі вибору методики побудови СУІБ на рис. 1. ураховує наявність потенційних внутрішніх зв'язків між згенерованими критеріями. За допомогою таких зв’язків можна виділити більш сильну залежність одних критеріїв від інших.

Таким чином відбулося розширення моделі AHP задачі вибору певної методики, на основі якої будувати СУІБ, шляхом моделювання складніших взаємозв’язків та залежностей на базі мережевої структури. Завдяки такій трансформації, вимагається більш досконалний аналіз взаємозв’язків та залежностей у розрізі задачі, що розглядається, а це позитивно впливає на результати оптимізації за рахунок збільшення даних для моделювання.

Список використаних джерел:

1. Saaty R. W. The analytic hierarchy process-what it is and how it is used. Great Britain : Pergamon Journals LTD, 1987. – 1 с. – (9).
2. Фукс М. А. Стратегія захисту інформації на основі теоретико-ігрового підходу з використанням економічних показників : кваліфікаційна робота : 125. Харків, 2022. 64 с.
3. Saaty T. L. The analytic network process. Decision making with the analytic network process. P. 1–26. URL: https://doi.org/10.1007/0-387-33987-6_1 (дата звернення: 02.03.2024).

УДК 621.396:004.056.5

ДОСЛІДЖЕННЯ ЗАХИСТУ VPN З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ KILL SWITCH

Юркевич М.О.
Науковий керівник – к.т.н., ст. викл. Марчук А.В
Харківський національний університет радіоелектроніки, каф. ІКІ,
м. Харків, Україна
e-mail: maksym.iurkevych@nure.ua

This research investigates the effectiveness and implications of VPN protection augmented by Kill Switch technology, exploring its capacity to fortify digital privacy, prevent data exposure, and bolster overall cybersecurity in an increasingly interconnected digital landscape.

Технологія віртуальних приватних мереж VPN створює захищений від зовнішних впливів тунель для передачі інформації [1]. Збільшується рівень безпеки та конфіденційності. Інтернет-трафік спрямовується через віддалений сервер. Це маскує IP-адресу користувача та його місцезнаходження, що ускладнює відстеження його активності в Інтернеті для інтернет-провайдера або інших осіб. Як правило трафік, що передається шифрується, однак іноді деякі провайдери VPN іноді цим нехтують. VPN технологія особливо корисна для обходу географічних обмежень, захисту даних від прослуховування в незахищених мережах, покращення конфіденційності.

Одним з недоліків технології VPN є залежність від стабільності інтернет-з'єднання. Низький рівень сигналу, пропадання сигналу, не якісне конфігурування маршрутизаторів або брандмауерів, атаки на канал, що призводять до втрати зв’язку.

Для вирішення цієї проблеми в багатьох VPN вбудовуються програми вимикачі Kill Switch [2].

Якщо VPN-з'єднання несподівано розривається, Kill Switch негайно відключає інтернет-з'єднання. Це дуже важливо, тому що розрив VPN-з'єднання без "вимикача" може розкрити справжню IP-адресу користувача та активність в Інтернеті, що зводить нанівець сенс використання VPN. Цей додатковий рівень захисту гарантує, що навіть якщо основне VPN-з'єднання на мить обірветься, конфіденційні дані залишаться захищеними.

Однак важливо враховувати обмеження використання інтегрованого VPN з Kill Switch:

- потенційний вплив на продуктивність. Шифрування і маршрутизація через віддалений сервер можуть сповільнити швидкість інтернет-з'єднання;
- не є надійним рішенням, тому що, як правило, Kill Switch є частиною VPN, що надаються як комплексне рішення окремими провайдерами.

Надавачі послуг іноді можуть використовувати своє програмне забезпечення для вбудовування реклами, збору інформації про користувачів і інформації, що передається.

Тому актуальною є задача усунення існуючих недоліків системи VPN з Kill Switch.

Використовується два типи Kill Switch: вимикач на системному рівні і на рівні додатків.

Аварійний вимикач на системному рівні блокує всі вхідні та вихідні з'єднання для всієї системи, гарантуючи, що жодна програма або процес не зможе вийти в Інтернет.

Аварійний вимикач на рівні додатків працює так само, але тільки з додатками, які вибирає користувач у меню «Налаштування». Якщо VPN-з'єднання обривається, всі вхідні та вихідні з'єднання відключаються тільки для цих додатків, у той час як всі інші програми, як і раніше, можуть без проблем виходити в Інтернет.

Пропонується відокремити Kill Switch від інтегрованого VPN і зменшити залежність від надавача послуг. Для вирішення цієї задачі можно побудувати вимикач Kill Switch на основі відомої технології iptables [3]. Iptables є функцією ядра і не залежить від служби VPN.

Основні вимоги до впровадження цього рішення: машина з Linux з правами root і встановленим iptables.

Був проведений пошук можливих програмних рішень iptables в якості вимикача Kill Switch. Для перевірки працездатності рішення по використанню вимикача на базі iptables були проведені експериментальні дослідження таких програм. Було дві групи досліджень: для безпроводового і проводового доступу в Інтернет. Отримані результати показали на можливість використання вимикача Kill Switch при спеціальному налаштуванні iptables.

Список використаних джерел

1. If you're using a VPN without a kill switch, you're putting your privacy at risk. CNET. URL: https://www.cnet.com/tech/services-and-software/vpn-kill-switch-what-is-it-and-should-you-enable-it/ (дата звернення: 27.02.2024).

2. VPN kill switch – protected at all times. NordVPN. URL: https://nordvpn.com/features/vpn-kill-switch/ (дата звернення: 01.03.2024).

3. How To Create A VPN Killswitch Using Iptables on Linux. URL: https://linuxconfig.org/how-to-create-a-vpn-killswitch-using-iptables-on-linux (дата звернення: 01.03.2024).

ІНФОКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 004.032:621.391

МЕТОДИ ТА ІНСТРУМЕНТАЛЬНІ ЗАСОБИ ПЛАНУВАННЯ Wi-Fi МЕРЕЖ

Бондар С. О.
Науковий керівник — д.т.н., проф. Рапін В.В.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: stanislav.bondar2@nure.ua

The research topic is devoted to methods and tools for planning Wi-Fi networks. In the context of the rapid development of wireless technologies, especially Wi-Fi, there is a need for effective network planning to ensure the highest level of performance and reliability. The article analyzes various Wi-Fi network planning methods, including analytical and computational approaches. In addition, modern tools designed to automate the planning process, such as software packages and services using artificial intelligence algorithms, are discussed. Highlights the advantages and disadvantages of various Wi-Fi network planning methods and tools, as well as their potential applications in real-world scenarios.

Зростання кількості Wi-Fi мереж та інтенсивності їх використання призвело до підвищення вимог до їх характеристик. Одним із факторів, що впливають на успішне вирішення цієї проблеми, є якість планування мереж. Тому професійне планування Wi-Fi мереж є важливим етапом для створення ефективної та надійної бездротової інфраструктури.

На сьогодні найбільш поширені два способи планування Wi-Fi мереж — це створення і дослідження віртуальної моделі мережі та точка доступу на “палиці”. Перший спосіб передбачає використання спеціальних програм-симуляторів, де створюється віртуальна модель приміщення з віртуальними стінами та іншими перешкодами, враховується вид використаного будівельного матеріалу та специфіка перешкод. На плані розміщуються та конфігуруються віртуальні точки доступу. Можна налаштувати стандарт, канал, ширину каналу, тип антени тощо. Процес інтерактивний: невдале розміщення можна легко скоригувати, трудовитрати невеликі. Сьогодні Wi-Fi є чи не обов'язковим компонентом кожного офісу, ресторану, готелю.

В даний час на ринку пропонується велика кількість таких симуляторів. Це Cisco Packet Tracer, OMNeT++, GNS3, які є безкоштовними і багато потужних плантних професійних симуляторів, наприклад, Riverbed Modeller, NetCracker, Boson NetSim.

Однак цей метод має низку недоліків. Мережеві пристрої у симуляторі обмежені командами та функціями, запрограмованими у них. З цієї причини багато додаткових можливостей, які присутні на реальних мережних пристроях, відсутні в аналогах, що імітуються.

У симуляторах точно прогнозувати поширення Wi-Fi сигналу дуже складно, оскільки на це впливає велика кількість факторів, наприклад: робота промислового обладнання, робота іншого бездротового обладнання в окрузі, робота побутових приладів і інше.

Для кожного приміщення ці фактори будуть унікальними і, отже, Wi-Fi мережа на кожному об'єкті працюватиме по-своєму, що неможливо передбачити та врахувати під час створення її віртуальної моделі.

Симулятори використовуються для моделювання мереж у приміщеннях та на порівняно невеликих територіях. Проблеми виникають при моделюванні Wi-Fi на стадіонах або в паркових зонах.

Другий спосіб планування Wi-Fi мереж має на увазі використання радіообстеження. Радіообстеження до розгортання мережі, тобто, радіорозвідка проводиться для визначення радіочастотної обстановки на об'єкті, що дозволяє зібрати емпіричні дані про радіочастотний спектр.

Це дає можливість ефективно аналізувати зону покриття та якість роботи мережі Wi-Fi. Під час радіорозвідки можна не тільки з'ясувати, чи є у сусідів бездротові мережі, яка їхня потужність, які канали вони використовують і так далі, але й отримати інформацію про перешкоди, що виникають на частотах 2.4 і 5 ГГц. Ця процедура забезпечує безперебійну роботу обладнання та при подальшій експлуатації. Вона дозволяє виявити сторонні перешкоди, що з'явилися, і шуми, які можуть перешкодити нормальному використанню мережі. Радіообстеження дає найбільш повну інформацію про те, як поширюється сигнал у приміщенні, ступеня його згасання у перегородках та стінах. Обстеження об'єкта має ключову перевагу, якої немає у традиційного планування – дані збираються безпосередньо в місці розгортання мережі.

Отримати дані достатньої точності при використанні методу комп'ютерного моделювання неможливо, тому радіообстеження проводиться тільки експериментально. Проведення даної процедури дозволяє налаштувати роботу Wi-Fi найбільш ефективним чином.

Проводити радіочастотне обстеження потрібно після завершення всіх робіт з налаштування бездротового обладнання. З його допомогою можна оцінити, наскільки точно були виконані розрахунки, тобто, наскільки хорошим буде покриття. Наприклад, якщо при радіорозвідці було виявлено слабке джерело шуму, повністю усунути яке не можна, то радіочастотне обстеження після розгортання мережі дасть уявлення про те, чи вдалося мінімізувати негативні фактори. Важливо також мати уявлення про те, наскільки далеко поширюється бездротовий сигнал від цієї мережі, де можливий його прийом та підключення до Wi-Fi. Точка доступу на штативі — це особливий метод обстеження об'єкта до розгортання мережі, при якому одна тестова точка доступу використовується для імітації зони покриття мережі. Вона зазвичай закріплюється на штативі в передбачуваному місці встановлення реальної точки доступу, а

тестувальник обходить обстежуваний простір, щоб визначити зону покриття та фактори, що послаблюють сигнал. Потім точка доступу переноситься до іншого місця і процес повторюється. Розміщення одиночної тестової точки доступу проводиться таким чином, щоб висота відповідала висоті майбутньої постійної точки доступу, потім замір рівня сигналу, переміщення в нову позицію, знову замір, і так далі, поки не настане повне задоволення від рівня сигналу по всій площі і від відповідності плану вимогам по ємності, надмірності і т.д. Заміряють і відзначають на плані сигнал, зазвичай, за допомогою програм для інспектування мереж. Після збору даних з кількох точок з об'єднують і створюють віртуальну карту покриття, як би на об'єкті вже була розгорнута мережа. Причому при обстеженні можна використовувати моделі точок доступу, які потім будуть встановлені на об'єкті.

Радіообстеження та радіорозвідка повинні виконуватися за допомогою спеціалізованого обладнання і в даний час компаніями пропонується маса варіантів, від високопрофесійного обладнання до програмного забезпечення для звичайних ноутбуків та телефонів, які дають лише часткове уявлення про стан мережі.

Додаток AirScout Live від компанії Greenlee перетворить Android-смартфон на зручний та портативний аналізатор WiFi мережі. У безкоштовній версії продукту доступна вся необхідна інформація, яка може знадобитися для швидкого аналізу стану невеликих офісних або домашніх мереж Wi-Fi та виявлення базових проблем з їх продуктивністю. Для використання додаткових функцій, які не доступні в безкоштовній версії програмного забезпечення без додаткового обладнання, потрібно контролер AirScout або комплект, що включає контролер і віддалені клієнти.

Програма NetSpot — це програмне рішення для дослідження, аналізу та покращення WiFi мереж. Комерційна версія використовує картографічний інструментарій для теплової візуалізації зон покриття, однак у безкоштовній версії для домашнього використання він недоступний.

Застосування радіообстеження — це реальна можливість, при правильному проведенні, отримати достатньо підстав для створення працездатного рішення бездротової мережі з передбачуваними характеристиками.

Список використаних джерел:

1. Редакція новин. Що таке радіообстеження Wi-Fi мережі та навіщо це потрібно?. URL: https://bluescreen.kz/chto-takoie-radioobsliedovaniie-wi-fi-sieti-i-zachiem-eto-nuzhno/ (дата звернення: 29.02.2024). WI-FI Heatmap Software – Visualize Coverage and Capacity Ekahau. 2. URL:https://www.ekahau.com/solutions/wi-fi-heatmaps/(дата звернення: 29.02.2024).

УДК 004.77:640.43 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.100

ДОСЛІДЖЕННЯ ДИНАМІЧНОГО САЙТУ ДЛЯ КАФЕ

Валюх Д.М.
Науковий керівник – к.т.н., доц. Кривенко С.А.
Харківський національній університет радіоелектроніки, каф. IMI
Харків, Україна
e-mail dmytro.valiukh@nure.ua,

This work is built around a fictional business case. The business case provides a way to explore cloud-computing topics in the context of relatable business needs. This scenario is intended to provide an example of the real-world applicability of researched technical concepts. In this work, an application was deployed on an Amazon Elastic Compute Cloud (Amazon EC2) instance. The application enables the café to accept online orders. After testing that the application worked as intended in the first AWS Region (the development environment), then an Amazon Machine Image (AMI) was created from the EC2 instance. A second instance of the same application was also deployed as the production environment in another AWS Region.

Робота побудована навколо вигаданого бізнес-кейсу. Бізнес-кейс надає спосіб досліджувати теми хмарних обчислень у контексті відповідних бізнес-потреб. Цей сценарій має на меті надати приклад застосовності технічних концепцій, які досліджуються, у реальному світі.
Після того, як кафе запустило першу версію свого веб-сайту, клієнти розповіли персоналу кафе, як гарно виглядає веб-сайт. Однак, окрім похвали, клієнти часто запитували, чи можна зробити онлайн-замовлення.
Власники бізнесу і менеджер Софія обговорили ситуацію. Вони погодилися, що їхня бізнес-стратегія та рішення повинні зосереджуватися на тому, щоб задовольнити своїх клієнтів і забезпечити їм найкращі враження від кафе.

Бізнес-запит для кафе: Запуск динамічного веб-сайту.

Кав’ярня хоче запровадити онлайн-замовлення для клієнтів, а також можливість персоналу кафе переглядати зроблені замовлення. Їх поточна архітектура веб-сайту, де веб-сайт розміщено на Amazon S3, не підтримує нові бізнес-вимоги.

У першій частині цієї роботи виконується роль Софії та за допомогою Amazon EC2 створено динамічний веб-сайт для кафе [1].
Метою даної роботи є створення динамічного веб-сайту кафе за допомогою Amazon EC2 для розробки моделі дослідження можливостей та вразливостей цього веб-сайту.

У цій роботі виконані такі завдання: аналіз наявного екземпляра EC2; підключення до IDE на примірнику EC2; аналіз середовища стеку LAMP і підтвердження того, що веб-сервер доступний; встановлення програми café; тестування веб-додатку; створення AMI та запуск іншого

екземпляра EC2; перевірка нового екземпляра café [2].

Бізнес-запит для кафе: підготовка екземпляра EC2 для розміщення веб-сайту (Проблема №1).

Кав'ярня хоче запровадити онлайн-замовлення для клієнтів, а також можливість персоналу кафе переглядати зроблені замовлення. Їх поточна архітектура веб-сайту, де веб-сайт розміщено на Amazon S3, не підтримує нові бізнес-вимоги. У першій частині цієї роботи розглядається роль Софії. Налаштовано екземпляр Amazon EC2 так, щоб він був готовий розмістити веб-сайт для кафе. У першому завданні записані деталі про наявний екземпляр EC2, створений в обліковому записі AWS. Завдання 2 – це підключення до IDE на примірнику EC2. AWS Cloud9 — це сервіс, який може працювати на екземплярі EC2. Він забезпечує інтегроване середовище розробки (integrated development environment - IDE), яке включає такі функції, як редактор коду, налагоджувач і термінал. Використовуючи середовище AWS Cloud9, не потрібно завантажувати пару ключів і підключатися до примірника EC2 за допомогою PuTTY або подібного програмного забезпечення Secure Shell (SSH). Використовуючи AWS Cloud9, також не потрібно використовувати інструменти редагування тексту командного рядка (наприклад, vi або nano) для редагування файлів на примірнику Linux. Завдання 3 – це аналіз середовища стеку LAMP і підтвердження того, що веб-сервер доступний. Мета цієї роботи — це налаштувати примірник EC2 для розміщення нового динамічного веб-сайту для кафе. У цьому завданні виконано аналіз того, що вже встановлено.

Нова бізнес-вимога: встановлення динамічної програми веб-сайту на примірнику EC2 (Проблема №2)

У попередньому завданні налаштовано примірник EC2. Тепер відомо, що PHP інстальовано, а середовище програми має запущену реляційну базу даних. Крім того, середовище має запущений веб-сервер, до якого можна отримати доступ з Інтернету. Тепер є основні налаштування для розміщення динамічного веб-сайту для кафе. У другій частині цієї роботи виконана роль Софії та встановлена програма café на примірнику EC2. Завдання 4 – це встановлення програми café. Завдання 5 – це тестування веб-додатку.

Нова бізнес-вимога: створення веб-сайтів для розробки та виробництва в різних регіонах AWS (Проблема №3).

Усі в кафе вражені новим динамічним веб-сайтом, який створила Софія! Клієнти в захваті від того, що тепер вони можуть розміщувати онлайн-замовлення та планувати вивезення десертів. Задоволеність клієнтів зросла завдяки скороченню часу очікування. Однак, крім похвали, виникає ще одна вимога до бізнесу. Власники хотіли б мати два веб-сайти кафе: один веб-сайт, який можна використовувати як *середовище розробки* для моделювання нових функцій і веб-дизайну, перш ніж вони будуть

доступні клієнтам; окремий веб-сайт, на якому розміщено *виробниче середовище*, яким користуються клієнти. Софія обговорила нову вимогу з досвідченим інженером AWS SysOps, коли він одного ранку зайшов у кафе випити кави. Він припустив, що в ідеалі ці два середовища повинні існувати в різних регіонах AWS. Така конструкція матиме додаткову перевагу, забезпечуючи більш надійне аварійне відновлення (disaster recovery - DR) у малоймовірному сценарії, коли регіон AWS стає тимчасово недоступним. Софія зараз дуже зайнята! Коли вона виконує більш вражаючу роботу, її навички стають більш затребуваними. Завдання 6 – це створення AMI та запуск іншого екземпляра EC2. Оскільки веб-сайт кафе вже добре працює на існуючому екземплярі EC2, Софія вирішує дублювати його, створивши з нього AMI. Потім вона запустить новий екземпляр із нового AMI. Для виконання цього завдання виконувалась роль Софії. Перед створенням AMI з цього екземпляра, була створена нова пара ключів, яку важливо мати в цій роботі. Завдання 7 – це перевірка нового екземпляра café.

Софія тепер герой у кафе! Вона створила динамічний веб-сайт, а також дублікат того самого веб-сайту, який працює в другому регіоні AWS.

Софія вирішила призначити перший екземпляр EC2, який вона створила — той, що знаходиться в регіоні us-east-1 — як екземпляр розробки. Другий примірник, який вона створила — той, що знаходиться в Орегоні (регіон us-west-2) — буде робочим примірником.

Таким чином, Софія та будь-які інші розробники додатків можуть тестувати вдосконалення додатків на сайті розробки, не впливаючи на робочий сайт. Потім, коли розробники вирішають, що вдосконалення виглядають добре і вони повністю їх перевірили, вони зможуть перенести код на робочий сайт.

Софія пояснила власникам, що вона зробила. Хоча вони не повністю розуміли всі технічні терміни, які використовувала Софія, вони були раді дізнатися, що веб-сайт тепер може приймати онлайн-замовлення. Вони також були раді почути, що тепер вони можуть тестувати нові вдосконалення веб-сайту, не повідомляючи про ці зміни клієнтам.

2. Список використаних джерел:

1. AWS academy, «Set up demo,» 2024. URL: https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-100-ACFNDS-20-EN/Module_6_EC2+v2.0.mp4.
2. AWS CLI Command Reference. URL: https://awscli.amazonaws.com/v2/documentation/api/latest/reference/ec2/index.html

УДК 621.391:37.018.43 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.103

ОПТИМІЗАЦІЯ ПРОЦЕСУ ОНЛАЙН НАВЧАННЯ НА ПЛАТФОРМІ OPEN EDX

Галій А.К.
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: anna.halii@nure.ua

This work is devoted to the creation of new effective solutions and forms of organization of the educational process, adapted to today's conditions, which is extremely important and relevant in the conditions of martial law in Ukraine. The purpose of the report is to research the Open edX platform and develop customizations for the platform that will help optimize consideration of the needs of users and instructors for distance learning. In this work, the development of customization for Open edX for user registration in the program was carried out.

В усьому світі сьогодні великої популярності та широкого розповсюдження набирають системи електронного навчання (E-learning). Унікальні переваги електронного навчання (необмежений доступ до знань, гнучкість, персоналізоване навчання, економічність, інтерактивність, відстеження продуктивності тощо) роблять його безцінним інструментом для отримання знань і здобуття освіти. Згідно з дослідженнями IBM, програми електронного навчання займають на 40-60% менше часу, ніж традиційне навчання в аудиторії, учасники електронного навчання вивчають у п’ять разів більше матеріалу за той самий проміжок часу [1]. Крім того, можливість навчання в надзвичайних умовах (пандемія, війна тощо) в електронному форматі є надзвичайно актуальним явищем.

В даний момент в багатьох регіонах Україні через війну очне навчання є неможливим. Освітній процес відбувається дистанційно за допомогою інформаційно-комунікаційних мереж та спеціальних освітніх платформ, що дозволяє здобувачам отримувати освіту максимально безпечно та ефективно. В умовах воєнного стану освіта потребує нових підходів до навчання, швидких та ефективних рішень, інноваційних форм організації освітнього процесу, адаптованих до умов сьогодення [2]. Тому галузь електронного навчання безупинно розвивається, з’являються нові технології, а також інструменти для розвитку і покращення створюваного контенту.

Існують різні платформи для електронного навчання, серед яких великої популярності набули платформи з відкритим кодом (наприклад, Moodle, Open edX, Canvas тощо). В Україні широко використовується платформа Open edX. Open edX – це навчальна платформа з відкритим кодом, створена Гарвардським університетом та Массачусетським

технологічним інститутом. Open edX – це веб-платформа для створення, надання та аналізу онлайн-курсів, це програмне забезпечення, на якому працює edx.org та багато інших освітніх онлайн-сайтів [3].

Метою доповіді є дослідження платформи Open edX та розробка кастомізації для платформи, що допоможе оптимізувати врахування потреб користувачів та інструкторів для дистанційного навчання.

Кастомізація – це зміна продукту чи послуги відповідно до уподобань чи вимог особи або компанії. У стандарній інсталяції платформи немає реєстрації у програму, як наприклад є реєстрація на курс. Моя мета розширити стандартний функціонал для потреб користувачів платформи. В даній роботі виконано розробку кастомізації для Open edX для реєстрації у програмі.

В роботі застосовано наступні критерії приймання для бізнес логіки:

– студент вважається зарахованим до програми, якщо він зарахований принаймні на один з курсів програми;

– оброблюються та відображаються помилки реєстрації.

Back-end кастомізації виконаний на мові програмування Python. В роботі створено контролер program_enroll, що відповідає за приймання запиту та його обробку. У контролері є перевірка стану користувача, при негативному сценарії контролер відправляє негативний HttpResponse клієнту зі статус кодом 401 – Unauthorized. При позитивному отримується інстанс програми за її ідентифікатором та відбувається реєстрація користувача на курси. При успішній реєстрації на усі курси у програмі клієнт отримує HttpResponse зі статус кодом 200 – Success.

Front-end частина кастомізації створена за допомогою бібліотеки React. Логіка полягає у тому, що при натисканні на кнопку «Enroll in program» відправляється запит на Back-end, який обробляється та відповідає статус кодом. Front-end приймає відповідь та на основі статус коду відображає певну інформацію. Мої зміни полягають у компоненті, що відповідає за відображення головної частини сторінки програми.

Список використаних джерел:

1. Stunning Statistics That Prove The Power Of eLearning // Schoox. 2018. URL: Режим доступу до ресурсу: https://www.schoox.com/blog/stunning-statistics-that-prove-the-power-of-elearning/.

2. Загальна середня освіта // Міністерство освіти і науки України. 2024. URL: https://mon.gov.ua/ua/tag/zagalna-serednya-osvita.

3. Open edX Developer’s Guide // Axim Collaborative. 2024. URL: https://docs.openedx.org/en/latest/developers/references/developer_guide/index.html.

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.105

РОЗРОБКА ПРОГРАМАТОРА ДЛЯ РАДІОСТАНЦІЙ MOTOROLA GM-300, M-120

Головенко О.О.
Науковий керівник – доцент кафедри IMI Іваненко С.А.
Харківський національний університет радіоелектроніки, каф. IMI
м.Харків, Україна
e-mail: oleksii.holovenko@nure.ua

The Motorola GM-300 and M-120 radios have a wide frequency range that allows them to work in a variety of conditions and environments. However, to use these stations effectively, you need to be able to program their settings, including frequencies and signal parameters.This report describes the development of a programmer specifically designed for these radios. This programmer will allow users to easily and efficiently program the settings of their radio stations, which will ensure optimal operation and high quality of communication. In addition, the programmer also provides the possibility of rebroadcasting the signal, which significantly expands the range of radio stations.

Робота присвячена розробці програматора для радіостанцій серії MOTOROLA GM-300 та інших.

Рисунок 1 – Радіостанція Motorola GM-300

Не дивлячись на те, що радіостанція доволі давно знята з виробництва, вона не втратила своєї актуальності і зараз, завдяки визначним технічним характеристикам, надійності і не високій вартості на вторинному ринку.

Через це вона набула значної популярності серед інженерів зв’язку, зокрема для організації ретрансляторів.

Таблиця 1 – Технічні характеристики Motorola GM-300

Робочі частоти	134-174/400-430/440-470 МГц
Вихідна потужність	25/40 Вт
Кількість каналів	16, прогарамуються з комп'ютера
Частотне рознесення каналів	12,5 кГц

Габаритні розміри	50.8×178×198мм
Вага	1700 грам

Однак негативною стороною сучасного використання цих радіостанцій є особливості програмно-апаратного забезпечення, а саме:

- застарілість оригінальної програми MOTOROLA RSS для прошивки, яка розрахована під використання в системі DOS;

- складність пошуку оригінального програматора та вимоги до його використання із комп'ютером, який має апаратний COM-порт.

Тому мета роботи полягає в розробці доступного програматора, та випробування можливості його використання із MOTOROLA RSS на сучасних операційних системах Windows, із використанням емуляторів DOS.

Схема досліджуваного програматора зображена на рис.2.

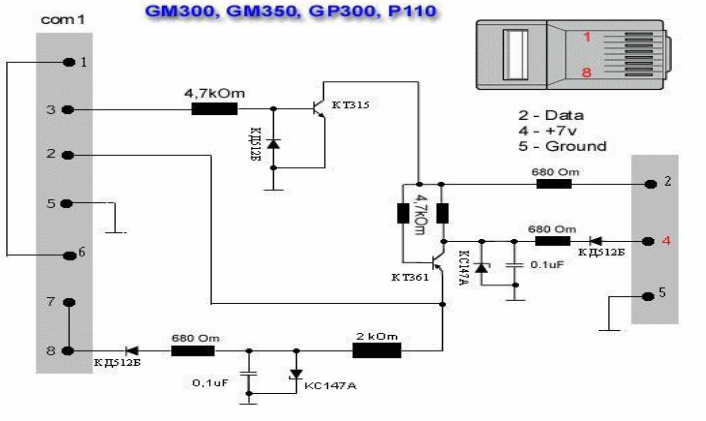


Рисунок 2 – Схема програматора

Він розрахований на використання COM-порту комп'ютера та LAN-роз'єму на передній панелі радіостанції. Схема зібрана на транзисторах КТ315 та КТ361, які можна замінити на КТ3102 та КТ3107. КД512Б – діоди КД503, 2Д521, 1N4148. КС147А – стабілітрони 5В.

Список використаних джерел:

1. Motorola GM300 URL: https://radioua.biz/radiostanciyi/motorola-gm300-detail (дата звернення: 03.03.2024)

УДК 004.773:004.75 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.107

РОЗРОБКА КОМПОНЕНТІВ СИСТЕМИ ДЛЯ ОБМІНУ ПОВІДОМЛЕННЯМИ В РЕЖИМІ РЕАЛЬНОГО ЧАСУ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ХМАРНИХ СЕРВІСІВ

Гробовий Д. В.
Науковий керівник – проф. Безкоровайний В. В.
Харківський національний університет радіоелектроніки, каф. СТ
м. Харків, Україна
e-mail: danylo.hrobovyi@nure.ua

In today's digital world, the ability to communicate instantly is not just a convenience but a necessity for both personal connections and business operations. Developing an application for real-time messaging using cloud services is at the forefront of meeting this need. The integration of cloud technology ensures that this kind of app can offer scalable, reliable messaging solutions that are accessible from anywhere, at any time. This initiative addresses the essential demand for immediate communication while leveraging the power and flexibility of the cloud. By focusing on the technical and practical aspects of cloud-based messaging, developers can create a platform that facilitates seamless, secure exchanges of information. This approach not only simplifies communication but also introduces a level of efficiency and connectivity that is vital in our fast-paced digital age. The journey of developing such an application involves navigating through various challenges, from ensuring data security to providing a user-friendly interface. Yet, the potential to enhance how we communicate makes this venture a compelling and worthwhile pursuit.

Месенджери та додатки для обміну повідомленнями в режимі реального часу стали невід'ємною частиною нашого щоденного життя, сприяючи миттєвому зв'язку між людьми незалежно від відстані. Розвиток хмарних технологій відкрив нові можливості для створення більш ефективних та масштабованих комунікаційних рішень. Використання хмарних сервісів у розробці додатків для обміну повідомленнями може значно поліпшити їхню продуктивність, безпеку та доступність.

Мета даної роботи полягає у створенні додатку для обміну повідомленнями, який використовує хмарні технології для забезпечення високої масштабованості та надійності сервісу. Додаток надаватиме користувачам можливість миттєвого обміну текстовими повідомленнями, медіафайлами, а також створення групових чатів. Об'єктом дослідження є додаток, що інтегрує хмарні сервіси для обміну повідомленнями, а предметом дослідження є програмне забезпечення та хмарні технології, які забезпечують його функціонування.

Під час аналізу існуючих рішень було розглянуто такі популярні месенджери, як «Telegram», «WhatsApp» та «Signal». Вони пропонують

широкий спектр функцій для комунікації, але кожен із них має свої особливості та обмеження, що стосуються приватності, безпеки даних та інтеграцій. Новий додаток буде зосереджений на забезпеченні високого рівня безпеки обміну повідомленнями та простоті інтеграції хмарними платформами, що дозволить користувачам з легкістю зберігати та обмінюватися медіафайлами або транслювати медіапотоки.
Розробка додатку включає в себе такі основні компоненти:

- Функціональні компоненти: це інтерфейс користувача, система управління повідомленнями, механізми аутентифікації та авторизації, а також інтеграція з хмарними сховищами для транслювання та зберігання медіафайлів.
- Компоненти системи опрацювання даних: включають в себе сервери для обробки запитів в реальному часі, бази даних для зберігання інформації про користувачів та їх повідомлення, а також системи керування мережевими з'єднаннями.

Інтеграція хмарних технологій у розробку додатку для обміну повідомленнями відкриває ряд переваг:

- Масштабованість: хмарні сервіси дозволяють легко масштабувати інфраструктуру в залежності від потреб користувачів, забезпечуючи високу доступність сервісу незалежно від кількості активних користувачів.
- Безпека: хмарні платформи пропонують передові рішення для захисту даних та інформаційної безпеки, що є критично важливим для додатків, що працюють з персональною інформацією.
- Економічність: використання хмарних сервісів зменшує потребу в значних початкових інвестиціях для розгортання та підтримки власної інфраструктури, знижуючи загальні витрати на розробку та обслуговування.

У підсумку, новий додаток для обміну повідомленнями, розроблений з використанням хмарних технологій, він буде забезпечувати високу швидкість обміну повідомленнями та високий рівень безпеки, сприяючи ефективній та безпечній комунікації між користувачами.

Список використаних джерел:

1. AWS Messaging and Targeting: вебсайт: https://aws.amazon.com/products/messaging/
(дата звернення: 05.03.2024).
2. MDN Web Docs WebSocket: вебсайт: https://developer.mozilla.org/en-US/docs/Web/API/WebSockets_API
(дата звернення: 05.03.2024).
3. Google Cloud Messaging Solutions: https://cloud.google.com/solutions/messaging/
(дата звернення: 05.03.2024).

УДК 621.396.676:623.746-519
DOI https://doi.org/10.30837/IYF.PDICIMT.2024.109

АНАЛІЗ АНТЕННИХ СИСТЕМ УПРАВЛІННЯ БПЛА

Домарєв А.С.
Науковий керівник – доцент. Іваненко С.А.
Харківський Національний Університет Радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail:andrii.domariev@nure.ua

This study provides analysis of antenna systems used in unmanned aerial vehicles (UAVs). The research explores various types of antennas, their characteristics, and applications in the UAV industry. The practical significance of this research lies in enhancing the efficiency and safety of UAV operations across diverse fields. By selecting the most suitable antenna system, UAV manufacturers and operators can improve communication reliability, extend operating ranges, and enhance overall performance. This study serves as a valuable resource for engineers, researchers, and professionals involved in UAV technology development and implementation.

Безпілотні літальні апарати (БПЛА) стали невід'ємною частиною сучасних технологій, знаходячи широке застосування у військовій справі, аерофотозйомці, агропромисловості та інших галузях. Одним з ключових елементів управління БПЛА є антенні системи, які відповідають за забезпечення зв'язку та керування.

Аналіз антенних систем управління БПЛА є актуальним завданням, оскільки від їхньої ефективності залежить успішність місій та дальність і безпека використання таких апаратів. Мета даного дослідження полягає в аналізі готових рішень для керування БПЛА, та розробка визначення найбільш ефективних антенних конфігурацій. Результати цього дослідження можуть бути корисними як для операторів БПЛА, так і для виробників.

Керування БПЛА відбувається як правило в діапазоні частот від 700 MHz до 5.8 GHz. Обрання конкретних частот залежить від:

- необхідної швидкості передачі сигналу;
- умов розповсюдження радіохвиль;
- можливості встановлення тих чи інших типів антен та їх розмірів.

За сукупністю цих показників підбираються оптимальні частоти, якщо мова йде про модульні конструкції із можливістю обрання радіопередавального обладнання.

Для керування на великій відстані при однакових потужностях радіопередавачів за можливості потрібно обирати нижчі частотні діапазони, а для мініатюризації антен вищі.

Основні антени які використовуються на БПЛА: спрямовані і всеспрямовані. У сфері БПЛА широке застосування отримали антени як лінійної так і кругової поляризації.

На рис. 1 представлені всеспрямовані антени. Цей вид антен розповсюджує сигнал рівномірно в усі боки, тому цей тип антен найчастіше розташований на самому БПЛА.

Рис. 1 – Всеспрямовані антени кругової поляризації

Направлені антени можемо бачити на рис. 2.

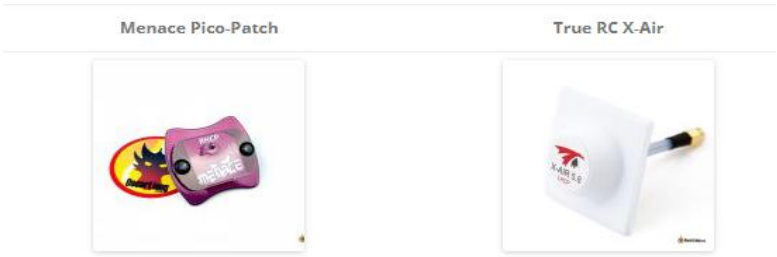


Рис.2 – Направлені антени кругової поляризації

Вони мають перевагу в дальності дії, оскільки в них високий коефіцієнт підсилення, але є обмеження кутом прийому/передачі сигналу. Такий вид антен найчастіше використовується на боці оператора, і вони встановлюються на пульт або окуляри.

Отже, для ефективного використання БПЛА необхідно враховувати, що якість антенного обладнання грає визначний фактор і треба враховувати їх характеристики: частота роботи, направленість та поляризація.

Список використаних джерел:

1. «Що таке FPV і в чому різниця 2.4ГГц і 5.8ГГц ?» *.maroder.com.ua*.
URL: https://maroder.com.ua/obzor/chto-takoe-fpv-i-v-chem-raznitsa/ (дата звернення 04.03.2024)

2.«Як працюють FPV дрони?». *aviatsiyahalychyny.com* URL:https://www.aviatsiyahalychyny.com/blog/rozbyraiemos-iak-pratsiuiut-fpv-drony/ (дата звернення 04.03.2024)

3. «Базові знання по радіо для FPV простими словами».*youtube.com* URL:https://www.youtube.com/watch?v=x9G1zFIQhZs&t=136s (дата звернення 04.03.2024).

УДК 004.65 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.111

ДОСЛІДЖЕННЯ МЕТОДІВ ОПТИМІЗАЦІЇ ЗАПИТІВ В SQL SERVER ДЛЯ ЗАБЕЗПЕЧЕННЯ ВИСОКОЇ ПРОДУКТИВНОСТІ ТА МАСШТАБОВАНОСТІ КОРПОРАТИВНИХ ДОДАТКІВ

Жабський Д.С.
Науковий керівник – к.т.н., ст. викл. Яцик М.В.
Харківський національний університет радіоелектроніки, каф. СТ
e-mail: dmytro.zhabskyi@nure.ua

The exploration of query optimization methods in SQL Server is undertaken to enhance the performance and scalability of enterprise applications. The necessity for efficient data handling and processing in large-scale systems is paramount in today's data-driven environment. This study delves into advanced techniques and approaches for optimizing SQL Server queries, including execution plan analysis, indexing, and data partitioning, to significantly improve system responsiveness and throughput.

У цій роботі розглядається розробка методів оптимізації запитів в SQL Server, які дозволяють підвищити продуктивність та масштабованість корпоративних додатків. Оптимізація запитів є критично важливою для забезпечення швидкодії та ефективності обробки даних у великих обсягах. Аналіз планів виконання, індексація та партиціонування даних є ключовими аспектами, на які зосереджено увагу у цьому дослідженні.

Значна увага приділяється використанню аналітичних і практичних підходів до оптимізації запитів. Це охоплює глибоке розуміння внутрішньої архітектури SQL Server, а також застосування сучасних методик та інструментів для аналізу та покращення продуктивності системи [1].

Основні напрямки дослідження включають:

– аналіз планів виконання запитів, який допомагає ідентифікувати неефективні запити та їх компоненти, використовуючи інструменти SQL Server Management Studio (SSMS) та Transact-SQL (T-SQL) [2];

– індексація, включаючи створення і оптимізацію індексів, для зниження часу обробки запитів, з особливим акцентом на вибір ключових стовпців для індексації та використання стратегій індексації [3];

– партиціонування даних як метод розділення даних на частини для покращення продуктивності та управління обсягами даних.

Використання технології In-Memory OLTP [4] для оптимізації роботи з високопродуктивними транзакціями та аналіз впливу на продуктивність системи також є частиною цієї роботи. Практична реалізація запропонованих методів демонструє їх ефективність у реальних корпоративних додатках.

Це дослідження демонструє, як застосування цілеспрямованих методів оптимізації може значно підвищити продуктивність та

масштабованість корпоративних систем, що працюють на базі SQL Server, тим самим сприяючи ефективнішому використанню ресурсів та покращенню загальної швидкодії системи.

Список використаних джерел:

1. Microsoft SQL Server 2019 Documentation. [Електронний ресурс] – https://docs.microsoft.com/en-us/sql/sql-server/sql-server-2019-documentation.
2. Itzik Ben-Gan. T-SQL Querying. Microsoft Press, 2015.
3. Grant Fritchey. SQL Server Execution Plans. Redgate Books, 2018.
4. Kalen Delaney. SQL Server Internals: In-Memory OLTP. Redgate Books, 2017.

УДК 004.77:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.113

НОВІ МОЖЛИВОСТІ ОБРОБКИ ІНФОРМАЦІЇ В ІКС: ВИКЛИКИ ПІД ЧАС ВІЙНИ

Кабаченко В.О.
Науковий керівник – доц. каф. ІМІ Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: viacheslav.kabachenko@nure.ua.

The war in Ukraine has had a significant impact on all aspects of life, including the information and communications sector. On the one hand, new opportunities for information processing and communication have emerged due to the development of artificial intelligence, cloud technologies, and the Internet of Things. On the other hand, the war has also created new challenges, such as the spread of disinformation, cyberattacks, and disruption of critical infrastructure. In times of war, access to reliable and unbiased information becomes even more important than ever. ICT (information and communication systems) play a key role in providing people with such information, offering new opportunities for its processing.

Інформаційно-комунікаційні система (ІКС) це сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле [1]. В умовах війни доступ до достовірної та неупередженої інформації стає ще більш важливим, ніж будь-коли. ІКС (інформаційно-комунікаційні системи) відіграють ключову роль у забезпеченні людей такою інформацією, пропонуючи нові можливості для її обробки. В ІКС постійно вдосконалюються засоби і методи обробки інформації, які вдосконалюють способи взаємодії з даними та забезпечують більш ефективну роботу звичайних користувачів та військових, щоб швидше приймати рішення та надавати більш точно і правдиву інформацію. Сучасні ІКС використовують нейронні мережі та інші методи штучного інтелекту для виявлення взаємозв'язків у великих обсягах даних, що дозволяє здійснювати прогнозування, оптимізацію та приймати стратегічні рішення та швидше діяти в екстрених ситуаціях на основі аналізу інформації.

Тенденцій і нова можливості обробки інформації (ІКС) під час війни:

1. Штучний інтелект (ШІ) широко використовується в обробці інформації. ШІ може допомогти збирати та аналізувати розвіддані, виявляти цілі, координувати дії військ та керувати безпілотними системами також може автоматизувати небезпечні завдання, такі як розмінування, розвідка та бойові дії.
2. Обробка природної мови – це нові методи та моделі обробки природної мови, які дозволяють комп'ютерам краще розуміти та генерувати людську мову. Також може допомогти виявити та протидіяти

дезінформації, пропаганді та фейковим новинам і допомогти зберегти культурну спадщину, яка пошкоджена або зруйнована війною.

3. Комп'ютерний зір - відкриває нові можливості в розпізнаванні образів, аналізі відео, розробці систем відстеження та розпізнаванні обличь. Також може допомогти з логістикою, координацією допомоги та пошуком зниклих людей.

4. Квантові обчислення мають змінити підхід до обробки інформації. Квантові комп'ютери можуть зламати будь-яке шифрування, яке використовується сьогодні, що може призвести до крадіжки даних, кібератак та інших проблем.

5. Розширена реальність (Augmented Reality, AR) відкриває нові можливості для взаємодії з інформацією в реальному часі. AR може допомогти солдатам краще бачити поле бою, візуалізувати дані та отримувати інформацію про цілі також може використовуватися для проектування прицільних сіток на окуляри солдатів, що може допомогти їм точніше стріляти.

6. Інтернет речей (Internet of Things, IoT) - збільшення кількості підключених пристроїв сприяє величезному обсягу даних, які можна збирати та аналізувати для оптимізації процесів у різних сферах, від міст до промисловості.

7. Блокчейн може використовуватися для захисту даних про військових та мирних жителів від кібератак. Також для створення децентралізованих фінансових систем, які можуть допомогти українській економіці залишатися стійкою під час війни.

Технології обробки зображень та відео також розвиваються швидкими темпами, що відкриває нові можливості для аналізу розвідки в умовах військового стану та має великих обсягів візуальних даних. Системи розпізнавання об'єктів, облич та інших елементів стають дедалі точнішими і швидшими, що дозволяє застосовувати їх у різних сферах, від медицини до маркетингу. Ще однією перспективною галуззю є розвиток квантових обчислень, що може значно розширити можливості обробки інформації в ІКС [2]. Квантові комп'ютери в змозі ефективно обробляти складні алгоритми та розв'язувати задачі, які зараз вважаються непідйомними для класичних комп'ютерів.

Усі ці нові можливості обробки інформації в ІКС покликані покращити продуктивність, забезпечити точність аналізу та зробити взаємодію з даними більш інтуїтивно зрозумілою та ефективною для військових. Також допомогти людям отримати доступ до достовірної та неупередженої інформації, що є надзвичайно важливо під час війни.

Список використаних джерел:

1. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління

технологічними процесами [Електронний ресурс] // Наказ Адміністрації Держспецзв\'язку. – 2023. – Режим доступу до ресурсу: https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami.

2. Обробка інформації на основі блокчейн в ІКС [Електронний ресурс] // IEEE. – 2021. – Режим доступу до ресурсу: https://ieeexplore.ieee.org/document/8340112.

3. Обробка інформації [Електронний ресурс] // Вища школа. – 2021. – Режим доступу до ресурсу: https://stud.com.ua/59732/informatika/obrobka_informatsiyi.

4. Положення про інформаційно-комунікаційну систему 112 [Електронний ресурс] // Міністерстві юстиції України. – 2023. – Режим доступу до ресурсу: https://ips.ligazakon.net/document/re40044?an=1.

УДК 004.738.5:339]:004.056

ДОСЛІДЖЕННЯ ЗАСОБІВ БЕЗПЕКИ В СИСТЕМАХ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Карабанов Д.С., Чеботарьова Д.В.
Науковий керівник – проф. Безрук В.М.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: denys.karabanov@nure.ua
e-mail: dariia.chebotarova@nure.ua

The work is devoted to the research of current problems of information security and the analysis of modern security tools in electronic commerce systems. Recently, the number of cyber-attacks and fraud in e-commerce systems has increased significantly. A comprehensive approach to solving information security problems, including the use of modern software and technical tools, improvement of regulatory and legal support, implementation of certain organizational measures, will allow to achieve effective results in the field of protection of electronic commerce systems.

В усьому світі швидкими темпами зростають масштаби впровадження та використання систем електронної комерції. Сьогодні ринок електронної комерції величезний і постійно змінюється. Великим поштовхом для повсюдного використання електронної комерції стала пандемія covid-19, що призвела до суттєвого збільшення онлайн покупок та цифрових фінансових послуг під час карантинних обмежень. За цей час компанії і користувачі відчули всі переваги електронної комерції, тому тепер її використання тільки зростає. Навіть в Україні, незважаючи на війну, ринок електронної комерції продовжує зростати.

Електронна комерція та цифрові фінансові послуги демонструють значні переваги: зручність, суттєва економія часу, новий рівень ефективності та прозорості, автоматизація процесів, зменшення кількості помилок, покращення обслуговування клієнтів, зниження витрат на організацію та підтримку бізнесу, спрощення розширення бізнесу та виходу на міжнародні ринки та багато інших. Серед недоліків найважливіше місце посідає проблема безпеки конфіденційних даних та фінансових операцій. Зі зростанням обсягів електронної комерції збільшується кількість кібератак, шахрайства, фінансових втрат та витоків даних.

Основними кіберзагрозами для електронної комерції є фішинг, malware- та ransomware-атаки, SQL-ін’єкції, DDoS та брутфорс-атаки, спрямовані на злам доступу до облікових записів [1]. Крім того, зловмисники постійно використовують нові технології та вдосконалюють свої методи. Саме тому питання безпеки є надзвичайно актуальними та потребує досліджень та розробки нових засобів безпеки. Забезпечення

безпеки електронної комерції є важливим для підтримки довіри клієнтів, мінімізації фінансових втрат та дотримання відповідних норм і галузевих стандартів [2].

Метою доповіді є дослідження актуальних проблем інформаційної безпеки та аналіз сучасних засобів безпеки в системах електронної комерції. В роботі детально проаналізовано проблеми безпеки (вразливості, загрози, атаки) та різні засоби (методи, інструменти, програми) захисту систем електронної комерції.

В системах електронної комерції важливо захищати дані всіх користувачів та гарантувати безпеку всіх транзакцій, особливо фінансових. Тому надійний захист систем електронної комерції вимагає побудови концепції безпеки на основі багатогранного та комплексного підходу. Значно підвищити безпеку мережі та знизити ризики кібератак допоможе впровадження та використання таких засобів: управляння доступом та багатофакторна автентифікація; шифрування SSL; брандмауери веб-додатків; рішення для захисту від DDoS-атак; вдосконалена аналітика та алгоритми машинного навчання для виявлення підозрілих моделей і поведінки, які можуть свідчити про шахрайство; аналітика ризиків даних; оцінка вразливостей та тестування на проникнення; постійні оновлення безпеки та регулярні виправлення; неперервне навчання співробітників; моніторинг мережі та виявлення вторгнень, використання протоколів захищеного обміну інформацією та безпечних електронних транзакцій тощо.

Комплексний підхід до вирішення проблем безпеки інформації, зокрема використання сучасних засобів програмно-технічного характеру, удосконалення нормативно-правового забезпечення, вжиття актуальних організаційних заходів, дозволить досягнути ефективних результатів у сфері захисту інформації та фінансових транзакцій в системах електронної комерції.

Забезпечення надійної безпеки мережі для електронної комерції є першорядним. Кіберзагрози постійно розвиваються, кількість атак збільшується, тому фінансовим установам і окремим користувачам вкрай важливо застосовувати найкращі методи захисту конфіденційних та фінансових даних.

Список використаних джерел:

1. Липська В. 10 головних челенджів для електронної комерції у 2024 році [Електронний ресурс] / В. Липська // Wezom. – 2024. – Режим доступу до ресурсу: https://wezom.com.ua/ua/blog/10-golovnih-chelendzhiv-dlya-elektronnoyi-komertsiyi-u-2024-rotsi.

2. Payment security: An in-depth, actionable guide for businesses [Електронний ресурс] // Stripe. – 2023. – Режим доступу до ресурсу: https://stripe.com/resources/more/payment-security.

УДК 004.89:613.2 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.118

ПРОБЛЕМИ ЗДОРОВОГО ХАРЧУВАННЯ ТА ЇХНЄ ВИСВІТЛЕННЯ В ІНФОРМАЦІЙНИХ МОБІЛЬНИХ ЗАСТОСУНКАХ

Коваленко А. В.
Науковий керівник – к. т. н., доц. Носова Я. В.
Харківський національний університет радіоелектроніки, каф. ШІ
м. Харків, Україна
e-mail: arsenii.kovalenko@nure.ua

The present investigation is dedicated to the examination of mobile applications aimed at addressing issues pertaining to healthy dietary practices. An exploration into the significance of sound nutritional habits within the human sphere is conducted. Central to the inquiry is the identification of nutritional disparities as the principal concern addressed by informational applications. The primary avenues of digital interventions in the realm of healthy nourishment are delineated. Furthermore, the merits of employing a chatbot as a potent instrument for tailoring interactions to individual users while concurrently accessing a broad demographic are substantiated.

Раціональне збалансоване харчування є одним з найголовніших чинників стану здоров’я людини й суспільства. З порушеннями харчової поведінки пов’язують найбільш розповсюджені захворювання, що призводять до важких, нерідко летальних випадків. Здорове харчування стає запорукою комфортності життя та його повноцінності. Формування культури збалансованого споживання якісної їжі від самого народження дитини забезпечує її щасливе тривале життя та різносторонню реалізацію у суспільстві. Особливо гостро ситуація виглядає в Україні, яка за спостереженнями дослідників, очолює список європейських країн за смертністю через порушення здорового харчування [3].

Проблема культури харчування широко висвітлюється у сучасних наукових дослідженнях. Зокрема, зауважується на зменшенні споживання рослинної їжі, зелені та овочів на користь продуктам тваринного походження [3]. Серед основних ознак порушення харчової поведінки називається зловживання складних вуглеводів, трансжирів та жирів тваринного походження, консервантів та підсилювачів смаку, недотримання режиму харчування [4]. Перевага споживання тих чи інших видів продуктів спричиняє незбалансованість харчування, нестачу споживних речовин, що призводить до розвитку хронічних хвороб.

Недостатня поінформованість споживачів щодо складу продуктів та поживних речовин для повноцінного життя стає причиною зловживання неякісною їжею з великою кількістю консервантів, підсилювачів смаку та покращувачів зовнішнього вигляду, хімічних добавок. На подолання цієї проблеми спрямовані зусилля зі створення інформаційних застосунків,

присвячених поширенню здорового способу життя та харчування. Окрема увага приділяється розробці програм з «моніторингу стану здоров'я громадян» [5] та рекомендацій щодо його покращення. Інші застосунки орієнтовані на збирання даних та визначення загального стану, діагностики здоров'я людини [4]. Зауважується також на комплексності функціоналу застосунка [5], який допомагає вирішенню відразу декількох завдань. Не менш важливою складовою є створення мобільних програм для «маломобільних груп населення» [4], з метою інформаційної підтримки й популяризації здорового харчування для такої мало захищеної категорії користувачів. Серед численного різноманіття інформаційних інструментів особливо ефективними визначаються мобільні застосунки та месенджери, у яких пропонується розміщати тести та опитування [3], задіяти видовищну складову у вигляді піктограм тощо. Наведені прийоми дозволяють охопити якомога широку аудиторію користувачів, дослідження якої потребує особливої уваги.

Серед користувачів дослідники вирізняють декілька різних категорій та досліджують особливості переваг кожної з груп у виборі застосунків для здорового харчування. Зокрема, виділяються «мотивовані здоров'ям, мотивовані тілом та мотивовані розумом» люди [2]. Незважаючи на різні смаки між групами у підході до здорових дієт та продуктів, спільним критерієм є «зручна навігація та надійна база даних про продукти» [2]. Наявність спільних ознак дозволяє зробити програму однаково затребуваною серед різних верств населення. Широко розповсюдженою є також практика поєднання в застосунках інформації зі здорового харчування, фізичної активності та здорового способу життя [5]. Однак така універсальність може призвести до втрати певної частини аудиторії через різницю в інтересах та інформаційному попиті. Є й зворотній підхід, коли створюються чат-боти для вибіркового сегменту споживачів, як наприклад, для осіб з головним болем [1].

Вирішення проблем здорового харчування за допомогою чат-бота є особливо перспективним, завдяки інтерактивному характеру його функціонування та наявності необхідної для людини комунікації, що активізує та робить інформаційний процес більш видовищним, захопливим та продуктивним. Чат-бот виглядає зручнішим за інші мобільні застосунки, оскільки останні потрібно окремо встановлювати, в той час коли чат-бот розміщується у месенджері, яким людина зазвичай користується найчастіше. Інформаційну базу мобільних застосунків переважно складають рецепти, опис продуктів та складових речовин. Функціонал мобільного застосунку часто складається зі щоденника харчування, лічильника калорій, споживання води тощо [4]. У чат-боті ці опції теж можуть бути доступні, проте комунікація у чат-боті робить підхід до користувача більш індивідуальним.

Найбільш ефективним при застосуванні чат-бота виглядає зосередження на одному з напрямків, наприклад, харчування й усіх супутніх з ним підтем: рівні й правила вживання їжі, вплив харчової поведінки на гормональний обмін, біохімічні процеси людського організму та особливості засвоєння вітамінів та мінералів, ефективність поєднання різних речовин при одночасному прийомі в їжу. Це дозволить сформувати індивідуальний підхід до кожного користувача, котрий у спілкуванні з чат-ботом матиме змогу навчитися жити в діалозі з власним організмом, виробити індивідуальну модель харчової поведінки відповідно до особливостей своєї природи. Такі застосунки водночас звужені у базі та функціоналі, але, з іншого боку, розширені через різні причини походження симптомів, що вимагає доволі великої інформаційної бази.

Список використаних джерел

1. Ulrich S, Gantenbein AR, Zuber V, Von Wyl A, Kowatsch T, Künzli H Development and Evaluation of a Smartphone-Based Chatbot Coach to Facilitate a Balanced Lifestyle in Individuals With Headaches (BalanceUP App): Randomized Controlled Trial. *J Med Internet Res.* 2024. №26:e50132. doi: 10.2196/50132
2. Verain, M.C.D., Raaijmakers, I., Meijboom, S., van der Haar, S., Differences in drivers of healthy eating and nutrition app preferences across motivation-based consumer groups. *Food Quality and Preference*. 2024. doi: https://doi.org/10.1016/j.foodqual.2024.105145
3. Іщенко В. О. Популяризація культури харчування як один з пріоритетних напрямків у сфері громадського здоров'я. *Актуальні питання підготовки та наукової діяльності магістрів галузі знань "Охорона здоров'я":* матеріали І Міжвузівської науково-практичної конференції з міжнародною участю, 24 листопада 2020 р. Житомир-Ужгород, 2020. С. 61-64.
4. Ляшенко О., Пославський С., Кирийчук Д., Прачик В., & Бунккус С. Розроблення мобільного додатку для відстеження стану здоров'я та планування харчування маломобільних груп населення в умовах надзвичайних ситуацій. *Інформаційні технології та суспільство*. 2023. №2 (8). С. 42-50. https://doi.org/10.32689/maup.it.2023.2.5
5. Орлов В. І. Розробка додатку для інформаційного забезпечення та контролю здорового способу життя. *Стан, досягнення і перспективи інформаційних систем і технологій* : матеріали XX Всеукр. наук.-техн. конф. молодих вчених, аспірантів та студентів, 21-22 квіт. 2020 р. Одеса, 2020. Т. І. С. 153–154.

УДК 621.391:623.746-519 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.121

РОЗРОБКА ПОВІТРЯНОГО РЕТРАНСЛЯТОРУ ДЛЯ ЗВ'ЯЗКУ З БПЛА

Козінець В.О.
Науковий керівник – доц. Іваненко С.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: volodymyr.kozinets@nure.ua

This paper describes the problem of limited range of unmanned aerial vehicles (UAVs) and the need for high-quality video transmission to the operator. The use of an aerial retransmitter becomes a crucial element for optimizing this process. The development and implementation of such a retransmitter can significantly enhance the efficiency and range of UAV usage, ensuring a stable and reliable connection with the operator over long distances.

Проблема обмеження дальності польоту безпілотних літальних апаратів (БПЛА) та передачі відеоінформації до оператора є актуальною у сучасному світі. Завдяки розвитку технологій, БПЛА стали важливим інструментом у багатьох галузях, включаючи військову сферу, кіно, агропромисловість та інше. Проте, обмежена дальність польоту зменшує їх ефективність, особливо у великих відкритих просторах. Крім того, низька якість або втрата відеосигналу може ускладнювати контроль використання БПЛА[1].

Одним із рішень цих проблем є використання повітряного ретранслятора, який може підвищити ефективність та дальність використання БПЛА, забезпечуючи стабільний та надійний зв'язок з оператором на великій відстані. Розробка та впровадження такого ретранслятору є важливим завданням у галузі розвитку безпілотних технологій. Такий пристрій дає можливість успішного вирішення бойових завданьна відкритих місцевостях, у важкодоступних районах або у зоні дії електромагнітних перешкод [2]. Крім військового застосуваня, повітряні ретранслятори можуть бути корисні в галузі екстремального туризму або пошукових рятувальних операцій, де вони допоможуть забезпечити безперервний зв'язок з групою у складних умовах.

Метою роботи є розгляд проблеми обмеження дальності польоту безпілотних літальних апаратів (БПЛА) та необхідності забезпечення якісної передачі відеоінформації до оператора. Робота спрямована на висвітлення важливості використання повітряного ретранслятора для оптимізації цих процесів, а також на представлення можливостей підвищення ефективності та дальності використання БПЛА за допомогою такого ретранслятора.

На сьогодні на ринку є пропозиції, наприклад, відеопередавач Matek VTX з популярними для цієї моделі відеоприймачами Fat Shark Recon V3,

які працюють на частоті 1,2 ГГц. І можуть бути використані як складова частина повітряного ретранслятору. Matek VTX є компактним і потужним відеопередавачем, спеціально призначеним для використання в різних умовах польоту. Основні переваги Matek VTX включають широкий діапазон частот, високу потужність передачі сигналу, низький рівень спотворень та інтерференції. Ці характеристики роблять його якісним вибором для забезпечення стабільного зв'язку з БПЛА-ретранслятором на великій відстані, що в цілому забезпечить збільшення дальності відеозв’язку із основним керованим БПЛА..

Технічна реалізація такого ретранслятору включає встановлення Matek VTX на дрон або окремий БПЛА, та налагодження його параметрів, відеосигнал на нього подається, наприклад, від відеоприймача на 5.8 ГГц, який приймає відеосигнал від дрона зв’язко і з яким треба підтримувати на великій відстані. Відеоприймач отримує сигнал через антенну від БПЛА, після чого вони декодують його і виводять на вхід MATEK VTX. [3].

Зважаючи на проблему обмеження дальності польоту БПЛА та необхідність якісної передачі відеоінформації, використання повітряного повітряного ретранслятора для управління БПЛА, виявляється важливим кроком у вдосконаленні засобів зв'язку та підвищенні ефективності використання БПЛА. Розробка та впровадження таких технологій може сприяти забезпеченню стабільного зв'язку з оператором на великій відстані.

Список використаних джерел:

1. Туранський М.О. Історія розвитку та застосування розвідувальних і розвідувально-ударних безпілотних комплексів у збройних конфліктах сучасності [Електронний ресурс] / М.О. Туранський, О.В. Пулим, О.В. Корольова // Chtyvo – 2019. – Режим доступу до ресурсу: https://shron1.chtyvo.org.ua/Turanskyi_Mykola/Istoriia_rozvytku_ta_zastosuvannia_rozviduvalnykh_i_rozviduvalno-udarnykh_bezpilotnykh_kompleksiv.pdf?PHPSESSID=nnae15382dr24radqah54uaft5

2. Мельников С.В. Застосування безпілотних літальних систем як мобільних комплексів радіозв’язку [Електронний ресурс] / С.В. Мельников, О.Є. Волков, М.В. Коршунов, Ю.Ю. Грищенко // Usim – 2017. – Режим доступу до ресурсу: http://usim.org.ua/arch/2017/5/6.pdf

3. Стратонов В.М. Перспективи застосування військових бпла українського виробництва для робіт з розмінування територій [Електронний ресурс] / В.М. Стратонов // Perspectives – 2023. – Режим доступу до ресурсу: http://perspectives.pp.ua/index.php/nts/article/view/4584/4608

УДК 004.056.523:57.087.1 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.123

АНАЛІЗ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

Копиця А.А.
Науковий керівник – к.т.н., доц. Скорик Ю.В.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: alla.kopytsia@nure.ua.

This work is devoted to the analysis of biometric identification methods. Biometrics is a type of information technology that is rapidly developing during the XXI century and determines the development of means of verification and identification systems for individuals. This technology is used in management and control systems to ensure security. The main advantage of biometrics is the ability to quickly and easily identify a person without causing inconvenience to the person. Today, biometrics is a science that uses unique human measurement parameters for verification. It includes access systems based on fingerprints and palm prints, iris, facial geometry, vein patterns, DNA, signature and voice, etc.

Технологіями біометричної ідентифікації та аутентифікації користуються більшість людей в різних країнах світу. Застосування біометричних технологій є одним із найважливіших чинників, який визначає успішність і конкурентоспроможність суб'єкта суспільного життя – приватної особи, компанії чи держави [1].

Людина повсякчас зустрічається з біометрією у житті – від отримання закордонного паспорта або візи до придбання сучасного гаджета.

Основною перевагою біометрії є можливість швидкої та простої ідентифікації або аутентифікації без спричинення незручностей людині [1].

На практиці застосовується риси та характеристики людини, найпоширеніші серед них – розпізнавання за відбитками пальців, райдужною оболонкою очей і зображенням обличчя.

Ідентифікація в біометричній системі проходить чотири стадії [2]: запис (зразок людини запам'ятовується системою); виокремлення (відзняті зразки аналізуються системою); порівняння (отриманий зразок порівнюється з наявним зразком); збігання/незбігання (визначається збіг представлених біометричних зразків і ухвалюється відповідне рішення).

Наразі існує дві групи методів біометрії – статичні та динамічні [1].

Статичні методи – ґрунтуються на фізіологічній та унікальній характеристиці фізичної особи, яка надана від народження, є невід'ємною складовою людини та не змінюється з часом [2].

Відбиток пальця – унікальний малюнок папілярних узорів на пальцях.

Форма долоні – індивідуальна геометрія долоні, кисті руки або пальця.

Малюнок вен на долоні або пальці руки – за допомогою інфрачервоної камери зчитується малюнок вен на лицьовій стороні долоні (кисті руки) або пальця.

Райдужна оболонка ока – для її сканування використовується портативна камера та спеціалізоване програмне забезпечення, за допомогою якої сканується відповідна частина обличчя і виділяється зображення ока.

Сітківка ока – малюнок кровоносних судин очного дна.

Форма обличчя – формування двовимірного або тривимірного зображення обличчя людини.

ДНК – з причин відсутності можливостей роботи у реальному часі, системи, які застосовують цей метод, в основному використовуються тільки для спеціалізованих експертиз.

Динамічні методи – ґрунтуються на аналізі поведінкових характеристик, особливостей рухливих дій та підсвідомих рухів особи [2].

Рукописний почерк – використовується підпис людини. Цифровий ідентифікаційний код формується залежно від необхідного ступеня захисту і наявності необхідного устаткування. Ідентифікація за рукописним почерком буває двох типів [2]: за самим підписом та за динамічними характеристиками написання підпису.

Клавіатурний почерк – використовується набір кодового слова і не потребує зовні жодного спеціального устаткування, окрім переобладнаної стандартної клавіатури.

Голос – існує багато способів формування кодів ідентифікації за голосом, але, як правило, це різні поєднання частотних і статистичних характеристик голосу.

Загальне сортування найпоширеніших методів за якістю від кращого до гіршого [2]:

1. ДНК;
2. райдужна оболонка ока, сітківка ока;
3. відбиток пальця, термографія обличчя, форма долоні;
4. форма обличчя, розташування вен на кисті руки і долоні;
5. підпис;
6. клавіатурний почерк;
7. голос.

Статичні методи ідентифікації вважаються набагато якіснішими, ніж динамічні, але водночас значно дорожчими [1].

Список використаних джерел:

1. Joseph N. Pato, Lynette I. Millett (2010). Biometric Recognition: Challenges and Opportunities‖, Editors: Whither Biometrics Committee; National Research Council.

2. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. Львів: ЛьвДУВС, 2015. 492 с.

УДК 621.391:004.77 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.125

РОЗРОБКА ПЛАТФОРМИ ДЛЯ МОНІТОРИНГУ ОФІСНИХ ПРИСТРОЇВ В ЛОКАЛЬНІЙ МЕРЕЖІ З ВИКОРИСТАННЯМ ХМАРНИХ ТЕХНОЛОГІЙ

Кулініч А.О
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: anton.kulinich@nure.ua

This article is devoted to the advantages of remote management of office equipment. In this context, it is important to consider the potential and benefits of creating a platform for monitoring and managing office equipment. Such applications can become an integral part of the modern office environment, allowing businesses to maintain efficiency and productivity. The article also emphasizes the advantages of cloud technologies. Providing centralized management from the cloud allows you to effectively monitor and manage all devices in the local network from one place. This simplifies the management process and provides a single point of access to all necessary tools.

Сьогодні інтеграція цифрових інструментів у всі сфери життя є буденним явищем, особливо у сферах управління бізнесом, підприємствами та офісними процесами. Завдяки швидкому темпу розвитку цифрових технологій існують нові можливості та підходи для оптимізації, підвищення продуктивності, надійності та ефективності робочих процесів.

Офісне обладнання (принтери, сканери, камери, кліматична техніка тощо) є невід'ємною складовою сучасного офісного середовища. Проте, управління офісним обладнанням може стати викликом через складність, різноманіття або несумісність пристроїв. Необхідність постійного моніторингу та технічної підтримки офісного обладнання є важливою складовою забезпечення ефективної роботи офісу. Одним із важливих аспектів є ефективне управління офісним обладнанням і ресурсами, в тому числі віддалене [1] та централізоване [2]. Сучасні інформаційні технології дозволяють створювати нові інструменти та програмні рішення, що спрощують процеси моніторингу, управління та підтримки роботи офісного обладнання. Такі рішення допомагають підприємствам ефективно використовувати свої ресурси, забезпечуючи безперебійну роботу та підвищуючи якість обслуговування користувачів [1, 2]. Для оптимізації процесів керування також ефективно застосовувати хмарне програмне забезпечення [3].

Метою доповіді є аналіз та розробка платформи для моніторингу офісних пристроїв в локальній мережі з використанням хмарних технологій. Для покращення управління офісним обладнанням

пропонується створення платформи для моніторингу та керування, що дозволить ефективно контролювати та керувати різноманітними пристроями, забезпечуючи безперебійну роботу офісу без фізичної присутності адміністратора в офісі. Ця платформа також буде надавати аналітичні дані для оптимізації використання ресурсів.

Для досягнення поставленої мети пропонується використовувати хмарну платформу від Microsoft – Azure. Використання хмарних технологій зробить цю платформу доступною з будь-якої точки світу, де є інтернет-з'єднання, забезпечить єдину точку доступу та спростить процес управління навіть поза офісом. На рис. 1 зображено архітектуру взаємодії між платформою керування та підприємством.

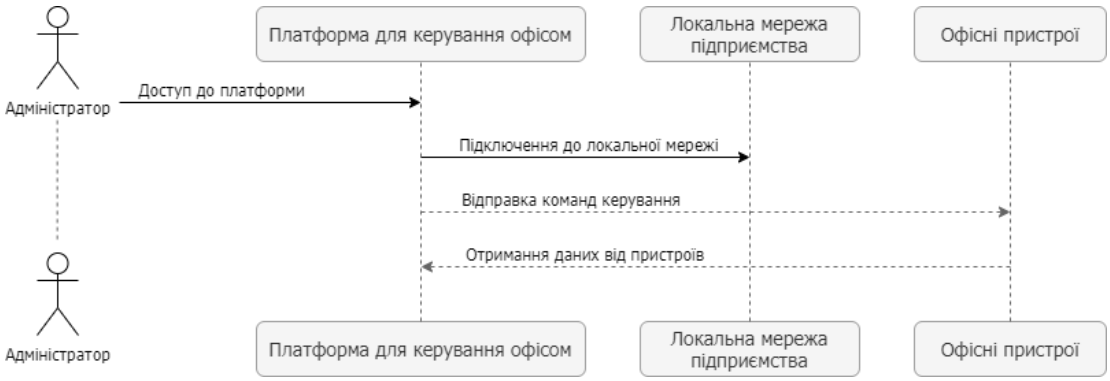


Рисунок 1 – Архітектура взаємодії між платформою керування та підприємством

Такий підхід також дозволить інтегруватися з іншими хмарними сервісами та додатками, що відкриє нові можливості для оптимізації робочих процесів та покращення співпраці між різними департаментами компанії. Крім того, він забезпечить гнучке та ефективне розгортання, що знизить витрати на підтримку та розвиток інфраструктури.

Список використаних джерел:

1. Benefits of Remote Access / Ron Samson // ClearNetwork. 2023.URL: https://www.msp360.com/resources/blog/remote-access-overview-benefits-and-best-practices/.

2. Top 4 Benefits of Centralized Remote Control over the Campus // Qnextech. 2023. URL: https://qnextech.com/blog/top-4-benefits-of-centralized-remote-control-over-the-campus/.

3. The Benefits of Cloud-Based Software // Geodecisions. 2021. URL: https://www.geodecisions.com/blog/benefits-of-cloud-software/.

УДК 004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.127

ТЕОРІЯ РИЗИКІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В WORDPRESS

Кутя Б.С.
Науковий керівник – доц. Скорик Ю.В.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
email: bohdan.kutia@nure.ua

Information security risk theory is a key aspect in managing the security of WordPress websites. This abstract explores the theoretical framework of risk management in the context of WordPress, one of the most widely used content management systems worldwide. The abstract highlights key risk factors such as vulnerabilities in WordPress core software, themes, and plugins. In addition, it discusses strategies to prevent and mitigate risks, including regular software updates, strong password policies, and implementing security plugins like Wordfence. By understanding and effectively applying information security risk theory, WordPress site owners and administrators can increase the resilience and integrity of their online platforms in the face of emerging cybersecurity challenges.

Ключові слова: WordPress, веб-сайт, плагін, теми.

WordPress — це відкрите програмне забезпечення для створення та керування веб-сайтами та блогами. Як основа для програмного забезпечення PHP і розробників баз даних MySQL. Та для відтворення контенту використовується HTML, CSS, Javascript. WordPress починався як платформа для створення простих веб-сайтів, без особливо складного функціоналу, але з роками перетворився на потужний інструмент для створення веб-сайтів будь-якого типу, включаючи корпоративні сайти, онлайн-магазини, фотогалереї тощо. З можливістю відтворення будь-якого функціоналу.

Однією з основних переваг WordPress є його простота в установці та використанні. Людина без особливих знань може створити свій веб-сайт та розмістити його в інтернеті, для будь-якої задачі. Він має інтуїтивно зрозумілий і легкий у використанні інтерфейс, який дозволяє користувачам без технічних навичок створювати, редагувати та опубліковувати контент на своєму веб-сайті. Крім того, для WordPress існує велика кількість безкоштовних та платних тем і плагінів, що дозволяє розширювати функціональність сайту за допомогою додаткових модулів. Також є можливість використовування білдерів. Для створення одразу візуального вигляду веб-сайту, та функціоналу, але для специфічного функціоналу потрібно мати навички з програмування.

WordPress також відомий своєю гнучкістю та налаштовуваністю. Він дозволяє користувачам створювати унікальний дизайн для свого сайту, використовуючи теми та кастомізуючи їх з використанням власного CSS і HTML. Крім того, завдяки широким можливостям налаштування та плагінам, WordPress може бути адаптований під різні потреби користувачів.

Але з таким різноманітними платними, безплатними темами, плагінами відкривається проблеми з безпекою в Wordpress:

1. Будь-яке програмне забезпечення, WordPress має потенціал до уразливості, які можуть бути використані зловмисниками для злому сайту або отримання несанкціонованого доступу до інформації.
2. Важливо регулярно оновлювати ядро WordPress, теми та плагіни, оскільки це допомагає уникнути використання вразливостей зловмисниками.
3. Слабкі або легко вгадувані паролі можуть бути скомпрометовані зловмисниками, що може призвести до порушення безпеки.
4. Недостатньо не захищені або оброблені запити до бази даних можуть призвести до SQL-ін'єкцій, що може дати зловмисникам виконувати шкідливі запити до бази даних.
5. Не правильно налаштовані права доступу можуть призвести до несанкціонованого доступу до важливої інформації або можливості редагування вмісту.
6. Некоректне налаштування веб-сервера може призвести до потенційних загроз безпеці.
7. Неправильне організування регулярних резервних копій може ускладнити відновлення сайту

Для захисту веб-сайту потрібно не робити ці всі правила, та використовувати провіренні плагині та теми. Та дотримуватися всіх правил, які були перераховані.

Наприклад для захисту веб-сайту можна використовувати плагін Wordfence. Він закриває більшість проблем з безпекою в Wordpress. Можливості Wordfence:

1. Блокує шкідливий трафік: Wordfence аналізує весь трафік на веб-сайті в реальному часі і блокує будь-які спроби несанкціонованого доступу, DDoS-атаки, спамерів і ботів.
2. Виявляє вразливості: автоматично перевіряє веб-сайт на наявність вразливостей в темах, плагінах та ядрі WordPress.
3. Блокує атак на паролі: має функцію блокування авторизації за неправильними паролями, що допомагає уникнути атак перебору паролів.
4. Відшукує віруси та шкідливі програми: сканує веб-сайт на наявність вірусів, шкідливих програм та інших загроз і надає детальний звіт про виявлені проблеми.
5. Оновлює безпеку: автоматично оновлює важливі безпекові скрипти та файли, щоб забезпечити веб-сайт останніми захистами.
6. Фаервол: має вбудований веб-фаервол з додатковими правилами, які допомагають захистити веб-сайт від різних атак.

Список використаних джерел:

1. https://wordpress.org/documentation/
2. https://www.wordfence.com/
3. Hope P., Walther B. Web Security Testing Cookbook: Systematic Techniques to Find Problems Fast. O'Reilly Media, 2008.

УДК 621.391:004.415.538 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.129

ОРГАНІЗАЦІЯ АВТОМАТИЧНОГО ТЕСТУВАННЯ ІНФОКОМУНІКАЦІЙНОГО ОБЛАДНАННЯ ТА ДОДАТКІВ

Красніков В. О.
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: vsevolod.krasnikov@nure.ua

This report is devoted to the study, development and organization of an automatic testing system for information communication equipment and applications. The paper describes the prototype of organized testing processes in a company providing information and communication services. The general approach to organizing these processes was divided into several stages that can be universal for any approach in development and testing. This approach is determined by the need for continuous improvement and ensuring a high level of customer satisfaction in the rapidly changing world of information and communication technologies.

Для ефективного та надійного функціонування продуктів в сфері інфокомунікаційних технологій необхідно використовувати тестування. Через високі вимоги якості та доволі стислі терміни актуальним є впровадження автоматизованих засобів тестування в процес розробки продукту, що дозволяє оптимізувати час та ефективність розробки та випуску продукта.

Автоматизація тестування має великий перелік переваг. Вона дозволяє виконувати тести значно швидше та з більш високою точністю порівняно із ручним тестуванням, допомагає виявляти і виправляти помилки в програмному забезпеченні на ранніх етапах розробки, забезпечує стабільність і надійність програм, дозволяє ефективніше використовувати ресурси команди розробників. Точність та обхідність помилок забезпечуються завдяки виключенню людського фактора. Автоматизація є ефективним засобом для тестування великих обсягів даних та функціональності. Автоматизація полегшує впровадження нових функцій, забезпечує тестування збіжності та зворотної сумісності [1].

Метою доповіді є опис організації автоматичного тестування для інфокомунікаційного обладнання та додатків. В роботі наведено опис прототипу організованих процесів тестування в компанії по наданню інфокомунікаційних послуг. Загальний підхід до організації цих процесів був поділений на декілька етапів, які можуть бути універсальними для будь-якого підходу в розробці та тестуванні.

Початковим етапом є визначення сценаріїв тестування, де враховуються ключові функціональності та можливості інформаційних та комунікаційних послуг.

На етапі тестування функціональності проводяться різнобічні тести, спрямовані на перевірку всіх процесів в мережі, правильності виконання основних операцій (телефонія, інтернет тощо), налаштування мережі, тестування додатків для взаємодії з користувачем.

Окрему увагу приділяють тестам витривалості та навантаження для оцінки стабільності системи під тривалим використанням та в екстремальних умовах. Тестування безпеки включає аналіз потенційних точок злому та виявлення вразливостей для забезпечення конфіденційності даних користувачів [1].

Додатково проводиться тестування якості зв'язку, що включає в себе вимірювання параметрів якості послуг (QoS) та оцінку якості сигналу в різних умовах та областях.

Впровадження та організація автоматичного тестування в компанії, що надає інфокомунікаційні послуги, виявляється стратегічно важливою ініціативою, яка сприяє підвищенню ефективності, стабільності та якості надання послуг [2, 3]. Автоматизація тестування дозволяє не лише прискорити процес перевірки функціоналу, але й забезпечити високий ступінь надійності і витривалості інфокомунікаційних систем.

Автоматичне тестування дозволяє швидко виявити та усунути помилки, підтримувати високу якість сервісу та реагувати на зміни в найбільш ефективний спосіб. Автоматизовані тести забезпечують повторюваність та точність в проведенні тестових сценаріїв, що особливо важливо в галузі інфокомунікацій, де стабільність та безперебійність сервісу є ключовими чинниками.

Автоматичне тестування допоможе оптимізувати витрати ресурсів та часу, звільнить розробників від рутинних робіт та дозволить їм зосередитися на більш складних та творчих аспектах розробки.

Впровадження автоматичного тестування стає стратегічним рішенням для компаній у сфері інфокомунікацій, забезпечуючи покращення надійності, швидкості внесення змін та конкурентоспроможності. Такий підхід визначається потребою в неперервному вдосконаленні та забезпеченні високого рівня задоволеності клієнтів у швидкозмінному світі інфокомунікаційних технологій.

Список використаних джерел:

1. Parsa S. Software Testing Automation: Testability Evaluation, Refactoring, Test Data Generation and Fault Localization / Saeed Parsa . Springer, 2023. 604p

2. Jackvony K. The Complete Software Tester: Concepts, Skills, and Strategies for High-Quality Testing / Kristin Jackvony. Kindle Edition, 2021. 514 p.

3. Forgacs I. Modern Software Testing Techniques: A Practical Guide for Developers and Testers / I. Forgacs, A. Kovacs. APress, 2024. 266 p.

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.131

СПІЛЬНЕ ВИКОРИСТАННЯ МІЛІМЕТРОВИХ ТА СУБМІЛІМЕТРОВИХ ХВИЛЬ

Лютий А.О.
Науковий керівник – д.т.н., проф. Коляденко Ю.Ю.
Харківський національний університет радіоелектроніки
каф. ІКІ ім В.В. Поповського,
м. Харків, Україна
e-mail: artem.liutyi@nure.ua

Current new 5G millimeter-wave (mm-wave) radio (NR) systems, as well as future 6G radio access technologies (RATs) in the terahertz (THz) band, will rely heavily on beamforming to combat excessive path loss. In addition, both RATs are designed for the same inelastic traffic that requires high data rates and is susceptible to blocking phenomena. To improve service reliability in these systems, multiple connections can be used to dynamically switch ongoing sessions between the two technologies. The purpose of this work is to investigate the use of millimeter and submillimeter waves for joint use.

Розглянемо стадію розгортання систем міліметрових хвиль (ММХ) NR і зосередимося на одній комірці ММХ базової станції (БС) круглої форми з радіусом R_M, (рис. 1), де R_M є таким, що блокування на краю комірки не призводить до відключення. Поряд з ММХ БС знаходиться ТГц БС, що характеризується радіусами покриття $R_{T,1}$ і $R_{T,2}$, де перший радіус такий, що жодні сеанси, які знаходяться всередині (0, $R_{T,1}$), не зазнають відключення у випадку блокування, в той час як сеанси з кільця ($R_{T,1}$, $R_{T,2}$) можуть зазнати відключення у випадку блокування.

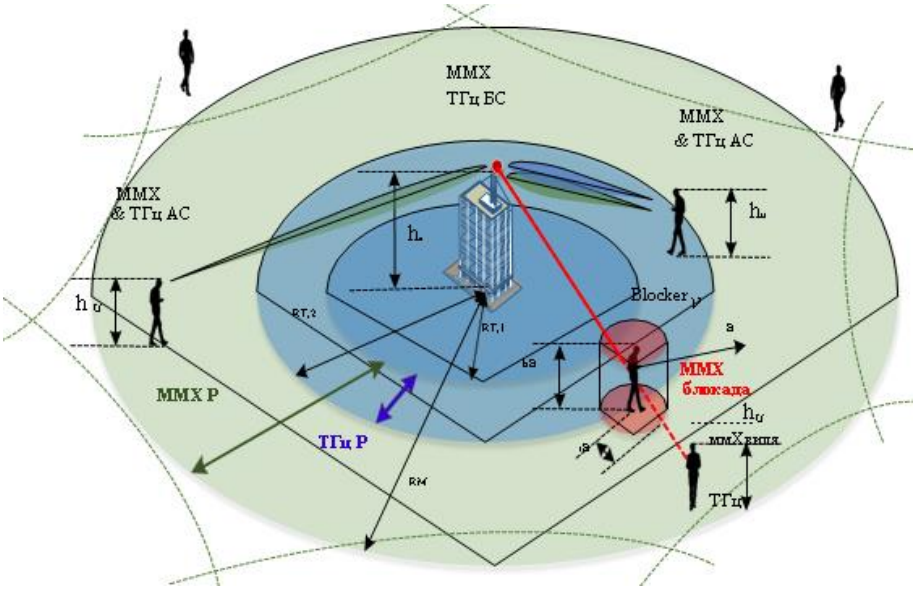
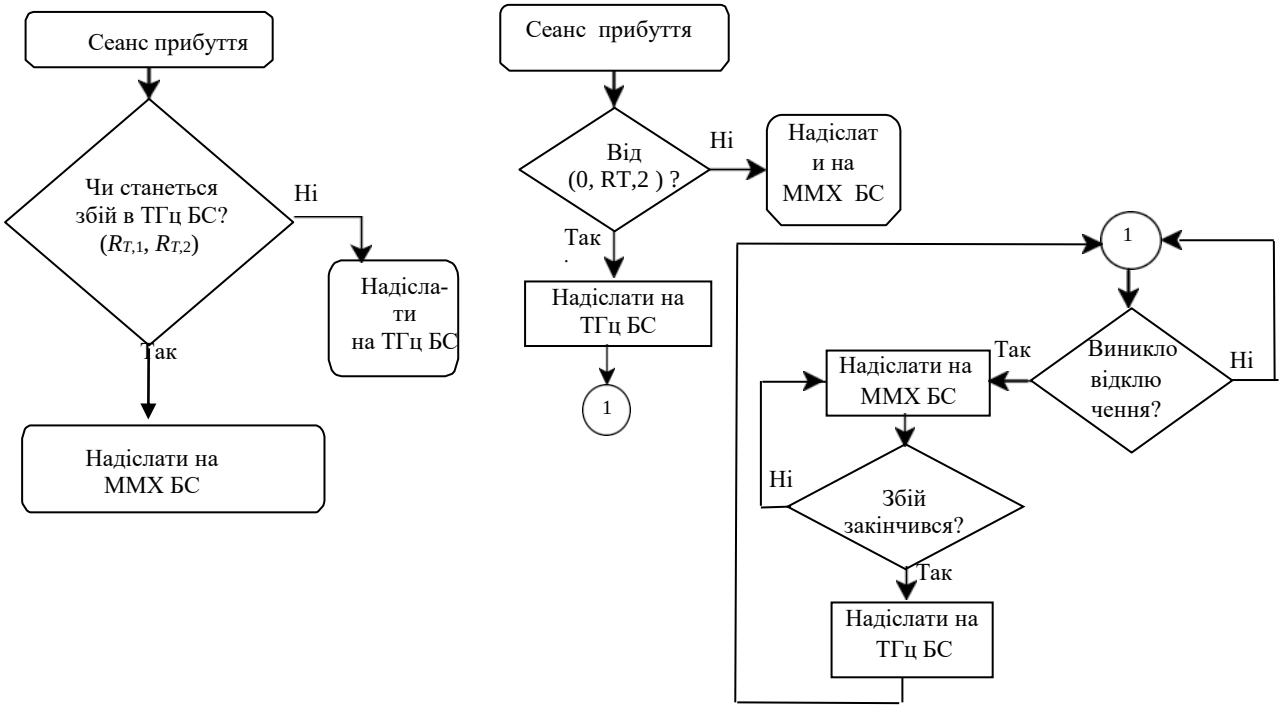


Рис. 1. Розгорнута система 6G зі спільним розміщенням БС ММХ/ТГц.

Висота БС однакова, h_A. Висота АС - h_U. Смуга пропускання БС ММХ і ТГц - B_M і B_T.

Процес надходження сеансів є пуассонівським з інтенсивністю λ_A сес./с·м2. Вважається, що геометричні місця розташування сеансів рівномірно розподілені в зоні покриття ММХ. Час обслуговування сеансів розподілено за експоненціальним законом з параметрами μ. Кожен сеанс вимагає швидкість передачі даних R_b Мбіт/с.

Передбачається, що всі АС підтримують функцію мультизв'язності [4]. Оскільки основне погіршення продуктивності в розглянутих майбутніх щільних розгортаннях 6G ММХ/ТГц спричиняється динамічним блокуванням людського тіла, розглядаємо дві схеми об'єднання: ММХ (ММХ Р) і ТГц (ТГц Р) (рис. 2).



а) б)

Рис. 2. Схема об’єднання: (a) перевага надається ММХ, (b) перевага надається ТГц

У першій схемі на ТГц БС приймаються лише ті сеанси, які не зазнають відключення через блокування. Це відповідає колу радіусом $R_{T,1}$ на рис. 1. Решта сеансів надходять до ММХ БС і залишаються там, доки їх обслуговування не буде завершено або сеанс не буде припинено.

У схемі, якій надається перевага в ТГц, сеанси, що надходять з кола радіусом $R_{T,2}$, спочатку приймаються в ТГц БС.

Ті сеанси, які зазнають відключення з ТГц БС в кільці ($R_{T,1}$, $R_{T,2}$) тимчасово перенаправляються на ММХ БС і повертаються назад, як тільки блокування з ТГц БС закінчується.

У цій схемі більше трафіку спочатку спрямовується на ТГц БС, але частина сеансів може зазнати відключення в результаті блокування.

Сесія, яка прийнята на обслуговування в ММХ БС, може бути втрачена в результаті переходу в стан блокування.

Хоча в цьому випадку не відбувається відключення, кількість ресурсів, необхідних для обслуговування, збільшується через схему модуляції та кодування нижчого порядку.

Якщо у ММХ БС немає достатньої кількості ресурсів, сеанс зв'язку обривається.

Сеанси, які прийняті в ТГц БС в колі радіусом $R_{T,1}$, ніколи не втрачаються. Однак, у схемі, якій надається перевага в ТГц, сесія, що зазнає блокування на ТГц БС в кільці ($R_{T,1}$, $R_{T,2}$), може бути втрачена на ММХ БС, якщо немає достатньої кількості ресурсів, щоб тимчасово вивантажити її на ММХ БС.

Список використаних джерел:

1. Muliar B., Koliadenko Y., Moskalets M., Loshakov V., Ageyev D. Interaction Model and Phase States at Frequency Resource Allocation in a Grouping of Radio-Electronic Equipment of 5G Mobile Communication Network. IEEE 9th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). Kharkiv. Ukraine. 2022. P. 495–501. doi: 10.1109/PICST57299.2022.10238581.

2. Polese M., Jornet J.M., Melodia T., Zorzi M. Toward end-to-end, full-stack 6G terahertz networks. IEEE Commun. Mag. 2020. 58. P. 48–54.

3. Moltchanov D., Samuylov A., Lisovskaya E., Kovalchukov R., Begishev V., Sopin E., Gaidamaka Y., Koucheryavy Y. Performance Characterization and Traffic Protection in Street Multi-Band Millimeter-Wave and Microwave Deployments. IEEE Trans. Wir. Comm. 2022. Vol. 21. P. 163–178.

4. Аналіз продуктивності багатодіапазонних мікрохвильових і міліметрових систем 5G NR / В. Бегішев, Є. Сопін, Д. Молчанов, Р. Пірмагомедов, А. Самуйлов, С. Андрєєв, Ю. Кучерявий, К. Самуйлов // IEEE Trans. Wirel. Commun. 2021. Vol. 20. P. 3475–3490.

УДК 621.391:004.3 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.134

РОЗШИРЕННЯ ФУНКЦІОНАЛУ УКХ РАДІОСТАНЦІЇ QUANSHENG UV5(K8)

Мельнікова Д. С.
Науковий керівник – к.т.н. Іваненко С.А.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
e-mail: daria.melnikova@nure.ua

In today's world, where mobile communication is not always available, radio stations remain an indispensable tool for communication in various fields. this work is devoted to the study of the characteristics and functionality of the radio station Quansheng UV-K5. The Quansheng UV-K5 walkie-talkie is a reliable and high-quality radio equipment, and can be an ideal choice for a variety of consumers. This radio station contains many interesting and important functions that allow you to use it for both amateur and professional communication.

В роботі розглядається радіостанція QUANSHENG UV5 (K8).

Ця багатодіапазонна радіостанція з робочим діапазоном частот 50-600МГц (включаючи авіа та річний діапазони) і вихідною потужністю 5 Вт дозволяє покривати задачі радіозв’язку як для комерційних так і для приватних користувачів.

Характеристики обраної радіостанції у деяких аспектах схожі з характеристиками її аналогів, що існують на ринку. Проте Quansheng UV-K5 (K8) має широкий додатковий функціонал та варіанти його покращення за допомогою додавання нової прошивки системи.

Для більш детального ознайомлення з основними характеристиками інших радіостанцій, нижче представлено порівняння радіостанції Quansheng UV-K5 (K8) з її аналогами на ринку (таблиця 1).

Таблиця 1 – Порівняння характеристик обраної радіостанції з її аналогами [1,2,3]

Назва	Ціна	Діапазон частот	Потужність	Ємність акумулятора	Функції
Quansheng UV-K5	700 – 1000грн	VHF:136-174MHz UHF:400-470MHz	5W	1600mAh	FM-радіо, сканування частот, VOX, CTCSS/DCS, TOT, DTMF, APRS
Baofeng UV-5R	500 – 700грн	VHF:136-174 MHz UHF: 400-520MHz	8W	1800mAh	FM-радіо, сканування частот, VOX, CTCSS/DCS, TOT
Retevis RT22	700 – 900грн	UHF:462MHz	3W	1000mAh	FM-радіо, сканування частот, VOX, CTCSS/DCS, TOT, GPS

Доволі високі показники щодо приймального тракту радіостанції можливі завдяки використанню більш високоякісного приймально-

передавального чіпу Beken BK4819. Що суттєво підвищило динамічні характеристики радіоприймача.

Ще однією особливістю та великою перевагою цієї моделі є можливість покращити ті функції, які вже має рація, а також додати нові, завдяки встановленню прошивок. Наразі існує багато їх варіантів, як офіціальних, так і користувальницьких. Також є можливість створити власну версію прошивки з тими додатковими функціями, які потрібні користувачу.

Зокрема до нових функцій цієї радіостанції можуть бути отримані наступні:

- панорамний спектроаналізатор;
- месенджер повідомлень AFSK ;
- RSSI bar.

Панорамний спектроаналізатор візуалізує спектр радіочастот в певному діапазоні. На рисунку 1(а) можна побачити, як даний аналізатор виглядає в моменті використання. Спочатку панорамний спектроаналізатор сканує певний радіочастотний діапазон, далі для кожного з сигналів, що отримали, вимірюється рівень та результат відображається у вигляді графіку. Така функція може бути корисна: для пошуку вільних каналів, аналізу завантаженості ефіру, виявлення джерел шуму та моніторингу активності (тобто можна зафіксувати коли та на яких частотах ведуться радіопереговори).

AFSK (англ. Audio Frequency Shift Keying) - це метод модуляції, який використовується для передачі цифрових даних по радіоканалу. В даному випадку він використовується для передачі текстових повідомлень. Відправник вводить текст повідомлення на дисплеї рації, рація модулює текст за допомогою AFSK та передає модульований сигнал в ефір. Інша рація, яка має функцію AFSK, приймає сигнал, демодулює його та відображає на дисплеї текст надісланого повідомлення. На рисунку 1(б) зображено вигляд надісланих/отриманих повідомлень з двох рацій.

RSSI (англ. Received Signal Strength Indicator) - це індикатор рівня прийнятого сигналу. Він показує, наскільки сильний сигнал від приймаючої рації. Принцип роботи даної функції дуже простий: рація приймає сигнал від іншої рації, вимірює рівень отриманого сигналу та відображає результат на дисплеї. Приклад реалізації даної функції зображено на рисунку 1(в). Цю функцію можна використовувати для того, щоб визначити найкраще місце прийому; щоб дізнатися місцезнаходження іншої рації; також за допомогою RSSI bar можна виявити несправність антени. Якщо рівень сигналу біля антени буде низький, це може вказувати та її пошкодження.

Рисунок 1 – Приклади реалізації налаштованих функцій на радіостанції QUANSHENG UV5 (K8): а) панорамний спектроаналізатор; б) месенджер повідомлень AFSK; в) RSSI bar

Для того, щоб прошити нову прошивку – необхідний кабель для програмування, який можна придбати у виробника та встановити відповідне програмне забезпечення. Існує декілька офіційних ПЗ, які можна знайти на сайті виробника, а також безліч користувацьких, які розробляли безпосередньо користувачі. Кожна прошивка може містити в собі одну додаткову функцію, або одразу декілька. Офіційних програмних забезпечень існує 6 версій саме для радіостанції QUANSHENG UV5 (K8), а саме: v2.01.17; v2.01.19; v2.01.23; v2.01.25; v2.01.26; v2.01.31. Користувацькі прошивки можна знайти на різних інтернет-ресурсах.

Список використаних джерел:

1. 39.76€ 37% OFF|Retevis rt22s Freis prec heinrich tung Walkie Talkie 2 stücke rt22 Upgrade Vox Hidden Display Zwei Wege Funk Transceiver Walkie Talkies Reisen/Camp| | - AliExpres : вебсайт. URL: http://surl.li/rggkx (дата звернення: 01.03.2024)

2. 18.44€ 75% OFF|1/2pcs baofeng UV 5R 8w Tri Power Walkie Talkie Hochleistungs Dualband Langstrecken 128 ch tragbare Handheld UV 5r Schinken Zwei Wege Radio| | - AliExpress : вебсайт. URL: http://surl.li/rggmy (дата звернення: 01.03.2024)

3. 39.76€ 37% OFF|Retevis rt22s Freis prec heinrich tung Walkie Talkie 2 stücke rt22 Upgrade Vox Hidden Display Zwei Wege Funk Transceiver Walkie Talkies Reisen/Camp| | - AliExpress : вебсайт. URL: http://surl.li/rggle (дата звернення: 01.03.2024)

4. GitHub - amnemonic/Quansheng_UV-K5_Firmware: Quansheng UV-K5 Firmware : вебсайт. URL: https://github.com/amnemonic/Quansheng_UV-K5_Firmware (дата звернення 04.03.2024)

УДК 621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.137

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ ЗАСТОСУВАННЯ М-ПОСЛІДОВНОСТЕЙ ДЛЯ РЕАЛІЗАЦІЇ МЕТОДА КОДОВОГО РОЗПОДІЛУ КАНАЛІВ

Міцай Д.В.
Науковий керівник – к.т.н., доц. Бондар Д.В.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: dmytro.mitsai@nure.ua

This work is devoted to assessing the possibility of using signals of pseudo-random binary sequences as spreading sequences in a code division transmission system. Attention is drawn to the presence of families of pseudo-random binary sequences formed in accordance with the parameter of their period. Correlation processing is used as a method for identifying a subscriber channel. The study is based on the results of computer modeling. A conclusion is formulated about the prospects of this method of implementing the multichannel communication method.

В сучасних телекомунікаційних системах, які ґрунтуються на застосуванні цифрових технологій зв'язку, для формування інформаційних потоків застосовують широкосмугові двійкові сигнали. Цей факт обумовлений можливістю використання методів узгодженої фільтрації сигналів з метою розпізнавання двійкових інформаційних символів в сигналі, що передається та приймається. Потужним засобом в цьому аспекті є методи кореляційної обробки. Кореляційна обробка ґрунтується на розрахунку кореляційних функцій сигналів.

Метод широкосмугового зв'язку передбачає розширення частотної смуги спектру інформаційного сигналу, якій первинно можна вважати вузькосмуговим. Один з методів розширення спектру інформаційного сигналу є метод прямого розширення спектру (DSSS − direct sequence spread spectrum). Цей метод передбачає перетворення кожного інформаційного двійкового символу на певного вигляду широкосмугову двійкову послідовність. В якості послідовності, що розширює, можна використати псевдовипадкову послідовність максимальної довжини, яку ще часто називають m-послідовністю.

Відомо, що m-послідовність має автокореляційну функцію (АКФ) дуже подібну на АКФ білого шуму з високим та вузьким центральним максимумом та мінімальним рівнем бічних пелюстків. Саме ця особливість АКФ допомагає зробити процес розпізнавання m-послідовності більш впевненим. Крім того корисною особливістю m-послідовності є простий метод (алгоритм) її генерування на основі регістру зсуву, охопленого лінійним зворотним зв'язком. Таким чином m-послідовності можна розрізняти за кількістю розрядів регістра n.

Довжина m-послідовності визначається як $N = 2^n - 1$. Ця величина також є періодом послідовності. Кількість m-послідовностей з періодом N визначається формулою:

$$M = \frac{\Phi(N)}{n}$$

де $\Phi(N)$ – функція Ейлера, що показує кількість натуральних взаємно простих з N чисел в діапазоні від 1 до N. З ростом N функція Ейлера стрімко зростає. Тому і кількість m-послідовностей з періодом N також швидко росте. Наприклад для довжини $N = 3$ маємо 2 послідовності, а для $N = 1023$ маємо вже 60 послідовностей. Таким чином можна вважати, що для певних N виникає сім'я m-послідовностей в кількості M.

Метод кодолового розподілу каналів в системі багатоканального зв'язку вимагає застосування сім'ї широкосмугових послідовностей, які призначені грати роль кодів абонентів. З огляду на це виникає питання чи можна використати m-послідовності перної сім'ї, яка визначається параметром N в якості кодів абонентсіких в груповому потоці системи зв'язку.

Проведемо моделювання кодового ущільнення каналів на комп'ютері за допомогою пакету MathCad. З цією метою розроблено ряд макросів, які дозволяють генерувати масиви сім'ї m-послідовностей, розраховувати їхні кореляційні функції, створювати масив групового сигналу та проводити розпізнавання інформаційних символів.

Моделювання проведено з використанням сім'ї m-послідовностей з $N = 7$. В цій сім'ї всього дві послідовності, ким відповідають генеруючі поліноми: $1 + x^2 + x^3$ та $1 + x + x^3$. Схеми генераторів цих послідовностей наведені на рис. 1.

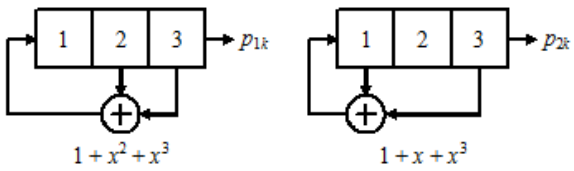


Рисунок 1 – Генератори двох m-послідовностей з сім'ї $N = 7$

Моделюванню підлягає система передачі з двома каналами, в яких задано два двійкових тестових сигнали: 0011 та 0101. Після розширення інформаційних символік кожного з каналів своєю m-послідовністю груповий сигнал багатоканального зв'язку набере вигляду, який наведено на рис. 2.

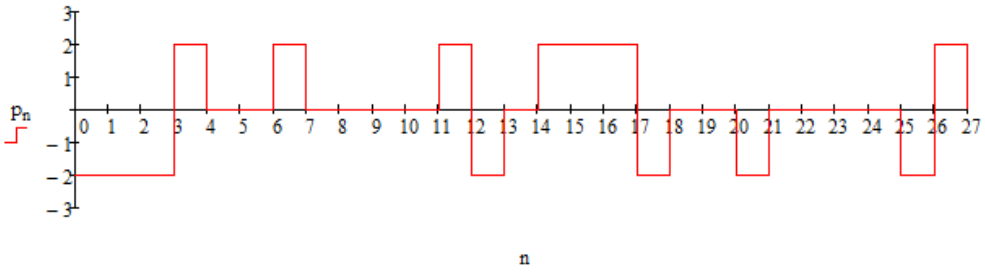


Рисунок 2 – Часова діаграма групового сигналу

Наступним кроком в моделюванні буде розрахунок ВКФ групового сигналу з двома m-послідовностей. Результати зображені на рис. 3.

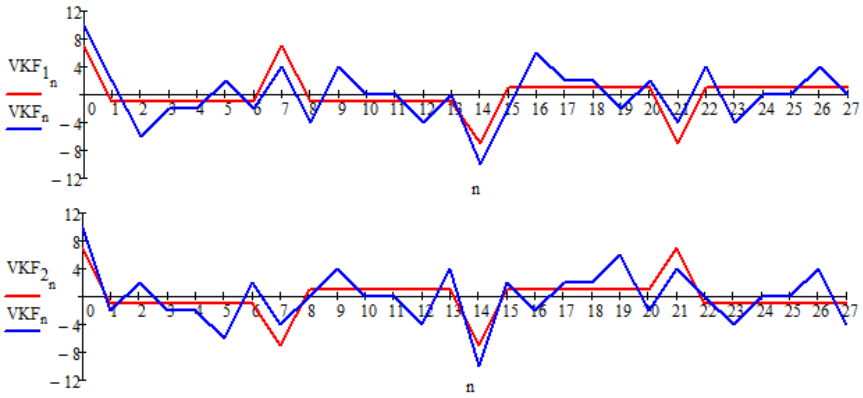


Рисунок 3 – Результати розрахунку ВКФ групового сигналу двома m-послідовностями

Червоною кривою для порівняння зображено АКФ відповідної двома m-послідовності. Результати свідчать про те що перспектива використання двома m-послідовностей в якості кодових сигналів при методі кодового розподілу каналів виглядає непереконливою.

Список використаних джерел:

1. Варакин Л. Е. Системы связи с шумоподобными сигналами. Москва, 1985. 384 с.
2. https://www.gaussianwaves.com/2018/09/maximum-length-sequences-m-sequences/

УДК 004.056:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.140

АНАЛІЗ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕНЬ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЙНИХ МЕРЕЖ

Михайлова А.С., Чеботарьова Д.В.
Науковий керівник – доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: anna.hmyria1@nure.ua
e-mail: dariia.chebotarova@nure.ua

This work is devoted to the issues of information security in information networks, namely the analysis of intrusion detection and prevention systems (IDS/IPS). The purpose of the report is a multi-criteria analysis of intrusion detection and prevention systems, taking into account a set of quality indicators. All considered IDS/IPS systems have their own characteristics, so the choice of the optimal system will vary depending on the circumstances, conditions and needs of a particular network.

Сьогодні електронні комунікації, зокрема інформаційні мережі, є ключовою частиною нашого життя. Інформаційні мережі широко використовуються в побуті та різних галузях, таких як навчання, бізнес, інфокомунікації, виробництво, комерція, розваги, охорона здоров'я тощо. Найбільш значною проблемою інформаційних мереж є безпека інформації, яка передається мережею, а також зберігається та опрацьовується в кінцевих пристроях мережі. Останнім часом кількість загроз та атак суттєво збільшується, тому питання захисту інформації в інформаційних мережах стає все більш актуальним.

Питання безпеки інформаційної мережі є одним із найбільш важливіших. Саме тому для попередження атак, мінімізації загроз та захисту мереж необхідно використовувати найбільш потужні засоби безпеки. До таких засобів відносяться спеціальні пристрої та програми, а також методи моніторингу, сповіщення та перевірки мережних з'єднань. Серед таких засобів великої популярності також набули сьогодні системи виявлення та запобігання вторгненням (IDS/IPS - (Intrusion Detection System /Intrusion Prevention System), які дають можливість виявити мережні атаки та запобігти вторгненню, ще до того як вони завдадуть шкоди та призведуть до негативних наслідків.

Метою доповіді є багатокритеріальний аналіз систем виявлення та запобігання вторгненням для захисту інформаційної мережі. В процесі багатокритеріального порівняння необхідно враховувати велику кількість параметрів систем IDS/IPS.

В наш час на ринку існує багато пропозицій IDS/IPS [1]. Сучасні системи виявлення та запобігання вторгнень є досить різноманітними, базуються на використанні різних методів, але окрім переваг, мають також

свої певні недоліки. Ці недоліки можуть бути пов'язані зі структурою систем або з реалізованим методом виявлення вторгнень [2].

Саме тому вибір оптимальної системи IDS/IPS для захисту конкретної інформаційної мережі з урахуванням сукупності показників якості та особливостей мережі є досить складною задачею. Компанії можуть вибирати з низки недорогих і потужних рішень IDS/IPS, які відповідають різноманітним потребам - від стартапів з обмеженим бюджетом до глобальних підприємств. Деякі з них є окремими рішеннями, а інші – функціями, доданими до інших продуктів безпеки [1]. У переважній більшості системи IDS/IPS використовують поєднання різних рішень на базі синтезу відповідних методів [2].

Зазвичай при виборі оптимальної системи IDS/IPS трьома найважливішими факторами при прийнятті рішення є функціональність, надійність і ціна [3].

В роботі проведено огляд та аналіз найбільш сучасних систем IDS/IPS за версією [1]: AIDE, BluVector Cortex, Check Point Quantum IPS, Cisco NGIPS, Fail2Ban, Fidelis Network, Hillstone Networks, Kismet, NSFOCUS, OpenWIPS-NG, OSSEC, Palo Alto Networks, Sagan, Samhain, Security Onion, Semperis, Snort, SolarWinds Security Event Manager IDS/IPS, Suricata, Trellix (McAfee + FireEye), Trend Micro, Vectra Cognito, Zeek, ZScalar Cloud IPS. В роботі пропонується порівнювати ці системи з урахуванням таких показників якості: підтримувані платформи та пристрої, типи виявлення загроз, вартість, відкритість коду, масштабованість, ємність, необхідність додаткового апаратного чи програмного забезпечення, затримка, тип ідентифікатору (HIDS, NIDS), інтеграція з іншими засобами безпеки, зручність інтерфейсу.

Усі розглянуті системи IDS/IPS мають свої особливості, переваги та недоліки. Тому вибір найкращої системи буде змінюватись в залежності від обставин, умов та потреб конкретної мережі.

Список використаних джерел:

1. Samson R. Top 10 Intrusion Detection And Prevention Systems [Електронний ресурс] / Ron Samson // ClearNetwork. – 2023. – Режим доступу до ресурсу: https://www.clearnetwork.com/top-intrusion-detection-and-prevention-systems/.

2. Лукова-Чуйко Н. В. Методи виявлення вторгнень у сучасних системах IDS / Н. В. Лукова-Чуйко, С. В. Толюпа, І. І. Пархоменко // Безпека інформаційних систем і технологій. Інформаційна та кібернетична безпека. – 2021. – № 1(5). – С. 19 – 26.

3. Hock F. Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks / Filip Hock, Peter Kortiš // Research Gate. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/publication/307853397.

УДК 004.946 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.142

РОЗРОБКА ГРИ НА ІГРОВОМУ РУШІЇ UNREAL ENGINE 5 ЗА ДОПОМОГОЮ ПЛАГІНУ GAMEPLAY ABILITY SYSTEM

Обершев В.О.
Науковий керівник – к.т.н., ст. викл. Яцик М.В.
Харківський національний університет радіоелектроніки
(61166, м. Харків, пр. Науки, 14, каф. Системотехніки,
e-mail: vladyslav.obershev@nure.ua

In the modern game engine market, Unreal Engine 5, created by Epic Games, is known as one of the best. It allows developers to create graphically stunning games while maintaining high performance. The new version of Unreal Engine 5 features Nanite, Lumen, World Partition, and Niagara, allowing developers to create realistic game worlds with large amounts of geometry and realistic lighting. The Marketplace allows developers to buy or sell resources for their projects. One of the popular plugins for Unreal Engine 5, Gameplay Ability System, allows developers to create complex game abilities and mechanics, providing fast and effective implementation. The "Dungeon crawl" genre, which focuses on exploration, combat, resource gathering, and character progression in underground labyrinths, has been chosen. Developing a game in the "Dungeon crawl" genre using Unreal Engine 5 and Gameplay Ability System is an innovative idea.

У наш час одним з передових ігрових рушіїв є Unreal Engine 5 [1], створений компанією Epic Games. Цей потужний інструментарій для розробки відеоігор та інтерактивних додатків став одним із найпопулярніших та найвикористовуваніших ігрових рушіїв у світі. Нова версія Unreal Engine 5 надає розробникам доступ до високоякісного графічного рушія, набору інструментів для створення, управління та редагування вмісту гри, а також різноманітних функцій для розробки ігрового середовища. Основними перевагами нової версії рушія є Nanite (технологія, яка дозволяє відображати величезні кількості геометрії в реальному часі без значного впливу на продуктивність), Lumen (система глобального освітлення, яка автоматично розраховує освітлення у реальному часі), World Partition (функція, яка дозволяє автоматично розділяти великі гри на менші фрагменти, що дозволяє оптимізувати роботу з великими ігровими світами та прискорює процес розробки), Niagara (покращений візуальний ефектний редактор, який дозволяє створювати складні та реалістичні візуальні ефекти у реальному часі).

Неможливо не згадати про Marketplace – це онлайн-магазин, де розробники можуть придбати та продавати різноманітні ресурси, такі як 3D моделі, текстури, анімації, аудіофайли, плагіни, проектні шаблони та інші активи, які можна використовувати в проектах, створених на рушії Unreal Engine. Marketplace є важливим ресурсом для розробників, що

дозволяє швидко та ефективно знаходити та використовувати різноманітні ресурси для своїх проектів, що сприяє швидкому та ефективному розвитку відеоігор та інших інтерактивних додатків.

Один із популярних плагінів для Unreal Engine 5 є Gameplay Ability System [2]. Це розширення надає розробникам гнучку та потужну систему для створення та керування різноманітними ігровими можливостями або здібностями в їх іграх. Плагін розроблений компанією Epic Games спрощує створення складних систем геймплею та забезпечує швидку і ефективну реалізацію різноманітних ігрових механік. Він має вже готову систему атрибутів, ефектів та здібностей з якою зручно працювати, та завжди можна допрацьовувати та доповнювати під потреби.

Обрано жанр гри "Dungeon crawl". Це піджанр рольових відеоігор, що акцентується на дослідженні, бойових сценах, зборі ресурсів та прокачуванні персонажа у великих лабіринтах або підземних просторах, які часто відображаються у вигляді сітки кімнат і коридорів.

Враховуючи всі вищезазначені фактори, було вирішено, що розробка гри у жанрі Dungeon crawl за допомогою ігрового рушія Unreal Engine 5 та плагіну Gameplay Ability System є інноваційною ідеєю.

Список використаних джерел:

1. Unreal Engine 5 / Офіційний сайт. [Електронний ресурс] – https://www.unrealengine.com/en-US/unreal-engine-5.

2. Gameplay Ability System / Документація плагіну. [Електронний ресурс] – https://docs.unrealengine.com/5.0/en-US/gameplay-ability-system-for-unreal-engine.

УДК 004.032.2:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.144

ПРОГНОЗУВАННЯ ТРАФІКУ В ЛОКАЛЬНИХ МЕРЕЖАХ, ПОБУДОВАНИХ З ВИКОРИСТАННЯМ ОБЛАДНАННЯ JUNIPER

Парінцев Д.О.
Науковий керівник – доц. Омельченко А.В.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
e-mail: dmytro.parintsev@nure.ua

Organizations of all sizes are looking for innovative solutions to improve the efficiency of their network infrastructure. One of the leading manufacturers in this field is Juniper Networks, known for its advanced technologies and wide range of products. Solving the network traffic prediction problem is of great interest in areas such as congestion control, loss control, and bandwidth allocation. The article examines the effectiveness of traffic forecasting algorithms in local networks taking into account fractality.

Організації будь-якого розміру шукають інноваційні рішення для оптимізації своєї мережевої інфраструктури. Для багатьох локальні мережі стають ключовим елементом управління та обміну даними. Використання сучасного обладнання є запорукою стабільної та ефективної роботи мережі. Одним з провідних виробників у цій галузі є компанія Juniper Networks, відома своїми передовими технологіями та широким асортиментом продукції. Обладнання Juniper Networks дозволяє організаціям досягти високої продуктивності та безпеки мережі. Juniper Networks пропонує рішення для різних потреб, включаючи маршрутизацію, комутацію, безпеку та управління мережею. Серед найважливіших напрямків - розробка і впровадження передових технологій, таких як програмно-визначені мережі (SDN) і мережі на основі намірів (IBN), які дозволяють автоматизувати і оптимізувати роботу мереж. Оптимізація локальних мереж з обладнанням Juniper стає серйозним викликом для мережевих інженерів з такими технологіями, як QoS (Quality of Service), VLAN (Virtual Local Area Networks), LAG (Link Aggregation) і багатьма іншими. Juniper Networks постійно працює над вдосконаленням своїх продуктів і розробкою нових рішень для задоволення зростаючих мережевих потреб сучасних організацій. Окрім надання стабільного та надійного обладнання, компанія також впроваджує інтелектуальні системи управління мережею, які відіграють важливу роль в індустрії. При управлінні мережами слід враховувати явище фрактальності (самоподібності) трафіку. При цьому значний інтерес для таких областей, як контроль перевантажень, контроль втрат та розподіл смуги пропускання має задача прогнозування мережевого трафіку.

Самоподібність трафіку в комп'ютерних мережах була вперше описана в класичних роботах [1, 2]. Такий трафік характеризується значною нерівномірністю, що приводить до погіршення його обслуговування. Інтуїтивно самоподібність означає, що властивості об'єкта зберігаються незалежно від масштабування часу або простору. У комп'ютерних мережах нас цікавить статистична самоподібність, тобто поведінка автокореляційної функції на різних часових масштабах. Ступінь нерівномірності фрактального трафіку зазвичай характеризується параметром Херста. Більшість досліджень зосереджено на прогнозуванні трафіку за допомогою таких методів, як ARIMA; різні версії ARIMA (наприклад, SARIMA, Fractional-ARIMA) використовуються для врахування тенденцій у часовій еволюції обсягів трафіку [2]. SARIMA (Seasonal ARIMA) - це метод, який використовується для аналізу сезонних та циклічних моделей трафіку з метою виявлення повторюваних моделей попиту користувачів. Метою даного дослідження є оцінка ефективності алгоритму прогнозування трафіку в локальних мережах. Дослідження включає порівняльний аналіз декількох алгоритмів прогнозування, включаючи LV-predictor, прогнозування на основі моделей ARIMA(1,0,0) та ARIMA(1,0,0), просте експоненціальне згладжування та подвійне експоненціальне згладжування. Для оцінки алгоритмів використовується середньоквадратична помилка прогнозу. Результати проведеного дослідження підтвердили, що просте експоненціальне згладжування дає найкращі прогнози для заданого трафіку. Такі прогнози еквівалентні використанню моделі часового ряду ARIMA(0,1,1). Перехід до подвійного згладжування не покращив точність прогнозу, що можна пояснити відсутністю чіткого тренду у трафіку, що розглядається. Використання авторегресійних моделей 1-го та 2-го порядку, що належать до класів ARIMA(1,0,0) та ARIMA(1,0,0) відповідно, суттєво відстає за точністю прогнозу від простого експоненціального згладжування, яке є найбільш придатним для ARIMA(0,1,1) процесів.

Список використаних джерел:

1. Beran J., Sherman R., Taqqu M.S. Willinger W., Long-Range Dependence in Variable-Bit Rate Video Traffic. IEEE Transactions on Communications. Vol. 43. № 2,3,4. 1995.

2 Leland W.E., Taqqu M.S., Willinger W., Wilson D.V. On the self-similar nature of ethernet traffic // IEEE/ACM Transactions of Networking, 2(1), 1994. P. 1-15.

УДК 621.391:004.4 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.146

ПЕРЕВАГИ ЗАСТОСУВАННЯ КРОСПЛАТФОРМНИХ ЗАСОБІВ ПРИ РОЗРОБЦІ МОБІЛЬНИХ ЗАСТОСУНКІВ

Попов І.К.
Науковий керівник – к.т.н., доц. каф. ІМІ, Харченко Н.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: illia.popov@nure.ua.

Створення мобільного застосунку у традиційній формі є процесом трудомістким та коштовним, так як для різних мобільних операційних систем треба виділяти окремі ресурси та затрати у часі, оскільки кожна з них базується на окремій мові програмування та потребує урахування особливостей функціонування. Одним з ефективних шляхів вирішення вказаної проблеми є використання концепції гібридних мобільних застосунків та застосування у процесі розробки особливостей кросплатформності, що передбачає можливість створювати застосунки для кількох платформ одночасно. Використання гібридних застосунків у ряді випадків є більш економічно ефективним рішенням, ніж нативна розробка застосунків для найбільш популярних мобільних платформ, але слід враховувати також наявність недоліків такої концепції.

Розробка мобільних застосунків є відносно молодою областю наукових досліджень. Але завдання, що виконуються мобільними застосунками, їх складність та кількість постійно зростають. Мобільні застосунки тісно інтегруються з операційною системою телефону. Їх взаємодія виконується через так званий програмний інтерфейс API (Application Programming Interface). Код, який реалізує API-функції, знаходиться у пам'яті тільки в одному екземплярі, відповідно застосунки займають менший об’єм пам’яті та економніше споживають ресурси мобільного пристрою. Проте створення мобільного застосунку у традиційній формі є процесом трудомістким та коштовним, так як для різних мобільних операційних систем треба виділяти окремі ресурси та затрати у часі, оскільки кожна з них базується на окремій мові програмування та потребує урахування особливостей функціонування. За таких умов доводиться залучати до роботи різних спеціалістів (розробників, дизайнерів, тестувальників) для кожної окремої платформи, що підвищує вартість розробки [1].

З урахуванням вищезазначеного, об’єктивною необхідністю є пошук можливих напрямів здешевлення і спрощення процесу розробки застосунку.

Одним з ефективних шляхів вирішення вказаної проблеми є використання концепції гібридних мобільних застосунків та застосування у процесі розробки особливостей кросплатформності, що передбачає можливість створювати застосунки для кількох платформ одночасно.

Гібридний мобільний застосунок – це програмне забезпечення для мобільних пристроїв, що базується на основі WebView мобільної платформи. Тобто, по суті, це – мобільний сайт, розміщений в оболонці нативного застосунку, що забезпечує доступ до нативних функцій смартфону, таких як GPS, камера, здійснення дзвінків тощо [1].

Відзначимо також, що гібридна кросплатформна розробка потребує, у середньому, на 66,7% менше витрат, ніж одночасна нативна розробка окремих додатків для Android та iOS [1].

Таким чином відзначаємо велику кількість переваг при використанні гібридних мобільних застосунків [2]. Особливо пирвабливими є:

- економічна ефективність. Розробка одного застосунку, що може використовуватись всіма платформами, замість окремих розробок під кожну платформу логічно зменшує витрати як ресурсів, так і часу. Також значно полегшується процес оновлення та додавання нових функцій;

- легкість розробки застосунку. У сучасних умовах будь-який веброзробник може створити гібридний мобільний застосунок без необхідності вивчення додаткових технологій, також розроблено та є у вільному доступі велика кількість різних інструментів (HTML, CSS та JavaScript), банків безкоштовних бібліотек, плагінів та фреймворків;

- використання без доступу до інтернету. Використання API та зберігання даних локально на пристрої є об’єктивною необхідністю для користувачів з невеликою швидкістю інтернет-з’єднання;

- швидке встановлення. На відміну від нативних застосунків, гібридні не потребують встановлення на пристрої, а додаються безпосередньо з браузера.

Звісно будь-яка технологія має свої недоліки, у гібридних застосунків це нижча продуктивність, порівняно з нативними, що буде дещо погіршувати роботу програмного забезпечення. Тому при виборі платформи для розробки мобільних застосунків в першу чергу слід враховувати бізнес-задачі, які він має вирішувати, та вимоги, яким має відповідати

Список використаних джерел:

1. Moroz, T., & Endres, V. (2019). Advantages of hybrid mobile applications and progressive web apps for entrepreneurs . Ukrainian Black Sea Region Agrarian Science, 23(1), 96-102. DOI: 10.31521/2313-092X/2019-1(101)-14 2. Скачков Д.А. РОЗРОБКА ПРАКТИЧНИХ МЕТОДіВ ПРОЕКТУВАННЯ ТА СТВОРЕННЯ ВЕБ-ДОДАТКіВ // SR. 2015. №2 (14). URL: https://cyberleninka.ru/article/n/rozrobka-praktichnih-metodiv-proektuvannya-ta-stvorennya-veb-dodatkiv.

3. К.В. Харченко Методи та засоби розробки програмних додатків для операційної системи андроїд.// Збірник наукових праць. Серія: Нові рішення в сучасних технологіях. – Х.: НТУ «ХПІ». – 2014. - № 17. – С. 68-72.

УДК 004.032:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.148

АНАЛІЗ ПРИНЦИПІВ КОНТЕЙНЕРНОГО УПРАВЛІННЯ НА БАЗІ СИСТЕМИ KUBERNETES

Приходько О.С.
Науковий керівник – доц. Колтун Ю.М.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: oleksii.prykhodko@nure.ua

A key solution used for service orchestration is Kubernetes, an open source software for automating the deployment, scaling and management of containerized applications. At the core of Kubernetes is container technology, which is made up of Docker containers. A container is a small virtual machine that performs one simple task, meaning it actually implements a single microservice. The aggregate of microservices forms a microservice platform. The paper makes a detailed analysis of Kubernetes system architecture, its components and services. The options of traffic management between multiple microservices of Kubernetes container platform with the help of Istio are analyzed.

Нинішнє согодення все гостріше потребує розв'язання задач, що пов'язані з реалізацією та розгортанням сучасних мережних і хмарних сервісів, а також забезпечення можливостей, щодо їх автоматизації, управління, маршрутизації, виявлення і усунення проблем, і т. ін. Програмні системи та платформи, що реалізують такі підходи, вже досить широко використовуються сучасними інформаційними платформами (такими як Google, Amazon, Ebay, Facebook, YouTube, тощо) завдяки значній гнучкості та економічності в реалізації своїх рішень [1].

Серед рішень, розроблених для оркестрації сервісів, виділяється система Kubernetes - відкрите ПЗ для автоматизації розгортання, масштабування та управління контейнеризованими додатками. Це ПЗ з відкритим вихідним кодом розміщене на серверах Cloud Native Computing Foundation (CNCF). Основою системи Kubernetes є котейнерна технологія, яку утворюють docker контейнери, що є базовими для створення сервісів. Контейнер по суті є міні операційною системою з необхідним функціоналом тільки для виконання певної задачі. Вони займають дуже мало дискового простору, а їх запуск триває невеликий час. Іншими словами - це класична віртуальна машина дуже маленького розміру, яка виконує одну досить просту задачу. Виходячи з цього, контейнер фактично реалізує один мікросервіс, а їх сукупність формує мікросервісну платформу або, інакше, котейнерну технологію, що лежить в основі Kubernetes, де кожен сервіс характеризується незалежністю один від одного [1].

Метою доповіді є аналіз можливостей застосування Kubernetes для автоматизації розгортання, управління та моніторингу сервісів з використанням контейнерів. У процесі аналізу такої складної системи як

Kubernetes треба відстежувати сервіси в контейнерах, збирати та систематизувати метрики, налаштувати безпеку, враховувати аспекти мережного управління трафіком у процесі взаємодії мікросервісів, тощо.

Традиційно сервіси розгортали безпосередньо на вузлах із вихідних кодів або інсталяційних пакетів. З появою систем класу CMT (Configuration Management Tools), таких як puppet, ansible, chef, - цей процес став більш автоматизованим, але все ще потребував участі фахівця в плануванні інфраструктури сервісної платформи і написанні конфігураційних файлів для автоматизації процесів, що пов'язані із виконанням рутинних задач. Головним недоліком такого підходу є низька продуктивність [2].

У разі застосування Kubernetes підхід щодо розгортання сервісів буде відмінним від традиційного, де контейнери подано як об'єкти, що не піддаються змінам (Immutable infrastructure). Контейнери розташовуються між вузлами кластера виходячи з політик розподілу (за замовчуванням розташовуються рівномірно між робочими вузлами кластера). Ізоляція між сервісами виконується на рівні контейнерної віртуалізації та мережевих модулів з можливістю шифрування до кінцевого пункту призначення. На рівні кластера існує безліч абстракцій щодо ізоляції об'єктів [2].

У роботі зроблено детальний аналіз архітектури системи Kubernetes, її компонентів і служб. Проаналізовано варіанти управління трафіком між мікросервісами за допомогою Istio, що представляє собою виділений рівень інфраструктури, який називається Service Mesh. Він допомагає обробляти зв'язок між сервісами, повторні запити, тайм-аути та автоматично шифрувати з'єднання і забезпечує можливості з управління трафіком між сервісами, збір статистики, моніторинг і безпеку в складних розгортаннях [3]. Зокрема в роботі аналізується управління трафіком на основі маршрутизації запитів, балансування навантаження, A/B-тестування та інші.

Всі варіанти управління трафіком мають свої особливості, переваги та недоліки. Тому вибір найкращого варіанта управління трафіком в мікросистемній платформі Kubernetes буде залежати від її налаштувань, структури та потреб сервісної інфраструктури.

Список використаних джерел:

1. Kubernetes Documentation: Overview of Kubernetes [Електронний ресурс] // KubeCon + CloudNativeCon Europe 2024. – Режим доступу до ресурсу: https://kubernetes.io/docs/concepts/overview/.

2. Kelsey Hightower, Brendan Burns, Joe Beda “Kubernetes: Up and Running: Dive into the Future of Infrastructure 1st Edition” – O’Reilly Media, 2017. 272 p.

3. Lee Calcote, Zack Butcher “Istio: Up and Running: Using a Service Mesh to Connect, Secure, Control, and Observe 1st Edition” – O’Reilly Media, 2019. 272 p.

УДК 621.391:623.746-519 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.150

ОПТИМІЗАЦІЯ КАНАЛУ ВІДЕОЗВ'ЯЗКУ ПІД ЧАС УПРАВЛІННЯ БПЛА

Світличний А.О.
Науковий керівник – к.т.н. Іваненко С.А.
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
e-mail: andrii.svitlychnyi@nure.ua

The problem of limited range of wireless connections is always faced by users of such technologies. With the increase in the energy capacity of UAV batteries and the possibility of their economical energy consumption, this problem has reached this industry as well. Despite the wide selection of both powerful transmitters and high-quality sensitive receivers for control, the limitation of the control range of UAVs is one of the biggest factors affecting their use. As a solution to the problem, the use of remote video image receivers is proposed, which allow to increase the height of the antenna suspension with minimal loss of the radio budget.

Проблема обмеженості дальності роботи бездротових з'єднань зажди постає перед користувачами таких технологій. Із збільшенням енергоємності акумуляторів БПЛА та можливості їхнього економічного енергоспоживання така проблема досягла і цієї галузі.

Не дивлячись на широкий вибір як потужних передавачів так і якісних чутливих приймачів для керування, обмеження дальності управління БПЛА є одним із найбільших факторів, що впливають на їх використання.

В першу чергу це викликано особливостями використовуваного діапазону частот радіохвиль для їхньої роботи. Як правило це діапазон УКХ. Його використання викликано в першу чергу компактністю антенного устаткування, яке використовується як на боці оператора так і БПЛА. Для оператора компактні антени потрібні для FPV шолома або окулярів, для борта їх розміри викликані зменшенням парусності, ваги та і загальною малогабаритністю БПЛА, розмір яких може бути співрозмірна із долонею.

Але на цьому переваги діапазону УКХ закінчуються – цей діапазон радіохвиль має суттєвий недолік, пов'язаний із тим, що надійний зв'язок можливий лише в межах прямої видимості. Формула, яка описує дистанцію прямої видимості для умов нормальної рефракції наведена нижче [1]:

$$r_0 = 3{,}57\left(\sqrt{h_1}+\sqrt{h_2}\right),$$

r_0 – відстань прямої видимості, км;

h_1, h_2 – висоти підвісу антен. (1).

Виходячи із формули рішенням цієї проблеми є збільшення висот підвісу антен зв'язку бездротової системи. Якщо у випадку БПЛА його антена може бути розташована на тій же висоті, що і сам борт, і ця висота може бути від декількох метрів до декількох сотень метрів, то у випадку із антеною оператора ситуація менш оптимістична: реально висота антени оператора не перевищує 1-2 метрів. А враховуючи той факт, що рельєф місцевості може бути несприятливим: пагорби, яри тощо, або оператор знаходиться в споруді із покрівлею, то прямої видимості може не бути і взагалі. Цей факт суттєво погіршує умови експлуатації БПЛА.

В якості вирішення такої проблеми пропонується використання виносних антен, які можуть забезпечити винос антени для забезпечення прямої видимості як такої, а розміщення антени на щоглі дозволяє також збільшити висоту підвісу.

Однак у такого рішення також є і свої недоліки, а власне збільшення довжини фідера. А враховуючи частоти на яких відбувається зв'язок (як правило це 2,4 -5.8 ГГц) і втрати на таких частотах на доступних фідерах можуть складати 0,7 дБ/м для 2,4 ГГц і 1,2 дБ/м на 5.8 ГГц . Тобто при висоті підвісу хоча б 10 м втрати можуть бути вже дуже суттєвими. Таким чином рішення, яке дозволяє організувати пряму видимість, віднімає значну частину енергетичного бюджету.

Оскільки проблема найбільш гостра для аналогового каналу відеозв'язку (частота 5.8 ГГц), то в якості рішення, яке дозволяє вирішити цю проблему, пропонується використання виносного аналогового відео приймача FPV. На ринку присутня доволі якісна модель чутливого радіоприймача від виробника Skyzone R600 [2]. Він є доволі бюджетним і якісним приймачем.

Ідея його використання полягає в тому, що приймач має відеовихід із аналоговим стандартом PAL/Secam, який передається на частоті десятків МГц, і втрати сигналу на цих частот у фідері будуть менші ніж 0.01 дБ/м. Таким чином ця проблема вирішується: енергетичний бюджет збережений і висота підвісу антени оператора збільшена, обидва ці фактори суттєво можуть збільшити дистанцію зв'язку для управління БПЛА на УКХ із використанням аналогового каналу відеозображення.

Список використаних джерел:

1. «Расчет дальности прямой видимости» URL: https://3g-aerial.biz/onlajn-raschety/dopolnitelnye-raschety/raschet-dalnosti-pryamoj-vidimosti (дата звернення 04.03.2024)

2. «Skyzone R600 5.8G 32ch» URL: https://hobbyking.com/ru_ru/skyzone-r600-5-8g-32ch-wireless-av-receiver.html?___store=ru_ru (дата звернення 04.03.2024)

УДК 004.415:004.72 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.152

ПОРІВНЯННЯ МОНОЛІТНОЇ ТА МІКРОСЕРВІСНОЇ АРХІТЕКТУРИ У РОЗРОБЦІ У ВЕБЗАСТОСУНКІВ

Скворцов В. Х.
Науковий керівник – к.т.н., доц. Золотарьов В. А.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: vladyslav.skvortsov@nure.ua.

This paper is dedicated to the analysis and comparison of two approaches to software architecture in modern web development: monolithic and microservices. It discusses the characteristics, advantages, and challenges of each approach with the aim of determining the optimal solution for specific projects or organizations. The principles and advantages of microservices architecture are examined, along with the challenges faced by developers, compared to the main principles and advantages of the monolithic approach. Various aspects are considered during the analysis, including flexibility, scalability, and risk management, to provide a comprehensive assessment of both architectural models.

На сьогодні існує два підходи до архітектури програмного забезпечення у вебзастосунках: монолітна та мікросервісна (див. рисунок 1). На зображенні представлені такі елементи, як монолітна (Monolith) та мікросервісна (Microservices) архітектури, інтерфейс користувача (UI), бізнес-логіка (Business Logic) та доступ до даних (Data Access).
Метою доповіді є проаналізувати та порівняти два підходи до архітектури програмного забезпечення. Через огляд їх особливостей, переваг та викликів прагнемо з'ясувати, який підхід може бути найвигіднішим для конкретного проєкту чи організації.

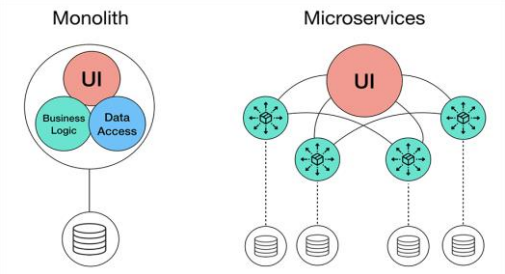


Рисунок 1 – Порівняння мікросервісної та монолітної архітектур
Мікросервісна архітектура (Microservices architecture) – це сучасний підхід до розробки програмного забезпечення, що базується на розбитті великих застосунків на невеликі, незалежні, добре визначені та автономні сервіси, які спілкуються між собою через API [1].

Мікросервісна архітектура ґрунтується на кількох принципах, які формують його основу. Перш за все, це розбиття застосунку на невеликі сервіси, кожен з яких відповідає за конкретну функціональність, і, важливо, ці сервіси повинні бути максимально незалежними та автономними. Далі, сервіси взаємодіють між собою через API, яке може працювати на різних протоколах, таких як HTTP, gRPC, та інші, що забезпечує легкість інтеграції та зміни. Кожен сервіс може мати свою власну базу даних або використовувати різні системи збереження даних, такі як SQL або NoSQL бази, що зменшує залежність між ними та сприяє легшому масштабуванню [2].

Крім того, кожен сервіс може бути розгорнутий незалежно від інших, що дозволяє швидко впроваджувати зміни та оновлення без необхідності перекомпіляції всього застосунку. Нарешті, сервіси можуть бути масштабовані незалежно один від одного залежно від навантаження, що дозволяє ефективно використовувати ресурси.

Щодо переваг мікросервісної архітектури, вона забезпечує гнучкість у внесенні змін та розвитку окремих сервісів, масштабованість, що дозволяє легко реагувати на потреби, швидкість розгортання нових функцій та оновлень через незалежність сервісів, та зменшення ризиків виникнення великих збоїв.

Однак, існують і виклики, зокрема, складність управління та моніторингу багатьох сервісів, збільшення мережевих витрат через збільшення комунікації, а також ускладнене тестування та налагодження через розподілений характер архітектури. Таким чином, мікросервісний підхід може бути ефективним для великих, складних застосунків, але потребує додаткових зусиль у проєктуванні та управлінні порівняно з традиційними монолітними архітектурами.

Монолітна архітектура (Monolithic architecture) – це традиційний підхід до розробки програмного забезпечення, при якому весь застосунок побудований як єдине ціле, з усіма його компонентами та функціональністю, які взаємодіють між собою в межах одного кодового базису [3].

Основні принципи монолітної архітектури полягають у тому, що застосунок розробляється та підтримується як єдине ціле. Усі компоненти та функціональність зазвичай знаходяться в межах одного кодового базису, що робить розробку простішою [4].

Проте така єдність також призводить до того, що всі компоненти взаємозалежні, а це своєю чергою ускладнює управління ризиками. Проблеми в одному компоненті можуть мати каскадний ефект на всю систему, роблячи виявлення та виправлення проблем складнішими. Крім того, масштабування такої архітектури також може бути проблематичним, оскільки всі компоненти знаходяться в межах одного кодового базису. Хоча є переваги, наприклад, простота розробки та зменшення накладних

витрат, через меншу потребу у комунікації та інтеграції, проте виклики монолітної архітектури, такі як складність масштабування та залежність компонентів, можуть стати перешкодою для великих та складних систем.
Тому монолітний підхід може бути ефективним для менших проєктів або проектів з обмеженими ресурсами, але не завжди підходить для великих та складних систем, які вимагають гнучкості та масштабованості.
У монолітної архітектури є переваги, зокрема простота розробки та зменшення накладних витрат на комунікацію та інтеграцію, оскільки весь код знаходиться в одному місці. Однак це може призвести до проблем з масштабуванням та управлінням ризиками, оскільки всі компоненти взаємозалежні. З іншого боку, мікросервіси дозволяють розділити застосунок на окремі сервіси, що полегшує розробку та підтримку, а також дозволяє більш гнучко масштабувати окремі частини системи та управляти ризиками.
Вибір між монолітною та мікросервісною архітектурою залежить від потреб та вимог проєкту. Монолітний підхід підходить для менших проєктів або тих, що мають обмежені ресурси, де важлива простота та швидкість розробки. Однак він може бути непрактичним для великих та складних систем, які потребують гнучкості та масштабованості. Мікросервіси відповідають складним та розподіленим системам, де ключові гнучкість, масштабованість та управління ризиками.
На закінчення відзначимо, що обидві архітектури мають свої переваги та недоліки, і рішення має ґрунтуватися на конкретних вимогах проєкту, що розглядається. Ретельно оцінюючи компроміси між монолітною та мікросервісною архітектурою, можна вибрати найбільш відповідне рішення для досягнення цілей.

Список використаних джерел:

1. What are microservices IBM: вебсайт. URL: https://www.ibm.com/topics/microservices (дата звернення: 10.02.2024).
2. What are microservices AWS: вебсайт. URL: https://aws.amazon.com/ru/microservices/ (дата звернення: 10.02.2024).
3. Monolithic Architecture: вебсайт. URL: https://www.geeksforgeeks.org/monolithic-architecture/ (дата звернення: 10.02.2024).
4. Understanding Monolith Architecture: A Guide for Product Managers: вебсайт. URL: https://bootcamp.uxdesign.cc/understanding-monolith-architecture-a-guide-for-product-managers-1c7bd3c3a3cf (дата звернення: 10.02.2024).

УДК 621.391:[004.3+004.4] DOI https://doi.org/10.30837/IYF.PDICIMT.2024.155

ПОРІВНЯННЯ ПІДХОДІВ ДО СТВОРЕННЯ ПРОГРАМ ДЛЯ МОБІЛЬНИХ ПРИСТРОЇВ

Скворцов В. Х.
Науковий керівник – к.т.н., доц. Золотарьов В. А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: vladyslav.skvortsov@nure.ua.

This work is dedicated to comparing two main approaches to mobile application development: native apps, specifically adapted to certain operating systems, and web applications, accessed through a web browser. The characteristics of each approach, their advantages, and disadvantages are discussed. It is noted that native apps provide high performance and tight integration with the operating system, while web applications offer greater accessibility and scalability. The conclusions of the work enable a better understanding of which development approach to choose depending on the specific needs of the project and the conditions of application use.

Сьогодні інформаційно-комунікаційні технології стають дедалі важливішим елементом повсякденного життя. Однією з областей у сфері інформаційно-комунікаційних технологій є розробка мобільних програм, які надають користувачеві доступ до різноманітних сервісів та функцій через мобільні пристрої. Виникає лише питання вибору між нативними програмами, спеціально адаптованими під певні операційні системи, та вебзастосунками, доступ до яких здійснюється через веббраузер.

Метою доповіді є порівняння цих основних підходів до створення мобільних програм, аналіз їх особливостей.

Нативні програми – це програмні рішення, спеціально спроєктовані для використання на конкретній операційній системі або пристрої. Вони створюються з використанням мов програмування та інструментів, оптимізованих під цю платформу. Головна їхня перевага полягає в тісній інтеграції з особливостями та функціоналом обраної операційної системи [1]. Ці програми забезпечують високу продуктивність, тому що написані мовою, оптимізованою для конкретної платформи, а також мають прямий доступ до апаратних ресурсів пристрою, таких як камера, геолокація та інші. Це розширює можливості функціонала, який можна впровадити у застосунок [3].

Нативні застосунки мають природний інтерфейс користувача, інтегруються з операційною системою та легко публікуються в офіційних магазинах, що спрощує їхнє поширення та встановлення.

Втім, розробка нативних програм може вимагати більше часу та ресурсів через необхідність створення окремих версій для кожної платформи. Це

також може зробити їх менш сумісними з іншими пристроями та операційними системами.

Вебпрограми являють собою програми, які можна використовувати через веббраузер, не встановлюючи їх на пристрій. Вони розробляються за допомогою вебтехнологій, таких як HTML, CSS та JavaScript, та працюють на різних пристроях, включаючи комп'ютери, смартфони та планшети [2]. Однією з їх ключових особливостей є доступність через інтернет, що дозволяє користувачам звертатися до них з будь-якої точки світу без необхідності встановлення.

Оновлення вебпрограм відбуваються на сервері, тому користувачі автоматично отримують доступ до останніх версій без завантаження чи інсталяції. Вони також платформонезалежні, що дозволяє працювати на різних пристроях та операційних системах [3]. Вебзастосунки легко масштабуються за потреби, обслуговуючи велику кількість користувачів. Розробники можуть оперативно вносити виправлення та покращення без необхідності встановлення оновлень на пристроях користувачів, оскільки оновлення виконуються на сервері.

Інтеграція з іншими вебсервісами та API дає розширені можливості як для користувачів, так і розробників. Всупереч перевагам, вебпрограми можуть обмежуватися доступом до апаратних ресурсів пристрою та залежать від якості інтернет-з'єднання. Однак з розвитком вебтехнологій та можливостей браузерів, вебпрограми стають все більш потужними та функціональними, що робить їх привабливим вибором для багатьох завдань.

Порівняння вебзастосунків і нативних програм допомагає обрати оптимальний підхід до розробки. Вебзастосунки працюють через веббраузер, нативні – з магазину. Вебпрограми мають обмежений доступ до ресурсів, нативні – повний. Підтримка платформ для вебзастосунків простіша, оновлення вони робляться автоматично. Продуктивність вебзастосунків може бути нижчою, нативні зазвичай працюють швидше. Вибір між ними залежить від потреб проєкту, ресурсів і очікувань користувачів.

Список використаних джерел:

1. Типи мобільних застосунків : вебсайт. URL: https://smile-ukraine.com/ua/mobile-apps/mobile-apps-types (дата звернення: 15.02.2024).
2. Як створити вебзастосунок : типи, переваги, принцип роботи : вебсайт. URL: https://wezom.com.ua/ua/blog/kak-sozdat-veb-prilozhenie (дата звернення: 15.02.2024).
3. Розробка гібридних програм або нативна розробка : що краще для вашого проєкту? : вебсайт. URL: https://webbookstudio.com/ua/articles/hybrid-app-development-vs-native-which-is-best-for-your-project/ (дата звернення: 15.02.2024).

УДК 004.032:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.157

ЗАСТОСУВАННЯ РЕАКТИВНИХ ВЕБФРЕЙМВОРКІВ ІЗ ВИКОРИСТАННЯМ ПІДХОДУ "ОДИН РАЗ, ЗАПУСКАЙ СКРІЗЬ" (WRITE ONCE, RUN EVERYWHERE)

Скворцов В. Х.
Науковий керівник – к.т.н., доц. Золотарьов В. А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: vladyslav.skvortsov@nure.ua.

This paper explores the "Write Once, Run Everywhere" principle in the context of using reactive web frameworks. The main objective is to examine the key aspects of cross-platform development, including the advantages, disadvantages, and core principles of this approach. The study analyzes the role of popular reactive frameworks such as React, Vue, and Angular in creating universal applications capable of running on various devices and operating systems. It discusses the challenges developers face when applying this principle and proposes strategies for overcoming them.

"Один раз, запускай скрізь" (Write Once, Run Everywhere) – принцип, що дозволяє написати програму один раз і запускати її на різних платформах без змін у коді. Такий підхід забезпечує універсальність програм та їхню платформонезалежність, спрощуючи розробку для різних операційних систем і пристроїв [1].

Метою доповіді є ознайомлення з основними аспектами кросплатформової розробки, висвітлення її переваги, недоліки та ключові принципи.

Реактивні вебфреймворки здобули популярність завдяки здатності надавати потужні інструменти для створення сучасних та інтерактивних вебзастосунків. Їх можна легко поєднати з принципом "один раз, запускай скрізь", що дозволяє розгортати застосунки на різних платформах та пристроях без переписування коду під кожну з них.

Реактивні вебфреймворки, такі як React, Vue та Angular [2], відіграють ключову роль у створенні високопродуктивних та адаптивних інтерфейсів. Принцип спрощує розробку, дозволяючи створювати програми, які працюють на різних пристроях та операційних системах. Проте виникають виклики, такі як забезпечення кросплатформної сумісності та оптимізація продуктивності для різних пристроїв і браузерів.

Основні аспекти реактивних вебфреймворків включають компонентний підхід, що розділяє застосунок на частини, щоб створювати модульні системи. Віртуальний Document Object Model (Модель Об'єктів Документа) оптимізує продуктивність, мінімізуючи маніпуляції з DOM із застосуванням альтернативного представлення. Двостороннє зв'язування

даних автоматично оновлює інтерфейс при зміні даних, роблячи програми чутливішими та зрозумілішими. Реактивні фреймворки підтримують композицію компонентів і перевикористання коду для гнучких та ефективних застосунків.

Концепція "один раз, запускай скрізь" базується на кількох ключових принципах. Вона передбачає універсальність програмного забезпечення, яке працює на будь-яких платформах без модифікації коду, ефективність розробки через повторне використання компонентів та коду, масштабованість програм для різних пристроїв та операційних систем, платформонезалежність і економію часу та ресурсів. Використання цієї концепції дозволяє створювати універсальні та ефективні застосунки, що працюють на різних пристроях та платформах без додаткового кодування чи адаптації [3].

Принцип має свої переваги та недоліки, які важливо враховувати при розробці програмного забезпечення. Переваги цього підходу полягають в ефективності розробки, оскільки код може бути написаний лише один раз і використаний на різних платформах, універсальності, що дозволяє запускати програмне забезпечення на різних пристроях без необхідності модифікації, а також у масштабованості та збереженні ресурсів. Однак існують недоліки, такі як обмежені можливості на деяких платформах, складнощі з сумісністю та оптимізацією, а також ускладнення підтримки та оновлень на різних пристроях. Таким чином, при розробці програмного забезпечення потрібно уважно враховувати ці переваги та недоліки, а також конкретні вимоги проєкту та потреби користувачів, перш ніж вирішувати, чи використовувати принцип "один раз, запускай скрізь".

Отже, вибір використання принципу "один раз, запускай скрізь" повинен бути здійснений з урахуванням конкретних вимог проєкту та потреб користувачів. При правильному використанні цей принцип може значно спростити та прискорити розробку програмного забезпечення, але потребує уважного аналізу та підходу для подолання можливих викликів та обмежень.

Список використаних джерел:

1. Write Once, Run Anywhere: вебсайт. URL: https://key2consulting.com/write-once-run-anywhere-best-application-development-frameworks/ (дата звернення: 21.02.2024).
2. npm trends : вебсайт. URL: https://npmtrends.com/angular-vs-react-vs-vue (дата звернення: 21.02.2024).
3. Building Cross Platform Applications Overview: вебсайт. URL: https://learn.microsoft.com/en-us/xamarin/cross-platform/app-fundamentals/building-cross-platform-applications/overview (дата звернення: 21.02.2024).

УДК 004:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.159

ГЕНЕРАЦІЯ НЕСТАЦІОНАРНИХ ІМІТАЦІЙНИХ ПРОЦЕСІВ АВТОРЕГРЕСІЇ

Старокожко Д. А.
Науковий керівник – проф. Тихонов Вячеслав Анатолійович
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: denys.starokozhko@nure.ua.

The problem of obtaining non-stationary, correlated time series is considered. The use of an additive mixture of sinusoids with white noise to obtain them has limited practical value. The proposed method includes a stationary autoregressive model and a special case of a non-stationary autoregressive model - an integrated moving average. Formulas are given that make it possible to methodologically use the proposed model.

Послідовності подій, до яких відносяться часові ряди, викликають особливий інтерес [1]. Він викликаний їх накопиченням, різноманітністю, еволюцією та зміною у часі. Розглянемо часові ряди, тобто, послідовності спостережень, що є автокорельованими випадковими процесами. Саме вони несуть інформацію про фізичний чи інформаційний процес. Наприклад, випадкові часові ряди широко використовуються в цифровій обробці мовних сигналів, розпізнаванні голосу та економетриці, а також у багатьох інших додатках. До випадкових часових рядів відносяться також номенклатура та ціни товарів, економічні дані, екологічні дані, режими протікання того чи іншого виробничого процесу та інше.

Відліки часового ряду логічно та статистично пов'язані. Цілі дослідження часових рядів можуть бути різними. Для стаціонарних і нестаціонарних процесів можна, наприклад, проводити вимірювання характеристик часового ряду, вирішувати завдання виявлення фізичного явища, робити прогноз, на підставі історичних даних минулого, керувати процесом, знаходити спектр процесу, намагатися з'ясувати механізм, що лежить в основі процесу, прибрати складові нестаціонарного процесу.

У моделі, якою користується контролер, мають бути визначені математичні операції, які він має виконувати. У зв'язку з цим зростає роль використовуваних алгоритмів генерації випадкових процесів [2]. На них, насамперед, випробуються методи і алгоритми обробки сигналів та процесів.

Випадкові часові ряди можна розділити на стаціонарні та нестаціонарні. Якщо зі стаціонарними процесами особливих проблем немає, і вони досить добре вивчені, то нестаціонарні випадкові процеси дуже складно вивчати і обробляти. Яскравим прикладом може бути дуже складне завдання - передбачення котирувань на біржі. Ці котирування нестаціонарні і, крім цього, мають тренд і високий рівень шуму.

Аналіз наукової літератури показує, що у нестаціонарних процесів немає єдиної теорії. Найбільшу популярність для певного виду нестаціонарності, має модель авторегресії – проінтегрованого ковзного середнього (АРПКС). Для моделі нестаціонарного процесу АРПКС можна навести її декомпозицію на складові. Нестаціонарна модель розглядається як подання нестаціонарного процесу у вигляді адитивної суми

$$\omega_1[t] = m[t] + c[t] + \omega[t],$$

де $\omega_1[t]$ – нестаціонарний процес, $m[t]$, $c[t]$, $\omega[t]$ – тренд, сезонна складова, корельована випадкова стаціонарна складова. Сезонна складова характерна для циклічних процесів. Без втрати спільності, далі сезонну складову не враховуватимемо. Стаціонарна модель авторегресії (АР), описується рівнянням

$$x[t] = \sum_{j=1}^{p} \Phi[j]x[t-j] + a[t], \quad (1)$$

де $\Phi[j]$– коефіцієнти АР, $a[t]$– некорельовані випадкові відліки, p – порядок моделі АР. В операторній формі модель АР(p), описувана рівнянням (1), може бути представлена у вигляді

$$\Phi(z)x[t] = a[t], \quad (2)$$

де в (2) оператор АР $\Phi(z)$ представляється як

$$\Phi(z) = 1 - \Phi[1]z^{-1} - \ldots - \Phi[p]z^{-p}.$$

Дії оператора зсуву z^{-i} на поточний відлік $x[t]$ описується наступним виразом

$$z^{-i}x[t] = x[t-i].$$

Показано [3], що при використанні моделі АРПКС, процедура видалення тренда, здійснюється відніманням із наступного значення відліку попереднього значення. Для нестаціонарного процесу з трендом, у цьому випадку, дією оператора $\nabla^d = (1-z)^d$, тренд видаляється. Тобто тренд видаляється дискретною операцією диференціювання.

Тоді процес без тренда можна показати у вигляді дії на процес із трендом $\omega_1[t]$, оператора взяття різниці. Зазвичай, обмежуються найпростішими випадками лінійного та квадратичного тренду. Для цих випадків $d=1,\ d=2$ відповідно. Тоді процес АР без тренда, можна записати можна записати у вигляді

$$x[t] = \nabla\omega_1[t] = \omega_1[t] - \omega_1[t-1],$$

або при квадратному тренді

$$x[t] = \nabla^2\omega_1[t] = \nabla(\omega_1[t] - \omega_1[t-1]) = (\omega_1[t] - 2\omega_1[t-1] + \omega_1[t-2]).$$

Розглянемо завдання генерації імітаційного нестаціонарного процесу зі згаданими трендами. Характеристичне рівняння АР можна записати наступним чином

$$c^p - \Phi[1]c^{p-1} - ...\Phi[p] = \prod_{i=1}^{p}(c - c[i]) = 0$$

Із [4] слідує, що коефіцієнти АР пов'язані з коренем характеристичного рівняння. Наведемо деякі формули для $p = 2,4$:

$$\Phi[1] = c[1] + c[2];$$
$$\Phi[2] = -c[1]c[2];$$
$$\Phi[1] = c[1] + c[2] + c[3] + c[4];$$
$$\Phi[2] = -(c[3]c[4] + c[2]c[3] + c[1]c[3] + c[4]c[1] + c[2]c[3] + c[2]c[4]);$$
$$\Phi[3] = c[1]c[3]c[4] + c[2]c[3]c[4] + c[1]c[2]c[3] + c[1]c[2]c[4];$$
$$\Phi[4] = -c[1]c[2]c[3]c[4].$$

Корінь характеристичного рівняння задається центральною частотою і її шириною полоси процесу [4].

В операторній формі, формуючий імітаційний АР процес, є рекурсивний фільтр. Білий шум використовується як утворюючий процес. Формуючий фільтр стаціонарного процесу описується рівнянням

$$x[t] = H(z)a[t] = \frac{a[t]}{\Phi(z)}.$$

Для моделі нестаціонарного процесу проінтегрованої авторегресії другого порядку з лінійним трендом

$$(1 - \Phi[1]z^{-1} - \Phi[2]z^{-2})(1 - z^{-1})\omega_1[t] = a[t].$$

Тоді стаціонарний процес АР(2) описується виразом

$$(1 - \Phi[1]z^{-1} - \Phi[2]z^{-2})x[t] = a[t].$$

Воно є окремим випадком (1). Для моделі нестаціонарного процесу проінтегрованої авторегресії четвертого порядку з квадратним трендом маємо

$$(1 - \Phi[1]z^{-1} - \Phi[2]z^{-2} - \Phi[3]z^{-3} - \Phi[4]z^{-4})(1 - z^{-1})^2\omega_1[t] = a[t].$$

Стаціонарний процес АР(4) описується виразом

$$(1 - \Phi[1]z^{-1} - \Phi[2]z^{-2} - \Phi[3]z^{-3} - \Phi[4]z^{-4})x[t] = a[t].$$

Список використаних джерел:

1. Марпл. –мл. С. Л. Цифровой спектральный анализ и его приложения. – М.: Мир, 1990. – 584 с.

2. Быков В.В. Цифровое моделирование в статистической радиотехнике. – М.: Сов. Радио, 1971. – 326 с.

3. Бокс Дж., Дженкинс Г. Анализ временных рядов: Пер. с. англ. – М.: Мир, 1974. – Вып.1. – 406с.

4. Тихонов В.А., Русановский Д.Е., Тихонов Д.В. Генерирование узкополосных имитационных случайных процессов // Радиоэлектроника и информатика. – 1999. – № 4. – С. 83-85.

УДК 004.77:364 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.162

ІНФОКОМУНІКАЦІЇ В СОЦІАЛЬНІЙ СФЕРІ

Славгородський Я.В.
Науковий керівник – доц. Харченко Н.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: yaroslav.slavhorodskyi@nure.ua.

Information and communication technologies (ICTs) have become an integral part of the social sphere, transforming the way people interact and communicate with each other. The rapid advancement of ICTs has led to the emergence of new forms of social communication, such as social media platforms and online communities. These platforms have enabled individuals and groups to connect and share information and ideas on a global scale, irrespective of geographical location or time constraints.On the other hand, the rise of ICTs has also raised concerns about their potential negative impact on social interactions and well-being.It is important to be aware of the potential challenges and risks associated with their use, and to adopt responsible practices to ensure a positive and healthy online experience.

Інформаційні технології та комунікації зазнали стрімкого розвитку в останні десятиліття, що відкрило безліч можливостей для їх використання у соціальній сфері. Застосування інфокомунікаційних засобів в сфері соціальних послуг, освіти, здоров'я та інших аспектах громадського життя значно змінило спосіб взаємодії між людьми та організаціями, а також покращило доступ до різноманітних ресурсів та послуг.

Крім того, інформаційні технології дозволяють покращити якість надання соціальних послуг. Електронні системи управління даними та онлайн-системи реєстрації можуть спростити процеси роботи з клієнтами та забезпечити більш ефективну організацію робочого процесу.

Вплив інфокомунікацій на соціальні послуги:

1. Цифрові платформи для надання соціальних послуг: платформи онлайн-послуг забезпечують ефективну організацію соціальних послуг, забезпечуючи швидкий доступ до інформації та можливість отримання допомоги в будь-який час і в будь-якому місці.
2. Технології для покращення якості життя: використання інфокомунікаційних технологій у розробці додатків для здоров'я, медичних порадників та платформ для онлайн-терапії дозволяє покращити доступність та якість медичних послуг.

Інформаційні технології в освіті:

1. Дистанційна освіта та онлайн-навчання: інтернет та цифрові технології створили можливість для розвитку дистанційної освіти, що розширює доступність освіти для різних категорій населення та сприяє постійному навчанню.

2. Інтерактивні навчальні платформи: розробка інтерактивних навчальних ресурсів та платформ дозволяє створювати індивідуальні підходи до навчання та підвищує зацікавленість учнів у процесі навчання.

Вплив інфокомунікацій на соціальну взаємодію:

1. Соціальні мережі та комунікаційні платформи: соціальні мережі стали важливим інструментом для спілкування, обміну думками та ідеями, а також для організації соціальних рухів та заходів.

2. Громадські ресурси та платформи з підтримки: інфокомунікаційні засоби відкривають можливості для створення громадських ресурсів та платформ з підтримки, які об'єднують людей навколо спільних інтересів та проблем.

Перспективи розвитку інфокомунікацій в соціальній сфері:

1. Штучний інтелект та аналітика для покращення соціальних послуг: використання штучного інтелекту для аналізу великих обсягів даних дозволяє удосконалити процеси надання соціальних послуг та забезпечити більш ефективну реакцію на потреби громадян.

2. Розвиток віртуальної реальності для соціального включення: віртуальна реальність може бути використана для створення іммерсивних середовищ, які допомагають людям з обмеженими можливостями відчувати себе більш соціально включеними та взаємодіяти з оточуючим світом.

Проте, на шляху впровадження інформаційних технологій у соціальній сфері стоять певні виклики. Одним із найважливіших є забезпечення безпеки та конфіденційності даних клієнтів. Також важливо враховувати цифрову нерівність, адже деякі групи населення можуть мати обмежений доступ до технологій або не мати достатньої освіти для їх ефективного використання.

Інфокомунікаційні технології відіграють ключову роль у трансформації соціальної сфери, забезпечуючи покращений доступ до різних ресурсів та послуг, сприяючи ефективнішій комунікації між людьми та організаціями, та створюючи нові можливості для соціального розвитку та взаємодії. Важливо продовжувати дослідження в цьому напрямку та розробляти нові інноваційні підходи для максимального використання потенціалу інфокомунікацій у соціальній сфері.

Список використаних джерел:

1. Інформація та соціальні комунікації сучасного світу: тренди глобалізації // Державний університет телекомунікацій. 2021. URL: https://moodle.znu.edu.ua/mod/resource/view.php?id=511206.

2. The Role of Information and Informational and Communication Technologies in Modern Society // Nadezhda N. ISACHENKO. 2020. URL: https://www.redalyc.org/journal/279/27957591031/html/.

3. Information Communication Technology Ensures a Safe Social Media Ecosphere // DivyeshAegis. 2021. URL: https://www.datasciencecentral.com/information-communication-technology-ensures-a-safe-social-media/.

УДК 621.391.1:004.032 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.164

МОЖЛИВОСТІ ПРОГНОЗУВАННЯ ТРАФІКУ У МУЛЬТИСЕРВІСНИХ МЕРЕЖАХ

Смірнов Є.А.
Науковий керівник – к.т.н., доц. каф. ІМІ, Харченко Н.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: yevhen.smirnov@nure.ua.

In modern multi-service networks, it is necessary to carry out a preliminary assessment of the level of requirements for the main parameters of the network, primarily for the productivity of switching centers and the necessary transmission speed of digital communication paths, which allows establishing the correspondence between demand, capacity and throughput. Modern research has found that telecommunication traffic is characterized by self-similarity, so the ON/OFF model is well suited for modeling fractal backbone network traffic. The proposed model is particularly convenient for simulating processes in multiservice networks with a stable number of sources and allows predicting load distribution in integrated information flows.

Ріст популярності мультисервісної мережі (МСМ) зв’язку – одна із самих помітних тенденцій ринку телекомунікаційних послуг в останні роки. Послуги такої мережі в першу чергу призначені для компаній, орієнтованих на інтенсивний розвиток бізнесу, оптимізацію витрат, автоматизацію бізнес-процесів, сучасні методи керування й забезпечення інформаційної безпеки.

В умовах необмежених обчислювальних ресурсів і пропускної здатності каналів проектування МСМ стає суто технічною задачею. Проблеми виникають як раз у випадку деякого обмеження ресурсів. Причому ці проблеми виявляються різними для різних видів трафіку.

В сучасних мультисервісних мережах необхідно проведення попередньої оцінки рівня вимог до основних параметрів мережі, в першу чергу до продуктивності центрів комутації і необхідної швидкості передачі цифрових трактів зв'язку, що дозволяє встановити відповідність між попитом, ємністю і пропускною спроможністю і дає відповідь на питання про можливість надання того чи іншого виду послуг. Однак розв'язанню цієї проблеми перешкоджає велика кількість факторів, таких як слаба вивченість телекомунікаційних мереж з інтегральним трафіком, відсутність загальних методик розрахунку характеристик трафіка в таких мережах і ін. [1].

Велика кількість параметрів, наприклад широкий діапазон швидкостей передачі, істотний статистичний характер інформаційних потоків, велика різноманітність мережних конфігурацій, значно

ускладнюють опис трафіка в мультисервісних системах в порівнянні з класичними мережами зв'язку.

У ряді робіт аналіз характеристик трафіка проводиться на основі його статистичного характеру в системах з довготривало залежними процесами на вході [2]. Однак, в загальному вигляді проблема оперативного отримання характеристик реального трафіка в мультисервісних мережах на сьогодні не вирішена [3]. Відповідно, актуальною є задача отримання оперативної оцінки статистичних характеристик трафіка, утвореного на комутаційних вузлах мережі при агрегуванні окремих інформаційних потоків, які направляються одним маршрутом [3].

Щоб задовольняти всі потреби користувачів й забезпечити гарантії надійності та доступності різноманітних сервісів мультисервісної мережі, потрібно застосовувати моделі, які відображають характеристики реального навантаження мережі. Сучасні дослідження виявили, що телекомунікаційному трафіку властива самоподібність, тому для моделювання фрактального магістрального мережного трафіка добре підходить ON/OFF модель. Традиційна ON/OFF модель формує процес, який є процесом приросту фрактального броунівського руху. ON/OFF модель широко використовується для моделювання джерел, які періодично генерують повідомлення [3].

При цьому якщо до такої моделі застосувати ієрархічний принцип побудови, це дозволить також врахувати групову передачу пакетів від одного джерела. Період активності буде розбиватися на менші ON й OFF періоди для урахування впливу більш низьких рівнів протоколу передачі даних. Тобто таким чином можливо також прогнозування поведінки окремих типів трафіку при передачі їх у загальному мультиплексованому потоку.

Список використаних джерел:

1. Кучук, Г.А. Моделювання трафіка мультисервісної розподіленої телекомунікаційної мережі [Текст] / Г.А. Кучук, І.Г. Кіріллов, А.А. Пашнєв // Системи обробки інформації. – Х.: ХУ ПС, 2006. – Вип. 9 (58). – С. 50 – 59.

2. Свиридов А. С., Коваленко А. А., Кучук Г. А. Метод перерозподілу пропускної здатності критичної ділянки мережі на основі удосконалення ON/OFF-моделі трафіку. Сучасні інформаційні системи. 2018. Т. 2, № 2. С. 139–144. DOI: https://doi.org/10.20998/2522-9052.2018.2.24

3. Кліменко О.А., Пархоменко Д.О., Щенякін О.В. Метод побудови On/Off моделі магістрального трафіка мультисервісної мережі. *Наука і техніка Повітряних Сил Збройних Сил України*. 2021. № 4(45). С. 111-15. https://doi.org/10.30748/nitps.2021.45.14.

УДК 004.77:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.166

АРХІТЕКТУРУ БЕЗПЕКИ "НУЛЬОВОЇ ДОВІРИ"

Усов О.О.
Науковий керівник – Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. IMI, м. Харків, Україна
e-mail: oleksandr.usov@nure.ua

Zero Trust is one of the latest cybersecurity buzzwords. Therefore, it is important to understand what Zero Trust is – and what Zero Trust is not. Zero Trust is a strategic initiative that helps prevent data leaks by eliminating the concept of trustworthiness from an organization's network architecture. The basic principle is “don’t believe anything without checking.” Zero Trust protects modern digital environments by leveraging network segmentation, preventing threat propagation, providing application-level threat defense, and simplifying granular access control for users.

Архітектура безпеки "нульової довіри" (Zero Trust Security Architecture) - це політика безпеки, яка полягає в тому, що жодна частина мережі або окремий користувач не повинні мати довіри до жодного об’єкту або суб’єкту мережі без перевірки. Тобто цей підхід базується на принципі "ніколи не довіряй, завжди перевіряй". Замість традиційного периметру безпеки, в якому внутрішній мережевий трафік вважається довіреним, у архітектурі "нульової довіри" кожен запит на доступ до ресурсів або сервісів обробляється і перевіряється.

Ця архітектура передбачає, що кожен запит на доступ до ресурсу або послуги повинен бути автентифікований, авторизований та обмежений за необхідності. Навіть користувачі, які знаходяться всередині мережі, повинні проходити через той самий процес перевірки, як і зовнішні користувачі. Основні принципи архітектури "нульової довіри" включають мінімізацію дозволів доступу, мікросегментацію мережі, багаторівневу автентифікацію та авторизацію, шифрування даних у спокійному стані та в руху, а також неперервний моніторинг та аналіз активності.

Переваги «нульової довіри»:

1. Зменшує ризик несанкціонованого доступу до ресурсів.
2. Знижує ризик витоків і розкриття даних у разі порушення безпеки.
3. Підвищує гнучкість: дозволяє безпечно надавати доступ до ресурсів користувачам, які працюють віддалено або з мобільних пристроїв.
4. Спрощує управління: централізує управління доступом до ресурсів.

Впровадження нульової довіри - це складний процес, який потребує

ретельного планування та виконання.

Безперервне підтвердження справжності учасників суб'єктів і об'єктів інформаційного доступу – постійна автентифікація та авторизацію з урахуванням усіх доступних точок доступу даних, підсилена ідентифікація пристрої та розмежування прав доступу користувачів

Налаштування доступу з мінімальними правами – обмеження доступу користувачів за часом і обсягом прав, застосування адаптивної політики безпеки, яка ґрунтується на основі оцінювання інформаційних ризиків; застосування апаратно-програмних засобів захисту, які не впливають на продуктивність мережі.

Розгляд кожного запиту на роботу в мережі як порушення безпеки - зменшення радіусу можливої атаки та обмеження доступу до сегментів інфокомунікаційної мережі; застосування наскрізного шифрування.

Незважаючи на багатоцілісні переваги, архітектура "нульової довіри" може зустрітися з певними викликами та обмеженнями. Наприклад, її впровадження може вимагати значних витрат на час та ресурси, а також технічний експертизи. Крім того, необхідно забезпечити сумісність з існуючими інфокомунікаційними системами та процесами, що може бути складно в деяких випадках.

Однак не зважаючи на ці виклики, архітектура "нульової довіри" залишається однією з найефективніших стратегій захисту інформації в інфокомунікаціях, яка забезпечує надійний захист від кіберзагроз та захистити дані від розкриття та модифікаціїтам .

Список використаних джерел:

1. Was ist eine Zero-Trust-Architektur? [Електронний ресурс] // The Forrester Wave™: Privileged Identity Management. – 2018. – Режим доступу до ресурсу: https://www.paloaltonetworks.de/cyberpedia/what-is-a-zero-trust-architecture.

2. Zero Trust Architecture [Електронний ресурс] / S.Rose, O. Borchert, S. Mitchell, S. Connelly // NIST Special Publication. – 2020. – Режим доступу до ресурсу: https://doi.org/10.6028/NIST.SP.800-207.

3. Zero Trust Architecture / [C. Green-Ortiz, B. Fowler, D. Houck та ін.]. – Singapore: O\'Reilly, 2023. – 336 с. – (Cisco Press).

УДК 621.396:004.7]:004.056
DOI https://doi.org/10.30837/IYF.PDICIMT.2024.168

ШИФРУВАННЯ WI-FI 6-МЕРЕЖ

Фодченко А.В.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: anastasiia.fodchenko@nure.ua

The purpose of this article is to look at and analyze the main aspects of encryption in Wi-Fi 6 in order to understand its importance, effectiveness and impact on the security and privacy of data. The report aims to present the technical details of encryption, including the developed cryptographic algorithms and protocols, as well as evaluate its effectiveness against a variety of threats and attacks. In addition, the evidence can include continuous analysis of the latest versions of Wi-Fi protocols, highlighting the advantages and disadvantages of the new approach to encrypting Wi-Fi data.

Розвиток Wi-Fi технології потребує удосконалення методів шифрування для забезпечення конфіденційності та цілісності даних у бездротових мережах. Покращення шифрування Wi-Fi 6-мереж (802.11ax) – запорука безпеки бездротового з'єднання. У 2018 р. організація Wi-Fi випустила нове покоління протоколу шифрування відоме як WPA3, розроблене для забезпечення простішої конфігурації та надійнішого шифрування та безпеки ніж його попередник WPA2 [1]. WPA3 є останнім поколінням протоколу захисту Wi-Fi, розробленим для забезпечення високого рівня безпеки в бездротових мережах.

Одним із найбільших удосконалень захисту приватності у WPA3 є реалізація підвищеної політики безпеки паролів за допомогою системи обміну ключами Dragonfly також відому як Simultaneous Authentication of Equals (SAE), який замінює метод Pre-Shared Key (PSK) у WPA2. SAE ускладнює злом паролів за рахунок більш «тонкого» методу встановлення з’єднання з Wi-Fi та нейтралізує атаки зловмисників на основі словника, від яких страждає PSK, таким чином, ефективно запобігає автоматизованому пошуку паролів для WLAN.

WPA3 також блокує раніше дозволені небезпечні хеші, такі як SHA1 або MD5. Для хешованого пароля Wi-Fi тепер використовується криптографія з еліптичною кривою: client і Wi-Fi роутер. Учасники інформаційного обміну домовляються про параметри еліптичної кривої і за допомогою пароля створіть точку на цій кривій. Потім кожна сторона вибирає випадкове число; клієнт використовує випадкове U, Wi-Fi роутер використовує число V. Клієнт обчислює uR, тобто кратне R на еліптичній кривій, яка в свою чергу обчислює і відправляє vR. Потім обидві сторони обчислюють і порівнюють загальний добуток і багато іншого як ключ. Проблема зловмисників полягає в тому, що, хоча вони перехоплюють R і

uR, а також vR, вони не можуть обчислити u і v з них, тому що їм довелося б обчислювати дискретний логарифм. Ще одна перевага аутентифікації за допомогою SAE полягає в тому, що навіть після перехоплення інформації, зловмисники не можуть потім розшифрувати записані повідомлення. Цей принцип називається Perfect Forward Secrecy (PFS) [2].

WPA3 застосовує вдосконалений стандарт шифрування AES у режимі GCM, який є надійнішим за AES-CCMP, що використовується в WPA2. Використання в WPA3 режиму захисту Opportunistic Wireless Encryption (OWE) забезпечує захищене з'єднання без необхідності введення пароля навіть при підключенні до невідомих або ненадійних мереж.

WPA3 використовує уніфіковану криптографію з більш надійним 192-бітним шифруванням, допомагаючи уникнути об'єднання протоколів безпеки, визначених у стандарті 802.11. Також WPA3 вимагає узгодження MPF (Protected Management Frames). PMF додає додатковий рівень безпеки для захисту від атак деаутентифікації та деасоціації [3].

До того ж WPA3 надає індивідуальне шифрування для кожного бездротового з'єднання. Тобто злам зловмисником одного з'єднання не дозволяє йому автоматично отримати доступ до інших з'єднань у мережі. Нагадаємо, що WPA2 використовує спільний ключ шифрування для всіх пристроїв, підключених до однієї мережі, і у разі компрометації ключа створює ризики для безпеки, якщо ключ буде скомпрометований.

WPA3 захищає від атак типу KRACK (Key Reinstallation Attacks), до яких був вразливий WPA2, завдяки вдосконаленій методології аутентифікації та захисту від атак на основі бокового каналу.

Отже Wi-Fi 6 є безпечнішим за попередні версії протоколів Wi-Fi. Впровадження WPA3, удосконалене та індивідуальне шифрування даних дозволяють підвищити рівень безпеки та захисту приватності у бездротових мережах. Втім слід пам'ятати, що безпека мережі залежить не лише від технологічних рішень, але й від правильної конфігурації та використання заходів безпеки всіма користувачами.

Список використаних джерел:

1. WiFi 6 vs WiFi 5, Which is Better in Performace? [Електронний ресурс]. – 2022. – Режим доступу до ресурсу: https://www.vsolcn.com/blog/wifi-6-vs-wifi-5.html.

2. WPA3 на Fritzbox [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: https://www.chip.de/artikel/WPA3-Neue-WLAN-Verschluesselung-optimal-nutzen_148220425.html.

3. У 2019 був затверджений стандарт WiFi 6. Що це таке і якими функціями забезпечили Wi-Fi 6? [Електронний ресурс] / GDS. – 2023. – Режим доступу до ресурсу: https://realweb.net.ua/blog/u-2019-buv-zatverdzhenij-standart-wifi-6-sho-ce-take-i-yakimi-funkciyami-zabezpechili-wi-fi-6_1.

УДК 004.9:378.091.279.7 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.170

ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ СИСТЕМИ АВТОМАТИЗАЦІЇ ПЕРЕВІРКИ ВИКОНАННЯ ПРАКТИЧНИХ ЗАВДАНЬ В ЛОКАЛЬНОМУ ВІРТУАЛЬНОМУ ОТОЧЕННІ КОРИСТУВАЧА

Федорченко О.М.
Науковий керівник – к.т.н., доцент Костромицький А.І.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: oleksandr.fedorchenko@nure.ua

The digital transformation of education necessitates tools that not only facilitate theoretical learning but also accurately assess practical skills in a remote setting. Traditional Learning Management Systems (LMS) are adept at delivering content and conducting tests but often fail to evaluate hands-on skills effectively. This thesis introduces a way to improve prototype system designed to bridge this gap by automating the verification of practical tasks performed in a user's local virtual environment, seamlessly integrated with LMS through the Learning Tools Interoperability (LTI) protocol. This system aims to overcome the limitations of existing solutions, offering a scalable and integrable approach to enhance distance learning's effectiveness and accessibility. There is way of improvement of existing prototype solution based on LMS with LTI protocol system.

Цифрова трансформація освіти потребує інструментів, які не лише полегшують теоретичне навчання, але й точно оцінюють практичні навички у віддаленому середовищі. Традиційні системи управління навчанням (LMS) добре справляються з наданням контенту та проведенням тестів, але часто не здатні ефективно оцінювати практичні навички. Потрібно розглянути способи вдосконалення прототипу системи, призначеної для подолання цього розриву шляхом автоматизації перевірки практичних завдань, що виконуються в локальному віртуальному середовищі користувача, безперешкодно інтегрованої з LMS через протокол Learning Tools Interoperability (LTI). Ця система має на меті подолати обмеження існуючих рішень, пропонуючи масштабований та інтегрований підхід для підвищення ефективності та доступності дистанційного навчання.

Розвиток LMS від простих механізмів доставки контенту привів до складних платформ, здатних підтримувати широкий спектр навчальних стратегій, включаючи перевернуті класи, змішане навчання та повністю онлайн-курси. Аналіз показує, що, незважаючи на свою еволюцію, платформи LMS часто залишаються обмеженими власними інструментами оцінювання, які, як правило, оптимізовані для опитувань і письмових завдань, тим самим маргіналізуючи оцінювання практичних навичок, які мають вирішальне значення в вивченні технологічних дисциплін

Що стосується протоколу LTI, то в аналізі літератури підкреслюється його значення як стандарту для інтеграції сторонніх навчальних додатків з LMS, що сприяє безперешкодному обміну інформацією та досвідом користувачів між різноманітними освітніми інструментами. У цьому розділі детально розглянуто, як LTI може поєднати можливості LMS зі спеціалізованими інструментами для таких завдань, як вправи з кодування, лабораторні симуляції та інші практичні види діяльності, але при цьому підкреслено, що інтеграції часто бракує глибини з точки зору автентичного оцінювання та механізмів зворотного зв'язку для складних завдань.

Дослідження технологій автоматизованого оцінювання представляє огляд існуючих рішень, включаючи платформи на основі штучного інтелекту, інструменти експертного оцінювання та тестування на основі симуляцій оточень. Хоча ці досягнення є значним кроком на шляху до подолання обмежень традиційних оцінювань LMS, вони часто не забезпечують надійної основи для детального оцінювання практичних завдань.

Сучасним технологіям бракує таких можливостей, як здатність точно моделювати реальні умови, надавати змістовний зворотній зв'язок і оцінювати широкий спектр практичних навичок у контекстно-релевантний спосіб.

Таким чином, існує необхідність розробки або поліпшення рішення, яке не лише використовує інтеграційні можливості протоколу LTI, але й долає поточні обмеження технологій автоматизованого оцінювання. Таке рішення має забезпечити більш достовірне та ефективне оцінювання практичних завдань, пристосоване до унікальних вимог різних дисциплін та узгоджене з педагогічними цілями сучасних освітніх систем.

Вдосконалення вищенаведеного рішення містить в собі:

1. Автоматизація процесів інтеграції, тестування та доставки коду, що може значно прискорити розробку та знизити ризик помилок при розгортанні. Це також сприяє швидкому впровадженню нових функцій і патчів безпеки.

2. Автоматизація тестування, розширення покриття коду юніт-тестами, інтеграційними тестами та тестами навантаження що допоможе забезпечити високу якість та надійність програмного забезпечення. Використання інструментів автоматизації тестування може спростити цей процес.

3. Забезпечення безпеки на рівні коду та інфраструктури. Регулярне сканування коду на предмет вразливостей, використання засобів шифрування для зберігання даних та передачі даних, а також налаштування правил міжмережевих екранів і систем виявлення та запобігання вторгненням можуть значно підвищити безпеку вашої системи.

УДК 004.056.55 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.172

ДОСЛІДЖЕННЯ ІНСТРУМЕНТІВ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Чалий Д.В.
Науковий керівник – ст. вик. кандидат технічних наук Калюжний М.М.
кафедри інформаційно-Мережної інженерії
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна
email: dmytro.chalyi@nure.ua

Cryptographic methods of information security are one of the key elements of modern information security; they themselves help to protect special information from malicious actors. These methods include a variety of encryption methods: symmetric and asymmetric encryption, hash functions, digital signatures, authentication and key exchange protocols, as well as cryptographic mechanisms such as factor authentication and quantum cryptography. Yu. The combination of all these methods makes it possible to create complex data protection systems that ensure a reliable level of security in the current digital environment.

Криптографічні методи захисту інформації є одним з ключових елементом сучасної інформаційної безпеки. Ці методи включають різні способи шифрування: симетричне та асиметричне шифрування, хеш-функції, цифрові підписи, протоколи аутентифікації та обмін ключами, а також криптографічні механізми факторної аутентифікації та квантову криптографію. Поєднання всіх цих методів дозволяє створити комплексні системи захисту даних, що забезпечують надійний рівень безпеки в сучасному цифровому середовищі.

Класифікація методів криптографічного захисту даних:

- Симетричне шифрування;
- Асиметричне шифрування;
- Хеш-функції;
- Цифровий підпис;
- Протоколи аутентифікації та обміну ключами;
- Контейнери даних та цифрові підписи;
- Криптографія мультифакторної аутентифікації;
- Квантова криптографія.

Симетричне шифрування - це метод в якому використовується один і той самий ключ як для шифрування, так і для розшифрування повідомлень. Головна мета цього методу запобігання отримання ключа, так як без нього розшифрувати дані не можливо. Приклади алгоритмів симетричного шифрування: AES, IDEA, Blowfish, Twofish, DES. Цей метод використовується в захисті даних в інтернеті, мобільних додатках, зберігання даних на сервері та в інших сверах.

Асиметричне шифрування – це метод в якому використовуються відкритий ключ, він використовує пари ключів: приватний і публічний. Публічний ключ використовується для шифрування повідомлень, а приватний ключ використовується для розшифрування. Цей метод використовується в багатьох сверах. В протоколах передачі даних, як TLS/SSL, та для шифрування трафіку,

цифрових підписах, SSH для безпечного з’єднання з віддаленим сервером, PGP/GPG для захисту електронної пошти та файлів, та в авторизації і аутентифікація.

Хеш-функції - це криптографічні алгоритми, які приймають вхідні обсях даних будь-якої довжини і перетворюють їх у фіксований вихідний хеш-код фіксованої довжини. Основна ціль хеш-функцій полягає в тому, що вони повинні бути односторонніми для того щоб неможливо було віднтворити вихідних даних з хеш-коду, стійкими до колізій (різних вхідних даних, що дають один і той самий хеш) та незмінні (той самий вхід завжди дає один і той самий вихід). Хеш-функції часто використовуються для перевірки цілісності даних. Це означає, що вони дозволяють перевірити, чи були дані змінені або пошкоджені під час передачі чи зберігання. Також хеш-функції використовуються для створення унікальних ідентифікаторів для об'єктів, файлів, повідомлень. Це може бути використано для швидкого пошуку чи ідентифікації об'єктів. Хеш-функції використовуються також для збереження паролів у вигляді хеш-кодів. Взамін зберігання самого пароля, система зберігає його хеш-код, що забезпечує більшу безпеку, оскільки паролі не зберігаються у відкритому вигляді. Також один з випадків використання хеш функцій для створення цифрових підписів, які дозволяють перевірити автентичність повідомлення та ідентифікацію відправника. Використовуються хеш-функції:

- Хеш-функції використовуються в криптографічних протоколах та системах для забезпечення безпеки даних;
- Хеш-функції використовуються для швидкого пошуку та індексації даних у базах даних;
- Хеш-функції використовуються для перевірки цілісності файлів та даних, що передаються через мережу;
- Хеш-функції використовуватися для створення унікальних ідентифікаторів для доступу до ресурсів чи послуг;
- Хеш-функції використовуються для збереження та обробки паролів користувачів в різних системах та сервісах.

Квантова криптографія базується на принципах квантової механіки для забезпечення безпеки комунікаційних каналів. Основною ідеєю квантової криптографії є використання фізичних властивостей квантових систем для забезпечення безпеки передачі даних. Вона дає надійну захист від криптоаналізу квантовими комп'ютерами, які можуть швидко розв'язувати складні математичні проблеми, що застосовуються у сучасних криптографічних алгоритмах.

Список використаних джерел:

1. Dong L., Chen K. Cryptographic Protocol. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. URL: https://doi.org/10.1007/978-3-642-24073-7;
2. Otruba K. CEC1702 Cryptographic Embedded Controller - Data Sheet. Microchip Technology Incorporated, 2016.
3. Petrov A. a. Computer security. Cryptographic methods of protection. Book on Demand Ltd., 2018. 450 p.

УДК 621.391:004.9 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.174

РОЗРОБКА ДОДАТКУ ДЛЯ АНАЛІЗУ МЕРЕЖНОГО ТРАФІКУ

Чистюк Д.С.
Науковий керівник – к.т.н., доц. Чеботарьова Д.В.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
e-mail: dmytro.chystiuk@nure.ua

The purpose of the work is to formulate the concept of network traffic analysis, to explore methods of analyzing corporate traffic, working principle of the network traffic analyzer and its advantages. As a result, own traffic analysis application was developed. This application provides real-time visualization of network traffic activity and creation of customized reports in different types of content such as text, graphics, and graphs. These tools will enable many network professionals to create secure, efficient, well designed and performance optimized networks.

У сучасну цифрову епоху мережі відіграють вирішальну роль у функціонуванні організацій будь-якого розміру та типу. Для ефективного керування мережею велике значення має моніторинг. Він є джерелом інформації про функціонування корпоративних додатків, що враховується при розподілі коштів, планування обчислень потужності, виявленні та локалізації відмов, рішень питань безпеки. Відстежуючи мережний трафік на предмет незвичайної активності, спеціалісти з мережної безпеки можуть виявляти та попереджувати різні загрози.

Аналіз мережного трафіку – це процес аналізу активності та доступності мережі, для виявлення незвичайної поведінки об’єктів, яка може вказувати на зловмисну діяльність [1, 2]. Ця операція передбачає відстеження того, які та коли надходять дані у різні частини мережі. Загальні випадки його використання включають:

- збір даних про те, що відбувається в мережі в режимі реального часу та за попередні періоди;
- виявлення зловмисного програмного забезпечення;
- виявлення використання вразливих протоколів і шифрів;
- усунення несправностей повільної мережі;
- покращення внутрішньої видимості та усунення сліпих зон.

Впровадження рішень, які можуть безперервно відстежувати мережний трафік, дає уявлення, необхідні для оптимізації продуктивності мережі, мінімізації поверхні атак, підвищення безпеки та покращення керування ресурсами.

Метою доповіді є дослідження систем аналізу мережного трафіку та розробка власного додатку для аналізу мережного трафіку.

Сьогодні популярними інструментами для аналізу мережних протоколів є аналізатори протоколів (protocol analyzer) та сніфери (sniffer).

Такі пристрої існують в апаратному та програмному вигляді. Аналізатор протоколів на основі апаратного забезпечення використовується в роботі зі складними інтерфейсами протоколів, в той час як програмний аналізатор є менш потужним але простішим та дешевшим в використанні.

Лідером ринку серед додатків для аналізу мережного трафіку є Wireshark [3]. Wireshark – це інструмент із відкритим кодом для моніторинга мережного трафіку та аналізу пакетів, який дає змогу адміністраторам мережі проводити глибокий аналіз трафіку, що переміщується через мережу. Програмне забезпечення дає можливість вивчення деталей трафіку на різних рівнях, починаючи від інформації на рівні підключення до бітів, які складають один пакет. Перехоплення пакетів може надати мережному адміністратору інформацію про окремі пакети, наприклад час передачі, джерело, призначення, тип протоколу та дані заголовка.

В роботі проведено детальний огляд найважливіших функцій Wireshark та виконано розробку власної реалізації програми аналізатора мережного трафіку. Корисна функція, яка надається операторам мого додатку – це наглядне відображення мережних інтерфейсів. Ця функція реалізована для комфортного, зрозумілого, легкого отримання інформації про мережні пристрої. Користувачам більше не треба шукати в параметрах комп'ютера ці відомості, вистачить зайти на сторінку відображення мережних інтерфейсів, де будуть представлені картки з існуючими мережними інтерфейсами, а також їхні короткі описи.

Розроблений додаток своїм функціоналом задовольнить користувачів та за допомогою реалізації різноманітних можливостей, таких як перехоплення мережного трафіку, побудова графіків навантаження мережі, графу ip-адрес, відображення деталей підключених мережевих пристроїв, він може стати конкуренто-спроможним вже на першій ітерації програмного продукту. Варто зазначити, що граф IP-адрес та графік залежності кількості пакетів до IP-адрес не реалізовані в програмному додатку Wireshark, а отже є унікальними функціями розробленого додатку.

Список використаних джерел:

1. Ashtari H. What Is Network Behavior Analysis? Definition, Importance, and Best Practices [Електронний ресурс] / Hossein Ashtari // Spiceworks. – 2022. – Режим доступу до ресурсу: https://www.spiceworks.com/tech/networking/articles/network-behavior-analysis/.

2. Janani A. K. Network Traffic Analysis [Електронний ресурс] / A. K. Janani // Atatus. – 2022. – Режим доступу до ресурсу: https://www.atatus.com/glossary/network-traffic-analysis/.

3. About Wireshark [Електронний ресурс] // Wireshark Foundation. – 2024. – Режим доступу до ресурсу: https://www.wireshark.org/about.html.

УДК 004.89:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.176

ПЕРСОНАЛЬНИЙ АСИСТЕНТ МЕРЕЖНОГО ІНЖЕНЕРА ЯК ІНСТРУМЕНТ ПІДВИЩЕННЯ ЯКОСТІ ТЕЛЕКОМУНІКАЦІЙНИХ ПОСЛУГ

Чечоткін Є.Є.
Науковий керівник – к.т.н., доцент Костромицький А.І.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: yevhenii.chechotkin@nure.ua

This article assesses the potential of artificial intelligence in the telecommunications industry and identifies potential areas of its application to improve the efficiency of network engineers and the quality of telecommunications services. The paper also describes the functional capabilities of a personal assistant, such as the generation of necessary and relevant information with subsequent self-analysis and learning. For specialists in technical fields, this is an opportunity to use an unlimited information resource that will be designed to meet individual information needs. At the current stage, the topic has a high potential and can be implemented in many industries.

Щодня у світі інфокомунікацій з’являються нові можливості та ідеї покращення усіх галузей людського життя. Але насамперед треба оцінити можливість впровадження штучного інтеллекту (ШІ) не тільки в концепції інтелектуальної машини для відповідей, а й як повноцінного асистента мережевого адміністратора або архітектора. Проблемою щодо застосування штучного інтелекту фахівцями телекомунікаційного спрямування стає неможливість використання специфічних математичних розрахунків, плутанина у вимогах і нормах, необхідних для розгортання та налаштування мережі локального чи регіонального типу, великий перелік діючих застарілих та сучасних мережних технологій різного покоління, які повинні працювати узгоджено в межах единої інфокомунікаційної інфраструктури. Тим самим в подальшому інженер, навіть з великим досвідом, стикається з проблемою прогнозування розвитку мережі і недостатньою відмовостійкістю, що у свою чергу призводить до фінансових і часових витрат для перебудови вже існуючої архітектури.

Суттєво підвищити ефективність роботи мережного інженера можуть технології ШІ, зокрема, пропонується ідея створення персонального помічника (The Perfect AI for Productivity, Recollection, and Planning - ваш ідеальний штучний інтелект для продуктивності, пам’яті та планування) у галузі інформаційно-мережної інженерії.

Основою для розгортання можуть бути різні відкриті чи пропрієтарні платформи, технології чи моделі. Порівняння ефективності різних варіантів реалізації такого помічника може бути наступним етапом

досліджень, а наразі за основу цій роботі візьмемо MindOS - платформу яка в першу чергу пропонує автоматизацію робочих процесів та може виконувати таке функціональне навантаження як: ведення нотаток, стенографування зустрічей або фіксації всіх ваших важливих робочих документів, може організувати будь-які зображення або текст у своїй цифровій пам'яті для подальшого використання; крім того помічник може полегшити та пришвидшити процеси які потребують постійного та своєчасного оновлення, таких як: планування та розширення мережі, що може включати навички персонального-асистента з аналізу ринку мережевого обладнання та пошуку актуальних рішень і подальше впровадження нових технологій, моніторинг та ведення документації. Платформа MindOS доступна через браузер та для встановлення на персональний комп'ютер з операційною системою Microsoft Windows.

Для того щоб створити якісного помічника, його потрібно «познайомити» з відповідною технічною літературою, внести лінки та посилання на веб-сайти. Наразі база даних має обмеження за розміром і кількістю посилань на електронні ресурси але навіть у такому вигляді її вистачає для підтримки наявної інформації в актуальному стані та можливості для подальшої актуалізації інфраструктури. Також передбачена можливість інтегрування різних платформ та сервісів за допомогою API-з'єднань, за допомогою яких функціональність стане масштабованішою та еластичнішою у використанні.

Якщо на загальновідомі теоретичні питання можна швидко отримати відповідь від стандартних моделей типу ChatGPT без необхідності попереднього налаштування то на специфічні питання навченні ШІ помічники повинні давати відповіді які більше задовольнять мережного інженера в нашому випадку.

Таким чином, наразі з'являється можливість забезпечення адміністраторів інформаційно-комунікаційних мереж особистим віртуальним помічником, тим самим зменшити безпосередньо навантаження на людину при виконанні повсякденних завдань, прибрати ризики "людського фактору", зробити легшим процес адаптації нових співробітників, а у підсумку отримати збільшену продуктивність і ефективність роботи яка виконується.

Список використаних джерел:

1. Jakob Mökander1 · Ralph Schroeder AI and social theory AI & SOCIETY (2022) 37:1337–1351 https://doi.org/10.1007/s00146-021-01222-z
2. Artificial Intelligence: Foundations of Computational Agents" by David L. Poole and Alan K. Mackworth
3.Maria Virvou Department of Informatics, University of Piraeus, Piraeus, 2022 13th International Conference on Information, Intelligence, Systems & Applications (IISA) Greece DOI: 10.1109/IISA56318.2022.9904422

УДК 621.396:004.056.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.178

КОНЦЕПТУАЛЬНІ ЗАСАДИ МЕТОДУ ЗМІШУВАННЯ БІТ ДЛЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ШИФРУВАННЯ PE-ФАЙЛІВ НА БАЗІ БЛОКОВИХ АЛГОРИТМІВ

Шавлак А.В., Чалий Д.В., Бондаренко Г.Р.
Науковий керівник – к.т.н., с.н.с. Калюжний М.М.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: artem.shavlak@nure.ua,e-mail:dmytro.chalyi.@nure.ua,
e-mail: hryhorii.bondarenko@nure.ua

Block encryption algorithms provide high encryption speed and are relatively simple to implement. However, under certain conditions, a decrease in stability may be observed. For example, for DES in ECB mode, in the case of encryption of EXE files and files of other types, the first block of which is the header of this file, since knowing its content, it is possible to significantly reduce the time of breaking the cipher itself. To avoid such situations, it is suggested to perform a bit-mixing operation on the original message to be encrypted. Such an operation destroys semantic features in the file being encrypted, thereby creating conditions for increasing the cryptographic stability of the cipher.

Криптосистема DES, завдяки архітектурним особливостям, забезпечує високу швидкість обробки та рівень стійкості, достатній для шифрування конфіденційних даних, що не належать категорії секретних. При цьому, найвища швидкодія забезпечується у режимі ECB (Electronic Codebook).

Разом з тим, у випадку шифрування файлів деяких типів (dll, exe, drv, sys, mui тощо), що наслідують формат PE, застосування DES-ECB може вести до швидкого розкриття шифру зловмисником. Це зумовлено тим, що, шифрування DES здійснюється на рівні блоків 64 біта. При цьому, у режимі ECB усі блоки, виокремлені у межах файлу, шифруються незалежно один від одного з єдиним ключем, тоді як заголовок PE-файлу має також довжину 64 біта. Ураховуючи те, що зміст заголовку є, по-перше, стандартним, а, по-друге, чітко виокремлюється з довільного потоку даних завдяки характерним сигнатурам (зокрема, 0x5A4D та 0x3C), завдання реконструкції вихідного файлу стає тривіальним.

Для усунення зазначеного недоліку пропонується застосувати метод попереднього змішування біт PE-файлу, тим самим руйнуючи семантичні ознаки заголовку. При цьому, така процедура має відповідати наступним вимогам:

- проста алгоритмічна та математична реалізація, що дозволяє виконувати шифрування у режимі реального часу, не вносячи помітну затримку;
- порядок змішування біт повинен бути динамічним;

- процедуру має бути побудовано у вигляді окремого модулю, що передує шифруванню, тим самим не вносячи змін у базовий алгоритм.

Щоб виконати умову щодо динамічного порядку змішування, для файлу пропонується попередньо обчислити ряд інформативних ознак $q_1 \dots q_n$, які далі буде використано у ролі опцій для побудови процесу. При цьому, якщо такі інформативні ознаки обчислено на базі змісту файлу, їх подальше використання, по-перше, створює умови для можливості побудови унікального сценарію змішування, а по-друге – користувач буде позбавлений необхідності самостійно встановлювати параметри процедури.

Розглянемо сценарій реалізації процедури змішування, побудований на базі двох технологічних етапів, а саме:

- циклічного бітового зсуву даних заголовку та службових полів на рівні байт позиції заголовків та службових полів;
- виконання байтового зсуву на рівні усього файлу для зміни позиції службових компонент та заголовку.

У ході першого технологічного етапу кожен байт b заголовку та службових полів, загальною кількістю n, спочатку конкатенують між собою на рівні біт, тим самим утворюючи суцільний масив біт B. Після зазначеної процедури у межах масиву B виконується операція sh циклічного зсуву на ξ позицій, за результатами чого утворюється змінений масив B':

$$B' = sh(d; \xi; B; n), \quad (1)$$

$$n > 8,$$

де n - кількість байт, включених у множину B, що визначається на базі раніше розрахованої інформативної ознаки у загальному вигляді, як $n = \phi(q_1)$; вимога щодо величини масиву B зумовлюється необхідністю внесення невизначеності у структуру файлу ще до етапу шифрування;

d - напрямок зсуву, що визначається також на базі однієї з попередньо обчислених інформативних ознак як $d = f(q_2)$.

Для обчислення кроку ξ циклічного бітового зсуву, так само, як і для визначення напрямку d, тут використовується будь-яка інша з виявлених інформативних ознак у загальному вигляді $\xi = \varphi(q_3)$.

У свою чергу, зсув змісту файлу та службових даних на рівні байт для зміни стартової позиції Φ першого біту PE-заголовку може виконуватися аналогічно принципу, зазначеному виразом (1), а саме:

$$\Phi' = sh(\bar{d}; \bar{\xi}; \Phi), \quad (2)$$

де Φ' - позиція першого біту PE-заголовку після виконання зсуву;

$\bar{\xi}$ - крок байтового зсуву, що обчислюється аналогічно ξ, проте для його розрахунку може використовуватися інша інформативна ознака та функціональне перетворення;

$\bar{d}$ - напрямок байтового зсуву, який знаходиться за тим же принципом, як і напрямок d, але, у загальному випадку, на базі іншої інформаційної ознаки і функціонального перетворення.

Отже, побітовий зсув на рівні PE-заголовку спочатку порушує його структуру, а також структуру деякої кількості службових полів, тим самим маскуючи характерні семантичні ознаки. У свою чергу, циклічний байтовий зсув на другому етапі процесу змішування змінює позицію вже модифікованої ділянки файлу, де міститься у т.ч. заголовок.

Таким чином, сформовано концептуальні засади методу попереднього змішування біт файлів PE-архітектури, що забезпечує подальше ефективне його шифрування на базі криптографічної системи DES у режимі ECB.

У рамках методу передбачається використання системи інформаційних ознак, що розраховується для кожного файлу, який підлягає шифруванню, окремо, виходячи з особливостей його змісту. Такі інформаційні ознаки виступають у ролі параметрів реалізації процесу змішування. Це, у свою чергу, дозволяє забезпечити унікальний перебіг процесу, а також повністю його автоматизувати.

Реалізація методу змішування біт відповідно до запропонованої концепції дозволяє протидіяти криптоаналітичним атакам - таким, як атака за відомим відкритим повідомленням, та подібним їй. Це є актуальним не лише для DES-ECB, але і для інших симетричних шифросистем з розміром блоку, рівним 64 біта.

У рамках подальшого розвитку концепції передбачається:

- формування математичного апарату для розрахунку системи інформативних ознак файлу;
- проведення експериментального дослідження для виявлення ефективного діапазону розмірів файлів, відносно якого може бути використано створюваний метод.

Список використаних джерел:

1. Portable Executable // Iana URL https://www.iana.org/assignments/media-types/application/vnd.microsoft.portable-executable (дата звернення: 05.03.2024)

2. Special Feature Exhaustive Cryptanalysis of the NBS Data Encryption Standard // Computer URL https://www.computer.org/csdl/magazine/co/1977/06/01646525/13rRUwInvDu (дата звернення: 05.03.2024)

3. Block Ciphers // Uwaterloo URL https://cacr.uwaterloo.ca/hac/about/chap7.pdf (дата звернення: 05.03.2024)

УДК 004.773.3:004.056 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.181

НАЙПОШИРЕНІШІ ЗАГРОЗИ БЕЗПЕЦІ ЕЛЕКТРОННІЙ ПОШТІ ТА МЕТОДИ ЗАХИСТУ ВІД НИХ

Шевчук В.В.
Науковий керівник – к.т.н., доц. Золотарьов В.А.
Харківський національний університет радіоелектроніки, каф. ІМІ
м. Харків, Україна
e-mail: vladyslav.shevchuk@nure.ua

The most common 2023 attacks are considered and effective methods of protection against them are proposed. Phishing, social engineering, virus attacks, and other forms of cybercrime often attempt to use mail to gain unauthorized access to sensitive information or cause other harmful effects. Therefore, there is a need to effectively protect users and organizations from cyber threats that can lead to large financial losses, violate privacy, and increase malware.

Найпоширенішими атаками на електронну пошту у 2023 р. стали: фішинг, спуфінг, цільовий фішинг, програми-вимагачі, віруси/шкідливе програмне забезпечення та спам. Порівняння вдалих атак у 2023 р. і 2019 р. наведено на рисунку 1.

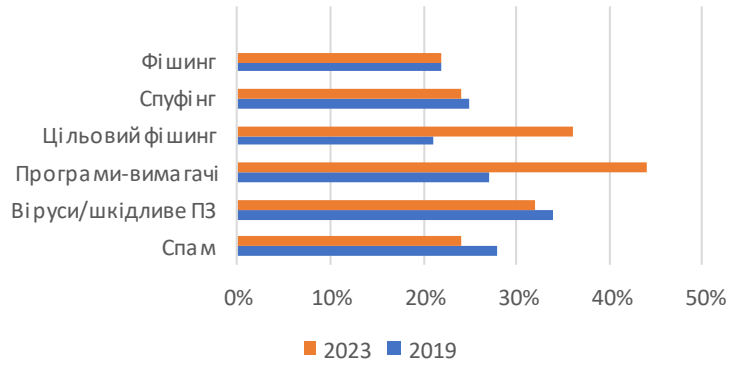


Рисунок 1 – Діаграма вдалих атак на електронну пошту

–Фішинг (Phishing) – вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних. Сценарій такої атаки заснований на незнанні користувачами основ мережевої безпеки, та перенаправлення на фішингові сайти або ураження пристрою програмою-вимагачем, або шифрувальником.

–Спуфінг (spoofing) – це атака, під час якої надають неправдиві дані, аби здаватися справжніми користувачами, наприклад, надсилання листа з акаунта, який має вигляд офіційної банківської email-адреси.

–Цільовий фішинг (Spear phishing) – вид фішингової атаки електронної пошти, спрямована на конкретну організацію чи особу з метою отримання несанкціонованого доступу до конфіденційної інформації.

–Програми-вимагачі (Ransomware) – це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер. Такий тип програм поділяються на три типи: шифрування даних, блокування системи, та блокування або перешкода роботи в браузері.

–Віруси/шкідливе ПЗ (malware) – програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до приватних комп'ютерних систем, частіше проявлятися у вигляді коду, скрипту, активного контенту або іншого програмного забезпечення.

–Спам (Spam) – це небажані повідомлення у будь-якій формі, надіслані у великій кількості. Найчастіше спам надсилається у формі комерційних електронних листів на велику кількість адрес, а також через миттєві та текстові повідомлення (SMS), соціальні медіа або голосову пошту.

Аналізуючи атаки, загрози та вразливі місця в системах захисту електронної пошти, можна розробити ефективні методи захисту від цих атак. Методи використовуються на рівні користувачів послуг та на рівні постачальників послуг електронної пошти.

Головний аспект захисту починається з усвідомлення користувачами політики безпеки та використання ефективних методів її реалізації. Це застосування надійних паролів і періодична їхня зміна, заборона використання однакових паролів на різних сервісах. Застосування багатофакторної аутентифікації значно зменшує ризик несанкціонованого доступу до електронної пошти. Слід навчити співробітників розпізнавати фішингові атаки, усвідомлювати можливі ризики та додержуватися правил безпеки на їхньому рівні. Такі організаційні заходи дозволяють уникнути чисельних атак на електрону пошту.

На рівні постачальників послуг одним з ефективним методом захисту являється застосування різних методів автентифікації. Існує три типи автентифікації електронної пошти, які можна налаштувати під потреби користувача:

–Sender Policy Framework (SPF) – це технічний стандарт і метод автентифікації електронної пошти, який допомагає захистити відправників і одержувачів електронної пошти від спаму, підробки повідомлень та фішингу. SPF встановлює метод отримання поштових серверів для перевірки того, що вхідна пошта з домену була надіслана з хоста, авторизованого адміністраторами цього домену.

–DKIM (DomainKeys Identified Mail) – це протокол, який дозволяє організації взяти на себе відповідальність за передачу повідомлення, підписавши його таким чином, щоб постачальники поштових скриньок

могли перевірити. Перевірка запису DKIM стала можливою за допомогою криптографічної автентифікації.

–DMARC Domain-based Message Authentication, Reporting, and Conformance) – технологія, що дозволяє отримувачу електронної пошти перевірити справжність її відправника. Визначає масштабований механізм визначення політик та налаштувань для валідації, розташування, та журналювання електронних повідомлень на стороні відправника, якими може скористатись отримувач для поліпшення оброблення електронних листів.

Важливим методом захисту є резервне копіювання всіх даних, яке унеможливіть їхню втрату або видалення. Завжди потрібно створювати резервні копії всіх важливих листів. Для цього можна вибрати зовнішній жорсткий диск, USB-накопичувач або завантаження даних в хмарне сховище. Слід пам’ятати, що фізичний зовнішній жорсткий диск або USB-накопичувач можна загубити або пошкодити, а при зберіганні у хмарі хакери також мають можливість розкрити конфіденційні дані.

Застосування проксі-серверів забезпечує додатковий захист електронної пошти, дає змогу зберігати конфіденційність інформації про свою геолокацію, надсилати листи і проводити онлайн-дослідження, не розкриваючи власний IP-адрес.

Використання шифрування дає ефективний захист від перехоплення повідомлень. Для шифрування повідомлень використовують захищені протоколи TLS (Transport Layer Security) або SSL (Secure Sockets Layer), або метод шифрування End-to-end encryption (E2EE), який забезпечує конфіденційність повідомлень від усіх, у тому числі від служби обміну повідомленнями. При використанні E2EE, повідомлення з’являється лише в розшифрованому вигляді для особи, яка надсилає повідомлення, і для особи, яка отримує повідомлення.

Важливим аспектом безпеки є ефективний моніторинг та виявлення вразливостей в системі захисту. Для цього застосовується система виявлення вторгнень (IDS), яка дозволяє вчасно розпізнавати та реагувати на підозрілу активність, чи спроби отримати несанкціонований доступ до поштових серверів. Слід застосувати журнал для реєстрації та аналізу інцидентів , таких як невдалі спроби входу, чи надмірне споживання тих або інших ресурсів, обмежити надсилання великої кількості повідомлень.

Список використаних джерел:

1. Тенденції безпеки електронної пошти 2023 [Електронний ресурс] // Softprom. – 2023. – Режим доступу до ресурсу: https://softprom.com/ua /tendentsiyi-bezpeki-elektronnoyi-poshti-2023.

2. Zinkovska O. Надійні рішення для захисту електронної пошти: 12 найкращих практик [Електронний ресурс] / Olena Zinkovska // stripo.email. – 2023. – Режим доступу до ресурсу: https://stripo.email/ua/blog/top-email-security-practices/.

УДК 004.032:621.391 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.184

АНАЛІЗ ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ AD-HOC МЕРЕЖ ТА МОЖЛИВОСТІ ПІДВИЩЕННЯ ЇХ ПРОДУКТИВНОСТІ

Широкий Є.В.
Науковий керівник – к.т.н., доц. каф. ІМІ, Харченко Н.А.
Харківський національний університет радіоелектроніки, каф. ІМІ,
м. Харків, Україна
e-mail: yevhen.shyrokyi@nure.ua.

Modern wireless networks are quite complex multi-level systems. Increasing the complexity of the wireless network structure leads to an increase in the volume of service information, especially routing protocols affect this, which in turn reduces the share of useful traffic and, accordingly, the efficiency of such networks will also decrease. The paper presents a study of multipath routing protocols used in Ad-hoc networks, based on several indicators that affect the reliability of routing. Their advantages and disadvantages are identified, the direction of further research is proposed to improve the quality of the functioning of protocols in wireless networks.

Mesh-мережі - перспективний клас широкосмугових бездротових мереж передачі мультимедійної інформації, який на сьогоднішній день знаходить все більш широке застосування в різних областях інфокомунікаційного простору.

Сучасні бездротові інформаційно-комунікаційні мережі представляють собою досить складні багаторівневі системи. Тому їх ефективність залежить від багатьох параметрів: показників якості обслуговування, надійності, продуктивності та ін.. Також значення цих показників може нерівномірно змінюватися залежно від миттєвих значень завантаженості мережі, що призводить до нестабільності в наданні певного рівня QoS.

Також одним з основних недоліків в Mesh-мережі є затримка при надсиланні інформації в мережі. Головна проблема тут в тому, що при транспортуванні даних завжди використовуються проміжні пункти, при цьому їх кількість може постійно змінюватися за рахунок складності алгоритмів маршрутизації [1].

Постійний розвиток телекомунікаційних технологій, та потреба у підвищеннях швидкостей при передачі інформації призводить до актуалізації питання управління трафіком у мережах. Часто цей процес зводиться до реалізації постійного моніторингу як стану окремих вузлів, так і їх взаємодії по каналам зв’язку. При цьому треба враховувати, що пропускна здатність бездротової мережі, на відміну від проводової, обмежується максимальною ефективністю використовуваного логічного каналу. Частина цієї пропускної здатності використовується для передачі даних, решта – для службового трафіка, що містить в собі досить велику

кількість спеціальних пакетів від різних протоколів. Підвищення складності структури бездротової мережі призводить до зростання об’єму службової інформації, особливо на це впливають протоколи маршрутизації, а це в свою чергу зменшує долю корисного трафіка і відповідно ефективність таких мереж теж буде знижуватись. Відповідно, завдання зменшення службового трафіка є актуальним та становить науковий та практичний інтерес.

На сьогоднішній день в Ad-hoc мережах використовуються два види маршрутизації: одношляхова та багатошляхова. Особливістю Ad-hoc є самоорганізація, тобто кожен вузол, що працює в ній може грати роль як передавача своєї інформації, так і ретранслятора загального потоку даних. Відповідно в таких мережах завжди існує декілька шляхів між парою вузлів. Сенс багатошляхової маршрутизації полягає в тому, щоб надати вузлу можливість вибору одного оптимального маршруту із усіх можливих варіантів. Використання протоколів багатошляхової маршрутизації є більш оптимальним з точки зору забезпечення балансування навантаження у мережі та захисту від збоїв при передачі трафіку. Такий підхід дозволяє оптимально використовувати ємність каналу зв'язку і підвищити загальну пропускну здатність. Додатково забезпечується відмовостійкість мережі і надійність передачі [2].

Протягом останніх років було запропоновано і розроблено велику кількість багатошляхових протоколів і методів маршрутизації для Ad-hoc мереж. Існуючі на даний момент протоколи прийнято класифікувати за принципом роботи [2-3]. Виділяють три базові групи протоколів: проактивні, реактивні та гібридні. Кожен клас протоколів має свої переваги і недоліки при використанні в бездротових Ad-hoc мережах. При проактивній маршрутизації (протоколи OSPF, OLSR, TBRPF, FSR і ін.) адресація досить проста в реалізації, але вона має проблеми з масштабуванням у великих мережах. Реактивні протоколи (AODV-BR, AOMDV, TORA, ROAM, MDSR, SMR) також мають проблеми з масштабуванням. Для підвищення показника масштабування, необхідно підвищити контроль при визначенні та обслуговуванні маршруту. Це може бути досягнуто шляхом локалізації поширення керуючого повідомлення в певному сегменті, де знаходиться пункт призначення [2]. Гібридні протоколи маршрутизації (SPREAD, ZRP, NAMP, E-NAMP, HSPREAD) є протоколами що створені на основі двох попередніх видів. Як правило, вони розбивають мережу на окремі логічні підмережі (зони), всередині яких функціонує проактивний протокол, а взаємодія між цими підмережами здійснюється реактивними методами. Перевага цих протоколів полягає в тому, що вони підтримують сильний мережевий зв'язок (проактивно) в зонах маршрутизації при визначенні віддаленого маршруту (за межами зони маршрутизації) швидше, ніж інші, а також вони можуть взаємодіяти з іншими протоколами маршрутизації для підвищення

продуктивності і надійності [2]. Недоліком гібридних протоколів є їхня складність реалізації та збільшення часу затримки сигналів при переході між підмережами.

Проблему роботи гібридних протоколів маршрутизації можна вирішити завдяки використанню структурного підходу, що включатиме в себе кластерний аналіз та візуалізацію даних. Алгоритми кластерізації дозволяють покращити показники затримки, масштабованості та сукупні витрати енергії при обробці пакетів у проміжних пунктах. Щоб підвищити ефективність роботи протоколів маршрутизації також можна застосувати обмеження на кількість точок доступу в одному кластері, що полегшить їх взаємодію між собою.

Список використаних джерел:

1. ВСЕУКРАЇНСЬКА НАУКОВО-ПРАКТИЧНА КОНФЕРЕНЦІЯ «TELECOMMUNICATION: PROBLEMS AND INNOVATION 2020. URL: http://www.dut.edu.ua/uploads/p_1739_44635808.pdf – Дата звернення 05.02.2024.

2. Пількевич, І. А., Бойченко, О. С., & Гуменюк, І. В. (2019). Метод децентралізованого управління мережевими ресурсами інформаційно-комунікаційних мереж. *Технічна інженерія*, (2(84), 100–108. https://doi.org/10.26642/ten-2019-2(84)-100-108

3. Traffic engineering in software-defined networking: Measurement and management / *Zhaogang Shu, Jiafu Wan, Jiaxiang Lin and other* // Access IEEE. – 2016. – Vol. 4. – P. 3246–3256.

4. Аналіз ефективності методів маршрутизації на основі OLSR і AODV з балансуванням навантаження трафіку мережі Wi-Fi URL: https://openarchive.nure.ua/bitstream/document/12709/1/Kry2016predt.pdf – Дата звернення 13.02.2024

УДК 004.934 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.187

ОЦІНКА ЯКОСТІ РОЗПІЗНАВАННЯ ГОЛОСОВИХ КОМАНД ЛЮДИНИ

Шишаков Є.В.
Науковий керівник – доц., к.т.н. Омельченко С.В.
Харківський національний університет радіоелектроніки, каф. IMI,
м. Харків, Україна
E-mail: yevhenii.shyshakov@nure.ua.

This work is devoted to assessing the field of artificial neural networks has grown rapidly in recent years. This has been accompanied by an insurgence of work in speech recognition. Most speech recognition research has centered on stochastic models, in particular the use of hidden Markov models (HMMs). Alternate techniques have focused on applying neural networks to classify speech signals. The inspiration for using neural networks as a classifier stems from the fact that neural networks within the human brain are used for speech recognition. This analogy unfortunately falls short of being close to an actual model of the brain, but the modeling mechanism and the training procedures allow the possiblility of using a neural network as a stochastic model that can be discrimitively trained.

Автоматичне розпізнавання мовлення (ASR), яке спрямоване на природну взаємодію між людиною та машиною, було предметом інтенсивних досліджень протягом десятиліть. Багато основних технологій, таких як моделі суміші Гауса (GMM), приховані моделі Маркова (HMM), кепстральні коефіцієнти мел-частоти (MFCC) та їх похідні, моделі мови ngram (LM), дискримінаційне навчання та різні методи адаптації, були розроблені разом До речі, переважно до нового тисячоліття. Ці методи значно просунули сучасний рівень ASR та суміжних галузей. Порівняно з цими попередніми досягненнями, прогрес у дослідженні та застосуванні ASR у десятиліття до 2010 року [1] був відносно повільним і менш захоплюючим, хоча важливі методи, такі як розрізнювальна підготовка послідовності GMM–HMM, у цей період добре працювали в практичних системах.

Однак за останні кілька років ми спостерігаємо новий сплеск інтересу до ASR. На нашу думку, ця зміна була спричинена підвищеними вимогами до ASR у мобільних пристроях і успіхом нових мовних програм у мобільному світі, таких як голосовий пошук (VS), диктування коротких повідомлень (SMD) і віртуальні мовні помічники (наприклад, Siri від Apple, Google Now і Cortana від Microsoft). Не менш важливою є розробка методів глибокого навчання [2][4][5] в системі безперервного розпізнавання мовлення великого словника (LVCSR), що базується на великих даних і значно покращує обчислювальну здатність. Поєднання набору методів глибокого навчання призвело до зниження частоти

помилок більш ніж на 1/3 у порівнянні зі звичайною сучасною структурою GMM–HMM для багатьох реальних завдань LVCSR і допомогло подолати поріг прийняття для багатьох користувачів реального світу. Наприклад, точність слова в англійській мові або точність символів в китайській мові в більшості систем SMD зараз перевищує 90 %, а в деяких системах навіть 95 % [3].

У розпізнаванні мовлення один із найпоширеніших генеративних підходів до навчання базується на прихованих моделях Маркова на основі моделі суміші Гауса, або GMM-HMM [1]. Як обговорювалося раніше, GMM-HMM — це статистична модель, яка описує два залежні випадкові процеси, спостережуваний процес і прихований процес Маркова. Передбачається, що послідовність спостереження генерується кожним прихованим станом відповідно до розподілу суміші Гауса. GMM-HMM параметризується вектором попередніх ймовірностей стану, матрицею ймовірностей переходу стану та набором залежних від стану параметрів у моделях суміші Гаусса. З точки зору моделювання мовлення, стан у GMM-HMM зазвичай асоціюється з підсегментом телефону в мовленні [3].

Одним з важливих нововведень у використанні HMM для розпізнавання мовлення є введення контекстно-залежних станів, мотивоване бажанням зменшити варіабельність вихідних векторів ознак мови, пов’язаних з кожним станом, загальною стратегією для «детального» генеративного моделювання. Наслідком використання залежності від контексту є значне розширення простору станів HMM, яким, на щастя, можна керувати методами регулярізації, такими як зв’язування станів.

Виявляється, така залежність від контексту також відіграє вирішальну роль у нещодавньому прогресі розпізнавання мовлення в області глибокого навчання на основі дискримінації.

Запровадження HMM та відповідних статистичних методів для розпізнавання мовлення в середині 1970-х років можна вважати найбільш значущою зміною парадигми в галузі, як обговорювалося та аналізувалося в. Однією з головних причин такого раннього успіху є високоефективний алгоритм EM. Цей метод максимальної правдоподібності, який часто називають алгоритмом Баума-Велча, був основним способом навчання систем розпізнавання мовлення на основі HMM до 2002 року, і досі є одним із основних кроків (серед багатьох) у навчанні цих систем сьогодні. Цікаво відзначити, що алгоритм Баума-Велча служить одним з головних мотивуючих прикладів для подальшого розвитку більш загального алгоритму EM.

Використання генеративної моделі HMM для представлення (порізно стаціонарного) динамічного шаблону мовлення та використання EM-алгоритму для навчання пов’язаних параметрів HMM є одним з найвидатніших і успішних прикладів генеративного навчання в розпізнаванні мовлення [1]. Цей успіх був міцно закріплений мовленнєвою

спільнотою та широко поширений на машинне навчання та пов’язані спільноти. Насправді HMM став стандартним інструментом не лише для розпізнавання мовлення, але й для машинного навчання, а також у суміжних областях, таких як біоінформатика та обробка природної мови. Для багатьох дослідників машинного навчання та розпізнавання мовлення успіх HMM у розпізнаванні мовлення є дещо дивним через добре відомі недоліки HMM у моделюванні динаміки мовлення.

Список використаних джерел:

1. Automatic Speech and Speaker Recognition: Large Margin and Kernel Methods, by Joseph Keshet, Samy Bengio (January 2009)
2. Speech Recognition Over Digital Channels: Robustness and Standards, by Antonio Peinado and Jose Segura (September 2006)
3. Speech Processing — A Dynamic and Optimization-Oriented Approach, by Li Deng and Doug O’Shaughnessy (June 2003)
4. Digital Speech Processing: Synthesis, and Recognition, Second Edition, by Sadaoki Furui (June 2001)
5. Speech Communications: Human and Machine, Second Edition, by Douglas O’Shaughnessy (June 2000)

ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ, МЕТРОЛОГІЧНЕ ЗАБЕЗПЕЧЕННЯ, СТАНДАРТИЗАЦІЯ І СЕРТИФІКАЦІЯ

УДК 004.738.5:339

РЕАЛІЗАЦІЯ ФУНКЦІЙ CRM-СИСТЕМИ З ПРОДАЖУ КНИГ ЗА ДОПОМОГОЮ МЕТОДІВ DATA MINING

Бараніченко Ю.А.
Харківський національний університет радіоелектроніки, каф. СТ
м. Харків, Україна
email: yuliia.baranichenko@nure.ua.

This work is devoted to the development of a CRM system for the sale of books. For this, an algorithm has been developed to provide users with recommendations based on their past purchases. When analyzing purchases, their price range is also taken into account in order to provide the client with the best offer.

CRM або Customer Relationship Management [1] – це рішення, призначене для управління роботою з наявними та потенційними замовниками. Такий програмний продукт об'єднує всі необхідні інструменти для роботи з клієнтами і збільшення продажів. Це системи управління відносинами з клієнтами, які допомагають автоматизувати процес продажів, сформувати клієнтську базу і побудувати правильну комунікацію «фірма – клієнт». CRM спрощує роботу бізнесу та робить її зручнішою, за рахунок виконання рутинних завдань.

Особливістю розробленої CRM-системи з продажу книг є таке: – для залучення клієнтів кожному покупцю пропонується картка яка дає процентну або фіксовану знижку на книги. Під час отримання карти, клієнт заповнює анкету, інформація якої дозволяє отримати персональні данні (П.І.Б., e-mail, номер телефону тощо). Данні анкет заносяться до системи, а клієнту надсилається пропозиція зареєструватися у системі, використовуючи свої данні;

– кожен клієнт може отримати рекомендації від магазину, що подаються на особистій веб-сторінці, або висилаються на е-пошту.

За алгоритмом роботи системи клієнту подається інформація за найпопулярнішими або новими книгами (акції). Після перегляду конкретної книги, якщо покупки не було, до особистих рекомендацій користувача додається інформація про книги, які аналогічне переглянутому за категорією, жанром, автором та ціновим діапазоном тощо.

У системі користувач може мати одну з трьох ролей «Гість» (незареєстрований користувач), «Клієнт» (зареєстрований користувач) та «Менеджер». Статус користувача визначається при вході у систему. «Гість» має доступ до бізнес-функцій з перегляду каталогу книг та взаємодії з кошиком. «Клієнт» має доступ до бізнес-функцій з оформлення замовлення та редагування особистого кабінету (редагування особистої інформації). «Менеджер» має доступ до бізнес-функцій зміни статусів замовлень.

У CRM-системі реалізовані наступні бізнес-функції для управління взаємодіями з клієнтами:

– збір і збереження даних перегляду каталогів та товарів, що роблять зареєстровані клієнти у випадку коли вони не купують книги. Ця інформація використовується для підготовки пропозицій (акцій) для покупки аналогічних (за категорією, жанром, автором тощо) книг, або пропозицій на покупку книг, що щойно поступило у продаж;

– для зареєстрованих клієнтів, що роблять регулярні покупки, створюються особисті пропозиції, які готуються на основі історії його замовлень (дати замовлень, категорії, тип, моделі взуття тощо). Ці дані система отримує за допомогою методів Data Minning [2].

Для керування пропозицією до клієнтів використовуються їх особисті дані – картки даних клієнтів. Картка даних формується за допомогою методів Data Minning і містить інформацію визначених асоціативних правил та класи клієнтів за весь період роботи з системою:

– вік (6 діапазонів);

– стать користувача;

– улюблений тип взуття або комбінації типів взуття (сезон, модель, виробник взуття);

– сума витрат (за сезон, місяць, квартал, півріччя, рік тощо);

– дати покупки взуття (сезон, місяць).

Для реалізації серверної частини CRM-системи обрано СУБД MySQL.

Сервер MySQL [3] забезпечує надійність, стабільність, стійкість, продуктивність та якісну сервісну підтримку. Також слід відмітити підтримку багатопоковості.

Для реалізації клієнтської частини використовувалися мови програмування Java та JavaScript, мова розмітки HTML та таблиці стилів CSS. Інтерфейс користувача, який відображається в браузері, створено за допомого HTML та удосконалено з використанням стилів CSS. За допомогою JavaScript-бібліотеки JQuery реалізовано асинхронні запиту до бекенду системи.

Бекенди системи реалізовано на Java за допомогою платформи Spring [4]. Запити обробляються у класах-сервлетах які використовують класи-сервіси для доступу до серверної частини. Для розробки було використано середу розробки IntelliJ IDEA з використанням JDK v.11.

Список використаних джерел:

1. Селіщев М. Що таке CRM: Навіщо потрібні, різновиди, як впровадити. URL: https://horoshop.ua/ua/blog/chto-takoe-crm/

2. Witten I. H., Ian H. Data mining: practical machine learning tools and techniques. Morgan Kaufmann series in data management systems. 2005.

3. Documentations for MySQL. URL: https://www.mysql.com/.

4. Mark Pollack, Oliver Gierke. Spring Data: Modern Data Access for Enterprise Java. O'Reilly. 2012.

УДК 504 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.193

МЕТРОЛОГІЧНІ АСПЕКТИ КОЛЬОРОМЕТРИЧНОГО МЕТОДУ МОНІТОРИНГУ ЕКОЛОГІЧНОГО СТАНУ ДОВКІЛЛЯ

Валюженич О.О.
Науковий керівник – к.т.н., проф. Ключник І.І.
Харківський національний університет радіоелектроніки,
каф. Інформаційно-вимірювальних технологій, м. Харків, Україна
e-mail: oleksandr.valiuzhenych@nure.ua

Today, our country is just beginning to calculate the environmental damage caused by Russia during the full-scale invasion. Considering the considerable significance of the issue of today's ecological state of the environment, it is expedient to carry out ecological monitoring in order to assess the quality of the environment from the point of view of the severity of the environmental damage caused.One of the possible methods of assessing the state of environmental quality can be a colorimetric method - an analysis method that uses a change in color to determine the concentration of certain chemicals in the environment.

На сьогоднішній день наша країна тільки починає підраховувати екологічні збитки завдані Росією у період повномасштабного вторгнення. Забруднення ґрунту та води, забруднення повітря, руйнування екосистем та біорізноманіття, обмеження доступу до природних ресурсів – вплив війни, що менш помітний на тлі людських та економічних втрат, але від того не менш значущий.

За даними Державної екологічної інспекції станом на січень 2023 року, за 11 місяців військової агресії РФ збитки для екології України складають вже понад 1 трильйон 743 мільярди гривень, або понад 47,6 мільярда доларів. І це тільки приблизні розрахунки, поки досі залишається окупованою частина українських територій [1].

Зважаючи на чималу значущість питання сьогоднішнього екологічного стану довкілля, доцільним є проведення екологічного моніторингу, з метою оцінки якості довкілля з точки зору важкості завданих екологічних збитків. Одним із можливих методів оцінки стану якості навколишнього середовища може стати кольорометричний метод – метод аналізу, який використовує зміну кольору для визначення концентрації певних хімічних речовин у навколишньому середовищі. Застосування цього методу стає можливим у зв’язку з тим, що багато хімічних сполук при реакції з певними реагентами змінюють свій колір в залежності від їх концентрації. Кольорометричний метод може бути використаний для оцінки якості води, ґрунту та повітря шляхом вимірювання концентрації забруднювачів, таких як важкі метали, фосфати, нітрати та інші хімічні речовини. Застосування кольорометричного методу включає збір проб навколишнього середовища, додавання специфічних реагентів, які викликають зміну кольору в присутності аналізованої речовини, та порівняння інтенсивності кольору з еталонною шкалою або

використання спеціалізованого обладнання для більш точного кількісного аналізу [2]. Метрологічні аспекти кольорометричного методу моніторингу екологічного стану довкілля особливо важливі при оцінці точності, відтворюваності та надійності вимірювань, що виконуються для аналізу забруднювачів та інших характеристик довкілля. Кольорометричний метод дозволяє визначати концентрації певних хімічних речовин у водних середовищах, повітрі або ґрунтах за характерними змінами кольору реагентів під впливом цих речовин. Для ефективного застосування цього методу важливо враховувати наступні метрологічні аспекти:

а) калібрування приладів – для точних вимірювань необхідно регулярно калібрувати кольорометричне обладнання, використовуючи стандартні розчини відомої концентрації;

б) визначення межі детекції та квантифікації – важливо встановити мінімальну концентрацію речовини, яку може виявити метод (межа детекції), та мінімальну концентрацію, при якій можливе надійне кількісне визначення (межа квантифікації);

в) валідація методу – процес валідації включає перевірку точності (правильності), прецизійності (відтворюваності), специфічності та робастності методу;

г) вибір реагентів та умов вимірювання – чутливість та специфічність кольорометричного методу залежать від вибору реагентів та умов проведення аналізу (температура, pH, час реакції тощо);

д) аналіз впливу матриці зразка – склад зразка може впливати на результати кольорометричного аналізу через наявність інших речовин, які можуть взаємодіяти з реагентами або впливати на колір розчину.

е) інтерпретація результатів – аналіз отриманих даних вимагає розуміння можливих джерел помилок та обмежень методу [3].

Використання кольорометричного методу моніторінгу довкілля доцільне для регіонів, які мають нафтопереробні підприємства, на території яких розміщені об’єкти хімічної промисловості, та для регіонів, що розміновуються. Підвищення метрологічних характеристик приладів, що працюють на основі кольорометричного методу, дозволить забезпечувати достатню достовірність отриманої інформації для прийнятя рішень щодо оцінки та управління екологічним станом довкілля.

Список використаних джерел:

1. Овсяний К. До і після. Наслідки повномасштабної війни для екології України. URL: https://www.radiosvoboda.org/a/skhemy-ekolohiya-viyna/32284610.html (Дата звернення: 18.02.2024).2. Чеботарьова І.Б. Основи метрології, стандартизації та управління якістю: навч. посібник. Харків: ХНУРЕ. 2023. 112 с. 3. МЕТОДИ ВИМІРЮВАННЯ ПАРАМЕТРІВ НАВКОЛИШНЬОГО СЕРЕДОВИЩА: кол. моногр. Сєвєродонецьк, 2019, 166 с.

УДК 629.3.07

УДК 629.3.07

АНАЛІЗ ОБОВ'ЯЗКОВОГО ТЕХНІЧНОГО КОНТРОЛЮ СТАНУ КОЛІСНИХ ТРАНСПОРТНИХ ЗАСОБІВ В УКРАЇНІ

Дерюга І.М.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: illia.deriuha@nure.ua

The article analyses the mandatory technical inspection of wheeled vehicles in Ukraine and its impact on road safety. The author examines the regulatory framework and procedure of technical inspection, the problem of the absence of mandatory technical inspection for non-commercial vehicles and corruption risks.

Технічний контроль – це перевірка відповідності об'єкта (продукції або процесу, від якого залежить її якість) встановленим технічним вимогам. Головною метою обов'язкового технічного контролю колісних транспортних засобів (КТЗ) є забезпечення безпеки дорожнього руху. Автомобільна індустрія та законодавче регулювання у цій галузі постійно змінюються, що створює необхідність аналізу її нинішнього стану. Метою аналізу є оцінювання стану галузі обов'язкового технічного контролю КТЗ (далі – технічний контроль) на теперішній час відносно ефективності виконання нею своєї головної функції, тобто, забезпечення безпеки дорожнього руху.

Основною нормативно-правовою базою для проведення технічного контролю є:

- Закон України «Про дорожній рух»;
- Закон України «Про автомобільний транспорт»;
- Наказ Міністерства інфраструктури України від 26.11.2012 № 710 «Про затвердження Вимог до перевірки конструкції та технічного стану колісного транспортного засобу, методів такої перевірки» (далі – Наказ);
- Постанова Кабінету Міністрів України від 30 січня 2012 р. № 137 «Про затвердження Порядку проведення обов'язкового технічного контролю та обсягів перевірки технічного стану транспортних засобів, технічного опису та зразка протоколу перевірки технічного стану транспортного засобу» (далі – Порядок) [3].

Вимоги до засобів, за допомогою яких проводиться технічний контроль, виконується обслуговування та ремонт КТЗ, викладено у Технологічних вимогах до засобів перевірки технічного стану, обслуговування і ремонту колісного транспортного засобу, затверджених Наказом Міністерства інфраструктури України від 15.02.2012 №106. Зокрема, у них наведено повний перелік стандартів до всіх видів зазначеного обладнання [4].

Процедура технічного огляду стану КТЗ в Україні типово проходить наступним чином:

- замовник привозить КТЗ, повністю укомплектований та заправлений експлуатаційними рідинами, до суб'єкта проведення технічного контролю;
- проводиться зовнішній контроль з метою ідентифікації КТЗ та звірки ідентифікаційних номерів з даними реєстраційних документів;
- замовник сплачує вартість послуги, та здійснюється технічний контроль відповідно до Порядку;
- суб'єкт видає замовнику протокол перевірки технічного стану [3].

Порядок наразі встановлює позбавлення від обов'язкового технічного контролю легкових автомобілів, причепів, мотоциклів, мопедів та ін.; для таких, що не використовуються з метою отримання прибутку – безстроково, а для таких, що використовуються – із строком експлуатації до двох років. Також, у статтях 1.3.1-2 Порядку наведено повний перелік стандартів, які використовуються для ідентифікації КТЗ з метою визначення вимог і методів для його перевірки [2].

Зазначена норма створює проблеми через два фактори. По-перше, за даними відкритих джерел, на 2021 рік було зареєстровано 8.8 млн. легкових автомобілів, більшість з яких є приватними і звільненими від обов'язкового технічного контролю за даним Порядком. По-друге, середній вік українських автівок складає 22.7 років, що робить цей автопарк найстарішим у Європі. Перший фактор може здаватися дуже значним через потенційно великий ризик ДТП, викликаних технічними несправностями. Проте статистика Національної поліції за 2023 рік говорить, що їх відсоток від загальної кількості складає всього 0.17% (40 випадків відносно 23 462 загальних) [2]. Тобто, загрозу безпеці дорожнього руху через відсутність технічного контролю за цим фактором можна вважати нехтовно малою. Але другий фактор має значний вплив: старі автомобілі потребують частішого ремонту та обслуговування, що збільшує витрати їх власників. Старі машини зазвичай викидають більше забруднюючих речовин у навколишнє середовище, оскільки їхні системи нейтралізації можуть бути видалені з метою економії коштів.Оскільки технічний огляд некомерційних автівок не є обов'язковим, відповідальності за такі дії власники не несуть [3], і це створює значну загрозу для екологічного стану в країні. Міністерство інфраструктури пропонує відновити обов'язковий технічний огляд некомерційних автомобілів з 2022 року, але через повномасштабне військове вторгнення процес призупинено. Ця реформа випливає з Угоди про асоціацію з ЄС, а саме необхідністю відповідності законодавства Директиві 2014/45/ЄС, яка встановлює обов'язковий технічний контроль для всіх видів КТЗ [1]. Таким чином, реформа буде проведена лише після завершення війни.

Нинішня процедура технічного огляду з боку питання використовуваних стандартів та технічних вимог не має значних недоліків, бо багато з них є

міжнародними або базуються на них [4]. До того ж, українська галузь стандартизації постійно розвивається та проходить гармонізацію з європейськими стандартами, які вже довели свою ефективність.

З юридичного боку процедура має високі корупційні ризики через можливу підробку протоколів, які підтверджують придатність автомобіля до використання [1]. Хоча нинішній Порядок передбачає обов'язкову фіксацію процесу проведення технічного контролю, у якості доказів фіксації приймаються фотографії. Враховуючи сучасні досягнення у галузі обробки графічних матеріалів, їх наразі стає відносно нескладно підробити. Проблему можна вирішити декількома способами, зокрема:

- відеофіксацією процесу техогляду в «онлайн» режимі;
- введення блокчейн-системи для ведення реєстру виданих сертифікатів відповідності;
- підвищенням відповідальності за неправомірну видачу позитивних сертифікатів [1].

Список використаних джерел:

1. Громадська спілка "Ін-т досліджень авторинку". Обов'язковий техогляд у 2023: бути чи не бути?. *Інститут досліджень авторинку*. URL: https://eauto.org.ua/news/243-obov-yazkoviy-tehoglyad-u-2023-buti-chi-ne-buti (дата звернення: 05.03.2024).
2. Патрульна поліція України. Статистика ДТП в Україні за 2023 рік. *Патрульна поліція України*. URL: https://patrolpolice.gov.ua/wp-content/uploads/2024/01/12.2023.xlsx (дата звернення: 05.03.2024).
3. Про затвердження Порядку проведення обов'язкового технічного контролю та обсягів перевірки технічного стану транспортних засобів, технічного опису та зразка протоколу перевірки технічного стану транспортного засобу : Постанова Каб. Міністрів України від 30.01.2012 р. № 137 : станом на 25 серп. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/137-2012-%D0%BF#Text (дата звернення: 05.03.2024).
4. Про затвердження Технологічних вимог до засобів перевірки технічного стану, обслуговування і ремонту колісного транспортного засобу : Наказ М-ва інфраструктури України від 15.02.2012 р. № 106. URL: https://zakon.rada.gov.ua/laws/show/z0356-12#Text (дата звернення: 05.03.2024).

УДК 006.91:004.89 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.198

КАЛІБРУВАННЯ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ ЗА ДОПОМОГОЮ ШТУЧНИХ НЕЙРОННИХ МЕРЕЖ

Довгополий С.О.
Науковий керівник – к.т.н., доцент. Запорожець О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: serhii.dovhopolyi@nure.ua

Traditional methods of calibrating measuring equipment require considerable effort, time and resources. The use of artificial intelligence, in particular artificial neural networks (ANNs), allows to minimize human involvement and increase the accuracy of calibration. This not only reduces calibration time, but also improves overall efficiency. A complex algorithm for calibration of measurement tools using artificial neural networks is proposed. Artificial intelligence technologies open up new prospects for automation and increasing the efficiency of calibration processes, which is an important factor in modern conditions.

Точність засобів вимірювальної техніки є важливою складовою для забезпечення достовірних результатів вимірювань. Традиційні методи калібрування засобів вимірювальної техніки вимагають значних зусиль, часу та ресурсів. У процедурах калібрування людина відіграє ключову роль, визначаючи методи калібрування, відповідаючи за контроль якості вихідних даних та вирішення можливих проблем у процесі калібрування.

Доведено, що людський фактор є одним із ключових джерел похибок при калібруванні, що може впливати на достовірність результатів[2].

Кваліфікація фахівця не гарантує повної відсутності похибок, вплив різних факторів таких як: суб'єктивність інтерпретації результатів вимірювань, неправильне налаштування та калібрування приладів, недотримання вимог щодо калібрування та повірки засобів вимірювання, помилку у розрахунках, втому, неуважність – впливає на результати при калібруванні. Фахівець відповідає за умови калібрування, вибір еталонів та зразків для порівняння, а також дотримання процедур і протоколів. Помилки на цих етапах можуть викликати неточності результатів вимірювань.

Впровадження автоматизації калібрування на базі штучних нейронних мереж дозволяє мінімізувати вплив людського фактору, підвищити об'єктивність та точність калібрування.

Штучні нейронні мережі (ШНМ) відкрили нові можливості для оптимізації різних технологічних процесів. Однією з таких областей є вимірювальна техніка та її калібрування, де застосування ШНМ може призвести до значного зменшення похибок при калібруванні.

Застосування штучних нейронних мереж при калібруванні дозволить вирішити багато з представлених проблем, забезпечуючи автоматизоване

калібрування засобів вимірювальної техніки. ШНМ можуть адаптуватися до змін у середовищі та компенсувати знос обладнання, забезпечуючи стабільні та надійність вимірювання, бути навчені розпізнавати патерни у вимірювальних даних та коригувати відхилення безпосередньо під час використання. Це дозволить скоротити час, необхідний для калібрування, та підвищить ефективність процесу.

Алгоритм створення та навчання штучної нейронної мережі:

1. Збір даних, створення Dataset – підготовка навчальних даних на основі відомих еталонних значень, стандартів і відповідних показників приладу для різних умов вимірювання.

2. Вибір архітектури. Архітектури нейронних мереж, які можна застосувати для вирішення завдання калібрування:

– згорткові нейронні мережі (Convolutional Neural Networks, CNN). Ефективні для аналізу даних, що мають "просторову" структуру – зображення, аудіо, відео;

– рекурентні нейронні мережі (Recurrent Neural Networks, RNN). Добре працюють з послідовними даними, коли потрібно враховувати контекст і динаміку в часі;

– глибинні нейронні мережі (Deep Neural Networks, DNN). Мають велику кількість шарів, що дозволяє моделювати складні залежності в даних;

– нейронні мережі з довгою короткочасною пам'яттю (Long Short-Term Memory, LSTM). Різновид RNN, оптимізований для запам'ятовування віддалених залежностей в даних;

– згортаючі нейронні мережі (Convolutional LSTM, ConvLSTM). Поєднують можливості CNN і LSTM;

– рекурентні нейронні мережі з затримками в часі (Time Delay Neural Network, TDNN). Використовують затримки для обробки динамічних даних.

3. Машинне навчання – навчання багатошарової нейронної мережі на підготовлених даних[6]. Мережа навчається встановлювати залежність між еталонними значеннями і показниками приладу.

4. Ініціалізація ваг мережі. Встановлення випадкових початкових ваг з'єднань між нейронами, ініціалізація зміщень нейронів.

5. Тренування мережі. Поетапна подача навчальних даних на вхід мережі, обчислення значення функції втрат, коригування ваг та зміщень за алгоритмом оптимізації, повторення до мінімізації функції втрат.

6. Перевірка якості навчання. Тестування мережі на контрольній вибірці даних. Оцінка точності результатів мережі, коригування архітектури та гіперпараметрів за необхідності.

7. Застосування навченої мережі. Використання мережі для прогнозування еталонних значень та порівняння прогнозів з реальними

даними приладу коригування налаштувань приладу за результатами порівняння.

8. Порівняння виходу нейромережі (розрахункових еталонних значень) з реальними показниками приладу.

9. Якщо різниця перевищує допустиму похибку, робиться висновок про необхідність калібрування приладу.

10. Коригування показників приладу для мінімізації відхилення від еталонних значень.

11. Повторення процедури контролю після калібрування.

Застосування штучних нейронних мереж в калібруванні засобів вимірювальної техніки є перспективним напрямком розвитку. Ця технологія дозволяє значно підвищити точність та ефективність процесу калібрування.

По-перше, нейронні мережі здатні з високою точністю моделювати складні нелінійні залежності між показниками приладів та еталонними значеннями. Це дає змогу підвищити адекватність математичних моделей, що використовуються при калібруванні.

По-друге, алгоритми глибинного навчання дозволяють автоматизувати процедури порівняння показників з еталонами і коригування похибок. Це значно пришвидшує процес калібрування і зменшує вплив людського фактору.

По-третє, нейромережі можуть застосовуватися в системах дистанційного моніторингу метрологічних характеристик обладнання. Це надає можливості віддаленого калібрування та контролю стану приладів.

Отже, технології штучного інтелекту відкривають нові перспективи автоматизації та підвищення ефективності процесів калібрування, що є важливим фактором в сучасних умовах. Їх впровадження дозволить підняти метрологічне забезпечення виробництв на якісно новий рівень.

Список використаних джерел:

1. Aggarwal, Charu C. Neural Networks and Deep Learning: A Textbook. Springer, 2023. 529 p.

2. Geron, A. Hands-On Machine Learning with Scikit-Learn, Keras, and TensorFlow. O'Reilly Media, 2019. 856 p.

3. Руденко О.Г., Бодянський Є.В. Штучні нейронні мережі: навчальний посібник. Харків, ТОВ "Компанія СМІТ", 2006. 404 с.

4. Дегтярев А.В., Запорожец О.В., Овчарова Т.А. Идентификация нелинейных динамических средств измерений с помощью искусственной нейронной сети // Метрологія та прилади. Вип. № 2/II/(41). 2013. С. 85–89.

5. Zaporozhets O.V., Shtefan N.V. Using Artificial Neural Network for Compensation of Semiconductor Thermistor Nonlinearity // 2019 IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL), Sozopol, Bulgaria, 6-8 Sept. 2019. PP. 703–706.

УДК 006.015.5:[004.738.5:621.391]
DOI https://doi.org/10.30837/IYF.PDICIMT.2024.201

ДОСЛІДЖЕННЯ ТА РОЗРОБКА МЕТОДІВ ПОКРАЩЕННЯ ЯКОСТІ МОБІЛЬНОГО ЗВ'ЯЗКУ ТА МОБІЛЬНОГО ІНТЕРНЕТУ В ШВИДКІСНИХ ПОТЯГАХ

Жигло С.В.
Науковий керівник – к.т.н, доцент Штефан Н.В.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: serhii.zhyhlo@nure.ua

In today's world, high-speed trains are an important part of the transport infrastructure, but passengers often face mobile communication problems while traveling. At the moment, the relevance of this topic is justified by the broad interest of the state represented by the Ministry of Digital Transformation, the national carrier of goods and passengers JSC Ukrainian Railways, leading electronic communications operators, end users of electronic communications services, and the practical need to solve this problem.

Current methods include the construction of new base stations on each "problematic" section of the railway, but this is not economically feasible, as it requires significant capital investment, and the revenue from services will not cover operating costs.

This report is dedicated to analyzing the existing problems and developing new methods to improve the quality of mobile communications.

Світовий досвід забезпечення пасажирів швидкісних потягів якісним бездротовим зв’язком та інтернетом полягає у трьох різних принципах побудови такої системи.

1. Інтернет від Starlink

Компанією SpaceX побудована велика супутникова система для роздачі високошвидкісного інтернету в місцях, де він не доступний або небезпечний. При цьому використання цієї системи у швидкісних потягах України створює перні труднощі:

по-перше, сама технологія Starlink не розрахована на роботу в високошвидкісних потягах;

по-друге, 1 комплект при статичному використанні здатний забезпечити швидкість передачі даних у 100Мбт/с. Кількість пасажирів у потягу Інтерсіті+ становить 579. Навіть за допомогою 4-х комплектів середня швидкість на одного користувача не буде перевищувати 500 кбт/с (частковий трафік забере внутрішньопотягове обладнання.);

по-третє, використання голосового зв’язку можливо лише з повноцінним впровадження технології VoWiFi (Wi-Fi Calling – технологія, яка дозволяє здійснювати дзвінки, надсилати й отримувати SMS і MMS повідомлення навіть за відсутності покриття мобільної мережі, незалежно

від вашого місцезнаходження чи оператора з використанням Wi-Fi-мережі);

по-четверте, це безпекова складова цього процесу. Досвід використання українськими військовими Starlink показав не стабільність технології, оскільки «керується ззовні».

2. Система Trackside Network (TSN)

TSN – це окрема бездротова мережа з широкосмуговим доступом до Інтернету.

Типова мережа TSN складається з 2-х основних частин:

- оптичної магістралі вздовж усієї залізничної лінії;
- бездротове обладнання у вигляді базових станцій на стовпах та терміналів на даху поїзда.

Необхідною умовою для будівництва виділеної мережі зв'язку «поїзд-земля» є прокладання оптичного кабелю вздовж усієї залізничної лінії. На деяких ділянках можна використовувати фіксований бездротовий зв'язок між базовими станціями TSN-мережі, але оптика вздовж шляхів - це основна умова.

Залежно від обраної технології, частотного діапазону та інших умов (таких як дощові зони ITU) проводяться розрахунки енергетичного запасу лінії між терміналом на поїзді та базовою станцією та визначається рекомендована відстань між базовими станціями.

В Україні в 2010 році Укрзалізниця вже мала негативний досвід будівництва власної мережі. Проект не мав доставнього ефекту. Наразі будувати окрему мережу для поїздів не вигідно і це важко піддається реалізації, оскільки потребує колосальних інвестицій як на тво, так і на експлуатацію.

3. Мобільний зв’язок та інтернет від операторів мобільного зв’язку

Основними перевагами використання цієї моделі є :

- використання вже існуючої базової інфраструктуру операторів мобільного зв'язку з необхідною модернізацією за відсутності потреби побудови нової мережі;
- можлива синергія існуючих мереж усіх операторів;
- мінімальні безпекові ризики, оскільки надавачі послуг є резидентами України;
- можливість користуватися як інтернетом, так і голосовим зв'язком.

При цьому існує ряд недоліків використання цієї моделі:

- не достатнє покриття залізної дороги за межами населених пунктів;
- затухання сигналу у вагоні на рівні 20дБ;
- затримка реєстрації абонентів в нових сотах станцій при збільшенні швидкості потягу;
- падіння пропускної спроможності при одночасній реєстрації великої кількості абонентів у соті;

- несиметричний характер зв'язку, коли швидкість скачування (download) приблизно 20 разів вище, ніж швидкість вивантаження (upload).

Основними способами модернізації існуючих мереж мобільних операторів під можливість забезпечення якісного мобільного зв’язку та мобільного інтернету в високошвидкісних потягах є використання:

- адаптивних антенний систем - розробка антенн, які можуть динамічно змінювати свої параметри для оптимізації прийому сигналу в залежності від розташування та швидкості потяга;
- антен з високий коефіцієнтом випромінювання для зменшення втрат сигналу та підвищення якості зв’язку;
- штучного інтелекту для оптимізації зв’язку - застосування алгоритмів машинного навчання для аналізу даних про якість зв’язку та автоматичного вибору найкращого каналу зв’язк;
- прогнозування потенційних перешкод у зв’язку та автоматичне переключення на альтернативні частоти.

При цьому створення єдиної інтегрованої системи, яка об’єднає сигнали усіх операторів, супутниковий зв’язок з іншими системами потягу (система приймання та обробки сигналів, внутрішньопотягова система WiFi, система GPS, система управління рухом) забезпечить стабільний та якісний сервіс пасажирам у вигляді доступу бездротового доступу до високошвидкісної мережі Інтернет та якісний мобільний зв’язок незалежно від розташування та швидкості руху потягу.

Список використаних джерел:

1. Generalized Frequency Division Multiplexing for 5th Generation Cellular Networks [Електронний ресурс] / [N. Michailow, M. Matthé, I. Gaspar та ін.]. URL: https://www.vodafone-chair.org/media/publications/legacy/n-michailow/Generalized_Frequency_Division_Multiplexing_for_5th_Generation_Cellular_Networks.pdf (дата звернення: 01.03.2024).

2. Дослідження основних недоліків базових станцій різних поколінь стільникового зв’язку / Р. С. Одарченко та ін. Телекомунікаційні та інформаційні технології. 2016. С.107-110.

3. План заходів щодо підвищення якості послуг рухомого (мобільного) зв’язку, затверджено Розпорядженням Кабінету Міністрів України від 30 вересня 2020 р. № 1189-р [Текст]// URL: https://zakon.rada.gov.ua/laws/show/1189-2020-%D1%80#Text (дата звернення: 02.03.2024).

4. Нікітенко О.М., Єгоров А.Б., Штефан Н.В. Сучасні інструменти управління якістю. Харків: ХНУРЕ, 2019. 245 с.

УДК 006.015.5:004.77 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.204

РЕАЛІЗАЦІЯ МОДЕЛІ SQFD ДЛЯ ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ФУНКЦІОНУВАННЯ IT-СЕРВІСІВ

Заболотний Є. О.
Науковий керівник – к.т.н., ст. викл. Мощенко І.О.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: yevhen.zabolotnyi@nure.ua

This paper presents the SQFD (Service Quality Function Deployment) model as an effective method for ensuring the quality of IT service functioning. SQFD helps organizations to identify user needs, translate them into technical characteristics, and develop services that meet these needs. This work explores the implementation of the SQFD model to enhance the quality of the language learning applications as a case study. Through SQFD, user requirements are prioritized, and translated into technical features. The model enables the assessment of user satisfaction, comparison with competitors, and evaluation of technical feasibility. This comprehensive approach facilitates informed decision-making for product enhancement.

Забезпечення якості функціонування IT-сервісів є ключовим фактором успіху будь-якої організації. Активна цифровізація процесів діяльності людей в сучасному світі невпинно розширює сфери застосування IT-технологій, що в свою чергу виносить на перший план проблеми забезпечення якості, надійності, зручності, функціональності та безпеки програмних систем (яскравим прикладом є активний розвиток порталів та застосунків надання державних послуг).

Найбільш важливим аспектом забезпечення якості є найповніше задоволення вимог користувачів (за ДСТУ ISO 9001:2015 Системи управління якістю. Вимоги (ISO 9001:2015, IDT) та ДСТУ ISO/IEC 20000-10:2019 Інформаційні технології. Керування послугами. Частина 10. Концепції та словник термінів (ISO/IEC 20000-10:2018, IDT)) [1]. Одним з ефективних методів досягнення цієї мети є використання моделі управління якістю IT-сервісів SQFD (Service Quality Function Deployment).

SQFD – це адаптована модель QFD (Quality Function Deployment), яка використовується для розгортання функції якості в контексті IT-сервісів. Вона допомагає організаціям чітко визначити суб'єктивні вимоги користувачів, перекласти їх в інженерні технічні характеристики та розробити сервіси, які відповідають цим потребам [1]. Проблеми застосування SQFD для IT-сервісів полягають у складності точного визначення потреб користувачів, обмеженості доступних даних щодо конкурентів та високої вартості інтеграції з існуючими процесами розробки продукту. Основні переваги моделі SQFD полягають в орієнтації на споживача, зручному візуальному представленні інформації та

комплексному структурованому підході до прийняття рішення щодо поліпшення продукту [2].

Реалізація моделі SQFD для забезпечення якості IT-сервісів здійснена на прикладі застосунку для вивчення іноземних мов (рис. 1).

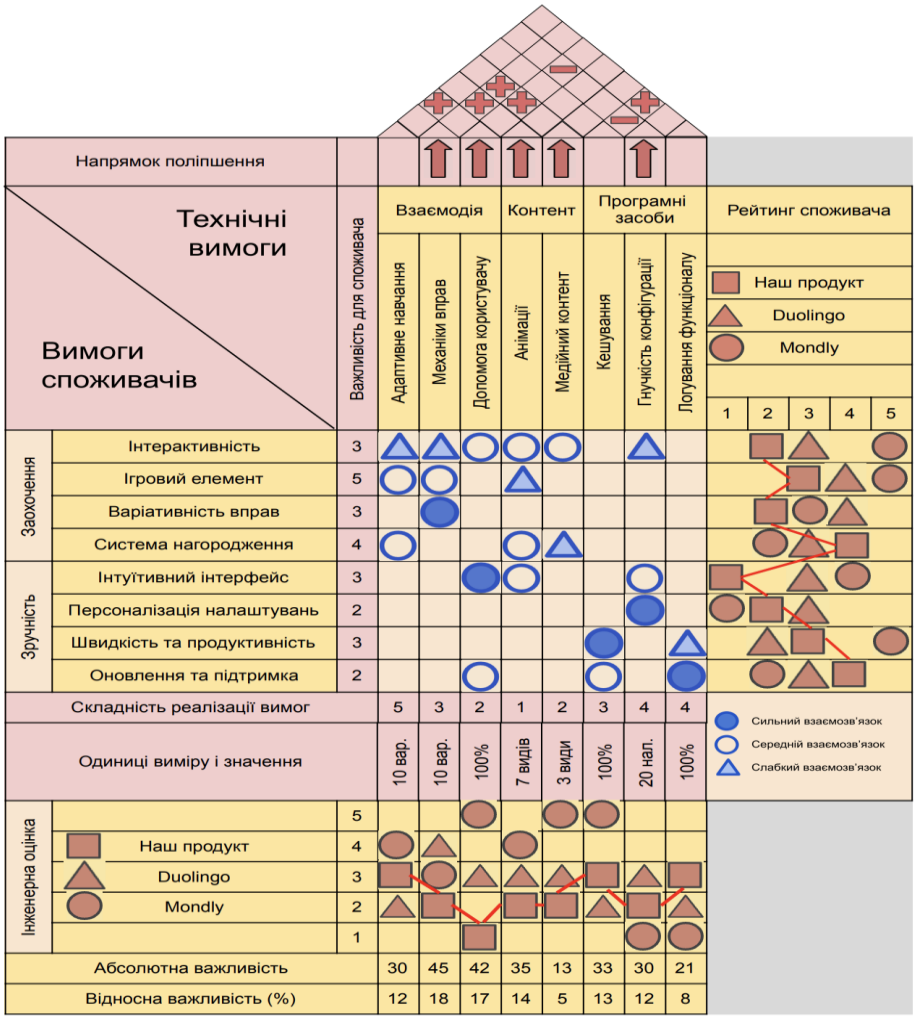


Рисунок 1 – Приклад матриці розгортання функції якості

Основні вимоги користувачів такого застосунку можна розділити на дві основні категорії: заохочення користувача до навчання та зручність використання. Першу категорію можна деталізувати до таких вимог: інтерактивність, наявність ігрового елементу, висока варіативність занять, система нагородження, а другу до наступних: інтуїтивний інтерфейс, персоналізація налаштувань, швидкість та продуктивність, оновлення та підтримка.

В ході розгортання функції якості визначається рейтинг важливості вимог споживача і оцінюється задоволеність цих вимог в порівнянні з конкурентними продуктами. Далі формулюються технічні вимоги до продукту, які мають забезпечити реалізацію вимог користувачів, і визначається взаємозв’язок між технічними та користувацькими вимогами.

До прикладу реалізація різноманітних механік вправ безпосередньо задовольняє вимогу користувача у варіативності занять; відпрацьована система допомоги користувачу з використання застосунку (початкове ознайомлення з інтерфейсом, довідка, система нагадувань і підказок) покращує інтуїтивність інтерфейсу; анімації та медійний контент покращують інтерактивність застосунку; кешування покращує швидкість та продуктивність; гнучкість конфігурації забезпечують персоналізацію; продумана система логування покращує підтримку застосунку.

Крім взаємозв'язку між користувацькими і технічними вимогами, метод SQFD дозволяє показати вплив одних технічних характеристик на інші. Також важливо порівняти реалізацію технічних рішень з конкурентами та оцінити складність втілення технічних властивостей в нашому програмному продукті. Результатом застосування є ранжування показників якості IT-сервісів за ступенем пріоритетності реалізації, що розраховується на основі аналізу користувацьких вимог, технічних можливостей та обмежень команди розробки, а також конкурентної ситуації на ринку надання IT-послуг.

Список використаних джерел:

1. Корніцький С., Мощенко І. Огляд міжнародних стандартів в сфері управління якістю IT-послуг // Розвиток наукової думки постіндустріального суспільства: сучасний дискурс: матеріали IV Міжнародної наукової конференції, м. Івано-Франківськ, 17 листопада, 2023. Вінниця: ТОВ «УКРЛОГОС Груп, 2023. С. 154 – 155.

2. Ficalora Joseph P., Cohen L. Quality function deployment and Six Sigma: a QFD handbook. 2nd ed. Prentice Hall. 2010. 527 p.

УДК 006.029:781.1

СТАНДАРТИЗАЦІЯ В МУЗИЦІ

Захарова Е.О.
Науковий керівник – д.т.н., професор Захаров І.П.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: evelina.zakharova@nure.ua

The history of choosing the musical scale reference point is considered. The issues of standardization of scale frequencies are investigated. The history of the construction of a universal scale is described. The methodology for constructing a 12-step uniformly tempered scale is outlined. The standardization of musical scale frequencies has been studied. Different types of musical scales are compared.

Стандартизація в музиці стосується, насамперед, частот звукоряду, стандартизація яких забезпечує точність налаштування інструментів та сумісність їхнього загального звучання. Стандартизація звукоряду починається з вибору його «реперної» точки, в якості якої беруть ноту «Ля» першої октави. Частота цієї ноти в різні часи набувала різних значень. У XVI-XVII століттях це була частота 405-407 Гц. У 1619 Преторіус запропонував використовувати як еталонну висоту тону – звук із частотою 422,5 Гц. При введенні метричної системи було прийнято нову частоту − 435гц [1]. В 1836 Штудгартська конвенція підвищила частоту ноти ля до 440 Гц. Цю ж частоту визначили 1939 р. на Міжнародній конференції у Лондоні. Цю частоту наказує стандарт ISO 16:1975 [2]. Слід зазначити, що припустима похибка налаштування музичного інструменту цієї частоти становить від ±0,5 Гц [2] до ±0,76 Гц.

Стандартизація частот звукоряду також має власну історію [3]. Перші звукоряди спиралися на т.зв. чистий стрій, в основі якого лежать цілочислові співвідношення частот музичних інтервалів: октава 2:1, квінта 3:2, кварта 4:3, велика терція 5:4, мала терція 6:5, велика секунда 9:8 тощо.

Ще Піфагор (VI століття до н.е.) висловив ідею, що єдину шкалу утворюють звуки, отримані відкладанням від деякого вихідного звуку будь-якої кількості квінт вгору і вниз, з перенесенням нот, що виходять, у всі октави. Однак піфагорів лад міг існувати тільки в умовах одноголосся, оскільки єдиними інтервалами, які можна в ньому виконати в одночасному звучанні, є октава, квінта і кварта.

Теоретики XVI століття Царліно та Фольяні запропонували звукоряд, який отримав назву чистого ладу: він включає відкладені від основного тону октаву, квінту та кварту, а також великі терції від основного тону, квінти та кварти. Однак у чистому ладі, як і в піфагоровому, інтервали між сусідніми ступенями звукоряду виявляються неоднаковими. І це означає, що у чистому ладі не можна відкладати будь-які інтервали від будь-яких щаблів звукоряду. Наприклад, чистий лад характеризується абсолютно

чистим звучанням квінти на першому ступені основної тональності, але при цьому інші квінти звучать вже не так чисто, а деякі – відверто фальшиво (вовча квінта). Для того щоб темперувати («вгамувати», «згладити») піфагорів або чистий звукоряд, доводилося вдаватися до штучного невеликого підвищення або зниження окремих ступенів звукоряду (на величину коми) при грі в ряді тональностей. Вільного переходу (модуляції) від однієї тональності до іншої не могло бути.

Одним із шляхів подолання цих труднощів здавалося збільшення числа ступенів у октаві. Було запропоновано велику кількість «математичних» строїв з різним числом щаблів: від 16 (Царліно) до 53 (Меркатор). Виготовлялися кнопкові інструменти з різним числом кнопок на октаву (аж до 31). Незважаючи на це, спроби побудови універсального звукоряду зі збереженням «чистоти» інтервалів зайшли в глухий кут. Потрібно було принципово нове рішення – і цим рішенням став 12-ступінчастий рівномірно темперований звукоряд, для переходу до якого знадобилося більше 2 тисячоліть.

Поступово темперований звукоряд складається з 12 нот, розміщених у межах однієї октави. Частоти цих нот утворюють геометричну прогресію з основою 21/12. Порівняння цього звукоряду з частотами «чистого» ладу показують, що похибка їх для першої октави може досягати 4 Гц, проте цей недолік, помітний тільки для надідеального музичного слуху, тьмяніє в порівнянні з можливістю виконання музичних творів на тому самому інструменті в будь-якій тональності [4].

Ця можливість дозволяє здійснити транспонування будь-якого твору на будь-яку з 12 тональностей у разі нездійсненності або трудомісткості виконання його голосом або на будь-якому інструменті в оригінальній тональності.

Список використаних джерел:

1. Documents diplomatiques. De la conference du metre. Paris. Imprimerie Nationale, 1875, 149 p.

2. ISO 16:1975. Acoustics – Standard tuning frequency (Standard musical pitch).

3. Ivanov P.B. A Hierarchical Theory of Scale Perception: Musical Scales // Leonardo, 1994, v. 27, no. 5, pp. 417–421.

4. Helmholts H. Tonempfindungen. Braunschweig, 1863, 720 p.

УДК 543.062 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.209

ОСОБЛИВОСТІ ОЦІНЮВАННЯ НЕВИЗНАЧЕННОСТІ АНАЛІТИЧНІ ВИМІРЮВАНЬ

Захаров О.І.
Науковий керівник – к.т.н., доцент Запорожець О.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
e-mail: oleksandr.zakharov4@nure.ua

The problem of measurement uncertainty evaluation when carrying out quantitative chemical analysis is considered. Existing regulatory documents of EURACHEM / CITAC devoted to this issue are analyzed. The main features of analytical measurements are covered. The difficulties and ambiguities that arise when measurement uncertainty evaluation are identified. Recommendations are given on ways to overcome them.

В основі аналітичних вимірювань лежить кількісний хімічний аналіз, який полягає в експериментальному визначенні вмісту одного чи ряду компонентів у пробі. Результат хімічного аналізу повинен супроводжуватися характеристиками невизначеності вимірювань.

Оцінюванню невизначеності аналітичних вимірювань присвячені документи EURAHIM/CITAC [1-5]. Однак їх застосування на практиці викликає ряд труднощів і неоднозначностей. Це зумовлено наступними особливостями оцінювання невизначеності в аналітичних вимірюваннях.

1. Широкий спектр моделей вимірювань, які застосовують в кількісному хімічному аналізі, (одноразові та багаторазові прямі та непрямі вимірювання використовуються при безпосередньому проведенні аналітичних вимірювань, обробка кількох груп прямих (непрямих) вимірювань – при проведенні внутрішньолабораторних та міжлабораторних звірень; сумісні вимірювання використовують при калібруванні засобів вимірювальної техніки, наприклад газових хроматографів) призводить до необхідності застосування різних методів обробки результатів вимірювань та оцінювання їх невизначеності.

2. У модельних рівняннях аналітичних вимірювань, на відміну від геометричних, електричних та інших, використовується значно більша кількість вхідних величин. Це призводить до необхідності застосування на початкових етапах оцінювання невизначеності вимірювань причинно-наслідкових діаграм та використання у процесі роботи спеціалізованих програмних засобів. Розробку останніх доцільно проводити на основі бюджетів невизначеностей.

3. Під час проведення сумісних вимірювань використовуються стандартні зразки, невизначеністю яких не можна знехтувати. Цей факт має враховуватися щодо коефіцієнтів калібрувальної залежності шляхом застосування методів конфлюентного аналізу.

4. Невелика кількість паралельних вимірювань призводить до зміщення оцінки стандартної невизначеності та її сильного розсіювання. Перше усувається запровадженням поправочного коефіцієнта, друге – до необхідності врахування степенів свободи під час оцінювання розширеної невизначеності.

5. При проведенні паралельних вимірювань через використання однієї й тієї ж проби очевидна значна кореляція типу *B* між результатами вимірювання. Цей факт має враховуватись при оцінюванні невизначеності цих вимірювань.

6. Настанови [1-5] не враховують нелінійність модельних рівнянь. Незважаючи на те, що модельні рівняння непрямих вимірювань, що застосовуються при кількісному хімічному аналізі найчастіше являють собою добуток або частку від ділення вхідних величин, дослідження границь застосування методу лінеаризації при обробці непрямих вимірювань показують, що при суттєвих значеннях невизначеності вхідних величин, що входять до нелінійного рівняння вимірювань, призводить не тільки до зміщеної оцінки результату вимірювання, але і до суттєвих похибок оцінювання стандартної та розширеної невизначеності вимірюваної величини.

7. У ряді випадків оцінювання невизначеності вимірювань доцільно проводити за результатами внутрішньолабораторних досліджень придатності методу. Як показує порівняльний аналіз різних підходів до оцінювання невизначеності, недоліками класичного підходу є суттєва трудомісткість і можливість отримання завищених оцінок невизначеності. Для оцінювання невизначеності вимірювань за результатами внутрішньолабораторних досліджень доцільно застосовувати спеціалізовані програмні засоби.

Список використаних джерел:

1. EURACHEM / CITAC Guide CG 4. Quantifying Uncertainty in Analytical Measurement. Third Edition. QUAM:2012. 141 p.

2. EURACHEM / CITAC Guide. Guide to Quality in Analytical Chemistry. An Aid to Accreditation. Third Edition. QAC 2016. 66 p.

3. EURACHEM / CITAC Guide. Measurement uncertainty arising from sampling. A guide to methods and approaches. Second Edition 2019. Produced jointly with Eurolab, Nordtest, and RSC Analytical Methods Committee. 120 p.

4. Eurachem / CITAC Guide. Use of Uncertainty Information in Compliance Assessment. Second Edition. 2021. 38 p.

5. Eurachem / CITAC Guide. Metrological Traceability in Chemical Measurement. A guide to achieving comparable results in chemical measurement. 2nd Edition in English. 2019. 45 p.

УДК 621.38

ПІРОЕЛЕКТРИЧНІ ДЕТЕКТОРИ ДЛЯ ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНИХ МОДУЛІВ

О. Ю. Бондаренко, І. Іг. Ключник, аспірант, Зіненко М.С. аспірант
Наукові керівники – к.т.н., доц. О. В. Дегтярьов, к.т.н., проф. І.Ів. Ключник
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
email: d_mme@nure.ua

A problem of divergence between datasheets and corresponding final inspection certificates in sensors and actuators is known. Pyroelectric detectors are not found to be an exception. As a solution, a new complete identification method for obtaining extended pyroelectric detector specifications, being successfully approved in practice, has been proposed.

Відома проблема різниці між технічними характеристиками та технічними паспортами компонентів елементної бази. Піроелектричні детектори не стали винятком. В якості рішення для отримання розширеного переліку характеристик піроелектричних детекторів запропоновано новий метод повної ідентифікації, який було успішно випробувано на практиці.

Піроелектричні детектори (ПД), як і будь-які інші вироби в галузі електроніки, мають свої технічні паспорти (ТП). В ТП вноситься інформація, отримана шляхом вимірювання того чи іншого параметра стосовно кожного окремо взятого виробу. ТП складаються на основі результатів контрольних операцій, що проводяться відділом технічного контролю підприємства або відповідною лабораторією фірми-виробника. При цьому, слід розрізняти технічні паспорти та технічні характеристики [1, 2]. В останніх виробники надають лише, так звані, загальні значення відповідних параметрів, і нерідко дрібним шрифтом додають інформацію про те, що вони залишають за собою право змінювати будь-які параметри без попереднього повідомлення споживачів. Як результат, в деяких випадках спостерігаються значні розбіжності при оцінках параметрів ПД, що призводить до помилок при обранні елементної бази для електронних пристроїв на їх основі. У зв'язку з цим виникає необхідність в чіткому розмежуванні параметрів ПД, які надані в ТП, та їх загально-технічних характеристик. Така ситуація спостерігається, перш за все, в наслідок того, що, нажаль, єдиного стандарту на піроелектричні детектори, щонайменше узгодженого між виробниками, не існує, хоча деякі параметри в технічних паспортах, що підлягають вимірюванню, зустрічаються постійно. До таких параметрів відносяться піроелектричний відгук та шум. Ще один параметр – питома виявляюча здатність, обчислюється за стандартизованою методикою.

Отже, всі параметри піроелектричних детекторів можуть бути поділені на дві групи. До першої групи відносяться загальні, а до другої – ті що

підлягають вимірюванню, включаючи такі, що розраховуються (в тому числі, у зв'язку з неможливістю або з складнощами їх вимірювання, що пов'язано з особливостями піроелектричних перетворювачів).

До загальних параметрів технічного паспорту пірodетекторів, наприклад, компанії DIAS-Infrared GmbH [3] відносяться серійний номер ПД, назва його моделі, пропускна спроможність вхідного вікна, розміри чутливого елемента та його площина, а також частота модуляції, на якій проводилось вимірювання відгуку та шуму. Параметр "вікно" в цьому ТП означає діапазон довжин хвиль та відсоток їх пропускної спроможності. Якщо оптична характеристика вікна не надається, за замовчуванням береться стандартна оптична характеристика даного матеріалу вікна. "Частота 10 Гц" вказує на те, що обертання модуляційного диску забезпечує модуляцію теплового потока постійної величини з частотою 10 Гц. Для ПД вказаного вище виробника загальні параметри зведено в табл. 1, а вимірювальні наведено в табл. 2.

Номер	Модель	Вікно	Розміри	Площина	Частота
xxxxxx	LTA G2 xx-xx	8–14 μм	2 мм ×2 мм	4 мм^2	10 Гц

Таблиця 1 – Параметри пірodетектора що не підлягають вимірюванню

Відгук	Спектральний шум	Питома виявляюча здатність
111 В/Вт	92 нВ/√Гц	$2.41 \cdot 10^8$ см√Гц/Вт

Таблиця 2 – Параметри пірodетектора, які підлягають вимірюванню та обчисленню

Відгук, зазвичай, вимірюється наступним чином. Пірodетектор розміщується на одній оптичній осі з абсолютно чорним тілом, яке працює при заданій температурі. Між абсолютно чорним тілом та пірodетектором встановлюється обтюратор, вікно якого співпадає з оптичною осью "випромінювач-приймач". Пірodетектор підключається до входу синхронного підсилювача, налаштованого на частоту модуляції, і далі до вторинного вимірювального прилада. Отримане значення вноситься в технічний паспорт. При цьому, коректний запис обов'язково включає одиниці вимірювання відгуку, а також додаткові відомості стосовно умов, за яких відбувалося вимірювання, а саме: температура абсолютно чорного тіла, температура навколишнього середовища, відстань між абсолютно чорним тілом та пірodетектором, частота модуляції теплового потоку, діаметри апертур, якщо використовуються.

Вимірювання шуму проводиться за таким же принципом, але пірodетектор має бути екранований від впливу випромінювання. Отримане значення вноситься в технічний паспорт.

Питома виявляюча здатність розраховується виходячи з отриманих результатів відгуку та шуму, а також площини чутливого елемента. Результуюча питома виявляюча здатність обчислюється як відношення відгуку до спектрального шуму, яке помножене на корінь квадратний з площини чутливого елемента.

На жаль, таких даних недостатньо при необхідності прийняття рішенн що до використання ПД за умов експлуатації, при яких потрібно враховувати інші параметри, ніж ті що вказані в ТП. Це стосується випадків визначення параметрів ПД при інших частотах модуляції теплового потоку (що необхідно при підборі піродетектора для інформаційно-вимірювального ОЕМ-модуля газоаналізатора), або в режимі без модуляції (наприклад, у складі датчика руху). Відповіді на такі запити потребують проведення ідентифікації піроелектричних детекторів, тобто отримання математичної моделі у вигляді рівняння, яке описує повний цикл перехідного процесу в ПД. Моделювання електричної еквівалентної схеми на основі цього рівняння дає можливість отримувати недостатні числові дані та будувати будь-які характеристики, в тому числі, часові (перехідні, імпульсні) та всі можливі частотні. Чим точніше проведена ідентифікація, тим точніші будуть всі інші характеристики піроелектричних детекторів. Під ідентифікацією в даному випадку слід розуміти математичне рівняння, яке є апроксимацією розподілу дискретних даних, отриманих шляхом вимірювання. Приклади двох технічних паспортів для піродетекторів LTA G2 та LME-302 з розширеним переліком характеристик, отриманих за методом повної ідентифікації, представлено в [4].

Висновки. Таким чином, для багатьох можливих сфер застосування піродетекторів даних, наведених в ТП та різного рода технічній документації, виявляється недостатнім. Відсутні параметри та характеристики можливо отримати шляхом побудови електричної еквівалентної схеми та подальшого проведення симулції в будь-якому пакеті програмного забезпечення за методом повної ідентифікації та правилами будування еквівалентних електричних схем. Саме для піродетекторів процес ідентифікації є особливо важливим у зв’язку з особливостями вимірювання деяких їх параметрів. Підвищення точності оцінки цих та інших параметрів ПД визначається точністю виконана ідентифікації піродетектора.

Список використаних джерел:

1. URL:https://www.dias-infrared.de/pdf/ltag2_eng.pdf (Дата звернення: 20.01.2024).
2. URL:https://media.infratec.eu/infratec-datasheet-lme-302.pdf?mp_enc=bXBfZGlyPTY1MTY3Jm1wX2lkPTE2ODM2MzQ5MTg= (Дата звернення: 20.01.2024).
3. DIAS-Infrared, GmbH. Технічний паспорт піродетектора.
4. Bondarenko A. Examples of Extended Pyroelectric Detector Specifications for Advanced Engineers. Google Books, 2022. 58 p. URL: https://www.google.com.ua/books/edition/Examples_of_Extended_Pyroelectric_Detect/YApZEAAAQBAJ?hl=en&gbpv=1&dq=inauthor:%22Alexander+Bondarenko%22&printsec=frontcover (Дата звернення: 20.01.2024).

УДК 006.015.5 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.214

АНАЛІЗ УМОВ ЗАСТОСУВАННЯ ТА ВІЗУАЛІЗАЦІЇ СТАТИСТИЧНИХ ІНСТРУМЕНТІВ УПРАВЛІННЯ ЯКІСТЮ

Кобрін І.С.
Науковий керівник – к.т.н., ст. викл. Мощенко І.О.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
e-mail: ivan.kobrin@nure.ua

This article discusses the conditions for applying and visualizing statistical quality management tools and the importance of improving product quality. The implementation of seven quality management tools will help the enterprise to maintain and improve the high level of quality in production, given the relevance of the possibility of product integration into the European market. For the effective use of quality control tools, it is necessary to understand and take into account the peculiarities of their application depending on the input statistical information, advantages, disadvantages and visualization capabilities.

Настанови щодо вибору та використання статистичних методів контролю якості надає міжнародний стандарт ISO 10017:2021 Quality management - Guidance on statistical techniques for ISO 9001:2015 [1]. Ця настанова містить визнані методи обробки статистичної інформації, рекомендовані для управління якістю відповідно до конкретних пунктів і підпунктів стандартів серії ISO 9000, і визначає необхідність кількісних даних (якісні дані також можуть використовуватися, якщо вони можуть бути продемонстровані в кількісній формі) для виконання вимог цих пунктів.

Статистичні інструменти управління якістю базуються на застосуванні сімох традиційних основних інструментів контроля якістю: контрольний аркуш, контрольна мапа, гістограма якості, стратифікація (розшарування), діаграма розкиду, причинно-наслідкова діаграма (діаграма Ішікави), діаграма Парето [2]. Кожен з цих інструментів в процесі реалізації циклу PDCA забезпечує якість продукції, що на сьогодні дуже актуально, враховуючи можливості інтеграції вітчизняної продукції на європейський ринок.

Контрольний аркуш є інструментом управління якістю, що використовується для систематичного збору та аналізу даних про якість продукції чи послуг. Він допомагає встановити стандарти якості, моніторити процес виробництва, виявляти проблемні області та служить доказом якості.

Контрольна мапа - це інструмент, що дає змогу відстежувати перебіг протікання процесу і впливати на нього (за допомогою відповідного негативного зворотного зв'язку), попереджаючи його відхилення від висунутих до процесу вимог. Вона відображає стабільність технологічного

процесу. З використанням даних карт можлива реалізації аналітики з позиції динамічного передбачення оцінки досягнення меж допуску і необхідності попереджувальних дій.

Гістограма якості - це інструмент, що дає змогу візуально оцінити закон розподілу статистичних даних. Вигляд гістограми дозволяє зробити висновки про придатність процесу забезпечувати необхідний рівень якості у визначений момент часу та надати рекомендації щодо поліпшення ситуації.

Розшаровування (стратифікація) - це інструмент, що дає змогу здійснити селекцію (кластеризацію) даних, що відображає необхідну інформацію про процес.

Діаграма розкиду є потужним інструментом статистичного аналізу, що використовується для візуалізації взаємозв'язку між двома змінними. В контексті управління якістю, діаграми розкиду можуть бути використані для виявлення зв'язку між двома параметрами, такими як витрати і якість, температура і рівень виробництва тощо.

Причинно-наслідкова діаграма (схема Ішікави) - дає змогу ефективно знаходити рішення в складних ситуаціях і виробляти нові ідеї, знаходити суттєві чинники, що впливають на кінцевий результат.

Діаграма Парето - це інструмент, що дає змогу виявити основні причини проблем і продумати план з їхнього вирішення.

Для ефективного застосування інструментів контролю якості потрібно розуміти і враховувати особливості їх реалізації в залежності від вхідної статистичної інформації, переваги, недоліки, можливості візуалізації (табл. 1).

Таблиця 1 – Рекомендації щодо застосування інструментів управління якістю

Інструмент	Переваги	Недоліки	Рекомендації щодо застосування
Контрольний аркуш	Простота у використанні, заздалегідь розроблені стандартні бланки	Неможливість врахувати появу непередбачуваних дефектів для їх вчасного виявлення	Вхідна статистична інформація використовується для першого етапу збору, впорядковування та формалізації даних. Візуалізується у вигляді таблиць або нескладних графіків методами дескриптивної статистики
Контрольна мапа	Можливість контролювати хід процесу та відстежувати можливі негативні тенденції задля попередження появи дефектів	Висока працемісткість процесу фіксації контрольованих параметрів у реальному часі	Вхідні дані є неперервними випадковими величинами, значення яких є кількісними даними параметра якості, або дискретними випадковими величинами (якісні дані). Візуалізуються у вигляді графіків

Продовження табл. 1

Інструмент	Переваги	Недоліки	Рекомендації щодо застосування
Стратифікація (розшарування)	Наочність зображення великої кількості даних, згрупованих за факторами впливу	Потрібно досконало розуміти процес, щоб максимально якісно виокремити фактори групування	Розкид статистичних даних всередині страт повинен бути меншим, ніж до процесу розшарування. Візуалізуються у вигляді графіків
Діаграма розкиду	Спрощення контролю технологічного процесу завдяки визначенню кореляційного зв'язку між двома факторами	Неможливість в реальних умовах виробництва повністю усунути або врахувати вплив інших факторів	Статистичні дані, які аналізуються на наявність кореляції, повинні бути незалежними від інших можливих факторів впливу, або ця залежність повинна бути врахована. Візуалізуються у вигляді графіків
Причинно-наслідкова діаграма (діаграма Ішікави)	Можливість наочно зобразити велику кількість факторів впливу та прослідкувати ланцюжок причин	Складність усебічного аналізу можливих факторів, навіть малоймовірних з першого погляду	Вхідна інформація має якісний, а не кількісний характер. Отримується експертним методом. Візуалізується у вигляді схеми або інтелектуальної мапи
Діаграма Парето	Надає можливість скерувати зусилля на найбільш значущих факторах. Дозволяє проаналізувати вартісний вплив факторів	Можна випустити з уваги менш значущі фактори, які можливо мають тенденцію до збільшення впливу	Для максимальної ефективності аналізу виникнення конкретної проблеми кількість факторів впливу рекомендується обирати в діапазоні від 7 до 10. Візуалізуються у вигляді графіків

Висновки. За допомогою методу порівняльного аналізу надано рекомендації щодо умов застосування та візуалізації традиційних інструментів управління якістю, проаналізовано переваги, недоліки кожного на практиці в процесі контролю якості на виробництві.

Список використаних джерел:

1. ISO 10017:2021 Quality management – Guidance on statistical techniques for ISO 9001:2015.

2. Мощенко І. О., Нікітенко О. М., Козлов Ю. В. Візуалізація інструментів контролю якості циклу PDCA засобами інформаційно-комунікаційних технологій. *Збірник наукових праць ОДАТРЯ*. 2022. № 1 (20). С. 6–15.

УДК 621.317:34 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.217

ЗАКОНОДАВЧІ АСПЕКТИ ОЦІНКИ ВІДПОВІДНОСТІ ЗАСОБІВ ВИМІРЮВАЛЬНОЇ ТЕХНІКИ

Кондратенко В.О.
Науковий керівник – к.т.н., доц. Штефан Н. В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
e-mail: vadym.kondratenko@nure.ua

The purpose of the work is to reduce the risk of violation of the requirements of technical regulations and legislation of Ukraine on metrology and metrological activities during release from production and providing measuring equipment on the market. The existing contradictions in technical regulations are considered, which allow manufacturers of measuring equipment or their authorized representatives (including importers) to violate the requirements of technical regulations. Proposed to consider and recognize existing contradictions as a risk of violation of the requirements of the legislation of Ukraine on metrology and metrological activities, a method for minimizing these risks is proposed.

Відповідно до Закону України «Про технічні регламенти та оцінку відповідності» *оцінка відповідності* - процес доказу того, що певні вимоги щодо продукції, процесу, послуги, системи, особи або органу були виконані; *технічний регламент* - нормативно-правовий акт, в якому визначено характеристики продукції або пов'язані з ними процеси та методи виробництва, включаючи відповідні адміністративні положення, додержання яких є обов'язковим; *суб'єкти господарювання* - виробники, уповноважені представники, імпортери та розповсюджувачі, а відповідно до деяких технічних регламентів - також інші фізичні та юридичні особи. Згідно п.1 статті 16 Закону України «Про метрологію та метрологічну діяльність» оцінка відповідності законодавчо регульованих засобів вимірювальної техніки вимогам технічних регламентів проводиться у разі, коли це передбачено відповідними технічними регламентами. Наразі маємо три технічних регламента щодо засобів вимірювальної техніки:

1. Технічний регламент законодавчо регульованих засобів вимірювальної техніки. Цей регламент встановлює вимоги, яким повинні відповідати засоби вимірювальної техніки (ЗВТ), *які призначені* для застосування у сфері законодавчо регульованої метрології, коли вони надаються на ринку та/або вводяться в експлуатацію для виконання завдань, пов'язаних з вимірюваннями. Дія цього Технічного регламенту поширюється на ЗВТ, перелік яких наведено у додатку 1 цього регламенту;
2. Технічний регламент засобів вимірювальної техніки. Цей Технічний регламент встановлює вимоги до ЗВТ та його дія поширюється на засоби вимірювальної техніки, зазначені у додатках 3-12 цього регламенту;
3. Технічний регламент щодо неавтоматичних зважувальних приладів.

Дія цього Технічного регламенту поширюється на всі неавтоматичні зважувальні прилади, які поділені на 7 категорій застосування (зазначені у підпунктах 1-7 пункту 2 цього регламенту).

На ринку України можуть надаватися тільки прилади, які відповідають вимогам зазначених Технічних регламентів, навіть показ та/або демонстрація ЗВТ, які не відповідають вимогам Технічного регламенту, під час проведення ярмарків, виставок, показів чи демонстрації в інший спосіб є можливими за умови, якщо у видимому позначенні буде чітко зазначено, що такі засоби вимірювальної техніки не можуть бути надані на ринку та/або введені в експлуатацію до приведення їх у відповідність з вимогами Технічних регламентів (стосується регламентів зазначених у п.1, п.2).

Технічний регламент щодо неавтоматичних зважувальних приладів (п.3) зобов'язує виробників ще на етапі проектування та виготовлення приладів (зазначених у підпунктах 1-6 пункту 2 регламенту) забезпечувати їх відповідність суттєвим вимогам цього Технічного регламенту, а на інші прилади (зазначені у підпункті 7 пункту 2 регламенту) які не відповідають суттєвим вимогам виробники повинні наносити видимі, чіткі символи *обмеженого використання.* Завдяки цьому та чітко розділеним категоріям застосування мінімізується ризик порушення вимог Технічного регламенту щодо неавтоматичних зважувальних приладів під час надання приладів на ринку та їх введення в експлуатацію.

Наявні протиріччя в Технічному регламенті законодавчо регульованих засобів вимірювальної техніки дозволяють суб'єктам господарювання порушувати вимоги законодавства з відомої причини - комерційна вигода. Запропоновано розглянути та визнати наявні протиріччя як такі, що підвищують ризик порушення вимог законодавства України про метрологію та метрологічну діяльність, та спосіб мінімізації цих ризиків.

Протиріччя в Технічному регламенті законодавчо регульованих засобів вимірювальної техніки виникає з п.1 загальної частини регламенту, а саме з питання до яких ЗВТ встановлено вимоги - «… встановлює вимоги, яким повинні відповідати засоби вимірювальної техніки, *які призначені* для застосування у сфері законодавчо регульованої метрології». Якщо робиться акцент на сфері застосування (де саме буде застосовано засіб вимірювальної техніки), то поширюється дія цього регламенту на ЗВТ чи ні визначає кінцевий споживач (підприємство, організація, тощо). Виникає питання звідки виробник може знати чи буде використана його продукція у сфері законодавчо регульованої метрології чи ні, і як він може виконувати вимоги регламенту на етапах виробництва, демонстрації, наданні на ринку цієї продукції. Інша річ, якщо фразу «*які призначені* для застосування у сфері законодавчо регульованої метрології» розуміти як *теоретичну можливість* використання ЗВТ в законодавчої сфері і робити

акцент на групах ЗВТ, призначених для застосування у сфері законодавчо регульованої метрології, згідно Додатку 1 регламенту. У такому випадку усі ЗВТ, що належать до цих груп, незалежно від сфери їх застосування кінцевим споживачем повинні відповідати вимогам Технічного регламенту та проходити процедуру оцінки відповідності до їх надання на ринку. В такому випадку в комплекті постачання цих ЗВТ за замовчуванням повинна бути Декларація відповідності, яка підтверджує відповідність ЗВТ вимогам технічного регламенту.

У зв'язку з наявними фактами надання на ринку України ЗВТ, що не відповідають вимогам Технічного регламенту законодавчо регульованих засобів вимірювальної техніки, але відносяться до груп ЗВТ, які зазначені у переліку Додатка 1 цього регламенту, сфера дії Технічного регламенту законодавчо регульованих засобів вимірювальної техніки потребує уточнення. Ці уточнення повинні чітко встановлювати необхідність ЗВТ відповідати вимогам технічного регламенту незалежно від сфери застосування цих ЗВТ кінцевим споживачем.

Згідно вимог Закону України «Про метрологію та метрологічну діяльність» та постанови Кабінету Міністрів України від 4 червня 2015 року № 374 «Про затвердження переліку категорій законодавчо регульованих засобів вимірювальної техніки, що підлягають періодичній повірці» кінцевий споживач в залежності від сфери використання ЗВТ організовує виконання повірки чи калібрування, а необхідність наявності в комплекті постачання ЗВТ Декларації відповідності повинна встановлюватись технічним регламентом.

Список використаних джерел:

1. Закон України «Про технічні регламенти та оцінку відповідності», Відомості Верховної Ради (ВВР). 2015. URL: https://zakon.rada.gov.ua/laws/show/124-19#Text (дата звернення 15.02.2024).
2. Закон України «Про метрологію та метрологічну діяльність», Відомості Верховної Ради (ВВР). 2014. URL: https://zakon.rada.gov.ua/laws/show/1314-18#Text (дата звернення 15.02.2024).
3. Технічний регламент засобів вимірювальної техніки, затверджено постановою Кабінету Міністрів України від 24.02.2016 № 163 [Текст] // Офіційний вісник України. – 2016 – № 21. 89 с.
4. Технічний регламент щодо неавтоматичних зважувальних приладів, затверджено постановою Кабінету Міністрів України від 16.12.2015 № 1062 [Текст] // Офіційний вісник України. – 2015 – № 102. 103 с.
5. Перелік категорій законодавчо регульованих засобів вимірювальної техніки, що підлягають періодичній повірці, затверджено постановою Кабінету Міністрів України від 04.06.2015 № 374 [Текст] // Офіційний вісник України. – 2015 – № 46. 150 с.

УДК 006.91:622.691 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.220

САМОДІАГНОСТУВАННЯ ВИТРАТОМІРА НА БАЗІ МЕТОДУ ЗМІННОГО ПЕРЕПАДУ ТИСКУ ПІД ЧАС ВИЗНАЧЕННЯ ВИТРАТИ ПРИРОДНОГО ГАЗУ

Луценко В.О., Пономарьов Ю.В., Протас С.О.
Інститут транспорту газу, м. Харків, Україна
lutcenko-va@utg.ua, ponomarev-yv@utg.ua, protas-sa@utg.ua

The purpose of this communication is to present a methodology for self-diagnosis of a flowmeter based on the method of variable differential pressure under operating conditions of Ukrainian gas networks, which have mostly non-stationary modes of gas flows in pipelines. The implementation of this methodology will reduce operating costs by switching to preventive maintenance of the flowmeter based on the variable differential pressure method, taking into account the risks of metrological failures.

Вступ

В Україні для обліку природного газу під час його транспортування, розподілу газопроводами та закачування/відбирання (зберігання) у підземні сховищах газу широко застосовним є метод змінного перепаду тиску (МЗПТ) завдяки своїй простоті, надійності та дешевизні. Принципи роботи витратоміра на базі МЗПТ досить легкий в розумінні та завдяки довгій історії експлуатації добре описаний, зокрема у нормативних документах.

Проте традиційно існує думка, що витратомір на базі МЗПТ не має можливості самодіагностування і тільки перехід на ультразвукову технологію може спростити такий недолік. Та це безумовно хибна думка.

У 2008 та 2009 роках було запропоновано загальну методологію самодіагностування витратоміра на базі МЗПТ [1], яку було практично підтверджено в ході експериментальних випробувань. Результати цих випробувань стали основою комплексної методології перевірки, що дозволяє зменшити експлуатаційні ризики та досягти більшої достовірності результатів вимірювання витратоміра на базі МЗПТ.

Метою цього повідомлення є викладення методики самодіагностування витратоміра на базі МЗПТ в умовах експлуатації українськими газовими мережами. Упровадження цієї методології дасть змогу зменшити експлуатаційні витрати за рахунок переходу до профілактичного обслуговування витратоміра на базі МЗПТ із урахуванням ризиків від метрологічних відмов.

Класичні принципи роботи витратоміра на базі МЗПТ і принципи самодіагностування

На рисунку 1 подано схему підключення витратоміра на базі МЗПТ, що має можливість самодіагностування в режимі реального часу.

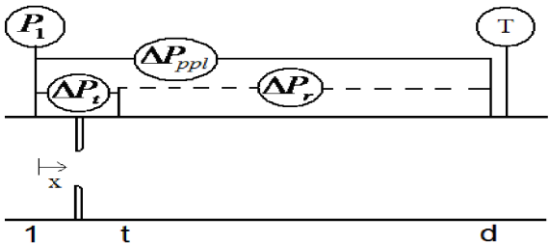


Рисунок 1 – Витратомір на базі МЗПТ з ескізом підключення приладів

На рисунку 2 наведено спрощений графік зміни коливання тиску в вимірювальному трубопроводі.

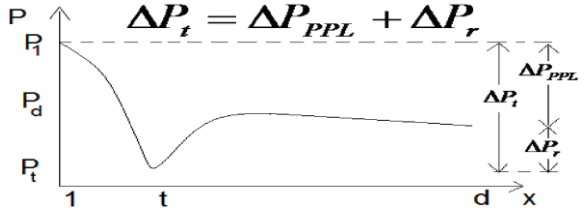


Рисунок 2 – Графік коливання тиску після витратоміра на базі МЗПТ

У разі застосування класичного витратоміра на базі МЗПТ зчитують вхідний тиск P_1 із перерізу 1, безпосередньо перед витратоміром, а також перепад тиску ΔP_t між вхідним тиском і тиском, безпосередньо після витратоміра в точці низького тиску t. Вимірювальний перетворювач температури установлюють нижче за потоком на відстані $2D$ від діафрагми.

Крім того, у витратомірі на базі МЗПТ установлюють давач тиску в точці d, розташованій далі за потоком від діафрагми. Це важливе доповнення в конструкції витратоміра на базі МЗПТ із метою вимірювання двох додаткових перепадів тиску, тобто перепад тиску між відводами тиску на виході (d) і низького тиску (t). Цей перепад тиску характеризує постійну втрату тиску (permanent pressure loss (PPL)),ΔP_{PPL}. Додавання двох додаткових вимірювань у витратомірі на базі МЗПТ дає інформацію про повний профіль тиску після витратоміра у вимірювальному трубопроводі.

Перше перевірення працездатності витратоміра на базі МЗПТ здійснюють перевіркою його цілісності за таким рівнянням:

$$\Delta P_t = \Delta P_r + \Delta P_{PPL} \qquad (1)$$

Кожне з трьох значень перепадів тиску дає змогу використовувати їх для незалежного визначення прогнозного значення витрати.

Класичний вузол обліку газу на базі МЗПТ – це один витратомір.

Відповідно до запропонованої методики кожен витратомір на базі МЗПТ розглядають як три послідовно з'єднаних витратоміра.

У такому випадку одна й та ж витрата газу має три значення для одного і того ж вимірювального трубопроводу, а це означає, що їх можна порівнювати, тобто ми маємо діагностичну систему.

Для кожної конструкції витратоміра на базі МЗПТ можна обрати прийнятну максимальну різницю між двома значеннями витрати.

Діагностична система передбачає порівняння результатів між:

– між класичним витратоміром на базі МЗПТ і витратоміром PPL;

– між класичним витратоміром на базі МЗПТ і витратоміром розширення;

– між витратоміром розширення і витратоміром PPL.

Загальне правило діагностування має такий вигляд:

– якщо фактична різниця менша допустимої різниці (тобто їхнє відношення менше або дорівнює 1), то несправність витратоміра не виявлено, а якщо більша за 1, то витратомір несправний.

Для практичного використання, коли необов'язково знати тонкощі діагностування, результати зручно відображати на так званому діагностичному блоці.

Таким чином, якщо всі точки знаходяться всередині діагностичного блока або на його границі, то під час обслуговування витратоміра на базі МЗПТ немає проблем вимірювання і таким результатам можна довіряти. В іншому випадку, якщо одна або кілька точок виходять за межі діагностичного блока, таким результатам вимірювання витрати газу не можна довіряти. Чим більше віддалені від діагностичного блоку точки, тим більша невизначеність вимірювання й більш значна похибка [2,3,4].

Список використаних джерел:

1. Steven, R. Diagnostic Methodologies for Generic Differential Pressure Flow Meters, North Sea Flow Measurement Workshop October 2008, St Andrews, Scotland, UK.

2. Degtiarov, O.V., Development of point method for measuring magnetic characteristics of technical object [Text] / Sclyarov V.V., Zaporozhets O.V. // 33nd International scientific symposium “Metrology and Metrology Assurance (MMA-2023), 7th-11th September 2023, Sozopol, Bulgaria. (conference paper) (scopus) https://ieeexplore.ieee.org/document/10317931.

3. Degtiarov, O.V., Utilizing of Univariate Analysis of Variance for Evaluation of Uncertainties Measurement Results of Properties of Reference Materials / Sclyarov V.V., Zaporozhets O.V. // 32nd International scientific symposium “Metrology and Metrology Assurance (MMA-2022), 7th-11th September 2022, Sozopol, Bulgaria. (conference paper) (scopus) DOI: 10.1109/MMA55579.2022.9992863.

4. OV Degtiarov, RS Alrawashdeh Development of the theoretical basis of magnetic measurement uncertainty evaluation // 2019 IEEE 8th International Conference on Advanced Optoelectronics and Lasers (CAOL), 2019/9/6, P. 671-674.

УДК 621.317:53.08]:006.91 **DOI** https://doi.org/10.30837/IYF.PDICIMT.2024.223

ОЦІНКА НЕВИЗНАЧЕНОСТІ ВИМІРЮВАНЬ ПРИ КАЛІБРУВАННІ МІРНИКІВ ЕТАЛОННИХ

Новосьолов О.А.
Науковий керівник – д.т.н., проф. Захаров І.П.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: oleh.novosolov@nure.ua

The problem of calibration of working standards used during the verification of measuring equipment, which are in operation and used in the field of legally regulated metrology, is considered. The procedure for estimating the uncertainty of measurements when calibrating a standard 2-digit meter using the volumetric method is described - recording the measurement model, estimating the input and measured values, estimating the standard uncertainties of the input and measured values, and estimating the extended uncertainty. The measurement uncertainty budget was drawn up.

Однією з умов забезпечення єдності вимірювань є відповідність будь-якого засобу вимірювальної техніки усім вимогам відповідних нормативно-технічних документів.

Відповідно до другої частини статті 27 Закону України «Про метрологію та метрологічну діяльність» [1] (далі – Закон), Міністерство розвитку економіки України своїм наказом від 10.08.2020 за номером № 1518 «Про затвердження Порядку калібрування вторинних та робочих еталонів» [2] (далі – Порядок) затвердило порядок калібрування вторинних та робочих еталонів. Цей Порядок установлює процедуру та умови калібрування вторинних та робочих еталонів, які використовують під час повірки засобів вимірювальної техніки, що перебувають в експлуатації та застосовуються у сфері законодавчо регульованої метрології.

Згідно Порядку, калібрування робочих еталонів повинно проводитися за методиками калібрування, які містяться в національних стандартах або розроблені виконавцями з урахуванням національних стандартів, гармонізованих з відповідними міжнародними та європейськими стандартами, та документів, прийнятих міжнародними та регіональними організаціями з метрології. Наразі, калібрування робочих еталонів здійснюють акредитовані Національним агентством з акредитації України калібрувальні лабораторії та наукові метрологічні центри, які мають документально підтверджену простежуваність своїх еталонів до національних еталонів, еталонів інших держав або міжнародних еталонів відповідних одиниць вимірювання.

Порядок проведення повірки законодавчо регульованих засобів вимірювальної техніки (далі – ЗР ЗВТ), регламентовано наказом Міністерства економічного розвитку України від 08.02.2016 року за

номером № 193 «Про затвердження Порядку проведення повірки законодавчо регульованих засобів вимірювальної техніки, що перебувають в експлуатації, та оформлення її результатів», в якому встановлена вимога щодо відношення розширеної невизначеності (за довірчої ймовірності 95 %) значення величини, яку відтворює або вимірює еталон, до максимально допустимої похибки ЗР ЗВТ, що підлягає повірці, та яка має бути не більше ніж один до трьох.

На сьогоднішній день, калібрування робочих еталонів відбувається за методиками калібрування розробленими самими виконавцями, які проводять калібрування та оцінюють невизначеність вимірювань за своїм розумінням та на свій розсуд. Щоб переконатися в цьому, досить ознайомитися зі «Сферами акредитації» калібрувальних лабораторій, де заявлені найкращі калібрувальні та вимірювальні можливості (Calibration and Measurement Capability) лабораторій з калібрування одного і того ж типу робочого еталона відрізняються між собою в декілька разів. Такий підхід у забезпечені єдності вимірювань, веде до хаосу у метрологічній діяльності.

Відсутність стандартизованих методик калібрування робочих еталонів не забезпечує єдності вимірювань у законодавчо регульованій сфері метрології та порушує вимоги частини третьої статті 27 Закону, тому що, калібрування та оформлення його результатів повинні проводитися відповідно до національних стандартів, гармонізованих з відповідними міжнародними та європейськими стандартами, та документів, прийнятих міжнародними та регіональними організаціями з метрології.

Відповідно до ДСТУ 8912:2019 «Метрологія. Колонки паливороздавальні для рідкого палива. Методика повірки» [3] в якості робочих еталонів для повірки такого важливого ЗР ЗВТ як колонка паливороздавальна для заправки автомобілів, застосовують мірники еталонні 2-го розряду згідно ДСТУ 7218:2011 «Мірники металеві еталонні. Методика повірки (калібрування)» [4], номінальної місткості 10, 20, 50, 100, 200, 500, 1000 л, при цьому, розширена відносна невизначеність повинна не перевищувати 0,15 %. Цю вимогу слід розуміти так, що мірник 2-го розряду, наприклад, номінальною місткістю 10 л, забезпечує вимірювання об'єму 10 л з розширеною невизначеністю не більше 0,015 л. Але, згідно того ж [4] границі основної допустимої похибки мірників 2-го розряду за температури 20 °С мають бути ± (0,05 - 0,1) %. Тобто, найбільше значення невизначеності вимірювань об'єму 10 л мірником 2-го розряду номінальною місткістю 10 л перевищує його максимально допустиму похибку як мінімум в 1,5 рази.

По-друге, максимально допустима похибка деяких типів паливороздавальних колонок складає ± 0,25 % і в цьому випадку, якщо брати до уваги найбільше значення невизначеності вимірювань 0,15 %, яке

повинен забезпечувати еталонний мірник і яке прописано у [3], необхідне співвідношення 1:3 не витримується.
Слід також зауважити, що у [4] відсутній розділ з оцінки невизначеності вимірювань при калібруванні мірників еталонних. Враховуючи обов'язковість калібрування застосовуваних при повірці робочих еталонів, зокрема мірників еталонних 2-го розряду, відсутність стандартизованої методики калібрування сприяє порушенню забезпечення єдності вимірювань в законодавчо регульованій сфері метрології, тому, [4] потребує актуалізації.
За [4] повірку мірників 2-го розряду проводять об’ємним або масовим методом, місткість мірників визначають два рази, як остаточний результат беруть середнє арифметичне отриманих значень. При калібруванні мірника 2-го розряду, для достовірного встановлення дійсного значення його місткості, кількість вимірювань повинна бути як мінімум 5 разів для можливості визначення грубих похибок і промахів при застосуванні статистичних критеріїв виділення аномальних спостережень.
В статті описано процедуру оцінювання невизначеності вимірювань під час калібрування мірника 2-го розряду об’ємним методом, який є методом прямого порівняння і може застосовуватися двома різними способами: наливанням питної води в попередньо змочений мірник з мірника 1-го розряду, як це застосовано у [4], або зливанням питної води з мірника, що калібрується, у мірник 1-го розряду.
На основі рекомендацій EA-4/02 M:2013 «Evaluation of the Uncertainty of Measurement in Calibration» [5] складено модельне рівняння вимірювань, оцінені вхідні та вимірювана величин, проведено оцінювання стандартних невизначеностей вхідних та вимірюваної величин, оцінена розширена невизначеність, складено бюджет невизначеності вимірювань.

Список використаних джерел:

1. Про метрологію та метрологічну діяльність : закон України від 05.06.2014 № 1314–VII.
2. Про затвердження Порядку калібрування вторинних та робочих еталонів : наказ Мінекономіки України № 1518 від 10.08.2020.
3. ДСТУ 8912:2019. Метрологія. Колонки паливороздавальні для рідкого палива. Методика повірки.
4 ДСТУ 7218:2011. Мірники металеві еталонні. Методика повірки (калібрування).
5. EA-4/02 M:2013. Evaluation of the Uncertainty of Measurement in Calibration. EA, 2013. 75 p.

УДК 006.015.5:664.4 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.226

АНАЛІЗ ФАКТОРІВ ВПЛИВУ НА ЯКІСТЬ ВИРОБНИЦТВА СОЛІ ЙОДОВАНОЇ ЗА МЕТОДОМ ІШІКАВИ

Сафонов О.В.
Науковий керівник – к.т.н., ст. викл. Мощенко І.О.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: oleksii.safonov2@nure.ua

This paper explores the use of Ishikawa diagrams for analyzing factors affecting the quality of iodized salt. The importance of systematic quality management of products and problem-solving during its production is emphasized. Moisture content is identified as a serious quality issue of the product under investigation, and the Ishikawa diagram helps to analyze the causes contributing to its accumulation. By addressing moisture-related issues, the quality of iodized salt can be improved, the amount of defective product can be reduced, and production efficiency can be increased to supply quality products to the consumer.

У зв'язку з інтеграцією на європейський ринок збуту, Україна повинна приділяти особливу увагу підвищенню якості своєї продукції. Висока якість продуктів харчування забезпечує не тільки відповідність стандартам та законодавчим вимогам, а й сприяє формуванню довгострокових партнерських відносин та довіри з боку споживачів. Тільки постійне покращення виробничих процесів та продукції дозволяє успішно увійти на конкурентоспроможні ринки. Йодована сіль привертає особливу увагу у контексті суворих європейських стандартів якості та безпеки у зв'язку з проблемою йододефіциту за допомогою йодованої солі за рекомендацією Всесвітньої організації охорони здоров'я (ВООЗ).

Одним з найбільш ефективним інструментом аналізу факторів впливу на якість виробництва є методологія Ішікави, технологічним засобом реалізації якої є діаграма Ішікави або причинно-наслідкова діаграма.

Діаграма Ішікави використовується для аналізу причин виникнення проблеми на виробництві, також вона відома як діаграма причин та наслідків. Вона допомагає виявити основні фактори, що впливають на негативні результати, та визначити можливі шляхи їх усунення. Переваги інструменту контролю якості: структурування інформації, виявлення кореневих причин, співпраця команди. Недоліки: обмеженість у обробці великих обсягів даних, можливість пропуску деяких факторів, залежність від якості формулювання питань.

Проаналізуємо фактори впливу на якість виробництва солі йодованої.

Сіль йодована виготовляється згідно з вимогами Закону України «Про основні принципи та вимоги до безпечності та якості харчових продуктів» та за рекомендаціями національного стандарту ДСТУ 4307:2004 Сіль йодована. Технічні умови.

Згідно з нормативною документацією показниками якості об’єкта дослідження є: запах і смак (слабкий запах йоду властивий продукту, солодкий із присмаком йодувальної добавки), масова частка оксиду заліза (III) (не більша ніж 0,040 % у перерахунку на суху речовину), масова частка вологи (не більша ніж 1,0 %), допустимий рівень вмісту токсичних речовин не більше ніж мг/кг: ртуть (0,01), миш’як (1,00), мідь (3,00), свинець (2,00), кадмій (0,10), цинк (10,00), масова частка йоду ($40 \pm 15 \cdot 10^{-4}$ %), крупність просіяна (кам’яна й осідна): крупність 1 від 0,8 мм до 1,2 мм включ., (не менша ніж 85,0 %).

Проаналізуємо фактори, які можуть викликати невідповідність показника якості «масова частка вологи» нормативним значенням за допомогою діаграми Ішікави (рис. 1).

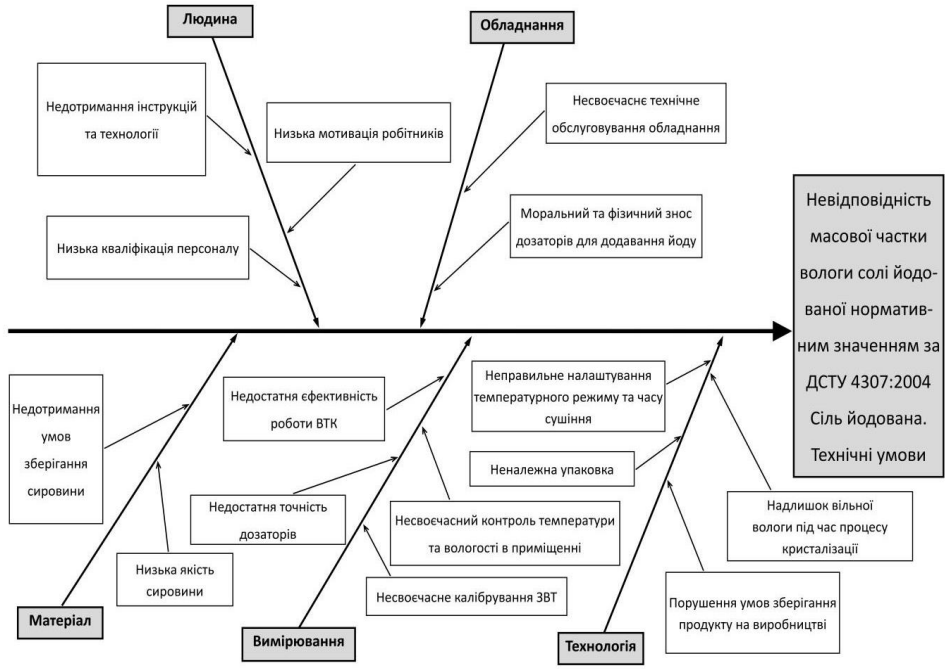


Рис. 1. Діаграма Ішікави

Для кожного фактору впливу на виникнення невідповідності показника якості продукту нормативним значенням, експертним методом визначено вагові коефіцієнти від 1 до 50 (таблиця 1).

Таблиця 1 – Вагові коефіцієнти

Причина	Оцінка в балах
Недотримання інструкцій та технології	13
Низька кваліфікація персоналу	2
Низька мотивація робітників	1
Несвоєчасне технічне обслуговування обладнання	28
Недостатня точність дозаторів	7

Моральний та фізичний знос дозаторів для додавання йоду	17
Недотримання умов зберігання сировини	6
Низька якість сировини	4
Несвоєчасне калібрування ЗВТ	5
Неправильне налаштування температурного режиму та часу сушіння	9
Несвоєчасний контроль температури та вологості в приміщенні	7
Недостатня ефективність роботи ВТК	3
Порушення умов зберігання продукту на виробництві	48
Надлишок вільної вологи під час процесу кристалізації	10
Неналежна упаковка	15

З експертного аналізу діаграми Ішікави можна зробити висновок, що найбільший вплив на появу дефектних виробів здійснюють фактори з найбільшими ваговими коефіцієнтами, а саме: порушення умов зберігання продукту на виробництві, несвоєчасне технічне обслуговування обладнання та моральний та фізичний знос дозаторів для додавання йоду, тобто фактори, пов’язані з технологією організації процесу виробництва солі йодованої та її контролем. Тому під час виробництва солі йодованої потрібно особливо увагу звернути на контроль визначених процесів та своєчасно впроваджувати заходи щодо їх стабілізації в разі виявлення відхилень показників від номінальних значень.

Список використаних джерел:

1. Нікітенко О. М. Сучасні інструменти управління якістю /О. М. Нікітенко, А. Б. Єгоров, Н. В. Штефан [Електронний ресурс]. Харків : ХНУРЕ, 2019. 245 с.

2. Мощенко І.О., Нікітенко О.М., Козлов Ю.В. Візуалізація інструментів контролю якості циклу PDCA засобами інформаційно-комунікаційних технологій. Збірник наукових праць ОДАТРЯ. № 1(20). 2022. С. 6-15.

УДК 004.43:006 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.229

СУЧАСНІ ТЕНДЕНЦІЇ У ВИКОРИСТАННІ МОВ ПРОГРАМУВАННЯ ДЛЯ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ В МЕТРОЛОГІЇ

Юношев Д.Є.
Науковий керівник – к.т.н, доц. Штефан Н.В.
Харківський національний університет радіоелектроніки, каф. ІВТ
м. Харків, Україна
e-mail: dmytro.yunoshev@nure.ua

In the modern world, metrology has become an increasingly important field as accuracy and measurement impact various aspects of our lives, including science, industry and technology. Metrology software development plays a key role in ensuring accurate and reliable measurements. This raises the question of choosing programming languages to create highly efficient and innovative solutions. The dissertation examines current trends in the use of programming languages for software development in metrology and their impact on the productivity and development of this industry.

Метрологія, як наука про вимірювання та вимірювальні засоби, набуває все більшої важливості в різних галузях, починаючи від промисловості та закінчуючи науковими дослідженнями. Забезпечення точності та надійності вимірювань у метрології має вирішальне значення для гарантії якості продукції, безпеки, та наукових висновків. Мови програмування в контексті розрахунків в метрології виходять на перший план оскільки надають точність та швидкість обробки великих обсягів даних.

Програмування в сфері метрології сприяє автоматизації вимірювань, оскільки забезпечує повторюваність та усуває людський фактор при розрахунку вимірювань. Автоматизовані системи дозволяють виконувати вимірювання швидше та ефективніше, а також знижують ймовірність виникнення помилок.

Програмування в метрології дозволяє виконувати та розв’язувати наступні задачі [1]:

- обробка та аналіз даних вимірювань;
- керування вимірювальним обладнанням;
- автоматизація вимірювань;
- обробка та виведення результатів;
- забезпечення відслідковуваноті та перевірки.

Для демонстрації автоматизованого розрахунку в метрологічних цілях можна привести приклад розрахунку стандартної невизначеності типу А для результатів багаторазових вимірювань згасання атенюатора [2].

Для демонстрації цієї задачі були визначені значення згасання атенюатора [табл. 1.]

Таблиця 1. Значення згасання атенюатора

Вимірювальна величина	Результати вимірювання, дБ			
	A_1	A_2	A_3	A_4
A	34,55	34,56	34,54	34,53

Для обчислення даних значень використовувалась мова програмування Python версії 3.13 з використанням бібліотеки NumPy для визначення вибіркового стандартного відхилення та квадратного кореня. [рис. 1.]

```python
import numpy as np

data = [34.55, 34.56, 34.54, 34.53]
measurement_data = np.array(data)

def calc_type_a(data):
    # Вибіркове стандартне відхилення
    standard_care = np.std(data, ddof=1)
    # Кількість вимірювань
    n = len(data)
    # Обчислення стандартної невизначеності типу A
    uncertainty_type_A = standard_care / np.sqrt(n)

    return uncertainty_type_A

result = calc_type_a(measurement_data)
print(f'Стандартне відхилення типу A: {calc_type_a(data)}')
```

Рисунок 1 – Алгоритм розрахунку стандартної невизначеності типу А для результатів багаторазових вимірювань згасання атенюатора

В даному випадку визначення стандартної невизначеності розрахується коректно [рис. 2.] [3].

```
Стандартне відхилення типу A: 0.00645497224367912
```

Рисунок 2 – Результат алгоритму

Автоматизація розрахунків в метрології відіграє важливу роль у підвищенні ефективності та точності вимірювань. Використання сучасних програмних інструментів дозволяє оптимізувати процеси обробки даних, спрощує взаємодію з вимірювальним обладнанням та сприяє стандартизації в метрологічних вимірах.

Список використаних джерел:

1. Клименко О. Ф., Шарапов О. Д., Головко Н. Р. Інформатика та комп’ютерна техніка. Київ, 2005. 276 с.

2. Захаров И. П. Теория неопределенности в измерениях : учеб. пособ. [для студ. высш. учеб. зав.]. Харьков : Консум, 2002. 137 с.

3. Василевський О. М. Алгоритм оцінювання невизначеності у вимірюваннях при виконанні метрологічних робіт // Інформаційні технології та комп’ютерна інженерія. 2006. № 3 (7). С. 56.

УДК 006.015.5:005.334 DOI https://doi.org/10.30837/IYF.PDICIMT.2024.231

ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ МЕТОДОЛОГІЇ МЕНЕДЖМЕНТУ ЯКІСТЮ «ШІСТЬ СИГМА» ДЛЯ УПРАВЛІННЯ РИЗИКАМИ НА ВИРОБНИЦТВІ

Якимович М. В.
Науковий керівник – к.т.н., ст. викл. Мощенко І.О.
Харківський національний університет радіоелектроніки, каф. ІВТ,
м. Харків, Україна
e-mail: mykyta.iakymovych@nure.ua

This study demonstrates the application of Six Sigma methodology for risk management in manufacturing. It employs FMEA-analysis to identify, assess, and mitigate risks, enhancing production processes. Through a case study, it showcases how Six Sigma minimizes defects, improves efficiency, and optimizes resources. This integration provides a systematic framework for risk assessment, root cause analysis, and continuous improvement, leading to enhanced manufacturing outcomes.

У сучасному світі однією з ключових умов економічного зростання є виробництво конкурентоздатної продукції. Якість є вирішальним елементом конкурентоспроможності. Глобалізація економічних процесів суттєво підсилює конкуренцію вже не лише між компаніями в межах однієї країни, але й між організаціями різних держав. Розширення ринку надає покупцям можливість стати більш вимогливими до товарів, обираючи якісніші. У зв'язку з розвитком ринкової економіки, яка передбачає жорстке конкурентне середовище, актуальність проблеми якості зростає для всіх товарів і послуг.

Новою стратегічною ініціативою менеджменту якості в компаніях, що успішно розвиваються у XXI ст., є комплексна модель управління якістю «Шість сигма». «Шість сигма» – це система управління якістю, заснована на вдосконаленні процесів через пошук і виключення причин помилок або дефектів у виробничих процесах з урахуванням критично важливих для споживача вихідних параметрів, що залучає всіх співробітників від нижнього рівня до вищої ланки.

Реалізація управління бізнес-процесами за концепцією «Шість сигма» задокументована в нормативних документах ДСТУ ISO 13053-1:2016 Статистичний контроль. Кількісні методи покращення процесу. Шість Сигма. Частина 1. Методологія (ISO 13053-1:2011, IDT) та ДСТУ ISO 13053-2:2016 (ISO 13053-2:2011, IDT) Статистичний контроль. Кількісні методи покращення процесу. Шість Сигма. Частина 2. Інструменти і методи. Згідно цих стандартів при практичному впровадженні концепції «Шість сигма» на підприємстві рекомендується застосовувати такі інструменти контролю якості: методи описової статистики, діаграма Парето, матриця пріоритетів, діаграма Ганта, бенчмаркінг, діаграма

спорідненості, мозкова атака, пока-йоке, метод 5S, метод FMEA, розгортання функції якості QFD, методи Тагучі, тощо [1, 2].

Так, використання інструментів «Шість сигма» - методу FMEA та методу матриці пріоритетів – дозволяє здійснювати ефективне управління ризиками на підприємстві та вчасно впроваджувати заходи щодо запобігання виникненню потенційних дефектів.

FMEA - це метод систематичного аналізу і управління ризиками, який використовується для ідентифікації потенційних відмов, визначення їх можливих наслідків та впливу на систему або процес. Основна мета FMEA - виявлення та усунення можливих дефектів або проблем ще до того, як вони виникнуть, що дозволяє запобігти можливим втратам, покращити якість продукції, знизити ризики та підвищити ефективність виробничих процесів.

Матриця пріоритетів – інструмент якості для обробки статистичних даних, отриманих при побудові матричних діаграм, з метою виявлення пріоритетних напрямів вирішення проблемної ситуації.

Застосування методів FMEA та матриці пріоритетів для управління ризиками, які виникають під час виробництва спортивного харчування дозволило отримати наступні результати (табл. 1, 2).

Таблиця 1 – FMEA-аналіз

Потенційний дефект	Наслідки потенційного дефекту	S	Потенційна причина	O	Методи виявлення дефекту	D	ПЧР
Невідповідність сировинних матеріалів нормативним значенням	Погіршення якості продукції та безпеки споживачів	10	Контамінація сировини або використання неякісних сировинних матеріалів	2	Аналіз сировини, мікробіологічний моніторинг	7	140
Порушення умов виробничого процесу	Зниження поживної цінності, можливість виникнення шкідливих речовин	6	Неправильне вимішування інгредієнтів, некоректне термічне оброблення	4	Візуально	3	72
Некоректне маркування	Неправильне використання продукту, алергічні реакції	10	Неправильне маркування або відсутність інформації для споживачів	3	Візуально	3	60

За результатами FMEA-аналізу найбільше значення Пріоритетного числа ризику (ПЧР) отримано для дефекту «Невідповідність сировинних матеріалів нормативним значенням».

Експертною групою для запобігання виникнення цього дефекту було запропоновано впровадження наступних заходів: (1) впровадження системи контролю якості, (2) навчання персоналу, (3) стратегічне

партнерство з постачальниками сировини, (4) постійне вдосконалення процесів, (5) автоматизація виробництва. Визначено критерії для оцінювання пріоритетності рішень: (1) працемісткість не перевищує 50 люд/год, (2) вартість реалізації рішення не перевищує 20000 грн, (3) залучена кількість персоналу не більше 30 осіб, (4) зниження витрат на брак не менше ніж в 1,5 рази. Визначаємо пріоритетність кожного рішення за методологією матриці пріоритетів (табл. 2).

Таблиця 2 – Матриця пріоритетів

Рішення	Критерії			
	працемісткість не перевищує 50 люд/год	вартість реалізації рішення не перевищує 20000 грн	залучена кількість персоналу не більше 30 осіб	зниження витрат на брак не менше ніж в 1,5 рази
	Коефіцієнт: 1	Коефіцієнт: 3	Коефіцієнт: 9	Коефіцієнт: 9
впровадження сис-теми контролю якості	9	3	27	27
навчання персоналу	1	3	27	81
стратегічне партнер-ство з постачаль-никами сировини	1	27	9	9
постійне вдоско-налення процесів	9	3	27	81
автоматизація виробництва	9	3	81	9

Розподіляємо рішення в порядку пріоритетності: 120 – постійне вдосконалення процесів; 112 – навчання персоналу; 102 – автоматизація виробництва; 66 – впровадження системи контролю якості; 46 – стратегічне партнерство з постачальниками сировини.

Висновки: За результатами застосування методів «Шість сигма» для управління ризиками під час виробництва спортивного харчування були виокремлені найбільш значущі ризики та запропоновані ранжовані за пріоритетністю заходи щодо їх мінімізації.

Список використаних джерел:

1. ДСТУ ISO 13053-1:2016 Статистичний контроль. Кількісні методи покращення процесу. Шість Сигма. Частина 1. Методологія.

2. ДСТУ ISO 13053-2:2016 (ISO 13053-2:2011, IDT) Статистичний контроль. Кількісні методи покращення процесу. Шість Сигма. Частина 2. Інструменти і методи.

3. Нікітенко О.М., Єгоров А.Б., Штефан Н.В. Сучасні інструменти управління якістю. Харків: ХНУРЕ, 2019. 245 с.

АЛФАВІТНИЙ ПЕРЕЛІК

ЗМІСТ

ДЛЯ НОТАТКІВ

«РАДІОЕЛЕТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ»

МАТЕРІАЛИ 28-го МІЖНАРОДНОГО МОЛОДІЖНОГО ФОРУМУ

Відповідальний за випуск: А.В. Снігуров

Комп'ютерна верстка О.І. Ільїна

Матеріали збірника публікуються в авторському варіанті без редагування

Підп. до друку _____2024 Формат 60x84 1/16 Спосіб друку - ризографія
Умов. друк. арк. _____ Тираж _____ прим.
Зам. No __-____. Ціна договірна

ХНУРЕ. Україна. 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ

61166, Харків, просп. Науки, 14

Матеріали XXVIII Міжнародного молодіжного форуму

«Радіоелектроніка та молодь у XXI столітті»

Харківський національний університет радіоелектроніки