

# НПК МНІС ІП-2020

ЗБІРНИК НАУКОВИХ ПРАЦЬ  
МОЛОДИХ  
НАУКОВЦІВ І СТУДЕНТІВ

ЧАСТИНА 1



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Хмельницький національний університет

Військовий інститут Київського національного університету  
ім.Тараса Шевченка

ПВНЗ “Університет економіки і підприємництва”

Вінницький національний технічний університет

Західноукраїнський національний університет

## **Інтелектуальний потенціал - 2020**

збірник наукових праць молодих науковців і студентів

сформовано за матеріалами  
Всеукраїнської науково-практичної конференції  
молодих науковців і студентів  
«Інтелектуальний потенціал – 2020»

9-10 листопада 2020 р.

Частина 1

Хмельницький  
2020

ББК 74.480.278

С.88

«Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020.  
– Частина 1. – 104 с.

***Відповідальний редактор: Желавська Н.В.***

***Відповідальний за випуск: Чешун В.М.***

***Редакційна колегія:***

*Ленков С.В. (ВІКНУ)*

*Яцків В.В. (ЗУНУ)*

*Якименко І.З. (ЗУНУ)*

*Желавський О.Б. (ПВНЗ УЕП)*

*Желавська Н.В. (ПВНЗ УЕП)*

*Кльоц Ю.П. (ХНУ)*

*Чешун В.М. (ХНУ)*

*Тимофєєва Л.В. (ХНУ)*

## ЗМІСТ

Білаш О. Ю., Пятін І.С. <b>Модель визначення спектральної густини потужності сигналу на антені</b> .....	5
Біндер Т. С., Пятін І.С. <b>Модель цифрової системи зв'язку з завадостійким згортковим кодуванням</b> .....	8
Гадомський А.В., Таранчук А.А. <b>Метод моніторингу мережі WLAN WI-FI</b>	11
Горбань В.В. Таранчук А.А. <b>Високошвидкісна локальна корпоративна мережа з послугою VoIP – телефонії</b> .....	14
Данілова Л.В., Лавров Є.А., Токар А.С. <b>Оптимізація діалогової людино-машинної взаємодії в комп'ютерних системах</b> .....	18
Єрмаков М. С., Борисенко О.А. <b>Завадостійкий біноміальний таймер</b> .....	21
Казімірко А.О., Таранчук А.А. <b>Аналіз механізмів захисту мережевого устаткування від хакерської атаки типу TCP SYN Flood</b> .....	23
Ковальчук О.Л., Кучерявий Є.І., Таранчук А.А. <b>Модель «розумної» мережі енергопостачання житлового будинку</b> .....	26
Красильников С.Р. <b>Зміст курсу «Комп'ютерний практикум» у професійній підготовці фахівців спеціальності 015.20 «Професійна освіта. Транспорт»</b> .....	30
Крикун Є. О., Підченко С.К. <b>Технологія побудови сенсорної мережі IoT з використанням протоколу LoRaWAN</b> .....	32
Кубатий Н. О., Таранчук А.А. <b>Пропускна здатність мережі голосової IP-телефонії</b> .....	35
Локазюк В.Ю., Медзатий Д.М. <b>Розробка системи відкритого світу в Unreal Engine 4</b> .....	39
Маниленко М.П., Полікаровських О.І. <b>Обчислювальний метод формування вихідного сигналу синтезатора високих частот</b> .....	42
Матюк Д.С., Мишко О.Є., Деркач М.В. <b>Вплив температури повітря на точність локалізації мобільного робота</b> .....	46
Мельник О. Д., Журавська І. М. <b>Використання технології розпізнавання образів для автоматизації обліку показників побутових лічильників енергії</b> .....	49
Михальський В.М, Полікаровських О.І. <b>Метод нейромережевого керування системою адаптивного радіозв'язку Software Defined Radio</b>	53
Ніколайчук І.А., Пятін І.С. <b>Моделювання транспортного каналу з полярними кодами для мобільного зв'язку п'ятого покоління</b> .....	57

<b>Джулій А.В., Огневий О.В. Проблема верифікації протоколів когерентності пам'яті .....</b>	<b>60</b>
<b>Огневий О.В., Огнева А.М., Капустян М.В. Особливості захисту інформаційних ресурсів під час проведення відеоконференцзв'язку.....</b>	<b>64</b>
<b>Полянчикін В. Г., Гнезділов М. Д., Журавська І. М. Діагностично-тренувальні прилади для відновлення рефлексів ушкоджених кістей та пальців рук.....</b>	<b>69</b>
<b>Руденко І.В. Інформаційна технологія для класифікації марок автомобілів з використанням згорткової нейронної мережі.....</b>	<b>72</b>
<b>Слободян М.О., Бабій Д.Р., Підченко С.К. Моделювання хаотичного генератора Лоренца засобами Matlab/Simulink .....</b>	<b>76</b>
<b>Слюсарчук О.О., Підченко С.К. Математична модель багаточастотної автоколивальної системи як динамічного об'єкта .....</b>	<b>77</b>
<b>Тогоєв О. Р. Організація захисту інфраструктури електронної комерції на базі протоколів DoT та DoH .....</b>	<b>82</b>
<b>Трач Б.В., Підченко С.К. Моделювання систем зв'язку з OFDM модуляцією .....</b>	<b>85</b>
<b>Чеснюк М.В., Медзатий Д.М. Алгоритм визначення пробудження людини під час сну.....</b>	<b>90</b>
<b>Шпірук М. С., Пятін І.С. Моделювання спотворень сигналу у каналі передачі і їх впливу на коефіцієнт бітових помилок цифрової системи зв'язку .....</b>	<b>93</b>
<b>Яшина О.М., Прейзнер Є.Е. Продукційна модель експертної системи для вибору оптимального раціону харчування.....</b>	<b>97</b>

## Модель визначення спектральної густини потужності сигналу на антені

Білаш О. Ю.

Науковий керівник – к.т.н., доц. Пятін І.С.

Хмельницький національний університет

Векторні аналізатори сигналів використовують для досліджень радіосигналів складної форми, наприклад, сигналів з цифровою квадратурною модуляцією, а також високочастотних імпульсних і нестационарних процесів. Наприклад, сигналів, що застосовуються в системах зв'язку GSM, GPRS, EDGE, WCDMA, CDMAOne і CDMA2000, а також з довільними видами модуляції. Параметри таких коливань важко оцінити за допомогою звичайних приладів. Щоб отримати вичерпні відомості про модуляції і характеристиках сигналу у часовій і частотній областях, необхідно досліджувати двокомпонентний (векторний) процес, що відображає зміни в часі амплітуди і фази вихідного сигналу. Засоби цифрової обробки сучасних векторних аналізаторів дозволяють реєструвати подібні процеси і виділяти всю інформацію про параметри прийнятого сигналу. Ці можливості заслуговують на увагу фахівців з радіоконтролю з урахуванням проблем, які виникають при аналізі сигналів сучасних систем з часовим і кодовим поділом каналів, псевдовипадковою перебудовою частоти і цифровою модуляцією. Прилади характеризуються високою точністю та швидкістю аналізу спектра, широкими можливостями апаратно- програмної взаємодії з іншими комплексами та приладами.

Аналізатори сигналів поділяються на цифрові і аналогові. Цифрові моделі користуються попитом, оскільки дозволяють відстежити зміни спектральної картини і побудувати спектрограми за весь період вимірювання. При цьому цифрові аналізатори спектра володіють необмеженими можливостями у разі обробки сигналів, що збережені в пам'яті.

За частотним діапазоном роботи прилади поділяються на:

- широкосмугові радіочастотні ;
- оптичного діапазону;
- низькочастотні.

За поданням результатів аналізу виділяють два типи приладів:

- скалярні аналізатори. Прилади використовуються для вивчення амплітудних характеристик. Їх застосовують на виробничих лініях для виявлення несправних компонентів;

- векторні аналізатори. Ці пристрої призначені для аналізу сигналів, які мають складну форму, нестационарних імпульсів і високочастотних процесів. Векторний аналізатор застосовується для дослідження амплітудних і фазових параметрів.

Аналіз параметрів радіосигналів поряд з їх виявленням становить одну з основних операцій радіоконтролю. У процесі аналізу оператор або

комп'ютерна програма визначають характеристики виявленого радіосигналу, такі як несуча частота, рівень, форма і ширина спектра, параметри модуляції тощо. Результати цих вимірювань використовуються для перевірки відповідності параметрів контрольованих систем встановленим нормам або служать вихідними даними для процедур класифікації та ідентифікації сигналів і радіосистем, в яких ці сигнали використовуються.

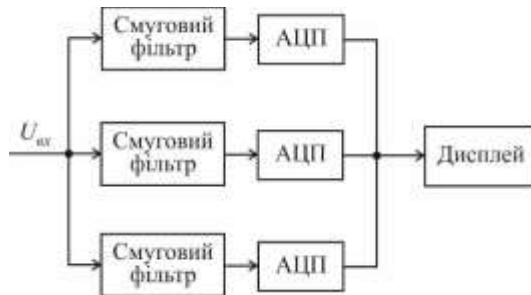
Щоб отримати детальну інформацію про прийняті сигнали, необхідно досліджувати їх поведінку в часі і виконати спектральний аналіз в частотній області. Якщо виявлений сигнал модульований, потрібно визначити вид модуляції і оцінити часові і частотні параметри модульованих сигналів.

Для вимірювання всієї сукупності параметрів системи контролю радіосигналу доводиться використовувати кілька спеціалізованих приладів: аналізатори спектру, вимірювальні приймачі та аналізатори модуляції.

У частотній області для досліджень форми спектра, вимірювання рівнів і несучих частот радіосигналів використовуються головним чином послідовні аналізатори спектра. Такий прилад формує спектральну картину послідовно в процесі перебудови керованого генератора перетворювача частоти і вимірювання рівнів на виході смугового фільтра, як показано на рис. 1, а.



а)



б)

Рисунок 1 – Структурна схема аналізаторів спектра послідовного (а) і паралельного (б) типу

Паралельний аналізатор оцінює весь спектр відразу, оскільки містить групу налаштованих на суміжні частоти смугових фільтрів (рис.1б). Оскільки

реалізація аналогової структури такого виду складна, на практиці використовується її цифровий еквівалент у вигляді ШПФ - аналізатора, який обчислює спектр за допомогою алгоритмів швидкого перетворення Фур'є (ШПФ). У порівнянні з послідовними аналоговими, цифрові паралельні ШПФ - аналізатори володіють певними перевагами: більш високою роздільною здатністю і швидкістю роботи, можливістю аналізу імпульсних і одноразових сигналів. Вони здатні обчислювати не тільки амплітудний, але і фазовий спектри, а також одночасно представляти сигнали в часовій і частотній областях. На жаль, паралельні ШПФ - аналізатори через обмежені можливості аналого- цифрових перетворювачів (АЦП) працюють тільки на відносно низьких частотах.

Основна перевага вимірювального приймача - більш висока в порівнянні з аналізатором спектру чутливість і наявність на вході смугових фільтрів (для виконання попередньої вибіркової), частота яких перебудовується, які істотно підвищують заводо захищеність в умовах щільного завантаження радіодіапазонів, характерних для задач радіоконтролю. Калібрований за коефіцієнтом підсилення і частотою тракт вимірювального приймача використовується для оцінки рівнів і частот радіосигналів і має в своєму складі декілька стандартних демодуляторів для дослідження характеристик модуляції прийнятого сигналу у часовій області. Разом з тим, можливості аналізу сигналів в частотній області у приладів цього класу, як правило, обмежені.

Аналізатори модуляції застосовуються для досліджень процесів на виходах стандартних демодуляторів. Вибираючи необхідний тип демодулятора, оператор отримує відомості про характер і параметрах зміни амплітуди, частоти або фази прийнятого сигналу.

Останнім часом у зв'язку з інтенсивним розвитком систем рухомого і супутникового радіозв'язку і широким впровадженням перспективних цифрових методів модуляції і поділу каналів, вимоги до апаратури аналізу сигналів істотно змінилися. На зміну послідовним аналізаторам спектру і панорамним приймачам з простими амплітудними і частотними демодуляторами приходять нові прилади, здатні ефективно працювати відразу в трьох областях подання радіосигналів: часовій, частотній і в області модулюючих процесів. Вони дозволяють представляти сигнал в різних ракурсах і підвищувати можливості його аналізу і виявлення похибок.

#### Перелік посилань

1. Основы метрологии и техники измерения физических величин. Учебное пособие для иностранных студентов технических специальностей в трех частях. Часть III. Методы и средства измерения параметров электрических сигналов и цепей / Д.Б. Головкин, В.В. Белозуб, В.А. Дубровский, Ю.А. Скрипник, В.И. Скрипник. Киев, КНУТД, 2002 – 120с.



2. Афонский А.А. Цифровые анализаторы спектра, сигналов и логики / А.А. Афонский, В.П. Дьяконов. - М.: Солон Пресс, 2009. - 248 с.

3. Афонский А.А. Измерительные приборы и массовые электронные измерения / А.А. Афонский, В.П. Дьяконов. - М.: Солон Пресс, 2007. - 544 с.

### **Модель цифрової системи зв'язку з завадостійким згортковим кодуванням**

Біндер Т. С.

Науковий керівник – к.т.н., доц. Пятін І.С.

Хмельницький національний університет

Завадостійким називається кодування, при якому здійснюється виявлення або виявлення та виправлення помилок в прийнятих кодових комбінаціях. Можливість завадостійкого кодування здійснюється теоремою, Шенона, згідно з якою: якщо продуктивність джерела менше пропускної здатності каналу зв'язку, то існує принаймні одна процедура кодування і декодування при якій ймовірність помилкового декодування як завгодно мала, якщо ж продуктивність джерела більше пропускної здатності каналу, то такої процедури не існує [1].

Завадостійке кодування відбувається додаванням під час передачі в корисні дані спеціальним чином структурованої надлишкової інформації (наприклад, контрольного числа), а при прийомі використання цієї надмірної інформації для виявлення і виправлення помилки. Число помилок, яке можна виправити, обмежена і залежить від конкретного застосовуваного коду.

Коди виявлення помилок (які можуть тільки встановити факт помилки) належать до тих же класів кодів, що і коди, що виправляють помилки. Фактично будь-який код, що виправляє помилки, може бути також використаний для виявлення помилок (при цьому він буде здатний виявити більше число помилок, ніж був здатний виправити). Коди, що виправляють помилки, застосовуються в системах цифрового зв'язку, в тому числі: супутникової, радіорелейної, стільникової, передачі даних по телефонних каналах, а також в системах зберігання інформації, в тому числі магнітних і оптичних. Коди, що виявляють помилки, застосовуються в мережевих протоколах різних рівнів.

За способом роботи з даними коди, що виправляють помилки, діляться на блокові, що ділять інформацію на фрагменти постійної довжини і обробляють кожен з них окремо, і згорткові, що працюють з даними як з безперервним потоком.

Згорткові коди засновані на перетворенні вхідної послідовності двійкових символів в вихідну послідовність двійкових символів, у якій на кожний символ вхідної послідовності формується більше одного символу

вихідної послідовності [2]. На відміну від блокових кодів, вони не ділять інформацію на фрагменти і працюють з нею як із суцільним потоком даних.

Згорткове кодування - це ітеративна обробка потоку бітів, що створює залежність кожного біта від кількох попередніх. Згорткове кодування задають за допомогою породжуючих поліномів, які визначають структуру двійкового кодера згорткового коду. Кодове слово на виході такого кодера складається у вигляді двох послідовностей, які у двійковій формі представляють коефіцієнти відповідних породжуючих поліномів.

Приклад згорткового кодера наведено на рис. 1. Він містить трьохрозрядний зсувний регістр, на вхід якого надходить вхідна послідовність двійкових символів. Кодер складається з 3-розрядного регістра зсуву і 2-х суматорів за модулем 2. Схема згорткового кодера для цифрового телебачення DVB-T приведена на рис. 2.

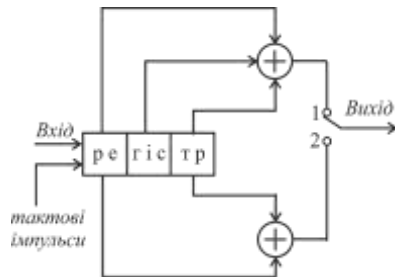


Рисунок 1 – Кодер згорткового коду швидкістю 1/2

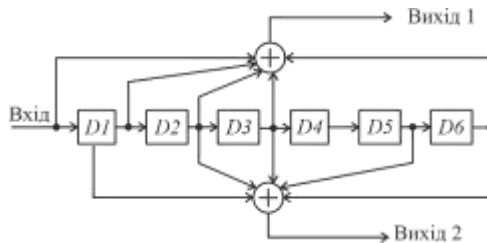


Рисунок 2 – Схема згорткового кодера цифрового телебачення DVB-T

Інформаційна послідовність надходить на вхід регістра. Вміст регістра обробляється суматорами, на виходах яких утворюється кодова послідовність, яка надходить на вихід. Відносна швидкість цього коду зменшується ( $R = 1/2$ ), а тактова частота зростає в два рази.

Розглянемо декодування згорткових кодів. Декодування реалізує алгоритм Вітербі, заснований на принципі максимальної правдоподібності (рис. 3). Алгоритм включає в себе обчислення міри подібності (або відстані

Хеммінга), між сигналами на вході декодера і на його виході. Декодер приймає рішення шляхом виключення менш ймовірних шляхів.

Згорткові коди ефективно працюють в каналі з білим шумом, але погано справляються з пакетами помилок. Більш того, якщо декодер помиляється, на його виході виникає пакет помилок, який виправляється кодом РС. Згорткові коди використовуються при низькому відношенні сигнал-шум, коли виправляючої здатності блокових кодів стає недостатньо.

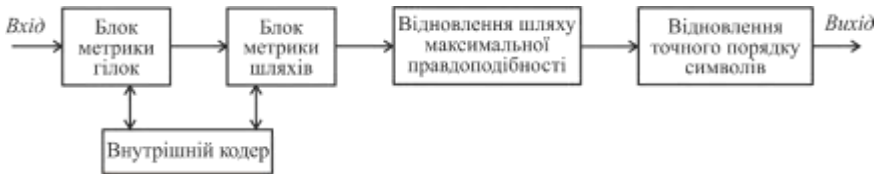


Рисунок 3 – Декодер згорткових кодів за алгоритмом Вітербі

Алгоритм оптимізований за рахунок використання особливостей структури конкретної решітки коду. Перевага декодування Вітербі в порівнянні з декодуванням за методом повного перебору полягає в тому, що складність декодера Вітербі не є функцією кількості символів в послідовності кодових слів.

Алгоритм включає в себе обчислення відстані між сигналом, отриманим в момент часу  $t_i$ , і всіма шляхами решітки, що входять в кожний стан в момент часу  $t_i$ . В алгоритмі Вітербі не розглядаються ті шляхи решітки, які, згідно з принципом максимальної правдоподібності, не можуть бути оптимальними. Якщо в один і той же стан входять два шляхи, вибирається той, який має кращу метрику; такий шлях називається виживаючим. Відбір виживаючих шляхів виконується для кожного стану. Таким чином, декодер заглиблюється в решітку, приймаючи рішення шляхом виключення менш ймовірних шляхів. Попередня відмова від малоімовірних шляхів спрощує процес декодування. Завдання відбору оптимальних шляхів можна виразити як вибір кодового слова з максимальною метрикою правдоподібності або мінімальною метрикою відстані.

На вхід декодера надходить сегмент послідовності  $r$  довжиною  $b$ , що перевищує кодову довжину блоку  $n$ . Назвемо  $b$  вікном декодування. Порівняємо всі кодові слова даного коду (в межах сегмента довжиною  $b$ ) з прийнятим словом і виберемо кодове слово, найближчим до прийнятого. Перший інформаційний кадр обраного кодового слова приймається в якості оцінки інформаційного кадру декодованого слова. Після цього в декодер вводиться  $n_0$  нових символів, а введені раніше найстаріші  $n_0$  символів скидаються, і процес повторюється для визначення наступного

інформаційного кадру. Таким чином, декодер Вітербі послідовно обробляє кадр за кадром, рухаючись по решітці, яка аналогічна використуваній кодером. У кожен момент часу декодер не знає, в якому вузлі знаходиться кодер, і не намагається його декодувати. Замість цього декодер за прийнятою послідовністю визначає найбільш правдоподібний шлях до кожного вузла і визначає відстань між кожним таким шляхом і прийнятою послідовністю. Ця відстань називається мірою розбіжності шляху. В якості оцінки прийнятої послідовності вибирається сегмент, який має найменшу міру розходження. Шлях з найменшою мірою розбіжності називається вижившим шляхом.

#### Перелік посилань

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение/ Б. Скляр. Изд. 2-е, испр.: Пер. с англ. – М. : Издательский дом «Вильямс», 2003.– 1104 с.
2. Прокис Д. Цифровая связь / Д. Прокис. Пер. с англ. под ред. Д.Д. Кловского. – М.: Радио и связь, 2000. – 800 с.
3. Банкет В. Л. Завадостійке кодування в телекомунікаційних системах: навч. посіб. з вивчення модуля 4 дисципліни ТЕЗ / В.Л. Банкет, П.В. Іващенко, М.О. Іщенко. – Одеса: ОНАЗ ім. О. С. Попова, 2011. – 100 с.

### **Метод моніторингу мережі WLAN WI-FI**

Гадомський А.В.

Науковий керівник: к.т.н. доцент Таранчук А.А.

Хмельницький національний університет

Реалізації Wi-Fi дозволяють отримати швидкість передачі даних понад 100 Мбіт/с, при цьому користувачі можуть переміщуватися між точками доступу території покриття мережі Wi-Fi, використовуючи мобільні пристрої, які оснащені клієнтськими приймально-передавальними (ПП) пристроями Wi-Fi для отримання доступу до мережі Інтернет. Наявність ПП Wi-Fi дозволяє користувачу підключитися до мутаційного шлюзу, а також підтримувати з'єднання декількох кінцевих пристроїв користувача між собою.

В сучасних умовах зростання обсягів трафіку інтернет мереж необхідно забезпечувати користувачів якісним абонентським доступом до мережі Wi-Fi та покращувати і розвивати сферу послуг.

Дальність передавання інформації залежить від потужності передавача Wi-Fi, наявності і характеристик перешкод, типу антени тощо. Ядром безпроводової мережі Wi-Fi є так звана точка доступу (англ. Access Point), яка підключається до певної наземної мережевої інфраструктури каналів Інтернет-провайдера та забезпечує передачу радіосигналу [1].

Зазвичай, точка доступу складається із приймача, передавача, інтерфейсу для підключення до проводової мережі та містить відповідне програмне забезпечення для її налаштування. Навколо точки доступу формується просторова область радіусом від 50 до 100 метрів, яку називають зоною Wi-Fi (хот-спот) і у межах якої, можна користуватися безпроводовою мережею [1].

Для того, щоб під'єднатися до точки доступу й відчути всі переваги безпроводової мережі, власнику ноутбуку або мобільного пристрою, з адаптером Wi-Fi, необхідно потрапити в радіус її дії. Усі дії з аутентифікації пристрою та налаштування мережі, більшість операційних систем персональних комп'ютерів і мобільних пристроїв виконують автоматично. Автоматичне з'єднання дозволяє комп'ютерам і портативним пристроям зв'язуватися один з одним безпосередньо за існуючим протоколом Wi-Fi без використання маршрутизаторів і точок доступу [2]. Тобто з'єднання встановлюється так само просто, як через Bluetooth. Важливим моментом є те, що для організації прямого з'єднання досить, щоб тільки один з пристроїв відповідав технології Wi-Fi Direct. Іншими словами, до сертифікованої апаратури може бути підключене будь-яке сучасне обладнання з підтримкою Wi-Fi.

При плануванні та подальшому розгортанні мереж WLAN часто використовують спеціальні програми для моніторингу. Вони дозволяють оперативно реагувати на аномальну діяльність в межах локальних мереж Wi-Fi, відслідковувати всі мережеві процеси та автоматизувати частину рутинної діяльності мережевого адміністратора. Одним з таких засобів програмних продуктів для планування та розгортання Wi-Fi мереж всередині приміщень є програмне забезпечення NetSpot Pro [3].

За допомогою програмного забезпечення (ПЗ) NetSpot Pro можна отримати розрахунки зони радіопокриття для подальшої розстановки точок доступу Wi-Fi у лабораторіях кафедри «Телекомунікацій та радіотехніки» (рисунок 1) та провести комплексну візуалізацію покриття безпроводової мережі перед її фактичним розгортанням.

ПЗ NetSpot Pro дозволяє дослідити [3]:

– відношення сигнал / шум за допомогою побудови теплової карти радіопокриття, що дозволить дослідити проблемні зони в приміщенні з низьким рівнем сигналу (рисунок 2). Причинами слабого сигналу можуть бути занадто велика відстань від Wi-Fi шлюза до кінцевого пристрою користувача, або наявність фізичних перешкод в зоні поширення сигналу між шлюзом і пристроєм;

– наявність високого рівня шуму по тепловій карті. Шум може бути викликаний електронними пристроями, безпроводовими телефонами, пристроями мережі Bluetooth та безпроводовими відеокамерами;

- перекриття каналів. Теплова карта перекриття каналів показує відношення сигнал / завада. Цей вид перешкод може викликатися іншими радіопередавачами, такими як безпроводові мережі сусідів інших мереж;
- низьку швидкість Інтернету. При активному скануванні мережі, можна виявити області з повільною швидкістю Інтернет-з'єднань.

SSID	BSSID	Area	Signal	% APs	Min	Average	Lock	Band	Channel	WDS	Vendor	Security	Mode	SSID type
4276 E	00:12:8B:49:12:12		-70	32	-82	-69	01	2.4	8	39	D-Link	Open	2	8 n/a/gn
Amn	94:08:5F:8F:00:00		-74	26	-78	-62	71	2.4	1	39		Open	2	8 n/a/gn
Amn_Ext	94:08:5F:8F:00:00		-77	22	-81	-60	74	2.4	1	39		Open	2	8 n/a/gn
Amn_Ext (2)	94:08:5F:8F:00:00		-77	22	-81	-62	74	2.4	1	39		Open	2	8 n/a/gn
Amn_Ext (3)	94:08:5F:8F:00:00		-80	18	-86	-70	78	2.4	8	39	TP-LINK	WPA2 Personal	2	8 n/a/gn
Amn_Ext (4)	94:08:5F:8F:00:00		-81	17	-86	-80	80	2.4	8	39	Motorol	Open	2	8 n/a/gn
Amn_Ext (5)	94:08:5F:8F:00:00		-81	17	-86	-80	80	2.4	8	39	Motorol	Open	2	8 n/a/gn
Amn_Ext (6)	94:08:5F:8F:00:00		-82	16	-81	-75	84	2.4	8	39	Motorol	Open	2	8 n/a/gn
Amn_Ext (7)	94:08:5F:8F:00:00		-83	15	-88	-75	84	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (8)	94:08:5F:8F:00:00		-83	15	-88	-75	84	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (9)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (10)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (11)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (12)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (13)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (14)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (15)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (16)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (17)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (18)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (19)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn
Amn_Ext (20)	94:08:5F:8F:00:00		-84	14	-89	-80	80	2.4	8	39		Open	2	8 n/a/gn

Рисунок 1- Кількість точок Wi-Fi на 2-му поверху ХНУ, які працюють на частоті 2,4 ГГц

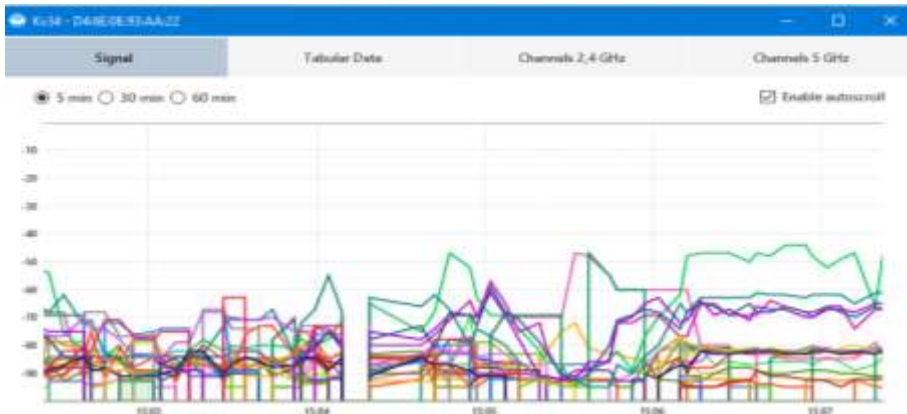


Рисунок 2 - Графік потужності сигналу прийомо-передавачів Wi-Fi

Дальність поширення радіосигналу можна розрахувати, як [1] :

$$L = 20 \log f + N \log d + P(n) - 28, (1)$$

де  $d$  - відстань в метрах;  $f$  - частота в мегагерцах;  $N$  - коефіцієнт втрати потужності сигналу за відстанню;  $n$  - кількість перешкод;  $P(n)$  - параметр втрати потужності сигналу при проходженні сигналу через перешкоди.

Модель (1) враховує втрати при багаторазовому проходженні сигналу через підлогу та стіни, що дозволяє при розгортанні мережі повторно використовувати частоти на різних поверххах будівлі.

Коефіцієнти втрати потужності  $N$  в (1), включають в неявному вигляді поправку на втрати при проходженні сигналу через стіни або через перешкоди, а також на інші механізми, що викликають втрати і виникають в межах одного поверху університету.

Використаний метод моніторингу та аудиту мережі дозволяє спроектувати і оптимізувати безпроводову мережу Wi-Fi ще на етапі її проектування, а також дозволить значно зменшити витрати на обладнання при її розгортанні або розширенні.

#### Перелік посилань

1. Горбатий І. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи / А. Бондарев, І. Горбатий // Львів: Львівська політехніка, 2016. – 336 с.
2. Павлиш В. Основи інформаційних технологій і систем. / В. Павлиш, Л. Гліненко, Н. Шаховська// Львів: Львівська політехніка, 2018. – 476 с.
3. Офіційний сайт NetSpotPRO – [Електронний ресурс] – Режим доступу: <https://www.netspotapp.com>

### **Високошвидкісна локальна корпоративна мережа з послугою VoIP – телефонії**

Горбань В.В.

Науковий керівник – к.т.н., доц. Таранчук А.А.

Хмельницький національний університет

При виборі топології мережі необхідно знайти компроміс між вартістю мережевого обладнання та його надійністю і продуктивністю, врахувати можливе розширення мережі, необхідність підключення до мережі міні-комп'ютерів або робочих станцій.

Якщо до мережі ставляться високі вимоги щодо продуктивності і надійності, рекомендується використовувати шинну топологію і метод доступу Ethernet [1]. Наявні на ринку мережеві адаптери та комутатори Ethernet забезпечують швидкість передачі від 100 Мбіт/с до 10 Гбіт/с за прийнятну вартість. Для мереж з кількістю користувачів близько двох-трьох десятків достатньо пропускної спроможності Ethernet до 100 Мбіт/с.

При проектуванні мережі слід дотримуватися ієрархічної моделі, яка має багато переваг в порівнянні з «плоскою мережею»: спрощується розуміння організації мережі, модель передбачає модульність, що означає можливість розширення мережі, простоту знаходження та локалізації проблеми, підвищення відмовостійкості за рахунок дублювання пристроїв та покладання функцій щодо забезпечення працездатності мережі на різні пристрої [1].

Побудована локальна мережа (рис. 1) розгорнута у компанії, яка має два офіси в м. Хмельницькому. Виділяється чотири групи користувачів: бухгалтерія (Б), фінансово-економічний відділ (ФЕВ), виробничо-технічний відділ (ВТВ) та інші користувачі (ІК), які розмежовані і не мають прямого доступу між собою.

Сервери віртуалізації мережі (С) входять в окрему групу і забезпечують роботу мережі під управлінням Ubuntu Linux та програмного забезпечення Asterisk - програмної телефонної станції голосової IP- телефонії [2,3].

Схеми побудованої мережі у відповідності до рівнів моделі OSI (мережевий, каналний, фізичний) [1] представлені на рисунках 1-3.

Відповідно до моделі (рис.1), мережа розбивається на три логічних рівня:

- ядро мережі (Core Layer: високопродуктивні пристрої, головне призначення – швидкий та безперебійний транспорт) забезпечує маршрутизатор 2811;

- розподільчий рівень (Distribution Layer: забезпечує застосування політик безпеки, QoS, агрегацію і маршрутизацію у VLAN, визначає широкомовні домени). На цьому рівні використаний комутатор 2960 оскільки на ньому агрегуються в загальний транк всі VLAN-мережі.

- рівень доступу (Access Layer: як правило, у якості обладнання використовують комутатори, до яких підключаються кінцеві пристрої). Комутатори 2950 будуть використовуватись в якості пристроїв доступу (Access). До них будуть підключатися кінцеві користувачі, офісна техніка, сервери.

Схема мережевого рівня (рис. 1) показує логіку маршрутизації локальних підмереж системи центральним маршрутизатором.

На схемі каналного рівня (рис. 2) показані кінцеві робочі станції користувачів, сервери та мережеве обладнання та позначені VLAN-підмережі.

Будова фізичного рівня спроектованої локальної корпоративної мережі із зазначенням портів для підключення пристроїв наведена на схемі (рис. 3).



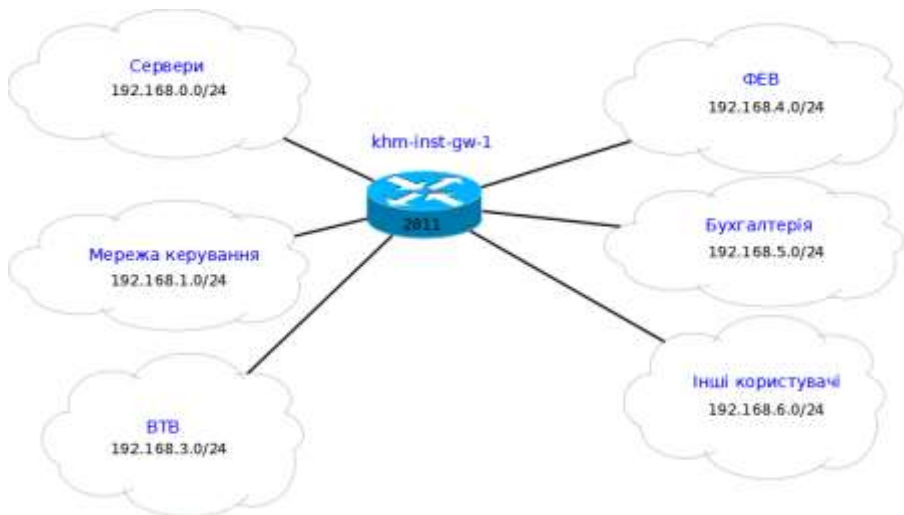


Рисунок 1 - Схема комп'ютерної мережі мережевого рівня

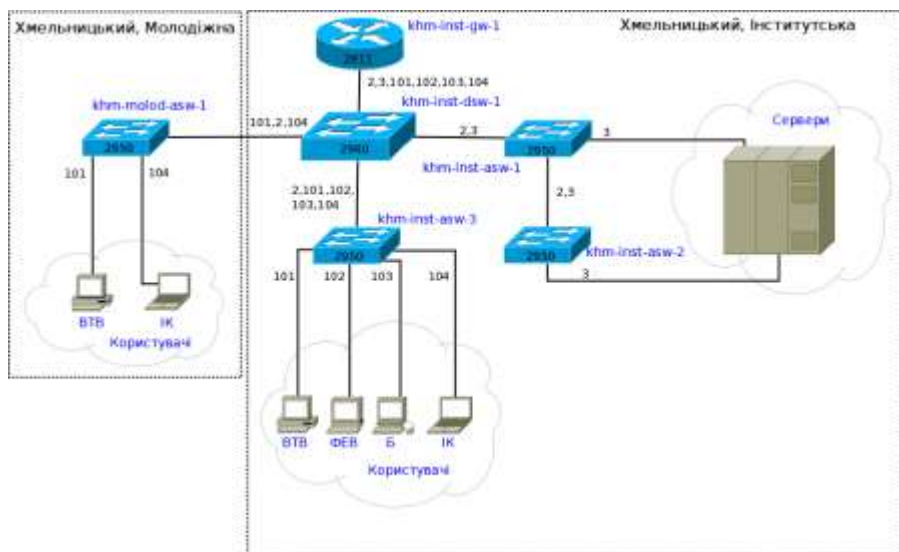


Рисунок 2 – Схема комп'ютерної мережі каналного рівня

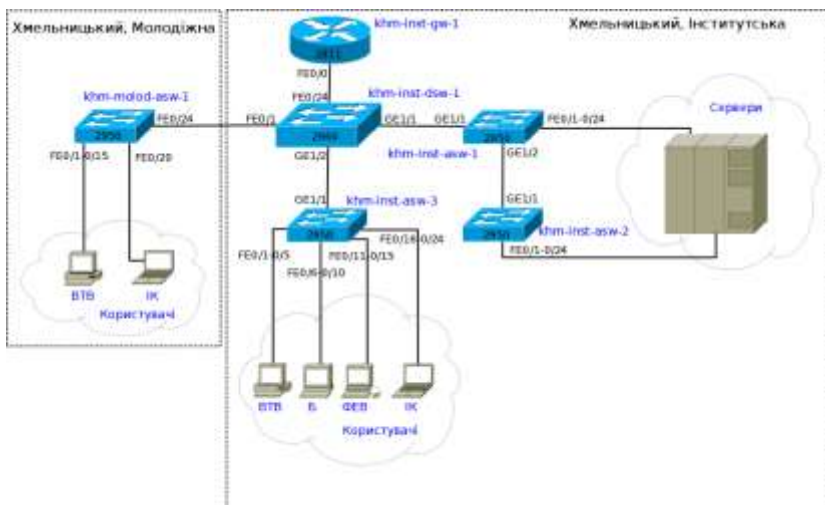


Рисунок 3 – Схема комп’ютерної мережі фізичного рівня

Кожна група пристроїв виділяється в окрему VLAN. Таким чином досягається обмеження широкомовних доменів. Також введено спеціальний VLAN для управління пристроями. Номери VLAN з 4 по 100 зарезервовані для майбутніх потреб.

При призначенні номерного поля системи IP- телефонії та схеми викликів враховані наступні вимоги: кожен працівник отримує особистий внутрішній і зовнішній телефонні номери та до трьох голосових ліній; передбачається можливість гнучкої переадресації вхідних викликів, у разі коли всі лінії абонента зайняті; можливість переходу будь-якої групи викликів у режим «Кол-центру» із застосуванням голосових меню.

Використання високоякісних телефонних з’єднань IP-телефонії призведе до економії смуги пропускання, зниження тарифів на телефонні корпоративні розмови та забезпечить високу надійність і універсальність, за рахунок використання програмного забезпечення з відкритим вихідним кодом Asterisk.

#### Перелік посилань

1. Азарова, А. О. Комп’ютерні мережі та телекомунікації: навчальний посібник / Азарова А. О., Лисак Н. В. – Вінниця : ВНТУ, 2012. – 293 с.
2. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP+Телефония. – М.: Радио и связь, 2001. –336 с.: ил.
3. Asterisk - Окончательное руководство, 4-е издание –Название с экрана. – Электронный ресурс]. – Режим доступа: <http://surl.li/gqtr>

## Оптимізація діалогової людино-машинної взаємодії в комп'ютерних системах

Данілова Л.В., Лавров Є.А., Токар А.С.  
Сумський державний університет

Тенденція активного поширення автоматизації основних процесів у системах управління продовжує конкурувати з використанням роботи людини-оператора. Авіація, будівництво, сільське господарство, хірургія – сфери людської діяльності, контроль над операціями яких не може бути здійсненим у повністю автоматизованому вигляді без втрати рівня якості результату, або навіть отримання негативних наслідків [1].

Підхід Human Adaptive Mechatronics (НАМ) дозволяє спроектувати інформаційну систему відповідно до відмінностей між її користувачами. Оптимальні параметри для інформаційної системи можуть бути визначені після процесу оцінювання навичок і продуктивності користувача.

Евристичні методи і підходи, засновані на знаннях, що використовуються за умови відсутності можливості формування точної математичної моделі користувача, можуть успішно застосовуватися для адаптації інформаційної системи до рівня експертності користувача і його динамічних характеристик.

Для отримання найвищого рівня точності необхідно використовувати математичні методи, що нерозривно пов'язані із врахуванням рівня експертності людини-оператора, і дозволяють оптимізувати діалогову людино-машинну взаємодію. Якщо розробити механізми оптимізації діалогової взаємодії між людиною та інформаційною системою на основі моделі користувача, то можна підвищити рівень ефективності комп'ютерної системи шляхом задоволення потреб операторів з різними рівнями досвіду.

Аналіз методів теорії прийняття рішень, а саме марковських та напівмарковських процесів, дає змогу сформулювати і вирішити задачу оптимізації діалогової людино-машинної взаємодії на основі прихованої марковської моделі.

Прихована марковська модель – це статистична модель, що імітує роботу процесу, який схожий на марковський процес, але з невідомими вхідними параметрами.

Задачею вважається прогнозування невідомих параметрів на основі спостережуваних. Оскільки стани системи невідомі (а лише ймовірності переходів), то ми маємо можливість спостерігати лише за змінними, на які впливає даний стан (при цьому кожен стан має вірогідніший розподіл серед множини всіх вихідних значень) [2].

Загальна структура прихованої марковської моделі складається з таких змінних:  $x(t)$  – значення невідомої змінної в обраний період часу  $t$ ,  $y(t)$  – значення відомої змінної в момент часу  $t$ . Змінні взаємопов'язані (Рис.1).

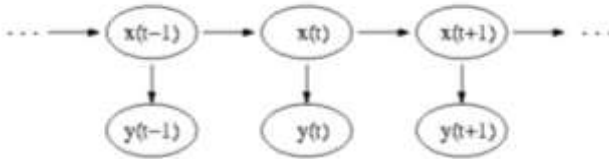


Рисунок 1 – Структура прихованої марковської моделі

Значення невідомої змінної  $x(t)$  в момент часу  $t$  залежить лише від спостережуваної змінної в момент часу  $(t-1)$ , що відображає основну властивість Маркова. У той же час значення відомої змінної  $y(t)$  залежить від невідомої -  $x(t)$  (в момент часу  $t$ ). Задамо ймовірність появи послідовності  $Y=y(0), y(1), \dots, y(L-1)$  довжиною  $L$ , що дорівнює:

$$P(Y) = \sum_X P(Y|X)P(X), \quad (1)$$

де сума враховує кожну послідовність прихованих вузлів:

$$X=x(0), x(1), \dots, x(L-1) \quad (2)$$

Метод повного перебору ускладнює задачу. Саме для раціонального розрахунку будемо використовувати алгоритм Вітербі, що являє собою алгоритм пошуку списку станів (шлях Вітербі), який за умови розгляду марковських ланцюгів приймає найбільш імовірну послідовність подій, що відбулися. Відноситься він до алгоритмів динамічного програмування, і заснований на таких припущеннях:

- Спостережувані і невідомі стани повинні утворювати послідовність.
- Дві послідовності повинні бути вирівнянні (всі стани повинні відповідати один одному).
- Обчислення найбільш імовірної прихованої послідовності до моменту часу  $t$  повинно залежати тільки від спостережуваної події в даний момент часу і від найбільш імовірної послідовності до моменту часу  $(t-1)$ .

Нехай існує прихована марковська модель з простором станів:

$$S=\{s_1, s_2, \dots, s_K\}, \quad (3)$$

де  $K$  – загальна кількість можливих станів системи.

Стани, які приймає система, невідомі. Визначимо через  $x_t$  стан системи у певний момент часу  $t$ . На виході отримуємо видиме спостереження:

$$y_t \in O = \{o_1, o_2, \dots, o_N\}, \quad (4)$$

де  $N$  – кількість можливих спостережуваних значень на виході.

Якщо  $R_i$  - це початкова ймовірність перебування системи в стані  $i$ , а  $a_{i,j}$  - ймовірності переходу зі станів  $i$  в стани  $j$ .

Нехай на виході спостерігається послідовність  $y_1, \dots, y_T$ , тоді найбільш імовірна послідовність станів системи  $x_1, \dots, x_T$  для заданої послідовності можна розрахувати за допомогою наступних рекурентних співвідношень:

$$V_{1,k} = P(y_1|k) \times R_k, \quad (5)$$

$$V_{t,k} = \max_{x \in S} (P(y_t|x) \times a_{x,k} \times V_{t-1,x}), \quad (6)$$

де  $V_{t,k}$  – це імовірність найбільш вірогідної послідовності станів, що співвідносяться з першим  $t$  спостережених значень, які завершуються в стані  $k$ . У свою чергу, шлях Вітербі знаходиться за рахунок показників, що записували стани  $x$  у другому рівнянні.

Нехай  $\text{Ptr}(k,t)$  – це функція, яка повертає значення  $x$ , що використовується для підрахунку  $V_{t,k}$ , якщо  $t \geq 1$ , тоді:

$$x_T = \arg \max_{x \in S} (V_{T,x}) \quad (7)$$

$$x_{t-1} = \text{Ptr}(x_t, t) \quad (8)$$

де  $\arg \max$  – це аргумент максимізації.

Ймовірності переходу можна підсумувати в матриці, з сумою кожного ряду, що дорівнює 1. Така матриця називається стохастичною матрицею  $(I, j)$  і визначається як  $p_{i,j}$  - ймовірність переходу між  $i$  і  $j$ . При розрахунку потужності матриці  $P^k$  запис  $(i, j)$  представляє ймовірність переходу зі стану  $i$  в стан  $j$  на  $k$  кроці. Найчастіше, маємо вектор початкових ймовірностей  $q = (q_1, \dots, q_n)$  для кожного стану в момент часу  $t = 0$ . Таким чином, імовірність перебування у стані  $i$  в момент часу  $t$  буде дорівнювати  $i$ -му запису вектора  $P^k q$ .

Процеси адаптації насамперед пов'язані із використанням систематичного підходу до автоматизованого регулювання контролерів у режимі реального часу. Даний підхід використовується для досягнення і підтримання необхідного рівня працездатності (коли параметри динамічної моделі невідомі), що прямо пропорційно впливає на рівень задоволеності потреб користувача. Для досягнення високого рівня точності за умови ймовірності виникнення вагомих невідомих змін параметрів моделі використаємо адаптивний підхід управління. Перш за все необхідно задати показники для циклу управління. На наступному кроці знайти динамічну модель системи, яку необхідно контролювати і розробити метод проектування контролера.

Показники циклу управління – це вхідні дані до моделі користувача, які були описані під час аналізу цільової аудиторії сайту. Динамічна модель

система заснована на використанні прихованої марковської моделі, вирішеної методом з використанням алгоритму Вітербі. За отриманими результатами розробки механізмів формалізуються й оптимізуються основні варіанти діалогової людино-машинної взаємодії.

#### Перелік посилань

1. Harashima, F. and Suzuki, S. Human Adaptive Mechatronics – Interaction and Intelli-gence. In Proceedings of the 9th IEEE International Workshop on Advanced motion control, Istanbul, Turkey, 2006, pp. 1–8 (IEEE, USA).

2. Бояринов Ю.Г., Дли М.И., Круглов В.В. Оценка диапазона возможных значений вероятности пребывания в заданном состоянии марковской модели производственно-экономической системы // Программные продукты и системы. 2009. № 4. - 230с.

### **Завадостійкий біноміальний таймер**

Єрмаков М. С.

Науковий керівник – д.т.н., професор Борисенко О.А.

Сумський державний університет

Електроніка є універсальним і винятковим засобом при вирішенні проблем в різних областях. Сфера її застосування постійно розширюється. Практично кожна досить складна технічна система оснащується електронними пристроями і відповідно функції пристроїв стають все більш різноманітними. Одним із найбільш поширених пристроїв в цифровій електроніці є таймери. Таймери важливі не тільки самі по собі, але і з точки зору нових рішень схемотехніки в області цифрових пристроїв, тому що до них можна віднести будь-який пристрій, який в процесі роботи проходить через декілька станів. В більшості випадків таймери використовують як пристрої керування в системах, де треба вимірювати час, наприклад при необхідності автоматизованого запуску і вимкненню електрообладнання в наперед задані моменти часу.

Не дивлячись на велику кількість розроблених таймерів навіть в даний час залишається досить актуальним завдання створення таймерів, які можуть працювати без помилок в середовищі зі значним завданнями. Одним із варіантів вирішення цієї задачі є застосування таймерів на основі завадостійких біноміальних лічильників. Біноміальні лічильники, що працюють в біноміальній системі числення мають ряд переваг:

а) значне зменшення апаратури, необхідної для дешифрування їх станів. У ряді випадків це може привести до того, що кількість витрат апаратури в пристрої з біноміальними лічильниками в цілому зменшиться в порівнянні з

пристроєм, що містить двійкові лічильники. Крім того, ці лічильники дозволяють зміною коефіцієнта перерахунку адаптуватися до інтенсивності і характеру перешкод;

б) другою важливою, якщо не основною, перевагою лічильників, що працюють в перешкодостійких системах числення, є можливість перебирати комбінаторні конфігурації, наприклад, поєднання, поєднання з повтореннями, перестановки, тощо. Таким чином, лічильники завадостійких систем числення володіють важливими перевагами - завадостійкість і багатофункціональність.

в) наявність комбінацийних матричних суматорів, які виконують функції перенесення і схем контролю та в звичайних лічильниках відсутні. Крім того, вони в значній мірі виконують функції дешифратора. Тому дешифрування станів біноміального лічильника значно спрощується.

г) однорідність структури і можливість простої перебудови коефіцієнта перерахунку і відповідно ступеня завадостійкості.

Завадостійкі таймери можливо використовувати в спеціалізованих перешкодостійких пристроях автоматики і телемеханіки в якості надійних розподільників імпульсів, перерахункових схем, кодерів і декодерів.

Розглянемо роботу таймера який побудований на основі завадостійкого біноміального лічильника (рис. 1).



Рисунок 1 - Структурна схема завадостійкого біноміального таймера

Робота таймер починається з генератор тактових імпульсів (ГТІ), що виробляє послідовність імпульсів з заданою частотою. За допомогою дільника частоти для роботи таймера в якості приладу вимірювання часу було зменшено частоту до 1 Гц. Потім імпульси з дільника частоти надходять на синхронний вхід лічильника. В якості лічильника використовуємо завадостійкий біноміальний лічильник, який працює в біноміальній системі числення. Біноміальні лічильники однорідні і стійкі перед перешкодами і мають здатність виявляти помилки без застосування додаткових блоків. Імпульси з виходів лічильника надходять на входи дешифратора, що розшифровує стани лічильника. До виходів дешифратора підключається пристрій відображення інформації (ПВІ). В якості пристрою відображення інформації було обрано семисегментний індикатор. Цифри на семисегментних індикаторах формуються з надходженням кодових комбінаций з дешифратора, що

відповідають певній заданій цифрі.

#### Перелік посилань

1. Борисенко А. А. Биномиальные автоматы - Суми: СумДУ, 2006 р. – с. 120
2. Борисенко А. А. Биномиальный счет и счетчики: монография. – Сумы: СумГУ, 2008. – 152 с.

### **Аналіз механізмів захисту мережевого устаткування від хакерської атаки типу TCP SYN Flood**

Казімірко А.О.

Науковий керівник – к.т.н., доц. Таранчук А.А.  
Хмельницький національний університет

В основі зв'язку та обміну повідомленнями між хостами користувачів глобальної мережі Інтернет лежить набір протоколів TCP / IP - це простий набір правил (стек) обміну інформацією, або протокол управління передачею [1].

Даний стек має слабкі місця, які полягають в його вразливості до хакерських атак типу TCP SYN Flood при підключенні хост машин користувачів до мережі Інтернет. Користуючись цією слабкістю, хакери можуть атакувати систему певного користувача в будь-який час. Мережева атака SYN Flood полягає у відправці великої кількості пакетів SYN-запитів на підключення за протоколом TCP до операційної системи іншого хосту, причому пакети надсилаються в дуже короткий інтервал часу [1].

Основна ідея атаки полягає в тому, щоб під час процесу запуску сесії TCP, змушувати хост зберігати досить велику кількість напівз'єднань для вичерпання його ресурсів і не можливості встановлення нових зв'язків.

В основі процесу початку TCP сеансу лежить алгоритм «потрійного рукоєстикання», який реалізується за три кроки (рис.1) [2]:

1) хост А надсилає пакет з прапором SYN на сервер Б (скор. від англ. synchronize - запит на підключення за протоколом TCP). Якщо відправлений пакет з прапором SYN, це означає, що хост А запитує у хосту Б з'єднання;

2) хост Б надсилає у відповідь пакет з прапором SYN / ACK (скор. від англ. acknowledges), що містить криптографічну інформацію хосту А;

3) хост А надсилає пакет з прапором ACK до хосту Б, що означає – зв'язок встановлений.

Розглянемо як відбувається атака SYN Flood на деякий хост мережі Інтернет.



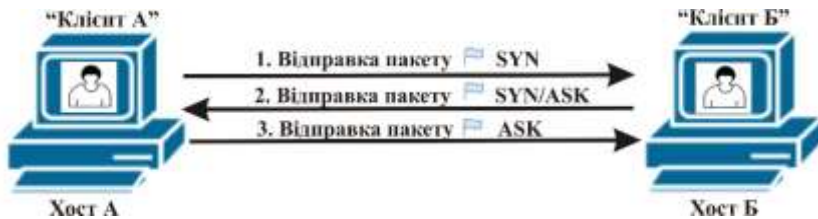


Рисунок 1 – Реалізація алгоритму «потрійного рукостискання»

Мережева атака TCP SYN Flood використовує тристоронній механізм рукостискання, описаний вище (рис.1). При цьому, з хосту А зловмисник відправляє пакет з прапором SYN (зазвичай використовується підмінена IP - адреса - англ. spoofing) хосту Б (ціль атаки), запрошуючи ініціалізацію нової сесії TCP у операційній системі хосту Б. Далі хост Б відправляє пакет з прапором SYN/ACK хосту А. За звичайним тристороннім механізмом рукостискання, при відкритій сесії TCP, хост А повинен надіслати хосту Б пакет з прапором ACK. Однак атакуюча система А не відповідає ні на один з повернутих пакетів SYN / ACK. У цьому випадку хост Б, очікуючи пакет з прапором ACK від хосту А знаходиться в «напіввідкритому» статусі, встановлюючи неповне з'єднання, яке зберігається у черзі таблиці з'єднань (англ. Transmission Control Block table - TCB). Через 75 секунд неповне з'єднання видаляється із черги TCB і руйнується (рекомендація RFC 4987). Зловмисники використовують цю відкриту сесію, відправляючи на порт хосту Б (ціль атаки) швидкий потік SYN- пакетів, перш ніж хост Б видалить неповні з'єднання з черги TCB у разі не отримання відповідей на надісланий пакет SYN/ACK. За цей час на хості Б черга запитів на підключення переповниться за рахунок зберігання великої кількості фальшивих «напіввідкритих» з'єднань, які займають всю пам'ять TCB. Коли кількість вхідних з'єднань досягне максимального рівня, тоді всі наступні запити будуть відхилені операційною системою хосту Б. У цьому випадку хост Б взагалі не зможе встановити TCP- з'єднання за рахунок втрати продуктивності. Цей процес називається «відмовою в обслуговуванні» (рис. 2) [2].

Успішна атака залежить від трьох параметрів: розміру загородження; частоти з якою створюються загородження та засобів вибору IP-адрес для підробки (містифікації).

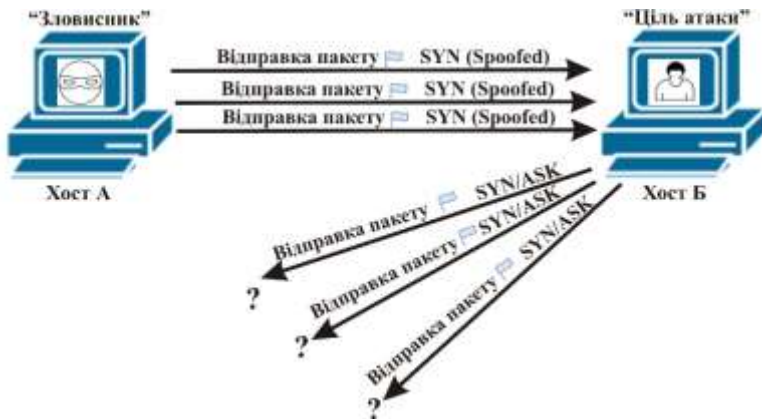


Рисунок 2 – Мережева атака SYN Flood та процес - «відмова в обслуговуванні»

Існує декілька механізмів захисту мережевого обладнання (хостів), які можуть частково забезпечити захист від SYN Flood – атак [3]:

1. Налаштування стеку. Для цього можна налаштувати стек TCP, зменшивши його час «напіввідкритої» сесії з'єднань, або, іншими словами, тайм-аут звільнення пам'яті, виділеної для з'єднання, а також час виділений на блокування вхідних з'єднань. Але у цих налаштувань можуть бути побічні ефекти у вигляді втрати частини легітимних з'єднань через затримки і нестабільні канали.

2. Реалізація механізму SYN-Cookie. Для створення TCP-з'єднання хост А відправляє хосту Б TCP-пакет з прапором SYN і своїм номером послідовності. Механізм SYN cookies зовсім не використовує чергу SYN. Хост Б відправляє пакет з прапором SYN-ACK, який містить унікальну інформацію, що ідентифікує клієнта Б: IP - адресу; номер порту; час відправки пакету та прийнятий унікальний номер послідовності хосту А. Хост «зловмисника» ніколи не отримує ці пакети і тому не надасть на них відповідь. На завершальній відповіді хостом А ця інформація (хеш) вже включена в пакет з прапором ACK. При успішній перевірці ACK – пакету відповіді на SYN cookie, хостом Б виділиться пам'ять для з'єднання, навіть, якщо в черзі SYN не має відповідного запису. Для використання механізму хешування (порівняння даних) необхідно, щоб усі хости, які приймають участь в передачі трафіку його підтримували. Якщо SYN cookie включені, то «зловмисник» не зможе обійти такі міжмережеві екрани відправкою ACK-пакета з довільним номером послідовності поки не підбере вірний. SYN cookies потрібно включати тільки для публічно доступних портів. Включення механізму SYN cookies – це простий спосіб боротьби проти атаки SYN Flood. Однак при його використанні

буде більше завантаженість процесора клієнта під час створення та звірки cookies.

3. Обмеження запитів на нові підключення від конкретного джерела за визначений проміжок часу.

4. Використання мережевого протоколу транспортного рівня SCTP (англ. Stream Control Transmission Protocol - протокол передачі з керуванням потоком), який є більш сучасним, на відміну від TCP. Даний протокол використовує механізм SYN cookie та не підданий SYN- Flood атакам. Передача трафіку за протоколом SCTP здійснюється багатьма потоками, а синхронне з'єднання між двома хостами по двох та більше незалежних фізичних каналах (multi-homing) [3].

#### Перелік посилань

1. W. M. Eddy, "TCP SYN Flooding Attacks and Common Mitigations," RFC 4987, August 2007. [Online]. Available: <http://tools.ietf.org/html/rfc4987>.

2. S. Gavaskar, R. Surendiran and Dr. E. Ramaraj, "Three Counter Defense Mechanism for SYN Flooding Attacks", International Journal of Computer Applications, Volume 6 – No. 6, pp. 12-15, Sep. 2010.

3. Seggelmann, R.; Tuxen, M.; Rathgeb, E.P. SSH over SCTP - Optimizing a multi-channel protocol by adapting it to SCTP // Communication Systems, Networks & Digital Signal Processing (CSNDSP), 2012 8th International Symposium on : journal, 2012. - P. 1-6.

### **Модель «розумної» мережі енергопостачання житлового будинку**

Ковальчук О.Л., Кучерявий Є.І.

Науковий керівник – к.т.н., доц. Таранчук А.А.

Хмельницький національний університет

В країнах ЄС активно впроваджуються «інтелектуальні» мережі Smart Grid, які поєднують в собі елементи традиційної електроенергетики та новітні електроенергетичні технології, комплексні інструменти контролю та моніторингу, інформаційно-комунікаційні технології та «інтелектуальні» вимірювальні системи [1,2].

В Україні на даний момент показник втрат електроенергії досягає 15%. При цьому в розвинених країнах Європи він становить лише 6%. Домогтися таких же показників на українській території може допомогти впровадження технології Smart Grid. Оптимальний результат досягається за рахунок впровадження інноваційних рішень, ефективного регулювання і управління розподілом електроенергії [1].

В даній роботі побудована імітаційна модель «розумної» мережі енергопостачання житлового будинку в симуляторі Cisco Packet Tracer [3], яка

забезпечує абонента мережі послугою автономного енергозабезпечення (рис.1).

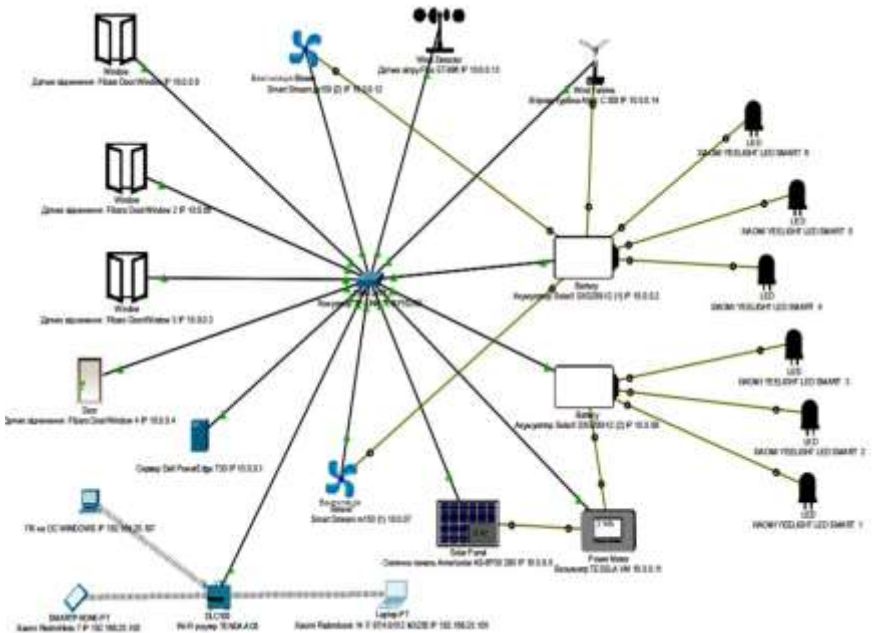


Рисунок 1 - Імітаційна модель «розумної» мережі енергопостачання житлового будинку

Джерелами, від яких проєктована мережа може отримувати електроенергію, зазвичай є великі підстанції енергосистеми або місцеві електростанції, що входять в енергосистему. В обох випадках, в години найбільших навантажень необхідно мати резерв джерела по активній потужності, достатній для підключення додаткових абонентів проєктованої мережі. Для цього, у розробленій «розумній» мережі енергопостачання (рис.1) передбачено два джерела перетворювача енергії - сонячна панель і вітряна турбіна, які призначені для перетворення сонячної енергії та енергії вітру в постійний електричний струм.

Керування роботою всієї мережі енергопостачання здійснює центральний сервер. За допомогою використання протоколу DHCP (англ. Dynamic Host Configuration Protocol), який відповідає за динамічну видачу IP-адрес пристроям, що підключаються до мережі, спрощується адміністрування мережею [2]. За потреби забезпечення високих вимог до безпеки мережі, усім

пристроєм мережі адміністратором вручну призначаються IP - адреси та MAC за попередньо складеним IP - планом.

Наявність IoT монітору симулятора CRT дозволяє здійснювати моніторинг системи енергозабезпечення, наочно відстежувати процес підключення пристроїв IoT, здійснювати опитування інформації про стан будь-якого пристрою IoT мережі, усувати неполадки, пов'язані з функціональністю їх роботи, а також управляти оновленнями програмного і мікропрограмного забезпечення.

Абонент енергетичної мережі має змогу здійснювати автоматичне та ручне керування енергозабезпеченням будинку, настройку пристроїв IoT, а також отримувати різні вимірювальні дані за допомогою спеціального програмного забезпечення, що встановлюється на смартфон, ноутбук або персональний комп'ютер. Для підключення безпроводових пристроїв IoT в домашній мережі передбачена точка доступу Wi-Fi. На рис. 2 представлена конфігурація IoT пристроїв, підключених до «розумної» мережі енергозабезпечення і розміщених у будинку.

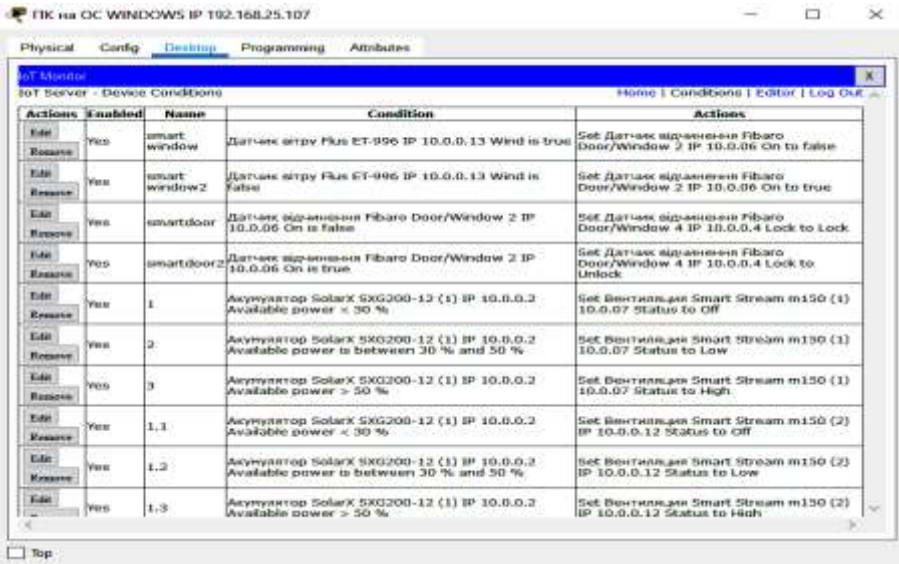


Рисунок 2 - Конфігурація IoT пристроїв налаштованих на IoT сервері

На рис. 3 наведена функціональна схема розміщення обладнання побудованої «розумної» мережі енергопостачання житлового будинку.



Рисунок 3- Функціональна схема розміщення обладнання мережі

Побудована модель «розумної» мережі енергопостачання володіє функціями управління генерацією електроенергії розподіленими по всій енергетичній системі будинку поряд з добре налагодженими «розумними» приладами і системами управління навантаженням, здатними працювати в симбіозі та в режимах заданих користувачем.

Використання технології «розумного будинку» підвищує якість життя користувачів, розширюючи можливості звичних використовуваних пристроїв і предметів - кавоварок, штор, вентиляторів, камер відеоспостереження. Використання пристроїв інтернет речей дає змогу будувати «розумні будинки», наділяючи їх новими інтелектуальними програмованими можливостями. Інтелектуальні системи автоматизації, безпеки; моніторингу та домашні мережі, знаходять особливе застосування в ключових прикладах проектування мереж «розумного будинку» [4].

#### Перелік посилань

1. SmartGrid в Україні – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <https://ua.energy/wp-content/uploads/2018/01/3.-Smart-Grid.pdf>
2. Tamilaran Vijayapriya. Smart Grid: An Overview / Smart Grid and Renewable Energy 02(04): pp. 305-311.
3. Cisco Networking Academy – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <https://www.netacad.com>.
4. Кокорева И. Системы "Интеллектуальное здание" и "Умный дом": эффективные решения и новейшие разработки. – Электроника: НТБ, 2008, № 7, с. 22–27.

## **Зміст курсу «Комп'ютерний практикум» у професійній підготовці фахівців спеціальності 015.20 «Професійна освіта. Транспорт»**

Красильников С.Р.

Хмельницький національний університет

Глобальні економіко-технологічні зміни в суспільстві, зростання інформатизації суспільства та впровадження інноваційних та інформаційних технологій в усі сфери життя людини, зрослі потреби ринку праці як окремих регіонів, так і країни в цілому впливають на формування нових вимог до підготовки фахівців та їхніх компетентностей.

Для успішної фахової діяльності сучасний педагог професійної освіти під час навчання має набути спеціальні компетентності, що залежать від предметної області, та не менш важливі для його особистісного розвитку – загальні компетентності, зокрема здатність адаптуватися до змін техніки та володіти спектром інформаційних технологій.

Відтак, стандарт вищої освіти зі спеціальності 015 «Професійна освіта (за спеціалізаціями)» підготовки бакалаврів містить низку компетентностей, що мають забезпечити «цифрову грамотність» майбутніх педагогів [1]: навички використання інформаційних і комунікаційних технологій (ЗК 06); здатність використовувати сучасні інформаційні технології та спеціалізоване програмне забезпечення та інтегрувати їх в освітнє середовище (ФК 16); здатність використовувати відповідне програмне забезпечення для вирішення професійних завдань, відповідно до спеціалізації (ФК 19); здатність використовувати у професійній діяльності основні положення, методи, принципи фундаментальних та прикладних наук (ФК 22); здатність виконувати розрахунки технологічних процесів в автотранспортній галузі (ФК 23); здатність управляти комплексними діями/проектами, відповідати за прийняття рішень у непередбачуваних умовах та професійний розвиток здобувачів освіти і підлеглих (ФК 24).

Для формування означених компетентностей у майбутнього педагога професійної освіти освітньо-професійною програмою підготовки 015.20 «Професійна освіта. Транспорт» передбачені обов'язкові освітні компоненти:

- Інженерна та комп'ютерна графіка (10 кредитів ЄКТС);
- Інформаційно-комунікаційні технології (5 кредитів ЄКТС);
- Пакети прикладних програм (5 кредитів ЄКТС).

Вивчення таких навчальних дисциплін забезпечить досягнення програмних результатів навчання:

- розуміти особливості комунікації, взаємодії та співпраці в міжнародному культурному та професійному контекстах (ПРН 04);
- володіти культурою мовлення, обирати оптимальну комунікаційну стратегію у спілкуванні з групами та окремими особами (ПРН 05);
- відшуковувати, обробляти, аналізувати та оцінювати інформацію,

що стосується професійної діяльності, користуватися спеціалізованим програмним забезпеченням та сучасними засобами зберігання та обробки інформації (ПРН 09);

- знати основи психології, педагогіки, а також фундаментальних і прикладних наук (відповідно до спеціалізації) на рівні, необхідному для досягнення інших результатів навчання, передбачених цим стандартом та освітньою програмою (ПРН 10);

- застосовувати програмне забезпечення для e-learning і дистанційного навчання і здійснювати їх навчально-методичний супровід (ПРН 22);

- володіти основами управління персоналом і ресурсами, навичками планування, контролю, звітності на виробництвах, в установах, організаціях галузі/сфери (ПРН 24).

Для подальшого поглиблення та удосконалення цифрових навичок майбутніх педагогів, освітньо-професійною програмою передбачена вибіркова навчальна дисципліна «Комп'ютерний практикум», метою якої є формування навичок використання сучасних інформаційно-комунікаційних технологій та спеціалізованого програмного забезпечення для вирішення професійних завдань відповідно до спеціалізації.

Дисципліна викладається студентам у 7 семестрі обсягом 4 кредити ЄКТС. Запланована навчальна діяльність: лекції – 22 год, лабораторні заняття – 22 год., самостійна робота – 76 год. Вид семестрового контролю – залік.

Дисципліна містить три розділи «Робота із програмами MS Office», «Можливості додатків Інтернет та технології їх створення» та «Редактори векторної та растрової графіки». Зміст першого розділу дисципліни містить загальну характеристику пакету прикладних програм Microsoft Office і охоплює роботу у програмах Microsoft Word, Microsoft Excel, Microsoft Access. Другий розділ дисципліни складається з основних відомостей про комп'ютерні мережі, глобальну мережу Інтернет та її сервіси, мову HTML, використання каскадних таблиць стилів, мови сценарії JAVASCRIPT, мови PHP тощо. У третьому розділі розглядаються основні правила виконання креслень та зображень, складального креслення, робочих креслень деталей, планів дільниць та цехів, а також методика виконання креслень в системі КОМПАС – 3D.

Перелік лабораторних занять з курсу «Комп'ютерний практикум» наведений нижче:

- Створення бази даних в СУБД ACCESS.
- Створення запитів і звітів бази даних СУБД ACCESS.
- Проектування та використання форм в СУБД ACCESS.
- Робота з програмою створення презентацій POWER POINT.
- Хмарні технології. Додаткові послуги глобальної мережі інтернет.

Провайдери.



- Структура HTML-документа і елементи форматування тексту.
- Карти-зображення математичні формули на веб-сторінках.
- Ознайомлення з технологією каскадних таблиць стилів (CSS).
- Ознайомлення з мовою сценаріїв JAVASCRIPT.
- Загальні відомості про програмне середовище КОМПАС 3D.

Підготовка файлу креслення.

- Ознайомлення з основними командами системи КОМПАС 3D.

Самостійна робота передбачає вивчення студентами динаміки розвитку інформаційних технологій та представлення результатів самостійної роботи у вигляді презентацій, рефератів, есе тощо. Індивідуальне завдання з курсу полягає у розробленні веб-сторінок за заданною тематикою.

Отже, запропонована структура та зміст курсу «Комп'ютерний практикум» забезпечують подальше поглиблення та удосконалення цифрових навичок майбутніх педагогів з професійної освіти, сприяють їх успішній професійній діяльності.

#### Перелік посилань

1. Стандарт вищої освіти України перший (бакалаврський) рівень, галузь знань 01 – «Освіта / Педагогіка», спеціальність 015 – «Професійна освіта (за спеціалізаціями)» [Електронний ресурс]. – Режим доступу: <https://mon.gov.ua/storage/app/media/vishcha-osvita/zatverdzeni%20standarty/2019/11/22/2019-11-22-015-B.pdf> / (дата звернення: 4.11.2020)

2. Бакалавр. Професійна освіта. Транспорт. 2017. URL: <https://www.khnu.km.ua/root/page.aspx?l=0&r=50&p=1&f=%D0%91> (дата звернення: 4.11.2020).

### **Технологія побудови сенсорної мережі IoT з використанням протоколу LoRaWAN**

Крикун Є. О.

Науковий керівник – д.т.н., доц. Підченко С.К.

Хмельницький національний університет

На теперішній час концепція інтернет речей (абр. internet of things - IoT) завойовує все більше місця в різних галузях народного господарства. При цьому кількість пристроїв за останні роки значно зростає. Так за прогнозами аналітиків, найбільше зростання IoT - пристроїв до 2022 року очікується в таких областях, як: транспорт; логістика; автомобілебудування; охорона здоров'я; сільське господарство та промислового секторі. При цьому, за їх словами, для ефективного використання IoT – рішень та збільшення бізнес – прибутку необхідно використання комплексних базових технологій зі збору

даних з сенсорів та їх аналізу в контексті інших даних: довідкової інформації; фінансових даних і т. інш. [1].

Всі існуючі пристрої IoT використовують вихід в мережу інтернет і взаємодіють через неї один з одним. Керування IoT здійснюється через глобальну мережу Інтернет за допомогою відправлення певних команд користувачами цих пристроїв. Економічне підключення пристроїв IoT до Інтернету є важливою проблемою для вбудованих пристроїв із низьким енергоспоживанням, які призначені для конкретного завдання [2].

Існуючі технології безпроводового зв'язку такі як GSM та LTE не спроможні забезпечити вимоги, щодо споживання енергії та вартості обслуговування великої кількості IoT – пристроїв.

На сьогодні, у всьому світі, активно впроваджуються та розгортаються широкопasmові мережі з низькими потужностями та швидкостями передачі, які забезпечують покриття великих територій. До таких технологій відносяться LoRaWAN, SigFox, NB-IoT, Weightless та інші комунікаційні технології, що працюють у ГГц діапазонах та успішно забезпечують усі перелічені вище функціональні можливості, однак LoRaWAN привернула найбільшу увагу організацій, спільнот та дослідників і стала популярною технологією LPWAN (англ. Low-power Wide-area Network - «енергоєфективна мережа дальнього радіусу дії»), придатною саме для IoT - рішень. Мережі LPWAN мають на меті вирішити проблеми, які можуть бути придатними для широкомасштабного розгортання та підключення кінцевих пристроїв IoT малої потужності. Загальними характеристиками LPWAN, що відрізняють їх від інших технологій традиційних телекомунікаційних мереж є [2]:

- мале енергоспоживання підключених мережесих та пристроїв IoT;
- невелика вартість використання та обслуговування каналу зв'язку;
- усі пристрої та додатки системи потребують потужного механізму безпеки;
- можливість побудови мереж в приміщеннях та забезпечення стійкого зв'язку;
- необхідність забезпечення завадостійкості передачі та використання потужної модуляції при розгортанні мереж в щільно забудованих територіях;
- наявність сервера обробки та аналізу даних отриманих з інформаційних та вимірвальних сенсорів.

Технологія LoRaWAN – сукупна система, що використовує протокол фізичного рівня LoRa (абр. Long Range) та каналного рівня LoRaWAN моделі OSI [2], яка застосовується в комплексних рішеннях IoT для збору і обробки даних з інформаційних сенсорів. Пристрої LoRaWAN працюють в неліцензованих частотних ISM- діапазонах (433, 868, 915 МГц), що є додатковою перевагою використання даної технології. Архітектура мережі LoRaWAN наведена на рисунку 2.

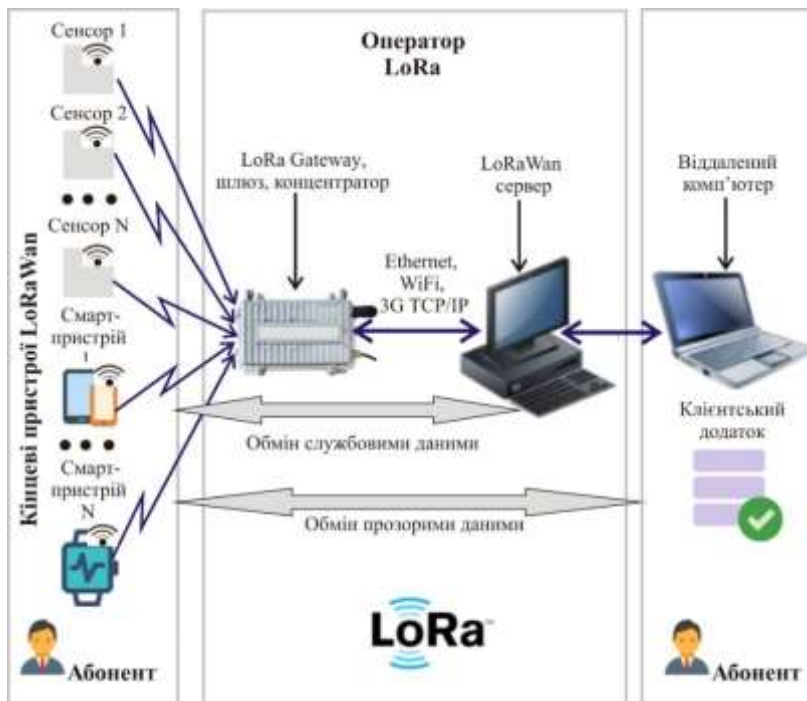


Рисунок 2- Архітектура мережі LoRaWAN

Архітектура мережі LoRaWAN містить (рисунок 2) [2]:

1. Кінцеві вузли, у якості яких зазвичай виступають сенсори фізичних величин, смарт – пристрої, що здійснюють функції вимірювання або керування та пристрої IoT. LoRaWAN рахується самою енергоефективною технологією за рахунок того, що кінцеві пристрої LoRa, які повністю автономні, можуть працювати від батарей на одному заряді до 10 років [2].

2. Шлюз, або концентратор LoRa, який приймає по безпроводовому каналу дані від кінцевих пристроїв LoRa і передає їх в канали зв'язку. Зв'язок з сервером відбувається за стандартними протоколами TCP/IP за допомогою телекомунікаційних каналів Ethernet, Wi-Fi, 4G/LTE і інш. В LoRaWAN передбачений захист інформації, що передається за допомогою використання шифрування блоковими кодами AES128.

3. Мережевий сервер LoRa, який управляє мережею та реалізує функції усунення дублювання пакетів, управління розкладом, підтвердження і управління швидкістю передачі даних та вихідною потужністю радіопередавача для кожного кінцевого пристрою окремо, завдяки реалізації алгоритму адаптивної швидкості передачі даних (adaptive data rate, ADR) та

використання технологій з розширенням спектру. За таким алгоритмом дані, які передаються від різних кінцевих вузлів з різними швидкостями не заважають один одному і створюють різні віртуальні канали, що збільшує пропускну здатність шлюзу. Максимальна швидкість передачі даних в мережах LoRaWAN дорівнює 50 Кбіт/с.

4. Віддалений комп'ютер, який може контролювати дії кінцевих вузлів або збирати дані з них.

5. Віддалений сервер (клієнтський додаток), що призначений для розшифрування переданої інформації. При цьому, кожен кінцевий пристрій має вбудований ідентифікатор за яким сервер додатків розпізнає приналежність кожного пакету даних певному IoT пристрою мережі.

Мережі LoRaWAN побудовані за фізичною топологією зірка, де кінцеві вузли LoRa через шлюзи утворюють прозорі мости для ретрансляції повідомлень та спілкуються з центральним сервером мережі. Зазвичай передбачається, що шлюзами і серверами володіє оператор LoRa мережі, а абоненти підключають свої модеми, по аналогії зі стільниковим зв'язком.

На сьогодні національним оператором lifecell сумісно з компанією IoT Ukraine планується національне покриття мережами LoRaWAN всієї території України, яка зможе обслуговувати до 7-10 млн. підключених до неї кінцевих пристроїв [4].

#### Перелік посилань

1. DataArt IoT trends and predictions for 2019: IoT goes mainstream. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <http://surl.li/gkvb>

2. What is LoRaWAN. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <https://lora-alliance.org/resource-hub/what-lorawan>

3. Mehmet Ali Ertürk. A Survey on LoRaWAN Architecture, Protocol and Technologies / Mehmet Ali Ertürk, Muhammed Ali Aydın, Muhammet Talha Büyükkakka and Hayrettin Evirgen //MDPI. – Future internet, 2019, no.11. – P. 34.

4. Тимур Ягофароф. Национальное LoRaWAN-покрытие появится к 2020 г. Назва з екрану. – [Електронний ресурс]. – Режим доступу: <http://surl.li/gkvq>

### **Пропускна здатність мережі голосової IP- телефонії**

Кубатий Н. О.

Науковий керівник – к.т.н., доц. Таранчук А.А.

Хмельницький національний університет

Телекомунікаційні мережі для передачі голосу через Інтернет (англ. Voice over Internet Protocol, або іншими словами – VoIP телефонія) створюються з урахуванням безлічі різних змінних. Якість зв'язку і витрати на

розгортання мережі з пакетною комутацією – це два найбільш важливих фактори, які необхідно враховувати при проектуванні мережі. При цьому, такий параметр, як якість зв'язку вважається найбільш важливим для задоволення клієнта, а витрати завжди впливають на отриманий прибуток провайдером мережі [1].

При проектуванні і налагодженні мереж VoIP телефонії, які є чутливими до трафіку використовують кілька різних моделей трафіку, які необхідно правильно обирати та використовувати. Існуючі моделі теорії масового обслуговування дозволяють проектувальникам мереж робити припущення про роботу мереж на основі минулого досвіду [1,2].

Аналіз трафіку VoIP мереж дає можливість визначити необхідну пропускну здатність (продуктивність) мережі. Поняття трафіку включає відношення між спробами виклику обладнання, чутливого до трафіку, і швидкістю виконання цих викликів. Проектування трафіку направлено на вирішення проблем зв'язаними з визначенням таких параметрів якості зв'язку, як рівень обслуговування та коефіцієнт блокування. Зазвичай, для визначення навантаження, обирається період часу найбільшого навантаження на мережу, який характеризується максимальною інтенсивністю трафіку, який здатна витримати мережа. Результатом є величина інтенсивності трафіку, яка називається трафіком в час найбільшого навантаження (ГЧНН) [2].

Для аналізу трафіку систем масового обслуговування (СМО) [2,3], які використовують необмежену кількість джерел, випадкове надходження трафіку на вхід комутаційної системи та утримання заблокованих викликів за експоненціальним розподілом часом утримання, застосовують так звану модель Пуассона. В такій моделі заблоковані виклики утримуються, поки канал не стане доступним. За моделлю Пуассона абонент може зробити тільки одну спробу здійснити виклик, і заблоковані виклики втрачаються. Модель Пуассона зазвичай використовується для розрахунку окремих груп магістральних каналів груп з запасом.

Для обчислення моделі трафіку Пуассона використовується наступний вираз [4]:

$$p_k(Y) = \frac{(Y)^k}{k!} e^{-Y}, \quad (1)$$

де  $p_k(Y)$  – імовірність надходження  $k$  викликів,  $Y=203,6$  Ерл. – інтенсивність трафіку (розрахована для наступних змінних: кількість абонентів VoIP – телефонії в офісі провайдера – 749 чол.; середня кількість викликів, які ініціює один абонент офісу – 3,4 викликів за годину).

Модель трафіку, що розрахована за розподілом Пуассона (1), наведена на рисунку 1.

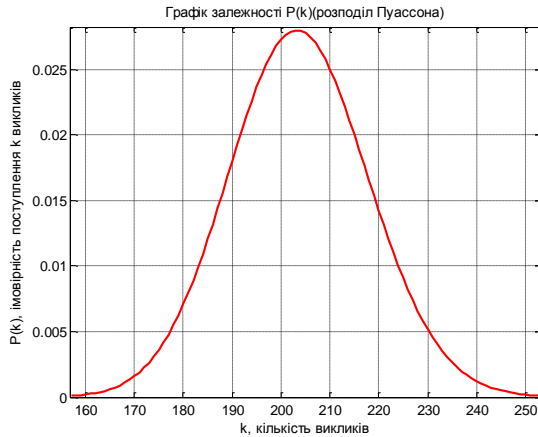


Рисунок 1 - Графік залежності  $p_k(Y)$  від кількості викликів

Згідно розподілу Пуассона (рис. 1) для обробки навантаження 203,6 Ерл. з ймовірністю блокування 2,4% СМО проектованої мережі може обслужити 216 викликів.

Модель трафіку Ерланг В використовується, при заблокованих викликах перенаправлених без повернення до вихідної групи магістральних каналів. Ця модель передбачає випадкове надходження викликів. Абонент робить тільки одну спробу виклику. У випадку блокування цього виклику, він перенаправляється. Модель Ерланг В зазвичай використовується для розрахунку груп магістральних каналів з низьким коефіцієнт блокування, обслужених з першої спроби, без потреби врахування відсотку повторних викликів, тому що абоненти перенаправляються.

Для обчислення моделі трафіку Ерланг В використовується наступний вираз [3,4]:

$$E_v(Y) = \frac{Y^v / v!}{\sum_{i=1}^v Y^i / i!}, \quad (2)$$

де  $E_v(Y)$  - ймовірність блокування викликів;  $v$  - кількість каналів;  $Y$  - інтенсивність трафіку.

Використаємо модель трафіку Ерланг В для перепроєктування вихідних груп магістральних каналів для міжміських викликів, які зараз блокуються під час години найбільшого навантаження. Врахуємо, що під час найбільшого навантаження на групу магістральних каналів надходить 203,6 Ерл. трафіку (рис.2). При розрахунках кількості каналів скористуємось методом підбору (2) та графічним методом [4].

При порівнянні між собою результатів, отриманих шляхом підбору за допомогою (2) і результатів отриманих графічним методом (рис. 2) можна зробити висновок, що отримана, за обома методами, необхідна кількість каналів однакова. За результатами моделювання (рис. 2) видно, що з ймовірністю блокування 0,024, необхідна кількість магістральних каналів для оброблення заданого навантаження трафіку дорівнює – 216 каналам.

Отже, програмна реалізація методу підбору в системі математичного моделювання Matlab працює коректно.

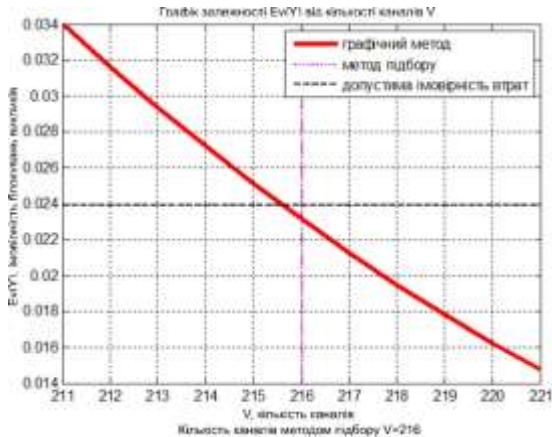


Рисунок 2 - Графік залежності  $E_v(Y)$  від кількості каналів

При використанні такої кількості магістральних каналів та за умови використання голосового кодека G.711 (загальна пропускна здатність кодека G.711 - 107,2 Кбіт/с [3, табл.4]), максимальна пропускна здатність мережі сягає 23,155 Мбіт/с.

Розрахунки показали, що магістральна мережа спроектована якісно, має високу продуктивність та низький коефіцієнт блокування. За таких даних, якість обслуговування значно підвищується, а витрати зменшуються.

#### Перелік посилань

1. Характеристики голосового трафіка. – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <http://surl.li/gqrv>.
2. Еременко, В.Т. Методы и модели теории телеграфика: учебное пособие / В.Т. Еременко [и др.]. – Орёл: ОГУ им. И.С. Тургенева, 2019. –244 с.
3. Ложковський А.Г. Теорія масового обслуговування в телекомунікаціях / А.Г. Ложковський. – Одеса: ОНАЗ ім. О.С. Попова, 2010. – 112 с.
4. Системи комутації – Назва з екрану. – [Електронний ресурс]. – Режим доступу: <http://vnstele.com/system-komut.html>.

## Розробка системи відкритого світу в Unreal Engine 4

Локазюк В.Ю.

Науковий керівник – к.т.н., доц. Медзятий Д.М.

Хмельницький національний університет

Перша версія движка Unreal Engine з'явилася в далекому 1998 році, коли компанія Epic Games випустила шутер Unreal. Уже тоді він демонстрував універсальність, поєднуючи в собі графічний і фізичний движки, систему штучного інтелекту, управління файлової і мережевої системами, а також включаючи готову середу для розробки ігор. Автори движка спростили взаємодія з ним, щоб розробники могли зосередитися на створенні основних елементів ігор, не відволікаючись на дрібниці на зразок налагодження мережевого коду або обчислення колізій. Розвиток Unreal Engine йшло поступово, рік за роком: движок міняв версії, обростав новими технологіями - багато в чому, до речі, революційними для свого часу. Кожна версія UE привносила нові вражаючі графічні ефекти, показання Epic Games в високотехнологічних демо (на кшталт «Самарянина»). Завдяки простоті використання, а також лояльним умовам ліцензування, движок використовували багато студій, від інді-команд до найбільших компаній, що випускають дорогі AAA-блокбастери.

Станом на 2020 рік Unreal Engine (вже в четвертій номерній версії) залишається надзвичайно затребуваним движком, дуже гнучким, зручним у використанні і абсолютно різноплановим - поставте поруч гранично похмуру RTS Battlefleet Gothic: Armada і веселу «Королівську битву» Fortnite, і ви ні за не здогадаєтеся, що обидві гри виконані на одному двигуні. Epic Games продовжує регулярно оновлювати його, використовуючи, в тому числі, і для своїх проєктів, включаючи вищезгадану мегапопулярну Fortnite.

Як вже говорилося, Unreal Engine дуже гнучкий і універсальний. На відміну від Unity, який вимагає установки безлічі плагінів (часто - платних), UE4 вже «з коробки» забезпечений всіма необхідними інструментами розробки. Користувачі, які знають C ++, освоюють движок швидше, адже він використовує саме цю мову програмування. Втім, для тих, хто не знайомий з C ++, Unreal Engine теж піддається без проблем - все завдяки візуальному редактору Blueprints, який дозволяє створювати скрипти і розміщувати об'єкти, не написавши жодного рядка коду.

До того ж, движок містить безліч інструментів, які полегшують роботу з ним. Наприклад, підтримує безліч форматів текстур, точно передає фізичні властивості матеріалів, дозволяє змінювати об'єкти в реальному часі, задавати для них функції і коментарі, автоматично вибрати джерела освітлення, додати туман і інші ефекти, і так далі. Велику колекцію Ассет (платних і безкоштовних) можна використовувати при розробці ігор, а відкритий вихідний код движка дає можливість вносити в нього зміни при необхідності.



Движок гнучко підлаштовується під платформу розробки, що дозволяє оптимізувати гри під консолі, мобільні гаджети та ПК.

Eric Games стабільно тримає лідерські позиції в області передових технологій, тому Unreal Engine 4 напханий ними під зав'язку, забезпечуючи, при належному майстерності розробників відеогри, вражаючу візуальну складову з якісним освітленням (трасування променів в реальному часі, звичайно ж, підтримується), м'якими тінями, чесними відображеннями, достовірної анімацією персонажів і іншими ефектами. За рахунок цього, до речі, движок також використовується в створенні комп'ютерної графіки в кіноіндустрії - наприклад, його силами було створено дроїд K-2SO для «ізгоя-1» сцени з «У пошуках Дорі» і «Мандалорца».

Движок ідеально підходить для тривимірних AAA-проектів, особливо шутерів і пригодницьких екшенів, що підтверджується списком ігор, розроблених на Unreal Engine (причому всіх версій, а не тільки четвертої), в якому домінують представники саме цих жанрів. Ми відзначали, що UE створений для професіоналів, і в руках досвідченої команди цей движок здатний показати запаморочливу картинку.

Відкритий світ - місцевість без входу і виходу. Зазвичай це місто, острів або поселення, при спробах вибратися з яких персонаж наштовхується на стіну, пробку або щось подібне, що заважає перетнути кордон світу. В кінці-кінців, гравцеві це набридає, а при спробах повністю пройти карту він раз у раз знаходить нові цікаві мікролокації або квести, тому бажання знайти кінець світу відходить на другий план.

Завдання геймдизайнера при створенні безшовного світу - розробити локацію так, щоб вона повертала гравця до гри, а не супроводжувала його пошуків кінця карти. Тому міста можуть бути закільцьовані - всі вулиці будуть вести один на одного, а основна гра відбуватиметься десь в центрі карти.

У той же час безшовний світ відкриває нові можливості для досліджень місцевості. Наприклад, вентиляційні ходи і шахти в багатьох іграх з відкритим світом знаходяться в постійній досяжності. Дослідження їх захоплює людину і дає йому шлях безпечного переміщення між ділянками ігрової карти, що особливо важливо, якщо в грі часто ведуться поєдинки.

Незважаючи на те, що в реальному житті вентиляція є далеко не скрізь, а людина середньої комплекції навряд чи зміг би вільно по ній переміщатися, така опція в грі не здається дивною, а навпаки, додає ефект занурення. Це стосується і інших способів переміщення у відкритому безшовному світі.

Використання реалістичних локацій також йде на користь занурення. Театр, торговий центр, концертний зал - місця, в яких людина неодноразово бував в житті. Зберігаючи логіку будови локації, ви позбавляєте гравця від втрати часу на вивчення карти: опинившись в знайомій місцевості, простіше діяти інтуїтивно.

Основною складністю в геймдизайна є дотримання балансу між

свободою відкритого світу і структурою драматичного сюжету. Оскільки гравці можуть виконувати дії, про які геймдизайнер не припускав, сценаристи гри повинні придумати дотепні способи нав'язати гравцеві сюжет, не перешкоджаючи при цьому його волі. Як наслідок, в іграх з відкритим світом іноді сюжет гри може бути розділений на серію завдань, також сюжет може бути представлений в досить спрощеному вигляді. У деяких іграх побічні завдання, пропонувані гравцеві, не припиняють виконання основного завдання. У більшості ігор з відкритим світом новостворений персонаж не має будь-яких виражених особливостей, щоб гравець міг самостійно втілювати в ньому свої задуми. Проте, в деяких іграх на зразок Landstalker пропонується розширений набір діалогів при створенні персонажа. У 2005 році Девід Бребен так описав структуру оповіді в комп'ютерних іграх: «мало відрізняється від фільмів з Гарольдом Ллойдом 1920-х років» і щиро вважав, що сюжети з відкритим фіналом стануть «Святим Граалем, який ми шукаємо в п'ятому поколінні комп'ютерних ігор». Геймдизайнер Манвір Хейр (англ. Manveer Heir), який працював в Electronic Arts над іграми Mass Effect 3 і Mass Effect: Andromeda, говорив, що в геймдизайні ігор з відкритим світом присутні складності в порівнянні з лінійним геймдизайном, оскільки досить складно передбачити підхід гравців до вирішення задач, поставлених перед ними грою, це повинно бути рушійною силою розробки з самого початку. На думку Хейра, критичні недоліки в Andromeda стали наслідком того, що відкритий світ був введений в геймплей на занадто пізній стадії розробки.

Відкритий світ може являти собою простір без будь-яких заздалегідь заданих меж і орієнтирів, як в Minecraft, але в багатьох випадках розробники вважають за краще «підштовхувати» гравця до створення для нього цікавих місць і завдань, змусивши його зосередитися на певній галузі світу. Одним із способів це зробити є поділ світу на регіони з визначеними кордонами, так, щоб гравець освоював їх послідовно. При цьому гра може пропонувати гравцеві спосіб відкрити всі пункти інтересів в певному регіоні відразу, в нагороду за виконання якогось завдання або випробування

#### Перелік посилань

1. Движок unreal engine 4 – Режим доступу до ресурсу – <https://cubiq.ru/dvizhok-unreal-engine/>
2. Level design в комп'ютерних іграх: основи створення безшовної світу – Режим доступу до ресурсу – <https://koloro.ua/blog/3d-tekhnologii/level-design-v-kompyuternykh-igrakh-osnovy-sozdaniya-besshovnogo-mira.html>
3. Unreal Engine 4.x Scripting with C++ Cookbook - Second Edition By John P. Doran, William Sherif, Stephen Whittle Mastering Game Development with Unreal Engine 4 - Second Edition By Matt Edmonds

#### **Обчислювальний метод формування вихідного сигналу синтезатора високих частот**

Перспективним методом формування гармонійного сигналу синтезаторів високих частот є метод CORDIC (for COordinate Rotation DIgital Computer) [1,2], який використовує прості зсуви та операції віднімання та додавання для обертання координат вектору. Алгоритм CORDIC може бути використаний у 2-х режимах: векторний режим і режим обертання. В режимі обертання – робота алгоритму полягає у тому, що операція обертання розбивається на елементарні базисні повороти. Кожен базисний поворот може бути реалізований за рахунок зсуву, додаткового зсуву та арифметичної операції додавання. Режим обертання може бути використаний для обчислення значень синуса та косинуса кута  $\theta$ .

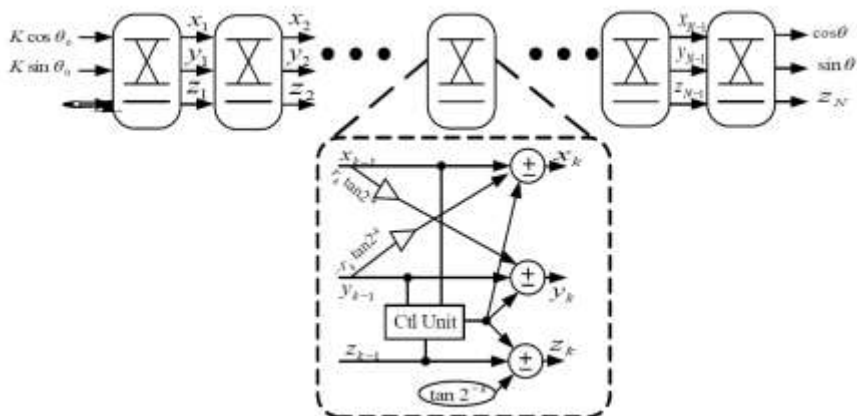


Рисунок 1 – Блок діаграма методу CORDIC [3]

Цей метод є затратним з точки зору апаратури, і є доцільним лише у разі застосування мікросхем ПЛІС (Програмованох Логічних Інтегральних Схем) або ASIC (Application-specific integrated circuit, «інтегральна схема для специфічного застосування»), аналіз показав, що архітектура побудована на основі методу CORDIC виграє у класичної архітектури, що заснована на Постійному запам'ятовуючому пристрої у разі застосування фазового слова більшого за 9-біт. Також метод CORDIC є ефективним для рішень квадратурного змішування частот. Звичайний квадратурний змішувач потребує двох суматорів, 4-х перемножувачів та пам'ять із значеннями косинуса/синуса додатково. А у методі CORDIC той самий результат

досягається із використанням 4-х перемножувачів, двох суматорів і ПЗП без використання опорного синтезатора частоти DDS, див. рис.2

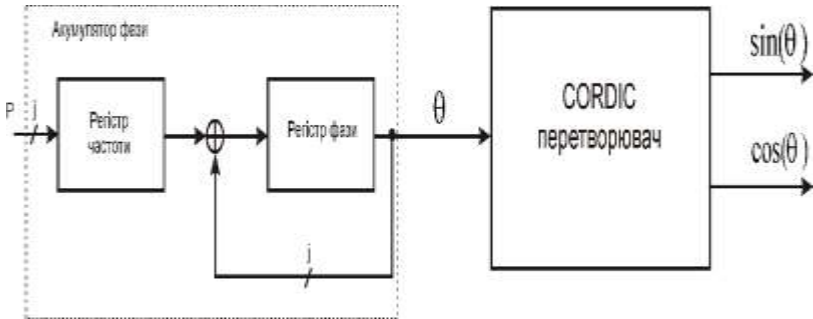


Рисунок 2 Спрощена діаграма синтезатора DDS, що базується на CORDIC алгоритмі

При реалізації CORDIC синтезаторів у високошвидкісній архітектурі досягається мала затримка синтезованого сигналу за рахунок конвеєрних регістрів між стійкими станами. Проте, кожна ітерація CORDIC вимагає утримування значень попередніх станів, що призводить до зростання площі схеми у разі зростання вимог до максимальної синтезованої частоти. Отже для оптимізації синтезу гармонійних сигналів, що ґрунтуються на CORDIC алгоритмі, необхідно забезпечити невелику розрядність вхідного кодового слова. Що призведе до зменшення необхідної площі, а отже споживаної потужності.

Основною ідеєю пропонованого методу є апроксимація вихідного сигналу рядом Тейлора і застосування замість 2-х ПЗП з відліками функцій синуса та косинуса однієї схеми CORDIC [3,4]. Таким чином вхідний сигнал CORDIC блока рівний  $i$  менший на  $i + j = N - 3$  біта. Відповідно для  $k$  біт вихідного розрізнення нам необхідно лише  $i$  біт вхідного фазового слова. Для досягнення поставленої мети роботи були застосовані наступні нововведення: використано апроксимацію рядами Тейлора другого порядку для забезпечення точності синтезу, використано конвеєрну CORDIC архітектуру для оптимізації системної швидкості, фазовий кут поділяється наступним чином:

$$N = i + j + 3.$$

Для генерації синусоїдального сигналу необхідно мати синусоїдальні та косинусоїдальні складові для апроксимації. На рис. 3 представлено функціональну схему методу, що пропонується. Фазу з акумулятора поділено

на дві частини:  $\varphi_0$  та  $\varphi - \varphi_0$ . Для першої частини фази  $\varphi_0$  конвеерний алгоритм CORDIC використовується для обчислення синусоїдальної та косинусоїдальної функцій від  $\varphi_0$ . А друга частина кута  $\varphi - \varphi_0$  використовується для обчислення ряду Тейлора. Відповідно до рівняння: використовується два суматори та три перемножувачі для апроксимації [5,6].

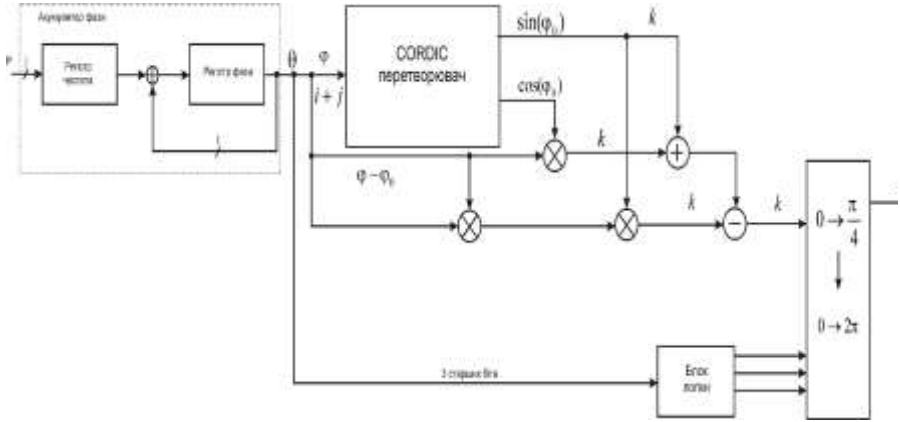


Рисунок 3 – Структурна схема перетворення кутів у алгоритмі CORDIC

Розглянуто результати моделювання запропонованої архітектури синтезатора. Для моделювання використано розмірність кута фази у 20 біт ( $i=10$  біт та  $j=10$  біт). Отже вихідне розрізнення CORDIC синтезатора складає 20 біт. Результати моделювання спектру вихідного сигналу синтезатора наведені на рис.4. Величина зменшення бічних складових синтезованого гармонійного сигналу складає 112 дБ. Ця величина залежить від точності перетворювача CORDIC, так для слова в 16 біт і 24 біти подавлення складе відповідно 82 дБ та 148 дБ.

Моделювання проводилось у САПР Xilinx Vivado 2013 із застосуванням мови VHDL. Моделювання проведено для пристрою VIRTEX 5 XC5VFX200T з тактовою частотою 50 МГц [7].

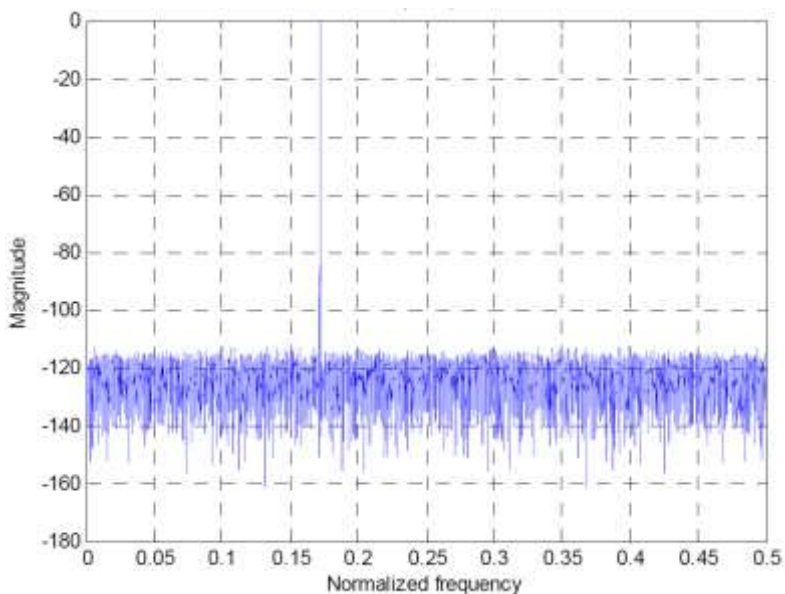


Рис.4 Спектр сигналу DDS пропонованого методу

В роботі показано, що застосування пропонованого методу апроксимації гармонійного вихідного сигналу рядами Тейлора та CORDIC є хорошою альтернативою для перспективних цифрових синтезаторів прямого синтезу (DDS). Поділ кута і конвеєризація CORDIC дає можливість значно зменшити затримки, що виникають у синтезаторах з іншою архітектурою. Порівняння із відомими методами показує на високу максимальну синтезовану частоту даного типу синтезаторів поряд із високим подавленням бічних складових. Пропонований метод застосовує апроксимацію Тейлора другого порядку, що дає можливість використати малий обсяг постійного запам'ятовуючого пристрою при значній величині фазового акумулятора. У перспективі необхідно розглянути оптимізацію такого синтезатора у ASIC мікросхемах, попередній аналіз показує що максимальна робоча частота такого синтезатору може досягти - 600 МГц.

#### Перелік посилань

1. Antelo E. Low-Latency Pipelined 2D and 3D CORDIC Processors / Antelo E., Villabla J., Zapata E.L. // IEEE Transaction on Computers. – 2008. – V. 57. – №3. – P. 404–417.
2. Mondwurf S.W. Versatile COFDM Demodulation Based on the CORDIC-Algorithm / Mondwurf S.W. // IEEE Transaction on Consumer Electronics. – 2002. – V. 48. – №3. – P. 718–723.

3. Полікарівських О.І. Прямі цифрові синтезатори частоти з комбінованим методом формування вихідного гармонічного сигналу / Полікарівських О.І. // Вісник Хмельницького національного університету. – м.Хмельницький, 2014.– №1. – С.178–185
4. Полікарівських О.І, Мішан В.В. Методи підвищення якості спектральних характеристик високошвидкісних обчислювальних синтезаторів частоти (DDS) / О.І. Полікарівських // Вісник Хмельницького національного університету. –м.Хмельницький, 2013.– №5. – С.208–211
5. Park Y. Fixed–point error analysis of CORDIC processor based on the variance propagation formula. / Park Y., Cho N. I. // IEEE Transaction Circuits and system I. – 2004. – V. 51. – 3. P. 573–584.
6. Valls J. The use of CORDIC in software defined radios: A tutorial. / Valls J., Sansaloni T., Pascual A. // IEEE Communications . –2006. – V. 44. – №9. – pp. 46–50.
7. Полікарівських О.І. Оцінка співвідношення сигнал–шум у CORDIC цифрових обчислювальних синтезаторах /О.І.Полікарівських // Міжнародний науково–технічний журнал Вимірювальна та очислювальна техніка в технологічних процесах. – Хмельницький, 2012.– №3– С.52–57

### **Вплив температури повітря на точність локалізації мобільного робота**

Матюк Д.С., Мишко О.Є.

Науковий керівник – к.т.н. Деркач М.В.

Східноукраїнський національний університет імені Володимира Даля

В останні роки великий інтерес для дослідників представляють автономні мобільні роботи, здатні здійснювати точну локалізацію та оптимальну навігацію, завдяки новітнім технологіям [1]. В зв'язку з чим, була здійснена розробка мобільного колісного робота, що передбачає наявність рухомого шасі з керованими приводами та ультразвукових датчиків, які дозволять сприймати навколишнє середовище й орієнтуватися в ньому.

Загалом, у розробці були використані наступні компоненти (рис. 1):

1. 32-бітовий мікроконтролер виробництва STMicroelectronics.
2. Ультразвукові датчики відстані безконтактного типу HC-SR04.
3. Драйвери двигунів L9110S.
4. Макетна плата та двигуни.

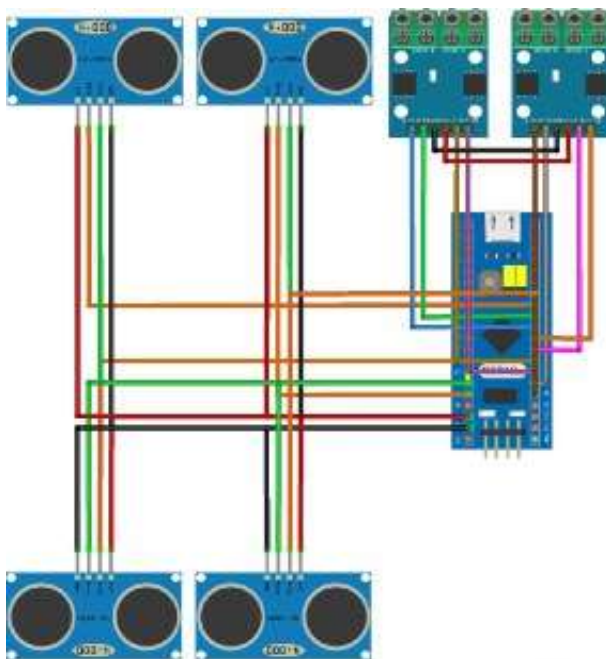


Рисунок 1 – Схема підключення компонентів мобільного робота

Датчики за допомогою ультразвукових хвиль виконують сканування навколишнього середовища на наявність перешкод при переміщенні мобільного робота. Принцип дії таких датчиків полягає в наступному: на платі модуля є п'єзо-ультразвуковий передавач та мікрофон, що відчуває високочастотну хвилю (25-40 кГц), яка відбивається перешкодою протягом імпульсу певної тривалості. За допомогою мікроконтролера відбувається злагоджена робота приймача і передавача ультразвуку, обчислення відстані до об'єкту, розрахунок зміни параметрів ехо-імпульсу [2]. І хоча, на відміну від інфрачервоних далекомірів на ультразвуковий датчик HC-SR04 не впливають джерела світла або колір перешкоди, є суттєвим той факт, що швидкість звуку в повітрі залежить від температури. Це впливає на точність датчиків, а як наслідок і на точність локалізації мобільного робота. Залежність швидкості звуку  $v$  від температури повітря (табл. 1) виражається формулою (1):

$$v = \sqrt{\frac{\gamma \cdot R \cdot T}{M}}, \quad (1)$$



де  $\gamma = 1,40$  – показник адиабати повітря;  $M = 29 \cdot 10^{-3}$  кг/моль – молярна маса повітря;  $R = 8,31$  Дж/моль·К – газова постійна;  $T$  – температура повітря в Кельвінах.

Таблиця 1 - Залежність швидкості звуку від температури повітря

Температура повітря		Швидкість ультразвуку в залежності від температури повітря	
t, °C	T, К	м/с	км/год
0	273,15	331,0	1191,6
10	283,15	337,0	1213,2
20	293,15	342,9	1234,4
22	295,15	344,1	1238,8

Тоді, як зазвичай, для ультразвукових датчиків прийнято вважати  $v = 340$  м/с - швидкість ультразвуку. На прикладі відстані мобільного робота до можливої перешкоди рівної 55 см в залежності від зміни температури від 0°C до 22°C перерахуємо й отримаємо відповідні відстані 52см, 53см, 54см та 55 см.

Таким чином, найменша похибка при локалізації мобільного робота спостерігається при реальній температурі приміщення 22°C. Вирішити ж проблему локалізації для різного температурного режиму можна, встановивши датчик температури і регулювати значення швидкості ультразвуку в залежності від показань датчика температури.

#### Література

1. Nagy C. Ultrasound-Based Indoor Robot Localization Using Ambient Temperature Compensation / C. Nagy, Z. Biró-Ambrus, L. Márton // Acta Universitatis Sapientiae Electrical and Mechanical Engineering. – Vol. 8. – 2016. – pp. 19-28.

2. Stączek P. Digital signal processing in ultrasonic based navigation system for mobile robots / P. Stączek // ITM Web of Conferences. – Vol. 15. – 2017.

## **Використання технології розпізнавання образів для автоматизації обліку показників побутових лічильників енергії**

Мельник О. Д.

Науковий керівник – д.т.н., проф. Журавська І. М.

Чорноморський національний університет імені Петра Могили

На теперішній час багато уваги приділяється автоматизації обліку спожитих енергоресурсів та безперервного моніторингу їх витрачання для попередження їх несанкціонованого відбору [1]. Поки що не існує єдиної концепції розв'язання даної задачі [2]. Але велика увага приділяється дослідниками можливості автоматизованого обліку електроенергії даної системи на базі мікроконтролерів Raspberry Pi [3]. Слід зауважити, що існуючі розробки передбачають безпосереднє підключення мікроконтролера до пристрою обліку (електролічильника) засобами кабельної лінії зв'язку. Але тільки 30 % лічильників електроенергії, встановлених у приватних оселях, мають вбудований порт RS-485 для автоматичної передачі показників до загальної облікової системи. Тому актуальним є саме використання технології розпізнавання образів (в даному випадку цифрових значень у вікнах щитка лічильника) для автоматизації обліку показників побутових лічильників. Запропонований підхід спроможний забезпечити автоматизований облік показників не тільки побутових лічильників електроенергії, але й будь-яких, що мають цифрове табло на корпусі (лічильники газу, тепла, гарячої та холодної води).

Суть роботи пристрою в тому, що він зчитуватиме цифри, передаватиме їх на сервер та відправлятиме їх на сайт енергопостачального підприємства. Сторінку сайту АТ «Миколаївобленерго» з даними обліку показано на рис.1. Додатковою функцією буде формування графіків спожитих ресурсів та порівняння їх із графіками оплати по рахункам.

Для розробки зазначеного пристрою знадобляться такі компоненти (рис. 2):

- 1) одноплатний мінікомп'ютер Orange PI;
- 2) відеокамера ESP32-CAM;
- 3) WiFi-модуль;
- 4) джерело живлення.

Потужності одного Orange PI вистачить, щоб обробляти дані з великої кількості камер, тому система буде працювати стабільно незалежно від кількості отримуваних даних.

Дані з лічильника енергії потрапляють на камеру ESP32-CAM візуальним контактом (англ. Line-of-Sight або LoS). Висока роздільна здатність матриці датчика відеокамери OV2640 від компанії OmniVision Technologies – 1600 × 1200 пікселів (UXGA) – робить отримане зображення придатним до подальшого посимвольного розпізнавання показників лічильника енергії. Сам модуль має потужні характеристики, які дозволяють отримувати не тільки зображення, а за необхідністю й відеопотік.

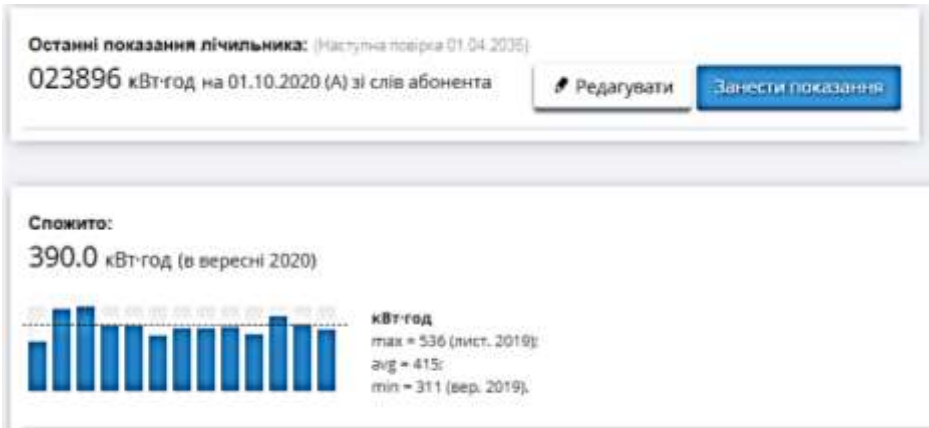


Рисунок 1 – Сторінка для заповнення показників лічильнику та графік динаміки споживання електроенергії на сайті АТ «Миколаївобленерго»

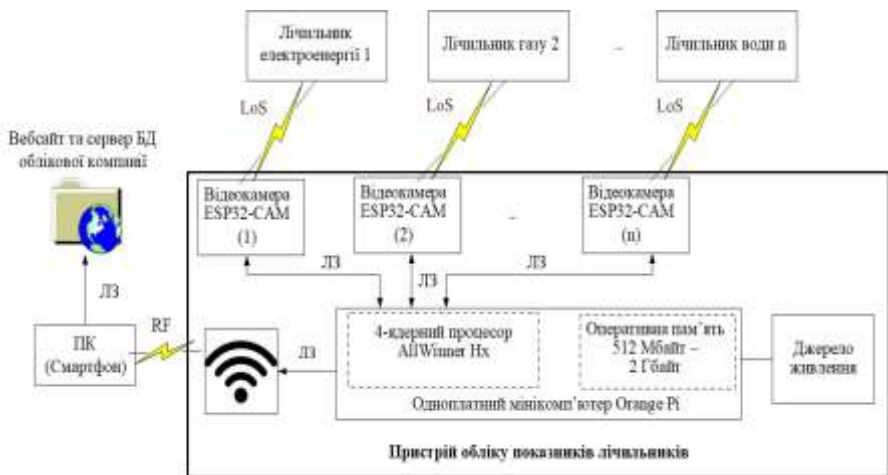


Рисунок 2 – Структурна схема підключення пристроїв до системи моніторингу показників побутових лічильників

Простота підключення та налаштування зазначеного модулю роблять всю автоматизовану систему збору даних не тільки продуктивною, а ще й простою в експлуатації. Також перевагою є невелика ціна цього модулю (від 5\$ US).

Послідовність обробки даних передбачає такі етапи:

- 1) отримання зображення з лічильнику за допомогою модулю камери ESP32-CAM;
- 2) передача зображення на одноплатний комп'ютер Orange PI;
- 3) оброблення зображення одним з обраних алгоритмів [4] та внесення в базу значення з лічильнику;
- 4) оброблення значень, побудова графіків спожитих ресурсів;
- 5) автоматичне внесення даних на сайт облікової компанії через інтернет-з'єднання.

Найбільш популярними моделями розпізнавання для описаної системи можна визначити такі, що базуються на згорткових нейронних мережах (англ. convolutional neural network або CNN). Це такі моделі як VGG-16 [5], Resnet та Inception v4 [6]. Модель VGG має два серйозні недоліки:

- дуже повільна швидкість навчання;
- сама архітектура згорткової мережі важить надто багато (з'являються проблеми з розміром пам'яті – біля 500 Мбайт – і пропускнуою здатністю).

Модель ResNet має менше фільтрів та складність менше ніж мережі VGG навіть з тривірневими блоками [50/101/152]. При тестуванні використовуються усі шари, але їх виходи можуть бути модифіковані — помножені на ймовірність використання саме цього шару при навчанні.

У моделі Google Inception введено новий рівень організації у формі «Початкового модуля», а також збільшена сама мережа. Гібридна архітектура Inception-ResNet значно покращує продуктивність розпізнавання. Це важливо, коли у лічильниках використовується не суцільне механічне або електронне табло (рис. 3, а, б), а окремі неконтрастні цифри, значно заглиблені – кожна в окремому віконці (нп., у лічильниках води, рис. 4).

Таким чином, вибір моделі для розпізнавання показників лічильників має бути обґрунтованим для кожної конструкції табло в залежності від похибки розпізнавання.



а)



б)

Рисунок 3 – Суцільне механічне (а) та електричне (б) табло у лічильниках та механічне табло з поглибленими цифрами у віконцях



Рисунок 4 – Механічне табло з поглибленими цифрами у віконцях

У програмній частині проекту використовується мова програмування Python. Для цієї мови написана велика кількість бібліотек для розпізнавання образів, машинного навчання. Також за допомогою цієї мови програмування можна легко отримувати інформацію із сайтів за допомогою парсингу сайту. Розпізнавання цифр з фото може здійснюватися з використанням бібліотеки OpenCV. Це бібліотека комп'ютерного зору і машинного навчання з відкритим вихідним кодом. Вона є популярною та легкою у використанні, тому не буде ніяких складнощів в розробці програмного забезпечення для цієї системи.

Розроблювана автоматизована система моніторингу витрачання енергії може бути корисною при створенні технічного погодинного обліку спожитої енергії для багатотарифних лічильників. води, газу, тепла та електроенергії

#### Перелік посилань

1. Автоматична система контролю і обліку енергоносіїв. URL: <https://novator-tm.com/index.php?id=meters-askoe> (дата звернення: 25.10.2020).
2. Гонекс О.В. Аналіз функцій системи управління базами даних в системі / О.В. Гонекс, В.О. Бобровнік, А.В. Додик // Вісник Вінницького політехнічного інституту. – 2008. – № 1. – С. 59–64.
3. Осіпова А.О. Енергоефективна автоматизація багатоквартирних будинків на основі технології IoT / А.О. Осіпова, В.Ю. Харламенко // Гірничий вісник. – 2017. – Вип. 102. – С. 154–158.
4. Tonioni A. Domain invariant hierarchical embedding for grocery products recognition / A. Tonioni, L. Di Stefano // Computer Vision and Image Understanding. – 2019. – Vol. 182. – P. 81–92.
5. Simonyan K. Very deep convolutional networks for large-scale image recognition / K. Simonyan, A. Zisserman // Conference paper at ICLR. – 2015. – 14 p.
6. Szegedy C. Inception-v4, inception-resnet and the impact of residual connections on learning / C. Szegedy, S. Ioffe, V. Vanhoucke, A. A. Alemi // Association for the Advancement of Artificial Intelligence (AAAI). – 2017. – P. 4278–4284.

## **Метод нейромережевого керування системою адаптивного радіозв'язку Software Defined Radio**

Михальський В.М

Науковий керівник – д.т.н., проф. Полікарівських О.І.

Хмельницький національний університет

У сучасних радіо - передавальних/радіоприймальних засобах широко використовується технологія SDR (Software Defined Radio), що дає можливість швидкого переналаштування параметрів сигналів приймально-передавальних пристроїв, таких як: частота, вид модуляції, вид кодування у середині повідомлення, що передається. Це обмежує можливості моніторингу та перехоплення повідомлень у ефірі. На перший план виходить швидкість визначення параметрів сигналів, що передаються. Пропонований метод спрямований на вирішення проблеми швидкого аналізу радіосигналів на основі SDR шляхом застосування нейромережевих методів розпізнавання сигналів. Розробка методу дасть можливість створити системи зв'язку із покращеними тактико-технічними характеристиками; системи радіозв'язку із стрибачими частотами, системи зв'язку когнітивного радіо.

Розвиток найважливіших галузей сучасної науки і техніки, особливо таких як телекомунікації, радіолокація і радіонавігація, значною мірою визначається рівнем розвитку засобів радіозв'язку. Історично однією з перших реалізацій систем SDR була система SPEAKeasy [1], яка стала успішним проектом по використанню комунікаційних систем на базі технології Software Defined Radio у військовому обладнанні США. Система випробовувалася в США в 1970 році. SPEAKeasy дозволяла цифровій апаратній платформі загального призначення здійснювати зв'язок з іншими системами в широких діапазонах частот, видів модуляції, методів кодування даних і варіювання інших параметрів. Розробники обладнання мобільної телефонії, розглядають технологію Software Defined Radio, як на альтернативу традиційній архітектурі сьогоденних стільникових телефонів. Апаратне забезпечення стільникового телефону з архітектурою SDR потенційно підтримує всі стандарти мобільної телефонії, а його фактичні параметри визначаються завантаженою прошивкою вбудованого програмного забезпечення. Такий мобільний пристрій спроможний більш ефективно використовувати радіочастотний спектр і споживану від джерела живлення енергію, легко перемикається із будь якого стандарту зв'язку на інший. Операційна система SDR, як правило, використовує відкриту архітектуру і це дозволяє пристроям обмінюватись інформацією між собою. Шифрування сигналів програмується і є доволі гнучким. Наприклад, на SDR радіостанції можливо завантаження відомого алгоритму шифрування SINCGARS, або іншого спеціалізованого програмного забезпечення. SDR технологія дає користувачу велику функціональну гнучкість, яка реалізується на єдиній апаратній платформі, і дає змогу

працювати з різними класами радіозв'язку. Однією з ключових переваг SDR у військовій сфері, є взаємодія між засобами зв'язку попередніх поколінь і сучасними системами. Оновлення військових систем радіозв'язку не може зрівнятися темпами з розвитку сучасних цивільних комунікаційних засобів. Тому дуже важливо, щоб нові і старі системи могли працювати сумісно і забезпечити поступовий перехід на нові стандарти когнітивного радіозв'язку. SDR здійснює адаптацію до спектрів протоколів. Таким чином, можлива взаємодія між різними моделями радіостанцій. Також SDR може виконувати роль ретранслятора і брати участь в створенні безпроводних мереж передачі даних, автоматично, без необхідності введення даних користувачем. При цьому оператор може використовувати станцію для зв'язку в будь-який момент часу. В роботах авторів [2,3,4] лишилися не вирішеними питання пов'язані із зростанням часу затримки формування сигналів когнітивного радіо. Проте не запропоновано шляхів її однозначного та простого вирішення. Подальшого дослідження потребують методи та способи створенні високошвидкісних когнітивних засобів визначення зайнятості діапазонів, а також нейромережеві методи визначення параметрів радіосигналів.

Когнітивні радіомережі поділяють на два типи, первинні (ліцензованих користувачів) і вторинні (не ліцензованих користувачів). Первинні користувачі мають пріоритет для використання ліцензованої смуги частот. Вторинний користувач може використовувати ліцензовану смугу частот, не впливаючи на пріоритетне використання спектру основним користувачем, що підвищує ефективність використання ліцензованого спектру. Питаннями збільшення ефективності використання радіочастотного спектра займався Д. Мітола (J. Mitola) [1], і на основі його робіт з'явилася концепція когнітивного радіо. Когнітивне радіо - це бездротова інтелектуальна система зв'язку, здатна аналізувати навколишнє середовище і пристосовуватися до неї за допомогою навчання, реагуючи на зміни в оточенні, зміною своїх власних параметрів (наприклад, несучої частоти, потужності, способу модуляції) в реальному часі з метою збільшення ефективності використання спектрального ресурсу. Відмінною особливістю систем когнітивного радіо є їх здатність виявляти і динамічно використовувати вільні діапазони радіочастот для доступу абонентів до мережі когнітивного радіо. Така можливість здійснюється за допомогою автономного моніторингу спектра в усьому робочому діапазоні радіочастот, який може становити від одиниць МГц до декількох ГГц і залежить від стандарту, що використовує когнітивні функції. Основним завданням моніторингу спектра (МС) в когнітивному радіо є виявлення сигналів, що діють у всьому робочому діапазоні частот, і розбиття цього діапазону на «зайняті» та «вільні» смуги. Оскільки процес МС в когнітивному радіо виключає присутність оператора, коригуючого параметри системи, потрібне застосування таких алгоритмів виявлення, якісні характеристики яких були б

стійкі по відношенню до невідомих параметрам і властивостям реєстрованих сигналів в широкому діапазоні робочих частот. Завдання виявлення сигналів в когнітивному радіо ускладнюється обмеженістю апіорних даних про радіосигнали які необхідно виявляти, а, найчастіше, вони повністю відсутні. Одним із шляхів подолання апіорної невизначеності полягає в застосуванні адаптивних алгоритмів виявлення (АВ). В даному напрямку працювали такі вчені як А.М. Рембовский, А.Б. Токарев. Існуючі адаптивні параметричні АВ радіосигналів синтезовані на основі моделей стандартних законів розподілу, таких як розподіл Гауса, Релея, Раїса і ряду інших подібних розподілів, і в разі зміни виду функції розподілу сигналу ефективність виявлення таких алгоритмів (оптимальних, як правило, тільки для однієї моделі розподілу) різко знижується. Іншим шляхом подолання апіорної невизначеності може бути застосування алгоритмів, що використовують принципи інваріантності. В останній час завданням синтезу інваріантних АВ займалися такі фахівці як В. А. Богданович, М.С. Шевченко, А.О. Чемаров. Розроблені цими вченими алгоритми забезпечують ефективне виявлення лише вузькосмугових сигналів, характерних, в основному, для КВ діапазону. Такі АВ можуть бути засновані на застосуванні кореляційного аналізу, вейвлет-аналізу або перевірки спостережуваного сигналу на циклостационарність. Зазначені методи мають високу завадостійкість щодо класичного енергетичного приймача, але при цьому вимагають великих обчислювальних витрат. Крім того, для більшості даних алгоритмів необхідно апіорне знання ширини смуги виявленого сигналу, що на практиці найчастіше не реалізовується. Сучасні стандарти бездротової передачі даних комбінують в собі вузькосмугові і широкосмугові сигнали, що використовують різні види модуляцій, що не дозволяє створити єдину модель для статистичного опису всіх типів використовуваних сигналів, тому особливу увагу при розробці АВ для систем когнітивне радіо слід звернути на непараметричні методи виявлення. Таким чином, в даний час є актуальною задача створення алгоритмів виявлення радіосигналів, орієнтованих на застосування в умовах апіорної невизначеності щодо діючих в робочій смузі радіосигналів для вирішення завдання моніторингу сигналів в когнітивному радіо у широкому діапазоні частот.

Проблема дослідження когнітивних радіомереж є актуальною в Україні, тому що ліцензовані смуги радіоспектра можуть використовувати тільки ті оператори, за якими вони закріплені. Однак смуги радіочастот, у яких здатні працювати сучасні телекомунікаційні системи, є кінцевим ресурсом. Використання цього ресурсу ефективно не на всіх доступних частотах. Отже, удосконалення топології когнітивних радіомереж є актуальним напрямком.

Не менш важливим питанням є використання нейромережевих алгоритмів [5]. Нейромережеві алгоритми - досить потужний засіб аналізу сигналів. Вони можуть з успіхом застосовувати для широкого класу прикладних задач, враховуючи ті, які важко, а іноді і зовсім неможливо



розв'язати іншими методами. Однією з переваг таких алгоритмів є те, що вони можуть застосовувати навіть на складних завданнях, там, де не існує ніяких інших, ефективних методів рішення. Все ж на сьогоднішній день питання нейромережових алгоритмів залишається мало дослідженим у напрямку застосування до систем SDR.

Одним з перспективних підходів до розпізнавання видів цифрової модуляції є метод використанням кумулянтів і моментів високого порядку; суть даного методу полягає в використанні у якості інформаційних ознак розпізнавання сигналів з різними видами модуляції моментів і кумулянтів високих порядків, що обчислюються за зареєстрованими значенням відліків квадратурних складових радіосигналу. Особливістю методу є формування правил розрізнення видів модуляції за результатами експертного аналізу значень кумулянтів для різних видів модуляції сигналів. Формування правил розрізнення здійснюється з використанням різних методів інтелектуального аналізу, наприклад методом штучних нейронних мереж. Високу ефективність побудови розділюючих поверхонь в багатомірному випадку показує такий тип штучної нейронної мережі як розділюючий перцептрон. Такий підхід є безумовно новим та оригінальним.

Розробка методу нейромережевого керування системою адаптивного радіозв'язку SDR цифрового радіозв'язку з когнітивним методом керування каналом і з підвищеною швидкістю дасть поштовх для розвитку телекомунікаційної галузі України. Розробка високошвидкісного методу дасть можливість застосувати SDR в існуючих та перспективних системах радіозв'язку, таких як системи транкінгового зв'язку, системи радіозв'язку із стрибуючою частотою. А така система SDR може мати важливе значення для розвитку військової техніки.

#### Перелік посилань

1. Software-Defined Radio for Engineers, by Travis F. Collins, Robin Getz, Di Pu, and Alexander M. Wyglinski, 2018, ISBN-13: 978-1-63081-457-1.
2. K. Vachhani and R. A. Mallari, "Experimental study on wide band FM receiver using GNURadio and RTL-SDR," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Kochi, 2015, pp. 1810-1814. doi: 10.1109/ICACCI.2015.7275878
3. J. Muslimin, A. L. Asnawi, A. F. Ismail and A. Z. Jusoh, "SDR-Based Transceiver of Digital Communication System Using USRP and GNU Radio," 2016 International Conference on Computer and Communication Engineering (ICCCE), Kuala Lumpur, 2016, pp. 449-453. doi: 10.1109/ICCCE.2016.100
4. M. Bhowmik and P. Malathi, "Load balancing using game theory in cognitive radio network," 2016 International Conference on Computing, Communication and Automation (ICCCA), Noida, 2016, pp. 582-587. doi: 10.1109/CCAA.2016.7813788

5. D. Block, D. Töws and U. Meier, "Implementation of efficient real-time industrial wireless interference identification algorithms with fuzzified neural networks," 2016 24th European Signal Processing Conference (EUSIPCO), Budapest, 2016, pp. 1738-1742. doi: 10.1109/EUSIPCO.2016.7760546

### **Моделювання транспортного каналу з полярними кодами для мобільного зв'язку п'ятого покоління**

Ніколайчук І. А.

Науковий керівник – к.т.н., доц. Пятін І.С.  
Хмельницький національний університет

Технології завадостійкого кодування є невід'ємною частиною сучасних систем зберігання і передачі інформації. Протягом розвитку теорії завадостійкого кодування було побудовано велике число різноманітних кодів, що виправляють помилки. Однак їх характеристики залишаються далекими від теоретичних меж, а ймовірність помилки декодування, демонстрована ними при використанні в системах передачі інформації, виявляється гірше принципово досяжної. Однією з причин цього є неможливість практичного використання оптимальних алгоритмів декодування, складність яких виявляється надмірно високою.

Одним з головних методів підвищення надійності та ефективності передачі даних по каналах цифрового та супутникового зв'язку є завадостійке кодування. Полярні коди [1] досягають пропускну здатності двійкового симетричного каналу без пам'яті (ДСКБП), також відрізняються простотою побудови, кодування і декодування.

Кодування. Полярний код  $C$  задається набором параметрів  $(N, K, A_c)$ , де  $N$  - довжина кодового слова;  $K$  - розмір інформаційної частини кодового слова;  $A_c$  - множина «заморожених» символів, що грають роль перевірючих символів,  $|A_c| = N - K$ ,  $A_c \subset \{0, \dots, N-1\}$ .

Множина  $A_c$  може бути отримано за допомогою поляризації каналу. Поляризація каналу описується лінійним перетворенням, що задається матрицею  $F^{\otimes n}$ , де  $F$  - ядро поляризації;  $F = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ ;  $\otimes n$  -  $n$ -кратний добуток матриць Кронекера;  $n = \log_2 N$ ,  $N$  - довжина кодового слова.

Процедура кодування описується виразом  $x_1^N = u_1^N G_N$ , де  $x_1^N$  - кодове слово;  $u_1^N$  - вектор, що включає інформаційні символи ( $u_i \notin A_c$ ,  $1 \leq i \leq N$ ) і «заморожені» біти ( $u_i \in A_c$ ,  $1 \leq i \leq N$ );  $G_N$  - породжуюча матриця, що задається виразом  $G_N = B_N F^{\otimes n}$ , де  $B_N$  - матриця перестановок.

Для здійснення операції поляризації необхідно провести трансформацію скалярного каналу в векторний канал, ототожнюючи його з функцією щільності умовної ймовірності вихідного символу. Це досягається за рахунок створення копій ДСК рекурсивним способом, як представлено на рис. 1.

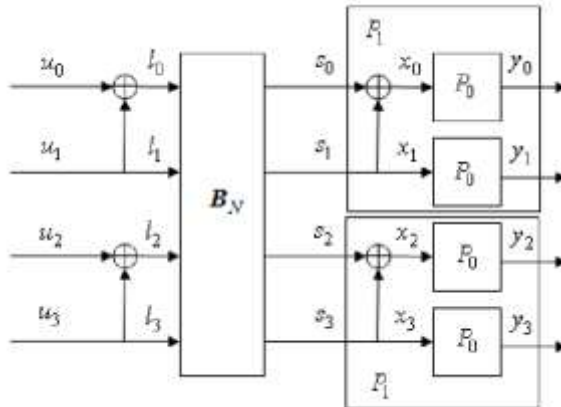


Рисунок 1 – Рекурсивний спосіб формування кодового вектора

Рекурсія починається з 0-го рівня ( $n = 0$ ) за допомогою застосування тільки одного примірника  $P$ , і йому ставиться у відповідність  $P_0 = P$ . На першому рівні рекурсії схема поєднує в собі дві незалежних копії  $P_0$ , тим самим ми отримуємо канал  $P_1$  з ймовірністю переходів  $P_1(y_0 | y_1 | u_0, u_1) = P(y_0 | u_0 \otimes u_1) \cdot P(y_1 | u_1)$ . Схема побудови такої системи кратна степені 2, починаючи з нуля. На рис. 1.2 матриця перестановок  $B_N$  має входи  $(l_0, l_1, l_2, \dots, l_{N-1})$ .

Загальна форма рекурсивної залежності дорівнює:  $P_N(y_0^{N-1} | u_0^{N-1}) = P^N(y_0^{N-1} | u_0^{N-1} \cdot G_N)$ . Процес формування матриці  $B_N$  задовольняє наступним співвідношенням (для випадку  $m = 2$ ):  $l_0 \rightarrow s_0, l_1 \rightarrow s_2, l_2 \rightarrow s_1, l_3 \rightarrow s_3$ . Тобто, входи ранжуються по парних і непарних номерах (залежить від нульової точки - нумерація з «0» або «1»), їм ставляться у відповідність виходи, які нумеруються строго по порядку з нульової точки. Вказаний метод полягає у поданні  $P_N(y_0^{N-1} | u_0^{N-1})$  як сукупності  $P' = \{P_N^{(i)}(y_0^{N-1}, u_0^{N-1} | u_i), 0 \leq i \leq N\}$  двійкових каналів, що представлено на рис 2.

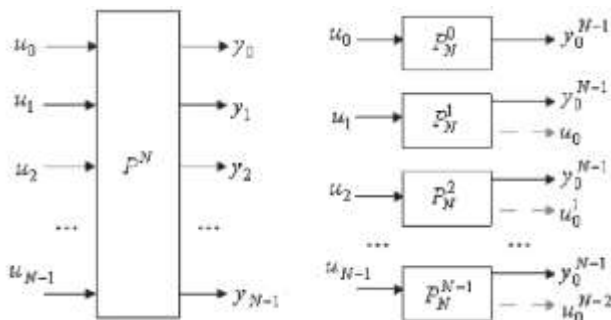


Рисунок 2 – Еквівалентні схеми векторного і скалярного каналів

Декодування. Для декодування полярних кодів використовується алгоритм послідовного виключення (SC). Алгоритм заснований на розрахунку коефіцієнта правдоподібності для кожного символу на кожному рівні поляризації каналу. Число вузлів визначається як  $N(\log_2 N + 1)$ . Також варто відзначити, що SC-декодування є алгоритмом з м'яким рішенням.

Застосування м'яких методів обробки отриманих даних дозволяє домогтися додаткового енергетичного виграшу, а застосування полярних кодів є новим етапом розвитку кодових методів обробки інформації. Пропускна здатність ДСК визначається співвідношенням  $C_{ДСК} = 1 + (1 - \varepsilon) \cdot \log_2(1 - \varepsilon) + 2 \cdot \log_2 \varepsilon$ , де  $\varepsilon$  - ймовірність помилки на біт. У випадку застосування двійкового стираючого каналу зв'язку (ДСКЗ), пропускна здатність дорівнює

$$C_{ДСКЗ} = 1 - q + (1 - p - q) \cdot \log_2 \frac{1 - p - q}{1 - q} + p \cdot \log_2 \frac{p}{1 - q},$$

де  $q$  - ймовірність

стирання, а  $p$  - ймовірність помилки стертого символу [16]. Очевидно, що

$C_{ДСК} \leq C_{ДСКЗ}$ , причому рівність досягається при значенні  $p, \varepsilon \rightarrow 0$ . Позначимо

через величину  $C_{МД}$  пропускну здатність каналу зв'язку при м'яких методах

обробки символів, тоді  $C_{ДСК} \leq C_{МД} \leq C_{ДСКЗ}$ .

Технологія обробки полярних кодів (ПК) спирається на перетворення безперервного каналу зв'язку в систему векторних каналів з перехресними зв'язками і повним виключенням з аналізу прийнятої послідовності тих каналів, в яких передача бітів виявляється ненадійною. Пропускна здатність таких каналів прийнято вважати рівною нулю (канали вважаються «замороженими»), а відновлення даних здійснюється за рахунок інформації, отриманої з надійних каналів. За рахунок використання ПК досягається підвищення енергетичної ефективності системи зв'язку. Однак, для полярних

кодів, результат кожного кроку декодування повністю залежить від достовірності оцінок інформаційних бітів попередніх кроків.

#### Перелік посилань

1. V. Bioglio, C. Condo and I. Land, "Design of Polar Codes in 5G New Radio," in *IEEE Communications Surveys & Tutorials*, pp.1, Jan. 2020, <https://doi.org/10.1109/COMST.2020.2967127>.

2. Z. B. Kaykac Egilmez, L. Xiang, R. G. Maunder and L. Hanzo, "The Development, Operation and Performance of the 5G Polar Codes," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 96-122, Firstquarter 2020, <https://doi.org/10.1109/COMST.2019.2960746>.

3. J. Bae, A. Abotabl, H. Lin, K. Song and J. Lee, "An overview of channel coding for 5G NR cellular communications," *APSIPA Transactions on Signal and Information Processing*, 8, E17. 2019, <https://doi.org/10.1017/ATSIP.2019.10>.

### **Проблема верифікації протоколів когерентності пам'яті**

Джулій А.В.<sup>1</sup>, Огнєвий О.В.<sup>2</sup>

Університет економіки і підприємництва, м.Хмельницький<sup>1</sup>

Хмельницький національний університет<sup>2</sup>

Мультипроцесори із загальною пам'яттю відносяться до базових класів високопродуктивних обчислювальних систем. Останнім часом такі системи отримали розвиток у формі багатоядерних мікропроцесорів, які об'єднують кілька процесорів (ядер) на одному кристалі. Характерно, що кількість ядер таких мікропроцесорів постійно збільшується. Розробкою багатоядерних мікропроцесорів і мультипроцесорних комплексів займаються в основному зарубіжні фірми (зокрема, IBM, Intel і AMD).

Основною проблемою, що виникає при створенні мультипроцесорів із загальною пам'яттю, є забезпечення узгодженого (когерентного) стану пам'яті. Кожне ядро має в своєму складі локальну кеш-пам'ять, через що в системі можуть співіснувати кілька копій одних і тих же даних: одна копія в основній пам'яті і кілька копій в кеш-пам'яті процесорів. При зміні будь-якої копії інші копії повинні бути або видалені, або змінені певним узгодженим чином. За це відповідають так звані контролери когерентності - пристрої підсистеми пам'яті, об'єднані в мережу що взаємодіють один з одним по спеціальному протоколу - протоколу когерентності.

Розробка механізмів, що відповідають за когерентність пам'яті, здійснюється в два етапи: проектування протоколу когерентності і реалізація протоколу в апаратурі. Зважаючи на складність сучасних протоколів на обох етапах можливі помилки. Помилки в протоколі когерентності особливо критичні і повинні бути виявлені до початку реалізації підсистеми пам'яті.

Пропуск помилок в протоколі може привести до помилок в реалізації, які не будуть знайдені до випуску мікропроцесора, і проявлять себе тільки під час роботи випущеного мікропроцесора.

В ході проектування мікропроцесорних систем протоколи когерентності спочатку розробляються на концептуальному рівні, в рамках створення мікроархітектури системи. Потім здійснюється їх реалізація шляхом складання RTL-опису (Register Transfer Level) сукупності пристроїв, які повинні працювати відповідно до протоколу когерентності пам'яті (RTL-опису мікропроцесора). При цьому поширеною практикою є аналіз протоколу його розробниками вручну, а потім перевірка його реалізації тестовими програмами з псевдовипадковими впливами [1]. Для скорочення часу моделювання мікропроцесорної системи розробляються прототипи системи, засновані на ПЛІС [2], а також в деяких випадках застосовується інтеграція RTL-опису і програмних моделей підсистеми пам'яті.

Даний підхід відкладає початок верифікації на місяці з моменту початку проектування. Верифікація реалізації протоколу проходить за відсутності будь-якої впевненості в коректності самого протоколу і це призводить до того, що навіть через роки після початку верифікації, все ще виявляються помилки в самому протоколі (і, відповідно, в реалізації некоректного протоколу). Псевдовипадкові тестові послідовності не забезпечують повноту покриття простору станів протоколу за прийнятний час. Незважаючи на те, що тестові програми з випадковими впливами дозволяють знайти велику кількість помилок, деякі помилки, а особливо помилки, пов'язані з нетривіальною організацією передачі повідомлень між частинами системи, можуть виявитися непоміченими.

Таким чином, надзвичайно важливим є завдання верифікації самих протоколів когерентності. Його рішення дозволить починати верифікацію на ранніх етапах проектування, при взаємодії розробників і верифікаторів. Вирішити задачу верифікації протоколів когерентності можна за допомогою розробки і аналізу математичних моделей протоколів.

Формальні методи дозволяють отримати математичний доказ відповідності моделі об'єкту що перевірається його специфікації, тобто набору властивостей, яким він повинен задовольняти.

Методика формальної верифікації протоколів передбачає наявність:

1. Засобів моделювання протоколів. Зазвичай в цій ролі виступають мови опису моделей.
2. Засобів (мов) специфікації протоколів для перевірки властивостей.
3. Методів верифікації, що дозволяють встановити, чи відповідає модель протоколу його специфікації.

Формальні методи поділяються на дві групи: методи, засновані на моделях і методи, засновані на доказах.

У методах, заснованих на моделях, верифіковані система представляються моделлю  $M$  формул деякої логіки. Специфікація представлена формулою  $sp$  даної логіки. Метод верифікації встановлює, чи є  $M$  моделлю  $sp(M \neq \phi)$ . Для кінцевих моделей таке встановлення, як правило, може бути автоматизовано.

У методах, заснованих на доказах (методах дедуктивної верифікації), система, що підлягає верифікації, представляється множиною формул  $F$  деякої логіки. Специфікація є іншою формулою  $ep$  даної логіки. Метод верифікації полягає в спробі знаходження доказу того, що  $sp$  виведена з  $F$  в даній дедуктивній системі  $F \neq \phi$ . Побудова такого висновку зазвичай не може бути повністю автоматизовано.

Для верифікації протоколів когерентності пам'яті застосовуються методи, засновані на моделях, методи, засновані на доказах, і комбіновані методи. В основному ці методи основані на використанні моделей протоколів когерентності у вигляді множин взаємодіючих процесів. І якщо навіть використовуються лінгвістичні засоби моделювання все одно це не дозволяє представляти процеси в явному вигляді.

При розробці методів верифікації протоколів когерентності пам'яті потрібно враховувати, що процеси є моделями кеш-контролерів і системного комутатора.

В роботі [3] пропонується використовувати в якості верифікованих протоколів протоколи German і FLASH. Протокол FLASH є складним, але якщо метод може верифікувати цей протокол, то існує ймовірність, що такий метод може бути придатний для верифікації протоколів реальних систем. Протокол German є істотно більш простим, однак він також відображає деякі риси реалістичних протоколів когерентності.

Аналіз методу перевірки моделей і автоматизованого доведення теорем показав, що метод перевірки моделей є повністю автоматизованим, але він може бути застосований лише до протоколів систем з 3-4 ядрами, а метод автоматизованого доведення теорем можна використати і для систем з будь-якою кількістю ядер, але це вимагає колосального обсягу ручної роботи.

Промисловість потребує методів верифікації систем з великим числом процесорних ядер (8, 16 і так далі), що робить метод перевірки моделей непридатним для верифікації протоколів когерентності сучасних систем.

Обмеження автоматизованого доведення теорем - необхідність надмірного обсягу ручної роботи і відсутність діагностичної інформації в ході верифікації - робить застосування даного методу недоцільним.

У зв'язку з постійним збільшенням кількості процесорних ядер сучасних мікропроцесорних систем, завдання верифікації протоколів когерентності пам'яті, що забезпечують узгодженість даних в таких системах, сформульована як задача параметризованої верифікації.

Протокол когерентності можна розглядати як параметризовану систему, що складається з певної кількості різних процесів і безліч ідентичних процесів, розмір яких є параметром. Іншими словами, протокол когерентності можна розглядати як нескінченне сімейство протоколів з кінцевим числом станів, в якому перший протокол спроектований для системи з двох ядер, другий протокол - для системи з трьох ядер і так далі. У зв'язку з цим завдання верифікації протоколів когерентності пам'яті доцільно поставити як завдання параметризованої верифікації.

У загальному випадку задача верифікації параметризованих моделей (параметризовані верифікації) алгоритмічно нерозв'язна [2]. У зв'язку з цим розробка методів її рішення ведеться в двох напрямках:

- розробка повних методів верифікації певних класів моделей з явним зазначенням всіх обмежень на моделі;
- розробка неповних методів, для яких немає гарантій завершення.

Класифікація методів параметризованої верифікації протоколів когерентності пам'яті наведена на рис. 1. Зазначені групи методів не є взаємно виключаючими і часто засновані на загальних ідеях.

Огляд методів параметризованої верифікації протоколів когерентності пам'яті показує, що більшість з них націлені на перевірку властивостей-інваріантів, і лише деякі розглядають перевірку властивостей живучості.

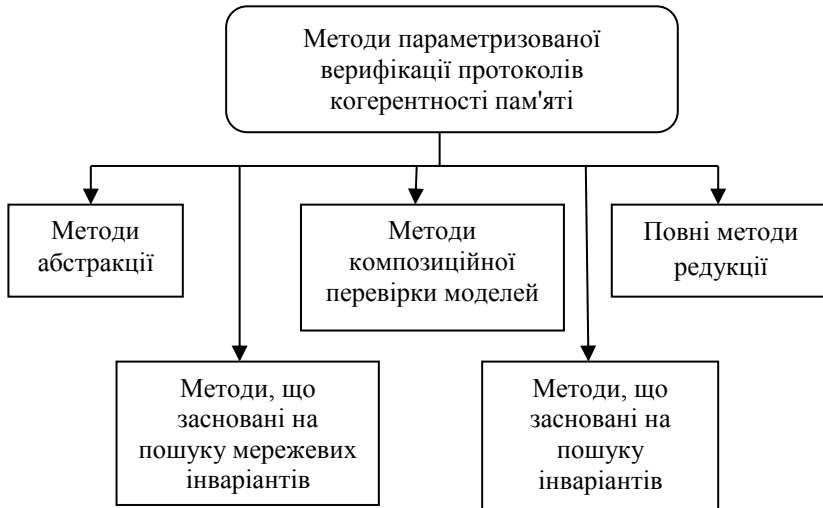


Рисунок 1 – Класифікація методів параметризованої верифікації протоколів когерентності пам'яті

#### Перелік посилань

1. Буренков В. С. Анализ применимости формальных методов к



верификации протоколов когерентности кэш-памяти масштабируемых систем / В. С. Буренков // Вопросы радиоэлектроники. – 2015. – Выпуск 1. – Сер. ЭВТ. – С. 105–116.

2. Буренков В. С. Генератор тестов для верификации протокола когерентности кэш-памяти / В. С. Буренков // Вопросы радиоэлектроники. – 2014. – Выпуск 3. – Сер. ЭВТ. – С. 56–63.

3. Chou C. A Simple Method for Parameterized Verification of Cache Coherence Protocols / Ching-Tsun Chou, Phanindra K. Mannava, Seungjoon Park // Formal Methods in Computer-Aided Design. – Springer Berlin Heidelberg, 2004. – P. 382–398.

### **Особливості захисту інформаційних ресурсів під час проведення відеоконференцзв'язку**

Огнєвий О.В., Огнева А.М., Капустян М.В.  
Хмельницький національний університет

На сьогоднішній день технологія відеоконференцзв'язку активно розвивається та впроваджується в Україні, що пов'язано з розвитком міжнародних відносин в суспільстві та з необхідністю оперативного зв'язку між користувачами в країні та по всьому світі. Використання систем відеоконференцзв'язку стало доступним з розвитком сучасних технологій та на відміну від голосового зв'язку або електронної пошти, дозволяє отримати різноманітний обсяг інформації, задіяти при спілкуванні текстові та візуальні графічні матеріали: малюнки, таблиці, схеми і діаграми, враховувати вираз обличчя та міміку співрозмовника. Організація відеоконференцзв'язку використовується для проведення переговорів та групових обговорень, в тих випадках, коли у користувачів немає можливості, або це недоцільно, бути присутнім особисто, що дає можливість значної економії засобів і часу.

Розвиток та впровадження інформаційних та телекомунікаційних технологій, збільшення пропускної здатності каналів передачі інформації зробило проведення конференцій, з використанням засобів аудіо та відео зв'язку, зручним засобом спілкування. Сеанси відеозв'язку проводяться для обміну досвідом між різними фахівцями, організації корпоративних нарад, широко використовується для дистанційних занять в освітніх цілях. На сьогодні технології відеозв'язку в основному знаходять застосування в наступних областях: виробнича діяльність (бізнес переговори, спільні проекти), освітні процеси (дистанційне навчання, наукові конференції, семінари), при проведенні судових засідань, для особистих потреб людей (спілкування з родичами і друзями) тощо.

Великою популярністю користуються різні системи для проведення відеоконференцій (ВК) за допомогою глобальних телекомунікаційних мереж.

Найчастіше такі конференції призначені для обмеженого кола користувачів, тому питання захисту інформації в таких системах виходять на передній план. Існує велика кількість таких систем, їх використання пов'язано з підвищеними ризиками, які призводять до виникнення проблем з можливим несанкціонованим доступом, прослуховуванням чи аналізом сигнальної інформації використовуваних протоколів.

В зв'язку із запровадженням карантину в Україні, органи державної влади та місцевого самоврядування, підприємства та організації, особливо ті, що належать до об'єктів критичної інфраструктури, забезпечили роботу своїх працівників в режимі реального часу через мережу Інтернет. Віддалена робота співробітників установи з системами, в яких обробляються державні інформаційні ресурси, інформація з обмеженим доступом, вимога щодо захисту якої визначена законодавчо, повинна відповідати політиці безпеки інформації та вимогам законодавства у сфері захисту інформації.

Відеоконференцзв'язок (ВКЗ) - це телекомунікаційна технологія інтерактивної участі двох і більше віддалених абонентів, при якому між ними відбувається обмін аудіо та відео у режимі реального часу.

Необхідність підтримання інформаційної безпеки автоматизованих систем визначена на державному рівні та спрямована на забезпечення інформаційної безпеки відносин, пов'язаних із збиранням, накопиченням, обробкою та передачею інформації.

Забезпечення захисту інформаційних ресурсів ВКЗ здійснюється шляхом застосування засобів і методів технічного захисту інформації, впровадження організаційних та інженерно-технічних заходів комплексної системи захисту інформації, спрямованих на недопущення блокування інформації, несанкціонованого доступу до неї, її модифікації або спотворення.

Систему ВКЗ прийнято вважати сукупністю наступних елементів: кінцевих вузлів системи - серверів і клієнтів відеоконференцій, та каналів зв'язку, що з'єднують ці вузли. Сервером відеоконференції є комплекс програмно-технічних засобів і систем, що забезпечує управління відеоконференцією, виконання функції ідентифікації і аутентифікації клієнтів, прийому, обробки та перенаправлення даних відеоконференцій. Клієнти представляють собою комплекс програмного і апаратного забезпечення і є джерелом даних системи. Зв'язок клієнтів відбувається через сервера за допомогою каналів зв'язку. Під каналом зв'язку прийнято розуміти множину ліній зв'язку та засобів передачі даних, що беруть участь в процесі відео конференції [3].

До головних особливостей технології ВКЗ можна віднести наступні: мінімізація витрат на поїздки, інтерактивне спілкування між учасниками, групове спілкування або навчання співробітників, проведення оперативних зустрічей з візуальним контролем, легкість в управлінні та підключенні, практично в будь-якому місці, де є доступ до Інтернету, надійність і безпека інформації.

Сучасна ВКЗ має масу унікальних можливостей, найзначніші з них:

– Телеприсутність. Засоби ВКЗ дозволяють обробляти і транслювати високу якість зображення, яке формуються на спеціально розташованих дисплеях з високою роздільною здатністю, створюючи ефект присутності кількох учасників з протилежного боку лінії зв'язку.

– Багатоточкове з'єднання. Дає можливість одночасно вести конференцію з великою кількістю програмних і апаратних пристроїв, створюючи сучасний центр з обміну оперативною інформацією та спільної роботи.

– Трансляція різних аудіо та відео матеріалів. Дана можливість надає підключення до ВКЗ будь-якого аудіо або відео обладнання для показу документів, презентацій, аудіо-відео записів і багато іншого.

– Інтеграція в автоматизовану систему управління. ВКЗ без проблем впроваджується в будь-яку сучасну технологію автоматизації, об'єднуючи всі системи в централізоване управління.

– Формування якісного зображення. Апаратні системи ВКС дозволяють відображати на екрані монітора відмінне і стабільне зображення в Full HD якості.

Система ВКЗ - це технічний комплекс програмно-апаратних засобів для організації аудіо-відео зв'язку між двома та більш користувачами, через мережу Інтернет. В даний момент, на ринку ВКЗ присутні два основних типи виконання: програмне і апаратне. Під програмним рішенням мається на увазі оснащення обчислювальної техніки (комп'ютера або ноутбука) спеціальним ПЗ, за допомогою якого буде організовуватися індивідуальний або груповий відеозв'язок в HD якості. Апаратне, має на увазі професійне обладнання (відеотермінал, аудіовізуальні технології) для побудови повноцінного аудіо-відео зв'язку між абонентами.

Проблеми надійності систем відеоконференцій є як ніколи актуальними на сьогоднішній день, так як дистанційне навчання з причини своєї доступності в будь-якій точці світу стає все більш популярним, при цьому організаторами конференцій висуваються високі вимоги до якості послуг, що надаються. При великій кількості бажуючих приєднатися до відкритої конференції і невеликої пропускної спроможності каналу найважливішим стає забезпечення доступності для всіх учасників.

Для забезпечення надійності відеоконференцій існує необхідність обмежити доступ сторонніх осіб (неавторизованих користувачів), а також організувати ідентифікацію користувача пристроїв і аутентифікацію учасників конференції (авторизацію).

Основною проблемою організації надійної системи відеоконференцзв'язку на сьогоднішній день є забезпечення оптимальної швидкості передачі даних при максимальній швидкості обробки аудіо та відео потоку. Для вирішення цієї проблеми розроблено кодеки, що дозволяють стискати сигнал і кодувати його для каналу зв'язку, а також відновлювати і декодувати на приймальній стороні.

Питання, пов'язані із захистом інформації в мережах ВКЗ є дуже важливими. Відповідно до законодавства України, як засоби захисту інформації можуть використовуватися тільки сертифіковані засоби [1].

Для систем ВКЗ актуальні різні загрози інформаційної безпеці, які притаманні будь-якій інформаційній системі (рис. 1).

Відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення. Усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами повинні блокуватися.



Рисунок 1 – Види інформації, що встановлені законом та підлягають захисту в інформаційних, телекомунікаційних та інформаційно - телекомунікаційних системах

ВКЗ схильні до загроз з боку зловмисників, форс-мажорних обставин, випадкових дій користувачів і адміністраторів [2]. Відповідно до загальноприйнятої класифікації, загрози інформаційної безпеки можна

поділити на такі види: загрози конфіденційності, цілісності і доступності та загрозу підтвердження авторства. В тій чи іншій мірі для ВК актуальні всі ці види загроз, однак, в рамках розгляду питань надійності ВКЗ найбільш актуальними є загрози цілісності та доступності.

Окрім гарантованої доставки, в якості засобу забезпечення надійності ВКЗ використовується авторизація користувачів. Авторизація - надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій [2]. При збільшенні кількості користувачів навантаження зростає і саме авторизація дозволяє обмежити мережеве навантаження, що підвищує надійність системи ВКЗ і дозволяє забезпечити контролювання смуги пропускання. Для кожного суб'єкта в системі визначається набір прав, які він може використовувати при зверненні до ресурсів ВКЗ. До найбільш поширених способів авторизації відносять: дискреційний (DAC), мандатний (MAC), управління доступом на основі ролей, контроль доступу на основі контексту (CBAC), контроль доступу на основі решітки (LBAC)[3] .

Одним з перспективних рішень проблеми забезпечення надійності систем ВКЗ на сьогодні є використання технологій розподілу навантаження інфокомунікаційної мережі.

Основними методами підвищення надійності систем ВКЗ на сьогодні є: застосування маршрутизації для оптимального і раціонального використання каналного ресурсу системи; використання алгоритмів децентралізованих самоорганізованих мереж, які дозволяють розподілити навантаження на усі елементи пропорційно їх ресурсам і характеристикам, тим самим збільшуючи масштабованість та зменшуючи вартість такого рішення за відсутності необхідності підтримки протоколів прикладного рівня на мережевому обладнанні; застосування механізмів динамічного перерозподілу швидкості передачі інформації при спільному обслуговуванні трафіку сервісів реального часу і трафіку даних, що допускає затримку [3].

Оптимальний розподіл мережевого навантаження дозволяє забезпечувати задані характеристики ВКЗ за рахунок керування інформаційними потоками.

Проведений аналіз показує, що на сьогоднішній день найбільш поширеними технологіями відеоконференцзв'язку є: системи відеоконференцзв'язку високої якості, засновані на застосуванні спеціальних протоколів; серверні системи, в основу принципу дії яких покладено стиснення відеопотоку. Більшість систем комп'ютерного відеоконференцзв'язку складається з наступних частин: - програмно-апаратне забезпечення сервера; - програмно-апаратне забезпечення клієнта; - лінії зв'язку; - мережеве обладнання.

Перелік посилань

1. Бараннік В. В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцв'язку / В. В. Бараннік, А. В. Власов, Р. В. Тарнополов // Наукоємні технології. - 2014. - № 1. - С. 55-60. - Режим доступу: [http://nbuv.gov.ua/UJRN/Nt\\_2014\\_1\\_13](http://nbuv.gov.ua/UJRN/Nt_2014_1_13).

2. Живко З. Б. Інформаційні загрози: суть і проблеми / З.Б. Живко, М.О. Живко // Системи обробки інформації. – 2009. – № 7(81). – С. 116-118.

3. Лебедева К. Алгоритмы и программные решения организации защищенного доступа к компьютерным видеоконференциям / К. Лебедева, А. Томилина // XVIII Решетневские чтения : Международная научная конференция, посвященной 90-летию со дня рождения генерального конструктора ракетно-космических систем академика М.Ф. Решетнева, 11-14 ноября 2014 : материалы конференции. – в 3 ч. – Красноярск : СибГАУ, 2014. – Ч. 2. – С. 320-322.

### **Діагностично-тренувальні прилади для відновлення рефлексів ушкоджених кістей та пальців рук**

Полянчикін В. Г., Гнезділов М. Д.

Науковий керівник – д.т.н., проф. Журавська І. М.

Чорноморський національний університет ім. Петра Могили

Після пошкодження шийно-грудного відділу хребта та нервів кисті рук рухові та/або сенсорні функції порушуються, особливо дрібна моторика окремих пальців або групи пальців. Посттравматична та постінсультна спастичність кінцівки – одне з найчастіших рухових порушень. Спастичність від ураження верхніх кінцівок відзначається більш ніж у 12 мільйонів осіб у всьому світі [1]. Програми реабілітації поєднують фізичну терапію з набуттям та відновленням рефлексів. Використанням апаратних тренажерів в амбулаторних та/або у домашніх умовах дозволяє досягти максимального результату [2].

Підвищити ефективність зазначеного процесу можливо за допомогою серії малогабаритних діагностично-тренувальних (ДТ) приладів «Reflex-Txx». Прилади розроблені на основі платформи Arduino з використанням на рухомій робочій зоні датчиків Холла або датчиків дотику та світлодіодів, частота спалахів яких регулюється в залежності від результатів тренувань. Авторизація пацієнта виконується за допомогою RFID-карти.

Якщо тренуванню підлягають декілька пальців, то використовується ДТ-прилад з датчиками Холла на рухомій робочій зоні – «Reflex-TH3» («Training Hall 3 Sensors»). В такому разі до кольорового майданчика біля спалахнувшого світлодіода треба доторкнутися магнітним інструментом («холдером»), що утримується щепотью з пальців, які підлягають тренуванню (на рис. 1, а – два пальці). Для тренування одного пальця (рис. 1, б)

використовується робоча зона з датчиками дотику на приладі «Reflex-ТТЗ» («Training Touch 3 Sensors»).

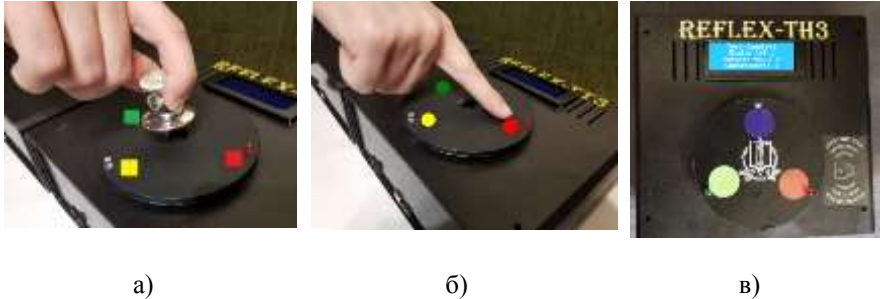


Рисунок 1 – ДТ-прилади серії «Reflex-Тхх»: а – з датчиками Холла на рухомій робочій зоні; б – з датчиками дотику; в – з відображенням результатів тренувань на LCD-екрані корпусу

Зважаючи на те, що робоча зона зі світлодіодами насаджена на шпindelь сервопривода, вона рухається на заданий градус по колу «за» або «проти» годинникової стрілки. Таке технічне рішення забезпечує тренування кісті руки, яка повертається вслід за рухомою робочою зоною ДТ-приладу.

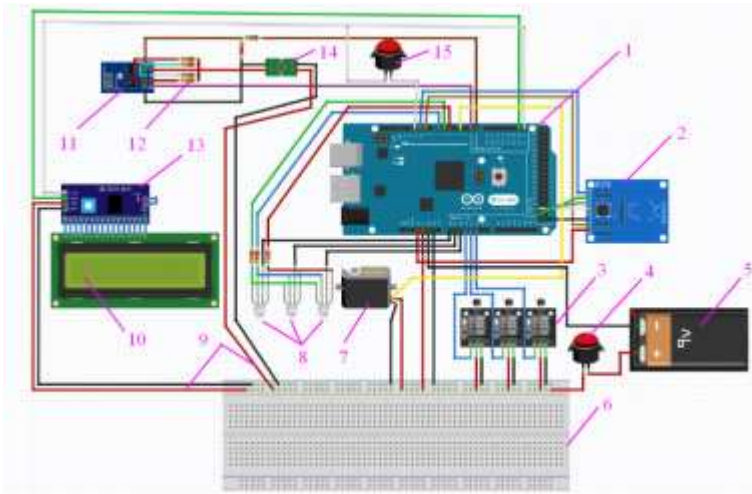
Для компонування розроблених прототипів електронних компонентів та документування було використано програмний застосунок з вільним доступом Fritzing v. 0.9.3 (рис. 2).

Результати тренувань відображаються на LCD-моніторі на корпусі ДТ-приладу (рис. 1, в), передаються через Інтернет до єдиного центру, де вони накопичуються за профілем кожної окремої особи, відображаються та аналізуються на мікросервісах розробленої апаратно-програмної системи (АПС) й доступні на гаджетах користувача за допомогою розробленого мобільного застосунку під керуванням ОС Android.

Для дослідження ефективності методики тренувань використаний метод середнього ковзного [3]. Для оцінки ефективності тренування застосований метод середнього ковзного, який дозволяє визначити ступінь покращення або погіршення результатів вже під час тренування. В такому разі розраховується середнє значення  $AVG_i$  швидкості реакції:

$$AVG_i = \frac{1}{CurCoAc} \sum_{n=1}^{Att} \sum_{i=1}^{CoAc} TR_{i,n}, \quad (1)$$

де  $CoAc$  – загальна кількість дій у спробі (вбачається, що у кожній з  $Att_n$  виконується дій  $CoAc = 20$ );  $CurCoAc$  – кількість виконаних дій на поточний момент часу від початку;  $Att$  – кількість спроб у сесії ( $Att = 5$ ).



Позначення: 1 – мікроконтролерна плата Arduino; 2 – RFID модуль; 3–датчики (Холла або дотику); 4 –кнопка живлення; 5 – Li-Po акумулятор 9V; 6 – монтажна плата; 7 – сервопривод; 8 – LED світлодіоди (RGB); 9 – перемички Дюпон; 10 – LCD екран; 11 – Wi-Fi модуль; 12 – резистори; 13 – I<sup>2</sup>C модуль; 14 – DC конвертор 3V/5V; 15 – кнопка «Старт».

Рисунок 2 – Схема з’єднання модулів ДТ-приладів серії «Reflex – Txx»

Для оцінки ефективності тренінгу під час навчання ковзне середнє (англ. Moving Average)  $MOV\_AVG_i$  обчислюється за декількома сусідніми діями  $NMA$  у спробі (у наведеному прикладі  $NMA = 3$ ):

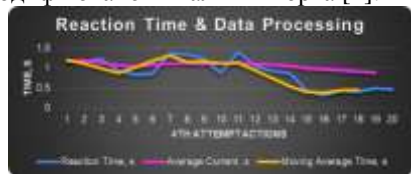
$$MOV\_AVG_i = \frac{1}{NMA} \sum_{i=NMA}^{Ai=NMA} TR_i. \quad (2)$$

Якщо навчання проходить успішно, то його поточне  $MOV\_AVG_i$  становиться меншим за  $AVG_i$ , тобто, час реакції зменшується з плином тренування (рис. 3).

результаті підвищення інтенсивності рухових навантажень з залученням хапальний рухів пальцями руки у пацієнтів, що тренувалися на апаратах серії «Reflex Txx», до 3-го тижня відзначалося зменшення спастичності руки на 2 бали за даними модифікованої шкали Ешворта [1].



а)



б)



Рисунок 3 – Тренування з покращенням (а) та з погіршенням (б) результатів з плином часу

З відновленням рефлексів, зростанням м'язової сили і підвищенням швидкості реакції користувачі розробленої АПС можуть зіткнутися з тим, що платформа Arduino перестане справлятися з тим обсягом обчислень, який очікується від неї отримати. Може не вистачати швидкодії у розрахунках, оновленні інформації на дисплеях, відправки даних та інших ресурсовитратних дій, а ще може просто закінчитися оперативна пам'ять. В такому випадку можна перейти на більш просунуту платформу STM32.

#### Перелік посилань

1. Матвієнко Ю. О. Спастичність: огляд проблеми // Медицина світу. – Квітень 2008. – Т. XXIV, № 4. – URL: <http://msvitu.com/archive/2008/april/article-3.php?print=1>
2. Saunders R., Astifidis R., Burke S., Higgins J., McClinton M. A. Hand and upper extremity rehabilitation. – E-book: A practical guide. – Elsevier Health Sciences, November 2, 2015. – 608 p.

### **Інформаційна технологія для класифікації марок автомобілів з використанням згорткової нейронної мережі**

Руденко І.В.

Хмельницький національний університет

*Розглянуто прикладні аспекти розробки інформаційної системи для класифікації та розпізнаванню марок автомобілів на фотографіях та візуалізації отриманих результатів для подальшого аналізу. Запропонована інформаційна система забезпечує точну і швидку класифікацію розпізнавання об'єктів на фото відповідно до заданих категорій.*

*Applied aspects of information system development for classification and car brands in the photo retrieval and visualization of the obtained results for further analysis are considered. The offered information system provides accurate and fast classification of the objects in photo according to the given categories.*

З розвитком нових технологій та постійним підвищенням рівня інформатизації суспільства проблема машинної класифікації та розпізнавання об'єктів на фото набуває особливого значення.

Оптимізація гіперпараметрів — задача машинного навчання по вибору множини оптимальних гіперпараметрів для алгоритму машинного навчання. Гіперпараметр є параметром, значення якого використовується для керування

процесом навчання. На відміну від значень інших параметрів (наприклад, вагових коефіцієнтів), які потрібно вивчити.

Одні й ті ж види моделей машинного навчання можуть мати різні обмеження, ваги або потребувати певної швидкості навчання для різних видів даних. Ці параметри називаються гіперпараметрами і їх слід підбирати так, щоб модель могла оптимально вирішити завдання навчання. Для цього знаходиться кортеж гіперпараметрів, який дає оптимальну модель, що оптимізує задану функцію втрат на заданих незалежних даних. Цільова функція бере кортеж гіперпараметрів і повертає пов'язані з ними втрати. Часто використовується перехресне затвердження для оцінки цієї узагальнюючої здатності.

Метою роботи є розробка інформаційної системи для класифікації марок автомобілів з використанням згорткової нейронної мережі та візуалізації отриманих результатів для подальшого аналізу.

З існуючих підходів розглянемо найвідоміші дієві варіанти реалізації:

- пошук по ґратці;
- випадковий пошук;
- байсова оптимізація;
- оптимізація на основі градієнтів;
- уволюційна оптимізація;
- на основі заселення;
- інше (на основі радіально-базисної функції (РБФ) і спектрального методу).

Налаштування гіперпараметрів згорткової нейронної мережі трохи складніше, ніж налаштування щільних мереж. Це пов'язано з тим, що алгоритм використовує випадковий пошук найкращої з можливих моделей, що, в свою чергу, може призвести до невідповідності кількох умов, щоб цього не сталося, нам потрібно розробити архітектуру згорткової нейронної мережі, а потім відрегулювати гіперпараметри в алгоритмі, щоб отримати нашу найкращу модель.

Згорткові нейронні мережі (рис. 1) мають кілька різних фільтрів / ядер, що складаються з параметрів, що піддаються навчання, які можуть обертатися на даному зображенні просторово для виявлення таких функцій, як краї та фігури.

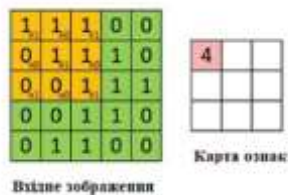


Рисунок 1 – Алгоритм згортки

Ця велика кількість фільтрів по суті вчиться фіксувати просторові особливості із зображення на основі вивчених ваг шляхом зворотного розповсюдження, а складені шари фільтрів можуть бути використані для виявлення складних просторових форм з просторових об'єктів на кожному наступному рівні. Отже, вони можуть успішно звести дане зображення у дуже абстраговане зображення, яке легко передбачити.

У щільних мережах ми намагаємось знайти закономірності у значеннях пікселів, що вводяться як напр. якщо пікселі 25 і 26 перевищують певне значення, це може належати до певного класу та кількох складних варіацій того самого. Воно може легко вийти з ладу, якщо ми можемо мати об'єкти де завгодно на зображенні і не обов'язково в центрі.

Функція активації ReLU (рис.2) - це індивідуальна математична операція.

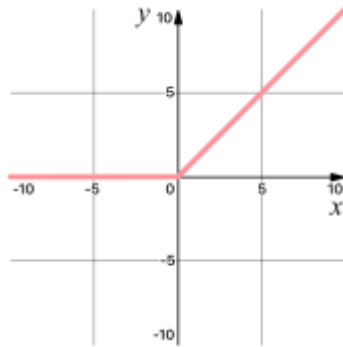


Рисунок 2 - Графічна функція активації ReLU, яка ігнорує всі негативні дані.

Ця функція активації застосовується поетапно до кожного значення вхідного тензора. Наприклад, якщо застосувати ReLU до значення 2.24, результат буде 2.24, оскільки 2.24 більше 0. Ви можете спостерігати, як застосовується ця функція активації, клацнувши нейрон ReLU у мережі вище. Функція випрямленої лінійної активації (ReLU) виконується після кожного згорткового рівня в мережевій архітектурі, описаній вище. Зверніть увагу на вплив цього шару на карту активації різних нейронів у всій мережі!

$$\text{Softmax}(x_i) = \frac{\exp(x_i)}{\sum_j \exp(x_j)} \quad (1)$$

Операція softmax має ключову мету: переконатися, що виходи мережі складають 1. Через це операції softmax корисні для масштабування результатів моделей на ймовірності. Для візуальної індикації впливу кожного логіту

(масштабоване скалярне значення) вони кодуються за допомогою світло-оранжевої → темно-оранжевої кольорової шкали. Після проходження функції softmax кожен клас тепер відповідає відповідній ймовірності.

Формула зображена вище (1).

Нейронні мережі надзвичайно поширені в сучасних технологіях - адже вони настільки точні! Сьогодні найефективніші мережі складаються з великої кількості шарів, які здатні вивчати все більше і більше можливостей. Частина причин, завдяки яким ці новаторські мережі можуть досягти таких надзвичайних точностей, полягає в їх нелінійності. ReLU застосовує в моделі вкрай необхідну нелінійність. Нелінійність необхідна для отримання нелінійних меж рішення, так що вихідні дані не можуть бути записані як лінійна комбінація входів. Якби нелінійна функція активації була відсутня, глибокі архітектури мережі перетворилися б на єдиний, еквівалентний згортковий рівень, який не працював би майже так само добре. Функція активації ReLU спеціально використовується як нелінійна функція активації, на відміну від інших нелінійних функцій, таких як Sigmoid, оскільки емпірично зауважено, що мережа, що використовує ReLU, швидше навчається, ніж її аналоги.

Отже, розроблений алгоритм, який використовує згорткову нейронну мережу, може бути застосований для розв'язання завдань онлайн-розпізнавання об'єктів на фото. Точність розпізнавання достатньо висока. Ефективність реалізованої системи залежить від розміру навчальної та тестової вибірок, кількості шарів та нейронів у кожному шарі. Точність вирішення поставленого завдання з використанням моделі згорткової нейронної може бути поліпшена практично до 99%.

#### Перелік посилань

1. Nils J. Nilsson, Introduction to Machine Learning. (англ.)
2. Trevor Hastie, Robert Tibshirani and Jerome H. Friedman (2001). The Elements of Statistical Learning, Springer. ISBN 0-387-95284-5. (англ.)
3. Pedro Domingos (September 2015), The Master Algorithm, Basic Books, ISBN 978-0-465-06570-7 (англ.)

#### **Моделювання хаотичного генератора Лоренца засобами Matlab/Simulink**

Слободян М.О., Бабій Д.Р.

Науковий керівник – д.т.н., доц. Підченко С.К.

Хмельницький національний університет

Цікавим та перспективним напрямком в сучасній радіотехніці є розробка теорії та практичне застосування пристроїв із хаотичною динамікою для передачі інформації. Хаотичні генератори характеризуються сильною залежністю від початкових умов, що дозволяє генерувати шумоподібні сигнали з широким неперервним спектром потужності [1, 2]. Пристрої із хаотичною поведінку, побудовані на основі дискретних нелінійних моделей,

можуть бути застосовані в функціональних блоках цифрових телекомунікаційних систем для стиснення, шифрування і модуляція сигналів. Неперервні хаотичні генератори можуть служити джерелом широкосмугових сигналів в аналогових системах зв'язку [3].

Розглянемо в якості математичної моделі генератора хаотичних коливань динамічну систему Лоренца, яка складається з трьох звичайних диференціальних рівнянь першого порядку:

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(r - z) - y; \\ \dot{z} = xy - bz \end{cases} \quad (1)$$

де  $\sigma, r, b$  – дійсні додатні параметри системи.

У хаотичному режимі система Лоренца генерує широкосмугові сигнали складної форми із неперервним спектром та високими кореляційними та ортогональними властивостями [1, 2].

Схемотехнічна реалізація хаотичного генератора, побудованого на основі моделі Лоренца в системі Matlab/Simulink представлена на рис.1. Схема є модифікацією однойменного генератора, описаного авторами в роботі [4], що в свою чергу базується на варіанті реалізації, який був представлений Паулем Хоровіцем в його онлайн-публікації [5].

Схема на рис.1 побудована на базі двох операційних підсилювачів та двох аналогових помножувачів. Номінали пасивних елементів наведені в табл.1.

Таблиця 1. Номінали пасивних елементів схеми генератора Лоренца

<i>R1</i>	<i>R2</i>	<i>R3</i>	<i>R4</i>	<i>R6</i>	<i>R7</i>	<i>R10</i>	<i>C1</i>	<i>C2</i>	<i>C3</i>
100k	100k	35,7k	1M	250k	250k	133	1n	1n	3n

Часові діаграми напруг, що пропорційні координатам  $x, y$  та  $z$  системи (1), які були отримані в результаті імітаційного моделювання роботи схеми рис.1, зображені на рис.2.

Фазові портрети атратора в проекціях на площини  $x$ - $y$  та  $x$ - $z$  зображені на рис.3.

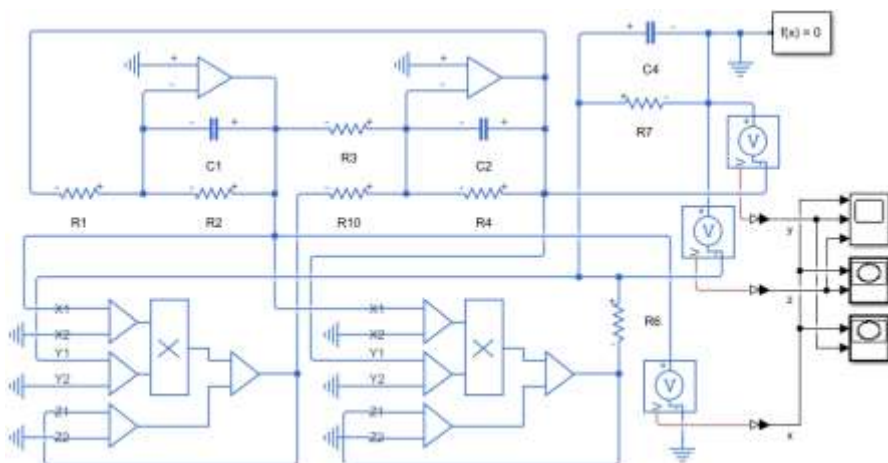


Рисунок 1. Схемотехнічна реалізація хаотичного генератора Лоренца, побудована в середовищі Matlab/Simulink

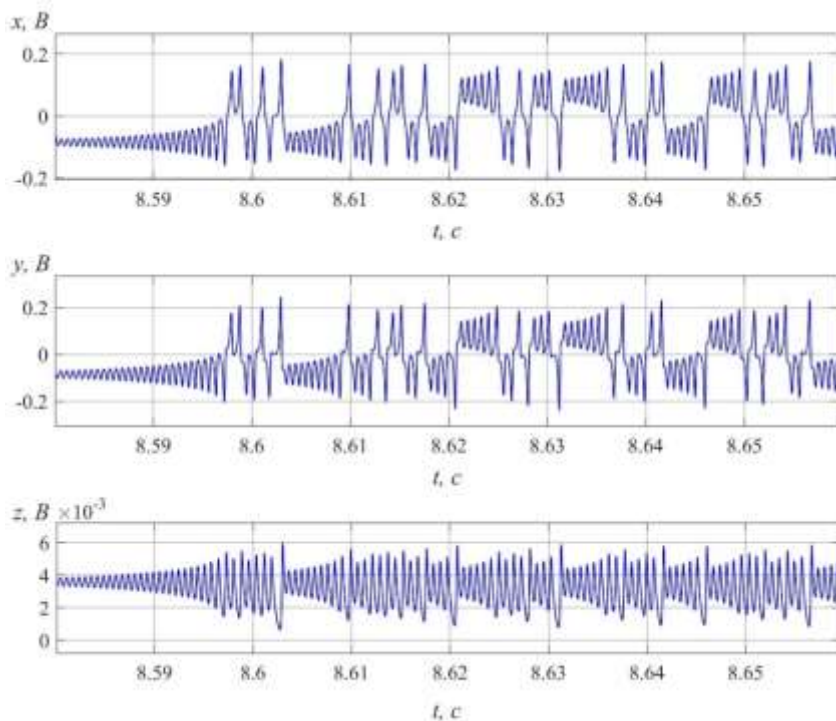


Рисунок 2. Часові діаграми напруг, що пропорційні координатам  $x$ ,  $y$  та  $z$

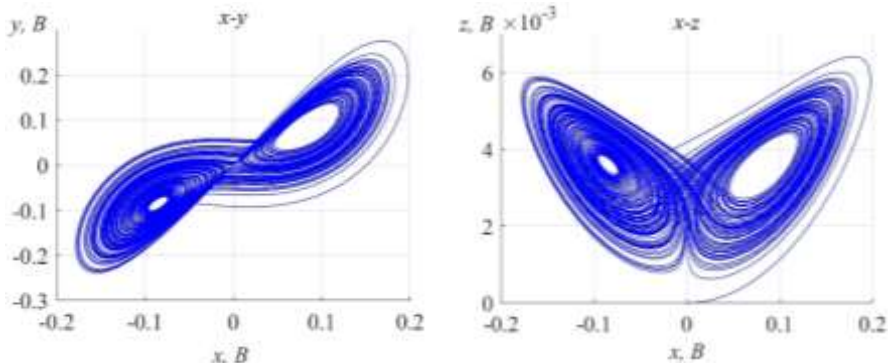


Рисунок 3. Фазові портрети атрактора в проекціях  $x-y$  та  $x-z$

Варто зазначити, що представлена в роботі схема генератора є низькочастотною (ширина спектру вихідних хаотичних коливань становить декілька одиниць кілогерц), однак теоретично може бути модифікована для використання в діапазоні високих та надвисоких частот.

Перспектива використання пристроїв із хаотичною динамікою в сучасних засобах телекомунікації обумовлена рядом факторів, серед яких висока інформаційна ємність, широкий спектр частот та конфіденційність передачі повідомлень. Можливість реалізації на базі одного пристрою великої кількості хаотичних режимів в перспективі дає можливість побудови багатоканальних систем передачі інформації. Сильна залежність від початкових умов та нестійкість фазових траєкторій дозволяє за рахунок малих впливів керувати динамікою хаотичних генераторів та здійснювати модуляцію з великою швидкістю.

#### Перелік посилань

1. Дмитриев А.С. Динамический хаос: новые носители информации для систем связи / А.С. Дмитриев, А.И. Панас. – М. : Изд-во Физико-математической литературы, 2002. – 252 с.

2. Прикладне застосування теорії хаотичних систем у телекомунікаціях: монографія / [Ю.Я. Бобало, С.Д. Галюк, М.М. Климаш, Р.Л. Політанський]; Нац. ун-т «Львів. політехніка». – Львів: Коло, 2015. – 178 с.

3. Агуреев К.И. Применение детерминированного хаоса для передачи информации / К.И. Агуреев // Известия ТулГУ. Технические науки. – 2014. – Вып. 11. Ч. 2. – С.197–212.

4. Кузнецов С.П. Простые электронные генераторы хаоса и их схемотехническое моделирование // С. П. Кузнецов / Известия вузов. Прикладная нелинейная динамика. – 2018. Т. 26, № 3. С. 35–61.

5. Horowitz P. Build a Lorenz attractor:  
[http://seti.harvard.edu/unusual\\_stuff/misc/lorenz.htm](http://seti.harvard.edu/unusual_stuff/misc/lorenz.htm)

## Математична модель багаточастотної автоколивальної системи як динамічного об'єкта

Слюсарчук О.О.

Науковий керівник – д.т.н., доц. Підченко С.К.

Хмельницький національний університет

Для багаточастотної коливальної системи, якщо власні частоти контурів не перебувають у співвідношенні простих цілих чисел і затухання контурів досить малі, укорочені диференціальні рівняння представляються системою виду (для одноконтурних автогенераторів), які отримуються на основі символічного методу огинаючих [1,2]:

$$\begin{aligned} X_1 &= F_1(X_1, \dots, X_n); \\ X_2 &= F_2(X_1, \dots, X_n); \end{aligned} \quad (1)$$

$$X_n = F_n(\overset{\dots}{X_1}, \dots, X_n),$$

де 
$$F_i = [S_i(X_1, \dots, X_n)R_i k_{зз} - 1]X_i. \quad (2)$$

В (1), (2) прийнято наступні позначення:  $X$  – відносні безрозмірні амплітуди коливань;  $S_i$  – середня крутизна для основної частоти;  $R_i$  – еквівалентний резонансний опір контуру;  $k_{зз}$  – коефіцієнт зворотного зв'язку.

Рівняння стаціонарного режиму отримуються із (1), (2), якщо прийняти  $X_1 = X_2 = \dots = X_n = 0$ :

$$F_i = 0, \quad i = 1, 2, \dots, n, \quad (3)$$

звідки визначаються стаціонарні значення амплітуд коливань  $X_{i_0}$ .

Для дослідження стійкості стаціонарного режиму коливань необхідно скласти рівняння лінійного наближення для варіацій амплітуд  $\xi_i$ . Дані рівняння мають вигляд:

$$\xi_i = s_{i1}\xi_1 + s_{i2}\xi_2 + \dots + s_{ij}\xi_j + \dots + s_{in}\xi_n, \quad i, j = 1, 2, \dots, n, \quad (4)$$

де  $s_{ij} = dF_i / dX_j$ ,  $j = 1, 2, \dots, n$ , і визначено в точці дослідження стаціонарного режиму ( $X_i = X_{i_0}$ ).

У загальному вигляді одержати прості умови стійкості стаціонарного режиму не представляється можливим, тому в даній системі обмежуються



дослідженням системи симетричних зв'язаних автогенераторів, що мають однакові коефіцієнти взаємного зв'язку  $k$ . Так, для симетричного режиму, отримано наступні умови стійкості [2]:

$$s_{ii} - s_{ik} < 0; s_{ii} + s_{ik}(n-1) < 0, \quad i, k = 1, 2, \dots, n. \quad (5)$$

В ряді робіт представлений метод гармонічної лінеаризації для досліджень багаточастотних коливань в нелінійних системах. Наприклад, в [3] розглянута модель багаточастотної системи (рис. 1), яка описується системою рівнянь:

$$x + W_1(p)W_2(p)y - W_2(p)z = 0; \quad (6)$$

$$y = F(x). \quad (7)$$

Сигнали на вході та виході нелінійного елемента (НЕ):

$$x = x_0 + Ae^{j\omega_1 t} + Be^{j\omega_2 t} e^{j\alpha}; \quad (8)$$

$$y = y_0 + AW(\omega_1 / \omega_2) e^{j\omega_1 t} + BW(\omega_2 / \omega_1) e^{j\omega_2 t} e^{j\alpha}, \quad (9)$$

де  $W(\omega_1 / \omega_2)$  – передатна функція НЕ на частоті  $\omega_1$  при впливі сигналу на частотах  $\omega_1$  і  $\omega_2$ ;  $W(\omega_2 / \omega_1)$  – передатна функція НЕ на частоті  $\omega_2$  при впливі сигналу на частотах  $\omega_2$  і  $\omega_1$ ;  $A, B$  – амплітуди коливань.

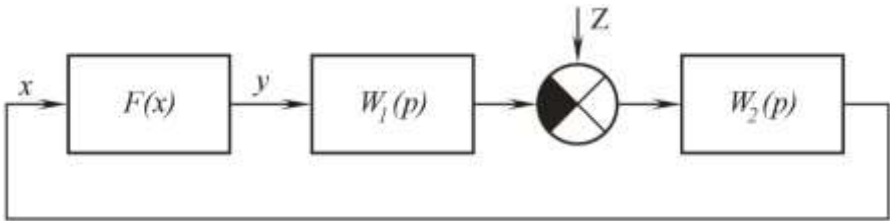


Рисунок 1 – Модель багаточастотної системи:  $x, y$  – параметри на вході та виході НЕ;  $Z$  – зовнішній вплив;  $F(x)$  – характеристика НЕ;  $W_1(p), W_2(p)$  – передатні функції лінійних частин системи

Зовнішній вплив задається у вигляді:

$$Z = z_0 + z_1 e^{j\omega_1 t} e^{j\beta_1} + z_2 e^{j\omega_2 t} e^{j\beta_2}. \quad (10)$$

В результаті отримуються рівняння для частот  $\omega_2$  і  $\omega_1$ :

$$W(\omega_1/\omega_2) = -W_1^{-1}(j\omega_1)W_2^{-1}(j\omega_1) + W_1^{-1}(j\omega_1)\frac{z_1}{A}e^{j\beta_1}; \quad (11)$$

$$W(\omega_2/\omega_1) = -W_1^{-1}(j\omega_2)W_2^{-1}(j\omega_2) + W_1^{-1}(j\omega_2)\frac{z_2}{B}e^{j(\beta_2-\alpha)}. \quad (12)$$

В подібних системах, гармонічна лінеаризація може бути застосована не тільки для одно- або двочастотних коливань, але й для коливань з будь-якою кількістю частот і при будь-якому співвідношенні між частотами та амплітудами складових. Однак, при цьому, значно зростає громіздкість аналітичних викладок, тому часто обмежуються розглядом окремих випадків.

Наприклад, для  $y = x^3$  та  $\omega_1 < \omega_2 < \omega_3$ :

$$x = x_0 + A \sin \omega_1 t + B \sin(\omega_2 t + \alpha_2) + C \sin(\omega_3 t + \alpha_3); \quad (13)$$

$$y = y_0 + A W_{HE_1} \sin \omega_1 t + B W_{HE_2} \sin(\omega_2 t + \alpha_2) + C W_{HE_3} \sin(\omega_3 t + \alpha_3). \quad (14)$$

Для випадку співвідношення частот  $\omega_1 : \omega_2 : \omega_3 = 1 : 3 : 5$  отримуємо систему рівнянь тричастотного режиму [3]:

$$\begin{aligned} W_{HE_1} &= \frac{3}{4}A^2 + \frac{3}{2}(B^2 + C^2) - \frac{3}{4}ABe^{j\alpha_2} - \frac{3}{2}BCe^{j(\alpha_3-\alpha_2)}; \\ W_{HE_2} &= \frac{3}{4}B^2 + \frac{3}{2}(A^2 + C^2) - \frac{1}{4}\frac{A^3}{B}e^{-j\alpha_2} - \frac{3}{4}\frac{A^2C}{B}e^{j(\alpha_3-\alpha_2)}; \\ W_{HE_3} &= \frac{3}{4}C^2 + \frac{3}{2}(A^2 + B^2) - \frac{3}{4}\frac{A^2B}{C}e^{j(\alpha_3-\alpha_2)}. \end{aligned} \quad (15)$$

Необхідно відзначити, що представлені математичні моделі призначені лише для наближеної оцінки деяких параметрів багаточастотних систем на достатньо тривалому інтервалі часу. До таких, в першу чергу, відносяться амплітуди і частоти коливань, а також граничні значення параметрів за яких система втрачає стійкість [1].

#### Перелік посилань

1. Теорія і реалізаційні основи інваріантних багаточастотних п'єзорезонансних пристроїв та систем / С. К. Підченко. – Хмельницький: ХНУ, 2014. – 400 с.
2. Уткин Г.М. Автоколебательные системы и волновые усилители / Г.М. Уткин – М.: Сов. радио, 1978. – 272 с.
3. Письменный И.Л. Многочастотные нелинейные колебания в

газотурбинном двигателі / И.Л. Письменный – М.: Машиностроение, 1987. – 128 с.

## **Організація захисту інфраструктури електронної комерції на базі протоколів DoT та DoH**

Тогоєв О. Р.

Чорноморський національний університет імені Петра Могили

Цифровізація та діджиталізація сучасної економіки в цілому та економіки України як її складової вимагає найретельнішої уваги до забезпечення безпеки торговельних операцій в онлайні [1].

Забезпечення безпеки названо першою з п'яти головних проблем Інтернету в програмі дій нової міжнародної ініціативи побудови Інтернету майбутнього. Сьогодні Інтернет є ефективним, але непередбачуваним середовищем, в якому присутня безліч різноманітних загроз і небезпек. Серед ризиків, на які наражається комп'ютерна мережа: несанкціонований доступ до мережевих ресурсів, атак з використанням різноманітних технологій, метою яких є відключення певних послуг. Для запобігання цим ризикам необхідно впровадження новітніх технічно-програмних рішень реалізації електронних транзакцій [2].

Кожен комп'ютер в інтернеті має власну унікальну IP-адресу, яка складається з чотирьох (у протоколі IPv4) або шістнадцяти (у протоколі IPv6) байтів [3]. Спочатку перетворення між доменними та IP-адресами вироблялося з використанням спеціального текстового файлу *hosts*, який складався централізовано й автоматично розсилався на кожну з машин у своїй локальній мережі. З ростом інтернет-мережі виникла необхідність в ефективному, автоматизованому механізмі, яким стала ієрархічна розподілена система доменних імен (англ. Domain Name System – DNS).

Запити та відповіді DNS пересилаються по мережі у вигляді звичайного тексту в незашифрованому вигляді, що робить його вразливим для шпигунства або зміни відповіді і перенаправлення браузеру на шкідливі сервери. Шифрування DNS ускладнює відстеження DNS-запитів або їх зміну під час передачі. Шифрування DNS-запитів і відповідей захищає від атаки Man-in-the-Middle, виконуючи ті ж функції, що і традиційний протокол DNS з відкритим текстом.

За останні кілька років були впроваджені два протоколи шифрування DNS:

- DNS-over-HTTPS (DoH);
- DNS-over-TLS (DoT).

Ці протоколи мають одну спільну рису: навмисно ховають DNS-запити від будь-якого. Зазначені протоколи в основному використовують протокол TLS (Transport Layer Security) для встановлення зашифрованого з'єднання між клієнтом (який виконує запити) і сервером (що дозволяє запити DNS) через порт, який зазвичай не використовується для трафіку DNS.

Конфіденційність запитів DNS є великою перевагою цих протоколів. Однак, вони створюють проблеми службі безпеки, яка повинна стежити за мережевим трафіком, виявляти і блокувати шкідливі з'єднання. Оскільки протоколи різняться за своєю реалізацією, методи аналізу будуть також відрізняються у DoH і DoT.

DoH використовує порт 443 для HTTPS, для якого в п. 8.1 RFC 8484 спеціально зазначено, що завдання полягає в тому, щоб змішати трафік DoH з іншим трафіком HTTPS в одному і тому ж з'єднанні, утруднити аналіз трафіку DNS і, таким чином, обійти заходи корпоративного контролю.

Протокол DoH використовує шифрування TLS і синтаксис запитів, що надається загальними стандартами HTTPS і HTTP/2, додаючи запити і відповіді DNS поверх стандартних запитів HTTP (рис.1).

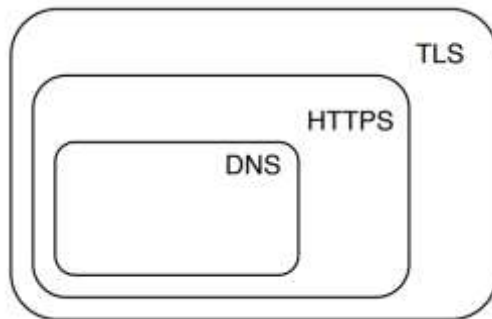


Рисунок 1 – DNS всередині HTTPS

Але при використанні протоколу DoH є певні ризики. Якщо немає можливості відрізнити звичайний HTTPS-трафік від запитів DoH, то застосунки всередині локальної мережі організації будуть обходити локальні налаштування DNS, перенаправляючи запити на сторонні сервери, які відповідають на запити DoH. Тобто, зазначений механізм обходить будь-який моніторинг та знищує можливість контролю за DNS-трафіком. Тоді необхідно впроваджувати контроль за DoH, використовуючи функції розшифрування HTTPS.

У той час як протокол DoH прагне змішуватися з іншим трафіком на тому ж порту, DoT за замовчуванням використовує спеціальний порт, зарезервований з цією метою, забороняючи використання того ж порту для традиційного незашифрованого трафіку DNS (RFC 7858, Розділ 3.1), як показано на рис.2.

Протокол DoT використовує протокол TLS для забезпечення шифрування, який інкапсулює стандартні запити протоколу DNS з трафіком, що використовують порт 853 (RFC 7858, розділ 6). Протокол DoT був

розроблений з метою спрощення або блокувати трафік з порту, або погоджуватися на його використання, але включити розшифровку на цьому порту.

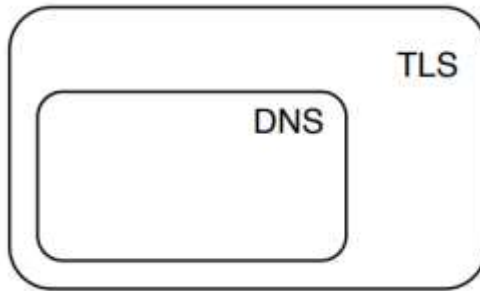


Рисунок 2 – DNS всередині TLS

Зважаючи на масштабне поширення інтернет-комерції із застосуванням технології Google, корпорація Google реалізувала DoT в своєму клієнтові Android 9 Pie і пізніших версіях, передбачивши за замовчанням автоматичне використання DoT, якщо він доступний. Для використання DoT на рівні організації необхідно, щоб мережеві адміністратори явно дозволяли вихідний трафік на порт 853 через свій периметр для цього нового протоколу.

Таким чином, обидва протоколи шифрування – й DoH, й DoT – мають певні ризики використання. Головними серед яких є необхідність забезпечення видимості і контролю трафіку. Для DoH таким є налаштування в NGFW розшифровки трафіку HTTPS і блокування трафіку DoH. Для DoT необхідно налаштування NGFW для розшифрування всього трафіку для порту призначення 853. В якості альтернативи можна повністю заблокувати движком App-ID трафік 'dns-over-tls' через порт 853 (замовчуванням).

Крім того, слід зазначити, що DoH працює тільки на рівні додатку, це означає, що до сервера будуть відправлятися запити надіслані тільки браузером, ні на які інші системні аплікації налаштування браузера не поширюються.

Однозначно, при використанні монетизації YouTube-каналів, розширеній електронній торгівлі за допомогою Google Tag Manager та ін. доцільно впроваджувати реалізацію сервера DNS поверх TLS-протокола, тобто технологію DoT [4].

#### Перелік посилань

1. Експортна стратегія для сектору інформаційних технологій : дослідження; Міністерство розвитку економіки, торгівлі та дослідження сільського господарства України. 2019–2023. URL:

<https://www.me.gov.ua/Documents/Download?id=6deb0289-40af-41ab-91eb-ce7f8d298fc4> (дата звернення: 06.11.2020).

2. Трофименко О. Моніторинг рівня кібербезпеки України у світових рейтингах / О. Трофименко, Ю. Прокоп, Н. Логінова, О. Задерейко // Інформаційна безпека людини, суспільства, держави. – 2019. – № 3 (27). URL: <http://academy.ssu.gov.ua/ua/page/inf-arch.htm> (дата звернення: 06.11.2020).

3. Samson I. Comparative analysis between IPv4 and IPv6 / I. Samson, A. Jamilu // Int. Journal of Information Systems and Engeneearing. – 2015. – Vol.2, No. 3. – P.20–26. DOI: 10.24924/ijise/2016.11/v4.iss2/20.26.

4. Кухаренко А. Как настроить расширенную электронную торговлю с помощью Google Tag Manager / А. Кухаренко // NetpeakJournal. URL: <https://netpeak.net/ru/blog/kak-nastroit-rasshirennuyu-elektronnyu-torgovlyu-s-pomoshch-yu-google-tag-manager/> (дата обращения: 06.11.2020)

## **Моделювання систем зв'язку з OFDM модуляцією**

Трач Б. В.

Науковий керівник – д.т.н., проф. Підченко С.К.

Хмельницький національний університет

Мультиплексування з ортогональним частотним розділенням каналів (OFDM) - це ефективний формат модуляції, що використовується в сучасних системах бездротового зв'язку, включаючи 5G. OFDM поєднує в собі переваги квадратурної амплітудної модуляції (QAM) і мультиплексування з частотним поділом (FDM) для створення системи зв'язку з високою швидкістю передачі даних. QAM відноситься до цифрових типів модуляції: BPSK (двійкова фазова маніпуляція), QPSK (квадратурна фазова маніпуляція), 16QAM (16-позиційна QAM), 64QAM (64-позиційна QAM).

FDM - це просто ідея про те, що декілька каналів зв'язку можуть співіснувати, призначаючи зріз частотного спектра для кожного каналу. Типовим прикладом цього є FM-радіомовлення: загальний розподіл частот становить від 87,8 МГц до 108 МГц, розділених на канали шириною 0,2 МГц (рис. 1). Розподіл частот FDM не повинно перекриватися і часто має захисні смуги між каналами для мінімізації завад від сусідніх каналів.

Базова концепція OFDM була вперше запропонована Р. У. Чангом, визнавши, що ортогональні сигнали з обмеженою смугою частот можна комбінувати із значним перекриттям, уникаючи при цьому міжканальних завад. Використовуючи OFDM, ми можемо створити масив піднесучих, які працюють разом для передачі інформації в діапазоні частот.

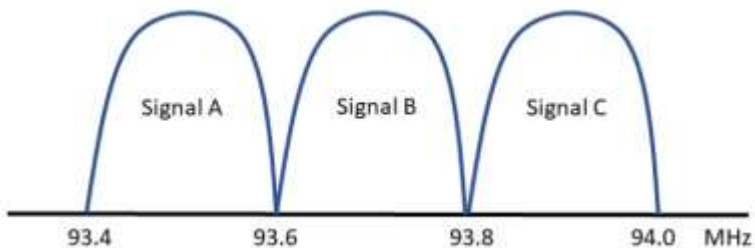


Рисунок 1 – Мультиплексування з частотним поділом каналів

Ці піднесучі повинні бути ортогональними функціями. Точне математичне визначення ортогональності між двома функціями полягає в тому, що інтеграл їх добутку за вказаний інтервал часу дорівнює нулю. У більш широкому сенсі ми можемо розглядати ортогональні функції як статистично не пов'язані.

На рис. 2 показано, як  $N$  рівновіддалених піднесучих можна об'єднати для формування масиву паралельних сигналів. Кожна з піднесучих модулюється з використанням QAM. Ці модульовані піднесучі можуть використовуватися для підтримки незалежних сигналів основної смуги частот, але частіше їх комбінують, щоб забезпечити максимальну пропускну здатність для одного потоку даних.

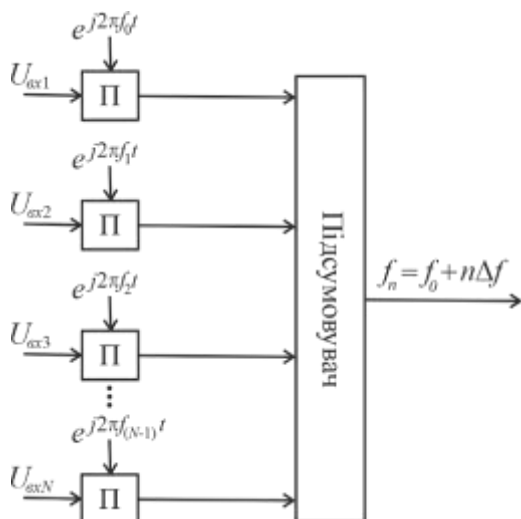


Рисунок 2 – Модулятор OFDM підсумовує сигнали різних частот.

Ми можемо представити ці піднесучі математично, використовуючи комплексну форму, що узгоджується з використанням QAM.

$$x(t) = \sum_{n=0}^{N-1} c_n e^{j2\pi f_n t},$$

де  $f_n = f_0 + n \cdot \Delta f$ .

Наведені вище рівняння є безперервними функціями, і системи OFDM реалізовані в аналоговій формі. Однак, сучасні системи майже всі цифрові, в них використовуються новітні технологічні вузли напівпровідників і цифрова обробка сигналів.

Сучасні системи OFDM використовують піднесучі, які існують в дискретній (дискретизованій) формі з частотою дискретизації:

$$f_s = \frac{1}{\Delta t}$$

З  $N$  піднесучими, розділеними

$$\Delta f = \frac{1}{N\Delta t}$$

Для простоти на рис. 3 показані тільки чотири немодульовані піднесучі в області часу. Чорна складова – це несуча ( $f_0$ ), а інші складові - це піднесучі з більш високими частотами, що рознесені з інтервалом, кратним  $\Delta f$ . Чотири піднесучі OFDM в області часу представлені на рис. 3.

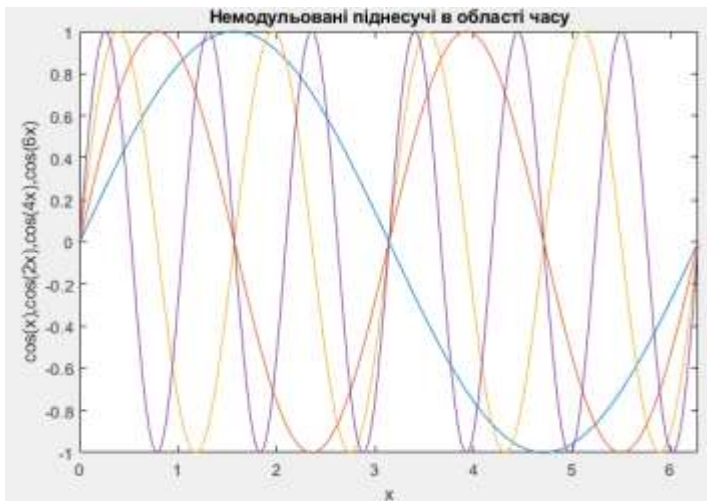


Рисунок 3 – Цей сигнал OFDM містить чотири несучих, розділених відстанню  $\Delta f$



На рис. 4 показані ці ж піднесучі в частотній області, показані з деякою шириною смуги модуляції, щоб вказати перекриття між піднесучими. Піднесучі ортогональні одна одній і будуть мати мінімальні завади для інших піднесучих, що призведе до ефективного використання смуги пропускання. Зверніть увагу, що амплітуда кожної піднесучої перетинає нуль в центрі інших піднесучих, мінімізуючи вплив сусідніх піднесучих.

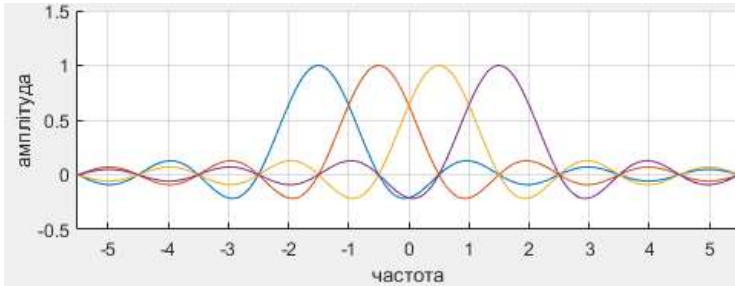


Рисунок 4 – Несучі OFDM-сигналу в області частоти

На рис. 5 показана базова блок-схема повної наскрізної системи OFDM, що складається з передавача і приймача. Бітовий потік надходить в систему зліва на схемі. Як правило, цей єдиний потік бітів демультимплексується (DEMUX) на менші бітові потоки, які подаються на окремі модулятори QAM для кожної з  $N$  піднесучих.

Ключовим фактором для OFDM є використання оберненого швидкого перетворення Фур'є (ОШПФ) для ефективного створення сигналу у області часу з масиву модульованих піднесучих. Результуючий сигнал OFDM в цифровій формі управляє цифро-аналоговим перетворювачем (ЦАП), який перетворює його в аналоговий сигнал. Цей сигнал основної смуги частот зазвичай перетворюється з підвищенням частоти (ПвЧД) до більш високої частоти ( $i$ , можливо, пісилується) перед передачею по ефірному каналу.

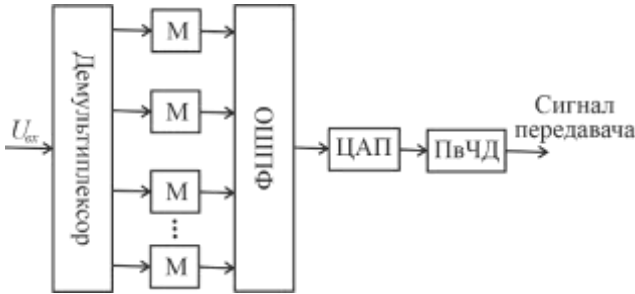
У приймачі процес зворотний. Аналоговий перетворювач з пониженням частоти (ПнЧД) переводить сигнал OFDM назад в смугу модулюючих частот. Аналого-цифровий перетворювач (АЦП) перетворює сигнал в цифрову форму і передає його в блок ШПФ. Блок ШПФ перетворює сигнал з області часу назад в масив піднесучих, несучих модуляцію QAM, в області частоти. Демодулятори QAM відтворюють потік бітів від кожної піднесучої, який потім мультимплексується для відтворення початкового одиночного потоку даних.

Таким чином, основні переваги сигналів з OFDM:

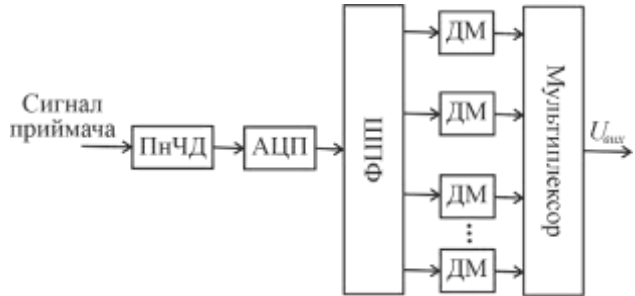
1) об'єднання множини піднесучих QAM для створення широкосмугової системи;

2) використання ШПФ і ОШПФ для ефективного перетворення цих піднесучих в єдиний бездротовий сигнал. Можна використовувати діапазон

модуляції QAM, починаючи з BPSK (один біт на символ) до 256QAM (8 біт на символ). Поєднання цього з використанням множини піднесучих (можливо, 4096) приводить до дуже високих швидкостей передачі даних.



а)



б)

Рис. 5. Цифрова система зв'язку з OFDM: а – передавач; б - приймач (М – QAM модулятор; ОШПФ – обернене швидке перетворення Фур'є;

ЦАП – цифро-аналоговий перетворювач; ПвЧД – підвищуючий перетворювач частоти дискретизації; ПнЧД – понижуючий перетворювач частоти дискретизації; АЦП – аналого-цифровий перетворювач ШПФ – швидке перетворення Фур'є; ДМ – QAM демодулятор)

#### Перелік посилань

1. Мелихов С.В. Аналоговое и цифровое радиовещание / С.В. Мелихов. – Томск: Томск гос. Ун-т систем управления и радиоэлектроники, 2012. – 233 с.
2. Скляр Б. Цифровая связь. Теоретические основы и практическое применение/ изд. 2-е, испр.; пер. с англ. Москва: Вильямс, 2003. 1104 с.
3. Прокис Д. Цифровая связь / под ред. Д.Д. Кловского. Москва: Радио и связь, 2000. 800 с.

#### Алгоритм визначення пробудження людини під час сну

Для постачальників послуг смартфонів вкрай важливо визнати характеристики споживачів. Процес розпізнавання цих характеристик зазвичай називають профілем користувача, який забезпечує основу знань для прийняття бізнес-рішень, забезпечує інтелектуальні послуги та забезпечує унікальну конкурентоспроможність. Як основний компонент профілю користувача, час сну може відображати спосіб життя, стан здоров'я та заняття людей. У цій роботі представлений гнучкий алгоритм під назвою ВТР (Bedtime Prediction), який призначений для прогнозування часу пробудження та сну за допомогою аналізу стану екрану смартфона. ВТР спочатку збирає дані журналу стану екрану смартфона користувача та проводить попередню обробку з низкою допоміжних профілів користувача. Тоді, він виявляє та реєструє час пробудження та сну користувачів за один день шляхом пошуку та поєднання основних періодів гасіння екрану за останні 24 години. Нарешті, ВТР передбачає майбутній час сну, узгоджуючи поточну послідовність стану екрану з усіма історичними записами. Застосовуючи ВТР, більшість програм, що базуються на нічних та ранкових сценаріях, можуть надавати більш уважні послуги, а не дотримуватися фіксованого часу виконання, наприклад будильника. Експерименти з практичних додатків доводять, що ВТР може ефективно прогнозувати час пробудження та час сну без застосування складних алгоритмів машинного навчання або завантаження даних на сервер. а не слідувати фіксованому часу виконання, як будильник.

Процес виявлення та прогнозування АТС може бути придушений багатьма інцидентами. Недостатньо використовувати лише дані журналу стану екрана. У реальних проектах та дослідженнях ми зіткнулися з такими труднощами.

Перший - це ненормальна поведінка. Хтось живе регулярно, але повертається додому дуже пізно або час від часу залишається на вулиці. Цей випадок слід визначити як відхилення в теорії аналізу даних. ВТР містить моделі, засновані на знанні шаблонів, тому ці викиди слід виявити та відмовитись.

Друге - несподіване переривання. Коли люди сплять, вхідні дзвінки, отримання повідомлень та сповіщення від програм можуть засвічуватися на екрані, дзвонити або вібрувати, а потім спричиняти пробудження. Також можливо, що люди засинають глибоким сном і ігнорують ці події. Але для даних журналу стану екрану тривалий період гасіння екрану переривається дивною подією.

Третій - вимкнення смартфона. Якщо смартфон вимкнено, стан екрана та допоміжні події відсутні. Деякі люди не люблять режим польоту, вони

вимикають смартфон перед сном і запускають його, коли встають. Але гірше, користувач може забути зарядити акумулятор, а потім автоматично вимкнути живлення смартфона. Втрата даних журналу є найбільшою загрозою та ризиком ВТР. На малюнку 3 показано стан екрану випадку вимкнення.

Три вищезазначені труднощі згадуються при виявленні, а четверта стосується передбачення. Зважаючи на різний життєвий досвід, норми часу неспанья та сну між людьми пристосовані.

Більшість людей працює в офісі або на заводі, тобто в стабільному цільовому місці. Вони показують ідентифікований час пробудження та розподіл сну протягом робочих днів. Але багато з них - вихідні у вільний стиль. Інші не працюють з понеділка по п'ятницю. Через свої професійні особливості вони демонструють дивні розподіли, такі як ходити на роботу кожні два дні чи три дні роботи та один день відпочинку. Це призводить до великої помилки при прогнозуванні за допомогою простих моделей часових рядів або спробі описати ці закономірності за тижнями та вихідними. Окрім труднощів, ми можемо використати дві переваги для виправлення та вдосконалення нашої моделі. Одне - подія будильника. Для більшості людей вони ходять на роботу в будні. Момент дзвінка будильника - це також час пробудження. Це правило має дуже високу впевненість, і ми можемо перевірити подію, що активується прискорювачем, щоб підтвердити це. Інша подія - активована акселерометром. Коли активовано акселерометр, ми знаємо, що смартфон переміщується і користувач прокинувся. Ми долаємо та зменшуємо ефект чотирьох зазначених вище труднощів за допомогою наступних рішень.

1. Аномальна поведінка. ВТР припускає, що люди сплять вдома. Він відмовився від послідовностей не вдома, щоб уникнути впливу ненормальної поведінки.

2. Несподіване переривання . Порушення сну вирішуються шляхом злиття суміжних періодів стану загасання екрану. Тут ми визначаємо центральну точку сну, приблизно 3 години, найсонніший час доби. Коли людей прокидає подія переривання біля центральної точки сну, вони, швидше за все, залишаються спати через кілька хвилин. Але коли вони менш сонні, наприклад о 5:00, люди можуть вставати по справах.

3. Вимкнення смартфона . Для користувачів, які регулярно та розумно вмикають і вимикають, ВТР розглядає події ввімкнення та вимкнення як час пробудження та час сну. Але ми трактуємо нерегулярне вимкнення живлення як відхилення і відмовляємось від нього.

4. Індивідуальні правила між людьми. Раніше ми вважали, що прогнозування поведінки користувачів має базуватися на робочих днях і вихідних днях, але це заплутано в налаштованих правилах робочого дня, що призводить до більшої помилки. Потім ми змінили нашу стратегію та порівняли поточну послідовність стану екрану з іншими послідовностями кожного минулого дня. Найбільш схожі послідовності представляють

однакову модель поведінки. Оскільки прокидання та лягання спати - це початок і кінець цілоденних занять, вони природно відображаються у цій подібній системі моделей.

Підводячи підсумок, ми ефективно покращуємо точність та доступність послідовності стану екрану при виявленні та прогнозуванні часу пробудження та сну, представляючи низку допоміжних подій. Основний процес ВТР показаний на малюнку 1. ВТР спочатку збирає дані журналу стану екрану користувача та інші допоміжні події, а потім здійснює пошук та підключення періодів гасіння головного екрану, щоб отримати щоденний результат виявлення. Тоді прогнозування здійснюється шляхом узгодження поточної послідовності стану екрана з історичними послідовностями, такими як К-Найближчий сусід.



Рисунок 1 - Потік обробки ВТР.

Тепер дійшла черга до структури даних. По-перше, ми визначаємо структуру даних. Дані журналу містять інформацію як про стан екрану, так і про допоміжний фактор. Подія складається з дати, моменту та події. Різні події відрізняються кодами подій. Тут код SON являє собою загоряння екрану. Для першого завдання, визначення часу пробудження та сну, ми вводимо набір даних журналу з усіма типами подій зі смартфона протягом багатьох днів.

ВТР використовує (1), щоб визначити, чи можна цей період об'єднати з сусідніми періодами; тобто, якщо тимчасовий інтервал між ними коротше ніж  $T$ , ми з'єднаємося дві суміжних послідовностей, як один.  $T$  є поріг, який визначає, слід поєднати дві послідовності, і використовуються для настройки абсолютного значення,  $t$  знаходиться в декількох хвилинах від 12:00 до середини періоду,  $s$  знаходиться в декількох хвилинах від 12:00 до часу, що люди мають глибокий сон, і  $off$  це значення зміщення.

$$T = 1 \cdot \frac{1}{1 + e^{|t-c|/60-off}} \quad (1)$$

У цій роботі представлений алгоритм передбачення сну під назвою ВТР. Метою ВТР є точне виявлення та прогнозування часу пробудження та сну людини шляхом видобутку журналу стану екрану смартфона. Реалізація ВТР не залежить від будь-якої актиграфічної або хмарної інфраструктури, що робить її придатною для популярних додатків та забезпечує захист конфіденційності.

Перелік посилань

1. С. Сеневіратне, А. Сеневіратне, П. Мохапатра та А. Маханті, “Прогнозування властивостей користувачів за допомогою знімка програм, встановлених на смартфоні”, ACM SIGMOBILE Mobile Computing and Communications Review, 2014.

2. А. Андерсен та Р. Карлсен, “Профілювання користувачів за допомогою взаємодії NFC: видобуток інформації про користувачів на основі NFC з мобільних пристроїв та внутрішніх систем”, у Матеріалах 14-го Міжнародного симпозиуму ACM з питань управління мобільністю та бездротового доступу, MobiWac 2016.

3. Ю. Фан, Ю. Чень, К. Тунг, К. Ву та А. Л. Чен, “Структура для забезпечення профілювання переваг користувачів за допомогою журналів Wi-Fi”, у матеріалах 32-ї Міжнародної конференції з питань інженерії даних IEEE 2016 (ICDE)..

4. G. Orellana, SM Held, PA Estevez et al., «Метод класифікації збалансованого сну / неспання на основі актиграфічних даних у підлітків», у матеріалах 36-ї щорічної міжнародної конференції IEEE Товариства з медицини та біології, EMBC 2014.

### **Моделювання спотворень сигналу у каналі передачі і їх впливу на коефіцієнт бітових помилок цифрової системи зв'язку**

Шпірук М. С.

Науковий керівник – к.т.н., доц. Пятін І.С.

Хмельницький національний університет

У сучасних системах передачі інформації необхідно забезпечити тактову синхронізацію передавача і приймача. При цьому використання незалежних задаючих генераторів призводить до різниці частот дискретизації сигналів передавача і приймача. Приймач повинен знати, де починається і де закінчується кожний символ. Ця інформація необхідна, щоб знати відповідний інтервал інтегрування для прийняття рішення про значення символу [1]. Символьна синхронізація передбачає генерацію в приймачі частини переданого сигналу. Це прямокутні коливання, що синхронізовані зі швидкістю передачі символів.

Останнім часом при побудові цифрових систем зв'язку, все більше функцій, що традиційно виконуються аналоговими пристроями, реалізуються на базі цифрових сигнальних процесорів (ЦСП). В поєднанні з додаванням ЦСП межа між аналоговим і цифровим сегментами систем зв'язку, що розділені АЦП, невблаганно рухається до антени.

SDR включає аналогові компоненти: антени, попередні фільтри, комутатори, попередні підсилювачі і підсилювачі потужності, та цифрові компоненти: GPP (процесор загального застосування); DSP (цифровий

сигнальний процесор); FPGA (програмована користувачем матрична БІС); ASIC (спеціалізована інтегральна схема). З цими уніфікованими обчислювальними і керуючими вузлами можна реалізувати велику кількість різноманітних функцій, наприклад, модуляцію, демодуляцію, фільтрацію, кодування. Схема ASIC не програмується, а спеціально розробляється для кожного варіанту застосування. Для неї характерні низькі витрати на виробництво, невелика споживана потужність і висока продуктивність.

Матричні БІС (FPGA) незамінні в програмних радіопристроях, завдяки високій продуктивності і програмованості. Їх обчислювальна продуктивність набагато вище, ніж у DSP або GPP. Це обумовлено можливістю квазіпаралельної обробки даних. Схеми DSP і GPP здійснюють тільки послідовну обробку даних і в деяких випадках ітеративну. Основними перевагами DSP і GPP є їх програмованість і можливість перебудови конфігурації.

У загальному випадку при проектуванні системи зв'язку необхідно враховувати такі основні фактори, що впливають на сигнал при його поширенні в каналі зв'язку:

- вплив адитивного білого гаусового шуму (теплого шуму);
- частотне і фазове зміщення сигналу, що може бути викликане взаємним рухом антени передавача і приймача або неузгодженістю їх гетеродинов, викликане нестабільністю джерел опорної частоти;
- затримка сигналу в каналі зв'язку, що викликано розповсюдження від антени передавача до антени приймача і в фідерних системах;
- завмирання, викликані багатопроменевим поширенням сигналу від передавача до приймача, явищами рефракції в атмосфері і перевідбиваннями від різних об'єктів.

При моделюванні систем зв'язку на персональному комп'ютері особливу увагу необхідно приділити питанням затримки сигналу в каналі зв'язку. Оскільки моделювання на комп'ютері принципово може бути тільки дискретним в області часу, для проведення коректних досліджень систем синхронізації приймального пристрою необхідно створювати дробову затримку в каналі зв'язку.

Розглянемо математичну модель сигналу на вході приймача. Нехай передавач формує цифрову інформацію за допомогою  $m$  сигналів  $s(t) = \{s_m(t)\}$ , де  $m$  - кількість точок у сигнальному сузір'ї цифрової модуляції [1]. Для модуляції QPSK  $m=4$ .

$$s_1(t) = \sqrt{\frac{2E}{T}} \cos(\omega_0 t + \pi/4); \quad s_2(t) = \sqrt{\frac{2E}{T}} \cos(\omega_0 t + 3\pi/4);$$

$$s_3(t) = \sqrt{\frac{2E}{T}} \cos(\omega_0 t + 5\pi/4); \quad s_4(t) = \sqrt{\frac{2E}{T}} \cos(\omega_0 t + 7\pi/4).$$

Кожний сигнал передається на символному інтервалі  $T$  проміжком часу  $0 \leq t \leq T$ . Канал спотворює сигнал за допомогою адитивного білого гаусового шуму (АБГШ). Таким чином, сигнал на вході приймача на інтервалі  $0 \leq t \leq T$  можна записати виразом [2]:

$$r(t) = s_m(t) + n(t),$$

де  $n(t)$  означає реалізацію АБГШ з двобічною спектральною густиною потужності  $\Phi_n(f) = N_0/2$ .

Положимо, що на вхід узгодженого фільтра, за яким розташований пристрій дискретизації, надходить сигнал  $r(t)$ . Сигнал на виході узгодженого фільтра можна представити за допомогою передаточної функції фільтра  $H(f)$  і спектральної густини сигналу на вході  $S(f)$ :

$$s_{\text{вф}}(t) = \int_{-\infty}^{\infty} H(f)S(f)e^{j2\pi ft} df$$

Дисперсія шуму на виході  $\sigma_0^2$  визначається виразом:

$$\sigma_0^2 = \frac{N_0}{2} \int_{-\infty}^{\infty} |H(f)|^2 df$$

Приймач складається з двох частин: демодулятор сигналу і детектор. Функція демодулятора складається у перетворенні сигналу  $r(t)$  у вектор  $r = \{r_1, r_2, r_3, r_4\}$ . Функція детектора полягає у вирішенні, який з можливих сигналів  $m$  був переданий. Розглянемо Simulink модель цифрової системи зв'язку з QPSK модуляцією, що представлена на рис. 1.

Random Integer Generator є джерелом інформаційного цифрового сигналу. Далі, згідно моделі, відбувається низькочастотна QPSK модуляція, узгоджена фільтрація і перенесення спектра сигналу в область високих частот у блоці Upconverter. Блок Phase/Frequency Offset застосовує зміщення фази і частоти до комплексного високочастотного сигналу [3]. Якщо вхідним сигналом є  $u(t)$ , то вихідний сигнал:

$$y(t) = u(t) \cdot \left( \cos \left( 2\pi \int_0^t f(\tau) d\tau + \varphi(t) \right) + j \sin \left( 2\pi \int_0^t f(\tau) d\tau + \varphi(t) \right) \right),$$

де  $f(t)$  - зміщення частоти;  $\varphi(t)$  - зміщення фази.



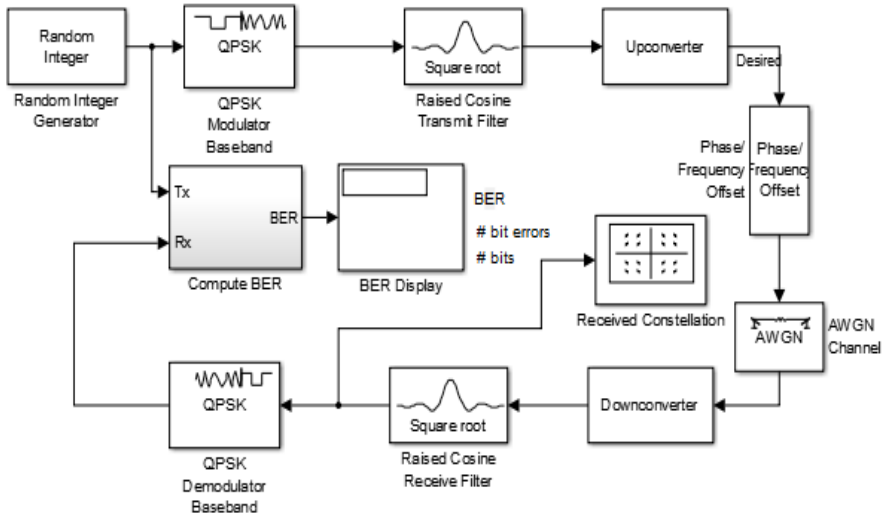


Рисунок 1 – Simulink модель цифрової системи зв'язку з QPSK модуляцією

На боці приймача виконується перенесення спектра сигналу в область нульових частот блоком Downconverter, узгоджена фільтрація і низькочастотна QPSK демодуляція.

Якщо зміщення фази встановити у  $20^0$ , то кожна точка в сузір'ї буде повернута на  $20^0$  проти годинникової стрілки. Коефіцієнт бітових помилок дорівнює 0 при відношенні сигнал-шум 20 дБ. Сузір'я QPSK модуляції в цьому випадку зображено на рис. 2. Якщо для параметра «Зміщення частоти» встановлено значення 2 Гц, а зміщення фази = 0, то кути точок в сузір'ї змінюються лінійно з часом. Це призводить до радіального зміщення точок на діаграмі розсіювання, як показано на рис. 3.

Відбувається обертання сузір'я з частотою 2 Гц проти годинникової стрілки. Коефіцієнт бітових помилок дорівнює 0,5 при відношенні сигнал-шум 20 дБ. При наявності кола символної синхронізації і введенні зміщення частоти у 2 Гц коефіцієнт бітових помилок стає 0,002. Це означає підвищення ефективності у 250 разів або на 24 дБ.

Таким чином, для зменшення впливу спотворень у каналі зв'язку, необхідно забезпечувати синхронізацію сигналів передавача і приймача. Це суттєво ускладнює приймач, але дозволяє зменшити кількість бітових помилок від відношення сигнал-шум цифрової системи зв'язку.

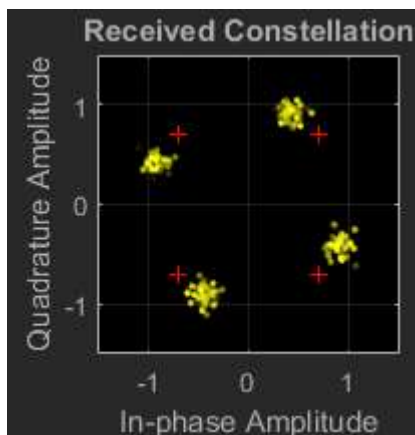


Рисунок 2 – Сузір'я QPSK модуляції, обумовлене зміщенням фази

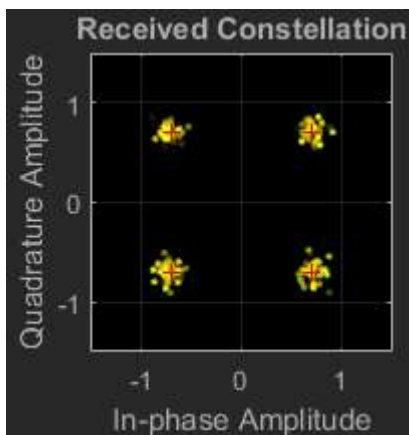


Рисунок 3 – Сузір'я QPSK модуляції, обумовлене зміщенням частоти

Енергетична ефективність не когерентної цифрової системи зв'язку з модуляцією QPSK при виникненні фазового зміщення  $30^\circ$  у середовищі розповсюдження зменшується на 10 дБ. Додавання кола символної синхронізації компенсує цей поворот сигнального сузір'я. Збільшення фазового зміщення у середовищі розповсюдження до  $45^\circ$  для когерентної системи зв'язку приводить до зменшення енергетичної ефективності на 2 дБ.

#### Перелік посилань

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение/ Б. Скляр. Изд. 2-е, испр.: Пер. с англ. – М. : Издательский дом «Вильямс», 2003. – 1104 с.
2. Прокис Д. Цифровая связь / Д. Прокис. Пер. с англ. под ред. Д.Д. Кловского. – М.: Радио и связь, 2000. – 800 с.
3. Rice M. Digital communications: a discrete-time approach. – New Jersey: “Pearson Education, Inc.”, 2009. – 778 p.

### **Продукційна модель експертної системи для вибору оптимального раціону харчування.**

Яшина О.М., Прейзнер Є.Е.

Хмельницький національний університет

В умовах сьогодення питання збалансованого харчування стоїть в центрі уваги сучасної медицини та включене до списку найважливіших

проблем, що розглядаються Всесвітньою організацією охорони здоров'я. Швидке збільшення чисельності населення нашої планети призвело до відповідного зростання виробництва харчових ресурсів і продуктів харчування. Різноманіття продуктів, в свою чергу, ставить питання культури харчування і розумного споживання їжі для збереження здоров'я. У раціоні сучасної людини все частіше зустрічається висококалорійна їжа: кондитерські вироби, борошняні вироби, жирне м'ясо, алкоголь. Важливо відзначити, що незбалансоване, висококалорійне харчування і переїдання є основними причинами розвитку надмірної ваги і ожиріння, що в свою чергу призводить до серцево-судинних захворювань, діабету та інших важких хвороб. З іншого боку голодування та недоїдання з метою схуднення можуть призвести до появи не менш серйозних захворювань.

Метою даної роботи є створення програмної системи для формування рекомендацій по оптимізації раціону харчування для користувача на основі аналізу інформації про його стан здоров'я та цілей, які він хоче досягти.

Аналіз літературних джерел дозволив встановити, що в сфері штучного інтелекту для вирішення поставлених задач найбільше підходить методологія експертних систем.

До основних переваг експертних систем відносять:

- збереження знань системи протягом довгого часу;
- легкість передачі або відтворення;
- можливість одержання й об'єднання експертних знань з багатьох джерел;
- формалізація і перевірка знань;
- можливість застосування у якості інтелектуальної бази даних;
- об'єктивний результат за будь-яких обставин;
- можливість пояснення рішень.

Таким чином, в розроблюваному програмному комплексі експертна система буде використовуватись для раціонального вибору продуктів та страв на основі властивостей продуктів і раціону в цілому за критеріями харчової та біологічної цінності в залежності від стану здоров'я людини (зріст, вага тіла, стать, наявність алергій та хвороб), її щоденної активності та цілей, які вона хоче досягти.

Для вирішення наведених задач буде використовуватись продукційна модель експертної системи. Під даною моделлю мається на увазі система, заснована на продукційних правилах. Кожне з таких правил містить дві частини: умова та дія.

Загальна стратегія вирішення проблем в продукційній моделі полягає в розбитті завдань на фрагменти, які можна легше довести. При цьому, існують 2 підходи до вирішення завдань:

- прямий логічним висновок;
- зворотній логічний висновок.

Системи з прямим логічним висновком знаходяться під управлінням фактів. Вони починають свою роботу з відомих початкових фактів і продовжують, використовуючи правила для створення висновків або виконання певних дій. Подібна логіка вирішення проблем ідеально підходить для нашого випадку, тому системи зі зворотнім логічним висновком розглядати не доцільно.

Таким чином при побудові програмного забезпечення буде вперше удосконалено процес вибору оптимального раціону харчування за допомогою засобів штучного інтелекту.

Крім того, після використання експертної системи потрібно ще підрахувати розміри порцій добового раціону, враховуючи не повторюваність цих страв, їх поживну цінність та кількість мінералів. Для досягнення цього буде використовуватись алгоритм формування індивідуального меню с урахуванням індивідуальних особливостей людини та математична модель, яку можна описати наступним чином:

$$\mu_k = \begin{Bmatrix} 0 \\ 1 \end{Bmatrix} \quad (2.1)$$

де  $\mu_k$ - змінна включення до складу раціону при наступних обмеженнях:

1) по не повторюваності страв в добовому раціоні

$$\mu_k = 1 ; k \in k_a, k_b, k_c \quad (2.2)$$

2) на граничну калорійність одного прийому їжі

$$\sum_k \mu_k Q_k \leq Q_{\text{доб}} \eta_1 \quad (2.3)$$

де  $Q_k$  - нормативна калорійність  $k$ -тої страви, ккал;  $Q_{\text{доб}}$  - гранична калорійність добового раціону, ккал;  $\eta_1$  - частка добової калорійності, яка припадає на сніданок, обід і вечерю, таким чином, що

$$\sum_1 \eta_1 = 1 \quad (2.4)$$

3) на граничний обсяг сніданку, обіду та вечері

$$\sum_k \mu_k V_k \leq V_{\text{доб}} \omega_1 \quad (2.5)$$

де  $V_{\text{доб}}$  - граничний добовий обсяг раціону, г;  $V_k$  - об'єм  $k$ -тої страви, г;  $\omega_1$  - частка добового обсягу, що припадає на сніданок, обід і вечерю, таким чином, що

$$\sum_1 \omega_1 = 1 \quad (2.6)$$

4) по верхньому і нижньому кордонах змісту і-го хімічного елемента

$$B_i^{\min} \leq \mu_k \sum_j \alpha_{ij} Z_{jk} \leq B_i^{\max} \quad (2.7)$$

де  $B_i^{\min}$  та  $B_i^{\max}$  - відповідно нижні і верхні обмеження на вміст в добовому раціоні білків, жирів та вуглеводів, мг;  $\alpha_{ij}$  - зміст і-го елемента хімічного складу в одиниці j-го продукту;  $Z_{jk}$  - рекомендований вміст j-го продукту в k-ій страві, г;

5) по масі k-ої страви, г

$$\sum_j Z_{jk} = Z_k \quad (2.8)$$

Таким чином на основі викладеного вище можна сформулювати схему руху і перетворення даних при роботі системи (Рисунок 1).

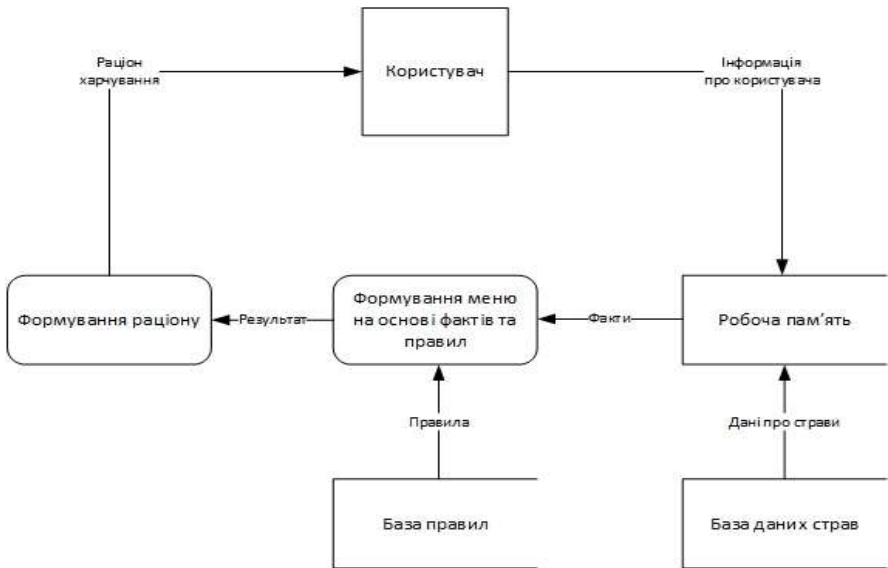


Рисунок 1 – Модель роботи програмної системи

Робота програмної системи складається з таких кроків:

1. Введення користувачем інформації про себе.

2. Завантаження даних про здоров'я користувача до робочої пам'яті.
3. Завантаження даних про страви до робочої пам'яті.
4. Завантаження фактів до експертної системи.
5. Завантаження правил до експертної системи.
6. Формування меню, яке найкраще підходить користувачу, на основі фактів та правил.
7. Формування раціону на основі результатів роботи експертної системи.
8. Виведення сформованого раціону у вікно інтерфейсу користувача.

Отже, в даній роботі вдосконалено продукційну модель для вибору оптимального раціону харчування. В процесі розробки, на основі ряду досліджень та публікацій було проаналізовано процес формування і оптимізації раціону харчування людини, пояснено що являє собою раціональне та нераціональне харчування і чим вони відрізняються. Використання розробленої продукційної моделі здатне зробити процес вибору раціону харчування більш ефективним. Крім того, створену модель можна покращити, додавши нові правила в базу знань.

#### Література

1. Сидоркина И.Г. Системы искусственного интеллекта: учебное пособие [текст] / И.Г Сидоркина// М.: КНОРУС. – 2011. – 248 с.
2. Глазкова И.В., Ивашкин Ю.А. Оптимизация рационов питания с использованием компьютерных технологий// Пищевая промышленность. – 2010. – №6. – С.61-63.
3. Герасименко Н.Ф. Здоровое питание и его роль в обеспечении качества жизни / Герасименко Н.Ф., Позняковский В.М., Челнакова Н.Г. // Технологии пищевой и перерабатывающей промышленности АПК - продукты здорового питания. – 2016. – № 4 (12). – С. 52-57.
4. Хох В.Д. Дослідження методів побудови експертних систем / В. Д. Хох, Є. В. Мелешко, М. С. Якименко // Системи управління, навігації та зв'язку. – 2016. – № 4 (10). – С. 48-52.
5. Седих О. Л. Дослідження методології побудови та принципів функціонування експертних систем / О. Л. Седих, В. О. Овчарук // Международное периодическое научное издание. Научные труды SWorld. – Иваново : Научный мир, 2016. – № 1 (42). – С. 13–19.







## Наукове видання

«Інтелектуальний потенціал – 2020» - збірник наукових праць молодих науковців і студентів / Колектив авторів – Хмельницький: ПВНЗ УЕП, 2020.  
– Частина 1. – 104 с.

**Відповідальність за зміст текстів і якість редагування матеріалів  
покладена на авторів і наукових керівників.**

Комп'ютерна верстка: Чешун В.М.  
Дизайн Хмельовський В.Р.

---

**Здано до складання 09.11.20. Підписано до друку 09.11.20. Формат 60x84/16. Папір друкарський. Тираж 50 прим. Умовних друківаних аркушів – 7,5.**

**Редакційний відділ ПВНЗ УЕП 29016, м. Хмельницький,  
вул. Львівське шосе, 51/2.**

ББК 74.480.278  
С.88