МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

XV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 ЧЕРВНЯ 2025 Р.

М. КИЇВ

MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
STATE UNIVERSITY "KYIV AVIATION INSTITUTE"
STATE SERVICE OF SPECIAL COMMUNICATION AND INFORMATION PROTECTION OF UKRAINE
SCIENTIFIC CYBER SECURITY ASSOCIATION OF UKRAINE

PROCEEDINGS

OF THE SCIENTIFIC AND PRACTICAL CONFERENCE

«OPERATIONAL AND SECURITY PROBLEMS OF INFORMATION AND COMMUNICATION SYSTEMS»

June, 4 – 6, 2025
Kyiv, Ukraine

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
«КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 червня 2025 р.

м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 4 – 6 червня 2025 р., Державний університет «Київський авіаційний інститут». – К.: Вид-во КАІ, 2025. – 187 с.

ISBN: 978-611-01-0740-2

ОРГКОМІТЕТ КОНФЕРЕНЦІЇ

Голова:

Гнатюк С.О. — проректор з наукових досліджень та трансферу технологій Державного університету «Київський авіаційний інститут», доктор технічних наук, професор;

Члени оргкомітету:

Гнатюк В.О. — кандидат технічних наук, доцент, завідувач кафедри телекомунікаційних та радіоелектронних систем Державного університету «Київський авіаційний інститут», **головний редактор редколегії**;

Юдін О.Ю. — кандидат технічних наук, заступник начальника Державного науково-дослідного інституту технологій кібербезпеки та захисту інформації;

Одарченко Р.С. — доктор технічних наук, професор, декан Факультету аеронавігації, електроніки та телекомунікацій Державного університету «Київський авіаційний інститут»;

Бахтіяров Д.І. — кандидат технічних наук, доцент, заступник декана Факультету аеронавігації, електроніки та телекомунікацій Державного університету «Київський авіаційний інститут»;

Секретар:

Лавриненко О.Ю. — кандидат технічних наук, доцент, доцент кафедри телекомунікаційних та радіоелектронних систем Державного університету «Київський авіаційний інститут».

ЗМІСТ

Д. Є. Антіпов, Д. І. Бахтіяров
КОНЦЕПЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ХМАРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ РІШЕНЬ HUAWEI..... 10

В.С. Багмет
ОПТОВОЛОКОНОННИЙ КАНАЛ ЗВЯЗКУ ДЛЯ БПЛА В УМОВАХ ІНТЕНСИВНОГО ВИКОРИСТАННЯ РЕБ..... 12

А.І. Битько
ДОСЛІДЖЕННЯ НОВІТНІХ ВИКЛИКІВ ТА РОЛІ РАДІОЧАСТОТНОГО ВИЯВЛЕННЯ БПЛА..... 14

I.V. Bohush
DESIGN OF A WIRELESS FIRE AND SECURITY ALARM SYSTEM FOR SMART HOME ENVIRONMENTS..... 16

Р.М. Гамрецький, В.О. Гнатюк
ОСОБЛИВОСТІ ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯДРА 5G..... 18

І.С. Гируцький, Б.С. Чумаченко
МЕТОД НАЛАШТУВАННЯ VPN-ТУНЕЛІВ НА БАЗІ ОБЛАДНАННЯ MIKROTIK..... 20

Я.О. Горда, В.М. Чуприн
ВІРТУАЛЬНА СЕРВЕРНА ІНФРАСТРУКТУРА НА БАЗІ ТЕХНОЛОГІЇ HYPER-V..... 22

І.Ю. Гордієнко, В.М. Чуприн
ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА ПАКЕТНОЇ ПЕРЕДАЧІ ДАНИХ НА БАЗІ ОБЛАДНАННЯ JUNIPER..... 26

Ю.Р. Гриценко, В.В. Антонов
СИСТЕМА ВІДЕОКОНФЕРЕНЦІЇ НА БАЗІ VOIP 29

І.І. Гуменний, А.О. Осіпчук
РОЗРОБКА ПОЛІТИК БЕЗПЕКИ ТА ЇХ ВПРОВАДЖЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO 31

Э.О. Гусєв, В.В. Антонов
ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ЗАПОБІГАННЯМ ЗАГРОЗАМ У ТКМ 35

В.Є. Данилюк
ДОСЛІДЖЕННЯ ПРОБЛЕМИ ДОСТУПУ ДО ДАНИХ З ВИКОРИСТАННЯМ МЕРЕЖІ СТАНДАРТУ LTE 37

Т.С. Денисенко
ПРОЕКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПРОМИСЛОВОГО ПІДПРИЄМСТВА: ВИМОГИ, ПРИНЦИПИ ТА ТЕХНОЛОГІЇ 39

O.S. Dmytrenko
METHODS FOR DETECTING AND PREVENTING DDOS ATTACKS IN VOIP SYSTEMS 41

М.О. Дроздовський, Д. І. Бахтіяров
КОНЦЕПЦІЯ БЕЗДРОТОВОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ WI-FI 7 ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ HUAWEI..... 43

М.В. Дубович
ПРОЕКТУВАННЯ ТА ТЕХНІЧНА ЕКСПЛУАТАЦІЯ СИСТЕМИ ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ В ШКОЛІ 45

А.О. Ємельянов
АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЛЯ АС КЛАСУ 2 ТА МЕТОДИ ЇХ НЕЙТРАЛІЗАЦІЇ 47

B.S. Yefimenko
VIPER. REMOTE VIDEO AND CONTROL UNIT 48

В.В. Кальєв
СИСТЕМАУПРАВЛІННЯРОЗУМНИМБУДИНКОМНА ОСНОВІ TELEGRAM-БОТА 50

Б.Р. Кальчук, В.М. Чуприн
СИСТЕМА ЛОКАЛЬНОГО ПОЗИЦІОНУВАННЯ НА БАЗІ ТЕХНОЛОГІЇ IEEE 802.15 52

В.В. Каракай
СИСТЕМА ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ ОСОБИ В ДИСТАНЦІЙНОМУ БАНКІВСЬКОМУ ОБСЛУГОВУВАННІ 56

І.В. Касьян
КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ (НА ПРИКЛАДІ ГРУПИ КОМПАНІЙ «НОВА ПОШТА») 58

А.О. Кобилінський
ШТУЧНИЙ ІНТЕЛЕКТ У ПОБУТОВОМУ ВИКОРИСТАННІ ЛЮДИНИ: КОЛИ АІ СТАЄ ЧАСТИНОЮ НАШОГО ЖИТТЯ 60

Д.В. Коваль
МОДЕЛЮВАННЯ СЕГМЕНТОВАНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ VLAN 62

М.М. Козуб, М.Б. Гумен
MESH СИСТЕМА ПРИСТРОЇВ IOT 64
М.С. Колот, В.О. Гнатюк
МОДЕЛЬ АДАПТИВНОГО УПРАВЛІННЯ РЕСУРСАМИ В IP-ТЕЛЕФОНІЇ 68
Д.С. Короткевич
ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKROTIK 70
А.І. Кошель, В.М. Чуприн
МОДЕЛЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА БАЗІ ПЛАТФОРМИ ВІРТУАЛІЗАЦІЇ UNETLAB 72
Д.В. Кравцов, А.Г. Тараненко
SD-WAN ПРОТИ ТРАДИЦІЙНИХ WAN: СУЧАСНИЙ ПОГЛЯД НА ПРОДУКТИВНІСТЬ МЕРЕЖІ 76
А. О. Левченко, Д. І. Бахтіяров
СИСТЕМА IP-ВІДЕОСПОСТЕРЕЖЕННЯ ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ HUAWEI 78
Максимов М.Д., Малоєд М.М.
РОЗРОБКА АВТОМАТИЗОВАНИХ ТЕСТІВ ДЛЯ ВЕБ-ДОДАТКІВ 80
В.С. Мацько, М.М. Малоєд
МЕТОД ЗНИЖЕННЯ ЕНЕРГОСПОЖИВАННЯ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ 82
В.С. Мензюк, В.В. Антонов
МЕРЕЖА ДОСТУПУ З ВИКОРИСТАННЯМ VDSL2 ТЕХНОЛОГІЇ 84
В.В. Нагорний
СИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ В ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ НА БАЗІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ 86
Д.С. Нефедов
ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ РОЗПІЗНАВАННЯ ТА КЕРУВАННЯ БАГАЖЕМ 89
В.О. Окусков
СИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОСТЕЙ У МЕРЕЖЕВОМУ ТРАФІКУ НА ОСНОВІ НЕЙРОМЕРЕЖ 91

С.В. Онацька, В.В. Антонов
КОРПОРАТИВНА VOIP МЕРЕЖА 93
С. О. Передерій
ОПТИМІЗАЦІЯ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ЦИВІЛЬНИХ ТА ПРОМИСЛОВИХ СФЕРАХ 96
І.Р. Потіха
МЕТОДИ ПОКРАЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ КЛІЄНТІВ ІНТЕРНЕТ-ПРОВАЙДЕРА 98
Rohozha I.O.
CLASSIFICATION OF CRITICAL INFRASTRUCTURE OBJECTS AND MONITORING SYSTEMS. COMPONENTS, DATA TRANSFER AND PROTOTYPE SYSTEM. CRITERIA FOR EVALUATING EFFECTIVENESS 100
Я.Ю. Руденко
СЕРВІС ПЕРЕДАЧІ ДАНИХ МОБІЛЬНОГО АБОНЕНТА 102
Я.Є. Ружин, В.В. Антонов
МІЖМІСЬКА ТРАНСПОРТНА МЕРЕЖА OTN 104
Самойленко О.А., Зуєв О.В.
СИСТЕМА МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ 107
О.М. Сахно
НЕЙРОННІ ТЕХНОЛОГІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЯХ 109
З.О. Сердюк, В.В. Антонов
ВОЛОКОННО-ОПТИЧНА ЛІНІЯ З ТЕХНОЛОГІЄЮ СПЕКТРАЛЬНОГО УЩІЛЬНЕННЯ MWDM 111
Д.А. Сіньков
ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ВИЯВЛЕННЯ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ БПЛА 114
Я.Р. Смолій
РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЦИФРОВІЙ ОБРОБЦІ ЗОБРАЖЕНЬ 116
А.В. Сова, Д.І. Бахтіяров
СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ..... 118
І.В. Tregubenko
VULNERABILITIES OF INTELLIGENT CLOUD APPLICATIONS WITH MICROSERVICE ARCHITECTURE 122

Д. Б. Хмель, Д.І. Бахтіяров
СИСТЕМА ВИЯВЛЕННЯ ЗАГРОЗ В IoT-МЕРЕЖАХ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ 124
Д.В. Черненко
СИСТЕМА КОНТРОЛЮ ВИСОТИ ПОЛЬОТУ БЕЗПІЛОТНОГО ЛУТАЛЬНОГО АПАРАТУ 126
M.S. Chubenko
INTELLIGENT SYSTEM OF INFORMATION PROCESSING BASED ON RFID IDENTIFICATION 128
Д.К. Шевченко
THREAT ANALYSIS SYSTEMS IN 5G NETWORKS: ARCHITECTURE, CHALLENGES, AND FUTURE DIRECTIONS 130
В.А. Шемет
СУЧАСНІ АКТИВНІ ТА ПАСИВНІ ЗАСОБИ ПРОТИДІЇ ТЕХНІЧНИМ КАНАЛАМ ВИТІКУ ІНФОРМАЦІЇ 132
М.О. Шихов
РОЗРОБКА ЗАХИЩЕНОЇ API-ІНФРАСТРУКТУРИ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ СЕРВІСІВ 134
D.V. Yanovskyi
FRAGMENT OF 5G NETWORK BASED ON NOKIA EQUIPMENT..... 136
А.С. Шостак
ІНТЕЛЕКТУАЛЬНА СИСТЕМА РОЗПІЗНАВАННЯ ОБЛИЧЧЯ: ТЕОРЕТИЧНІ ЗАСАДИ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ БАЗОВОГО АЛГОРИТМУ..... 138
В.С. Коваль
СОНЯЧНІ ДЖЕРЕЛА ЖИВЛЕННЯ ОБЛАДНАННЯ ДЛЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ..... 140
В.В. Петруньок
ДОСЛІДЖЕННЯ ВПЛИВУ МАТЕРІАЛІВ СТІН НА ПОШИРЕННЯ СИГНАЛУ 4G/5G..... 142
С.В. Макаренко
ДОДАТОК ДЛЯ ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ МОБІЛЬНОГО ПРИСТРОЮ..... 144
Д.О. Сай, В.В. Антонов
СИСТЕМА АВТОМАТИЗАЦІЇ БУДІВЛІ..... 146

А. Р. Курликін
РОЗРОБКА ЦИФРОВОГО ФІЛЬТРА ГЛІССАДНОГО МАЯКА ІНСТРУМЕНТАЛЬНОЇ СИСТЕМИ ПОСАДКИ..... 149

І.О. Гаврищук, М.М. Малоєд
ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ НОМЕРІВ АВТОМОБІЛІВ МЕТОДАМИ ГЛИБОКОГО НАВЧАННЯ..... 151

Н.С. Андріяшина
СЛІДКУЮЧИЙ ФАЗОВИЙ РАДІОПЕЛЕНГАТОР ДЛЯ БПЛА..... 153

М.В. Романчук, М.М. Малоєд
МОДИФІКОВАНИЙ МЕТОД ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В IoT-СИСТЕМАХ..... 155

Б.П. Котик, П.В. Наконешний
МЕТОД ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕЮ ТА ОПТИМІЗАЦІЇ ТРАФІКУ НА ОСНОВІ SDN І ШТУЧНОГО ІНТЕЛЕКТУ..... 157

А.В. Лелеко, Д.І. Бахтіяров, П.В. Наконешний
МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЯКОСТІ МОБІЛЬНОГО ЗВ'ЯЗКУ ШЛЯХОМ ЗАСТОСУВАННЯ НАДШИРОКОСМУГОВИХ ТЕХНОЛОГІЙ..... 160

О.А. Добринчук, В.В. Лукашенко
ОСОБЛИВОСТІ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ ТА КЕРУЮЧИХ СИСТЕМ АТОМНОЇ СТАНЦІЇ ЯК ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ..... 163

O. Lavrynenko
VOICE CONTROL COMMAND RECOGNITION SYSTEM OF UAV BASED ON CEPSTRAL ANALYSIS..... 168

O. Lavrynenko
COMPRESSION ALGORITHM OF VOICE CONTROL COMMAND OF UAV BASED ON WAVELET TRANSFORM..... 174

O. Lavrynenko
COMPARATIVE ANALYSIS OF SPEECH RECOGNITION ALGORITHMS UAV..... 180

УДК 004.77:004.72(043.2)

Д. Є. Антіпов, Д. І. Бахтіяров канд. техн. наук, доцент
Державний університет
«Київський авіаційний інститут», м. Київ

КОНЦЕПЦІЯ ІНТЕЛЕКТУАЛЬНОЇ ХМАРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА ОСНОВІ РІШЕНЬ HUAWEI

Сучасний етап розвитку інформаційних технологій характеризується невпинною цифровою трансформацією бізнесу, де хмарні обчислення є ключовою інфраструктурною платформою. Підприємства стикаються зі зростанням обсягів даних, ускладненням кіберзагроз та потребою у гнучких IT-рішеннях. Традиційні мережеві архітектури часто не відповідають цим вимогам через складність управління та обмежену адаптивність. Це зумовлює актуальність переходу до інтелектуальних хмарних мереж, які поєднують переваги хмарних технологій, віртуалізації, програмно-конфігурованих підходів (SDN) та штучного інтелекту (AI). Дана робота присвячена розробці концепції такої інноваційної мережі на базі рішень компанії Huawei.

Запропонована концепція інтелектуальної хмарної мережі підприємства ґрунтується на комплексному підході Huawei, що об'єднує передові апаратні та програмні рішення. В основі архітектури лежить багаторівнева інфраструктура (доступ, агрегація, ядро), побудована на комутаторах CloudEngine та S-серії, маршрутизаторах AR та NE, а також точках доступу AirEngine. Безпека забезпечується міжмережевими екранами HiSecEngine/USG. Ключовим елементом є платформа віртуалізації Huawei FusionCompute, яка віртуалізує фізичні ресурси серверів, сховищ та мережі. Це дозволяє ефективно реалізувати принципи SDN та віртуалізації мережевих функцій (NFV), забезпечуючи швидке розгортання сервісів та оптимізацію використання ресурсів. Підтримується побудова гібридних хмарних середовищ для інтеграції локальної інфраструктури з публічними сервісами Huawei Cloud, забезпечуючи безперервність бізнес-процесів.

Центральну роль в управлінні, моніторингу та аналітиці відіграє інтелектуальна платформа iMaster NCE. Вона надає єдину точку контролю над фізичними та віртуальними мережевими ресурсами та взаємодіє з платформою FusionCompute для оркестрації віртуалізованого середовища. iMaster NCE використовує алгоритми AI

та машинного навчання (ML) для автоматизації мережевих операцій, проактивного виявлення потенційних проблем, інтелектуальної діагностики та оптимізації продуктивності мережі. Це дозволяє реалізувати концепцію "Все-в-одній мережі" Huawei, де локальні, глобальні мережі та ресурси ЦОД управляються як єдина система.

Реалізація такої архітектури забезпечує високу доступність завдяки механізмам VM HA та DRS у FusionCompute, а також протоколам мережевої надмірності. Гарантується багаторівнева безпека, що включає сегментацію на основі VLAN/VXLAN та групи безпеки для віртуальних машин. Також забезпечується ефективне управління якістю обслуговування (QoS) для пріоритезації критичного трафіку. Практичне застосування охоплює сценарії об'єднання філій через SD-WAN, підтримку віддаленої та мобільної роботи, зокрема через VDI-рішення Huawei FusionAccess, розгортання уніфікованих комунікацій та побудову захищеної інфраструктури для Інтернету Речей (IoT).

Представлена концепція інтелектуальної хмарної мережі підприємства на базі рішень Huawei є ефективним підходом до модернізації корпоративних IT-інфраструктур. Завдяки передовому мережевому обладнанню, платформі віртуалізації FusionCompute та інтелектуальній системі управління iMaster NCE досягається значне підвищення гнучкості, масштабованості, надійності та безпеки мережі. Впровадження такої архітектури дозволяє підприємствам оптимізувати операційні витрати, підвищити ефективність використання ресурсів та створити технологічний фундамент для інноваційних цифрових сервісів. Подальший розвиток подібних інтегрованих та інтелектуальних систем є ключовим напрямком розвитку корпоративних IT-рішень.

Список використаних джерел:

1. Global Digitalization Index (GDI) 2024 : White Paper / Huawei Technologies Co., Ltd. – [Б. м.], 2024. – Режим доступу: https://www-file.huawei.com/-/media/corp2020/gdi/pdf/gdi-2024-en.pdf (дата звернення: 29.05.2025).

2. Stallings W. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud / William Stallings. – Boston : Addison-Wesley Professional, 2016. – 560 p.

3. A survey of software-defined networking: Past, present, and future of programmable networks / B. A. A. Nunes, M. Mendonca, X. N. Nguyen et al. // IEEE Communications Surveys & Tutorials. – 2014. – Vol. 16, No. 4. – P. 1617–1634.

УДК 621.391

В.С. Багмет
Державний університет
«Київський авіаційний інститут», м. Київ

ОПТОВОЛОКОНОННИЙ КАНАЛ ЗВЯЗКУ ДЛЯ БПЛА В УМОВАХ ІНТЕНСИВНОГО ВИКОРИСТАННЯ РЕБ

На сьогоднішній день військові конфлікти демонструють важливу роль безпілотних літальних апаратів (БПЛА) для спостереження, розвідки, та інших завдань. Традиційні радіочастотні системи є вразливими до засобів радіоелектронної боротьби, що призводить до втрат сигналу, втрат БПЛА, та як наслідок невиконання завдань. В якості вирішення цієї проблеми пропонується використання волоконно оптичних систем (ВОС). На оптоволокно не впливають електромагнітні перешкоди, що робить неможливим глушіння за допомогою РЕБ чи перехоплення сигналу. Також ВОС дозволяє передавати великі обсяги даних, що забезпечує високу пропускну здатність, а також мініальну затримку. Мінімальна затримка є важливим фактором, оскільки дозволяє миттєво реагувати оператору на зміни в середовищі. Актуальністю роботи є створення надійної системи управління, нечутливої до РЕБ, з високою пропускною здатністю, мінімальною затримкою та неможливістю перехоплення сигналу.

Метою роботи є розробка БПЛА який керується через оптоволоконну лінію, що забезпечує захищену та стабільну передачі даних та відеосигналу в умовах широкого використання РЕБ; проаналізовано вразливості та обмеження управління через радіосигнал; обґрунтовано принципи будови та переваги застосування волоконно-оптичної системи; розроблено структурну схему волоконнно-оптичної системи управління БПЛА, до якої входить бортовий та наземний сегменти зі спеціальними оптичними модулями; обґрунтовано вибір одномодового оптичного волокна стандарту G.657.A , в якого низька чутливість до вигинів; Встановлено необхідні технічні характеристики оптичних модулів(підримка аналогового відеосигналу NTSC/PAL з оцифровкою на борту для передачі по оптоволокну, швидкість до 1 Мбіт/с); проведено експерементальне дослідження шляхом аналітичних розрахунків для оцінки ефективності та працездатності розробленої системи; Також розроблена архітектура передбачає використання модулів BiDi (BiDirectional), які забезпечують двосторонню передачу оптчного сиг-

налу по одному волокну на різних довжинах хвиль. Наземний медіаконвертер перетворює електричні сигнали в світловий імпульс в свою чергу бортовий медіаконвертер перетворює оптичний синал в електричний та подає цей сигнал контролеру польоту який в свою чергу подає команди на силову установку. В зворотному напрямку бортовий модуль отримує електричні сигнали від камери та контролера польту, оцифровує їх та перетворює в оптичний сигнал, Наземний сегмент отримуючи оптичний сигнал перетворює його в електричний (у випадку з аналоговим відеосигналом в аналоговий сигнал) та подає його на монітор. Для підтвердження працездатності системи було проведено компютерне моделювання та аналітичні розрахунки. Розрахунки показали що для довжини оптоволокна в 20 км необхідні модулі в яких рівень потужності не менше 11 дБ. Тому були обрані рішення від компанії Axisflying. Модуль Opticallink GBD для наземної станції управління та Opticallink SKY для встановлення на дроні. Данні модулі призначені для передачі даних по оптоволокну з використання технології BiDi.Також була розрахована затримка передачі сигналу по оптоволокну яка становить 0,098 мс. (або 0,000098 с) для 20 кілометрів. Зважаючи на те що людське око не сприймає затримку менше 10-20 мс. та те що затримка у більшості дронів з традиційним радіо зв’язком вища, затримку у 0,098 мс можна назвати мізерною.

Запропонований волоконно-оптичний канал зв’язку для БПЛА є ефективним рішенням для забезпечення стабільного та захищеного зв’язку в умовах інтенсивної роботи засобів радіоелектронної боротьби. Основними перевагами є нечутливість до електромагнітних завад, що робить неможливим його глушіння за допомогою РЕБ, а також стабільність передачі даних на великі відстані, що підтверджено розрахунками. Затосування технології BiDi та оптичного волокна G.657.A2 дозволяють досягти високої продуктивності каналу зв’язку. Хоч дана система має збільшену вагу та потребує плавності в управлінні, проте це компенсується невразливістю до РЕБ та хорошим зв'язком у місцях де радіосигнал не найкращої якості. Отже, дана система є перспективним рішенням для задань де є високий ризик для життя людини, де втрати керування або даних неприпустимі. Отримані результати можуть стати основою для подальшого розвитку волоконно-оптичного зв’язку для безпілотних платформ.

УДК 621.391

А.І. Битько
Державний університет
«Київський авіаційний інститут», м. Київ

ДОСЛІДЖЕННЯ НОВІТНІХ ВИКЛИКІВ ТА РОЛІ РАДІОЧАСТОТНОГО ВИЯВЛЕННЯ БПЛА

Стрімке поширення безпілотних літальних апаратів (БПЛА), що перетворилися з нішевої технології на повсюдний інструмент, створює безпрецедентні виклики для приватності, безпеки та контролю повітряного простору. Від незаконного спостереження до потенційних терористичних загроз, несанкціоноване використання дронів вимагає розробки ефективних засобів протидії. Традиційні системи виявлення (оптичні, акустичні, радарні) часто виявляються обмеженими через малі розміри БПЛА, їхню низьку акустичну сигнатуру та чутливість до погодних умов. У цьому контексті радіочастотні (РЧ) системи виявлення набувають критичного значення. Вони використовують пасивний моніторинг радіоспектру для аналізу сигналів керування, телеметрії та відеопередачі БПЛА, надаючи унікальну можливість не лише виявити дрон, а й ідентифікувати його за притаманною йому РЧ-сигнатурою. Це дає значно більше інформації, ніж просто факт присутності об'єкта, і є основою для подальших рішень щодо протидії.

Дослідження зосереджено на концептуальній розробці та програмному моделюванні системи радіочастотного виявлення БПЛА, що базується на принципах програмно-визначуваного радіо (SDR) та передових методах машинного навчання. Центральним елементом архітектури є програмний комплекс, здатний взаємодіяти з SDR для потокового прийому та оцифровки радіочастотних сигналів.

Алгоритми виявлення функціонують шляхом постійного сканування визначених РЧ-діапазонів (2.4 ГГц, 5.8 ГГц, 900 МГц, 433 МГц), аналізу спектральної щільності потужності за допомогою швидкого перетворення Фур'є (FFT) та застосування адаптивних порогових методів для виявлення піків активності, що відповідають сигналам БПЛА.

Ключовою особливістю системи є ідентифікація типу БПЛА за його унікальною РЧ-сигнатурою. Для цього з виявлених сигналів вилучається комплекс специфічних ознак, які відображають апаратні не ідеальності передавача (наприклад, точний частотний офсет, фазовий шум, характеристики модуляції та перехідні процеси сигналу). Ці

ознаки подаються на вхід згорткової нейронної мережі (CNN), навченої на великому наборі синтетичних РЧ-даних, що імітують випромінювання різних моделей БПЛА з урахуванням шуму та перешкод. Моделювання показало високу ефективність розробленого підходу: ймовірність виявлення (PD) перевищує 95% при відношенні сигнал/шум (SNR) вище 10 дБ, демонструючи надійність навіть у зашумленому середовищі. Більше того, точність ідентифікації сягає 89.2% на тестовій вибірці з 5 класів БПЛА, що свідчить про здатність алгоритму розрізняти різні моделі дронів за їхніми "радіовідбитками". Окрім виявлення та ідентифікації, в моделі було продемонстровано можливість локалізації БПЛА з середньою похибкою близько 12 метрів на дистанції до 800 метрів, використовуючи метод визначення кута приходу сигналу (AoA) з віртуальним багатоантенним масивом. Ці результати підтверджують, що запропонована архітектура та алгоритми забезпечують надійний та інформативний моніторинг повітряного простору.

Результати проведеного моделювання переконливо демонструють, що розроблена концепція системи радіочастотного виявлення БПЛА є життєздатною та високоперспективною. Її здатність пасивно виявляти та ідентифікувати дрони за унікальними РЧ-сигнатурами робить її цінним інструментом для широкого спектру застосувань – від захисту критичної інфраструктури до моніторингу громадського простору. Хоча моделювання дозволило глибоко дослідити поведінку системи, подальша її розробка вимагатиме переходу до реальних випробувань та розширення бази даних РЧ-сигнатур, зібраних від реальних БПЛА в різноманітних умовах. Майбутні напрямки досліджень включають інтеграцію з іншими сенсорними технологіями для створення гібридних систем, розробку адаптивних алгоритмів для роботи в динамічному радіоефірі, оптимізацію для роботи в реальному часі та підвищення стійкості до радіоелектронних завад. Впровадження таких комплексних рішень забезпечить суттєве підвищення рівня безпеки та ефективний контроль за повітряним простором в умовах зростаючого використання БПЛА.

UDC 654.924.5:728:004 (076.2)

I.V. Bohush
State University
"Kyiv Aviation Institute", Kyiv

DESIGN OF A WIRELESS FIRE AND SECURITY ALARM SYSTEM FOR SMART HOME ENVIRONMENTS

The increasing adoption of smart home technologies, driven by the rapid development of the Internet of Things (IoT), microcontrollers, and automation platforms, presents new challenges for ensuring residential safety. Traditional fire and security alarm systems often fail to meet the requirements of modern intelligent homes in terms of integration, remote accessibility, scalability, and adaptability to dynamic living environments. Moreover, the growing demand for user-friendly, cost-effective, and standards-compliant safety solutions motivates the exploration of novel approaches based on open technologies and flexible microcontroller architectures. This research addresses these challenges by proposing a compact and modular wireless fire and intrusion alarm system designed for use in smart residential spaces.

The core objective of this bachelor thesis is the development of a fully functional, scalable, and economically justified fire and security alarm system for a two-storey smart house. The proposed system is built around the ESP32 microcontroller, known for its low power consumption, wireless communication capabilities (Wi-Fi/Bluetooth), and rich GPIO interface for sensor integration. The project includes an in-depth analysis of modern smart building subsystems, types of fire and intrusion detectors, response algorithms, and compliance with international safety standards. A comprehensive architectural design was created, encompassing the layout of a typical residential house, zoning strategies, optimal sensor placement, and logical response models for different threat scenarios such as fire, gas leakage, unauthorized entry, or glass breakage.

At the technical level, the system integrates various types of sensors—optical smoke detectors, gas and temperature sensors, PIR motion detectors, magnetic contact switches, and sound/vibration-based glass break detectors—organized into functional zones and controlled via centralized logic executed by the ESP32 platform. All events are processed through rule-based algorithms that include multi-factor validation, temporal correlation, and escalation models. The system reacts dynamically to

detected threats by activating alarms, sending push/email alerts, unlocking emergency exits, turning on lights, or shutting down electrical appliances. Wireless communication is implemented using the MQTT protocol, enabling real-time data transmission to cloud dashboards and mobile applications. The firmware is developed using MicroPython and integrates seamlessly with Home Assistant for visualization and control.

A detailed cost analysis confirms the economic viability of the solution, demonstrating that the proposed design can reduce system cost by up to 40% compared to commercial proprietary solutions, without sacrificing reliability or compliance with standards like EN 54, EN 50131, and local building codes. The implementation also includes considerations for cybersecurity, power backup, environmental impact, and ergonomic human-machine interaction. A risk assessment highlights potential failure points during installation and use, with corresponding mitigation strategies such as fallback logic, redundant sensors, and secure communication protocols.

In conclusion, the developed wireless alarm system prototype demonstrates a successful balance between innovation, affordability, and technical excellence. It offers homeowners enhanced safety, real-time awareness, and integration with broader smart home systems while remaining adaptable to future upgrades and device extensions. The proposed solution is especially suitable for private residences and small-scale deployments, providing a practical foundation for future commercial or open-source smart safety systems. The results of the project validate the effectiveness of using ESP32-based architectures in life-critical applications and illustrate the potential for democratizing smart home security through open, scalable technologies.

УДК 004.415.5:004.9:621.396.96

Р.М. Гамрецький[1], В.О. Гнатюк[1,2]
[1]Державний університет «Київський авіаційний інститут», м. Київ
[2]ДержНДІ технологій кібербезпеки, м. Київ

ОСОБЛИВОСТІ ОЦІНКИ ЯКОСТІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ЯДРА 5G

Розвиток технологій мобільного зв'язку п'ятого покоління (5G) висуває підвищені вимоги до якості програмного забезпечення (ПЗ), особливо в частині ядра мережі (5G Core). Ядро 5G складається з низки мікросервісів, що реалізують функціональність таких логічних елементів, як AMF, SMF, UPF, PCF та інших. Надійність і продуктивність цих компонентів безпосередньо впливають на забезпечення критичних сервісів: eMBB, URLLC, mMTC. Тому питання оцінки якості ПЗ ядра 5G є надзвичайно актуальним.

Метою цієї роботи є аналіз сучасних моделей оцінки якості ПЗ в контексті ядра 5G, виявлення їх переваг і обмежень, а також визначення специфічних вимог до оцінки якості ПЗ у мікросервісній архітектурі 5G Core.

Стандартизовані моделі, як-от ISO/IEC 25010, передбачають оцінку таких характеристик, як функціональна придатність, надійність, ефективність, безпека, переносимість, сумісність тощо. Однак вони не враховують специфіку динамічного масштабування, оркестрації, хмарної розгортки, характерних для 5G Core. Існують також дослідження, присвячені оцінці якості в телеком-домені, зокрема за допомогою метрик QoS (Quality of Service) і QoE (Quality of Experience), але вони, як правило, фокусуються на рівні користувацького досвіду, а не на якості окремих компонентів ядра [1], [2].

ПЗ 5G Core має мікросервісну архітектуру, розгортається у контейнерах (наприклад, у середовищах Kubernetes), що дозволяє масштабування залежно від навантаження. Це створює нові виклики в оцінці якості, зокрема:

- Стабільність при оновленнях (rolling updates);
- Затримки та їх варіації (jitter) між компонентами;
- Масштабованість компонентів SMF/UPF під навантаженням;
- Fault-tolerance у разі збою одного з мікросервісів;
- Інтерфейсна сумісність між N-функціями (N1, N2, N4 тощо).

Також варто враховувати специфіку обробки PDU-сесій, маршрутизації пакетів через UPF, взаємодії з NF-репозиторієм, що створює підґрунтя для розширення традиційних метрик.

Для моделювання та оцінки поведінки компонентів ядра 5G було використано open-source платформу Free5GC у поєднанні з емулятором терміналів UERANSIM. Проведено тестування стабільності SMF/UPF під умовами підвищеного навантаження (1000+ одночасних PDU-сесій). Застосовано метрики:

- Availability – частка часу безвідмовної роботи;
- Response time – середній час відповіді SMF;
- Resource consumption – при масштабуванні;
- Packet loss – рівень втрати пакетів між UPF і зовнішніми DN.

Окрім класичних метрик, у дослідженні застосовано підхід до динамічного профілювання навантаження, що дозволяє відстежувати деградацію продуктивності на ранніх етапах. Для підвищення точності оцінювання якості впроваджено механізм логування ключових подій SMF і UPF з подальшим аналізом логів для виявлення аномалій у поведінці сервісів. Це дозволило ідентифікувати ситуації, в яких мікросервіси тимчасово втрачали стабільність або надмірно використовували ресурси.

Оцінка якості ПЗ ядра 5G вимагає поєднання традиційних моделей якості з новими підходами, орієнтованими на мікросервісність і хмарну архітектуру. Результати дослідження свідчать про потребу створення гібридної моделі оцінки якості, що враховує характеристики ISO/IEC 25010 і метрики реального навантаження в 5G Core. У подальшому планується розробка методу оцінки якості ПЗ ядра 5G з урахуванням метрик, притаманних інформаційно-комунікаційним системам.

Список літератури

1. Afolabi, I., Taleb, T., Samdanis, K., Ksentini, A., & Flinck, H. (2018). Network slicing and softwarization: A survey on principles, enabling technologies, and solutions. IEEE Communications Surveys & Tutorials, 20(3), 2429–2453. DOI: 10.1109/COMST.2018.2815638

2. G. Lando, L. A. F. Schierholt, M. P. Milesi and J. A. Wickboldt, "Evaluating the performance of open source software implementations of the 5G network core," NOMS 2023-2023 IEEE/IFIP Network Operations and Management Symposium, Miami, FL, USA, 2023, pp. 1-7, doi: 10.1109/NOMS56928.2023.10154399

УДК 621.396.4 (043.2)

І.С. Гируцький, Б.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОД НАЛАШТУВАННЯ VPN-ТУНЕЛІВ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

Захист даних у сучасних мережах є критичним елементом для забезпечення конфіденційності та стабільності як корпоративних, так і приватних комп'ютерних мереж. У сучасному світі постійне зростання кількості даних і кількості кіберзагроз вимагають розробки нових методів захисту, а також застосування високотехнологічних рішень для безпечного передавання інформації. Вибір правильного рішення для створення безпечного зв'язку є ключовим етапом у процесі побудови приватних мереж, де використання VPN-технологій відіграє одну з основних ролей.

У роботі розглянуто методи налаштування VPN-тунелів на базі обладнання MikroTik, що є ефективним і економічним вибором для малих та середніх підприємств. MikroTik надає потужні інструменти для організації безпечних з’єднань, що дозволяє організаціям з різними вимогами до безпеки створювати надійні канали зв'язку. Важливість цих рішень особливо відчутна в умовах постійно зростаючого попиту на безпеку в цифрових мережах.

У роботі здійснено всебічний аналіз принципів побудови приватних мереж, зокрема технологій передавання даних, методів шифрування та автентифікації, а також класів VPN та їх можливостей для забезпечення безпеки зв'язку. Особливу увагу приділено аналізу технологій захисту трафіку в мережах, таких як брандмауери, системи виявлення та запобігання вторгненням, а також засобам моніторингу й аудиту для своєчасного виявлення загроз. Дослідження показало, що для створення високоякісної захищеної інфраструктури важливо комплексно підходити до вибору інструментів захисту, щоб забезпечити високий рівень безпеки в умовах сучасних кіберзагроз.

Проаналізовано обладнання MikroTik, яке є економічно вигідним та ефективним рішенням для малих та середніх підприємств. MikroTik підтримує популярні VPN-протоколи, зокрема IPSec, WireGuard та OpenVPN, що дозволяє налаштовувати безпечні VPN-тунелі для організацій з різними вимогами. Порівняння з іншими виробниками мере-

жевого обладнання, такими як Cisco та Fortinet, показало, що MikroTik є оптимальним вибором для більшості користувачів завдяки доступності, гнучкості налаштувань і підтримці новітніх технологій, при цьому він є значно більш економічним у порівнянні з конкурентами, що робить його чудовим вибором для малих і середніх компаній з обмеженим бюджетом.

У роботі були розглянуті конкретні етапи налаштування VPN-тунелів на платформі MikroTik, з особливим акцентом на безпеку з'єднання та використання сучасних методів шифрування, зокрема використання алгоритмів AES для шифрування даних і протоколу IKEv2 для аутентифікації. Під час налаштування також розглядалися питання, пов'язані з керуванням ключами та управлінням політиками доступу, що дозволяє більш ефективно контролювати мережеві з'єднання. Результати тестування показали, що налаштування VPN на MikroTik забезпечує стабільність і високу швидкість з'єднання, що є важливим для підприємств з обмеженими фінансовими ресурсами. Платформа також показала високу продуктивність навіть за великих обсягів трафіку.

З проведеного дослідження можна зробити висновок, що обладнання MikroTik є оптимальним і економічно обґрунтованим вибором для малих і середніх підприємств, які потребують надійних і безпечних VPN-з'єднань. Продуктивність, доступність і простота налаштування роблять MikroTik ідеальним рішенням для підприємств, які шукають економічні варіанти без шкоди для якості і безпеки мережі. У той же час для великих організацій з високими вимогами до безпеки та масштабованості можуть бути доцільними більш потужні та масштабовані рішення від таких виробників, як Cisco або Juniper. Однак, завдяки доступності і простоті налаштування, MikroTik є відмінним вибором для компаній, які не потребують надскладних рішень.

Проте, завдяки розвитку технологій і інтеграції нових протоколів, таких як WireGuard, MikroTik продовжує залишатися конкурентоспроможним вибором на ринку для малих і середніх підприємств, забезпечуючи оптимальне співвідношення ціни та якості. Інтеграція нових протоколів дозволяє підвищити ефективність використання ресурсів, покращити швидкість з'єднань і забезпечити ще більш високий рівень безпеки, що є важливим для розвитку сучасних корпоративних мереж.

УДК 004.75:004.032.26 (043.2)

Я.О. Горда, В.М. Чуприн
Державний університет
«Київський авіаційний інститут», м. Київ

ВІРТУАЛЬНА СЕРВЕРНА ІНФРАСТРУКТУРА НА БАЗІ ТЕХНОЛОГІЇ HYPER-V

Вступ. В епоху цифрової трансформації та стрімкого зростання обсягів даних, вимоги до серверної інфраструктури невпинно зростають. Організації потребують гнучких, масштабованих, надійних та економічно ефективних рішень для розміщення своїх інформаційних систем та сервісів. Технології віртуалізації серверів відіграють ключову роль у відповіді на ці виклики, дозволяючи оптимізувати використання наявних апаратних ресурсів, підвищити рівень автоматизації та керованості, а також забезпечити безперервність бізнес-процесів. Серед провідних платформ віртуалізації особливе місце займає технологія Hyper-V від корпорації Microsoft, яка інтегрована в операційні системи Windows Server та пропонує потужний інструментарій для створення та управління віртуальними машинами. Актуальність даної теми зумовлена необхідністю дослідження сучасних можливостей Hyper-V, переваг її використання для побудови віртуальних серверних інфраструктур та аналізу практичних аспектів її впровадження в контексті сучасних тенденцій розвитку інформаційних технологій, зокрема гібридних хмарних сценаріїв та програмно-визначуваних датацентрів.

Основна частина. Технологія Hyper-V, розроблена корпорацією Microsoft, являє собою систему апаратної віртуалізації, що дозволяє створювати та керувати віртуальними машинами (ВМ) на фізичному сервері. В основі Hyper-V лежить гіпервізор типу 1 (bare-metal), який встановлюється безпосередньо на апаратне забезпечення хоста, що забезпечує високу продуктивність та безпеку. Архітектура Hyper-V включає батьківський розділ (parent partition), який має прямий доступ до апаратних ресурсів та керує дочірніми розділами (child partitions), де функціонують віртуальні машини з гостьовими операційними системами. Взаємодія між гостьовими ОС та апаратними ресурсами оптимізується за допомогою служб інтеграції (Integration Services). Мережева взаємодія ВМ реалізується через віртуальні комутатори (virtual switches), які підтримують різні конфігурації, включаючи ізольовані,

приватні та зовнішні мережі, а також розширені функції, такі як віртуалізація мережевих функцій (NFV) та програмно-визначувані мережі (SDN). Для зберігання даних віртуальних машин використовуються файли віртуальних жорстких дисків у форматах VHDX та VHD, причому VHDX підтримує більший об'єм (до 64 ТБ) та має покращену стійкість до пошкоджень.

Функціональні можливості Hyper-V надають широкий спектр інструментів для побудови відмовостійкої та гнучкої серверної інфраструктури. Динамічна міграція (Live Migration) дозволяє переміщувати працюючі віртуальні машини між фізичними хостами кластера без простою сервісів, що є критичним для забезпечення безперервності роботи. Міграція сховища (Storage Migration) дає можливість переносити файли віртуальних дисків на інші сховища також без зупинки ВМ. Для завдань аварійного відновлення призначена функція Hyper-V Replica, яка забезпечує асинхронну реплікацію віртуальних машин на резервний сайт. Висока доступність ВМ досягається шляхом використання кластеризації відмовостійкості (Failover Clustering) на базі Windows Server, що дозволяє автоматично перезапускати ВМ на іншому вузлі кластера у випадку збою основного хоста. Ефективне використання оперативної пам'яті забезпечується технологією динамічної пам'яті (Dynamic Memory), яка дозволяє гнучко розподіляти та перерозподіляти пам'ять між ВМ відповідно до їх поточних потреб.

Сучасні версії Hyper-V, зокрема в Windows Server 2022 та оновленнях, що очікуються в Windows Server 2025, продовжують розвивати безпекові аспекти. Екрановані віртуальні машини (Shielded VMs) захищають ВМ від несанкціонованого доступу з боку адміністраторів хоста або шкідливого програмного забезпечення на рівні інфраструктури. Ця технологія використовує Host Guardian Service для забезпечення довіреного запуску та шифрування даних ВМ. Також важливим є підтримка Secure Boot для ВМ та віртуального модуля TPM (vTPM).

Однією з ключових переваг використання Hyper-V є її тісна інтеграція з екосистемою продуктів Microsoft, включаючи System Center Virtual Machine Manager (SCVMM) для централізованого управління, Windows Admin Center для спрощеного адміністрування та PowerShell для автоматизації завдань. Це дозволяє створювати комплексні рішення для управління IT-інфраструктурою. Крім того, Hyper-V забезпечує ефективне використання апаратних ресурсів, що призводить до зни-

ження капітальних витрат на обладнання та операційних витрат на електроенергію та охолодження.

Планування та впровадження віртуальної інфраструктури на базі Hyper-V вимагає ретельного аналізу вимог до продуктивності, доступності та безпеки. Необхідно правильно розрахувати ресурси хост-серверів (процесор, пам'ять, дискова підсистема, мережеві адаптери), спроектувати мережеву архітектуру з урахуванням різних типів трафіку (управління, міграція, доступ до ВМ, зберігання даних), а також розробити стратегії резервного копіювання та аварійного відновлення. Важливим аспектом є моніторинг продуктивності інфраструктури за допомогою вбудованих засобів Windows Server (Performance Monitor, Event Viewer) та спеціалізованих інструментів для своєчасного виявлення та усунення вузьких місць.

Сучасні тенденції розвитку Hyper-V спрямовані на поглиблення інтеграції з хмарними сервісами Azure. Azure Arc дозволяє управляти серверами Hyper-V та віртуальними машинами з єдиної консолі Azure, незалежно від їх фізичного розташування. Azure Stack HCI є гіперконвергентним рішенням, яке використовує Hyper-V та Storage Spaces Direct для створення локальної інфраструктури, тісно інтегрованої з Azure, надаючи хмарні сервіси в локальному дата-центрі. Це відкриває шлях до побудови гібридних сценаріїв, де локальні ресурси можуть гнучко доповнюватися хмарними потужностями. Також Hyper-V активно використовується для підтримки контейнерних технологій, таких як Windows Containers та Docker, забезпечуючи ізольоване середовище для запуску контейнеризованих додатків. Очікується, що майбутні версії Hyper-V, як частина Windows Server 2025, принесуть подальші покращення в продуктивності, безпеці та можливостях управління, зокрема оптимізації для файлової системи ReFS та розширені функції для роботи з великими навантаженнями.

Висновок. Віртуальна серверна інфраструктура, побудована на основі технології Hyper-V, є стратегічно важливим рішенням для сучасних підприємств, що прагнуть оптимізувати свої IT-ресурси, підвищити операційну ефективність та забезпечити високий рівень надійності та доступності критичних бізнес-сервісів. Розглянуті архітектурні особливості, функціональні можливості, зокрема динамічна міграція, кластеризація, реплікація та засоби безпеки, демонструють зрілість та потужність платформи Hyper-V.

Впровадження Hyper-V дозволяє значно скоротити капітальні та операційні витрати за рахунок консолідації серверів, спростити процеси адміністрування та розгортання нових сервісів, а також забезпечити гнучке масштабування ресурсів відповідно до поточних потреб. Інтеграція з іншими продуктами Microsoft та хмарними сервісами Azure, такими як Azure Arc та Azure Stack HCI, розширює можливості Hyper-V, дозволяючи створювати сучасні гібридні інфраструктури та використовувати переваги хмарних технологій. Постійний розвиток функціоналу Hyper-V, зокрема в контексті підвищення продуктивності, безпеки та підтримки новітніх технологій, таких як контейнеризація, підтверджує її актуальність та перспективність як основи для побудови надійних, масштабованих та економічно ефективних віртуальних серверних інфраструктур. Таким чином, технологія Hyper-V надає комплексний інструментарій для вирішення ключових завдань, що стоять перед IT-відділами в умовах динамічного бізнес-середовища.

Список використаних джерел

1. Microsoft. (2024). What's new in Windows Server 2025 Hyper-V. Microsoft Learn. (Адаптовано з огляду нових функцій та можливостей, що обговорюються для Windows Server 2025).

2. Smith, J. (2023). Advanced Hyper-V Configuration and Management for Enterprise Environments. TechPress Publishing.

3. Kravchenko, O. (2024). Сучасні підходи до забезпечення безпеки віртуалізованих інфраструктур на базі Hyper-V. Безпека інформації: науково-практичний журнал, 2(1), 45-52.

4. The Business Research Company. (2024). Server Virtualization Software Global Market Report 2024.

5. Roth, H. (2024). Open to options: How to build your modern virtualization strategy. Red Hat Blog.

УДК 004.725.3 (043.2)

І.Ю. Гордієнко, В.М. Чуприн
Державний університет
«Київський авіаційний інститут», м. Київ

ВІРТУАЛЬНА ПРИВАТНА МЕРЕЖА ПАКЕТНОЇ ПЕРЕДАЧІ ДАНИХ НА БАЗІ ОБЛАДНАННЯ JUNIPER

Вступ. В епоху цифрової трансформації та стрімкого зростання обсягів передачі даних, віртуальні приватні мережі (VPN) відіграють ключову роль у забезпеченні безпечного, надійного та ефективного з'єднання між територіально розподіленими корпоративними ресурсами, хмарними середовищами та кінцевими користувачами. Обладнання компанії Juniper Networks, відомої своїми інноваційними рішеннями в галузі мережевих технологій, є поширеною платформою для побудови VPN різного масштабу та складності. Сучасні VPN-рішення на базі Juniper характеризуються високою продуктивністю, гнучкістю конфігурації та підтримкою передових протоколів пакетної передачі даних. Актуальність теми зумовлена постійною еволюцією мережевих загроз, зростаючими вимогами до пропускної здатності та необхідністю інтеграції VPN з новітніми парадигмами, такими як програмно-визначувані мережі (SDN) та функції мережевої віртуалізації (NFV). Метою даних тез є аналіз ключових аспектів функціонування віртуальних приватних мереж пакетної передачі даних на базі обладнання Juniper, включаючи архітектурні особливості, технології забезпечення безпеки та новітні тенденції розвитку.

Основна частина. Обладнання Juniper Networks надає широкий спектр можливостей для створення VPN, що відповідають різноманітним вимогам щодо продуктивності, безпеки та функціональності. Однією з ключових технологій є MPLS, яка дозволяє створювати VPN рівня 2 (L2VPN) та рівня 3 (L3VPN). MPLS L3VPN, зокрема, забезпечують масштабовану та безпечну сегментацію IP-мереж, ізолюючи трафік різних клієнтів або підрозділів в межах єдиної фізичної інфраструктури провайдера. Маршрутизатори серії MX від Juniper є потужною платформою для реалізації MPLS VPN, підтримуючи високу щільність портів та розширені функції маршрутизації.

Для забезпечення конфіденційності та цілісності даних, що передаються через публічні мережі, широко використовується набір протоколів IPsec. Пристрої безпеки Juniper SRX Series інтегрують функції міжмережевого екранування нового покоління (NGFW) з потужними можливостями IPsec

VPN, дозволяючи створювати як site-to-site VPN, так і VPN для віддаленого доступу. Сучасні реалізації IPsec на обладнанні Juniper підтримують новітні алгоритми шифрування та автентифікації, забезпечуючи надійний захист від несанкціонованого доступу та перехоплення даних.

З розвитком технологій віртуалізації дата-центрів та хмарних обчислень набула популярності технологія EVPN-VXLAN. EVPN (Ethernet VPN) у поєднанні з VXLAN (Virtual Extensible LAN) дозволяє створювати гнучкі та масштабовані мережі рівня 2 поверх існуючої IP-інфраструктури. Обладнання Juniper, зокрема комутатори серії QFX та маршрутизатори MX, підтримує EVPN-VXLAN, забезпечуючи ефективну мобільність віртуальних машин та сегментацію трафіку в багатокористувацьких середовищах. Як зазначається в документації до Contrail Networking, починаючи з версії 21.4, впроваджено підтримку Graceful Restart для маршрутів EVPN Type 2, що підвищує стійкість мережі.

Рішення Juniper Contrail SD-WAN є відповіддю на зростаючі потреби підприємств у гнучкому та оптимізованому управлінні глобальними мережами. Воно дозволяє централізовано керувати політиками маршрутизації та безпеки, автоматично обирати оптимальні шляхи для передачі трафіку додатків та спрощувати розгортання нових філій. Contrail Networking, як основа для SD-WAN, забезпечує розширені можливості аналітики та автоматизації. Відгуки користувачів за травень 2025 року підкреслюють масштабованість, спрощене управління та надійну безпеку як ключові переваги рішень Juniper SD-WAN, хоча вказують і на виклики, пов'язані з розгортанням в локальних середовищах та інтеграцією з хмарними сервісами Mist.

Питання безпеки є наріжним каменем при побудові будь-якої VPN. У 2024-2025 роках було виявлено низку вразливостей в продуктах Juniper, що підкреслює важливість своєчасного оновлення програмного забезпечення та проактивного моніторингу безпеки. Наприклад, вразливість CVE-2025-21590 в Junos OS, як повідомлялося, експлуатувалася для отримання несанкціонованого доступу до маршрутизаторів. Компанія Juniper оперативно випускає оновлення безпеки для усунення подібних загроз. Крім того, Juniper Networks активно працює над майбутніми викликами безпеки, анонсуючи плани щодо інтеграції квантово-безпечних криптографічних алгоритмів у свої рішення до 2025 року, що є важливим кроком на шляху до захисту даних від загроз, пов'язаних з розвитком квантових обчислень.

Автоматизація та інтелектуальне управління мережею стають дедалі важливішими. Juniper активно впроваджує технології AIOps (AI for IT Operations) для прогнозування проблем, автоматизації рутинних завдань та оптимізації продуктивності мережі. Це дозволяє знизити операційні витрати та підвищити надійність VPN-сервісів. Здатність аналізувати великі обсяги телеметричних даних та приймати обґрунтовані рішення в автоматичному режимі є ключовою перевагою сучасних мережевих платформ.

Висновок. Віртуальні приватні мережі пакетної передачі даних на базі обладнання Juniper Networks є потужними та гнучкими рішеннями, що задовольняють сучасні вимоги бізнесу до безпеки, продуктивності та масштабованості. Використання передових технологій, таких як MPLS, IPsec, EVPN-VXLAN, та інноваційних підходів, включаючи SD-WAN, AIOps та підготовку до квантово-безпечної криптографії, дозволяє компанії Juniper утримувати лідируючі позиції на ринку. Водночас, постійна еволюція кіберзагроз вимагає безперервного вдосконалення механізмів безпеки, своєчасного реагування на виявлені вразливості та проактивного підходу до захисту мережевої інфраструктури. Подальший розвиток VPN-рішень Juniper, ймовірно, буде зосереджений на глибшій інтеграції штучного інтелекту, розширенні можливостей автоматизації та забезпеченні ще вищого рівня безпеки пакетної передачі даних в умовах гібридних та багатохмарних середовищ.

Список використаних джерел

1. Juniper Networks. (2024). Contrail Networking Release Notes, Release 21.4.L4.1. Retrieved from https://www.juniper.net/documentation/us/en/software/contrail-networking21/release-notes/contrail-release-notes-21.4-l4.1/contrail-release-notes-21.4-l4.1.pdf

2. PeerSpot. (2025, May). Juniper Contrail SD-WAN Reviews, Ratings, and Features. Retrieved from https://www.peerspot.com/products/juniper-contrail-sd-wan-reviews

3. Abrams, L. (2025, March 13). Juniper patches bug that let Chinese cyberspies backdoor routers. Bleeping Computer. Retrieved from https://www.bleepingcomputer.com/news/security/juniper-patches-bug-that-let-chinese-cyberspies-backdoor-routers-since-mid-2024/

УДК 004.738.5:004.774

Ю.Р. Гриценко, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ВІДЕОКОНФЕРЕНЦІЇ НА БАЗІ VOIP

У сучасних умовах стрімкого розвитку цифрових технологій та зростаючої глобалізації бізнес-процесів, ефективні засоби комунікації відіграють вирішальну роль у забезпеченні конкурентоспроможності та продуктивності організацій. Системи відеоконференцзв'язку (ВКЗ), що базуються на технологіях Voice over IP (VoIP), стали невід'ємною частиною сучасної корпоративної інфраструктури. Вони пропонують неперевершену гнучкість, високу масштабованість та значну економічну вигоду порівняно з традиційними системами зв'язку. Актуальність даного дослідження зумовлена постійною необхідністю розробки та вдосконалення таких систем, які б відповідали динамічним вимогам щодо якості зв'язку, надійності та безпеки в умовах розподілених команд та поширеної дистанційної роботи. Метою даної роботи є комплексне проектування та всебічна оцінка ефективності функціонування системи відеоконференцзв'язку, призначеної для інтеграції в корпоративну мережу на основі сучасних VoIP-технологій.

Перший розділ роботи присвячений детальному викладу теоретичних основ VoIP-технологій. У ньому розглядається історія їх еволюції, починаючи від перших експериментів до становлення як домінуючого стандарту передачі голосових та мультимедійних даних через IP-мережі. Особлива увага приділяється ключовим принципам функціонування VoIP, включаючи оцифрування та стиснення голосу, пакетну передачу даних та механізми маршрутизації [1]. Окремо аналізується архітектура сучасних систем відеоконференцій, їхня класифікація за типами (наприклад, апаратні, програмні, хмарні рішення), а також докладно описуються основні компоненти, такі як термінали, шлюзи, сервери конференцій та системи управління, що є фундаментальними для розуміння побудови та функціонування подібних рішень.

Другий розділ зосереджений на глибокому аналізі основних комунікаційних протоколів, що регулюють роботу VoIP-відеоконференцій. Детально досліджуються Session Initiation Protocol (SIP), H.323 та Real-time Transport Protocol (RTP), які є основою для

встановлення, управління та передачі мультимедійних потоків. Проводиться їхнє порівняння з точки зору архітектури, механізмів встановлення сесій, можливостей розширення та забезпечення якісної передачі відео та голосу, а також стабільності з'єднання в умовах різного навантаження [2]. Особлива увага приділяється розгляду ролі програмних АТС, зокрема Asterisk, як універсальної та гнучкої платформи для побудови кастомізованих комунікаційних рішень, що дозволяє інтегрувати різні протоколи та сервіси.

Ключовим аспектом даної роботи є практичне дослідження ефективності розробленої або запропонованої системи відеоконференцзв'язку. У третьому розділі детально описано процедуру та методологію тестування системи відеоконференцій, яка була реалізована на базі інтеграції програмної АТС Asterisk та відкритої платформи Jitsi. Визначено та обґрунтовано основні метрики якості послуг (Quality of Service – QoS), що використовувалися для об'єктивної оцінки якості зв'язку, включаючи пропускну здатність мережі, затримки передачі даних (latency), варіації затримок (jitter) та рівень втрати пакетів [3]. Отримані результати експериментальних досліджень підтверджують високу продуктивність та стабільність розробленої системи, демонструючи її придатність для використання в реальних умовах експлуатації та здатність забезпечувати якісний відеоконференцзв'язок.

Підсумовуючи, запропонована та досліджена система відеоконференції на базі VoIP є високоефективним інструментом для оптимізації корпоративних комунікацій, сприяючи підвищенню продуктивності та зниженню витрат. Результати проведеного дослідження надають цінні емпіричні дані та теоретичні висновки, які можуть бути використані для подальшого вдосконалення подібних систем, розробки нових функціональних можливостей, а також для формування практичних рекомендацій щодо їх ефективного впровадження та адміністрування в існуючих мережевих інфраструктурах

Список використаних джерел:

1. Davidson, J., & Peters, J. (2018). *Voice over IP Fundamentals*. Cisco Press.
2. Zar, S. (2019). *VoIP Protocols for Internet Telephony*. Artech House.
3. Kurose, J. F., & Ross, K. W. (2021). *Computer Networking: A Top-Down Approach*. Pearson.

УДК 004.738.5.056 (043.2)

І.І. Гуменний, А.О. Осіпчук
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА ПОЛІТИК БЕЗПЕКИ ТА ЇХ ВПРОВАДЖЕННЯ В КОРПОРАТИВНІЙ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ CISCO

Вступ. У контексті стрімкої цифровізації сучасного бізнесу, забезпечення кіберстійкості корпоративних мереж набуває статусу критичного імперативу. Зростаюча кількість та витонченість кіберзагроз зумовлюють нагальну потребу в розробці та імплементації комплексних, науково обґрунтованих політик інформаційної безпеки. Провідна роль у формуванні захищених мережевих інфраструктур належить обладнанню та технологічним рішенням компанії Cisco Systems, функціональні можливості якого дозволяють реалізовувати глибоко ешелоновані системи захисту. Ефективність таких систем безпосередньо корелює з якістю розроблених політик безпеки та їх адекватною технічною реалізацією. Дана робота присвячена дослідженню методологічних аспектів розробки та практичного впровадження політик безпеки в корпоративних мережах, що функціонують на базі обладнання Cisco, з акцентом на побудові моделі захищеної мережі та демонстрації застосування специфічних технологій Cisco для забезпечення інформаційної цілісності та конфіденційності.

Постановка завдання дослідження. Незважаючи на значний обсяг досліджень у сфері інформаційної безпеки, завдання ефективного впровадження політик у складних корпоративних мережах, особливо тих, що інтенсивно використовують обладнання Cisco, залишається актуальним та потребує подальшого наукового опрацювання. Ключові проблеми включають необхідність адаптації загальних принципів безпеки до специфіки конкретних апаратних платформ, оптимального використання багатогранного інструментарію безпеки, інтегрованого в операційні системи Cisco (IOS, IOS XE, ASA OS, NX-OS), та забезпечення узгодженості політик на всіх рівнях мережевої ієрархії – від доступу до ядра та периметра. У зв'язку з цим, основними завданнями дослідження є: обґрунтування багаторівневої архітектурної моделі корпоративної мережі на основі рішень Cisco; систематизація ключових політик безпеки, що охоплюють сегментацію, контроль доступу, захист периметра, безпеку віддалених підключень та автентифікацію;

демонстрація специфічних технологій та механізмів Cisco, які слугують інструментами для їх практичної реалізації; а також аналіз передових практик конфігурування обладнання Cisco для досягнення відповідності встановленим політикам та організації ефективного моніторингу стану безпеки.

Висвітлення проблеми дослідження. Для забезпечення ефективного впровадження політик безпеки пропонується модель корпоративної мережі, що використовує багаторівневу архітектуру, побудовану на обладнанні Cisco. Рівень доступу, реалізований на комутаторах Cisco Catalyst (зокрема, серій 2960-X, 9200, 9300), забезпечує підключення кінцевих точок та початкове застосування політик безпеки портів, включаючи механізми DHCP snooping, Dynamic ARP Inspection (DAI), IP Source Guard, та автентифікацію за стандартом 802.1X з інтеграцією із системою управління ідентифікацією Cisco Identity Services Engine (ISE). Рівень розподілу, на базі потужних комутаторів Cisco Catalyst (наприклад, серії 9500), агрегує трафік, здійснює маршрутизацію між віртуальними локальними мережами (VLAN) та слугує важливим вузлом для застосування списків контролю доступу (ACL). Ядро мережі, побудоване на високопродуктивних комутаторах Cisco Nexus або Catalyst вищих серій, забезпечує швидкісну комутацію. Периметр мережі, що включає маршрутизатори Cisco ISR/ASR та міжмережеві екрани нового покоління (NGFW) Cisco Firepower або ASA with FirePOWER Services, є першою лінією оборони, де реалізуються політики захисту від зовнішніх загроз, VPN-з'єднання, трансляція мережевих адрес (NAT/PAT) та функціонал систем запобігання вторгненням (NGIPS). Центр обробки даних (ЦОД) використовує комутатори Cisco Nexus з підтримкою технологій VXLAN та Cisco Application Centric Infrastructure (ACI) для мікросегментації. Бездротова інфраструктура на базі контролерів Cisco WLC та точок доступу забезпечує захищений доступ через WPA3-Enterprise з інтеграцією з ISE. Централізоване управління та моніторинг здійснюються за допомогою Cisco ISE, платформи оркестрації Cisco SecureX та системи аналізу трафіку Cisco Stealthwatch.

Розробка та впровадження ключових політик безпеки з використанням технологій Cisco є наступним логічним кроком. Політика сегментації мережі та контролю доступу, спрямована на ізоляцію критичних ресурсів та обмеження латерального руху зловмисників, реалізується шляхом використання VLAN, ACL на маршрутизаторах та L3-

комутаторах, VRF для повної ізоляції маршрутизації, а також технології Cisco TrustSec із застосуванням Security Group Tags (SGTs) та Security Group ACLs (SGACLs) під управлінням Cisco ISE для динамічної рольової сегментації. На маршрутизаторах Cisco IOS може застосовуватись Zone-Based Policy Firewall (ZPF).

Політика захисту периметра та запобігання вторгненням, що має на меті блокування неавторизованого зовнішнього доступу та нейтралізацію атак, втілюється на міжмережевих екранах Cisco Firepower NGFW через конфігурацію політик контролю доступу з інтегрованим NGIPS (на базі Snort), системою Advanced Malware Protection (AMP for Networks), URL-фільтрацією та контролем видимості додатків (AVC), а також через налаштування NAT та інспекції трафіку. Актуалізація захисних механізмів забезпечується інтеграцією з хмарною аналітичною системою Cisco Talos.

Політика безпечного віддаленого доступу та Site-to-Site VPN, що гарантує конфіденційність та цілісність даних при віддалених підключеннях, реалізується за допомогою клієнта Cisco AnyConnect Secure Mobility Client для SSL VPN або IKEv2 VPN на платформах Cisco ASA/Firepower, а також через налаштування IPsec IKEv1/IKEv2 тунелів між маршрутизаторами або міжмережевими екранами Cisco. Для масштабованих Site-to-Site з'єднань ефективним є використання технології Dynamic Multipoint VPN (DMVPN).

Політика автентифікації, авторизації та обліку (AAA) та управління пристроями, призначена для контролю адміністративного доступу до мережевих пристроїв та доступу користувачів до ресурсів, впроваджується шляхом налаштування протоколів TACACS+ (для адміністрування пристроїв) та RADIUS (для доступу до мережі) на всіх пристроях Cisco з інтеграцією з центральним AAA-сервером, яким виступає Cisco ISE. Автентифікація користувачів на портах комутаторів здійснюється за допомогою стандарту 802.1X. Важливим елементом є захист площини управління пристроями (Control Plane Policing, CoPP).

Нарешті, політика моніторингу та реагування на інциденти, що забезпечує своєчасне виявлення порушень безпеки, реалізується шляхом конфігурації Syslog для централізованого збору журналів подій, NetFlow для аналізу мережевого трафіку (з використанням, наприклад, Cisco Stealthwatch) та SNMP для моніторингу стану пристроїв.

Висновок. Науково обґрунтований підхід до розробки та впровадження політик безпеки, що спирається на використання технологіч-

ного потенціалу обладнання Cisco, дозволяє формувати ефективні та багаторівневі системи захисту корпоративних мереж. Представлена модель мережевої архітектури та деталізація реалізації ключових політик безпеки демонструють, як специфічні функціональні можливості пристроїв Cisco можуть бути синергетично задіяні для забезпечення належного рівня інформаційної безпеки. Інтегрований характер рішень Cisco, що передбачає взаємодію між різними компонентами безпеки (наприклад, ISE, Firepower, Stealthwatch через платформу pxGrid), суттєво підвищує загальну стійкість інфраструктури до сучасних кіберзагроз та оптимізує процеси управління безпекою. Перспективними напрямками подальших досліджень є розробка методів автоматизації конфігурування та аудиту відповідності політикам безпеки на обладнанні Cisco, а також застосування технологій штучного інтелекту для проактивного аналізу та прогнозування інцидентів безпеки.

Список використаних джерел

1. Cisco SAFE Reference Guide and Design Guides. Cisco Press.
2. Odom, W. (2023). CCNA 200-301 Official Cert Guide, Volume 1 & 2. Cisco Press.
3. Held, G. (2020). Cisco Security Professional’s Guide to Secure Network Design. CRC Press.
4. Implementing and Administering Cisco Solutions (CCNA) v1.0. Cisco Networking Academy.
5. Документація з безпеки для Cisco IOS XE, ASA, Firepower, ISE (www.cisco.com/c/en/us/support/security/index.html).
6. Стандарти ISO/IEC 27001:2022 та ISO/IEC 27002:2022.

УДК 004.056.621.39 (043.2)

Э.О. Гусєв, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ЗАПОБІГАННЯМ ЗАГРОЗАМ У ТКМ

Вступна частина

Телекомунікаційні мережі стали частиною нашого повсякденного життя. Ми постійно користуємося мобільним зв'язком, інтернетом та різними онлайн сервісами. Але разом з розвитком технологій зростає й кількість кіберзагроз. Хакери придумують нові способи атак, а старі методи захисту вже не завжди справляються. Саме тому тема захисту телекомунікаційних мереж є дуже важливою. У роботі розглядається, як можна використовувати штучний інтелект для того, щоб виявити та зупиняти кібератаки. Це сучасний напрям, який дає нові можливості для безпеки.

Основна частина

В основній частині роботи розглянуто, що таке кіберзагрози й чому вони небезпечні для телекомунікаційних мереж. Серед найбільш поширених загроз — DDoS-атаки, атаки на мережеве обладнання, фішинг, соціальна інженерія. Вони можуть порушити роботу компаній, призвести до втрати даних або навіть вплинути на роботу державних служб.

Традиційні методи захисту, такі як антивіруси чи фаєрволи, працюють за простими правилами й не завжди помічають нові, хитрі атаки. Штучний інтелект допомагає у цій ситуації, бо вміє аналізувати великі обсяги даних, розпізнавати незвичайні ситуації й швидко реагувати.

Окремий розділ роботи присвячено вивченню прикладу компанії **Fortinet**, яка є одним із лідерів у впровадженні ШІ у кібербезпеку. Її продукти, такі як FortiAI та FortiGuard, використовують машинне навчання для швидкого виявлення загроз, аналізу трафіку й автоматичного реагування. Fortinet збирає дані з усього світу, щоб постійно оновлювати свої системи й надавати клієнтам найсучасніший захист. Цей приклад показує, як ШІ вже сьогодні допомагає компаніям у реальному світі, а не тільки на папері.

Наприклад, FortiAI здатен розпізнати нові види загроз, яких раніше не було в базах даних, а FortiGuard забезпечує глобальний захист, оновлюючи інформацію про атаки в режимі реального часу. Такі рішення дозволяють

не тільки швидко реагувати на проблеми, а й передбачати можливі ризики наперед.

У роботі також підкреслюється, що ШІ не просто “працює замість людини”, а допомагає їй. Автоматизація рутинних завдань дає змогу фахівцям зосередитися на важливіших питаннях — наприклад, плануванні стратегій захисту, аналізі складних атак або підготовці компанії до нових викликів.

Додатково в роботі розглянуто, які технічні підходи використовуються всередині таких систем: моделі машинного навчання, алгоритми виявлення аномалій, автоматичні системи реагування. Важливо розуміти, що впровадження ШІ — це не лише встановлення готового продукту, а й налаштування його під конкретну мережу, навчання алгоритмів на специфічних даних компанії, а також постійне оновлення моделей.

Також окремо зазначається, що будь-яке застосування ШІ потребує висококваліфікованих фахівців. Без належного налаштування навіть найсучасніша система може бути неефективною. Тому компаніям потрібно не тільки купувати технології, а й вкладати в навчання персоналу й розвиток експертизи у сфері ШІ та кібербезпеки.

Висновки

Підсумовуючи, можна сказати, що штучний інтелект — це перспективний напрям для кібербезпеки телекомунікаційних мереж. Він дозволяє швидше виявляти загрози, автоматизувати захист і підвищити надійність мережі.

Для України впровадження ШІ дає шанс посилити кіберзахист як на рівні компаній, так і на рівні держави. Це допоможе не лише запобігати атакам, але й створити більш стабільну та безпечну телекомунікаційну систему для всіх користувачів.

Джерела:

1. https://www.techtarget.com/searchenterpriseai/definition/AI-Artificial-Intelligence
2. https://www.britannica.com/technology/artificial-intelligence/Reasoning
3. https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai

УДК 621.391

В.Є.Данилюк
Державний університет
«Київський авіаційний інститут», м. Київ

ДОСЛІДЖЕННЯ ПРОБЛЕМИ ДОСТУПУ ДО ДАНИХ З ВИКОРИСТАННЯМ МЕРЕЖІ СТАНДАРТУ LTE

Проблематикою дослідження є доступ до обладнання системи обробки даних, що включає у себе безперервну роботу обладнання для зберігання важливих даних, з забезпеченням варіантів резервування живлення, та резервним каналом зв'язку, що не залежить від роботи локального мережевого обладнання, виконуючи умову швидкого розгортання у разі переміщення, з простотою експлуатації та зменшенням витрат підприємства.

Об'єктом дослідження є функціонування системи обробки даних за допомогою мобільних мереж останніх поколінь, що використовуються в Україні та є каналом зв'язку в умовах, де прокладання проводової мережі не є можливим, з урахуванням оптимального споживанням ресурсів створеної системи.

Для вирішення завдання можна застосувати одноплатний комп'ютер,що виготовляє компанія Raspberry PI, проте додаткові модулі зв'язку, периферії і т.д, вимагають окремого придбання, що позначається на собівартості пристрою.

Апаратне забезпечення для рішення поставленого завдання, базується на використанні мобільного телефону на базі операційної системи Android, з підтримкою технології мобільного зв'язку стандарту LTE та вищими потужностями процесора, порівняно з попереднім розглянутим рішенням, які є достатніми для використання у якості системи обробки даних в автономному режимі, з вбудованими модулями зв'зку.

Вагомою перевагою використання мобільного телефону у якості апаратної платформи для системи обробки є екологічність - такий підхід до проблеми зменшує кількість відходів, зі скороченням витрат ресурсів, порівняно з витратами при виробництві нового обладнання.

Для наукового обґрунтування результатів досліджень роботи системи обробки даних у мережі LTE, застосовано експериментальний метод, що включає створення телекомунікаційної мережі, з включен-

ням головного елемента для безпосередньої обробки даних з доступом до нього, та клієнтське обладнання. У ході застосування даного методу результатом є знаходження оптимальних параметрів створеної системи для комфортної роботи з нею.

Розрахунки споживчої потужності для різних варіантів систем обробки даних доводять: варіант вирішення проблеми з пропонованою елементною базою є найоптимальнішим, зокрема через стандартизацію напруги живлення для таких пристроїв (5 вольт), з можливістю роботи від блока живлення для мобільного телефону, чи джерел живлення з малою потужністю.

Щодо інакших варіантів для вирішення поставленого завдання, проблема ощадливого енергоспоживання для безперервної роботи обладання пояснюється складністю оптимізації систем безперебійного живлення для серверів та ПК, що вимагає використання інверторів за відсутності живлення, які витрачають додаткову потужність резервного джерела при перетворенні (до 20%).

У ході досліджень порівняно оптимальні показники мобільної мережі LTE для комфортного використання системи, з оптимальним споживанням енергії, шляхом обрання стандарту мобільної мережі в налаштуваннях операційної системи пристрою а також оптимізацією супутніх програм в операційній системі.

При застосуванні експериментального методу було отримано результати споживчої потужності у межах 10-15 Вт, при виборі оптимального стандарту мережі (LTE), з показником допустимої потужності прийнятого сигналу від базової станції -80dBm (1×10^{-11} Вт), що вистачає для безперервної та безперебійної роботи пристрою, без втрат даних при передачі, враховуючи статичність пристрою.

На підставі отриманих результатів можна сказати про доцільність застосування розробленого методу у якості готового рішення для обробки та збереження даних, врахувуючи його переваги, що вирішує проблему забезпечення безперебійної роботи системи та заощаджує енергетичні та фінансові ресурси при її створенні та експлуатації.

Список використаної літератури:

1. https://www.clearesult.com/80plus/sites/80plus/files/manufacturer-certificate/dell-d750ps0-9038.pdf
2. https://www.gsmarena.com/xiaomi_mi_5-6948.php

УДК 621.396:004.056.5

Т.С. Денисенко
Державний університет
«Київський авіаційний інститут», м. Київ

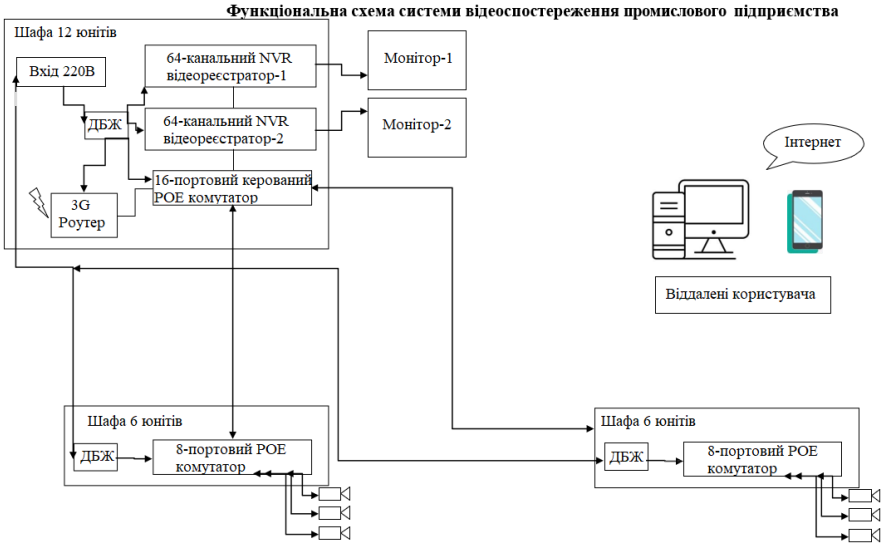
ПРОЕКТУВАННЯ СИСТЕМИ ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ ПРОМИСЛОВОГО ПІДПРИЄМСТВА: ВИМОГИ, ПРИНЦИПИ ТА ТЕХНОЛОГІЇ

Сучасні промислові підприємства стикаються з високими вимогами до безпеки та безперервного виробничого процесу, що робить актуальним питання впровадження ефективних систем відеоспостереження. Традиційні системи поступово замінюються цифровими рішеннями, які інтегруються в IT-інфраструктуру підприємства й забезпечують не лише фіксацію, а й активне запобігання загрозам.

У роботі виконано огляд класифікації систем безпеки та відеоспостереження, розглянуто основні компоненти: камери (включно з характеристиками, що визначають вибір моделей для промислових умов), мережеві реєстратори, програмне забезпечення (VMS) і засоби передачі сигналу. Особливу увагу приділено класифікації за масштабом системи (від малих до великих) і типом архітектури (централізовані, децентралізовані, гібридні).

Проєктування системи відеоспостереження розпочинається з детального передпроєктного обстеження об'єкта, оцінки умов експлуатації, визначення зон спостереження й вимог до обладнання. З урахуванням зонування підприємства розробляється технічне завдання, що враховує особливості виробництва, умови середовища та вимоги до безперервності роботи. У дослідженні представлено характеристику основних зон виробничого об'єкта, а також технічне обґрунтування вибору обладнання.

Запропонована конфігурація передбачає централізоване розміщення технічної шафи з PoE-комутатором і ДБЖ, прокладання кабельної інфраструктури з використанням витої пари Cat 6 у захисних каналах, а також віддалене збереження архіву у серверному приміщенні. Система відповідає вимогам стабільної роботи у 24/7-режимі, високої якості зображення (8 Мп), стійкості до пилу й вологи (IP67) та підтримує аналітичні функції виявлення.



Отримані результати демонструють, що поєднання правильної архітектури системи, вибору технічних компонентів та зонального підходу дозволяє створити ефективну та гнучку систему відеоспостереження, яка підвищує безпеку праці та виробничих процесів. Запропоновані технічні рішення можуть бути адаптовані до інших об’єктів промисловості зі схожими умовами експлуатації.

UDC 621.311.17(045)

O.S. Dmytrenko
State University
"Kyiv Aviation Institute, Kyiv, Ukraine

METHODS FOR DETECTING AND PREVENTING DDOS ATTACKS IN VOIP SYSTEMS

Voice over Internet Protocol (VoIP) is fundamental to modern communications but is vulnerable to Distributed Denial of Service (DDoS) attacks, which disrupt services and degrade Quality of Service (QoS). The increasing sophistication of these attacks necessitates advanced defenses. The relevance of this work lies in addressing the critical need for robust security to protect VoIP communications and maintain user trust.

The aim of this work is to comprehensively analyze existing methodologies and propose effective strategies for detecting and preventing DDoS attacks targeting VoIP systems. To achieve this aim: VoIP system functionality and vulnerabilities, such as weak authentication in signaling protocols or improperly configured session timers, are analyzed for attack classification. Common DDoS attack types on VoIP (targeting SIP and RTP) and their QoS impacts, leading to call drops, severe audio degradation, and potential service unavailability, are investigated. Attack characteristics across different VoIP protocols (SIP, RTP, H.323) are examined to inform countermeasure development. Traditional detection methods (signature-based, threshold-based) are reviewed, highlighting their limitations against encrypted or polymorphic attacks. Advanced detection techniques, particularly machine learning (ML) and artificial intelligence (AI), which offer proactive threat identification before significant service impact, are explored. Network traffic analysis approaches like deep packet inspection (DPI) and behavioral analysis are considered for identifying subtle attack patterns. Established prevention methods, including firewalls and Intrusion Detection/Prevention Systems (IDS/IPS), are discussed regarding their VoIP applicability. Distributed security approaches like Software-Defined Networking (SDN) are evaluated for dynamic traffic management and attack mitigation. The importance of comprehensive security policies, robust access controls, and the central role of Session Border Controllers (SBCs) in functions like call admission control, protocol repair, and topology hiding is substantiated. Finally, the necessity for

experimental validation of proposed methods, including attack modeling and key evaluation metrics (FPR, FNR, detection delay, resource utilization), is assessed.

Securing VoIP systems is challenging due to protocol complexities and real-time service demands. Traditional security often fails against voluminous or VoIP-specific DDoS attacks. This research emphasizes a multi-faceted approach, combining insights from protocol analysis with advanced detection and mitigation. Effective detection is transitioning from static methods to dynamic, behavior-based ML systems (e.g., SVM, neural networks) capable of adapting to new threats. However, these systems often require substantial labeled datasets for effective training, careful tuning to minimize false alarms, and continuous retraining to address the evolving nature of attack vectors. These systems rely on thorough network traffic analysis for early anomaly identification.

For prevention, a layered security architecture is key. While firewalls and IDS/IPS offer baseline defense, VoIP-specific elements like SBCs are indispensable. SBCs manage session signaling and media, enforcing policies like rate limiting, malformed packet detection, and also facilitating critical functions like secure NAT traversal and interworking between different VoIP networks. SDN can add agility by enabling programmable network control for rapid attack response and traffic engineering. Strong authentication, clear security policies, regular security audits, timely patching of all system components, and staff training form the bedrock of a secure VoIP deployment. Validating these methods through realistic simulations and in live testbed environments is essential to ensure their practical effectiveness.

In conclusion, safeguarding VoIP systems from DDoS attacks requires a comprehensive, adaptive strategy. This work has analyzed threats, explored advanced ML-based detection, and discussed robust prevention techniques. A multi-layered approach integrating protocol-aware security, intelligent detection, and agile response is vital for building resilient infrastructures. Future research should focus on enhancing automation, developing real-time adaptive and self-learning defense systems, exploring the use of distributed ledger technologies for enhanced signaling security, and improving threat intelligence sharing within the VoIP ecosystem.

УДК 004.773: 621.395.721.1(043.2)

М.О. Дроздовський, Д. І. Бахтіяров канд. техн. наук, доцент
Державний університет
«Київський авіаційний інститут», м. Київ

КОНЦЕПЦІЯ БЕЗДРОТОВОЇ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ WI-FI 7 ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ HUAWEI

Сучасний етап розвитку інформаційних технологій характеризується експоненційним зростанням обсягів бездротового трафіку та кількості підключених пристроїв, таких як Інтернет речей (IoT), мобільні пристрої та системи доповненої/віртуальної реальності (AR/VR). Це супроводжується зростаючими вимогами до швидкості передачі даних, низької затримки та надійності бездротових мереж у сферах бізнесу, освіти та розваг. Традиційні бездротові архітектури часто не в змозі ефективно відповідати цим викликам. Поява нового стандарту Wi-Fi 7 (IEEE 802.11be, Extremely High Throughput – EHT) пропонує революційні можливості для побудови високопродуктивних бездротових мереж. Компанія Huawei, як провідний виробник телекомунікаційного обладнання, активно розробляє та впроваджує рішення на базі Wi-Fi 7. Дана робота присвячена розробці та обґрунтуванню концепції побудови такої мережі для підприємства на базі обладнання Huawei.

Запропонована концепція бездротової телекомунікаційної мережі Wi-Fi 7 підприємства ґрунтується на комплексному підході Huawei, що об'єднує передові апаратні та програмні рішення. В основі архітектури лежить багаторівнева інфраструктура, що включає рівень доступу (точки доступу Huawei AirEngine Wi-Fi 7), рівень керування (контролери Huawei AC series) та рівень агрегації/ядра (комутатори CloudEngine та маршрутизатори AR). Ключовими технологічними нововведеннями стандарту Wi-Fi 7, що підтримуються обладнанням Huawei, є Multi-Link Operation (MLO) для одночасного використання кількох діапазонів частот, канали шириною до 320 МГц, модуляція 4096-QAM, покращений MU-MIMO та Multi-RU в OFDMA.

Центральну роль в управлінні, моніторингу та аналітиці відіграє інтелектуальна платформа iMaster NCE. Вона надає єдину точку контролю над мережевими ресурсами, використовує алгоритми штучного інтелекту (AI) та машинного навчання (ML) для

автоматизації мережевих операцій, проактивного виявлення потенційних проблем, інтелектуальної діагностики та оптимізації продуктивності мережі. Реалізація такої архітектури забезпечує надзвичайно високу пропускну здатність (теоретично до 46 Гбіт/с), низьку затримку, підвищену надійність з'єднання та покращену ефективність використання спектру. Гарантується багаторівнева безпека, що включає підтримку WPA3, автентифікацію 802.1X, сегментацію трафіку та захист від несанкціонованого доступу.

Практичне застосування охоплює сценарії побудови високощільних Wi-Fi мереж в офісах, на виробництві (розумні фабрики, промисловий IoT, AGV), у логістиці, освітніх закладах (онлайн-навчання, VR-лабораторії), мультимедійних залах (8K-стрімінг), а також у готельному бізнесі та роздрібній торгівлі для надання персоналізованих сервісів та AR-досвіду

Представлена концепція бездротової телекомунікаційної мережі Wi-Fi 7 підприємства на базі рішень Huawei є ефективним підходом до модернізації корпоративних IT-інфраструктур. Завдяки передовому мережевому обладнанню AirEngine, контролерам AC та інтелектуальній системі управління iMaster NCE, у поєднанні з перевагами стандарту Wi-Fi 7, досягається значне підвищення продуктивності, гнучкості, масштабованості, надійності та безпеки мережі. Впровадження такої архітектури дозволяє підприємствам оптимізувати операційні витрати, підвищити ефективність бізнес-процесів та створити технологічний фундамент для інноваційних цифрових сервісів. Подальші дослідження можуть бути спрямовані на інтеграцію Wi-Fi 7 з технологіями 5G/6G та розробку нових додатків, що використовують переваги EHT.

Список використаних джерел:

1. Huawei Enterprise BG. Huawei AirEngine Wi-Fi 7: Pioneering Enterprise-Grade Extremely High Throughput (Technical White Paper).

2. IEEE P802.11be™/D7.0 March 2024. Draft Standard for Information Technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications – Amendment 8: Enhancements for Extremely High Throughput.

УДК 614.841.3(043.2)

М.В. Дубович
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЕКТУВАННЯ ТА ТЕХНІЧНА ЕКСПЛУАТАЦІЯ СИСТЕМИ ПОЖЕЖНОЇ СИГНАЛІЗАЦІЇ В ШКОЛІ

Забезпечення пожежної безпеки в освітніх закладах є актуальною проблемою, оскільки від ефективності виявлення загоряння та своєчасного оповіщення залежить життя та здоров’я учнів і персоналу. У навчальних установах зазвичай перебуває значна кількість людей, а складна структура приміщень ускладнює евакуацію. Це вимагає впровадження сучасних технологічних рішень у галузі пожежної сигналізації, які дозволяють забезпечити своєчасне реагування та знизити ризики поширення пожежі. Особливого значення ця проблема набуває у школах, де необхідно враховувати вікові особливості дітей, їх здатність до швидкої орієнтації у стресових ситуаціях та потребу в надійному інформуванні про небезпеку.

У роботі проведено аналіз наявної системи пожежної сигналізації у типовій загальноосвітній школі. Встановлено, що використовується застаріле обладнання, яке не підтримує адресне визначення джерела пожежі та не інтегрується з евакуаційним освітленням і системами димовидалення. Це знижує ефективність протипожежного захисту та ускладнює координацію дій персоналу в умовах надзвичайної ситуації. Практичне значення полягає у можливості впровадження результатів дослідження у школах для підвищення рівня пожежної безпеки, зменшення часу реагування на загрозу та покращення умов для безпечної евакуації.

У межах дослідження проаналізовано вимоги чинних нормативно-правових актів у сфері пожежної безпеки, зокрема Правил пожежної безпеки в Україні, ДБН В.2.5-56:2014 та ДБН В.2.2-3:2018, щодо проєктування та експлуатації систем пожежної сигналізації у навчальних закладах. Проведено обстеження типового освітнього об'єкта — школи №1, визначено категорії пожежонебезпеки приміщень та виявлено недоліки у наявній системі пожежної сигналізації, серед яких: відсутність адресного визначення місця спрацювання, застаріле обладнання, недостатня інтеграція з іншими підсистемами безпеки (димо- та тепловидалення, евакуаційне освітлення).

звукового та голосового оповіщення, інтеграцію з евакуаційним освітленням і системою контролю доступу. Розроблено функціональну і принципову електричну схеми, що забезпечують гнучкість адаптації системи до особливостей будівлі, та враховують можливість майбутньої модернізації.

Систему передбачено як модульну з можливістю масштабування. Вона розрахована на безперервну експлуатацію та здатна зберігати працездатність у разі відключення основного живлення. Вибір обладнання обґрунтовано за критеріями надійності, сумісності та відповідності технічним характеристикам, визначеним нормативами.
Практична цінність розробленого проєкту полягає в можливості його безпосереднього впровадження в існуючі освітні заклади з метою модернізації систем протипожежного захисту. Передбачена структура дозволяє адаптувати рішення до будь-якої архітектури шкільної будівлі, враховуючи як звичайні класи, так і спеціалізовані приміщення (лабораторії, їдальня, спортивна зала). Наукова новизна дослідження полягає у поєднанні традиційних технологій виявлення загоряння з сучасними цифровими системами моніторингу та управління, що відкриває можливості для інтеграції з системами "розумної школи".

Окрему увагу приділено технічному обслуговуванню системи, зокрема регулярній перевірці сповіщувачів, тестуванню оповіщення та моніторингу працездатності приймально-контрольного обладнання. Запропоновано створити цифрову базу обліку технічного стану СПС, що дозволить автоматизувати контроль і своєчасно проводити профілактичні заходи.

Запропонована система пожежної сигналізації для навчального закладу забезпечує своєчасне виявлення загорянь, інформування персоналу та учнів, а також автоматичне керування евакуацією і локалізацією пожежі. Впровадження такого проєкту підвищить рівень безпеки в освітніх установах, зменшить ймовірність виникнення надзвичайних ситуацій та сприятиме збереженню життя і здоров’я людей.

Висновки підтверджують ефективність розробленої системи пожежної сигналізації. Вона не лише відповідає сучасним вимогам безпеки, а й забезпечує високу адаптивність до умов конкретного навчального закладу. Упровадження такої системи дозволить значно підвищити рівень захисту учасників освітнього процесу, знизити ризики для життя та здоров’я у разі пожежі та забезпечити відповідність сучасним стандартам пожежної безпеки в освітній сфері.

УДК 621.391

А.О.Ємельянов
Державний університет
«Київський авіаційний інститут», м.Київ

Аналіз загроз інформаційній безпеці для АС класу 2 та методи їх нейтралізації.

Аналіз загроз інформаційної безпеки – це процес виявлення, оцінки та розуміння можливих загроз, які можуть вплинути на безпеку інформації в комп'ютерних системах, мережах. Загрози інформаційної безпеки можуть бути різними – від технічних проблем до зловмисних дій, спрямованих на крадіжку даних або завдання шкоди системам. Наприклад, до технічних проблем можна віднести некоректну роботу обладнання, падіння систем, помилки в програмному забезпеченні тощо. До зловмисних дій можна віднести кібератаки, віруси, хакерські атаки, фішингові атаки, вимагання викупу.

Аналіз загроз інформаційної безпеки включає в себе такі етапи:

1. Виявлення загроз – процес виявлення можливих загроз для інформаційної безпеки в комп'ютерних системах і мережах. 2. Оцінка загроз – процес оцінки потенційного впливу загроз на безпеку інформації та визначення ризику. 3. Розуміння загроз – процес аналізу властивостей та взаємозв'язку загроз, що дозволяє зрозуміти їх природу та можливості. 4. Розробка стратегії захисту – процес розробки стратегій та заходів для запобігання або зменшення впливу загроз на безпеку інформації. 5. Реалізація заходів захисту – процес реалізації стратегій та заходів захисту для забезпечення безпеки інформації. 6. Моніторинг і оновлення – процес стеження за виникненням нових загроз та оновлення захисних заходів відповідно до зміни ситуації.

Для аналізу загроз інформаційної безпеки можуть використовуватися різні методи та інструменти, такі як аудит безпеки, сканування портів, тестування на проникнення, аналіз журналів подій, аналіз вразливостей та інші. Важливо пам'ятати, що аналіз загроз інформаційної безпеки – це процес, який потребує постійного оновлення та вдосконалення, оскільки внаслідок розгортання гібридних воєн у глобальному інформаційному просторі нові загрози з'являються щодня.

UDC 621.37 (043.2)

B.S. Yefimenko
State University
«Kyiv Aviation Institute», Kyiv

VIPER. REMOTE VIDEO AND CONTROL UNIT

VIPER is a specialized remote device for FPV drones, focused on delivering dependable, stable, and high-quality video transmission and control channels. A key advantage is its ability to have the remote video and control unit installed on a mast away from the operator, enhancing operator safety in combat scenarios. The system features a high-quality Walksnail Avatar VRX digital video communication system, which employs the H.265 (HEVC) video encoding for efficient compression and an OFDM transmission scheme for reliable wireless communication. For control, the drone is equipped with two ELRS TX control modules operating at 915 MHz and 433 MHz, providing a wider range of radio channels and better resistance to electronic warfare.

The VIPER unit is powered by the **Walksnail Avatar digital HD FPV** system, which is engineered for high-fidelity video, operational robustness, and critically, low-latency real-time performance essential for situational awareness and precise piloting. The Walksnail Avatar system uses the H.265 (HEVC) video compression standard, offering a significantly higher compression ratio than H.264 for the same video quality. This efficiency reduces the volume of video data, minimizing bandwidth requirements and processing load on both transmitter and receiver, thereby contributing to reduced encoding/decoding times and enabling high-quality video at lower bitrates.

For signal transmission, Walksnail Avatar utilizes an **OFDM (Orthogonal Frequency Division Multiplexing)** modulation scheme. This digital multi-carrier technique uses many closely spaced, orthogonal sub-carriers, each modulated at a low symbol rate, making the system highly resilient to issues like frequency-selective fading and inter-symbol interference from multipath propagation. This robustness allows for reliable high-data-rate transmission even in complex RF environments. The combination of efficient H.265 encoding and robust OFDM transmission results in an exceptionally low end-to-end video latency, typically as low as 22 milliseconds.

This advanced digital system is further enhanced by specialized mini horn-type antennas (Gain: 14 dBic; Beamwidth H/V: 37°/33°; VSWR: <1.3 from 4.9-6.0 GHz; Circular/Linear Polarization), which are assembled separately to improve operational range and interference rejection. The video subsystem has an approximate power output of 50W.

Dual-ExpressLRS Control system

VIPER integrates a reliable control system with two ExpressLRS (ELRS) transmitters (TX) for controlling FPV drones. ELRS is an open, high-performance communication channel known for its long range, low latency, and interference penetration, which often uses LoRa modulation and configurable packet transmission rates.

The use of two modules tuned to different frequencies, in our case 915 MHz and 433 MHz bands, allows us to cover a wider frequency spectrum. If, due to external factors, such as frequency suppression in a certain spectrum by electronic warfare means, we lose control of one of the modules, we will continue to transmit and receive data from the other module. Each TX uses Yagi-Uda antennas (VSWR: <1.2; Impedance: 50 ohms; Linear Polarization) for efficient, directional transmission.

Switching between modules and internal communication REMOTE VIDEO AND CONTROL UNIT is provided by the central ESP32 microcontroller (MCU). If the signal deteriorates or is completely lost, the ESP32 instantly switches the control module, which is not noticeable during flight.

Engineered for critical tasks, the VIPER device provides exceptional image clarity and control stability through its real-time, low-latency video (H.265, OFDM) and dual-frequency ELRS control managed by an ESP32. Its proven resistance to interference, especially in electronic warfare environments, makes it indispensable for demanding applications. Moreover, VIPER's design prioritizes operator safety; by placing the unit on a mast connected to a ground-based system, the pilot can remain in a secure location while the unit maintains reliable, high-quality communication from an open area, ensuring both mission effectiveness and user security."

УДК 621.391

В.В. Кальєв, О.Ю. Лавриненко
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА УПРАВЛІННЯ РОЗУМНИМ БУДИНКОМ НА ОСНОВІ TELEGRAM-БОТА

Концепція розумного будинку (Smart Home) передбачає автоматизоване управління побутовими системами (освітленням, вентиляцією, безпекою тощо) для підвищення комфорту, енергоефективності та безпеки. Ринок пропонує багато рішень: брендові екосистеми (Google Home, Apple HomeKit. Alexa), програмовані контролери (I3 Engineering, KNX), а також open-source-платформи (Home Assistant). Водночас, їхня реалізація часто вимагає значних витрат або складного налаштування. Використання Telegram-бота як інтерфейсу управління для саморобних систем домашньої автоматизації є одним із перспективних напрямів, адже він пропонує просту інтеграцію, кросплатформенність, широкі можливості та зручність для користувача.

Метою роботи є створення бюджетної, автономної системи розумного будинку, що не потребує окремого сервера та забезпечує дистанційне управління і моніторинг через Telegram. В основі лежить мікроконтролер Arduino Uno R4 WiFi. Проєкт мав забезпечити: стабільність, масштабованість, швидку реакцію на події, інтуїтивний інтерфейс та роботу напряму з Telegram API. Для реалізації проєкту обрано Arduino Uno R4 WiFi — потужну плату із вбудованим Wi-Fi модулем й доступними 256 КБ FLASH-пам’яті та 32 КБ RAM, яких достатньо для зберігання базових налаштувань (пороги температури, стан сценаріїв) та великої за об’ємом програмної частини. Додатково використано Sensor Shield V5.0 для зручного масштабування та підключення сенсорів. У якосты сенсорыв було обрано давачі DS18B20, DHT22, аналоговий давач протікання та геркони. Telegram-бот розроблений з використанням спеціалізованої бібліотеки, що дозволяє використовувати увесь функціонал Telegram API. Всі GET/POST запити до Telegram API надсилаються Arduino без проміжного сервера за допомогою HTTPS-запитів у форматі JSON. Меню розділене на вкладки: «Світло», «Системи», «Давачі», «Сценарії», «Налаштування». Кожна з них викликає відповідні

функції на мікроконтролері. Наприклад, «Світло» дозволяє вмикати/вимикати реле з підключеними до них освітлювальними приладами, а «Давачі» дозволяють переглядати показники температури, вологості, протікань та стану дверей. Автоматизація реалізована через розклади, які користувач створює самостійно, та сценарії «Охорона» і «Вологе прибирання». Перший надсилає сповіщення при відкритті дверей, другий тимчасово вимикає захист від протікань. У системі реалізовано аварійні сповіщення у вигляді окремих повідомлень Telegram, що дозволяє користувачу миттєво отримувати push-оповіщення. Передбачено чотири типи повідомлень: про протікання, проникнення, переохолодження та перегрів. У кожному випадку бот надсилає окреме повідомлення з вказанням часу події, місця або поточної температури, що забезпечує швидке реагування та інформативність. Налаштування доступні через меню: зміна порогів температури, створення та редагування розкладів, дистанційне перезавантаження Arduino. Всі дані вводяться в Telegram-чаті, після чого система оновлює відповідні значення у пам’яті. Для зручності реалізовано повідомлення з інструкціями щодо введення даних та форматів. Безпека реалізована просто: всі команди приймаються лише від одного Chat ID, прописаного в коді, що виключає стороннє втручання. Відповідь на команди відбувається у реальному часі, без затримок. Візуальна частина бота містить емодзі-індикатори, які інтуїтивно показують стан пристроїв (ввімкнено/вимкнено).

У результаті створено функціональну, автономну систему управління розумним будинком без використання сервера, лише з Arduino та Telegram. Система забезпечує моніторинг і контроль стану житла, реагування на аварійні ситуації, налаштування розкладів та сценаріїв, збереження даних у EEPROM і можливість масштабування. Порівняно з аналогами, вона є дешевшою (використано доступні компоненти), простішою у впровадженні (без складних інсталяцій), гнучкою (можливість додавання нових функцій). Практичні тести показали високу стабільність роботи, оперативну реакцію на команди та простоту використання. Такий підхід може бути ефективно застосований у невеликих квартирах чи приватних будинках, а також як освітній або хобі-проєкт для вивчення основ IoT та автоматизації.

УДК 004.738.52 (043.2)

Б.Р. Кальчук, В.М. Чуприн
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ЛОКАЛЬНОГО ПОЗИЦІОНУВАННЯ НА БАЗІ ТЕХНОЛОГІЇ IEEE 802.15

Вступ. В останні роки спостерігається стрімкий розвиток технологій локального позиціонування (LPS), що зумовлено зростаючими потребами в точному визначенні місцезнаходження об'єктів та людей у приміщеннях та на обмежених територіях. Стандарт IEEE 802.15, зокрема його модифікації, такі як IEEE 802.15.4 (відомий як Zigbee) та IEEE 802.15.4z (що включає технологію надширокосмугової передачі даних HRP UWB), надає перспективну основу для створення енергоефективних та точних систем локального позиціонування. Актуальність даної теми полягає у необхідності дослідження та розробки ефективних методів позиціонування, що використовують переваги стандартів IEEE 802.15 для вирішення широкого кола прикладних задач, від промислової автоматизації до персональної навігації та безпеки. Метою даної роботи є аналіз можливостей та викликів при створенні системи локального позиціонування на базі технології IEEE 802.15, а також формулювання основних принципів її побудови та функціонування.

Основна частина. Системи локального позиціонування на основі стандарту IEEE 802.15 відкривають значні перспективи завдяки своїй гнучкості та енергоефективності. Зокрема, технологія IEEE 802.15.4, що лежить в основі таких протоколів як Zigbee, дозволяє створювати бездротові сенсорні мережі (WSN) з низьким енергоспоживанням, які можуть бути використані для позиціонування з помірною точністю. Для визначення місцезнаходження в таких системах часто використовуються методи, що базуються на вимірюванні рівня прийнятого сигналу (RSSI). Перевагою RSSI-методів є їх простота реалізації та низька вартість, оскільки не потрібне спеціалізоване обладнання. Однак, точність таких систем суттєво залежить від умов навколишнього середовища, зокрема наявності перешкод, багатопроменевого поширення сигналу та інтерференції, що обмежує їх застосування у складних умовах.

Значний прорив у точності локального позиціонування пов'язаний з впровадженням стандарту IEEE 802.15.4z, який стандартизує використання надширокосмугових сигналів (UWB) з високою роздільною здатністю по часу (HRP). Технологія UWB дозволяє досягти сантиметрової точності визначення відстані завдяки використанню коротких імпульсів, що робить її стійкою до багатопроменевого поширення. Основними методами вимірювання відстані в UWB-системах є часпролітні методи, такі як двосторонній обмін даними (Two-Way Ranging, TWR) або симетричний двосторонній обмін даними з подвійним підтвердженням (Symmetric Double-Sided Two-Way Ranging, SDS-TWR). Ці методи дозволяють точно виміряти час прольоту сигналу між двома пристроями (анкером та міткою), на основі якого розраховується відстань. Для визначення координат об'єкта в двовимірному або тривимірному просторі використовуються алгоритми трилатерації або мультилатерації, що потребують наявності щонайменше трьох або чотирьох анкерів з відомими координатами відповідно.

Архітектура системи локального позиціонування на базі IEEE 802.15 зазвичай включає наступні компоненти: мобільні мітки (теги), що кріпляться до об'єктів, місцезнаходження яких потрібно визначити; стаціонарні анкери (опорні вузли), що розміщуються у відомих координатах і слугують для вимірювання параметрів сигналу від міток; та центральний сервер (обчислювальний вузол), який збирає дані від анкерів, виконує алгоритми розрахунку координат та надає інформацію про місцезнаходження користувачам або іншим системам. Зв'язок між мітками та анкерами, а також між анкерами та сервером, може здійснюватися за допомогою протоколів на базі IEEE 802.15. Важливим аспектом є синхронізація анкерів, особливо для методів TDoA, де точна часова прив'язка є критичною. Для UWB-систем з використанням TWR або SDS-TWR такої жорсткої синхронізації не потрібно, що спрощує розгортання системи.

Вибір конкретного алгоритму позиціонування залежить від вимог до точності, енергоспоживання, складності реалізації та умов експлуатації. Окрім класичних методів ToF, ToA, TDoA та RSSI, перспективними є також методи, що базуються на аналізі кута прибуття сигналу (Angle of Arrival, AoA) або кута відправлення (Angle of Departure, AoD), які можуть бути реалізовані за допомогою антенних решіток. Гібридні підходи, що комбінують різні методи вимірювання, дозволяють підвищити надійність та точність системи. Наприклад, поєд-

нання RSSI з ToF може компенсувати недоліки кожного з методів окремо. Сучасні дослідження також зосереджені на використанні методів машинного навчання для калібрування системи, врахування впливу навколишнього середовища та покращення точності позиціонування, зокрема шляхом створення радіокарт (fingerprinting).

Застосування систем локального позиціонування на базі IEEE 802.15 є надзвичайно широким. У промисловості вони можуть використовуватися для відстеження активів, моніторингу персоналу, оптимізації логістичних процесів та підвищення безпеки. У сфері охорони здоров'я такі системи дозволяють відстежувати переміщення пацієнтів та медичного обладнання. В інтелектуальних будівлях вони можуть використовуватися для персоналізованого керування освітленням, опаленням та вентиляцією, а також для навігації всередині приміщень. Перспективним є також використання таких систем у робототехніці для навігації автономних мобільних роботів.

Незважаючи на значні переваги, існують і певні виклики при розробці та впровадженні систем локального позиціонування на базі IEEE 802.15. Одним з ключових викликів є забезпечення високої точності в складних умовах з великою кількістю перешкод та металевих конструкцій, що можуть спотворювати радіосигнали. Енергоефективність міток залишається важливим фактором, особливо для довготривалих застосувань. Масштабованість системи, тобто здатність обслуговувати велику кількість об'єктів, що відстежуються, та забезпечення низької затримки при визначенні координат також є актуальними задачами. Крім того, питання безпеки та конфіденційності даних про місцезнаходження потребують ретельного опрацювання.

Висновок. Технологія IEEE 802.15, зокрема її розширення у вигляді стандарту IEEE 802.15.4z (HRP UWB), надає потужний інструментарій для створення точних та енергоефективних систем локального позиціонування. Проведений аналіз показав, що вибір конкретних методів та архітектури системи залежить від специфічних вимог до точності, вартості, енергоспоживання та умов експлуатації. UWB-технологія демонструє найкращі показники точності, тоді як системи на базі RSSI є більш простими та дешевшими. Подальші дослідження повинні бути спрямовані на розробку більш стійких до завад алгоритмів позиціонування, вдосконалення методів калібрування системи, інтеграцію з іншими технологіями (наприклад, інерційними датчиками) для підвищення надійності, а також на розробку стандартизованих

протоколів обміну даними для забезпечення сумісності обладнання різних виробників. Вирішення цих завдань дозволить значно розширити сфери застосування систем локального позиціонування та підвищити їх ефективність.

Список використаних джерел

1. Alarifi, A., Al-Salman, A., Alsaleh, M., Alnafessah, A., Al-Hadhrami, S., Al-Ammar, M. A., & Al-Khalifa, H. S. (2023). Ultra-Wideband Indoor Positioning Technologies: A Comprehensive Review. IEEE Access, 11, 2345-2370.

2. Barac, F., Miloš, A., & Stojanović, R. (2024). Performance Evaluation of UWB-Based Indoor Positioning System in Complex Industrial Environments. Sensors, 24(3), 789.

3. Chen, L., Zhang, Y., Li, Y., & Wang, J. (2023). A Novel TDOA-Based UWB Indoor Positioning Algorithm with NLOS Mitigation. Electronics, 12(15), 3321.

4. Jiménez, A. R., Seco, F., Zampella, F., & Prieto, J. C. (2023). A Review on UWB IPS Channel Modeling and Fingerprinting. Sensors, 23(5), 2789.

5. Rydlo, L., Svub, J., & Kaller, O. (2023). An Enhanced UWB Indoor Localization System for Dynamic Environments Using Machine Learning. IEEE Internet of Things Journal, 10(21), 19005-19017.

6. Zhang, W., Liu, K., & Li, X. (2024). Energy-Efficient UWB Localization for IoT Devices Based on Compressed Sensing. IEEE Transactions on Mobile Computing, 23(1), 456-469.

УДК 621.391

В.В. Каракай, О.Ю. Лавриненко
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ГОЛОСОВОЇ ІДЕНТИФІКАЦІЇ ОСОБИ В ДИСТАНЦІЙНОМУ БАНКІВСЬКОМУ ОБСЛУГОВУВАННІ

У сучасних умовах стрімкого розвитку дистанційного банківського обслуговування виникає необхідність у впровадженні ефективних засобів захисту від несанкціонованого доступу до фінансових ресурсів. Ідентифікація користувачів стала одним з ключових етапів інформаційної безпеки, особливо в контексті зростання кількості фішингових атак, витоків даних та соціальної інженерії. Традиційні методи автентифікації дедалі частіше демонструють свою обмежену ефективність. У зв'язку з цим зростає інтерес до біометричних технологій, зокрема до голосової ідентифікації, як до зручного, економічного та надійного способу підтвердження особи.

Голосова біометрія базується на аналізі фізіологічних і поведінкових характеристик голосу, що є унікальними для кожної людини. На відміну від інших біометричних параметрів, таких як відбитки пальців чи зображення обличчя, голос можна зчитувати за допомогою вже наявного обладнання — мікрофонів, вбудованих у смартфони чи комп'ютери. Це забезпечує високу доступність технології, її економічність та масштабованість для використання у різних інформаційно-комунікаційних системах. Додатково, використання голосу як біометричного маркеру спрощує користувацьку взаємодію, що є критично важливим для систем з великою кількістю користувачів.

У ході дослідження виконано аналіз сучасних методів розпізнавання мовлення та можливостей використання нейромереж і машинного навчання. Запропоновано архітектуру системи, що поєднує спектральну обробку мовного сигналу, виділення ознак та класифікацію із застосуванням моделі SVM. Реалізована система забезпечує реєстрацію голосових шаблонів та їх ідентифікацію в реальному часі. Тестування на відкритих датасетах показало точність понад 91% при середньому часі обробки до 2 с. Для забезпечення захищеності від атак типу spoofing реалізовані алгоритми виявлення штучно згенерованого

мовлення, що підвищує довіру до системи з боку кінцевих користувачів.

Система має гнучкий модульний підхід, що дозволяє масштабувати її функціональність залежно від обсягів трафіку, потреб замовника та цільової платформи інтеграції. Особлива увага приділялася захисту від атак типу replay та spoofing, що є одними з ключових загроз для голосової ідентифікації. У розробці враховано методи детекції синтетичного мовлення, а також стратегії для адаптації до змін у голосі користувача, що можуть виникати внаслідок вікових змін або хвороб. Це дозволяє підтримувати надійність системи у довгостроковому періоді експлуатації.

Суттєвою перевагою запропонованої системи є можливість інтеграції з мобільними додатками та онлайн-сервісами без необхідності використання спеціалізованого обладнання. Адаптивність, економічність і висока точність роботи системи забезпечують її перспективність для застосування в цифровому банкінгу.

Окрім технічної ефективності, система має високий потенціал комерційної реалізації: вона може застосовуватись не лише в банківській галузі, а й у сферах електронного урядування, телемедицини, страхування та сервісних контакт-центрах. Розроблені підходи можуть бути масштабованими для обробки великої кількості запитів, зберігаючи при цьому точність і швидкодію. Перспективним напрямом подальших досліджень є інтеграція голосової ідентифікації з багатофакторними моделями автентифікації, що дозволить ще більше підвищити рівень захисту систем.

Таким чином, розроблена система голосової ідентифікації особи дозволяє суттєво підвищити рівень захисту банківських послуг, покращити користувацький досвід та забезпечити відповідність вимогам інформаційної безпеки у фінансовій сфері. Запропоноване рішення є перспективним напрямом розвитку інформаційно-комунікаційних технологій у сфері безпечної взаємодії людини з цифровими системами.

Список літератури:

1. Jain A., Ross A., Nandakumar K. Introduction to Biometrics. Springer, 2011.

2. Furui S. Digital Speech Processing. Synthesis and Recognition. CRC Press, 2018.

УДК 681.518.5

І.В.Касьян
Державний університет
«Київський авіаційний інститут», м. Київ

КОМПЛЕКСНА СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ (НА ПРИКЛАДІ ГРУПИ КОМПАНІЙ «НОВА ПОШТА»)

В сучасних умовах корпоративні мережі є важливою складовою частиною інфраструктури підприємства будь-якої галузі. Сьогодні важко знайти компанію, в якій би не було створено хоча б невелику локальну мережу. Адже за її допомогою забезпечується обмін інформацією та синхронізація праці усіх працівників організації не лише в межах одного офісу, а й між різними філіями та відділеннями підприємства незалежно від їх географічного розташування. Проте чим більш розгалуженою є корпоративна система, чим більшу кількість користувачів вона об'єднує, тим більше вразливою вона стає для різного роду зовнішніх загроз. Пошкодження інформації або затримка її передачі може призвести до негативних, а іноді – і до критичних наслідків для компанії. В таких умовах суттєво зростає актуальність проблеми захисту інформації в корпоративних мережах.

В умовах гібридної війни, яку російська федерація веде проти України, інформаційна сфера стала одним з основних театрів бойових дій. Задля досягнення своїх геополітичних цілей ворог активно застосовує методи інформаційно-психологічного впливу, кібератаки та інші деструктивні технології. Враховуючи зазначене, сьогодні, як ніколи раніше, особливого значення набуває законодавче регулювання інформаційної безпеки. Варто зауважити, що існуюча нормативно-правова база з питань інформаційної безпеки певно мірою не встигає за реальним розвитком інформаційних технологій та появою нових викликів і загроз. У зв'язку з цим актуальним завданням є постійне вдосконалення законодавства в даній сфері, його адаптація до сучасних реалій.

В управлінні логістичною діяльністю Групи компаній «Нова Пошта» інформаційні системи виконують ключову роль. Оскільки до групи входять українські та міжнародні компанії, зокрема Нова пошта, NovaPay, Nova Global, Nova Post у Молдові, Литві, Польщі, Чехії, Румунії, Німеччині, а також авіакомпанія Supernova Airlines, корпоративна мережа Групи побудована з урахуванням діяльності як на

національному, так і на міжнародному рівні. Вона дозволяє компанії ефективно керувати своїми глобальними операціями, обмінюватися даними та інформацією між відділеннями, надавати послуги клієнтам з усього світу та забезпечувати безпеку та надійність своїх інфраструктур. Мережа забезпечує динамічний розподіл IP-адрес, обмеження доступу до різних ресурсів для забезпечення безпеки та можливість взаємодії між відмінними віртуальними та фізичними мережами підприємства.

Для налаштування корпоративної мережі Групи компаній «Нова Пошта» використовуються наступні пристрої: маршрутизатори, які використовуються для передавання інформації між різними сегментами мережі; комутатор – для перемикання сигналів між пристроями в мережі, забезпечуючи передачу даних; сервер DHCP - використовуються для динамічного призначення IP-адрес; сервер DNS, що дозволяє надавати доменні імена для веб-серверу замість доступу за IP-адресою.

Для забезпечення надійного та безпечного функціонування мережі в компанії використовуються такі стратегії захисту:

1. Аутентифікація та авторизація: впровадження паролів для привілейованого режиму та SSH забезпечує контрольний рівень доступу до системних ресурсів та забезпечує захищений віддалений доступ.

2. Розділення на сегменти: застосування VLAN та методу «Router-on-a-stick» допомагає розділити мережу на сегменти, знижуючи ризик перетоку даних та небажаної комунікації.

3. Файрвол та керування доступом: використання списків керування доступом (ACL) дозволяє ефективно блокувати небезпечні протоколи та контролювати доступ до мережевих сервісів.

4. Захист від атак із зовнішньої мережі: застосування технологій та стратегій допомагає захистити мережу від різних кіберзагроз, таких як DDoS-атаки та несанкціонований доступ.

Група компаній «Нова пошта» вживає заходів для захисту від кібератак та інших загроз, зокрема, попереджує про фішингові листи та рекомендує активувати двофакторну аутентифікацію. Наголошує на важливості перевірки безпеки акаунтів та видалення підозрілих листів.

Впроваджені заходи безпеки забезпечують конфіденційність, цілісність даних та надійний доступ до ресурсів для всіх відділень компанії. Мережа компанії може ефективно функціонувати у сучасному цифровому середовищі, забезпечуючи стійкість до різних загроз та відповідність вимогам безпеки.

УДК 004.8:004.738.5(043.2)

А.О. Кобилінський
Державний університет
«Київський авіаційний інститут», м. Київ

Штучний інтелект у побутовому використанні людини: коли AI стає частиною нашого життя

Ще кілька років тому «штучний інтелект» здавався чимось із майбутнього або, принаймні, тим, що стосується лише великих лабораторій чи високих технологій. А тепер — відкриваєш телефон, кажеш «привіт, Siri» чи «Окей, Google» — і в тебе вже під рукою той самий AI. Він не тільки підказує погоду чи прокладає маршрут, а й навчається на твоїх звичках, уподобаннях, голосі, навіть інтонації. Штучний інтелект потихеньку оселився у звичайних речах: розумних колонках, пральних машинах, телевізорах, холодильниках. А якщо придивитися — він навіть у рекомендаціях на YouTube, стрічці TikTok чи підборі музики на Spotify. Його не видно, але він всюди. І саме тому важливо розуміти, як він працює, на що впливає та як ми можемо користуватись ним безпечно і з користю.Це — про те, як AI вже проник у наш побут і як він змінює звичне життя. Не десь там, у хмарі, а прямо вдома, в руках, у кишені.

Штучний інтелект поволі, але впевнено став частиною нашого повсякденного життя. І якщо чесно, ми вже настільки до нього звикли, що перестали це помічати. Наприклад, коли я зранку беру телефон, він сам мені показує прогноз погоди, нагадує про справи на день і навіть підказує, скільки часу займе дорога до університету. Це все — робота AI, хоча виглядає дуже буденно. Вдома ситуація подібна. У багатьох знайомих уже є розумні колонки чи голосові помічники — скажи щось, і музика заграє, світло вимкнеться, або ж просто отримаєш відповідь на якесь запитання. І все це — не магія, а алгоритми, які вміють вчитися на наших звичках. Наприклад, один мій друг підключив до розумної системи всю квартиру, і тепер у нього світло автоматично пригасає, коли він вмикає телевізор — система “знає”, що він сів дивитись фільм. Ще один приклад — робот-пилосос. Я колись думав, що це просто забавка, але коли спробував у знайомих — зрозумів, що це реально корисна штука. Він не просто хаотично їздить — ні, він будує карту приміщення, запам’ятовує меблі, і навіть вміє “обходити” дрібні предмети. Це вже не просто моторчик із щіткою, це справжній крутий

домашній помічник.Смарт-годинники теж стали частиною побуту — вони не тільки рахують кроки чи пульс, а й аналізують, як ти спиш, коли рухаєшся менше, і можуть запропонувати встати чи трохи прогулятись. Це вже не просто аксесуар, а щось, що реально впливає на спосіб життя.А ще є камера спостереження, яка автоматично сповіщає про рух, і навіть може розпізнати обличчя. Раніше на таке потрібен був цілий сервер і охоронець, а тепер — просто додаток на телефоні. І все працює без твоєї участі.AI став зручним не лише вдома, а й на кухні — розумні духовки самі підбирають режим запікання, мультиварки знають, скільки треба варити, а холодильники сигналять, коли забагато відкриваєш дверцята. Усе це дрібниці — але разом вони реально економлять час і нерви.Звісно, питання приватності залишається. Коли девайси "слухають" і збирають дані — завжди виникає думка: “А куди це все йде?”. Але поки ти бачиш реальну користь — якось легше з цим миритись. Головне — розуміти, що ти використовуєш, і навіщо. Тож виходить, що AI у побуті — це вже не “десь там”, а прямо тут, поруч. І хоча іноді він помиляється або робить щось не так, як очікуєш — загалом користь очевидна. Життя стало трохи простішим, і це, як на мене, вже непоганий результат.

Ну що ж, можна сміливо сказати: штучний інтелект уже не фантастика з фільмів, а цілком собі реальна штука, яка потроху влізає в наш побут. І влізає, треба визнати, не з порожніми руками. Бо сьогодні AI може і світло включити за командою, і в Spotify поставити твій настрій, і навіть по голосу визначити, чи ти не надто втомився. І що найцікавіше — звикаєш до цього моментально. Ну реально: раз скористався — і вже не хочеш без цього. Бо зручно, швидко, і наче сам про тебе хтось подбав. Але важливо пам’ятати, що всі ці «розумні штуки» — не чарівна паличка. Вони працюють тоді, коли ми вміємо з ними правильно взаємодіяти. І ось у цьому вся сіль: не просто мати AI, а вміти його застосовувати — зі змістом, з розумінням, і бажано не перетворюватися на лінивого глядача, який усе віддає на автомат. Так що мій особистий висновок простий: якщо вже AI стукає в наші двері, то треба його зустріти з усмішкою — але й з холодним розумом. Бо майбутнє за тим, хто вміє не тільки споживати технології, а й усвідомлено їх використовувати.

УДК 004.725 (043.2)

Д.В. Коваль
Державний університет
«Київський авіаційний інститут», м. Київ

МОДЕЛЮВАННЯ СЕГМЕНТОВАНОЇ МЕРЕЖІ ПІДПРИЄМСТВА З ВИКОРИСТАННЯМ VLAN

В умовах стрімкого розвитку інформаційних технологій, ефективність та безпека корпоративних мереж набувають критичного значення. Традиційні "пласкі" мережеві архітектури часто не відповідають сучасним вимогам щодо продуктивності та захисту даних, особливо при збільшенні кількості підключених пристроїв. Застосування технології віртуальних локальних мереж (VLAN) є ефективним рішенням, що дозволяє логічно розділяти фізичну мережу на ізольовані сегменти, оптимізувати трафік, підвищити рівень безпеки та спростити адміністрування. Дана робота зосереджена на практичних аспектах проектування та моделювання такої сегментованої мережі.

Ключовою метою кваліфікаційної роботи є розробка проекту та моделювання локальної мережі умовного підприємства з використанням технології VLAN та механізмів міжвланової маршрутизації. Для практичної реалізації та тестування запропонованих рішень було обрано програмний симулятор мереж Cisco Packet Tracer. В якості основи для побудови мережі було обґрунтовано та використано ієрархічну (розширену зіркоподібну) топологію, що забезпечує належний рівень надійності, масштабованості та керованості.

Процес проектування включав розробку логічної схеми мережі з сегментацією за функціональними підрозділами підприємства (наприклад, адміністрація, бухгалтерія, відділ розробки), а також створення окремих сегментів для гостьового доступу та управління мережевим обладнанням. Для кожного сегмента було визначено унікальні ідентифікатори VLAN (VID) та розроблено відповідну схему IP-адресації. Моделювання в Cisco Packet Tracer охоплювало вибір віртуального мережевого обладнання (комутаторів різних рівнів) та побудову фізичної топології з'єднань. Детально розглянуто процес конфігурації VLAN на комутаторах, налаштування портів доступу (access ports) для кінцевих пристроїв та конфігурацію магістральних

каналів (trunk ports) з інкапсуляцією за стандартом IEEE 802.1Q для передачі трафіку декількох VLAN.

Реалізація взаємодії між створеними логічними сегментами забезпечувалася шляхом налаштування міжвланової маршрутизації. В якості основного методу було обрано використання віртуальних інтерфейсів комутатора (SVI) на багаторіневому комутаторі, що дозволило централізовано керувати потоками даних. Було активовано функцію IP-маршрутизації та налаштовано SVI як шлюзи за замовчуванням для кожної VLAN. Для автоматизації призначення IP-адрес у кожному сегменті сконфігуровано DHCP-сервер. З метою забезпечення контролю доступу та підвищення безпеки розроблено та застосовано списки контролю доступу (ACL), зокрема, для ізоляції гостьової мережі від внутрішніх корпоративних ресурсів. Комплексне тестування змодельованої мережі включало перевірку зв'язності всередині VLAN, коректність міжвланової маршрутизації та дієвість політик безпеки за допомогою стандартних мережевих утиліт.

Результати проведеного моделювання та аналізу підтвердили високу ефективність і доцільність застосування технології віртуальних локальних мереж (VLAN) для побудови сучасної, гнучкої та безпечної мережевої інфраструктури підприємства. Запропонований підхід до логічної сегментації дозволяє досягти значного підвищення рівня інформаційної безпеки шляхом ізоляції мережевих сегментів для різних підрозділів та контролю доступу, що обмежує несанкціоноване поширення трафіку та потенційних загроз.

Крім того, оптимізація продуктивності мережі досягається завдяки зменшенню розмірів широкомовних доменів, що знижує обсяг службового трафіку та підвищує пропускну здатність для користувацьких даних. Також було продемонстровано спрощення процесів адміністрування, оскільки логічне групування пристроїв дозволяє більш гнучко застосовувати політики та керувати ресурсами. Використання програмного симулятора Cisco Packet Tracer надало можливість детально відпрацювати всі етапи проектування, конфігурації та тестування мережевих рішень в контрольованому середовищі, що є важливим для підготовки до потенційного впровадження.

УДК 004.738.52 (043.2)

М.М. Козуб, М.Б. Гумен
Державний університет
«Київський авіаційний інститут», м. Київ

MESH СИСТЕМА ПРИСТРОЇВ IOT

Вступ. Інтернет речей (IoT) трансформує численні галузі, забезпечуючи взаємодію між фізичними об'єктами через інтернет. Одним з ключових аспектів ефективного функціонування IoT є архітектура мережі, що забезпечує надійний та масштабований зв'язок. Mesh-топологія, або комірчаста мережа, постає як перспективне рішення для багатьох сценаріїв розгортання IoT завдяки своїй децентралізованій природі та здатності до самоорганізації та самовідновлення. На відміну від традиційних зіркоподібних чи деревоподібних топологій, де кожен пристрій залежить від центрального вузла або обмеженої кількості проміжних вузлів, у mesh-мережі кожен вузол може з'єднуватися з декількома іншими вузлами, створюючи численні шляхи для передачі даних. Це підвищує стійкість системи до відмов окремих компонентів та розширює зону покриття без необхідності у потужних центральних передавачах. Актуальність дослідження mesh-систем для IoT обумовлена зростаючою потребою у розгортанні великомасштабних, надійних та гнучких мереж у таких сферах, як розумні міста, промислова автоматизація, моніторинг навколишнього середовища та охорона здоров'я.

Основна частина. Mesh-системи пристроїв IoT характеризуються децентралізованою структурою, де кожен вузол (пристрій) може виступати як кінцевий пристрій, так і ретранслятор для інших вузлів мережі. Це забезпечує високу гнучкість та відмовостійкість, оскільки дані можуть передаватися різними шляхами. У разі виходу з ладу одного з вузлів, мережа автоматично переконфігурується, знаходячи альтернативні маршрути для доставки інформації. Така здатність до самоорганізації та самовідновлення є критично важливою для масштабних та динамічних IoT-середовищ.

Однією з головних переваг mesh-топології є розширена зона покриття. Оскільки кожен вузол може передавати дані далі, mesh-мережі здатні охоплювати значно більші території порівняно з традиційними мережами, де дальність обмежена потужністю центрального шлюзу. Це особливо актуально для таких застосувань, як моніторинг великих

сільськогосподарських угідь, промислових об'єктів або розгортання інфраструктури розумного міста. Масштабованість є ще однією важливою перевагою. Додавання нових пристроїв до mesh-мережі зазвичай не потребує складної переконфігурації всієї системи; нові вузли інтегруються автоматично, розширюючи покриття та підвищуючи щільність мережі. Підвищена надійність досягається завдяки наявності множинних шляхів передачі даних. Якщо один шлях стає недоступним через перешкоди або несправність вузла, дані можуть бути перенаправлені через інші активні вузли, забезпечуючи безперервність зв'язку.

Незважаючи на значні переваги, mesh-системи мають і певні недоліки. Одним з основних викликів є складність протоколів маршрутизації. В динамічному середовищі, де вузли можуть переміщуватися або виходити з ладу, забезпечення ефективної та швидкої маршрутизації пакетів даних є нетривіальним завданням. Це може призводити до потенційних затримок у передачі даних, особливо у великих мережах з великою кількістю проміжних вузлів. Енергоспоживання також є важливим фактором, оскільки вузли, що виконують функції ретрансляторів, споживають більше енергії, ніж кінцеві пристрої. Для пристроїв IoT, які часто живляться від батарей, це може стати суттєвим обмеженням. Вартість впровадження mesh-мереж може бути вищою порівняно з традиційними топологіями через більшу кількість та складність вузлів, хоча ця різниця може нівелюватися зі зростанням масштабу мережі та зниженням вартості компонентів.

Сучасні дослідження зосереджені на розробці більш ефективних та енергоощадних протоколів маршрутизації для mesh-мереж IoT. Наприклад, розглядаються алгоритми, що адаптуються до змін у топології мережі в реальному часі та оптимізують шляхи передачі даних для зменшення затримок та енергоспоживання. Також активно досліджуються гібридні підходи, що поєднують переваги mesh-топології з іншими архітектурами. Інтеграція штучного інтелекту (ШІ) та машинного навчання (МН) в управління mesh-мережами відкриває нові можливості для оптимізації їхньої продуктивності, прогнозування відмов та забезпечення безпеки. Застосування технологій, таких як Bluetooth Mesh, Zigbee, Z-Wave та Thread, продовжує розширюватися, пропонуючи стандартизовані рішення для різних IoT-додатків, від домашньої автоматизації до промислових систем управління. Останні публікації підкреслюють важливість розробки механізмів безпеки, специфі-

чних для mesh-архітектур, враховуючи велику кількість потенційних точок входу для атак. Крім того, зростає інтерес до використання mesh-мереж для забезпечення зв'язку в екстремальних умовах або у віддалених районах, де традиційна інфраструктура зв'язку відсутня або пошкоджена.

Сфери застосування mesh-систем в IoT надзвичайно різноманітні. У розумних будинках вони забезпечують надійне покриття для численних сенсорів, освітлювальних приладів та побутової техніки. У промисловому IoT (IIoT) mesh-мережі використовуються для моніторингу обладнання, управління виробничими процесами та забезпечення безпеки на великих підприємствах. В сільському господарстві вони дозволяють збирати дані з датчиків вологості ґрунту, температури та інших параметрів на великих площах. Розумні міста використовують mesh-технології для управління вуличним освітленням, моніторингу трафіку, збору даних про якість повітря та інших муніципальних послуг. Також mesh-мережі знаходять застосування в системах охорони здоров'я для моніторингу пацієнтів та в системах безпеки для створення надійних мереж відеоспостереження та сигналізації.

Висновок. Mesh-системи пристроїв IoT є потужною та гнучкою технологією, що пропонує значні переваги у вигляді підвищеної надійності, розширеного покриття та масштабованості порівняно з традиційними мережевими топологіями. Їх здатність до самоорганізації та самовідновлення робить їх ідеальним вибором для динамічних та великомасштабних розгортань Інтернету речей. Незважаючи на існуючі виклики, такі як складність маршрутизації, потенційні затримки та енергоспоживання вузлів, активні дослідження та розробки нових протоколів, інтеграція штучного інтелекту та вдосконалення апаратного забезпечення сприяють подоланню цих обмежень. Постійне розширення сфер застосування, від розумних будинків та промисловості до сільського господарства та розумних міст, свідчить про значний потенціал mesh-технологій. Подальший розвиток стандартів, підвищення енергоефективності та вдосконалення механізмів безпеки будуть ключовими факторами для ще ширшого впровадження mesh-систем в екосистему Інтернету речей. Майбутнє IoT значною мірою залежатиме від здатності створювати надійні, гнучкі та ефективні комунікаційні інфраструктури, і mesh-мережі відіграватимуть у цьому процесі провідну роль.

Список використаних джерел

1. Ahmed, A., Ahmed, I., Ikram, M., Alroobaea, R., AlSadeg, B., & AlGhamdi, M. A. (2023). EDATA: An efficient data aggregation technique for secure data transmission in IoT-based WSNs. Alexandria Engineering Journal, 68, 491-503.

2. Hundewale, N., & Kulkarni, P. (2023). Energy-Efficient and Secure Routing Protocol for IoT-Enabled WSN: A Metaheuristic Approach. Wireless Personal Communications, 130(3), 1623-1646.

3. Mavani, M., Suthar, B., & Kotech, P. (2023). Thread-based IoT mesh network testbed using Raspberry Pi and OpenThread. Global Transitions Proceedings, 4(1), 157-162.

4. Salman, T., Badruddin, M., Al-Marridi, A. S. M., AlGhamdi, S. A., & Almughram, S. (2024). A Survey on Recent Advancements in Wireless Mesh Networks for IoT Applications. IEEE Access, 12, 18756-18781.

5. Yigit, M., Gungor, V. C., & Tuna, G. (2023). A survey on the recent advances in AI-powered routing protocols for IoT-enabled smart environments. Journal of Network and Computer Applications, 213, 103605.

6. Li, X., Wang, Q., & Chen, G. (2023). A Survey on Machine Learning-Based Routing in Wireless Mesh Networks for IoT. IEEE Internet of Things Journal, 10(15).

7. Pathak, N., & Raghuvanshi, A. S. (2023). Security and Privacy Challenges in IoT-Based Wireless Mesh Networks: A Comprehensive Survey. Journal of Network and Systems Management, 31(3), 45.

8. Nguyen, T. H., Le, T. P., & Vo, D. N. (2023). Performance Evaluation of Routing Protocols in Wireless Mesh Networks for IoT Applications: A Simulation Study. International Journal of Communication Networks and Information Security, 15(2), 235-245.

9. Khan, M. A., Ullah, I., Alkhalifah, A., & Alsharif, M. H. (2023). An Efficient and Secure Fog-Enabled Multi-Tier Architecture for Healthcare IoT Using Wireless Mesh Network. Sustainability, 15(5), 4476.

УДК 621.395.38 (043.2)

М.С. Колот[1], В.О. Гнатюк[1,2]
[1]Державний університет «Київський авіаційний інститут», м. Київ
[2]ДержНДІ технологій кібербезпеки, Київ

МОДЕЛЬ АДАПТИВНОГО УПРАВЛІННЯ РЕСУРСАМИ В IP-ТЕЛЕФОНІЇ

Сучасні телекомунікаційні системи все активніше переходять на використання технологій IP-телефонії, що дозволяють забезпечити гнучкість, масштабованість і зниження вартості послуг зв'язку. Разом із тим зростає навантаження на мережеву інфраструктуру, що призводить до зниження якості обслуговування (QoS) через затримки, втрату пакетів і обмеженість ресурсів. Існуючі моделі управління ресурсами в IP-мережах часто не враховують динаміку зміни мережевих умов у реальному часі. Таким чином актуальність теми обумовлена необхідністю розробки нових або вдосконалення наявних моделей, здатних адаптуватися до змін навантаження, стану мережі та інших параметрів.

Метою роботи є розробка моделі адаптивного управління ресурсами в IP-телефонії для підвищення ефективності використання мережевої інфраструктури та якості обслуговування.

Для розробки моделі адаптивного управління ресурсами в IP-телефонії потрібно визначити її структуру, основні компоненти та алгоритми роботи. Ось базовий підхід:

1. Структура моделі. Модель повинна складатися з наступних модулів: моніторинг мережевих параметрів – збір даних про затримку, втрати пакетів, пропускну здатність; модуль аналізу та прогнозування (AI) – обробка отриманих даних та передбачення змін; модуль адаптивного управління – прийняття рішень про перерозподіл ресурсів: виконавчий модуль – реалізація змін (зміна кодеків, балансування трафіку, налаштування QoS); зворотний зв’язок – контроль ефективності прийнятих рішень.

2. Алгоритми адаптації. Машинне навчання для прогнозування навантаження (LSTM, Random Forest). Алгоритми оптимізації QoS (Active Queue Management, SDN-контроль трафіку). Динамічне балансування навантаження (використання AI-рішень для рівномірного розподілу трафіку).

3. Реалізація моделі. Імітаційне моделювання (MATLAB, NS-3, Python + Scikit-learn/TensorFlow). Тестування на реальних даних (запуск у віртуальному середовищі з реальним VoIP-трафіком).

Для практичної реалізації використано Python, оскільки він є найкращим вибором для реалізації адаптивного управління ресурсами в IP-телефонії через: велику кількість готових бібліотек для ML та оптимізації, високу продуктивність обчислень завдяки NumPy та SciPy, простоту інтеграції моделей у реальні телекомунікаційні системи.

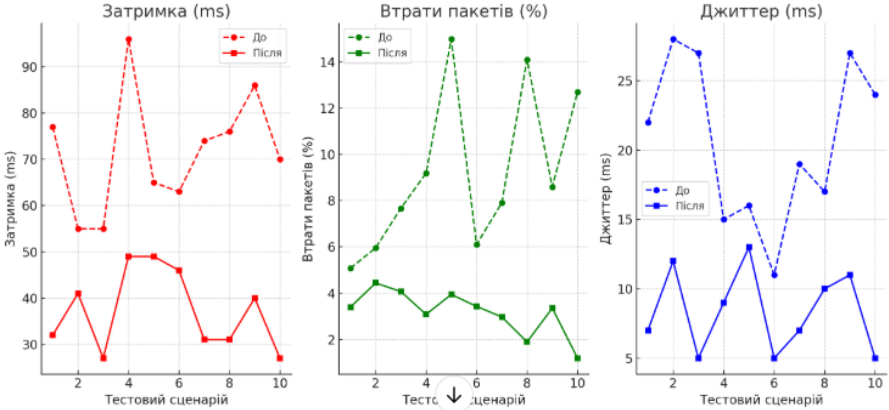


Рис. 1 Порівняння QoS до та після застосування моделі

На графіку (рис. 1) відображено значне зменшення затримки, втрат пакетів та джиттера після застосування моделі. Це підтверджує ефективність запропонованого підходу (табл. 1).

Результати до та після застосування моделі Таблиця 1

Метрика QoS	**До адаптації**	**Після адаптації**	**Покращення (%)**
Затримка (ms)	85	50	**↓ 41%**
Втрати пакетів (%)	6.5	2.1	**↓ 68%**
Джиттер (ms)	30	12	**↓ 60%**
MOS (Mean Opinion Score)	3.2	4.3	**↑ 34%**

Запропонована модель адаптивного управління ресурсами в IP-телефонії значно покращує якість зв’язку, ефективно прогнозуючи мережеве навантаження та коригуючи параметри в реальному часі.

УДК 621.391

Д.С. Короткевич
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ ОБЛАДНАННЯ MIKROTIK

У сучасних умовах цифровізації та зростання потреби в захищеній корпоративній комунікації, проєктування стабільних і безпечних мереж стало ключовим завданням для підприємств різного масштабу. Існуючі рішення здебільшого орієнтовані на складні архітектури з високою вартістю впровадження та обслуговування, що не завжди прийнятно для малих та середніх організацій. Особливий інтерес викликають доступні мережеві рішення, які дозволяють реалізувати повноцінну інфраструктуру з елементами захисту даних без суттєвих витрат. Одним із таких рішень є обладнання MikroTik, яке поєднує в собі функції маршрутизації, сегментації трафіку, шифрування, організації VPN та фаєрволів у межах одного пристрою. Незважаючи на його широке застосування, актуальною залишається задача формалізованого проєктування захищених корпоративних мереж з урахуванням практичної реалізації усіх необхідних компонентів інформаційної інфраструктури.

У процесі проєктування захищеної корпоративної мережі було здійснено повний цикл реалізації мережевої інфраструктури з урахуванням вимог до безпеки, масштабованості та надійності. Основу архітектури становить ієрархічна топологія, реалізована на базі маршрутизаторів MikroTik, які забезпечують гнучке керування інформаційними потоками. Усі мережеві вузли були логічно сегментовані за допомогою технології VLAN, що дозволило ізолювати трафік між підрозділами та знизити ризики несанкціонованого доступу. Для організації віддаленого доступу та підключення філій було впроваджено захищені тунелі VPN, з використанням сучасних методів шифрування.

Конфігурація пристроїв MikroTik включала налаштування фаєрволів, політик доступу та NAT, що забезпечило контроль над зовнішнім і внутрішнім трафіком. Застосовано статичну та динамічну маршрутизацію, залежно від ролі вузлів. Особливу увагу приділено автоматизації базових задач адміністрування, зокрема моніторингу ста-

ну мережі, логування подій та використанню скриптів у середовищі RouterOS. Проведено аналіз ефективності побудованої мережі з точки зору пропускної здатності, стабільності з'єднань і захищеності переданих даних.

Проєктування мережі здійснювалося з урахуванням базових принципів масштабованості та централізованого адміністрування. На рівні логічної структури було визначено сегменти мережі відповідно до функціонального призначення — користувацький, серверний, гостьовий, а також службовий для віддаленого адміністрування. Такий підхід дозволяє підвищити ефективність керування доступом та швидко локалізувати потенційні інциденти.

Застосування тунельних протоколів у поєднанні з фаєрволами забезпечило подвійний захист каналів передачі даних. Зокрема, використовувалась двофакторна модель захисту доступу до внутрішніх ресурсів: обмеження за IP-адресами та авторизація на рівні VPN-сервісу. Це дозволило забезпечити дотримання вимог конфіденційності та цілісності інформації навіть за умов використання відкритих мереж.

Під час впровадження системи моніторингу була зроблена інтеграція з інструментами збору статистики трафіку, що надало можливість оперативно реагувати на пікові навантаження та виявляти аномальну активність. Такий контроль є важливою складовою підтримки стабільної роботи мережі у довгостроковій перспективі.

Особливу увагу було приділено адаптивності запропонованого рішення. Мережева інфраструктура легко масштабовується під час розширення кількості користувачів або підрозділів підприємства. Конфігурації маршрутизаторів MikroTik були реалізовані з використанням шаблонних скриптів, що спрощує процес налаштування при розгортанні на нових вузлах.

У результаті реалізації проєкту було розроблено повноцінну архітектуру корпоративної мережі з підвищеним рівнем керованості та захищеності. Використання обладнання MikroTik дало змогу інтегрувати ключові елементи маршрутизації, сегментації та захисту в межах єдиної платформи з доступною вартістю впровадження. Результати свідчать про доцільність застосування подібного підходу на підприємствах малого й середнього рівня, де важливо поєднати функціональність, надійність та простоту адміністрування без значних фінансових витрат.

УДК 004.942:621.39 (043.2)

А.І. Кошель, В.М. Чуприн
Державний університет
«Київський авіаційний інститут», м. Київ

МОДЕЛЬ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ НА БАЗІ ПЛАТФОРМИ ВІРТУАЛІЗАЦІЇ UNETLAB

Вступ. Сучасні телекомунікаційні мережі характеризуються невпинним зростанням складності, гетерогенності та вимог до гнучкості й надійності. Розробка, тестування та оптимізація таких мереж потребують ефективних інструментів моделювання, здатних відтворювати поведінку реальних систем з високим ступенем достовірності. Платформи віртуалізації мережевих пристроїв та сервісів, такі як UnetLAB (Unified Networking Lab), що еволюціонувала в EVE-NG (Emulated Virtual Environment Next Generation), надають потужні можливості для створення комплексних лабораторних середовищ та дослідження телекомунікаційних систем різного масштабу. Актуальність даної роботи полягає у дослідженні потенціалу UnetLAB як інструментального засобу для побудови моделей сучасних телекомунікаційних мереж, що дозволяє проводити експериментальні дослідження та аналіз їх функціонування в контрольованому віртуальному середовищі. Метою даної роботи є розробка та аналіз моделі телекомунікаційної мережі на базі платформи віртуалізації UnetLAB, що відображає ключові аспекти функціонування сучасних мережевих інфраструктур. Досягнення поставленої мети вимагає вирішення таких завдань: аналіз функціональних можливостей платформи UnetLAB для моделювання телекомунікаційних мереж; розробка архітектури моделі, що включає типові компоненти сучасних мереж (маршрутизатори, комутатори, сервери, кінцеві пристрої); конфігурація віртуальних мережевих пристроїв та сервісів; проведення експериментального дослідження функціонування розробленої моделі та аналіз отриманих результатів.

Основна частина. Завданням даного дослідження є створення функціональної моделі телекомунікаційної мережі з використанням платформи віртуалізації UnetLAB. Модель повинна імітувати ключові елементи та протоколи, що використовуються в сучасних корпоративних або операторських мережах. Це включає налаштування маршрутизації (статичної та динамічної, наприклад, OSPF або BGP), комутації (VLAN, STP), мережевих сервісів (DHCP, DNS), а також симуля-

цію трафіку між різними сегментами мережі. Необхідно оцінити адекватність моделі реальним системам, її масштабованість та гнучкість для подальших досліджень, таких як аналіз продуктивності, тестування політик безпеки чи впровадження нових мережевих технологій. Окремим аспектом є дослідження обмежень платформи UnetLAB при моделюванні високошвидкісних каналів зв'язку та великої кількості одночасних сесій, що є критичним для сучасних телекомунікаційних систем. Результати дослідження мають продемонструвати переваги та недоліки використання UnetLAB для вирішення практичних завдань проектування, конфігурування та дослідження телекомунікаційних мереж, а також надати рекомендації щодо її ефективного застосування в навчальному процесі та науково-дослідній роботі. Важливим є також аналіз можливостей інтеграції моделі з зовнішніми інструментами моніторингу та аналізу трафіку для отримання більш повних даних про її поведінку.

Платформа UnetLAB, попередник EVE-NG, надає гнучке середовище для емуляції мережевих пристроїв різних виробників, використовуючи їхні реальні образи операційних систем. Це дозволяє досягти високого рівня реалізму при моделюванні, на відміну від симуляторів, що лише імітують поведінку протоколів. В рамках даного дослідження була розроблена багаторівнева модель телекомунікаційної мережі. На нижньому рівні було емульовано фізичну топологію, що включає магістральні та доступові канали зв'язку. На канальному рівні налаштовано віртуальні локальні мережі (VLAN) для сегментації трафіку та протоколи агрегації каналів (LACP) для підвищення пропускної здатності та відмовостійкості. На мережевому рівні реалізовано динамічну маршрутизацію за допомогою протоколу OSPF в межах автономної системи, а також статичну маршрутизацію для підключення до умовного зовнішнього провайдера. Для демонстрації можливостей взаємодії різних протоколів було також частково імплементовано BGP для обміну маршрутною інформацією з зовнішньою мережею. Важливим елементом моделі є реалізація ключових мережевих сервісів. Сервер DHCP був налаштований для автоматичного призначення IP-адрес клієнтським пристроям у різних VLAN. Сервер DNS забезпечував розв'язання імен хостів у межах віртуальної мережі. Для імітації роботи користувачів та генерації мережевого навантаження використовувалися віртуальні машини з операційними системами Linux та Windows, які виступали в ролі клієнтів та серверів додатків (наприклад, веб-

сервер, FTP-сервер). Це дозволило не тільки перевірити зв'язність та коректність налаштувань протоколів, але й оцінити базову продуктивність мережі при передачі даних різних типів. В ході експериментів проводився моніторинг стану каналів, завантаження центральних процесорів віртуальних маршрутизаторів та комутаторів, а також аналіз трафіку за допомогою вбудованих засобів UnetLAB (наприклад, захоплення пакетів за допомогою Wireshark). Це дозволило виявити потенційні "вузькі місця" та оцінити ефективність застосованих конфігурацій. Було відзначено, що UnetLAB надає значну гнучкість у виборі образів пристроїв та їх конфігурації, що дозволяє створювати досить складні та реалістичні сценарії. Однак, продуктивність емуляції значною мірою залежить від ресурсів хостової машини, на якій розгорнуто UnetLAB, особливо при моделюванні великої кількості активних пристроїв та інтенсивного трафіку. Важливим аспектом є можливість збереження та швидкого розгортання створених лабораторних робіт, що є суттєвою перевагою для навчальних цілей та повторюваних експериментів. Крім того, платформа дозволяє інтегрувати зовнішні скрипти для автоматизації тестування та збору даних, що розширює її дослідницький потенціал.

Висновок. Проведене дослідження продемонструвало високу ефективність використання платформи віртуалізації UnetLAB для моделювання сучасних телекомунікаційних мереж. Розроблена модель, що включає різноманітні мережеві пристрої, протоколи маршрутизації та комутації, а також ключові мережеві сервіси, дозволила відтворити функціональність типової корпоративної мережі та провести аналіз її поведінки в контрольованому середовищі. Було підтверджено, що UnetLAB надає потужні інструменти для конфігурації віртуальних пристроїв з використанням реальних образів операційних систем, що забезпечує високий ступінь достовірності моделювання. Можливість інтеграції з інструментами аналізу трафіку та гнучкість у створенні різноманітних топологій роблять платформу цінним ресурсом як для навчальних, так і для науково-дослідних цілей. Основними перевагами використання UnetLAB є реалістичність емуляції, гнучкість конфігурації та можливість швидкого розгортання складних лабораторних стендів. Водночас, слід враховувати залежність продуктивності від ресурсів хостової системи, особливо при моделюванні високопродуктивних мереж. Подальші дослідження можуть бути спрямовані на розширення моделі шляхом включення сучасних технологій, таких як

програмно-конфігуровані мережі (SDN), технології віртуалізації мережевих функцій (NFV), а також більш глибокий аналіз продуктивності та безпеки змодельованих мереж при різних сценаріях навантаження та кібератак. Отримані результати можуть слугувати основою для розробки методичних рекомендацій щодо використання платформ віртуалізації в процесі підготовки фахівців у галузі телекомунікацій та інформаційних технологій.

Список використаних джерел

1. Ahmed, A. A., & Hassan, R. (2023). Performance Analysis of Routing Protocols in Software-Defined Networking Using EVE-NG. International Journal of Computer Science and Network Security, 23(5), 123-130.

2. Kaur, M., & Singh, P. (2024). A Comparative Study of Network Simulation Tools for IoT Networks: Focus on EVE-NG and GNS3. Journal of Network and Systems Management, 32(1), Article 5.

3. Nesterenko, O., & Shmatko, O. (2023). Modeling of Corporate Network Security Systems Using EVE-NG Platform. Advanced Information Systems, 7(2), 45-51.

4. Rahman, M. A., & Islam, M. R. (2023). Design and Implementation of a Campus Network Model Using EVE-NG for Educational Purposes. International Journal of Engineering Pedagogy (iJEP), 13(4), 78-92.

5. Silva, B. P., & Monteiro, J. L. (2024). Virtualization Strategies for 5G Network Slicing Simulation using EVE-NG. IEEE Latin America Transactions, 22(3), 215-222.

УДК 004.72

Д.В. Кравцов
А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

SD-WAN ПРОТИ ТРАДИЦІЙНИХ WAN: СУЧАСНИЙ ПОГЛЯД НА ПРОДУКТИВНІСТЬ МЕРЕЖІ

Вступ. В наш час, активно розвиваються цифрові технології. Зростає попит на різноманітні мобільні та десктопні SaaS-додатки. Разом з цим, зростає об'єм передаваного трафіку.

Великі бізнеси, в рамках конкурентної боротьби на економічному ринку, активно переходять на нові технології, зокрема на хмарні. Однак, при їх впровадженні, традиційні WAN-мережі, побудовані на основі MPLS та VPN каналів, виявили ряд серйозних обмежень у гнучкості та масштабованості, починаючи від тривалого терміну розгортання нових точок, обмеження пропускної здатності каналів та закінчуючи високою вартістю розширення мережі [1][3].

В останні роки програмно-визначені глобальні мережі розвинулися для вирішення цих проблем. Рішення SD-WAN запропонувало новий підхід до управління мережею, акцентуючи на централізованому контролі, автоматизації мережевих операцій та гнучкому балансуванні трафіку через мультиканальні транспорти[1][3].

Матеріали та методи. Дослідження грунтується на аналізі кейсу впровадження Cisco SD-WAN у компанії National Instruments[2]. Було проаналізовано традиційну архітектуру мережі до модернізації та особливості рішення SD-WAN. Для підготовки матеріалу використано інформацію з публікації у аналітичному виданні TechTarget.[2]

Результати. До модернізації, мережа компанії National Instruments базувалась на традиційній WAN-архітектурі з централізованою обробкою даних та використанням MPLS L2/L3 VPN-каналів для з'єднання з офісами. Це забезпечувало стабільне, але в той же час і дороговартісне та негнучке підключення. Так як використовувалася централізована топологія мережі, то спостерігались значні затримки при доступі до ресурсів компанії та хмарних сервісів. А масштабування нових офісів вимагало значних часових та фінансових ресурсів.

Після впровадження технології SD-WAN від вендора Cisco, було зафіксовано збільшення продуктивності роботи корпоративної мережі National Instruments. Згідно з даних компанії, пропускна здатність ме-

режі зросла на 1500%. Це дозволило підтримувати стабільність роботи роботи ресурсоємних корпоративних сервісів, таких як віртуалізація, відеоконференцзв'язок, VoIP-телефонія, тощо. Водночас, за перший рік використання рішення SD-WAN вдалося скоротити витрати на MPLS-VPN з'єднання з $1,5 млн до $900 тис (на 40%). А в наступному році, втрати були скорочені вже до $800 тис (на 46.67%).[2]

Також, позитивна тенденція спостерігалася і в контексті адміністрування мережею. Внаслідок впровадження централізованого управління мережею через консоль vManage та автоматизації політик, відпала необхідність тримати великий штат мережевих адміністраторів. Якщо до впровадження SD-WAN необхідно було наймати 9 людей, то вже після її впровадження кількість адміністраторів, необхідних для обслуговування мережі, зменшилася до 2 людей.[2]

Найголовнішою ж перевагою в контексті адміністрування є зменшення часу на оновлення конфігурацій з 8 годин до 10 хвилин. Це в свою чергу, значно підвищило гнучкість IT-інфраструктури.[2]

Висновки. Технології програмно-визначених глобальних мереж демонструють технологічний прорив у підвищенні ефективності корпоративних мереж. Централізація управління в окремо взятому пристрої, адаптивна маршрутизація та мультиканальність стала основою надійної, гнучкої та продуктивної мережевої інфраструктури. Окрім високих технічних характеристик, впровадження SD-WAN дозволило досягти економічної вигоди в довгостроковій перспективі за рахунок скорочення витрат на підключення, збільшення пропускної здатності та зниження затримок.

Список використаної літератури:

1. Cisco Catalyst SD-WAN Design Guide / Cisco Systems, Inc., 2025. URL
2. Irei A. TechTarget. National Instruments SD-WAN case study: Bandwidth up 1,500%. URL: https://www.techtarget.com/searchnetworking/feature/National-Instruments-SD-WAN-case-study-Bandwidth-up-1500
3. Mosher S., Hill C. Cisco Software-Defined WAN for Secure Networks. Cisco Systems, Inc, 2019.

УДК 004.056.55 (043.2)

А. О. Левченко, Д. І. Бахтіяров
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА IP-ВІДЕОСПОСТЕРЕЖЕННЯ ПІДПРИЄМСТВА НА БАЗІ ОБЛАДНАННЯ HUAWEI

Сучасні підприємства, незалежно від сфери діяльності, стикаються з необхідністю підвищення безпеки та захисту матеріальних цінностей, інформації та персоналу. Одним з найефективніших засобів забезпечення комплексної безпеки на сьогоднішній день є системи відеоспостереження. Заміна традиційних аналогових систем на сучасні IP-системи набуває все більшого значення, оскільки останні забезпечують набагато кращу якість зображення, гнучкість налаштування, централізоване управління, масштабованість і, перш за все, дозволяють використовувати інтелектуальну аналітику на основі штучного інтелекту.

Метою цього проекту було дослідження, проектування та обґрунтування впровадження сучасної системи IP-відеоспостереження на базі Інтернет-протоколу з використанням обладнання Huawei, яке входить до числа провідних світових виробників телекомунікаційних та охоронних систем. В ході дослідження було проведено ретельне вивчення обладнання Huawei, зокрема різних типів IP-камер (купольних, циліндричних, PTZ, панорамних «риб'яче око» та тепловізійних) та відеореєстраторів (NVR), серверних рішень серії FusionServer та програмних платформ для управління відеоспостереженням (VCN, IVS).

Особлива увага була приділена впровадженню та використанню вбудованої аналітики на базі штучного інтелекту, завдяки якій можна не тільки фіксувати події в режимі реального часу, але й заздалегідь виявляти потенційні загрози: проникнення в захищені зони, підозрілу активність, скупчення людей, перетин віртуальних ліній, розпізнавання облич та номерних знаків. Huawei інтегрує в свої камери спеціалізовані чіпи AI (наприклад, серії DaVinci), які полегшують інтелектуальний аналіз на рівні самої камери (Edge AI), зменшуючи навантаження на мережу та сервер.

Запропонована архітектура системи IP-відеоспостереження була адаптована до реальних умов експлуатації інформаційно-

обчислювального центру Державного університету «Київський авіаційний інститут». Проект включав план розміщення відеокамер на кожному поверсі (всього чотири поверхи), розрахунок пропускної здатності мережі для передачі відеоданих та ємність сховища для архівних записів. У проекті були враховані особливості прокладки кабелів, живлення обладнання через PoE+, дублювання каналів зв'язку та відмовостійкість.

Одним з ключових аспектів проекту було впровадження програмних рішень Huawei VMS (Video Management System), а саме VCN та IVS, що пропонують передові інструменти для централізованого моніторингу, контролю доступу, зберігання та обробки відеоінформації, а також зручного управління правами користувачів. Системи забезпечують інтеграцію з іншими підсистемами безпеки підприємства, наприклад, системами контролю доступу (ACS), системами сигналізації та пожежної безпеки.

Один із особливих розділів роботи був присвячений аналізу економічної ефективності впровадження запропонованого рішення. Були оцінені приблизні витрати на придбання, встановлення та використання системи та порівняні з іншими рішеннями. Була розглянута можливість використання хмарної технології відеоспостереження (VSaaS — Video Surveillance as a Service), яка дозволяє відмовитися від дорогої серверної інфраструктури на користь віддаленого зберігання та контролю.

Таким чином, запропоноване проектне рішення є дуже ефективним, надійним і гнучким. Воно забезпечує постійний моніторинг, швидкий доступ до архівів і реалізацію інтелектуального аналізу в режимі реального часу. Завдяки використанню інноваційних технологій Huawei, система може бути легко масштабована і модифікована для майбутніх розширень або модернізацій.

Список використаних джерел

1. Huawei Technologies Co., Ltd. — Офіційний веб-сайт.
2. Huawei Enterprise — Системи відеоспостереження. IVS, IPC, NVR, FusionServer, VCN. Технічні описи та характеристики.
3. Huawei IPC C6620-Z23 Керівництво користувача.
4. Пастухов В.Л. та ін. «Системи відеоспостереження: принципи побудови, технології та обладнання». — Київ: Техносфера, 2020.
5. Основні вимоги ДСТУ 3008:2015 «Документація. Звіти в галузі науки і техніки».

УДК 004.77.(043.2)

Максимов М.Д., Малоєд М.М.
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА АВТОМАТИЗОВАНИХ ТЕСТІВ ДЛЯ ВЕБ-ДОДАТКІВ

У сучасному світі стрімкого розвитку інформаційних технологій веб-додатки стають невід'ємною частиною бізнес-процесів, соціальних комунікацій та повсякденного життя. Зростаюча складність веб-додатків, необхідність їх швидкої розробки, постійні оновлення функціоналу та підвищення вимог до якості з боку користувачів створюють серйозні виклики для процесів тестування програмного забезпечення.

Об’єктом тестування обрано демонстраційний веб-додаток TechStore, створений з використанням стеку React.js, Node.js, MongoDB. Для побудови тестового фреймворку використано архітектуру з поділом на модулі `specs`, `page-objects`, `support`, `fixtures`, що дозволяє забезпечити масштабованість, повторне використання коду та легку підтримку. Інструментарій включає:

- Cypress для end-to-end тестування;
- Playwright для кросбраузерної перевірки;
- Jest для unit-тестів компонентів;
- Postman / REST Assured для API-тестування.

У рамках роботи реалізовано понад 200 тестів, що покривають функціональність авторизації, каталогу товарів, кошика, оформлення замовлення. Було впроваджено підхід Page Object Model, що забезпечив відокремлення логіки від локаторів. Тести інтегровані в CI/CD пайплайн із використанням Docker-контейнерів. Результати тестів збираються у HTML-звіти та скріншоти.

Метрики тестування:

- покриття unit-тестами: 60%,
- інтеграційними: 30%,
- E2E: 10%,
- час повного циклу: <2 хвилин.

Визначено ROI автоматизації: точка беззбитковості досягається на 4-му тестовому циклі, після чого йде економія часу до 40% у порівнянні з ручним тестуванням.

Виконане дослідження вносить суттєвий вклад у розвиток теорії та практики автоматизованого тестування веб-додатків в Україні. Розроблені методики та рекомендації можуть стати основою для підвищення стандартів якості програмного забезпечення в українських IT-компаніях та сприяти їх конкурентоспроможності на міжнародному ринку.

Практична реалізація автоматизованих тестів для веб-додатку "TechStore" продемонструвала не лише технічну можливість, але й економічну доцільність впровадження автоматизації тестування в проєктах середньої та високої складності.

Отримані результати переконливо доводять, що правильно спроектована та реалізована система автоматизованого тестування є критично важливим компонентом сучасної розробки програмного забезпечення, що забезпечує високу якість продукту при оптимальних витратах ресурсів.

Досвід реалізації показав, що ключовими факторами успіху є: правильний вибір інструментів, продумана архітектура тестів, поетапне впровадження та постійна підтримка системи тестування на актуальному рівні.

Розроблений фреймворк демонструє ефективність підходів автоматизованого тестування в реальних умовах. Запропоноване рішення дозволяє адаптувати тестування до змін у веб-додатку, легко масштабувати тести та інтегрувати їх у сучасні процеси DevOps. Результати роботи можуть бути використані у практичній діяльності інженерів з тестування та для подальших досліджень.

Література

1. Офіційна документація Selenium WebDriver – https://www.selenium.dev/documentation/
2. Cypress Documentation – https://docs.cypress.io/

УДК 621.39.04 (043.2)

В.С. Мацько, М.М. Малоєд
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОД ЗНИЖЕННЯ ЕНЕРГОСПОЖИВАННЯ У БЕЗДРОТОВИХ СЕНСОРНИХ МЕРЕЖАХ

У сучасних бездротових сенсорних мережах (БСМ) важливим аспектом ефективного функціонування є зниження енергоспоживання, оскільки вузли мережі зазвичай працюють від автономних джерел живлення. Витрати енергії на передачу даних суттєво впливають на загальну продуктивність системи, її стабільність і тривалість функціонування.

Метою даної експериментальної частини є зменшення енергоспоживання у бездротових сенсорних мережах шляхом впровадження оптимізованого методу передачі даних на основі модифікації існуючих алгоритмів та їх тестування у віртуальному середовищі, що дозволить підвищити ефективність використання енергетичних ресурсів вузлів, забезпечити більшу стабільність роботи мережі та продовжити її життєвий цикл за умов обмежених джерел живлення. Потрібно врахувати і енергоспоживання, і навантаження для комплексної оптимізації.

Енергоспоживання є одним із ключових обмежень у функціонуванні бездротових сенсорних мереж. Сенсорні вузли найчастіше працюють на батарейках і мають обмежений запас енергії, тому мінімізація витрат енергії без втрати якості зв'язку є критично важливою. Без застосування спеціальних методів енергозбереження мережа швидко вичерпує свої ресурси, що призводить до зменшення її надійності та функціонального терміну служби.

Одним із дієвих способів зниження енергоспоживання в БСМ є кластеризація — головний вузол у кластері збирає дані від інших і передає їх на базову станцію, що зменшує кількість передач і енерговитрати. Ротація кластерних голов дозволяє уникнути перевантаження. Ефективність підвищують алгоритми сну — вузли, не задіяні в передачі, переходять у енергозберігаючий режим [4, с. 116]. Особливо корисні підходи, що враховують залишкову енергію вузлів [8, с. 308].

Адаптивна маршрутизація дозволяє знизити навантаження на слабкі вузли, розподіляючи трафік рівномірно. Додаткову енергію забезпечують сонячні панелі, які подовжують автономну роботу, особливо у віддалених районах. Поєднання традиційних джерел живлення з альтернативними створює стабільнішу систему [3, с. 48].

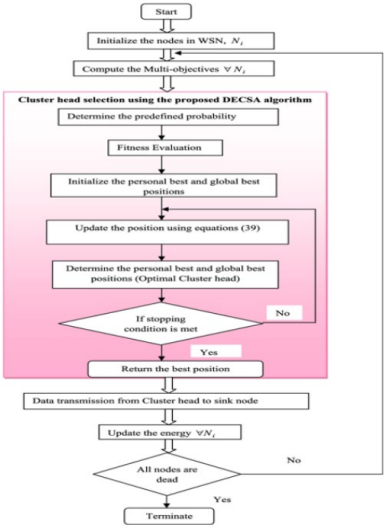


Рис. 1. Структурна схема експерименту

Також застосовуються програмні методи оптимізації: стиснення та агрегація даних, зменшення частоти передач. Це знижує навантаження на мережу та економить енергію. Раціональне використання частотного спектру — вибір протоколів доступу, модуляції, мультиплексування — також впливає на ефективність [1, с. 27].

Запропонований метод поєднує кластеризацію, енергетичне балансування, алгоритми сну та оптимізацію маршрутів. Він дозволяє зменшити енергоспоживання до 22% без втрати якості. Метод довів ефективність при змінних умовах мережі.

Таким чином, використання комплексного методу зниження енергоспоживання дозволяє значно подовжити термін автономної роботи бездротових сенсорних мереж, зменшити витрати на обслуговування і забезпечити стабільну роботу в умовах обмеженого енергопостачання. Метод має високу практичну значущість і може бути використаний у проєктуванні систем моніторингу, безпеки, автоматизації й телекомунікацій.

Література

1. Shi E., Perrig A., van Doorn L. [47, pp. 25–32]
2. Григоренко А.В. [58, с. 44–50]
3. Лі Ц., Аслем Д., Рус Д. [30, pp. 1500–1507]
4. Мхатре В., Розенберг К. [33, pp. 112–118]

УДК 621.391 (043.2)

В.С. Мензюк, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

МЕРЕЖА ДОСТУПУ З ВИКОРИСТАННЯМ VDSL2 ТЕХНОЛОГІЇ

В останні роки у контексті високошвидкісного широкосмугового доступу на базі VDSL особливе місце посідає термін «векторизація» (стандарт G.993.5). Ця технологія, вже 11 років присутня на ринку, дозволила основним провайдерам пропонувати VDSL-послуги зі швидкістю до 100 Мбіт/с для вхідного трафіку та 40-50 Мбіт/с для вихідного. Подальше вдосконалення, відоме як «супервекторизація», обіцяє значне зростання швидкостей – до 250 Мбіт/с.

Детальніше про принцип векторизації. Векторизація – це складна, але ефективна стандартизована процедура (ITU-T G.993.5, або G.vector), розроблена для мінімізації "перехресних перешкод" (NEXT та FEXT). Ці перешкоди є результатом фізичного впливу між сусідніми паралельними мідними кабелями і суттєво погіршують якість сигналу, обмежуючи швидкість VDSL-з'єднання. Усунення цих перешкод є критично важливим для збільшення пропускної здатності.

Рис. 1. Перешкоди на мідних ліній зв'язку

Розглянемо два основні типи перешкод на мідних лініях:

- **NEXT (Near End Crosstalk):** Виникають у місцях розташування комутаційного обладнання та між передавальними/приймальними пристроями. Завдяки використанню різних частот, проблема NEXT наразі вважається вирішеною.
- **FEXT (Far End Crosstalk):** Цей тип перешкод з'являється по всій довжині кабелю від мультиплексора до абонентської розетки, що обумовлено одночасною передачею вхідного та вихідного трафіку по

численним жилам одного кабелю. До появи векторизації єдиним методом боротьби з FEXT було обмеження швидкості до 50 Мбіт/с.

Векторизація, розроблена Alcatel-Lucent у 2010 році, революціонізувала підхід до FEXT. Її принцип простий і геніальний: система визначає рівень перешкод між скрученими парами та компенсує їх. Мультиплексор генерує спеціальний сигнал, який, накладаючись на вихідний, вже спотворений перешкодами, нейтралізує їх, забезпечуючи абоненту чистий і високоякісний сигнал.

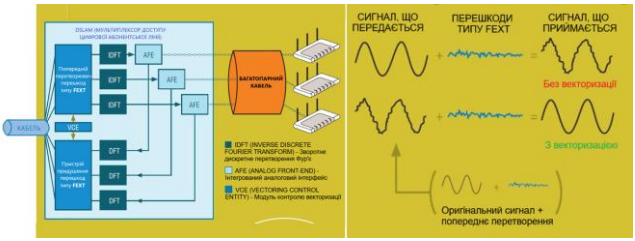


Рис. 2. Обладнання для використання та ефект від застосування технології векторизації

Для функціонування векторизації мультиплексор оснащується двома ключовими компонентами: **модулем контролю векторизації (Vectoring Control Entity, VCE)**, який обчислює необхідні корекції для компенсації FEXT, та **попереднім перетворювачем (Precoder)**, який застосовує ці корекції до сигналу, що передається абоненту (і, відповідно, до зворотного каналу).

Висновок. Технологія векторизації дозволяє повною мірою використовувати швидкісний потенціал існуючих мідних кабелів у VDSL-мережах. На сьогоднішній день це найефективніше рішення, якщо не передбачається прокладання додаткових мідних ліній. Вимірювання демонструють, що векторизація дійсно забезпечує заявлені 100 Мбіт/с на завантаження, проте ця швидкість досяжна лише за умови, що абонент знаходиться на відстані не більше 500 метрів від найближчого мультиплексора.

Список використаних джерел

1. ITU-T Recommendation G.993.5 (04/2010) - Vectoring for DSL transceivers.

2. ITU-T Recommendation G.993.2 (02/2015) - Very high speed digital subscriber line transceivers 2 (VDSL2).

3. Breschi, E., Fanti, A., Ginis, G., & Van Kerckhoven, H. (2011). Vectoring in DSL: A Primer. *IEEE Communications Magazine*, *49*(5), 118-124.

УДК 004.056.53

В.В. Нагорний
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ ВТОРГНЕННЯМ В ТЕЛЕКОМУНІКАЦІЙНУ МЕРЕЖУ НА БАЗІ АЛГОРИТМІВ МАШИННОГО НАВЧАННЯ

В роботі виконано аналіз існуючих методів виявлення та запобігання несанкціонованим вторгненням в телекомунікаційні мережі глобального та локального рівнів. У табличній формі представлено перелік цих методів з характеристиками обмежень щодо ефективності та областей їхнього застосування. Показано, що недоліки цих методів щодо забезпечення інформаційної безпеки можуть бути компенсовані шляхом застосування штучного інтелекту (ШІ). Програмно-апаратні засоби, що створені на основі ШІ, здатні аналізувати поведінку мережі в режимі реального часу, майже миттєво фіксувати будь-які відхилення від штатного режиму функціонування мережі та ефективно виявляти потенційні порушення безпеки.

Зокрема, показано, що традиційні підходи до мережевої безпеки включають Firewall, системи виявлення IDS / попередження вторгнень IPS, віртуальні приватні мережі (VPN), списки контролю доступу (ACL), сегментацію мережі та шифрування. Ці методи спрямовані на моніторинг і блокування підзорного трафіку, контроль надходження і захист даних від несанкціонованого доступу або модифікації [1]. Обмеження щодо сфер застосування традиційних підходів наведено в таблиці 1.

Таблиця 1 Обмеження сфер застосування традиційних методів забезпечення інформаційної безпеки

Метод	Обмеження
Firewall	— обмежена здатність перевіряти зашифрований трафік (тільки інформація заголовка). — неможливість знайти складні атаки, що використовують дозволені протоколи або служби.
Системи виявлення (IDS)	— ймовірність помилкових спрацьовувань, що призводять до перебоїв у сповіщенні. — обмежена ефективність проти вразливості нульового дня або просунутих постійних загроз.
Системи запо-	— аналогічні обмеження, що і в IDS, включаючи помилкові

бігання вторгненням (IPS),	спрацьовування та обмежену ефективність проти вразливості нульового дня.
віртуальні Gриватні мережі (VPN)	— вразливі для атак "людина посередині", якщо ключі шифрування скомпрометовані. — не забезпечує захист від внутрішніх загроз або заражених шкідливим програмним забезпеченням кінцевих точок, що отримують доступ до мережі.
Списки контролю доступу (ACL),	— статичними правилами може бути складно керувати у великих мережах з мінливими вимогами до доступу. — відсутність детального контролю за діями користувача після надання доступу.

Основні сфери використання ШІ для оптимізації телекомунікаційних мереж за критеріями інформаційної безпеки показані на рисунку 1.

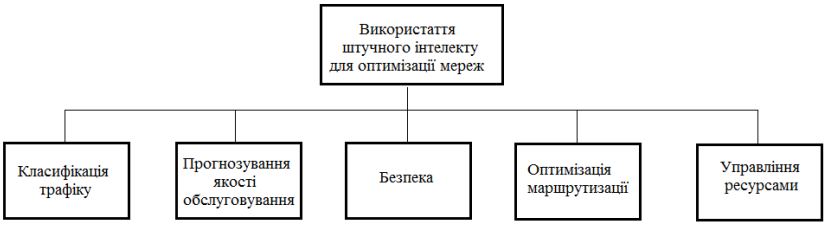


Рисунок 1 Використання ШІ для оптимізації телекомунікаційних мереж

Одним із ключових методів виявлення вторгнень є використання алгоритмів машинного навчання для порівняння поточної поведінки мережі із штатним режимом її функціонування з метою виявлення несанкціонованих інцидентів (потенційного вторгненя) [2]. Тому в даній роботі основну увагу приділено методам використання машинного навчання для запобігання вторгненням в телекомунікаційну мережу.

Моделі загального класифікаційного машинного навчання (ML) для виявлення вторгнення в телекомунікаційну мережу наведено в таблиці 2.

Таблиця 2 Моделі загального класифікаційного машинного навчання (ML) для виявлення вторгнення в телекомунікаційну мережу

Назва методу	Опис методу
Методи опорних векторів	ефективні для завдань бінарної класифікації,

(SVM)	обробляють багатовимірні дані з нелінійними взаємозв'язками за допомогою функцій ядра.
Метод випадкового лісу	використовує кілька дерев прийняття рішень для класифікації, придатних для несбалансованих наборів даних і великих обсягів даних з високою розмірністю.
K-найближчі сусіди (KNN)	простий та інтуїтивно зрозумілий метод класифікації точок даних на основі більшості голосів їхніх сусідів, непараметричний та підходить для різних наборів даних.
Gradient Boosting Machines (GBM)	послідовно будує дерева рішень, виправляючи помилки попередників, підходить для різноманітних даних і фіксує складні взаємозв'язки.
Логістична регресія	моделює ймовірність двійкового результату, піддається інтерпретації та ефективна з погляду обчислень, підходить для великомасштабних наборів даних.
Наївний алгоритм Байєса	ймовірнісний класифікатор, заснований на теоремі Байєса з припущенням незалежності ознак, простий та швидкий, ефективний для певних типів даних.
Нейронні мережі	моделі глибокого навчання, такі як CNNs і RNNs, можуть автоматично отримувати ієрархічні функції з необроблених даних, що ефективно для захоплення складних шаблонів.

Виявлення вторгнень передбачає різноманітні методи та підходи, кожен із яких має свої сильні та слабкі сторони. Вибір відповідного методу залежить від характеру даних, контексту проблеми та конкретних вимог програми.

В роботі надані рекомендації щодо коректного вибору методу виявлення вторгнень в залежності від конкретних умов використання інформаційних мереж. Такий вибір, в багатьох випадках, має вирішальне значення щодо забезпечення інформаційної безпеки, оскільки різні умови використання висувають різні вимоги до точності, інтерпретації та ефективності методів ШІ. Наприклад, у сфері кібербезпеки систем спеціального призначення виявлення в режимі реального часу з високою точністю має вирішальне значення, тоді як у сфері охорони здоров’я більш важливими можуть бути методи інтерпретації та мінімізації помилкових спрацьовувань.

УДК 004.89:681.5:656.078.5

Д.С.Нефедов
Державний університет
«Київський авіаційний інститут», м. Київ

ДОСЛІДЖЕННЯ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ РОЗПІЗНАВАННЯ ТА КЕРУВАННЯ БАГАЖЕМ

Аеропорт - не просто місце яке допомагає людям добратися до потрібної точки призначення, він є складним логістичним комплексом, який слугує хабом для множин авіакомпаній та невід'ємною частиною економічної інфраструктури країни. Ключовим викликом у питанні розвитку аеропортів залишається точне, швидке та безпечне керування багажем. У сучасних умовах втрати або затримки валіз не лише викликають дискомфорт у пасажирів, яких це зачепило, але й можуть призвести до порушення усього графіку відправлення рейсів та подальших фінансових втрат. Саме тому і виникає потреба в розробці інтелектуальної системи керування багажем яка здатна витримати сучасні реалії та тиск аеропортів, що і стало метою роботи.

У межах дослідження було розглянуто повний цикл обробки багажу - від моменту реєстрації пасажира до завантаження валізи на борт ПС, із детальним вивченням логіки сортувальних систем (BHS), процедур безпеки, зчитування ідентифікаторів та буферного зберігання. Особливу увагу приділено системам автоматичного сканування, зокрема технологіям штрихкодової ідентифікації, RFID-міток і іміджевих сканерів. Окремо було досліджено використання машинного навчання та нейронних мереж у BHS на прикладі кількох методів їх застосування. Далі було проведено порівняльний аналіз за параметрами точності зчитування, стійкості до пошкоджень, вимог до інфраструктури, вартості впровадження та сумісності з глобальними стандартами, зокрема тими що були запроваджені IATA. На основі цього аналізу як найбільш збалансоване рішення було обрано штрихкодову систему у поєднанні з OCR-модулями, що дозволяє досягти високої точності при відносно низьких витратах. Вибір такої комбінації зумовлений прагненням усунути типовий недолік штрихкодів - стирання, пошкодження, неправильне розміщення бірки на валізі, що викликає збої у корректному зчитуванні інформації. Завдяки цьому система набуває

властивостей самовідновлення і підвищеної точності зчитування в складних умовах.

Наступним кроком було розглянуто міжнародний аеропорт Гонконгу (HKIA) як приклад високотехнологічного логістичного хабу, де успішно реалізовано принципи автоматизованої обробки багажу. Отримані результати та спостереження стали основою для побудови власної моделі інтелектуальної системи керування багажем, адаптованої до типових умов великих транспортних вузлів. Особливу увагу приділено стандартам, встановленими IATA, зокрема положенням Resolution 740, що регламентують структуру, зміст та спосіб кодування інформації на багажній бірці. Також було охоплено практику використання штрихкодів у форматі Code 128, який дозволяє закодувати інформацію з високою щільністю та збереженням контрольної суми. У роботі проаналізовано процес генерації таких кодів, починаючи зі збору вхідних даних під час реєстрації пасажира, формування послідовності символів згідно з обраним профілем кодування, до розміщення фінального штрихкоду на друкованій етикетці. Було розроблено архітектуру та алгоритм роботи модифікованої системи, обрано відповідний промисловий протокол (OPC-UA). Увагу приділено майбутньому розвитку цієї системи, що безпосередньо залежить від сучасності та точності комп'ютерного зору.

Для розробленої системи було підібрано технічне обладнання, яке відповідає вимогам до швидкості, гнучкості впровадження, точності та надійності зчитування інформації в умовах інтенсивного багажного потоку. На основі загальної логіки функціонування системи та аналізу типової аеропортової топології було виконано розрахунок орієнтовної кількості необхідних пристроїв. Враховано довжину конвеєрної мережі, середню щільність вузлів зчитування, потребу в дублюванні зон на критичних ділянках, а також окреме оснащення зон реєстрації пасажирів, пунктів самостійної здачі багажу, сортувальних центрів та зон завантаження на літак. Описано спосіб налаштування цих приладів.

Запропонована система має високу стійкість, задовільне співвідношення між ціною впровадження та ефективністю роботи, модульність та гнучкість у налаштуванні. Вона не потребує глибокої перебудови інфраструктури, що дозволяє її впроваджувати поетапно, з можливістю поступової модернізації.

УДК 004.056 (043.2)

В.О.Окусков
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ВИЯВЛЕННЯ АНОМАЛЬНОСТЕЙ У МЕРЕЖЕВОМУ ТРАФІКУ НА ОСНОВІ НЕЙРОМЕРЕЖ

У сучасних комп'ютерних мережах зростає кількість кіберзагроз, пов'язаних зі зловмисною активністю, витоками даних, DDoS-атаками тощо. Традиційні системи захисту, побудовані на сигнатурному аналізі, часто не в змозі вчасно виявити нові або змінені типи атак, оскільки потребують попереднього знання шаблонів загроз. Водночас сучасні тенденції розвитку інформаційної безпеки демонструють високу ефективність поведінкових моделей і самонавчальних систем на основі методів машинного навчання. Особливо перспективними є нейронні мережі, здатні виявляти приховані закономірності у великих обсягах даних

У рамках дипломного дослідження розроблено систему виявлення аномальної поведінки в мережевому трафіку, що базується на поєднанні математичної моделі ARIMA для прогнозування трафіку в реальному часі та нейронної мережі для класифікації типів поведінки. Для збору та підготовки даних використано бібліотеку Scapy (Python), яка дозволила захоплювати трафік, фільтрувати службові пакети та формувати часові ряди на основі статистичних показників (довжина пакету, частота з'єднань, тип протоколу). Побудовано функцію визначення аномалій шляхом порівняння реальних і прогнозованих значень. У реалізації також передбачено інтерфейс користувача для перегляду спрацьовувань системи.

Система демонструє високу продуктивність: затримка обробки даних не перевищує 100 мс, рівень точності класифікації становить понад 92 %, при цьому кількість хибнопозитивних спрацьовувань зменшена завдяки багатокритеріальному аналізу. Всі спрацювання журналюються у базу MongoDB, що дозволяє проводити історичний аналіз інцидентів безпеки. Порівняння ефективності ARIMA та нейронних мереж показало, що саме комбінований підхід забезпечує найкращий результат в умовах змінної мережевої поведінки.

Особливістю реалізованої системи є підтримка адаптивного аналізу, що дозволяє зменшити кількість хибнопозитивних спрацьовувань. Ефективність обраного підходу оцінювалася за метриками точності, повноти та F1-міри. Результати експериментів показали, що інтеграція ARIMA з нейронною мережею дозволяє виявляти як відомі, так і zero-day атаки із затримкою менше 100 мс. Система може бути інтегрована в інфраструктуру підприємств з високими вимогами до кібербезпеки або застосовуватись як навчальний інструмент.

Запропонована архітектура системи передбачає модульність, що забезпечує гнучкість у налаштуванні та масштабуванні. Зокрема, компоненти збору даних, прогнозування та класифікації можуть бути замінені або доповнені альтернативними алгоритмами без суттєвого перепроєктування всієї системи. Такий підхід сприяє підвищенню адаптивності до змін у мережевому середовищі та появі нових загроз. Крім того, реалізація в контейнеризованому середовищі Docker забезпечує простоту розгортання та інтеграції з існуючими засобами моніторингу й кіберзахисту.

Перспективним напрямом подальшого розвитку системи є впровадження механізмів активного навчання, коли система не лише пасивно аналізує трафік, а й взаємодіє з адміністратором для уточнення результатів класифікації. Це дозволить підвищити точність виявлення нетипової поведінки в специфічних мережах та зменшити залежність від апріорних даних. Крім того, у майбутньому планується розширення системи для підтримки міжмережевого аналізу, що дозволить виявляти розподілені атаки, які важко зафіксувати в межах одного вузла.

УДК 621.395.48 (043.2)

С.В. Онацька, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

КОРПОРАТИВНА VOIP МЕРЕЖА

Технологія VoIP, завдяки гнучкості та економічності платформи Asterisk, відкриває широкі можливості для організації зв'язку компаній будь-якого масштабу – від невеликих стартапів до великих корпорацій. Для цього необхідно розглянути питання процесу вибору необхідного апаратного забезпечення та основні етапи налаштування IP-АТС Asterisk, використовуючи як приклад модернізацію існуючої офісної телефонної системи**.**

Етапи налаштування IP-АТС Asterisk

Процес розгортання IP-АТС на базі Asterisk включає наступні ключові етапи:

1. Вибір та налаштування апаратного забезпечення з інтерфейсом E1 (за потреби інтеграції з ТМЗК):
   - Якщо необхідно підключити Asterisk до традиційних телефонних ліній E1 (наприклад, для інтеграції з існуючою інфраструктурою або для забезпечення резервного зв'язку), потрібно обрати сервер, що підтримує встановлення спеціалізованих плат з інтерфейсом E1. Прикладом може бути будь-яка плата потоку E1 від різних виробників у PCI форм-факторі.
   - На цьому етапі здійснюється фізичне встановлення плати E1 в сервер, її первинна конфігурація на рівні BIOS (за потреби) та встановлення необхідних драйверів на операційній системі.
2. Встановлення операційної системи:
   - Asterisk найкраще працює на базі операційних систем сімейства Linux (наприклад, CentOS, Debian, Ubuntu Server). Рекомендується використовувати стабільні та перевірені дистрибутиви.
   - Процес встановлення включає вибір дистрибутива, завантаження інсталяційного образу, запис його на носій (USB-флешку або DVD), завантаження з цього носія та виконання кроків інсталятора.
3. Встановлення програмного забезпечення Asterisk та драйверів:
   - Після успішної інсталяції операційної системи необхідно встановити безпосередньо програмне забезпечення Asterisk та необхідні

драйвери для встановленого апаратного забезпечення (наприклад, драйвери DAHDI для плат E1/T1/аналогових ліній).

- Встановлення зазвичай здійснюється за допомогою пакетного менеджера операційної системи (наприклад, yum для CentOS/RHEL, apt для Debian/Ubuntu). Потрібно додати репозиторії Asterisk (за потреби) та встановити основні пакети Asterisk, Asterisk-core, Asterisk-chan-sip (або Asterisk-chan-pjsip для сучаснішого протоколу SIP), Asterisk-dialplan, а також необхідні кодеки та інші модулі.

4. Налаштування телефонної плати потоку E1 з Asterisk (або аналогічної плати E1):

- Для того, щоб Asterisk міг взаємодіяти з встановленою платою E1, необхідно правильно налаштувати відповідні конфігураційні файли. Це зазвичай включає редагування файлів конфігурації DAHDI (Digital Hardware Interface Driver), який забезпечує інтерфейс між Asterisk та апаратними платами телефонії.
- У конфігураційних файлах DAHDI (наприклад, dahdi_system.conf, chan_dahdi.conf) визначаються параметри плати, кількість каналів E1, тип сигналізації та інші специфічні налаштування.

5. Загальні налаштування програмного додатка Asterisk:

- На цьому етапі здійснюється базова конфігурація Asterisk, включаючи налаштування основних параметрів, мережевих інтерфейсів, кодеків, протоколів (SIP, IAX2 тощо), користувачів та розширень (extensions).
- Основні конфігураційні файли Asterisk знаходяться в каталозі /etc/asterisk/ і включають asterisk.conf, sip.conf (або pjsip.conf), iax.conf, extensions.conf (де описується план нумерації), voicemail.conf та інші.

6. Налаштування потоку E1 із сигналізацією PRI:

- Якщо використовується підключення E1 з сигналізацією PRI, необхідно правильно сконфігурувати відповідні параметри в файлах DAHDI та в плані нумерації Asterisk (extensions.conf). Це включає визначення кількості каналів, налаштування DID (Direct Inward Dialing) для маршрутизації вхідних дзвінків на конкретні внутрішні номери, а також налаштування правил для вихідних дзвінків через транки E1.

7. Налаштування DAHDI:

- DAHDI є ключовим компонентом для роботи Asterisk з апаратними інтерфейсами телефонії (E1/T1, аналогові лінії). Налаштування DAHDI включає конфігурацію файлів dahdi_system.conf для визначення фізичних інтерфейсів та chan_dahdi.conf для налаштування ка-

налів, що використовуються Asterisk. Правильне налаштування DAHDI є критично важливим для стабільної та коректної роботи з традиційними телефонними мережами (PSTN).

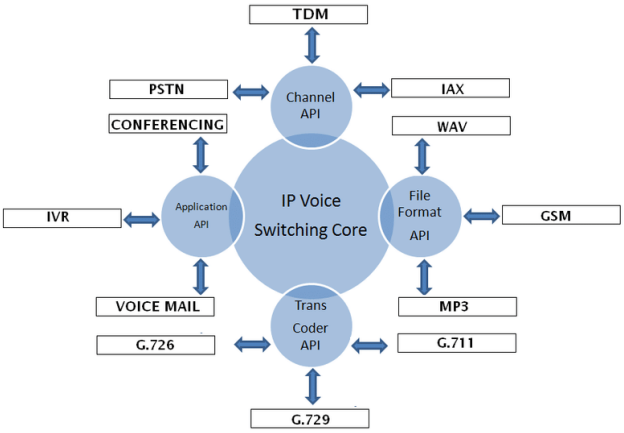


Рис. Модульна архітектура Asterisk для забезпечення гнучкості платформи

Висновок:

В роботі було проаналізовано, що питання, присвячені вибору обладнання та налаштування IP-АТС на базі Asterisk, є ключовим етапом модернізації офісної АТС, а також є критично важливим для стабільної та коректної роботи всієї платформи.

Список використаних джерел

1. https://www.terratel.eu/solutions.html
2. Anatol Badach, Erwin Hoffmann. Technik der IP-Netze: Grundlagen der IPv4- und IPv6-Kommunikation. Carl Hanser Verlag GmbH & Co. KG; 5., überarbeitete Edition 2022. – 1185 s
3. Anatol Badach. Voice over IP - Die Technik: Grundlagen, Protokolle, Anwendungen, Migration, Sicherheit, Notrufdienste, Videotelefonie. Carl Hanser Verlag GmbH & Co. KG; 5., überarbeitete und erweiterte Edition 2022. – 655 s.
4. http://www.voip-information.de/vorteile-voip.html

УДК 004.946:629.735

С. О. Передерій
Державний університет
«Київський авіаційний інститут», м. Київ

ОПТИМІЗАЦІЯ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ У ЦИВІЛЬНИХ ТА ПРОМИСЛОВИХ СФЕРАХ

Застосування безпілотних літальних апаратів (БПЛА) у межах промислових і цивільних процесів поступово трансформується від експериментального до інфраструктурного. Поширення цих систем спирається не лише на зниження вартості компонентів і зростання ринкової пропозиції, а й на зміну концепції управління об’єктами в повітряному просторі. Експлуатація БПЛА вже не обмежується одноразовими польотами для зйомки або моніторингу. З’являється потреба в системному підході, який передбачає оптимізацію використання апаратів за критеріями енергоспоживання, маршрутизації, обробки даних та інтеграції в наявні мережеві структури [1, с. 17].

Незважаючи на технічний прогрес, рівень впровадження дронів залишається фрагментарним. Зокрема, відсутність адаптивних маршрутних моделей з урахуванням особливостей ландшафту, погодних факторів і трафіку призводить до підвищених витрат енергії. Дослідження показують, що при фіксованих маршрутах без попереднього моделювання навантаження й типу перешкод витрати акумулятора можуть перевищувати розрахункові на 15–20 % [2, с. 40]. Також встановлено, що ефективність експлуатації залежить від щільності інформаційного трафіку: чим вища частота обміну з наземними станціями, тим вища ймовірність перевантаження каналів у реальному часі [5, с. 59].

Запропонована модель оптимізації складається з трьох взаємопов’язаних модулів: маршрутизатора з урахуванням змін середовища, системи локальної обробки даних (edge computing) та комунікаційного протоколу зі стисканням і пріоритизацією трафіку. Імітаційне моделювання показало, що інтеграція механізмів попереднього аналізу на борту дозволяє знизити навантаження на канали зв’язку до 45 %, зберігаючи при цьому базові характеристики точності позиціювання й передачі [4, с. 78]. Водночас автономні обчислення відкривають мож-

ливість для впровадження навчальних алгоритмів, які коригують параметри маршруту в процесі польоту.

Враховуючи технологічну структуру сучасних БПЛА, особливо у сфері логістики та моніторингу, доцільним виявляється використання багатоканальних ретрансляторів на основі технологій MIMO та mesh-архітектури. Це дозволяє підтримувати зв'язок навіть при переміщенні між зонами з перешкодами або слабким сигналом, що особливо актуально для виконання завдань у міських агломераціях чи гірських районах [5, с. 59]. У разі втрати стабільного з'єднання дані буферизуються, а пакетне шифрування знижує ризики їх компрометації.

Разом з тим, існує ряд обмежень. Поточні алгоритми моделювання не враховують повною мірою турбулентність, електромагнітні завади та соціальні обмеження, пов'язані з використанням камер у громадських місцях. Правові прогалини, зокрема щодо визначення зон відповідальності оператора, залишаються неврегульованими [3, с. 61]. Більше того, наявні протоколи сертифікації апаратів часто не враховують їхню здатність до автономної адаптації, що ускладнює інтеграцію розумних дронів у загальну систему повітряного трафіку.

Таким чином, запропонований підхід дозволяє покращити техніко-економічні показники експлуатації БПЛА, однак потребує подальшого доопрацювання в частині адаптивної логіки, нормативного узгодження та перевірки в умовах змінного середовища. Очікується, що зростання ролі автономних обчислень у структурі дронів сприятиме розвитку нових форм мобільної інфраструктури, що функціонуватиме як розподілена система реагування на потреби конкретної галузі.

Список використаних джерел:

1. Моргун В.І. Технологічні рішення у системах управління БПЛА / В.І. Моргун, О.М. Завгородній. – К.: Аеромехпрес, 2021. – 168 с.

2. Колесник А.М. Енергоефективність дронів у промисловості. // Наук. вісник КАІ. – 2022. – № 1. – С. 37–42.

3. Чорний І.В. Штучний інтелект у системах навігації БПЛА. – К.: Техніка, 2023. – 192 с.

4. Завгородній С.О. Оптимізація передавання даних у БПЛА: сучасні підходи / С.О. Завгородній // Вісник КАІ. – 2024. – № 2. – С. 75–82.

5. Ткаченко Д.С. Телекомунікаційні мережі для БПЛА. – Львів: Спектр, 2020. – 146 с.

УДК 658.8(043.2)

І.Р. Потіха
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОДИ ПОКРАЩЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ КЛІЄНТІВ ІНТЕРНЕТ-ПРОВАЙДЕРА

У сучасному інформаційному суспільстві якість телекомунікаційних послуг відіграє ключову роль у задоволеності клієнтів та успішності компаній-провайдерів. У XXI столітті Інтернет є не лише джерелом інформації, а й важливим інструментом у бізнесі, навчанні та державному управлінні. Це зумовлює необхідність не лише стабільного з'єднання, а й високого рівня сервісного обслуговування. Особливої актуальності набуває впровадження інноваційних рішень, таких як CRM-системи, чат-боти, мобільні додатки. На цьому тлі проблема вдосконалення клієнтського сервісу стає предметом наукового та прикладного інтересу.

У дослідженні проаналізовано процес обслуговування клієнтів у компанії ТОВ "Мережа Ланет". Застосовано комплекс методів: аналіз літературних джерел, стандартизації (ISO, ITIL, QoS), соціологічне опитування, SWOT-аналіз, а також порівняльний аналіз з конкурентами. Результати свідчать, що хоча більшість клієнтів компанії задоволені стабільністю з'єднання та оперативністю технічної підтримки (91% і 87% відповідно), існують критичні напрями для вдосконалення сервісу.

Серед основних проблем виділено затримки у виїзному обслуговувані в сільських районах, обмежену функціональність мобільного застосунку Lanet, повторні звернення з одних і тих самих питань, а також перевантаження контакт-центру у пікові години. У роботі визначено шляхи їх вирішення: удосконалення логістики виїзних бригад, редизайн інтерфейсу мобільного застосунку, впровадження автоматизованих рішень (чат-боти, IVR), підвищення кваліфікації операторів першої лінії. Особлива увага приділяється психологічній підготовці персоналу та розвитку комунікативної культури.

Окрім технічних і організаційних заходів, вагому роль відіграє наявність чітких стандартів взаємодії з клієнтами. Встановлення єдиних алгоритмів обробки звернень, типових сценаріїв спілкування та

протоколів реагування дозволяє підвищити послідовність і якість обслуговування, зменшивши ризик помилок та забезпечити кращу взаємозамінність працівників.

Проведено порівняльний аналіз підходів до обслуговування серед провідних українських інтернет-провайдерів: “Київстар”, “Воля”, “ФРІНЕТ”. Результати свідчать, що хоча “Мережа Ланет” має сильні технічні показники та репутацію, вона поступається за рівнем автоматизації, гнучкості мобільного обслуговування та реалізації програм лояльності. Запропоновані заходи дозволяють не лише усунути слабкі місця, а й посилити конкурентні переваги.

Зростання ролі клієнтського досвіду в інтернет-послугах також пов’язане зі змінами в поведінці споживачів. Користувачі очікують не лише швидкого реагування, а й зручності у взаємодії - через мобільні платформи, доступні інтерфейси та персоналізовані пропозиції. Саме тому дедалі більше значення мають інструменти big data та аналітика поведінки клієнтів, які дозволяють формувати індивідуальні сценарії обслуговування.

Крім того, впровадження принципів клієнтоорієнтованого підходу потребує змін в організаційній культурі компанії. Важливо, щоб усі працівники - від технічного персоналу до керівництва - поділяли спільні цінності сервісу та прагнули до постійного вдосконалення. Регулярне навчання, система внутрішньої мотивації сприяють формуванню ефективної команди, здатної реагувати на виклики сучасного телекомунікаційного ринку.

Таким чином, підвищення рівня якості сервісу в інтернет-провайдера можливе за рахунок інтеграції технічних, організаційних та психологічних компонентів. Вдосконалення клієнтського досвіду, адаптація до змін у запитах споживачів, використання міжнародних стандартів і цифрових інструментів дозволяють забезпечити високий рівень лояльності та стабільне зростання компанії у складних умовах сучасного телекомунікаційного ринку. Крім цього, важливо формувати довгострокову сервісну стратегію, що враховує не лише технічні виклики, а й культурні особливості взаємодії зі споживачами. Отже, якісний сервіс стає не лише фактором утримання абонентів, але й конкурентною перевагою, що визначає майбутнє компанії на ринку.

УДК 621.39 (043.2)

Rohozha I.O.
State University
"Kyiv Aviation Institute", Kyiv

CLASSIFICATION OF CRITICAL INFRASTRUCTURE OBJECTS AND MONITORING SYSTEMS. COMPONENTS, DATA TRANSFER AND PROTOTYPE SYSTEM. CRITERIA FOR EVALUATING EFFECTIVENESS.

Making the research on the topic we firstly have to classify the subject area. Critical infrastructure (CI) encompasses vital sectors such as smart grids, intelligent transportation systems, and urban smart city initiatives.

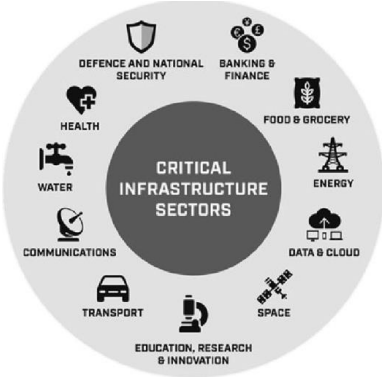


Fig.1. Classification of critical infrastructure sectors

Monitoring systems within these domains can be broadly classified by their application, ranging from fundamental environmental surveillance at remote facilities and structural health analysis to more complex, time-critical control applications. These systems inherently differ in their requirements for data throughput, latency, and reliability, necessitating advanced solutions to overcome the inherent limitations of legacy monitoring approaches.

The prototype system is proposed to be designed with a pragmatic, modular architecture utilizing readily available technologies. At the edge, ESP32-based sensor nodes for data acquisition due to their integrated connectivity and cost-effectiveness.

Fig. 2. Microcontroller ESP32

A commercial 5G Customer Premise Equipment (CPE) router served as the pivotal connectivity module, providing the high-speed, low-latency 5G backbone for data transmission.

Data aggregation and distribution were managed by an MQTT broker, a lightweight and efficient protocol for IoT environments.

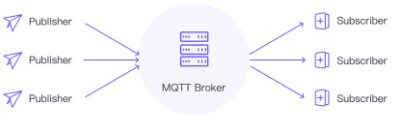


Fig. 3. MQTT Broker

Finally, a centralized IoT dashboard facilitated real-time data visualization and alert notifications. This implementation strategy prioritized the use of off-the-shelf components to validate the system's core design principles and demonstrate efficient data transfer over a 5G link within a practical, university-level context.

The effectiveness of the monitoring system is evaluated against key performance indicators (KPIs) critical for vital infrastructure. These criteria include: Data Transmission Reliability, measuring the success rate of packet delivery; End-to-End Latency, quantifying the time delay from sensor reading to dashboard display or alert reception; Data Stability and Integrity, assessing the accuracy and consistency of received data; System Responsiveness, evaluating the speed of alert generation and propagation upon threshold breaches; and Connectivity Robustness, a qualitative assessment of the system's ability to maintain and recover 5G connectivity. These metrics collectively provided a comprehensive evaluation of the prototype's ability to meet the stringent demands of critical infrastructure monitoring.

УДК 654.9

Я.Ю. Руденко
Державний університет
«Київський авіаційний інститут», м. Київ

СЕРВІС ПЕРЕДАЧІ ДАНИХ МОБІЛЬНОГО АБОНЕНТА

Актуальність дослідження обумовлена тим, що у сучасних мобільних мережах зростають обсяги мультимедійного та текстового трафіку, що вимагає підвищеної ефективності передачі даних, мінімізації затримок і оптимізації ресурсів радіоінтерфейсу.

Цільова група користувачів – це абоненти 4G/5G мереж, які очікують безперервного доступу до інтернет–сервісів за будь–яких умов.

Мета дослідження – розробити рекомендації щодо вибору та адаптації сервісів передачі даних у мобільних мережах із фокусуванням на підвищення QoS, зниження BER та оптимізацію використання смуги пропускання радіоканалу.

Для досягнення цієї мети потрібно вирішити ряд завдань:

1. Провести аналіз існуючих сервісів передачі текстових та мультимедійних даних у мобільних мережах. У сучасних мобільних мережах активно використовуються сервіси OTT (Over-The-Top), зокрема WhatsApp, Viber, Telegram, які забезпечують передачу не лише текстових повідомлень, а й зображень, відео та аудіо. Ці сервіси створюють додаткове навантаження на мережу, зокрема у години пік, і вимагають високої надійності та пропускної здатності.
2. Оцінити ключові параметри якості (SNR, BER, затримка, jitter) для сервісів SMS, OTT–месенджерів та IP–дзвінків.
3. Розглянути методи стискання даних для тексту та зображень із урахуванням обмежених ресурсів радіоінтерфейсу.
4. Розробити рекомендації щодо вибору алгоритмів стиснення та мережних протоколів для оптимальної роботи на абонентському рівні.

Методика дослідження передбачає аналіз стандартів мобільного зв’язку GSM, LTE та 5G NR; моделювання BER і SNR у каналі AWGN; порівняння алгоритмів стиснення (Huffman, LZW, JPEG, PNG) за критеріями ступеня стиснення, обчислювальної складності та впливу на якість контенту.

Основні результати дослідження полягають у наступному:

1. Визначені критичні значення параметрів: смуга пропускання нижче 1 МГц призводить до зростання BER > 10^{-3} у випадку PSK-модуляції без адаптивного кодування.
2. Запропоновано гібридний підхід стискання: для тексту – це комбінований LZW + RLE; для зображень – це JPEG XS із динамічною корекцією квантізації.
3. Розроблені рекомендації щодо налаштування QoS: пріоритизація SIP та RTCP у LTE–eDRX для зниження jitter до < 20 мс.

Висновки:

Використання адаптивних алгоритмів стиснення у поєднанні з налаштуванням параметрів MAC–рівня Wi–Fi 4G/5G NR дозволяє знизити затримку на 15 % і підвищити ефективність використання радіоресурсу на 20 % без зниження якості переданих даних.

Додатково встановлено, що для сценаріїв передачі зображень зі змінним фоном (наприклад, у відеозв'язку) доцільно використовувати попередню сегментацію зображення перед стисканням, що дозволяє знизити загальне навантаження на канал.

Отримані результати можуть бути використані при розробці адаптивних мобільних додатків, які автоматично підлаштовують якість переданих даних залежно від умов каналу та рівня навантаження на мережу.

Список літератури:

1. Весоловський В. М. Системи рухомого радіозв'язку. — 2006.
2. Гепко В. Н. Сучасні безпроводові мережі. — 2009.
3. 3GPP TS 36.300: E–UTRA and E–UTRAN Overall description.
4. ISO/IEC 14495–1: Information technology — Lossless and near–lossless compression of continuous–tone still images.
5. Cisco Annual Internet Report (2018–2023). Cisco Systems.
6. 3GPP TS 38.300: NR; NR and NG-RAN Overall description.
7. Tanenbaum A. S., Wetherall D. J. *Computer Networks*. — 5th ed., Pearson, 2010.
8. Sayood K. Introduction to Data Compression. — 5th ed., Morgan Kaufmann, 2018.
9. Ericsson Mobility Report, November 2023. Ericsson AB.

УДК 621.391.63

Я.Є. Ружин, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

МІЖМІСЬКА ТРАНСПОРТНА МЕРЕЖА OTN

У сучасному світі інтенсивний обмін даними є основою функціонування всіх секторів економіки, науки та суспільства. Зростаючі обсяги інформації, швидкість передачі та висока надійність стали ключовими вимогами успішної глобальної взаємодії. Саме тому міжміські оптичні транспортні мережі (ОТМ) посідають центральне місце у світовій системі зв'язку.

Для подальшого розвитку міжміських OTN-мереж необхідно розглянути їхню архітектуру, принципи функціонування, ключові технології.

Шари архітектури OTN

Ефективність мультиплексування та швидке транспортування трафіку забезпечує як раз ієрархія шарів OTN.

1. OPU – Optical Chanel Payload Unit.

Цей шар відповідає за відображення (мапування) клієнтського сигналу (наприклад, Ethernet, SDH/SONET, IP) у стандартизований фрейм OTN. OPU забезпечує прозору передачу клієнтських даних, адаптуючи їх до формату OTN.

2. ODU - Optical Channel Data Unit.

ODU є основним контейнером для передачі даних OTN. Він включає OPU, а також додаткову інформацію для моніторингу, управління та обслуговування (OAM&P). ODU забезпечує можливості моніторингу якості каналу, виявлення несправностей та сигналізації, що є критично важливим для надійної роботи мережі. ODU може бути мультиплексований або комутований на проміжних вузлах мережі.

3. OTU - Optical Channel Transport Unit.

OTU є верхнім шаром цифрової обгортки OTN і представляє сигнал на лінії після додавання механізмів прямого виправлення помилок (FEC). Він відповідає за передачу ODU через фізичний оптичний канал. FEC дозволяє відновлювати помилки, що виникають під час передачі, значно підвищуючи цілісність даних на великих відстанях.

4. OCh - Optical Channel.

Цей шар представляє собою окрему довжину хвилі світла, по якій передається інформація. В контексті міжміських мереж, OCh часто інтегрується з технологією щільного мультиплексування з поділом за довжиною хвилі (DWDM), дозволяючи передавати десятки або сотні незалежних оптичних каналів по одному фізичному волокну.

5. OMS - Optical Multiplex Section та OTS - Optical Transmission Section.

Ці шари відповідають за фізичне транспортування груп оптичних каналів (у випадку OMS) або всього оптичного сигналу по волокну (у випадку OTS) між оптичними елементами мережі, такими як мультиплексори/демультиплексори DWDM та оптичні підсилювачі.

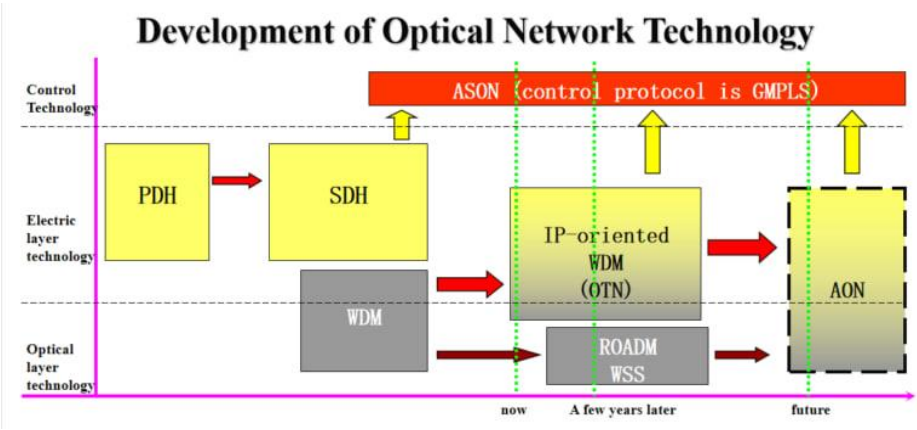


Рис. Розвиток технології оптичних мереж

Ключові технології

Варто почати з щільного мультиплексування з поділом за довжиною хвилі (DWDM). Завдяки цій технології можна передавати близько сотні окремих оптичних каналів, кожен з яких працює на своїй довжині хвилі, по одному оптичному волокну. Як результат, ми маємо можливість максимізувати пропускну здатність існуючої мережі, не прокладаючи додаткові фізичні кабеля.

Важливою частиною структури OTN є механізми прямого виправлення помилок (FEC), визначеною стандартом ITU-T G.709. Ця технологія вирішує проблему виникнення помилок на маршруті та ви-

правляє їх на приймальному кінці без запиту на повторну передачу даних. Звісно передача оптичних сигналів на довгі дистанції неминуче супроводжується різними спотвореннями та шумом, але FEC добре виконує свої функції та покращує ефективну швидкість бітових помилок (BER) для клієнтського сигналу.

Список використаних джерел

1. Гілкріст А. Короткий довідник з оптичних транспортних мереж OTN / А. Гілкріст. – К. : Артеч Хаус, 2015.
2. Nokia launches next generation OTN architecture for wholesale services // Nokia. – 2022.
3. Interfaces for the Optical Transport Network (OTN) : Recommendation G.709/Y.1331 (06/2020). – ITU-T, 2020.
4. WDM vs OTN: What is the Difference Between WDM and OTN? // Fibermall Team. – 2022.

УДК 621.396.664 (043.2)

Самойленко О.А.,здобувач, Зуєв О.В., к.т.н., доцент
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА МОНІТОРИНГУ ТА УПРАВЛІННЯ ЕНЕРГОСПОЖИВАННЯМ

Протиріччя між сучасним рівнем інформаційних систем, засобів вимірювань, діагностування, моніторингу обладнання систем енергоспоживання (СЕС) і традиційними методами обробки діагностичної інформації, вироблення правил прийняття рішень вказує на недостатню ефективність методів управління технічним станом (ТС) обладнання зазначених систем в умовах стохастичною невизначеності вихідної інформації.

Збільшення розмірності і неоднорідності інформаційного простору, необхідність врахування кореляційних зв'язків різних параметрів для достовірного опису станів СЕС вимагають певного вдосконалення процесів обробки вихідної діагностичної інформації[1]. Ці процеси повинні здійснюватися у керованих та контрольованих умовах, що передбачає здійснення постійного моніторингу параметрів окремих засобів та складових СЕС різноманітного призначення.

Моніторинг – це процес установлення відповідності між об'єктивним станом об'єкта і заздалегідь заданою нормою на можливі стани об'єкта, що здійснюється шляхом обробки отриманої інформації, формування та видачі рішення про результати встановлення відповідності [1,2]. Операторну схему моніторингу стану СЕС показано на рис.

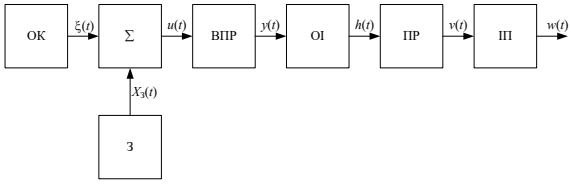


Рисунок - Схема моніторингу технічного стану СЕС: ОК – об'єкт моніторингу;ВПР – оператор, який визначає роботу вимірювального приладу; ОІ – оператор обробки інформації; ПР –

оператор прийняття рішення; ІП – оператор, який визначає роботу індикаторного пристрою; З – оператор завад вимірювання

Метою даної роботи є розробка системи моніторингу та управління енергоспоживанням, яка дозволяє в реальному часі відстежувати рівень споживаної електроенергії, а також керувати електроприладами у складі СЕС дистанційно. Така система повинна бути простою у використанні, доступною для впровадження у побуті або на невеликих підприємствах, та мати можливість подальшого розширення функціоналу.

На ринку існує велика кількість систем моніторингу та управління енергоспоживанням, зокрема такі продукти як TP-Link Tapo, Shelly, Tuya Smart, Xiaomi Mi Home. Однак більшість із них мають високу вартість, обмежені можливості кастомізації, або залежність від хмарних сервісів, що робить їх менш привабливими для користувачів . Крім того, деякі з них не дозволяють повноцінного локального управління, що може бути критичним у разі перебоїв з інтернетом або бажанні зберігати дані виключно локально. Запропонована система вирішує ці проблеми, пропонуючи доступну, гнучку та розширювану платформу з відкритим API, яка дозволяє локальне або віддалене керування приладами без необхідності підключення до сторонніх серверів. Це робить її вигідною альтернативою існуючим комерційним рішенням.

Для реалізації системи моніторингу та керування енергоспоживанням було побудовано архітектуру, що складається з двох ключових компонентів: Серверна частина – реалізована на Node із з використанням фреймворку Express. Вона відповідає за приймання даних від пристроїв, зберігання інформації та обробку запитів на керування станом пристроїв. Клієнтська частина (емуляція пристрою) – представляє умовний «розумний» пристрій, який періодично надсилає дані про енергоспоживання на сервер, використовуючи HTTP-запити.

Список використаних джерел

1. *Системи* експлуатації авіаційних радіоелектронних систем та комплексів: Конспект лекцій / *Уклад.:* О.В. Соломенцев, М.Ю. Заліський, О.В.Зуєв, С.В. Рудий.- Кривий Ріг: КК НАУ, 2017 .- 62 с.
2. Basics of radioelectronic equipment reliability, operation and repair theory: Lecture synopsis / O.V.Zuiev, O.M. Akmaldinova, O.V. Solomentchev, Ju.M. Khmelko.- Kyiv: NAU, 2011. - 60 p.

УДК 004.8:621.391(043.2)

О.М.Сахно
Державний університет
«Київський авіаційний інститут», м. Київ

НЕЙРОННІ ТЕХНОЛОГІЇ В ЕЛЕКТРОННИХ КОМУНІКАЦІЯХ

Сучасні системи електронних комунікацій функціонують в умовах високої динаміки, багатоформатності інформаційних потоків та зростаючих вимог до адаптивності, безперервності та якості обслуговування. В таких умовах дедалі більшої ваги набувають нейронні технології, зокрема штучні нейронні мережі (ШНМ), які здатні не лише аналізувати та передавати інформацію, але й прогнозувати трафік, фільтрувати сигнали, приймати автономні рішення та адаптуватися до змін середовища.

У роботі розглянуто теоретико-методологічні основи застосування нейронних технологій в телекомунікаційних системах. Проаналізовано еволюцію ШНМ — від перцептронів до глибоких трансформерів — та охарактеризовано їхні ключові архітектури: згорткові (CNN), рекурентні (RNN, LSTM), трансформерні та автоенкодери. Розкрито їх застосування для обробки аудіо-, відео- та текстової інформації, зокрема в системах відеоконференцій, розпізнавання мовлення, автоматичного перекладу та голосової взаємодії з користувачем.

Практична частина дослідження присвячена аналізу застосування нейронних технологій у системах обробки, передавання та фільтрації сигналів. Розглянуто використання автоенкодерів для стиснення даних з мінімальними втратами інформації, нейронних декодерів для корекції помилок, а також моделей шумозаглушення (DnCNN, DeepFilterNet, U-Net) в аудіо- та відеосистемах реального часу. Показано переваги таких підходів над класичними методами в умовах нестабільного з’єднання та обмежених ресурсів.

Окрему увагу приділено впровадженню штучного інтелекту в автоматизоване управління телекомунікаційними мережами. Зокрема, розглянуто моделі глибинного навчання та підкріпленого навчання (Deep Q-Learning, A3C, PPO), що використовуються для динамічного розподілу пропускної здатності, оптимізації маршрутів трафіку, передбачення перевантажень та забезпечення якості обслуговування (QoS/QoE).

На основі проведеного аналізу запропоновано модель інтелектуальної системи управління параметрами комунікаційної мережі на основі нейромережевого прогнозування. Система включає функціональний блок обробки даних, самонавчальний модуль, засоби прийняття рішень у реальному часі та механізми моніторингу трафіку. Запропоновану архітектуру адаптовано до умов роботи в мережах п'ятого покоління (5G) з підтримкою мобільності, низької затримки та масштабованості.

Результати дослідження підтверджують перспективність впровадження нейронних технологій у сучасні електронні комунікації. Вони дозволяють суттєво підвищити ефективність, гнучкість та стійкість систем зв'язку до зовнішніх збурень, зменшити витрати на управління мережею та наблизити архітектуру телекомунікацій до когнітивної моделі функціонування.

Запропоновані підходи можуть бути впроваджені в системах зв'язку критичної інфраструктури, хмарних сервісах, платформах відеоспостереження, VoIP-комунікаціях, а також в інтерфейсах «людина–машина». Усі наведені рішення відповідають актуальним технологічним трендам і забезпечують конкурентні переваги в умовах цифрової трансформації суспільства.

УДК 621.391.8 (043.2)

З.О. Сердюк, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

ВОЛОКОННО-ОПТИЧНА ЛІНІЯ З ТЕХНОЛОГІЄЮ СПЕКТРАЛЬНОГО УЩІЛЬНЕННЯ MWDM

У сучасному світі, де потреба у високошвидкісній передачі даних зростає експоненціально, оптичні волокна стали незамінним фундаментом глобальних комунікаційних мереж. Однак, щоб повністю розкрити їхній потенціал, інженери розробили низку передових технологій, що дозволяють передавати величезні обсяги інформації по одному оптоволокну. Однією з найважливіших інновацій у цій галузі є мультиплексування за довжиною хвилі (WDM). Ця технологія дозволяє передавати кілька світлових сигналів різних довжин хвиль (кольорів) одночасно по одному волокну, значно збільшуючи його пропускну здатність. Проте, не всі WDM-системи однакові. З цією метою буде розглянуто та порівняно чотири ключові технології WDM: CWDM, DWDM, MWDM та LWDM.

CWDM: Простота та економічність для коротких відстаней

CWDM (Coarse Wavelength Division Multiplexing), або грубе мультиплексування за довжиною хвилі, є однією з найбільш ранніх та економічно ефективних WDM-технологій. Її назва «грубе» відображає відносно великий інтервал між каналами, який зазвичай становить 20 нм. Це дозволяє використовувати ширший діапазон довжин хвиль, як правило, від 1270 нм до 1610 нм, надаючи до 18 незалежних каналів.

Основною перевагою CWDM є її проста структура. Системи CWDM зазвичай не вимагають оптичних лінійних підсилювачів (OLA), що значно знижує їхню складність та вартість розгортання. Завдяки великому рознесенню каналів, немає потреби у складному балансуванні потужності, що спрощує експлуатацію. Ще однією значною перевагою є низьке енергоспоживання. Це досягається завдяки використанню неохолоджуваних лазерів, які не потребують складної системи контролю температури. Це не тільки зменшує енергоспоживання, але й робить CWDM-пристрої меншими за фізичним розміром.

Все це робить CWDM ідеальним рішенням для коротких відстаней (до 80 км) та застосувань у міських мережах, де вартість кінцевого

обладнання доступу є більш важливою, ніж вартість передачі на довгі відстані.

DWDM: Висока продуктивність для магістральних мереж

На противагу CWDM, DWDM (Dense Wavelength Division Multiplexing), або щільне мультиплексування за довжиною хвилі, розроблене для досягнення максимальної пропускної здатності на великих відстанях. Головна відмінність DWDM полягає у значно меншому інтервалі між каналами, який може становити 0.8 нм, 0.4 нм або навіть 0.2 нм. Це дозволяє розмістити набагато більше каналів в одному волокні – до 40, 80 або навіть 160 (або до 192 в деяких системах), що робить DWDM ідеальною для передачі величезних обсягів даних.

DWDM-системи зазвичай працюють у C-діапазоні (1525-1565 нм) та L-діапазоні (1570-1610 нм), які оптимально підходять для оптичних підсилювачів. Це дозволяє сигналам DWDM долати значно більші відстані без втрати якості, що є критично важливим для магістральних мереж. DWDM-системи мають складнішу структуру, часто включаючи оптичні підсилювачі та компоненти для балансування потужності. Вони також споживають більше енергії через використання охолоджуваних лазерів, які потребують точного температурного контролю для підтримки стабільності довжини хвилі. Лазери DWDM також більші за фізичним розміром. Незважаючи на це, для магістральних мереж, де вартість прокладання нових волокон є надзвичайно високою, DWDM надає неперевершені переваги у збільшенні пропускної здатності і, відповідно, є рентабельним рішенням.

MWDM та LWDM: Рішення для мереж 5G Front-haul

З появою технології 5G виникли нові виклики для мережевої інфраструктури, зокрема для так званих *Front-haul мереж*, які з'єднують базові станції з центральними вузлами. Оператори зіткнулися з дилемою: обирати дорогі активні WDM-системи з високою ефективністю управління чи бюджетні пасивні WDM, які можуть не відповідати майбутнім потребам. У відповідь на це з'явилися інноваційні підходи, такі як *MWDM (Medium Wavelength Division Multiplexing) та LWDM (LAN Wavelength Division Multiplexing).*

MWDM є унікальним рішенням, спеціально розробленим для 5G Front-haul. Його принцип полягає у використанні існуючих 6 хвиль 25G CWDM-спектру. Проте, ключова інновація полягає у додаванні TEC (термоелектронного охолоджувача) для точного контролю температури. Це дозволяє змістити кожну з початкових 6 хвиль вліво та

вправо на 3.5 нм, ефективно створюючи 12 довжин хвиль. Таке рішення не тільки значно економить волоконні ресурси, але й повторно використовує вже зрілу індустріальну цепочку CWDM, що робить його економічно вигідним. MWDM дозволяє задовольняти потреби 5G у прямих з'єднаннях на відстані до 10 км, забезпечуючи необхідну кількість каналів для всіх фронтальних мереж 5G.

LWDM (LAN Wavelength Division Multiplexing), або мультиплексування за довжиною хвилі для локальних мереж, є ще одним підходом, що базується на каналах Ethernet (LAN WDM). Його рознесення каналів становить від 200 до 800 ГГц, що розміщує його між щільним інтервалом DWDM (100 ГГц, 50 ГГц) та широким інтервалом CWDM (близько 3 ТГц). LWDM також є частиною рішення для 5G Front-haul та інших високошвидкісних застосувань. Ця технологія використовує DML (Directly Modulated Laser) на передавальній стороні оптичного модуля та PIN (Photo Diode) на приймальній стороні. LWDM також демонструє потенціал для спільного використання індустріальної цепочки з високошвидкісними стандартами, такими як 400G LR8 та LR4, що свідчить про її перспективність для майбутніх мереж.

Висновок

У підсумку, вибір технології WDM залежить від конкретних потреб мережі. CWDM є економічним та простим рішенням для коротких відстаней, ідеально підходячи для міських та корпоративних мереж. DWDM пропонує неперевершену пропускну здатність та дальність передачі, що робить її незамінною для магістральних та міжміських мереж. А MWDM та LWDM представляють собою інноваційні та гнучкі рішення, що виникають у відповідь на специфічні вимоги 5G Front-haul, забезпечуючи оптимальний баланс між вартістю, продуктивністю та ефективністю використання волоконних ресурсів.

Список використаних джерел

1. D. Zhang *et al*., "Toward Manageable Cost-Effective 5G C-RAN: Semi-Active Front-Haul by Multi-Carrier Pilot-Tone OAM and MWDM," in *IEEE Wireless Communications*, vol. 30, no. 5, pp. 58-66, October 2023

2. ITU-T Recommendation G.694.2 (02/2015) - Spectral grids for WDM applications: CWDM wavelength grid.

3. ITU-T Recommendation G.694.1 (02/2012) - Spectral grids for WDM applications: DWDM wavelength grid.

УДК 621.391

Д.А. Сіньков
Державний університет
«Київський авіаційний інститут», м. Київ

ІНТЕЛЕКТУАЛЬНІ СИСТЕМИ ВИЯВЛЕННЯ ОБ'ЄКТІВ ЗА ДОПОМОГОЮ БПЛА

Сучасні технології автоматизації відіграють дедалі важливішу роль у різноманітних сферах діяльності людини, зокрема в моніторингу, охороні, розвідці, рятувальних операціях та екологічному контролі. Одним із ключових інструментів, що активно впроваджуються у ці сфери, є безпілотні літальні апарати (БПЛА). Завдяки своїй мобільності, здатності до автономної роботи та можливості охоплення значної території, дрони стали основою для розвитку новітніх цифрових рішень, зокрема систем автоматичного аналізу візуальної інформації.

Одним із найперспективніших напрямів застосування БПЛА є розпізнавання наземних об'єктів у режимі реального часу. Ця задача набуває особливої актуальності в умовах, коли необхідно оперативно приймати рішення на основі даних, отриманих із камер дронів, без прямого втручання оператора. Завдяки розвитку штучного інтелекту, зокрема технологій глибинного навчання та комп'ютерного зору, стало можливим створення інтелектуальних систем, здатних самостійно аналізувати зображення та виявляти об'єкти різних типів — транспортні засоби, людей, будівлі, техніку тощо.

Актуальність теми дослідження обумовлена нагальною потребою в оперативному та точному обробленні візуальних даних, які надходять з бортових сенсорів БПЛА. В умовах динамічного середовища, коли змінюються освітлення, ракурси, швидкість руху, а також присутні візуальні перешкоди, система розпізнавання має демонструвати високу точність та стабільність.

У межах дослідження було розглянуто процес побудови системи автоматичного розпізнавання наземних об'єктів з використанням глибинних нейронних мереж. Основними етапами створення такої системи є: формування навчального набору даних (dataset), проведення розмітки зображень (annotation), вибір відповідної архітектури моделі (наприклад, YOLOv5s), навчання моделі (training)

з урахуванням особливостей апаратної платформи, а також подальше впровадження у практичне середовище.

Особлива увага приділялася тому, щоб обрана модель працювала ефективно в умовах обмежених обчислювальних ресурсів, які характерні для вбудованих систем. Використовувалися методи машинного навчання, здатні обробляти зображення в реальному часі. Тренування моделі проводилося на основі датасетів, що містять приклади об’єктів із різних класів, з метою досягнення високої узагальнювальної здатності. У процесі налаштування моделі досліджувалися параметри кількості епох, швидкості навчання, функцій втрат, а також критерії оцінки ефективності.

Результатом дослідження стало створення робочого прототипу системи, здатної розпізнавати об’єкти на зображеннях у реальному часі з мінімальною затримкою. Проведене тестування в умовах, наближених до реальних показало, що модель здатна стабільно працювати та виявляти об’єкти з високою точністю. Було встановлено, що ключовими чинниками успішного функціонування є баланс між обсягом навчального набору та складністю архітектури нейромережі.

Загалом, поєднання технологій комп’ютерного зору, глибинного навчання та мобільності БПЛА дозволяє створювати автономні інтелектуальні системи спостереження, які можуть діяти незалежно від людини. Результати дослідження можуть бути використані для удосконалення. Перспективи подальших досліджень полягають у підвищенні точності моделей, зменшенні споживання ресурсів та адаптації систем до нових, більш складних сценаріїв застосування.

Список використаних джерел

1. Bochkovskiy A., Wang C.-Y., Liao H.-Y. M. YOLOv4: Optimal Speed and Accuracy of Object Detection // arXiv preprint arXiv:2004.10934. – 2020.

2. Redmon J., Farhadi A. YOLOv3: An Incremental Improvement // arXiv preprint arXiv:1804.02767. – 2018.

3.Ultralytics YOLOv5 documentation. – https://docs.ultralytics.com

4.Goodfellow I., Bengio Y., Courville A. Deep Learning. – MIT Press, 2016.

5. https://www.mdpi.com/1424-8220/24/18/6053

УДК 004.8:004.932

Я.Р. Смолій
Державний університет
«Київський авіаційний інститут», м. Київ

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЦИФРОВІЙ ОБРОБЦІ ЗОБРАЖЕНЬ

Штучний інтелект відіграє важливу роль у цифровій обробці зображень, усуваючи недоліки класичних методів, таких як відновлення, фільтрація чи вейвлет-перетворення, зокрема недостатню точність, низьку адаптивність та обмежену ефективність при роботі зі складними чи пошкодженими зображеннями. Завдяки алгоритмам машинного та глибоке навчання штучний інтелект самостійно аналізує, відновлює та покращує якість зображення у реальному часі, успішно подолавши обмеження класичних методів, забезпечуючи вищу точність, адаптивність і здатність працювати з великими обсягами складних і зашумлених даних, що особливо важливо для сфер, наприклад, медична діагностика, системи відеоспостереження та автономний транспорт, де критичною є швидкість і точність обробки.

У дослідженні, було використане медичне рентгенівське зображення, згенероване за допомогою моделей штучного інтелекту, яке оброблялось у середовищі MATLAB із застосуванням Image Processing Toolbox. Застосування штучного інтелекту дозволило отримати зображення високої якості, що стало хорошою основою для подальшої цифрової обробки та збереженням конфіденційних даних.

Дослідження охоплює ключові методи цифрової обробки зображень, а саме – відновлення, фільтрацію, вейвлет-перетворення та стиснення. У процесі відновлення було проаналізовано ефективність інверсної фільтрації, фільтр Вінера та сліпої деконволюції. Найвищі показники якості за метриками PSNR і SSIM продемонструвала сліпа деконволюція, хоча вона потребує значно більше часу. Для зменшення шумів застосовувалися маскова та медіанна фільтрації. Маскова фільтрація показала кращу якість збереження структури, тоді як медіанна – вищу швидкість. Вейвлет-перетворення із застосуванням функцій Хаара та Добеші також продемонстрували високу ефективність, де функція Хаара забезпечує кращу точність відновлення, а Добеші – оптимальний баланс між швидкістю та

якістю. Щодо стиснення, порівняння форматів JPEG (зі втратами) та PNG (без втрат) виявило, що JPEG забезпечує більший ступінь стиснення, натомість PNG дозволяє зберігати максимальну якість зображення.

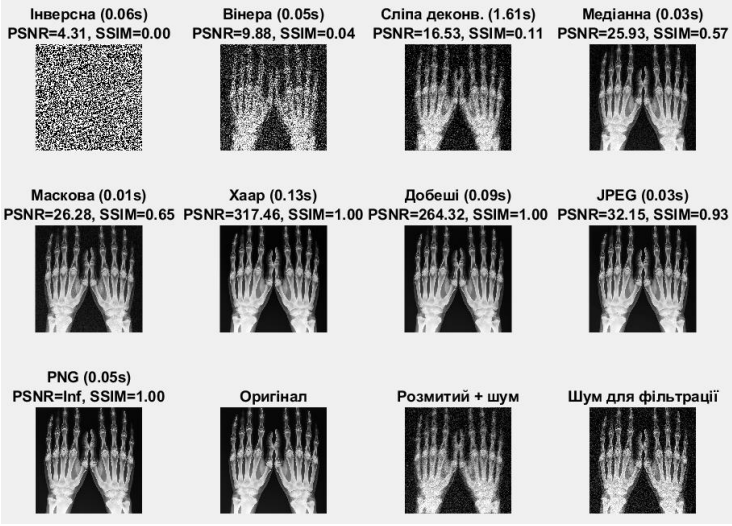


Рис.1 Результат класичних методів обробки зображень

Вибір конкретних методів варіюється залежно від пріоритетів між точністю, швидкістю та збереженням якості, що дозволяє адаптувати обробку до різних практичних завдань.

Результати досліджень підтверджують ефективність поєднання класичних методів цифрової обробки зображень із алгоритмами штучного інтелекту. Розглянуті класичні методи, значно покращують якість зображення, що підтверджено високими показниками PSNR і SSIM. З іншого боку, використання ШІ забезпечує більш точне виявлення деталей, адаптивність до різних типів зображень, а також автоматизацію складних завдань у реальному часі. Інтеграція нейронних мереж дозволяє значно підвищити точність аналізу та знизити похибки та попри широкі можливості, застосування ШІ також вимагає вирішення питань конфіденційності даних, необхідності великих навчальних наборів та значних фінансових витрат на тренування складних моделей. Запропонований підхід є ефективним для широкого спектра застосувань, особливо для медичних зображень, які розглянуті у дослідженні.

УДК 004.056.5:004.7 (043.2)

А.В. Сова, Д.І. Бахтіяров
Державний університет
«Київський авіаційний інститут», м. Київ

СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ КОРПОРАТИВНИХ МЕРЕЖ

Вступ. В умовах стрімкої цифровізації суспільства та глобалізації бізнес-процесів, корпоративні мережі перетворилися на фундаментальну інфраструктурну складову для переважної більшості підприємств, державних установ та освітніх закладів. Вони забезпечують обмін даними, доступ до критично важливих ресурсів та взаємодію між співробітниками, партнерами і клієнтами. Однак, паралельно зі зростанням залежності від мережевих технологій, невпинно збільшується кількість та складність кіберзагроз. Зловмисники постійно вдосконалюють свої методи, спрямовані на отримання несанкціонованого доступу до конфіденційної інформації, порушення працездатності систем, фінансові шахрайства та промисловий шпіонаж. Такі загрози, як витік даних, неавторизований доступ до систем, цілеспрямований саботаж ІТ-інфраструктури та інфільтрація шкідливого програмного забезпечення (ШПЗ), становлять реальну та значну небезпеку для стабільного функціонування та економічної безпеки будь-якої організації. У світлі зазначених викликів, проблема забезпечення надійного та ефективного захисту корпоративних мереж набуває особливої актуальності. Це вимагає не просто впровадження окремих засобів безпеки, а розробки та реалізації комплексної, багатоешелонованої стратегії, здатної адаптуватися до динамічного ландшафту кіберзагроз. Продуманий підхід до кібербезпеки повинен враховувати як технологічні, так і організаційні аспекти, а також постійно еволюціонувати для протидії новим векторам атак. Дана доповідь присвячена аналізу сучасних підходів до захисту корпоративних мереж, систематизації ключових методів та технологій, а також представленню моделі захищеної мережевої інфраструктури.

Постановка проблеми. Основною метою даного дослідження є аналіз сучасних стратегій та технологічних рішень для забезпечення комплексного захисту корпоративних мереж в умовах постійно зростаючих кіберзагроз. Для досягнення поставленої мети необхідно вирішити наступні завдання: систематизувати основні загрози безпеці

корпоративних мереж, включаючи витік конфіденційних даних, несанкціонований доступ до інформаційних ресурсів, атаки на відмову в обслуговуванні, розповсюдження шкідливого програмного забезпечення та інші деструктивні впливи; проаналізувати ключові компоненти сучасної системи інформаційної безпеки мережі, такі як шифрування трафіку, механізми контролю та управління доступом, принципи розмежування прав користувачів, системи мережевого моніторингу та аудиту, а також стратегії резервного копіювання та відновлення даних; розглянути ефективність та особливості застосування сучасних технологій захисту, зокрема, систем виявлення та запобігання вторгненням (IDS/IPS), технологій віртуальних приватних мереж (VPN), методів сегментації мережі для ізоляції критичних ресурсів та зменшення поверхні атаки; оцінити вплив людського фактора на загальний рівень безпеки корпоративної мережі та визначити важливість розробки чітких політик безпеки, а також регулярного навчання персоналу основам кібергігієни та правилам безпечної поведінки в цифровому середовищі; розробити та описати концептуальну модель корпоративної мережі з інтегрованою багаторівневою системою захисту, що базується на принципі "найменших привілеїв" та включає сучасні програмно-апаратні засоби захисту; обґрунтувати ефективність запропонованої моделі шляхом теоретичного аналізу її стійкості до поширених типів кібератак та визначити напрямки для її потенційної адаптації та подальших досліджень. Вирішення цих завдань дозволить сформувати цілісне уявлення про сучасні підходи до побудови захищених корпоративних мереж та запропонувати практичні рекомендації для підвищення рівня їх інформаційної безпеки.

Сучасні підходи до захисту корпоративних МЕРЕЖ. Забезпечення безпеки корпоративних мереж є багатогранним завданням, що вимагає комплексного підходу, який охоплює технологічні, організаційні та процедурні аспекти. Сучасні стратегії захисту базуються на принципі ешелонованої оборони (Defense in Depth), де відмова одного рівня безпеки компенсується іншими. Фундаментальними складовими інформаційної безпеки мережі є шифрування трафіку, контроль доступу та розмежування прав, мережевий моніторинг та резервне копіювання. Криптографічний захист даних під час їх передачі, що досягається протоколами TLS/SSL, IPsec та WPA2/3, є обов'язковим для запобігання перехопленню та модифікації інформації, доповнюючись шифруванням даних у стані спокою. Ефективні механізми автентифі-

кації, авторизації та аудиту (AAA), включаючи надійні парольні політики, багатофакторну автентифікацію (MFA) та принцип найменших привілеїв (PoLP) з рольовими моделями доступу (RBAC), формують основу контролю доступу. Постійний моніторинг мережевого трафіку та системних журналів, часто за допомогою систем SIEM, дозволяє своєчасно виявляти підозрілу активність, а наявність актуальних резервних копій та перевіреного плану відновлення забезпечує стійкість до атак та збоїв.

На цих засадах базується застосування сучасних технологій та методів захисту. Системи виявлення (IDS) та запобігання (IPS) вторгненням, як мережевого (NIDS/NIPS), так і хостового (HIDS/HIPS) типів, аналізують трафік та системні події для виявлення та блокування загроз. Технології віртуальних приватних мереж (VPN), що використовують протоколи IPsec або OpenVPN, створюють захищені канали зв'язку через публічні мережі, забезпечуючи безпеку віддаленого доступу та об'єднання філій. Важливим методом зниження ризиків є сегментація мережі за допомогою VLAN та підмереж, що ізолює критичні ресурси та обмежує поширення атак, доповнюючись міжмережевими екранами (Firewalls). Сучасні міжмережеві екрани нового покоління (NGFW) пропонують розширені функції, такі як глибока інспекція пакетів (DPI) та контроль додатків, слугуючи першою лінією оборони. Технологія NAT (Network Address Translation) також сприяє безпеці, приховуючи внутрішню структуру IP-адресації.

Однак, навіть найдосконаліші технології не можуть повністю нівелювати людський фактор. Соціальна інженерія, фішинг та недотримання політик безпеки залишаються поширеними векторами атак. Тому розробка та впровадження чітких політик безпеки, що регламентують усі аспекти використання інформаційних ресурсів, та регулярне навчання персоналу основам кібергігієни, розпізнаванню загроз та правилам безпечної поведінки є невід'ємною частиною комплексної стратегії захисту.

В рамках дослідження була розроблена практична модель корпоративної мережі з багаторівневою системою захисту. Її архітектура передбачає демілітаризовану зону (DMZ) для публічних серверів, сегментацію внутрішньої мережі на логічні зони (VLAN), впровадження принципу "найменших привілеїв", використання NGFW на периметрі та між сегментами, застосування NAT, централізований сервер журналювання (Syslog/SIEM), VPN-сервер для віддаленого доступу та ін-

теграцію NIDS/NIPS. Тестування цієї моделі на стійкість до симульованих базових атак, таких як підбір паролів, ARP-спуфінг та міжмережеве сканування, продемонструвало високу ефективність реалізованих захисних механізмів: міжмережеві екрани блокували неавторизований доступ, IDS фіксували аномалії, а сегментація обмежувала поширення умовних атак.

Висновок. Проведене дослідження підтверджує, що побудова надійної та ефективної системи захисту корпоративної мережі є складним, але критично важливим завданням, що вимагає цілісного, проактивного та адаптивного підходу. Недостатньо покладатися лише на окремі технологічні рішення; успіх залежить від їх грамотної інтеграції, узгодженості з бізнес-процесами та постійного вдосконалення відповідно до еволюції кіберзагроз. Ключовими аспектами сучасних підходів до захисту є ешелонована оборона, що поєднує шифрування, суворий контроль доступу, безперервний моніторинг, сегментацію мережі та надійне резервне копіювання. Технології, такі як системи виявлення та запобігання вторгненням, VPN та міжмережеві екрани нового покоління, відіграють важливу роль у протидії сучасним атакам. Однак, не менш значущим є людський фактор: розробка чітких політик безпеки та систематичне навчання персоналу основам кібергігієни суттєво підвищують загальний рівень захищеності.

Список використаних джерел

1. Кузнєцов О. О., Євсеєв С. П., Корольов Р. В. Моделі та методи забезпечення інформаційної безпеки в корпоративних мережах. Харків: Вид-во ХНЕУ, 2021. 288 с.

2. Сіденко І. В., Прокопенко Т. М. Сучасні технології захисту інформації в комп'ютерних мережах. Київ: КПІ ім. Ігоря Сікорського, 2022. 350 с.

3. Stallings, W., & Brown, L. Computer Security: Principles and Practice. 4th ed. Pearson, 2024. 768 p.

4. Whitman, M. E., & Mattord, H. J. Principles of Information Security. 7th ed. Cengage Learning, 2023. 736 p.

5. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія. Практика. Застосування. Харків: Форт, 2019. 870 с.

UDC 004.056

I.B. Tregubenko
State Scientific and Research Institute of Cybersecurity Technologies and Information Protection, Kyiv

VULNERABILITIES OF INTELLIGENT CLOUD APPLICATIONS WITH MICROSERVICE ARCHITECTURE

Methods of building, basic architectures and technologies, including software, for creating modern information systems are constantly evolving. The deployment of intelligent technologies, quantum computing, and cloud-based heterogeneous ecosystems has a significant impact on these processes. At the same time, the number and quality of vulnerabilities of such information ecosystems and their components are increasing. The likelihood of confidential information leakage and possible end-user losses are increasing.

It is advisable to study the changes and effectiveness of protection technologies in the case of building intelligent cloud applications based on modern types of architecture [1, p.727-729]. One of the most widely used and relevant approaches at present is the approach to building software based on microservice architecture. According to Gartner's report [2, p.1], about 74% of enterprises that participated in the survey use microservices, and an additional 23% of enterprises plan to use microservices.

We should consider the features of microservices. The advantages include: increased efficiency and reduced costs, scalability according to requirements, improved fault tolerance, increased developer productivity, navigation of testing complexity. The main disadvantages are: higher complexity in management, delay and complexity of network communication, data consistency risk, limited code reuse, dependence on DevOps, difficulty in global testing and debugging.

Modern cloud environments are complex and heterogeneous, consisting of many different components. These include application development servers, various services used by developers, customer applications, hosting services, and more. There is constant end-to-end authentication between these components. This interaction differs significantly from user authentication processes directly on the cloud platform and in numerous user applications. With technical authentication, due to the fact that threats at this level have long been ignored and not taken into account, there are many

opportunities to act on behalf of the developer. These access technologies are currently the least secure.

Modern software development practices rarely use the principle of building a security system at the design stage of a software product. Undoubtedly, this leads to an increase in the likelihood of cybersecurity breaches during the operation of the software system and the entire information cloud ecosystem. There are more vulnerabilities.

As a specific example, we can consider the research[3, p.727-743] that studied modern WeChat applications and microservices to identify vulnerabilities. Baidu applications were also investigated. This example proved the existence of non-obvious types of vulnerabilities that are caused by development technologies and features of microserver architecture.

Most often, the vulnerability is provided by strong authentication in the application for the purposes of developers. Moreover, a study [3, pp.727-743] shows that it is possible to stop the application from functioning both for an attacker who has his own account on the relevant platform and for an attacker who does not have registration and his own account. At the same time, such an attacker will be able to access confidential information, use phishing, organize spam emails, etc.

Since the heterogeneous and multifactorial nature of threats in cyberspace is rapidly changing, both in terms of technology and basic architecture, traditional approaches are not working. The search for new algorithms and methods of threat detection is urgent.

References

1. Tregubenko I.B., Kotetunov V.Y. Problems of information security of hybrid integration ecosystems based on cloud technologies. // March Scientific Discourse 2025 on the topic: "Synergy of Education, Science and Business in the Age of Global Transformations": collection of materials of the III International Scientific and Practical Conference: NGO "Scientific and Educational Innovation Center for Social Transformations",2025-780p-pp.727-729. ISBN 978-617-8431-06-8. DOI: https://doi.org/10.54929/conf_reicst_27_02_2 (In Ukrainian)

2. Microservices Architecture: Have Engineering Organizations Found Success? Gartner. Peer community, URL: https://www.gartner.com/peer-community/oneminuteinsights/omi-microservices-architecture-have-engineering-organizations-found-success-u6b

3. S. Baskaran, L. Zhao, M. Mannan, A. Youssef. Measuring the Leakage and Exploitability of Authentication Secrets in Super-apps: The WeChat Case. RAID '23: Proceedings of the 26th International Symposium on Research in Attacks, Intrusions and Defenses Pages 727–743 https://doi.org/10.1145/3607199.3607236

УДК 004.056.5 (043.2)

Д. Б. Хмель, Д.І. Бахтіяров
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ВИЯВЛЕННЯ ЗАГРОЗ В IoT-МЕРЕЖАХ МОДЕЛЕЙ МАШИННОГО НАВЧАННЯ

Інтенсивне впровадження концепції Інтернету речей (IoT) у різноманітні сфери діяльності – від побутових систем до критичної інфраструктури – призводить до зростання кількості підключених пристроїв із мінімальними обчислювальними можливостями. Ці пристрої часто не мають вбудованих механізмів захисту, що створює серйозні загрози для їхньої безпечної експлуатації. Переважна більшість класичних сигнатурних систем виявлення загроз (IDS) демонструє обмежену ефективність у виявленні нових, модифікованих або прихованих атак, особливо в динамічному IoT-середовищі. З огляду на це, виникає потреба в розробці більш гнучких та адаптивних механізмів захисту, які зможуть функціонувати у режимі реального часу, адаптуватися до змін у поведінці мережевого трафіку та забезпечувати високий рівень точності при роботі з обмеженими ресурсами. Одним із перспективних напрямів розв'язання цієї проблеми є інтеграція методів машинного навчання, здатних формувати профілі поведінки, виявляти аномалії та ефективно класифікувати трафік навіть у відсутності сигнатур.

Розроблена система виявлення загроз для IoT-середовища базується на методах машинного навчання та враховує особливості SDN-архітектур. Для навчання моделі використано об'єднаний датасет із трьох джерел: Normal_data.csv (нормальний трафік), metasploitable-2.csv (шкідлива активність) та OVS.csv (трафік, сформований у середовищі Open vSwitch). Такий підхід дозволив забезпечити варіативність навчальної вибірки та адаптацію моделі до реальних умов. Попередня обробка включала відбір тільки тих ознак, які доступні SDN-контролеру, нормалізацію Min-Max, кодування міток і балансування класів за допомогою SMOTE. Це дозволило

зменшити викривлення у навчанні та забезпечити стабільну роботу моделі на гетерогенних даних.

Для підвищення ефективності застосовано GridSearchCV з 5-кратною крос-валідацією для налаштування гіперпараметрів. У ході дослідження було протестовано низку моделей машинного навчання, зокрема k-Nearest Neighbors, Decision Tree, SVM, Naive Bayes, CNN, MLP, а також рекурентну нейронну мережу LSTM. За результатами порівняльного аналізу найкращі показники досягла модель Random Forest, яка забезпечила оптимальний баланс між точністю класифікації, швидкодією обробки та помірним рівнем використання обчислювальних ресурсів. Інші моделі, зокрема нейромережеві архітектури, показали нижчу ефективність у контексті IoT-середовищ, де важливою вимогою є економне використання обчислювальних потужностей. Запропонована система добре адаптується до програмно-конфігурованих (SDN) інфраструктур, здатна працювати в режимі, наближеному до реального часу, та демонструє високий рівень точності при класифікації загроз. Модель Random Forest досягла точності 98,7% та F1-score понад 0,97, що підтверджує її придатність для впровадження у критично важливих сегментах IoT-інфраструктур.

Порівняльний аналіз показав, що ця модель демонструє кращий баланс між точністю, швидкістю обробки та стійкістю до різноманітних типів загроз у порівнянні з нейромережевими підходами. Практична реалізація системи свідчить про її придатність до роботи в умовах обмежених обчислювальних ресурсів та її ефективність у виявленні як відомих, так і нових атак. Розроблена система може бути використана як основа для впровадження в галузях, що потребують високого рівня безпеки, зокрема у промисловій автоматизації, енергетиці, транспортній логістиці та медицині. Крім того, результати роботи можуть слугувати базисом для подальшого розвитку розподілених аналітичних систем у сфері кібербезпеки.

УДК 629.735.058:681.586:004.896

Д.В.Черненко
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА КОНТРОЛЮ ВИСОТИ ПОЛЬОТУ БЕЗПІЛОТНОГО ЛІТАЛЬНОГО АПАРАТУ

У сучасних умовах використання безпілотних літальних апаратів (БПЛА) охоплює широкий спектр завдань — від моніторингу навколишнього середовища до виконання високоточних операцій у складних умовах. Забезпечення точного контролю висоти польоту є критично важливим для безпеки польоту, стабільності апарата та ефективного виконання місій. Сьогодні на ринку існує багато рішень, але більшість із них базуються на одній технології, що обмежує їхню універсальність і точність у різних середовищах. Саме тому актуальним є підхід до комбінування методів вимірювання висоти, зокрема на основі GPS та Lidar.

Основна частина проєкту присвячена аналізу, порівнянню та реалізації систем, що поєднують переваги двох найбільш поширених технологій: супутникової навігації (GPS) та лазерного сканування (Lidar). Розглянуто особливості роботи кожної з систем, їхні переваги, недоліки та типові помилки вимірювання. Виявлено, що використання тільки GPS може дати похибки у визначенні висоти, особливо в міських умовах або поблизу природних перешкод. У той час як Lidar забезпечує значно кращу абсолютну точність, однак обмежується в умовах сильного туману або опадів.

Результатом дослідження стала розробка інтегрованої системи контролю висоти, яка поєднує дані від GPS-модуля та Lidar-датчика, працюючи на платформі Arduino. Була написана програма, яка дозволяє в режимі реального часу отримувати, обробляти та фільтрувати дані для отримання максимально точного показника висоти. Такий підхід дозволяє компенсувати недоліки кожної окремої технології й отримати стабільні результати навіть у складних умовах.

Крім технічної реалізації, були проаналізовані можливі сфери застосування запропонованої системи: аграрні безпілотники, геодезичні роботи, інспекція інфраструктури, логістика, а також рятувальні операції. У всіх зазначених галузях точність висоти визначає якість виконання завдання, тому впровадження комбінованої системи виглядає як ефективне рішення.

Проведені випробування продемонстрували стабільність і надійність роботи запропонованої системи. Вона відзначається простотою реалізації, невеликою вартістю компонентів та гнучкістю в налаштуванні, що робить її доступною для широкого кола користувачів — від аматорських проєктів до промислових рішень. З огляду на темпи розвитку БПЛА, подальші дослідження можуть бути спрямовані на інтеграцію й інших сенсорів, наприклад, барометричних або оптичних, з метою підвищення адаптивності системи.

Таким чином, запропонована інтегрована система контролю висоти на базі GPS і Lidar забезпечує значно кращу точність у порівнянні з традиційними методами, що відкриває нові можливості для точного та безпечного управління польотом безпілотних літальних апаратів.

UDC 658.841.2 (043.2)

M.S. Chubenko
State University
"Kyiv Aviation Institute", Kyiv

Intelligent system of information processing based on RFID identification

The use of self-service technologies in retail is gaining popularity due to its ability to improve the shopping process, reduce queues and increase store efficiency. One of the most promising technologies is the use of RFID and artificial intelligence (AI) to automate the process of product identification. This thesis is devoted to the development of an intelligent self-service system that uses these technologies to ensure accurate and fast product detection without the need for human intervention.

Self-service systems and their features: this section has described the main characteristics and advantages of self-service systems, as well as identified their disadvantages. Self-service systems can significantly reduce the workload of cashiers, reduce personnel costs and speed up the purchase process for the end consumer. However, traditional systems have limitations, in particular in cases of damaged barcodes or problems with clear reading of labels. Architecture of an intelligent self-service system: the main components of the system are considered, which include RFID readers, cameras for reading labels and user interfaces. The settings of RFID readers are separately considered, including RSSI parameters, which ensure reading accuracy at all stages of user interaction with the system. AI-based product detection mechanism: this section describes how the system uses AI to automatically recognize products using OCR (optical character recognition) and computer vision technologies. Each product is given a unique identification, allowing for accurate identification of the user's selection even in the case of damaged RFID tags. Product Detection Process and RFID Integration: The process of product detection based on RFID and AI is discussed. It details how RFID readers work to quickly identify products, and how the system uses images to supplement detection when tags are damaged or blocked by other products. It also describes the importance of RFID reader settings for accurate and fast scanning.

Evaluation of results and recommendations: the section evaluates the effectiveness of the developed system based on the test results. The system

demonstrates high accuracy and speed in reading goods, however, it is recommended to improve user interaction and adaptability to different lighting conditions and label shapes. The developed intelligent self-service system has significant potential to improve the shopping process, ensuring high accuracy and speed of product identification using RFID and AI. Further development of technology, improvement of AI algorithms and increase in reliability of RFID systems will significantly increase the efficiency of such solutions, reduce the impact of the human factor and reduce costs for business.

УДК 621.396.13:004.056.5

Д.К. Шевченко
Державний університет
«Київський авіаційний інститут», м. Київ

Threat Analysis Systems in 5G Networks: Architecture, Challenges, and Future Directions

The fifth generation (5G) networks are becoming the backbone of modern digital infrastructures, offering unprecedented data transfer rates, low latency, and massive device connectivity. However, the adoption of advanced network virtualization (SDN, NFV), multi-segment architecture (network slicing), and open interfaces (O-RAN, MEC) also brings increased information security risks. The key challenges include the growing number of attack vectors, complex interactions of heterogeneous components, and the need to comply with high standards of service quality and data protection.

As part of the review, particular attention was paid to the architecture of 5G networks, including the interaction of key components—user equipment (UE), the radio access network (RAN), multi-access edge computing (MEC), and the service-based architecture (SBA) core. Understanding the layered and dynamic architecture is essential for identifying potential attack surfaces and vulnerabilities. These include not only traditional network vulnerabilities, but also new risks associated with virtualization and open interfaces.

The analysis emphasizes that threat analysis systems must consider the unique features of 5G networks. Conventional security models that rely solely on perimeter-based defenses are no longer sufficient. Instead, flexible and adaptive threat analysis systems are required to monitor complex interactions across virtualized and physical network segments. Such systems should combine signature-based methods for known threats with behavioral analytics and advanced machine learning techniques for detecting new and evolving attack patterns.

Among the key challenges faced by threat analysis systems in 5G networks are the need to process large volumes of encrypted traffic in real time, maintain high detection accuracy, and ensure minimal latency to support mission-critical services such as URLLC. Furthermore, these systems must be compatible with 3GPP, ITU, and ETSI security standards, and be capable of dynamic reconfiguration to address emerging threats.

The review concludes that future research should focus on the development of integrated, hybrid threat analysis systems that can operate seamlessly

across the entire 5G architecture—from the edge and fog layers to the cloud. Promising directions include the use of federated learning for distributed threat detection without compromising data privacy, the enhancement of security analytics for MEC and network slicing, and the integration of threat intelligence feeds for proactive defense. By addressing these challenges, threat analysis systems can play a crucial role in ensuring the resilience and security of 5G networks in the face of constantly evolving cyber threats.

УДК 681.518.5

В.А. Шемет
Державний університет
«Київський авіаційний інститут», м. Київ

СУЧАСНІ АКТИВНІ ТА ПАСИВНІ ЗАСОБИ ПРОТИДІЇ ТЕХНІЧНИМ КАНАЛАМ ВИТІКУ ІНФОРМАЦІЇ

В теперішній час цифровізації стає актуальним питанням захисту інформації від витоку інформації через технічні канали (ТКВІ). ТКВІ виникають внаслідок побічних фізичних процесів, таких як електромагнітні випромінювання, акустичні коливання та інші, що супроводжують роботу технічних засобів обробки інформації.

Такі витоки є особливо небезпечними, оскільки вони відбуваються непомітно, без втручання в системи або носії. У багатьох випадках користувачі навіть не підозрюють, що їхні пристрої можуть стати джерелом втрати конфіденційної інформації. Тому проблема виявлення та нейтралізації ТКВІ є пріоритетною в сучасній системі інформаційної безпеки.

Ефективний захист таким загрозам вимагає застосування активних та пасивних засобів захисту.

Застосування лише одного виду засобів або тільки активних, або лише пасивних зазвичай є недостатнім. Комплексний підхід дозволяє врахувати різноманітні вектори загроз та забезпечити багаторівневу оборону інформаційних ресурсів.

Активні засоби захисту передбачають створення перешкод для потенційних засобів перехоплення інформації. До них належать генератори електромагнітного та акустичного шуму, що маскують сигнали, генератори імпульсів для виявлення і знешкодження закладних пристроїв, а також зашумлення електроживлення, що ускладнює витік інформації через електромережі.

Активні засоби зазвичай застосовуються в режимних приміщеннях або у випадках, коли ризик витоку є високим. Наприклад, у залах для проведення конфіденційних нарад використовуються спеціальні акустичні системи, що генерують шум у діапазоні людської мови, роблячи її нерозбірливою для мікрофонів прихованого запису.

Пасивні засоби захисту спрямовані на зменшення або усунення побічних випромінювань та коливань, що можуть стати каналами витоку інформації. Це реалізується через екранування та заземлення те-

хнічних засобів, звукоізоляцію приміщень, фільтрацію електроліній, використання діелектричних вставок у комунікаціях, а також організаційні обмеження, як-от контроль доступу та заборона сторонніх пристроїв під час конфіденційної роботи.

До пасивних заходів належить також правильне розміщення обладнання в приміщеннях наприклад, віддалення комп'ютерів від зовнішніх стін або вікон, застосування сейфів для зберігання пристроїв у неробочий час, використання спеціального кабелю з екранованою оплiткою.

Комбіновані засоби захисту це коли поєднуються активні та пасивні методи для досягнення максимального ефекту. Наприклад, ми поєднуємо екранування разом із генераторами шуму це забезпечить більш надійний захист від ТКВІ.

У реальних системах захисту завжди рекомендується поєднувати методи, створюючи багаторівневу структуру безпеки. Такий підхід дає змогу компенсувати слабкі сторони одного типу захисту сильними сторонами іншого.

Ефективний та сучасний захист інформації від технічних каналів витоку вимагає особливого комплексного підходу, що включає в себе активні та пасивні засоби захисту, тобто комбінований. Застосування сучасних технологій та регулярний моніторинг каналів витоку дозволить нам значно знизити ризик несанкціонованого доступу до конфіденційної інформації та витоку інформації через технічні канали.

Крім того, важливо проводити регулярне навчання персоналу з правил поводження з інформацією, впроваджувати політики безпечного користування пристроями, проводити періодичну перевірку на наявність закладних пристроїв та сканування спектрів електромагнітних випромінювань. Без людського чинника навіть найдосконаліші засоби технічного захисту можуть бути малоефективними.

УДК 621.391

М.О. Шихов
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА ЗАХИЩЕНОЇ API-ІНФРАСТРУКТУРИ ДЛЯ ТЕЛЕКОМУНІКАЦІЙНИХ СЕРВІСІВ

Телекомунікаційні компанії все частіше стикаються з проблемами безпеки при впровадженні API для своїх сервісів. За даними OWASP, кількість атак на API зросла на 40% за останній рік, при цьому телекомунікаційний сектор є однією з найбільш вразливих галузей через обробку персональних даних користувачів та фінансової інформації. Основними загрозами є несанкціонований доступ до даних абонентів, компрометація паролів та токенів автентифікації, а також атаки на доступність сервісів. Існуючі підходи до захисту API часто не враховують специфічні вимоги телекомунікаційних систем: необхідність обробки великої кількості запитів від абонентів, вимоги до швидкості відповіді та високі стандарти надійності роботи. Аналіз літературних джерел та досвіду провідних операторів показав, що найпоширенішими рішеннями є використання REST API з механізмами автентифікації OAuth 2.0 та JWT токенами, проте питання їх практичної реалізації для телекомунікаційної галузі залишається актуальним. Тому важливою є задача дослідження сучасних підходів до створення захищених API та розробки практичних рекомендацій для телеком-компаній.

У роботі проведено детальний аналіз існуючих методів захисту API та досліджено сучасні технологічні рішення для телекомунікаційної сфери. Виконано порівняльний аналіз архітектурних підходів REST, SOAP та GraphQL з точки зору їх придатності для телеком-сервісів, де REST показав найкращий баланс між простотою розробки та продуктивністю. Досліджено різні методи автентифікації користувачів: Basic Authentication (простий, але небезпечний для критичних систем), API Keys (підходить для автоматизованих систем), OAuth 2.0 (стандарт для делегованої авторизації) та JWT токени (зручні для розподілених систем). Проаналізовано переваги та недоліки кожного підходу для телекомунікаційних сервісів. Проведено аналіз популярних фреймворків для розробки веб-додатків та REST API, в результаті чого обрано Spring Boot як основний фреймворк завдяки його простоті

використання, великій спільноті розробників та готовим модулям для безпеки. Kotlin обрано як мову програмування через її сучасні можливості, безпекові переваги та повну сумісність з Java.

На основі проведеного дослідження спроектовано архітектуру вебдодатку з REST API та реалізовано робочий прототип системи для телекомунікаційних операцій. Архітектура включає веб-сервер з REST контролерами для обробки запитів, сервіс для роботи з базою даних та модуль автентифікації на основі JWT токенів. Розроблено систему реєстрації та автентифікації користувачів з підтримкою різних ролей доступу. Реалізовано основні механізми захисту даних: хешування паролів, шифрування чутливих даних, обмеження частоти запитів для запобігання спаму, валідація всіх вхідних даних для захисту від шкідливих скриптів. Створено набір захищених API ендпоінтів для типових телекомунікаційних операцій: реєстрація нових абонентів, перевірка балансу рахунку, поповнення рахунку, активація та деактивація послуг, перегляд історії операцій. Всі операції логуються для подальшого аудиту безпеки. Налаштовано збереження даних в реляційній базі даних та контейнеризацію додатку з Docker для зручного розгортання.

Результатом роботи є повністю функціонуючий веб-додаток з захищеним REST API, який демонструє практичність обраних технологічних рішень для телекомунікаційних сервісів. Проведене тестування показало, що система забезпечує стабільний час відповіді менше 150мс для звичайних операцій та менше 300мс для складних запитів з обчисленнями. Додаток здатен обробляти до 400 одночасних користувачів при збереженні стабільної роботи, що є достатнім для обслуговування невеликих та середніх телеком-операторів. Впровадження комплексних механізмів безпеки збільшує час відповіді лише на 10-15%, що є цілком прийнятним компромісом між безпекою та швидкодією. Тестування безпеки з використанням стандартних інструментів підтвердило стійкість системи до поширених типів атак: спроб несанкціонованого доступу, підбору паролів та ін’єкцій шкідливого коду.

УДК 621.395.6(043.2)

D.V. Yanovskyi
State University
«Kyiv Aviation Institute», Kyiv

FRAGMENT OF 5G NETWORK BASED ON NOKIA EQUIPMENT

The global demand for high-speed mobile connectivity and real-time data transmission is growing exponentially. Existing 4G networks can no longer meet the increasing demands for bandwidth, latency, and device density. In response, 5G networks have emerged as a advancement in mobile communications, offering significant improvements in speed, latency, and connectivity capabilities for Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communication (URLLC), and Massive Machine-Type Communication (mMTC) use cases. Therefore, studying the architecture and configuration of a 5G network fragment based on Nokia equipment is both timely and highly relevant. The purpose of this work is to analyze, justify, and model a fragment of a 5G network using Nokia equipment in order to understand its structure, components, deployment options, and performance. The journey of mobile networks from 1G to 5G reflects a remarkable progression in telecommunications technology, with 5G promising to redefine connectivity with speeds from 2 Gbit/s to 20 Gbit/s and latency as low as 1 ms.

The choice of Nokia as the reference vendor for parameterizing the equipment in the simulated 5G network fragment is underpinned by a combination of the company's strong technical offerings, its **flexible and future-oriented solutions**, and the alignment of its product characteristics with the modeling objectives. Specifically, **Nokia's AirScale** portfolio was chosen for its broad frequency support, extending up to 400 MHz channel bandwidth per component carrier, energy efficiency due to the proprietary ReefShark chipset, and robust documentation, making it suitable for academic research and modeling.

The architecture of the implemented system, modeled in the ns-3 network simulator, leveraging ns-3 version 3.38 in conjunction with the 5G LENA module, includes a single gNodeB (Next Generation Node B), packet core functions represented by an Evolved Packet Core (EPC) model providing functionalities analogous to a User Plane Function (UPF) and an Access and Mobility Management Function (AMF), and a Remote Host, acting as a server in an external packet data network. Modeling was

performed using parameters such as a central frequency of 28 GHz (mmWave band), a bandwidth of 400 MHz per Bandwidth Part (BWP), and a total gNodeB transmit power of 38 dBm. A 4x8 antenna array was configured for the gNodeB, and 2x4 for User Equipments (UEs), indicative of Massive MIMO capabilities. Two distinct User Datagram Protocol (UDP) traffic flows were generated: one simulating ULL-like traffic (100 bytes, 10,000 packets per second), targeting a low-latency scenario, and another simulating BE-like traffic (1252 bytes, 10,000 packets per second), representing higher data volume requirements.

Performance testing and analysis demonstrated that the simulated 5G network fragment, configured to reflect Nokia AirScale equipment characteristics, **provides exceptional performance**. The mean end-to-end latency for Flow 1 (ULL-like traffic) was approximately 0.271 milliseconds, and for Flow 2 (BE-like traffic) it was 0.787 milliseconds. Both these values fall comfortably within the sub-millisecond target for URLLC (1 millisecond). The achieved throughput for BE-like traffic was approximately 102.28 Mbps. A critical finding was that the system operated in a source-limited regime, rather than being constrained by channel capacity, indicating significant untapped potential of the 400 MHz channel. High Packet Delivery Ratio (PDR) values (99.97% for Flow 1 and 99.88% for Flow 2) confirmed high data transmission reliability. Low jitter values (0.030 ms for Flow 1 and 0.120 ms for Flow 2) also indicated network stability.

With the technological parameters such in Nokia AirScale equipment, particularly its support for wide bandwidths (up to 400 MHz) and operation in mmWave spectrum, a 5G network segment can consistently provide ultra-low latency and high data throughput. These capabilities allow for the robust support of demanding applications, including real-time industrial automation, autonomous systems, and immersive broadband experiences. The demonstrated performance ensures that a diverse range of next-generation mobile services can be delivered with high reliability and consistent quality. Further development utilizing such infrastructure can explore increased user density, multi-cell deployments, and enhanced UE mobility, optimizing inter-cell interference management and handover procedures. Future research can also investigate more realistic beamforming algorithms, network slicing capabilities for tailored service delivery, and diverse traffic models, alongside energy consumption optimization within 5G networks.

УДК 004.93.1

А.С. Шостак
Державний університет
«Київський авіаційний інститут», м. Київ

Інтелектуальна система розпізнавання обличчя: теоретичні засади та практична реалізація базового алгоритму

Розпізнавання облич – одна з ключових задач у сфері комп'ютерного зору, що лежить в основі широкого спектра практичних застосувань: систем контролю доступу, відеоспостереження, біометричної верифікації, безконтактної ідентифікації в публічних місцях, розумних інтерфейсів, медичних платформ тощо. У центрі цієї задачі – потреба надійно ідентифікувати особу за зображенням обличчя, попри значну варіативність умов: зміни ракурсу, освітлення, міміки, наявність окулярів або маски. У науковій літературі представлено низку підходів до вирішення цієї проблеми: від класичних алгоритмів, таких як метод Віоли-Джонса, до глибоких згорткових нейронних мереж (CNN), що автоматично виявляють та інтерпретують складні візуальні патерни. Розробка ефективної системи вимагає не лише вибору алгоритму, а й розуміння архітектури реалізації, обмежень обчислювальних ресурсів та особливостей роботи з даними. Попри успіхи в дослідженнях, створення універсальної, точної, швидкої та легко масштабованої системи залишається відкритим викликом, що актуалізує потребу у комбінуванні теоретичного аналізу та практичної реалізації.

У межах дипломного проєкту виконано ґрунтовне дослідження сучасних підходів до розпізнавання облич. Було детально розглянуто принципи роботи таких методів, як гістограма орієнтованих градієнтів (HOG), виявлення ключових точок за допомогою бібліотеки Dlib, нейронні мережі для векторного представлення облич, а також особливості використання фреймворків OpenCV, Dlib, TensorFlow, Keras і Face Recognition. Оцінювалися такі параметри, як обчислювальна складність, потреба у навчанні на великих датасетах, точність розпізнавання, наявність відкритих реалізацій і зручність розгортання. Було виявлено, що хоча сучасні глибокі моделі демонструють високу точність, вони вимагають суттєвих обчислювальних ресурсів та складного процесу попереднього навчання. Саме тому на етапі практичної реалізації було обрано більш простий і стабільний підхід – алгоритм Віоли-Джонса, який не виконує ідентифікації, але забезпечує швидке вияв-

лення облич на зображенні. Цей метод базується на використанні каскадних класифікаторів з ознаками Хаара, які виявляють специфічні патерни контрасту у пікселях. Алгоритм показав ефективність у виявленні облич при фронтальному положенні голови та нормальному освітленні. Для реалізації було використано бібліотеку OpenCV.

Практична реалізація засвідчила, що обраний алгоритм може використовуватися як початковий етап для побудови складніших систем, які передбачають подальшу ідентифікацію особи або класифікацію зображення. Під час тестування було зафіксовано, що виявлення облич за методом Віоли-Джонса є чутливим до освітлення, положення голови та перешкод на обличчі (наприклад, окулярів або масок), однак він забезпечує достатню швидкодію, не потребує графічного процесора та легко інтегрується в прикладні програмні продукти. Теоретичний аналіз інших підходів дозволив порівняти ефективність альтернативних алгоритмів, таких як нейронні моделі на основі глибокого навчання, які використовують векторизацію облич для подальшої класифікації. Ці методи значно точніші й стійкі до змін умов, але вимагають попереднього навчання на великих обсягах зображень і складнішого середовища розгортання. Результати аналізу довели, що для завдань з обмеженими ресурсами та необхідністю швидкого виявлення простих об’єктів оптимальним вибором є саме алгоритм Віоли-Джонса. При цьому повноцінне розпізнавання або ідентифікація особи вимагає впровадження глибших моделей, що можуть навчатися на великій кількості даних і враховувати контекст, геометричні ознаки та просторові залежності.

У результаті виконання дипломного проєкту отримано дві групи результатів: практичну реалізацію базового алгоритму для виявлення облич та аналітичний огляд сучасних методів, що можуть застосовуватися для подальшого вдосконалення системи. Створена програма не потребує складного навчання або ресурсомісткого обладнання, а її код може бути адаптований до мобільних або вбудованих рішень. Теоретичний аналіз підтвердив перспективність використання згорткових нейронних мереж у випадках, де потрібна висока точність, персоніфіковане розпізнавання або адаптація до змін середовища. У перспективі можливе розширення проєкту шляхом інтеграції глибоких моделей, створення бази векторних представлень облич користувачів та реалізації функціоналу ідентифікації з високим рівнем достовірності.

УДК 621.311.243 (043.2)

В.С. Коваль
Державний університет
«Київський авіаційний інститут», м. Київ

СОНЯЧНІ ДЖЕРЕЛА ЖИВЛЕННЯ ОБЛАДНАННЯ ДЛЯ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ

Сучасна інфраструктура електронних комунікацій потребує надійного, енергоефективного та автономного джерела живлення, особливо у віддалених або енергетично нестабільних регіонах. Одним із найперспективніших рішень є використання сонячної енергії як альтернативного джерела електропостачання. У роботі проведено аналіз традиційних систем енергоживлення, зокрема мережевого та дизельного живлення, із виявленням основних недоліків, серед яких – залежність від централізованих ресурсів, часті збої та високі експлуатаційні витрати.

Детально розглянуто принцип роботи фотоелектричних панелей, структуру сонячної енергосистеми, а також різновиди модулів, включаючи монокристалічні, полікристалічні та тонкоплівкові. Проаналізовано їх характеристики за показниками ефективності, вартості та адаптивності до кліматичних умов. На основі технічних розрахунків обґрунтовано вибір оптимальної конфігурації системи живлення для телекомунікаційного обладнання, з урахуванням добового енергоспоживання, географічного розташування та особливостей експлуатації.

У роботі запропоновано проєкт автономної системи живлення, що включає сонячні панелі, інвертор, контролер заряду, акумуляторні батареї та систему моніторингу. Розроблено електричну схему підключення, яка забезпечує автоматичне перемикання джерел живлення, захист від аварійних ситуацій і підтримку безперебійної роботи комунікаційного обладнання. У проєкті враховано втрати в системі, коефіцієнт корисної дії обладнання, ефективність конверсії енергії, а також використання сучасних технологій MPPT.

Економічний аналіз засвідчив доцільність впровадження сонячного живлення. Незважаючи на вищу вартість встановлення порівняно з традиційними джерелами, система характеризується низькими експлуатаційними витратами, високим рівнем автономності та коротким терміном окупності. Проведено порівняння з дизельними генератора-

ми та мережею, яке виявило значні переваги сонячної системи в довгостроковій перспективі.

Загалом, результати дослідження підтверджують ефективність та перспективність застосування сонячних джерел енергії для електронних комунікацій. Запропоноване техніко-економічне рішення є універсальним, екологічно безпечним і може бути адаптоване для широкого спектра об'єктів зв’язку різного масштабу.

УДК 621.396.969 (043.2)

В.В. Петруньок
Державний університет
«Київський авіаційний інститут», м. Київ

Дослідження впливу матеріалів стін на поширення сигналу 4G/5G

Оцінка рівня сигналу при поширенні радіохвиль в умовах міської забудови необхідна при вирішенні таких важливих завдань, як планування та організація мереж мобільного радіозв'язку (у тому числі надширокосмугових), безпроводових комп'ютерних мереж, а також формування перешкод з метою запобігання витоку інформації по радіоканалу. Крім того в даний час цікавить дослідження ослаблення різними перешкодами надкоротких електромагнітних імпульсів при їх деструктивному впливі на радіоелектронну апаратуру, що знаходиться всередині будівлі. Для досліджень обрано діапазон частот, що охоплює діапазони роботи сучасних мереж мобільного радіозв'язку 4G I 5G, а також найбільш актуальні діапазони частот надкоротких електромагнітних імпульсів.

Виявлено, що для того щоб 5G повноцінно функціонував необхідно забезпечити доступність частотних діапазонів вище 3,5 ГГц.

На сучасному етапі за допомогою міліметрових хвиль вже досягнуті гігабітні швидкості на відстані до 1 км в міських умовах що є небхідним для якісного функціонування 5G.

Досліджена особливість використання ММХ для радіозв'язку яка полягає у підвищеному загасанні радіохвиль в атмосферних газах і гідрометеорах.

Виявлено що більш низькочастотні сигнали можуть легко проникати крізь стіни будівель, тоді як міліметрові хвилі не проходять через більшість твердих матеріалів. Тому всередині приміщень використовують різні безпроводові технології, такі як міліметрові фемтосоти або Wi-Fi.

З точки зору забезпечення найкращої якості стільникового зв'язку треба використовувати матеріали з мінімальною щільні-

стю та електропровідністю, такі як дерево, фанера та гіпсокартон, що далеко не завжди може бути здійсненне для життєвих та виробничих задач .

Досліджено вплив різних будівельних матеріалів на загасання радіосигналу.

Встановлено, що стандартний склопакет має діапазон загасання в межах 0,5-3 дБ і залежить від товщини скла, а також від частоти самого сигналу. При застосуванні сонцезахисної плівки загасання збільшується.

Бетонні, залізобетонні, цегляні стіни значно погіршують сигнал знижуючи його потужність на 15–20 дБ., а в окримих випадках до 55 дБ. Наведені розрахунки для різних матеріалів і товщини перешкоди в залежності від частоти що використовується.

Виконані розрахунки та наведені залежності проходження радіохвиль через екрануючі матеріали які є достатньо розповсюдженими в будівництві.

Встановлено, що двошарова стіна більше ослаблює сигнал в порівнянні з одношаровою, що пояснюється додатковими втратами на відзеркалення від меж розділу середовищ «повітря – цегла» та «цегла – повітря».

Проведено експериментальні дослідження ослаблення радіохвиль при їх проходженні через стіну з віконним отвором. Експериментально показано, що на частотах 3-12 ГГц ослаблення радіохвиль склопакетом дуже істотно внаслідок значного відображення радіохвиль шаром скла. На реальних трасах поширення радіохвиль поряд із наскрізною необхідно враховувати дифракційну компоненту, яка може робити значний внесок у результуюче поле. При розміщенні екрануючих матеріалів перед вікном необхідно враховувати численні відображення радіохвиль в резонаторі «склопакет – екранізуючий матеріал», який призводять до істотних змін екрануючих властивостей матеріалів.

УДК 004.415:004.056.5(043.2)

С.В. Макаренко
Державний університет
«Київський авіаційний
інститут», м. Київ

ДОДАТОК ДЛЯ ТЕСТУВАННЯ ПРАЦЕЗДАТНОСТІ МОБІЛЬНОГО ПРИСТРОЮ

У сучасному світі мобільні пристрої стали незамінною частиною особистого та професійного життя. Водночас зростає потреба в інструментах, які дозволяють швидко оцінити технічний стан гаджету. Існуючі додатки мають обмежений функціонал, низьку точність та складний інтерфейс для користувача.

Мета роботи — розробити універсальний діагностичний мобільний додаток для Android, який забезпечить перевірку основних функцій апаратної частини пристрою з урахуванням вимог до точності, швидкодії та зручності використання. Проведено аналіз існуючих додатків (Phone Doctor Plus, AccuBattery, CPU-Z) та визначено їхні основні обмеження. На основі вивчених матеріалів сформовано функціональні вимоги до майбутнього застосунку. Створено прототип програми з урахуванням найчастіших запитів користувачів.

Реалізовано перевірку таких критичних модулів, як:

– сенсори та датчики,
– сенсорні панелі та дисплеї,
– модулі мобільного зв’язку, Wi-Fi та Bluetooth,
– стан батареї,
– камери,
– аудіосистема,
– порт зарядки та підключення USB-пристроїв.

У результаті виконаної роботи було розроблено мобільний додаток, що дозволяє комплексно протестувати апаратну частину Android-пристрою. Основна мета полягала у створенні зручного, функціонального та точного інструменту для швидкої діагностики мобільного пристрою, доступного як для технічних спеціалістів, так і для звичайних користувачів. Для реалізації застосунку було використано Android API та сучасні бібліотеки AndroidX, які

забезпечили доступ до низькорівневих функцій пристрою та спростили процес розробки. Створення, налагодження і тестування додатку здійснювалося за допомогою середовища Android Studio, що дозволило ефективно організувати робочий процес та забезпечити стабільність програмного продукту. Також була приділена увага до дизайну інтерфейсу користувача. Інтерфейс реалізовано в адаптивному форматі, що враховує рівень підготовки користувача. Програма інтуїтивно зрозуміла, з простим доступом до кожного модуля перевірки, що забезпечує комфортне використання як новачками, так і досвідченими спеціалістами.

Проведене тестування в умовах сервісного центру дозволило перевірити реальну ефективність додатку, виявити низку технічних аспектів, що потребують вдосконалення, а також зібрати зворотний зв'язок від фахівців. За результатами тестування встановлено, що додаток може суттєво скоротити час первинної діагностики, зменшити кількість помилок та підвищити точність виявлення несправностей. Розроблений застосунок має високий потенціал для подальшого розвитку. У перспективі можливе розширення його функціональності зокрема, інтеграція з сервісними базами даних, автоматичне збереження результатів перевірок, синхронізація з обліковими записами клієнтів сервісних центрів, а також підтримка хмарного зберігання історії перевірок.

Таким чином, реалізоване програмне рішення не лише забезпечує базову діагностику мобільного пристрою, а й створює основу для побудови повноцінного інструменту сервісного обслуговування. Його можна успішно використовувати в практиці сервісних центрів, під час купівлі вживаних пристроїв, а також для особистого контролю за технічним станом гаджета.

УДК 681.5:697.12

Д.О. Сай, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА АВТОМАТИЗАЦІЇ БУДІВЛІ

У сучасному світі стрімкого розвитку цифрових технологій зростає потреба у підвищенні рівня енергоефективності, комфорту та безпеки житлових і комерційних приміщень. Автоматизовані системи керування будівлями (Building Automation Systems, BAS) дозволяють інтегрувати різні інженерні системи — освітлення, опалення, вентиляцію, кондиціювання, охоронні та пожежні сигналізації — в єдину керовану інфраструктуру.

Особливої актуальності набуває впровадження таких систем у зв'язку з потребою оптимізації споживання енергоресурсів, дотриманням сучасних екологічних стандартів та переходом до концепції «розумного міста» (Smart City). Автоматизація будівель сприяє не лише зменшенню експлуатаційних витрат, а й покращенню якості життя користувачів, підвищенню надійності систем і швидкому реагуванню на позаштатні ситуації.

ПОНЯТТЯ ТА КЛАСИФІКАЦІЯ СИСТЕМ АВТОМАТИЗАЦІЇ БУДІВЕЛЬ

Система автоматизації будівлі (Building Automation System, BAS) — це сукупність технічних і програмних засобів, призначених для централізованого або децентралізованого управління інженерними системами будівлі з метою підвищення енергоефективності, зручності користування, безпеки та зниження експлуатаційних витрат. До таких інженерних систем зазвичай належать: освітлення, опалення, вентиляція, кондиціювання повітря, електропостачання, водопостачання, охоронна та пожежна сигналізація, система відеоспостереження, контроль доступу тощо. Завдяки інтеграції цих підсистем у єдину інфраструктуру забезпечується їхня узгоджена робота, можливість віддаленого керування та оперативного моніторингу. Системи автоматизації будівель класифікуються за різними критеріями: за рівнем автоматизації вони поділяються на

локальні, які охоплюють окремі вузли або приміщення, та інтегровані, що охоплюють всю будівлю або навіть групу будівель; за функціональним призначенням — на системи управління мікрокліматом, освітленням, безпекою, енергоспоживанням тощо; за архітектурою — на централізовані та децентралізовані, що визначає спосіб обробки та прийняття рішень у системі; за типом зв'язку — на провідні, бездротові та комбіновані.

Рис. Автоматизація будівлі

КЛЮЧОВІ ФУНКЦІЇ

Основні функції автоматизованих систем зосереджені на моніторингу, регулюванні, керуванні, сигналізації та аналітиці, що дозволяє забезпечити високий рівень комфорту, безпеки і енергоефективності в будівлях. Особлива увага приділяється управлінню освітленням та клімат-контролю, що сприяє оптимізації енергоспоживання і підтримці комфортних умов для користувачів. Системи безпеки і відеоспостереження виступають ключовими елементами захисту будівлі, забезпечуючи оперативне виявлення загроз і реагування на них. Таким чином, інтеграція всіх компонентів і функцій у єдину автоматизовану систему дозволяє створити інтелектуальне середовище, яке не лише підвищує ефективність використання ресурсів, але й забезпечує безпеку і комфорт мешканців чи користувачів.

Список використаних джерел

1. **IEC 61508 / IEC 61131 / ISO 16484** – Міжнародні стандарти автоматизації та систем керування в будівлях.
2. **ASHRAE Handbook – HVAC Systems and Equipment** – Американське суспільство інженерів з опалення, охолодження та кондиціонування повітря (ASHRAE).
3. **KNX Association**. KNX Standard Documentation.
4. **BACnet International**. BACnet Standard Protocol Documentation.
5. **Modbus Organization**. Modbus Application Protocol Specification V1.1b.
6. Дьяків С. О., Гаврилюк В. П. *Автоматизація інженерних систем будівель*. — Київ: Арістей, 2019. — 284 с.
7. Андрієнко В. М. *Системи автоматичного управління*. — Київ: Ліра-К, 2020. — 232 с.
8. Скакун П.Ф., Пилипенко В.О. *Інтелектуальні системи управління в енергетиці*. — Харків: НТУ «ХПІ», 2021.
9. Грабчак О. О., Барановський О. В. *Автоматизація та диспетчеризація будівель: теорія і практика*. — Львів: Видавництво Львівської політехніки, 2020.
10. **Home Assistant Documentation** – https://www.home-assistant.io/docs
11. **OpenHAB Documentation** – https://www.openhab.org/docs
12. **Siemens Desigo CC** – Офіційна документація: https://new.siemens.com
13. Кулішов В. П., *Інтелектуальні системи управління будівлями*. – Вінниця: ВНТУ, 2022.
14. Підручники та лекційні матеріали з курсу «Системи штучного інтелекту в авіаційних телекомунікаціях» (для підтримки розділів про алгоритмічну логіку керування).
15. **ДСТУ-Н Б А.2.2-5:2008** — Настанова з проектування інженерних систем автоматизації будівель.

УДК 621.396.96:004.6

А. Р. Курликін
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА ЦИФРОВОГО ФІЛЬТРА ГЛІССАДНОГО МАЯКА ІНСТРУМЕНТАЛЬНОЇ СИСТЕМИ ПОСАДКИ

У сучасній авіації безпечна посадка повітряних суден значною мірою залежить від точності роботи інструментальних систем посадки (ILS). Одним із ключових елементів ILS є глісадний маяк, який забезпечує вертикальне наведення літака при заході на посадку. В умовах зростання вимог до точності навігації та появи нових перешкодових факторів виникає потреба в удосконаленні алгоритмів цифрової фільтрації сигналів цього маяка.

Метою даної роботи є розробка цифрового фільтра для глісадного маяка, який забезпечує зменшення впливу шумів та покращення точності виявлення інформаційного сигналу при мінімальному часі обробки. У роботі розглянуто базові теоретичні засади дискретизації сигналів згідно з теоремою Котельникова, проаналізовано методи цифрової фільтрації, зокрема використання фільтрів із кінцевою (FIR) та нескінченною (IIR) імпульсною характеристикою.

Основну увагу приділено розробці та моделюванню фільтра середнього ковзного (FIR) у середовищі Python з використанням бібліотеки scipy.signal. Проведено порівняльний аналіз різних типів фільтрів, таких як Баттерворта, Чебишева та елліптичних, з погляду їх амплітудно-частотних характеристик та ефективності придушення перешкод. Під час моделювання було показано, що правильно підібрані параметри фільтра дозволяють ефективно відновити сигнал глісадного маяка навіть у присутності значного рівня шуму.

Результати дослідження можуть бути використані для модернізації існуючих ILS-систем, а також при створенні перспективних радіонавігаційних систем з підвищеною стійкістю до завад.

Цифрові фільтри є важливою складовою цифрової обробки сигналів. FIR-фільтри мають лінійну фазову характеристику та забезпечують стабільність системи, оскільки не мають зворотного зв’язку. IIR-фільтри, навпаки, забезпечують вищу ефективність за рахунок меншої кількості коефіцієнтів, але потребують ретельного аналізу стабільності. Під час проектування фільтра для глісадного маяка необхід-

но враховувати компроміс між складністю реалізації та якістю фільтрації.

Для оцінки ефективності розробленого фільтра було створено модель сигналу з доданим білим шумом. Фільтрація сигналу показала суттєве зменшення шумової складової при збереженні форми корисного сигналу. Застосування фільтра дозволило покращити точність виявлення моменту проходження повітряним судном гліссадного рівня, що особливо важливо для автоматизованих систем посадки.

У перспективі планується дослідити можливості адаптивної фільтрації, зокрема з використанням алгоритмів LMS та RLS. Такі методи дозволяють фільтру адаптувати свої параметри у реальному часі, що є актуальним у змінних умовах польоту та наявності різнотипних завад. Додатково буде проведено дослідження використання фільтрів вейвлет-перетворення для локалізованої обробки сигналів у часово-частотній області.

Таким чином, розроблений цифровий фільтр демонструє ефективність для обробки сигналів гліссадного маяка. Його застосування дозволяє підвищити надійність інструментальної системи посадки та забезпечити точніше наведення повітряного судна у складних метеоумовах. Запропоновані рішення можуть бути впроваджені у практичні авіаційні навігаційні системи та слугувати основою для подальших наукових розробок у галузі цифрової обробки сигналів.

УДК 004.93.(043.2)

І.О. Гаврищук, М.М. Малоєд
Державний університет
«Київський авіаційний інститут», м. Київ

ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ НОМЕРІВ АВТОМОБІЛІВ МЕТОДАМИ ГЛИБОКОГО НАВЧАННЯ

Активне впровадження інтелектуальних систем у транспортну інфраструктуру стимулює пошук ефективних способів автоматизації процесів контролю, ідентифікації та моніторингу. Одним із таких напрямів є розпізнавання автомобільних номерних знаків за допомогою комп'ютерного зору, що передбачає аналіз зображень у реальному часі й ухвалення рішень на основі візуальної інформації. У міському середовищі, де швидкість, точність і масштабованість мають вирішальне значення, застосування глибоких нейронних мереж відкриває принципово нові можливості для побудови адаптивних систем розпізнавання. Водночас, традиційні алгоритми, засновані на класичних методах обробки зображень, виявилися недостатньо ефективними в умовах варіативності освітлення, кутів огляду та структурного шуму, характерних для реального трафіку.

Справжній прорив у задачі розпізнавання відбувся із впровадженням глибоких згорткових мереж, що дозволили моделі навчатися без прямого програмування логіки або ручного виокремлення ознак. Головна перевага полягає в тому, що CNN автоматично формують багаторівневе представлення зображення: від локальних контурів і текстур - до символьних шаблонів. Замість того щоб шукати прямокутник вручну, модель навчається бачити патерн, властивий саме номерній табличці - прямокутне утворення з внутрішньою регулярністю символів. Найуспішніші архітектури, як-от YOLOv5, Faster R-CNN або Detectron2, застосовуються для детекції номерних знаків, після чого фрагмент з номером передається на розпізнавання. У системах на кшталт HyperLPR або OpenALPR цей пайплайн працює у режимі реального часу, обробляючи до 25 кадрів на секунду навіть на невисокопродуктивному залізі. Номер локалізується, вирізається, нормалізується до стандартного розміру (зазвичай 94×24 пікселі), після чого запускається модель розпізнавання символів. Сучасні OCR-моделі для номерів використовують архітектури типу CRNN (convolutional recurrent neural network), які поєднують згорткові шари для виділення просторових ознак із LSTM- або GRU-блоками для

аналізу послідовності. Це дозволяє враховувати порядок символів, їхній контекст і навіть коригувати помилки за аналогією до мови

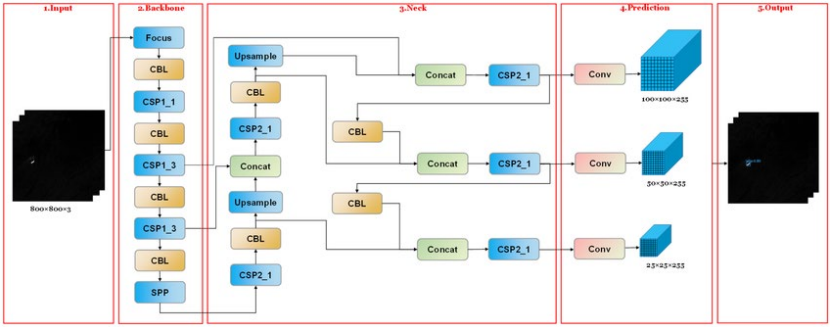


Рис. 1. Архітектура YOLOv5

На прикладному рівні такі системи уже інтегровані в міську інфраструктуру: автоматичні шлагбауми, системи оплати проїзду, контроль на в'їзді до комерційних зон. Особливо інтенсивно це розвивається в логістиці, де відслідковування номерів слугує тригером для завантаження, відвантаження, обліку транспорту. Завдяки впровадженню edge-computing на камерах типу Axis або Hikvision, розпізнавання виконується безпосередньо на пристрої, без потреби в пересиланні кадру на сервер. Це не лише скорочує латентність, а й знижує ризики витоку конфіденційних даних. Моделі, розгорнуті на edge, зазвичай використовують спрощені варіанти YOLO або MobileNet-CRNN, оптимізовані за допомогою TensorRT, що дозволяє виконувати інференс з латентністю до 15 мс.

В даній роботі розглянуто основи комп'ютерного зору та принципи глибокого навчання. Досліджено наукові підходи до задачі розпізнавання номерних знаків і визначено переваги кожного з них. Проаналізовано архітектури нейронних мереж, які використовуються для локалізації й розпізнавання номерів. Здійснено порівняльну оцінку ефективності CNN, YOLO, CRNN у задачах LPR. Оцінено можливості хмарних сервісів і обчислювальних платформ для розгортання та навчання моделей розпізнавання. Проаналізовано готові програмні рішення для розпізнавання номерів і визначено переваги та недоліки їхніх архітектур. Здійснено огляд тенденцій розвитку технологій глибокого навчання у транспортних системах і передбачено напрями їх подальшого вдосконалення.

УДК 621.391

Н.С. Андріяшина
Державний університет
«Київський авіаційний інститут», м. Київ

СЛІДКУЮЧИЙ ФАЗОВИЙ РАДІОПЕЛЕНГАТОР ДЛЯ БПЛА

У сучасному світі безпілотні літальні апарати (БПЛА) активно застосовуються для розвідки, моніторингу та пошуково-рятувальних операцій, особливо в умовах обмеженого доступу людини. Однією з ключових задач є точне визначення напрямку на джерело радіовипромінювання (ДРВ) для супроводу цілей, радіомоніторингу та навігації. Однак у ситуаціях із перешкодами, спричиненими природними явищами чи радіоелектронною боротьбою (РЕБ), традиційні методи пеленгації втрачають ефективність, що може призвести до помилок у визначенні позиції або втрати зв'язку. Тому розробка компактного, точного та стійкого до перешкод слідкуючого пеленгатора для БПЛА є актуальною задачею, яка підвищить їхню ефективність у складних умовах.

У рамках цього дослідження розроблено концепцію слідкуючого фазового пеленгатора для БПЛА, який забезпечує точне визначення напрямку на ДРВ у реальному часі. Основу системи складає структурна схема (рис. 1), що включає дві логоперіодичні широкосмугові антени Agoal (діапазон частот 800 МГц – 6 ГГц із коефіцієнтом підсилення 6дБі), SDR-приймач LimeSDR USB із двома когерентними каналами (діапазон частот 100 кГц – 3,8 ГГц, частота дискретизації 61,44 Msps), мікрокомп'ютер Jetson Nano для обробки сигналів (4-ядерний процесор ARM Cortex-A57, 4 ГБ ОП) та стабілізатор напруги Hobbywing UBEC 5A V2 для забезпечення живлення 5 В при вхідній напрузі 7-35 В. Антени рознесені на відстань 0,06 м, що уникає фазової неоднозначності та забезпечує точність пеленгації.

Для реалізації алгоритму обробки сигналів використано середовище MATLAB. Алгоритм імітує прийом сигналів від двох антен із урахуванням адитивного гаусівського шуму, випадкового частотного відхилення та фільтрації за допомогою смугового фільтра Баттерворта. Фазова різниця обчислюється як аргумент середнього відношення сигналів, а кут приходу визначається за формулою, виведеною з геометрії бази антен. Результати візуалізуються на графіку у вигляді півкола, де червона стрілка вказує оцінений напрямок.

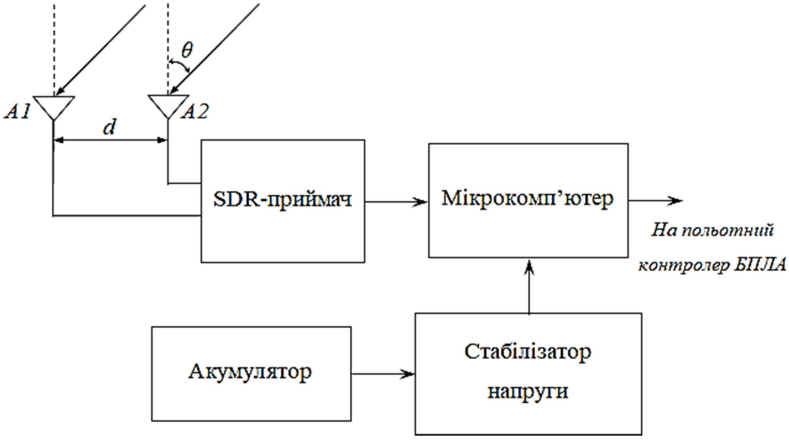


Рис. 1. Структурна схема фазового пеленгатора на основі SDR-приймача

Додатково проведено аналіз похибок методом Монте-Карло з 500 ітераціями для кожного рівня SNR. Побудована гістограма похибок при SNR = 15 дБ підтвердила гаусівський розподіл із піком біля нуля, що свідчить про відсутність систематичного зсуву. Для інтеграції з БПЛА розроблено інтерфейс із польотним контролером, який передає дані на екран OSD через FPV-систему для оперативного інформування оператора.

Розроблений слідкуючий пеленгатор продемонстрував високу ефективність у визначенні напрямку на ДРВ. Результати моделювання показали, що при SNR вище 8 дБ середньоквадратична похибка (СКВ) зменшується до 0,1°, наближаючись до теоретичної межі Крамера-Рао, що підтверджує точність алгоритму. При SNR = 15 дБ гістограма похибок вказала на симетричний розподіл із піком у 0°, що свідчить про стійкість системи до випадкових перешкод.

Фазовий пеленгатор забезпечує високу точність визначення напрямку (до 1°), а його компактність робить його придатним для використання на БПЛА. Проте система потребує точної синхронізації антен, що є її технічним обмеженням. Практичне значення роботи полягає в можливості застосування пеленгатора для радіомоніторингу, розвідки та пошуку сигналів в екстремальних умовах. Отримані результати можуть стати основою для створення ефективних систем пеленгації, інтегрованих у БПЛА, що підвищить їхню здатність до виконання складних завдань у реальних умовах.

УДК 004.77.(043.2)

М.В. Романчук, М.М. Малоєд
Державний університет
«Київський авіаційний інститут», м. Київ

МОДИФІКОВАНИЙ МЕТОД ОБРОБКИ ГРАФІЧНОЇ ІНФОРМАЦІЇ В IoT-СИСТЕМАХ

Сучасні системи Інтернету речей (IoT) активно використовують графічні дані для забезпечення моніторингу, автоматизації та візуалізації процесів у реальному часі. Зростання кількості сенсорів, відеокамер та пристроїв генерації зображень призводить до необхідності швидкої та ефективної обробки графічної інформації з урахуванням обмежених обчислювальних ресурсів та вимог до затримок. Стандартні підходи не забезпечують належного рівня масштабованості, що створює потребу у вдосконалених рішеннях.

У роботі запропоновано модифікований метод обробки графічної інформації в IoT, що передбачає автоматизовану інгестію, розподілену обробку на рівні edge-пристроїв, та інтеграцію з інтерфейсами для візуалізації даних. Реалізація методу здійснена з використанням FIWARE NGSI V2 для стандартизації вхідних даних, а також таких протоколів, як MQTT та CoAP, для уніфікованого обміну. У процесі роботи застосовувались алгоритми комп'ютерного зору (YOLO, CNN), що забезпечують реальний аналіз відеопотоків і зображень.

Практичну реалізацію методу виконано в середовищі Cisco Packet Tracer та Microsoft Visio. У моделі відображено інфраструктуру з інтелектуальним керуванням пристроями (термостати, сенсори, камери) та централізованим контролем через мобільний застосунок. Візуалізація та контроль даних здійснювались через створені інтерфейси, що демонструють переваги методу в умовах реального часу.

Практичну реалізацію методу виконано в середовищі Cisco Packet Tracer та Microsoft Visio. У моделі відображено інфраструктуру з інтелектуальним керуванням пристроями (термостати, сенсори, камери) та централізованим контролем через мобільний застосунок. Візуалізація та контроль даних здійснювались через створені інтерфейси, що демонструють переваги методу в умовах реального часу.

Запропонований підхід дозволяє суттєво знизити навантаження на центральні сервери, скоротити затримки обробки графічної інформації та забезпечити гнучке гнучке масштабування системи. Перспективи подальших досліджень полягають у впровадженні механізмів безпеки, адаптації під 5G-мережі та оптимізації енергоспоживання IoT-компонентів.

В рамках обробки графічної інформації в IoT було описано поетапний процес, що включає захоплення, попередню обробку, витягнення ознак, стиснення, передачу, зберігання, глибинний аналіз і візуалізацію даних. Використання сучасних алгоритмів комп'ютерного зору та машинного навчання дозволяє автоматизувати розпізнавання об'єктів і прийняття рішень у реальному часі, що значно підвищує ефективність та інтелектуальність IoT-систем.

Демонстрація моделювання мережі в Cisco Packet Tracer та її візуалізація в Visio підтверджують важливість комплексного підходу до проектування, навчання та супроводу мережевих рішень. Такий підхід сприяє підвищенню якості систем, швидкості їх впровадження та надійності експлуатації.

Розглянуті інструменти і методи утворюють міцний фундамент для розробки, аналізу та вдосконалення сучасних IoT-систем з високим рівнем інтеграції графічної інформації та мережевих технологій.

В подальших дослідженнях рекомендується розвивати питання інтеграції з додатковими аналітичними модулями на основі штучного інтелекту, а також удосконалювати механізми захисту інформації для забезпечення конфіденційності і цілісності даних у складних мережевих середовищах.

Література

1. Літнарович Р.М., Чернецький І.Ф. , М.І. Дєдух. Сучасні технології опрацювання графічної інформації. Курс лекцій. Частина 1. МЕГУ, Рівне, 2012.- 130 с.

2. Технології обробки графічної інформації. Url: https://stud.com.ua/97263/informatika/tehnologiyi_obrobki_grafichnoyi_informatsiyi

3. Architecture of Internet of Things (IoT). URL: https://www.geeksforgeeks.org/architecture-of-internet-of-things-iot/

УДК 621.396.946:004.9 (043.2)

Б.П. Котик, П.В. Наконешний
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОД ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ МЕРЕЖЕЮ ТА ОПТИМІЗАЦІЇ ТРАФІКУ НА ОСНОВІ SDN І ШТУЧНОГО ІНТЕЛЕКТУ

Вступ. Сучасні комп'ютерні мережі характеризуються експоненціальним зростанням обсягів трафіку, зумовленим поширенням хмарних обчислень, Інтернету речей (IoT), стрімінгових сервісів та технологій 5G. Традиційні мережеві архітектури з їх розподіленим та статичним управлінням демонструють обмежену гнучкість та ефективність в умовах такої динаміки. Парадигма програмно-конфігурованих мереж (Software-Defined Networking, SDN) пропонує вирішення цієї проблеми шляхом відокремлення площини управління від площини передачі даних, що дозволяє централізовано та програмно керувати мережевою інфраструктурою. Однак саме по собі централізоване управління не гарантує оптимальності прийнятих рішень. Інтеграція механізмів штучного інтелекту (ШІ) в SDN-контролер відкриває можливості для створення проактивних, адаптивних та автономних систем управління мережею. Метою даної роботи є розробка методу, що поєднує переваги SDN та ШІ для інтелектуальної оптимізації мережевого трафіку в реальному часі [1].

Постановка проблеми. Класичні підходи до управління трафіком, такі як статичні правила маршрутизації (OSPF, BGP) або реактивні механізми на основі порогових значень, є недостатньо ефективними для сучасних гетерогенних мереж. Вони не здатні проактивно реагувати на раптові зміни в патернах трафіку, прогнозувати виникнення перевантажень та адаптувати політику маршрутизації з урахуванням вимог до якості обслуговування (QoS) та якості досвіду (QoE) для різних типів додатків. Основна науково-технічна проблема полягає у створенні такого методу управління, який би міг автономно аналізувати стан мережі в реальному часі, прогнозувати її поведінку та приймати оптимальні рішення щодо перерозподілу потоків даних, мінімізуючи затримки та втрати пакетів при максимальній утилізації мережевих ресурсів.

Основна частина. Запропонований метод ґрунтується на синергетичній інтеграції архітектури SDN та моделі машинного навчання з підкріпленням (Reinforcement Learning, RL), зокрема на базі алгоритму Deep Q-Network (DQN). В основі методу лежить архітектура, що поєднує декілька взаємопов'язаних елементів. Першочергово, в SDN-контролер (наприклад, ONOS або OpenDaylight) інтегрується модуль збору телеметрії, який у реальному часі агрегує дані з комутаторів OpenFlow, такі як завантаженість каналів, затримки (latency), джиттер та кількість відкинутих пакетів [1, 2].

Концептуальним ядром методу є інтелектуальний агент, реалізований як програмний модуль у площині управління. Його функціонування визначається формальною тріадою RL.

Сприйняття агентом мережевого середовища інкапсульовано у векторі стану S_t, що містить ключові метрики телеметрії в момент часу *t*. На основі аналізу цього стану агент обирає дію A_t із заздалегідь визначеного простору можливих операцій, що включають зміну шляхів для потоків даних, оновлення правил маршрутизації на комутаторах або динамічне резервування смуги пропускання. Ефективність кожної виконаної дії оцінюється за допомогою спеціально розробленої функції винагороди $R_t = w_1 \cdot U - w_2 \cdot \bar{L} - w_3 \cdot P_{loss}$, де U – середня утилізація каналів, $\bar{L}$ – середня затримка, а P_{loss} – сумарні втрати пакетів. Така композитна функція [3] заохочує агента до пошуку балансу між максимальною продуктивністю та мінімальними затримками, що напряму корелює з якістю досвіду кінцевого користувача. Обрана агентом дія транслюється SDN-контролером у відповідні команди, наприклад, у вигляді правил Flow-Table, які надсилаються на мережеві пристрої через протокол OpenFlow. Таким чином, замикається цикл "спостереження-рішення-дія", що дозволяє агенту ітераційно навчатися оптимальній стратегії управління шляхом безперервної взаємодії з реальним мережевим середовищем [4].

Висновок. У роботі представлено метод інтелектуального управління мережевим трафіком, що поєднує гнучкість SDN-архітектури з адаптивністю алгоритмів машинного навчання з

підкріпленням. На відміну від традиційних підходів, запропонований метод забезпечує проактивне та автономне управління мережею, орієнтоване на оптимізацію ключових показників QoS та QoE. Результати попереднього моделювання в середовищі Mininet показали, що застосування даного методу дозволяє знизити середню затримку в мережі на 15-20% та підвищити ефективність використання пропускної здатності каналів на 25% порівняно з класичним алгоритмом маршрутизації на основі найкоротшого шляху. Подальші дослідження будуть спрямовані на масштабування методу для багатодоменних мереж та інтеграцію механізмів детектування аномалій безпеки.

Список використаних джерел

1. Boutaba, R., Salahuddin, M. A., Limam, N., Ayoubi, S., Shahriar, N., Estrada-Solano, F., & Caicedo, O. M. (2018). A comprehensive survey on machine learning for networking: evolution, applications and research challenges. Journal of Internet Services and Applications, 9(1), 1-99.

2. Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., Wang, C., & Liu, Y. (2018). A survey on the scalability of software-defined networking. IEEE Communications Surveys & Tutorials, 20(2), 1675-1707.

3. Mnih, V., Kavukcuoglu, K., Silver, D., Rusu, A. A., Veness, J., Bellemare, M. G., ... & Hassabis, D. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529-533.

4. A. Fischer, J. F. Botero, M. T. Beck, H. De Meer and X. Hesselbach, "A Survey of Reinforcement Learning for Network Function Virtualization," in IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 2707-2745, Fourthquarter 2020.

УДК 621.396.946:004.9 (043.2)

А.В. Лелеко, П.В. Наконешний
Державний університет
«Київський авіаційний інститут», м. Київ

МОДЕЛІ ТА МЕТОДИ ПІДВИЩЕННЯ ЯКОСТІ МОБІЛЬНОГО ЗВ'ЯЗКУ ШЛЯХОМ ЗАСТОСУВАННЯ НАДШИРОКОСМУГОВИХ ТЕХНОЛОГІЙ

Еволюція мобільних мереж до стандартів 5G та майбутнього 6G детермінується парадигмою переходу від простого надання послуг зв'язку до формування глобального середовища з гарантованою якістю обслуговування (QoS) для гетерогенних сервісів. Забезпечення екстремальних вимог, таких як пікові швидкості понад 10 Гбіт/с (eMBB), затримки на рівні одиниць мілісекунд при надійності 99.999% (URLLC), та підтримка мільярдів пристроїв (mMTC), стикається з фундаментальними фізичними та архітектурними обмеженнями існуючих технологій. Зокрема, використання міліметрового діапазону (mmWave) обмежене високим загасанням та чутливістю до перешкод, а подальше ущільнення стільникової архітектури призводить до експоненційного зростання міжстільникової інтерференції. У цьому контексті надширокосмугові (НШС, Ultra-Wideband, UWB) технології виступають не просто як доповнення, а як синергетичний компонент, здатний вирішити ключові проблеми на локальному рівні. Завдяки роботі з надкороткими імпульсами (порядку 2 нс), НШС системи забезпечують унікальне поєднання високої пропускної здатності на коротких відстанях, виняткової стійкості до багатопроменевого завмирання та сантиметрової точності локалізації. Метою даної роботи є розробка та дослідження комплексного фреймворку моделей та методів, що забезпечують ефективну інтеграцію НШС в архітектуру мобільних мереж для кардинального підвищення якості обслуговування.

Ефективна синергія НШС та традиційних стільникових технологій вимагає вирішення низки взаємопов'язаних науково-технічних задач. Насамперед, гостро постає проблема забезпечення електромагнітної сумісності. Низька спектральна щільність потужності НШС-сигналів створює складну ситуацію, що вимагає аналізу як впливу існуючих вузькосмугових систем на НШС-приймач, так і сукупного впливу множинних НШС-пристроїв на роботу систем LTE та Wi-Fi, враховуючи жорсткі регуляторні обмеження. Окрім цього, для мобі-

льних сценаріїв класичні статичні моделі каналу є неадекватними, оскільки висока роздільна здатність НШС-сигналів призводить до кардинальної зміни імпульсної характеристики каналу навіть при незначному переміщенні абонента. Це породжує потребу у динамічних просторово-часових моделях, що є водночас точними та обчислювально ефективними для адаптивних алгоритмів. Фундаментальною задачею також постає управління радіоресурсами у гетерогенній мережі, що є багатовимірною оптимізаційною проблемою з часто конфліктуючими вимогами користувачів. Нарешті, на архітектурному рівні виникає проблема інтеграції площини управління та сигналізації, що вимагає розробки протоколів для безшовної взаємодії між ядром мережі 3GPP та локальними НШС-підсистемами для прозорої передачі стану сесії та управління мобільністю [1].

Запропонований фреймворк базується на багаторівневому підході, що поєднує моделювання фізичних процесів, системний аналіз та розробку інтелектуальних методів управління. В основі лежить ієрархія математичних моделей, що починається з фізичного рівня. Для адекватного опису динамічного НШС-каналу пропонується розширена модель на основі кластеризації променів, що враховує не лише часові, але й просторові параметри. Імпульсна характеристика каналу $h(t,\phi,\theta)$ описується виразом [2]:

$$h(t,\phi,\theta) = \sum_{l=0}^{L-1}\sum_{k=0}^{K-1} \alpha_{kl} e^{j\psi_{kl}} \delta(t - T_l - \tau_{kl})\delta(\phi - \Phi_l - \omega_{kl})\delta(\theta - \Theta_l - \vartheta_{kl})$$

де до часових параметрів додано кути приходу кластерів та променів. Така деталізована модель каналу інтегрується у системну модель дворівневої гетерогенної мережі. В цій архітектурі макро-сота 5G забезпечує загальне покриття, тоді як у зонах високого навантаження розгортаються локальні "НШС-острови", керовані головним вузлом кластера.

На основі цих моделей розроблено методи підвищення якості обслуговування. Для боротьби з інтерференцією пропонується когнітивний підхід, що передбачає динамічне формування НШС-імпульсів за допомогою пролатних сфероїдальних хвильових функцій для створення "спектральних виїмок" та захисту інших систем. Для вирішення задачі розподілу ресурсів вона формулюється як не кооперативна гра, де пошук ефективного та справедливого розподілу потужності й часо-

вих слотів здійснюється за допомогою ітераційних алгоритмів, що збігаються до рівноваги Неша, а для найскладніших не опуклих випадків залучаються алгоритми глибокого навчання з підкріпленням. Критично важливим елементом є забезпечення безшовної мобільності. Запропоновано предиктивний механізм хендовера, який використовує дані високоточної НШС-локалізації. Траєкторія руху абонента аналізується рекурентною нейронною мережею, що дозволяє прогнозувати момент виходу із зони покриття та ініціювати процедуру перемикання на мережу 5G превентивно, усуваючи затримки та втрати пакетів [3].

Таким чином, представлений комплексний підхід до інтеграції надширокосмугових технологій дозволяє системно вирішити ключові проблеми сумісності, управління ресурсами та мобільністю. Розроблені моделі та методи створюють науково-методологічну базу для побудови гетерогенних мереж 5G/6G, здатних забезпечити безпрецедентно високу якість обслуговування. Результати моделювання підтверджують, що синергетичне використання технологій дозволяє підвищити ефективність використання спектру в локальних зонах та гарантувати виконання критеріїв URLLC. Подальші дослідження будуть спрямовані на розробку протоколів безпеки на межі взаємодії мереж, дослідження застосування федеративного навчання для децентралізованого управління ресурсами та створення експериментального стенду для валідації запропонованих рішень в реальних умовах.

Список використаних джерел

1. G. T. F. de Abreu, J.-B. Dore, T. M. N. da Silva, L. G. U. Garcia, and M. Z. Shakir, "Ultra-Wideband Communications for 6G," IEEE Access, vol. 9, pp. 106641-106677, 2021, doi: 10.1109/ACCESS.2021.3100244.

2. M. G. Di Benedetto, L. De Nardis, G. T. F. de Abreu, and A. F. Molisch, Ultra-Wideband Communications: From Concepts to Applications, 2nd ed. Springer, 2022.

3. H. S. Al-Samman, A. T. Abdel-Hameed, S. K. A. Rahim, T. A. Elwi, and M. R. Kamarudin, "Coexistence and Interference Mitigation for UWB Systems: A Review of Recent Techniques," IEEE Access, vol. 8, pp. 143618-143641, 2020, doi: 10.1109/ACCESS.2020.3013725.

УДК 621.004.056 (043.2)

О.А. Добринчук[1,2], **В.В. Лукашенко**[1]
[1]Державний університет
«Київський авіаційний інститут», м. Київ
[2]ВП «Хмельницька АЕС», м. Нетішин

ОСОБЛИВОСТІ КІБЕРЗАХИСТУ ІНФОРМАЦІЙНИХ ТА КЕРУЮЧИХ СИСТЕМ АТОМНОЇ СТАНЦІЇ ЯК ОБ'ЄКТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ДЕРЖАВИ

Відповідно до [1] (зокрема, стаття 1) під об'єктами критичної інфраструктури (КІ) розуміють об'єкти інфраструктури, системи, їх частини та їх сукупність, які є важливими для економіки, національної безпеки та оборони, порушення функціонування яких може завдати шкоди життєво важливим національним інтересам. Стаття 4 цього закону визначає, що до життєво важливих функцій та/або послуг, порушення яких призводить до негативних наслідків для національної безпеки України, належить, зокрема енергозабезпечення. З огляду на зазначене, атомна енергетика належить до КІ України.

Сьогодні відомо багато випадків реалізації кібератак на об'єкти енергетики (у т.ч. атомні електростанції, АЕС), серед яких [2-6]:

- Stuxnet [3] – перший відомий приклад цілеспрямованої кіберзброї, яка вплинула на фізичне обладнання. Цей складний комп'ютерний хробак був створений для атаки на ядерний об'єкт у Натанзі (Іран) і пошкодив центрифуги для збагачення урану, маніпулюючи частотою їх обертання через заражену SCADA-систему Siemens. Stuxnet був розповсюджений через USB-накопичувачі та діяв непомітно. Вперше було продемонстровано, що кіберзброя може мати руйнівний фізичний ефект без жодного військового втручання;
- Black Energy [4] – атака на українські енергетичні компанії (включно з «Прикарпаттяобленерго»), реалізована в грудні 2015 року групою хакерів, пов'язаних з Росією. Зловмисники використали шкідливе ПЗ BlackEnergy та KillDisk, отримали доступ до корпоративної мережі, а згодом і до систем SCADA. Внаслідок атаки понад 230 тис. споживачів залишилися без електропостачання. Це була перша підтверджена кібератака, яка спричинила масштабне енергетичне відключення.
- Industroyer [4] – ще одна атака, що була спрямована на енергетичний сектор України у 2016 році продемонструвала ще вищий рі-

вень складності. Фактично, це модульне шкідливе ПЗ, спеціально розроблене для маніпулювання енергетичними протоколами, що призвело до відключення живлення у Києві. Вперше було продемонстровано здатність коду безпосередньо взаємодіяти з енергетичними мережами, імітуючи операторські дії на рівні промислового обладнання.

- Wolf Creek Nuclear Facility [5] – американська АЕС Wolf Creek була однією з цілей кібератаки у 2017 році. Хоча зловмисникам не вдалося проникнути до операційної мережі, спроби вторгнення у корпоративні системи продемонстрували вразливість ядерної інфраструктури. Було використано зловмисниками спам-кампанії з зараженими документами та фішингом. Подія посилила увагу до розмежування мереж у енергетиці.
- South Korea Nuclear Plant Attack [6] – кібератака на АЕС Південної Кореї у 2014 році, коли північнокерейські хакери зламали комп'ютерні системи компанії KHNP, який є оператором 23 атомних реакторів у країні. У результаті атаки в мережу були викладені внутрішні документи, зокрема технічні креслення, навчальні посібники та особисті дані працівників. Зловмисники також публічно вимагали зупинити роботу кількох реакторів. Хоча KHNP заявила, що критичні системи управління залишилися недоторканими, інцидент викликав серйозні занепокоєння щодо кіберзахисту ядерної інфраструктури. Цей випадок став важливим сигналом для міжнародної спільноти про необхідність зміцнення кібербезпеки об'єктів КІ, зокрема у сфері атомної енергетики.

Відповідно до [7] кіберзахист інформаційних та/або керуючих систем (ІКС) АЕС – це комплекс адміністративних, технічних і програмних заходів та засобів, метою яких є запобігання, виявлення і реагування на кібератаки та кіберзагрози. Відповідно, під кібератаками на ІКС АЕС розуміють дії, які здійснюються за допомогою засобів електронних комунікацій (охоплюючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на компрометацію ІКС АЕС через використання вразливостей. Кіберзагроза ІКС АЕС – це наявні та потенційно можливі явища і чинники, що можуть стати потенційною причиною кіберінциденту (подія, під час виникнення якої піддаються компрометації ІКС АЕС, її компоненти або мережеве обладнання), який може спричинити нанесення шкоди ІКС АЕС.

У [7] також задекларовано глибокоешелонований та диференційований кіберзахист ІКС АЕС, включаючи адміністративні, технічні, програмні та програмно-технічні заходи, які забезпечують:

- попередження шкідливих дій через протидію та захист;
- застосування засобів виявлення, затримки та реагування на шкідливі дії;
- пом’якшення наслідків шкідливих дій, включно із заходами з відновлення нормального функціонування ІКС АЕС.

Розглянемо вимоги міжнародних стандартів у цій галузі [8-10]:

IEC 60880:2006 [8] забезпечує надійність ПЗ систем категорії А, які є критично важливими для безпеки ядерного об'єкта. Хоча сам стандарт не є суто кібербезпековим, його вимоги до структурованої розробки, ретельної верифікації, відмовостійкості та формального аналізу прямо сприяють мінімізації ризиків, пов’язаних із потенційними кіберзагрозами. Надійне ПЗ без помилок – основа для запобігання успішним кібератакам через експлуатацію вразливостей у коді або логіці.

IEC 62138-2018 [9] стосується ПЗ для менш критичних функцій (категорії B і C), але він також враховує загрози кібербезпеці. У контексті кіберзахисту важливим є забезпечення документованого управління змінами, застосування перевірених компонентів, контроль доступу та належне тестування функцій безпеки. Навіть у системах з нижчим рівнем критичності зловмисник може використати вразливості як «точки входу» для масштабної атаки на інші системи, тому відповідність цьому стандарту є ключовою частиною кіберзахисту в глибину (defense-in-depth).

IEC 62645:2019 [10] – це основний міжнародний стандарт, безпосередньо присвячений кіберзахисту в атомній енергетиці. Він вимагає створення комплексної програми безпеки, яка включає ідентифікацію активів, зонування, оцінку ризиків, захист від несанкціонованого доступу, протидію зовнішнім і внутрішнім загрозам, моніторинг подій і безперервне удосконалення заходів безпеки. Стандарт гармонізований із принципами IAEA NSS 33-T та відповідає кращим практикам побудови кіберстійкості ядерної інфраструктури. Його дотримання є обов'язковим елементом у захисті АЕС від сучасних кібератак.

Кіберзахист атомної енергетики є критично важливим, оскільки комп’ютеризовані системи керування, моніторингу та безпеки на АЕС безпосередньо впливають на фізичну безпеку об’єкта, персоналу та

навколишнього середовища. Вразливості в інформаційних та технологічних системах можуть бути використані зловмисниками для виведення з ладу систем безпеки, порушення контролю над реактором або створення умов для аварійних ситуацій.

У роботі проаналізовано особливості кіберзахисту ІКС АЕС згідно міжнародних стандартів та вітчизняних нормативних документів. Подальші дослідження буде присвячено розробці структурно-аналітичної моделі забезпечення вимог кіберзахисту ІКС АЕС та моніторингу їх виконання в процесі функціонування об’єктів захисту.

Список використаних джерел

1. Закон України «Про критичну інфраструктуру» (Відомості Верховної Ради, 2023, № 5, ст.13), https://zakon.rada.gov.ua/laws/show/1882-20#Text

2. Вінтенко, Б., Миронець, І., Смірнов та ін. (2024). Дослідження вимог та аналіз кібербезпеки програмного забезпечення інформаційно-керуючих систем АЕС, важливих для безпеки, Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 3 (23), с. 111-131. https://doi.org/10.28925/2663-4023.2024.23.111131

3. N. Thapliyal and S. Dhariwal, "Protecting A Nuclear Power Plant Against A Stuxnet Attack: Power Of Computer Security," 2023 International Conference on Communication, Security and Artificial Intelligence (ICCSAI), Greater Noida, India, 2023, pp. 598-603, doi: 10.1109/ICCSAI59793.2023.10421224.

4. R. Štefko, K. Eliáš, K. Glajc, A. Hyseni, F. Margita and J. Šimčák, "Cybersecurity Challenges in the Power Sector: Analysing Attacks on Electrical Grids and Substations," *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, Stará Lesná, Slovakia, 2025, pp. 000459-000464, doi: 10.1109/SAMI63904.2025.10883298.

5. Hackers Are Targeting Nuclear Facilities, Homeland Security Dept. and F.B.I. Say, https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html

6. Revisiting the 2014 Korea Hydro and Nuclear Power Hack: Lessons Learned for South Korean Cybersecurity, https://www.38north.org/2024/03/revisiting-the-2014-korea-hydro-and-nuclear-power-hack-lessons-learned-for-south-korean-cybersecurity

7. Наказ ДІЯР України № 223 від 22.03.2022 «Про затвердження Вимог до кіберзахисту інформаційних та керуючих систем атомних станцій для забезпечення ядерної та радіаційної безпеки» https://zakon.rada.gov.ua/laws/show/z0395-22#Text

8. IEC 60880:2006 – Nuclear power plants – Instrumentation and control systems important to safety –Software aspects for computer-based systems performing category A functions, 2006.

9. IEC 62138-2018 – Nuclear power plants – Instrumentation and control systems important for safety – Software aspects for computer-based systems performing category B or C functions, 2018.

IEC 62645:2019 – Nuclear power plants – Instrumentation and control systems – Requirements for security programs for computer-based systems, 2019.

UDC 621.391

O. Lavrynenko
State University "Kyiv Aviation Institute"

VOICE CONTROL COMMAND RECOGNITION SYSTEM OF UAV BASED ON CEPSTRAL ANALYSIS

In this paper, as proposed and described in detail an algorithm for calculation mel-frequency cepstral coefficients (MFCC), which is used to create a basic voice recognition system, on the basis of which can be built more complex solutions of voice control such as the system of voice radio control functions of UAV for qualitative decision of tasks in the military intelligence purposes, which is a new approach in this field of application [1]. The main goal of this article is to design the voice command recognition new system based on cepstral analysis for controlling the UAV with its subsequent optimization. The following objectives need to be met in order to fulfill this goal. a) To do research on the methods of detection individual features of speech signals MFCC, used in voice recognition systems. b) To do research on the voice recognition system and algorithm for calculation of MFCC in the MATLAB as an example of identification of different subjects spoken commands: «Up», «Down», «Right», «Left». c) To carry out a comparative assessment of the calculated values from the selected minimum distance criterion, which is the main indicator of the quality of voice recognition test. d) To do research on the voice command recognition system based on cepstral analysis in software package MATLAB. The developed voice command recognition system based on cepstral analysis has two operation modes: the learning mode and the recognition mode (testing). These modes include a functional scheme of voice command recognition system based on cepstral analysis (Fig.1), a task which is the primary processing of speech recognition and feature selection, which are mainly used in MFCC. If the system is in the learning mode received in step release values recognition features are saved in the reference database of voice images. When the system is in a state of recognition, the values set of MFCC of subject of controll of voice command sequentially compared to all sets of MFCC values from the database of standard voice samples. The task function of the decision to determine the best result of the comparison to one of the specified criteria, and to give recognition result. This research article considers the approach

to solving the problem of recognition of voice commands using MFCC splitting (Fig. 2) for the semantic identification of voice commands.

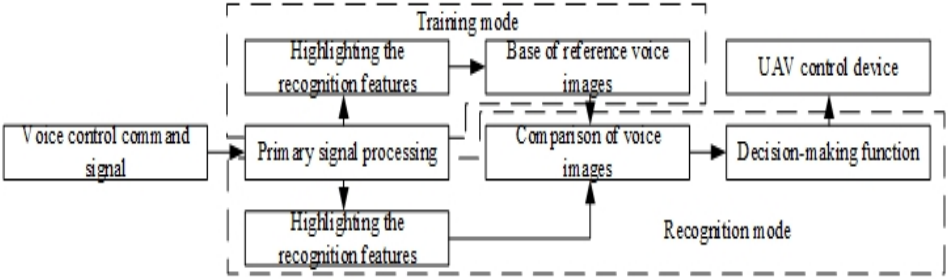


Fig. 1. Voice Control Command Recognition System of UAV based on Cepstral Analysis

The main objective of this research articles is to select in the speech signal features that are relevant for voice command recognition task, that is, information of a semantic component of the voice control of the subject. Selected features will be used to form the base of standard voice samples or for comparison with the voice registered samples MFCC in the database.

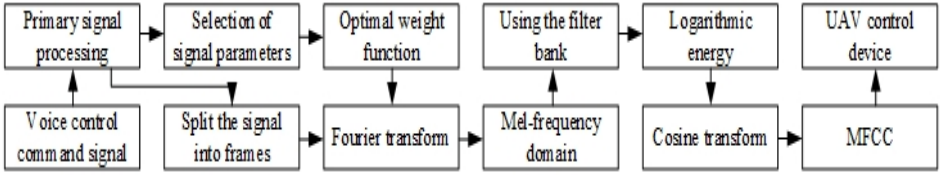


Fig. 2. Algorithm for calculation of MFCC for UAV voice control

Selection of the best parametric features of voice signal is an important task in the development of any UAV voice control system. It significantly affects the quality of recognition.

Calculation of MFCC includes the following steps [2]. At the input of the algorithm speech signal is supplied frequency band, which is very limited and is in the range from 300 to 4000 Hz. The prevailing approach to speech signal processing procedure is to use short-term analysis. That is, the signal is split into fixed size time window, in which signal parameters do not change. For speech signal the window size is usually chosen in the range of 10-30 ms. For a more accurate signal notation between the windows do overlap, equal to half the length of the window. Then algorithm recognition features selection of (MFCC) is applied to each window. Based on the foregoing, the pre-processing of the speech signal is divided into K frames for N counts, split into $1/2$ of frame length. The input of a dis-

crete Fourier transform (DFT) is fed a sequence readout portion of the speech signal (K frame), investigated in this iteration, $x_0, \ldots, x_{N-1}$. Weighting function, and then the DFT is used for a given sequence. In practice, as the weighting function is often used Hamming window which is as follows:

$$w[n] = 0.53836 - 0.46164 \cdot \cos\left(2\pi \frac{n}{N-1}\right), \; n = 0, \ldots, N-1$$

where, N - window length expressed in counting.

Then DFT weighted speech signal can be written as a formula:

$$X[k] = \sum_{n=0}^{N-1} x[n] w[n] e^{\frac{-2\pi j}{N} kn}, \; k = 0, \ldots, N-1.$$

The representation of the speech signal in the frequency domain is divided into bands with the help of the bank (comb) triangular filters. Multiplying the function to filter, we average it at a certain site. Each triangular filter finds a weighted average of the spectral amplitude values corresponding to frequencies in the range between the lower and upper frequency for this filter. If the amplitude corresponds exactly to the average of frequency bands, it is multiplied by a ratio equal to one. When moving the corresponding amplitude value of the frequency from the middle to the lower or upper limit of the coefficient decreases from one to zero. The resulting of the amplitudes on the coefficients are added and divided by the number of amplitude values. The result is the weighted average for a given frequency band. Filter's edges are calculated in mel scale. This scale is the result of research on the human ear's ability to perceive sounds at different frequencies [3]. Transformation into mel-frequency domain is carried out according to the formula:

$$M = 1127.01048 \ln\left(1 + F / 700\right).$$

The inverse transformation is expressed in hertz by the formula:

$$F = 700\left(e^{M/1127.01048} - 1\right).$$

The formula for dividing the frequency axis into triangular filters will be as follows:

$$f[m] = \left(\frac{N_f}{Fs}\right) M^{-1}\left(M\left(F_{\min}\right) + m \frac{M\left(F_{\max} - F_{\min}\right)}{N_f + 1}\right),$$

where, N_f - the amount of mel-filters (usually use about 24 filters), Fs - sampling frequency, $M\left(F\right)$ - frequency transfer function in hertz into frequency in mel, discussed earlier, $M\left(F_{\max}-F_{\min}\right)$ - the analyzed frequency range in Mel, which is divided into N_f evenly distributed overlapping ranges and calculated in the corresponding edges in the linear frequency. We form bank triangular filters according to the following formula:

$$H_m\left[k\right]=\begin{cases}0, & k<f\left[m-1\right]\\ \dfrac{\left(k-f\left[m-1\right]\right)}{\left(f\left[m\right]-f\left[m-1\right]\right)}, & \mathrm{f}\left[m-1\right]\le k<f\left[m\right]\\ \dfrac{\left(f\left[m+1\right]-k\right)}{\left(f\left[m+1\right]-f\left[m\right]\right)}, & f\left[m\right]\le k\le f\left[m+1\right]\\ 0, & k>f\left[m+1\right]\end{cases}$$

where, $H_m\left[k\right]$ - filters weighted coefficients.

The use of the filter is pair-wise multiplication of its values with the values of the spectrum. Because filters have N_f, coefficients will be the same. Filters are applied to the square of the modulus of the DFT coefficients, that is, we need to apply mel-filters not to the values of the spectrum, but to his energy. Do so, you need to calculate the energy for each window, and then take the logarithm of results. It is believed that in this way the sensitivity to noise ratios is decreased. The logarithm of the spectrum energy values are taken and represented as follows:

$$E\left[m\right]=\ln\left(\sum_{k=0}^{N-1}\left|X\left[k\right]\right|^2 H_m\left[k\right]\right),\ m=0,\ \ldots,N_f-1.$$

The final step in calculating MFCC to reduce the number of output parameters and de-correlation component is DCP, which is given by the formula:

$$c\left[n\right]=\sum_{m=0}^{N_f-1}E\left[m\right]\cos\left(\frac{\pi n\left(m+\frac{1}{2}\right)}{N_f}\right),\ n=0,\ \ldots,N_f-1.$$

This transformation has the property of compactness of energy: greater energy corresponds to a smaller amount of information. The resulting set of values is called MFCC. $c[0]$ coefficient is not used, as is the energy of the speech signal. Thus, we have a very small set of values, which in recognizing successfully replaces thousands of samples of the speech signal. Typically, it retained only the first few elements (8 to 16), which later produced the identification of voice commands [4]. Fig. 3 shows calculated by developed algorithm of MFCC experimental samples of voice commands control subject №1: «Up», «Down», «Right», «Left».

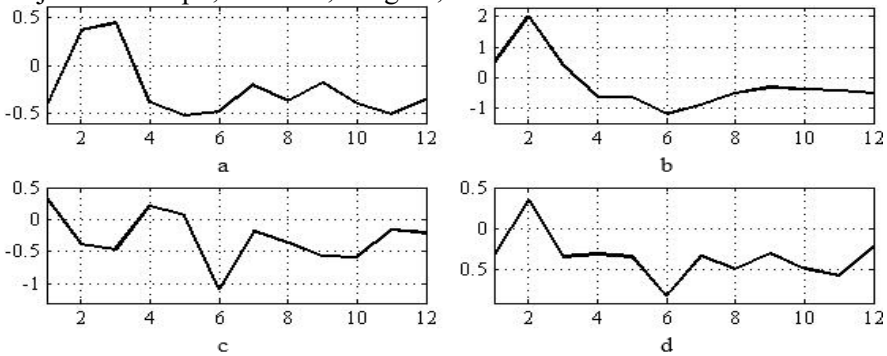


Fig. 3. MFCC voice commands control subject №1:
a - «Up», b - «Down», c - «Right», d - «Left»

In this system for evaluation of the results of automatic recognition of voice commands a classifier built by the criterion of minimum distance is used. As such indicator figure stands variance of the difference of the expectation value of MFCC saved in base of standard voice samples with expectation value of MFCC at the testing system level. The dispersion of the difference of the expectation values of the two samples of voice commands (MFCC), written as follows:

$$D = \frac{\sum_{i=1}^{n} \left(\frac{\sum_{i=1}^{n} x_i}{n} - \frac{\sum_{i=1}^{n} \overline{x}_i}{n} \right)^2}{n},$$

where, x_i - saved in base of standard voice samples, $\overline{x}_i$ - at the testing system level, n - amount of MFCC. The decision of semantic identification of the voice commands accepted by the criterion of minimum dispersion, ie

the least deviation compared MFCC in a certain threshold of recognition which is given by:

if $D_{\min} < \Theta$

"identified! "

else

"not identified! "

end

where, $D_{\min}$ - minimal dispersion, $\Theta = 1 - \Delta$ - specified threshold of allowable recognition (in practice usually $\Delta = 0.80 \ldots 0.90$ is used). Minimal dispersion, which became a specified threshold of allowable recognition is the best result of the comparison, and therefore, the command is identified (recognized) - "identified! ". Otherwise, the voice command fails semantic identification (not recognized) - "not identified! "[4].

This paper introduces voice command recognition system based on cepstral analysis, which allows to increase the efficiency of voice recognition. The paper details the results of preliminary experimental studies on which conclusions on the desirability of further research and practical application of the developed voice command recognition system based on cepstral analysis algorithm for calculation of MFCC, as well as justification of scientific importance of research. The comparative assessment of the calculated values from the selected minimum distance criterion, which is the main indicator of the quality of voice recognition test has been carried out.

References

[1] S.S. Anand, R. Mathiyazaghan, “Design and Fabrication of Voice Controlled Unmanned Aerial Vehicle,” International Journal of Robotics and Automation, vol. 5, no. 3, pp. 205-212, 2016.

[2] D. Bakhtiiarov, G. Konakhovych, and O. Lavrynenko, “Protected System of Radio Control of Unmanned Aerial Vehicle,” Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 196-199, 2016.

[3] O. Lavrynenko, G. Konakhovych, and D. Bakhtiiarov, “Method of Voice Control Functions of the UAV,” Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 47-50, 2016.

[4] O. Lavrynenko, G. Konakhovych, R. Odarchenko and D. Bakhtiiarov, “Voice Command Signal Compression Algorithm by Functions of Unmanned Aerial Vehicles,” Aerospace Technic and Technology, vol. 130, no. 3, pp. 57-67, 2016.

UDC 621.391

O. Lavrynenko
State University "Kyiv Aviation Institute"

COMPRESSION ALGORITHM OF VOICE CONTROL COMMAND OF UAV BASED ON WAVELET TRANSFORM

In voice control systems UAV there is a problem of speech redundancy. One of the main problem of the speech signal compression algorithm is the methods of optimal reduction of redundancy of voice data and optimization of its parameters with the parameters of the UAV control system. The solution of the problem will allow to increase the capacity of linear paths and channels in the conditions of specified criterions of communication UAV quality.

The reduction of redundancy of voice data, while maintaining the required quality of speech perception allows to transmit the data at lower speeds, thereby increasing the channel UAV capacity.

1. Need to develop a digital speech signal compression algorithm based on wavelet transform (WT) using entropy arithmetic coding and optimization of its parameters with the parameters of the UAV control system, which allows to achieve desired results in the enhancement of data compression while maintaining the intelligibility of speech, which in its turn will transmit speech data at low speeds and decreasing the flow of transmitted information, thereby increasing the bandwidth of existing linear paths and channels UAV.

2. Need to prove experimentally and substantiate the usefulness of using digital speech signal compression algorithm based on WT in voice control systems UAV.

The objectives of the experimental studies:

a) To develop and research the proposed digital speech signal compression algorithm based on WT in the software package MATLAB.

b) To calculate the bit rate (BR), the compression ratio (CR), the correlation coefficient (CC), the signal / noise ratio (SNR), peak signal / noise ratio (PSNR) and root-mean square error (RMSE) of experimental example of the speech up and after the application of the compression algorithm.

c) To carry out a comparative evaluation of the CR, CC, SNR and PSNR depending on BR.

d) To carry out a comparative evaluation of the CR, CC, SNR and PSNR depending on CR.

The developed digital speech signal compression algorithm based on WT providing optimal solutions of the relevant tasks such as digital speech data compression, the maximum speech signal quality at a certain level of compression, the possibility of the release of some bandwidth of the communication channel for the transmission of digital data (commands), security of transmitted speech data, the possibility to implement the algorithm microprocessor with low productivity to reduce the cost of the developed device.

Developed and researched digital speech signal compression algorithm based on WT using entropy arithmetic coding provides a reduction in volume of digital speech data with together with speech intelligibility and thereby increases the bandwidth of the communication channel. The results of experimental studies suggest the feasibility of further practical application of the proposed digital speech signal compression algorithm based on wavelet transform into different models of vocoding devices.

The article presents the developed digital speech signal compression algorithm based on WT using entropy arithmetic coding (Fig. 1). In the research as an input digital speech compression algorithm is used male voice recording with a sampling rate of 8 kHz and the quantization bit depth of 8 bits per sample, which corresponds to the basic digital channels of the telephone network – 64 Kbit / s. The main task of speech signal compression is to reduce the flow of data transmitted over the digital communication channel with a slight deterioration of the restored-term speech at the receiving end.

Speech signal compression according to the developed algorithm takes place in several phases. In the first phase for noise reduction and normalization of frequency spectrum of digital speech signal is supplied to 2nd order Butterworth low pass filter, where $n=5$ with a bandwidth 300…3400 Hz, which is represented as a row vector b and a, having a length $2n+1$ and the polynomial coefficients of numerator and denominator of transmitting function descending powers of z: $H(z)=\frac{B(z)}{A(z)}=\frac{b(1)+b(2)z^{-1}+\ldots+b(n+1)z^{-n}}{1+a(2)z^{-1}+\ldots+a(n+1)z^{-n}}$. Butterworth filter cutoff frequency is the frequency at which transmission coefficient module is

$\sqrt{1/2}$. Fig. 2 shows diagram of frequency-response characteristic (FRC), phase-frequency response (PFC), impulse response (IR) of synthesized 10th order Butterworth filter with a bandwidth 300…3400 Hz.

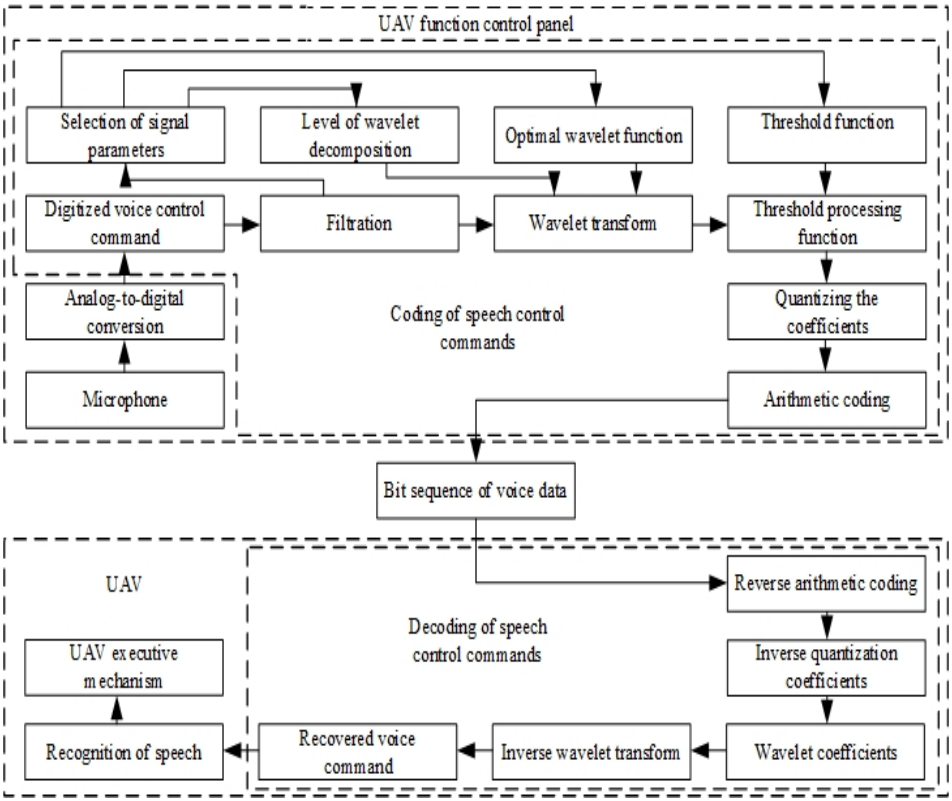


Fig. 1. Compression Algorithm of Voice Control Command of UAV based on Wavelet Transform

In the second phase compression algorithm normalized after filtration speech signal after filtering comes on the discrete wavelet transform (DWT) block [1]. Since the speech signal is a non-stationary random process, then to process it was proposed to use DWT the input of which receives the digital samples of the speech signal, and the output generated wavelet coefficients (WC).

Based on an earlier experimental study as a mother wavelet function is appropriate to use the Daubechies wavelet of order 12.

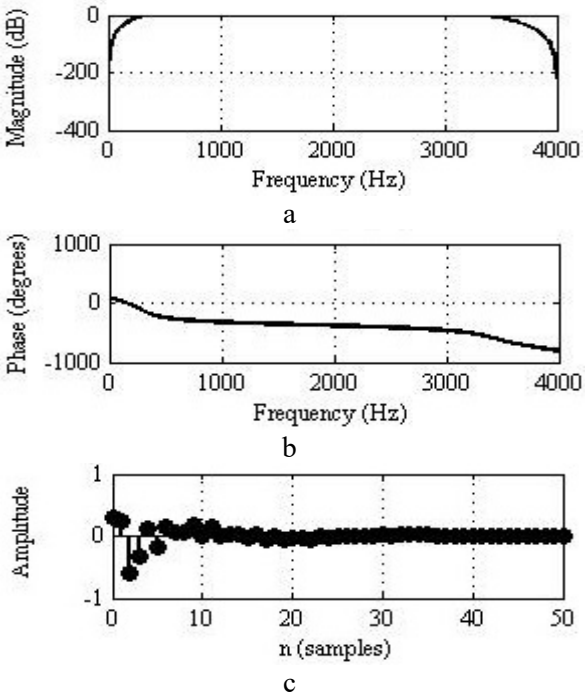


Fig. 2. a – FRC, b – PFC, c – IR of synthesized 10th order Butterworth filter with a bandwidth 300…3400 Hz

Calculation of the order N Daubechies scaling filter comes to finding the roots of a polynomial of degree $4N$, whose coefficients

$$a(k) = \frac{\prod_{l=-N+1}^{N}\left(\frac{1}{2}-l\right)}{\prod_{l=-N+1}^{N}(k-l)},\ k=1,...N;$$

for all $k \neq l$ form sets $\{a(N)\ \ 0\ \ a(N-1)\ \ 0\ ...\ 0\ \ a(1)\ \ 1\ \ a(1)\ \ 0\ \ a(2)\ \ 0\ ...\ 0\ \ a(N)\}$ [2].

In the third phase WC after DWT come on the thresholding block. The main property of DWT is that the converted signal is represented by a large number of redundant WC, which, after thresholding are reset WC resets via a given threshold function, WC low or equal to that will be equal to zero,

and the rest will remain unchanged. WC with an absolute value close to zero only contain a small part of the signal energy. WC resetting results in negligible energy losses. This property makes DWT attractive for compressing voice data [3].

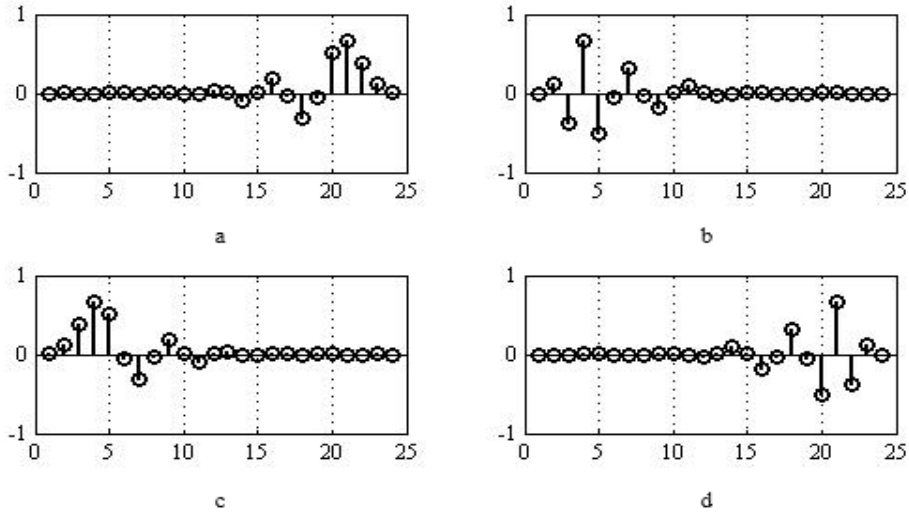


Fig. 3. Orthogonal Daubechies filter of order 12:
a – decomposition low-pass filter, b – decomposition high-pass filter,
c – reconstruction low-pass filter, d – reconstruction high-pass filter.

$$y = \begin{cases} x, |x| > \Theta \\ 0, |x| \le \Theta \end{cases}$$

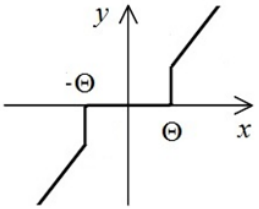


Fig. 4. The threshold function

The Fig. 4 shows a threshold function for processing the WC speech signal, where x – the value of the WC before the threshold, y – the value of WC after threshold, Θ – threshold. Threshold enhancement will increase the degree of redundancy reduction, but at the same time will decrease speech intelligibility. Lowering the threshold to reduce the loss of informational WC, but also reduces the effectiveness of signal compression [4].

In the fourth phase of the WC compression algorithm after thresholding is introduced as 8-bit integers. This format is also used for the data transmission. Since detail and approximation of WC are real numbers, then before you performing of speech compression by the arithmetic coding, it is necessary to convert the WC which passed threshold in a numerical range corresponding to the selected format. Otherwise, the WC compression flow will be bigger than speech signal flow. This operation can be performed using the quantization. Thus arises the quantization error, which introduces additional distortion in the transmitted speech signal. In the fifth phase of the of compression algorithm, the quantized WC encoded by the by arithmetic coding, whereby in the output the compressed bit sequence of speech signal data is generated. A distinctive feature of the arithmetic coding from well-known coding methods is that neither the encoder or decoder does not store all possible set of code words. Instead, in the transmission of a particular sequence x the code word $c(x)$ is calculated only for predetermined sequence x. Encoding rules are known to the decoder, and it restores x by $c(x)$, not having a full list of code words [5].

References

[1] O. Lavrynenko, G. Konakhovych, and D. Bakhtiiarov, “Method of Voice Control Functions of the UAV,” Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 47-50, 2016.

[2] D. Bakhtiiarov, G. Konakhovych, and O. Lavrynenko, “Protected System of Radio Control of Unmanned Aerial Vehicle,” Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 196-199, 2016.

[3] G.F. Konakhovych, O.Y. Lavrynenko, V.V. Antonov, and D.I. Bakhtiiarov, “A digital speech signal compression algorithm based on wavelet transform,” Electronics and control systems, vol. 48, no. 2, 30-36, 2016.

[4] L.F. Sanchez, H. Abaunza, P. Castillo, "Safe navigation control for a quadcopter using user's arm commands", Unmanned Aircraft Systems (ICUAS) 2017 International Conference on, pp. 981-988, 2017.

[5] G.F. Konahovich, A.I. Davletyants, A.Y. Lavrynenko, and D.I. Bakhtiyarov, “The comparative analysis the Fourier transform, cosine transform and wavelet transform as a spectral analysis of the digital speech signals,” Science-Based Technologies, vol. 27, no. 3, pp. 210-220, 2015.

UDC 621.391

O. Lavrynenko
State University "Kyiv Aviation Institute"

COMPARATIVE ANALYSIS OF SPEECH RECOGNITION ALGORITHMS UAV

Although automatic speech recognition systems have dramatically improved in recent decades, speech recognition accuracy still significantly degrades in noisy environments. While many algorithms have been developed to deal with this problem, they tend to be more effective in stationary noise such as white or pink noise than in the presence of more realistic degradations such as background music, background speech, and reverberation. At the same time, it is widely observed that the human auditory system retains relatively good performance in the same environments. The goal of this thesis is to use mathematical representations that are motivated by human auditory processing to improve the accuracy of automatic speech recognition systems. Throughout this work we propose a number of signal processing algorithms that are motivated by these observations and can be realized in a computationally efficient fashion using real-time online processing. We demonstrate that these approaches are effective in improving speech recognition accuracy in the presence of various types of noisy and reverberant environments.

The Frequency scales describe how the physical frequency of an incoming signal is related to the representation of that frequency by the human auditory system. In general, the peripheral auditory system can be modeled as a bank of bandpass filters, of approximately constant bandwidth at low frequencies and of a bandwidth that increases in rough proportion to frequency at higher frequencies. Because different psychoacoustical techniques provide some-what different estimates of the bandwidth of the auditory filters, several different frequency scales have been developed to fit the psychophysical data. Some of the widely used frequency scales include the MEL scale, the BARK scale, and the ERB (Equivalent rectangular bandwidth) scale. The popular Mel Frequency Cepstral Coefficients (MFCCs) incorporate the MEL scale, which is represented by the following equation:

$$Mel(f) = 2595 \log\left(1 + \frac{f}{700}\right).$$

The MEL scale that was proposed by Stevens describes how a listener judges the distance between pitches. The reference point is obtained by defining a 1000 Hz tone 40 dB above the listener's threshold to be 1000 mels. Another frequency scale, called the Bark scale, was proposed by Zwicker:

$$Bark(f) = 13\arctan(0,00076f) + 3.5\arctan\left(\frac{f}{7500}\right)^2.$$

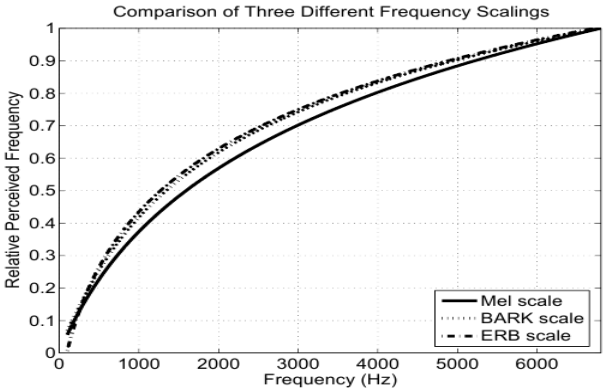


Fig. 1. Comparison of the MEL, Bark, and ERB frequency scales

Frequency relation is based on a similar transformation given by Schroeder:

$$\Omega(f) = 6\ln\left(\frac{f}{600} + \left(\frac{f}{600}\right)^{0,5}\right).$$

More recently, Moore and Glasberg proposed the ERB (Equivalent Rectangular Bandwidth) scale modifying Zwicker's loudness model. The ERB scale is a measure that gives an approximation to the bandwidth of filters in human hearing using rectangular bandpass filters; several different approximations of the ERB scale exist. The following is one of such approximations relating the ERB and the frequency f:

$$ERB(f) = 11.17\log\left(1 + \frac{46.065f}{f + 14678.49}\right).$$

Fig. 1 compares the three different frequency scales in the range between 100 Hz and 8000 Hz. It can be seen that they describe very similar relationships between frequency and its representation by the auditory system [1].

Auditory nonlinearity is related to how humans process intensity and perceive loudness. The most direct characterization of the auditory nonlinearity is through the use of physiological measurements of the the average firing rates of fibers of the auditory nerve, measured as a function of the intensity of a pure-tone input signal at a specified frequency. As shown in Fig. 2, this relationship is characterized by an auditory threshold and a saturation point. The curves in Fig. 2 are obtained using the auditory model developed by Heinz [2].

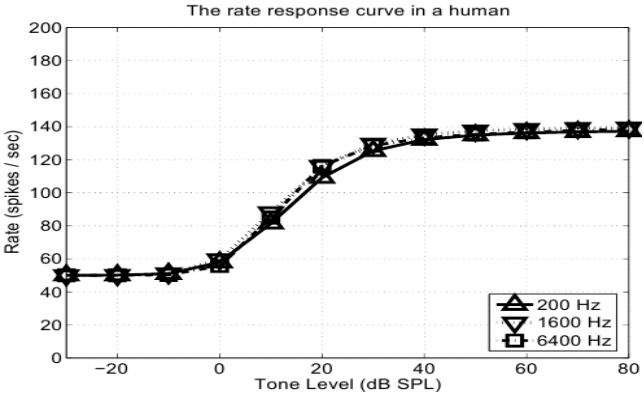


Fig. 2. The rate-intensity function of the human auditory system as predicted by the model of Heinz et al. for the auditory-nerve response to sound

Another way of representing auditory nonlinearity is based on psychophysics. One of the well-known psychophysical rules is Steven's power law, which relates intensity and perceived loudness in a hearing experiment by fitting data from multiple observers in a subjective magnitude estimation experiment using a power function:

$$L = \left(\frac{I}{I_0} \right)^3 .$$

Another common relationship used to relate intensity to loudness in hearing is the logarithmic curve, which was originally proposed by Fechner to relate the intensity-discrimination results of Weber to a psychophysical transfer function. MFCC features, for example, use a logarithmic function to relate input intensity to putative loudness, and the definition of sound pressure level (SPL) is also based on the logarithmic transformation:

$$L_p = 20\log_{10}\left(\frac{p_{rms}}{p_{ref}}\right).$$

The commonly-used value for the reference pressure p_{ref} is $20\mu Pa$, which was once considered to be the threshold of human hearing, when the definition was first established [3].

In Fig. 3, we compare these nonlinearities. In addition to the nonlinearities mentioned in this Sec., we included another power-law nonlinearity which is an approximation to the physiological model of Heinz et al. between 0 and 50 dB SPL in the Minimum Mean Square Error (MMSE) sense. In this approximation, the estimated power coefficient is around 1/10.

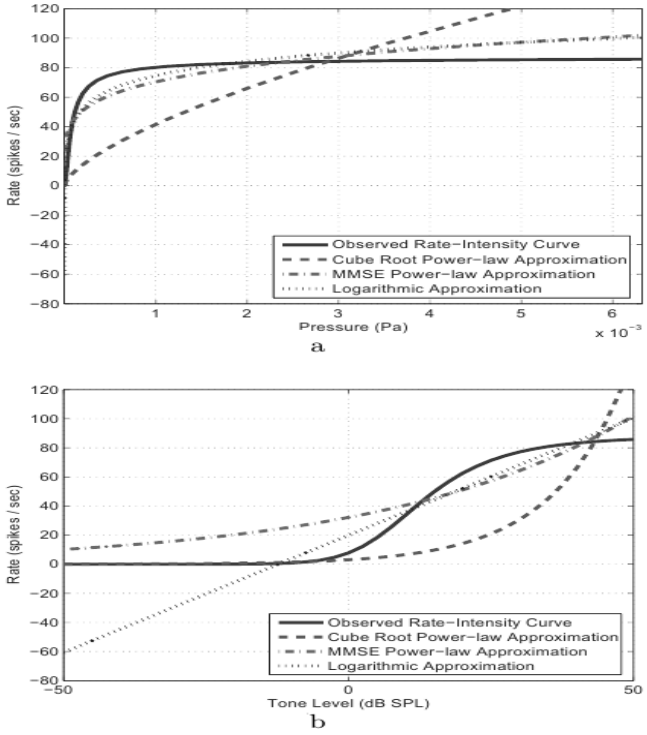


Fig. 3. Comparison of the cube-root power law nonlinearity, the MMSE power-law nonlinearity, and logarithmic nonlinearity. Plots are shown using two different intensity scales: pressure expressed directly in P_a (upper panel) and pressure after the log transformation in dB SPL (lower panel)

In Fig. 3 (a), we compare these curves as a function of sound pressure directly as measured in Pa. In this figure, with the exception of the cube power root, all three curves are very similar. Nevertheless, if we plot the curves using the logarithmic scale (dB SPL) to represent sound pressure level, we can observe a significant difference between the power-law nonlinearity and the logarithmic nonlinearity in the region below the auditory threshold. This difference plays an important role for robust speech recognition [4].

The most widely used forms of feature extraction are Mel Frequency Cepstral Coefficient (MFCC) and Perceptual Linear Prediction (PLP). MFCC processing begins with pre-emphasis, typically using a first-order high-pass filter. Short-time Fourier Transform (STFT) analysis is performed using a hamming window, and triangular frequency integration is performed for spectral analysis. The logarithmic nonlinearity stage follows, and the final features are obtained through the us of a Discrete Cosine Transform (DCT) [5]. PLP processing, which is similar to MFCC processing in some ways, begins with STFT analysis followed by critical-band integration using trapezoidal frequency-weighting functions. In contrast to MFCC, pre-emphasis is performed based on an equal-loudness curve after frequency integration. The nonlinearity in PLP is based on the power-law nonlinearity proposed by Stevens. After this stage, Inverse Fast Fourier Transform (IFFT) and Linear Prediction (LP) analysis are performed in sequence. Cepstral recursion is also usually performed to obtain the final features from the LP coefficients. The simplest way of performing normalization is using CMN or MVN. Histogram normalization (HN) is a generalization of these approaches. CMN is the most basic form of noise compensation schemes, and it can remove the effects of linear filtering if the impulse response of the filter is shorter then the window length. By assuming that the mean of each element of the feature vector from all utterances is the same, CMN is also helpful for additive noise as well.

CMN can be expressed mathematically as follows:

$$\overline{c}_i = c_i[j] - \mu_{c_i},\ 0 \le i \le I-1,\ 0 \le j \le J-1$$

where μ_{c_i} is the mean of the i^{th} element of the cepstral vector. In the above equation, $c_i[j]$ and $\overline{c}_i[j]$ represent the original and normalized cepstral coefficients for the i^{th} element of the vector at the j^{th} frame index. I denotes the dimensionality of the feature vector and J denotes the num-

ber of frames in the utterance [6].

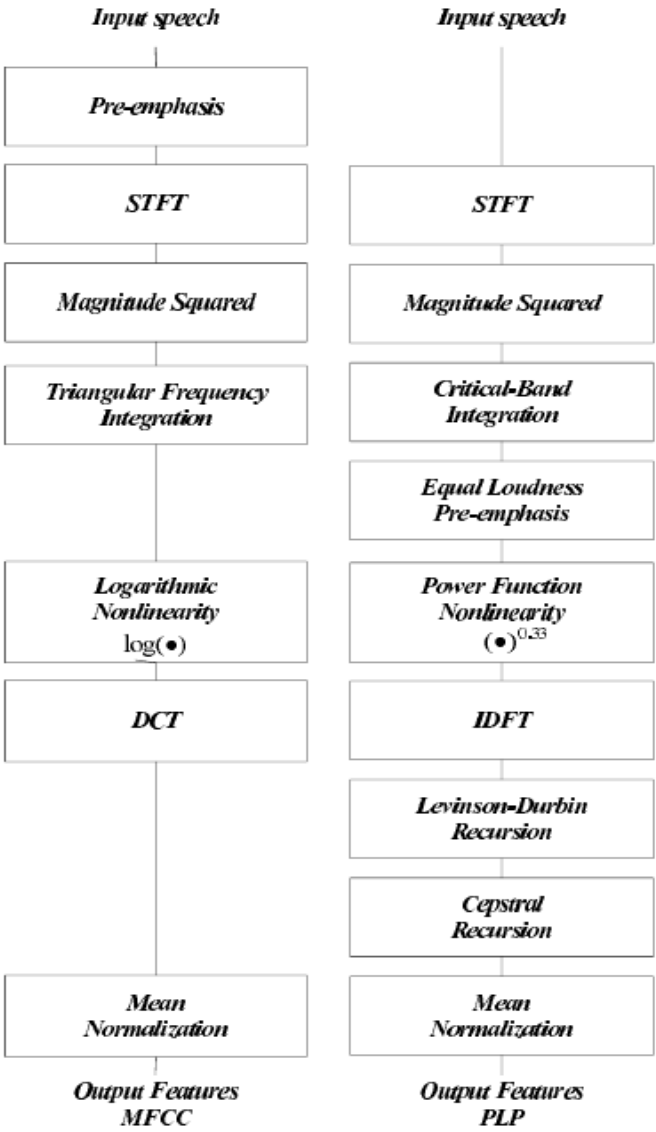


Fig. 4. Block diagrams of MFCC and PLP processing

MVN is a natural extension of CMN and is defined by the following equation:

$$\overline{c}_i[j] = \frac{c_i[j] - \mu_{c_i}}{\sigma_{c_i}},\ 0 \le i \le I-1,\ 0 \le j \le J-1$$

where μ_{c_i} and σ_{c_i} are the mean and standard deviation of the i-th element of the cepstral vector [7].

References

[1] O. Lavrynenko, G. Konakhovych, and D. Bakhtiiarov, "Method of Voice Control Functions of the UAV," Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 47-50, 2016.

[2] D. Bakhtiiarov, G. Konakhovych, and O. Lavrynenko, "Protected System of Radio Control of Unmanned Aerial Vehicle," Methods and Systems of Navigation and Motion Control (MSNMC), IEEE 4th International Conference, pp. 196-199, 2016.

[3] G.F. Konakhovych, O.Y. Lavrynenko, V.V. Antonov, and D.I. Bakhtiiarov, "A digital speech signal compression algorithm based on wavelet transform," Electronics and control systems, vol. 48, no. 2, 30-36, 2016.

[4] O. Lavrynenko, G. Konakhovych, R. Odarchenko and D. Bakhtiiarov, "Voice Command Signal Compression Algorithm by Functions of Unmanned Aerial Vehicles," Aerospace Technic and Technology, vol. 130, no. 3, pp. 57-67, 2016.

[5] G.F. Konahovich, A.I. Davletyants, A.Y. Lavrynenko, and D.I. Bakhtiyarov, "The comparative analysis the Fourier transform, cosine transform and wavelet transform as a spectral analysis of the digital speech signals," Science-Based Technologies, vol. 27, no. 3, pp. 210-220, 2015.

[6] I.O. Kozliuk, D.I. Bakhtiiarov, O.Y. Lavrynenko, and I.V. Tretiak, "Problems of unauthorized interference to the work of UAV and methods of its solving," Science-Based Technologies, vol. 30, no. 2, pp. 206-211, 2016.

[7] G.F. Konahovich, D.I. Bakhtiyarov, and O.Y. Lavrynenko, "Computer modeling of drone protected control channel," Science-Based Technologies, vol. 28, no. 4, pp. 283-290, 2015.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

XV МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

4 – 6 ЧЕРВНЯ 2025 Р.

М. КИЇВ

ГОЛОВНИЙ РЕДАКТОР ГНАТЮК В.О.

КОМП'ЮТЕРНА ВЕРСТКА ЛАВРИНЕНКО О.Ю.

КОНТАКТНИЙ E-MAIL: pezix@tks.nau.edu.ua

ВІДПОВІДАЛЬНІСТЬ
ЗА ЗМІСТ ТА ФОРМУ ВИКЛАДЕННЯ НАУКОВИХ РЕЗУЛЬТАТІВ
НЕСУТЬ АВТОРИ МАТЕРІАЛІВ ТЕЗ.

ЕЛЕКТРОННА ВЕРСІЯ ТЕЗ КОНФЕРЕНЦІЇ ЗРОБЛЕНА СПЕЦІАЛЬНО ДЛЯ РОЗМІЩЕННЯ НА САЙТІ
ДЕРЖАВНОГО УНІВЕРСИТЕТУ «КИЇВСЬКИЙ АВІАЦІЙНИЙ ІНСТИТУТ»
http://tks.nau.edu.ua