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

ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

НАУКОВА АСОЦІАЦІЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

ТЕЗИ

XVI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

28 ТРАВНЯ 2026 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»

May, 28, 2026
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»

28 травня 2026 р.

м. Київ, Україна

УДК 621.39: 004.9 (082)

Проблеми експлуатації та захисту інформаційно-комунікаційних систем: Тези науково-практичної конференції; м. Київ, 28 травня 2026 р., Державний університет «Київський авіаційний інститут». – К.: Вид-во КАІ, 2026. – 124 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

УДК 621.396.96:623.746

Б.С. Авдєєв, В.П. Климчук
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОГРАМНО ОРІЄНТОВАНИЙ РАДІОПРИЙМАЛЬНИЙ ПРИСТРІЙ УДАРНОГО БПЛА

Актуальність. Досвід збройних конфліктів останніх років переконливо демонструє зростаючу роль безпілотних літальних апаратів (БПЛА) ударного класу в сучасних бойових діях. Ефективність таких апаратів значною мірою визначається надійністю їх радіоелектронного обладнання — зокрема, систем управління та відеопередачі. Водночас насичена радіоелектронна обстановка сучасного поля бою, що характеризується активним застосуванням засобів радіоелектронної боротьби (РЕБ) противника, висуває жорсткі вимоги до гнучкості та завадостійкості бортових радіосистем.

Традиційні вузькосмугові радіоприймачі з фіксованими параметрами не здатні адаптуватися до динамічно змінюваної радіообстановки. Альтернативним рішенням є концепція програмно орієнтованого радіо (Software Defined Radio, SDR), що забезпечує широкосмуговий прийом та гнучке програмне перелаштування без заміни апаратури. Метою роботи є розробка бортового SDR-приймача для ударного БПЛА з охопленням діапазонів каналів управління та відеопотоку FPV.

Аналіз радіосигнатур сучасних ударних БПЛА — Bayraktar TB2, Lancet-3, Shahed-136 та FPV-дронів — показав, що основні бойові радіосигнали зосереджені у чотирьох частотних діапазонах: 433 МГц та 868 МГц (канали управління на базі протоколів ELRS та MAVLink), 2.4 ГГц (протоколи ExpressLRS, Crossfire) та 5.8 ГГц (аналоговий та цифровий FPV-відеопотік).

Апаратну основу розробленого пристрою складає SDR-платформа USRP B210 на базі мікросхеми AD9361. За результатами порівняльного аналізу чотирьох платформ (RTL-SDR, HackRF One, LimeSDR, USRP B210) саме USRP B210 забезпечує необхідне перекриття діапазону 70 МГц – 6 ГГц, 12-бітну розрядність АЦП та смугу

пропускання до 56 МГц. Для підвищення чутливості приймача застосовано зовнішні малошумні підсилювачі SPF-5189Z (NF = 0.6 дБ, діапазони 433/868 МГц) та PGA-103+ (NF = 1.4 дБ, діапазон 5.8 ГГц). Перемикання між чотирма цільовими діапазонами здійснюється програмно через ВЧ-комутатор SKY13414-485LF. Цифрова обробка сигналів реалізована на одноплатному комп'ютері NVIDIA Jetson Nano (472 ГФлопс) під керуванням GNU Radio та Python.

Розрахунок коефіцієнта шуму системи за формулою Фріса показав NF = 5.36 дБ для діапазонів 433/868 МГц та NF = 9.02 дБ для діапазону 5.8 ГГц. Розрахована чутливість пристрою становить –105.6 дБм у діапазонах 433/868 МГц та –80.7 дБм у діапазоні 5.8 ГГц, що відповідає або перевищує вимоги технічного завдання. Миттєва смуга пропускання при частоті дискретизації 56 МСамп/с становить 44.8 МГц, динамічний діапазон без шпурів SFDR = 77.2 дБ. Загальне енергоспоживання пристрою — 6.6 Вт, маса модуля — до 200 г, що відповідає обмеженням бортового застосування.

Програмне забезпечення реалізує трирівневий алгоритм обробки сигналів з автоматичним визначенням виду модуляції на основі аналізу миттєвої фази прийнятого сигналу. Алгоритм підтримує демодуляцію сигналів з модуляцією GFSK, FHSS, OFDM та FM. Точність автоматичної класифікації виду модуляції при SNR ≥ 10 дБ перевищує 95%. Практична дальність надійного прийому сигналів ELRS 433 МГц за результатами польового тестування становить 1500–2000 м.

Висновки. Розроблено програмно орієнтований радіоприймальний пристрій для ударного БПЛА, що забезпечує охоплення чотирьох цільових частотних діапазонів у межах єдиної апаратної платформи. Пристрій характеризується чутливістю –105.6 дБм у каналах управління та –80.7 дБм у діапазоні FPV-відеопотоку, SFDR = 77.2 дБ та енергоспоживанням 6.6 Вт. Поєднання широкосмугової апаратної платформи USRP B210 з гнучким програмним середовищем GNU Radio забезпечує можливість оперативного перелаштування алгоритмів обробки без зміни апаратури, що є суттєвою перевагою в умовах динамічної радіоелектронної обстановки сучасного поля бою.

УДК 621.391

В.В. Антонов, В.П. Климчук, А.О. Квятковська
Державний університет «Київський авіаційний інститут»,
Київський фаховий коледж зв'язку, м. Київ

ЗАХИЩЕНИЙ КАНАЛ АВІАЦІЙНОГО ПОВІТРЯНОГО РАДІОЗВ'ЯЗКУ

У зв'язку із загостренням світових політичних протиріч документами ІСАО визначена доцільність створення та подальшого застосування обладнання аналогового радіозв'язку, зокрема в каналах «пілот – авіадиспетчер», на яких наразі використовуються стандартні вузько смугові аналогові VHF (Very High Frequency) радіоканали у діапазоні 118-137 МГц з дискретністю сітки частот 25кГц або 8,33кГц, але за умов, якщо це обладнання забезпечує високий рівень захищеності мовного обміну. Положеннями концепції ICAO CNS/ATM щодо розвитку мережі авіаційного електрозв'язку (ATN) декларується доцільність використання як VHF-ліній аналогового зв'язку, так і VHF-ліній цифрового зв'язку (тобто, лінії VDL Mode 2,3 та 4). Архітектура побудови VHF-ліній аналогового зв'язку не підпадає під семирівневу модель інформаційної взаємодії OSI ISO, через що при побудові засобів захисту виникають певні труднощі науково-технічного характеру, що пов'язані, головним чином, із вузькою смугою аналогових ліній штатних авіаційних систем повітряного радіозв'язку. Проте ІСАО із загальної кількості стандартних VHF-ліній (усього 760 ліній) для VDL-ліній зарезервувала лише чотири лінії, решта 756 ліній виділена під аналоговий мовний зв'язок. При цьому у концепції ICAO CNS/ATM підкреслюється, що навіть у середньостроковій перспективі VHF-лінії аналогового зв'язку будуть активно використовуватися як з частотним розносом у 25кГц, так і у 8,33кГц. Тому виникає задача забезпечення надійного захисту саме VHF-ліній аналогового радіозв'язку.

От же, у рамках існуючого розподілу радіочастотного ресурсу для авіаційних застосувань наразі можлива схема побудови мовного тракту аналогового радіоканалу на ділянці «пілот – авіадиспетчер», що використовує VHF-лінію аналогового зв'язку, може бути представлена так, як це показано на рис.1, де відображена узагальнена технологічна схема обробки мовного трафіка засобами системи авіаційного радіозв'язку для випадку, коли цей трафік потребує гарантованого захисту на рівні Г3 та вище. Схема передбачає необхідність «оцифровки»

потоку аналогових мовних сигналів (що є безальтернативною передумовою застосування криптографічних засобів захисту інформації) та компресії мовної інформації.

Найбільш доцільним шляхом технічної реалізації процедур стиснення та «оцифровки» мовної інформації, як показали результати багатьох досліджень, є застосування вокодерних технологій, оскільки функціональність вокодерів передбачає можливість одночасного здійснення названих вище процедур обробки потоку сигналів. При цьому, у технологічній схемі, що представлена на рис.1, суттєве значення мають два показники якості функціонування вокодера: показник розбірливості мови W, що забезпечує вокодер, під котрим розуміється відносна кількість (у відсотках) правильно прийнятих елементів артикуляційних таблиць, що були передані через канал транспортування мовної інформації та швидкість цифрового потоку мовних сигналів на виході вокодера R (див. точка А на рис.1), що характеризує його можливості із стиснення мовних повідомлень. Вибір вказаних параметрів необхідно проводити з урахуванням наступних особливостей.

Чим менше значення R, тим вище коефіцієнт стиснення мови, проте тим гірше її розбірливість. З іншого боку, спроби забезпечити прийнятний рівень розбірливості мови змушують включати у мовний тракт радіоканалу вокодери, що характеризуються невисокими можливостями щодо стискання мови і, отже, відносно високими значеннями R. За високих значень параметру R, у свою чергу, ширина смуги спектру маніпульованих сигналів мовного тракту на виході маніпулятора мовного сигналу (точка Б на рис.1) може виявитися настільки збільшеною, що після маніпуляції ефективна ширина смуги дискретно-аналогового мовного сигналу (точка Б на рис.1) не зможе вкластися у смугу частот мовного тракту радіоканалу.

Ще більш складніша ситуація щодо можливостей запобігання лінійних спотворень сигналів в каналі може виникнути, якщо криптографічне шифрування призводить до розширення спектру шифрованої послідовності. Бажано, щоб швидкості потоків сигналів на вході та виході шифратора були однаковими. Але таке не завжди можливо досягнути на практиці. Тому актуальним є завдання вибору обладнання криптографічного захисту: з одного боку, це обладнання має забезпечувати прийнятний у даних конкретних умовах рівень криптостійкості, а з іншого, генерувати шифровані послідовності із невисоким рівнем інформаційної надлишковості.

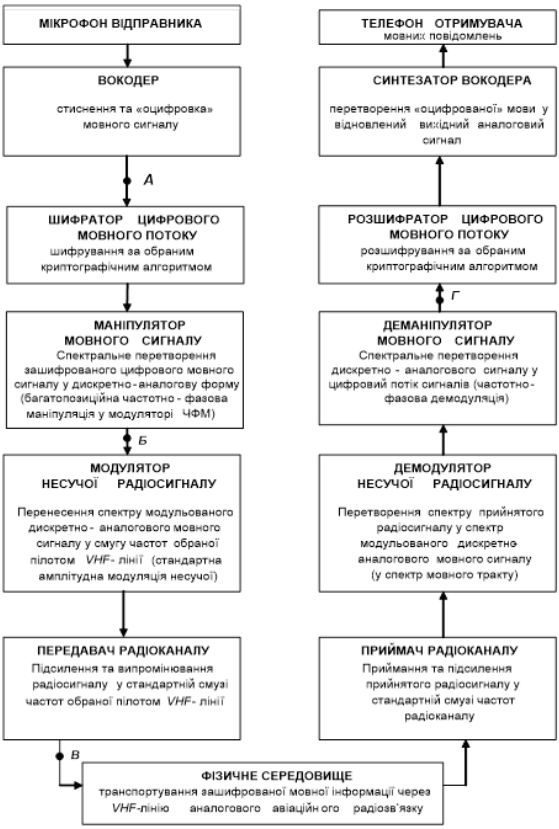


Рис. 1. Технологічна схема обробки захищеного мовного трафіка засобами обладнання авіаційних систем аналогового радіозв'язку.

Висновки

Вирішення названих вище завдань дозволить теоретично обґрунтувати технічну можливість (або неможливість) модернізації існуючого обладнання VHF-ліній аналогового авіаційного зв'язку в напрямку забезпечення норм щодо інформаційної безпеки у радіоканалі таким чином, щоб не порушити будь-якої із норм або рекомендацій, що існують у сферах електрозв'язку та організації повітряного руху.

Результати вирішення цих завдань дозволять визначити технічні параметри вокодера, шифратора/розшифратора та маніпулятора/деманіпулятора, що будуть слугувати в якості вихідних даних для їхнього проектування. Схема на рис.1 дозволяє здійснити конструювання названих пристроїв у вигляді конструктивних модулів, фізично відокремлених від штатного обладнання систем аналогового радіозв'язку.

Обробка сигналів в системах цифрового радіозв'язку (лінії VDL Mode 2,3 та 4) здійснюється за іншими технологічними схемами, які у даній роботі не розглядаються.

УДК 621.391

М.О. Безь, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЕКТУВАННЯ СТРУКТУРОВАНОЇ КАБЕЛЬНОЇ СИСТЕМИ РОЗУМНОГО ОФІСУ ЗА ДОПОМОГОЮ BIM-МОДЕЛЮВАННЯ

Стрімке зростання мережевого трафіку та перехід до кіберфізичних систем докорінно змінюють роль телекомунікаційної інфраструктури. Сьогодні структурована кабельна система (СКС) перетворюється з пасивного середовища на єдину платформу, що об'єднує інформаційні (IT) та операційні (OT) технології в "розумних будівлях".

Використання стандарту Power over Ethernet (IEEE 802.3bt) для передачі до 90 Вт потужності робить СКС не лише інформаційною, а й енергетичною магістраллю. Це, у свою чергу, вимагає ретельного проектування телекомунікаційних приміщень для ефективного охолодження та теплового менеджменту обладнання.

Через високий ризик просторових помилок традиційне 2D-проектування поступається BIM-моделюванню, де використовуються машинні правила (онтології) для автоматичної перевірки рішень. Водночас побудова сучасної СКС вимагає апаратного резервування (MC-LAG, Stacking) та VLAN-сегментації для кіберзахисту об'єднаних IT/OT середовищ. Відтак, розробка безпечної та відмовостійкої СКС на базі BIM-онтологій є актуальним науково-технічним завданням.

Інформаційне моделювання будівель (BIM) та онтології: Перехід від традиційних 2D-креслень до 3D-моделювання просторів. Застосування машинозчитуваних правил (онтологій) для автоматизованої перевірки телекомунікаційних кімнат на відповідність вимогам (кліренс, вогнестійкість, відсутність транзитних труб).

Конвергенція IT та OT середовищ: Об'єднання традиційних інформаційних мереж (IT) та операційних технологій (OT — системи освітлення, відеонагляду, HVAC, IoT) на єдиній фізичній інфраструктурі СКС.

Технологія Power over Ethernet (PoE): Використання мідного кабелю категорії 6A для забезпечення кінцевих пристроїв (Wi-Fi точок, IP-камер, датчиків) як каналом передачі даних, так і електроживленням високої потужності (до 90 Вт).

Механізми надійності та безпеки: Апаратне та логічне резервування (N+1): Використання стекування комутаторів (Stacking) для створення єдиного логічного пристрою та спільного використання резервних блоків живлення.

Агрегація ліній (MC-LAG/LACP) усуває єдині точки відмови (SPoF) та відкидає потребу блокування портів протоколом STP, тоді як мережева сегментація (VLAN) безпечно ізолює вразливі IoT-пристрої від корпоративних даних.

Контроль доступу: Використання апаратних брандмауерів (Firewalls), списків контролю доступу (ACL) та протоколу IEEE 802.1X для автентифікації пристроїв на рівні фізичних портів.

Економічна доцільність (CAPEX/OPEX): Впровадження архітектури "згорнутого ядра" та BIM-моделювання оптимізує капітальні витрати (CAPEX), виключаючи закупівлю зайвого обладнання та фізичні переробки. Водночас конвергенція IT/OT з живленням через PoE економить на прокладанні електромереж, а використання протоколів відмовостійкості (MC-LAG/Stacking) суттєво знижує операційні витрати (OPEX) і час простою бізнес-процесів.

Висновок: Розроблено проект відмовостійкої СКС для 3-поверхового офісу на базі архітектури «згорнутого ядра». Завдяки BIM-моделюванню з онтологіями усунуто просторові колізії ще до монтажу. Впровадження багатошасійної агрегації (MC-LAG) та VLAN-сегментації ліквідувало єдині точки відмови й надійно ізолювало IT-мережу від OT-пристроїв. Обладнання (кабель Cat 6A з підтримкою PoE до 90 Вт, оптика OM3/OM4) обрано за стандартами ISO/TIA/BICSI, а розрахунки втрат підтвердили дієздатність системи.

Отримані результати, розроблені структурні схеми та плани розміщення телекомунікаційного обладнання можуть бути безпосередньо використані підрядними організаціями та системними інтеграторами під час фізичного розгортання СКС на об'єктах комерційної нерухомості. Спроектована система має значний запас продуктивності, відповідає глобальним стандартам надійності та повністю готова до впровадження інноваційних інформаційнокомунікаційних сервісів.

УДК 621.396.2:004.7 (043.2)

Ілья БЕЛОКОНЬ, Олександр ЛАВРИНЕНКО
Державний університет «Київський авіаційний інститут», м. Київ

ОПТИМІЗАЦІЯ ПАРАМЕТРІВ БЕЗДРОТОВОЇ МЕРЕЖІ НА БАЗІ ТЕХНОЛОГІЇ MU-MIMO

Стрімка еволюція бездротових систем зв'язку за останні десятиліття кардинально трансформувала глобальну цифрову інфраструктуру. Експоненціальне зростання кількості користувачів супроводжується лавиноподібним збільшенням обсягів переданого мобільного трафіку, що створює безпрецедентне навантаження на телекомунікаційні мережі. У сучасних умовах повсюдного впровадження концепцій Інтернету речей (IoT) та хмарних сервісів виникає критична потреба у високошвидкісному та надійному обміні даними.

Традиційні (екстенсивні) підходи до підвищення пропускної здатності, такі як банальне розширення частотної смуги або нарощування випромінюваної потужності передавачів, практично вичерпали свій потенціал через жорстку обмеженість радіочастотного спектра та регуляторні бар'єри. Тому найбільш перспективним та ефективним шляхом інтенсивного розвитку мереж є перехід до просторової обробки сигналів за допомогою багатоантенних систем – технології MIMO (Multiple Input Multiple Output), а саме її розширеної багатокористувацької версії MU-MIMO.

Впровадження MU-MIMO дозволяє здійснювати гнучке просторове мультиплексування, динамічно розподіляючи надлишкові просторові потоки базової станції для паралельного обслуговування кількох абонентських терміналів на одній загальній несучій частоті. Це призводить до кратного підвищення спектральної та енергетичної ефективності радіоканалу без залучення додаткового частотного ресурсу.

У даній роботі проводиться комплексне дослідження та розробка аналітичної моделі для вибору оптимальної конфігурації параметрів бездротової обчислювальної мережі на основі технології MU-MIMO. Головною метою дослідження є знаходження чіткого балансу між економічною доцільністю (мінімізацією сукупних капітальних CAPEX та операційних OPEX витрат) і стовідсотковим забезпеченням гарантованої якості обслуговування (QoS) кінцевих абонентів навіть у години пікового навантаження.

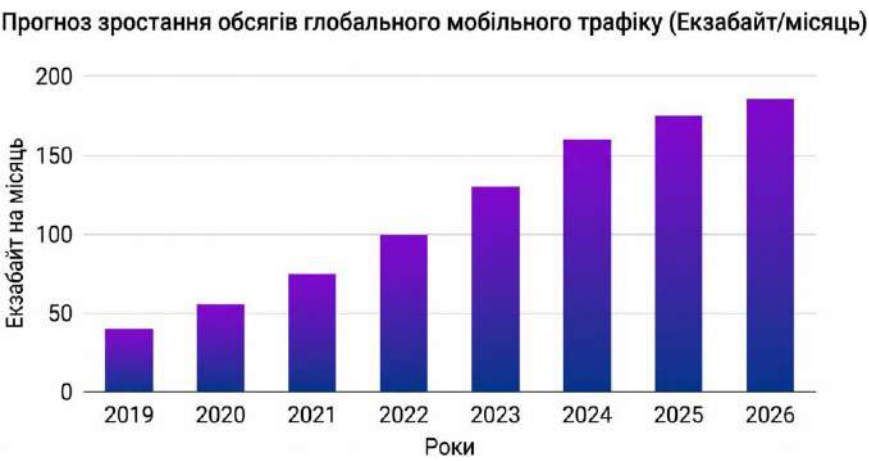


Рис. 1. Прогноз зростання обсягів глобального мобільного трафіку

Для вирішення завдання багатокритеріальної оптимізації інфраструктури в роботі застосовано метод системної декомпозиції, який розділяє складну задачу на три логічні підсистеми: модель оцінки пропускної здатності радіоканалів, просторовий розподіл точок доступу (з використанням алгоритмів багатовимірного кластерного аналізу) та комплексну оцінку економічних витрат.

Аналіз довів, що експлуатація застарілих стандартів (таких як 802.11n у діапазоні 2,4 ГГц) в умовах високої щільності абонентів є вкрай неефективною через критичний рівень міжканальної інтерференції (ACI). Раціональним кроком є використання обладнання сімейства IEEE 802.11ac/ax у діапазоні 5 ГГц. Цей діапазон характеризується значно меншою зашумленістю ефіру та наявністю ширшого спектрального ресурсу неперекриваючихся каналів, що дозволяє повноцінно задіяти механізми MU-MIMO та технологію об'єднання смуг (Channel Bonding).

Складний математичний апарат, розроблений у ході дослідження, дозволяє алгоритмічно компенсувати негативні ефекти багатопроменевого поширення радіохвиль (Multipath Propagation) і міжсимвольної інтерференції всередині закритих приміщень. Когерентне додавання сигналів та алгоритми просторово-часової обробки ефективно компенсують деструктивні замирання, підвищуючи сумарну стійкість каналу зв'язку до перешкод.

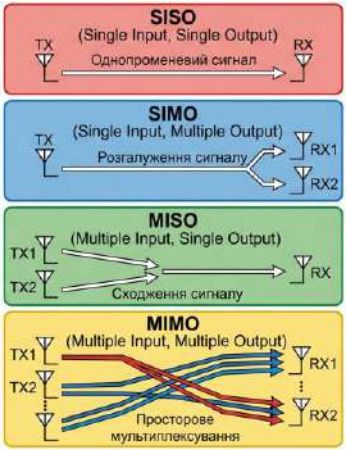


Рис. 2. Схеми базових конфігурацій приймально-передавальних антенних систем

Висновки. Впровадження багатоантенної технології MU-MIMO є безальтернативним та стратегічно обґрунтованим підходом до побудови високопродуктивних бездротових обчислювальних мереж наступних поколінь. Створена аналітична модель інтелектуального вибору параметрів надає інженерному складу готовий інструментарій для комплексного радіопланування, що гарантує ліквідацію надмірних витрат, оптимізацію розміщення точок доступу та надання абонентам максимально можливої якості обслуговування.

Список використаних джерел

1. Сайко В. Г., Шокало В. М. Сучасні системи бездротового зв’язку: технології та стандарти. Київ: КПІ ім. Ігоря Сікорського, 2022. 345 с.
2. Кравчук С. О. Оптимізація радіоресурсів у корпоративних мережах Wi-Fi 6 на базі технології MU-MIMO. Вісник телекомунікацій. 2021. № 4. С. 45–52.
3. Мельник А. О., Коваль В. В. Математичне моделювання та проектування бездротових мереж: підручник. Львів: Видавництво Львівської політехніки, 2023. 288 с.

УДК 004.056:656.07

О.В. Блонський, Г.Ф. Конахович
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ТРАНСПОРТНО-ЛОГІСТИЧНОГО ПІДПРИЄМСТВА

Сучасне транспортно-логістичне підприємство є складною організаційно-технічною системою, ефективність функціонування якої безпосередньо залежить від рівня впровадження та безперебійної роботи інформаційно-комунікаційних технологій. В умовах висококонкурентного ринку вантажних перевезень фізичний рух матеріальних активів нерозривно пов'язаний із безперервним циркулюванням супутніх інформаційних та фінансових потоків. Сучасна логістика спирається на системи управління транспортом (*TMS*), автоматизовані системи управління складами (*WMS*) та телематичні IoT-модулі, що формують єдину вразливу екосистему. Розгалужена організаційна архітектура, яка просторово розподілена між центральним офісом, регіональними філіями, диспетчерськими центрами та складськими терміналами, суттєво розширює поверхню потенційних кібератак. Інтенсифікація ризиків компрометації даних та загрози зупинки критичних сервісів диктують необхідність проєктування та впровадження науково обґрунтованої комплексної системи захисту інформації (*КСЗІ*), здатної забезпечити стійкість корпоративної інфраструктури.

У роботі проведено аналітичне обстеження об’єкта захисту, формалізацію ключових бізнес-процесів компанії та комплексне моделювання загроз. Запропоновано багаторівневу структуру КСЗІ, яка поєднує сучасні програмно-апаратні засоби та чіткі організаційні регламенти. Окрему увагу в межах проєкту приділено нейтралізації людського фактора, який є критичним вектором уразливості для логістичного документообігу. Для мінімізації соціотехнічних ризиків розроблено спеціалізовану програму підвищення обізнаності персоналу (Security Awareness), адаптовану до розпізнавання цілеспрямованого фішингу та маніпулятивних методів соціальної інженерії. Оскільки логістичний бізнес критично залежить від мобільного персоналу, архітектуру КСЗІ доповнено системами класу *MDM* (Mobile Device Management) для жорсткого контролю та шифрування терміналів збору даних (*ТЗД*) і

планшетів експедиторів. З метою безпечного об'єднання віддалених складів розгорнуто корпоративну мережу *SD-WAN* (Software-Defined Wide Area Network) із застосуванням криптографічно стійких VPN-тунелів. Технічний контур системи орієнтований на жорстке розмежування прав доступу та забезпечення безперервного контролю логічних потоків.

Операційну спроможність спроєктованого захисного контуру підтверджено радикальним покращенням часових метрик інцидент-менеджменту завдяки впровадженню сучасних аналітичних інструментів. У межах практичної реалізації розгорнуто централізовану SIEM-систему на базі відкритого стека ELK/Wazuh, що здійснює збір та кореляцію шифрованих логів за протоколом SNMPv3 в режимі реального часу. Для класифікації загроз, налаштування правил детектування (*Rulesets*) та моделювання поведінки зловмисників використано міжнародну матрицю тактик і технік кіберзагроз MITRE ATT&CK. Експериментальна валідація інфраструктури безпеки під час моделювання деструктивних впливів продемонструвала зниження середнього часу виявлення аномалій (*MTTD*) до 120–180 секунд, а часу локалізації та усунення зафіксованих загроз (*MTTR*) – до 5–7 хвилин, що гарантує виконання жорстких вимог угод про рівень надання послуг (*SLA*).

Валідацію та підсумковий перерахунок ризиків після впровадження засобів захисту виконано шляхом побудови порівняльних гістограм у середовищі MATLAB на основі ймовірнісної методології *FAIR* (Factor Analysis of Information Risk), що підтвердило повну ліквідацію критичних зон небезпеки. Сумарний показник очікуваних річних втрат (ALE_{after}) знизився до прийнятного контрольованого значення у 305 000 грн. Функціонально-вартісний аналіз за індексом ROSI продемонстрував високу фінансову ефективність на рівні 326%, підтвердивши, що капітальні та операційні витрати на реалізацію проєкту в розмірі 750 000 грн повністю окупаються протягом перших чотирьох місяців експлуатації системи. Окрім прямої фінансової вигоди, впроваджена КСЗІ мінімізує репутаційні ризики та гарантує повну відповідність процесів обробки клієнтських баз даних (адрес, контактів, паспортних даних вантажоодержувачів) вимогам Закону України «Про захист персональних даних» та європейського регламенту GDPR. Розроблена архітектура є готовим еталоном для модернізації систем інформаційної безпеки у транспортному секторі України.

УДК 004.932

О.А. Бондаренко,
М.М. Малоєд
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОДИ ПРОСТОРОВОЇ ОБРОБКИ ЗОБРАЖЕНЬ В MATLAB

Базовим методом цифрового кодування джерел зображень є імпульсно-кодова модуляція (ІКМ). Вона характеризується тим, що кожному закодованому в цифрову форму слову відповідає квантований в часі і за амплітудою відлік відеоінформації. При цьому повинні виконуватись вимоги теореми дискретизації $f_д > 2W_0$, де W_0 максимальна частота, яка міститься в сигналі. Щоб запобігти появі фальшивих контурів на однокольоровому зображенні необхідно більше 50 рівнів квантування, що відповідає 6-8 розрядному кодовому слову на кожний елемент (піксель) зображення. Через великі об'єми інформації ІКМ застосовується лише при внутрістудійній передачі телевізійних зображень паралельним кодом і в якості базового канонічного подання зображення у цифровій формі [1,2].

Методи кодування зображень з передбаченнями дозволяють стиснути зображення в 2-2,5 рази при простій технічній реалізації. Серед недоліків цих методів необхідно відзначити такі: похибки в місцях різких перепадів яскравості; низька завадостійкість. Інтерполяційні методи основані на числових методах апроксимації, за допомогою яких послідовність або двовимірний масив відліків яскравості наближено подаються через неперервні функції [3]. При цьому кодуються лише окремі відліки зображення, а сусідні з ними отримують в результаті інтерполяції поліномами, звичайно, не більше чим третього степеня. Основним недоліком інтерполяційних методів є великий об'єм обчислень при інтерполяції поліномами високих степенів, а також необхідність зберігання координат базових відліків зображення. Важливий клас методів кодування зображень - це методи кодування на основі перетворень.

Просторова обробка зображень — це сукупність методів, що передбачають безпосередню модифікацію значень пікселів у їх геометричному розташуванні. На відміну від частотних методів, які працюють у спектральній області (наприклад, у просторі Фур’є),

просторові методи оперують зображенням у його первинному вигляді. Це забезпечує інтуїтивність, простоту реалізації та можливість локального впливу на окремі ділянки кадру.

Основними задачами просторової обробки є покращення якості зображення, підсилення контрасту, виділення контурів, зменшення шумів, сегментація та підготовка даних для подальшого аналізу в системах комп'ютерного зору.

Точкові (інтенсивнісні) перетворення змінюють яскравість кожного пікселя незалежно від його оточення. Вони є базовими інструментами попередньої обробки. Нелінійні перетворення: логарифмічні, степеневі (гамма-корекція), експоненційні.

Точкові методи застосовуються для нормалізації освітлення, підсилення слабких сигналів та підготовки зображення до сегментації.

Гістограма відображає розподіл яскравостей у зображенні. Методи, що базуються на її аналізі, дозволяють автоматично покращувати контраст. Основні підходи: вирівнювання гістограми (Histogram Equalization, HE) — перетворення, що робить розподіл яскравостей рівномірнішим; адаптивне вирівнювання (CLAHE) — локальне покращення контрасту без надмірного підсилення шумів; гістограмне вирівнювання з обмеженням контрасту — компроміс між глобальним і локальним підходами. Ці методи широко застосовуються у медичній візуалізації, дистанційному зондуванні та відеоспостереженні.

Локальні фільтри використовують інформацію про сусідні пікселі, що дозволяє згладжувати шум або підсилювати деталі. Тут можна виділити наступні види фільтрації. Середнє згладжування зменшує випадковий шум, але розмиває контури. Гаусове згладжування оптимальне для придушення шуму при мінімальному спотворенні структури. Фільтр Вінера адаптивний фільтр, що враховує локальні статистичні властивості.

Список літератури

1. Поспєлов Д. А. Методи комп'ютерної обробки зображень. — К.: Наукова думка, 2018. — 284 с.

2. Russ J. C. The Image Processing Handbook. — 7th ed. — CRC Press, 2016. — 1052 p.

3. Боровицький В. М. Методи цифрової обробки зображень: Навчальний посібник. Харків: ХНУРЕ. – 2021. – 124 с.

УДК 621.396.6

Є.І. Габрусенко, А.Г. Тараненко, О.Ю. Лавриненко
Державний університет
«Київський авіаційний інститут», м. Київ

МОДЕЛЮВАННЯ ЯВИЩА БЛОКУВАННЯ РАДІОПРИЙМАЛЬНОГО ПРИСТРОЮ

Блокування радіоприймального пристрою (РПП) – це явище зменшення коефіцієнту підсилення вхідного каскаду (ВК) внаслідок дії в антені радіозавади, амплітуда якої значно перевищує амплітуду сигналу. Воно проявляється в зменшенні амплітуди корисного сигналу на виході РПП, а в разі переведення ВК в режим насичення амплітуда сигналу дорівнює нулю. Результатом явища блокування є втрата прийому радіосигналу, що може використовуватися в задачах радіоелектронної боротьби.

Розглянемо ситуацію, коли антена РПП перебуває під одночасним впливом слабкого сигналу $U_{\text{с}}$ та радіозавадою, амплітуда якої $U_{\text{З}}$ значно перевищує сигнал. Ця адитивна суміш подається з виходу антени до входу антенного підсилювача РПП.

Коефіцієнт підсилення K вхідного каскаду антенного підсилювача залежить від крутизни S в робочій точці його нелінійної вольт-амперної характеристики (ВАХ). Положення робочої точки задається значенням постійної напруги зміщення та залежить від амплітуди $U_{\text{З}}$. З урахуванням зазначених обставин коефіцієнт підсилення вхідного каскаду визначається співвідношенням

$$K = S \cdot R_{\text{н}} \qquad (1)$$

де $R_{\text{н}}$ – опір навантаження каскаду.

За умови $U_{\text{С}} << U_{\text{З}}$ середня крутизна S_{Σ} в робочої точці ВАХ зменшується, що спричиняє відповідне зменшення коефіцієнту підсилення (1) [1, 2]. Такий ефект можна представити як процес зміщення робочої точки ВАХ на її пологу частину, який відбувається під впливом сильної завади. При цьому виникає ефект блокування РПП сильною завадою, що призводить до зменшення результуючого коефіцієнта підсилення $K_{\Sigma} << K$. Ефект блокування оцінюється відповідним коефіцієнтом за формулою [1, 3]

$$K_{\text{бл}} = \frac{U_{\text{с вих}} - U_{\Sigma\text{вих}}}{U_{\text{с вих}}}. \qquad (2)$$

За умови відсутності завади середня крутизна ВАХ визначається як $S_\Sigma = S$, тоді коефіцієнт блокування $K_{\text{бл}} = 0$, тобто РПП не блокується. За наявності сильної завади робоча точка виводиться на пологу частину ВАХ, у якій середня крутизна S_Σ та коефіцієнт підсилення K зменшуються до 0, що призводить до втрати вхідним каскадом РПП підсилювальних властивостей.

Моделювання явища блокування доцільно проводити у програмному середовищі System View, робоче вікно якого з моделлю двохсигнальної дії на вхід РПП показано на рис. 1. Модель складається з генератора несучої частоти (0), генератора звукової частоти (1), генератора радіозавади (5). Сигнал з генераторів (0) та (1) подається на суматор (2). Адитивна суміш двох високочастотних сигналів з виходу суматора надходить на нелінійний елемент (3). На виході нелінійного елемента (3) виникає радіосигнал з амплітудною модуляцією (АМ).

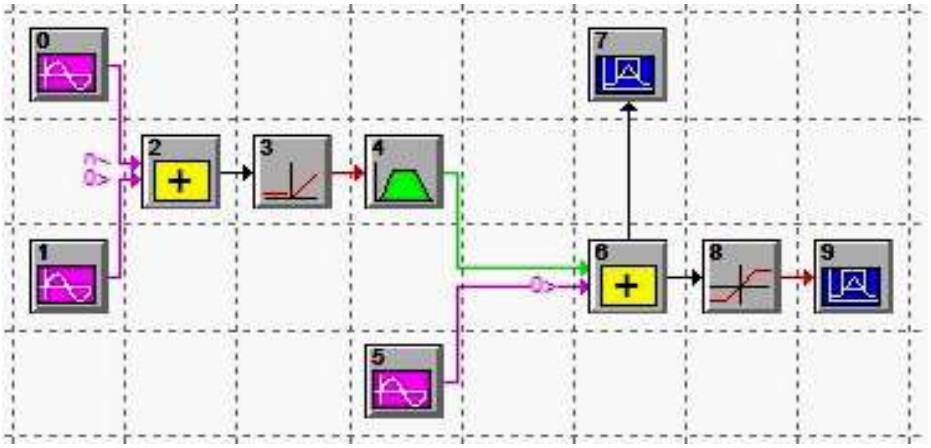
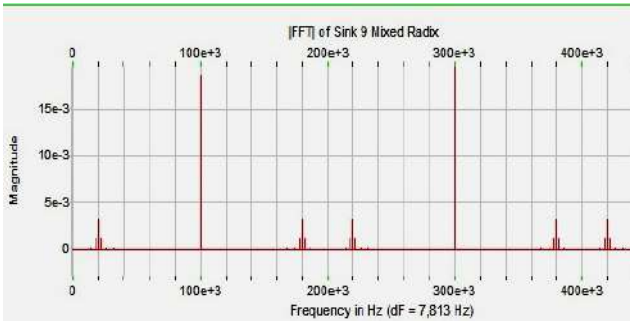


Рис. 1. Модель двохсигнальної дії на вході РПП
у середовищі System View.

Отриманий сигнал подається на вхід смугового фільтра (Band-pass) (4), в якому АМ-сигнал відфільтровується від небажаних спектральних складових. Сформований таким чином АМ-сигнал діє на антену радіоприймального пристрою одночасно з немодульованою сильною завадою, яка імітується за допомогою генератора (5). Антена імітується суматором (6), з виходу якого адитивна суміш слабкого

АМ-сигналу і сильної завади надходить на вхід нелінійного антенного підсилювача РПП, який імітується динамічною ланкою Limiter (8). Динамічні ланки (7) і (9) є аналізаторами сигналів на вході і виході нелінійного підсилювача (8) відповідно. На рис. 2 показано осцилограма (2а) та спектрограма (2б) на виході РПП, яку відображає аналізатор (9).

а)



б)

Рис. 2. Покази аналізатора вихідного сигналу моделі РПП.

В процесі моделювання явища блокування РПП здійснюється аналіз залежності коефіцієнта блокування $K_{бл}$ (2) від амплітуди радіозавади $U_З$ та її частоти, яка регулюється у вікні налаштування генератора (5). Покази аналізатора свідчать про зменшення рівня вихідного сигналу РПП та розширення його спектра при збільшенні амплітуди радіозавади.

Список джерел

1. В.М. Раєвський, В.О. Хмарюк. Передавальні і приймальні пристрої: Збірник термінів та визначень. К.: ВІТІ, 2026, 75 с.

2. A.G.Taranenko, Ye.I. Gabrusenko, A.G. Holubnychyi, O.Yu. Lavrynenko. Operational reliability management of the reserved electronic system/ Electronics and control systems No.1(63), 2021, pp. 86-92.

3. Unmanned aviation complexes: monogr. / V.G. Bashynskyi, V.B. Bzot, E.I. Zhilin et al. – Zaporizhzhia, 2019. – 211 p.

УДК 621.391

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

Інформаційні технології на основі штучного інтелекту в системах експлуатації засобів РТЗ

Сучасна цивільна авіація потребує надійного та безпечного функціонування наземних засобів радіотехнічного забезпечення польотів, які є важливою складовою систем зв'язку, навігації та спостереження — CNS. Вони забезпечують інформаційну підтримку польотів, аеронавігаційне обслуговування, контроль повітряної обстановки та підвищення рівня безпеки польотів. Тому вдосконалення систем експлуатації засобів РТЗ/CNS є актуальним завданням, оскільки від їх технічного стану залежить стабільність роботи авіаційної інфраструктури.

Система експлуатації наземних засобів РТЗ/CNS є складною організаційно-технічною системою, що охоплює технічні засоби, персонал, нормативну документацію, технологічні процеси, інформаційні ресурси, засоби контролю та матеріально-технічне забезпечення. Традиційні підходи до експлуатації базуються на планово-попереджувальному обслуговуванні, регламентних роботах і періодичних перевірках. Однак збільшення обсягів експлуатаційних даних і складності технічних систем потребує впровадження сучасних інформаційних технологій.

Перспективним напрямом є застосування статистичної обробки даних і методів штучного інтелекту для моніторингу технічного стану засобів РТЗ/CNS. Джерелами даних можуть бути журнали технічного обслуговування, результати наземних і льотних перевірок, параметри роботи обладнання, повідомлення про відмови, дані діагностичних систем, інформація від ремонтних центрів, виробників та експлуатаційних підрозділів. Об'єднання цих даних у єдиному інформаційному середовищі дає змогу точніше оцінювати стан обладнання та прогнозувати його працездатність.

Використання алгоритмів штучного інтелекту дозволяє перейти від реактивної моделі експлуатації до прогнозної. У такій моделі система не лише фіксує несправність, а й аналізує зміну параметрів, виявляє ознаки погіршення технічного стану, прогнозує ймовірність відмови та формує рекомендації для персоналу. Це сприяє зменшенню

простоїв обладнання, оптимізації витрат на технічне обслуговування та підвищенню ефективності функціонування систем РТЗ/CNS.

Запропонований підхід передбачає поетапне збирання, структурування, перевірку, статистичну обробку та інтелектуальний аналіз експлуатаційних даних. Спочатку формується база даних про технічний стан засобів РТЗ/CNS, далі здійснюється очищення та нормалізація інформації, після чого визначаються показники надійності, частота відмов і закономірності зміни параметрів. На завершальному етапі застосовуються алгоритми штучного інтелекту для прогнозування ризиків і підтримки прийняття рішень.

Практичне значення такого підходу полягає у можливості його використання під час модернізації систем експлуатації наземних засобів РТЗ/CNS цивільної авіації. Він може бути корисним для інженерно-технічного персоналу, експлуатаційних підрозділів, органів державного регулювання, навчальних закладів, ремонтних центрів і підприємств, що обслуговують радіотехнічне обладнання. Крім того, застосування такого підходу сприятиме підвищенню оперативності прийняття рішень, зменшенню ризику раптових відмов та більш раціональному плануванню технічного обслуговування. Це дозволить ефективніше використовувати наявні ресурси, своєчасно визначати проблемні елементи системи та підтримувати необхідний рівень готовності засобів РТЗ/CNS до виконання функціональних завдань.

Отже, впровадження інформаційних технологій, статистичної обробки даних і штучного інтелекту в системи експлуатації засобів РТЗ/CNS є важливим напрямом підвищення надійності та ефективності цивільної авіації. Такий підхід забезпечує якісніший контроль технічного стану, своєчасне виявлення несправностей, прогнозування відмов і прийняття обґрунтованих управлінських рішень. У перспективі це створює передумови для формування більш сучасної, цифровізованої та гнучкої системи експлуатації, здатної швидко реагувати на зміни технічного стану обладнання та потреби авіаційної інфраструктури.

УДК 004.056:34.09

Е.Х. Глушак, С.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОДИКА ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ КОРПОРАТИВНОЇ МЕРЕЖІ КЛАСУ АС-2

Сучасні корпоративні мережі являють собою складне, територіально розподілене гетерогенне середовище, що об'єднує різноманітні апаратні платформи, операційні системи та прикладне програмне забезпечення. Інтеграція технологій Intranet та Extranet на базі стека протоколів TCP/IP створює єдиний інформаційний простір для авторизованих суб'єктів, однак водночас критично розширює поверхню потенційних кібератак. В умовах багатокористувацької взаємодії забезпечення конфіденційності, цілісності, доступності та спостереженості даних є не лише питанням технічної надійності, а й суворою нормативною вимогою. Побудова комплексної системи захисту інформації (КСЗІ) для автоматизованих систем класу АС-2 відповідно до національних стандартів технічного захисту інформації (НД ТЗІ) є безальтернативним кроком для безпечного функціонування сучасного підприємства. Особливої актуальності набуває задача інтеграції віддалених працівників та філій у єдиний захищений контур із використанням криптографічних протоколів, сертифікованих згідно з національними стандартами.

У роботі здійснено системне проєктування та обґрунтування багаторівневої архітектури КСЗІ, яка повністю задовольняє вимогам керівного документа НД ТЗІ 2.5-004-99 щодо реалізації стандартного функціонального профілю захищеності за підкласом «2.КЦД». Згідно з нормативними вимогами, ядром системи розмежування прав стало поєднання механізмів дискреційного та мандатного керування доступом до інформаційних активів на рівні файлової системи. Основою логічної безпеки стало впровадження жорстких правил мікросегментації та маршрутизації між ізольованими віртуальними мережами (VLAN). Для забезпечення комплексного контролю доступу здійснено глибоку інтеграцію міжмережевих екранів наступного покоління (NGFW) з доменною інфраструктурою Active Directory. Для забезпечення нормативної вимоги щодо безперервності (доступності) інфор-

мації ядро мережі та периметральний кластер NGFW спроєктовано за схемою апаратного резервування High Availability (Active/Passive), що гарантує миттєве перемикання трафіку в разі технічних збоїв. Захист магістральних каналів зв'язку реалізовано шляхом розгортання IPsec VPN-тунелів із застосуванням стійких вітчизняних алгоритмів симетричного шифрування (відповідно до ДСТУ 7624:2014 «Калина»). Особливу увагу приділено підсистемі антивірусного захисту та контролю зовнішніх носіїв (Device Control), що унеможливлює несанкціоноване копіювання комерційної таємниці на USB-накопичувачі, закриваючи тим самим один із найпоширеніших векторів інсайдерських загроз. Окрім цього, розроблена архітектура посилена підсистемами глибокого аудиту (SIEM) для проактивного виявлення інцидентів та системами запобігання витокам даних (DLP) для аналізу корпоративного контенту.

Валідацію та експериментальне підтвердження ефективності прийнятих рішень проведено шляхом розгортання повнофункціональної моделі КСЗІ на базі віртуального тестового стенда в середовищі емуляції мережевої інфраструктури EVE-NG. У процесі тестування за допомогою інструментарію дистрибутива Kali Linux було зімітовано широкий спектр деструктивних впливів, включаючи спроби внутрішніх несанкціонованих порушень, активне сканування на вразливості та генерацію зовнішніх атак на відмову в обслуговуванні (DoS). Результати випробувань інструментально довели, що розроблений комплекс засобів захисту миттєво ідентифікує та блокує шкідливий трафік, зберігаючи при цьому заданий рівень продуктивності для легітимних бізнес-сервісів.

Проведений техніко-економічний аналіз підтвердив доцільність та рентабельність обраної стратегії. Спроєктована КСЗІ гарантує виконання нормативних вимог до систем класу АС-2 без будь-яких функціональних обмежень. Успішне проходження програми та методики попередніх випробувань підтверджує готовність розробленої системи до проведення державної експертизи у сфері ТЗІ. Це забезпечує надійний, легітимний та масштабований фундамент інформаційної безпеки корпоративної інфраструктури.

УДК 004.8:621.391

І.О. Горбачов[1], О.М. Литвинюк[1], В.О. Гнатюк[1,2]
[1]Державний університет
«Київський авіаційний інститут», м. Київ
[2]Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації, м. Київ

МЕТОД САМОНАВЧАЛЬНОГО УПРАВЛІННЯ РЕСУРСАМИ НА ОСНОВІ REINFORCEMENT LEARNING У ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

Розвиток сучасних телекомунікаційних систем, зокрема мереж 5G/6G, інтернету речей, віртуалізованих мережевих функцій та програмно-керованих мереж, супроводжується істотним зростанням динамічності трафіку, неоднорідності сервісів і вимог до QoS. У таких умовах ефективне управління мережевими ресурсами стає складною багатокритеріальною задачею, що потребує оперативного прийняття рішень за умов невизначеності, змінних навантажень і обмежених ресурсів. Традиційні методи управління ресурсами, засновані на статичних правилах, евристичних алгоритмах або класичних оптимізаційних підходах, демонструють обмежену ефективність у динамічних середовищах. Вони, як правило, не враховують складну взаємодію між параметрами мережі, не адаптуються до нових сценаріїв функціонування та не забезпечують автономного прийняття рішень у режимі реального часу. Використання методів прогнозування навантаження дозволяє покращити планування ресурсів, однак саме по собі прогнозування не забезпечує адаптивного механізму управління, здатного навчатися на основі досвіду експлуатації мережі.

Методи штучного інтелекту, зокрема Reinforcement Learning, відкривають можливості для побудови самонавчальних систем управління, які здатні формувати оптимальні стратегії розподілу ресурсів шляхом взаємодії із середовищем. Попри наявність досліджень у цій сфері, більшість існуючих рішень мають обмежену придатність до практичного застосування в телекомунікаційних системах через недостатнє врахування багатокритеріальних показників якості обслуговування, енергоефективності, масштабованості мереж та необхідності стабільної роботи в умовах високої мінливості трафіку. Таким чином, актуальною науково-прикладною проблемою є розробка методу самонавчального управління ресурсами телекомунікаційних систем на основі

навчання з підкріпленням, який забезпечує адаптивне прийняття рішень у реальному часі з урахуванням багатокритеріальних вимог до якості функціонування мережі, ефективності використання ресурсів та стабільності роботи інфокомунікаційної інфраструктури.

У роботі розроблено метод самонавчального управління ресурсами телекомунікаційних систем на основі навчання з підкріпленням, який забезпечує адаптивне прийняття управлінських рішень з урахуванням поточного та прогнозованого стану мережі. Запропонована архітектура включає модулі збору телеметрії, прогнозування навантаження, прийняття рішень, формування винагороди, управління мережею та контролю безпеки, що забезпечує замкнений цикл автономного управління. Розроблено математичну модель алгоритму, проведено аналіз його збіжності та обчислювальної складності, що підтверджує можливість застосування методу у системах реального часу. Запропонований підхід відрізняється інтеграцією прогнозування з алгоритмами навчання з підкріпленням, використанням багатокритеріальної функції винагороди та впровадженням механізмів безпечного управління.

Експериментальні дослідження показали, що використання запропонованого методу дозволяє суттєво зменшити затримку передачі даних, втрати пакетів та кількість порушень SLA, а також підвищити ефективність використання ресурсів і знизити енергоспоживання мережевої інфраструктури. Отримані результати підтверджують доцільність застосування методів навчання з підкріпленням для автоматизації управління ресурсами в сучасних телекомунікаційних системах.

Практичне значення роботи полягає у можливості інтеграції запропонованого методу в системи управління SDN/NFV-мережами, мережами 5G/6G та інфраструктурами інтернету речей, де спостерігається висока динамічність навантаження та необхідність автономного управління ресурсами.

До перспектив подальших досліджень належать: розширення методу на багаторівневі архітектури управління в ієрархічних телекомунікаційних системах; дослідження multi-agent підходів для розподіленого управління ресурсами; інтеграція федеративного навчання для збереження конфіденційності даних; адаптація алгоритму для ultra-reliable low-latency сценаріїв; експериментальна перевірка методу у реальних або напівреальних мережевих середовищах; оптимізація алгоритмів для edge-обчислень і енергообмежених пристроїв.

УДК 621.39:004.7 (043.2)

Дар'я ГРИБЕНИК, Олександр ЛАВРИНЕНКО, Віталій ТЕЛЬНИХ
Державний університет «Київський авіаційний інститут», м. Київ

МУЛЬТИСЕРВІСНА КОРПОРАТИВНА МЕРЕЖА ЗВ'ЯЗКУ НА БАЗІ ОБЛАДНАННЯ З КОМУТАЦІЄЮ ПАКЕТІВ

В умовах глобальної цифровізації та модернізації бізнес-процесів спостерігається стійка тенденція переходу підприємств від традиційних моносервісних телекомунікаційних архітектур до конвергентних мультисервісних корпоративних мереж (МКМ). Сьогодні ключовою парадигмою виступає концепція уніфікованих комунікацій (Unified Communications), яка дозволяє об'єднати передачу мультимедійного трафіку, транзит даних, послуги IP-телефонії (VoIP) та сучасних систем відеоконференцзв'язку (ВКЗ) у рамках єдиної надійної мережевої інфраструктури.

Метою даної роботи є дослідження принципів функціонування та проєктування мультисервісної корпоративної мережі на базі технологій пакетної комутації. Така мережа має забезпечувати безшовну інтеграцію традиційної аналогової телефонії, сучасних SIP-терміналів та високошвидкісних локальних обчислювальних мереж (ЛОМ) підприємства із гарантованою якістю обслуговування (QoS).

Для досягнення поставленої мети було розроблено та обґрунтовано еталонну трирівневу ієрархічну модель інфраструктури, яка строго декомпонується на рівень ядра (Core Layer), рівень розподілу (Distribution Layer) та рівень доступу (Access Layer). Рівень ядра виконує функцію високошвидкісної магістралі, агрегуючи потоки даних з найвищою пропускною здатністю. Рівень розподілу виступає інтелектуальною проміжною ланкою, здійснюючи міжмережеву маршрутизацію (зокрема між віртуальними мережами VLAN) та фільтрацію трафіку. Рівень доступу є периферійною межею інфраструктури, де відбувається фізична та логічна інтеграція різнорідних користувацьких пристроїв у загальний цифровий простір. Така архітектурна модель мінімізує затримки пакетів та забезпечує високу апаратну відмовостійкість усієї системи за рахунок резервування.

З метою оптимізації транспортного ресурсу магістралі було проведено глибокий математичний аналіз та моделювання інтенсивності телетрафіку. Розрахунок спирався на використання першої формули Ерланга для визначення необхідної пропускної здатності. Враховуючи

гетерогенну структуру мережі, яка об'єднує центральний офіс та три філії з різнорідною абонентською базою (понад 390 підключень), розрахунок ємнісних параметрів здійснювався з урахуванням специфікацій різних кодеків стиснення голосу. Для комунікації між філіями застосовано висококомпресійний стандарт G.723, що дозволило суттєво зекономити ємність з'єднувальних ліній, тоді як для транкових виходів у телефонну мережу загального користування (ТМЗК) обрано стандарти G.711 та G.726.

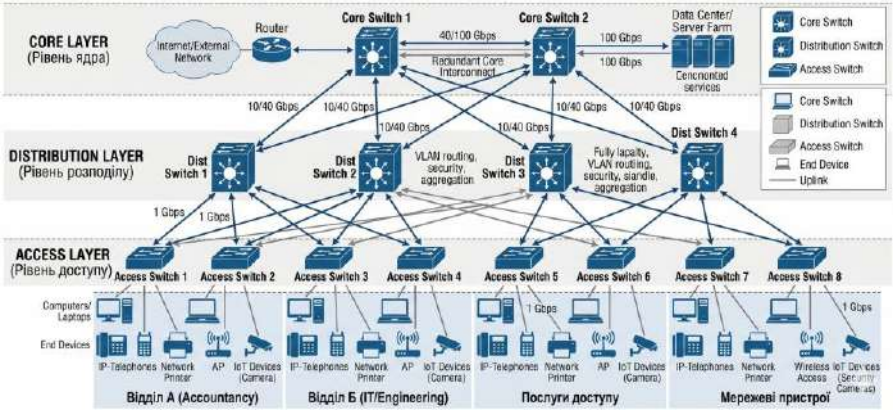


Рис. 1. Еталонна трирівнева ієрархічна модель ЛОМ підприємства

Фундаментом архітектури корпоративного зв'язку було обрано парадигму мереж наступного покоління (NGN) з імплементацією архітектури IP Multimedia Subsystem (IMS). У центральному офісі спроєктовано розгортання інтелектуального ядра управління — гнучкого програмного комутатора (Softswitch) та сервера голосової пошти, які у синергії з мультисервісними вузлами доступу (MSAN) в регіональних підрозділах гарантують централізоване управління викликами на основі протоколу SIP.

Окрему увагу в дослідженні приділено інтеграції сучасних підсистем відеоконференцзв'язку (ВКЗ), що виступає логістично ефективною альтернативою очним нарадам. Завдяки впровадженню технологій гарантованої якості обслуговування (QoS) та раціональному використанню протоколів маршрутизації стану каналів зв'язку (наприклад, OSPF), ізохронний відео- та аудіотрафік передається з мінімальними затримками (latency) та джиттером (jitter) незалежно від фонового інформаційного навантаження локальної мережі.

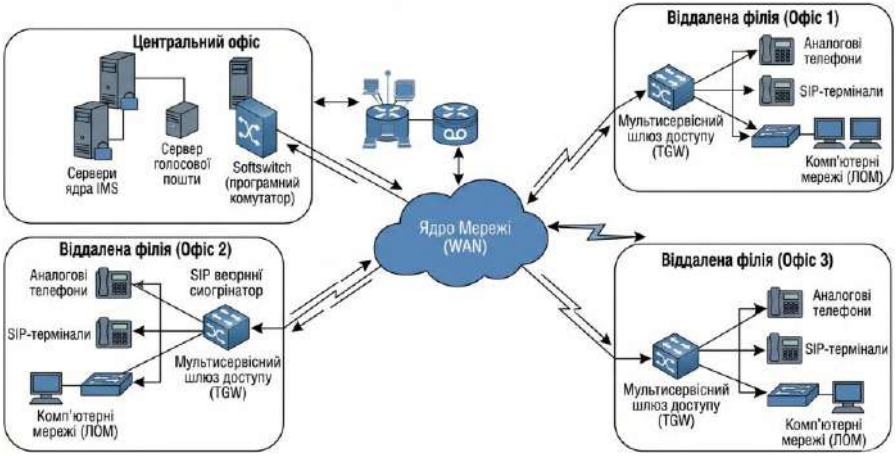


Рис. 2. Структурна схема розробленої мультисервісної корпоративної мережі

Висновки. Запропонована комплексна архітектурна модель корпоративної мережі на базі сучасного обладнання з комутацією пакетів є готовим масштабованим інженерним рішенням. Синтез трирівневої обчислювальної топології, впровадження інтелектуального ядра на базі IMS/Softswitch та математично обґрунтований розрахунок канальних ємностей дозволяють усунути «вузькі місця» інфраструктури. Такий підхід створює єдиний, надійний та захищений комунікаційний простір для організації безперервних бізнес-процесів компанії.

Список використаних джерел

1. Thomas C. Integrating Legacy Analog Telephony with SIP Infrastructure. Journal of Telecommunication Engineering. 2022. Vol. 14, No. 2. P. 45–53.
2. Jackson F. High-Definition Videoconferencing: Bandwidth Requirements and Resource Allocation. Multimedia Systems Journal. 2023. Vol. 29, No. 4. P. 501–515.
3. White B. Power over Ethernet (PoE) in Enterprise Switching: Standards IEEE 802.3af/at. Network Engineering Review. 2021. Vol. 10, No. 1. P. 22–30.
4. Harris G., Lewis P. Core Layer Architecture for Distributed Enterprise Networks. International Journal of Computer Networks. 2023. Vol. 15, No. 2. P. 110–125.

УДК 004.056 (043.2)

Максим ДАНИЛОВСЬКИЙ, Олександр ЛАВРИНЕНКО
Державний університет «Київський авіаційний інститут», м. Київ

МОДЕЛЬ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ВІД ЗОВНІШНІХ ЗАГРОЗ

В сучасному світі стрімкий розвиток інформаційно-комунікаційних технологій та глобальна цифровізація бізнес-процесів зумовлюють постійне зростання цінності корпоративних даних, що перетворює їх на першочергову ціль для зловмисників. В умовах сучасного ландшафту кіберзагроз, який характеризується високим рівнем автоматизації, використанням алгоритмів штучного інтелекту та поширенням цілеспрямованих атак (APT) і програм-вимагачів за моделлю подвійного шантажу (Ransomware-as-a-Service), класичні концепції захисту периметра мережі (модель «замок і рів») остаточно втратили свою ефективність. Для високотехнологічних підприємств (зокрема таких, що оперують критичною інтелектуальною власністю та об'ємними CAD/CAM-моделями), втрата конфіденційності, цілісності або доступності інформації призводить до катастрофічних фінансових та репутаційних наслідків.

Проведений аудит типової телекомунікаційної інфраструктури (на прикладі ЛОМ ТОВ «АероІнжиніринг») показав, що використання традиційних міжмережевих екранів, здатних виконувати лише базову фільтрацію пакетів (Stateful Inspection) на рівнях L3/L4 моделі OSI, залишає мережу відкритою до атак на рівні додатків (L7). Окрім того, відсутність мікросегментації, використання застарілих операційних систем та класичних сигнатурних антивірусів створюють сприятливі умови для несанкціонованого горизонтального переміщення (Lateral Movement) зловмисника всередині мережі.

З метою мінімізації виявлених ризиків у даній роботі запропоновано комплексну, відмовостійку та економічно обґрунтовану модель захисту корпоративної мережі, що базується на парадигмі «Нульової довіри» (Zero Trust Architecture – ZTA). Фундаментальний принцип ZTA передбачає безперервну верифікацію кожного користувача, пристрою та інформаційного потоку незалежно від їх фізичного чи логічного розташування. Жоден мережевий сеанс не отримує довіри за замовчуванням.

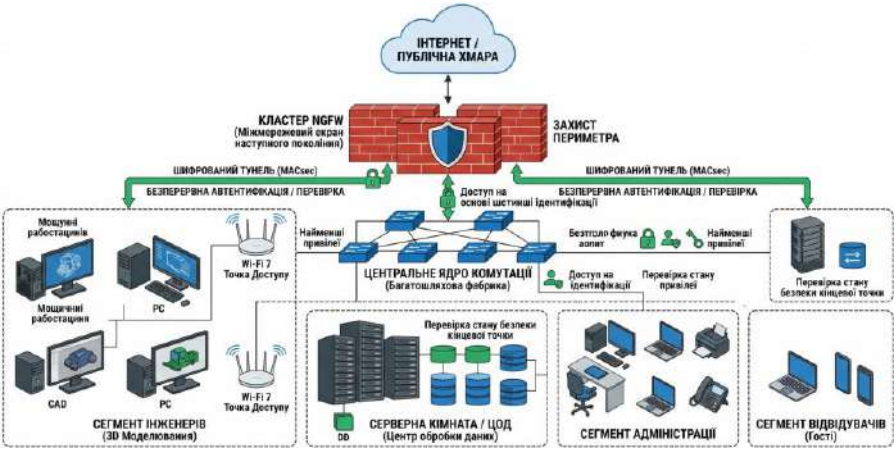


Рис. 1. Логічна схема корпоративної мережі, що демонструє архітектуру «Нульової довіри» (Zero Trust)

Технічною основою реалізації даної моделі виступає кластер міжмережевих екранів наступного покоління (NGFW), який виконує глибоку інспекцію пакетів (DPI) та дешифрування зашифрованого SSL/TLS-трафіку (включаючи стандарт TLS 1.3) у режимі реального часу. На рівні локальної маршрутизації застосовується математично обґрунтована мікросегментація із використанням апаратного шифрування магістральних каналів за протоколом MACsec (IEEE 802.1AE), що унеможливлює перехоплення даних (sniffing) усередині фізичного периметра.

Для забезпечення захищеної мобільності інженерного персоналу та підключення спеціалізованих діагностичних комплексів, бездротовий сегмент мережі модернізується до стандарту Wi-Fi 7 (IEEE 802.11be). Застосування технології багатокористувацького просторового мультиплексування (MU-MIMO) у поєднанні з криптографічним протоколом WPA3-Enterprise та суворою RADIUS-автентифікацією гарантує найвищий рівень захисту радіоефіру від зовнішніх втручань.

Крім апаратного рівня, розроблена модель передбачає впровадження платформи розширеного виявлення та реагування на інциденти (XDR). За рахунок консолідації телеметрії з EDR-агентів на кінцевих вузлах та NDR-сенсорів у мережі, система дозволяє в автоматичному режимі виявляти аномалії поведінки та миттєво блокувати при-

ховані загрози за допомогою методів машинного навчання, перевершуючи можливості класичних IDS/IPS систем.

Таким чином, запроєктована модель забезпечує адаптивну ешелоновану оборону інфраструктури. Вона повною мірою відповідає вимогам міжнародного стандарту ДСТУ ISO/IEC 27001:2023 та чинній нормативно-правовій базі України у сфері захисту інформації. Практичне впровадження запропонованих апаратно-програмних рішень дозволить мінімізувати ризики витоку комерційної таємниці, знизити ймовірність успішних мережевих вторгнень та забезпечити стабільну безперервність операційних бізнес-процесів компанії.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР.
2. ДСТУ ISO/IEC 27001:2023. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. Київ: ДП «УкрНДНЦ», 2023.
3. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture. NIST Special Publication 800-207. National Institute of Standards and Technology, 2020.
4. Офіційна технічна документація комутаторів Huawei CloudEngine S12700 [Електронний ресурс] / Huawei Enterprise. – Режим доступу: https://e.huawei.com/en/products/enterprise-networking/switches/campus-switches/s12700.
5. Стратегія кібербезпеки України: затверджено Указом Президента України (актуальна редакція станом на 2026 рік). URL: https://zakon.rada.gov.ua.
6. Palo Alto Networks. XDR: Redefining Endpoint and Network Security. Technical Report. Santa Clara, 2024. 40 p.
7. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу (з урахуванням рекомендацій ДССЗЗІ станом на 2025 р.). Київ: ДССЗЗІ України. 56 с.
8. Коваленко О. А. CAPEX та OPEX в IT-проєктах: оптимізація витрат. Фінанси підприємства, 2023. № 3. С. 77–84.

УДК 621.391

Д.О. Данилюк, М.Б. Гумен
Національний університет
«Київський авіаційний інститут», м. Київ

UWB-СИСТЕМА ІДЕНТИФІКАЦІЇ ОСІБ У ПРИМІЩЕННІ

Вступна частина. У сучасному світі зростає потреба в ефективному контролі доступу, моніторингу переміщення людей у приміщеннях, а також забезпеченні безпеки в умовах зростаючої урбанізації, автоматизації процесів та цифровізації середовища. Традиційні методи ідентифікації, такі як відеоспостереження або RFID, мають низку обмежень, зокрема недостатню точність, залежність від прямих візуальних контактів або велику затримку при передачі даних. У цьому контексті технологія надширокосмугового радіозв'язку (UWB) демонструє нові можливості – від високої точності позиціонування до низького рівня енергоспоживання..

Основна частина. Всебічний аналіз сучасних бездротових систем ідентифікації, їхніх видів, еволюції, принципів роботи та сфер застосування встановив їх основні переваги та недоліки (див. табл.).

Таблиця

Технологія	Переваги	Недоліки
RFID	Невелика вартість, проста в реалізації	Мала дальність, неможливість точного позиціювання
NFC	Зручна для мобільних рішень	Потребує близького контакту
BLE	Енергоефективна, підтримка смартфонів	Низька точність позиціювання
Wi-Fi	Використання існуючої інфраструктури	Високе енергоспоживання, низька точність
UWB	Висока точність, мала затримка	Висока вартість обладнання

На основі порівняння сучасних бездротових технологій – RFID, Wi-Fi, Bluetooth, ZigBee та UWB, методів ідентифікації в умовах впливу складного середовища, алгоритмів, що забезпечують точність,

швидкість та достовірність визначення особи, запропоновано гібридну архітектуру на базі UWB технології з обробкою даних на периферійних вузлах і сервері, що дозволяє досягнути високої продуктивності системи, її масштабованості та стійкості до збоїв та адаптуватися до складних умов.

Основу системи становлять UWB-приймачі та передавачі на базі модуля Decawave DWM1001, які взаємодіють між собою через ультраширокосмуговий радіоканал. Передавач періодично надсилає сигнали, які приймаються декількома стаціонарними приймачами, встановленими у визначених точках приміщення. Приймачі фіксують час надходження сигналу, що дозволяє обчислити координати передавача. Сигнал UWB стійкий до багатопроменевого поширення, що виникає через відбиття від різних перешкод у приміщенні. Всі сигнали передаються в зашифрованому вигляді, а доступ до інтерфейсу обмежений авторизованими користувачами.

Система здатна одночасно ідентифікувати велику кількість користувачів із закріпленими на них передавачами. Кожен передавач має унікальний ідентифікатор, що дає змогу центральному обчислювального модулю або серверу, який обробляє зібрані сигнали, розрахувати координати, зберігати історію переміщень і забезпечувати візуалізацію даних на екрані оператора. Програмне забезпечення реалізовано на базі Node-RED та MQTT-протоколу для комунікації між модулями. Інтерфейс системи розроблений з використанням HTML5/JavaScript, що дає змогу запускати систему в браузері без потреби у встановленні клієнтських програм. Для зберігання і обробки історії переміщень використовується реляційна база даних MySQL.

Для підвищення надійності і точності ідентифікації система інтегрується з камерами спостереження типу Xiaomi Mi Home Security 1080p з можливістю роботи через локальну мережу.

Оцінка характеристик системи підтвердила її високу ефективність: середня похибка позиціонування не перевищує 10 см, а затримка у відображенні даних становить близько 100 мілісекунд, що дозволяє здійснювати реальний контроль руху осіб у приміщенні.

Заключна частина. Розроблена система є сучасним, надійним і масштабованим рішенням для задач ідентифікації і контролю осіб у різноманітних приміщеннях. Вона має значний потенціал для подальшого вдосконалення і застосування у сферах безпеки, автоматизації доступу та моніторингу персоналу.

УДК 621.396.5

КОНЦЕПЦІЯ СИСТЕМИ ТЕЛЕМЕТРІЇ ТА ВІЗУАЛІЗАЦІЇ РЕАКТИВНИХ БПЛА ДЛЯ ЦИВІЛЬНИХ ЗАДАЧ ЕКСТРЕНОГО МОНІТОРИНГУ

С.О. Завгородній

Державний університет «Київський авіаційний інститут», м. Київ

Використання реактивних безпілотних літальних апаратів (БПЛА) у цивільній сфері, зокрема при ліквідації наслідків техногенних катастроф, дозволяє скоротити час прибуття до зони надзвичайної ситуації в 3–5 разів порівняно з гвинтовими аналогами. Проте висока динамічність польоту та специфіка роботи турбореактивних двигунів ставлять нові вимоги до систем телеметрії та методів візуалізації даних. Вони повинні забезпечити оператору миттєву ситуаційну обізнаність в умовах жорсткого дефіциту часу. Ефективне вирішення цього завдання дозволить мінімізувати ризики втрати керування швидкісним апаратом.

Функціонально система телеметрії має забезпечувати синхронну передачу навігаційних параметрів, даних про стан силової установки та показників цільового навантаження. Враховуючи високу швидкість апарата, частота оновлення критичних польотних даних повинна становити не менше 100 Гц [1]. Візуалізація інформації має реалізовуватися через інтелектуальні інтерфейси, що поєднують реальний відеопотік із накладеними шарами доповненої реальності (AR), які відображають прогнозовану траєкторію та вектори небезпеки. Це дозволяє оператору візуально зіставляти цифрові моделі загроз із реальною поверхнею безпосередньо під час виконання маневрів.

Основними нефункціональними вимогами до такої системи є висока продуктивність та мінімальна затримка. Для реактивного БПЛА, що рухається зі швидкістю 150 м/с, наскрізна затримка (end-to-end latency) понад 200 мс призводить до похибки позиціонування більше 30 метрів, що унеможливлює безпечне маневрування поблизу об'єктів критичної інфраструктури [2]. Оптимізація методів екстракції просторових даних, як-от використання фреймворків типу VORTEX, дозволяє значно знизити загальне обчислювальне навантаження. Завдяки цьому забезпечується висока точність вимірювання швидкості навіть за умов інтенсивного інформаційного потоку.

Аналіз протоколів передачі даних показує, що MAVLink залишається домінуючим стандартом, однак його вразливості потребують додаткового захисту. Для забезпечення криптостійкості без

надмірного навантаження на бортові обчислювальні ресурси доцільно використовувати легковагові шифри, такі як MAVShield. З метою мінімізації часу обробки інформації, архітектура наземної станції керування (GCS) використовує шаблони Producer-Consumer та Observer. Дослідження показують [3], що інтеграція з ROS 2 через інтерфейси типу WildBridge (затримка телеметрії менше 113 мс при 32 Гц) здатна забезпечити необхідну продуктивність.

Специфіка реактивних систем також вимагає впровадження інтелектуальної пріоритезації даних та надійних механізмів уникнення зіткнень. У разі обмеження пропускної здатності каналу зв'язку, система має автоматично надавати пріоритет телеметрії двигуна та даним про перешкоди. Валідація таких систем із використанням Hardware-in-the-Loop симуляції підтверджує їх здатність забезпечувати безпеку польотів навіть у разі втрати супутникових сигналів. Це гарантує живучість комплексу в умовах складної завадової обстановки або відсутності сигналу GNSS.

Впровадження реактивних БПЛА у цивільний сектор для екстреного моніторингу потребує обов'язкового переходу до високошвидкісних протоколів телеметрії із частотою оновлення даних від 100 Гц. Використання технологій доповненої реальності (AR), легковагового шифрування та шаблонів оптимізації обробки даних дозволяє мінімізувати критичні затримки та забезпечити оператора точною інформацією в реальному часі. Запропонована концепція інтеграції сучасних архітектурних рішень та інтелектуальної пріоритезації параметрів гарантує високу безпеку й ефективність польотів на великих швидкостях під час ліквідації надзвичайних ситуацій.

Список літератури

1. De Silva D. D. S., Bandara S. A. R. S., Herath M. M. H. M., et al. A Novel Cipher for Enhancing MAVLink Security. *arXiv preprint arXiv:2504.20626*, 2025.
2. Gallagher J. E., Capezzuto D. E. VORTEX: A Spatial Computing Framework for Optimized Drone Telemetry Extraction from First-Person View Flight Data. *arXiv preprint arXiv:2412.18505*, 2025.
3. WildBridge: Ground Station Interface for Lightweight Multi-Drone Control and Telemetry on DJI Platforms. *Proceedings of the 13th International Conference on Robot Intelligence Technology and Applications (RiTA)*, 2025.

УДК 621.396.4

А.М. Заколодний, А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

АНАЛІЗ ЕФЕКТИВНОСТІ БАГАТОАНТЕННИХ СИСТЕМ ПЕРЕДАЧІ ЦИФРОВИХ ДАНИХ

Сучасний етап розвитку систем бездротового зв'язку характеризується стрімким і невпинним зростанням вимог до пропускної здатності, надійності передачі даних та якості обслуговування користувачів (QoS). В умовах жорстко обмеженого частотного ресурсу традиційні одноантенні системи (SISO) вичерпали свої можливості щодо підвищення швидкості передачі інформації. Одним із найбільш дієвих та перспективних рішень цієї проблеми є впровадження технології MIMO (Multiple Input Multiple Output), яка дозволяє суттєво підвищити спектральну ефективність без необхідності розширення смуги частот або збільшення загальної потужності передавача. Використання декількох антен на передавальній та приймальній сторонах створює умови для просторового мультиплексування та рознесення, що є критично важливим для мінімізації негативного впливу багатопроменевого поширення радіохвиль та глибоких завмирань сигналу.

У роботі проведено ґрунтовний аналіз теоретичних засад побудови багатоантенних систем. Детально розглянуто еволюцію стандартів радіозв'язку та наведено класифікацію сучасних антенних конфігурацій. Досліджено фундаментальні принципи просторового мультиплексування, яке дозволяє передавати кілька незалежних потоків даних паралельно, та просторового рознесення, що значно підвищує надійність зв'язку. Крім того, проаналізовано технологію формування діаграми спрямованості (Beamforming), що забезпечує концентрацію випромінюваної енергії в напрямку конкретного абонента, тим самим знижуючи рівень внутрішньосистемних завад.

Окрему увагу приділено математичним моделям та алгоритмам обробки сигналів у приймально-передавальному тракті систем MIMO. Досліджено методи просторово-часового блочного кодування (STBC), які забезпечують високу завадостійкість за рахунок передачі ортогональних копій інформаційних символів через різні антени в різні моменти часу. Математичне моделювання каналів поширення проводилося з урахуванням статистичних моделей завмирань Релея та Райса,

що дозволило адекватно оцінити поведінку системи як за відсутності, так і за наявності складової прямої видимості (LOS) між кореспондентами. Також було виконано розрахунок теоретичної пропускної здатності каналу для різних антенних конфігурацій відповідно до теореми Шеннона-Гартлі для багатовимірних систем..

В межах практичної частини дослідження в програмному середовищі MATLAB було розроблено комплексну імітаційну модель тракту передачі даних. Під час симуляції досліджувався вплив різних схем багатопозиційної цифрової модуляції (зокрема, M-QAM та QPSK) на загальну спектральну ефективність системи в залежності від стану радіоканалу. Це дозволило провести глибоку оцінку ефективності застосування методів просторового кодування та отримати графічні залежності ймовірності бітової помилки (BER) від відношення сигнал/шум (SNR). Результати моделювання переконливо підтвердили, що перехід від базових систем SISO до конфігурацій MIMO 2x2 та 4x4 забезпечує енергетичний виграш у завадостійкості до 4–6 дБ для фіксованого рівня BER = 10^{-3}. Встановлено, що застосування алгоритмів просторової обробки дозволяє стабілізувати зв'язок у складних умовах щільної міської забудови з інтенсивним багатопроменевим перевідбиттям сигналів.

На основі отриманих результатів моделювання було сформовано низку практичних рекомендацій щодо розгортання та оптимізації багатоантенних систем у реальних умовах експлуатації. Крім того, окреслено вектори масштабування базових конфігурацій до архітектури Massive MIMO, де кількість антенних елементів на базовій станції вимірюється десятками, що радикально підвищує ємність стільника. З проведеного дослідження можна зробити висновок, що системи MIMO є не просто оптимальним, а безальтернативним рішенням для сучасних високошвидкісних бездротових мереж. Комплексне використання методів просторового кодування та мультиплексування дозволяє досягти компромісу між швидкістю передачі даних та якістю з'єднання, що робить цю технологію надійним фундаментом для подальшого розвитку стандартів 5G та розробки систем зв'язку наступних поколінь.

УДК 004.9:658.5:629.7

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

ІНФОРМАЦІЙНА МОДЕЛЬ ДОКУМЕНТООБІГУ АВІАЦІЙНОГО ПІДПРИЄМСТВА

У сучасних умовах діяльність авіаційних підприємств супроводжується обробкою значного обсягу інформації, пов'язаної з технічним обслуговуванням повітряних суден, ремонтними роботами, заявками на матеріали, виробничими завданнями, службовими документами та управлінською звітністю. Ефективність функціонування такого підприємства значною мірою залежить від своєчасної передачі інформації між технічним відділом, виробничими цехами, складом, службою контролю якості та керівництвом підприємства.

Однією з основних проблем традиційного документообігу є повільна передача документів між підрозділами, складність контролю виконання завдань, ризик втрати інформації, дублювання даних і тривале формування звітності. У випадку авіаційного підприємства ці проблеми є особливо важливими, оскільки більшість виробничих і технічних процесів потребує документального підтвердження, контролю відповідальних осіб і своєчасного прийняття управлінських рішень.

Метою роботи є розробка інформаційної моделі системи підтримки управлінських рішень авіаційного підприємства, орієнтованої на автоматизацію електронного документообігу між відділами та виробничими цехами. Запропонована система повинна забезпечувати створення електронних документів, передачу їх між підрозділами, зміну статусів, контроль виконання, збереження історії дій і формування аналітичної звітності для керівництва.

Для досягнення поставленої мети було визначено основні об'єкти інформаційної моделі: користувачі, ролі, підрозділи, документи, типи документів, статуси, маршрути передачі, історія змін, повітряні судна, технічне обслуговування та звіти. Центральним об'єктом моделі є електронний документ, який містить номер, назву, тип, автора, дату створення, термін виконання, поточний статус, підрозділ-відправник і підрозділ-одержувач.

У межах проєктування системи доцільно використовувати трирівневу архітектуру, яка включає рівень інтерфейсу користувача, рівень бізнес-логіки та рівень доступу до даних. Такий підхід дозволяє розділити функції відображення інформації, обробки документів і роботи з базою даних. Для моделювання структури та поведінки системи можуть бути використані UML-діаграми, зокрема діаграма варіантів використання, діаграма активності, діаграма послідовності та діаграма класів.

Програмна реалізація системи може бути виконана з використанням мови програмування C#, платформи .NET, середовища Microsoft Visual Studio та системи керування базами даних SQL Server. Використання реляційної бази даних дає змогу забезпечити цілісність інформації, зв’язок між основними сутностями системи, швидкий пошук документів і формування аналітичних запитів.

Основними функціональними модулями системи є модуль авторизації, модуль керування користувачами, модуль роботи з документами, модуль маршрутизації, модуль контролю статусів, модуль історії змін, модуль аналітики та модуль формування звітності. Кожен користувач системи отримує доступ до функцій відповідно до своєї ролі. Наприклад, адміністратор системи керує користувачами та довідниками, керівник переглядає аналітику й погоджує документи, працівник цеху обробляє отримані заявки, а працівник складу працює із заявками на матеріали.

Особливу роль у системі відіграє алгоритм маршрутизації документів. Він забезпечує передачу документа між підрозділами відповідно до виробничого процесу. Наприклад, заявка на ремонт може проходити маршрут: технічний відділ — ремонтний цех — служба контролю якості — керівник. На кожному етапі система фіксує зміну статусу документа та записує дію в історію змін.

Отже, запропонована інформаційна модель системи підтримки управлінських рішень авіаційного підприємства дозволяє підвищити ефективність документообігу, забезпечити централізоване зберігання документів, зменшити ризик втрати інформації, покращити контроль виконання завдань і надати керівництву актуальні дані для прийняття управлінських рішень. Розроблене рішення може бути використане як основа для створення програмної системи електронного документообігу між відділами та виробничими цехами авіаційного підприємства.

УДК 519.233.2: 621.391.83 (045)

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

ПОХИБКИ КЛАСИФІКАЦІЇ ТЕХНІЧНОГО СТАНУ ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

Під класифікацією властивостей об'єктів розуміємо експериментальний процес отримання інформації у вигляді висловлювання про стан об'єкта, що досліджується. Класифікація технічного стану (ТС) досліджуваних телекомунікаційних та радіоелектронних систем (ТКРС) здійснюється у результаті реалізації процесів їх моніторингу та контролю. Однією з основних цілей оцінки стану ТКРС є визначення можливого класифікованого стану (КС). Помилка класифікації, в цілому, це подія, що полягає в неправильному прийнятті рішення про належність об’єкта до можливого КС.

Процес визначення ТС обладнання ТКРС складається з сукупності елементарних операцій (ЕО). Кожна операція призначена для виконання певних функцій перетворення у визначеній послідовності відповідно до обраного алгоритму прийняття рішень про стан обладнання. Найпоширеніші моделі оцінки ТС обладнання використовують операції перетворення певного вектору станів (ВС) досліджуваного обладнання у визначений вектор реалізацій (ВР) внаслідок спільної дії сукупності ЕО. Отже, показники ефективності виконання оцінки ТС обладнання ТКРС залежать від якості виконання кожної з досліджуваної сукупності ЕО. Розглянемо перетворення ВС, що знаходиться перед оцінкою стану ТКРС в r-му КС, сукупністю послідовно виконуваних ЕО (Рис. 1).

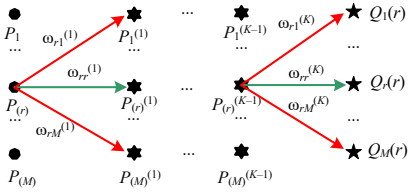


Рис.1 Перетворення ВС сукупністю послідовно виконуваних ЕО.

Якість оцінки на виході K-ої ЕО визначатиметься сукупністю безумовних ймовірностей сприйняття даною ЕО вектора станів, перетвореного спільною дією сукупності всіх попередніх ЕО, тобто

$$P^{(K-1)} = \left(P_{(1)}^{(K-1)}, P_{(2)}^{(K-1)}, \ldots, P_{(i)}^{(K-1)}, \ldots, P_{(M)}^{(K-1)}\right), \quad (1)$$

де $P_{(i)}^{(K-1)} = P\left\{\vec{\Xi}^{(N)} \in \Delta_{(i)}^{(K)}\right\}$, $i = \overline{1,M}$ є безумовна ймовірність сприйняття K-ою ЕО ВС, перетвореного сумісною дією сукупності $1,2,\ldots,i,\ldots,(K-1)$-ої ЕО, у i-му КС; $\Delta_{(i)}^{(K)}$ – сукупність ознак (норм), що розділяють i -ий КС після завершення $(K-1)$-го кроку.

Можливість помилок перетворення ВС, будемо визначати умовною ймовірністю переходу ВС з i-го в j-ий КС при виконанні K-ої ЕО, тобто

$$\omega_{ij}^{(K)} = P\left\{\vec{\Xi}^{(N,K)} \in \Delta_{(j)}^{(K)} / \vec{\Xi}^{(N,K-1)} \in \Delta_{(i)}^{(K-1)}\right\}. \quad (2)$$

Реальне перетворення ВС, здійснюється ЕО з похибкою, що з'являється у результаті сукупних перетворень з різницею

$$\vec{\varepsilon}^{(K)} = \vec{\Xi}^{(N,K)} - \vec{\Xi}^{[N_i(K-1)]}. \quad (3)$$

Зважаючи на те, що перетворення ВС, здійснювані ЕО, у загальному випадку може змінити або його фізичну сутність, або його масштаб, то й умови, що розділяють його КС, також змінюються відповідно до функції необхідного перетворення. Тобто, маємо:

$$\omega_{ri}^{(K-1)} = \frac{P\left\{\vec{\Xi}^{[N_i(K-1)]} \in \Delta^{(K-1)}(r); \vec{\Xi}^{[N_i(K-1)]} + \vec{\varepsilon}^{(K)} \in \Delta^{(K)}(i)\right\}}{P\left\{\vec{\Xi}^{(N)} \in \Delta^{(K-1)}(r)\right\}}. \quad (4)$$

Таким чином, отримано аналітичний вираз, що зв'язує показники точності виконання будь-якої ЕО, що визначаються перехідними ймовірностями $\omega_{ri}^{(K)}$, з показниками якості перетворення в сукупності спільної дії всіх попередніх ЕО, що визначаються ймовірністю його сприйняття в можливому КС і показниками якості виконання перетворення ВС. Отримані результати дозволяють оцінити похибки класифікації ТС у процесі експлуатації телекомунікаційних та радіоелектронних систем різноманітного призначення.

УДК 621.391

С.О. Іванов, М.М. Малоєд
Державний університет
«Київський авіаційний інститут», м. Київ

МЕТОД СЕГМЕНТАЦІЇ ЗОБРАЖЕНЬ З ВИКОРИСТАННЯМ НЕЙРОННОЇ МЕРЕЖІ

Стрімкий розвиток методів комп'ютерного зору та глибокого навчання відкрив нові можливості для автоматизованого аналізу цифрових зображень. Сучасні згорткові нейронні мережі здатні розв'язувати задачі, які донедавна вимагали ручної обробки висококваліфікованими фахівцями. Семантична сегментація — це задача присвоєння кожному пікселю зображення мітки класу, що дозволяє отримати піксельно-точне розуміння візуальної сцени. На відміну від класифікації, яка надає одну мітку всьому зображенню, та детекції, яка обмежується прямокутними рамками, сегментація забезпечує найбільш повну форму інтерпретації візуальної інформації. Особливе значення має задача сегментації будівель на супутникових знімках для оперативного оновлення геоінформаційних систем (ГІС), міського планування та моніторингу наслідків стихійних лих [1]. Однак сучасні методи семантичної сегментації стикаються з проблемою компромісу між точністю та обчислювальною ефективністю — найточніші архітектури вимагають значних обчислювальних ресурсів, що ускладнює їх практичне застосування. Метою роботи є аналіз методу семантичної сегментації зображень на основі архітектури FastFCN з модулем Joint Pyramid Upsampling (JPU), який забезпечує оптимальний баланс між точністю та обчислювальною ефективністю.

Архітектура FastFCN складається з трьох основних компонентів: backbone-мережі ResNet-50/101, попередньо навченої на ImageNet; модуля JPU для відновлення роздільної здатності та об'єднання багатомасштабного контексту; контекстної голови (Encoding, PSP або ASPP) для генерації фінальних передбачень. Ключова інновація FastFCN полягає у відмові від обчислювально дорогих атрових згорток у backbone, як це робиться у DeepLab та EncNet. Замість цього модуль JPU приймає карти ознак з трьох останніх блоків кодувальника (Conv3, Conv4, Conv5) і застосовує до них чотири паралельні розділені (depthwise-separable) атрові згортки 3×3 з коефіцієнтами розширення d = 1, 2, 4, 8. Це дозволяє ефективно захоплювати контекст на чотирьох різних масштабах при

значно меншій обчислювальній складності — depthwise-separable згортка має приблизно у 9 разів менше параметрів та операцій порівняно зі звичайною 3×3 згорткою. Експериментальні результати, отримані авторами архітектури на стандартному бенчмарку Pascal Context, демонструють, що FastFCN досягає state-of-the-art точності 53.1% mIoU при більш ніж триразовому прискоренні порівняно з базовою архітектурою EncNet — 32.02 FPS на NVIDIA Titan Xp проти 10.51 FPS у базовій конфігурації. Аблаційне дослідження модуля JPU підтверджує його перевагу над альтернативними методами підвищення роздільної здатності: білінійна інтерполяція забезпечує 46.47% mIoU, FPN — 49.59% mIoU, а JPU — 51.05% mIoU. Універсальність методу додатково підтверджується результатами на бенчмарку ADE20K (150 класів), де FastFCN покращує mIoU на 1.64% порівняно з базовою EncNet. У контексті дистанційного зондування метод є перспективним для адаптації до спеціалізованих датасетів сегментації будівель [2], зокрема SpaceNet-7 (MUDS), який містить понад 11 мільйонів анотованих об'єктів на шести континентах при просторовій роздільній здатності близько 4 м/піксель.

Метод FastFCN з модулем JPU є ефективним рішенням задачі семантичної сегментації зображень. Завдяки використанню розділених атрових згорток у компактному JPU-модулі замість повноцінних атрових згорток у backbone, метод досягає state-of-the-art точності при триразовому прискоренні. Це робить FastFCN перспективним інструментом для інтеграції в сучасні геоінформаційні системи з метою автоматичного картографування забудови, моніторингу інфраструктури та оцінки наслідків стихійних лих. Практичне впровадження методу дозволяє суттєво зменшити час обробки великих масивів супутникових даних. Перспективним напрямком подальших досліджень є адаптація методу до SpaceNet-7 та інтеграція з трансформерами (SegFormer, SAM-2).

Список літератури

1. Open Sourcing TensorFlowOnSpark: Distributed Deep Learning on Big-Data Clusters [Електронний ресурс] / L. Yang, J. Shi, B. Chern, A. Feng. – Режим доступу: https://developer.yahoo.com/blogs/157196317141/
2. Огляд моделей нейронних мереж для задач виявлення 2d-об’єктів. / М. Заліський, С.Белов., 2026. Science-based technologies 68(4):443-452. DOI:10.18372/2310-5461.68.20280

УДК 621.391.8

В.О. Калениченко, А.О. Осіпчук
Державний університет
«Київський авіаційний інститут», м. Київ

ДОСЛІДЖЕННЯ РАДІОЧАСТОТНОГО СПЕКТРА НА ОСНОВІ SDR ТЕХНОЛОГІЇ

Сучасний розвиток бездротових систем зв'язку призводить до значного збільшення кількості джерел електромагнітного випромінювання у діапазоні 2,4 ГГц. У даному частотному діапазоні функціонують Wi-Fi мережі, Bluetooth-пристрої, телеметричні системи, IoT-пристрої та інші цифрові засоби передавання інформації. Висока щільність сигналів створює значне навантаження на спектральний ресурс і призводить до виникнення електромагнітних завад, що ускладнює стабільну роботу бездротових систем зв'язку. У зв'язку з цим актуальним завданням є створення ефективних систем моніторингу радіочастотного спектра, здатних забезпечувати аналіз електромагнітної обстановки у режимі реального часу.

Одним із найбільш перспективних напрямів реалізації таких систем є використання технології програмно-визначуваного радіо SDR (Software Defined Radio). У роботі розроблено імітаційну модель дослідження радіочастотного спектра на базі SDR-приймача HackRF One та програмного забезпечення SDRSharp. Розроблена система забезпечує приймання сигналів, спектральний аналіз та візуалізацію електромагнітної обстановки у режимі реального часу. Структурно система складається з антени, SDR-приймача, блоку цифрової обробки сигналів та програмного середовища для аналізу результатів. Приймання сигналів здійснюється SDR пристроєм HackRF One, який підтримує широкий частотний діапазон та дозволяє виконувати аналіз різних типів радіосигналів.

У роботі досліджено можливості використання SDR-приймача HackRF One та програмного забезпечення SDRSharp для моніторингу діапазону 2,4 ГГц. Використання SDR-технології дозволяє реалізувати приймання, аналіз та візуалізацію сигналів програмними засобами без необхідності зміни апаратної частини системи. Під час дослідження виконувалось приймання та аналіз сигналів у діапазоні 2,3–2,5 ГГц. Особливу увагу приділено аналізу Wi-Fi та Bluetooth-сигналів, які формують основне спектральне навантаження у даному діапазоні.

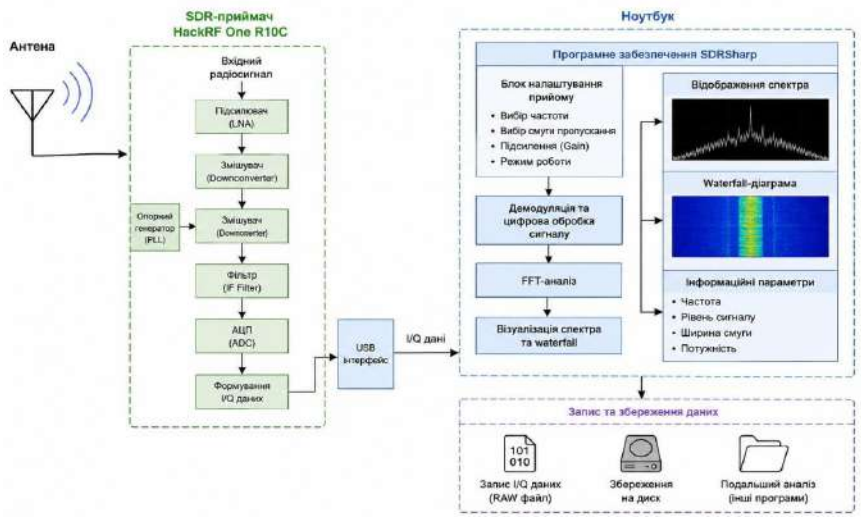


Рисунок 1. Структурна схема дослідження радіочастотного спектру на базі SDR HackRF One R10C

У процесі дослідження було встановлено, що найбільш завантаженими є Wi-Fi канали, у яких спостерігається значне перекриття частотних смуг. Це призводить до появи міжканальних завад та збільшення рівня шуму у спектрі. Аналіз waterfall-діаграм дозволив визначити динаміку використання каналів та виявити короткочасні сигнали Bluetooth-пристроїв. Отримані результати підтвердили ефективність використання SDR-технології для задач моніторингу радіочастотного спектра та аналізу електромагнітної обстановки. Розроблена система може бути використана у навчальних, науково-дослідних та прикладних задачах спектрального аналізу бездротових мереж.

Список використаних джерел:

1. HackRF One. HackRF documentation. URL: https://hackrf.readthedocs.io/en/latest/hackrf_one.html.
2. Sarbu A., Neagoie D. Wi-Fi Jamming Using Software Defined Radio. International conference KNOWLEDGE-BASED ORGANIZATION. 2020. Vol. 26, iss. 1. P. 162–166. DOI: doi.org.

УДК 621.391

В.П. Климчук, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

ЗАСТОСУВАННЯ НЕКОГЕРЕНТНОГО ЧФМ-МОДЕМУ У ЗАКРИТОМУ КАНАЛІ АВІАЦІЙНОГО РАДІОЗВЯЗКУ

Сучасні технології передавання конфіденційної мовної інформації стандартним авіаційним радіоканалом не здатні задовольнити вимог щодо ступеню захищеності та розбірливості прийнятих мовних повідомлень за умов, коли висуваються підвищені вимоги щодо забезпечення стабільності зв'язку. У даній роботі пропонується удосконалити вокодерну технологію передачі захищеної інформації через мовний тракт авіаційного радіоканалу за рахунок використання некогерентного модемного зв'язку.

Технологічна схема обробки захищеного мовного трафіку. Проведені аналітичні дослідження довели можливість застосування у вузькосмугових системах зв'язку некогерентного ЧФМ-модему, що не потребує використання пристроїв фазової синхронізації. Технологічна схема захисту та передачі мовного трафіку приведена на рис.1.

Для узгодження ширини спектру мовного сигналу із смугою пропускання мовного тракту стандартного авіаційного радіоканалу на передавальній стороні системи зв'язку здійснюється стиснення мовного сигналу шляхом усунення інформаційної надлишковості та «оцифровки» цього сигналу за допомогою засобів однієї із відомих вокодерних технологій. Зокрема, з цією метою доцільно використати двадцяти смуговий вокодер або вокодер із лінійним передбаченням (ліпредер).

Нестатистичне кодування алфавіту стисненого сигналу відкритої «оцифрованої» мови виконано згідно виразу (1):

$$K_U = \alpha \cdot (1 + \frac{K_м}{n_ц}) \cdot (log_2 N / log_2 m)/\lceil log_2 N_к / log_2 m \rceil \qquad (1)$$

де K_U – коефіцієнт нестатистичної надлишковості повідомлень; m – загальне число позицій сигналу.

Літери еквівалентного джерела повідомлень (ЕДП) (помітимо, що ЕДП складається із ДП та кодера повідомлень), що утворені послідовністю із α = 1, 2, 3, … літер ЕДП, кодуються рівномірним кодом із основою m.

У кожній кодовій комбінації (КК) міститься:

$$n = \left| \log_2 N_\chi / \log_2 m \right| \quad (2)$$

елементарних символів, а число літер в алфавіті ЕДП буде:

$$N_x = N^\alpha, \quad (3)$$

де N – число літер в алфавіті ДП; $\lceil x \rceil$ – позначає найближче більше цілочисельне значення χ.

Коефіцієнт K_U у загальному випадку визначається як:

$$K_u = (log_2 N_x / log_2 m)/\lceil log_2 N_x / log_2 m \rceil. \quad (4)$$

З урахуванням (3) та (4) визначимо R у вигляді:

$$R = (K_E \cdot \alpha \cdot log_2 N)/(\lceil \alpha \cdot log_2 N / log_2 m \rceil \ \tau . \quad (5)$$

Звідкіля видно, що при $N = const$, τ = const та K_E = const змінювання R можливо лише за рахунок змінювань α та m і в залежності від значень m R у виразі (5) має ступінчастий характер, при чому:

$$max\ R = K_E \cdot \alpha \cdot log_2 N / \tau \quad (6)$$

досягається при

$$m = N^\alpha. \quad (7)$$

Як видно із (7), дискретність послідовності значень N^α при α = 1, 2, 3,… є суттєвою, а спроба збільшити m супроводжується рядом труднощів, що проявляються як ускладнення обладнання, погіршення завадостійкості тощо. Якщо бажане значення m знаходиться у проміжку між N^α та $N^{\alpha-1}$, то можливе значення $max\ R$ у цій ситуації не буде досягнуто. Тому являє певний інтерес визначення такого перетворення алфавіту ДП, за котрим проміжки між можливими значеннями m, що максимізують R при $K_E = const$ та τ = const, були б мінімальними. Таке перетворення реалізується у маніпуляційному кодері (МК) наступним чином (9).

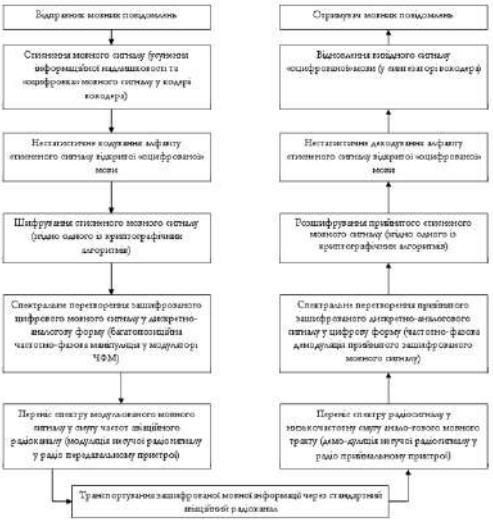


Рис.1. Технологічна схема обробки захищеного мовного трафіку в авіаційних системах радіозв'язку

На першому етапі послідовності із

$$n'_{и} = n_{и} + K_{м}, \quad \text{де } K_{м} = 1 - n_{и}, \quad 2 - n_{и}, \ldots, 0, 1, 2, \ldots \qquad (8)$$

символів вихідного коду з основою $m_{и}$ розглядаються як нові кодові комбінації /КК/, кількість яких дорівнює:

$$N_{Н} = \begin{cases} m_{и}^{n_{и}}, K_{М} \neq 0, n_{и}, 2n_{и}, \ldots; \\ N^{\alpha(1+K_{М}/n_{и})}, K_{М} = 0, n_{и}, 2n_{и}, \ldots; \end{cases} \qquad (9)$$

де $K_{М} = 1 - n_{и}, 2 - n_{и}, \ldots 0, 1, 2, \ldots$ – параметр МК, що дозволяє змінювати значення $N_{Н}$.

Величина $n_{и}$, що входить у (8) та (9), дорівнює:

$$n_{и} = \lceil \alpha \cdot \log_2 \cdot N / \log_2 m_{е} \rceil. \qquad (10)$$

На другому етапі алфавіт з основою $N_{Н}$ у МК кодується рівномірним кодом з основою m таким чином, що кількість символів у кодовій комбінації нового коду дорівнює:

$$N_{Н} = \lceil \log_2 N_{і} / \log_2 m \rceil. \qquad (11)$$

При такому процесі маніпуляційного кодування $K_{и}$ визначається виразом (1).

Шифрування стисненого мовного сигналу здійснюється відповідно до одного із відомих криптографічних алгоритмів – блокового або потокового.

Отримане таким чином закрите мовне повідомлення передається за допомогою некогерентного ЧФМ-модему у канал зв'язку, на приймальній стороні якого здійснюються зворотні перетворення з метою отримання відкритого мовного сигналу.

Висновки

Було вдосконалено технологічну схему захищеної передачі параметрів вокалізованої мовної інформації через стандартний авіаційний радіоканал. Процес удосконалення полягає у заміщенні когерентної системи транспортування вокалізованих мовних сигналів некогерентним модемним зв'язком, яким не передбачено використання пристроїв фазової синхронізації і усуває причину виникнення нестабільності при організації сеансів зв'язку. В якості складового елементу вокодерної технології застосовані процедури некогерентного прийому вокалізованих мовних сигналів.

УДК 621.391

Д.А. Коваленко, Ю. В. Петрова
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ПОЖЕЖНОЇ БЕЗПЕКИ НА БАЗІ МІКРОКОНТРОЛЕРА ESP32

У сучасних умовах забезпечення пожежної безпеки є одним із найважливіших напрямів захисту життя людей, матеріальних цінностей та об'єктів інфраструктури. Несвоєчасне виявлення пожежі або витоку газу може призвести до значних матеріальних збитків та створити загрозу для життя і здоров'я людей. У зв'язку з цим актуальним є створення автоматизованих систем, здатних оперативно виявляти небезпечні ситуації та повідомляти користувача про виникнення загрози, зменшуючи залежність від людського фактора.

Одним із перспективних напрямів розвитку сучасних систем безпеки є використання технологій Інтернету речей (IoT), які дозволяють реалізовувати дистанційний моніторинг і керування пристроями в режимі реального часу. Завдяки застосуванню сучасних мікроконтролерів з підтримкою бездротового зв'язку з'явилась можливість створення компактних, енергоефективних, доступних та функціонально розширюваних систем пожежної безпеки.

У роботі розглянуто розробку системи пожежної безпеки на базі мікроконтролера ESP32. Вибір даної платформи обумовлений наявністю вбудованих модулів Wi-Fi та Bluetooth, достатньою обчислювальною потужністю, низьким енергоспоживанням у порівнянні з аналогами та можливістю підключення великої кількості периферійних пристроїв. Це дозволяє створювати системи моніторингу, здатні працювати автономно, масштабуватися та інтегруватися з іншими цифровими сервісами та хмарними платформами.

Основним завданням системи є виявлення диму або горючих газів за допомогою датчика MQ-2 та автоматичне реагування у разі виникнення небезпечної ситуації. Після спрацювання датчика мікроконтролер активує виконавчі пристрої, зокрема вентилятор та помпу, які виконують функцію вентиляції та імітації первинного пожежогасіння. Одночасно система вмикає звукову та світлодіодну сигналізацію для локального оповіщення користувачів, що перебувають у зоні ризику.

Особливістю розробленої системи є можливість дистанційного моніторингу через мережу Wi-Fi. Для цього реалізовано інтеграцію з месенджером Telegram, що дозволяє надсилати повідомлення користувачу у разі виявлення небезпечної ситуації в режимі майже миттєвого реагування. Такий підхід забезпечує оперативне інформування незалежно від місцезнаходження користувача та підвищує загальний рівень безпеки об’єкта.

Для реалізації програмної частини системи використовувалося середовище Arduino IDE, яке забезпечує зручність розробки та швидке прототипування. Електричну схему пристрою було розроблено у програмі Fritzing, що дозволило візуалізувати підключення компонентів та спростити процес налагодження. У ході роботи виконано побудову структурної та електричної схем системи, розроблено алгоритм функціонування та програмний код для обробки даних із датчиків і керування виконавчими пристроями.

У процесі тестування було перевірено працездатність системи в різних режимах роботи, включаючи зміну концентрації газу та диму, а також умови нестабільного сигналу датчика. Отримані результати підтвердили стабільність функціонування системи, коректність обробки сигналів датчика MQ-2 та ефективність роботи механізму дистанційного сповіщення через Telegram. Також було підтверджено можливість автоматичного реагування системи на небезпечні ситуації без безпосереднього втручання користувача.

Проведений аналіз показав, що використання ESP32 є ефективним рішенням для побудови систем автоматизованої пожежної безпеки завдяки поєднанню високої функціональності, гнучкості, низької вартості та широких можливостей інтеграції з IoT-технологіями. Запропонована система може бути використана як базова платформа для подальшого вдосконалення та розширення функціоналу, зокрема шляхом підключення додаткових датчиків, інтеграції з системами «розумного будинку» або використання хмарних сервісів моніторингу.

Додатково слід зазначити, що практична реалізація подібних систем може бути масштабована для використання не лише в побутових умовах, але й на об’єктах малого бізнесу та навчальних закладах. Завдяки модульній архітектурі запропонованого рішення можливе поступове розширення функціоналу системи без суттєвих змін у базовій апаратній частині, що підвищує її універсальність та економічну доцільність впровадження.

УДК 621.391

Кононенко Д.П.
Климчук В.П.
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМИ МОНІТОРИНГУ ПОВІТРЯНИХ СУДЕН ADS-B НА БАЗІ ПРОГРАМНО ВИЗНАЧЕНОГО РАДІО

Технологія автоматичного залежного спостереження-мовлення (ADS-B) є ключовим елементом сучасних систем управління повітряним рухом, оскільки вона забезпечує високу точність визначення координат повітряних суден. Традиційні апаратні засоби приймання сигналів ADS-B на частоті 1090 МГц є високовартісними та складними у модернізації. Використання технології програмно визначеного радіо (SDR) дозволяє значно знизити вартість розгортання наземних станцій моніторингу, забезпечуючи гнучкість обробки сигналів на рівні програмного забезпечення.

Особливість SDR технології полягає в тому, що більшість функцій обробки радіосигналу виконуються за допомогою програмного забезпечення на комп'ютері, а не за допомогою складних апаратних схем (транзисторів, фільтрів), як у класичних приймачах.

Використання SDR технології дає змогу реалізувати наступні переваги організації авіаційного радіозв’язку:

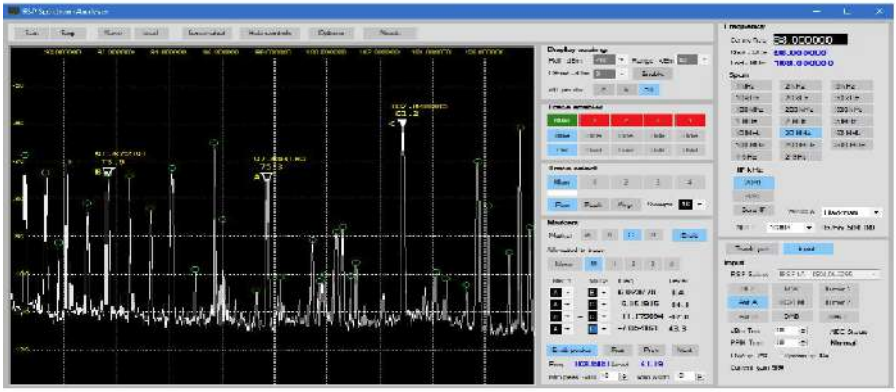
— **у**ніверсальність: один SDR-пристрій може приймати практично весь радіотрафік незалежно від робочого діапазону, методу модуляції — від радіомовлення та авіачастот до сигналів супутників і військових рацій.

— гнучкість та оновлення**:** щоб додати підтримку нового стандарту зв'язку, достатньо оновити програму (не потрібно встановлювати нове обладнання).

— візуалізація**:** на екрані монітора приймача можна бачити радіоефір у вигляді спектру, обираючи потрібні сигнали мишкою.

— доступність: базові USB SDR-донгли коштують недорого, перетворюючи звичайний ПК на потужну радіостанцію.

— екіпажу або диспетчеру зручно вибирати потрібного абонента користуючись наглядним монітором.



Візуалізація спектру радіосигналі Назви джерел радіосигналів

Приклад оформлення монітора SDR-приймача

Для побудови системи моніторингу в роботі розглядається використання доступних SDR-платформ, що підключаються до персональних комп'ютерів або мікрокомп'ютерів. Програмна складова реалізує алгоритми демодуляції сигналів з імпульсно-позиційною модуляцією (PPM) та декодування пакетів даних Mode S, які містять унікальний індекс ICAO літака, його координати, висоту, швидкість та курс.

Важливим аспектом дослідження є оцінка завадозахищеності та радіомоніторингу каналу зв'язку в умовах високої щільності повітряного руху. Використання цифрової обробки сигналів (DSP) у SDR дозволяє застосовувати адаптивні алгоритми фільтрації для зниження впливу фонових шумів та інтерференційних завад.

Таким чином, застосування концепції програмно визначеного радіо для моніторингу повітряних суден за технологією ADS-B демонструє високу ефективність, економічну вигідність та масштабованість. Запропоноване рішення може бути використане для створення резервних каналів спостереження, а також для проведення радіомоніторингу та оцінки безпеки інформаційно-комунікаційних систем цивільної авіації.

УДК 004.67

Б.В. Константин, А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

РАДІОМОДУЛЬ ДЛЯ СИСТЕМИ ПЕРЕДАЧІ ЦИФРОВИХ ДАНИХ

Розгортання сучасних бездротових мереж Інтернету речей (*IoT*) висуває жорсткі вимоги до апаратної частини кінцевих пристроїв. Традиційне безперервне передавання «сирих» даних призводить до перевантаження радіоінтерфейсу колізіями та швидкого вичерпання автономного живлення пристроїв. Тому актуальним інженерним завданням є проектування завадостійких радіомодулів, здатних ефективно працювати у протоколах *LPWAN* (*LoRaWAN*, *NB-IoT*). Для мінімізації навантаження на бездротовий канал зв'язку в архітектуру радіомодуля інтегровано концепцію периферійних обчислень (*Edge Computing*), яку ілюструє рис.1.

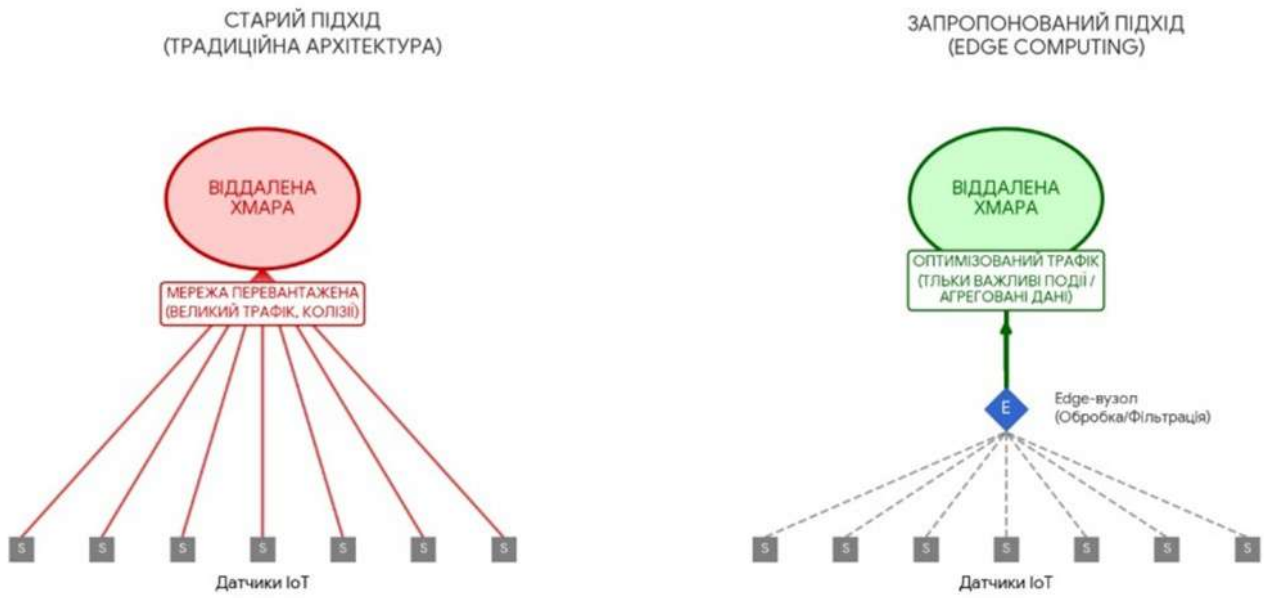


Рис.1. Порівняння архітектури IoT мереж
(традиційна хмарна та з періферійними обчисленнями)

Розроблений радіомодуль для системи передачі цифрових даних має наступні особливості.

1) Частотний діапазон: для забезпечення максимальної дальності зв'язку використано безліцензійні субгігагерцові смуги *ISM*-діапазону (наприклад, 868 МГц).
2) Адаптивний алгоритм передачі: радіоблок активується лише тоді, коли поточне цифрове значення параметра на виході датчика відхиляється від прогнозованого на величину, більшу за встановлений поріг похибки.
3) Локальне стиснення: використання просторово-часової агрегації зменшує розрядність пакетів даних.

Імітаційне моделювання розробленого радіомодуля у середовищі *MATLAB* підтвердило високу ефективність запропонованого підходу. Впровадження інтелектуальної фільтрації безпосередньо в радіоблоці дозволяє зменшити обсяг переданого трафіку на (70–85)%. Таке зниження активності передавача зменшує ймовірність колізій у топологіях типу «зірка» та збільшує термін автономної роботи пристрою від однієї батареї у 1.5–2 рази.

Проектування радіомодулів із підтримкою периферійної обробки є важливим для побудови масштабних та енергоефективних бездротових систем. Розроблений пристрій забезпечує надійний контроль параметрів при мінімальних витратах енергії і може бути інтегрований у промислові рішення для автоматизації та екологічного моніторингу.

Список використаних джерел

1. Singh A. K., Kumar N. A Novel Hybrid Compression Technique for IoT Medical Data over Low Bandwidth Channels. Multimedia Tools and Applications. 2022. Vol. 81. P. 4567–4585.
2. Sun L., Du Q. Energy-Efficient Data Aggregation for UAV-Assisted IoT Networks. IEEE Wireless Communications Letters. 2021. Vol. 10, No. 9. P. 1984–1988.
3. Tan H., Wang X. Multi-level Data Aggregation and Compression in Edge-Cloud IoT Systems. Future Generation Computer Systems. 2023. Vol. 141. P. 34–45.
4. Wang Y., Chen H. Spatial-Temporal Data Compression for Massive IoT Connectivity. IEEE Communications Magazine. 2022. Vol. 60, No. 1. P. 56–62.

УДК 621.391.8

Р. С. Крупина
А. О. Осіпчук
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОГРАМНИЙ ІНТЕРФЕЙС СИСТЕМИ МОНІТОРИНГУ РАДІОЕЛЕКТРОННОЇ ОБСТАНОВКИ В СЕРЕДОВИЩІ MATLAB

Сучасний розвиток бездротових систем зв’язку, програмно-визначених радіосистем та засобів радіоелектронної боротьби зумовлює необхідність створення ефективних систем моніторингу радіоелектронної обстановки (РЕО). Контроль радіочастотного спектра є важливим для забезпечення електромагнітної сумісності, виявлення несанкціонованих випромінювань, оцінювання завантаженості частотних діапазонів та оперативного реагування на радіоелектронні загрози. Особливу актуальність мають програмні комплекси, здатні виконувати спектральний аналіз сигналів у режимі реального часу та забезпечувати зручний графічний інтерфейс оператора.

У роботі розглянуто підхід до побудови програмного інтерфейсу системи моніторингу РЕО в середовищі MATLAB із використанням засобів цифрової обробки сигналів та інтерактивної візуалізації. Запропонована структура системи включає антенно-фідерний тракт, модуль аналого-цифрового перетворення, блок цифрової обробки сигналів, модуль класифікації, систему збереження даних та графічний інтерфейс користувача. Основою програмної реалізації є MATLAB App Designer, який дозволяє створювати багатовіконні інтерфейси з інтерактивними елементами керування та засобами відображення спектральної інформації.

Для аналізу сигналів використано алгоритм швидкого перетворення Фур’є з подальшим усередненням спектрів та адаптивним пороговим виявленням локальних максимумів. Такий підхід забезпечує достатню точність виявлення сигналів при помірних обчислювальних витратах. У роботі використовується FFT-аналіз із розміром перетворення 2048 відліків, що забезпечує компроміс між частотною роздільною здатністю та швидкодією системи.

Програмний інтерфейс реалізує відображення спектра сигналу, спектрограми та waterfall-діаграми у режимі реального часу. Для автоматичного виявлення сигналів використовується функція findpeaks із адаптивним порогом відносно рівня шуму. Додатково передбачено можливість застосування низькочастотної, високочастотної та смугової фільтрації сигналів перед виконанням спектрального аналізу. Це дозволяє підвищити якість виявлення слабких сигналів у присутності завад.

Запропонований інтерфейс забезпечує відображення основних параметрів виявлених сигналів, зокрема частоти, рівня потужності, співвідношення сигнал/шум та кількості активних піків у спектрі. Реалізовано механізм накопичення та усереднення спектральних кадрів, що дозволяє зменшити випадкові шумові коливання та підвищити стабільність спектральної оцінки. Для підтримки роботи в режимі реального часу використано таймери оновлення інтерфейсу та оптимізовані процедури обробки даних.

Перевагою використання MATLAB є наявність спеціалізованих інструментів для цифрової обробки сигналів, візуалізації та взаємодії з програмно-визначеними радіосистемами. Використання Signal Processing Toolbox, Communications Toolbox та Instrument Control Toolbox дозволяє реалізувати комплексну систему спектрального моніторингу без необхідності залучення великої кількості сторонніх бібліотек. Крім того, MATLAB забезпечує швидке прототипування алгоритмів та можливість подальшої генерації C/C++ коду для вбудованих систем. Підтвердженням доцільності є використання FFT-аналізу та інтерактивних MATLAB-інтерфейсів для задач моніторингу РЕО. Запропонований програмний інтерфейс може бути використаний як основа для створення систем спектрального контролю, навчальних комплексів, засобів аналізу радіочастотної обстановки та дослідницьких платформ у сфері цифрової обробки сигналів.

Список використаних джерел:

1. ITU-R SM.1392. Essential requirements for a spectrum monitoring system for developing countries.
2. MATLAB Signal Processing Toolbox Documentation. MathWorks.
3. MATLAB App Designer Documentation. MathWorks.
4. FFT-Based Spectrum Analysis for SDR Systems // IEEE Communications Magazine.

УДК 621.396.4

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

ПРОЄКТУВАННЯ ГІБРИДНОЇ АРХІТЕКТУРИ ЗАХИСТУ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІД DDOS-АТАК ПРИКЛАДНОГО РІВНЯ

Сучасні телекомунікаційні мережі, що забезпечують функціонування критичної інфраструктури, урядових порталів та корпоративного сектора, базуються на глибоко розподіленій хмаро-орієнтованій архітектурі. Незважаючи на впровадження гнучких моделей програмно-конфігурованих мереж (SDN) та віртуалізації мережевих функцій (NFV), проблема забезпечення їхньої безперервної доступності залишається гострою. Спостерігається стійка тенденція до зміщення вектору кіберзагроз від класичних об'ємних атак на мережевому та транспортному рівнях (L3/L4) до високоінтелектуальних розподілених атак на відмову в обслуговуванні (DDoS) на рівні додатків (L7 моделі OSI). Такі атаки майстерно імітують поведінку легітимних користувачів, обходячи традиційні засоби периметрального захисту, та призводять до катастрофічного виснаження обчислювальних ресурсів цільових серверів. До таких загроз, зокрема, належать низькошвидкісні атаки типу Slowloris, HTTP GET/POST флуд та виснаження сесій на етапі криптографічного TLS-узгодження (TLS Renegotiation), які практично неможливо виявити за допомогою стандартного аналізу TCP/UDP-заголовків.

У роботі здійснено комплексний аналіз проблематики прикладних DDoS-атак та обґрунтовано необхідність відмови від монолітних рішень на користь багаторівневих систем протидії. Запропоновано інноваційну гібридну архітектуру безпеки, яка синергетично поєднує можливості інтелектуальних екранів прикладного рівня (WAF), телекомунікаційних алгоритмів керування чергами для динамічного обмеження пропускної здатності та надійних механізмів поведінкової верифікації клієнтського середовища. Такий підхід дозволяє не лише фільтрувати паразитний трафік, але й здійснювати предиктивний аналіз аномалій на основі патернів взаємодії з вебдодатками. Для легітимізації клієнтів застосовано багаторівневий механізм, що включає перевірку виконання JavaScript-коду на стороні браузера (JS Challenge) та

алгоритми лімітування інтенсивності запитів (Rate Limiting) на базі математичної моделі маркерного кошика (Token Bucket). Окрім цього, архітектура передбачає безшовну інтеграцію з системами класу SIEM (Security Information and Event Management), що забезпечує централізований збір телеметрії, кореляцію подій безпеки та ретроспективний аналіз інцидентів.

Практичну реалізацію та експериментальне моделювання розробленої архітектури було проведено на базі спеціально створеного ізольованого телекомунікаційного стенда. Спроєктовано відмовостійкий замкнутий контур глибокої фільтрації, в основу якого покладено взаємодію граничного маршрутизатора операторського класу MikroTik (під управлінням RouterOS v7) та зворотного проксі-сервера Nginx з інтегрованим WAF-модулем ModSecurity. Ключовим інженерним досягненням стала автоматизація процесу ідентифікації прикладних аномалій: при виявленні шкідливих запитів на рівні L7 система миттєво генерує керуючі команди через захищений REST API (новий функціонал ядра RouterOS v7) для апаратного відкидання паразитних пакетів ще на етапі премаршрутизації у підсистемі Firewall Raw. Завдяки динамічному додаванню IP-адрес ботнетів до чорних списків (Address-Lists) шкідливий трафік відкидається (Drop) до потрапляння в ресурсоємний механізм відстеження з'єднань (Connection Tracking). Це повністю унеможливило виснаження пам'яті та процесорного часу (CPU) мережевого ядра.

Отримані під час тестування результати підтвердили виняткову ефективність запропонованої моделі. Зафіксовано надшвидке відновлення телеметричних показників сервера після початку атаки та гарантоване збереження стабільної пропускної здатності для легітимних абонентів. Інструментальні вимірювання показали, що час реакції автоматизованого контуру на нові вектори атак не перевищує кількох сотень мілісекунд. Для протидії гіпермасштабним розподіленим атакам, об'єм яких перевищує ємність фізичного лінку, розроблена система здатна ескалювати блокування на рівень вищестоящого магістрального провайдера за допомогою протоколу BGP (механізми Blackholing/FlowSpec). Розроблена гібридна інфраструктурна модель є інженерно та економічно збалансованим рішенням, повністю готовим до імплементації в сучасних мережах рівня Enterprise та ISP, що суттєво підвищує загальний рівень відмовостійкості національного кіберпростору.

УДК 621.396.4

М.М. Купчук, С.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА ТА АНАЛІЗ ЕФЕКТИВНОСТІ LORAWAN-МЕРЕЖІ ДЛЯ МОНІТОРИНГУ МУНІЦИПАЛЬНОЇ ІНФРАСТРУКТУРИ

Управління сучасним мегаполісом в умовах безперервної урбанізації та експоненційного зростання навантаження на комунальні системи вимагає невідкладного впровадження концепції «Розумне місто» (Smart City). Історично сформовані методи моніторингу житлово-комунального господарства, що базуються на періодичному ручному обході лічильників, демонструють критично низьку техніко-економічну ефективність. Це призводить до системних похибок у білінгу, неоптимізованої логістики комунального транспорту та неможливості оперативного виявлення аварійних ситуацій на магістралях. Для вирішення проблеми фрагментованості даних необхідним є розгортання енергоефективних бездротових мереж великого радіусу дії (LPWAN) у неліцензованому субгігагерцовому діапазоні. З-поміж існуючих рішень стандарт LoRaWAN (регіональна специфікація EU868) виступає найбільш збалансованою технологією для побудови єдиної муніципальної телеметричної інфраструктури.

У роботі здійснено комплексне проєктування апаратно-програмного комплексу моніторингу міської інфраструктури. Проведено детальний розрахунок бюджету радіолінії (Link Budget) та просторових зон Френеля, що дозволило теоретично обґрунтувати параметри покриття та оптимальну висоту розміщення базових станцій. В межах практичної реалізації проєкту було розгорнуто шлюз на базі апаратної платформи MikroTik (серія wAP LR8) під управлінням операційної системи RouterOS. Для централізованого управління маршрутизацією та автентифікацією вузлів розгорнуто сервер мережі LoRa Network Server (LNS). Захист даних на всьому шляху від сенсора до сервера реалізовано за допомогою наскрізного шифрування алгоритмом AES-128 (сесійні ключі NwkSKey та AppSKey). У рамках формування екосистеми кінцевих вузлів було досліджено специфіку використання пристроїв різних класів: високоавтономних сенсорів класу A (Class A) для збору показників водопостачання та актуаторів класу C (Class C) для безперервного керування муніципальним освітленням

без затримок. Крім того, розроблено спеціалізований програмний декодер (Payload Formatter) мовою JavaScript. Застосування такого підходу забезпечило безшовну трансформацію бінарних радіопакетів від кінцевих вузлів у структуровані масиви даних формату JSON, що дозволило інтегрувати систему з сучасними платформами аналітики та візуалізації InfluxDB та Grafana.

Ефективність та життєздатність запропонованих рішень підтверджено серією натурних експериментальних досліджень в агресивних умовах щільної міської забудови м. Києва. Встановлено, що використання фактора розширення спектра SF12 гарантує ультимативну завадостійкість і забезпечує стабільну передачу телеметрії на відстані до 4 км. Проте, для забезпечення масштабованості мережі та оптимізації ефірного часу (Airtime) активовано механізм адаптивної швидкості передачі даних (Adaptive Data Rate, ADR). Це дозволило системі динамічно знижувати SF до оптимальних значень для вузлів із високим рівнем сигналу (RSSI/SNR). Критично важливим результатом стало підтвердження можливості стабільного збору даних із важкодоступних локацій, зокрема з підвальних приміщень та залізобетонних інженерних колодязів. Більше того, налаштовані інформаційні дашборди у системі Grafana були доповнені модулем автоматичного сповіщення (Alerting), який у разі виявлення аномальних відхилень телеметрії (наприклад, різкого падіння тиску води або несанкціонованого відкриття люка) миттєво генерує тривожні сповіщення (Webhooks) для аварійних бригад. Розрахунки енергетичного балансу довели, що кінцеві сенсорні вузли здатні функціонувати у повністю автономному режимі понад 10 років за умови використання літій-тіонілхлоридних ($Li-SOCl_2$) елементів живлення.

Оцінка техніко-економічної доцільності переконливо продемонструвала фінансову перевагу розгортання власної LoRaWAN-інфраструктури у порівнянні з використанням комерційних стільникових мереж стандарту NB-IoT. Повна відсутність абонентської плати за використання радіочастотного спектра, відсутність залежності від покриття мобільних операторів, мінімальні капітальні (CAPEX) та операційні (OPEX) витрати, а також низька вартість кінцевого обладнання роблять розроблену систему високорентабельним і масштабованим інструментом для глобальної цифровізації міського господарства.

УДК 621.391

І.О. Луковецький, М.Б. Гумен
Національний університет
«Київський авіаційний інститут», м. Київ

БЕЗДРОТОВА ТЕЛЕМЕТРИЧНА СИСТЕМА МОНІТОРИНГУ БІОЛОГІЧНИХ ПОКАЗНИКІВ ЛЮДИНИ

Вступ. Сучасна медицина характеризується стрімким розвитком технологій дистанційного моніторингу здоров'я, що дозволяють здійснювати безперервне спостереження за життєво важливими показниками пацієнтів поза межами медичних закладів.

Телеметричні системи моніторингу біологічних показників відіграють все більш важливу роль у профілактиці, діагностиці та лікуванні різноманітних захворювань, особливо в умовах старіння населення та зростання поширеності хронічних захворювань серцево-судинної системи.

Актуальність проблеми зумовлена зростаючою потребою в доступних та ефективних засобах домашнього моніторингу здоров'я, що підтверджується світовими тенденціями розвитку телемедицини та персоналізованої медицини. Традиційні методи моніторингу, що вимагають регулярних відвідувань медичних закладів, часто не забезпечують достатньої частоти спостережень для своєчасного виявлення критичних змін стану пацієнта.

Основна частина. Архітектура розробленої телеметричної системи базується на мікроконтролері ESP32-S3 з інтегрованими Wi-Fi та Bluetooth модулями, що забезпечує оптимальний баланс між функціональністю та енергоспоживанням. Обґрунтований вибір датчиків включає оптичний сенсор MAX30102 для вимірювання пульсу та сатурації крові, цифровий термометр DS18B20 для температури тіла та акселеометр LSM6DS3 для контролю фізичної активності. Така конфігурація забезпечує комплексний моніторинг основних біологічних показників з медичною точністю.

Система живлення з літій-іонним акумулятором забезпечує автономність роботи до 8-16 діб залежно від інтенсивності моніторингу.

Розроблене програмне забезпечення включає ефективні алгоритми збору та обробки біологічних сигналів з використанням цифрової фільтрації та методів машинного навчання. Протокол передачі даних

забезпечує надійну доставку медичної інформації з багаторівневим шифруванням та адаптивним управлінням якістю обслуговування.

Мобільний додаток з інтуїтивним інтерфейсом дозволяє користувачам легко контролювати стан свого здоров'я та отримувати своєчасні сповіщення про критичні зміни.

Експериментальні дослідження підтвердили медичну придатність розробленої системи. Точність вимірювання частоти серцевих скорочень становить ±2.1 уд/хв, насиченості крові киснем - ±2.3%, температури тіла - ±0.08°C, що відповідає вимогам міжнародних стандартів для медичного обладнання. Дослідження характеристик бездротового зв'язку показали ефективну дальність до 45 метрів для Bluetooth LE та 80 метрів для Wi-Fi в приміщеннях із автоматичним відновленням з'єднання при тимчасових розривах.

Середнє споживання системи становить 6.6 мА в стандартному режимі та 2.3 мА в економному режимі, що забезпечує автономність роботи 8.3 та 16.2 доби відповідно. Система автоматично адаптує частоту моніторингу залежно від стабільності показників пацієнта та рівня заряду батареї.

Порівняльний аналіз з існуючими аналогами виявив конкурентні переваги розробленої системи. При вартості $150-200 система забезпечує точність, порівняну з професійним медичним обладнанням вартістю $2000-5000, та значно перевершує споживчі фітнес-трекери за медичною точністю. Відкрита архітектура та підтримка медичних стандартів забезпечують можливість інтеграції з різними медичними інформаційними системами.

Система класифікується як медичний пристрій класу BF з мінімальними ризиками для користувачів. Ергономічна конструкція забезпечує комфортне тривале носіння без негативного впливу на здоров'я.

Заключна частина. Розроблена телеметрична система має значний потенціал для практичного впровадження в системі охорони здоров'я України. Система може використовуватися для домашнього моніторингу хронічних хворих, післяопераційного спостереження, профілактичних обстежень та телемедичних консультацій.

Створена телеметрична система представляє собою інноваційне технічне рішення, що може внести значний вклад у розвиток цифрової медицини та покращення якості медичної допомоги населенню.

УДК 621.396.4

А.М. Маняхін, В.П. Климчук
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ МУЛЬТИСЕРВІСНОЇ БЕЗДРОТОВОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ АВІАЦІЙНИХ ОБ'ЄКТІВ

Сучасні авіаційні інфраструктурні комплекси, такі як міжнародні аеропорти, функціонують в умовах надвисокої щільності інформаційних потоків і висувають жорсткі вимоги до надійності, масштабованості та безпеки телекомунікаційних мереж. Специфіка пасажирських терміналів, що охоплюють значні площі та характеризуються складною архітектурною геометрією, створює надзвичайно агресивне середовище для поширення високочастотних радіохвиль. Наявність масивних залізобетонних перекриттів, металізованих конструкцій, ескалаторних зон та енергозберігаючого скління призводить до інтенсивного багатопроменевого перевідбиття, дифракції та значного загасання сигналів. У таких умовах класичні емпіричні моделі поширення радіохвиль є обмежено придатними, що зумовлює актуальність розробки нових підходів до проєктування мультисервісних бездротових мереж високої щільності на базі сучасних стандартів сімейства IEEE 802.11ax (Wi-Fi 6).

У роботі здійснено всебічний аналіз вимог до мережевої інфраструктури авіаційних об'єктів на прикладі Міжнародного аеропорту «Бориспіль». Досліджено структуру інформаційних потоків та розроблено архітектурні рішення для нівелювання пікових мікросплесків (micro-bursts) трафіку, які виникають під час масового скупчення пасажирів у зонах реєстрації та очікування. Для оптимізації спектральної ефективності запропоновано використання технології ортогонального частотного мультиплексування (OFDMA) та просторового рознесення MU-MIMO. Для забезпечення безперервності зв'язку під час переміщення абонентів великими площами термінала обґрунтовано необхідність імплементації протоколів безшовного роумінгу IEEE 802.11r/k/v. Крім того, розроблено політики якості обслуговування (QoS) з метою жорсткої пріоритетизації критично важливого голосового (VoIP) та службового диспетчерського трафіку над загальними запитами гостьових клієнтів.

Особливу увагу приділено побудові безкомпромісного ешелону інформаційної безпеки та логічній сегментації. Запропоновано комплексний підхід, який базується на впровадженні криптографічного стандарту WPA3-Enterprise з автентифікацією через RADIUS-сервер (802.1X), захисті службових кадрів управління відповідно до специфікації IEEE 802.11w, а також механізмах жорсткої ізоляції клієнтів (Client Isolation) всередині гостьових сегментів мережі. Ізоляція службового, пасажирського та IoT-трафіку (інтернет речей) реалізується за допомогою технологій VLAN та віртуальної маршрутизації VRF.

Ефективність та життєздатність прийнятих інженерних рішень верифіковано шляхом предиктивного комп'ютерного моделювання (Predictive Site Survey) в спеціалізованому програмному середовищі Ekahau Pro. Створена 3D-модель об'єкта дозволила точно врахувати радіофізичні властивості (коефіцієнти загасання) всіх конструкційних матеріалів термінала та оптимізувати розміщення точок доступу з урахуванням діаграм спрямованості їхніх антен. Результати симуляції підтвердили досягнення еталонного рівня радіопокриття не гірше -65 дБм та співвідношення сигнал/інтерференція+шум (SINR) на рівні не менше 20 дБ у всіх критичних зонах. Це гарантує стабільну роботу терміналів із використанням високорівневих схем квадратурної амплітудної модуляції (QAM). Окрім цього, у роботі розроблено базові алгоритми конфігурації комутаційного обладнання та бездротових контролерів у середовищі Cisco IOS, що підтверджує практичну готовність проєкту до імплементації.

Математично доведено, що синергія протоколів динамічної маршрутизації OSPF (у поєднанні з протоколом швидкого виявлення збоїв BFD) та технології апаратного дублювання контролерів (High Availability SSO) дозволяє досягти часу збіжності мережі на рівні мілісекунд та безпрецедентного показника доступності сервісів на рівні 99,999%. Багатофакторна оцінка надійності та техніко-економічне обґрунтування продемонстрували, що розгортання єдиної уніфікованої мультисервісної архітектури замість побудови кількох розрізнених фізичних мереж кардинально знижує як капітальні (CAPEX), так і операційні (OPEX) витрати підприємства. Результати дослідження можуть бути успішно екстрапольовані на інші об'єкти критичної інфраструктури зі схожими вимогами до якості та безпеки бездротового зв'язку.

УДК 621.396.2

М.М. Марєєв, С.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ СИСТЕМИ ШИРОКОСМУГОВОГО РАДІОДОСТУПУ ДЛЯ ПОДОЛАННЯ ПРОБЛЕМИ «ОСТАННЬОЇ МИЛІ» У ВІДДАЛЕНИХ РАЙОНАХ

Забезпечення високошвидкісним телекомунікаційним сервісом абонентів у віддалених населених пунктах залишається однією з найскладніших інженерних проблем сучасності, відомою як проблема «останньої милі». В умовах щільної урбанізованої забудови мегаполісів цей виклик успішно вирішується шляхом розгортання дротових оптичних топологій (xPON, FTTB). Однак у сільській місцевості з її екстремально низькою щільністю абонентів та значною просторовою розмежованістю класичні дротові підходи демонструють повну техніко-економічну неспроможність через надмірно тривалий термін окупності капітальних інвестицій. У цьому контексті безальтернативним та фінансово виправданим рішенням є розгортання мереж провайдерів бездротового доступу (WISP), здатних забезпечити гарантовану якість обслуговування (QoS) на значних територіях.

У роботі здійснено комплексне проєктування апаратно-програмної інфраструктури бездротової мережі для віддаленого району. Для побудови магістрального радіорелейного каналу (Backhaul) обґрунтовано використання топології «точка-точка» (PtP) із застосуванням вузькоспрямованих параболічних антен, тоді як для забезпечення абонентського доступу спроєктовано кластер базових станцій за топологією «точка-багатоточка» (PtMP). Використання технології просторового мультиплексування MIMO 2x2 у неліцензованому діапазоні 5 ГГц дозволило суттєво підвищити пропускну здатність сектора. Для забезпечення рівномірного покриття та обслуговування великої кількості абонентських терміналів на базових станціях передбачено використання ізольованих секторних антен із кутом випромінювання 90°–120°. З метою мінімізації міжканальної інтерференції та дотримання регуляторних норм щодо використання радіочастотного спектра застосовано механізми динамічного вибору частоти (DFS) та автоматичного регулювання потужності передавачів (ATPC).

Особливу увагу приділено логічній топології на базі операційної системи RouterOS: впровадження протоколу динамічної маршрутизації OSPF забезпечило високу збіжність мережі та автоматичне резервування магістральних каналів зв'язку. Водночас застосування тунельного протоколу PPPoE у поєднанні з L2-сегментацією трафіку через віртуальні локальні мережі (VLAN) дозволило реалізувати криптографічно захищену авторизацію користувачів, ізоляцію широкомовних доменів та прозорий білінговий облік. Для подолання проблеми несправедливого розподілу смуги пропускання (Bandwidth Starvation) розроблено багаторівневі механізми управління трафіком на базі ієрархічних черг HTB та алгоритму PCQ. Це гарантувало пріоритетну доставку чутливих до затримок сервісів, зокрема відеоконференцзв’язку та IP-телефонії, навіть за умов пікових навантажень на сектор.

Валідацію проєктних рішень виконано шляхом предиктивного геоінформаційного моделювання на основі цифрових матриць рельєфу SRTM, що інструментально підтвердило фізичну здійсненність стабільного радіопокриття цільової зони забудови з урахуванням чистих зон Френеля. Порівняльний аналіз методів доступу до середовища довів беззаперечну технічну перевагу використання пропрієтарного протоколу поллінгу TDMA (Nv2) над стандартним механізмом CSMA/CA. Впровадження Nv2 повністю нівелювало проблему «прихованого вузла», ліквідувало колізії в радіоефірі та забезпечило жорстко детермінований рівень затримок шляхом виділення кожному клієнтському пристрою (CPE) фіксованих часових слотів (Time Slots). З метою безперервної експлуатації мережі сформовано стратегію централізованого моніторингу за допомогою протоколу SNMP та програмного комплексу The Dude.

Проведене дослідження підтверджує, що розроблена система широкосмугового радіодоступу є цілісним, технічно досконалим та економічно рентабельним інструментом для ліквідації цифрової нерівності. Запропонована архітектура повністю відповідає сучасним вимогам до надійності, а закладені алгоритми управління трафіком роблять її максимально адаптивною, гарантуючи абонентам стабільний доступ до глобальної мережі незалежно від складності географічного ландшафту.

УДК 004.8:621.39

Р.М. Микитенко[1], В.О. Гнатюк[1,2]
[1]Державний університет
«Київський авіаційний інститут», м. Київ
[2]Державний науково-дослідний інститут
технологій кібербезпеки та захисту інформації, м. Київ

МОДЕЛЬ ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ РЕСУРСАМИ В ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ

Стрімкий розвиток сучасних телекомунікаційних мереж, зокрема впровадження технологій 5G/6G та концепцій програмно-конфігурованих мереж (SDN) і віртуалізації мережевих функцій (NFV), призводить до експоненційного зростання обсягів трафіку та підвищення вимог до якості обслуговування (QoS). Традиційні статичні або евристичні методи управління ресурсами не здатні ефективно адаптуватися до різких коливань навантаження та гетерогенності мережевих сервісів у режимі реального часу. У зв'язку з цим, застосування методів штучного інтелекту (ШІ) та алгоритмів машинного навчання для розробки інтелектуальних моделей розподілу пропускної здатності, маршрутизації та управління чергами є надзвичайно актуальним завданням, що дозволяє автоматизувати прийняття рішень та оптимізувати роботу мережі.

Мета дослідження полягає у підвищенні ефективності функціонування телекомунікаційної мережі шляхом розробки та впровадження моделі інтелектуального управління ресурсами на базі алгоритмів машинного навчання. Для досягнення поставленої мети було вирішено такі *завдання*: проаналізувати сучасні методи, протоколи передачі даних та технології управління ресурсами в мультисервісних телекомунікаційних мережах; розробити математичну та структурно-функціональну модель інтелектуального управління мережевими ресурсами з використанням обраного алгоритму машинного навчання; здійснити програмну реалізацію та комп'ютерне моделювання запропонованої системи у вибраному середовищі симуляції; провести порівняльну оцінку ефективності розробленої моделі з класичними методами на основі ключових показників якості мережі (затримка, пропускна здатність, втрати пакетів).

У ході дослідження здійснено системний аналіз сучасних тенденцій розвитку телекомунікаційних мереж (зокрема транспортних сег-

ментів 5G/6G) та методів забезпечення якості обслуговування (QoS). Встановлено, що перехід до архітектур програмно-конфігурованих мереж (SDN) відкриває можливості для централізованого управління, проте класичні евристичні та статичні протоколи маршрутизації не здатні ефективно адаптуватися до високодинамічного трафіку. Обґрунтовано доцільність застосування методів штучного інтелекту для автоматизації цих процесів.

Розроблено математичну та структурно-функціональну модель інтелектуального управління ресурсами. Задачу розподілу пропускної здатності та вибору маршрутів формалізовано як максимізацію загальної корисності мережі. Для її вирішення в режимі реального часу обґрунтовано вибір алгоритму глибокого навчання з підкріпленням (DRL). Запропоновано архітектуру, яка безшовно інтегрує DRL-агента з площиною управління SDN-контролера.

Виконано програмну реалізацію запропонованої системи з використанням середовища емуляції мережі Mininet, подієво-орієнтованого SDN-контролера Ryu та фреймворку для тензорних обчислень PyTorch. Сформовано комплексну функцію винагороди, яка враховує затримки, пропускну здатність та втрати пакетів. Розроблено репрезентативні сценарії моделювання (включаючи імітацію eMBB та URLLC трафіку) для перевірки мережі в умовах пікових та імпульсних навантажень.

Проведено комп'ютерне моделювання та порівняльну оцінку ефективності розробленої моделі з класичними методами маршрутизації (OSPF, ECMP). Доведено, що навчений DRL-агент здатний превентивно реагувати на загрози перевантаження мережі: досягнуто зменшення середньої наскрізної затримки для критичного трафіку на 65–70% (стабілізація на рівні 7–12 мс); підвищено ефективність утилізації каналів зв'язку ядра мережі до 88–90%; знижено коефіцієнт втрат пакетів на 80–90% порівняно з реактивними методами управління.

Визначено перспективи практичного впровадження. Розроблена модель довела свою ефективність у симуляційному середовищі та має високий потенціал для інтеграції в реальні інфраструктури операторів зв'язку (на рівні ядра мережі або Edge Computing). Подальшим етапом розвитку проєкту є апаратна апробація запропонованих алгоритмів SDN-маршрутизації на базі спеціалізованого обладнання, зокрема в умовах лабораторій Центру технологій KAI Huawei Excellence Center та лабораторії мобільного зв'язку Vodafone.

УДК 654.9

Ю.В. Михайлик, А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА МОНІТОРИНГУ І ПЕРЕДАЧІ МЕТЕОРОЛОГІЧНИХ ДАНИХ

Метою роботи є розробка системи моніторингу та передачі метеорологічних даних, зокрема пристрою, що буде вимірювати атмосферні показники та передавати їх на смартфон, планшет або віддалений сервер.

Актуальність роботи полягає у тому, що в наш час існує потреба в автоматичному спостереженні за погодними умовами, у тому числі використовуючи вимірювання атмосферних показників. На основі такого спостереження та вимірювання можна передбачити погоду.

З переліку багатьох показників, що є необхідними для спостереження та передбачення погодних умов, відзначимо температуру, вологість, атмосферний тиск, швидкість вітру та ультра фіолетовий індекс.

Основою системи моніторингу та передачі метеорологічних даних є метеостанція, що складається з вимірювальних пристроїв (датчиків), та передавача, за допомогою якого здійснюється передача виміряних метеоданих на певну відстань.

За принципом формування і передачі даних існують аналогові та цифрові системи.

За методами експлуатації існують дорожні, лісові, гідрологічні та побутові метеорологічні системи. Усі вони мають своє специфічне призначення та різні принципи роботи.

Розробка системи моніторингу та передачі метеоданих включає такі етапи: побудова структурної схеми, вибір елементів системи, розробка програмного забезпечення.

Структурна схема містить елементи, з яких складається система, та враховує з’єднання між ними.

Елементами системи моніторингу та передачі метеоданих є: плата Arduino Uno, макетна плата, датчик температури та вологості повітря, датчик тиску, годинник реального часу, дисплей, та елемент живлення (акумулятор).

Для повноцінної роботи системи моніторингу та передачі метеорологічних даних написано програму, що здійснює обробку метеоданих та їхню передачу на дисплей.

Пристрій передачі даних на певну відстань містить два компоненти.

Передача даних на невелику відстань здійснюється за допомогою модуля *Bluetooth*.

Передача даних на велику відстань здійснюється за допомогою радіопередавача, який складається з блоку управління, синтезатора частот, модулятора, підсилювача потужності радіосигналу та антени. Цей передавач формує високочастотний радіосигнал та здійснює передачу метеорологічної інформації на відстань орієнтовно до 100 кілометрів.

Принцип роботи передавача полягає у використанні іоносферного поширення електромагнітних хвиль. Антена передавача направлена вертикально вгору та здійснює перетворення модульованого сигналу в радіохвилі. Ці радіохвилі відбиваються від іоносфери та повертаються на землю.

Для модуляції високочастотного сигналу обрано метод *Quadrature Phase Shift Keying* (*QPSK*). Ця модуляція є відносно низькошвидкісною, але цього достатньо для передачі метеоданих, які оновлюються з періодичністю не менше ніж 1 секунда. У той же час модуляція *QPSK* забезпечує завадостійкість передачі даних в умовах перешкод і шумів штучного та природного походження.

Перевагами розробленої системи є зручність, компактність, автономність та мобільність.

Висновки.

У даній роботі було розроблено систему моніторингу та передачі метеорологічних даних на основі аналізу існуючих систем такого призначення, описано складові частини та програмне забезпечення метеостанції, розглянуто спосіб передачі метеорологічної інформації на велику відстань за допомогою радіопередавача, наведено переваги розробленої системи.

УДК 621.391

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

КОНФІДЕНЦІЙНІСТЬ ТА АНОНІМНІСТЬ КОРИСТУВАЧІВ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

Ми звикли вважати локальну домашню Wi-Fi мережу безпечним простором, особливо якщо вона захищена паролем. Але реальність диктує інші правила. Навіть найновіший протокол WPA3 має архітектурні вразливості (наприклад, атаки сімейства Dragonblood та downgrade-вразливості перехідного режиму), а поширений WPA2 зламується за лічені години. Завдяки сучасним PMKID-атакам та потужності звичайних відеокарт, паролі з низькою ентропією більше не є перешкодою. До того ж, атаки типу «людина посередині» (Evil Twin, ARP-spoofing) у публічному бездротовому середовищі взагалі не вимагають зламу криптографії — достатньо фізичної близькості зловмисника до радіодіапазону, щоб перехопити трафік і критично порушити конфіденційність даних користувача.

Проте захист лише канального рівня не вирішує проблему комплексно. Сучасний інтернет функціонує як середовище тотального і цілком легального збору даних. Навіть за умови використання надійного WPA3 та ідеального наскрізного шифрування (E2EE) у месенджерах, метадані продовжують розкривати особу користувача. Витоки через DNS, WebRTC, фінгерпринтинг браузера (canvas, WebGL) та телеметрія клавіатур передають інформацію ще до того, як вона буде зашифрована. Тут ми стикаємося з «дилемою балаклави»: спроба сховатися за допомогою Tor чи специфічних VPN парадоксальним чином виділяє користувача з натовпу. Сам інструмент анонімізації стає унікальним цифровим слідом, який фіксується провайдерами та системами аналітики.

Щоб розірвати це коло, було побудувано формальну модель загроз для типової домашньої Wi-Fi мережі. Адаптовано методологію STRIDE/DREAD, яка традиційно застосовується для тестування

корпоративного програмного забезпечення, під потреби звичайної фізичної особи. Проаналізувавши 13 компонентів архітектури, було виявилено 35 специфічних загроз. Характерно, що 43% з них належать до категорії Information Disclosure. Тобто головна небезпека сьогодні полягає не в активному хакерському втручанні, а в пасивному зборі метаданих.

Ефективний захист у таких умовах не може зводитися до встановлення одного «безпечного» додатка. Я пропоную багаторівневу стратегію (defense in depth), яка діє незалежно на чотирьох рівнях: користувач, пристрій, бездротова мережа та інтернет. На рівні Wi-Fi це вимагає переходу на WPA3-Only або WPA2 з обов'язковим PMF, повної відмови від WPS, ізоляції вразливих IoT-пристроїв у гостьовій мережі та зміни заводських налаштувань маршрутизатора. На вищих рівнях захист будується через жорстке розділення цифрових ідентичностей (compartmentalization), використання шифрованого DNS (DoH/DoT) для приховування запитів від провайдера та свідомий вибір засобів комунікації.

Жодна операційна система чи мережевий протокол не дають стовідсоткової безпеки «з коробки». Лише їх узгоджена композиція дозволяє зберегти приватність особистих даних в мережі.

УДК 627.7

Д.Ю. Німко, А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА ЛОКАЛІЗАЦІЇ МОБІЛЬНОГО АБОНЕНТА

Розвиток сучасних інформаційно-комунікаційних технологій вимагає точного та швидкого визначення координат користувачів. Аналіз систем локалізації рухомих об’єктів свідчить про стрімке зростання попиту на послуги, що базуються на визначенні місцезнаходження (*Location-Based Services*). Для побудови систем локалізації мобільного абонента застосовується або класична стільникова система визначення місцезнаходження мобільного абонента, або глобальні супутникові системи локалізації об’єкта. Кожен із цих підходів має свої обмеження в умовах щільної міської забудови або всередині приміщень. Це зумовлює необхідність розробки комплексних систем локалізації, які здатні адаптуватися до умов конкретного радіо-середовища.

Ефективне розгортання подібних сервісів спирається на сучасні методи локалізації мобільного абонента. Безпосередня локалізація в стільниковій системі найчастіше використовує три ключові методи вимірювання параметрів радіосигналу: метод часу приходу *Time Of Arrival* (*TOA*), метод різниці часу приходу *Time Difference Of Arrival* (*TDOA*) та метод кута приходу *Angle Of Arrival* (*AOA*) від базових станцій. З іншого боку, позиціонування в системі *Global Positioning System* (*GPS*) забезпечує високу точність на відкритій місцевості завдяки відліку часу від супутникових сузір’їв. Для подолання недоліків обох технологій найкращі результати демонструє комбінований метод локалізації, відомий як *Assisted-GPS* (*A-GPS*). Він дозволяє значно скоротити час першого визначення координат *Time To First Fix* (*TTFF*) та підвищити чутливість приймача за рахунок отримання допоміжних даних через канали стільникового зв’язку.

Головним фактором, що знижує точність позиціонування в реальних умовах, є поширення сигналу поза прямою видимістю через відбиття від будівель та рельєфу, що призводить до виникнення додаткової затримки. Технічна реалізація комбінованого методу вимагає чіткої взаємодії між апаратною частиною термінала та серверною інфраструктурою мережі. Ключовим етапом у цьому

процесі є математична обробка навігаційних даних, яка мінімізує похибки від багатопроменевого поширення радіохвиль. Структура обчислювача проектованої системи повинна мати високу продуктивність для паралельної фільтрації та декодування сигналів. Основним вузлом апаратної частини виступає кореляційний приймач, який здійснює пошук, захоплення та безперервне супроводження слабких супутникових сигналів у складній завадовій обстановці.

Основним вузлом апаратної частини виступає багатоканальний кореляційний приймач, побудований на принципах технології кодового розділення каналів (*CDMA*). Оскільки вхідний супутниковий чи стільниковий радіосигнал формується шляхом множення інформаційних даних на високошвидкісний цифровий опорний сигнал, кореляційний приймач виконує зворотну математичну операцію. У кожному каналі приймача реалізовано схеми автопідлаштування частоти та часової затримки, що дозволяє виділяти навігаційне повідомлення навіть за низьких значень відношення сигнал/шум, характерних для міської забудови.

Таким чином, запропонована комплексна система локалізації мобільного абонента на основі інтеграції стільникових та супутникових технологій дозволяє досягти оптимального балансу між точністю та швидкістю позиціонування. Реалізація ефективної структури обчислювача та використання кореляційного приймача забезпечують стабільну роботу системи навіть у несприятливих умовах радіоприйому, що відкриває широкі перспективи для її практичного впровадження в сучасних мережах зв’язку.

Список використаних джерел

1. H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi. UMTS Networks: Architecture, Mobility and Services (2nd Edition), 2005. – 464c.
2. D. Dardari, E. Falletti, M. Luise. Satellite and Terrestrial Radio Positioning Techniques: A Signal Processing Perspective, 2012. – 458c.

УДК 004.7:621.39 (043.2)

Альона ОСІЙЧУК, Денис БАХТІЯРОВ, Андрій ЛЕЛЕКО
Державний університет «Київський авіаційний інститут», м. Київ

ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ У СИСТЕМАХ МОНІТОРИНГУ МЕРЕЖЕВОГО ОБЛАДНАННЯ

Стрімкий розвиток телекомунікаційних технологій, масове розгортання стандартів зв’язку нового покоління (зокрема Wi-Fi 7) та перехід корпоративних мереж до програмно-визначених архітектур (SDN) зумовили експоненційне зростання обсягів мережевої телеметрії. Традиційні підходи до управління мережевою інфраструктурою, засновані на протоколі SNMP та моделі опитування «запит-відповідь» (Pull-model), демонструють критичну обмеженість у сучасних високонавантажених середовищах. Встановлення фіксованих порогових значень генерує величезну кількість хибних спрацювань і не дозволяє завчасно фіксувати приховані патерни деградації. У зв'язку з цим, виникає об’єктивна потреба у переході від пасивного спостереження до предиктивної аналітики за допомогою методів інтелектуального аналізу даних (ІАД) класу AIOps.

Метою даної роботи є підвищення надійності, відмовостійкості та загальної ефективності функціонування корпоративних мереж шляхом розробки підсистеми моніторингу на основі алгоритмів машинного навчання. Для досягнення мети було формалізовано об’єктну модель мережі на основі теорії графів, де кожен вузол інфраструктури (комутатори CloudEngine, точки доступу AirEngine) описується багатовимірним вектором стану. Основним джерелом даних обрано механізм Streaming Telemetry (на базі gRPC/ProtoBuf), що функціонує за моделлю підписки (Push-model). Це дозволило отримувати високодискретні метрики у реальному часі: рівень утилізації CPU та буферної пам'яті (RAM), варіацію затримки пакетів (джиттер) та коефіцієнт втрат.

Оскільки метрики мають різну фізичну природу, перед їхньою обробкою застосовано метод мінімаксної нормалізації (Min-Max Scaling). Інтелектуальне ядро системи включає ансамбль оптимізованих алгоритмів. Для діагностики відомих інцидентів (апаратне виснаження, DDoS-атаки) використано метричний алгоритм класифікації k-найближчих сусідів (k-NN) із застосуванням просторового індексування kd_tree, що забезпечує блискавичний пошук. Паралельно для

сегментації трафіку та виявлення невідомих аномалій (Zero-day) реалізовано алгоритм k-means. Важливим компонентом є прогностичне моделювання: за допомогою методу найменших квадратів (МНК) побудовано модель множинної лінійної регресії, яка екстраполює тренди завантаження і прогнозує час досягнення критичних меж пропускної здатності.

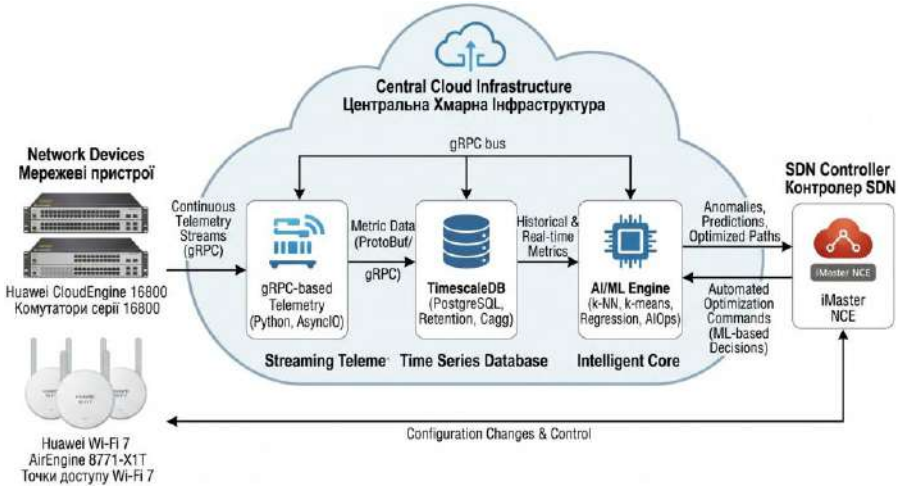


Рис. 1. Схема мікросервісної архітектури інтелектуальної системи моніторингу

Програмна реалізація комплексу базується на мікросервісній архітектурі з використанням мови Python 3.12+ та бібліотеки asyncio для обробки тисяч паралельних з'єднань. Надійне зберігання високоінтенсивних часових рядів забезпечено за допомогою реляційної СУБД PostgreSQL із розширенням TimescaleDB. Використання механізму Continuous Aggregates та індексів типу BRIN суттєво мінімізувало навантаження під час формування вибірок для навчання ШІ.

Результати експериментального тестування засвідчили перевагу запропонованого рішення. Точність класифікації аномалій алгоритмом k-NN досягла 98.7%. Час реакції системи на інциденти зменшився з 4 хвилин (у випадку SNMP) до 1.2 секунди завдяки потоковій обробці. Модель регресійного аналізу успішно передбачає перевантаження інтерфейсів за 18 годин до фактичного інциденту з точністю $R^2 = 0.94$. Таким чином, розроблена підсистема формує повністю готову платформу для проактивного моніторингу, здатну суттєво оптимізувати експлуатаційні витрати підприємств.

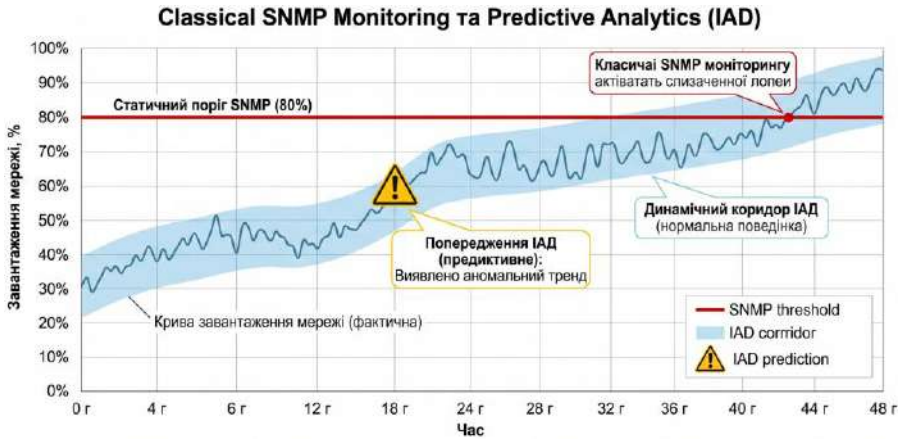


Рис. 2. Графік порівняння класичного SNMP-моніторингу та предиктивної аналітики IAД

Список використаних джерел

1. Шкільнюк, Д. О. Системи моніторингу IT-інфраструктури: від статичних тригерів до AIOps // Кібербезпека та комп'ютерна інженерія. – 2025. – № 1. – С. 34-41.
2. Якименко, Ю. І. Сучасні бездротові технології: впровадження та перспективи стандарту Wi-Fi 7 (IEEE 802.11be) // Радіоелектроніка, інформатика, управління. – 2024. – № 2. – С. 55-63.
3. Hastie, T., Tibshirani, R., & Friedman, J. The Elements of Statistical Learning: Data Mining, Inference, and Prediction. Springer, 2022.
4. Kotyk B., Bakhtiiarov D., Lavrynenko O., Chumachenko B., Antonov V., Fesenko V., Chupryn V. Neural network approach to 5G digital modulation recognition, (2025) CEUR Workshop Proceedings, 3925, pp. 82 - 92.
5. Huawei Technologies Co., Ltd. CloudEngine 16800 Series Switches: Telemetry Configuration Guide. Huawei Enterprise Support, 2025.
6. Bakhtiiarov D., Chumachenko B., Lavrynenko O., Chupryn V., Antonov V. Distribute load among concurrent servers, (2024) CEUR Workshop Proceedings, 3826, pp. 260 - 266.

УДК 004.72

Н.Т. Осінський, А.Г. Тараненко
Державний університет
«Київський авіаційний інститут», м. Київ

АНАЛІЗ ОСОБЛИВОСТЕЙ РАДІОІНТЕРФЕЙСУ ШИРОКОСМУГОВИХ СТІЛЬНИКОВИХ СИСТЕМ ПЕРЕДАЧІ ДАНИХ

На сучасному етапі розвитку глобальних інфокомунікаційних інфраструктур основними факторами швидкого зростання обсягів мобільного трафіку є розширення Інтернету речей (IoT), міжмашинної взаємодії (M2M) і масове споживання надвисокої чіткості мультимедійного контенту.

Надійне забезпечення таких сервісів вимагає постійної оптимізації радіоінтерфейсів стільникових мереж, основу яких складають широкосмугові системи стандарту LTE та їхня технологічна еволюція у напрямку мереж п'ятого покоління (5G). Головною фізичною проблемою при організації швидкісного безпроводового доступу в умовах щільної міської забудови залишається обмеженість спектра та явище багатопроменевого поширення радіохвиль. Для подолання цих ефектів у широкосмугових системах здійснюється перехід від застарілих методів кодового (WCDMA) чи часового (TDMA) розділення до технології ортогонального частотного мультиплексування (OFDM) [1, 2].

Математична основа OFDM базується на застосуванні дискретного та швидкого перетворення Фур'є (ДПФ/ШПФ), що дозволило розділяти високошвидкісний вхідний цифровий потік на велику кількість ортогональних піднесучих із низькою швидкістю передачі в кожному субканалі. Завдяки збільшенню тривалості символу в окремому субканалі та введенню циклічного префіксу (захисного інтервалу) вдається повністю нівелювати затримки багатопроменевого поширення та ліквідувати MCI.

Для організації ефективного двостороннього зв'язку та колективного доступу застосовуються різні модифікації OFDM. У прямому каналі (Downlink) використовується метод багатостанційного доступу з ортогональним частотним розділенням (OFDMA). Його додаткова ефективність підтримується механізмами адаптивної модуляції та кодування (AMC): залежно від поточного рівня

відношення сигнал/завада (SNR) система динамічно перемикає формати модуляції від завадостійкої QPSK до високоефективних 16QAM та 64QAM [3].

Проте базова технологія OFDM має суттєвий недолік — високе відношення пікової потужності до середньої (пік-фактор, PAPR). Якщо для базової станції у прямому каналі це не є критичним, то у зворотному каналі (Uplink) високий PAPR призводить до низького ККД підсилювача мобільного телефона і швидко виснажує його акумулятор. Для вирішення цієї проблеми у зворотному каналі застосовується технологія SC-FDMA. Завдяки додатковому ДПФ-кодуванню, яке виконується перед процедурою OFDM-модуляції, сформований сигнал набуває властивостей сигналу з однією несною. Це дозволяє знизити пік-фактор на 3–5 дБ, суттєво зменшити енергоспоживання абонентського термінала та розширити зону покриття базової станції [4].

Проведений аналіз свідчить, що комплексне використання технологій OFDMA у прямому каналі та SC-FDMA у зворотному каналі є оптимальним інженерним рішенням для побудови радіоінтерфейсів сучасних широкосмугових систем. Така архітектура забезпечує раціональний компроміс між пропускною здатністю мережі, її спектральною ефективністю та енергоощадністю абонентського обладнання, виступаючи надійним фундаментом для розгортання стільникових мереж наступних поколінь.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Кравчук С. О., Голубничий О. Г., Тараненко А. Г., Потапов В. Г., Ткалич О. П. Системи зв'язку з рухомими об'єктами: Підручник. – К.: Спринт-Сервис, 2012. - 452 с.*
2. *Гепко І. А., Олійник В. Ф., Чайка Ю. Д. Сучасні бездротові мережі: стан та перспективи розвитку. – К.: ЕКМО, 2009. 672 с.*
3. *Holma H., Toskala A. LTE for UMTS: Evolution to LTE-Advanced. Chichester : John Wiley & Sons, 2011. 576 p.*
4. *Cox C. An Introduction to LTE: LTE, LTE-Advanced, SAE and 4G Mobile Communications. Chichester : John Wiley & Sons, 2012. 352 p.*

УДК 621.391

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

ВПРОВАДЖЕННЯ ПРОГРАМНИХ МЕТОДІВ ЗАХИСТУ ДАНИХ У ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ НА БАЗІ ESET

Зростання обсягів передавання інформації, розвиток хмарних сервісів, мобільних технологій та інтернету речей призводить до суттєвого збільшення кіберзагроз. Телекомунікаційні мережі стають ключовою інфраструктурою, через яку здійснюються атаки на державні установи, бізнес та критичні об'єкти. Основними загрозами є перехоплення трафіку, несанкціонований доступ, шкідливе ПЗ, DDoS-атаки, фішинг, експлуатація вразливостей протоколів та сервісів. У таких умовах впровадження програмних методів захисту даних стає необхідною умовою забезпечення цілісності, конфіденційності та доступності інформації.

Сучасні телекомунікаційні мережі потребують надійного захисту від новітніх кіберзагроз (вірусів-вимагачів, APT-атак) [1]. Оскільки традиційні антивіруси втрачають ефективність, виникає гостра необхідність впровадження багаторівневих систем захисту кінцевих точок (Endpoint Security) із можливістю централізованого управління.

У роботі запропоновано модель комплексної системи безпеки на базі корпоративних рішень ESET. Архітектуру цільової мережі розподілено на три ізольовані сегменти: Server VLAN, Workstation VLAN та Guest VLAN. Для централізованого моніторингу інцидентів у реальному часі використовується платформа ESET PROTECT. Проактивний захист робочих станцій забезпечується синергією технологій поведінкового аналізу HIPS, розширеного сканера пам'яті та глобальної репутаційної системи ESET LiveGrid. Процес розгортання клієнтських модулів оптимізовано за допомогою комплексних автономних пакетів, які встановлюються у фоновому режимі. У межах інфраструктури налаштовано уніфіковані групові політики безпеки: фільтрацію міжсегментного трафіку брандмауерами та жорсткий контроль підключення периферійних USB-пристроїв (Device Control).

Продукти ESET широко застосовуються у корпоративних мережах завдяки поєднанню високої ефективності, низького навантаження на

систему та розвинених механізмів централізованого управління [2]. Основні переваги:

- ✓ Багаторівневий захист: сигнатурний аналіз, евристика, поведінковий моніторинг, машинне навчання.
- ✓ ESET LiveGrid — хмарна система репутацій, що забезпечує швидке виявлення нових загроз.
- ✓ Захист мережевого трафіку: фільтрація протоколів, виявлення експлойтів, блокування шкідливих з'єднань.
- ✓ Централізоване управління через ESET PROTECT: моніторинг, політики безпеки, звітність, автоматизація.
- ✓ Підтримка шифрування даних (ESET Full Disk Encryption) для захисту інформації у разі компрометації пристроїв.
- ✓ Сумісність із різними платформами: Windows, Linux, Android, macOS, серверні ОС.

Експериментальне тестування системи шляхом імітації шкідливого коду (стандартний файл EICAR) та несанкціонованого монтування носіїв даних підтвердило стовідсоткову надійність автоматичного перехоплення загроз. Розроблена архітектура забезпечує миттєву ізоляцію джерел небезпеки і може бути використана для модернізації систем кібербезпеки підприємств.

Впровадження програмних методів захисту даних у телекомунікаційних мережах на базі рішень ESET [3] є ефективним та економічно обґрунтованим підходом до забезпечення кібербезпеки. Продукти ESET дозволяють створити комплексну систему захисту, що охоплює антивірусний контроль, шифрування, моніторинг мережевої активності, виявлення аномалій та централізоване управління. Завдяки гнучкості, масштабованості та високій швидкості реагування на нові загрози ESET є оптимальним рішенням для сучасних телекомунікаційних мереж, які потребують надійного та безперервного захисту.

Список літератури

1. Stallings W. *Network Security Essentials: Applications and Standards*. 6th ed. Pearson, 2023. 480 p.

2. Kaufman C., Perlman R., Speciner M. *Network Security: Private Communication in a Public World*. 3rd ed. Prentice Hall, 2021. 752 p.

3. ESET. *ESET PROTECT Platform — Technical Overview*. ESET, 2024. URL: https://www.eset.com

УДК 004.732.057.4 (043.2)

Вадим ПЕТРОВ, Володимир КЛИМЧУК
Державний університет «Київський авіаційний інститут», м. Київ

КОРПОРАТИВНА МЕРЕЖА НА БАЗІ ОБЛАДНАННЯ CISCO

В сучасному світі ефективне функціонування будь-якого територіально розподіленого підприємства безпосередньо залежить від надійності, швидкодії та безпеки його інформаційно- комунікаційної інфраструктури. Традиційні підходи до побудови корпоративних мереж (КМ), засновані на жорстко детермінованих апаратних топологіях, вичерпали свій експлуатаційний потенціал. Стрімке зростання обсягів мультисервісного трафіку та безперервна еволюція кіберзагроз вимагають переходу до гнучких, програмно- керованих екосистем, таких як SD-WAN (Software-Defined Wide Area Network), та впровадження архітектури нульової довіри (Zero Trust).

Метою нашого дослідження є розробка проєкту сучасної, масштабованої та захищеної корпоративної мережі на базі актуального апаратного забезпечення Cisco, з урахуванням новітніх стандартів маршрутизації, інформаційної безпеки та вимог нормативно-правової бази України (зокрема стандартів ДССЗЗІ та регламентів НБУ).

В основу запропонованої архітектури покладено принцип максимальної децентралізації обробки трафіку при одночасному збереженні монолітного контролю над політиками безпеки. Наша розробка використовує технологію Cisco SD-WAN для абстрагування від типу фізичного транспорту (використовуючи Internet та MPLS канали), дозволяючи реалізувати механізм Dynamic Path Selection для оптимізації передачі критично важливих пакетів у режимі реального часу.

Апаратна реалізація мережі базується на використанні маршрутизаторів Cisco Catalyst 8000 Series (в ролі cEdge) та комутаторів ядра і доступу Catalyst 9000 Series із підтримкою технології UPOE+. Для гарантування конфіденційності даних розроблено багаторівневу модель кіберзахисту. Вона включає використання сертифікованих криптографічних алгоритмів (AES-256- GCM для шифрування ESP, ECDH Group 19/20 для забезпечення досконалої прямої секретності PFS) та інтеграцію системи централізованого контролю доступу Cisco Identity Services Engine (ISE).

Рис. 1. Структурна схема взаємодії центрального офісу та філій у межах КМ на базі Cisco SD-WAN

Концепція мікросегментації реалізована за допомогою технології Cisco TrustSec (зокрема, використання міток Security Group Tags - SGT), що унеможливлює горизонтальне переміщення загроз у мережі в разі компрометації окремого вузла. Для ефективної інтеграції різнорідних потоків даних (голосова телефонія, відеоконференцзв'язок, передача CAD-креслень) впроваджена модель диференційованого обслуговування (DiffServ).

Архітектура забезпечення якості обслуговування (QoS) побудована з використанням диспетчеризації черг CBWFQ (Class-Based Weighted Fair Queuing) та LLQ (Low Latency Queuing). У межах проєкту запропоновано інженерне рішення для копіювання маркерів DSCP у зовнішні заголовки IPSec тунелів, що дозволяє провайдерам транзитних мереж коректно розпізнавати та пріоритезувати чутливий до затримок трафік.

Виконані математичні розрахунки пропускної здатності та інтенсивності інформаційного навантаження підтверджують високу ефективність запропонованої топології. Отримані результати становлять готовий до впровадження інженерний проєкт модернізації IT-інфраструктури, що повністю відповідає викликам технологічного розвитку та забезпечує безперервність бізнес-процесів сучасної організації. Запропоновані архітектурні та апаратні рішення мінімізують капітальні та операційні витрати, створюючи надійний технологічний фундамент.

Список використаних джерел

1. Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, 2022.

УДК 004.056:621.391:004.94

Л.Г. Петросян[1], В.О. Гнатюк[1,2]
[1] Державний університет «Київський авіаційний інститут», Київ, Україна
[2] Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації, Київ, Україна

КОНТРОЛЬ ЦІЛІСНОСТІ ТЕЛЕМЕТРІЇ NETWORK DIGITAL TWIN ДЛЯ БЕЗПЕЧНОЇ ЕКСПЛУАТАЦІЇ ІКС

Сучасні інформаційно-комунікаційні системи (ІКС) дедалі частіше керуються на основі поточних даних про стан мережі. Для цього перспективним інструментом є Network Digital Twin (NDT) - цифровий двійник телекомунікаційної мережі, що відображає фізичну інфраструктуру у віртуальній моделі. ITU-T Y.3090 визначає NDT через поєднання даних, моделей та інтерфейсів, необхідних для аналізу, діагностики, емуляції і керування мережею [1]. Проте практична цінність такого двійника залежить від базового питання: чи можна довіряти телеметрії, на якій побудована його операційна картина?

Актуальність питання посилюється переходом до автоматизованого керування. ITU-T Y.3092 розглядає цифровий двійник як інструмент управління та оркестрації в мережах IMT-2020 і наступних поколінь [2], ETSI GR ZSM 015 пов'язує NDT із closed-loop підходами у zero-touch management [4], а 3GPP TR 28.915 виносить управлінські аспекти NDT у площину мобільних мереж [5]. У таких умовах помилка телеметрії вже не є лише помилкою моніторингу: вона може впливати на модель, прогноз, пріоритезацію аварійних робіт або переналаштування маршрутів.

Під цілісністю телеметрії пропонується розуміти не тільки криптографічну незмінність окремого пакета, а ширшу експлуатаційну властивість. Телеметрія є цілісною тоді, коли вона походить з очікуваного джерела, зберігає часову послідовність, не суперечить суміжним вимірюванням і достатньо повно відображає стан мережевого елемента. Такий підхід узгоджується з ITU-T X.2011, де серед напрямів захисту цифрового двійника мережі виділено довіреність даних, конфіденційність і захист інтерфейсів [3].

Найнебезпечнішими для NDT є помилки і атаки, які не виглядають як повна відмова. Якщо канал телеметрії недоступний, оператор бачить явну проблему. Натомість часткове спотворення

даних, затримка показників, підміна часових міток або заниження навантаження можуть створити для цифрового двійника правдоподібну, але хибну картину. У такому випадку модель може показувати стабільний стан там, де фізична мережа вже деградує, або навпаки - сигналізувати про критичну подію там, де достатньо штатного перерозподілу ресурсів.

Для практичного застосування доцільно вводити мінімальний контур контролю цілісності телеметрії NDT. Він має включати перевірку походження даних, часову перевірку, перехресне зіставлення суміжних джерел і поріг управлінського впливу. Якщо довіра до телеметрії нижча за заданий рівень, NDT може використовуватися для аналізу, але не для автоматичного втручання у фізичну мережу. З позиції кібербезпеки це можна подати як три зони довіри: зелену для планування та оптимізації, жовту для підтримки рішення з перевіркою людиною і червону для заборони автоматизованої зміни стану мережі.

Запропонований підхід дозволяє пов'язати якість функціонування NDT із безпечною експлуатацією ІКС. Якщо цифровий двійник сприймати як інструмент прийняття рішень, то якість його роботи визначається не лише точністю моделі, а й довірою до вхідної телеметрії. Така логіка узгоджується з NIST Cybersecurity Framework 2.0, де управління кіберризиком розглядається через цільові результати, а не через одну жорстко задану технологію [6]. Подальші дослідження доцільно спрямувати на формалізацію показника довіри до телеметрії та його інтеграцію в модель оцінювання якості функціонування Network Digital Twin телекомунікаційних систем.

Література

1. ITU-T Recommendation Y.3090. Digital twin network - Requirements and architecture. Geneva : ITU, 2022.

2. ITU-T Recommendation Y.3092. Digital twin for management and orchestration in IMT-2020 networks and beyond. Geneva : ITU, 2024.

3. ITU-T Recommendation X.2011. Security guidelines for digital twin network. Geneva : ITU, 2024.

4. ETSI GR ZSM 015 V1.1.1. Zero-touch network and Service Management; Network Digital Twin. Sophia Antipolis : ETSI, 2024.

5. 3GPP TR 28.915. Study on management aspect of Network Digital Twin. Release 19. Sophia Antipolis : 3GPP, 2025.

6. Pascoe C., Quinn S., Scarfone K. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg : NIST, 2024.

УДК 621.391

Є.О.Петухов, В.В. Антонов
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ МЕРЕЖІ PASSIVE OPTICAL LAN ДЛЯ СУЧАСНОЇ ОФІСНОЇ БУДІВЛІ

Стрімкий розвиток корпоративних інформаційних технологій, перехід до хмарних обчислень, впровадження систем відеоконференцзв'язку високої чіткості та Інтернету речей (IoT) висувають нові, більш жорсткі вимоги до телекомунікаційної інфраструктури сучасних офісних будівель.

Традиційні локальні обчислювальні мережі (ЛОМ), побудовані на базі мідної витої пари (Ethernet), поступово вичерпують свій технічний та економічний потенціал. Вони стикаються з фізичними обмеженнями щодо довжини кабельного сегмента (до 100 метрів), потребують значного простору у кабельних каналах та вимагають облаштування активних комутаційних вузлів на кожному поверсі.

У цьому контексті надзвичайно актуальним стає пошук та впровадження інноваційних рішень, одним з яких є технологія Passive Optical LAN (POL). Аналіз архітектури та технологічних переваг POL: Технологія POL базується на архітектурі пасивних оптичних мереж (PON) та передбачає доведення оптичного волокна безпосередньо до робочого місця користувача (Fiber-to-the-Desk). Топологія розробленої мережі POL будується за принципом «точка-багатоточка».

Центральним елементом є оптичний лінійний термінал (OLT), який встановлюється в головній серверній кімнаті. Замість поверхових комутаторів доступу використовуються пасивні оптичні сплітери (з коефіцієнтом розгалуження 1:32 або 1:64), які не потребують електроживлення, активного охолодження та налаштування.

На робочих місцях користувачів встановлюються компактні абонентські термінали (ONT), які конвертують оптичний сигнал в електричний та надають стандартні порти Gigabit Ethernet з підтримкою PoE для живлення IP-телефонів та точок доступу Wi-Fi. Математичне обґрунтування та оптичний бюджет: Критичним етапом проєктування є розрахунок оптичного бюджету лінії.

Математичні розрахунки сумарних втрат на одномодовому оптичному волокні, зварних з'єднаннях, конекторах та пасивних розгалужувачах доводять, що потужності сигналу OLT достатньо для гарантованого покриття всієї будівлі без використання додаткових підсилювачів або ретрансляторів, навіть за умови максимального абонентського навантаження. Економічна доцільність (CAPEX та OPEX): Порівняльний техніко-економічний аналіз мережі POL та традиційної мідної LAN підтвердив високу ефективність оптичного рішення. Використання одномодового оптичного кабелю замість пучків мідної витої пари дозволяє скоротити обсяги кабельних трас до 60%, що значно спрощує інженерні комунікації будівлі.

Відсутність активного обладнання на поверхах (комутаційних шаф) знижує операційні витрати (OPEX) на електроспоживання інфраструктури та кондиціонування до 50%.

Крім того, оптичне волокно унеможливлює несанкціоноване перехоплення даних електромагнітним шляхом, підвищуючи рівень інформаційної безпеки.

Висновок: Впровадження технології Passive Optical LAN є економічно вигідним та технічно обґрунтованим рішенням для сучасних офісних центрів. Вона ефективно вирішує поточні проблеми з пропускною здатністю, дефіцитом простору та високим енергоспоживанням.

POL формує надійний фундамент для масштабування, оскільки модернізація мережі (наприклад, міграція з GPON на XGS-PON) вимагатиме лише заміни кінцевого активного обладнання, зберігаючи існуючу кабельну інфраструктуру незмінною.

УДК 004.056

Н.О. Плахотнюк, С.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ ТА ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПРИВАТНОМУ ПІДПРИЄМСТВІ

У сучасних умовах розвитку цифрової економіки приватне підприємство функціонує не лише як суб'єкт господарювання, а й як складний об'єкт інформаційної діяльності (ОІД), у межах якого здійснюється безперервний цикл обробки та зберігання критично важливих комерційних даних. Зростання інтенсивності та складності цілеспрямованих кібератак, зокрема із застосуванням програм-вимагачів (Ransomware), диктує необхідність переходу від фрагментарних методів кіберзахисту до побудови глибоко ешелонованої та науково обґрунтованої комплексної системи захисту інформації (КСЗІ). Базовим принципом проєктування такої системи є мінімізація ризиків компрометації даних з урахуванням нормативних вимог та архітектурної специфіки корпоративної інфраструктури. Особливий акцент у дослідженні зроблено на протидії загрозам внутрішнього порушника (Insider Threat) та забезпеченні катастрофостійкості бізнес-процесів за рахунок впровадження систем запобігання витоку даних (DLP) та архітектури резервного копіювання за правилом «3-2-1».

У роботі здійснено системний аналіз вимог до захисту інформації відповідно до нормативних документів системи технічного захисту інформації (НД ТЗІ) України. Спроєктовано безпечну фізичну та логічну топологію об'єкта, яка базується на чіткому розмежуванні контрольованих зон (КЗ) та ізоляції критичних серверних сегментів за допомогою віртуальних локальних мереж (VLAN) із застосуванням жорстких списків контролю доступу (ACL). Для забезпечення конфіденційності та цілісності даних розгорнуто комплекс криптографічних засобів, що включає магістральне тунелювання трафіку за протоколом IPsec та обов'язкове повнодискове шифрування на кінцевих робочих станціях. Фундаментом логічної безпеки стала інтеграція системи централізованої автентифікації та контролю доступу на базі взаємодії Active Directory та RADIUS-сервера, що дозволило реалізувати портоорієнтований стандарт контролю доступу IEEE 802.1X. На рівні пери-

метра розгорнуто відмовостійкий кластер маршрутизаторів під управлінням RouterOS, які виконують функції міжмережевого екранування (Stateful Firewall) та трансляції адрес (NAT). Окрім цього, для організації безпечного віддаленого доступу співробітників (Remote Access VPN) впроваджено обов'язкову багатофакторну автентифікацію (MFA), що критично знижує ймовірність компрометації облікових записів через фішинг чи викрадення паролів.

Валідацію ефективності прийнятих інженерних рішень здійснено шляхом проведення комплексного тестування на проникнення (Penetration Testing) та інструментального аудиту конфігурацій активного мережевого обладнання. Експериментально доведено відсутність критичних вразливостей периметра та високу стійкість інфраструктури до атак типу Brute-Force і L2-аномалій (завдяки активації механізмів Dynamic ARP Inspection та DHCP Snooping). Завдяки застосуванню політик нульової довіри (Zero Trust) та мікросегментації повністю нівельовано ризики несанкціонованого горизонтального переміщення (Lateral Movement) зловмисників усередині корпоративного середовища. Додатково розроблено та імплементовано регламенти безперервного управління вразливостями (Vulnerability Management), що включають регулярне автоматизоване сканування інфраструктури на наявність відомих CVE (Common Vulnerabilities and Exposures) та централізоване розгортання оновлень безпеки (Patch Management). Інтегровані засоби автоматизованого реагування на базі систем класу SIEM (Security Information and Event Management) та EDR (Endpoint Detection and Response) дозволили мінімізувати час виявлення інцидентів та забезпечили безперервність надання бізнес-сервісів згідно з SLA.

Фінальна оцінка техніко-економічної ефективності підтвердила високу фінансову рентабельність впровадженої системи захисту. Математичне зіставлення сукупної вартості володіння інфраструктурою безпеки (TCO) із величиною відвернених потенційних збитків від компрометації комерційної таємниці продемонструвало надзвичайно високий рівень показника повернення інвестицій (ROSI). Розроблена архітектура є готовим, комерційно привабливим еталоном для модернізації систем інформаційної безпеки на підприємствах середнього та малого бізнесу.

УДК 004.056:338.49

О.В. Попович, С.С. Чумаченко
Державний університет
«Київський авіаційний інститут», м. Київ

ПРОЄКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Стабільне функціонування державних інститутів, економічна безпека та життєдіяльність суспільства безпосередньо залежать від безперебійної роботи об'єктів критичної інфраструктури (ОКІ). В умовах глобальної цифровізації відбувається незворотна конвергенція класичних корпоративних інформаційних технологій (IT) та промислових операційних технологій (OT), зокрема систем класу SCADA. Таке об'єднання суттєво розширює поверхню атак і створює безпрецедентні ризики кінетичних (фізичних) наслідків у разі успішного цілеспрямованого кібервтручання. Відповідно до вимог європейської директиви NIS2 та міжнародних стандартів кібербезпеки, побудова глибоко ешелонованої системи захисту інформації для таких підприємств є не просто бізнес-завданням, а критичною вимогою національної безпеки.

У роботі здійснено комплексний аналіз специфіки захисту інформації на ОКІ та спроєктовано відмовостійкий архітектурний шаблон КСЗІ, який повністю задовольняє жорсткі вимоги міжнародних стандартів серії IEC 62443 та ISO/IEC 27001. Ключовим інженерним рішенням стало чітке мікросегментування та розмежування меж довіри між корпоративним і промисловим середовищами на основі еталонної архітектурної моделі Пурдю (Purdue Enterprise Reference Architecture, PERA). Для забезпечення безпеки специфічного індустріального трафіку впроваджено міжмережеві екрани нового покоління (NGFW DPI) з можливістю глибокого інспектування промислових протоколів (Modbus TCP, DNP3, IEC 104), системи пасивного моніторингу аномалій (IDS) та апаратну ізоляцію зворотного каналу зв'язку за допомогою однонаправлених шлюзів (Data Diodes), сертифікованих за стандартом IEC 61850-3. Додатково розроблено жорсткі регламенти управління доступом на базі рольової моделі (RBAC), багатофакторної автентифікації (MFA) та систем контролю привілейованих користувачів (PAM). Враховуючи неможливість встановлення класичних антивірусних засобів на застарілі операційні системи автоматизованих робочих місць (АРМ) операторів, базовим механізмом захисту кінцевих

точок в OT-сегменті обрано технологію контролю додатків (Application Whitelisting) у режимі суворого блокування невідомого коду.

Практична реалізація проєкту охопила розгортання та конфігурування аналітичного ядра SIEM із застосуванням пасивного зняття копій трафіку (SPAN-порти) для нормалізації та кореляції розподілених у часі подій безпеки в режимі реального часу. Для підвищення точності детектування загроз систему збагачено індикаторами компрометації (IoC) від платформ Threat Intelligence (TI). З метою мінімізації людського фактора та прискорення реакції операторів SOC (Security Operations Center) імплементовано елементи систем автоматизації та оркестрації (SOAR). З метою забезпечення безперервності операційних процесів сформовано покроковий план реагування на інциденти (IRP) за методологією NIST SP 800-61 та стратегію управління життєвим циклом вразливостей (Virtual Patching). Особливу увагу приділено нівелюванню ризиків компрометації через ланцюжок постачання (Supply Chain Attacks). Для підрядних організацій та сервісних інженерів вендорів впроваджено концепцію захищеного віддаленого доступу (Secure Remote Access) на базі ізольованих термінальних серверів (Jump Hosts) із обов'язковим відеозаписом усіх привілейованих сесій. Окрім того, розроблено надійну стратегію аварійного відновлення інфраструктури (DRP), що базується на «золотому» інженерному правилі резервного копіювання «3-2-1».

Для валідації надійності розробленого комплексу проведено інструментальний аудит захищеності методом Gray Box. Експериментальні дослідження підтвердили високу ефективність впроваджених підходів до виявлення загроз та унеможливлення несанкціонованого горизонтального переміщення зловмисників. Кількісна оцінка засвідчила підвищення коефіцієнта готовності критичної інфраструктури до рівня «чотирьох дев'яток» (0.99990). Отримані результати становлять значну практичну цінність і можуть бути використані як готовий, нормативно обґрунтований архітектурний шаблон для модернізації систем кібербезпеки в енергетичному, телекомунікаційному та логістичному секторах.

УДК 621.391.6:004.72

В.М. Постельников, С.О. Завгородній
Державний університет
«Київський авіаційний інститут», м. Київ

МОДЕЛЬ МЕРЕЖІ ДОСТУПУ (NGAN) З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ FLEX ETHERNET

Актуальність. Стрімке зростання обсягів мережевого трафіку, зумовлене масовим поширенням відеопотоків 4K/8K, хмарних обчислень та розгортанням мереж п'ятого покоління (5G NR), ставить принципово нові вимоги до інфраструктури мереж доступу. За даними Cisco Visual Networking Index, глобальний IP-трафік до 2025 р. має перевищити 400 екзабайт на місяць. Разом з тим існуюча архітектура мереж доступу (NGAN — Next Generation Access Network) зіштовхується з фундаментальним протиріччям: традиційний Ethernet не забезпечує жорсткої ізоляції між сервісами різних класів, тоді як оптичні транспортні мережі (OTN), що надають детерміновану TDM-ізоляцію, є в 3–5 разів дорожчими. Технологія Flex Ethernet (FlexE), стандартизована OIF у специфікаціях OIF-FLEXE-01.0 (2016) та OIF-FLEXE-02.1 (2018), є оптимальним технічним рішенням, що усуває зазначене протиріччя.

Архітектура FlexE. FlexE вводить між фізичним рівнем (PHY) та рівнем MAC традиційного Ethernet новий субрівень — FlexE Shim, що складається з чотирьох функціональних модулів: Calendar Engine (зберігає Active/Pending Calendar та здійснює атомарне перемикання між ними без переривання сервісу), MUX/DEMUX (розподіляє 66-бітні блоки 64b/66b між FlexE Client-потоками), Overhead Generator (формує 64-байтний службовий кадр кожні 1024 блоки для OAM) та Deskew Module (компенсує різницю затримок між PHY-каналами до 120 нс). FlexE Group об'єднує до 8 PHY по 100GE, утворюючи до 800 Гбіт/с агрегованої пропускної здатності з гранулярністю 5 Гбіт/с на один слот Calendar.

Структурна модель мережі. Розроблено модель мережі NGAN для регіонального оператора (35 000 абонентів), що охоплює 24 вузли OLT стандарту XGS-PON (ITU-T G.9807.1), 6 вузлів агрегації (AN) з FlexE Group 4×100GE та 2 резервовані вузли ядра мережі. Виконано

інженерний розрахунок навантаження у годину найбільшого навантаження (ГНН): сумарне навантаження на аплінк одного AN складає 112 Гбіт/с, що обґрунтовує вибір FlexE Group 4×100GE із коефіцієнтом завантаження 28% у ГНН та достатнім резервом для N-1 захисту.

Розподіл слотів Calendar та QoS. Розраховано розподіл 80 слотів FlexE Calendar між чотирма сервісними FlexE Client-потоками: Client-1 Internet (Best Effort, 30 слотів, 150 Гбіт/с), Client-2 IPTV/VoD (Assured Forwarding, 6 слотів, 30 Гбіт/с), Client-3 Корпоративний VPN (Expedited Forwarding, 6 слотів, 30 Гбіт/с), Client-4 5G Backhaul та OAM (Network Control, 10 слотів, 50 Гбіт/с). Резерв IDLE складає 28 слотів (140 Гбіт/с). Розрахунок показників QoS за моделлю M/D/1 підтвердив затримку в чергах кожного FlexE Client менше 0,4 мкс, що на 4–5 порядків нижче вимог ITU-T G.1010 для IPTV (<10 мс).

Відмовостійкість. Змодельовано чотири сценарії відмов мережі. При відмові одного PHY у FlexE Group (найбільш поширений тип) час відновлення складає 11 мс за рахунок атомарного перемикання FlexE Calendar — що значно менше вимоги ITU-T G.808.1 (≤50 мс). Мережа залишається повністю функціональною з пропускною здатністю 300 Гбіт/с (η = 37,4%). При відмові вузла агрегації AN час відновлення складає 60 мс із застосуванням механізму SR-TI-LFA Fast ReRoute.

Висновки. Розроблено детальну модель мережі доступу NGAN з технологією Flex Ethernet. Підтверджено ключову перевагу FlexE: при аномальному навантаженні 120% від ГНН затримка IPTV-трафіку залишається меншою за 0,06 мкс завдяки TDM-подібній ізоляції FlexE Calendar — тоді як при традиційному Ethernet QoS затримка зростає до 5–15 мс. Застосування FlexE Group 2×100GE у практичному проекті для Печерського району м. Київ (5 000 абонентів) забезпечує економію ~33% порівняно з традиційним підходом (3×100GE) при одночасно кращій сервісній ізоляції. Технологія Flex Ethernet є перспективним рішенням для побудови гнучких та ефективних мереж доступу NGAN наступного покоління в умовах зростаючих вимог до пропускної здатності та якості обслуговування.

УДК 621.391

Нікіта ПОСТОВИЙ, Олександр ПУЗИРЕНКО
Державний університет
«Київський авіаційний інститут», м. Київ

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА МЕРЕЖА НА БАЗІ ТЕХНОЛОГІЇ NFV

Метою роботи є проектування інформаційно-комунікаційної мережі на базі технології віртуалізації мережевих функцій (NFV) та порівняння її з традиційною мережевою архітектурою за основними технічними характеристиками.

Актуальність роботи полягає у тому, що сучасні інформаційно-комунікаційні мережі мають відповідати зростаючим вимогам до гнучкості, масштабованості та економічної ефективності.

Традиційний підхід до побудови мереж, заснований на використанні спеціалізованого фізичного обладнання, обмежує швидкість розгортання нових сервісів та потребує значних капітальних витрат.

Кожна мережева функція: маршрутизація, фільтрація трафіку, побудова захищених з'єднань реалізується окремим апаратним пристроєм від конкретного виробника, що ускладнює масштабування та оновлення інфраструктури.

Розгортання нового сервісу потребує придбання, доставки та фізичного встановлення обладнання, що може займати від кількох тижнів до місяців.

Технологія NFV була запропонована у 2012 році консорціумом провідних телекомунікаційних операторів під егідою ETSI. Основна ідея полягає у перенесенні мережевих функцій із спеціалізованого обладнання у програмне середовище на стандартних серверах загального призначення.

Шар віртуалізації ізолює програмні функції від фізичного обладнання, дозволяючи запускати кілька незалежних функцій на одній фізичній платформі.

Архітектура NFV складається з трьох ключових компонентів. Перший - віртуальні мережеві функції (VNF), що є програмними еквівалентами фізичних мережевих пристроїв. Другий - інфраструктура NFV (NFVI), що включає стандартні сервери, сховище та мережеве обладнання на яких виконуються VNF. Третій - підсистема управління

та оркестрації (MANO), що забезпечує розгортання, конфігурацію та управління життєвим циклом VNF.

MANO складається з оркестратора (NFVO), менеджера VNF (VNFM) та менеджера віртуальної інфраструктури (VIM).

У даній роботі для реалізації рівня оркестрації використовується платформа Open Source MANO (OSM) - рішення з відкритим кодом під егідою ETSI, що повністю відповідає стандартам NFV MANO.

Як менеджер віртуальної інфраструктури використовується OpenStack, найпоширеніша платформа для управління хмарними ресурсами.

Для реалізації мережевих сервісів використовуються три віртуальні функції: віртуальний маршрутизатор (vRouter), віртуальний міжмережевий екран (vFirewall) та віртуальний VPN-шлюз (vVPN), які утворюють сервісний ланцюжок для обробки трафіку.

Проектована NFV-схема порівнюється з традиційною мережевою архітектурою за такими критеріями: вартість розгортання, час впровадження нових сервісів, масштабованість, гнучкість та зручність адміністрування.

Порівняльний аналіз показує що NFV забезпечує суттєві переваги у гнучкості та швидкості змін, тоді як традиційна архітектура зберігає переваги у передбачуваності та стабільності роботи.

Висновки.

У даній роботі розглянуто концепцію та архітектуру технології NFV, спроектовано інформаційно-комунікаційну мережу на базі OSM та OpenStack з використанням трьох віртуальних мережевих функцій, проведено порівняльний аналіз NFV та традиційної мережевої архітектури. Застосування технології NFV дозволяє суттєво скоротити час розгортання нових сервісів, знизити залежність від конкретних виробників обладнання та забезпечити централізоване програмне управління всією мережевою інфраструктурою. Розроблена схема може використовуватись як навчальний стенд для дослідження можливостей технології NFV.

УДК 621.396.2

Д.О. Романюк, В.П. Климчук
Державний університет
«Київський авіаційний інститут», м. Київ

РОЗРОБКА ТА АНАЛІЗ ТЕЛЕМЕТРИЧНОЇ СИСТЕМИ ДЛЯ МАЛИХ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ

У сучасній радіоелектроніці телеметрична система безпілотного літального апарату (БПЛА) є критично важливим апаратно-програмним комплексом, що забезпечує дистанційний моніторинг, збір та двосторонню передачу параметрів функціонування об'єкта в режимі реального часу. Для малих БПЛА, які мають суворі обмеження щодо масогабаритних показників та енергоспоживання, розробка високоефективних телеметричних каналів є фундаментом безпечної експлуатації. Необхідність безперервного контролю просторової орієнтації, навігаційних даних та стану енергетичних підсистем вимагає створення надійних радіоканалів, здатних працювати в умовах складної електромагнітної обстановки, інтенсивних завад та на значних відстанях від наземної станції керування.

У роботі проведено комплексне дослідження архітектури телеметричних систем та обґрунтовано вибір протоколу MAVLink як основного стандарту обміну даними, що забезпечує високу щільність упакування інформації та стійкість до втрат пакетів. Для підвищення надійності радіолінії на канальному рівні реалізовано алгоритми прямої корекції помилок (Forward Error Correction, FEC) та циклічного надлишкового кодування (CRC). На фізичному рівні (PHY) досліджено використання частотної маніпуляції з гауссівською фільтрацією (GFSK), що дозволяє звузити смугу випромінювання та зменшити позасмугові завади. Особливу увагу приділено розробці вбудованого програмного забезпечення на базі 32-бітних мікроконтролерів архітектури ARM Cortex-M з використанням подійно-орієнтованої архітектури Bare-metal. Такий підхід, у поєднанні з реалізацією скінченних автоматів (FSM) та механізмів прямого доступу до пам'яті (DMA), дозволив мінімізувати апаратні затримки під час трансляції пакетів та гарантувати стабільну роботу системи в умовах жорсткого реального часу без блокування обчислювального ядра процесора.

Окрему увагу приділено апаратній реалізації пристрою. Застосовано багатошарову топологію з розділенням цифрових та аналогових

(ВЧ) полігонів заземлення, а також встановлено екрануючі контури для захисту радіотракту від електромагнітних наведень з боку безколекторних моторів та силових установок БПЛА.

Для досягнення максимальної дальності зв'язку було розроблено оптимізовану асиметричну антенну систему. На борту БПЛА використано компактну всеспрямовану дипольну антену, тоді як наземна станція керування оснащена спрямованою антеною типу хвильовий канал з високим коефіцієнтом підсилення. Інтеграція розробленого апаратно-програмного комплексу з популярними відкритими платформами наземних станцій (наприклад, QGroundControl та Mission Planner) підтвердила коректність парсингу телеметричних пакетів та стабільність відображення польотних завдань на інтерфейсі оператора.

В межах практичної реалізації проєкту було створено фізичний прототип малогабаритного радіомодема. Лабораторні вимірювання інструментально підтвердили досягнення розрахункових характеристик: вихідна потужність передавача склала +22 дБм при збереженні високої енергоефективності (струмоспоживання у режимі передачі не перевищує 130 мА). Ключовим етапом дослідження стали натурні льотні випробування комплексу у складі реального БПЛА. Експериментально зафіксовано стійкий дуплексний обмін даними на дистанціях понад 10 км за умов прямої радіовидимості (LOS), при цьому рівень втрати пакетів залишався в межах 1%, навіть при критичних значеннях відношення сигнал/шум. Використання технології псевдовипадкового переналаштування робочої частоти під час випробувань дозволило значно підвищити стійкість каналу до впливу вузькосмугових завад.

Результати проведеного дослідження підтверджують високу ефективність запропонованих інженерних рішень та їх готовність до впровадження у серійне виробництво. Оптимізація програмно-апаратних засобів обробки сигналів дозволила досягти компромісу між дальністю дії та енергоспоживанням системи. Розроблена телеметрична система може бути використана як універсальна база для створення інтелектуальних комплексів моніторингу для потреб цивільної авіації та спеціальних підрозділів. Перспективи подальших досліджень полягають у впровадженні алгоритмів адаптивної зміни швидкості передачі даних залежно від стану радіоефіру, а також інтеграції криптографічних протоколів апаратного шифрування стандарту AES-128/256 для надійного захисту телеметричних даних від перехоплення та підміни (спуфінгу).

УДК 621.396.2

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

АНАЛІЗ ТА ПРОЄКТУВАННЯ ГІГАБІТНИХ ГІБРИДНИХ ВОЛОКОННО-КОАКСІАЛЬНИХ МЕРЕЖ ДОСТУПУ

Стрімке зростання попиту на надшвидкісний широкосмуговий доступ до мережі Інтернет спонукає операторів кабельного телебачення до радикальної модернізації існуючих мережевих інфраструктур. Традиційні гібридні волоконно-коаксіальні мережі (HFC), що десятиліттями домінували на ринку багатосервісних послуг, сьогодні стикаються з фізичними обмеженнями пропускної здатності коаксіального сегмента. Впровадження технологій гігабітного класу вимагає не лише оновлення активного обладнання, але й концептуальної зміни архітектури мережі в бік глибшого проникнення оптики (Fiber Deep) та переходу до розподіленої архітектури доступу (Distributed Access Architecture, DAA). Актуальність дослідження зумовлена необхідністю забезпечення конкурентоспроможності HFC-мереж у порівнянні з повністю оптичними топологіями (FTTH) за умови збереження наявних коаксіальних активів.

У роботі проведено ґрунтовний аналіз еволюції архітектури HFC та стандартів сімейства DOCSIS. Обґрунтовано перехід до версій DOCSIS 3.1 та 4.0, які використовують технологію багаточастотного мультиплексування з ортогональним частотним розділенням (OFDM/OFDMA) та модуляцію вищого порядку до 4096-QAM у поєднанні з високоефективними алгоритмами виправлення помилок з низькою щільністю перевірок на парність (LDPC). Досліджено специфіку коаксіального сегмента мережі, де основними дестабілізуючими факторами є накопичення шумів інверсії у зворотному каналі (Ingress Noise) та значне загасання сигналу на високих частотах. Запропоновано методи підвищення пропускної здатності шляхом розширення робочого діапазону частот до 1.2 ГГц (або до 1.8 ГГц у рамках специфікації Extended Spectrum DOCSIS – ESD) та впровадження гнучкого частотного планування з використанням архітектури High-Split для радикального розширення смуги зворотного (Upstream) каналу. Крім того, імплементація інструментів проактивного обслуговування мережі (Proactive Network Maintenance, PNM) на базі аналізу коефіцієнтів пе-

редікажень (Pre-equalization) дозволяє локалізувати мікропошкодження коаксіального кабелю та деградацію конекторів ще до моменту виникнення критичних збоїв у клієнтському сервісі.

В межах проєктування гігабітного сегмента мережі виконано детальний розрахунок бюджету втрат в оптичній та коаксіальній частинах тракту. Здійснено вибір оптимальної топології, що базується на принципі сегментації оптичних вузлів (Node Splitting) та винесенні фізичного рівня (PHY) з головної станції безпосередньо в оптичний вузол за допомогою технології Remote PHY (R-PHY). Це дозволяє радикально зменшити кількість абонентів на один спільний частотний ресурс, знизити рівень каскадування підсилювачів та нівелювати вплив аналогових оптичних шумів. Окремим вектором оптимізації стало використання віртуалізованих конвергентних платформ доступу (vCCAP), що дає змогу централізувати управління абонентськими сесіями на базі SDN-контролерів, суттєво зменшити енергоспоживання головних станцій та підвищити загальну відмовостійкість ядра мережі. Математично верифіковано показники якості сигналу, зокрема рівень модуляційної помилки (MER) та ймовірність бітової помилки (BER), що підтвердило стабільність роботи системи при трансляції гігабітних потоків даних. Розроблено структурну схему модернізованого сегмента, яка забезпечує високу відмовостійкість та підтримку механізмів Quality of Service (QoS).

Техніко-економічне порівняння запропонованого рішення продемонструвало, що модернізація HFC до рівня гігабітного доступу є значно рентабельнішою за повну заміну мережі на FTTH на етапі перехідного періоду. Використання існуючої кабельної інфраструктури в синергії з сучасними стандартами DOCSIS та вузлами DAA дозволяє досягти швидкостей, порівнянних з оптичними лініями, при значно менших капітальних витратах (CAPEX) та суттєвому зниженні операційних витрат (OPEX) за рахунок автоматизації технічного обслуговування. Результати роботи можуть бути використані операторами зв’язку для стратегічного планування розвитку мультисервісних мереж у житлових масивах із щільною забудовою.

УДК 621.394.4 (043.2)

Дмитро ТИМОФІЄВ, Олександр ЛАВРИНЕНКО
Державний університет «Київський авіаційний інститут», м. Київ

МУЛЬТИСЕРВІСНА МЕРЕЖА КОРПОРАТИВНОГО ЗВ'ЯЗКУ ДЛЯ СТАЦІОНАРНИХ ТА МОБІЛЬНИХ АБОНЕНТІВ

В умовах глобальної цифрової трансформації та масштабної модернізації бізнес-сектору, розгортання передових інфокомунікаційних технологій стає фундаментальною умовою ефективного функціонування сучасного підприємства. Операційна діяльність у 2026 році характеризується переходом до гібридних форматів роботи та активним впровадженням ресурсоємних сервісів, таких як ERP-системи, хмарні бази даних та корпоративний відеоконференцзв’язок надвисокої чіткості. Класичні підходи до побудови локальних мереж, що базуються на застарілих стандартах бездротового зв'язку та розділеній кабельній інфраструктурі, вже не здатні задовольнити зростаючі потреби у мобільності персоналу. Саме тому перехід до мультисервісних мереж зв'язку нового покоління (NGN) з глибокою інтеграцією технологій бездротового доступу є вкрай актуальним інженерним завданням. У даній роботі розроблено та обґрунтовано комплексне проєктне рішення щодо створення відмовостійкої корпоративної мультисервісної мережі, яка гармонійно поєднує технології фіксованого дротового зв'язку та широкосмугового бездротового доступу стандарту Wi-Fi 6E/7. Це дозволяє забезпечити швидкісний доступ як для стаціонарного серверного обладнання, так і для рухомих абонентів.

Рис. 1. Структурна логічна схема сучасної корпоративної мультисервісної мережі (NGN)

Центральним інтелектуальним ядром розробленої архітектури виступає програмний комутатор (Softswitch), який гнучко координує логіку обслуговування викликів. Використання протоколів SIP та стека MGCP/MEGACO гарантує надійне управління мультимедійним трафіком та підтримку корпоративної IP-телефонії за стандартом Voice over Wi-Fi (VoWiFi). Для математичного та топологічного обґрунтування архітектури було проведено системний аудит фізичного простору підприємства із загальною корисною площею 474 кв. м, що поділена на 14 ізольованих ділянок. Виявлена апаратна гетерогенність мережі включає 24 стаціонарних ПК, 33 портативних ноутбуки, 49 смартфонів та локальний серверний кластер. Моделювання зон бездротового радіопокриття здійснювалося із застосуванням спеціалізованого програмного середовища автоматизованого радіопланування, що враховує коефіцієнти загасання сигналу крізь архітектурні перешкоди.

Рис. 2. карта (Heatmap) радіопокриття Wi-Fi в одноповерховому офісі підприємства площею близько 500 м^2

Аналіз результатів моделювання підтвердив, що обрана просторова конфігурація точок доступу стандарту IEEE 802.11ax (Wi-Fi 6) забезпечує стовідсоткове гарантоване інформаційне покриття робочих зон. Впровадження технологій MU-MIMO та OFDMA повністю задовольняє вимоги до пропускної здатності навіть в умовах одночасної роботи всіх мобільних терміналів. У підсумку, спроєктована інфраструктура мультисервісної мережі зв'язку є цілісним та масштабова-

ним інженерним рішенням. Її практичне впровадження дає змогу підприємству повністю ліквідувати мережеві «вузькі місця», організувати безпечний безшовний роумінг по всій території об'єкта та підвищити загальну надійність передачі даних, що безпосередньо впливає на зростання економічної та управлінської ефективності компанії.

Список використаних джерел

1. Бондаренко В. М., Лисенко О. М. Аналіз ефективності технології MU-MIMO в корпоративних мережах стандарту IEEE 802.11ax. Зв'язок. 2021. № 3. С. 15–22.
2. Шевченко Т. Г., Бойко О. В. Проєктування телекомунікаційних мереж на базі протоколу SIP для взаємодії з ТМЗК. Вісник Національного авіаційного університету. 2023. № 1. С. 45–53.
3. Ткачук Р. В. Основи IP-телефонії та уніфікованих комунікацій: навчальний посібник. Львів : Видавництво Львівської політехніки, 2024. 312 с.
4. Кравченко Н. І. Оптимізація спектральної ефективності мереж ЛОМ за допомогою OFDMA. Радіоелектроніка, інформатика, управління. 2022. № 4. С. 112–120.
5. Kim S., Lee J. Target Wake Time Scheduling Optimization in 802.11ax. IEEE Internet of Things Journal. 2023. Vol. 10, No. 4. P. 2045–2055.
6. Al-Hassani R. Comparative Analysis of SIP and MGCP in Modern Enterprise Environments. International Journal of Communication Systems. 2021. Vol. 34, No. 8. P. e4800.
7. Tanaka Y. Interference Mitigation in Dense Wi-Fi Deployments using Directional Antennas. IEEE Transactions on Antennas and Propagation. 2021. Vol. 69, No. 10. P. 6023–6034.
8. Brown S., Taylor P. Cluster Analysis Applications in Wireless Node Placement. Journal of Network Planning. 2025. Vol. 12, No. 1. P. 15–28.
9. Гриценко В. В. Застосування платформи Asterisk для побудови відмовостійких систем голосового зв'язку в розподілених офісах. Інформаційно-керуючі системи. 2022. № 5. С. 40–47.
10. Романенко Ю. І., Костюк П. П. Оцінка накладної інформації в заголовках протоколів стеку RTP/UDP/IP при передачі голосового трафіку. Телекомунікаційні та інформаційні технології. 2026. № 1. С. 55–61.

УДК 621.391

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

КРИПТОГРАФІЧНО ЗАХИЩЕНА АВТОНОМНА СИСТЕМА АВТОМОБІЛЬНОЇ СИГНАЛІЗАЦІЇ З TELEGRAM-ІНТЕГРАЦІЄЮ

Стандартні автономні сигналізації можуть надати лише психологічний тиск на зловмисника за рахунок сирени, а дешеві датчики з китайський маркетплейсів мають слабкість до хибних спрацювань, через що від вітру, сирена почне надоїдати усім перехожим без причини. Але і звук сирени не завжди допомагає і потрібне власне втручання у ситуацію. Системи з дистанційним повідомленням тривоги – GPS трекери з GSM модулем, зазвичай споживають забагато електроенергії, тому вимушені підключатися до автомобільних акумуляторів, через що їх неможливо встановити на велосипед, або електросамокат. Так як звичайні сигналізії працюють за відкритими радіопротоколами і всім відомими частотами 433 – 868 МГц, професійні крадії можуть навіть не здіймаючи тривоги сигналізації, просто зняти її з охорони перехопивши радіосигнал за допомогою кодграберів і сканерів. Саме тому стандартні системи без криптографічного захисту є абсолютно беззахисним від професійних викрадачів.

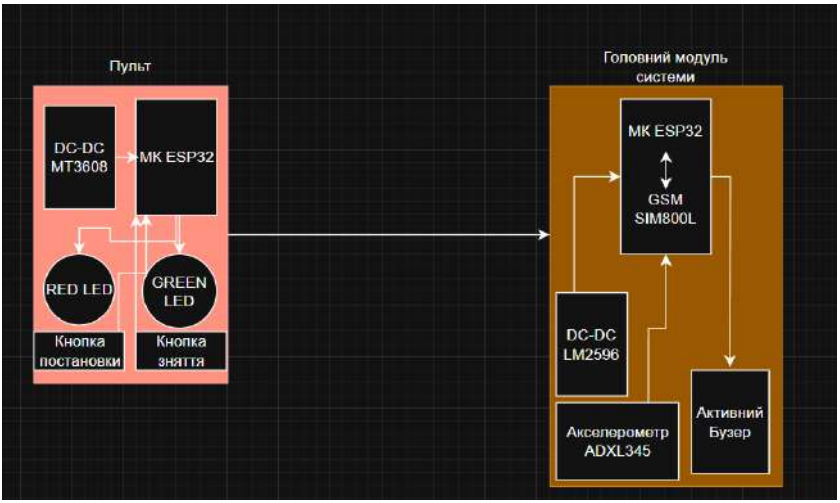
Система охорони автомобіля не тільки про дальність зв’язку та функціональне різноманіття. Якщо доступом до керування системою може отримати зловмисник, то сенсу від такої системи нема, бо не забезпечує очікуваний захист. Поява портативних “хакерських” пристроїв, напр. FlipperZero або на базі чіпа HackRF, обхід системи став більш доступним і легшим. Зловмисники мають декілька засобів для взлому системи охорони, такі як кодграбери, перехоплення сигналу, ретрансляція.

Найкраща протидія таким крадіям – це криптографічний захист каналу зв’язку, який дозволяє повністю обнулити загрозу перехоплення сигналу або взлому системи. Такий захист використовується в дорогих сегментах сигналізацій. У розробленому проєкті використовується алгоритм симетричного блочного шифрування AES-128. Цей алгоритм оперує 128-бітними блоками даних, який використовує ключ довжиною 128 біт. У еру цифрових технологій, де кожний може в

Інтернеті подивитися способи взлому сигналізацій це мінімальний надійних захист для дорогої техніки. Навіть маючи інформацію про те чим захищений транспорт, використовуючи повний перебор унікальних ключів для 128 бітного криптографічного захисту при величезній кількості ключей потрібно буде витратити більше трільйона років, маючи найпотужніший комп'ютер

Запланована система має функціонал детекту нахилу, удару по транспорту, підтримка серверу, надсилання стану системи на сервер за рахунок глобального каналу зв'язку через GSM, звукове сповіщення та можливість керування системою з іншого трансивера. Ділимо систему на два модуля – пульт, через який буде проходити керування системою (зняття, постановка під охорону) та головний модуль, який буде відповідати за сервер, звукове сповіщення, детект удару та зрушення транспорту. Споживання реалізовано через батарейки типу CR123A 3V 1.5A.

Без оптимізації компоненти працюють постійно у повнофункціональних статичних режимах. МК постійно активні, відбувається безперервне зчитування з сенсорів, а бездротові модулі постійно утримують безперервне з'єднання, в той час коли в конфігурації з оптимізацією вопроваджено апаратні переривання датчка, режими глибокого та модемного сну, а також роботи GSM трансивера в режимі сесій.



УДК 621.391

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

ОПТИМІЗАЦІЯ ІНФРАСТРУКТУРИ СУЧАСНИХ ЦОД НА БАЗІ ТЕХНОЛОГІЇ SWDM ТА ШИРОКОСМУГОВИХ ВОЛОКОН OM5

Перехід архітектури сучасних корпоративних, комерційних та хмарних центрів обробки даних (ЦОД) до технологій надвисокої щільності безпосередньо продиктований експоненційним зростанням обсягів хмарних обчислень та активним впровадженням систем штучного інтелекту. Подібна гіпермасштабованість, що реалізується через плоску дворівневу мережеву архітектуру Spine-Leaf та програмно-визначені мережі (SDN), вимагає колосальної кількості оптичних міжсерверних з'єднань. У цих умовах вибір оптимального фізичного середовища та технологій ущільнення стає критичним фактором для забезпечення пропускної здатності без дороговартісної фізичної реконструкції інженерних систем.

Аналіз технологій спектрального мультиплексування:

- Використання стандартів CWDM та DWDM є безальтернативним для магістральних та міських оптичних мереж, проте їх застосування всередині ЦОД на дистанціях до 150 метрів є економічно недоцільним через високу вартість трансиверів та систем термостабілізації.
- Технологія короткохвильового спектрального ущільнення (SWDM) виступає найбільш енергоефективним та фінансово виправданим рішенням для локальних підключень (ToR/EoR комутація).
- Застосування чотирьох довжин хвиль (850, 880, 910 та 940 нм) дозволяє передавати високошвидкісні сигнали (40G та 100G) по одному дуплексному багатомодовому волокну з роз'ємами типу LC.
- Це виключає необхідність переходу на складну паралельну оптику (роз'єми MPO/MTP), скорочує потребу у фізичних волокнах на 75% та суттєво розвантажує кабельні магістралі, покращуючи циркуляцію охолоджуючого повітря.

Фізичне середовище передачі та дисперсійні обмеження:

- Класичні стандарти OM3 та OM4, оптимізовані для роботи на довжині хвилі 850 нм, виявилися недостатньо ефективними для впровадження швидкостей 400G та 800G.

- Оптимальним середовищем для SWDM є новітнє широкосмугове багатомодове волокно OM5 (WBMMF) з градієнтним профілем, яке гарантує високу модову смугу пропускання в діапазоні від 850 до 953 нм та збільшує дальність передачі 100G до 150 метрів.
- Для нарощування пропускної здатності до 50 Гбіт/с та 100 Гбіт/с на канал впроваджено формат модуляції PAM4, який подвоює пропускну здатність, кодуючи 2 біти за такт.

Механізми надійності та математичне обґрунтування:

- Використання алгоритмів прямої корекції помилок (FEC) є критичною вимогою для ліній з модуляцією PAM4.
- Алгоритми RS-FEC знижують частоту бітових помилок (BER) з критичного рівня 10^{-5} до безпомилкового показника 10^{-12}.
- Математичне моделювання за допомогою марковських процесів з безперервним часом доводить абсолютну необхідність апаратного резервування.
- Моделювання системи з гарячим резервуванням ліній зв'язку (за схемою 1+1) продемонструвало видатні показники надійності.

Економічна доцільність (CAPEX)

Проектування сегменту дата-центру на 1000 серверів підтвердило високу ефективність архітектури Spine-Leaf у комбінації з волокнами OM5 та трансиверами 100G-SWDM4 і 400G-SR4.2. Комплексний економічний аналіз доводить, що такий підхід дозволяє оптимізувати початкові капіталовкладення (CAPEX) на 30-40% порівняно з розгортанням виключно одномодової мережі, зберігаючи при цьому потенціал для подальшого масштабування.

Висновки

Технологія SWDM у комбінації з волокном OM5 є високоефективним перехідним рішенням, яке дозволяє ЦОД максимально продовжити життєвий цикл багатомодової інфраструктури та оптимізувати витрати під час впровадження швидкостей 40G та 100G. Водночас, для швидкостей 400G+ та відстаней понад 150 метрів спостерігається стратегічний зсув індустрії у бік одномодового волокна (OS2). Відповідно, сучасне проектування гіпермасштабованих дата-центрів вимагає комбінованого підходу: багатомодові рішення (OM5/SWDM) застосовуються на рівні доступу між серверами, тоді як одномодові формують базову магістральну архітектуру.

УДК 621.391

Д.Є. Устенко, Ю. В. Петрова
Державний університет
«Київський авіаційний інститут», м. Київ

СИСТЕМА БЕЗКОНТАКТНОГО ОБМІНУ ДАНИМИ НА ОСНОВІ ТЕХНОЛОГІЇ NFC

У сучасних інформаційних системах важливого значення набувають технології швидкого, зручного та безпечного бездротового обміну даними. Однією з найбільш перспективних технологій малого радіуса дії є NFC (Near Field Communication), яка забезпечує безконтактну передачу інформації між електронними пристроями на невеликій відстані. NFC активно використовується у платіжних системах, електронній ідентифікації, системах контролю доступу, транспортних сервісах та IoT-пристроях.

Основною перевагою технології NFC є можливість автоматичного встановлення з'єднання між пристроями без складного налаштування та використання додаткових кабельних інтерфейсів. Технологія працює на частоті 13,56 МГц та базується на принципах радіочастотної ідентифікації RFID. Завдяки малому радіусу дії NFC забезпечує підвищений рівень безпеки під час передачі інформації.

Метою роботи є дослідження принципів побудови системи безконтактного обміну даними на основі технології NFC та реалізація системи зчитування інформації за допомогою NFC-міток.

У роботі проведено аналіз сучасних NFC-систем, стандартів та протоколів передачі даних. Особливу увагу приділено NFC-міткам типу NTAG213, які відповідають специфікації NFC Forum Type 2 та підтримують формат NDEF (NFC Data Exchange Format). Перевагою NTAG213 є відсутність необхідності використання окремого джерела живлення, оскільки живлення мітки здійснюється за рахунок електромагнітного поля NFC-зчитувача.

Для реалізації системи використано NFC-мітки NTAG213, смартфон із підтримкою NFC та програмне забезпечення NFC Tools. За допомогою мобільного застосунку виконувалось формування та запис NDEF-повідомлень службового типу. У роботі використовувалися тестові записи такого формату:

ID=001;ROLE=STUDENT;ACCESS=ALLOW
ID=002;ROLE=USER;ACCESS=DENY

Запропонована структура повідомлення дозволяє реалізувати базову систему ідентифікації користувачів та контролю доступу. Після запису інформації на NFC-мітку виконувалося зчитування та подальша обробка отриманих даних.

У процесі роботи було розроблено структуру системи безконтактного обміну даними та алгоритм її функціонування. Проведено тестування працездатності системи за різних умов експлуатації. Досліджено вплив відстані між NFC-міткою та зчитувачем на стабільність передачі даних. Результати експериментів підтвердили, що найбільш стабільна робота системи забезпечується на малих відстанях, що відповідає особливостям технології NFC.

Також у роботі проаналізовано економічну доцільність використання NFC-технології. Встановлено, що запропонована система характеризується низькою вартістю впровадження, не потребує складного обладнання та може бути реалізована із використанням доступних апаратних і програмних засобів. Використання готового програмного забезпечення NFC Tools дозволяє значно скоротити час розробки та спростити налаштування системи.

Результати дослідження підтвердили можливість створення ефективної системи безконтактного обміну даними на основі NFC. Основними перевагами запропонованого рішення є простота використання, сумісність із сучасними мобільними пристроями, енергоефективність та можливість подальшого розвитку системи для задач автоматизації, ідентифікації користувачів та контролю доступу.

Перспективним напрямом подальшого розвитку систем безконтактного обміну даними є інтеграція NFC-технології з IoT-пристроями та хмарними сервісами. Поєднання NFC із системами автоматизації дозволяє реалізовувати розумні системи доступу, моніторингу та керування обладнанням у режимі реального часу. Крім того, використання мобільних пристроїв як універсальних NFC-зчитувачів значно спрощує взаємодію користувачів із системою та зменшує витрати на додаткове обладнання.

Окрему увагу необхідно приділяти питанням інформаційної безпеки під час передачі даних через NFC. Незважаючи на малу відстань передачі сигналу, існує необхідність застосування додаткових механізмів захисту. Використання сучасних засобів захисту дозволяє підвищити надійність системи та забезпечити безпечне використання NFC-технології у практичних застосуваннях.

УДК 004.7:621.39 (043.2)

Євгеній ХІВРИЧ, Денис БАХТІЯРОВ, Сергій СОВА
Державний університет «Київський авіаційний інститут», м. Київ

МЕТОД ЗМЕНШЕННЯ ОБСЯГУ ДАНИХ IOT-ПРИСТРОЇВ ДЛЯ ЕФЕКТИВНОЇ ПЕРЕДАЧІ У БЕЗДРОТОВИХ МЕРЕЖАХ

Вступ. Сучасний етап розвитку інформаційних технологій характеризується стрімкою експансією систем Інтернету речей (IoT) в усі сфери життєдіяльності. Проте масове розгортання автономних сенсорних мереж створює ряд технічних викликів, головним серед яких є обмежена пропускна здатність бездротових каналів зв'язку та дефіцит енергетичних ресурсів кінцевих вузлів. Традиційна хмарно-орієнтована модель, де вся первинна інформація передається на центральний сервер для обробки, стає малоефективною при роботі з протоколами LPWAN (наприклад, LoRaWAN або NB-IoT), оскільки надмірний трафік призводить до колізій та передчасного вичерпання заряду батарей.

Аналіз проблеми та архітектурні рішення. Для вирішення зазначених проблем у роботі пропонується використання концепції периферійних обчислень (Edge Computing). Вона передбачає перенесення функцій аналізу та фільтрації даних безпосередньо на рівень кінцевих пристроїв або локальних шлюзів. Це дозволяє кардинально змінити парадигму передачі: замість неперервного потоку «сирих» даних мережею курсують лише змістовні події або агреговані показники.

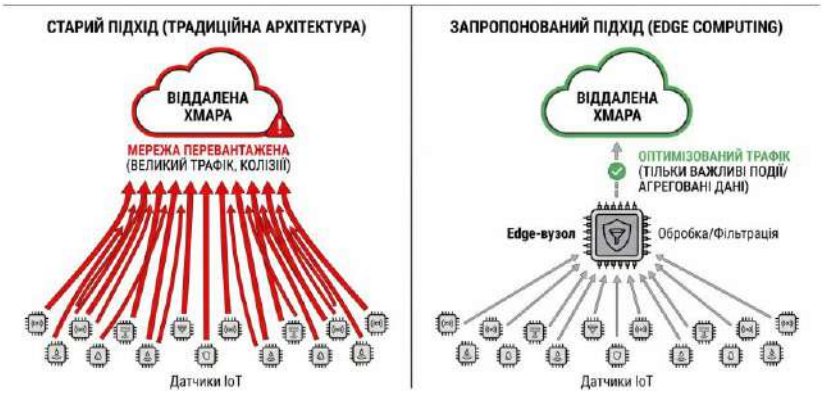


Рис. 1. Порівняння архітектури IoT мереж
(традиційна хмарна vs периферійні обчислення)

Методи оптимізації обсягу даних. У дослідженні розроблено інтегрований метод, що базується на трьох компонентах: просторово-часовій агрегації, кореляційному стисненні та алгоритмі подвійного прогнозування (DPA). Агрегація дозволяє об'єднувати вимірювання від групи функціонально подібних сенсорів, усуваючи дублювання ідентичного контексту. Кореляційне стиснення використовує математичні залежності між послідовними відліками фізичних величин, таких як температура чи вологість, для зменшення розрядності переданих значень.

Особлива увага приділена алгоритму подвійного прогнозування. Суть методу полягає у функціонуванні ідентичних прогностичних моделей на сенсорному вузлі та сервері. Передача даних ініціюється лише у випадку, якщо реальне значення x(t) відхиляється від прогнозованого x'(t) на величину, що перевищує заданий поріг ε. Це забезпечує динамічне підлаштування системи під мінливість навколишнього середовища.

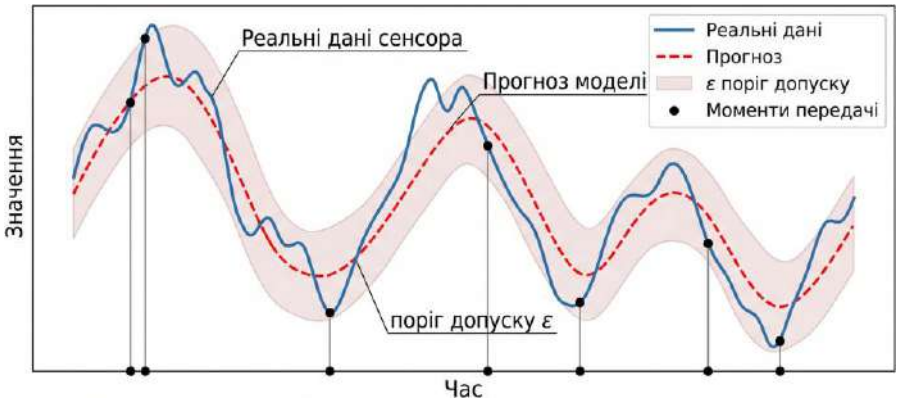


Рис. 2. Принцип адаптивної передачі даних за порогом ε

Результати моделювання. Для верифікації методу було проведено імітаційне моделювання у середовищі MATLAB. В якості тестових даних використано реальні часові ряди параметрів мікроклімату. Встановлено, що при допустимій похибці у 2-3%, обсяг переданого трафіку скорочується на 70-85%. Таке зниження активності радіомодуля дозволяє збільшити термін автономної роботи пристрою від стандартного джерела живлення у 1.5-2 рази. Крім того, математично об-

ґрунтовано зменшення ймовірності колізій у мережах з топологією «зірка», що підвищує загальну надійність системи моніторингу.

Висновки. Застосування периферійної обробки та інтелектуальних методів зменшення надмірності даних є критично необхідним для побудови масштабованих систем IoT. Запропонований метод дозволяє ефективно використовувати ресурс бездротових мереж, забезпечуючи високу точність контролю при мінімальних витратах енергії. Отримані результати можуть бути інтегровані у промислові рішення для автоматизації будівель та екологічного моніторингу.

Список використаних джерел

1. Singh A. K., Kumar N. A Novel Hybrid Compression Technique for IoT Medical Data over Low Bandwidth Channels // Multimedia Tools and Applications. – 2022. – Vol. 81. – P. 4567–4585.
2. Sun L., Du Q. Energy-Efficient Data Aggregation for UAV-Assisted IoT Networks // IEEE Wireless Communications Letters. – 2021. – Vol. 10, No. 9. – P. 1984–1988.
3. Tan H., Wang X. Multi-level Data Aggregation and Compression in Edge-Cloud IoT Systems // Future Generation Computer Systems. – 2023. – Vol. 141. – P. 34–45.
4. Wang Y., Chen H. Spatial-Temporal Data Compression for Massive IoT Connectivity // IEEE Communications Magazine. – 2022. – Vol. 60, No. 1. – P. 56–62.

УДК 004.942:534.8:629.7.072.8

В.Ю. Циганок, Р.С. Одарченко
Державний університет «Київський авіаційний інститут», м. Київ

МЕТОДИ ТА МОДЕЛІ СИНТЕЗУ АКУСТИЧНИХ СИГНАЛІВ ДЛЯ АВІАЦІЙНИХ ТРЕНАЖЕРІВ У СТРУКТУРІ ІКС

У сучасному світі підготовка авіаційного персоналу вимагає використання повнопілотажних тренажерів найвищого рівня (Level D). Такі симулятори є складними інформаційно-комунікаційними системами (ІКС), які обробляють гігабайти телеметричних даних у реальному часі. Традиційно розробники приділяють найбільшу увагу візуалізації та динаміці польоту, проте акустичне середовище кабіни пілота є не менш критичним каналом передачі інформації. Звуковий фон дозволяє екіпажу інтуїтивно оцінювати режими роботи двигунів, аеродинамічні навантаження, випуск механізації та роботу бортових систем.

Існуючі методи генерації звуку в тренажерах переважно базуються на семплуванні - відтворенні заздалегідь записаних аудіофайлів. Цей підхід має суттєвий недолік: він не здатний адекватно відтворювати перехідні процеси. Семпли звучать статично, а спроби їх мікшування призводять до фазових спотворень і неприродних артефактів. Головна мета даної роботи - розробити підхід, який дозволяє математично змоделювати кожен звук залежно від того, що робить пілот, відмовившись від статичних аудіофайлів на користь динамічного алгоритмічного синтезу.

Пропонується модель синтезу акустичних сигналів, що функціонує як окремий вузол у мережі симулятора. Основою моделі є генерація звукових хвиль шляхом розв'язання диференціальних рівнянь, що описують фізичні процеси в літаку. Сигнал генерується безперервно, а його параметри (амплітуда, частота, спектральний склад) жорстко прив'язані до поточних дій екіпажу та телеметрії.

Наприклад, звук роботи турбовентиляторного двигуна моделюється як суперпозиція гармонічних коливань. Базова частота коливань f_0 розраховується в реальному часі як функція від обертів роторів (N_1 та N_2), положення важеля керування двигуном (ВКД), що задає пілот, та щільності повітря:

$$s(t) = \sum_{i=1}^{k} A_i(\alpha, v) \cdot \sin(2\pi f_i(N_1, N_2)t + \phi_i) + W(t, M)$$

де A_i - динамічна амплітуда і-ї гармоніки, що залежить від кута атаки α та швидкості v; $W(t, M)$ - функція формування аеродинамічного шуму, що масштабується залежно від числа Маха M. Будь-який рух ВКД, здійснений пілотом, миттєво змінює змінні N_1 та N_2 у мережевому пакеті, що одразу впливає на обчислення функції, унеможливлюючи акустичну затримку.

Для реалізації такого підходу в структурі ІКС тренажера пропонується наступна архітектура обробки даних (рис. 1).

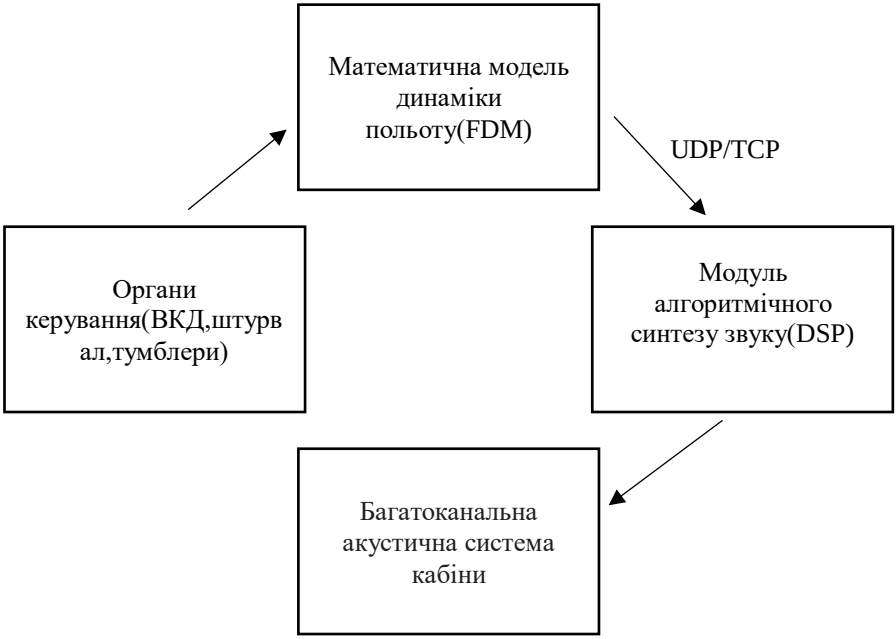


Рис. 1. Структурна схема алгоритмічного синтезу акустичних сигналів в ІКС тренажера

Як видно зі схеми, мережева взаємодія між модулем динаміки польоту та підсистемою звуку здійснюється через протоколи UDP. Це забезпечує мінімальну затримку (latency) при передачі команд пілота. Для усунення розривів у звучанні при частоті оновлення мережевих

пакетів у 60 Гц застосовується сплайн-інтерполяція параметрів між отриманими значеннями.

Окремо розраховується просторова локалізація джерел звуку. Якщо пілот перемикає конкретний тумблер на верхній панелі (Overhead panel), система вираховує імпульсний відгук кабіни (Impulse Response) для цих координат, накладаючи відповідний реверберaційний фільтр. Це забезпечує точне позиціонування звуку в тривимірному просторі кабіни без використання записаних семплів перемикачів.

Впровадження запропонованої математичної моделі синтезу дозволяє повністю відмовитися від великих баз даних аудіофайлів, що значно знижує навантаження на дискову підсистему тренажера. Звукова картина стає абсолютно неперервною, вона детально і без затримок реагує на кожну дію пілота (аж до зміни звуку від тертя шасі при різному зусиллі натискання на педалі гальма), що підвищує загальний рівень психофізіологічної адекватності тренажера та якість навчання льотного складу.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 № 80/94-ВР.

2. Бойко Ю. В., Мельник О. С. Математичне моделювання акустичного середовища кабіни пілота в умовах динамічних аеродинамічних навантажень. Наукоємні технології. 2024. № 2. С. 34–41.

3. Васильєв В. М., Романенко О. І. Цифрова обробка акустичних сигналів та фізичне моделювання у віртуальних середовищах. Вісник Київського політехнічного інституту. Серія: Радіотехніка. Радіоапаратобудування. 2022. Вип. 88. С. 15–22.

4. Müller J., Schmidt A. Real-time physical modeling of turbofan engine acoustics for flight simulators. Journal of the Audio Engineering Society. 2024. Vol. 72, No. 3. P. 112–125.

5. Zhao Y., Li H., Wang X. Low-latency UDP-based communication architecture for distributed flight simulation systems. IEEE Transactions on Aerospace and Electronic Systems. 2023. Vol. 59, No. 2. P. 1450–1462.

6. European Union Aviation Safety Agency (EASA). CS-FSTD(A) Certification Specifications for Aeroplane Flight Simulation Training Devices. Issue 3. Cologne: EASA, 2022. 210 p.

7. Smith J. O. Real-Time Acoustic Modeling and Signal Processing for Virtual Environments. 2nd ed. Stanford: W3K Publishing, 2021. 412 p.

УДК 621.396.24:004.7 (043.2)

Дмитро ЧЕРНИШ, Володимир КЛИМЧУК
Державний університет «Київський авіаційний інститут», м. Київ

СИСТЕМА РАДІОЗВ'ЯЗКУ СТАНДАРТУ NVIS: АРХІТЕКТУРА, ЗАВАДОСТІЙКІСТЬ ТА ІНТЕГРАЦІЯ В СУЧАСНІ IP-МЕРЕЖІ

На сучасному етапі розвитку телекомунікацій, в умовах інтенсивного застосування засобів радіоелектронної боротьби (РЕБ) та потенційного руйнування наземної інфраструктури, критичного значення набуває забезпечення живучості та автономності тактичних і аварійних мереж зв'язку. Супутникові системи, попри високу пропускну здатність, є вразливими до цілеспрямованого придушення, кібератак та мають обмежену доступність у складних фізико-географічних умовах. У зв'язку з цим спостерігається активне впровадження систем короткохвильового (КХ) зв'язку стандарту NVIS (Near Vertical Incidence Skywave – зенітне випромінювання), які використовують іоносферу Землі як природний, глобальний і невразливий рефлектор [1, 3, 5].

Базова концепція NVIS полягає у спрямуванні електромагнітної енергії під кутами, близькими до зеніту (від 70° до 90° відносно горизонту). На відміну від традиційного дальнього КХ-зв'язку (DX), де просторова хвиля відбивається під гострим кутом і формує багатокілометрові «мертві зони» (skip zones), зенітне випромінювання заломлюється у шарі F2 і повертається на поверхню безпосередньо навколо передавача. Це дозволяє сформувати суцільне, рівномірне радіопокриття в радіусі до 400 км, що є абсолютно нечутливим до рельєфу місцевості (гірських масивів, лісів чи щільної міської забудови) [4].

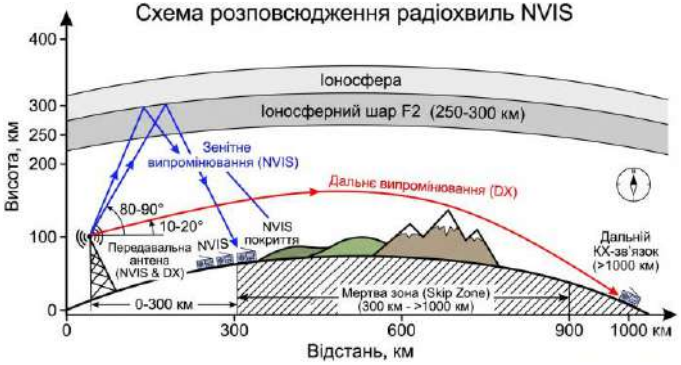


Рис. 1. Векторна схема розповсюдження радіохвиль NVIS

Однак, іоносферний тракт є високодисперсійним та нестаціонарним середовищем. Його параметри жорстко детерміновані добовими циклами сонячної іонізації та явищами космічної погоди (рентгенівськими спалахами, геомагнітними бурями). Ефективність радіолінії NVIS залежить від здатності апаратури балансувати у вузькому частотному вікні між найнижчою застосовною частотою (лімітується тепловим поглинанням у денному шарі D) та критичною частотою відбиття (f_oF2) [2].

Ця специфіка висуває жорсткі вимоги до антенно-фідерних пристроїв. Встановлено, що для забезпечення синфазного додавання прямої та відбитої від землі хвиль у зеніті, оптимальною є висота підвісу горизонтального диполя на рівні 0,15–0,22 довжини хвилі. Таке низьке розташування (2–5 метрів для частот 5 МГц) мінімізує амплітуду поверхневої хвилі (ground wave), радикально знижуючи ймовірність радіоперехоплення ворожими засобами розвідки. Для оптимізації конструкції низькопрофільних антен на мобільних платформах (бронетехніка) доцільним є використання Теорії характерних мод (ТСМ), що дозволяє декомпозувати поверхневі струми на ортогональні моди та ідентифікувати резонанси з ідеальною зенітною спрямованістю [6].

Для боротьби з багатопроменевим розсіюванням (що сягає 3–5 мс через розщеплення на звичайну та незвичайну магнітоіонні складові) та поляризаційним федингом, у роботі розроблено статистичну модель іоносферного каналу. Оскільки класичні порогові методи детектування неефективні при від'ємних значеннях відношення сигнал/шум (SNR), обвідна прийнятого сигналу описується як імовірнісна суміш розподілів Релея (для чисто шумових відліків) та Райса (для сигнальних відліків). Для адаптивної оцінки невідомих параметрів суміші в режимі реального часу застосовано ітераційний алгоритм максимізації математичного сподівання (ЕМ-алгоритм).

Забезпечення гарантованої доставки інформації в таких умовах вимагає переходу на програмно-визначені радіосистеми (SDR) та концепцію QRP (робота малою потужністю до 5–10 Вт). SDR-трансивери з архітектурою прямого оцифрування (Direct RF Sampling) дозволяють реалізувати цифрову фільтрацію з високим динамічним діапазоном, адаптивно звужуючи смугу пропускання та формуючи "нулі" для придушення вузькосмугових завад [7].

Серед форматів модуляції для систем NVIS найвищу завадостійкість демонструють багатотональна частотна маніпуляція (MFSK) та

сімейство протоколів Pactor. Унікальна технологія Memory ARQ (м'яке математичне комбінування пошкоджених пакетів у буфері приймача), реалізована в Pactor-II/IV, забезпечує передачу даних навіть при SNR на рівні -18 дБ. Для широкосмугових сесій оптимальним є стандарт OFDM із застосуванням циклічного префіксу (Cyclic Prefix), який повністю поглинає часове розсіювання сигналу, та каскадного кодування FEC [8].

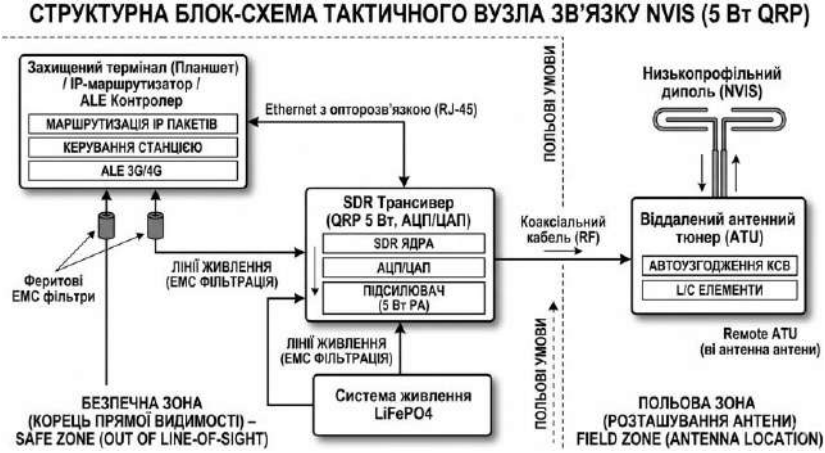


Рис. 2. Структурна блок-схема тактичного вузла зв'язку NVIS

Головним вектором розвитку сучасних систем NVIS є їхня повна інтеграція у глобальні IP-мережі. Цей процес забезпечується використанням систем автоматичного встановлення з'єднання (ALE 3G/4G), які перетворюють трансивер на когнітивний вузол. Контролер ALE у фоновому режимі аналізує матрицю якості каналу (LQA) і динамічно перемикає частоти залежно від стану іоносфери. Для інкапсуляції TCP/IP-трафіку використовуються проксі-сервери (PEP) за стандартом STANAG 5066. Вони нівелюють величезні затримки (RTT) КХ-каналу, надсилаючи локальні підтвердження і запобігаючи розриву транспортних сесій за таймаутом [9-10].

Висновки. Технологія NVIS, завдяки впровадженню алгоритмів програмно-визначеного радіо (SDR), складних статистичних моделей обробки сигналів та завадостійких протоколів (Pactor, OFDM), трансформувалася з резервного аналогового засобу у повноцінний криптозахищений транспортний рівень. Розроблена архітектура малопотужного тактичного комплексу з віддаленим антенним тюнером та когні-

тивним ALE-контролером дозволяє гарантувати доступність каналу та пропускну здатність до 6 кбіт/с у ближній і середній зонах. Це забезпечує ефективну передачу електронної пошти, телеметрії та інтеграцію розрізнених тактичних груп у єдиний мережево-центричний простір в умовах повної відсутності наземної інфраструктури.

Список використаних джерел

1. Witvliet B. A., Alsina-Pagès R. M. Radio communication via Near Vertical Incidence Skywave. IEEE Antennas and Propagation Magazine. 2017. Vol. 59, No. 2. P. 92–115.
2. Богомолов В. М., Козлов С. В. Моделювання іоносферних каналів зв’язку в умовах інтенсивних завад. Зв'язок. 2023. № 2. С. 14–21.
3. Coetzee P. J., du Plessis W. P. Performance Limiters of Near Vertical Incidence Skywave Propagation. IEEE Antennas and Propagation Magazine. 2020. Vol. 62, No. 4. P. 14–23.
4. Miers Z. T. Systematic Antenna Design Using the Theory of Characteristic Modes : doctoral thesis. Lund : Lund University, 2016.
5. STANAG 5066. Profile for High Frequency (HF) Radio Data Communications. Edition 3. Brussels : NATO Standardization Agency, 2014.
6. Горобець В. О., Романюк В. А. Перспективи застосування технології SDR у тактичних радіомережах. Системи озброєння і військова техніка. 2024. Вип. 3. С. 45–52.
7. Gillespie A. F., Trinder S. E., Clark P. D. Performance evaluation of OFDM in HF NVIS channels. IET Communications. 2019. Vol. 13, No. 12. P. 1754–1761.
8. Осадчий О., Ткаченко В. Адаптивне управління ресурсами у когнітивних радіомережах КХ-діапазону. Наукоємні технології. 2024. № 4. С. 101–108.
9. Ільченко М. Є., Кравчук С. О. Сучасні телекомунікаційні системи : монографія. Київ : Наукова думка, 2021. 712 с.
10. ITU-R Recommendation P.533-14. Method for the prediction of the performance of HF circuits. Geneva : International Telecommunication Union, 2019. 24 p.

НАУКОВЕ ВИДАННЯ

ТЕЗИ

XVI МІЖНАРОДНОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

«ПРОБЛЕМИ ЕКСПЛУАТАЦІЇ ТА ЗАХИСТУ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ»

28 ТРАВНЯ 2026 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