МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
Навчально-науковий Інститут комп'ютерних інформаційних технологій
Кафедра комп'ютерних інформаційних технологій

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
Савченко А.С.
"___" лютого 2020 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНА ОСВІТНЬО-КВАЛІФІКАЦІЙНОГО РІВНЯ

"МАГІСТР"

Тема: "Методи та засоби управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих факторів"

Виконала: Козаченко Антоніна Миколаївна

Керівник: проф. Віноградов Микола Анатолійович

Нормоконтролер з ЄСКД (ЄСПД): доц. Райчев Ігор Едуардович

Київ — 2020

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Навчально-науковий Інститут комп'ютерних інформаційних технологій

Кафедра комп'ютерних інформаційних технологій

Освітньо-кваліфікаційний рівень **Магістр**

Напрям (спеціальність) 122 "Інформаційні управляючі системи та технології"

(шифр, найменування)

ЗАТВЕРДЖУЮ

Завідувач кафедри

Савченко А.С.

"14" жовтня 2019 р.

ЗАВДАННЯ

на виконання дипломної роботи студента

Козаченко Антоніни Миколаївни

(прізвище, ім'я, по батькові)

1. Тема роботи: "Методи та засоби управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих факторів" затверджена наказом ректора від "25" вересня 2019 р. №2175/ст.
2. Термін виконання роботи: з 14 жовтня 2019 р. по 09 лютого 2020 р.
3. Вихідні дані до роботи: використовувалися методи теорії імовірностей та математичної статистики, теорії адаптації, теорії конфлікту та конфліктного управління, теорії фільтрації Калмана, комп'ютерне моделювання та розрахунки.
4. Зміст пояснювальної записки (перелік питань, що підлягають розробці): методи та засоби побудови захищеної системи передавання інформації у телекомунікаційних мережах нових поколінь (Next Generation Networks та Future Networks) за наявністю дестабілізуючих факторів з різними типами апріорної невизначеності.

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапу дипломного проекту (роботи)	Термін виконання	Примітка
1.	Отримання завдання на дипломну роботу	14.10.2019	
2.	Підбір і вивчення літературних джерел. Обґрунтування необхідності побудови захищеної системи передавання інформації у телекомунікаційних мережах нових поколінь	15.10.2019 – 02.11.2019	
3.	Огляд та аналіз методів і теорій для побудови системи	03.11.2019 – 08.11.2019	
4.	Аналіз необхідних інструментів	09.11.2019 – 23.11.2019	
5.	Вибір оптимальних інструментів для розробки	02.12.2019 – 25.12.2019	
6.	Розробка компенсаційних методів захисту від завад	08.01.2020– 18.01.2020	
7.	Технічне оформлення пояснювальної записки та графічних матеріалів.	19.01.2020 – 25.01.2020	
8.	Підготовка до захисту дипломної роботи.	26.01.2020– 03.02.2020	

Студентка Козаченко Антоніна Миколаївна

Керівник дипломної роботи Віноградов Микола Анатолійович

6. Консультанти з окремих розділів роботи:

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв

7.Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис студента)

Дата _____

РЕФЕРАТ

Пояснювальна записка до дипломного проекту: "Методи та засоби управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих факторів " містить 97 сторінок, 15 ілюстрацій, 3 таблиці, 73 джерел літератури.

Ключові слова: ДЕСТАБІЛІЗУЮЧІ ФАКТОРИ, *NEXT GENERATION NETWORKS, FUTURE NETWORKS, WLAN, OPEN SYSTEM INTERCONNECTION.*

Мета дипломного проекту — розв’язати задачу управління інформаційною безпекою телекомунікаційної мережі нового покоління за наявністю дестабілізуючих факторів з апріорно невідомими статистичними характеристиками.

Завдання дипломного проектування — навести класифікацію дестабілізуючих факторів телекомунікаційної мережі нового покоління; проаналізувати найбільш значимі дестабілізуючі фактори, обрати достатні статистики та оцінити діапазон невизначеності статистичних характеристик; розробити математичні моделі дестабілізуючих факторів з різними типами апріорної невизначеності; отримати асимптотичні оцінки ефективності виявлення дестабілізуючих факторів з різними типами апріорної невизначеності.

Об’єктом дослідження — є процеси захисту та технічної підтримки процедур передавання інформації у телекомунікаційних мережах.

Практична значимість проекту полягає в розробці компенсаційнійних методів захисту від завад як з одного з найбільш небезпечних зовнішніх дестабілізуючих факторів, особливо для безпроводових мереж.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NGN – Next Generation Networks

FN – Future Networks

ДФ – дестабілізуючі фактори

НС – надзвичайні ситуації

MAC – Medium Access Control

OSI – Open System Interconnection

CSMA/CA – Carrier Sense Multiple Access with Collision Avoidance

DSSS – Direct Sequence Spread Spectrum

DFS – Dynamic Frequency Selection Transmit Power Control

TPC – Transmit Power Control

EAP – Extensible Authentication Protocol

MIMO – Multiple In – Multiple Out

ВСТУП

Проектування, розробка, впровадження та експлуатація телекомунікаційних мереж здійснюється згідно з державними законами та міжнародними стандартами [1 – 3].

Сучасні телекомунікаційні мережі передавання даних – мережі нових поколінь (*Next Generation Networks*) та мережі майбутнього (*Future Networks*) мають принципові відмінності від традиційних мереж, наприклад, класичних мереж з комутацією каналів.

По-перше, основний принцип роботи нових мереж – множинний доступ з часовим розділенням каналів. Для реалізації цієї технології застосовуються цифрова обробка сигналів та пакетна комутація.

По-друге, якщо раніше в телекомунікаційних мережам циркулював виключно мовний трафік, а телеграфні та телетайпні повідомлення передавалися по окремим лініям зв'язку, то в сучасних телекомунікаційних мережах циркулює змішаний трафік. Це так званий трафік Triple Play (мова – відео – дані) або Quadruple Play (мова – відео – дані – мобільні абоненти). Із-за наявності змішаного мережного трафіку кардинально змінилася статистика потоків даних. Виникають спалахи інтенсивності трафіку (бурхливість – Burstiness), статистичні моделі Пуассона або Ерланга вже не дають задовільного опису реальної статистики потоків тощо. Змішаний трафік набуває властивості фрактальності або самоподібності. Статистика самоподібного трафіку описується імовірнісними розподілами з так званими "важкими хвостами" (Heavy-Tail Distributions) – Парето, Вейбулла, Бета- або Гамма-розподілами [4].

По-третє, у зв’язку із тенденцією значного застосування обчислювальної техніки та автоматизованих систем обробки інформації, особливої актуальності набуває проблема забезпечення її безпеки для забезпечення ефективного передавання інформації по телекомунікаційним мережам нових поколінь.

Нарешті, при повсюдному слідуванні стандартам відкритих систем та застосуванні відповідної еталонної моделі взаємодії [3], з одного боку, значно спрощується завдання приєднання до існуючих інформаційно-комунікаційних

систем, але, з іншого боку, виникають нові проблеми захисту інформації від несанкціонованого доступу [2].

Враховуючи все сказане раніше, можна стверджувати, що задача управління інформаційною безпекою інформаційно-комунікаційних систем та мереж, зокрема, телекомунікаційних мереж нових поколінь є актуальною. Більш того, нагальність цієї задачі з плином часу тільки зростатиме.

Мета роботи

Найчастіше у системах обробки інформації потрібне централізоване управління засобами захисту, або за допомогою адміністратора інформаційних ресурсів, або за допомогою спеціаліста інформаційної безпеки (Information Security Officer). Тому процедури захисту повинні реалізуватися в автоматизованих (людино-машинних) системах управління інформаційними ресурсами. Відповідно до принципової суті автоматизованих систем рутинні завдання, які постійно повторюються, повинні розв’язуватися у машинній частині системи. Оператор – людина, що приймає рішення – втручається у процес управління лише у випадку виникнення нештатних, нестандартних ситуацій, які потребують неформального, творчого підходу.

Однак, щоб мінімізувати помилки оператора, відсоток таких нестандартних ситуацій має бути якомога менше. Для досягнення такої мети бажано мати повну апріорну інформацію про стан та параметри системи – об’єкту керування, про внутрішні та зовнішні дестабілізуючі фактори тощо. Іншими словами, треба постійно розв’язувати задачу поточної ідентифікації системи. Звичайно, така постановка задачі є ідеальною конструкцією, яку можна побудувати тільки в асимптотичному сенсі. Реально навіть статистичні параметри дестабілізуючих факторів відомі не повністю, а інколи невідомі взагалі. По суті, приходиться приймати рішення за умов параметричної апріорної невизначеності, а інколи й за умов непараметричної апріорної невизначеності, коли навіть клас апріорних імовірнісних розподілів процесів впливу дестабілізуючих факторів визначити неможливо.

З урахуванням наведених міркувань сформулюємо **мету дослідження** наступним чином: розв’язати задачу управління інформаційною безпекою телекомунікаційної мережі нового покоління за наявністю дестабілізуючих факторів з апріорно невідомими статистичними характеристиками.

Для досягнення поставленої мети необхідно вирішити наступні **задачі дослідження**:

– навести класифікацію дестабілізуючих факторів телекомунікаційної мережі нового покоління;

– проаналізувати найбільш значимі дестабілізуючі фактори, обрати достатні статистики та оцінити діапазон невизначеності статистичних характеристик;

– розробити математичні моделі дестабілізуючих факторів з різними типами апріорної невизначеності;

– провести статистичний синтез пристрою виявлення дестабілізуючих факторів та оцінювання їх статистичних характеристик;

– отримати асимптотичні оцінки ефективності виявлення дестабілізуючих факторів з різними типами апріорної невизначеності.

Предметом дослідження є моделі, методи та засоби побудови захищеної системи передавання інформації у телекомунікаційних мережах нових поколінь (Next Generation Networks та Future Networks) за наявністю дестабілізуючих факторів з різними типами апріорної невизначеності.

Методи дослідження. У дипломному проекті використовувалися методи теорії імовірностей та математичної статистики, теорії адаптації, теорії конфлікту та конфліктного управління, теорії фільтрації Калмана, комп'ютерне моделювання та розрахунки.

Огляд попередніх робіт, терміни та визначення

Хоча поняття живучості відомо в техніці давно і практично використовується при створенні технічних систем різного призначення, досі не створено розвиненою теорії, яка містила б, як і теорія надійності, результати загального характеру, що дозволяють досліджувати цю властивість, оцінювати її

кількісно і розробляти практичні рекомендації проектувальника складних систем щодо забезпечення живучості.

В останні роки спостерігається значне підвищення інтересу до цієї характеристики як в теоретичному, так і в практичному відношенні. Це можна пояснити такими міркуваннями. По-перше, зростання масштабів і вартості систем призводить до значного зростання збитків від тривалого відключення навіть частини системи, збільшення частки технологічно пов'язаних порушень працездатності, а отже, масштабів "ураження" системи. По-друге, у великих системах зростає складність і трудомісткість відновлювальних операцій. Тому прагнення до зменшення розмірів "ураження" системи одночасно є прагненням до створення більш сприятливих умов для відновлення належного рівня функціонування. По-третє, внаслідок розвинених зв'язків між різними системами і підсистемами по різних каналах (по інформаційних каналах, по матеріальним і енергетичним потокам) значну роль можуть грати вторинні наслідки порушень працездатності елементів системи.

Вирішенню задач забезпечення живучості, сталості та відмовостійкості складних систем присвячені дослідження багатьох вітчизняних та зарубіжних учених, зокрема, В.І. Арнольда, М.М. Мойсеєва, О.Г. Додонова, Г.Н. Черкесова, F. Hellmann, S.E. Dreyfus, P. Csermely та ін. [5, 6, 9, 10 – 14].

Згадані завдання, як правило, розв’язуються за умов недостатньої (а іноді й взагалі відсутньої) апріорної інформації про стан та поточні параметри системи, що досліджується, а також про характеристики корисних сигналів, шумів, завад та дестабілізуючих факторів тощо. Аналіз при повній або хоча б достатній апріорній інформації – це недосяжний ідеал; реально приходиться працювати за умов відсутності апріорної інформації. Серед вчених, якими отримані глибокі та плідні результати в цьому напряму, перш за все треба відмітити Р.Л. Стратоновича, Г.П. Тартаковського, В.Г. Рєпіна [7,8].

Вище наведені імена вчених, якими отримані основоположні теоретичні результати, що складають фундаментальне підгрунтя для розв’язання прикладних

задач. Розглянемо більш докладно стан проблеми отримання прикладних результатів, які можна було б застосовувати на практиці.

У монографії [15] розглянуті методи забезпечення стійкості складних систем до впливу дестабілізуючих факторів. Предметну область складають пілотовані повітряні та космічні апарати. Зроблена спроба врахування впливу невизначеностей; у якості основного (по суті, єдиного) дестабілізуючого фактору розглядається протидія супротивника.

У наукових статтях [17 – 20] представлені результати розробки методів підвищення структурної живучості телекомунікаційних мереж. Судячи за змістом робіт та за посиланнями у списках літератури, згадані результати отримані з використанням наукових результатів, наведених у фундаментальній монографії [9] видатного українського вченого, наукового співробітника Київського інституту проблем реєстрації інформації НАН України доктора технічних наук професора Олександра Георгійовича Додонова.

У статті [21] розроблено модель розподіленої обробки інформації в умовах впливу дестабілізуючих факторів на телекомунікаційну мережу. Модель носить частинний характер і базується на способі функціонального резервування з урахуванням часових характеристик та обчислювальних ресурсів. Хоча в ключових словах є згадка про дестабілізуючі дії, у статті їх характеристики та результати впливів не конкретизовані. Таке ж обмеження притаманне і статті [22].

У монографії [23] основну увагу приділено спробі оптимізувати розподіл мережних ресурсів для забезпечення стійкого функціонування протоколів управління доступом до середовища. З цього передпосилання зроблено висновок про стійкість мережі в цілому, хоча доведення цього твердження відсутнє.

Робота [24] представляє собою стандарт Міжнародного Союзу електрозв’язку (ITU-T) стосовно протидії природним катастрофам для покращання стабільності та більш швидкого відновлення роботи мереж. Цей стандарт представляє собою, по суті, практичну рекомендацію, якої можна дотримуватися в усіх випадках.

У статті [25] декларується розробка методики розрахунку показників живучості каналів телекомунікаційної мережі, хоча, по суті, основний зміст роботи представляє операторний метод (метод Лапласа) розв'язання звичайних диференційних рівнянь з постійними коефіцієнтами. У якості умови живучості мережі прийнята умова стійкості операторного рівняння абстрактної замкненої системи. Далі робиться уповні очевидний висновок, що операторне рівняння є стійким, якщо полюси функції (корені полінома знаменника) знаходяться у лівій напівплощині *p*-площини комплексної змінної.

Стаття [26], яка носить оглядовий характер, присвячена опису методики оцінки сталості телекомунікаційної мережі при дії дестабілізуючих факторів. Методологічною основою служить апарат теорії катастроф, про що свідчить також посилання у статті на монографію академіка В.І. Арнольда [5]. Розроблено фазові портрети моделі дестабілізуючих факторів, які можна використовувати для отримання асимптотичних оцінок стійкості мережі.

У роботах [27, 28] розглянуті частинні оцінки живучості телекомунікаційних мереж різного масштабу та призначення.

На жаль, тільки в роботі [16] надано класифікацію основних видів дестабілізуючих факторів впливу на телекомунікаційну мережу, специфікою якої є застосування на залізничній станції, що декілька звужує сферу застосування результатів. Крім того, рішення проблем подолання апріорної невизначеності та адаптації мереж, забезпечення їх живучості, надійності, сталості далекі від завершення, і потребують подальшої розробки. У представленій дипломній роботі зроблено спробу пошуку хоча б частинного розв'язання цієї задачі

На закінчення хочеться підкреслити, що метою даного підрозділу є як огляд існуючих робіт по методам та засобам управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих факторів, так і погляди автора на принципи і основний зміст цих методів. Посилання на літературу носять далеко не систематичний характер. Якщо деякі читачі висловлять інші точки зору на порушені питання, то автор буде радий приводу обмінятися думками.

РОЗДІЛ 1

СТАН ПРОБЛЕМИ ТА ПОСТАНОВКА НА ДИПЛОМНЕ ПРОЕКТУВАННЯ

1.1. Методи забезпечення стійкості складних технічних систем до впливу дестабілізуючих факторів

У дипломному проекті розроблено систему управління безпекою безпроводової телекомунікаційної мережі як невід'ємної частини мереж майбутнього покоління, *Future Networks*. (Раніше широко використовувався термін "мережа наступного покоління" – *Next Generation Network, NGN*.) Специфікою сучасних безпроводових телекомунікаційних мереж, на відміну від проводових (кабельних та оптоволоконних) є наявність зовнішніх електромагнітних завад як ненавмисного, так і навмисного характеру. Завади будь-якого характеру треба віднести до зовнішніх дестабілізуючих факторів.

Дестабілізуючі фактори природного походження можуть викликати перебої в електроживленні, пошкодження окремих блоків вузла зв’язку, розриви проводів у блоках, короткі замикання, вихід технічних характеристик обладнання за межі допусків і т. ін. Наслідки дії цих факторів є явними, а їх впливи усуваються порівняно просто. Проводяться регламентні роботи, здійснюється пошук та усунення несправностей в апаратурі.

Дестабілізуючі фактори штучного походження, такі як техногенні катастрофи, також проявляються явно. Усунення наслідків потребує досить великих матеріальних та часових затрат.

Вельми небезпечними дестабілізуючими факторами є навмисні активні завади, особливо для безпроводових мереж.

Для таких мереж середовищем розповсюдження сигналів є атмосфера або вільний простір, внаслідок чого уразливість безпроводових мереж до активних завад є вельми великою. Для зниження уразливості такого роду треба застосовувати спеціальні заходи [71].

На рис. 1 наведений перелік (який, звичайно, не претендує на вичерпність та повноту) основних видів дестабілізуючих факторів, внаслідок дії яких матиме місце неналежна робота мережного обладнання, а іноді – повна відмова телекомунікаційної мережі.

Рис. 1 Основні види дестабілізуючих факторів

Спираючись на цей перелік, далі розглянемо ризики порушень у роботі мережі.

Проблема забезпечення стійкості складних технічних систем, тобто їх спроможності зберігати нормальне функціонування в процесі і після впливу дестабілізуючих факторів (радіаційних, термосилових, вібраційних та ін., включаючи людський фактор), є досить актуальною в різних прикладних областях.

Забезпечення стійкості складних технічних систем до впливу дестабілізуючих чинників є досить тривалим, трудомістким, ітераційним процесом, пов'язаним з урахуванням різного типу невизначеностей.

По-перше, цей процес охоплює всі основні етапи життєвого циклу системи, який може тривати десятиліття.

По-друге, визначення рівнів показників стійкості саме по собі є досить складним завданням, суттєво більш складною, ніж, наприклад, визначення рівнів показників надійності.

По-третє, оцінка стійкості складної технічної системи до впливу дестабілізуючих чинників вимагає великих знань в різних наукових і технічних галузях; це обумовлено необхідністю визначення фізичних механізмів впливу дестабілізуючих факторів на об'єкт, знання особливостей функціонування складної технічної системи, вміння прогнозувати реакцію функціонуючої системи на вплив, що супроводжується протіканням різних за своєю природою фізичних процесів.

І, нарешті, по-четверте, оцінка стійкості зазвичай утруднена недостатністю необхідних для цього даних.

Крім того, існує ще одна обставина, яка має важливе прикладне значення. Вона зумовлена необхідністю закласти в проектовану складну технічну систему такі рівні стійкості до впливу дестабілізуючих чинників, які могли б забезпечити її безвідмовне функціонування протягом всього життєвого циклу. З іншого боку, бажання забезпечити стійкість з великим запасом може спричинити негативні наслідки, які полягають в додаткових витратах, можливе погіршення інших характеристик системи, ускладненні технологічного процесу при виробництві і т.п. Тому знаходження розумного компромісу в даному випадку є нагальною потребою.

Телекомунікаційні мережі призначені для забезпечення зв'язком підприємств, організацій та всіх структурних підрозділів економіки і транспорту відповідно до вимог і правил технічної експлуатації.

Для сталого функціонування і надання абонентам заданої якості послуг електрозв'язку стан мережі і її елементів постійно контролюється, а якість послуг підтримується на заданому рівні. Однак, як показує досвід експлуатації, при виникненні нештатних ситуацій, зумовлених впливом дестабілізуючих факторів

(ДФ) і виникненням надзвичайних ситуацій (НС), не тільки знижується якість послуг, що надаються, а й відбуваються відмови в обслуговуванні абонентів.

Одним з основних способів забезпечення надійності та живучості сучасних інформаційно-телекомунікаційних систем є реалізація різних способів резервування. Однак в разі застосування структурного резервування, ресурси обчислювальних модулів, що входять до складу інформаційно-телекомунікаційних систем, в зв'язку з неповним робочим навантаженням, як правило, використовуються нераціонально. Розглянуто підхід до забезпечення надійності та живучості інформаційно-телекомунікаційних систем на основі функціонального способу резервування. Модель, що враховує ресурсно-часові характеристики цільових завдань і ресурсно-часові стану обчислювальних модулів, дозволяє отримати аналітичні співвідношення для оцінювання живучості інформаційно-телекомунікаційних систем, а також часу виконання цільових завдань в умовах деградації обчислювальної структури при реалізації різних способів завантаження обчислювальних модулів.

Будувати мережу зв'язку, не знаючи, як працює кабельна мережа, неможливо. Точно так же не можна надавати послуги по кабельній мережі, не знаючи, як працюють радіотехнології доступу. З плином часу з'явиться більш «важкий» контент: HDTV, 3D (в тому числі високої якості), онлайн-ігри; збільшиться число терміналів в квартирі і відповідно кількість незалежних потоків інформації. Перед створенням такі величезні обсяги даних в квартиру користувача, необхідно волокно. Мобільність же забезпечить радіодоступ: оптика доходить до приміщення абонента, а далі використовуються безпроводові технологія (як правило, WLAN стандартів IEEE 802.11x.). Розглянемо їх більш докладно.

1.2. Сімейство стандартів IEEE 802.11

Стандарт *IEEE* 802.11, розробка якого була завершена в 1997 році, є базовим стандартом і визначає протоколи, необхідні для організації безпроводових локальних мереж (WLAN). Основні з них - протокол управління

доступом до середовища *MAC* (*Medium Access Control* - нижній підрівень канального рівня) і протокол *PHY* передачі сигналів у фізичному середовищі. В якості останньої допускається використання радіохвиль і інфрачервоних променів.

Загальні характеристики стандартів IEEE 802.11

Стандарт безпроводової мережі 802.11x, який є складовою частиною стандартів локальних мереж IEEE802.x, охоплює тільки два нижніх рівні семирівневої моделі *OSI* (*Open System Interconnection*) – фізичний і канальний, найбільшою мірою відображають специфіку локальних мереж.

Протокол доступу до середовища (MAC)

Стандартом 802.11 визначено єдиний підрівень *MAC*, який взаємодіє з трьома типами протоколів фізичного рівня, що відповідають різним технологіям передачі сигналів - по радіоканалах у діапазоні 2,4 ГГц з широкосмугового модуляцією з прямим розширенням спектра (*Direct Sequence Spread Spectrum, DSSS*) і частотних стрибків (*Frequency Hopping Spread Spectrum, FHSS*), а також за допомогою інфрачервоного випромінювання. Обидві ці широкосмугові технології пропонуються в двох частотних діапазонах: один в районі частоти 915 МГц, інший в діапазоні від 2400 МГц до 2483,5 МГц. Але саме діапазон 2,4 ГГц є найбільш цікавим для використання його в безпроводових мережах, так як він найменш "зашумлений" сторонніми сигналами і дозволяє розширити смугу передачі. У режимі *FHSS* весь діапазон 2,4 ГГц використовується як одна широка смуга (з 79 підканалами). У режимі *DSSS* цей же діапазон розбитий на кілька широких *DSSS*-каналів, яких одночасно може бути використано не більше трьох. Метод *FHSS* передбачає зміну несучої частоти сигналу при передачі інформації. При використанні *FHSS* конструкція приймача виходить дуже простий, але цей метод можна застосовувати, тільки якщо пропускна спроможність не перевищує 2 Мбіт / сек. Як вже зазначалося вище, ця проблема стала однією з головних причин створення нових версій стандарту. Специфікаціями стандарту передбачені два значення швидкості передачі даних - 1 і 2 Мбіт/с.

У порівнянні з проводовими лініями зв'язку (ЛЗ) можливості Ethernet підрівня *MAC* розширені за рахунок включення в нього ряду функцій, зазвичай виконуваних протоколами більш високого рівня, зокрема, процедур фрагментації і ретрансляції пакетів. Це викликано прагненням підвищити ефективну пропускну спроможність системи завдяки зниженню накладних витрат на повторну передачу пакетів.

В якості основного методу доступу до середовища стандартом 802.11 визначено механізм *CSMA/CA* (*Carrier Sense Multiple Access with Collision Avoidance* – множинний доступ з виявленням несучої і запобіганням колізій).

Управління живленням

Для економії енергоресурсів мобільних робочих станцій, які використовуються в безпроводових ЛЗ, стандартом 802.11 передбачений механізм перемикання станцій в так званий пасивний режим з мінімальним споживанням потужності.

Архітектура і компоненти мережі

В основу стандарту 802.11 покладена стільникова архітектура, причому мережа може складатися як з однієї, так і декількох чарунок (стільників). Кожен стільник управляється базовою станцією, званою точкою доступу (*Access Point, AP*), яка разом з розташованими в межах радіусу її дії робочими станціями користувачів утворює базову зону обслуговування (*Basic Service Set, BSS*) Точки доступу багатостільникової мережі взаємодіють між собою через розподільну систему (*Distribution System, DS*), що є еквівалентом магістрального сегменту кабельних ЛЗ. Вся інфраструктура, що включає точки доступу і розподільну систему утворює розширену зону обслуговування (*Extended Service Set*).

Стандартом передбачений також одностільниковий варіант безпроводової мережі, який може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Роумінг

Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої в багатостільникових системах передбачені спеціальні

процедури сканування (активного і пасивного прослуховування ефіру) і приєднання (*Association*), однак строгих специфікацій по реалізації роумінгу стандарт 802.11 не передбачає.

Забезпечення безпеки

Стандартом *IEEE* 802.11 для захисту *WLAN* передбачено цілий комплекс заходів безпеки передачі даних під загальною назвою *Wired Equivalent Privacy* (*WEP*). Він включає засоби протидії несанкціонованому доступу до мережі (механізми і процедури аутентифікації), а також запобігання перехоплення інформації (шифрування).

Різновиди стандартів IEEE 802.11

IEEE 802.11*a*

Цей стандарт є найбільш "широкосмуговим" з сімейства стандартів 802.11, передбачаючи швидкість передачі даних до 54 Мбіт/с (редакцією стандарту, затвердженою ще в 1999 р, визначені три обов'язкових швидкості - 6, 12 і 24 Мбіт / с і п'ять необов'язкових - 9, 18, 36, 48 і 54 Мбіт/с).

На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями 802.11a передбачена робота в діапазоні 5 ГГц. В якості методу модуляції сигналу вибрано ортогональное частотне мультиплексування (*OFDM*). Найбільш істотна відмінність між цим методом і радіотехнологіями *DSSS* і *FHSS* полягає в тому, що *OFDM* передбачає паралельну передачу корисного сигналу одночасно за кількома частотам діапазону, в той час як технології розширення спектру передають сигнали послідовно. В результаті підвищується пропускна спроможність каналу і якість сигналу.

До недоліків 802.11*a* відносяться більш висока споживана потужність радіопередавачів для частот 5 ГГц, а так же менший радіус дії (обладнання для 2,4 ГГц може працювати на відстані до 300м, а для 5ГГц - близько 100м).

Підводячи попередній підсумок, відзначимо, що дана версія є як би "бічною гілкою" основного стандарту 802.11. Для збільшення пропускної спроможності каналу тут використовується діапазон частот передачі 5,5 ГГц. Для передачі в

802.11a використовується метод множини несучих, коли діапазон частот розбивається на підканали з різними несучими частотами (*Orthogonal Frequency Division Multiplexing*), за якими потік передається паралельно, розбитим на частини. Використання методу квадратурної фазової модуляції дозволяє досягти пропускної спроможності каналу 54 Мбіт/с.

IEEE 802.11*b*

Завдяки високій швидкості передачі даних (до 11 Мбіт/ с), практично еквівалентної пропускній спроможності звичайних дротових ЛЗ *Ethernet*, а також орієнтації на "освоєний" діапазон 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників устаткування для безпроводових мереж.

В остаточній редакції стандарт 802.11b, відомий також як *Wi-Fi* (*wireless fidelity* – торгова марка сімейства стандартів *IEEE* 802.11*x*), був прийнятий в 1999 р. В якості базової радіотехнології в ньому використовується метод *DSSS* з 8-розрядними послідовностями Уолша.

Оскільки обладнання, що працює на максимальній швидкості 11 Мбіт/с має менший радіус дії, ніж на більш низьких швидкостях, то стандартом 802.11*b* передбачено автоматичне зниження швидкості при погіршенні якості сигналу.

Як і в разі базового стандарту 802.11, чіткі механізми роумінгу специфікаціями 802.11*b* не визначені.

Цей стандарт є найбільш популярним на сьогоднішній день і, власне, він носить торгову марку *Wi-Fi*. Як і в первісному стандарті *IEEE* 802.11, для передачі в даній версії використовується діапазон 2,4 ГГц. Він не зачіпає канальний рівень і вносить зміни в *IEEE* 802.11 тільки на фізичному рівні. Для передачі сигналу використовується метод прямої послідовності (*DSSS – Direct Sequence Spread Spectrum*), при якому весь діапазон ділиться на 5 перекривають один одного піддіапазонів, по кожному з яких передається інформація. Значення кожного біта кодуються послідовністю додаткових кодів (*Complementary Code Keying*). Пропускна спроможність каналу при цьому становить 11 Мбіт/с.

IEEE 802.11*d*

Прагнучи розширити географію поширення мереж стандарту 802.11, *IEEE* розробляє універсальні вимоги до фізичного рівня 802.11 (процедури формування каналів, псевдовипадкові послідовності частот, додаткові параметри для *MIB* і т.д.). Відповідний стандарт 802.11*d* знаходиться в стадії активної розробки.

Стандарт визначає вимоги до фізичних параметрів каналів (потужність випромінювання і діапазони частот) і пристроїв безпроводових мереж з метою забезпечення їх відповідності законодавчим нормам різних країн.

IEEE 802.11*e*

Специфікації стандарту 802.11*e* дозволяють створювати мультисервісні безпроводові ЛЗ, орієнтовані на різні категорії користувачів, як корпоративних так і індивідуальних. При збереженні повної сумісності з уже прийнятими стандартами 802.11*a* і *b*, він дозволить розширити їх функціональність за рахунок підтримки потокових мультимедіа-даних і гарантованої якості послуг (*QoS*).

Створення даного стандарту пов'язано з використанням засобів мультимедіа. Він визначає механізм призначення пріоритетів різним видам трафіку - таким, як аудіо- і відеододатки.

IEEE 802.11*f*

Специфікації 802.11*f* описують протокол обміну службовою інформацією між точками доступу (*Inter-Access Point Protocol, IAPP*), що необхідно для побудови розподілених безпроводових мереж передачі даних. Дата затвердження цих специфікацій в якості стандарту поки була не визначена.

Даний стандарт, пов'язаний з аутентифікацією, визначає механізм взаємодії точок зв'язку між собою при переміщенні клієнта між сегментами мережі. Інша назва стандарту - *Inter Access Point Protocol*.

IEEE 802.11*g*

Специфікації 802.11*g*, що знаходяться зараз в стадії розгляду, є розвитком стандарту 802.11*b* і дозволяють підвищити швидкість передачі даних в безпроводових ЛЗ до 22 Мбіт/с (а можливо, і вище) завдяки використанню більш ефективної модуляції сигналу. З декількох пропозицій по базовій радіотехнології для стандарту робоча група *IEEE* недавно вибрала рішення компанії *Intersil*,

засноване на методі *OFMD*, проте потім очікується остаточне прийняття 802.11*g*. Одним з достоїнств майбутнього стандарту є зворотна сумісність з 802.11*b*.

IEEE 802.11*h*

Робоча група *IEEE* 802.11*h* розглядає можливість доповнення існуючих специфікацій 802.11 *MAC* (рівень доступу до середовища передачі) і 802.11*a* PHY (фізичний рівень в мережах 802.11a) алгоритмами ефективного вибору частот для офісних і вуличних безпроводових мереж, а також засобами управління використанням спектру, контролю випромінюваної потужності і генерації відповідних звітів.

Ці задачі планується розв’язати з використанням протоколів *Dynamic Frequency Selection* (*DFS*) *i Transmit Power Control* (*TPC*), запропонованих Європейським інститутом стандартів з телекомунікацій (*European Telecommunication Standard Institute, ETSI*). Зазначені протоколи передбачають динамічне реагування клієнтів безпроводової мережі на інтерференцію радіосигналів шляхом переходу на інший канал, зниження потужності або обома способами.

Розробка даного стандарту пов'язана з проблемами при використанні 802.11*a* в Європі, де в діапазоні 5 ГГц працюють деякі системи супутникового зв'язку. Для запобігання взаємних перешкод стандарт 802.11*h* має механізм "квазіінтелектуального" управління потужністю випромінювання і вибором несучої частоти передачі.

IEEE 802.11*i*

Стандартизація засобів інформаційної безпеки для безпроводових мереж 802.11 ставилася до ведення робочої групи *IEEE* 802.11*e*, але потім ця проблематика була виділена в самостійний підрозділ. Розроблюваний стандарт 802.1*X* покликаний розширити можливості протоколу 802.11 *MAC*, передбачивши засоби шифрування даних, що передаються, а також централізованої аутентифікації користувачів і робочих станцій. В результаті масштаби

безпроводових локальних мереж можна буде нарощувати до сотень і тисяч робочих станцій.

В основі 802.1*X* лежить протокол аутентифікації *Extensible Authentication Protocol* (*EAP*), який базується на *PPP*. Сама процедура аутентифікації передбачає участь в ній трьох сторін - що викликає (клієнта), що викликається (точки доступу) і сервера аутентифікації (як правило, сервера *RADIUS, Remote Authentication in Dial-In User Service* – протокол для реалізації аутентифікації, авторизації та збору відомостей,). У той же час новий стандарт, судячи з усього, залишить на розсуд виробників реалізацію алгоритмів управління ключами.

Розробляються засоби захисту даних повинні знайти застосування не тільки в безпроводових, а й в інших локальних мережах - *Ethernet* і *Token Ring*. Ось чому майбутній стандарт отримав номер *IEEE* 802.1X, а його розробку група 802.11i веде спільно з комітетом *IEEE* 802.1.

Метою створення даної специфікації є підвищення рівня безпеки безпроводових мереж. У ній реалізований набір захисних функцій при обміні інформацією через безпроводові мережі - зокрема, технологія *AES* (*Advanced Encryption Standard*) - алгоритм шифрування, що підтримує ключі довжиною 128, 192 і 256 біт. Передбачається сумісність всіх використовуваних в даний час пристроїв - зокрема, *Intel Centrino* - з 802.11*i*-мережами.

IEEE 802.11*j*

IEEE ще офіційно не сформував робочу групу для обговорення специфікації 802.11*j* на момент публікації. Передбачається, що стандарт буде обумовлювати існування в одному діапазоні мереж стандартів 802.11*a* і *HiperLAN*2. Специфікація призначена для Японії і розширює стандарт 802.11*a* додатковим каналом 4,9 ГГц.

IEEE 802.11*n*

Інститут *IEEE* веде роботу над створенням нової специфікації протоколу зв'язку в безпроводових локальних мережах (*WLAN*). 802.11*n* працює вдвічі швидше, ніж 54-мегабітні "*g*" і "*a*": на швидкості від 100 Мбіт/с. Новий стандарт зрівняє проводові і безпроводові системи, що дозволить корпоративним клієнтам

використовувати безпроводові мережі там, де це було неможливо через обмежену швидкості.

Визначення швидкісних характеристик для стандарту "*n*" буде більш суворим, ніж у "*g*" або "*b*". Воно ґрунтується на фактичній швидкості передачі файлів і потоків, а не на розмірі низькорівневого трафіку, забезпеченого безліччю службових заголовків. Прискорення досягається за рахунок більш раціонального використання частотного діапазону, аналогових радіочіпів, виконаних за поліпшеною *CMOS*-технологією (комплементарна технологія "метал-оксид-напівпровідник", *Complementary Metal-Oxide-Semiconductor*) і інтеграції *WLAN*-адаптера в один чіп.

У будь-якої технології є свої недоліки. Пристрій доступу за технологією *IEEE* 802.11 з двома антенами, що забезпечують режим *MIMO* (*Multiple In – Multiple Out*), збільшує електромагнітне навантаження на приміщення. Якщо в сім'ї є маленькі діти, це небажано. В цьому випадку можна прокласти мідні кабелі необхідної категорії.

1.3. Аналіз взаємного впливу дестабілізуючих факторів один на одного і на стійкість функціонування систем

Під стійкістю функціонування системи розуміється її спроможність виконувати покладені функції з заданими показниками якості в умовах впливу внутрішніх та зовнішніх дестабілізуючих факторів. Взаємний вплив дестабілізуючих факторів один на одного і на стійкість функціонування систем має складну природу.

До зовнішніх дестабілізуючих факторів, які знижують стійкість функціонування, можна віднести наступні:

- аварійні і віялові відключення електроживлення;
- інтерференція та багатопроменевість (стосовно безпроводових мереж);
- віруси й хакерські атаки.

До внутрішніх дестабілізуючих факторів, що знижують стійкість функціонування систем, відносять:

– збої і відмови технічних засобів;

– помилки в програмному забезпеченні;

– невдалі архітектурні рішення;

– нестиковки через різнотипність характеристик встановленого обладнання, неврахованих на стадіях проектування і розгортання;

– конфлікти і тупики через некоректний розподіл системних ресурсів, деяких обраних механізмів організації інформаційно-обчислювальних процесів, архітектурних особливостей компонентів систем.

Врахування взаємного впливу дестабілізуючих факторів є вельми нетривіальною задачею. Найбільш доступним та придатним для практичного застосування є статистичний підхід [61,62], зокрема, кореляційно-регресійний аналіз. Загальне призначення множинної регресії полягає в аналізі зв'язку між кількома незалежними змінними (званими також регресорами) і залежної змінної.

Технічні показники функціонування мережі, як правило, представляються таблицями статистичних даних:

$$\begin{pmatrix} y(1) & y(2) & \cdots & y(i) & \cdots & y(N) \\ x_1(1) & x_1(2) & \cdots & x_1(i) & \cdots & x_1(N) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_j(1) & x_j(2) & \cdots & x_j(i) & \cdots & x_j(N) \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ x_k(1) & x_k(2) & \cdots & x_k(i) & \cdots & x_k(N) \end{pmatrix}$$

Статистичні дані представляють собою вибірку деякої реалізації значень випадкових величин:

- i -а реалізація чисельного значення результату $y_i, i-1,2,\ldots,N$;

- j -а реалізація чисельного значення j -го фактора $x_j \;\; j=1,2,\ldots,N$.

Використання статистичних даних дозволяє домагатися оптимальних результатів, керуючи величинами факторів, або прогнозувати можливу величину результату при сформованих значеннях факторів.

Оцінювання проводиться за спостереженнями за входом (рядки матриці спостережень $\mathbf{X}$) і виходом (елементи вектора відгуків $\bar{\mathbf{y}}$).

Між випадковою величиною результату і випадковою величиною фактора є стохастична (випадкова) залежність, тобто існує кореляційний взаємозв'язок.

У загальному випадку, процедура побудови множинної регресії полягає в оцінюванні параметрів лінійного рівняння. Функціональна залежність результату від факторів представляється рівнянням регресії

$$\mathbf{E}\left[\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_m \end{pmatrix}\right] = \begin{pmatrix} E[y_1] \\ E[y_2] \\ E[y_3] \\ \vdots \\ E[y_m] \end{pmatrix} = \begin{pmatrix} 1 & x_{11} & x_{12} & \dots & x_{1n} \\ 1 & x_{21} & x_{22} & \dots & x_{2n} \\ 1 & x_{31} & x_{32} & \dots & x_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix} \cdot \begin{pmatrix} \theta_0 \\ \theta_1 \\ \theta_2 \\ \vdots \\ \theta_n \end{pmatrix}$$

або те ж саме в компактному вигляді:

$$E[\vec{y}] = \mathbf{X}\vec{\theta}.$$

В якості основних характеристик статистичного зв'язку зазвичай використовують матриці коефіцієнтів множинної кореляції і системи рівнянь множинної лінійної або поліноміальної регресії [66]. Крім того, для автоматизації вимірювань і розрахунків необхідно вибрати метод апроксимації кривих повторюваності змін *KPIs*. Найбільш гнучкими і точними методами є апроксимація поліномами по мінімуму середнього квадрата помилки [61,62] або апроксимації Паде [46].

Розглянемо процес прогнозу параметрів мережі як завдання передбачення *k*-ї змінної $\mathrm{Y_k},\ \mathrm{k}=\overline{1,\mathrm{N}}$ по M змінним $X_m,\ m=1,2,\ldots,M;\ m\neq k$. У загальному випадку $M\neq N$. При $m=1$ маємо рівняння лінійної або поліноміальної регресії незалежної змінної $\mathrm{X_m}$ на залежну змінну $\mathrm{Y_k}$, при $m>1$ маємо систему рівнянь множинної регресії змінних $X_1, X_2, \ldots, X_m$ на Y_k. (Мається на увазі функціональна,

а не статистична залежність.) У розглянутій задачі незалежні змінні $X_1, X_2, \ldots, X_m$ - це випадкові величини, які не обов'язково є статистично незалежними.

Змінну Y_k апроксимуємо функцією регресії $\psi(\cdot)$, що містить оцінки *KPIs* й невідомі коефіцієнти. Рівняння моделі лінійної регресії незалежних змінних $X_1, X_2, \ldots, X_m$ на залежну змінну Y_k запишемо в наступному вигляді:

$$Y_k = a_{0k} + a_{1k}X_1 + \ldots + a_{mk}X_m + \varepsilon \,, \qquad (1.1)$$

де ε - помилка апроксимації.

Нехай $X_{1j} = X_1^j$. Тоді можна записати рівняння поліноміальної регресії у вигляді

$$Y_k = a_{0k} + a_{1k}X_1 + a_{2k}X_1^2 \ldots + a_{mk}X_1^m + \varepsilon. \qquad (1.2)$$

Параметри моделі регресії оцінюються за вибіркою обсягу, взятої з деякою генеральної сукупності. Теоретично генеральна сукупність має нескінченний об'єм або є весь набір даних, який існує в принципі.

Вибірка формується таким чином. За результатами тесту функціонування мережі фіксуємо першу вибірку незалежних змінних $X_{11}, X_{12}, \ldots, X_{1m}$ і розраховуємо залежну змінну Y_1. Потім фіксуємо другу вибірку незалежних змінних $X_{21}, X_{22}, \ldots, X_{2m}$ і розраховуємо залежну змінну. Продовжуємо процедуру до отримання N змінних. Отримуємо вибірку з спостережень

$$\{Y_1 : X_{11}, X_{12}, \ldots, X_{1m}\}, \{Y_2 : X_{21}, X_{22}, \ldots, X_{2m}\}, \ldots, \{Y_N : X_{N1}, X_{N2}, \ldots, X_{Nm}\}.$$

Система рівнянь множинної лінійної регресії набуває вигляду:

$$\left.\begin{array}{l} Y_1 = a_{01} + a_{11}X_{11} + \ldots + a_{m1}X_{1m} + \varepsilon_1 \\ Y_2 = a_{02} + a_{12}X_{21} + \ldots + a_{m2}X_{2m} + \varepsilon_2 \\ \ldots \\ Y_k = a_{0k} + a_{1k}X_{k1} + \ldots + a_{mk}X_{km} + \varepsilon_k \\ \ldots \\ Y_N = a_{0N} + a_{1N}X_{N1} + \ldots + a_{mN}X_{Nm} + \varepsilon_N \end{array}\right\}, \qquad (1.3)$$

де $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$, $k = \overline{1, N}$ - невідомі коефіцієнти;

$\{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k, \ldots, \varepsilon_N\}$ - випадкові помилки, які логічно вважати нормальними однаково розподіленими з параметрами $\{0, \sigma_\varepsilon^2\}$.

Для отримання оцінок за методом найменших квадратів необхідно мінімізувати суму S_k квадратів відхилень в кожній точці. Найкраще наближення відповідає мінімальній величині виразу

$$S_k = \sum_{k=1}^{N} \left(Y_k - a_{0k} - a_{1k} X_{k1} - \ldots - a_{mk} X_{km}\right)^2 . \qquad (1.4)$$

Величина S_k є мірою помилки, пов'язаної з прив'язкою наявних даних до обраної моделі регресії. Мінімум S_k досягається диференціюванням останнього виразу за коефіцієнтами $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$, $k = \overline{1, N}$, прирівнюванням відповідних похідних нулю і розв'язанням системи рівнянь відносно $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$. Отримуємо систему рівнянь для оцінки частинних коефіцієнтів регресії:

$$\left.\begin{array}{l} Y_1 = \alpha_{01} + \alpha_{11} X_{11} + \ldots + \alpha_{m1} X_{1m} \\ Y_2 = \alpha_{02} + \alpha_{12} X_{21} + \ldots + \alpha_{m2} X_{2m} \\ \ldots \\ Y_k = \alpha_{0k} + \alpha_{1k} X_{k1} + \ldots + \alpha_{mk} X_{km} \\ \ldots \\ Y_N = \alpha_{0N} + \alpha_{1N} X_{N1} + \ldots + \alpha_{mN} X_{Nm} \end{array}\right\} . \qquad (1.5)$$

Тут $\alpha_{0k}, \alpha_{1k}, \ldots, \alpha_{mk}$ - оцінки для $\{a_{0k}, a_{1k}, \ldots, a_{mk}\}$.

Оцінки є незміщеними і ефективними, тобто мають мінімальну дисперсію для вибірки $X_1, X_2, \ldots, X_m$ серед всіх лінійних оцінок для прогнозування змінних Y_k, $k = \overline{1, N}$.

Регресійні коефіцієнти представляють вклади кожної незалежної змінної в прогнозування залежної змінної. Для відбору остаточного рівняння регресії зазвичай використовують два протилежних критерії.

Щоб зробити рівняння корисним для передбачення, спостерігач повинен прагнути включити в модель по можливості більше незалежних змінних з тим, щоб можна було більш надійно визначити прогнозовані величини.

Через витрати, пов'язані з отриманням інформації при великій її кількості і подальшою перевіркою, необхідно прагнути, щоб рівняння включало якнайменше незалежних змінних.

Введемо поняття відсутніх значень. При використанні одновимірних за своєю природою методів аналізу (наприклад, t-критерію [65]) найбільш розумний спосіб дії полягає у видаленні з вибірки елементів з відсутнім значенням $\boldsymbol{X}$ (аналізованої змінної). Однак ситуація змінюється при використанні істотно багатовимірних методів аналізу, тобто коли для кожного елемента вибірки є p спостережуваних змінних $X_1, X_2, \ldots, X_p$. Тепер, якщо елемент вибірки має відсутнє значення, скажімо, для змінної X_1, видалення цього елемента вибірки з аналізу не є необхідним, оскільки воно призводить до втрати інформації про змінних, що доставляється цим елементом. Так як множинний лінійний регресійний аналіз, так само як і інші багатовимірні процедури засновані на векторі середніх m і матриці коваріацій *S*, можна залишити цей елемент у вибірці і використовувати наявні в ньому виміри для обчислення оцінок вектора середніх $\bar{\mathbf{x}}$ і матриці коваріацій $\boldsymbol{\Sigma}$.

Уявімо систему рівнянь моделі множинної лінійної регресії (1.3) в матричної формі:

$$\mathbf{Y} = \mathbf{XB} + \mathbf{E}, \qquad (1.6)$$

де $\mathbf{X} = \begin{pmatrix} 1 & X_{11} & \cdots & X_{1m} \\ 1 & X_{21} & \cdots & X_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & X_{N1} & \cdots & X_{Nm} \end{pmatrix}$ - так звана матриця плану.

Для регресійній моделі, по суті, це матриця незалежних змінних, доповнена першим стовпцем вагових коефіцієнтів поточних спостережень;

$\mathbf{B}^{\mathrm{T}} = \{\beta_0, \beta_1 \ldots, \beta_m\}$ - вектор параметрів рівняння регресії; $\mathbf{E}^{\mathrm{T}} = \{\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_N\}$ - вектор помилок оцінювання, що має багатовимірний гаусівський розподіл з нульовим вектором математичних сподівань і матрицею дисперсій виду $\sigma^2\mathbf{I}$; $\mathbf{I}$ - одинична матриця; Т - символ транспонування.

Тоді рівняння (1.4) можна представити в матричному вигляді як

$$S = \left(\mathbf{Y} - \mathbf{XB}\right)^{\mathrm{T}} \left(\mathbf{Y} - \mathbf{XB}\right). \qquad (1.7)$$

Вектор оцінок за методом найменших квадратів є рішення системи нормальних рівнянь

$$\left(\mathbf{X}^{\mathrm{T}}\mathbf{X}\right)\mathbf{B} = \mathbf{XY}, \qquad (1.8)$$

розв'язок якої має вигляд

$$\mathbf{B} = \left(\mathbf{X}^{\mathrm{T}}\mathbf{X}\right)^{-1}\left(\mathbf{XY}\right). \qquad (1.9)$$

З урахуванням того, що матриця дисперсій вектора помилок оцінювання описується виразом $\sigma^2\mathbf{I}$, кореляційна матриця вектора $\mathbf{B}$ дорівнює $\mathbf{R}_{\mathrm{B}} = \sigma^2\left(\mathbf{X}^{\mathrm{T}}\mathbf{X}\right)^{-1}$.

Відзначимо також, що при збільшенні кореляції між різними ключовими показниками ефективності матриця $\mathbf{X}^{\mathrm{T}}\mathbf{X}$ буде мати діагонально-домінантну структуру, тобто діагональні елементи будуть превалювати над сумами елементів за відповідними рядками. При цьому процедури пошуку рішення рівнянь (1.6) і (1.7) спрощуються.

Очевидно, в даному випадку простіше замість оптимальної оцінки як вихідної величини, яка визначається матричних рівнянням, шукати оптимальну оцінку як рішення двоїстого йому різницевого рівняння. Коефіцієнти різницевого рівняння визначаються статистикою спостережень і перешкод і в загальному випадку є змінними величинами, залежними від часу. Перевагою такого підходу є те, що якщо навіть не вдається отримати аналітичний розв'язок різницевого рівняння, то завжди можна отримати його чисельне рішення на обчислювальній

машині. Більш того, рішення можна отримувати в реальному масштабі часу з урахуванням знову одержуваної інформації про зміни параметрів спостережень і перешкод.

Слідуючи [67], побудуємо ітераційний алгоритм розв'язання рівняння (1.6) у вигляді

$$\mathbf{FB}\left[\mathbf{X}(\mathrm{k})-\mathbf{X}(\mathrm{k}-1)\right]=\mathbf{G}\left[\mathbf{Y}-\mathbf{E}-\mathbf{X}(\mathrm{k})\mathbf{B}\right], \qquad (1.10)$$

де $\mathbf{F}$ та $\mathbf{G}$ – матричні множники, визначники яких не дорівнюють нулю, або ненульові скалярні множники.

Ці множники вибираються таким чином, щоб забезпечити максимальну швидкість збіжності без втрати стійкості алгоритму (1.10). Для оптимального вибору значень $\mathbf{F}$ та $\mathbf{G}$ можна застосувати до рівняння (1.10) операцію z-перетворення

$$\mathbf{FB}\left[\mathbf{X}(\mathrm{z})\left(1-\mathrm{z}^{-1}\right)\right]=\mathbf{G}\left[\mathbf{Y}-\mathbf{E}-\mathbf{X}(\mathrm{z})\mathbf{B}\right], \qquad (1.11)$$

і обчислити корені характеристичного рівняння, які повинні бути по модулю менше одиниці. Тоді загальний розв'язок рівняння (1.11) при необмеженому зростанні числа ітерацій $k\to\infty$ асимптотично сходиться до точного рішення рівняння (1.6). Швидкість збіжності залежить від величини максимального по модулю кореня характеристичного рівняння. Задаючись величиною модуля відносної помилки рішення, можна оцінити потрібне число ітерацій як локальну або нелокальну характеристику ефективності пошуку рішення.

Конкретизуючи чисельні значення результату $y_i, i-1,2,\ldots,N$, проаналізуємо ключові показники ефективності інформаційно-комунікаційних мереж.

Ключовими параметрами є затримка передачі, пропускна здатність, втрати пакетів і рівень безпеки. Ці параметри мають найбільший вплив на результуючу якість сервісу. В роботі [48] відзначається, що число *KPIs*, які обирають для

аналізу, має бути мінімальним, причому у всіх випадках недоцільно брати більше 20 таких показників. Ці міркування враховані при завданні набору *KPIs*.

У якості параметрів задачі, що оптимізуються, обрано такі:

- затримка передачі τ;
- пропускна здатність C_p;
- втрати пакетів при передачі даних L_p;
- рівень безпеки та захисту даних при передачі по мережі D_{sp};
- якість *Web*-сервісу;
- якість передачі аудіо (звукові файли, звичайна й *IP*-телефонія);
- швидкість і надійність обміну файлами по протоколу *FTP*;
- швидкість і надійність роботи електронної пошти (*E-mail*);
- якість передачі відео.

Розглянуто гіпотетичну мережу *WLAN IEEE* 802.11*n*, дані для розрахунку параметрів якої взяті з роботи [48]. Для розрахунків використовувалася програма множинного кореляційного аналізу, наведена в [66] і модифікована для даної задачі.

У табл. 1 наведені частинні коефіцієнти кореляції параметрів, що оптимізуються. За цими коефіцієнтами кореляції в подальшому з використанням рівнянь (1.1) – (1.3) можна розраховувати частинні коефіцієнти регресії.

Таблиця 1

Коефіцієнти взаємної кореляції параметрів, що оптимізуються

Пара-метр	Коефіцієнти кореляції									
τ		1,0								
C_p		0,98	1,0							
L_p		0,69	0,68	1,0						
D_{sp}		0,89	0,86	0,69	1,0					
Web		0,75	0,76	0,36	0,77	1,0				
Аудио		0,85	0,64	0,50	0,56	0,30	1,0			
FTP		0,27	0,75	0,63	0,61	0,57	0,44	1,0		
E-mail		0,17	0,22	0,34	0,78	0,30	0,36	0,16	1,0	
Видео		0,87	0,89	0,84	0,82	0,53	0,67	0,79	0,30	1,0
		τ	C_p	L_p	D_{sp}	*Web*	Аудіо	*FTP*	*E-mail*	Відео

Між основними ключовими параметрами виявляється сильна кореляція. Це пояснюється тим, що вони дають значний вплив на вимоги до якості сервісу. Виняток становить електронна пошта, оскільки, на відміну від потокового аудіо, відео, Web-сервісу і передачі файлів по протоколу FTP, для неї не критичні ні смуга пропускання каналу, ні затримка доставки. Однак необхідно відзначити, що параметр D_{sp} - рівень безпеки та захисту даних є критичним практично для всіх представлених параметрів, оскільки навіть для таких видів еластичного трафіку, як електронна пошта, захист даних є невід'ємною вимогою забезпечення якості сервісу *QoS*.

Результати кореляційного аналізу служать також ключовим індикатором моніторингу та регулювання потокових даних і *Web*-сервісу. Це необхідно для забезпечення безпечної передачі інформації по мережі, прогнозування і запобігання перевантажень контрольованого мережевого фрагмента. Таким чином, поточний моніторинг і управління рівнем безпеки в мережі, які є невід'ємною частиною завдання загального управління якістю сервісу, можна

успішно здійснювати статистичними методами, зокрема, методом кореляційно-регресійного аналізу.

Крім того, необхідно відзначити, що повністю скомпільована програма розрахунків займає в пам'яті обчислювального пристрою від 80 до 500 кілобайт в залежності від масштабу мережі і обсягу оброблюваної вибірки. Оскільки в даний час практично будь-який мережевий вузол, по суті, являє собою спеціалізований обчислювач або навіть багатопроцесорну систему, завдання апаратурної реалізації запропонованого методу може вирішуватися порівняно просто.

Розглянемо тепер різні методи оцінювання $\boldsymbol{\mu}$ та $\boldsymbol{\Sigma}$ (або, що еквівалентно, матриці кореляцій **R**), коли відсутні деякі значення [66].

Метод 1. Для обчислення оцінок $\boldsymbol{\mu}$ та $\boldsymbol{\Sigma}$ використовуються тільки n_c комплектних елементів. Цей метод називається методом *видалення елементів.*

Метод 2. Для отримання x_i використовуються n_i спостережень. Замість відсутніх значень змінної X_i підставляється величина $\bar{x}_i$. Потім, використовуючи укомплектовану таким чином вибірку обсягу n, отримують $\bar{\mathbf{x}}$ та $\mathbf{S}$. Цей метод називається методом *підстановки середнього*.

Метод 3. Використовується n_i спостережень для отримання $\bar{x}_i$ та s_i й n_{ij} спостережень - для обчислення s_{ij}. Ці статистики служать компонентами $\bar{\mathbf{x}}$ та $\mathbf{S}$.

Метод 4. Використовується n_i спостережень для отримання $\bar{x}_i$ та s_i й n_{ij} спостережень - для обчислення r_{ij}. Потім обчислюється значення s_{ij} як $s_{ij} = r_{ij} \cdot s_i \cdot s_j$, в чому і полягає відмінність даного методу від попереднього. Методи 3 і 4 звуться методів *попарного викреслювання*.

Метод 5. Використовується n_c комплектних елементів для оцінки регресії будь-якої змінної по всім іншим змінним. Наприклад, нехай рівняння регресії має вигляд $X_1 = f\left(X_2,\ldots,X_p\right)$. Тепер, якщо в j-му випадку є відсутнє значення X_1, воно замінюється оцінкою $x_{1j} = f\left(x_{2j},\ldots,x_{pj}\right)$. Аналогічні рівняння можна

отримати і для $X_2,\ldots,X_p$. Потім укомплектовані таким чином спостереження використовуються для обчислення $\bar{\mathbf{x}}$ та $\mathbf{S}$.

Метод 6. На відміну від методу 5 для передбачення значення, наприклад, використовується або одна змінна з $X_2,\ldots,X_p$, що найбільш корелювали з X_1, або деяка підмножина змінних з $X_2,\ldots,X_p$. Методи 5 і 6 носять назви методів *підстановки регресії*.

Основний недолік будь-якого з перерахованих методів пов'язаний з тим, що їх статистичні властивості за рідкісним винятком невідомі. Крім того, застосування таких методів часто призводить до зміщених оцінок.

Компроміс між цими критеріями може бути досягнутий за рахунок вибору "найкращого" рівняння, що включає оптимальну кількість незалежних змінних. В роботі для пошуку "найкращого" рівняння регресії застосований крокoвий метод (покрокова регресія).

З огляду на все це елементи вибірки та/або змінні з відсутніми значеннями повинні бути видалені так, щоб забезпечити баланс між рештою числа змінних і числом елементів, що залишилися, тобто, максимізувати число комплектних елементів вибірки.

Отже, якщо елемент містить багато пропусків, його потрібно видалити. З іншого боку, слід видалити змінну, якщо її значення невідомо для більшості елементів. Після цього можна звичайним чином використовувати метод найменших квадратів або процедури багатовимірного статистичного аналізу

Якщо число незалежних змінних велике, такий підхід для визначення найкращого підмножини практично не потрібен навіть при застосуванні ЕОМ. Наприклад, якщо p = 5, є всього 5 + 10 + 10 + 5 + 1 = 31 рівняння регресії, а якщо p = 10, то їх число становить вже 2× (10 + 45 + 120 + 210) + 252 + 1 = 1023. взагалі, коли число змінних дорівнює p, є 2P - 1 регресійних рівнянь. Обмеження на машинний час і допустимі витрати призводять до необхідності пошуку інших підходів.

Одним з рішень є покрокова регресія (пряма), коли незалежні змінні одна за одною включаються в підмножину згідно попередньо заданому критерію. У той же час деяка змінна може бути замінена іншою змінною, яка не входить в набір, або видалена з нього. Сукупність критеріїв, що визначають, які змінні включати, замінювати і видаляти, називається покроковою процедурою.

За допомогою покрокової процедури виходить упорядкований список предикторів. Наприклад, якщо p = 5, такий список може мати вигляд X_2, X_5, X_1, X_4 і X_3. Для визначення «найкращої» підмножини з цього списку вибираються $m \le p$ перших змінних так, щоб

a) вони можливо краще передбачали $\mathbf{Y}$ і

b) їх число t було якомога менше.

Іншими словами, економний набір складається зі змінних впорядкованого списку, які мають найбільш високу здатність до прогнозування. У прикладі, наведеному вище, такий набір міг би складатися тільки з змінних X_2 і X_3, якби регресія по ним була майже такою ж «якісною», як і регресія з X_2, X_5, X_1, X_4 та X_3

Процедура визначення числа t називається правилом зупинки. Таким чином, суть проведеного дослідження полягає саме в реалізації системного підходу. Методика безперервної діагностики мережі, тобто аналізу впливу дестабілізуючих факторів на загальну ефективність функціонування мережі полягає в розбитті процесу на наступні взаємопов'язані етапи.

1. На першому етапі проводиться діагностика на фізичному рівні для виключення помилок і правильної інтерпретації результатів подальшого тестування.

2. На другому етапі доцільно проводити діагностику термінальних вузлів мережі шляхом стресового тестування мережі в двох режимах:

- режим калібрування з навантаженням тільки на мережу для виявлення помилок апаратної і програмної реалізації;

- режим з навантаженням тільки на мережу для виявлення проблем взаємодії станцій, вузьких місць на сервері і в каналах зв'язку.

3. На наступному етапі проводиться діагностика каналів зв'язку і серверів з використанням аналізаторів протоколів і аналізаторів серверів. Спільна обробка і аналіз отриманих в процесі тестування швидкісних характеристик, трендів характеристик мережного трафіку і лічильників серверів також здійснюється статистичними методами, що дозволяє встановити причини неправильного функціонування того чи іншого каналу зв'язку (сервера) та дати кількісні оцінки впливу внутрішніх та зовнішніх дестабілізуючих факторів на ключові показники ефективності мереж.

ВИСНОВКИ ДО РОЗДІЛУ 1

В роботі проведено аналіз системи ключових параметрів ефективності і особливостей їх застосування для управління якістю сервісу телекомунікаційної мережі як складної інформаційно-комунікаційної системи. Показано, що при використанні статистичного підходу можна виділити залежності між ключовими параметрами мережі, що дає можливість побудови системи управління якістю сервісу та врахування найбільш небезпечних дестабілізуючих факторів. Встановлено, що матриці коефіцієнтів нормальних рівнянь для обчислення оцінок по мінімуму середнього квадрата помилки мають структуру, близьку до діагонально-домінантної, що дає можливість прискорення і спрощення процедур ітераційного пошуку рішень.

При використанні ключових параметрів ефективності складної системи із затримками сигнальної і керуючої інформації можна забезпечити передбачення її стану і вирішувати завдання управління якістю сервісу в реальному часі. За умов роботи мережі при неповній апріорній визначеності доцільно досліджувати задачі пріоритизації частинних показників ефективності, наприклад, методом аналізу ієрархій, для оптимізації інформаційних систем за багатьма, в тому числі суперечливими критеріями.

РОЗДІЛ 2

ПОРІВНЯЛЬНИЙ АНАЛІЗ МАТЕМАТИЧНИХ МОДЕЛЕЙ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ

2.1. Сучасні методи моніторингу та аналізу телекомунікаційних мереж

Систему управління будь-якою інформаційно-комунікаційною або обчислювальною мережею неможливо побудувати без ретельного та всебічного аналізу стану та параметрів мережі на всіх етапах її функціонування. Технологія моніторингу і аналізу закладається у процесі проектування телекомунікаційних мереж. Вона є невід'ємною частиною загальної проблеми забезпечення сталого функціонування мережі, зокрема, якості сервісу (*Quality of Service, QoS*). Задача проектування мережі включає три етапи: вибір топології мережі, вибір технологій, на основі яких буде здійснюватися практична реалізація, і вибір обладнання. У реальних ситуаціях, наприклад, при створенні безпроводових мереж, вибір топології диктується специфікою використання радіоканалу.

Найбільш прийнятними є топології “зірка” та комбінація топологій “кільце” та “загальна шина”. Вони, по суті, визначаються варіантами архітектури безпроводової мережі: незалежна конфігурація (*Ad Hoc*) та конфігурація з інфраструктурою (структурована мережа). Незважаючи на те, що відмінності між цими архітектурами незначні, вони помітно впливають на такі показники, як кількість користувачів, що можуть підключатися до мережі, радіус мережі, завадостійкість мережі тощо.

У свою чергу, серед технологій, що вибираються, перевага, як правило, віддається одній з багатьох.

Мережа – це велика система, до складу якої входить безліч компонентів: кабельна інфраструктура, активне устаткування, мережна операційна система і багато що інше. Концепція крізної діагностики мережі припускає уміння ефективно оцінити, як працюють всі компоненти мережі з урахуванням їх взаємозв'язків і взаємовпливу. Це уповні логічно, оскільки змішування різнорідних технологій у межах одного автономного сегмента мережі, безумовно, буде приводити до неузгодженості техніко-експлуатаційних характеристик, викликатиме необхідність підтримки великої кількості протоколів мережного обміну, розв’язання конфліктів між різнорідними протоколами та інтерфейсами тощо.

Як наслідок, матиме місце нераціональне використання мережного ресурсу та зниження продуктивності мережі.

Таким чином, проблема вибору обладнання набуває вирішального значення. Від цього залежать ключові показники ефективності функціонування мережі, так звані *Key Performance Indicators, KPIs* [47,48].

Ефективність використовування мережі в значній мірі визначається якістю управління в умовах перевантаження. Поки мережа завантажена незначно, число пакетів, що приймаються і оброблюються, рівне числу тих, що прийшли на вхід комутаційного вузла. Проте, коли в мережу поступає дуже великий об'єм даних, може виникнути перевантаження, і робочі характеристики погіршуються. Частково це може бути пов'язано з недостатністю пам'яті для вхідних буферів, але навіть якщо маршрутизатор має нескінченну пам'ять, ефект перевантаження може виявитися ще важчим. Це зв'язано з часом очікування обробки. Якщо воно перевищує тривалість тайм-ауту, з'являються повторно передані пакети, що приводить до зниження корисної пропускної спроможності мережі. Причиною перевантаження може бути повільний процесор або «вузьке горло» – низька пропускна спроможність окремої ділянки мережі.

Просте підвищення швидкодії процесора або інтерфейсу не завжди вирішує проблему – вузьке місце, як правило, переноситься в інший сегмент мережі. При

надмірних завантаженнях пропускна спроможність каналу або мережі може знизитися до нуля. Така ситуація приводить до колапсу мережі.

Перевантаження породжує лавинні процеси: переповнювання буфера приводить до втрати пакетів, які доведеться передавати повторно або навіть кілька разів. Процесор передаючої сторони одержує додаткове паразитне завантаження. Все це свідчить про те, що контроль перевантаження є украй важливим процесом.

Слід розрізняти контроль потоку і контроль перевантаження. Під контролем потоку мається на увазі балансування потоку відправника і можливості прийому і обробки одержувача. При цьому виді контролю передбачається наявність зворотного зв'язку між одержувачем і відправником. У процесі беруть участь, як правило, тільки два партнери. Перевантаження – загальніше явище, що відноситься до мережі в цілому або до її сегменту.

Одним з поширених методів боротьби з перевантаженнями є управління із зворотним зв'язком. Механізм управління із зворотним зв'язком може поліпшити продуктивність мережі, скорочуючи втрати пакетів, і запобігти розповсюдженню перевантаження. У принципі можна послати повідомлення про перевантаження відправнику, проте при цьому переобтяжена ділянка мережі навантажується ще більше. Тому задача управління розв'язується на транспортному рівні засобами протоколу *TCP* [49,50]. При виявленні перевантаження швидкість передачі знижується шляхом зменшення розміру ковзного вікна.

По суті, має місце управління із зворотним зв'язком, що запізнюється. При неправильному обліку характеристик запізнювання система може втратити стійкість і перейти в незгасаючий коливальний режим, або коректування інтенсивності потоку здійснюватиметься надто пізно [51]. Це приводить до погіршення продуктивності мережі, особливе для додатків реального часу. Компенсація затримки зворотного зв'язку може виконуватися методами прогнозу, наприклад, з використанням моделі авторегресії і ковзного середнього (АРКС) або шляхом усереднювання параметрів вікна. Другий варіант простіший, але, природно, забезпечує значно нижчу якість сервісу.

Позитивного результату також можна досягти шляхом варіації значень тайм-аутів, зміни політики повторної передачі пакетів. В деяких випадках позитивний результат може бути одержаний зміною схеми буферизації.

Управління із зворотним зв'язком широко використовується в архітектурі інтегрованих служб (*Integrated Service Architecture – ISA)* для підтримки служб з різними рівнями якості сервісу (*Quality of Service – QoS)* в Інтернет і в часткових об'єднаних мережах.

Крім того, необхідно враховувати, що на даний момент актуальним є питання проходження різних видів трафіку по широкосмугових мережах, наприклад, регіональних мережах або мережах мегаполісу (MAN) [2,6], у тому числі по безпроводових мережах. Кожен вид трафіку, що передається, має свої характеристики, які, як відомо, значно впливають на вимоги, що пред'являються до обладнання мережі. Тому дослідження статистичних характеристик трафіку є важливим для успішної роботи мережі.

Як показали дослідження останніх десятиліть, вхідний потік трафіку не завжди можна вважати простим [52 – 55]. Встановлено і експериментально підтверджено, що характер трафіку є фрактальним, або самоподібним. Також, в ході досліджень підтверджено, що самоподібність трафіку істотно впливає на характеристики мережі [56, 57].

Оскільки по сучасних мережах передаються різні види трафіку, то для забезпечення необхідної якості обслуговування використовування дисципліни черг *FIFO* (*First in First Out* – першим прибув, першим обслужений) не завжди буде оптимальним. У таких випадках використовуються пріоритети. Пріоритети можуть призначатися залежно від типу трафіку. Важливим є випадок призначення пріоритету на основі середнього часу обслуговування. Часто запитам з меншим очікуваним часом обслуговування дається більший пріоритет, ніж запитам з великим очікуваним часом обслуговування. При такій схемі продуктивність високопріоритетного трафіку збільшується. Також вищі пріоритети можуть призначатися трафіку, чутливому до затримок, наприклад, голосовому або відеотрафіку.

Затримки викликають необхідність в збільшенні буферної пам'яті пристроїв комутації і маршрутизації, оскільки вони не справляються з потоком пакетів вже при коефіцієнті використовування мережі 50-60%. Велика кількість пакетів відкидається і передається повторно, що приводить до ще більшого перевантаження мережі. Тому необхідно розраховувати необхідні розміри буфера з урахуванням характеристик трафіку.

Методи розрахунку вимог до мереж нових поколінь (пропускної спроможності каналів, місткості буферів і ін.) засновані на марківських моделях і формулах Ерланга, які з успіхом використовувалися при проектуванні телефонних мереж, можуть давати невиправдано оптимістичні рішення і приводити до недооцінки навантаження [56].

Отримання інформації про різні характеристики фізичних каналів передачі телекомунікаційних мереж практично необхідне для поточного контролю якості систем передачі. Вирішальний вплив на якість передачі інформації по каналах передачі мають такі характеристики мереж, як затримка, число втрачених пакетів, продуктивність мережі і пов'язані з ними передавальна, пропускна спроможність та інтегральна характеристика якості сервісу.

На практиці найбільший інтерес представляють затримка доставки та число втрачених пакетів як ключові чинники впливу на якість сервісу.

Окреме і дуже важливе місце у переліку ключових параметрів ефективності безпроводових мереж займають безпека передачі та захист даних. У зв’язку з принциповою відкритістю каналів зв’язку безпроводових мереж підтримання цих параметрів на належному рівні є нагальною проблемою.

2.2. Методи отримання інформації про сигнали та завади у мережі

Вимірювання і контроль по інформаційному сигналу є традиційними для систем автоматичного управління [59], проте не знаходять застосування у області передачі через те, що має місце просторове рознесення входу і виходу каналів передачі, внаслідок чого виникає необхідність передавати в пункт вимірювання і контролю відсутній там сигнал в неспотвореному вигляді. Крім того, мають місце

затримки сигнальної та керуючої інформації, що призводить до відповідних затримок у керуванні і, що більш небезпечно, може взагалі привести до втрати стійкості системи діагностики, моніторингу та керування в цілому. Цей же принциповий момент перешкоджає практичному використовуванню ряду споріднених методів вимірювання ключових характеристик каналів обміну даними.

Дані методи полягають в необхідності вимірювання деякої характеристики вхідного інформаційного сигналу, передачі інформації про неї в приймальний пункт (вихід каналу), вимірюванні аналогічної або спорідненої характеристики вихідного сигналу і обчисленні за отриманими даними необхідних характеристик самого каналу. У табл. 2.1 наведена класифікація методів вимірювання і контролю.

Таблиця 2.1

Класифікація методів вимірювання і контролю характеристик мережних каналів передачі

Методи вимірювання і контролю	
Прямі вимірювання	Складні непрямі вимірювання
Вимірювання амплітуд і фаз	Вимірювання імпульсних характеристик
Вимірювання АЧХ каналу	Вимірювання вхідного та вихідного сигналів
Вимірювання шумових характеристик	Вимірювання кореляційних характеристик

Один з прямих методів вимірювань заснований на вимірюванні амплітуд і фаз частотних складових спектру вимірювального сигналу з урахуванням того, що передатна (системна) функція каналу $H(z)$ рівна

$$H(z)=Y(z)/X(z)=\left|H(z)\right|\Phi(z), \qquad (2.1)$$

де $|H(z)|$ - модуль передатної функції каналу, $\Phi(z)$ – аргумент передатної функції каналу, а $Y(z)$ і $X(z)$ – зображення на z-площині відповідно вихідного і вхідного сигналів.

Припускається, що амплітуда вхідного сигналу незмінна і відома. Амплітуда вихідного дискретного гармонійного сигналу оцінюється кореляційним способом. Можлива оцінка тільки АЧХ каналу. Відмітимо, що АЧХ каналу обчислюється вздовж одиничного кола z-площини в інтервалі від $-\pi/T_d$ до π/T_d, де T_d – період дискретизації.

Можна визначити АЧХ каналу по співвідношенню

$$\left|H(z)H^*\left(z^{-1}\right)\right| = F_y(z)/F_x(z), \tag{2.2}$$

де $F_y(z) = \left|Y(z)Y^*\left(z^{-1}\right)\right|$, $F_x(z) = \left|X(z)X^*\left(z^{-1}\right)\right|$ – спектральні щільності потужності вихідного та вхідного сигналів відповідно. Тут передбачається, що спектральна щільність потужності вихідного сигналу підлягає вимірюванню, а спектральна щільність потужності вхідного сигналу відома наперед. Згідно третьому методу – методу взаємного спектру (ВС), частотні характеристики каналу визначаються по взаємному спектру вхідного і вихідного сигналів [38,39], згідно виразу

$$H(z) = F_{xy}(z)/F_x(z), \tag{2.3}$$

де $F_{xy}(z)$- взаємна спектральна щільність вхідного і вихідного сигналів, $F_x(z)$- спектральна щільність вхідного сигналу.

Відомий метод визначення частотних характеристик, заснований на вимірюванні імпульсної характеристики каналу [60]. Метод припускає вимірювання реакції каналу $h(n),\ \ n = 0,1,2,\ldots$ на короткий імпульс, який в теорії відображається дельта-символом Кронекера. За цим слідує дискретне перетворення Фур'є від імпульсної характеристики і визначення коефіцієнта передачі

$$H(k)=\frac{1}{N}\sum_{n=0}^{N-1}h(n)\exp\left(-\frac{j2\pi nk}{N}\right),\quad k=0,1,2,\ldots,K,\quad K=N \qquad (2.4)$$

Недоліком цього методу слід вважати ту обставину, що він не може бути віднесений до повністю суміщених, оскільки створює хоча і короткочасні, але достатньо потужні перешкоди передаванню. Модифікацією згаданого методу є визначення частотних характеристик, при якому вимірюється перехідна характеристика каналу $g(n)$. Згідно методу на вхід каналу впливають спеціальним сигналом, що відображається одиничною функцією включення, з подальшим визначенням імпульсної характеристики по відомому співвідношенню

$$h(n)=g(n)-g(n-1). \qquad (2.5)$$

Далі, отримана $h(n)$ перетвориться по Фур'є аналогічно тому, як це передбачалося попереднім методом. Помітимо, що при проведенні операції диференціювання, можлива поява істотних викидів, що усуваються згладжуванням $h(n)$ з використанням спеціальних вагових функцій (Дольф-Чебишева, Хеммінга, фон Ханна тощо).

Принципово можливе визначення характеристик каналу шляхом розв'язання рівняння дискретної згортки виду [60]

$$y(n)=\frac{1}{N-m+1}\sum_{m=0}^{N-m+1}x(n)h(n-m)=\frac{1}{N-m+1}\sum_{m=0}^{N-m+1}x(n-m)h(n),$$

(2.6)

$$y(n)=x(0)g(n)+\frac{1}{N-m+1}\sum_{m=0}^{N-m+1}x'(n)g(n-m)=$$

$$=x(0)g(n)+\frac{1}{N-m+1}\sum_{m=0}^{N-m+1}x'(n-m)g(n). \qquad (2.7)$$

В цьому випадку потрібне вимірювання вхідного $x(n)$ і вихідного $y(n)$ сигналів. Оскільки у даних, що передаються на фізичному рівні, є інформація про сигнал, то реалізація процесу вимірювання спрощується: відпадає необхідність в

передачі якої-небудь інформації про нього на приймальну станцію мережі. Вельми цікавим представляється метод визначення характеристик каналу по зміряній функції взаємної кореляції [33]. Метод заснований на визначенні $g(n)$ шляхом рішення рівняння згортки, що пов'язує $R_{xy}(m)$ з $h(m)$ і автокореляційною функцією $R_x(m)$ вхідного сигналу [60]

$$R_{xy}(m) = \frac{1}{N-m+1} \sum_{n=0}^{N-m+1} h(n) R_x(n-m) . \qquad (2.8)$$

У ряді випадків рішення цього рівняння є простим, наприклад, коли $R_x(m) \to \delta(m)$. У [61] приводиться приклад кореляційного методу вимірювань, що припускає ототожнення імпульсної реакції лінійної системи з взаємною кореляційною функцією вхідного і вихідного сигналів – метод взаємної кореляційної функції (ВКФ). Фактично це різновид попереднього методу [62]:

$$h(m) = R_{xy}(m) . \qquad (2.9)$$

Можливі застосування цього методу в автоматиці, ядерній фізиці і ряді інших областей. Метод є повністю суміщеним і орієнтований на застосування шумового або шумоподібного вимірювального сигналу низького рівня [63].

Для визначення моделей різноманітних систем управління [32, 59], для визначення характеристик каналів передачі використовуються методи теорії ідентифікації [34, 35, 37 – 41].

З результатів наведеного огляду й систематизації методів вимірювання і контролю характеристик каналів можна виявити основні напрями досліджень в цій області. Вельми перспективними слід вважати повністю суміщені методи вимірювання і контролю характеристик каналів передачі, тобто методи, які припускають поєднання вимірювального і інформаційного сигналів в каналі, як за часом, так і по спектру.

Маючи ці початкові дані, можна успішно розв’язувати задачі поточного управління мережами із застосуванням системного підходу. Розглянемо ці задачі більш докладно.

2.3. Узагальнена модель управління телекомунікаційними мережами

Критерії оптимізації ключових параметрів функціонування мережі і поточного управління мережею є неоднозначними і суперечливими. Урахування цих суперечностей і пошук компромісних рішень можливий при використовуванні статистичних методів, узгодження достовірності і детального аналізу початкових даних з урахуванням фізичного сенсу вирішуваних задач. При оптимізації параметрів і структури телекомунікаційних мереж до складу цільової функції входить велика кількість основних і додаткових параметрів, від яких залежить якість сервісу *QoS*. Тому при розробці загальних підходів до організації системи контролю комп'ютерної мережі як складної інформаційної системи (ІС) необхідно враховувати наступні особливості таких систем [32, 33].

1. Процес створення ІС – це багатоплановий процес, що складається з декількох взаємопов'язаних етапів. Після вибору структури системи, який супроводжується математичним моделюванням, виготовляється апаратура, що входить до складу системи.

Відбувається поступове нарощування апаратних засобів аж до створення апаратурних комплексів, що виконують задані функції ІС. Ця особливість ІС вимагає, щоб випробування на надійність також були безперервним і тривалим процесом.

2. Апаратні засоби ІС складаються з різних комплектуючих елементів. За своїм призначенням апаратура підрозділяється на засоби обчислювальної техніки, передачі, відтворення і зберігання інформації, відображення інформації, джерела живлення і т.д.

3. На надійність ІС роблять вплив різноманітні чинники. Ця особливість вимагає проведення випробувань, що дозволяють виявити їх вплив в різних режимах використання системи.

4. На всіх наступних етапах створення ІС враховуються результати перевірок та іспитів апаратури, елементи якої створені на попередніх етапах. За результатами цих іспитів уводяться корективи до початкового проекту. Отже,

процес створення ІС є процесом зі зворотним зв’язком та корекцією отриманих результатів за даними випробувань на проміжних етапах.

5. Кожна велика система вимагає розробки своєї методики випробувань, що відображає її особливості. контроль надійності елементів, що входять до складу великої системи, слід розглядати як попередній етап контролю надійності всієї системи.

Методи аналізу та керування мережами за своєю суттю є різновидом методів ідентифікації, тобто поточного оцінювання параметрів та стану складних систем [31 – 33]. Аналіз методів ідентифікації об’єктів керування і способів оцінювання їх поточного стану обумовлений тісним взаємозв’язком завдань ідентифікації та діагностики, оскільки ідентифікація є складовою частиною діагностики. При цьому потрібно відмітити, що методи розв’язання цих завдань у значній мірі залежать від класу, до якого можна віднести об’єкт ідентифікації (діагностики). Зокрема, для розподілених систем із затримками сигнальної та керуючої інформації, до яких можна віднести комп’ютерні та телекомунікаційні мережі, доцільно застосовувати методи ретроспективної та структурної ідентифікації [34 – 36]. Інформаційною основою методів ідентифікації є робота [37].

Абстрактні системи управління (системи управління загального призначення) описані у цілому ряді робіт, які носять фундаментальний характер [39 – 41]. На нашу думку, найбільш придатною для застосування у телекомунікаційних системах є спеціалізована система управління, яка носить назву "мережа управління телекомунікаціями" (*Telecommunication Management Network – TMN*). В даний час концепція управління *TMN* є одним з основних стандартів при побудові систем управління телекомунікаційними мережами є [31, 32]. Мережа управління телекомунікаціями *TMN* представляє собою спеціальну інфраструктуру, що забезпечує управління шляхом організації взаємодії з компонентами різних телекомунікаційних мереж за допомогою мережі передачі

даних на основі єдиних інтерфейсів і протоколів обміну інформацією. Детальний опис цієї системи даний у роботі [32].

Взаємозв'язок інфраструктури *TMN* з телекомунікаційною мережею показаний на рис. 2.1

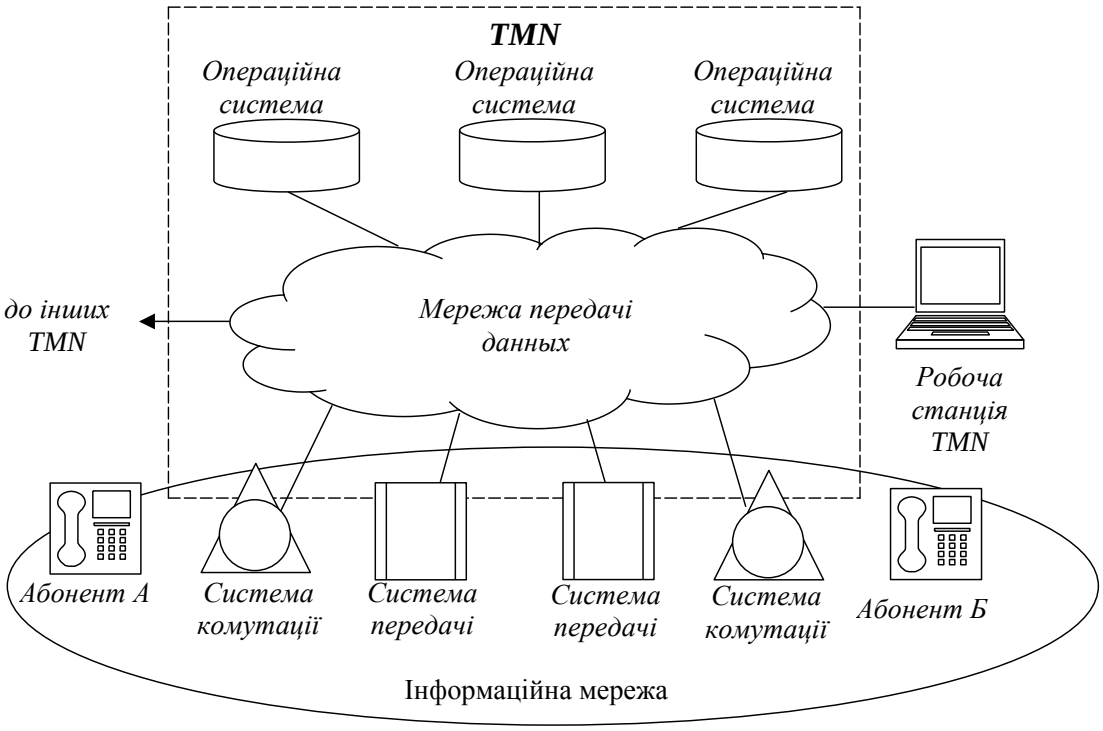


Рис. 2.1 Взаємозв'язок інфраструктури *TMN* з інформаційною мережею

Організаційна структура *TMN* створюється для реалізації задач управління, експлуатації і технічного обслуговування різнорідного телекомунікаційного обладнання, оперативного контролю і адміністрування мережних пристроїв, а також узгодженої взаємодії між різними типами систем управління в цілях надання послуг зв'язку із заданою якістю.

До сфери управління *TMN* входять практично всі існуючі в даний час види мереж і систем зв'язку, а також типи телекомунікаційного обладнання. Об'єктами управління *TMN*є телекомунікаційні ресурси, що фізично надають собою реальне обладнання зв'язку, на яке можливе здійснення цілеспрямованої управляючої дії. Фізично компоненти керованої мережі електрозв'язку (обладнання систем

комутації, систем передачі і т.д., визначувані як мережні елементи), можуть бути як зосередженими (централізованими), так і розподіленими.

Реалізація прикладних процесів управління здійснюється операційними системами шляхом обміну управляючою інформацією з мережними елементами. При цьому операційні системи забезпечують обробку даних, що поступають від мережних елементів, підтримують інформаційну модель мережі електрозв'язку, забезпечують роботу прикладних програмних засобів управління. Крім того, операційні системи забезпечують підтримку терміналів користувача у вигляді їх робочих станцій. Таким чином, *TMN* здійснює моніторинг всієї мережі електрозв'язку, виробляє управляючі рішення, виходячи з реальних мережних умов і супутньої інформації.

Модель управління безпекою телекомунікаційної мережі будується в рамках єдиної моделі управління телекомунікаційною мережею *TMN*, що включає в себе п'ять рівнів:

- рівень мережних елементів;
- рівень управління мережними елементами;
- рівень управління мережею;
- рівень управління сервісами;
- рівень управління бізнес-процесами.

Міжнародна організація по стандартизації (*ISO*) розділила завдання управління на п'ять функціональних груп :

- управління несправностями,
- управління конфігураціями,
- управління продуктивністю,
- управління безпекою,
- облік використання ресурсів.

Як видно з наведеної класифікації, управління безпекою нерозривно пов’язане з іншими завданнями управління, зокрема, з управлінням

несправностями та продуктивністю інформаційної системи. Комплексне рішення цих завдань є проблемою оптимального управління.

Управління конфігурацією реалізується у процесі моніторингу мережних елементів (їх типів, місцезнаходження, ідентифікації параметрів та стану і т.п.), включення елементів в роботу, їх конфігурування і виходу з робочого стану, встановлення і змін фізичних з'єднань між елементами.

Управління розрахунками – це контроль степеню використання мережних ресурсів і підтримання функції автоматичного нарахування оплати (білінгу).

Управління безпекою необхідне для захисту мережі від несанкціонованого доступу. Воно може включати обмеження доступу за допомогою паролів, видачу сигналів тривоги при спробах несанкціонованого доступу, відключення небажаних користувачів або, навіть, криптографічний захист інформації.

Відповідно до сучасних стандартів систем управління мережами і концепціями розвитку самих мереж викликає необхідність подальших досліджень і розробок питань по наступних напрямах.

1. Визначення стану системи в режимі її функціонування.

Особливістю контролю телекомунікаційної мережі у режимі реального функціонування є наявність в ній сигнальної інформації у момент перевірки, що практично виключає використання стимулюючих сигналів для визначення її стану [64]. Визначення параметрів та стану телекомунікаційної мережі може бути здійснена такими шляхами:

– визначенням матричного оператора динамічних характеристик контрольованого вузла чи елементу телекомунікаційної мережі;

– оцінкою стану об'єкту по збуреннях, що діють, внутрішніх шумів та завад і місць їх локалізації;

– з побудовою та налаштуванням еталонних моделей об'єкту.

Перший підхід відомий як ідентифікація об'єкту [34 – 41]. Потрібно оцінити необхідні умови для його вживання та розробити відповідні методи для застосування у даній предметній області.

Другий підхід є маловивченим, і його опрацювання представляє суто теоретичний інтерес. Щоб зрештою звести зміни в стані системи до дії внутрішніх і зовнішніх збурень, а саме це визначається контролем, потрібно мати вичерпну інформацію про параметри та стан системи на нескінченному інтервалі спостереження. На практиці можна отримати лише деякі асимптотичні оцінки на кінцевому інтервалі спостереження, але немає ніяких гарантій, що за цей період характеристики системи суттєво не зміняться.

Третій підхід – використання моделі, яка б адекватно відображала властивості об'єкту, для телекомунікаційної мережі порівняно великого масштабу представляє практично нереальне завдання (за тими ж міркуваннями, що й для другого підходу).

Для визначення оператора динамічних характеристик контрольованого вузла чи елементу телекомунікаційної мережі та статистичного синтезу системи управління інформаційною безпекою необхідні апріорні дані. У найкращому випадку повної апріорної визначеності вони зводяться до задавання законів розподілу імовірностей для всіх процесів, що циркулюють у системі, що синтезується. У цьому випадку можливо використовувати байєсівський критерій, який мінімізує ризик. Це – найкращій критерій з усіх наявних.

З урахуванням шумів і завад вихідна напруга приймача завжди матиме випадковий характер. Тому результати аналізу вихідного ефекту приймача оцінюються методами теорії ймовірностей і математичної статистики.

У процесі виявлення сигналів допустимі тільки два рішення: сигнал є або сигналу немає. Всякі ухильні рішення виключаються. Розглянемо можливі сполучення подій і рішень (табл.2.2).

Таблиця 2.2

Подія H_1 – сигнал є	Гіпотеза 11 – Сигнал є	Правильне виявлення $Đ_{1â}$
	Альтернатива 10 – Сигналу немає (наприклад, сигнал слабкий та замаскований завадою)	Пропуск сигналу $P_{пр}$ (похибка другого роду)

Подія H_0 – сигналу немає	Гіпотеза 00 – Сигналу немає	Правильне невиявлення $Đ_{1â}$
	Альтернатива 01 – Сигнал є (наприклад, сильна завада може бути прийнята за сигнал)	Хибна тривога $Đ_{õò}$ (похибка першого роду)

Для реалізації байєсівського критерію треба зарані знати апріорні ймовірності наявності та відсутності сигналу (апріорні імовірності p_{pr0} та p_{pr1} подій H_0 та H_1 відповідно). Коли спостерігач не в змозі оцінити апріорні імовірності p_{pr0} та p_{pr1}, байєсівське рішення знайти неможливо

Знаючи апріорні ймовірності p_{pr0} та p_{pr1}, спостерігач застосовує байєсівське рішення; його втрати при вірному рішенні представляють собою мінімальний (умовний) байєсівський ризик

$$C_{B\min}\left(p_{prj}\middle|p_{psk}\right),\quad j,k=\overline{0,1},\quad j=k; \tag{2.10}$$

при хибному рішенні втрати зростають;

$$C_{Bcur}\left(p_{prj}\middle|p_{psk}\right),\quad j,k=\overline{0,1},\quad j\neq k;\ C_{Bcur}\geq C_{B\min}. \tag{2.11}$$

Умовний байєсівський ризик – це функція штрафу за прийняття *k*-го рішення з апостеріорною імовірністю p_{psk}, коли насправді мала місце *j*-та подія з апріорною імовірністю p_{prj}.

Коли спостерігач застосовує байєсівський критерій, а прийняте рішення є хибним, середні втрати описуються прямою лінією, дотичною до кривої $C_{B\min}\left(p_{prj}\middle|p_{psk}\right)$ у точці $p_{prj}=p_{psk}$. Будь-яка точка цієї лінії для $p_{prj}\neq p_{psk}$ представляє собою середній ризик для можливих областей рішень, що відповідають апріорній імовірності p_{prj}. Оскільки байєсівський підхід дає

мінімальний середній ризик, крива $C_{B\min}\left(p_{prj}\middle|p_{psk}\right), j=k$ повинна лежати нижче прямої для $C_{Bcur}\left(p_{prj}\middle|p_{psk}\right), j\neq k$

Розглянемо імовірності похибок для випадку гаусівського розподілу шумів та завад:

$$p_k(x)=\frac{1}{\sigma\sqrt{2\pi}}\exp\left[-\frac{(x-a_k)^2}{2\sigma^2}\right],\ k=\overline{0,1},\ a_0<0<a_1 \quad . \qquad (2.12)$$

Функції розподілу зображені на рис. 2.2.

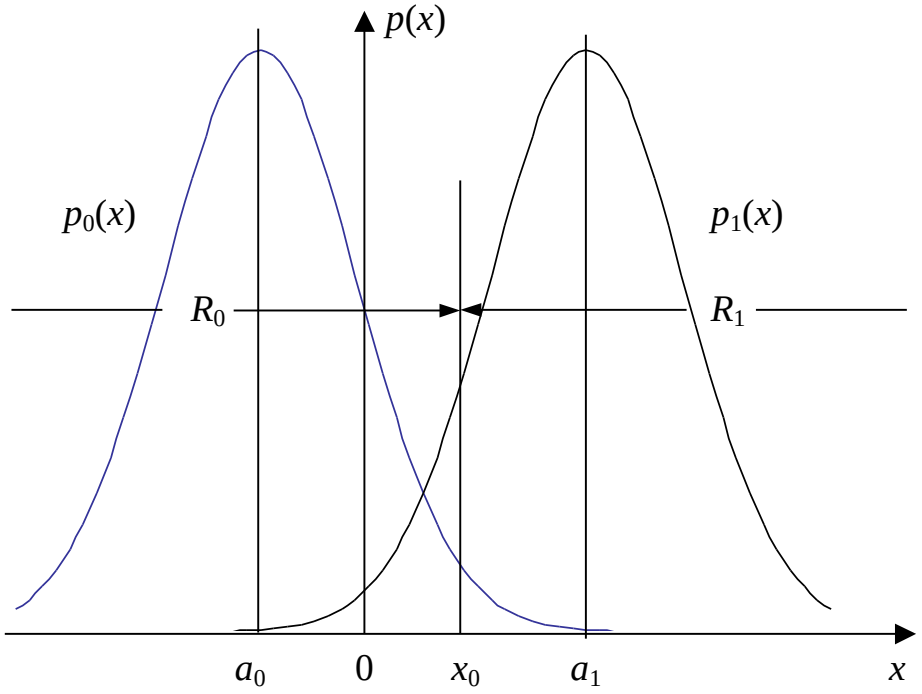


Рис. 2.2 Функції щільності ймовірності.

Тут прийняті такі позначення: $p_0(x)$ – розподіл щільності ймовірностідля випадку відсутності сигналу; $p_1(x)$ – розподіл щільності ймовірності для випадку наявності сигналу; x_0 – пороговий рівень; R_0, R_1 – області розміщення сигналу.

Концепція знання апріорних імовірностей, яка є підгрунтям байєсівського підходу, потребує можливості проведення такого числа спостережень, щоб довірчі ймовірності прагнули до одиниці. Іншими словами, різниця між довірчою

ймовірністю та одиницею є величиною вищого порядку малості, якою можна знехтувати на інтервалі спостереження.

Взагалі можна записати ціни прийнятих рішень кожного типу у вигляді матриці плат $\mathbf{C}$:

$$\mathbf{C} = \begin{pmatrix} C_{00} & C_{01} \\ C_{10} & C_{11} \end{pmatrix}, \qquad (2.13)$$

де C_{ij} - ціна прийняття рішення i, коли у дійсності справедлива гіпотеза j ($i, j = \overline{0,1}$). Ціни залежать від дій, які робляться після відповідного рішення, та від наслідків цих дій. При недостатній апріорній інформації часто застосовують спрощену матрицю цін: при правильному рішенні встановлюється нульова ціна, при буд-якому хибному рішенні однакова ціна похибки, що значно більше нуля:

$$\mathbf{C} = \begin{pmatrix} 0 & C_{err} \\ C_{err} & 0 \end{pmatrix}. \qquad (2.14)$$

Умовний ризик, що виникає при виборі рішення по гіпотезі H_0, визначається співвідношенням

$$C\left(H_0 \middle| x\right) = C_{00} p\left(H_0 \middle| x\right) + C_{01} p\left(H_1 \middle| x\right), \qquad (2.15)$$

а при виборі рішення по гіпотезі H_1, виразом

$$C\left(H_1 \middle| x\right) = C_{20} p\left(H_0 \middle| x\right) + C_{11} p\left(H_1 \middle| x\right). \qquad (2.16)$$

З урахуванням виразу (2.14) вирази (2.15 – 2.16) спрощуються:

$$\begin{cases} C\left(H_0 \middle| x\right) = C_{01} p\left(H_1 \middle| x\right) \\ C\left(H_1 \middle| x\right) = C_{20} p\left(H_0 \middle| x\right); \end{cases} \qquad (2.17)$$

Умовні імовірності гіпотез H_0 та H_1 за умовою, що при спостереженні було отримано значення *x*, дорівнюють

$$\begin{cases} p\left(H_0|x\right)=\dfrac{p_{pr}\left(x\right)p_0\left(x\right)}{p\left(x\right)}; \\ p\left(H_1|x\right)=\dfrac{\left[1-p_{pr}\left(x\right)\right]p_1\left(x\right)}{p\left(x\right)}, \end{cases} \qquad (2.18)$$

де $p\left(x\right)=p_{pr}\left(x\right)p_0\left(x\right)+\left[1-p_{pr}\left(x\right)\right]p_1\left(x\right)$ – повна імовірність результату *x* при всіх спостереженнях.

Нехай гіпотеза H_0 обирається, коли результат спостережень (виміру величини *x*) лежить в області R_0, а гіпотеза H_1 обирається, коли результат лежить в області R_1. Якщо апріорні ймовірності гіпотез H_0 та H_1 дорівнюють $p_{pr}\left(x\right)$ та $1-p_{pr}\left(x\right)$ відповідно, середній ризик при прийнятті рішення буде

$$\overline{C}=p_{pr}\left(x\right)\left[C_{00}\int\limits_{R_0}p_0\left(x\right)dx+C_{10}\int\limits_{R_1}p_0\left(x\right)dx\right]+$$
$$+\left[1-p_{pr}\left(x\right)\right]\left[C_{01}\int\limits_{R_0}p_1\left(x\right)dx+C_{11}\int\limits_{R_1}p_1\left(x\right)dx\right]. \qquad (2.19)$$

Члени у квадратних скобках – ризики прийняття рішень по гіпотезах H_0 та H_1. Вони множаться на певні вагові коефіцієнти, роль яких відіграють апріорні ймовірності гіпотез: $H_0\rightarrow p_{pr}\left(x\right)$; $H_1\rightarrow 1-p_{pr}\left(x\right)$.

Середній ризик $\overline{C}$ є мінімальним, якщо області R_0 та R_1 визначаються у відповідності з відношенням правдоподібності [43]. Для кожного спостереження обчислюється відношення правдоподібності – величина

$$\Lambda\left(x\right)=\frac{p_1\left(x_0\right)}{p_0\left(x_0\right)}=\frac{p_{pr}\left(x\right)C_0}{\left[1-p_{pr}\left(x\right)\right]C_1}, \qquad (2.20)$$

де $p_0(x)$ та $p_1(x)$ – розподіли щільності ймовірності для випадків відсутності та наявності сигналу відповідно. Зокрема, для гаусівського розподілу (2.12)

$$x_0 = \frac{a_0 + a_1}{2} + \frac{\sigma^2}{a_1 - a_0} \ln \frac{p_{pr}(x)}{\left[1 - p_{pr}(x)\right] C_1}. \qquad (2.21)$$

Якщо $p_{pr}(x) = 1 - p_{pr}(x) = 0{,}5,\ C_0 = C_1$, то $x_0 = (a_0 + a_1)/2$, тобто середнє значення математичних сподівань функцій розподілу при відсутності тв. наявності сигналу. Таке рішення відоме як критерій "ідеального спостерігача", за яким мінімізується повна (сумарна) імовірність похибки.

Значення x_0, що використовується спостерігачем, буде залежати від вартості для нього цих похибок (штрафу за похибку). Твір C_0Q_0 називається ризиком, відповідним гіпотезі H_0, а твір C_1Q_1 є ризик, що відповідає гіпотезі H_1. Середній ризик при ухваленні рішення

$$\overline{C}(x_0) = p_{pr}(x)Q_0 + \left(1 - p_{pr}(x)\right)Q_1 = p_{pr}(x)C_0 \int_{x_0}^{\infty} p_0(x)dx + \left(1 - p_{pr}(x)\right)C_1 \int_{-\infty}^{x_0} p_1(x)dx \qquad (2.22)$$

Коли спостерігач приймає рішення даним методом, повний штраф, який сплачується їм за хибне рішення. при досить великій кількості спостережень n буде близький до $n\overline{C}(x_0)$ за умови незмінності статистичних характеристик процесу на інтервалі спостереження.

Однак для поточної мінімізації, особливо за умов нерівноважності похибок першого та другого роду, зміни статистичних характеристик шумів та завад на інтервалі спостереження і ін. треба задіювати більш тонкі механізми управління ризиком як невід'ємною частиною загальної проблеми інформаційної безпеки.

Спостерігач, природно, обирає те значення , яке мінімізує його середній ризик $\overline{C}(x_0)$. Щоб знайти цю точку поділу, потрібно продиференціювати (2.13) по x_0 і прирівняти похідну нулю:

$$\frac{p_1(x)}{p_0(x)} = \frac{p_{pr}(x)C_0}{\left[1-p_{pr}(x)\right]C_1} = \mathbf{\Lambda}_0, \qquad (2.23)$$

тобто, в кінцевому рахунку, отримати відношення правдоподібності.

Для гаусівського розподілу (2.3) отримаємо таке оптимальне значення точки поділу x_0 областей R_0 та R_1, при встановленні якої мінімізується середній ризик:

$$x_0 = \frac{a_0 + a_1}{2} + \frac{\sigma^2}{a_1 - a_0} \ln \frac{p_{pr}(x)C_0}{\left(1-p_{pr}(x)\right)C_1}. \qquad (2.24)$$

Наприклад, якщо $p_{pr}(x) = 1 - p_{pr}(x) = 0{,}5$ та $C_0 = C_1$, то $x_0 = (a_0 + a_1)/2$.

Спостерігач обирає ту гіпотезу, для якої умовний ризик за результатом спостереження є меншим. Наприклад, умовний ризик $C(H_0|x)$ представляє собою середню ціну за одне рішення, якщо б в усіх випадках, коли результат виміру був у малій околиці $x \pm \varepsilon$ поблизу значення x, приймалася б гіпотеза H_0. У загальному випадку значення x_0, вибране згідно з (2.23) або (2.24), може бути підставлене в (2.22) для визначення мінімального середнього ризику. При цьому умовна ймовірність гіпотези H_0 за умови, що при спостереженні було отримано певне значення x, дорівнює

$$p(H_0|x) = \frac{p_{pr}(x)\,p_0(x)}{p(x)}; \qquad (2.25)$$

ймовірність гіпотези H_0 за тієї ж умови –

$$p(H_1|x) = \frac{\left[1 - p_{pr}(x)\right] p_1(x)}{p(x)}, \qquad (2.26)$$

де $p(x) = p_{pr}(x)\, p_0(x) + \left[1 - p_{pr}(x)\right] p_1(x)$ – повна щільність імовірностей результату *x* при всіх спостереженнях. Відповідні умовні ризики, які супроводжують вибір з перевагою тієї чи іншої гіпотези, описується співвідношеннями (2.15 – 2.17).

Якщо відомий апріорний розподіл станів, але параметри розподілу (математичне сподівання, дисперсія, вищі моменти тощо) невідомі, для встановлення критерію якості вибору рішення є можливість використовувати лише умовну функцію ризику за мінімаксним критерієм або за критерієм максимуму апостеріорної функції розподілу.

Якщо невідомий навіть апріорний розподіл станів, тобто коли кількість апріорної інформації прагне до нуля, для встановлення критерію якості вибору рішення встановлюється граничний випадок оцінки за максимумом апостеріорної імовірності – оцінка максимальної правдоподібності.

Іншими словами, можна розділити критерії оцінювання (і, відповідно, ризику) на три категорії:

– повна апріорна визначеність – байєсівський критерій, що мінімізує ризик;

– параметрична апріорна невизначеність – мінімаксний критерій (критерій максимуму апостеріорної функції розподілу), що мінімізує умовний ризик;

– непараметрична апріорна невизначеність – критерій, що мінімізує умовний ризик, усереднений по всім параметрам для найменш переважного розподілу (*Least Favourable Distribution, LFD*).

Розглянемо співвідношення між критеріями Байєса, максимуму апостеріорної функції розподілу та максимальної правдоподібності докладніше.

Якщо було б відоме значення апріорної імовірності $p_{pr0}(x)$, яка є результатом дій супротивника, очікуваних за гіпотезою H_0, спостерігач застосував би байєсівське рішення, яке відповідало б цьому значенню.

Взяття рівномірного розподілу в якості апріорного (в результаті чого метод Байєса збігається з методом максимальної правдоподібності) або будь-якого іншого, ні до чого не зобов'язуючого апріорного розподілу (що знаходяться, наприклад, за принципом максимальної негативної інформації – ентропії) не є єдино можливим прийомом.

Під час обговорення різних неясних формулювань, що стосуються визначення адаптації та містять твердження про "відсутність апріорних відомостей", корисно мати на увазі, що відсутність апріорних відомостей - це теж різновид апріорних відомостей.

Однак дана проблема не має великої гостроти. Справа в тому, що *при досить великій накопиченій інформації все розумні методи працюють добре (і приблизно однаково), а при малій кількості інформації методи дають різні рекомендації, але все погані* [42][1]. Тому можна вибрати найзручніший метод, наприклад Байєса, з рівномірним розподілом.

Зазначений факт нівелювання методів можна перевірити в рамках байєсівської теорії, досліджуючи незалежність результатів (їх асимптотичну інваріантність) від вибору апріорного розподілу.

Зі сказаного видно, що "апріорна трудність" долається діалектично. Відсутність апріорних даних не можна вважати аргументом на користь того, щоб відмовитися від апріорного розподілу (від байєсівської постановки), а скоріше навпаки – це аргумент за те, щоб багаторазово вирішувати завдання при різних апріорних розподілах. Те ж саме відноситься до невизначеності динамічних рівнянь, критерію якості тощо.

Конкретизуючи наведені міркування стосовно проблеми прийняття рішень в умовах невизначеності впливу дестабілізуючих факторів, можна зробити

[1] Це нагадує мудрий вислів, з якого починається роман Льва Миколайовича Толстого "Анна Кареніна": "Всі щасливі сім′ї схожі одна на одну, кожна нещаслива сім′я є нещасною по-своєму."

висновок, що найбільш доцільно обирати за основу комплексну байєсівську теорію управління, що містить у собі теорію статистичних рішень, оптимальне виявлення та фільтрацію (у загальному випадку – з неповним спостереженням). При такому підході поняття степеню оптимальності алгоритмів, швидкості збіжності і т. ін. має свій цілком певний сенс.

ВИСНОВКИ ДО РОЗДІЛУ 2

1. Систему управління будь-якою інформаційно-комунікаційною або обчислювальною мережею неможливо побудувати без ретельного та всебічного аналізу стану та параметрів мережі на всіх етапах її функціонування. У другому розділі розглянуто сучасні методи моніторингу та аналізу телекомунікаційних мереж та проведено їх порівняльний аналіз.

2. За результатами вивчення класифікації методів вимірювання і контролю характеристик мережних каналів передачі зроблено висновок, що, маючи ці початкові дані, можна успішно розв’язувати задачі поточного управління мережами із застосуванням системного підходу, теорії прийняття рішень та методу аналізу ієрархій

3. При дослідженні узагальненої моделі управління телекомунікаційними мережами вибрано та обгрунтовано критерії оптимізації ключових параметрів функціонування мережі і поточного управління мережею.

4. Також зроблені порівняння байєсівського та мінімаксного критеріїв прийняття рішень про наявність ти чи інших дестабілізуючих факторів. Зроблено обґрунтований висновок, що найбільш доцільно обирати за основу комплексну байєсівську теорію управління, що містить у собі теорію статистичних рішень, оптимальне виявлення та оцінювання.

РОЗДІЛ 3

РОЗРОБКА МЕТОДІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В УМОВАХ НЕВИЗНАЧЕНОСТІ ВПЛИВУ ДЕСТАБІЛІЗУЮЧИХ ФАКТОРІВ

3.1. Вибір методу накопичення апріорних даних у процесі роботи системи

Як відмічалося раніше, достоїнством мінімаксного критерію та відповідного правила рішення є здатність функціонувати за умов відсутності апріорної інформації про стан та параметри об’єкту (в нашому випадку – інформаційно-комунікаційної мережі). По суті, забезпечується здатність функціонувати, хоча і з мінімальною, але гарантованою якістю при найменш переважному апріорному розподілі.

Однак реально апріорні дані існують завжди, хоча їх обсяг змінюється у вельми широких межах. Зокрема, спираючись на накопичені результати попереднього досвіду, часто можливо зарані визначити якщо не параметри, то хоча б клас апріорних статистичних розподілів, що відповідає умовам параметричної апріорної невизначеності. При переході ж від непараметричної до параметричної апріорної невизначеності можна застосовувати критерій максимуму апостеріорної імовірності.

Звичайно, потрібне теоретичне обгрунтування методу збору інформації та її використання в якості апріорної на наступних етапах роботи системи. Крім того, від теоретичних передумов необхідно переходити до практичної розробки алгоритмів, пристроїв, комп'ютерних програм.

На нашу думку, для розв'язання цієї задачі найбільш придатним у всіх сенсах є метод дуального управління Фельдбаума [68,69]. Конкретизуємо цей метод стосовно цифрової телекомунікаційної мережі з пакетною комутацією.

Дуальне управління – це форма управління, при якій керуючі впливи служать одночасно для вивчення керованого об'єкта і для приведення його до оптимального стану. Дуальне управління використовується в таких ситуаціях, коли невідомі рівняння зміни стану об'єкта, а також немає початкової інформації, достатньої для того, щоб заздалегідь розрахувати оптимальний закон керування. Окремі риси дуального управління можна знайти в системах різних класів.

У системах автоматичного керування інформація про об'єкт управління складається з інформації, що визначає залежність вихідної величини від керуючого впливу, інформації про стан об'єкта, інформації про збурення чи заваду, що діє на об'єкт, інформації про заданий вплив та цілі управління. У системах з повною інформацією до початку функціонування є вся апріорна інформація, а поточну інформацію керуючий пристрій отримує по контуру зворотного зв'язку в процесі роботи системи. У системах з неповною інформацією апріорно відомі не самі дії, а лише статистичні характеристики випадкових вхідних впливів. Принцип дії цих систем полягає в тому, що вони накопичують інформацію, якої бракує вже під час роботи. Подібні системи отримали назву оптимальних систем з незалежним накопиченням інформації з огляду на те, що процес накопичення не залежить від алгоритму керуючого пристрою. В системі дуального управління передбачається активне вивчення характеристик об'єкта управління, які змінюються випадковим чином. При цьому на вхід об'єкта подаються впливу "вивчення", а реакція об'єкта аналізується керуючим пристроєм. Таким чином, керуючі дії не тільки для управління об'єктом, але одночасно також і для його вивчення.

Теорія дуального управління найбільший розвиток отримала при застосуванні у дискретних системах. При цьому основою для побудови алгоритму роботи керуючого пристрою стала теорія статистичних рішень, а показником якості - математичне сподівання загальної функції втрат, зване середнім ризиком.

На рис. 3.1 зображена структурна схема системи управління абстрактним об'єктом. Буквою **A** позначено керуючий пристрій, а буквою **B** – керований об'єкт. Природа об'єкта може бути будь-якою. Як вже згадувалося, в даному конкретному завданні керованим об'єктом є інформаційно-комунікаційна система – цифрова телекомунікаційна мережа з пакетною комутацією.

На виході об'єкта **B** з'являється керована величина *x*. Під керованою величиною розуміються параметри, якими характеризується стан керованого об'єкта. У загальному випадку є кілька таких параметрів $x_1,\ldots,x_n$. Зручно вважати ці величини координатами вектора $\bar{\mathbf{x}}$:

$$\bar{\mathbf{x}} = (x_1,\ldots,x_n). \qquad (3.1)$$

Вектор називається також вихідним вектором або вихідний величиною об'єкта **B**.

На вхід об'єкта **B** надходить керуючий вплив u від керуючого пристрою **A**. Якщо таких впливів декілька - $u_1,\ldots,u_r$, то їх можна об'єднати у вектор $\bar{\mathbf{u}}$ з координатами $u_j\ (j=1,\ldots,r)$:

$$\bar{\mathbf{u}} = (u_1,\ldots,u_r). \qquad (3.2)$$

На вхід керуючого пристрою **A** подається задаючий вплив x^*, що представляє собою інструкцію про те, якою має бути вихідна величина x об'єкта.

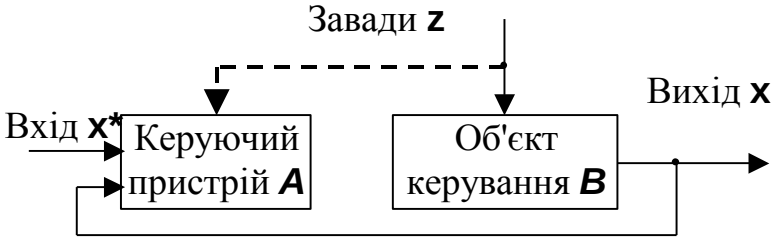


Рис. 3.1

Ця інструкція повинна конкретизувати мету управління.

Інструкція може являти собою колекцію з n величин $x_1^*,\ldots,x_n^*$, які будемо вважати координатами вектора $\bar{\mathbf{x}}^*$:

$$\bar{\mathbf{x}}^* = (x_1^*,\ldots,x_n^*) \qquad (3.3)$$

Наприклад, можна зажадати, щоб в ідеальному випадку задовольнялися умови

$$x_i = x_i^* \ (i = 1, \ldots, n), \qquad (3.4)$$

де x_i^* – задані функції часу.

Системи управління поділяються на два класи: розімкнуті і замкнуті системи. Останній клас називається також системами зі зворотним зв'язком.

У розімкнутих системах керуючий пристрій не отримує інформації про дійсний стан об'єкта **В.**

У замкнутих системах керуючий пристрій **А** отримує цю інформацію по лінії зворотного зв'язку (внизу на рис. 3.1). Принцип дії замкнутої системи може бути коротко охарактеризований наступним чином: якщо величина не відповідає вимогам, то управляючий пристрій А надає такий вплив і на об'єкт, щоб наблизити до цих вимог.

Відхилення величини х від вимог може статися від різних причин.

а) Неправильне, неточне або запізніле використання пристроєм А міститься в ньому або приходить до нього інформації про характеристики та стан об'єкта і про цілі управління. Цей недолік, в принципі, може бути виправлений удосконаленням закону дії (алгоритму) керуючого пристрою **А.**

б) Обмеження ресурсів управління, т. е. неможливість, з тих чи інших причин, подавати на об'єкт **В** такі керуючі впливи і, які забезпечили б необхідну поведінку х об'єкта. На практиці ресурси управління завжди обмежені, і цю обставину необхідно враховувати.

в) Причиною відхилення х від вимог може виявитися деякий заздалегідь непередбачене і не контрольоване збурення z, яке надходить на об'єкт **В** і впливає на його вихідну величину $\bar{\mathbf{x}}$. Якщо на різні частини об'єкта **В** діють збурення, то можна представити їх у вигляді вектора $\bar{\mathbf{z}}$:

$$\bar{\mathbf{z}} = (z_1, \ldots, z_l). \qquad (3.5)$$

Збурюючий вплив $\bar{\mathbf{z}}$ – це, по суті, завада, що діє на керований об'єкт **В** та може викликати заздалегідь не передбачену зміну його характеристик. Вплив зміни навантаження на об'єкт можна розглядати як окремий випадок дії завади.

Припустимо, що алгоритм керуючого пристрою **А** забезпечує успішну роботу системи при певних характеристиках об'єкта **В**. Однак при їх зміні робота системи може погіршитися, і величина $\bar{\mathbf{x}}$ стане значно відхилятися від встановлених вимог.

Принцип зворотного зв'язку в багатьох випадках створює можливість задоволення вимог, що пред'являються до величини $\bar{\mathbf{x}}$ навіть при наявності значної завади $\bar{\mathbf{z}}$, що діє на об'єкт **В**. Однак якщо характеристики об'єкта **В** складні і швидко змінюються в широкому діапазоні, то завдання управління ускладнюється. У таких випадках отримання інформації про заваді або хоча б про деякі її складові може надати істотну допомогу і покращує результат управління. Нехай завада вимірюється, і результат вимірювання надходить (дивись штрихову лінію на рис. 3.1) в керуючий пристрій **А**. Тоді у цьому пристрої може бути розраховано такий керуючий вплив $\bar{\mathbf{u}}$, який компенсує, нейтралізує вплив завади $\bar{\mathbf{z}}$ і призведе вихідну величину об'єкта в кращу відповідність до вимог. Цей прийом і називається власне компенсацією. Контур компенсації не є лінією зворотного зв'язку, оскільки по ній передається значення вхідної, а не вихідної величини об'єкта. Системи, в яких поряд з принципом зворотного зв'язку застосовується принцип компенсації, іноді називаються комбінованими.

Слід зазначити, що сфера застосування принципу компенсації значно вужчими області застосування принципу зворотного зв'язку. Це пояснюється головним чином тим, що на об'єкт **В** діє велика кількість різних завад $z_1,\ldots,z_r$. Значна частина цих завад взагалі не піддається виміру, а тому й не може бути скомпенсована за допомогою контуру, показаного штриховою лінією на рис. 3.1. Навіть якби й існувала принципова можливість вимірювання безлічі завад $\mathbf{z_i}$, то розрахунок нейтралізуючого їх впливу $\bar{\mathbf{u}}$ був би надмірно складним. Тому

керуючий пристрій **А** виявився б занадто громіздким, а результати роботи системи могли б все ж бути недостатньо успішними, оскільки не всі завади можна виміряти. Тим часом принцип зворотного зв'язку дозволяє вимірювати тільки відхилення керованої величини $\bar{\mathbf{x}}$ від вимог і формувати керуючий вплив $\bar{\mathbf{u}}$, який наближає $\bar{\mathbf{x}}$ до бажаного значення. Очевидно, що принцип зворотного зв'язку набагато більш універсальний і, взагалі кажучи, призводить до більш простих методів управління, ніж принцип компенсації. Однак в ряді випадків, коли вимір основного впливу, що обурює здійснюється досить просто, метод компенсації або його поєднання з принципом зворотного зв'язку виявляється найбільш вдалим.

Зазвичай об'єкт **В** заданий, і його властивості змінювати не можна. Тим часом алгоритм керуючого пристрою здебільшого зовсім не заданий, і його можна вибирати з широкого класу можливих алгоритмів[2]. Завдання побудови оптимальної системи зводиться, таким чином, до задачі розробки такого керуючого пристрою, який, в даному разі, найкращим чином керує об'єктом **В.**

На практиці до пристрою **А** зазвичай пред'являється ряд самостійних вимог, які не мають прямого відношення до об'єкту **В**. Наприклад, можна зажадати, щоб пристрій **А** був досить надійним, а також не занадто складним. Можна вимагати, щоб його вага, габарити або споживання енергії були не дуже великими. Можна для полегшення розрахунків або з інших міркувань прийняти пристрій **А** лінійними або навіть заздалегідь задати його структурну схему, вважаючи невідомими в ній тільки параметри окремих ланок. Однак нижче основну увагу звернено на такий розгляд, в якому відсутні будь-які вимоги або обмеження, що стосуються безпосередньо керуючого пристрою **А**. Припустимо, що, якщо буде потрібно, цей пристрій може бути будь-яким - наприклад, як завгодно складним, а також безінерційним. Така відсутність обмежень обумовлена великими можливостями сучасної обчислювальної техніки. Крім того, накладення додаткових обмежень на керуючий пристрій А може, взагалі кажучи, різко

[2] Нерідко потужна силова частина керуючого пристрою задана; тоді її слід відносити до керованого об'єкту і вважати його частиною. Тому іноді «керований об'єкт» замінюють поняттям «незмінна частина системи». Те ж саме - для ресурсу керування інформаційною системою.

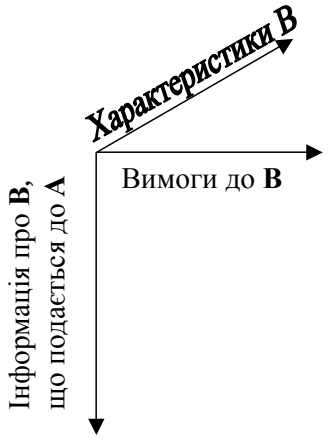
ускладнити задачу знаходження оптимальної системи. Таке ускладнення виникає, якщо, наприклад, вимагати, щоб складність або надійність, або вартість керуючого пристрою **А** не переходили через деяку верхню межу. Зрозуміло, якщо обмежити вибір пристрою **А** відомим, заздалегідь визначеним класом систем, або заздалегідь вибрати схему і вважати невідомими лише її параметри, то завдання сильно спрощується. Однак цінність її вирішення, як правило, падає у ще більшій мірі. Дійсно, найважче при створенні оптимального керуючого пристрою – це визначення загального вигляду, загальної структури алгоритму. На жаль, інтуїція інженера або математика може надати тут допомогу лише в найпростіших випадках і безсила в скільки-небудь більш складних. Тому заздалегідь, як правило, не відомі ні загальний вид алгоритму, ні навіть досить вузький клас залежностей, до якого він належить. Тому будь-який необґрунтований апріорний вибір вузького класу залежностей позбавляє рішення задачі тієї цінності, яку вона мала б за відсутності подібних обмежень.

Якщо обмеження, накладені на, відсутні, то алгоритм оптимального пристрою **А** визначається лише наступними факторами, що відносяться до об'єкта **В** і способу його сполуки з **А**:

1) характеристики об'єкта **В;**

3) вимоги, що пред'являються до об'єкту **В;**

3) характер інформації про об'єкт **В**, що надходить в управляючий пристрій **А**.



Докладний розгляд цих факторів необхідний з метою детальної постановки завдання. Можна символічно представити кожен із зазначених вище факторів у вигляді деякого напряму, ортогонального іншим, як це показано на рис. 3.4, і пов'язати з кожним типом оптимальних систем точку або область в такому тривимірному просторі.

Рис. 3.4

Зазначені на рис. 3.4 напрямки є напрямками класифікації оптимальних систем. Подібна класифікація корисна в тому відношенні, що дозволяє правильно визначити, місце кожного типу оптимальних систем серед інших типів. Дослідження всіх можливих типів оптимальних систем з спільних точок зору розкриває єдність основних положень теорії, незважаючи на істотні відмінності в окремих типах систем.

3.2. Розробка методу накопичення інформації про дестабілізуючі фактори

Розглянемо особливості застосування методу дуального управління для накопичення інформації про зовнішні дестабілізуючі фактори. У відповідності до наведеної раніше класифікації, під зовнішніми дестабілізуючими факторами зазвичай розуміють завади природного та штучного походження. Стосовно ж мереж, у яких середовищем розповсюдження є атмосфера або вільний простір (безпроводових мереж), проблема притлумлення ненавмисних та навмисних електромагнітних завад стоїть особливо гостро.

Після теоретичного обгрунтування методів накопичення інформації про характеристики завад можна розв’язувати технічні завдання розробки алгоритмів та пристроїв компенсації. Повернемося до системи управління захистом телекомунікаційної мережі як невід'ємної складової загальної системи управління телекомунікаціями *TMN*.

Управління з незалежним накопиченням інформації є особливо привабливим для системи управління телекомунікаціями *TMN*, яка є цифровою за самим принципом побудови. Різницеві рівняння, якими описується процес, природним чином вписуються в методи послідовного аналізу, методи дискретного оптимального управління, рівняння Колмогорова для еволюції умовних імовірностей тощо. Надалі, обговорюючи завдання трансформації апостеріорних даних на попередньому етапі збору та обробки інформації в апріорні дані на наступному етапі, будемо завжди припускати, що мова йде саме про дискретні системи та процеси.

Повертаючись до задачі дуального управління з одночасним накопиченням інформації та її використання в якості апостеріорної на наступних етапах обробки, будемо, як і раніше, вважати, що в керуючому пристрої **А** є повна інформація про оператор **Ф** об'єкта **В** і про цілі управління, тобто про форму критерію оптимальності **Q**. Інформація ж про вплив $\bar{x}^*$, що задає управління системою, про збурення $\bar{z}$, що діє на об'єкт **В**, і про вихідну величину $\bar{x}$ об'єкта може бути неповною. Далі, припустимо, що запас інформації про величинах $\bar{x}^*$, $\bar{x}$ і $\bar{z}$ може збільшуватися, накопичуватися з плином часу, причому процес цього накопичення не залежить від дій керуючого пристрою **А**. Якщо останній управляє об'єктом оптимальним чином, то такі системи називають оптимальними системами з незалежним або пасивним накопиченням інформації [70].

Накопичення інформації може відбуватися в двох випадках.

а) Нехай величина x * (або $\bar{z}$), яка вимірюється без похибки, є випадковий процес, більш складний, ніж марковський. Імовірнісні характеристики цього процесу можна уточнити, спостерігаючи його протягом певного проміжку часу. В цьому випадку спостереження дозволяє накопичити інформацію, уточнюючу поведінку процесу в майбутньому.

б) Величина $\bar{x}^*$ (або $\bar{z}$) вимірюється з деякою погрішністю, або результат вимірювання проходить через канал з шумами, що домішуються до корисного сигналу. В цьому випадку для уточнення значень корисного сигналу необхідно спостереження. Чим більше час спостереження, тим, взагалі кажучи, точніше можна визначити поведінку $\bar{x}^*$ в майбутньому.

Найбільш важливий другий випадок.

Типовий приклад системи з незалежним накопиченням інформації показаний на рис. 3.5.

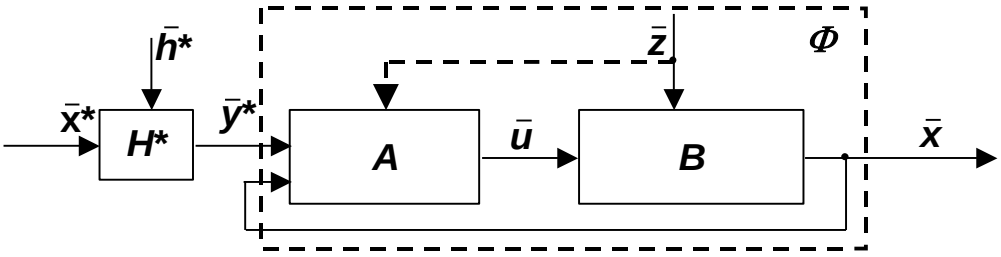


Рис. 3.5

В даному випадку на керуючий пристрій **А** по контуру зворотного зв'язку з виходу об'єкта **В** надходить інформація про значення керованої величини. Усередині замкнутого контуру системи завади і шуми відсутні. Однак вплив $\bar{\mathbf{x}}^*$, що задає управління, надходить на вхід **А** через канал з шумом. У цьому каналі шум змішується з корисним сигналом. На виході каналу з'являється величина $\bar{\mathbf{y}}^*$, що відрізняється від $\bar{\mathbf{x}}^*$, яка й подається на вхід керуючого пристрою **А** замість $\bar{\mathbf{x}}^*$. Завданням керуючого пристрою є відокремлення корисного сигналу від шуму; останнє можна здійснити з певним ступенем надійності, якщо спостерігати значення $\bar{\mathbf{y}}^*$ протягом певного проміжку часу. Оцінка значення $\bar{\mathbf{x}}^*$, зроблена після закінчення цього проміжку часу, буде залежати, взагалі кажучи, від значень $\bar{\mathbf{y}}^*$, які спостерігалися. Отже, оцінка $\bar{\mathbf{x}}^*$, а отже, і управляючий вплив, що робиться пристроєм **А** в даний, поточний момент часу t, залежать від «передісторії» вхідної величини $\bar{\mathbf{y}}^*(\tau)$ при $\tau < t$. Інакше кажучи, керуючий вплив в момент часу t є деякий функціонал $\Psi\left(\bar{\mathbf{y}}^*\right)$ від значень $\bar{\mathbf{y}}^*(\tau)$ при $\tau < t$. Але це означає, що на відміну від пристроїв, розглянутих в розділах III і IV, оптимальне котра управляє пристрій А в даному випадку вже не є безінерційним. Воно повинно бути динамічною системою, вихідна величина якої в даний момент часу залежить не тільки від поточних значень вхідних величин, але і від їх значень в минулому. У цій та наступній главах оптимальне котра управляє пристрій являє собою динамічну систему.

На рис. 3.5 показана схема замкнутої системи управління. Ставиться завдання синтезу оптимального керуючого пристрою - точніше, знаходження його оптимального алгоритму. Оскільки **А** являє собою динамічну систему, будемо говорити про оптимальну стратегію керуючого пристрою **А.**

Іноді завдання визначення оптимальної стратегії пристрою **А** в схемі рис. 3.5 вирішують, розбиваючи всю задачу на два етапи. На першому етапі розглядають всю систему всередині пунктирного контуру як один пристрій **Ф** і визначають оптимальний алгоритм цього пристрою в цілому. На другому етапі пристрій **Ф** розчленовують, знаходячи при заданому операторі об'єкта **В** закон дії пристрою **А**. Звичайно, при цьому можуть виникнути труднощі, пов'язані з товарність або грубістю отриманого пристрою **А**. Реалізованим назвемо такий пристрій, вихідна величина якого залежить, бути може, від поточних і минулих, але ні в якому разі не залежить від майбутніх значень вхідних величин, якщо останні не задані заздалегідь. Властивість грубості означає, що при досить малих змінах параметрів алгоритму керуючого пристрою зміна будь-яких вихідних величин або характеристик цього пристрою або системи в цілому як завгодно малі. Як тільки керуючий пристрій стає динамічною системою, ми змушені накласти на можливі типи таких пристроїв обмеження у вигляді умов реалізованості і грубості. Часто застосовується поняття фізичної можливості бути реалізованим включає в себе обидва зазначених вище поняття, як йому підпорядковані.

На рис. 3.6 показана розімкнена система з незалежним накопиченням інформації. Вплив x^*, що задає управління, як і на рис. 3.5, проходить через канал H^* з шумом h^*.

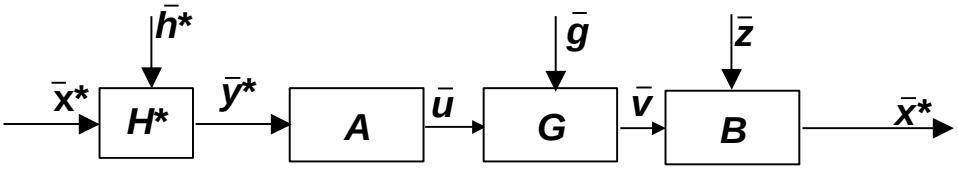


Рис. 3.6

З цього каналу вплив $\bar{y}^*$ – суміш корисного сигналу і шуму – надходить на вхід керуючого пристрою $\mathbf{A}$. Припустимо, що пристрій $\mathbf{A}$ діє на об'єкт **B** через канал **G** з шумом $\bar{g}$. Тому дійсний вплив $\bar{v}$, який надходить на вхід об'єкта **B,** може відрізнятися від впливу $\bar{u}$ на виході керуючого пристрою **A**. В цьому розділі ми будемо розглядати розімкнені системи, вихідна величина яких не подається на вхід **A.**

Випадкова завада $\bar{z}$, що надходить на об'єкт $\mathbf{B}$, в схемі рис. 3.6 не вимірюється. Тому керуючому пристрою **A** в цій схемі відомі лише апріорні імовірнісні характеристики завади $\bar{z}$, які можуть бути знайдені, наприклад, шляхом статистичної обробки дослідів в минулому і закладені в пристрій **A.** Ніяких відомостей про конкретну поведінку завади $\bar{z}$ в даному випробуванні пристрій **A** в схемі рис. 3.6 не отримує.

Можливий, проте, випадок, коли в ході випробування величина $\bar{z}$ вимірюється, і результат вимірювання надсилається на вхід пристрою **A**. Такий випадок зображений на рис. 3.7. Оскільки будь-яке вимірювання проводиться з деякою погрішністю, то можна уявити цей процес у вигляді передачі результату точного вимірювання завади $\bar{z}$ через канал **E** з шумом $\bar{e}$, який домішується до корисного сигналу. Значення суміші $\bar{w}$ на виході каналу **E**, яка подається на керуючий пристрій, взагалі кажучи, відрізняється від істинного значення.

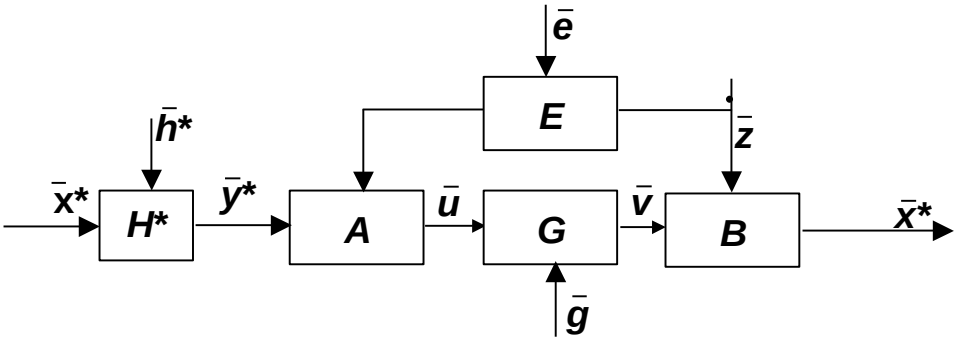


Рис. 3.7

Якщо завада $\bar{\mathbf{z}}$ вимірюється хоча б наближено, то з'являється можливість її точної або наближеній компенсації. Це означає, що вплив $\bar{\mathbf{u}}$ може бути розрахований таким чином, щоб нейтралізувати ефект дії завади $\bar{\mathbf{z}}$ і домогтися, точно або наближено, необхідного закону, який зв'язує $\bar{\mathbf{x}}$ і $\bar{\mathbf{x}}^*$, який в ідеальному випадку не повинен залежати від значень $\bar{\mathbf{z}}$.

Таким чином, наведені результати можуть використовуватися для надходження деяких параметрів відомого оператора об’єкта. Цей клас задач має велике прикладне значення. Він є вельми широким та різноплановим, тому для конкретизації розглянемо деякі частинні задачі вимірювання сигналів та компенсації завад у телекомунікаційних мережах спеціального призначення – безпроводових мережах стандартів *IEEE* 802.11*n*.

3.3 Компенсаційні методи захисту від завад у безпроводових мережах

Саме зв’язок мережних вузлів безпроводових мереж, через вільне середовище (радіозв’язок) є джерелом уразливості мережі до ненавмисних та навмисних завад. Стандартне обладнання безпроводової мережі не здатне розпізнати завади, створювані пристроями, що не відносяться до згаданої групи стандартів.

Розглянемо метод компенсації завади при відомих координатах джерела корисного сигналу з використанням алгоритму визначення координат джерела завади.

Захист автономного мережного вузла з двоканальним прийомом сигналу (рознесений прийом, *Rx Diversity* або *Single Input Multiple Output – SIMO* 1x2) при наявності завади, потужність якої достатня для ефективного притлумлення або перекручення корисного сигналу, виконується у такій послідовності:

– визначення наявності кутового рознесення джерел корисного сигналу та завади;

– обчислення кутових координат джерела завад;

– формування нуля (провалу) діаграми спрямованості антени у напрямі на джерело завади.

Розглянемо амплітудний двоканальний кутомірний датчик (моноімпульсний пеленгатор), який вимірює координати одного джерела й дозволяє визначити число рознесених по куту джерел (один чи два). Для розв'язання останньої задачі в [72] запропоновано використовувати значення показника

$$q = \frac{R_c\left(\overline{\dot{U}_1 \dot{U}_2^*}\right)}{\overline{\dot{U}_1 \dot{U}_2^*}},$$

де $\dot{U}_1$ та $\dot{U}_2^*$ – комплексні амплітуди сигналів на виходах першого та другого каналів.

Показник q є функцією кутового рознесення $\Delta\theta_{\text{Н}}$ джерел сигналів. Отже, при відомих кутових координатах можна визначити кутові координати джерела завад.

Формування нульової зони прийому (провалу) у напрямі на джерело завад при апріорно відомих координатах джерела корисного сигналу $\theta_{\text{Н}}$ у двоканальному пеленгаторі забезпечується при виконанні наступних умов:

$$\begin{aligned} \dot{K}_0 \dot{F}_0(\theta_{\text{Н}}) + \dot{K}_k \dot{F}_k(\theta_{\text{Н}}) &\neq 0; \\ \dot{K}_0 \dot{F}_0(\theta_{\text{П}}) + \dot{K}_k \dot{F}_k(\theta_{\text{П}}) &= 0, \end{aligned} \qquad (3.6)$$

де $\dot{F}_0(\theta)$ і $\dot{F}_k(\theta)$ – нормовані комплексні ДС основного та компенсаційного каналів;

$\dot{K}_0(\theta)$ і $\dot{K}_k(\theta)$ – комплексні коефіцієнти передавання відповідних каналів. Коефіцієнти спрямованої дії антен G_0 і G_k враховані в $\dot{K}_0(\theta)$ і $\dot{K}_k(\theta)$.

Для реалізації умов (3.6) знаходять застосування різні методи: амплітудного віднімання (некогерентний), високочастотний (когерентний), поляризаційний та ін.

На рис. 3.8 зображено схему амплітудного компенсатора завади. Для дійсних значень $F(\theta)$ і K, лінійних детекторів основного та компенсаційного каналів мають місце наступні умови компенсації:

$$\begin{aligned} K_0F_0(\theta_{\text{Н}}) - K_kF_k(\theta_{\text{Н}}) &\neq 0; \\ K_0F_0(\theta_{\text{П}}) - K_kF_k(\theta_{\text{П}}) &= 0, \end{aligned} \tag{3.7}$$

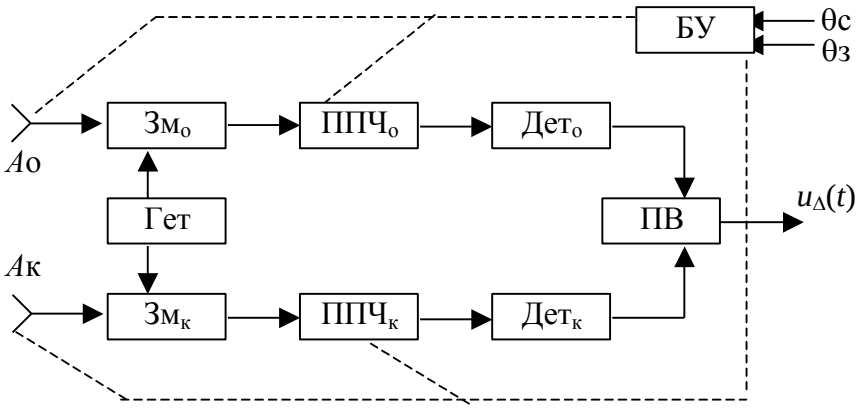


Рис. 3.8 Амплітудний компенсатор завад. Ао та Ак – індекси основного та компенсаційного каналів відповідно; Ао та Ак – антени; Гет – гетеродин; Зм$_о$ та Зм$_к$ – змішувачі; ППЧо та ППЧк – підсилювачі проміжної частоти; Дет – детектори; ПВ – пристрій віднімання; БУ – блок управління

Блок управління в загальному випадку змінює просторове положення ДС антен основного A_0 й компенсаційного A_k каналів та коефіцієнтів посилення приймальних каналів у відповідності зі значеннями $\theta_{\tilde{N}}$ і $\theta_{Ç}$ для виконання умови (3.7).

Положення ДС антен при формуванні нульової зони прийому на джерело завади показано на рис. 3 9. Амплітуди сигналів на виходах основного та компенсаційного приймачів з урахуванням позначень на рис. 3.8 та 3.9 запишуться у виді

$$\begin{aligned} U_0 &= K_0F_0(\theta_{01} - \Delta\theta_{\tilde{N}})U_{\tilde{N}} + K_0F_0(\theta_{01})U_{Ç} + \sigma_0; \\ U_k &= K_kF_k(\theta_{02} + \Delta\theta_{\tilde{N}})U_{\tilde{N}} + K_kF_k(\theta_{02})U_{Ç} + \sigma_k, \end{aligned} \tag{3.8}$$

де $U_{\text{С}}$ і $U_{Ç}$ – амплітуди корисного сигналу та завади відповідно;

θ_{01} і θ_{02} – зміщення максимумів ДС антен основного та компенсаційного

каналів відносно рівносигнального напряму (РСН); цей напрям співпадає з напрямом на джерело завади;

$\Delta\theta_{\text{Н}}$ – кутове рознесення джерел сигналу та завади;

σ_0 і σ_k – середньоквадратичні відхилення шумів на виходах приймачів.

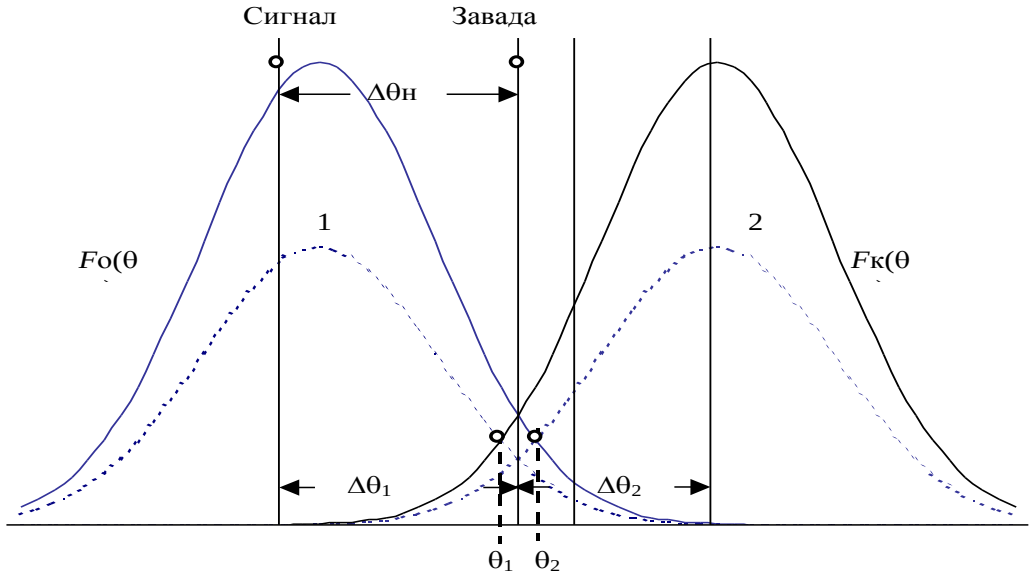


Рис. 3.9 Геометричні та енергетичні співвідношення у двоканальному амплітудному компенсаторі. Два варіанти функцій просторової фільтрації при різних величинах коефіцієнтів передачі каналів позначені суцільними та штриховими кривими

На виході пристрою віднімання у відповідності з (3.8) при

$$K_0 F_0\left(\theta_{01}\right) = K_k F_k\left(\theta_{02}\right) \qquad (3.9)$$

має місце компенсація завади. Значення корисного сигналу з урахуванням внутрішніх шумів дорівнює

$$U_{\text{С}} = K_0 F_0\left(\theta_{01} - \Delta\theta_{\text{Н}}\right)U_{\text{Н}} - K_k F_k\left(\theta_{01} + \Delta\theta_{\text{Н}}\right)U_{\text{Н}} + \sqrt{\sigma_1^2 + \sigma_2^2}\,. \qquad (3.10)$$

Відношення h вихідного сигналу до шуму при $K_0 = K_k = K$, $\sigma_0^2 = \sigma_k^2 = \sigma_{\text{ø}}^2$, $\theta_{01} = \theta_{02} = \theta_0$, $F_0\left(\theta\right) = F_k\left(\theta\right) = F\left(\theta\right)$ дорівнює

$$h = \frac{KU_{\text{í}}}{\sqrt{2}\sigma_{\text{ø}}}\left[F\left(\theta_0 - \Delta\theta_{\text{í}}\right) - F\left(\theta_0 + \Delta\theta_{\text{í}}\right)\right]. \qquad (3.11)$$

Дамо оцінку впливу складової $Q\left(\Delta\theta_{\text{í}}\right) = F\left(\theta_0 - \Delta\theta_{\text{í}}\right) - F\left(\theta_0 + \Delta\theta_{\text{í}}\right)$ на

відношення h у залежності від кутового рознесення джерел $\Delta\theta_{\text{Н}}$ при апроксимації ДС антен функцією $F(\theta)=\exp\left[-1,4\left(\frac{\theta}{\theta_{0,5}}\right)^2\right]$. Для ширини ДС антени по половинній потужності $\theta_{0,5}=60°$ і $\theta_0=30°$ значення Q як функції кутового рознесення $\Delta\theta_{\text{ї}}$ наведені на рис. 3.10.

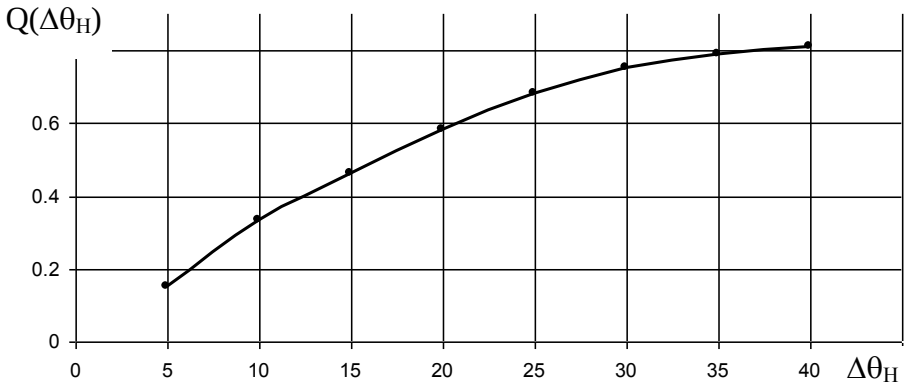


Рис. 3.10 Залежність вихідного відношення сигнал/шум від кутового рознесення джерел сигналу та завади

Мінімальне значення $\Delta\theta_{\text{ї}}$ залежить від рівня корисного сигналу (5) та алгоритму подальшої обробки в умовах урахування шумів.

Поточні кутові координати джерела завад в умовах нестаціонарної електромагнітної обстановки та числа користувачів, що змінюється випадковим чином, також можуть бути змінними. Це необхідно фіксувати спеціальними методами й засобами на приймальній стороні. Зміни РСН (положення нульової зони прийому) для компенсації завади при зміні кутових координат її джерела згідно з умовою (2) може бути забезпечено відповідними регулюваннями при незмінних ДС антен і коефіцієнтах K_0 і K_k.

Переміщення РСН внаслідок регулювання коефіцієнтів K_0 і K_k можна спостерігати на рис. 3.9, де крива 1 відповідає зменшенню K_0, що приводить положення РСН в θ_1, а крива 2 – зменшенню K_k (РСН зміщується в положення θ_2).

Визначимо зміщення рівносигнального напряму $\theta_{\text{СМ}}$ у відповідності з поточними координатами $\theta_{\text{ї}}$ відносно положення джерела корисного сигналу,

напрям на який співпадає з максимумом ДС антени A_0, в залежності від відношення $\frac{K_k}{K_0}$. З урахуванням (3.7) маємо

$$\frac{K_{kT}}{K_{0T}} = \frac{F_0\left(\theta_{\text{СМ}}\right)}{F_k\left(2\theta_0 - \theta_{\text{СМ}}\right)} = \frac{\exp\left[-1,4\left(\frac{\theta_{\text{СМ}}}{\theta_{0,5}}\right)^2\right]}{\exp\left[-1,4\left(\frac{2\theta_0 - \theta_{\text{СМ}}}{\theta_{0,5}}\right)^2\right]}.$$

Поточні значення K_{0T} і K_{kT} регулюються для забезпечення потрібної величини $\theta_{\text{СМ}}$ наступним чином: при $0 < \theta_{\text{СМ}} \le \theta_0$ коефіцієнт K_{0T} зменшується, тоді як значення K_k лишається незмінним; при $\theta_0 < \theta_{\text{СМ}} \le 2\theta_0$ зменшується коефіцієнт K_{kT}, в той час як лишається незмінним K_0.

На рис. 3.11 представлено залежність $\theta_{\text{СМ}}$ від відношення K_{kT}/K_{0T}

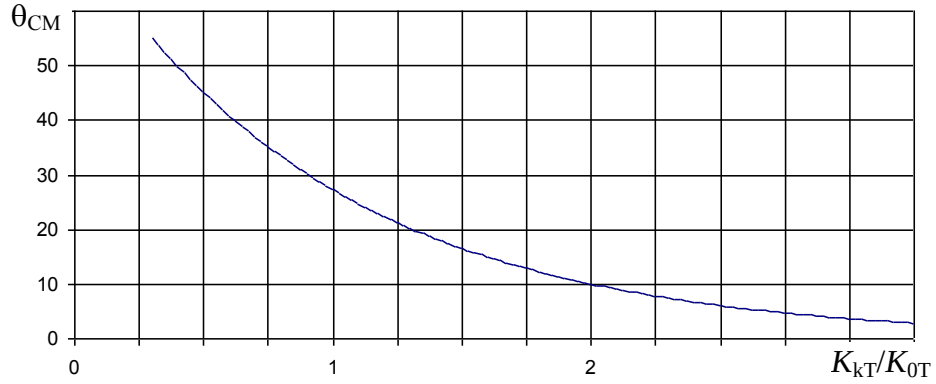


Рис. 3.11 Залежність зсуву РСН компенсатора від величини відношення коефіцієнтів передачі основного та компенсаційного каналів

Також представляє інтерес вплив регулювань – зміни одного з коефіцієнтів при незмінному іншому – на відношення сигнал/шум на виході пристрою віднімання. Вважаючи, що прийом корисного сигналу здійснюється у напрямі максимуму ДС антени основного каналу, у відповідності до (6) маємо

$$h = \frac{U_{\text{С}}}{\sigma_{\text{ø}}\sqrt{\left(\frac{K_{0\text{Т}}}{K_0}\right)^2 + \left(\frac{K_{k\text{Т}}}{K_k}\right)^2}}\left[K_{0\text{Т}}F_0\left(\theta\right) - K_{k\text{Т}}F_k\left(2\theta\right)\right], \qquad (3.12)$$

де $K_{0\text{т}} = \dfrac{K_{k\text{т}} F_k\left(2\theta_0 - \theta_{\text{см}}\right)}{F_0\left(\theta_{\text{см}}\right)}$; $K_{0\text{т}} = \text{var}$, $K_{k\text{т}} = K_k = \text{const}$;

$$K_{0\text{т}} = \frac{K_{0\text{т}} F_0\left(\theta_{\text{см}}\right)}{F_k\left(2\theta_0 - \theta_{\text{см}}\right)}; K_{k\text{т}} = \text{var},\ K_{0\text{т}} = K_0 = \text{const}.$$

Оцінка h у відповідності до (3.12) і значеннями K_{0T} і K_{kT} свідчить про зменшення рівня корисного сигналу у порівнянні з його номінальним значенням при варіаціях $K_0 F_0(\theta)$ у діапазоні кутів зміщення (рознесення джерел) $0 < \theta_{\text{см}} \le \theta_0$. По мірі зростання кута $\theta_{\text{см}}$ збільшується рівень корисного сигналу. У діапазоні $\theta_0 < \theta_{\text{см}} \le 2\theta_0$ рівень корисного сигналу залишається практично незмінним і дорівнює своєму номінальному значенню.

На завершення відмітимо, що наведені оцінки для різних варіантів амплітудної компенсації справедливі для завади, яка є не суміщеною по куту приходу з кутом приходу корисного сигналу. Результати розрахунків амплітуд корисного сигналу при переміщенні його джерела будуть корисними для роботи з мобільними абонентами безпроводової мережі при виборі найбільш ефективного режиму компенсації.

При зміні кутових параметрів джерел завад вже недостатньо здійснювати захист від заважаючих сигналів методами компенсації. Пропонується автоматизоване стеження за координатами джерела завади. Система стеження представляє собою комбіновану антенну систему з вузькою діаграмою спрямованості. Прийом корисного сигналу здійснюється всенаправленою антеною. Таким чином, пропонується розрізнювати антени для прийому корисного сигналу та антену для прийому та компенсації завади, рознесеної по куту з корисним сигналом. Безпроводові системи зв’язку, які працюють у щільному угрупуванні радіо пристроїв, також потребують притлумлення зовнішніх завад різними методами, найбільш перспективними з яких є методи амплітудної та фазової компенсації. Розглянемо принципові умов компенсації завад та загальні можливості компенсації просторово-рознесених завад у безпроводових мережах зв’язку.

Компенсація завади від одного джерела з кутовою координатою θ_{int} при прийомі від джерела сигналу з кутовою координатою θ_{sign} можлива при виконанні таких умов:

$$\dot{E}_{\text{int}}(t)\dot{F}_0(\theta_{\text{int}})G_0(\theta_{\text{int}})\dot{K}_0 - \dot{E}_{\text{int}}(t)\dot{F}_k(\theta_{\text{int}})G_k(\theta_{\text{int}})\dot{K}_k = 0; \qquad (3.13)$$

$$\dot{E}_{sign}(t)\dot{F}_0(\theta_{sign})G_0(\theta_{sign})\dot{K}_0 - \dot{E}_{sign}(t)\dot{F}_k(\theta_{sign})G_k(\theta_{sign})\dot{K}_k \neq 0, \qquad (3.14)$$

де $\dot{E}_{\text{int}}(t)$, $\dot{E}_{sign}(t)$ – комплексні амплітуди завади та сигналу відповідно;

$\dot{F}_0(\theta_{\text{int}})$, $\dot{F}_k(\theta_{\text{int}})$ – нормовані діаграми спрямованості (ДС) антен основного та компенсаційного каналів відповідно;

$\dot{K}_0$, $\dot{K}_k$ – коефіцієнти підсилення основного та компенсаційного каналів відповідно;

$G_0(\theta_{\text{int}})$, $G_k(\theta_{\text{int}})$ – коефіцієнти направленої дії відповідних каналів.

У мережах зв'язку зазвичай використовуються антени з досить широкими ДС в азимутальній площині (часто навіть не спрямовані антени). Тому для виконання умови (3.13) доцільно мати компенсаційний канал з досить вузькою ДС, яка переміщується по азимуту в напрямі прийому сигналу від джерела завад.

При амплітудній (енергетичній) компенсації компоненти виразів (3.13) та (3.14) є дійсними. Умови компенсації завади згідно з (3.14) при $E_{\text{int}0}G_0K_0 = E_{\text{int}k}G_kK_k$ зводяться до виконання рівності $F_0(\theta_{\text{int}}) - F_k(\theta_{\text{int}}) = 0$. На рис. 3.12 розглянуті положення ДС каналів у випадку, коли по основному каналу приймається суміш сигналу та завади, а по компенсаційному – тільки завада.

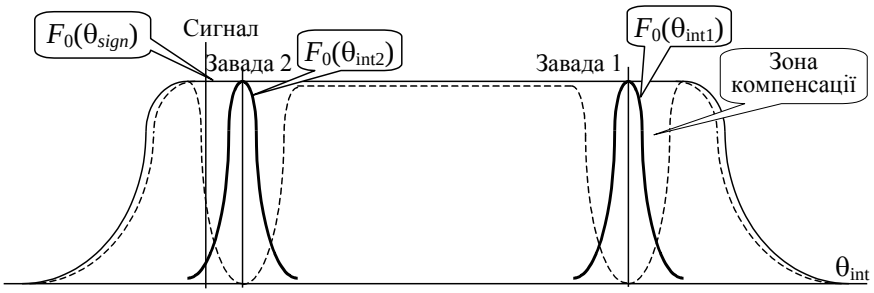


Рис. 3.12 Діаграми спрямованості основного та компенсаційного каналів.

Компенсація завади 1

Визначення кутових координат джерела здійснюється з похибками, що приводить до неповної компенсації завади. Степінь цієї неповноти ΔK при описі ДС антени виразом

$$F_k(\theta) = \exp\left[-1{,}4\left(\frac{\theta}{\theta_{0,5}}\right)^2\right]$$

$$\Delta K = 1 - F_k\left(\theta_{\text{int}} \pm \Delta\theta_{\text{int}\,0}\right) \approx 1 - \exp\left[-1{,}4\left(\frac{\theta_{\text{int}} \pm \Delta\theta_{\text{int}\,0}}{\theta_{\text{int}\,0,5}}\right)^2\right], \qquad (3.15)$$

де θ_{int} – напрям максимуму ДС на заваду, при якому забезпечується повна компенсація.

На рис. 3.13 показані залежності $\Delta K = f\left(\Delta\theta_{\text{int}\,0}\right)$ для $\theta_{0,5} = 5^\circ$ та $\theta_{0,5} = 10^\circ$.

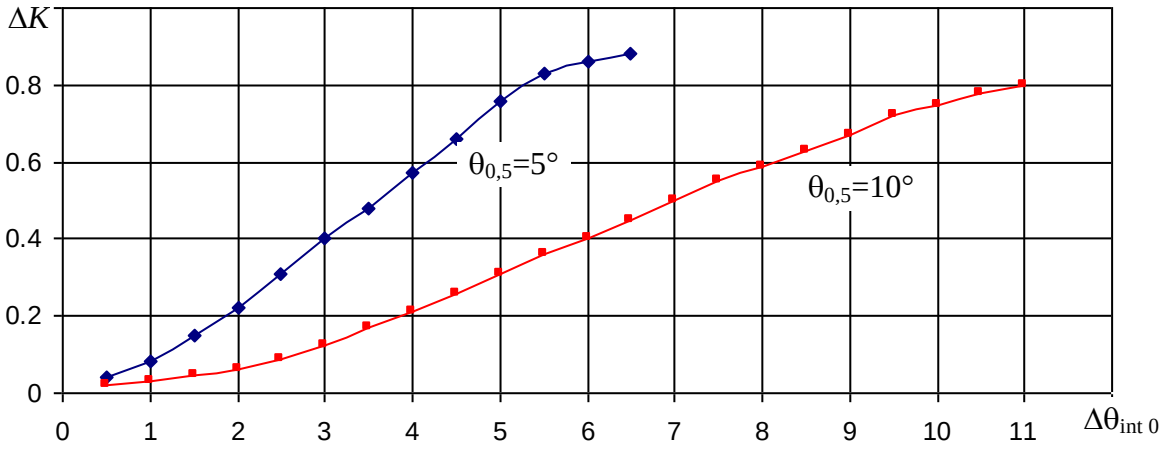


Рис. 3.13 Залежності степеню повноти компенсації від похибки визначення координати завади

Оцінку зменшення степеню компенсації зі збільшенням величини $\theta_{\text{int}\,0,5}$ необхідно давати з урахуванням особливостей методу визначення кутових координат. Зокрема, якщо кутове положення завади визначається по максимуму ДС, похибка зі зростом $\theta_{\text{int}\,0,5}$, очевидно, також зростатиме. Дослідимо характер цього зростання.

Знайдемо щільність імовірності показника неповної компенсації з урахуванням випадкового характеру похибок визначення кутових координат джерела завад. У якості базового приймемо нормальний закон розподілу похибок θ_{int}:

$$W\left(\theta_{\text{int}}\right)=\frac{1}{\sqrt{2\pi}\sigma_{\text{int}}}\exp\left[-\frac{\theta_{\text{int}}^2}{2\sigma_{\text{int}}^2}\right] \qquad (3.16)$$

та розміром зони компенсації, яким визначається показник повноти компенсації:

$$\Delta K=1-F_k\left(\theta\right)\approx 1-\exp\left[-1,4\left(\frac{\theta_{\text{int}}}{\theta_{\text{int}\,0,5}}\right)^2\right].$$

$$\text{При}\ \left(\frac{\theta_{\text{int}}}{\theta_{\text{int}\,0,5}}\right)^2<<1 \qquad \Delta K\approx\frac{1,4}{\theta_{\text{int}\,0,5}^2}\theta_{\text{int}}^2=\alpha\theta_{\text{int}}^2.$$

У відповідності з правилом перетворення випадкових величин [61] маємо

$$W_{\Delta K}\left(\Delta K\right)=W_{\text{int}}\left(\sqrt{\Delta K}\right)\frac{1}{\sqrt{2\Delta K}}+W_{\text{int}}\left(-\sqrt{\Delta K}\right)\frac{1}{\sqrt{2\Delta K}};\ \ \Delta K\to 0 \qquad (3.17)$$

Вводячи в (3.17) заданий закон (3.16) для $W\left(\theta_{\text{int}}\right)$, отримаємо

$$W_{\Delta K}\left(\Delta K\right)=\frac{1}{\sqrt{2\pi}\sigma_{\text{int}}}\cdot\frac{1}{2\sqrt{\alpha\theta_{\text{int}}^2}}\left\{\exp\left[-\frac{\left(\sqrt{\alpha\theta_{\text{int}}^2}\right)^2}{2\sigma_{\text{int}}^2}\right]+\exp\left[-\frac{\left(-\sqrt{\alpha\theta_{\text{int}}^2}\right)^2}{2\sigma_{\text{int}}^2}\right]\right\}=$$

$$=\frac{1}{\sqrt{2\pi}\sigma_{\text{int}}}\cdot\frac{1}{\sqrt{\alpha\theta_{\text{int}}^2}}\exp\left[-\frac{\left(\sqrt{\alpha\theta_{\text{int}}^2}\right)^2}{2\sigma_{\text{int}}^2}\right],\ \ \Delta K\to 0$$

$W_{\Delta K}\left(\Delta K\right)=0$ при $\Delta K\to 0$.

Одним з важливих питань для практики організації завадозахисту є розрізнювальна спроможність системи відносно кутового рознесення джерел сигналу та завади. При прийомі завади (сигнал відсутній) по компенсаційному каналу можлива достатньо глибока компенсація завади [61]; при наявності в

каналі сигналу у суміші з завадою степінь компенсації завади знижується наряду зі зменшенням рівня сигналу.

Дамо оцінку впливу розрізнювальної спроможності $\Delta\theta_{\text{res}} = \theta_{sign} - \theta_{\text{int}\,2}$ системи (див. рис. 3.12) на зниження рівню сигналу, що попадає в зону компенсації. Задача розв'язується аналогічно визначенню показника повноти компенсації (3.15). Треба тільки замінити $\theta_{\text{int}\,0}$ на $\Delta\theta_{\text{res}}$. Рівень зменшення сигналу оцінюється коефіцієнтом його ослаблення

$$K_{ws} = 1 - \exp\left[-1,4\left(\frac{\theta_{sign} - \theta_{\text{int}\,2}}{\theta_{\text{int}\,0,5}}\right)^2\right]. \qquad (3.18)$$

У табл. 3.1 наведені значення $K_{ws} = f\left(\frac{\Delta\theta_{\text{res}}}{\theta_{\text{int}\,0,5}}\right)$.

Таблиця 3.1

$\Delta\theta_{\text{res}}/\theta_{\text{int}\,0,5}$	2	1,5	1	0,5	0,25
K_{ws}	0,996	0,958	0,753	0,295	0,084

У якості показника розрізнювальної спроможності $\Psi(\theta_{\text{res}})$ прийняте значення θ_{res}, при якому

$E_{out} = K_{ws}E_{in} \geq E_{aclv}$, де E_{aclv} – припустимий рівень сигналу.

Порівнюючи залежності показника степеню компенсації завади ΔK та коефіцієнта ослаблення сигналу K_{ws} від ширини ДС антени компенсаційного каналу $\theta_{k\,0,5}$, можна помітити наступне. Зі збільшенням $\theta_{k\,0,5}$ ΔK зменшується, а K_{ws} зростає. Вказану обставину необхідно враховувати при виборі $\theta_{k\,0,5}$.

Розглянемо тепер метод амплітудної компенсації завад. На сучасному рівні розвитку технологій та елементної бази мережного обладнання метод амплітудної компенсації реалізується досить просто. Відмітимо деякі особливості його застосування.

1. Необхідність урахування принципу нормування рівнів сигналів у каналах. Так, постійна часу системи автоматичного регулювання посилення в компенсаційному каналі впливає на повноту компенсації у залежності від параметрів (довжини та частоти повторення) імпульсних завад.

2. Зменшення ефективності компенсації при перевіддзеркаленнях сигналів від будівель та споруд, водної поверхні тощо. Це пояснюється великою довжиною об'єктів, що перевіддзеркалюють сигнал, та відповідним розширенням кутового спектру.

3. Підвищення рівня внутрішніх шумів на виході пристрою віднімання

$$\sigma_{nout}^2 = \sigma_{nin0}^2 K_0^2 + \sigma_{nink}^2 K_k^2,$$

де σ_{nin0}^2 та σ_{nink}^2 – дисперсії шумів вхідних каскадів каналів приймачів.

Оскільки $G_k K_k = G_0 K_0$, $K_k = \dfrac{G_0 K_0}{G_k}$, тобто при $G_k >> G_0 \quad K_k << K_0$.

При високочастотній (фазовій) компенсації забезпечується отримання завад з однаковими амплітудами та фазами на виходах підсилювачів високої або проміжної частоти. Ці вихідні (завадові) сигнали у подальшому подаються на пристрій віднімання. Спрощений принцип роботи одноканального фазового компенсатора (рис. 3.14) полягає в наступному.

1. Нехай виконується умова перевищення довжини завади над довжиною сигналу: $\tau_{\text{int}} > \tau_{sign}$. Забезпечення рівності амплітуд сигналів $u_{\text{int}0}(t)$ та $u_{\text{int}k}(t)$ на вході пристрою віднімання у відповідності з виразом $K_k = \dfrac{G_0 K_0}{G_k}$ (при рівності вхідних напруг $U_{\text{int}0} = U_{\text{int}k}$) досягається шляхом введення автоматичного регулювання підсилення компенсаційного каналу по сигналу з основного каналу.

2. Рівність фаз завади на вході пристрою віднімання забезпечується шляхом автоматичного підстроювання фази.

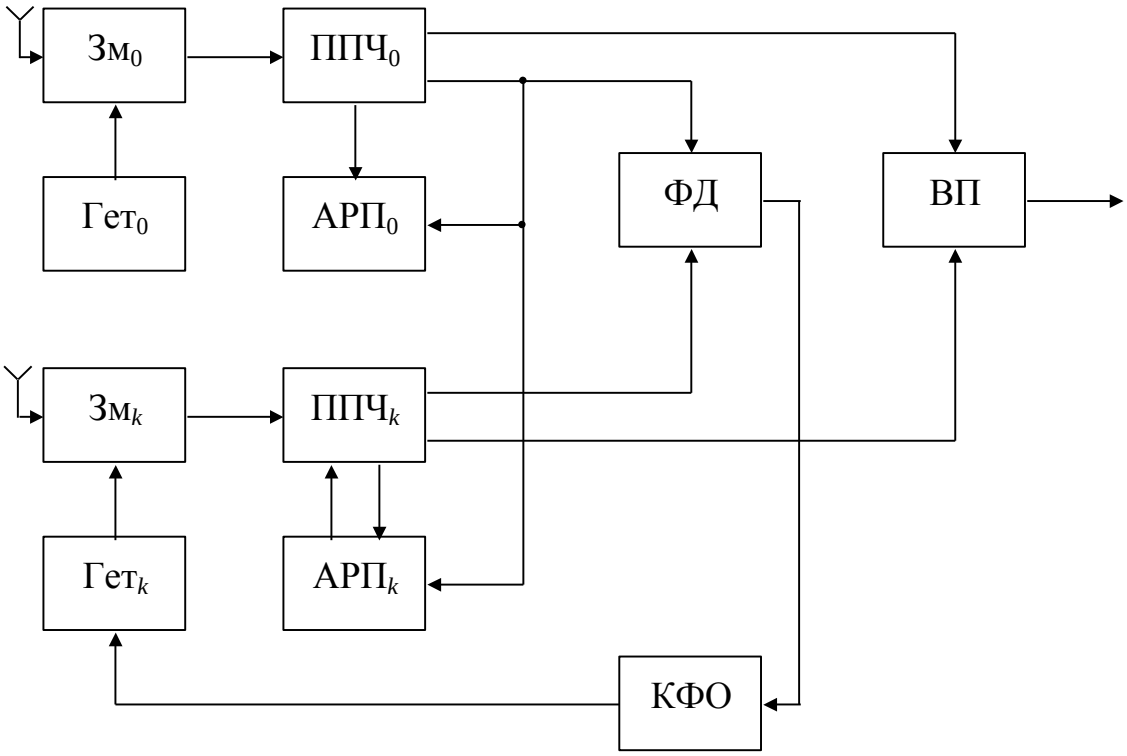


Рис. 3.14 Одноканальний фазовий компенсатор. Зм – змішувач; ППЧ – підсилювач проміжної частоти; Гет – гетеродин; ФД – фазовий детектор; АРП – пристрій автоматичного регулювання підсилення; ВП – відеопідсилювач; КФО – керований фазообертач

Сигнали з підсилювачів проміжної частоти поступають на фазовий детектор, на виході якого при малих величинах різниці $\varphi_{\text{int}\,0}$ та $\varphi_{\text{int}\,kc}$ маємо

$$u_{phd} = K_{phd}\left(\varphi_{\text{int}\,0} - \varphi_{\text{int}\,kc}\right),$$

де $\varphi_{\text{int}\,0}$ – фаза завади в основному каналі;

$\varphi_{\text{int}\,kc}$ – фаза завади в компенсаційному каналі (на виході керованого фазообертача).

Сигнал з фазового детектора поступає на керований фазообертач, за допомогою якого вирівнюються фази $\varphi_{\text{int}\,0}$ та $\varphi_{\text{int}\,kc}$.

Як показують результати розрахунків, у розглянутому пристрої при співпадінні частот сигналів забезпечується притлумлення немодульованої завади на 40 – 50 дБ. При розстроюванні частоти завади на ±(10 – 15) МГц степінь

притлумлення знижується до 25 дБ. Це пояснюється неідентичністю амплітудно-частотних (АЧХ) та фазочастотних (ФЧХ) характеристик трактів основного та компенсаційного каналів. Впевнене притлумлення завади не менш, чим на 40 дБ можливо при відмінності АЧХ трактів не більш ніж на 0,1 дБ, а ФЧХ – не більш ніж на 0,6°.

Амплітуду та фазу сигналу компенсації можна автоматично підбирати у спеціальному блоці, що складається з атенюаторів, фазообертачів та пристрою розділення. Можна також використовувати компенсацію завади пристроєм з кореляторами та квадратурними перетворювачами [61].

Компенсаційні методи захисту від просторово-рознесених завад необхідно розглядати як частину загального комплексу технічних та організаційних заходів захисту. Необхідність такого підходу диктується як складністю та динамічністю завадової обстановки, так і виникненням умов, за якими рівень притлумлення завади може стати незадовільним. Це потребує додаткових заходів захисту, за допомогою яких будуть подолані обмеження розроблених методів компенсації завад.

ВИСНОВКИ ДО РОЗДІЛУ 3

1. В умовах невизначеності впливу дестабілізуючих факторів найбільш придатним для аналізу та прийняття рішень можна вважати мінімаксний критерій, який, по суті, є інваріантним до апріорних статистичних розподілів.

2. Оскільки реально апріорні дані існують завжди, хоча їх обсяг змінюється у вельми широких межах, було б недоцільно зовсім відмовлятися від їх використання. Для поєднання завдань пошуку оптимальних статистичних рішень та накопичення поточних даних для подальшого вивчення досліджуваного об’єкта на наступних етапах запропоновано впровадити метод дуального управління Фельдбаума.

3. Досліджені різні методи накопичення інформації про дестабілізуючі фактори та розроблено комбінований метод, придатний для моніторингу стану та параметрів телекомунікаційної мережі. На підгрунті отриманих результатів розроблені компенсаційні методи від завад у безпроводових мережах.

ОСНОВНІ РЕЗУЛЬТАТИ ТА ВИСНОВКИ

Метою даної роботи є розробка методів та засобів управління інформаційною безпекою в умовах невизначеності впливу дестабілізуючих факторів. У якості предметної області дослідження обрано сучасну телекомунікаційну мережу майбутніх поколінь – Future Network. Проведено аналіз системи ключових параметрів ефективності і особливостей їх застосування для управління якістю сервісу телекомунікаційної мережі як складної інформаційно-комунікаційної системи. Показано, що при використанні статистичного підходу можна виділити залежності між ключовими параметрами мережі, що дає можливість побудови системи управління якістю сервісу та врахування найбільш небезпечних дестабілізуючих факторів. Встановлено, що матриці коефіцієнтів нормальних рівнянь для обчислення оцінок по мінімуму середнього квадрата помилки мають структуру, близьку до діагонально-домінантної, що дає можливість прискорення і спрощення процедур ітераційного пошуку рішень.

Розглянуто сучасні методи моніторингу та аналізу телекомунікаційних мереж та проведено їх порівняльний аналіз. При дослідженні узагальненої моделі управління телекомунікаційними мережами вибрано та обгрунтовано критерії оптимізації ключових параметрів функціонування мережі і поточного управління мережею за результатами кореляційно-регресійного анадізу. Використання ключових параметрів ефективності дає можливість оцінювання та прогнозу стану складної системи, якою є телекомунікаційна мережа.

Зроблено обґрунтований висновок, що за умов випадкового характеру дестабілізуючих факторів, які негативно впливають на якість сервісу та ефективність роботи мережі, треба шукати шляхи подолання апріорної невизначеності. Запропоновано комбінований метод статистичного синтезу інформаційних систем з використанням мінімаксного підходу та методу дуального управління Фельдбаума.

З використанням запропонованого методу подолання апріорної невизначеності розроблено компенсаційні методи захисту від завад як з одного з найбільш

небезпечних зовнішніх дестабілізуючих факторів, особливо для безпроводових мереж.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України "Про телекомунікації". - Документ 1280-IV, чинний, поточна редакція — Редакція від 04.11.2018, підстава - 2581-VIII, Відомості Верховної Ради України (ВВР), 2004, № 12, ст.155.

2. Про захист інформації в інформаційно-телекомунікаційних системах. Документ 80/94-ВР, чинний, поточна редакція — Редакція від 19.04.2014, підстава - 1170-VII. - Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286.

3. Data Networks and Open System Communications – Open System Interconnection – Basic Reference Model: International Standard ITU-T Rec. X.200 (1994 E): ITU 1994. - 59 p.

4. Stallings W. High-Speed Networks and Internets: Performance and Quality of Service / 2nd Ed. - Pearson Education, 2002. - 744 pp.

5. Арнольд В.И. Теория катастроф. – 3-е изд. – М.: Наука, 1990. – 128 с.

6. Н.Н. Моисеев. Математические задачи системного анализа. – М.: Наука, 1981. – 488 с.

7. Стратонович Р.Л. Принципы адаптивного приема. – М.: Сов. радио, 1973. – 144 с.

8. Репин В.Г., Тартаковский Г.П. Статистический синтез при априорной неопределенности и адаптация информационных систем. – М.: Сов. радио, 1977. – 432 с.

9. Додонов А.Г. Живучесть информационных систем. / А.Г. Додонов, Д.В. Ландэ.- К.: Наук. думка, 2011. - 256 с.

10. Черкесов Г.Н. Методы и модели оценки живучести сложных систем. – М.: Знание, 1987. - 32 с.

11. Csermely P. Weak Links The Universal Key to the Stability of Networks and Complex Systems. - Springer-Verlag Berlin Heidelberg 2009. - 404 p.

12. Dreyfus S.E. Some types of optimal control of stochastic systems. – Rand

Corp., Santa Monica, CA,USA, 1963. – 29 p.

13. Hellmann F. Survivability of Deterministic Dynamical Systems // Frank Hellmann, Paul Schultz, Carsten Grabow, Jobst Heitzig, Jürgen Kurths, 2016. – [Електронний ресурс]. Режим доступу: https://www.nature.com/articles/srep29654.pdf – 12 p.

14. Hellmann F. Survivability: A Unifiying Concept for the Transient Resilience of Deterministic Dynamical Systems // Frank Hellmann, Paul Schultz, Carsten Grabow, Jobst Heitzig, Jürgen Kurths, 2016. [Електронний ресурс]. Режим доступу: https://www.researchgate.net/publication/277722675 – 16 p.

15. Бакулин В.Н. Управление обеспечением стойкости сложных технических систем к воздействию дестабилизирующих факторов различной физической природы / В.Н. Бакулин, С.Ю. Малков, В.В. Гончаров, В.И. Ковалев. - М.: ФИЗМАТЛИТ, 2006. - 304 с.

16. Бекбаев Г. А. Модель для расчета устойчивости функционирования телекоммуникационной сети железнодорожной станции в условиях неблагоприятных воздействий на основе схемы функциональной целостности // Г. А. Бекбаев, А. А. Привалов. - Известия Петербургского государственного университета путей сообщения, № 4, 2016. - с. 460 - 471.

17. Князева Н.А. Повышение структурной живучести телекоммуникационной сети. International Journal "Information Models and Analyses" Vol. 2, Number 3, 2013. - с. 275 - 284.

18. Князева Н.А. Метод обеспечения структурной живучести телекоммуникационной сети. International Journal "Information Models and Analyses" Vol. 8, Number 2, 2014. - с. 152 - 166.

19. Князева Н.А. Метод обеспечения структурной живучести интеллектуальной надстройки // Князева Н.А., Зименко Л.Н. - Інформаційно-керуючі системи на залізничному транспорті, 2016, №6. - с. 23 - 29.

20. Князева Н.А. Метод обеспечения живучести телекоммуникационной сети на основе перераспределения ресурсов сети. // Н.А. Князева, И.В. Грищенко, С.В. Шестопалов - Холодильна техніка та технологія, № 4 (150), 2014. - с. 65 - 71.

21. Басыров А.Г. Модель распределенной обработки информации в условиях воздействия дестабилизирующих факторов на информационно-телекоммуникационную систему // Басыров А.Г., Швецов А.С., Широбоков В.В., Шушаков А.О. - Современные проблемы науки и образования, №2, 2015. Издательский Дом "Академия Естествознания". - С. 215 - 221.

22. Михайлов Р.Л. Оценка устойчивости сети связи в условиях воздействия на неё дестабилизирующих факторов // Михайлов Р.Л., Макаренко С.И. - Радиотехнические и телекоммуникационные системы, 2013, №4. - с. 69 - 79.

23. Zhang R. Resource Management for Multimedia Services in High Data Rate Wireless Networks. / Ruonan Zhang, Lin Cai, Jianping Pan. Springer International Publishing AG, Cham, Switzerland, 2017. - 140 pp.

24. Recommendation ITU-T L.392 (04/2016). Disaster management for improving network resilience and recovery with movable and deployable information and communication technology (ICT) resource units. [Електронний ресурс]. Режим доступу: http://handle.itu.int/

25. Отрох С.И. Методика расчета показателей живучести каналов современной телекоммуникационной сети. // С.И. Отрох, Н.В. Коршун, В.А. Ярош. - Сучасний захист інформації №4, 2016. - с. 52 - 57.

26. Толубко В.Б. Методика оцінки сталості телекомунікаційної мережі в умовах дії зовнішніх непрогнозованих дестабілізуючих факторів // Толубко В.Б., Беркман Л.Н., Отрох С.І., Ярош В.О. – Зв’язок – 2016 – №5. – с. 3 – 7.

27. Масесов Н.А. Оценка живучести иерархических телекоммуникационных сетей военного назначения // Н.А. Масесов, Л.А. Бондаренко, Е.А. Ефанова, О.И. Садыков - Сучасні інформаційні технології у сфері безпеки та оборони № 1(31), 2018. - с. 61 - 67.

28. Тюрин М.В. Экспертная оценка живучести телекоммуникационных систем и компьютерных сетей (ТСКС) в условиях неполноты информации // Автоматизация в промышленности №7, 2008. - с. 15 - 18.

29. Ромашкова О.Н. Живучесть беспроводных сетей связи в условиях чрезвычайной ситуации // О.Н. Ромашкова, Е.В. Дедова. - T-Comm #6-2014. - с. 40

- 43.

30. Нетес В.А. Надежность сетей связи в период перехода к NGN // В.А.Нетес – Вестник связи, №9. – 2007, С. 4-5.

31. Крук Б. И. Телекоммуникационные системы и сети: Учебное пособие. В 3 томах. Том 1 – Современные технологии / Б.И. Крук, В.Н. Попантонопуло, В.П. Шувалов; под ред. проф. В.П. Шувалова. – Изд. 3-е – М.: Горячая линия – Телеком, 2003. – 647 с.

32. Стеклов В.К., Кільчицький Є.В. Основи управління мережами та послугами телекомунікацій. – К: Техніка, 2002. – 438 с.

33. Бестугин А. Р. Контроль и диагностирование телекоммуникационных сетей. / А.Р. Бестугин, А.Ф. Богданова, Г.В. Стогов – СПб.; – Политехника, 2003. – 174 стр.

34. Родионов С.С. Идентификация возмущающих воздействий на входе приемного устройства. / С.С. Родионов, В.Л. Удовикин. – Киев, “Знание”, 1979, 36 стр.

35. Гельфандбейн Я.А., Колосов Л.В. Ретроспективная идентификация возмущений и помех. – М.: Сов. радио, 1972. – 232 с.

36. Бутковский А.Г. Структурная теория распределенных систем. – М.: Наука, 1977. – 320 с.

37. Цыпкин Я. З. Информационная теория идентификации. – М.: Наука. Физматлит, 1995. – 336 с.

38. Идентифицируемые модели [Електронний ресурс] Режим доступу: \\ http://www.sardismusic.com/topics/t5r4part3.html

39. Гроп Д. Методы идентификации систем. Пер. с англ. – М.: Мир, 1979. – 302 с.

40. Сэйдж Э. Идентификация систем управления. Пер. с англ. /Э. Сэйдж, Дж. Мелса – М.: Наука, 1974. – 248 с.

41. Эйкхофф П. Основы идентификации систем управления. Пер. с англ. – М.: Мир, 1975. – 683 с.

42. Стратонович Р.Л. Существует ли теория синтеза оптимальных адаптивных, самообучающихся и самонастраивающихся систем? // – Автоматика и телемеханика, 1968, № 1, 96–107.

43. Теория обнаружения сигналов / П.С. Акимов, П.А. Бакут, В.А. Богданович и др.; Под ред. П.А. Бакута. – М.: Радио и связь, 1984. – 440 с.

44. Abramovitz M., Stegun I.A.(Eds.) Handbook of Mathematical Functions. / National Bureau of Standards, 1972. – 1046 p.

45. Anderson T. W. The Statistical Analysis of Time Series / Hoboken: Wiley, 2011. – 704 p.

46. George A. Baker G.A. Pade Approximants / George A. Baker, Peter Graves-Morris. - Cambridge University Press, 2009. - 764 p.

47. Ye Ouyang, Hosein Fallah M. A Performance Analysis for UMTS Packet Switched Network Based on Multivariate KPIs // International Journal of Next Generation Network (IJNGN), Vol. 2, No. 1, March 2010, pp. 79 - 92.

48. Kreher R. UMTS Performance Measurement: A Practical Guide to KPIs for the UTRAN Environment. – John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, 2006. – 227 PP.

49. Bonaventure O. Computer Networking : Principles, Protocols and Practice. - Release Sep 07, 2018. - 272 p.

50. Dordal P.L. An Introduction to Computer Networks. - Release Mar 31, 2019. - 872 p.

51. Tanenbaum, A.S. Computer Networks, 5th Ed. / Andrew S. Tanenbaum, David J. Wetherall. – Prentice Hall, Cloth, 2011. – 960 pp.

52. Erramilli A., Narayan O., Willinger W.. Experimental Queuing Analysis with Long-Range Dependent Packet Traffic / IEEE/ACM Transactions on Networking, April 1996. – p. 38 – 56.

53. Fillatre L., Nikiforov I., Vaton S., Casas P. Sequential Non-Bayesian Network Traffic Flows Anomaly Detection and Isolation // [Електронний ресурс] Режим доступу:
http://iie.fing.edu.uy/investigacion/grupos/artes/publicaciones/casas_iwap2008_Fillatre

Final.pdf

54. Stallings W. High-Speed Networks and Internets: Performance and Quality of Service / 2nd Ed. - Pearson Education, 2002. - 744 pp.

55. Виноградов Н.А. Анализ потенциальных характеристик устройств коммутации и управления сетями новых поколений // Зв'язок. – 2004. – №4. – С. 10 – 17.

56. Виноградов Н.А., Дрововозов В.И., Лесная Н.Н., Зембицкая А.С. Анализ нагрузки на сети передачи данных в системах критичного применения // Зв'язок. – 2006. – №1. – С. 9-12.

57. Tsybakov B.S., Georganas N.D. Self-similar processes in communications networks // IEEE Trans. Inform. Theory, vol. 44. . Sep.1998. p. 1713 – 1725.

58. Forbes C. Statistical Distributions, 4th Ed. / C. Forbes, M..Evans, N. Hastings, B. Peacock – John Wiley & Sons, Inc., Hoboken, New Jersey, USA, 2010. – 230 pp.

59. Чинаев П.И. Самонастраивающиеся системы. – М.: Машгиз, 1963. – 303 с.

60. Справочник по устройствам цифровой обработки информации / Н.А. Виноградов, В.Н. Яковлев, В.В. Воскресенский и др.: Под ред. В.Н. Яковлева. – К.: Техника, 1988. - 415 с.

61. Бендат Дж. Применения корреляционного и спектрального анализа; пер. с англ./ Дж.Бендат, А.Пирсол // – М.: Мир, 1983. – 312 с.

62. Мирский Г.Я. Характеристики стохастической взаимосвязи и их измерения. – М.: Энергоиздат, 1982. – 320 с.

63. Виноградов Н.А. Исследование характеристик полезной пропускной способности в условиях меняющейся нагрузки // Н.А. Виноградов, Н.Н.Лесная, А.С. Савченко. – Проблеми інформатизації та управління: Зб. наук. пр. – К.: НАУ, 2009. – Вип. 4(28). – С. 28 – 31.

64. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. – М.: Лори, 2002. – 363 с.

65. Lehmann E.L. Testing Statistical hypotheses, 3rd ed. // E. L. Lehmann, J. P.

Romano. - Springer Science+Business Media, LLC, 2005. - 795 p.

66. Afifi A. Statistical Analysis, Second Edition: A Computer Oriented Approach 2nd Edition / A. A. Afifi, S. P. Azen. - Academic Press; 2 edition, 1979. - 442 pp.

67. Фаддеев, Д. К. Вычислительные методы линейной алгебры [Текст] / Д. К. Фаддеев, В. Н. Фаддеева. – Москва : Физматгиз, 1963. – 656 с.

68. Фельдбаум А. А. Основы теории оптимальных автоматических систем. – М.: Наука, 1966. – 624 с.

69. Фельдбаум А. А. Теоретические основы связи и управления. / А.А.Фельдбаум, А. Д. Дудыкин, А. П. Мановцев, Н. Н. Миролюбов. – М.: Физматгиз, 1963. – 932 с.

70. Цыпкин Я.З. Основы теории обучающихся систем. - М.: Наука, 1970. - 252 с.

71. Лазуткін Б.А. Радіотехнічні пристрої з компенсацією завад. – К.: Техніка, 1972. – 116 с.

72. Швець І. П. Визначення числа джерел випромінювання в завданні компенсації завад у безпроводовій локальній мережі / І. П. Швець // Телекомунікаційні та інформаційні технології. - 2017. - № 3. - С. 124-129. - Режим доступу: http://nbuv.gov.ua/UJRN/vduikt_2017_3_18

73. Швець І.П. Компенсаційні методи захисту від завад у безпроводовій локальній мережі // Телекомунікаційні та інформаційні технології. 2017. №4(57). с. 94 – 102.