Форма № Н-9.02

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)
Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))
Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (предметної, циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістра
(ступінь вищої освіти)

на тему «**Забезпечення оптимального функціонування бортових обчислювальних комплексів рухомих об'єктів в умовах навмисних зовнішніх впливів**»

Виконав: студент 2 курсу, групи 601 ТТ
спеціальності 172 «Електронні комунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності

Зоць Я. О.
(прізвище та ініціали)
Керівник Косенко В. В.
(прізвище та ініціали)
Рецензент Ломіга О.І.
(прізвище та ініціали)

Полтава – 2025 рік

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
Інститут Навчально-науковий інститут інформаційних технологій і робототехніки
Кафедра Автоматики, електроніки та телекомунікацій
Освітній рівень магістр
Спеціальність 172 «Електронні комунікації та радіотехніка»

ЗАТВЕРДЖУЮ
завідувач кафедри автоматики, електроніки та телекомунікацій
_____ д.т.н., проф. О.В. Шефер
"02" 09 2024 р.

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Зоцю Ярославу Олександровичу

1. Тема проекту (роботи) **«Забезпечення оптимального функціонування бортових обчислювальних комплексів рухомих об'єктів в умовах навмисних зовнішніх впливів»**
керівник проекту (роботи) Косенко Віктор Васильович, д.т.н., професор
затверджена наказом вищого навчального закладу від 09.08.2024 року № 818-ф,а
2. Строк подання студентом проекту (роботи) 19.12.2024 р.
3. Вихідні дані до проекту (роботи). Вихідними даними є матеріали зібрані під час проходження переддипломної практики.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Вступ. Оцінка функціонування бортових комплексів в умовах впливу електромагнітних випромінювань. Аналіз впливу зверхкороткого ЕМВ на елементи та вузли БЦОК. Аналітичний огляд методів та засобів забезпечення стійкості БЦОК. Аналіз нейромережевих методів виявлення деструктивних ЕМВ. Еволюційно-генетичний підход виявлення ЕМВ. Нейромережеві експертні системи для виявлення деструктивних ЕМВ. Нейро-нечіткі методи для виявлення деструктивних ЕМВ. Формування критеріїв оцінки вразливості БЦОК від впливу деструктивних ЕМВ. Розроблення сценаріїв роботи системи виявлення деструктивних ЕМВ на БЦОК. Розроблення процедури інтелектуальної оптимізації сервісу маршрутизації даних. Висновки.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів): Актуальність теми, об'єкт та предмет дослідження, мета роботи. Графічні залежності електромагнітного випромінювання. Залежності втрати інформаційних пакетів від деструктивних впливів. Функціональна схема інтелектуальної системи оцінки стійкості. Функціональна схема системи виявлення деструктивних впливів. Нейромережевий алгоритм та алгоритм Кохонена. Принципи нейромережі зустрічного розповсюдження. Алгоритм експертної оцінки та нейромережева експертна система. Нейро-нечітка мережа. Частотні залежності втрати інформаційних пакетів. Процедура перерозподілу трафіку. Оптимізаційна структура трафіку на основі інтелектуального сервісу маршрутизації. Алгоритм динамічної маршрутизації інформації.

7. Дата видачі завдання 02.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор №	Назва етапів магістерської роботи	Термін та обсяг виконання етапів роботи			Примітка (плакати)
1	Вступ. Оцінка функціонування бортових цифрових обчислювальних комплексів в умовах впливу електромагнітних випромінювань.	07.10.24		15%	Пл. 1
2	Аналіз особливостей впливу зверхкороткого ЕМВ на елементи та вузли БЦОК. Аналіз нейромережевих методів виявлення деструктивних ЕМВ.	16.10.24	I	25%	Пл. 2, 3
3	Інтелекятуальний аналіз даних у завданнях оцінки стійкості БЦОК. Еволюційно-генетичний підход виявлення деструктивних ЕМВ.	05.11.24		40%	Пл.4, 5
4	Нейромережеві експертні системи для виявлення деструктивних ЕМВ. Нейро-нечіткі методи для виявлення деструктивних ЕМВ.	12.11.24		50%	Пл.6
5	Розроблення критеріїв оцінки вразливості БЦОК від впливу деструктивних ЕМВ	19.11.24	II	60%	Пл.7
6	Розроблення сценаріїв роботи системи виявлення деструктивних ЕМВ на БЦОК	26.11.24		70 %	Пл. 8,9
7	Розроблення процедури інтелектуальної оптимізації сервісу маршрутизації даних	11.12.24		90 %	Пл. 10
8	Висновки. Формування додатків. Оформлення кваліфікаційної роботи та підготовка графічних матеріалів.	19.12.24	III	100%	Пл. 11, 12

Студент _____ Зоць Я. С.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Косенко В.В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ВСТУП

Останнім часом необхідність забезпечення захищеності елементів та вузлів інфокомунікаційних систем від потужних електромагнітних випромінювань (ЕМВ) стає обов'язковою умовою під час проектування багатьох об'єктів. Таку вимогу диктують новітні досягнення в галузі генерації надпотужних широкосмугових електромагнітних полів, а також наявні у багатьох складних технічних системах значні за довжиною розподілені кабельні мережі.

Мета кваліфікаційної роботи. Забезпечення стійкості функціонування бортових цифрових обчислювальних комплексів (БЦОК) в умовах впливу електромагнітних випромінювань, на основі розрахункових моделей оцінки впливу полів ЕМВ на елементи та вузли БЦОК.

Це дозволить проводити інтелектуальний аналіз параметрів спотворень інформаційного потоку в системі для запобігання деструктивному впливу ЕМВ, включаючи мінімізацію витрат часу на відновлення комплексу після збоїв.

Об'єктом дослідження є процес функціонування бортових цифрових обчислювальних комплексів на рухомих об'єктах.

Предметом дослідження є моделі аналізу та оцінки стійкості функціонування бортових цифрових обчислювальних комплексів.

Під впливом розвитку елементної бази мікроелектроніки всі процеси в інформаційних системах зміщуються у бік збільшення швидкодії. Причому підвищення швидкодії інфокомунікаційних систем сьогодні відбувається з часом перемикання - наносекунди, що дозволяє суттєво збільшувати обсяг інформації, яка обробляється в одиницю часу. Особливо високі вимоги до швидкодії висуваються до систем у реальному масштабі часу. У таких системах значення оцінки вартість/швидка з підвищенням швидкодії при постійної вартості завжди знижується.

При цьому необхідно мати на увазі, що компоненти будь-якої складної системи розподілені в просторі і зв'язок між ними фізично здійснюється за допомоги мережевих з'єднань, реалізованих у вигляді кабельних систем (коаксіальний кабель, кручена пара, оптоволокно і т.п.). Все це висуває певні вимоги як до електронного обладнання, так і до інформаційної інфраструктури, яку слід розглядати як єдине ціле, і порушення інформаційної цілісності в одній ланці призведе до порушення роботи всієї системи. До того ж, технологія, що забезпечує високі швидкості обробки інформації, має підвищену чутливість до наведених напруг і струмів, викликаних електромагнітними полями від різних джерел природного та штучного походження, включаючи навмисні силові електромагнітні впливи.

Особливо це стосується сучасних бортових цифрових обчислювальних комплексів, що функціонують в умовах навмисного впливу надкоротких електромагнітних випромінювань, які займають особливе місце в системах керування та контролю рухомими об'єктами, і все більшою мірою оснащуються електронними елементами, чутливими до електромагнітних впливів. У зв'язку з чим сьогодні особливо гостро стоїть завдання захисту бортових цифрових обчислювальних комплексів (БЦОК) від впливу надкороткимпульсного електромагнітного випромінювання.

Це призводить до того, що рівень наведених перешкод від ЕМВ стає майже рівним з інформаційним сигналом і, як наслідок, зростає ймовірність руйнування інформації, що оброблюється. Також встановлено, що зазначені деструктивні впливи призводять до часткового порушення цілісності та повної втрати інформаційного сигналу, що передається, а в деяких випадках до порушення функціонування елементів та вузлів рухомого обєкту. При цьому важливою особливістю даної дії є часто не фізична руйнація елементної бази обчислювальних комплексів та фізичних каналів зв'язку, а спотворення інформації, що обробляється.

Існуючі системи захисту в умовах впливу ЕМВ є, як правило, малоефективними, а в ряді випадків неприйнятними як з технічного, так і з економічного боку, що суттєво підвищує важливість вирішення проблеми пошуку нових методів забезпечення стійкого функціонування бортових систем керування.

Комплекси захисту від потужних електромагнітних впливів відіграють суттєву роль як на полі бою, так і у мирному житті суспільства. Вони використовуються для захисту критичних об'єктів (наприклад, атомних станцій та гідротехнічних споруд), різних підприємств стратегічного значення або важливих міжнародних зустрічей. Також деякі комплекси захисту допомагають цивільній авіації та судноплавству, виступаючи як навігаційне спорядження.

При системному підході до конструювання бортових цифрових обчислювальних комплексів ведеться пошук оптимальних варіантів з урахуванням усіх факторів, що визначають стійких та якість останніх.

До цих факторів належать:

- елементна база (електрорадіоелементи та радіокомпоненти);
- конструкційні матеріали;
- види електричних з'єднань;
- способи досягнення механічної міцності тощо.

При системному підході до конструювання необхідно враховувати обмеження, що накладаються умовами експлуатації, технологічністю схеми та конструкції, надійністю та ін.

1.АНАЛІТИЧНА ЧАСТИНА

1.1 Оцінка функціонування бортових цифрових обчислювальних комплексів в умовах впливу потужних електромагнітних випромінювань

Вирішення проблеми забезпечення стійкості БЦОК до впливу потужних імпульсних електромагнітних полів є складним багатоетапним процесом [1]. Особливістю завдань на розробку БЦОК є наявність одночасно різних за спектром ЕМВ, що вимагає аналізу та оцінки впливу такого випромінювання на окремі елементи та вузли, а зрештою на весь бортовий комплекс, вцілому.

Деструктивний вплив ЕМВ на бортові обчислювальні комплекси може бути обумовлено як безпосереднім впливом імпульсних електромагнітних полів на елементи бортового комплексу, так і наведеними в сполучних лініях та ланцюгах струмами та напругами. Чутливість елементів і вузлів БЦОК до впливу ЕМВ залежить від цілого ряду факторів, зокрема, положення щодо напрямку векторів електричного та магнітного полів, геометричних розмірів електричних ланцюгів та контурів, їх конфігурації, взаємних зв'язків, номіналів електричних навантажень, величин ємнісних та індуктивних зв'язків з елементами конструкцій системи та довкіллям, якості екранування і т.п.

При цьому слід мати на увазі, що навіть для тих елементів та вузлів БЦОК, корпуси яких можуть виконувати роль електромагнітних екранів, електромагнітні імпульси будуть деструктивно впливати через сполучні лінії та роз'єми. ОТже, всі види проводових систем, наявних у бортовому комплексі, відіграють роль колекторів небезпечної енергії ЕМВ. Наведені в провідниках струми та напруги можуть призвести або до електричного пробою (ізоляції кабелю), або пошкодження підключених до провідників пристроїв, якщо в них є чутливі до перенапруг елементи. Наведені імпульси можуть зруйнувати та порушити роботу елементів БЦОК майже одночасно в кількох місцях.

Особливу небезпеку для елементів та вузлів БЦОК, крім наявності можливих протяжних проводових систем представляє також порівняно низька електрична міцність елементів і, навпаки, висока чутливість до електричних перешкод. Одна з можливих областей застосування таких випромінювань є дистанційне ураження електронних компонентів, зокрема цифрових пристроїв. Сьогодні вони складають основну частину елементів, що використовуються. Необхідно враховувати, що на сучасному етапі відзначається різке збільшення долі програмного забезпечення порівняно з апаратними засобами при одночасному збільшення швидкості дії компонентів. Перехідо від систем PDH до систем синхронної оцифрової ієрархії (SDH) із застосування широкосмугових систем B-ISDN і ATM.

Роботи по створенню джерел потужних ЕМВ ведуться в наступних напрямках:

- створення джерел електромагнітного випромінювання з надширокимспектром в діапазоні від 0,1 до 10 ГГц. Ця технологія досягла високого рівня досконалості на базі генераторів з іскровими і напівпровідниковими ключовими елементами [2]. ЕМВ зазначеного типу наводять імпульси великої амплітуди на кабелі живлення, телефонні лінії зв'язку й т.п. Недоліком ЕМВ зі спектром нижче 100 МГц є необхідність створення передавальної антени великої довжини. В іншому випадку ефективність випромінювання ЕМВ різко падає.

- створення вузькосмугових надвисокочастотних ЕМВ, які більш ефективні ніж інші впливи на апаратуру, не тільки шляхом наводок на кабельні лінії, але й через отвори, щілини та екрани в апаратурі.

1.2 Аналіз особливостей впливу зверхкороткого ЕМВ на елементи та вузли БЦОК

Широкополосність і висока частота повторення зверхкоротного ЕМВ роблять цей вид електромагнітного впливу дуже небезпечним.

Особливістю ЕМВ є їх мала тривалість (від десятків – сотень пікосекунд до одиниця наносекунд для перших напівперіодових імпульсів за рівнем 0,5 від амплітуди), подібна до тривалості робочих сигналів електронної апаратури мереж передачі даних телекомунікаційних систем.

Основна спектральна щільність знаходиться у полосі частот від сотень мегагерц до диниць ГГц [2]. Висока шпаруватість забезпечує великі значення імпульсних напруженостей при низьких рівнях середньої потужності (<1Дж) та енергоспоживання джерела. У лабораторних генераторах зверх коротке електромагнітне випромінювання на виході генератора формує відеоімпульси, що періодично повторюються, позитивної чи негативної полярності (рисунок 1.1).

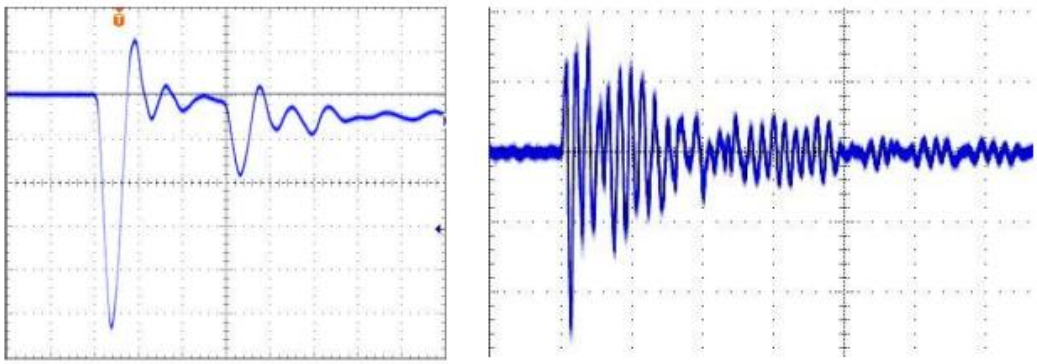


Рисунок 1.1 – Графіки електромагнітного випромінювання:
а) форма імпульса на виході генератора; б) форма імпульса на навантаженні мережевого інтерфейса, за умов ємнісної інжекції

Фізичним середовищем передачі структурно-складних систем, як правило, є вита пара, що являє собою систему з розподіленими параметрами: ємністю та індуктивністю. В результаті перехідних процесів, що відбуваються під час інжекції ЗК ЕМВ (у витій парі категорії 5,) сформований на виході генератора імпульс набуває оформу загасаючої синусоїди у процесі вимірювання на навантаженні мережевого інтерфейсу.

Це пояснюється тим, що кабель являє собою особливий коливальний контур з характерними ємністю і індуктивністю. Внаслідок цього на вхід мережевого інтерфейсу надходить імпульс більшої тривалості, модульований різними частотами. На рис. 1.1 а) показана початкова форма імпульсу на виході генератор, а на рис.1.1 б) форма імпульсної перешкоди на навантаженні мережного інтерфейсу ємнісного способу інжекції.

Аналіз сучасних бортових цифрових обчислювальних комплексів показав, що вони характеризуються такими особливостями:

1. БЦОК мають мінімальні масогабаритні характеристики.

2. Спостерігається неухильна тенденція підвищення показників надійностіої та якості окремих елементових й вузлів БЦОК.

3. БЦОК піддаються широкому аспекту впливу дестабілізуючих факторов.

У загальному випадку БЦОК повинні функціонувати в умовах динамічно змінних впливів на них, в залежності від траєкторії руху або умов зміни навколишнього середовища: магнітних, електромагнітних полів; безперервного імпульсного оіонізуючого випромінювання; широкого спектра механічних і кліматичних впливів.

4. До складу бортових систем входять як цифрові пристрої автоматики, телеметрії, цифрової обробки сигналів і т.п.), так і аналогові й гібридні пристрої (приймально-передавальні пристрої, пристрої навігації, підсилювальні та вимірювальні пристрої і.д.), які працюють у широкому інтервалі частот (від

одиниць Гц до ГГц), напруг (від десятих часток вольт до кіловольт) і струмів (від мА до сотень ампер).

5. У конструкторсько-технологічному плані БЦОК мають широкий спектр реалізацій, які базуються на різних принципах конструювання: моносхемному; функціонально-блочному; функціонально-модульному; функціонально-вузловому. У зв'язку з жорсткими вимогами до масогабаритних характеристик, а також наявністю різних типів пристроїв БЦОК широко застосовуються сучасні досягнення гібридно-інтегральних технологій, котрі, в свою чергу, сприяють прискоренню освоєння технічних досягнень в галузі створення перспективних радіотехнічних засобів.

6. Широкий спектр дестабілізуючих факторів і високі вимоги надійності приводять до необхідності використовувати спеціальні схемні, конструкторські та технологічні рішення, пов'язані з забезпеченням електричних, електромагнітних, теплових, аеродинамічних та інших характеристик БЦОК.

Забезпечення стійкості БЦОК до електромагнітних випромінювань на схемотехнічному рівні здійснюється за рахунок:

- гальванічної розв'язки по ланцюгам живлення та заземлення; усунення наскрізних струмів напівпровідникових прилади;
- введення до силових кіл живлення газових розрядників і спеціальних фільтрів;
- введення для окремих елементів спеціальних схем захисту від перевантажень по магнітному потоку і напрузі й т.д.

7. Реалізація БЦОК з мінімальними масогабаритними характеристиками в сукупності з досягненнями мікроміниатюризації, призводить до тісного взаємозв'язку фізичних процесів (електричних, електромагнітних, аеродинамічних, теплових, механічних, радіаційних і т.д.), що протікають у схемах і конструкціях БЦОК.

8. З точки зору оцінки впливу на елементи і вузли БЦОК, ЕМВ можуть бути розбиті на окремі складові. Це зумовлено наступними причинами:

- обмеженими можливостями існуючих методів оцінки впливу ЕМВ, в цілому;
- відмінністю вимог до БЦОК щодо захищеності від впливу ЕМВ;
- відсутністю випадків гальванічного зв'язку між усіма елементами БЦОК.

9. У загальному випадку факторами, що впливають, на функціональні елементи і вузли БЦОК, під час впливу ЕМВ, є:

- електромагнітні поля, що впливають на елементи та вузли БЦОК;
- електромагнітні поля, що проникають через екрановані поверхні вузлів та підсистем БЦОК;
- ЕМВ, що сполучаються з імпульсними струмами силових кабельних комунікацій і проникають у середину екранованих підсистем БЦОК;
- імпульсні напруги та струми, що наводяться у витій парі, котрі впливають на ізоляцію обладнання, яке має гальванічний зв'язок з силовими кабельними комунікаціями;
- імпульсні напруги та струми, що наводяться в міжстійкових кабелях, котрі проникають через неоднорідності екранів.

Отже, зазначені впливи ЕМВ можуть діяти за такими каналами: електромагнітним полем; по лініях зв'язку; по ланцюгах живлення; по металоконструкціям, тощо.

Імпульсні напруги, що виникають у внутрішніх частинах споживачів, в більшості випадків не являють небезпеки для самих кабельних ліній і електрообладнання, воно можуть представляти небезпеку для технологічних споживачів (випрямляючі пристрої, стабілізатори і т.п.) або знижувати їх перешкодостійкість. З цієї причини ці ефекти повинні бути також кількісно і якісно враховані для кожної конкретної системи.

Внаслідок впливу ЕМВ на елементи БЦОК, останні, можуть мати наступні пошкодження та відмови:

- порушення функціонування окремих підсистем або всієї системи вцілому, в результаті помилкових спрацьовувань імпульсних схемно-вхідних та вихідних калах апаратури;
- вихід з ладу пультів захистів, через пробій ізоляції вхідних або вихідних елементів цих блоків;
- вихід з ладу джерел живлення БЦОК, внаслідок пробою ізоляції трансформаторів у вхідних ланцюгах живлення, що призводить до відмови апаратури автоматики, пов'язаних з цим;
- повна втрата працездатності окремих підсистем БЦОК внаслідок пробою ізоляції та виходу з ладу кабелів [4].

В окремих випадках руйнування внаслідок перевантаження по потоку захисних розрядників, встановлених у вхідних ланцюгах, призводить до порушення роботи БЦОК.

Крім того, під час впливу ЕМВ, сучасним БЦОК, як вказують літературні джерела [4, 5], властиві не тільки фізичні руйнування елементної бази бортового комплексу, а ще і порушення функціональної цілісності інформації, що передається по каналах зв'язку та обробляється бортовими обчислювальними комплексами.

Одна з особливостей поширення імпульсних перешкод, що періодично повторюються, котрі створюються в кабелі (у витій парі) в результаті впливу ЕМВ, полягає в тому, що, незважаючи на симетричність вітих пар, частина перешкод проникає в кола мережевого адаптера через шину взаємодії.

Як відомо, в ідеальній симетричній витій опарі перешкоди, наведені у проводах пари, взаємно знищуються.

Від зверкороткого імпульса ЕМВ при загальній невисокій питомій енергії, має місце висока амплітуда імпульсу перешкоди, внаслідок чого деяка результуюча перешкода залишається і проникає далі [5].

Впливи по ланцюгах електроживлення малоймовірні, що пояснюється складним алгоритмом впливу і необхідністю врахування безлічі факторів роботи активного мережевого обладнання, таких як, наприклад, застосування захисних фільтрів живлення, захисту в блоці живлення активного мережного обладнання, рівня спрацьовування «інтелектуального» захисту обладнання, критичного рівня роботи елементної бази системи [5].

Необхідно зауважити, що впливові надкоротких електромагнітних імпульсів на фізичне середовище Ethernet, яке часто використовується в бортових обчислювальних комплексах, до теперішнього часу практично не приділялося належної уваги.

У зв'язку з цим, у кваліфікаційній роботі магістра цим питання приділено особливу увагу.

Механізм формування помилок при передачі даних заснований на тому, що модель ISO/OSI описує взаємозалежність систем мережі та складається з семі рівнів. Технологія Ethernet працює на перших двох рівнях цієї моделі: фізичному і канальному.

Середовище передачі та параметри сигналу визначаються фізичним рівнем. На канальному рівні неперервно передані послідовності байтів утворюють кадри. Передача самої інформації здійснюється за допомогою кадрів. Складність технології полягає в тому, що існує кілька типових кадрів, які мають різну структуру, тому кадр кожного типу повинен мати певний метод обробки для коректного прийому.

Поширюючись по витій парі, кадр Ethernet може піддатися впливу внутрішніх і зовнішніх факторів, які здатні змінити початковий вид кадру. Помилки Ethernet полягають у пошкодженні кадру або його некоректності,

внаслідок якої кадр не може бути правильно оброблений приймаючою стороною. Всі вони мають різні причини виникнення, викликані несправностями апаратної частини або програмного забезпечення, однак ознакою наявності помилки є пошкодження одного або декількох бітів кадру або невідповідність форми й структури кадру міжнародним стандартам IEEE.

У сучасному комутованому Ethernet колізії зведені до мінімуму, оскільки конкуренція на доступ до середовище відсутня, а максимальна частка помилок сучасних поколінь Ethernet, що опрацюють на швидкості 1 і 10 Гбіт/с, мізерна [5].

Мережі Ethernet, особливо мережі останніх поколінь, побудовані з використанням витої пари в якості фізичного середовища передачі, чутливі до зовнішніх електромагнітниї перешкод, які надають суттєвий вплив на передачу сигналу і призводять до виникнення ряду несправностей проводової системи [6]. Так, під час впливу ЗК ЕМВ на лінію зв'язку по кабелю, розповсюджуються імпульсні перешкоди, що періодично повторюються, які за амплітудою більші або рівні корисному сигналу Ethernet і призводять до спотворення вихідної послідовності символів.

Також варто згадати факт, що існують деякі граничні параметри стійкості функціонування мереж Ethernet, які індивідуальні для кожного виробника мережевого обладнання. Під час впливу ЗК ЕМВ на кабельну лінію бортової мережі та досягнення граничних параметрів, відбувається руйнування мережного з'єднання між кінцевими споживачами.

У зв'язку з цим остаточні значення параметрів, при яких відбувається руйнування мережевого з'єднання, можливо встановити тільки експериментальним шляхом [6].

На сьогодняшній день загальні рекомендації для усунення несправностей в бортових мережах, полягають у тому, що при виявленні помилки необхідно зібрати інформацію щодо несправності і локалізувати її до мінімально

можливого значення. Після цього локалізована частина мережі, що містить помилку, ізолюється, а помилка виправляється.

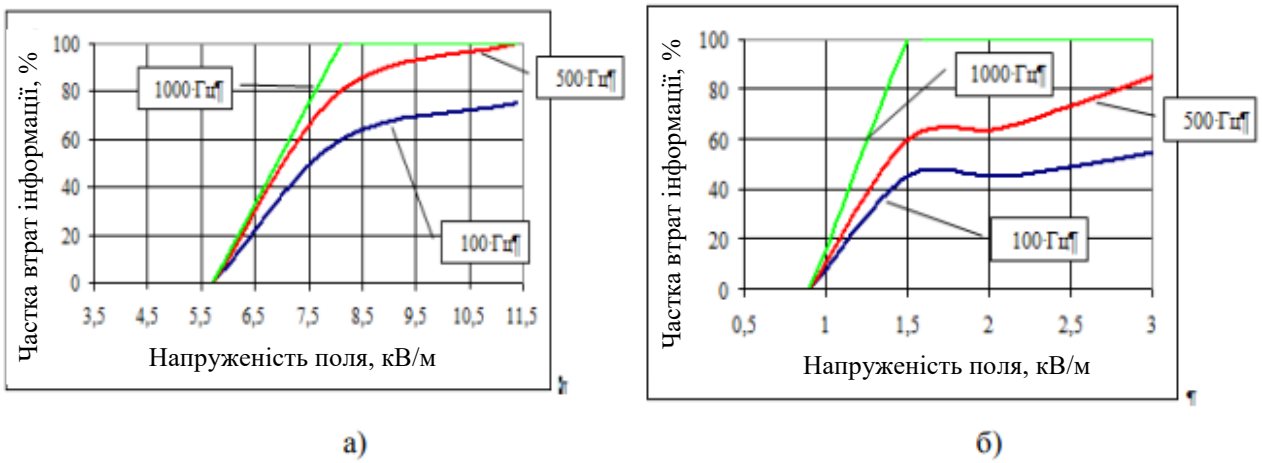
1.3 Аналітичний огляд методів та засобів забезпечення стійкості БЦОК

Серед доступних досліджень [6] можна виділити результати функціонування найпростішої локальної мережі за умов впливу ЗК ЕМВ різної амплітуди й частоти проходження в приміщенні й на відкритому просторі. Проведені дослідження з оцінки впливу частоти прямування імпульсів на фрагмент кабелю (неекранованої витої пари категорії 5е) локальної мережі Ethernet (10Base-Ti 100Base-T).

В якості джерела випромінювання використовувалась 4-рупорна антенна система апертурою 0,5 × 0,5 м, що збуджується генератором імпульсів напруги з максимальною амплітудою 40кВ та тривалістю фронту ~200 пс, без концентратора ~ 800 пс. Між комп'ютерами здійснювалося пересилання пакетів довжиною 64 байт.

На рис 1.2 (а та б) показано залежність частки втрати інформаційних пакетів від напруженості електричного поля під час опромінення інформаційного кабеля [7].

Встановлено, що амплітуда наводок на інформаційний кабель, при яких відбувається 100% втрата інформаційних пакетів (швидкість передачі даних в мережі дорівнює 0), становить від 6 до 15 В, а частота проходження імпульсів становила 100, 500, 1000 кГц.



а) б)

Рисунок 1.2 – Залежності частки втрат інформаційних пакетів від напруженості електричного поля в процесі опромінення інформаційного кабеля: а) без концентратора; б) з концентратором

В даний час для захисту інформаційно-телекомунікаційних систем від деструктивного електромагнітного впливу застосовуються такі методи:

1. Загальне та місцеве екранування телекомунікаційних вузлів та інформаційних ліній зв'язку. Проте, результати аналізу функціонального призначення БЦОК та техніко-економічної експертизи показують, що застосування методу екранування для захисту їх від деструктивного впливу ЗК ЕМВ у ряді випадків є недостатньо ефективним або економічно недоцільним з наступних причин:

- вплив джерельно ЗК ЕМВ характеризується широкою смугою частот і великою амплітудою випромінюваних електромагнітних полів, високою здатністю, що проникає в неоднорідності екранів. Тому для забезпечення ефективного екранування від такого виду впливу повинні виконуватися вимоги до цілісності побудови екранних конструкцій, а також виключатися можливості наявності щілин і неоднорідностей в роз'ємах і з'єднаннях. Реалізація цих умов, зазвичай, пов'язані з значними конструктивними труднощами і матеріальними затратами;

- БЦОК є розподіленою інфокомунікаційною системою, тому в більшості випадків технологічно неможливе виконання умови цілісності побудова екрануючих конструкції, що різко знижує ефективність застосування екранування як методу захисту.

2. Застосування технічних засобів для мінімізації або запобігання впливу електромагнітного випромінювання на БЦОК. Аналіз застосовуваних завадодавних фільтрів і газорозрядних елементів показав, що на даний момент їх застосування не дозволяє ефективно боротися з деструктивним впливом ЗК ЕМВ. Основний параметр сучасних газових розрядників, такий як його час спрацьовування, набагато нижче тривалості впливу надкороткого електромагнітного імпульсу. Частотні характеристики сучасних перешкод фільтрово і трансформаторів не дозволяють ефективно відокремлювати наведені перешкоди ЗК ЕМВ від корисного сигналу в інформаційних лініях. Тому застосування стандартних технічних засобів захисту БЦОК від електромагнітного випромінювання на сьогоднішній день не дозволяє виключити можливість руйнування інформаційних сигналів при впливові ЗК ЕМВ.

3. Застосування перешкодозахищеного кодування передачі інформації. Цей метод дозволяє ефективно боротися лише з невеликою кількістю помилок, що виникають в інформаційних лініях зв'язку внаслідок впливу випадкової, як правило, одиничної перешкоди. Основним недоліком даного методу є необхідність внесення в передану інформацію надмірності, яка залежить від кількості спотворень, що виникають, а в деяких випадках і повторна передача інформації, в т.ч. та спотвореною. Все це в свою чергу знижує пропускну спроможність інформаційних каналів зокрема і швидкодія БЦОК в цілому. Оскільки сучасні джерела ЗК ЕМВ дозволяють генерувати імпульси з частотою до декількох МГц, що створює в інформаційному каналі перешкоди з великою періодичністю. Тому застосування цього методу захисту за умов впливу ЗК

ЕМВ є також малоефективним. Усе це призводить до необхідності розробки спеціальних системних рішень, вибору параметрів сигналів і методів їх обробки, що може виявитися найбільш ефективним методом забезпечення стійкості, т.к. не вимагатиме застосування засобів захисту від перешкод по всіх шляхах їх поширення.

1.4 Висновки за розділом

На основі результатів аналізу стану питання з теоретичних та експериментальних методів дослідження впливу ЗК ЕМВ на БЦОК та методів оцінки стійкості можна зробити такі висновки:

1. БЦОК піддаються широкому спектру впливів електромагнітних дестабілізуючих факторів. У загальному випадку БЦОК функціонує в умовах впливу факторів, що динамічно змінюються, залежно від умов навколишнього середовища: електричних, магнітних, електромагнітних полів; широкого спектру механічних та кліматичних впливів.

2. До складу бортових систем керування входять як цифрові пристрої (пристрої автоматики, телеметрії, цифрової обробки сигналів тощо), так і аналогові та гібридні пристрої (пристрої електроживлення, приймально-передавальні пристрої, пристрої навігації, підсилювальні та вимірювальні пристрої,тощо), які працюють у широкому інтервалі частото (від одиниць Гц до ГГц), напруг (від десятих часток вольт до кіловольт) та струмів (від мА до сотень ампер).

3. Існуючі методи та засоби забезпечення стійкості в основному орієнтовані на вирішення проблеми електромагнітної сумісності, електромагнітних факторів природного та техногенного походження і не торкаються найскладнішого комплексу завдань стійкості БЦОК в умовах впливу ЗК ЕМВ.

2. ДОСЛІДНИЦЬКА ЧАСТИНА

2.1 Інтелектуальний аналіз даних у завданнях оцінки стійкості БЦОК

Під час формалізації задачі дослідження ґрунтуватимемося на наступному поданні інтелектуальної системи аналізу стійкості (ІСАС) бортового цифрового обчислювального комплексу (БЦОК) до деструктивного впливу ЕМВ (рис. 2.1).

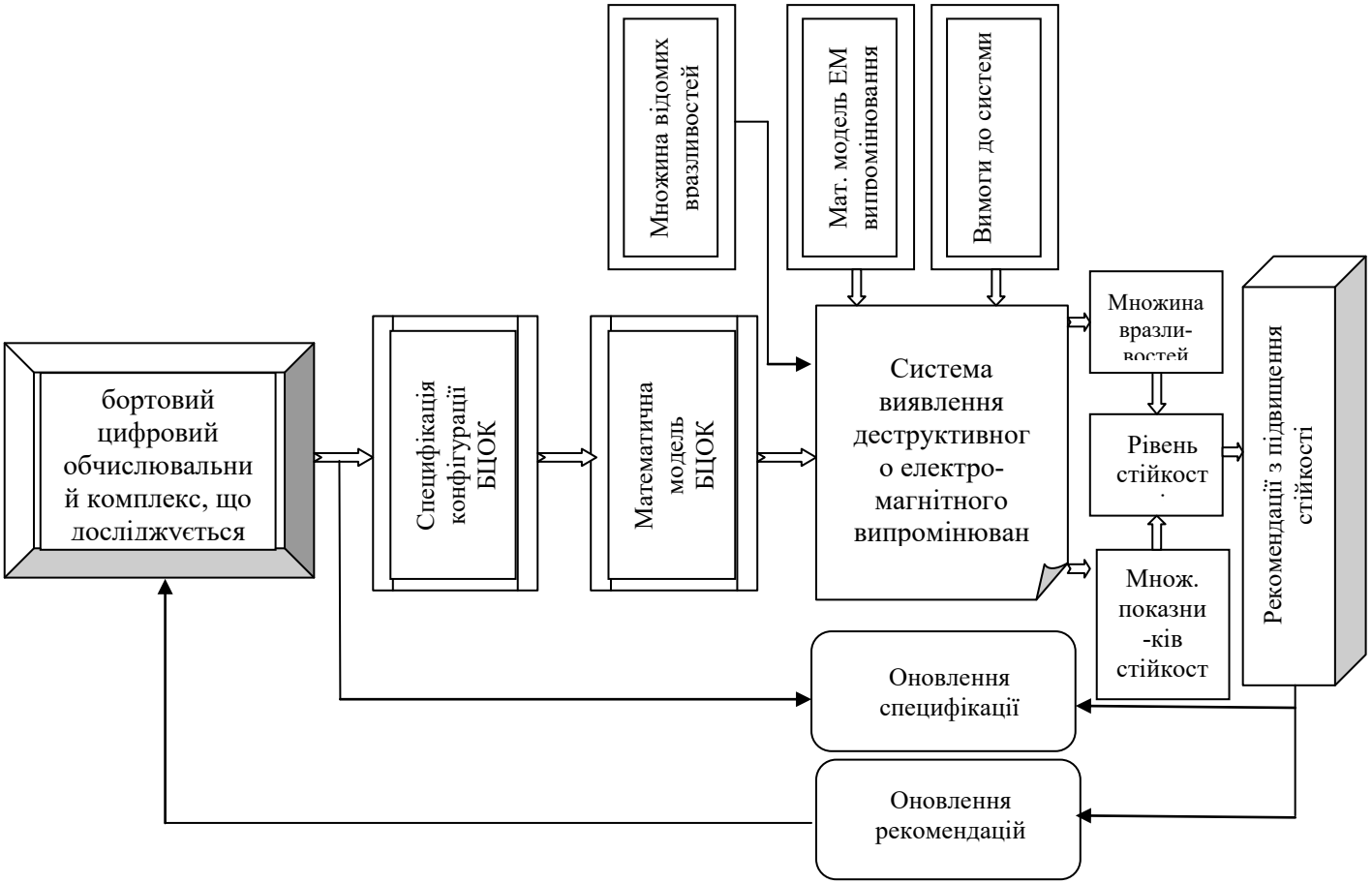


Рисунок 2.1 – Функціональна схема інтелектуальної аналітичної системи оцінки стійкості бортових цифрових обчислювальних комплексів до електромагнітного випромінювання

При цьому ІСАС повинна здійснювати аналіз та оцінку стійкості бортового обчислювального комплексу до деструктивного впливу ЕМВ так само, як було і на етапі проектування, так буде і на етапі експлуатації. Для цього будемо використовувати підхід, який ґрунтується на аналізі моделі БЦОК при побудові якої в якості бази приймемо набір специфікацій, що описують конфігурацію бортової мережі (топологію, склад програмного забезпечення (ПЗ) та апаратних засобів (АЗ)) та апаратні та програмні засоби, що реалізуються в ній і виявлення деструктивних дій. На етапі проектування бортового обчислювального комплексу такі специфікації формуються розробником, на етапі експлуатації за допомогою програмних модулів, що встановлюються на вузлах БЦОК, та формуються в автоматичному режимі [7].

У процесі функціонування ІСАУ має проводити аналіз сценаріїв поведінки бортового комплексу при впливі на його елементи та вузли електромагнітних впливів, з урахуванням моделей ЕМВ на всьому діапазоні частот, здійснювати розрахунок цільових показників, що характеризують стійкість БЦОК в цілому та його окремих підсистем до впливу ЕМВ, на основі топології бортової мережі, використовуваних апаратних засобів та програмного забезпечення, в т.ч. що забезпечують виявлення деструктивних електромагнітних впливів [7].

Стоїть завдання розробки методу аналізу та оцінки стійкості БЦОК до деструктивного впливу ЕМВ на етапах проектування та експлуатації. Реалізація даної методики дозволить як оцінювати рівень стійкості бортового обчислювального комплексу до деструктивному впливу ЕМВ, так і забезпечувати стійкість БЦОК шляхом застосування комплексу методів і засобів, наприклад, шляхом зміни конфігурації бортової мережі.

Одним з перших завдань із реалізації методики аналізу та оцінки стійкості БЦОК до деструктивного впливу ЕМВ на етапах проектування та експлуатації є розробка моделей впливів ЕМВ на елементи та вузли бортового

обчислювального комплексу, формування сценаріїв поведінки БЦОК при електромагнітних впливах на його елементи та вузли та оцінка рівня стійкості БЦОК до деструктивного впливу ЕМВ.

Надамо математичну формалізацію проблеми синтезу ІСАС БЦОК до деструктивного впливу ЕМВ. Для цього введемо такі позначення: G - комплекс заходів, що формуються системою аналізу стійкості та спрямованих на підвищення стійкості бортового комплексу (ObDC) до дії ЕМВ. Тоді ObDCG – конфігурація бортового комплексу з реалізованим у ньому комплексом заходів G, StabilityLevel(ObDCG) – функція, результатом якої є забезпечення стійкості БЦОК ObDC до деструктивних впливів ЕМВ. У цьому випадку цільовою функцією буде забезпечення максимального загального рівня стійкості бортового обчислювального комплексу StabilityLevel (ObDCG) $\rightarrow$ max (в окремому випадку цільову функцію можна задати у вигляді StabilityLevel (ObDCG) $\rightarrow$ ST, де ST – необхіжний критерій стійкості, що висувається до ІСАС:

- до своєчасності: $P_{СВ}$ ($t \le T^{ДОП}$) $\ge P_{СВ}^{ДОП}$, де $P_{СВ}^{ДОП} = 0.99$ та допустимому терміну проведення аналізу $T_{пр}^{ДОП} = T_{пр}^{Н}$, на етапі проектування $T_{пр}^{Н} = 45$ хв. та на етапі експлуатації $ТР^{Н}_{ек} = 25$ мксек - у зв'язку з тим, що з експлуатації автоматично реалізуються всі заходи цього етапу;

- до обґрунтованості: $N_С \ge \max N_С^S$, $N_к \ge \max N_к^S$ и $N_п \ge \max N_п^S$, где $N_С$, $N_к$, $N_п$ – кількість аналізованих сценаріїв поведінки БЦОК під час впливу на його елементи та вузли ЕМВ, кількість виявлених ІСАС вразливостей та кількість врахованих параметрів ІСАС, S - безліч варіантів реалізації ІСАС, $N_С^S$, $N_к^S$, $N_п^S$ – кількість аналізованих сценаріїв впливів ЕМІ на елементи та вузли БЦОК, виявлених уразливостей та врахованих параметрів s-ї реалізацією МСАУ відповідно.

При цьому будемо враховувати наступні параметри ІСАС:

а) архітектура бортового комплексу (у тому числі використані операційні системи, топологія бортової мережі та ін);

б) використані апаратні засоби та програмне забезпечення, що забезпечує виявлення деструктивних електромагнітних впливів (наприклад, мережеві фільтри, екранування окремих елементів та ін.);

в) характеристики ЕМВ (місце впливу, часові, частотні, енергетичні характеристики тощо);

г) системні характеристики (оновлення ЕМВ впливів, сценаріїв ЕМВ впливів, тощо);

- до ресурсоспоживання: $P_{РЕС}(r \leq R_{ДОП}) \geq P_{РЕС}^{ДОП}$, где $P_{РЕС}^{ДОП} = 0.99$, $R_{ДОП} = 0.15$ (15% загального ресурсу, доступного до виконання завдань, покладених на бортовий комплекс) для критичних ресурсів БЦОК.

У такій постановці, задачу аналізу та оцінки стійкості БЦОК до деструктивного впливу ЕМВ на етапах проектування та експлуатації можна декомпозувати на такі основні етапи:

1) Розроблення моделі бортового обчислювального комплексу, достатньою мірою адекватною, що описує аспекти, які впливають на процес аналізу стійкості до впливу ЕМВ.

2) Розроблення моделей впливу ЕМВ на елементи та вузли БЦОК, на яких базуються механізми формування сценаріїв ЕМВ впливів.

3) Розроблення сценаріїв поведінки БЦОК при ЕМВ впливах на його елементи, що відображають можливі варіанти реалізації таких впливів з урахуванням місця впливу, часових, частотних та енергетичних характеристик ЕМВ.

4) Розроблення методу оцінки рівня стійкості БЦОК до деструктивних ЕМВ впливів, що охоплює безліч впливів на елементи і вузли БЦОК.

5) Алгоритмізація основних процедур аналізу та оцінки стійкості БЦОК до деструктивних ЕМВ впливів на етапах проектування та експлуатації.

Методологічну систему аналізу та оцінки стійкості БЦОК до деструктивного впливу ЕМВ на етапах проектування та експлуатації можна представити так:

$$Met_{АО} = МП_{АО} \cup (M_{АС}, M_{М}, M_{ФС}\ M_{ОР}), \quad (2.1)$$

де $МП_{АО}$ – комплекс методів з реалізації основних етапів методу та інтеграції окремих моделей та методів аналізу та оцінки стійкості БЦОК;

$M_{АС}$ – модель аналізованої системи БЦОК,

$M_{М}$ – безліч моделей ЕМВ на елементи та вузли БЦОК,

$M_{ФС}$ – модель формування сценаріїв,

$M_{ОР}$ – модель оцінки рівня стійкості бортового комплексу.

Вихідними даними для реалізації основних етапів методу аналізу та оцінки стійкості БЦОК до деструктивного впливу ЕМВ будуть:

$$(SDC, SPC, EDB, P_{E}, P_{O}, R), \quad (2.2)$$

де SDC - специфікація БЦОК, що аналізується,

SPC - специфікація реалізованої в мережі політики безпеки,

EDB - зовнішня база даних ЕМВ,

P_{E} - множина параметрів, що характеризують ЕМВ,

P_{O} - множина параметрів, що характеризують процес аналізу стійкості,

R - вимоги до рівня стійкості БЦОК.

У процесі функціонування інтелектуальна система аналізу та оцінки стійкості БЦОК повинна реалізовувати комплекс заходів, що дозволяє максимально можливо підвищити стійкість бортового обчислювального комплексу при виконанні обмежень за іншими критеріями, що висуваються до ІСАС. Таким чином, ІСАС повинна дозволяти визначати множину:

$$\{V, SC, C, F, G\} \quad (2.3)$$

За умови $StabilityLevel(ObDC_G) \rightarrow max$ (або $(ObDC)$ $StabilityLevel(ObDC_G) \rightarrow ST$,

де ObDCG – конфігурація бортового комплексу з реалізованим у ньому комплексом заходів G,

V – множина виявлених вразливостей,

SC – сценарії ЕМВ впливів,

C – «вузькі» місця по електромагнітній сумісності бортового комплексу,

F – множина показників стійкості,

G – комплекс заходів щодо забезпечення необхідного рівня стійкості бортового комплексу,

$StabilityLevel(ObDC_G)$ - функція, результатом якої є забезпечення стійкості БЦОК ObDC до деструктивних впливів ЕМВ.

Ядром інтелектуальної системи аналізу та оцінки стійкості БЦОК до деструктивної дії ЕМВ буде система виявлення деструктивних електромагнітних впливів (ЕМВ), на яку покладаються функції інтелектуального аналізу сценаріїв електромагнітних впливів на елементи та вузли БЦОК та оцінки рівня стійкості бортового комплексу.

На виході цього модуля будемо мати множину виявлених вразливостей БЦОК, сценарії поведінки БЦОК під час ЕМВ на його елементи, найбільш критичні компоненти бортової мережі, ймовірність виходу з ладу яких найвища, і комплекс заходів щодо забезпечення стійкості бортового обчислювального комплексу.

Представлений функціонал наповнення системи виявлення деструктивних ЕМВ дозволяє сформулювати основне завдання цього модуля, яке полягає в автоматизації функцій забезпечення стійкості БЦОК.

За аналогією із системами виявлення атак у теорії захисту інформації, *системи виявлення деструктивних електромагнітних випромінювань* (СВДВ) у запропонованій методиці можна дати наступну класифікацію [7]:

а) за способом відповіді:

- пасивні СВДВ - фіксують факт електромагнітного впливу, записують дані у файл журналу, формують попередження та передають їх особі, що приймає рішення або оператору;

- активні СВДВ - фіксують факт електромагнітного впливу, записують дані у файл журналу та виконують функції протидії електромагнітному впливу, наприклад, шляхом мультиплексування трафіку бортової мережі.

б) за режимом роботи: автономні СВДВ – у певні проміжки часу проводять аналіз стану бортових систем (іноді після здійснення ЕМВ) на основі реєстраційних записів в електронних журналах БЦОК; СВДВ реального часу – здійснюють безперервний моніторинг стану всіх систем БЦОК, дозволяючи своєчасно виявляти факт електромагнітного впливу та здійснювати нейтралізацію наслідків ЕМВ.

При цьому рішення щодо нейтралізації наслідків ЕМВ приймаються СВДВ на самому початку впливу ЕМВ, виходячи з мінімальної кількості даних, що іноді знижує достовірність виявлення ЕМВ.

в) способом виявлення ЕМВ: системи виявлення аномального поведінки. Виявлення здійснюється за допомогою сигнатур, що характеризують електромагнітні дії (такі СВДВ дозволяють виявляти ЕМВ від відомих генераторів, але малоефективні для виявлення ЕМВ від нових генераторів).

Характерні реакції елементів і вузлів БЦОК на ЕМВ представляються у шаблоні, відхилення від якого вважаються аномалією. Такий клас СВДВ вимагає безперервного оновлення шаблонів; системи виявлення відмов та несправностей.

Процес аналізу ґрунтується на використанні апарату математичної статистики.

г) за способом збору інформації про електромагнітні впливи:

СВДВ верхнього рівня - визначають факт ЕМВ на основі аналізу даних у бортовій мережі. Такий клас СВДВ реалізують на базі кінцевих пристроїв (наприклад, бортових обчислювачів) або інтегрують у комутаційне обладнання;

СВДВ окремого вузла - визначають факт ЕМВ на основі аналізу інформації з електронних журналів реєстрації подій та різних додатків; СВДВ рівня додатків - визначають факт ЕМВ на основі аналізу наслідків від електромагнітного впливу у конкретному додатку.

З урахуванням проведеної класифікації пропонується наступна узагальнена структура СВДВ, що складається з п'яти основних груп функціональних компонентів (рис. 2.2):

- модулі-датчики, призначені для збору інформації про стан елементів та вузлів бортового комплексу;

- модулі виявлення ЕМВ, які здійснюють обробку даних, зібраних датчиками, та на її основі визначають факт ЕМВ;

- модулі реагування на ЕМВ, на основі своєчасно виявленого модулями виявлення ЕМВ факту електромагнітного впливу, які здійснюють нейтралізацію наслідків ЕМВ;

- базу даних для зберігання інформації, зібраної датчиками, а також про роботу СВДВ;

- модулі керування СВДВ.

У структурі БЦОК всі зазначені модулі СВДВ можуть бути територіально та функціонально розподілені. Первинною інформацією на функціонування СВДВ будуть дані від модулів-датчиками. Зрозуміло, що ефективність роботи СВДВ насамперед залежатиме від того, наскільки оперативно і точно модулі-датчики передали інформацію модулям виявлення ЕМВ.

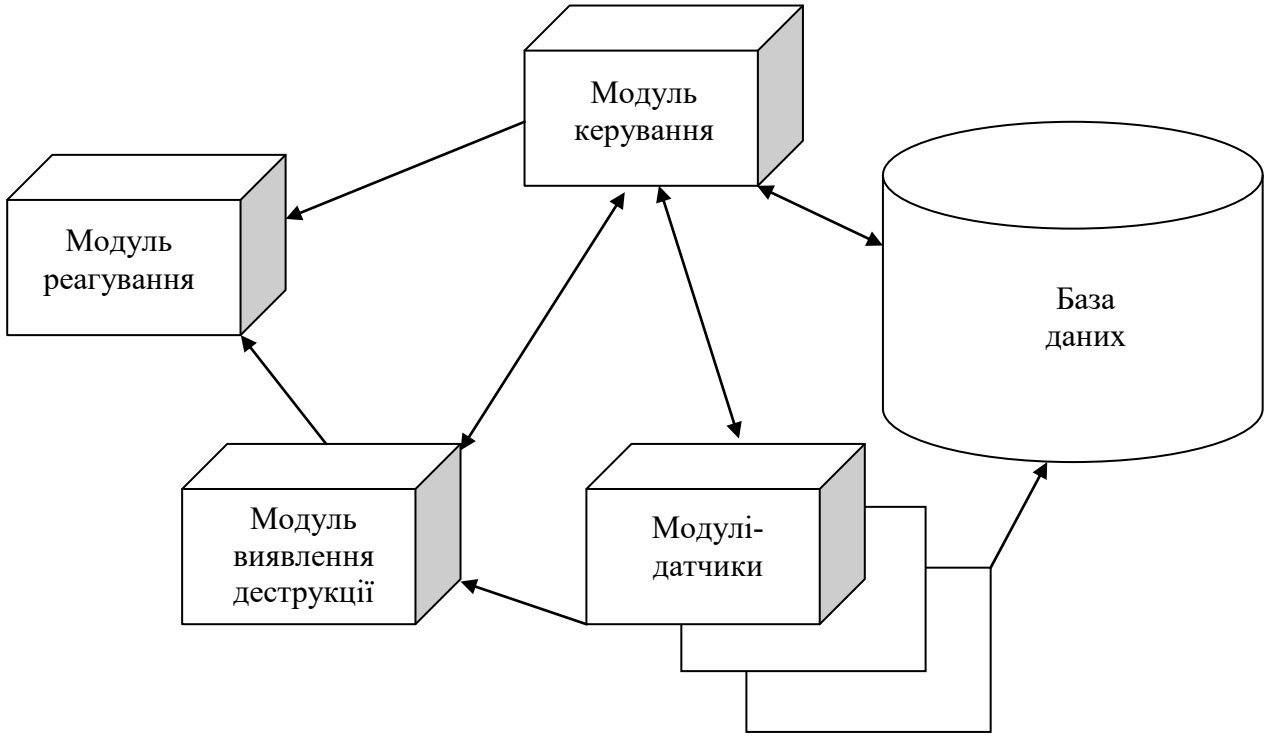


Рисунок 2.2 – Функціональна схема системи виявлення деструктивних електромагнітних випромінювань

Ключовим компонентом системи виявлення деструктивних ЕМВ є модуль виявлення електромагнітних впливів, тому що від нього безпосередньо залежить успішне функціонування всього бортового комплексу.

Аналіз характеристик сучасних методів виявлення електромагнітних впливів показав, що найперспективнішим підходом виявлення деструктивних електромагнітних впливів на БЦОК є вдосконалення методів інтелектуального аналізу даних бортового комплексу.

Традиційно виділяють такі основні завдання інтелектуального аналізу даних:

а) класифікація (виявлення ознак, що характеризують належність об'єкта до тієї чи іншої групи за допомогою аналізу вже категорованих об'єктів та використання певного набору правил);

б) прогнозування (оцінка значень прогнозованих змінних з урахуванням аналізу поведінки часових рядів);

в) кластеризація (віднесення об'єктів до тієї чи іншої групи з можливістю розширення переліку груп);

г) асоціація (виявлення структури зв'язків у безлічі корелюваних подій);

д) послідовність (різновид асоціації, в якій враховуються як порядок появи, так і тимчасові відрізки між подіями);

е) візуалізація даних (зручна для оператора чи ЛПР форма подання інформації, отримана з допомогою методів інтелектуального аналізу даних). Ряд завдань з представленого огляду вирішуються на основі передбачуваних моделей: за навчальною вибіркою із заздалегідь відомими наслідками розробляються моделі, які з великою ймовірністю дозволяють передбачати наслідки для наборів реальних даних. Ряд завдань із представленого огляду вирішуються на основі описових моделей: за виявленими залежностями у відомій вибірці, розробляються моделі для ситуаційних систем та систем прийняття рішень. Візуалізація даних, що є багатопараметричною інформацією, ґрунтується на виявленні багатовимірного простору налаштувань досліджуваних обчислень у просторі малої розмірності (двовимірні та тривимірні, зручні для подання оператору). Всі перераховані вище методи можуть бути інтегровані в рамках єдиної методології для виявлення деструктивних електромагнітних впливів на елементи та вузли БЦОК, не вступаючи в суперечність із традиційними сферами використання експертних систем, нейронних мереж, систем нечіткої логіки тощо [8].

2.2 Нейромережеві методи виявлення деструктивних ЕМВ

За рахунок своєї здатності виявляти вагомі ознаки та приховані закономірності у великих масивах різноманітних даних, консолідувати інформацію, часто ,в багатьох сучасних додатках для інтелектуального аналізу даних використовуються нейронні мережі [8]. Багато з перерахованих вище завдань можуть бути вирішені на основі багатошарових нейронних мереж.

Багатошарові нейронні мережі складаються з вхідного шару, ряду прихованих та вихідних шарів (рис. 2.3).

Вхідний шар (ВхШ) нейронної мережі - це реплікатор вхідного вектора (ВхВ) передачі координат вхідних сигналів (ВхС) всім формальним нейронам (ФН) 1-го прихованого шару.

Ядро нейронної мережі - це порядок зважених міжнейронних зв'язків різних прихованих та ВхШ, що формуються у процесі навчання. Таким чином, нейронна мережа, яка є навченою, здійснює необхідну обробку ВхВ, вектор вихідних сигналів (ВихС) в порядку зважених міжнейронних зв'язків, що утворюють надмірне розподілене інформаційне поле нейронної мережі [8]. Отже, приховані шари разом з вихідним шаром нейронної мережі запам'ятовують в ядрі функціональне перетворення вхідних даних у вихідну інформацію.

Такий процес, як обробка ВхВ та отримання вихідної інформації здійснюється шляхом обробки оперативної інформації у вигляді вхідного та проміжних векторів на основі довготривалої інформації нейронної мережі, що здійснюється в ядрі системи та нейронах послідовно розташованих шарів.

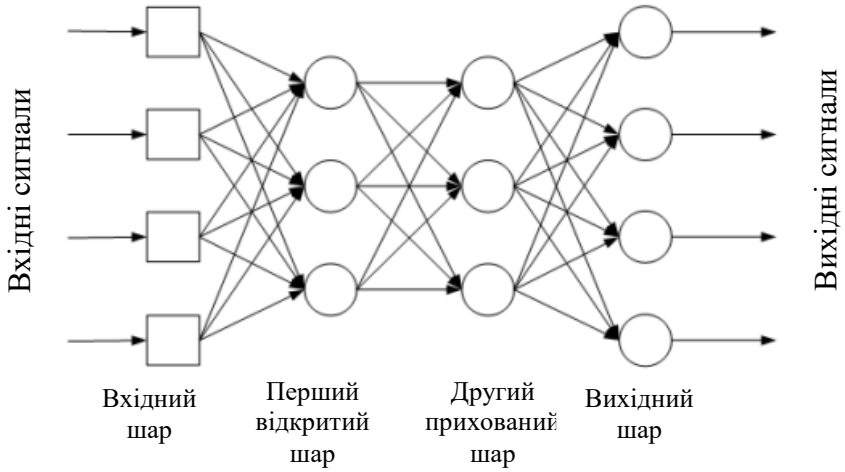


Рисунок 2.3 – Багатошарова нейронна мережа

Як показано в [7], деяку безперервну функцію ВхШ можливо уявити нейронною мережею з одним прихованим шаром і прямими повними зв'язками, для чого достатньо у разі n-вимірного ВхВ 2n+1 формальних нейронів прихованого шару з обмеженими функціями активації. В експериментальних нейронних мережах можуть бути чотири і більше прихованих шарів, що містить до 106 нейронів, отже, забезпечуючи велику надмірність розподіленої інтелектуальної нейронної мемрежі. Але нейронна мережа найчастіше містять один або два приховані шари, що включають 10*103 нейронів [8]. Обмеження за кількістю шарів та формальних нейронів пов'язані зі зростанням за експонентою витрат на обчислення при програмній емуляції нейронної мережі. Адаптація нейронних мереж з експертом та «вміння навчатися» є фундаментальною властивістю нейронної мережі, яка необхідна для створення пристосованих засобів виявлення деструктивних ЕМВ на елементи та вузли БЦОК.

Навчання нейронних мереж розглядається як налаштування різних зважених міжнейронних зв'язків мережі, які утворюють розподілену інтелектуальну платформу нейронної мережі, узгоджуючись із необхідною функціональною залежністю від значень ВхВ нейронної мережі [8]. Налаштування необхідне для визначення вагових коефіцієнтів зважених

зв'язків, топології нейронної мережі тощо. Відомі численні алгоритми адаптації з експертом [8]. Непогані результати отримані при використанні алгоритмів локальної оптимізації у поєднанні з процедурою подолання локальних мінімумів та збільшенням числа формальних нейронів [8].

Можливість самонавчання - необхідний та вкрай важливий атрибут нейронної мережі для аналізу та виявлення прихованих закономірностей у вхідній інформації, властивих більшості завдань інтелектуального виявлення деструктивних ЕМВ на елементи та вузли БЦОК. Самонавчання нейронної мережі не дає можливості отримання готових результатів на вхідні впливи, а полягає в тому, що з внутрішніх закономірностей інформації в нейронній мережі створюються певні умови для розбиття ВхВ за різними категоріями та формування структури класів інформації. У цьому випадку надлишкові дані та приховані закономірності, укладені в інформації, є свого роду експертом з навчання нейронної мережі. Зменшення ступеня надмірності вхідних даних дає можливість визначити головні незалежні ознаки, що дозволяє виявляти приховані в даних закономірності для ідентифікації впливів на елементи та вузли бортового цифрового обчислювального комплексу.

Базовим правилом для нейронних мереж, що самонавчаються, є правило, яке сформулював Хебб [9], що враховує ступінь активності входів і виходу формального нейрона і містить постулат про те, що нейронна мережа має властивість самоорганізації: «Якщо нейрони з обох сторін синапсу активізуються одночасно і регулярно, то сила синапт зростає». Правка синоптичного зв'язку з вагою Wij між виходом і-го нейрона і входом j-го формального нейрона після виконання р-ої ітерації за правилом Хебба може бути описано, наприклад, так:

$$\Delta w_{ij}(p) = \eta_{yj}(p) x_i(p), \qquad (2.4)$$

де η – показник швидкості навчання, $x_i(p)$ й $y_j(p)$ – відповідно значення передсинаптичної та постсинаптичної активності.

При диференційному поданні правила Хебба сильніше навчаються синапси, які з'єднують формальні нейрони з найбільш динамічно збільшеними виходами:

$$\Delta w_{ij}(p) = \eta[x_i(p) - x_i(p-1)][y_j(p) - y_j(p-1)]. \quad (2.5)$$

Однак, необхідно обмежувати зростання вектора терезів формального нейрона, наприклад, за правилом падіння сили синаптичного зв'язку: «Якщо нейрони з обох сторін синапсу активізуються асинхронно, то сила синаптичного зв'язку слабшає». Для зменшення ваги в правило Хебба необхідно ввести такий коефіцієнт, як коефіцієнт «забуття»:

$$\Delta w_{ij}(p) = \eta y_j(p) x_i(p) - \phi y_j(p) w_{ij}(p), \quad (2.6)$$

де ϕ – це коефіцієнт зі значеннями в інтервалі від 0 до 1 (зазвичай 0.01 та 0.1).

Загальний алгоритм навчання з Хеббу тоді можна формалізувати у вигляді послідовності ітерацій, що починається з p = 1:

1. Під час ініціалізації зважених зв'язків інтелектуальної платформи нейронної мережі записують деякі випадкові значення в інтервалі від 0 до 1, а показнику швидкості η та коефіцієнту ϕ варто надати деякі випадкові позитивні значення.

$$y_j(p) = \Sigma x_i(p)\, w_{ij}(p) - w_j, \quad (2.7)$$

де *i* число входів формального нейрона, w_j значення порога активного j-го формального нейрона. 3.

Під час навчання проводимо корекцію вагових міжнейронних зв'язків інтелектуальної платформи нейронної мережі:

$$\Delta w_{ij}(p+1) = w_{ij}(p) + \Delta w_{ij}(p), \quad (2.8)$$

де $\Delta w_{ij}(p)$ обчислюється відповідно до загального правила:

$$\Delta w_{ij}(p) = \phi_{y\,j}(p)[\lambda x_i\,(p) - w_{ij}(p)]. \quad (2.9)$$

4. Для завершення навчання необхідно перевірити досягнення необхідної стійкості результату роботи нейронної мережі. Такою умовою може бути, наприклад, евклідова відстань між ВихВ p-ою та (p-1) ітераціями. Якщо така відстань перевищує необхідне значення, то процедура триває, номери ітерації p збільшується на 1, відбувається повернення на п.2 і повторення етапів алгоритму.

В іншому випадку - нейронна мережа вважається навченою. Через те, що на стадії ініціалізації стан нейронів ВихС навченої нейронної мережі не визначено через випадковий розподіл ваг, то для приведення ВихВ навченої нейронної мережі до формалізованого подання необхідно включити в нейронну мережу ще один ВихС, який може бути визначений за методом зворотного поширення помилки. Інакше кажучи, визначення зважених зв'язків всіх ланок нейронної мережі (крім вихідного) найприйнятнішим буде спосіб самонавчання, а ВихС будемо налаштовувати методом навчання з учителем [8].

У загальному випадку, для візуалізації багатовимірних даних, більшість завдань *інтелектуального аналізу даних* (ІАД) вирішується в інтерактивному режимі за участю експерта предметної області [8], у нашому випадку, експерта з електромагнітної сумісності. Для чого інструментальне середовище ІАД має

забезпечувати експерта інтерфейсом, у тому числі графічним, для візуалізації багатовимірної інформації такого аналізу.

Одним з характерних прикладів можуть служити топографічні карти Кохонена, що самоорганізуються. Принцип дії яких базується на змагальному способі навчання нейронів [6]. При змагальному способі навчання формальні нейрони внутрішнього шару прагнуть бути активованими першими, так як у будь-який момент часу лише один формальний нейрон-прототип може бути активований, надалі такий формальний нейрон будемо називати нейрон-переможець. Застосування окремого виду нейронних мереж, іменованих, самоорганізуються картами Кохонена [10] та дозволяє наочно уявити результати самоорганізації нейронної мережі.

Картки Кохонена, що самоорганізуються, будуються на основі топографічного формування відображення: «Близькі вхідні вектори активують близькі нейрони вихідного шару нейронної мережі». Алгоритм Кохонена забезпечує налаштування зважених зв'язків поточної ітерації на основі даних вагових коефіцієнтів на попередній ітерації.

$$\Delta w_{ij}(p) = \eta[x_i(p) - w_{ij}(p-1)]. \qquad (2.10)$$

Алгоритм Кохонена аналогічний методу навчання за правилом Хебба, за винятком того, що на третьому кроці з шару нейронної мережі виявляють формальний нейрон-переможець зі значеннями синапсів близькими до ВхВ, і лише для нього відбувається підстроювання вагових коефіцієнтів Інші формальні нейрони шару через бічні, загальмовують зв'язки та деактивуються (рис. 2.4).

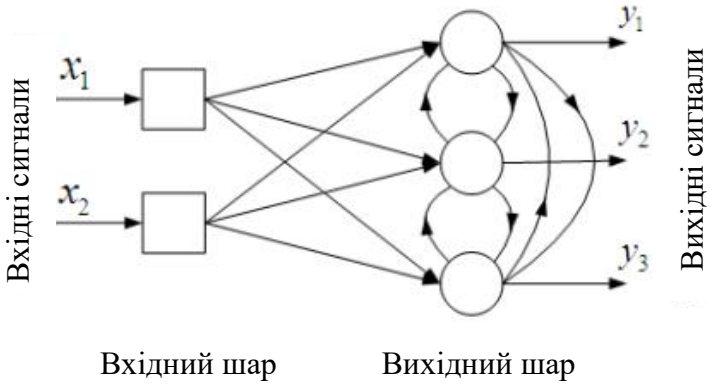


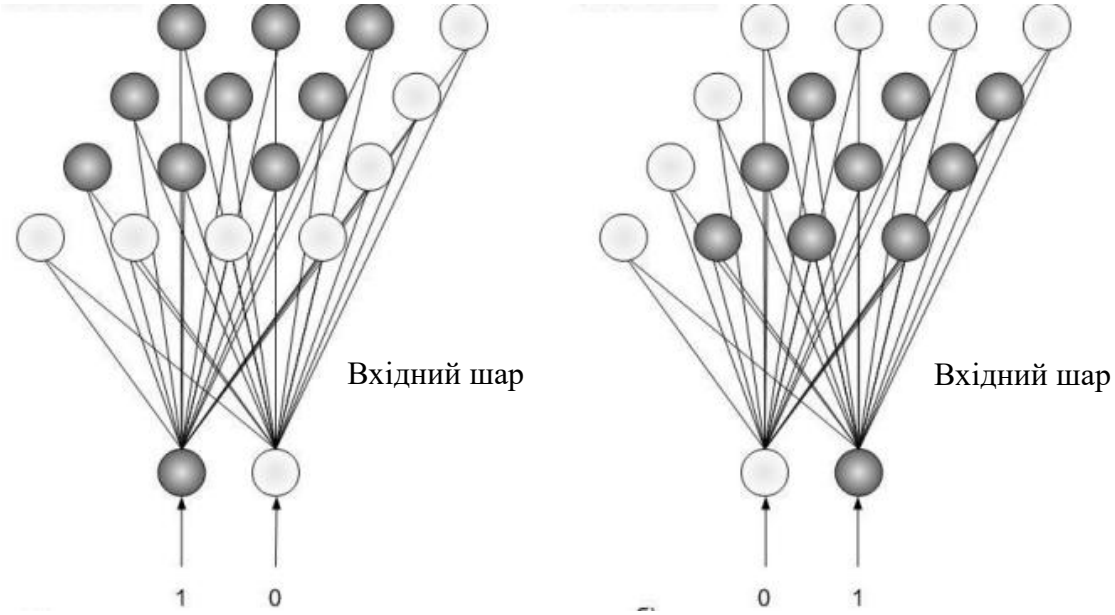
Рисунок 2.4 – Графічна ілюстрація алгоритму Кохонена

Як правило, такий вид нейронних мереж, як карти Кохонена, що самоорганізуються, візуалізується за допомогою двовимірного масиву нейронів, причому так, щоб забезпечувався взаємозв'язок кожного формального нейрона з всіма d вхідними вузлами (на рис. 2.5 d = 2).

На рис. 2.5 формальний нейрон-переможець показаний темно-сірим кольором, а білим – загальмовані на даній ітерації формальні нейрони.

Самоорганізовані карти Кохонена - окремий клас нейронних мереж, який використовує для навчання метод змагання, що визначає просторову околицю для кожного вихідного формального нейрона. При цьому після визначення у шарі формального нейрона-переможця відбувається навчання формальний нейронів - сусідів за просторовим околицями. Початкове наближення такої околиці, як правило, вибирається рівним 1/2 - 2/3 розміру нейронної мережі і зменшується за деяким правилом (наприклад, за законом експоненти).

У процесі навчання коригуються вагові коефіцієнти, пов'язані з нейроном-переможцем та його сусідами. Тому, до кінця навчання отримуємо більш точну картину груп нейронів, що відповідають тому чи іншому класу образів. у задачах інтелектуального виявлення деструктивних ЕМВ на елементи та вузли БЦОК.



а) б)

Рисунок 2.5 – Карти Кохонена, що самоорганізуються

Нейронна мережа зустрічного поширення - це інтеграція карт Кохонена, що самоорганізуються, [9] і зірок Гроссберга (рис. 2.6) [10].

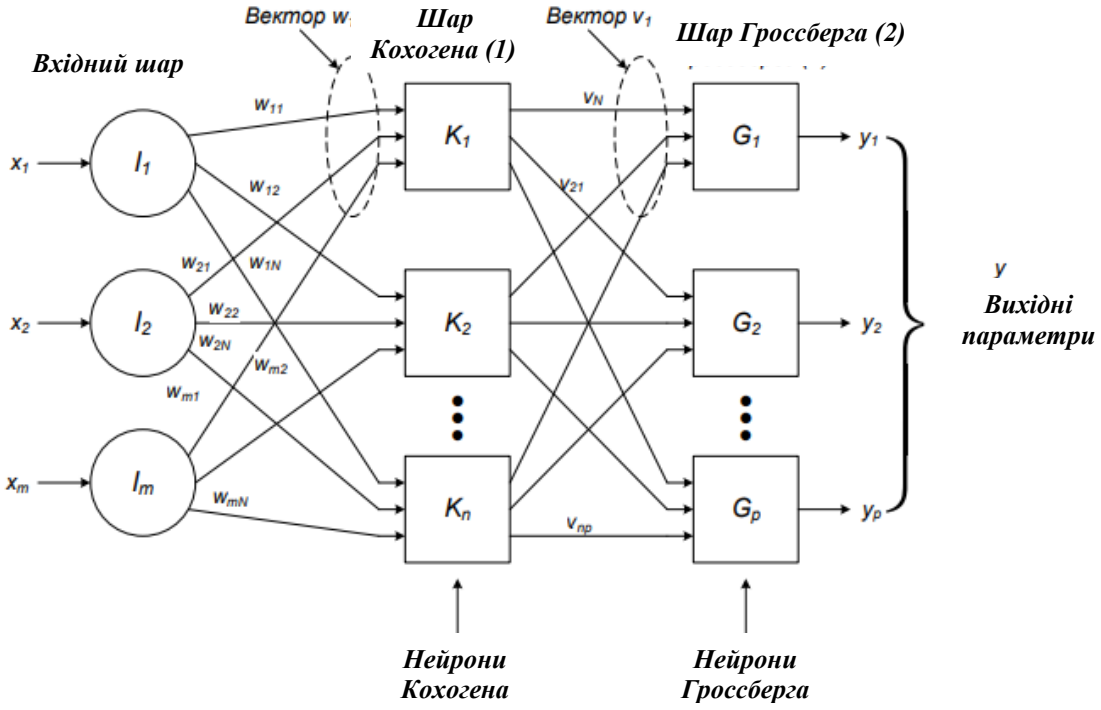


Рисунок 2.6 – Нейронна мережа зустрічного розповсюдження

Нейрони нульового шару є точками розбіжності на гілки. Кожен формальний нейрон нульового шару з'єднаний з кожним формальним нейроном першого шару, шаром Кохонена вагою w_{nm}, які у сукупності утворюють матрицю вагових коефіцієнтів W.

За аналогією, кожен формальний нейрон у шарі Кохонена з'єднаний з кожним формальним нейроном у шарі Гроссберга v_{np}, які також у сукупності дають нам матрицю вагових коефіцієнтів V.

У процесі функціонування такої нейронної мережі по ВхВ (X) розраховується ВихВ (Y). При навчанні вагових коефіцієнтів матриць V і W вони формуються так, щоб якомога точно забезпечити близькість значень розрахункового та еталонного ВихВ. Кожен шар такої нейронної мережі має переваги.

Так, шар Кохонена має властивість самонавчання і дозволяє класифікувати ВхВ. Це досягається за допомогою такого підстроювання ваги шару Кохонена, що близькі ВхВ активують один і той же формальний нейрон-переможець. А шар Гроссберга дозволяє визначати необхідні координати ВихВ. При цьому слід мати на увазі, що шар Гроссберга навчається з учителем.

Так ВхВ шару Кохонена приходить на шар Гроссберга і дозволяє визначити розрахункові значення координат ВихВ шару Гроссберга. Після чого, ваги матриці V змінюються лише тоді, коли вони пов'язані з формальним нейроном шару Кохонена, який має ненульовий вихід. Величина зміни ваги матриці V прямопропорційна відхиленням вагових коефіцієнтів від необхідного виходу нейрона Гроссберга, з яким він пов'язаний:

$$v_{ijx} = v_{ijc} + \beta(y_j - v_{ijc})k_i\,, \qquad (2.11)$$

де k_i – вихід і-го формального нейрона шару Кохонена; y_j - j-а компонента необхідного ВихВ;

β приймає значення 0.1 і знижується при навчанні. Окремо варто сказати і про час навчання нейронної мережі, оскільки цей параметр особливо важливий для оперативності відновлення стану засобів виявлення деструктивних ЕМВ на елементи та вузли БЦОК. Експериментальні дослідження показали, що навчання нейронної мережі зустрічного поширення на порядок (в 10 разів і більше) швидше, ніж навчання нейронної мережі зі зворотним поширенням помилки.

2.3 Еволюційно-генетичний підход виявлення деструктивних ЕМВ

Еволюційно-генетичний підход дозволяє будувати алгоритми оптимальних рішень, з генетичними алгоритмами, на основі моделювання біологічних механізмів популяційної генетики [10].

Пошук оптимального рішення здійснюється шляхом прямого маніпулювання з сукупністю декількох допустимих рішень, що утворюють популяцію, кожне з яких закодовано в двійковому коді. Слід виділити наступні властивості генетичних алгоритмів (ГА):

- незалежність від характера функції, з визначеним екстремумом;
- некритичність кількості компонентів вектора допустимого рішення;
- відсутність необхідності розрахунків похідних відцільової функції;
- на кожній ітерації алгоритму обчислюється кілька допустимих рішень;
- набір допустимих рішень про чергову ітерацію визначається з урахуванням інформації про всі попередні допустимі рішення;
- допускається багатокритеріальність завдання.

Розглянемо докладно основні етапи побудови генетичних алгоритмів і термінологію, що використовується в [10].

Подання допустимих розв'язків екстремальної задачі у вигляді бінарних строчок.

Допустиме рішення x ∈ D екстремальної задачі однокритеріального вибору є n-мірним вектором x = (x1, ..., xn). У разі, коли задача належить класу задач виборного типу, та має безліч допустимих розв'язків, у яких кожна компонента xi, i = 1, n вектора x ∈ D кодується за допомогою цілого невід'ємного числа [8]

$$\beta i \in [0, Ki\,], i = 1,n, \tag{2.12}$$

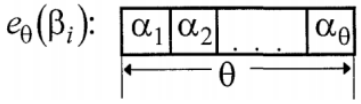
де $(Ki+1)$ – число можливих дискретних значень і-ої керованої змінної області пошуку D. Це дозволяє поставити взаємно однозначну відповідність кожному вектору $x \in D$, причому вектор β с цілочисленними компонентами

$$(x1,..., xn) \leftrightarrow (\beta 1,...,\beta n), \tag{2.13}$$

де для кажної компоненти βi ,$i = 1,n$ областю можливих значень є цілі числа від 0 до Ki. Далі пропонується ввести алфавіт B2, що містить лише два символи 0 та 1: $B2=\{0, 1\}$. Для того, щоб представити цілочислений вектор $\beta = (\beta 1,...,\beta n)$ в алфавіті $B2$ необхідно визначити максимальну кількість двійкових символів θ, котре достатньо для представлення в двійковому коді будь-якого значення βi з області його допустимих значень $[0, Ki]$. Неважко бачити, що параметр символьної моделі θ повинен задовольняти нерівності $K < 2\theta$, де $\max(K) = 1 \le i \le n\ Ki$. Записи довільного цілого невід'ємного числа за допомогою θ двійкових символів визначається співвідношенням:

$$\beta i = (0 \le \beta i < 2\theta),$$

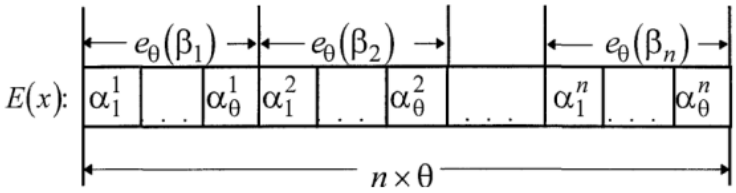
де 2θ – двійкове число, що дорівнює 0 або 1; θ - довжина двійкового слова, що кодує ціле число β*i*. Тоді символьний запис цілого коду βi для фіксованого значення керованої змінної x_i у звичайному двійковому коді запишеться у вигляді наступної бінарної комбінації:



де α_l – двійкові символи (0 або 1), l = 1,θ. Для представлення допустимого рішення $x \in D$ екстремальної задачі в алфавіте $B2$ варто обєднати символьні записи $e\theta$ (β*i*), що описують усі n компонент вектора x, у вигляді лінійної послідовності з бінарних комбінацій:

$$E(x) = (e\theta\ (\beta 1),...,e\theta\ (\beta n\ )).$$

Цьому запису відповідає (n×θ)-бітовий рядок із двійкових символів (0, 1):



Отже, символьна модель екстремальної задачі виборного типу може бути представлена у вигляді безлічі бінарних рядків, які описують кінцеву безліч допустимих розв'язків x, що належать області пошуку D [10]. Вибір символьної моделі вихідної екстремальної задачі багато в чому визначає ефективність і якість застосування генетичних алгоритмів.

Для кожного класу задач виборного типу повинна будуватися власна символьна модель, що відображає специфіку та особливості задачі. Найменшою неподільною одиницею, схильною до дії факторів еволюції, є особина a^t_k (індекс k позначає номер особини, а індекс t - деякий момент часу еволюційного процесу). В якості аналога особини a^t_k в екстремальній задачі

однокритеріального вибору приймається довільне допустиме рішення x ∈ D, якому присвоєно ім'я a^t_k. Дійсно, вектор керованості змінних (x1,...,xn) – це найменша неподільна одиниця, що характеризує внутрішні параметри задачі в кожному t-м кроці пошуку оптимального рішення, які змінюють свої значення в процесі мінімізації критерія оптимальності $Q(x)$.

Якісні ознаки особини a^t_k визначаються з символьної моделі екстремальної задачі як відповідний точці x з ім'ям a^t_k бінарний рядок E(x) і складові бінарної комбінації $e\theta(\beta 1),...,e\theta(\beta n)$.

У даній ситуації слід шукати такі структурні показники, від яких залежать всі суттєві властивості системи і які можна надати в числовому позначенні. В якості таких показників пропонується використовувати співвідношення компонент в системі, що відображають факт зв'язку цих компонентів.

Урахування зв'язків компонентів є природним способом моделювання структури будь-якої системи. Розглянувши всі наявні в системі зв'язку компоненти і побудову схему, ми, тим самим, побудуємо модель структури системи.

Побудовану модель назвемо моделлю зв'язків системи.

Поняття компонент системи (КС) досить загальне, до компонентів системи слід відносити компоненти будь-якої підсистеми - виду забезпечення. Тобто зв'язки КС можуть мати різний характер, що позначає як фізичну пов'язаність компонентів (зв'язок комп'ютерів в мережі), така просто спільну активність компонентів (комп'ютерне програмне забезпечення під час виконання процедури обробки інформації). В бортовій мережі над інформацією здійснюються такі дії:

- введення-виведення інформації;
- захист інформації (реалізація процедур захисту інформації);
- обробка інформації (реалізація процедури обробки інформації);
- зберігання інформації;

- передача інформації між елементами мережі.

Введення і виведення інформації, в принципі, є складовими практично будь-якої процедури обробки інформації, характеру зв'язків компонентів системи, при цьому алгоритм, такий же, як і під час обробки інформації, тому окремо їх можна не розглядати.

Зв'язки реалізації процедур захисту інформації мають ту ж природу, що і зв'язки реалізації процедур обробки інформації. Зв'язки компонентів у інших видів складових одиниць мають різну природу. Відповідно можна виділити наступні види зв'язків компонент в системі:

- зв'язки реалізації процедур обробки інформації, що мають на увазі одночасну або почергову активність компонентів тих чи інших видів забезпечення;

- зв'язки зберігання інформації, мають на увазі пов'язаність комп'ютера (як місця зберігання) з блоком даних або програмним комплексом (як об'єктом охорони);

- зв'язки під час передачі інформації, мають на увазі фізичну пов'язаність між різними комп'ютерами (автоматизованими робочими місцями). Для обліку всіх наявних про систему зв'язків розглядається декомпозиція [10] системи за видами забезпечення процесу обробки і захисту інформації (рис. 2.7).

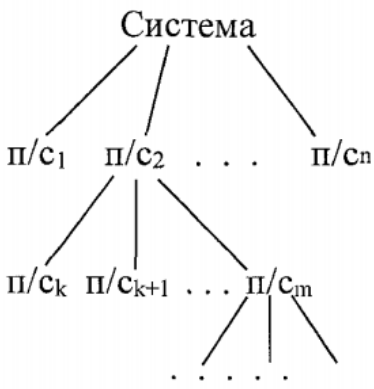


Рисунок 2.7 – Декомпозиція системи

Урахування всіх зв'язків необхідне для отримання повного уявлення про структуру системи.

В результаті декомпозиції виділено підсистеми видів забезпечення, причому компоненти підсистем нижчого рівня здійснюють повне забезпечення процесу обробки та захисту інформації в підсистемі вищого рівня, складовими частинами якої вони є (компоненти підсистем 1,..,n забезпечують процес обробки інформації системи в цілому, компоненти підсистем k,...,m забезпечують обробку інформації в підсистемі 2 і т.д.).

Графік функції f^i, характерний для комбінації двох зв'язаних підсистем представлено на рис. 2.8.

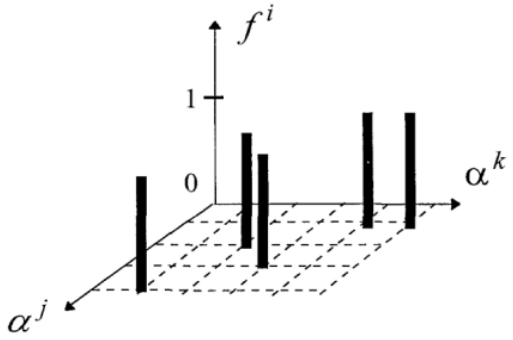


Рисунок 2.8 – Графік функцій зв’язку підсистем

По координатних осях відкладаються номери компонент відповідно j-й та k-й підсистем.

У реалізації процедур обробки та захисту інформації беруть участь компоненти підсистем першого рівня декомпозиції. Отже, необхідно врахувати всі можливі комбінації пов'язаних підсистем цієї групи складових. Якщо в будь-якої підсистеми першого рівня декомпозиції виділені власні складові, то необхідно врахувати всі можливі комбінації і в цій групі.

Зв'язки зберігання інформації характеризуються місцем зберігання та об'єктом зберігання. Зазвичай у системі виділяється одна підсистема технічного забезпечення, компоненти якої можна як місце зберігання інформації. Отже,

загальна кількість комбінацій пов'язаних підсистем дорівнює кількості видів забезпечення першого рівня декомпозиції, компоненти яких потребують певного місця зберігання.

Зв'язки передачі виникають лише у підсистемі, компоненти якої розглядаються як місце зберігання інформації, тобто. у межах підсистеми технічного забезпечення. Кількість комбінацій пов'язаних підсистем дорівнює кількості підсистем технічного забезпечення (зазвичай 1).

Знайти всі набори аргументів функцій зв'язків підсистем, на яких значення цих функцій дорівнює одиниці - означає знайти всі комбінації пов'язаних компонентів, тобто відновити структуру системи.

2.4 Нейромережеві експертні системи для виявлення деструктивних ЕМВ

Варто мати на увазі, що нейромережеві експертні системи істотно відрізняються за способом представлення та обробки інформації. Зорієнтовані на розподілену обробку даних, в ході якої складнено знайти процес вирішення задачі логічно «не прозорий», а накопичені в процесі навчання знання розподілені по всьому інформаційному полю нейромережі, що ускладнює пояснення їх конкретного місця розташування.

Апріорне опитування в експертних системах представляється в «прозорій» для користувача ієрархії правил IF-THEN, наприклад, у вигляді дерева рішень, а процес логічного висновку виходить з послідовним характером людських міркувань. Відомі методи організації ланцюжків міркувань, керованих даними (data-driven) і керованих метою (goal-driven). В обох випадках є передумовипаралелювання обробки висловлювань.

На відміну від експертних систем нейромережеві володіють властивістю адаптивності, причому процес навчання досить простий і оформалізований.

Водночас, завдання отримання знань з експертними системами значною мірою трудомісткий та суперечливий.

Крім того, орієнтована на чіткі достовірні дані ієрархія, як правило експертної системи має елементами осамоорганізації. У той час, як нейромережева сисема виявляє залежності і робить висновки в умовах невизначеності та неповної достовірності даних. Заснована на правилах експертна система (рис. 2.9) складається з бази знань (knowledge base), інформаційної бази (data base), механізму логічного виводу (inference engine), засобів пояснення результатів (explanation facilities) і інтерфейсу користувача (user interface) [8-10].

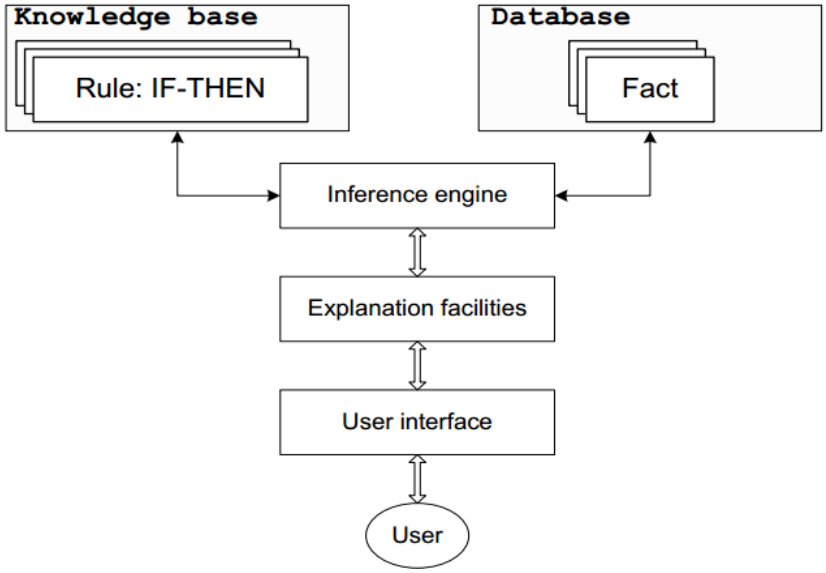


Рисунок 2.9 – Алгоритм експертної оцінки

Знання в експертної системи організовані як системи правил виду: IF (умова) THEN (наслідок). Система логічного висновку здійснює порівняння даних з інформаційної бази з полем бази знань та у разі чіткого збігу активізуються задані полем дії. Результати роботи експертної системи доступні користувачеві через діалоговий інтерфейс, який дозволяє ознайомитися також із

перебігом логічних «міркувань» системи, що спричинили отримання цього результату.

Нейромережна експертна система (рис. 2.10) має багато в чому аналогічну організацію. Проте принципова відмінність у тому, що база знань нейромережевої експертної системи (neural knowledge base) організована як нейронна мережа, знання у якій представлені у вигляді нечіткого адаптивного розподіленого інформаційного поля.

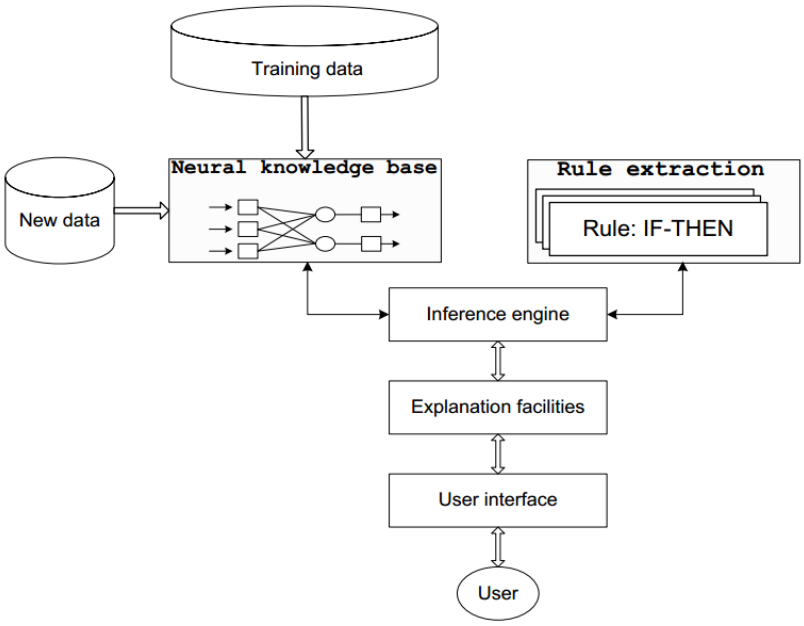


Рисунок 2.10 – Нейромережева експертна система

2.5 Нейро-нечіткі методи для виявлення деструктивних ЕМВ

Об'єднання можливостей нейронних мереж і нечіткої логіки є найбільш перспективним підходом до організації інтелектуальних систем виявлення деструктивних ЕМВ на елементи та вузли БЦОК.

Нейро-нечіткі методи компенсують дві основні «непрозорості» - уявлення знань та пояснень результатів роботи інтелектуальної системи та найкраще

доповнюють нейронні мережі. Нечітка логіка дозволяє формалізувати якісну інформацію, отриману від експертів у даній галузі знань, і повідомити їх у системі нечітких правил, що дозволяють відтрактувати результати обробки системи.

Нейронні мережі дають можливість відобразити алгоритми нечіткого логічного виводу в структурі, вводячи тим самим в інформаційне ополє мережі апріорну інформацію, яка в процесі навчання може коригуватися аналогічно випадку нейромережної експертної системи, розглянутої вище.

У нечітких системах властивість адаптивності дозволяє вирішувати не тільки окремо взяті завдання ідентифікації ЕМВ з наявними в системі шаблонами, але і автоматично формувати нові правила при зміні поля ЕМВ.

Нейро-нечітка система (рис. 2.11), є адаптивним функціональним еквівалентом нечіткої моделі виводу, наприклад, алгоритму Mamdani [11].

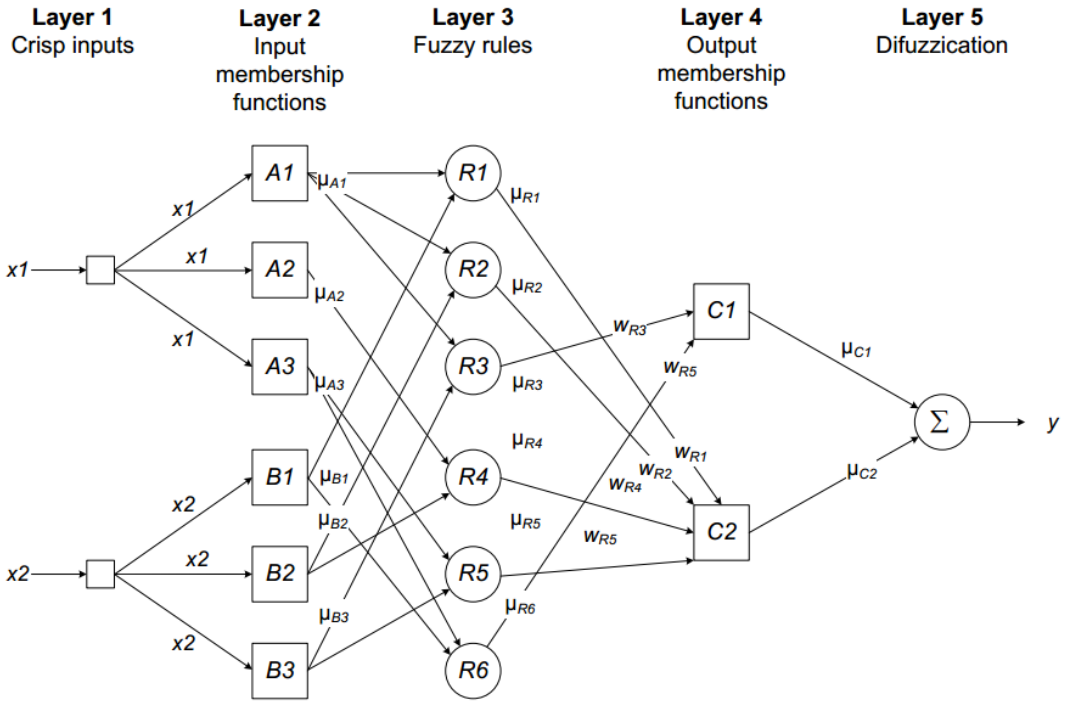


Рисунок 2.11 – Нейро-нечітка мережа

Основні етапи нечіткого логічного висновку за шарами мережі:

а) введення нечіткості (fuzzification) виконується шаром вхідних функцій приналежності A1-A3 B1-B3 (input membership functions), що здійснюють перетворення кожного з чітких вхідних позначень й crisp inputs в ступінь істинності відповідної передумови для кожного виправила

б) нечіткомулогічному висновку відповідає шар нечітких правил R1-R6 (fuzzy rules), який за ступенем істинності передумов формує висновки по кожному з правил відповідні нечіткі підмножини;

в) композиція нечітких підмножин виробляється шаром вихідних функцій приналежності C1, C2 (output membership functions) з метою оформлення нечітких підмножин;

г) об'єднання (aggregation) нечітких подмножин і приведення чіткості (dcfuzzification) виконується виходним шаром і призводить до формуванню вихідного чіткого позначення *y*.

За будь-якої структури нейромережевих експертних систем існує необхідність корекції інформаційного поля нейро-нечіткої системи шляхом передекслуатаційного навчання [11].

Знання експертів з проблемної області або даних експериментальних досліджень, представлені в формі нечітких змінних та нечітких правил, можуть бути прозорим способом відбитих в структурі нейронейро-нечіткої мережі. Наступне навчання дозволяє тільки налаштувати вагові коефіцієнти зв'язків (тобто відкоригувати достовірність окремих нечітких правил), та уникнути суперечливості системи нечітких правил загалом.

У разі відсутності апріорної інформації про подану предметну область, але при достатньому обсязі навчальної вибірки нейро-нечітка мережа автоматично перетворює приховані в даній навчальній виборці закономірності у систему правил нечіткого логічного виводу.

ANFIS - адаптивна нейро-нечітка система орієнтована на отримання знань у вигляді системи нечітких правил навчальної вибірки, характеризується відмінною збіжністю, відома під назвою адаптивна нейро-нечітка система виведення - ANFIS (Adaptive Neuro-Fuzzy Inference System) [11].

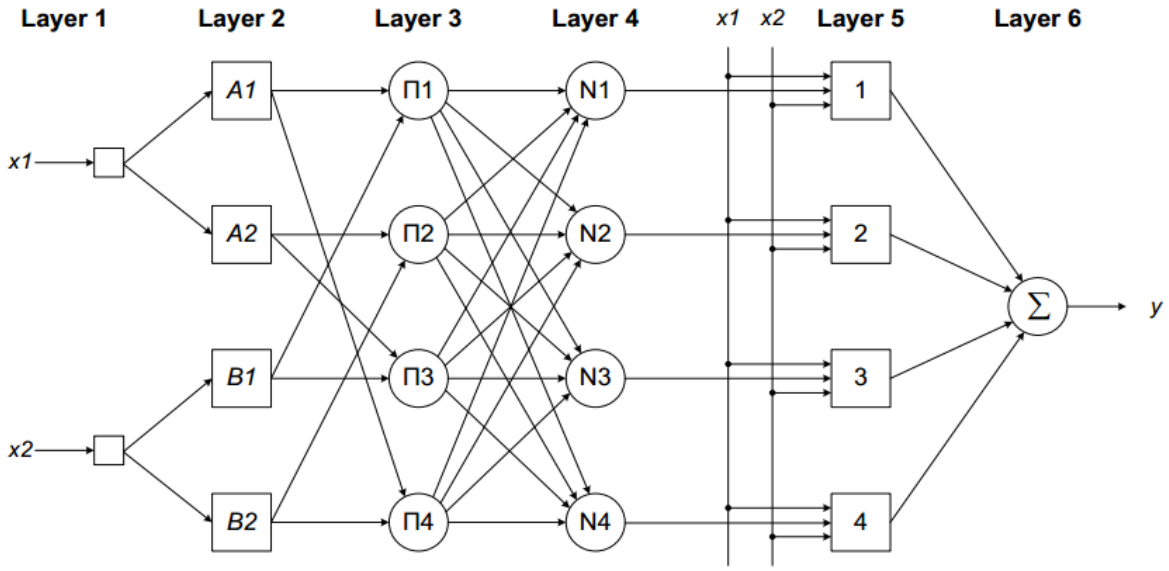


Рисунок 2.12 – Архітектура нейро-нечіткої системи ANFIS (Adaptive Neuro-Fuzzy Inference System)

Введення нечіткості виконується шаром функцій приналежності A1-A1, B1-B2 здійснюють перетворення вхідних значень ох1 і х2 у ступінь істинності відповідної передумови для кожного з 4-х правил. Нечіткомулогічному висновку відповідає шар нечітких правил R1- R4 (відповідні нейрони позначені П1-П4), який за ступенем істинності передумов формує висновки про кожне з правил.

2.6 Висновки за розділом

1. Проведені дослідження існуючих підходів застосування інтелектуальних засобів для вирішення задачі виявлення деструктивних впливів на елементи і вузли БЦОК показали, що найчастіше використовують підхід з адаптивних засобів виявлення деструктивних впливів із використанням нейронних мереж або гібридних систем на їх основі.

2. Показано, що використання нечіткої логіки складових нейромережевих засобів виявлення деструктивних впливів дозволяє враховувати апріорний досвід експертів, реалізувати властиве нейронним мережам нечітке представлення інформації.

3. Проведений аналіз показників для оцінки стійкості БЦОК до деструктивного впливу ЕМВ показав, що відомі оцінки відображають статичний стан комплексу, не враховують дійсну завантаженість вузлів і підсистем БЦОК та можливу динаміку зміни характеру ЕМВ й можливість визначення механізмів захисту.

3. КОНСТРУКТОРСЬКА ЧАСТИНА

3.1 Формування критеріїв оцінки вразливості БЦОК від впливу деструктивних ЕМВ

Під час впливу на БЦОК різного призначення визначались як оборотні ефекти впливу, так і незворотне ураження пристроїв.

Оборотні ефекти впливу виявлялися у тимчасовій відмові пристроїв воду-виводу, систем самодіагностики і т.д.

Необоротні відмови відбувалися при рівні дії від 4 до 10 більших, ніж рівні вразливості. Найбільш уразливими виявлялися зовнішні прояви.

У разі впливу ЕМВ на БЦОК спостерігалися наступні типи ефектів:

- часткова втрата тестових пакетів, зниження пропускної

здатності бортової мережі;

- повна втрата тестових пакетів, блокування обробки бортової мережі під час впливу;

- тимчасове блокування комутаційних пристроїв БЦОК;

– «зависання» БЦОК;

– «зависання» пристроїв введення-виведення інформації БЦОК.

У всіх випадках ефектом впливу була зміна напруги на виході мікросхеми, яке, залежно від параметрів впливу сигналів і типу інтегральної мікросхеми могло призводити до таких наслідків:

1. Зміна логічного стану мікросхеми. Перевищення тривалості збою над тривалістю перешкоди найбільш характерно для впливу над короткохвильових сигналів. Розглянутий ефект характерний для випадку, коли тривалість сигналів перешкоди набагато менше періоду тактових імпульсів мікросхеми.

2. Спотворення часових параметрових імпульсів на виході інтегральних мікросхем.

Ефект спостерігався під час дії на мікросхему довгих радіоімпульсів (наведені сигнали в низькочастотних лініях зв'язку) з несучою частотою в діапазоні 0,3 ... 0,5 ГГц з амплітудою, недостатньою для перемикання інтегральних мікросхем.

У результаті впливу відбувається істотне збільшення часового інтервалу, протягом якого вихід інтегральних мікросхем знаходиться в стані логічної одиниці.

3. Катастрофічна відмова інтегральних мікросхем. Дана відмова спостерігається на досить великих рівнях, або тривалостях впливу. Особливо характерний для впливу на мікросхеми імпульсу з максимумом спектра 0,3 ... 0,5 ГГц. Основними причинами незворотних відмов є тепловий вторинний пробій, викликаний ефектом «засувки» і надвеликими амплітудами сигналів.

На рис. 3.1 наведено залежності показника порушення функціонування логічних елементів від несучої частоти імпульсів (5, 50, 100 МГц). Знання цих залежностей дозволяє врахувати вплив параметрів елементної бази на вразливість до дії ЕМВ на етапі розроблення та експлуатації пристроїв БЦОК.

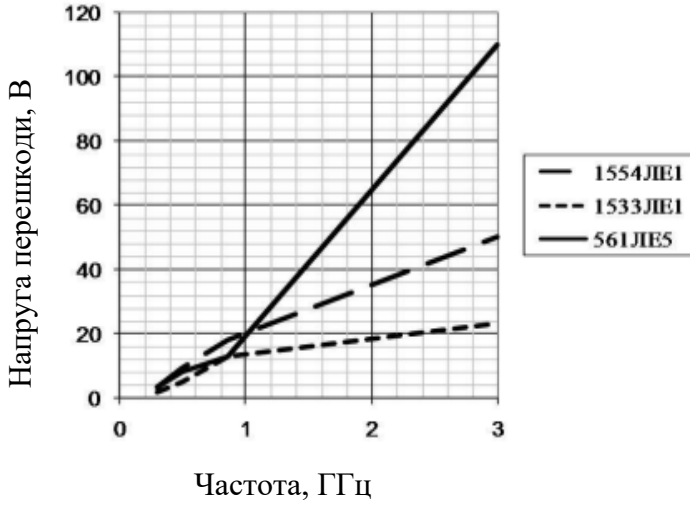


Рисунок 3.1 – Залежності показника порушення функціонування логічних елементів від несучої частоти впливу імпульсів

Основними показниками впливу ЕМВ на елементи і вузли БЦОК, за яких спостерігаються збої, є:

- амплітуда імпульсів поля 10 кВ/м;

- діапазон частот впливу імпульсів;

- тривалість імпульсів.

Необхідно відзначити, що під час впливу ЕМВ на комунікаційне обладнання (комутатор) з напруженостями електричного поля о2,5 кВ/м при тривалості впливу імпульсу 170 пс й 0,7 кВ/м при тривалості впливу імпульсу 790 пс спостерігалось повне блокування обробки БЦОК.

Оцінка залежності впливу ефективності функціонування БЦОК була проведена за критерієм відсотка втрат інформаційних пакетів. Дослідження проводилися для тривалостей ЕМВ 0,2 нс (рис. 3.2) та 0,8 нс (рис. 3.3):

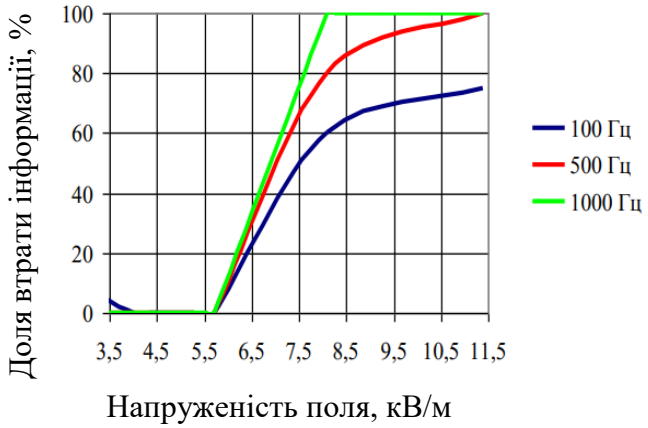


Рисунок 3.2 – Залежність втрати інформаційних пакетів бортової мережі від частоти впливу ЕМВ з тривалістю (0,2 нс)

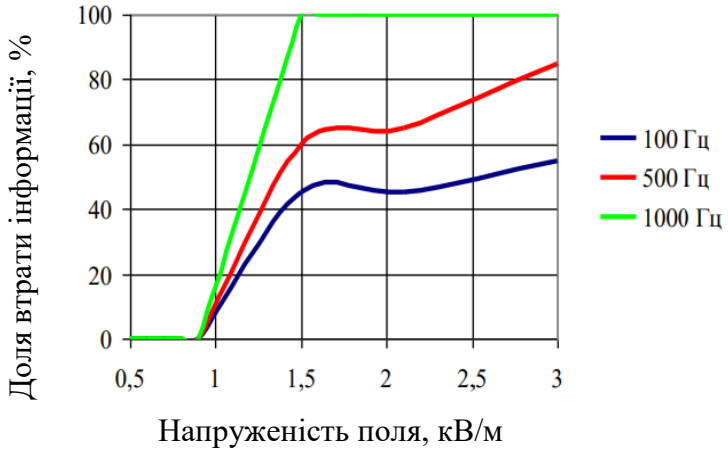


Рисунок 3.3 – Залежність втрати інформаційних пакетів бортової мережі від частоти впливу ЕМВ з тривалістю (0,8 нс)

Представлена на рис. 3.2 та 3.3 залежність імпульсної напруженості електричного поля в спектральному діапазоні забезпечує втрату інформації в бортовій мережі від частоти слідування імпульсів, що впливають.

Проведені дослідження також показали, що застосування екранованих обєктів для розміщення інформаційних пакетів значно знижує ефективність ЕМВ та дозволяє виключити їхвплив на функціонування цифрової апаратури до рівнів впливу не менше 20...25 кВ/м на поверхні з захисним екраном.

Встановлено, що основним і найбільш значущим ефектом при впливові на БЦОК ЕМВ є спотворення переданої по бортової мережі інформації. Причиною спотворення інформації є формування наводок на лініях зв'язку. Дослідження впливу параметрів функціонування БЦОК на її вразливість до дії ЕМВ показали, що найбільш уразливими є швидкодіючі системи, що використовують «довгі», понад 128 кБ, інформаційні пакети. На рис.3.4 показані залежності відсотка втрат інформації для різних розмірів інформаційних пакетів, що передаються.

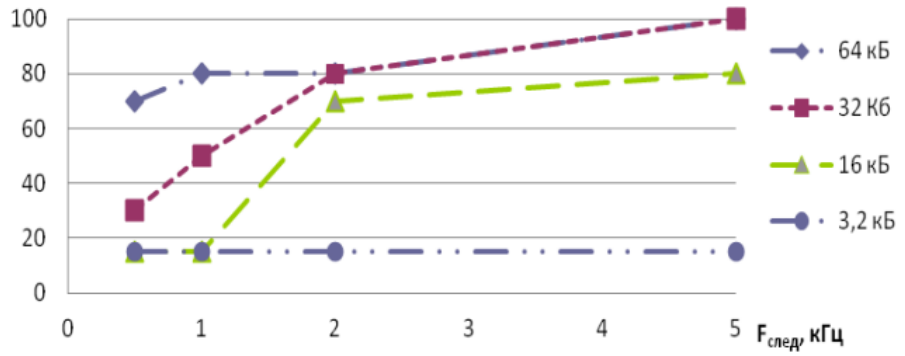


Рисунок 3.4 – Залежність відсотка втрат інформації від частоти слідування імпульсів ЕМВ

3.2 Розроблення сценаріїв роботи системи виявлення деструктивних ЕМВ на БЦОК

Слід зазначити, щовідмінною рисою впливу ЕМВ на сучасне бортове обладнання та його телекомунікаційну інфраструктуру є спотворення, порушення логічної цілісності інформації, що передається за цим лініям зв'язку та інформації, що обробляється обчислювальним комплексом, а не фізична руйнація елементної бази БЦОК каналів зв'язку.

Розглянемо наступні сценарії роботи системи виявлення впливу деструктивних ЕМВ на БЦОК [8]:

1) на основі методу аналізу параметрів спотворень інформаційного потоку в умовах дії ЕМВ;

2) з урахуванням методу аналізу інформації від датчиків виявлення ЕМВ.

Визначення параметрів наводок на зовнішньому детектуючому елементі та проведення аналізу параметрів спотворень інформаційного потоку є основними вихідними даними для функціонування системи виявлення та формування сигналу про початок дії ЕМВ.

Сценарій роботи системи виявлення на основі методу аналізу параметрів спотворень інформаційного потоку за умов впливу ЕМВ.

Наявність можливості своєчасного надходження команд управління зупинення або припинення роботи, комутаторів та інших телекомунікаційних пристроїв сучасних БЦОК в умовах впливу ЕМВ дозволяє мінімізувати кількість відмов та збоїв або зовсім їх виключити, суттєво скоротити часові витрати на відновлення роботи телекомунікаційного обладнання після виникнення збоїв і, як наслідок, підвищити якість функціонування БЦОК в цілому.

Даний підхід значно зменшує можливість подальшого надходження спотвореної інформації в обробку та дозволяє оперативно прийняти рішення щодо вибору режиму роботи БЦОК, який забезпечує зниження часу на відновлення працездатності складових елементів БЦОК після припинення впливу ЕМВ. Сценарій роботи системи виявлення на основі методу аналізу параметрів спотворень інформаційного потоку базується на аналізі інформаційного потоку, що обробляється інфокомунікаційними вузлами БЦОК та виявлення закономірності появи спотворених пакетів інформації. При виявленні факту впливу відомих джерел ЕМВ приймається рішення щодо блокування спотвореної інформації [11].

Основними ознаками впливу джерел ЕМВ на інформаційний потік є періодичність і кратність частоти появи спотворених пакетів частоті формування імпульсів відомими джерелами ЕМВ. З каналу зв'язку на вхід бортового обчислювального комплексу надходить послідовність сигналів, яка певним чином перетворюється і подається на вхід системи виявлення, де здійснюється її аналіз. Якщо вхідні дані внаслідок впливу ЕМВ на канал зв'язку будуть спотворені та не відповідатимуть вимогам за рівнем або формою сигналу, що задаються телекомунікаційним протоколом, то дані на виході БЦОК також не відповідатимуть вимогам телекомунікаційного протоколу. Отже, з'являється можливість визначення наявності впливу ЕМВ на лінію зв'язку, заснованого на проведенні порівняльного аналізу за відповідності

даних, що надходять на шину обміну даними БЦОК, вимогам телекомунікаційного протоколу.

Сценарій роботи системи виявлення на основі методу аналізу інформації від зовнішніх засобів виявлення ЕМВ [11].

Крім розглянутого підходу щодо виявлення впливу на БЦОК деструктивних ЕМВ пропонується використовувати датчики ЕМВ.

Сукупність застосовуваних датчиків повинна бути розгалуженою мережею, елементи якої повинні розміщуватися на лініях зв'язку та обчислювальних вузлах БЦОК. При фіксації факту впливу ЕМВ датчиками, від них у систему виявлення передається формалізований інформаційний сигнал про реєстрацію факту впливу ЕМВ на елементи бортової мережі. При надходженні цього сигналу система виявлення виробляє команди керування, що надходять лініями зв'язку на системну шину обміну даних, комутаторів та інших елементів БЦОК. При цьому команди керування враховують особливості функціонування всіх інфокомунікаційних пристроїв, що входять до складу БЦОК, а також особливості та характер збоїв у їх роботі.

В якості прикладу розглянемо процедуру поділу трафіку, що реалізується одним із режимів БЦОК під час впливу деструктивних ЕМВ [11]. Основною ідеєю режиму поділу трафіку є рознесення передачі по декількох фізичних каналах окремих частин даних, що передаються таким чином, щоб складність руйнування даних була максимально можливою. При подальшому пересиланні частин даних передбачається використовувати проміжні передавачі Fi [1, n] (рис. 3.5).

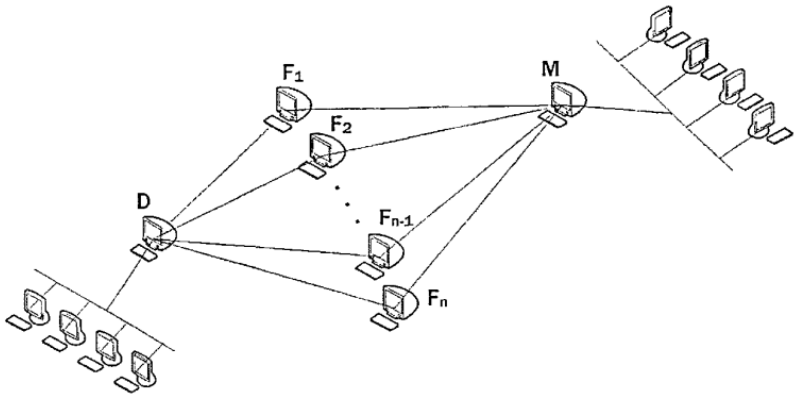


Рисунок 3.5 – Процедура перерозподілу трафіку

В магістерській кваліфікаційній роботі використовується така термінологія:

Демультиплексор (D) – модуль, який відповідає за розподіл вхідних даних на проекції та їх відправлення. Також на демультиплексор можуть бути покладені функції визначення стану бортової мережі на основі станів певних компонентів системи, таких як буфери передачі та певні службові сигнали (підтвердження).

Мультиплексор (M) – модуль, який виконує функції зворотні демультиплексору. Цей модуль збирає проекції (фрагменти даних), передані різними каналами в один потік, утворюючи вихідне повідомлення. Як і демультиплексор, мультиплексор здатний детектувати певні події в бортовій мережі за станом потоків, що входять до нього.

Логічний канал зв'язку між пристроями – логічне з'єднання протоколу передачі.

Фізичний канал – окрема, виділена ділянка передачі даних, отра являє собою деяке фізичне середовище передачі. В одному фізичному каналі може бути утворено безліч логічних каналів.

Зона передачі даних – сукупність логічних компонентів системи, є закінченою, самостійною функціональною одиницею. Зона здійснює рознесення, передачу та збір даних. Кожна зона містить мультиплексор, демультиплексор і щонайменше, пару передавачів.

Гілка передачі – послідовність логічних пристроїв з'єднаних за схемою: демультиплексор – передавач(и) – мультиплексор.

Основне призначення компонентів демультиплексор та мультиплексор - розподіл та збір даних. Також ці компоненти передають та приймають розділені дані.

Найбільш очевидний варіант реалізації системи у бортовій мережі – на сеансовому рівні моделі OSI. З цього випливає що для її коректного функціонування необхідне використання проміжних компонентів – передавачів. Вони виступають як вузлові точки, між якими встановлюються логічні сполуки.

Після обробки даних на рівні додатків стека протоколу передачі пакети передаються мережевому рівню. У заголовку отриманого пакета в полі відправник - стоїть адреса демультиплексора, а в полі одержувач - адреса передавача.

Якби мультиплексор і демультиплексор працювали один з одним безпосередньо, то неможливо було б зробити рознесення каналів, оскільки роздільні логічні потоки передавалися б (маршрутизувалися) по одному фізичного шляху.

Пропоноване рішення передбачає підвищення стійкості інформації при деструктивних електромагнітних впливах на бортову кабельну мережу на основі наявних фізичних засобів. Характерною особливістю процедури є те, що вона є повністю прив'язаною до властивостей середовища передачі та топології бортової мережевої структури, покладаючись на наявність структурної надмірності, яка особливо властива для бортових мереж Ethernet.

3.3 Розроблення процедури інтелектуальної оптимізації сервісу маршрутизації даних

В результаті дослідження проведеного в розділі 2 магістерської роботи, пропонується до використання вдосконалена система «демультиплексор – передавачі – мультиплексор», на основі розробленого інструментарію, який дозволяє передавачам виконувати автоматичну «інтелектуальну» маршрутизацію. Реалізація цього підходу полягає у встановленні на передавачах додатка «сервіс маршрутизації», що коригує роботу протоколів маршрутизації для маркованої інформації [12].

Сервіс маршрутизації (SM) дозволяє підвищити стійкість передачі інформації в бортових мережах в умовах впливу деструктивних ЕМВ.

SM - додаток, що дозволяє передавати дані специфічним маршрутом. Наведемо опис компонентів SM:

$$SM = \{SMS, SMC\}, \tag{3.1}$$

де SMC – керований компонент SM, який встановлюється на кінцевому обладнання та надає функцію для ініціалізації процесу передачі інформації з допомогою сервісу маршрутизації;

SMS – керуючий компонент SM, що встановлюється на БЦОК та виготовляється у захищеному виконанні й здійснює динамічну маршрутизацію інформації, що надходить на БЦОК.

$$SMS = \{Fs, Fsдост, M, f\}, \tag{3.2}$$

де Fs ={Fs1, FS2, ... , FSF} – безліч систем, виконаних у захищеному виконанні бортової мережі. Під системами, виготовленими у захищеному

виконанні, розуміється спеціалізована (або багатофункціональна) бортова цифрова обчислювальна машина (БЦОМ) бортової мережі, яка в результаті застосування спеціальних заходів (наприклад, екранування) не піддається впливу деструктивних ЕМВ.

F = | Fs | – кількість БЦОМ, виконаних у захищеному виконанні, бортової мережі.

Fs дост = { Fs1дост , Fs2дост,… , FsFдост} – безліч, що описує кількість доступних БЦОМ у захищеному виконанні початковий час t_0, а потім через інтервали часу, рівні t. $Fsi^{дост}$ - кількість доступних БЦОМ у захищеному виконанні, для Fsi, i [1, F],

M = {M1, M2, ..., MF) - безліч матриць маршрутизації. Матриця маршрутизації Mi формується на БЦОМ Fsi у початковий момент часу t_0, а потім переформується через інтервали t, i ϵ [1, F], Кожна матриця Mi ϵ Fs містить елементи mkj, що характеризують доступність БЦОМ у захищеному виконанні відносно один одного з Fsi, k ϵ [1, F], j [1, F].

$Fsi^{дост}$ обчислюється за допомогою елементів матриці Mi наступним чином:

$$F_{Si}^{дост} = \sum_{j=1}^{F} m_{ij} \qquad (3.2)$$

де f – параметр, що визначає кількість БЦОМ, що використовуються у захищеному виконанні на всьому маршруті від вихідного вузла до кінцевого протягом одного сеансу (розмір кластера сеансу передачі).

На БЦОМ з множини Fs встановлюється керуючий компонент сервісу – SMS, що виконує автоматичну «інтелектуальну» маршрутизацію трафіку [12].

Показано, що використання SM дозволило уникнути проходження трафіком ділянки, на яку виявлялося деструктивне ЕМВ (рис. 3.6) та таблиця 3.1.

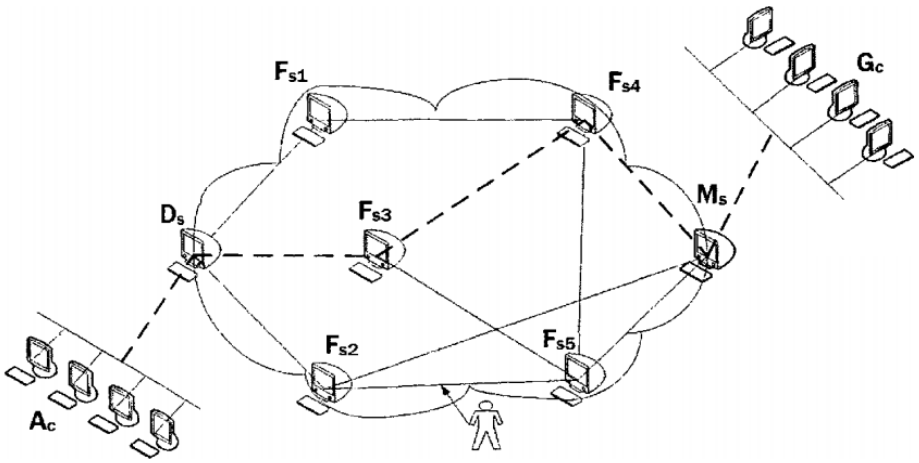


Рисунок 3.6 – Оптимізація маршруту трафіку за рахунок використання інтелектуального сервісу маршрутизації SM

Таблиця 3.1

Інтелектуальна маршрутизація топології SM

	DS	FS1	FS2	FS3	FS4	FS5	MS
DS	0	1	1	1	0	0	0
FS1	1	0	0	0	1	0	0
FS2	1	0	0	0	0	1	1
FS3	1	0	0	0	1	1	0
FS4	0	1	0	1	0	1	1
FS5	0	0	1	1	1	0	1
MS	0	0	1	0	1	1	0

Дана процедура SM (підсумковий маршрут) є імовірним з імовірністю прийняття p_j, $0 < p_j \leq 1$, j [1, k], де k – кількість різних маршрутів від Ds до Ms на графі з вершинами Ds, FS1, FS2, FS3, FS4, Fss, Ms та ребрами, що визначаються поточною топологією мережі.

На відміну від модулів SMC, які запускаються лише у випадках, коли необхідно здійснити передачу даних, модулі SMS працюють постійно.

Крім забезпечення процесу передачі, SMS Fsi через інтервал t обчислює коефіцієнти таблиці маршрутизації Mi Fsi, i [l, n], r [1, n].

Елементи визначаються так: mir= 0, якщо i=r або Fsr недоступна з Fsi (БЦВМ Fsr фізично вийшла з ладу, втрачено зв'язок з Fsr і т.п.); mir= 1, якщо Fsr доступна із Fsi.

В якості входу – тобто об'єктів, що використовуються функціональним блоком для одержання результату, виступають об'єкти: дані, пакети даних і пакети інструкцій, бази даних, таблиці маршрутизації.

В якості виходу – або результатом роботи системи виступають об'єкти:

дані, пакети даних та пакети інструкцій, бази даних БЦОМ у захищеному виконанні, таблиці маршрутизації, графи маршрутів, оцінки реалізації ЕМВ.

В якості управління – інформації, яка використовується у процесі виконання роботи, виступають об'єкти: топологія бортової мережі, протоколи маршрутизації, алгоритм динамічної маршрутизації, алгоритм генерації постуму ЕМВ, контрольовані ділянки, таблиці маршрутизації, бази даних БЦОМ, виконаних у захищеному виконанні.

Механізми – ресурси, які виконують роботу: обладнання, канали зв'язку;

БЦОМ, виготовлені у захищеному виконанні; додаток "сервіс маршрутизації".

Після опису методики в цілому проводиться розбиття її на великі фрагменти. Цей процес називається функціональною декомпозицією, а діаграми, які описують кожен фрагмент та взаємодію фрагментів, називаються діаграмами декомпозиції.

Алгоритм захисту інформації та динамічної маршрутизації трафіку в бортовій мережі від дії деструктивних ЕМВ представлений на рис. 3.7.

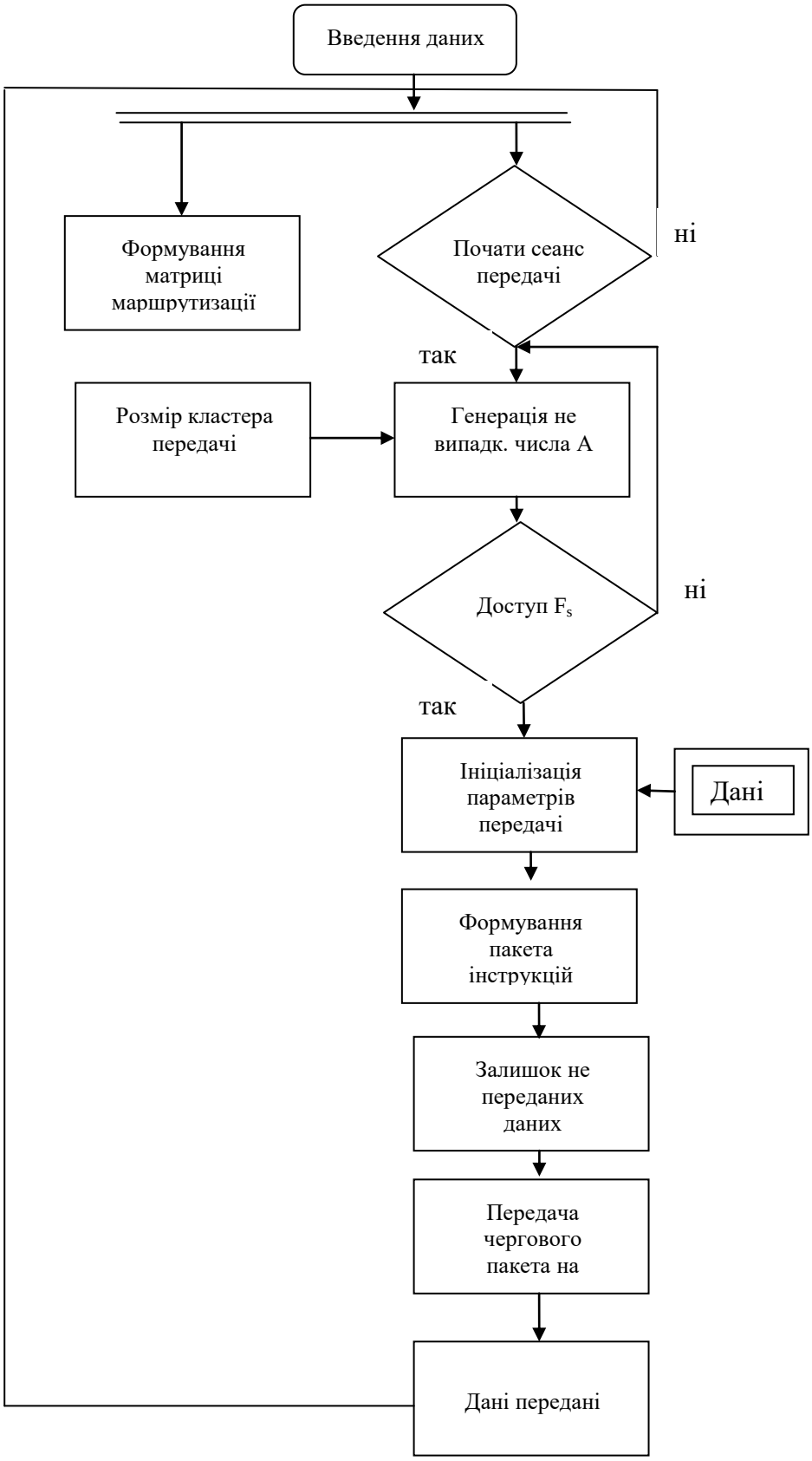


Рисунок 3.7 – Алгоритм динамічної маршрутизації інформації в бортових мережах

Алгоритм динамічної маршрутизації інформації в бортових мережах, описується наступними етапами:

Крок 1. Обчислення елементів множин матриць маршрутизації M і множин, що описують кількість доступних БЦОМ, $Fs^{дост}$ в початковий момент часу t0.

Крок 2. Ініціалізація передачі. При надходженні запиту SMC (керований компонент SM, який встановлюється на кінцевому обладнанні та надає функцію для ініціалізації процесу передачі інформації з сервісу маршрутизації) на ініціалізацію сеансу передачі даних виконуються такі дії:

2.1. Виконується запит значення параметра.

2.2. Створюється пакет інструкцій, що містить адресу джерела, адресу одержувача, розподіл по БЦОМ в захищеному виконанні.

2.3 Використовуючи операцію рандомізації, виходить псевдовипадкове число k.

2.4 Перевіряється доступність Fsk, якщо БЦОМ недоступний – повернення до п.2.3.

2.5 Формується пакет даних та маркується як пакет SM.

2.6. Надсилання пакета даних та пакета інструкцій на доступні БЦОМ Fsk.

Якщо потрібна подальша передача даних – повернення до п. 2.5.

2.7. Завершення роботи SMC.

Крок 3. Динамічна маршрутизація на БЦОМ FSI:

Формується нова матриця маршрутизації у разі, якщо різниця поточного часу та часу останньої зміни Mt більша за t. При отриманні пакетів SM – перехід до п. 3.2;

Відкриття отриманого пакета інструкцій, у розділі «БЦОМ у захищеному виконанні» додати адресу Fsi;

Якщо кількість записів у розділі «БЦОМ у захищеному виконанні» f, та пакети даних, що стосуються цього пакета інструкцій, відправляються на адресу джерела, то необхідне повернення на п. 3.1;

Використовуючи операцію рандомізації, виходить псевдовипадкове число k;

Перевірка доступності Fк, якщо БЦОМ недоступний - повернення до п. 3.4;

Перевірка наявності інформації про Fsk у розділі «БЦОМ у захищеному виконанні»: якщо Fsk є у цьому розділі - повернення до п. 3.4;

3.7. Відправлення пакета інструкцій та пакетів даних, що належать до нього БЦОМ, виконану у захищеному виконанні, Fsk; повернення до п. 3.1.

Крок 4. Отримання пакету даних та пакету інструкцій SMC, що визначається адресою отримувача.

У процесі передачі за допомогою SM дані проходять через кілька БЦОМ в захищеному виконанні, рівному f. Вибір кожної наступної БЦОМ відбувається динамічно. Враховуючи наведене вище визначення таблиць маршрутизації для SMS, вибір кожної наступної БЦОМ описується гіпергеометричний розподіл [13].

Для гіпергеометричного розподілу ймовірність прийняття випадкової величиною значення y_0 має вигляд:

$$p\ (y = y_o | n, d, c) = \frac{\binom{c}{y_o}\binom{n-c}{d-y_o}}{\binom{n}{d}} \qquad (3.3)$$

де d – число об'єктів, що мають ознаку a, у аналізованої сукупності обсягу n. При цьому y_0 набуває значень від $\max\{0, з - (n - d)\}$ до $\min\{n, d\}$, при інших y_0 ймовірність у формулі (3.3) дорівнює 0.

Отже, гіпергеометричний розподіл визначається трьома параметрами - обсягом генеральної сукупності n, числом об'єктів d в ній, що володіють ознакою й обсягом вибірки c.

Для сервісу маршрутизації вищенаведені параметри мають наступні значення:

n = F – кількість БЦОМ у захищеному виконанні;

di - FSідост(t) – кількість доступних БЦОМ у захищеному виконанні, для Fsi у момент часу t, c = 1 – кількість обраних БЦОМ у захищеному виконанні кожному етапі передачі;

y0 = 1 – кількість доступних БЦОМ у захищеному виконанні у вибірці. Таким чином, вибір кожної наступної БЦОМ описується гіпергеометричний розподіл HG(1, FSідост, F).

Підсумковий маршрут трафіку від джерела до отримувача під час використання SM і f БЦВМ у захищеному виконанні з F, що знаходяться в бортовій мережі, буде обраний з ймовірністю:

$$p_j = \prod_{i=0}^{f} \frac{\begin{pmatrix} F-i-1 \\ F_{Si}^{дост}-i-1 \end{pmatrix}}{\begin{pmatrix} F-i \\ F_{Si}^{дост}-i \end{pmatrix}}, j \in [1,k] \qquad (3.4)$$

де $Fsi^{дост}$ – число доступних БЦОМ для Fsi при вибірці Fs(i+1) БЦОМ захищеному виконанні, на i+1 кроці, що визначається формулою (3.3).

Формула (3.4) визначає ймовірність побудови системою SM одного з можливих маршрутів, що використовує тільки доступні БЦОМ в захищеному виконанні, як статичну систему.

Даний факт враховується у формі (3.4) за допомогою параметрів $Fsi_{дост}$.

Значно більший інтерес з точки зору оцінки вразливості SM представляє розрахунк імовірності побудови j-го маршруту (з k-можливих) і в такому випадку, коли виявляється вплив на ділянку, наприклад, між і-ою та (і+1)-ю БЦО М, виконаних у захищеному виконанні, що входять до маршруту трафіку.

Отже, можна об'єднати два підходи до забезпечення безпеки переданої інформації: з одного боку, знизити ймовірність ЕМВ впливу на канали зв'язку, що використовуються, а інший – застосувати логічне перетворення інформації.

3.5 Висновки за розділом

1. Запропоновано математичний апарат побудови адаптивної системи виявлення деструктивних ЕМВ на БЦОК, який включає наступні ієрархічні рівні, а саме: рівень формування ознак деструктивних ЕОМ, рівень ідентифікації деструктивних ЕМВ, рівень узагальнення і накопичення досвіду виявлення деструктивних ЕМВ. Адаптивний характер рівнів системи виявлення обумовлено використанням інтелектуальних засобів нечіткої логіки і нейронних мереж.

2. Розроблені сценарії роботи системи виявлення деструктивних впливів на БЦОК:

- на основі методу аналізу параметричних спотворень інформаційних потоків в умовах впливу ЕМВ;

- на основі методу аналізу інформації з датчиків виявлення ЕМВ.

3. Розроблено процедуру поділу трафіку. Основною ідеєю режиму поділу трафіку є рознесення передачі даних по кількох фізичних каналах.

4. На основі даної процедури реалізований «сервіс маршрутизації» передачі даних для бортової мережі.

ВИСНОВКИ

В ході виконання кваліфікаційної роботи магістра, повною мірою розв’язані поставлені задачі, відповідно до завдання, та отримано:

1. Проведені дослідження існуючих підходів застосування інтелектуальних засобів для вирішення задачі виявлення деструктивних впливів на елементи і вузли БЦОК показали, що найчастіше використовують підхід з адаптивних засобів виявлення деструктивних впливів із використанням нейронних мереж або гібридних систем на їх основі.

2. Показано, що використання нечіткої логіки складових нейромережевих засобів виявлення деструктивних впливів дозволяє враховувати апріорний досвід експертів, реалізувати властиве нейронним мережам нечітке представлення інформації.

3. Проведений аналіз показників для оцінки стійкості БЦОК до деструктивного впливу ЕМВ показав, що відомі оцінки відображають статичний стан комплексу, не враховують дійсну завантаженість вузлів і підсистем БЦОК та можливу динаміку зміни характеру ЕМВ й можливість визначення механізмів захисту.

4. Запропоновано математичний апарат побудови адаптивної системи виявлення деструктивних ЕМВ на БЦОК, який включає наступні ієрархічні рівні, а саме: рівень формування ознак деструктивних ЕОМ, рівень ідентифікації деструктивних ЕМВ, рівень узагальнення і накопичення досвіду виявлення деструктивних ЕМВ. Адаптивний характер рівнів системи виявлення обумовлено використанням інтелектуальних засобів нечіткої логіки і нейронних мереж.

5. Розроблені сценарії роботи системи виявлення деструктивних впливів на БЦОК:

- на основі методу аналізу параметричних спотворень інформаційних потоків в умовах впливу ЕМВ;

- на основі методу аналізу інформації з датчиків виявлення ЕМВ.

6. Розроблено процедуру поділу трафіку. Основною ідеєю режиму поділу трафіку є рознесення передачі даних по кількох фізичних каналах.

7. На основі даної процедури реалізований «сервіс маршрутизації» передачі даних для бортової мережі, чим забезпечується оптимальне функціонування бортових обчислювальних комплексів рухомих об’єктів в умовах навмисних зовнішніх впливів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Електромагнітна сумісність радіоелектронної апаратури./ Іванов В. О., Габрусенко Є. І., Ільницький Л. Я., Щербіна О. А – К.: НАУ, 2014. – 312 с.

2. Williams T. EMC for Product Designers. Fifth Edition – Newnes, 2016. – 564 p.

3. Теорія електромагнітного поля і основи техніки НВЧ: навч. посіб. / С.В. Соколов, Л.Д. Писаренко, В.О. Журба; за заг. ред. Г.С. Воробйова. – Суми: Сумський державний університет, 2011. – 393 с.

4. Приймальні та експлуатаційні випробування електроустаткування: Навч.посібник / Уклад.: В.Б.Абрамов, В.О.Бржезицький, О.Р.Проценко, під ред. Бржезицького В.О. – К.:НТУУ «КПІ», 2015. – 235 с.

5. J. Gao, J. Yang, D. Huang, H. Liu, S. Liu, Experimental application of vibrational resonance on bearing fault diagnosis. J. Braz. Soc. Mech. Sci. Eng. 41, 1 – 13 (2019).

6. V.N. Chizhevsky, G. Giacomelli, Experimental and theoretical study of vibrational resonance in a bistable system with asymmetry. Phys. Rev. E 73(2), 022103 (2006).

7. Brichard B., Fernandez A.F. Conference RADECS 2005, Short Course Notebook – New challenges for Radiation Tolerance Assessment / Ed. by Fernandez A. F. Cap d'Agde, 2005. P. 95–137.

8. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації: монографія. К. : ПоліграфКонсалтинг. 2007. 209 с.

9. Руденко О.Г., Бодянський Є.В. Штучні нейронні мережі: Навчальний посібник. – Харків: ТОВ «Компанія СМІТ», 2006. – 404 с.

10. Терейковський І.А. Використання нейронної мережі Кохонена для розпізнавання спаму. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2007. Випуск 1(14). С.106-114.

11. Генетика популяцій: підручник / О. Л. Трофименко, М. І. Гиль, О. Ю. Сметана; за ред. професора М. І. Гиль ; МНАУ. – Миколаїв: Видавничий дім «Гельветика», 2018. – 254 с.

12. Основи теорії цифрових систем автоматичного керування: LTI моделі для систем SISO та MIMO [Електронний ресурс]: навч. посіб. для студ. спеціальності 172 «Телекомунікації та радіотехніка» / КПІ ім. Ігоря Сікорського; уклад.: С.О. Кравчук, О. І. Лисенко, В. С. Явіся, В. І. Новіков. – Київ: КПІ ім. Ігоря Сікорського, 2021. – 196 с.

13. Теорія ймовірностей і математична статистика: навч. посібник / В. І. Авраменко, І. К. Карімов. – Дніпродзержинськ: ДДТУ, 2013. – 245 с

14. Espitia, H., Soriano, J., Machón, I., & López, H. (2019). Design methodology for the implementation of fuzzy inference systems based on boolean relations. Electronics, 8(11), 1243.

15. Qodar, G. L. (2020). The Application of Mamdani Method for Predicting The Best Portable Computer Based on Hardware and Price. Journal of Informatics and Telecommunication Engineering, 4(1), 33-47.

16. W.-X. Yan Shunt active power filter line current control based on T-S fuzzy model/ W.-X. Yan, Z.-C. Ji, and J. Hui: in 2009 4th IEEE Conference on Industrial Electronics and Applications, 2009, pp. 2241–2246.

17. S. P. K. Vanapalli Performance analysis of unified power quality conditioner controlled with ANN and fuzzy logic based control approaches/ S. P. K. Vanapalli, Satyanarayana, M. Venu Gopala Rao: Reg. 10 Conf. TENCON 2017 - 2017 IEEE, no. 2159–3450, 2017.

18. S. Musa Fuzzy logic controller based three phase shunt active power filter for harmonics reduction/ S. Musa, M. A. M. Radzi, H. Hisham, and N. I. Abdulwahab: in 2014 IEEE Conference on Energy Conversion (CENCON), 2014, pp. 371–376.

19. Радіотехніка: Енциклопедичний навчальний довідник: Навчальний посібник / За ред. Ю. Л.Мазора, Є.А.Мачуського, В.І.Правди. – К.: Вища шк., 1999. – 838 с.

20. Сучасні інформаційні системи і технології: управління знаннями: навчальний посібник / В. М. Антоненко, С. Д. Мамченко, Ю. В. Рогушина. – Ірпінь: Національний університет ДПС України, 2016. – 212 с.

ДОДАТКИ

1. ANALYTICAL PART

1.1 Evaluation of the functioning of on-board digital computing systems under the influence of powerful electromagnetic radiation

Solving the problem of ensuring the resistance of the BCOC to the influence of powerful pulsed electromagnetic fields is a complex multi-stage process [1]. A peculiarity of the tasks for the development of BCOC is the simultaneous presence of different EMF spectrums, which requires analysis and assessment of the impact of such radiation on individual elements and nodes, and ultimately on the entire on-board complex as a whole.

The destructive effect of EMF on on-board computing complexes can be caused both by the direct impact of pulsed electromagnetic fields on the elements of the on-board complex, and by the currents and voltages induced in the connecting lines and circuits. The sensitivity of the elements and nodes of the BCOC to the influence of EMF depends on a number of factors, in particular, the position regarding the direction of the electric and magnetic field vectors, the geometric dimensions of the electric circuits and circuits, their configuration, mutual connections, electrical load ratings, the values of capacitive and inductive connections connections with system design elements and the environment, the quality of shielding, etc.

At the same time, it should be borne in mind that even for those elements and nodes of the BCOC, the housings of which can act as electromagnetic shields, electromagnetic pulses will have a destructive effect through connecting lines and connectors. Therefore, all types of wiring systems present in the on-board complex play the role of

collectors of dangerous EMF energy. The currents and voltages induced in the conductors can lead to either an electrical breakdown (cable insulation) or damage to the devices connected to the conductors if they have surge-sensitive elements. These impulses can destroy and disrupt the operation of the BCOC elements almost simultaneously in several places.

In addition to the presence of possible long wire systems, relatively low electrical strength of the elements and, on the contrary, high sensitivity to electrical interference are a special danger for the elements and nodes of the BCOC. One of the possible areas of application of such radiation is remote damage to electronic components, in particular digital devices. Today, they make up the bulk of the elements in use. It should be taken into account that at the current stage there is a sharp increase in the share of software compared to hardware with a simultaneous increase in the speed of the components. Transition from PDH systems to synchronous digital hierarchy (SDH) systems using B-ISDN and ATM broadband systems.

Work on creating sources of powerful EMF is being carried out in the following directions:

- creation of sources of electromagnetic radiation with an ultra-broad spectrum in the range from 0.1 to 10 GHz. This technology has reached a high level of perfection based on generators with spark and semiconductor key elements [2]. EMFs of the specified type induce high-amplitude pulses on power cables, telephone communication lines, etc. The disadvantage of EMF with a spectrum below 100 MHz is the need to create a long transmitting antenna. Otherwise, the efficiency of EMF radiation drops sharply.

- the creation of narrowband ultra-high-frequency EMFs, which are more effective than other effects on equipment, not only by targeting cable lines, but also through holes, gaps and screens in the equipment.

1.2 Analysis of the features of the impact of ultrashort EMF on elements and nodes of BCOC

Broadband and high frequency of repetition of ultrashort EMF make this type of electromagnetic influence very dangerous.

A feature of EMFs is their short duration (from tens to hundreds of picoseconds to one nanosecond for the first semi-periodic pulses at the level of 0.5 of the amplitude), similar to the duration of the working signals of the electronic equipment of data transmission networks of telecommunication systems.

The main spectral density is in the frequency range from hundreds of megahertz to tens of GHz [2]. High sparability provides high values of impulse voltages at low levels of average power (<1J) and power consumption of the source. In laboratory generators from above, short electromagnetic radiation at the output of the generator forms periodically repeating video pulses of positive or negative polarity (Figure 1.1).

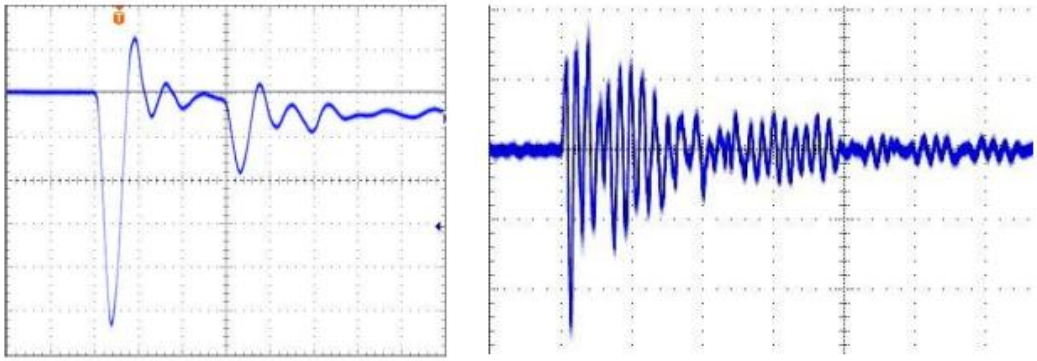


Figure 1.1 – Graphs of electromagnetic radiation:

a) pulse shape at the output of the generator; b) the shape of the pulse on the load of the network interface, under the conditions of capacitive injection

The physical transmission medium of structurally complex systems is usually a twisted pair, which is a system with distributed parameters: capacity and inductance. As a result of the transient processes that occur during the injection of the EMF circuit (in the twisted pair of category 5), the pulse formed at the output of the generator takes the form of a decaying sinusoid in the process of measurement on the load of the network interface.

This is explained by the fact that the cable is a special oscillating circuit with characteristic capacitance and inductance. As a result, a pulse of longer duration, modulated with different frequencies, arrives at the input of the network interface. In fig. 1.1 a) shows the initial pulse shape at the output of the generator, and Fig. 1.1 b) shows the pulse interference shape on the load of the network interface of the capacitive injection method.

Analysis of modern on-board digital computing systems showed that they are characterized by the following features:

1. BCOCs have minimum weight and size characteristics.

2. There is a steady tendency to increase the reliability and quality indicators of individual elements and nodes of the BCOC.

3. BCOCs are exposed to a broad aspect of the influence of destabilizing factors.

In general, BCOCs must function in conditions of dynamically changing influences on them, depending on the trajectory of movement or conditions of environmental change: magnetic, electromagnetic fields; continuous pulsed ionizing radiation; a wide range of mechanical and climatic influences.

4. On-board systems include both digital automation devices, telemetry, digital signal processing, etc.), and analog and hybrid devices (receiver-transmitting devices, navigation devices, amplifying and measuring devices, etc.), which operate over a

wide range of frequencies (from units of Hz to GHz), voltages (from tenths of volts to kilovolts), and currents (from mA to hundreds of amperes).

5. In terms of design and technology, BCOCs have a wide range of implementations, which are based on various design principles: single-circuit; functional block; functionally modular; functionally nodal. In connection with strict requirements for weight and size characteristics, as well as the presence of various types of BCOC devices, modern achievements of hybrid-integral technologies are widely used, which, in turn, contribute to the acceleration of the development of technical achievements in the field of creating promising radio equipment.

6. A wide range of destabilizing factors and high reliability requirements lead to the need to use special schematic, design and technological solutions related to ensuring electrical, electromagnetic, thermal, aerodynamic and other characteristics of the BCOC.

Ensuring the resistance of BCOC to electromagnetic radiation at the circuit level is carried out at the expense of:

• galvanic decoupling of power supply and grounding circuits; elimination of through currents of semiconductor devices;

• introduction of gas dischargers and special filters into power supply circuits;

• introduction of special schemes for protection against magnetic flux and voltage overloads, etc., for individual elements.

7. The implementation of BCOC with minimum weight and size characteristics, combined with the achievements of microminiaturization, leads to a close relationship of physical processes (electrical, electromagnetic, aerodynamic, thermal, mechanical, radiation, etc.) occurring in the schemes and designs of BCOC.

8. From the point of view of assessing the impact on elements and nodes of BCOC, EMV can be divided into separate components. This is due to the following reasons:

• the limited possibilities of existing methods of assessing the impact of EMF, in general;

• the difference in the requirements for BCOC regarding protection against EMF exposure;

• lack of cases of galvanic connection between all elements of the BCOC.

9. In the general case, the factors affecting the functional elements and nodes of the BCOC during exposure to EMF are:

• electromagnetic fields affecting the elements and nodes of the BCOC;

• electromagnetic fields penetrating through the shielded surfaces of nodes and subsystems of the BCOC;

• EMFs connecting with impulse currents of power cable communications and penetrating into the middle of the shielded subsystems of the BCOC;

• impulse voltages and currents induced in the twisted pair, which affect the isolation of equipment that has a galvanic connection with power cable communications;

• impulse voltages and currents induced in inter-post cables that penetrate through inhomogeneities of screens.

Therefore, the specified effects of EMF can act through the following channels: electromagnetic field; on communication lines; on power chains; on metal structures, etc.

Impulse voltages arising in the internal parts of consumers in most cases do not pose a danger to the cable lines and electrical equipment themselves, they can pose a danger to technological consumers (rectifiers devices, stabilizers, etc.) or reduce their immunity to interference. For this reason, these effects must also be quantitatively and qualitatively taken into account for each specific system.

As a result of the impact of EMF on the elements of the BCOC, the latter may have the following damages and failures:

o disruption of the functioning of individual subsystems or the entire system as a whole, as a result of false activations of the pulsed input and output circuits of the equipment;

• failure of protection panels, due to insulation breakdown of input or output elements of these blocks;

• failure of power sources of BCOC, as a result of insulation breakdown of transformers in input power circuits, which leads to the failure of automation equipment related to this;

• complete loss of performance of individual subsystems of the BCOC as a result of insulation breakdown and failure of cables [4].

In some cases, the destruction due to the overloading of the protective arresters installed in the input circuits leads to a malfunction of the BCOC.

In addition, during exposure to EMF, modern BCOCs, as indicated by literary sources [4, 5], are characterized not only by physical destruction of the elemental base of the on-board complex, but also by a violation of the functional integrity of information transmitted through communication channels and processed by on-board computing complexes.

One of the features of the propagation of periodically repeating impulse interference, which is created in the cable (in a twisted pair) as a result of the influence of EMF, is that, despite the symmetry of the twisted pairs, part of the interference penetrates into the circuits of the network adapter through the interaction bus.

As you know, in an ideal symmetrical twisted pair, the obstacles introduced in the wires of the pair cancel each other out.

From a very short EMF pulse with a total low specific energy, a high amplitude of the interference pulse occurs, as a result of which some resulting interference remains and penetrates further [5].

Impacts on power supply circuits are unlikely, which is explained by a complex impact algorithm and the need to take into account many factors of the operation of active network equipment, such as, for example, the use of protective power filters, protection in the power supply unit of active network equipment, the level of activation "intelligent" protection of equipment, the critical level of operation of the element base of the system [5].

It should be noted that the influence of ultra-short electromagnetic pulses on the physical environment of Ethernet, which is often used in on-board computing complexes, has not been paid enough attention until now.

In this regard, special attention is paid to these issues in the Master's thesis.

The mechanism of formation of errors during data transmission is based on the fact that the ISO/OSI model describes the interdependence of network systems and consists of seven levels. Ethernet technology works on the first two levels of this model: physical and channel.

The transmission medium and signal parameters are determined by the physical layer. At the channel level, continuously transmitted sequences of bytes form frames. The transfer of information itself is carried out with the help of frames. The complexity of the technology lies in the fact that there are several typical frames that have a different structure, so each type of frame must have a certain processing method for correct reception.

As it propagates along the twisted pair, an Ethernet frame can be exposed to internal and external factors that can change the original appearance of the frame. Ethernet errors are when the frame is corrupted or incorrect so that the frame cannot be processed correctly by the receiving end. All of them have different causes, caused by hardware or software malfunctions, but a sign of the presence of an error is the corruption of one or more bits of the frame or the non-compliance of the shape and structure of the frame with IEEE international standards.

In modern switched Ethernet, collisions are minimized, since there is no competition for access to the medium, and the maximum share of errors of modern generations of Ethernet operating at speeds of 1 and 10 Gbit/s is small [5].

Ethernet networks, especially networks of the latest generations, built using twisted pair as a physical transmission medium, are sensitive to external electromagnetic interference, which have a significant impact on signal transmission and lead to the occurrence of a number of malfunctions in the wired system [6]. Thus, during the impact of EMF on the cable communication line, periodically repeating impulse interference is propagated, the amplitude of which is greater than or equal to the useful Ethernet signal and leads to distortion of the original sequence of symbols.

It is also worth mentioning the fact that there are some limit parameters for the stability of the operation of Ethernet networks, which are individual for each manufacturer of network equipment. During the influence of ZK EMF on the cable line of the on-board network and reaching the limit parameters, the network connection between end users is destroyed.

In this regard, the final values of the parameters at which the destruction of the network connection occurs can only be established experimentally by [6].

Today, the general recommendations for troubleshooting on-board networks are that when an error is detected, it is necessary to collect information about the error and localize it to the minimum possible value. The localized portion of the network containing the error is then isolated and the error is corrected.

1.3 Analytical review of the methods and means of ensuring the sustainability of BCOC

Among the available studies [6], we can single out the results of the operation of the simplest local network under the conditions of exposure to electromagnetic waves of different amplitudes and frequencies in the room and in the open space.

Studies have been carried out to assess the effect of the pulse routing frequency on a cable fragment (unshielded twisted pair of category 5e) of the Ethernet local network (10Base-T and 100Base-T).

A 4-horn antenna system with an aperture of 0.5 × 0.5 m was used as a radiation source, excited by a voltage pulse generator with a maximum amplitude of 40 kV and a front duration of ~200 ps, without a concentrator ~800 ps. Packets with a length of 64 bytes were forwarded between computers.

Fig. 1.2 (a and b) shows the dependence of the share of loss of information packets on the intensity of the electric field during the irradiation of the information cable [7].

It was established that the amplitude of the attacks on the information cable, in which there is a 100% loss of information packets (the data transfer rate in the network is 0), is from 6 to 15 V, and the frequency of the pulses was 100, 500, 1000 kHz.

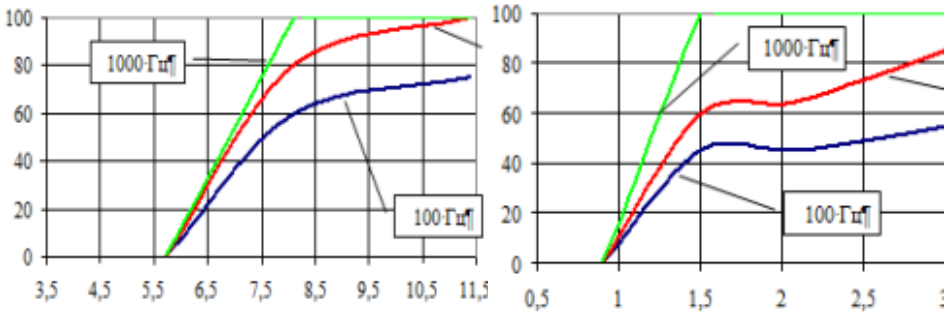


Figure 1.2 – Dependencies of the share of information packet losses on the electric field intensity during the irradiation of the information cable:

a) without a concentrator; b) with a hub

Currently, the following methods are used to protect information and telecommunication systems from destructive electromagnetic influence:

1. General and local shielding of telecommunication nodes and information communication lines. However, the results of the analysis of the functional purpose of BCOC and the technical and economic examination show that the use of the shielding

method to protect them from the destructive influence of the electromagnetic radiation in some cases is insufficiently effective or economically impractical for the following reasons:

- the influence of source-source EMF is characterized by a wide frequency band and a large amplitude of emitted electromagnetic fields, a high ability to penetrate the inhomogeneity of screens. Therefore, to ensure effective shielding from this type of impact, the requirements for the integrity of the construction of shield structures must be met, as well as the possibility of gaps and inhomogeneities in connectors and connections must be excluded. The implementation of these conditions is usually associated with significant structural difficulties and material costs;

- BCOC is a distributed information communication system, therefore in most cases it is technologically impossible to fulfill the condition of integrity by building shielding structures, which sharply reduces the effectiveness of shielding as a protection method.

2. The use of technical means to minimize or prevent the impact of electromagnetic radiation on BCOC. The analysis of the used old-fashioned filters and gas-discharge elements showed that at the moment their use does not allow to effectively fight against the destructive influence of EMF ZK. The main parameter of modern gas dischargers, such as its activation time, is much lower than the duration of exposure to an ultra-short electromagnetic pulse. The frequency characteristics of modern interference filters and transformers do not allow to effectively separate the indicated interferences of the EMF circuit from the useful signal in the information lines. Therefore, the use of standard technical means of protection of BCOC from electromagnetic radiation today does not allow to exclude the possibility of destruction of information signals under the influence of electromagnetic radiation.

3. Application of interference-protected encoding of information transmission. This method allows you to effectively deal with only a small number of errors that

arise in information communication lines due to the influence of a random, usually single, interference. The main disadvantage of this method is the need to add redundancy to the transmitted information, which depends on the number of distortions that occur, and in some cases, re-transmission of information, including and distorted. All this, in turn, reduces the throughput of information channels in particular and the speed of the BCOC as a whole. Because modern sources of EMF ZK allow generating pulses with a frequency of up to several MHz, which creates interference with a high frequency in the information channel. Therefore, the use of this method of protection under the conditions of exposure to ZK EMF is also ineffective. All this leads to the need to develop special system solutions, select signal parameters and methods of their processing, which may turn out to be the most effective method of ensuring stability, because will not require the use of means of protection against interference on all paths of their propagation.

1.4 Conclusions by section

The following conclusions can be made based on the results of the analysis of the state of the issue of theoretical and experimental methods of researching the impact of the EMF ZK on BCOC and methods of assessing stability:

1. BCOCs are exposed to a wide range of influences of electromagnetic destabilizing factors. In the general case, the BCOC functions under the influence of dynamically changing factors, depending on the environmental conditions: electric, magnetic, electromagnetic fields; a wide range of mechanical and climatic influences.

2. On-board control systems include both digital devices (devices for automation, telemetry, digital signal processing, etc.), and analog and hybrid devices (power supply devices, transceivers, navigation devices, amplifying and measuring devices, etc.), which operate in a wide range of frequency (from units of Hz to GHz),

voltages (from tenths of volts to kilovolts) and currents (from mA to hundreds of amperes).

3. The existing methods and means of ensuring stability are mainly focused on solving the problem of electromagnetic compatibility, electromagnetic factors of natural and man-made origin and do not touch on the most complex set of tasks of stability of BCOCs under the influence of electromagnetic radiation.

Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

Кафедра автоматики, електроніки та телекомунікацій

ЗАБЕЗПЕЧЕННЯ ОПТИМАЛЬНОГО ФУНКЦІОНУВАННЯ БОРТОВИХ ОБЧИСЛЮВАЛЬНИХ КОМПЛЕКСІВ РУХОМИХ ОБ'ЄКТІВ В УМОВАХ НАВМИСНИХ ЗОВНІШНІХ ВПЛИВІВ

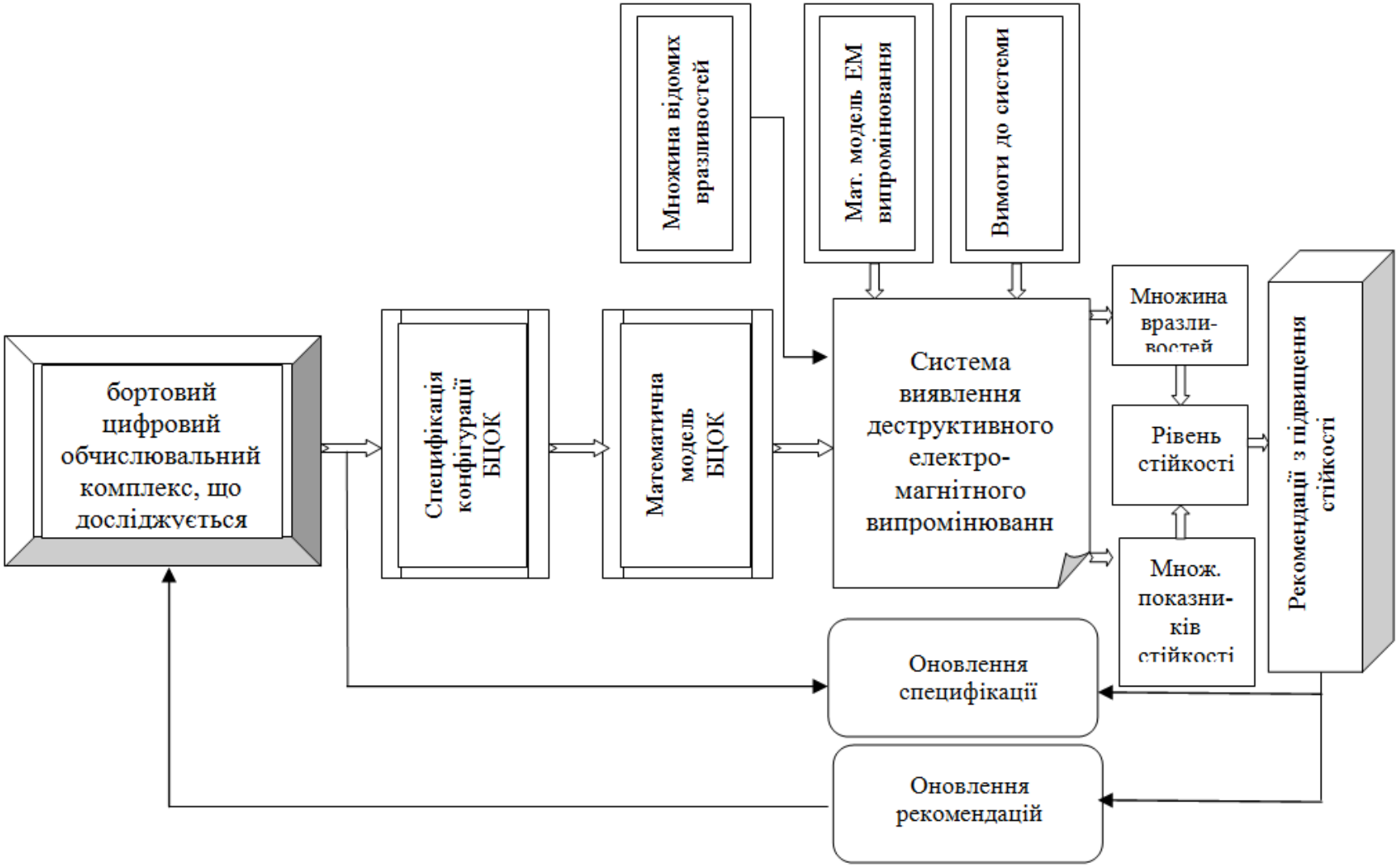
Кваліфікаційна робота магістра

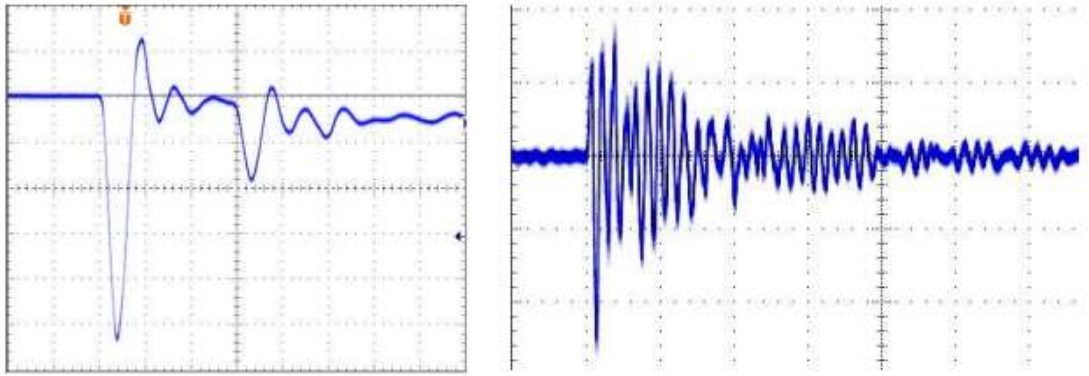
Виконав: **Я. О. Зоць**

Керівник:
д.т.н., професор **В.В. КОСЕНКО**

Полтава 2025

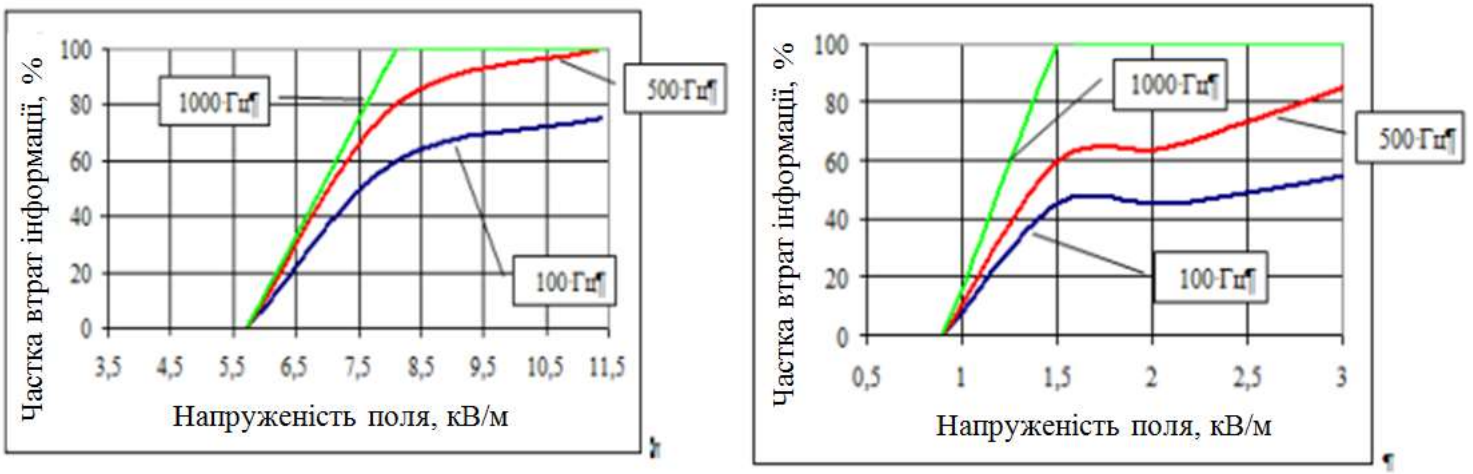
Функціональна схема інтелектуальної аналітичної системи оцінки стійкості бортових цифрових обчислювальних комплексів до електромагнітного випромінювання





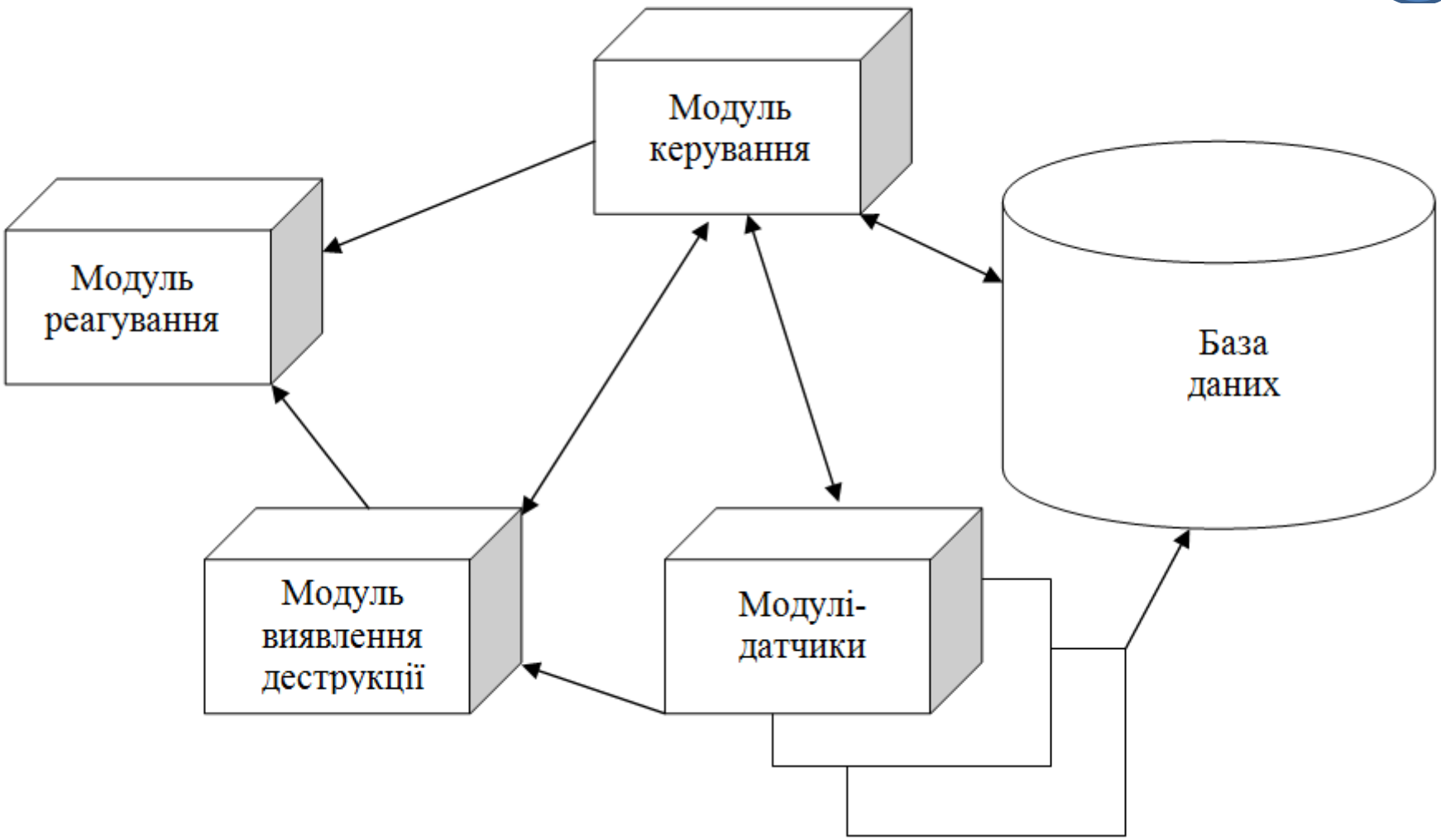
а) б)

Графіки електромагнітного випромінювання:
а) форма імпульса на виході генератора; б) форма імпульса на навантаженні мережевого інтерфейса, за умов ємнісної інжекції

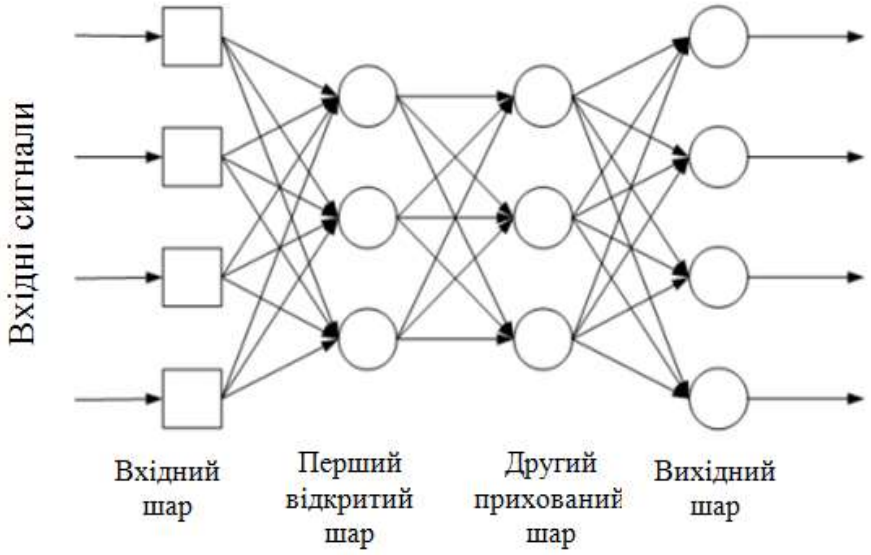


а) б)

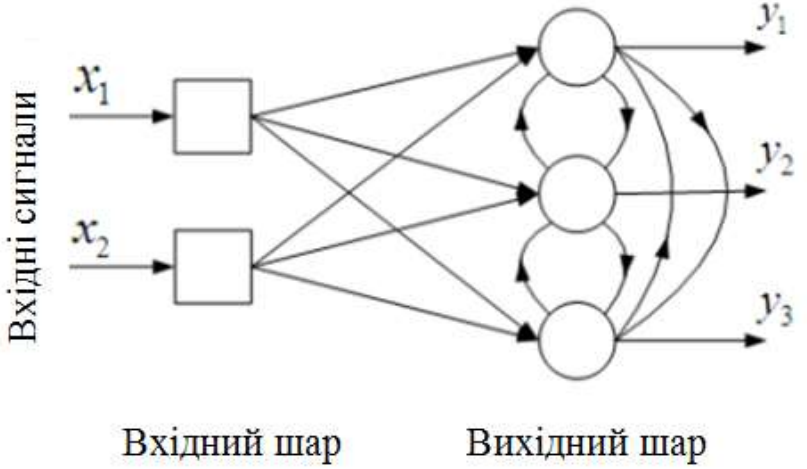
Залежності частки втрат інформаційних пакетів від напруженості електричного поля в процесі опромінення інформаційного кабеля: а) без концентратора; б) з концентратором



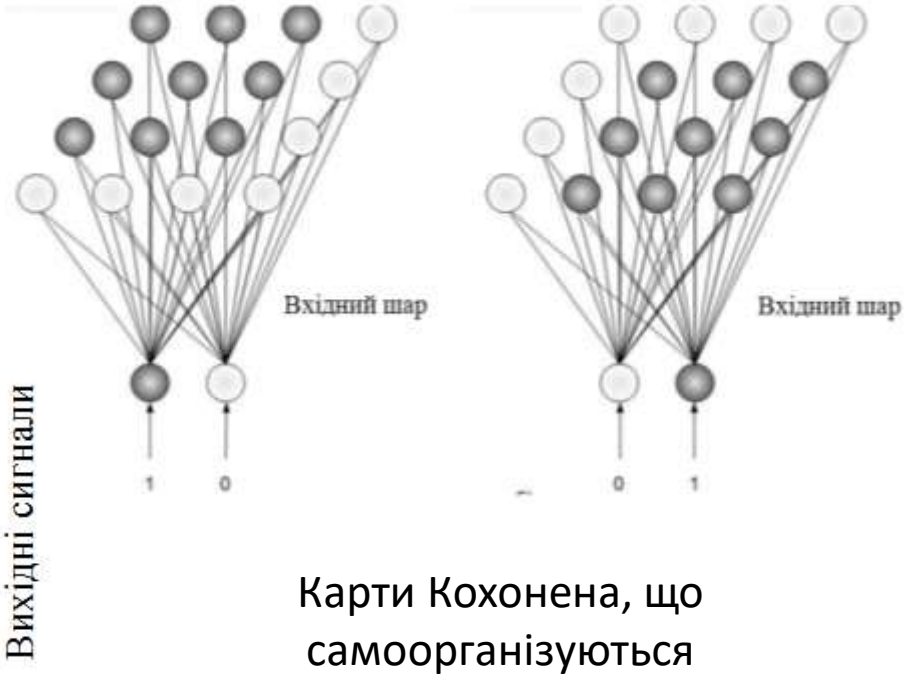
Функціональна схема системи виявлення деструктивних електромагнітних випромінювань



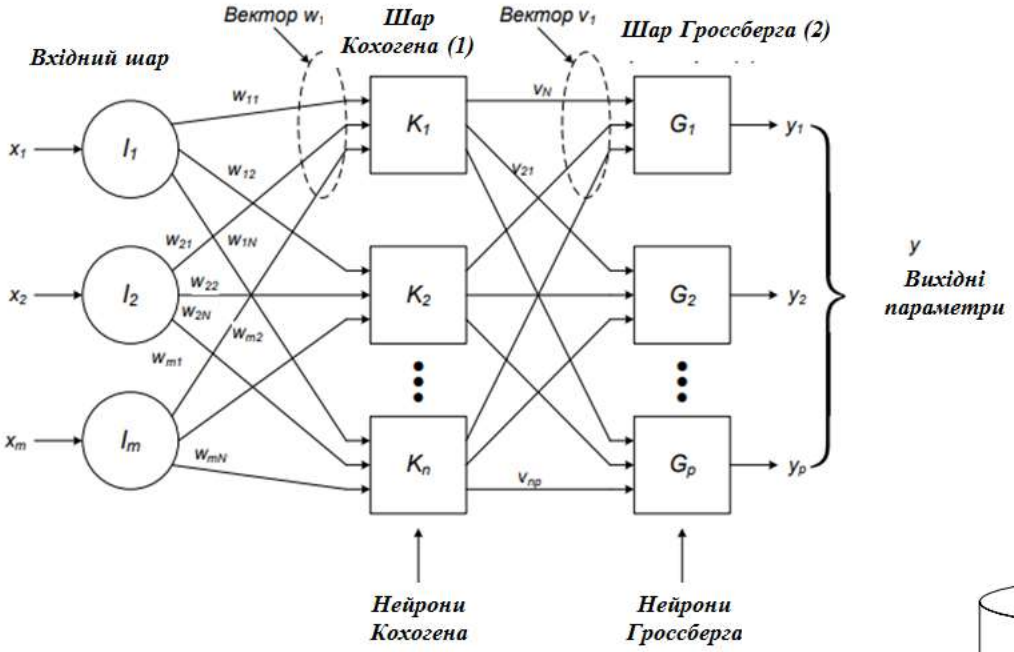
Багатошарова нейронна мережа



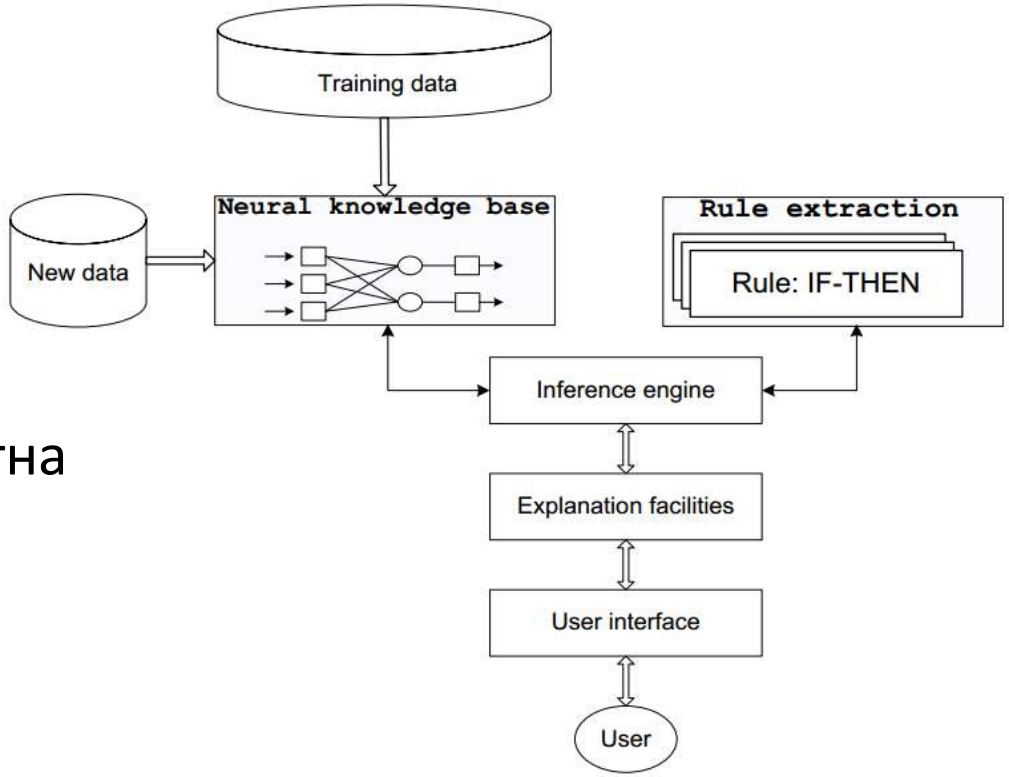
Графічна ілюстрація алгоритму Кохонена



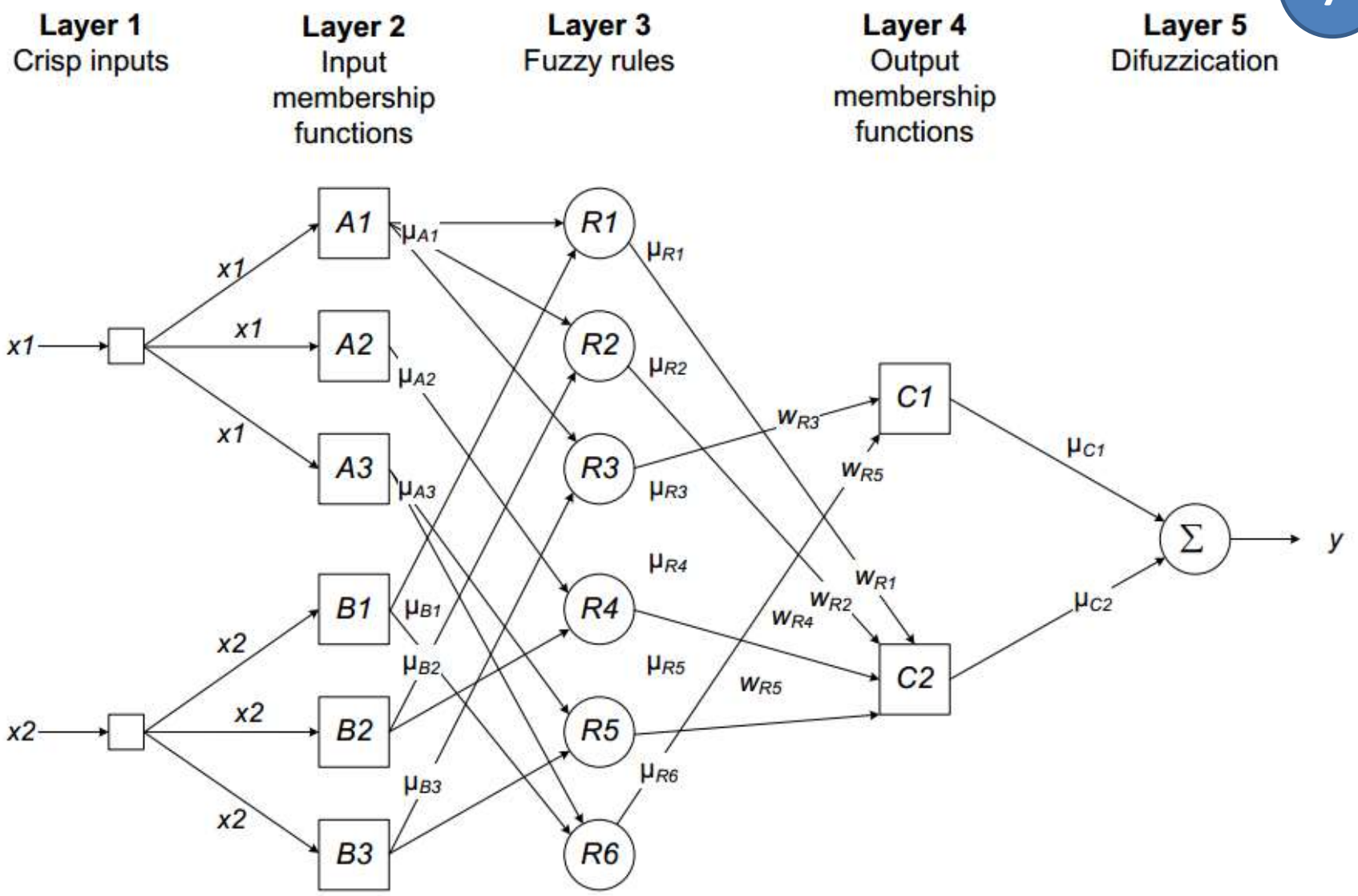
Карти Кохонена, що самоорганізуються



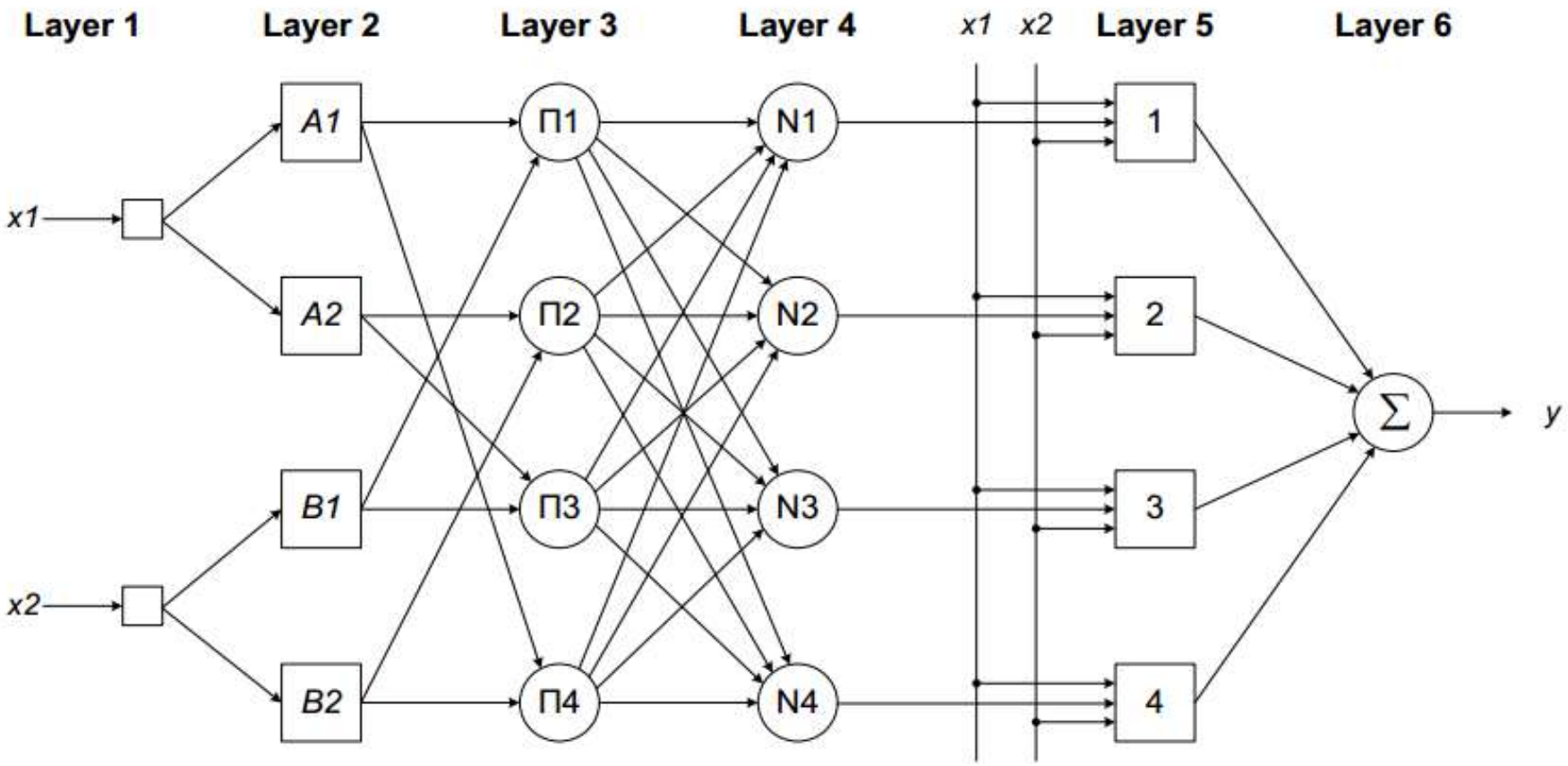
Нейронна мережа зустрічного розповсюдження



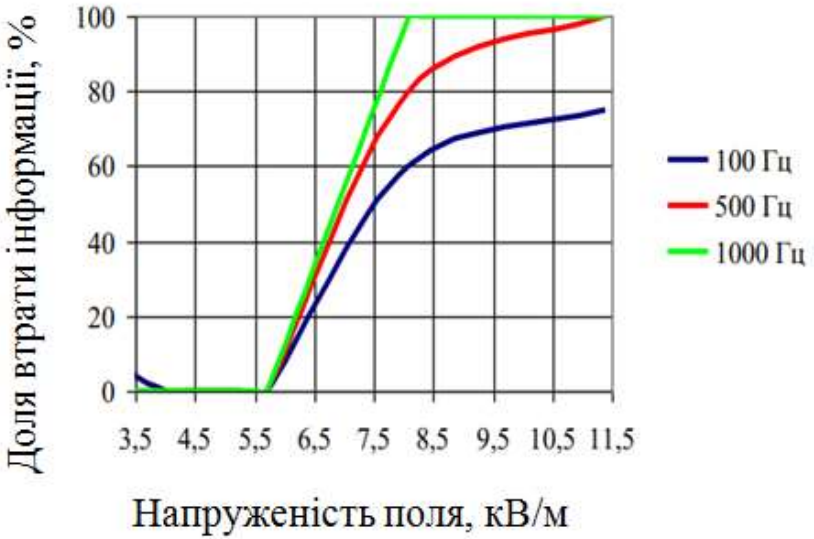
Нейромережева експертна система



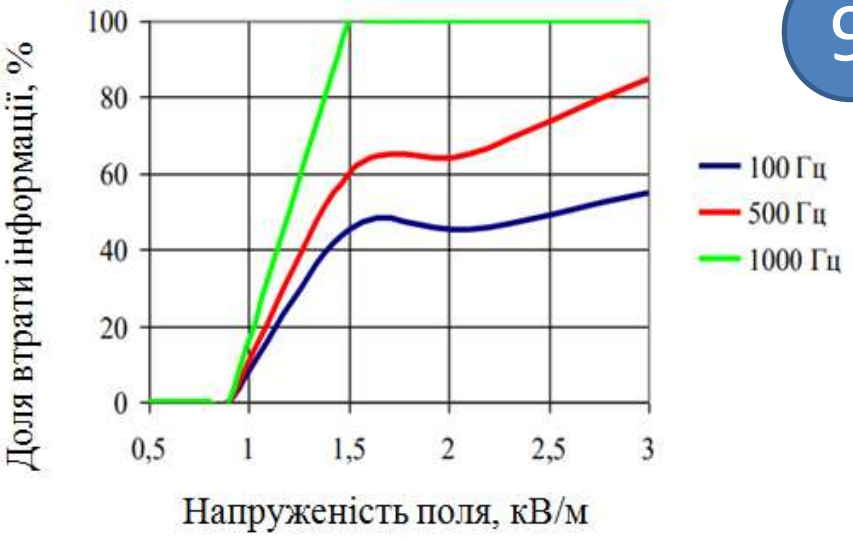
Нейро-нечітка мережа



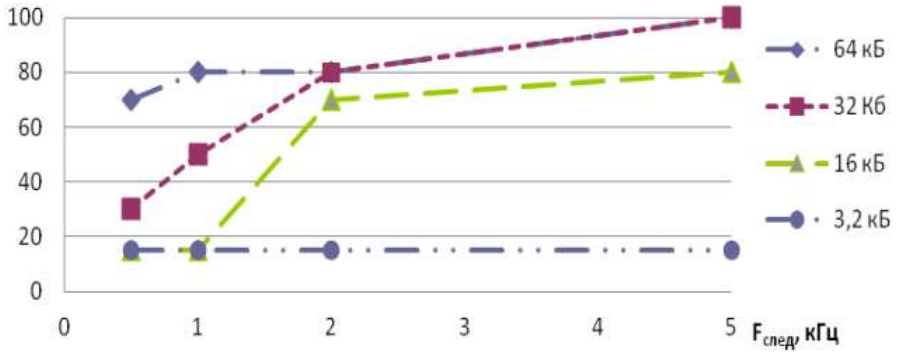
Архітектура нейро-нечіткої системи ANFIS (Adaptive Neuro-Fuzzy Inference System)



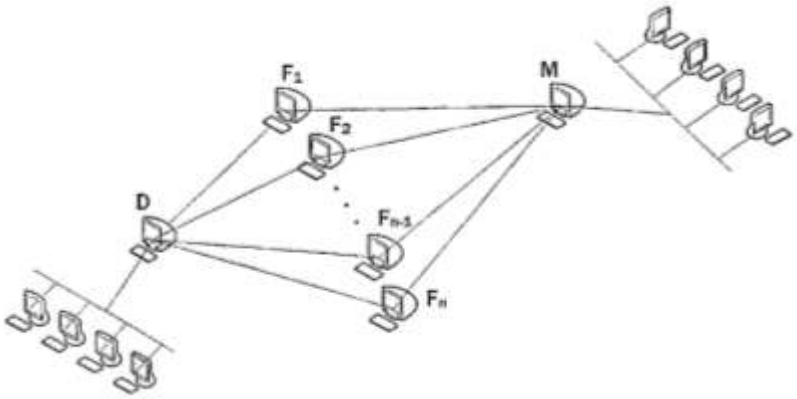
Залежність втрати інформаційних пакетів бортової мережі від частоти впливу ЕМВ з тривалістю (0,2 нс)



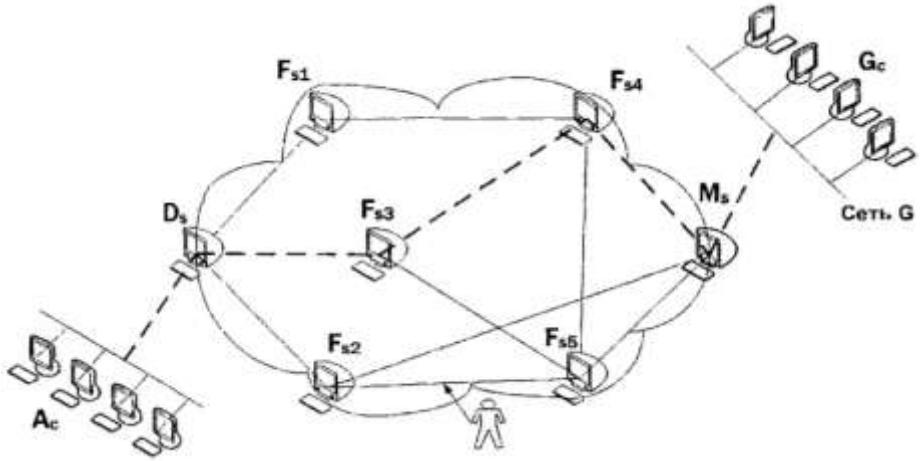
Залежність втрати інформаційних пакетів бортової мережі від частоти впливу ЕМВ з тривалістю (0,8 нс)



Залежність відсотка втрат інформації від частоти слідування імпульсів ЕМВ



Процедура перерозподілу трафіку

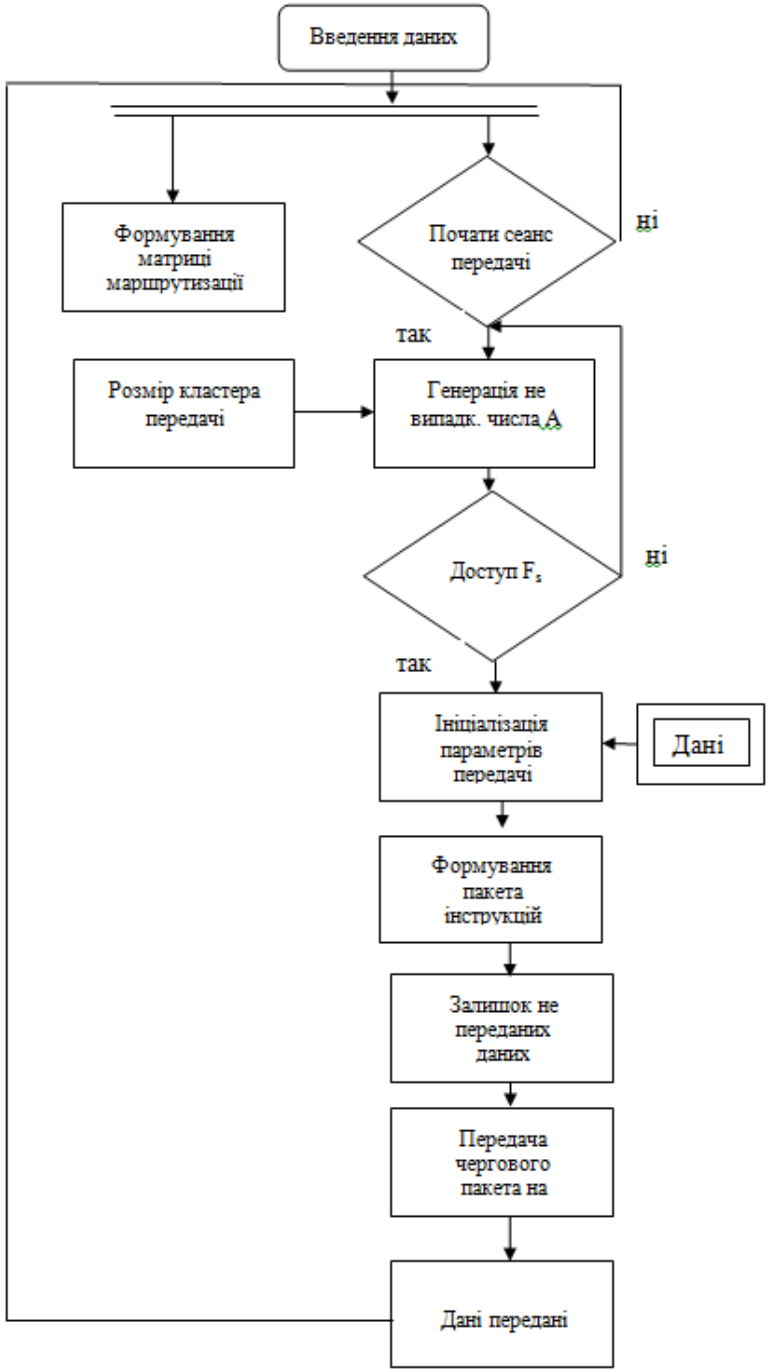


Оптимізація маршруту трафіку за рахунок використання інтелектуального сервісу маршрутизації SM

Інтелектуальна маршрутизація топології SM

	DS	FS1	FS2	FS3	FS4	FS5	MS
DS	0	1	1	1	0	0	0
FS1	1	0	0	0	1	0	0
FS2	1	0	0	0	0	1	1
FS3	1	0	0	0	1	1	0
FS4	0	1	0	1	0	1	1
FS5	0	0	1	1	1	0	1
MS	0	0	1	0	1	1	0

Алгоритм динамічної маршрутизації інформації в бортових мережах



ДЯКУЮ ЗА УВАГУ!