Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем і технологій

Бакалаврська дипломна робота на тему:

РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Виконав: студент 2-го курсу, групи ПЗТ-22мс
спеціальності 172 – Телекомунікації та радіотехніка
_____ Франчук О.В.

Керівник: д.т.н., проф., професор каф. ІКСТ
_____ Кичак В.М.
«11» 06 2024 р.

Рецензент: д.т.н., проф., професор каф. ІРТС
_____ Семенов А.О.
«11» 06 2024 р.

Допущено до захисту
Завідувач кафедри ІКСТ
_____ д.т.н., проф. Кичак В.М.
«11» 06 2024 р.

Вінниця ВНТУ – 2024 рік

Вінницький національний технічний університет
Факультет інформаційних електронних систем
Кафедра інфокомунікаційних систем та технологій
Рівень вищої освіти перший (бакалаврський)
Галузь знань 17 – Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма – Програмне забезпечення телекомунікаційних систем

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКСТ
д.т.н., професор В.М. Кичак
«06» 05 2024року

З А В Д А Н Н Я
НА БАКАЛАВРСЬКУ ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Франчуку Олександру Васильовичу
(прізвище, ім'я, по батькові)

1. Тема роботи: Розробка програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем,
керівник роботи Кичак Василь Мартинович, докт. техн. наук, професор,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ВНТУ від "11" березня 2024 року № 80

2. Строк подання студентом роботи: 07 червня 2024 року
3. Вихідні дані до роботи: тип вхідних сигналів – цифрові; режим зв'язку – дуплексний (двонаправлений); тип мережі – сигнальна СКС7 мережа; протокол зв'язку для контролю параметрів мережі – UDP.

4. Зміст розрахунково-пояснювальної записки роботи (перелік питань, які потрібно розробити): вступ, загальна характеристика цифрових телекомунікаційних мереж; аналіз відомих систем контролю та моніторингу; аналіз характеристик надійності систем контролю; розробка системи контролю та моніторингу цифрових телекомунікаційних систем; охорона праці.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень): узагальнена структура ІВС; загальна структура інтерфейсних модулів пристроїв прототипів; модель надійності програмного комплексу системи контролю; структура інтерфейсного модуля на основі КЛС; архітектура системи модулів та потоків даних ЛПМ.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Кичак В.М., професор кафедри ІКСТ	06.05.2024	11.06.2024
Охорона праці	Желебицька С.В. проф. каф. ВЖД, ПБ	06.05.2024	11.06.2024

7. Дата видачі завдання «06» травня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів бакалаврської дипломної роботи	Строк виконання етапів роботи	Примітка
1	Формування та затвердження теми та індивідуального завдання бакалаврської дипломної роботи (БДР)	06.05.2024р.	
2	Виконання спеціальної частини БДР. Перший рубіжний контроль виконання БДР	20.05.2024р.	
3	Виконання спеціальної частини БДР. Другий рубіжний контроль виконання БДР	31.05.2024р.	
4	Виконання розділу «Охорона праці»	04.06.2024р.	
5	Нормоконтроль БДР	05.06.2024р.	
6	Попередній захист БДР	06.06.2024р.	
7	Рецензування БДР	07.06.2024р.	
8	Захист БДР	12.06.2024р.	

Студент _____ (підпис) Франчук О.В.

Керівник роботи _____ (підпис) Кичак В.М.

АНОТАЦІЯ

УДК 621.396

Франчук О.В. Розробка програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем – бакалаврська дипломна робота студента спеціальності 172 – Телекомунікації та радіотехніка – Вінниця: ВНТУ 2024 р. 76 стор., 15 – рис., 5 – табл., 35 – бібл. – українською мовою.

У бакалаврській дипломній роботі проводиться дослідження програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем.

Робота присвячена розробці програмно-апаратних засобів для ефективного контролю та моніторингу цифрових телекомунікаційних систем, розглянуто сучасні методи та технології, що використовуються для забезпечення надійності та безпеки передачі даних у цифрових мережах.

Основною метою дослідження є отримання напрацювань для синтезу інтегрованої системи, яка поєднує програмні та апаратні компоненти для виявлення, аналізу та усунення проблем у телекомунікаційних мережах. Описано архітектуру синтезованої системи, включаючи модулі збору даних, обробки інформації та відображення результатів моніторингу. Особлива увага приділяється методам виявлення аномалій і запобіганню можливим загрозам безпеці.

Ключові слова: NMC, система моніторингу, телекомунікаційна мережа.

ANNOTATION

UDC 621.396

Franchuk O.V. Development of software and hardware implementations for control and monitoring of digital telecommunication systems – bachelor thesis of a student specialty 172 - Telecommunications and radio engineering - Vinnytsia: VNTU 2024. 76 pages, 15 - fig., 5 - table., 35 - bibl. - in the Ukrainian language.

Research is conducted in the bachelor thesis software and hardware means of control and monitoring of digital telecommunication systems.

The work is devoted to the development of hardware and software tools for effective control and monitoring of digital telecommunication systems, modern methods and technologies used to ensure the reliability and security of data transmission in digital networks are considered.

The main goal of the research is to obtain results for the synthesis of an integrated system that combines software and hardware components for detecting, analyzing and eliminating problems in telecommunication networks. The architecture of the synthesized system is described, including modules for data collection, information processing and display of monitoring results. Particular attention paid to methods of detecting anomalies and preventing possible security threats.

Keywords: NMC, monitoring system, telecommunication network.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ 7
ВСТУП 9
1 АНАЛІЗ ХАРАКТЕРИТСИК ВІДОМИХ СИСТЕМ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ 12
1.1 Загальна характеристика цифрових телекомунікаційних мереж 12
1.2 Особливості вимірювання та контролю параметрів цифрових телекомунікаційних систем 15
1.3 Аналіз відомих систем контролю та моніторингу 17
2 АНАЛІЗ ХАРАКТЕРИСТИК НАДІЙНОСТІ СИСТЕМ КОНТРОЛЮ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ 26
2.1 Надійність обчислювальних компонентів засобів контролю цифрових телекомунікаційних мереж 26
2.2 Методи оцінки показників надійності програмно-апаратних комплексів моніторингу цифрових телекомунікаційних мереж 28
2.3 Аналіз надійності програмного забезпечення 36
3 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ 44
3.1 Структурна організація та особливості роботи первинного перетворювача системи 44
3.2 Модель обробки даних первинного цифрового потоку та визначення часу подій в системі моніторингу 48
3.3 Загальна архітектура системи моніторингу та управління 50
3.4 Структура програмного забезпечення системи моніторингу 54
4 ОХОРОНА ПРАЦІ 57
4.1 Технічні рішення щодо безпечного виконання роботи 57

4.2 Технічні рішення з гігієни праці та виробничої санітарії 60
4.2.1 Мікроклімат 60
4.2.2 Склад повітря робочої зони 60
4.2.3 Виробниче освітлення 61
4.2.4 Виробничий шум 62
4.2.5 Виробничі випромінювання 63
4.3 Розрахунок параметрів пожежної безпеки 63
4.3.1 Технічні рішення системи запобігання пожежі 64
4.3.2 Технічні рішення системи протипожежного захисту 65
ВИСНОВКИ 66
СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ 68
Додаток А (обов'язковий). Ілюстративна частина 72
Додаток Б (обов'язковий). Протокол перевірки кваліфікаційної роботи на наявність текстових запозичень 78

ПЕРЕЛІК СКОРОЧЕНЬ

АП – Аналізатор протоколів

АСТС – Аналізатор сигналізацій телекомунікаційних систем

АТС – Автоматична телефонна станція

БД – База даних

ЗнСО – Значуща сигнальна одиниця

ЗСО – Заповнююча сигнальна одиниця

ІВС – Інформаційно-вимірювальна система

ІМ – Інтерфейсний модуль

КЗ – Канал зв’язку

КЛС – Контролер ланок сигналізацій

ЛПК – Локальний пункт контролю

ЛПМ – Локальний пункт моніторингу

МПД – Мережа передачі даних

ПЗ – Програмне забезпечення

ПЗО – Програмне забезпечення обробки даних

ПП – Первинний перетворювач

ПС – Пункт сигналізації

ПЦП – Первинний цифровий потік

СКС7 – Спільноканальна сигналізація №7

СК – Система контролю

СО – Сигнальна одиниця

СУБД – Система управління базами даних

ТфЗК – Телефонна мережа загального користування

ЦАТС – Центральна автоматична телефонна станція

ЦК – Центр контролю

ЦП – Центральний процесор

ЦПК – Центральний пункт контролю

ЦТМ – Цифрова телекомунікаційна мережа

CCS – Cross Connect System (система цифрової кросової комутації)

IN – Intelligent Network (інтелектуальна мережа)

LTE – Long Term Evolution (четверте покоління мерж мобільного зв'язку)

OSI – Open System Interconnection (модель взаємозв'язку відкритих систем)

SCP – Service Control Point (вузол управління послугами)

SP – Signalling Point (пункт сигналізації)

SSP – Service Switching Point (вузол комутації послуг)

STP – Signalling Transfer Point (транзитний пункт сигналізації)

TMN – Telecommunication Management Network (мережа керування зв'язком)

5G – Fifth Generation (п'яте покоління мерж мобільного зв'язку)

ВСТУП

Актуальність. На сьогодні ми споглядаємо стрімкий прогрес у галузі телекомунікацій, що значно розширює інтелектуальні та комунікативні можливості людей завдяки доступу до великих обсягів інформації та можливості спілкування незалежно від місця та часу. Розвиток традиційних мереж електрозв'язку і систем телеобробки призвів до виникнення сучасних телекомунікаційних мереж, які дозволяють передавати різноманітну інформацію по одній мережі [1].

У контексті стрімкого розвитку технологій у сфері телекомунікацій та постійного збільшення потоків даних виникає потреба у надійному контролі та відстеженні цифрових телекомунікаційних мереж (ЦТМ). Важливою складовою для забезпечення їхньої ефективності та безпеки стає створення та впровадження програмно-апаратних засобів контролю та моніторингу [2].

Ця проблематика має велике значення у забезпеченні стабільності та надійності роботи телекомунікаційних мереж, що є критичним для багатьох сфер життєдіяльності сучасного суспільства. Тому розробка програмно-апаратних засобів контролю та моніторингу ЦТМ є важливим напрямком досліджень та розвитку.

Аналіз останніх досліджень. Останні наукові вивчення у галузі систем контролю та управління телекомунікаційними мережами розкрили ряд важливих тенденцій та напрямків розвитку.

1. Автоматизація та штучний інтелект. Значна увага зосереджена на розвитку систем, що базуються на штучному інтелекті та машинному навчанні, для автоматизації процесів контролю та управління. Це сприяє підвищенню продуктивності мережі та автоматизації процесів моніторингу та прогнозування її роботи [3].

2.Впровадження технологій SDN та NFV. Розробка та впровадження технологій SDN (Software Defined Networking) та NFV (Network Function Virtualization) значно трансформують підхід до управління мережами, надаючи можливість гнучко налаштовувати та оптимізувати їхню роботу [4].

3.Забезпечення безпеки мереж. У зв'язку з постійними загрозами кібербезпеки, активно ведуться дослідження у напрямку розробки систем контролю та управління, спрямованих на виявлення та запобігання кібератакам та іншим загрозам безпеки мережі.

4.Оптимізація мережевих ресурсів. Використання аналізу даних та прогностичних моделей дозволяє ефективно управляти мережевими ресурсами, мінімізуючи витрати та максимізуючи продуктивність [5].

Усі ці дослідження свідчать про перехід від традиційних методів управління до більш інтелектуальних, гнучких та безпечних систем, що відповідає вимогам сучасного телекомунікаційного середовища.

Метою даної кваліфікаційної роботи є аналіз та розробка програмно-апаратних комплексів для контролю та моніторингу цифрових телекомунікаційних мереж (ЦТМ).

Для досягнення поставленої мети необхідно виконати *такі задачі:*

- провести аналіз загальних характеристик ЦТМ;
- визначити та описати основні особливості вимірювання параметрів ЦТМ;
- виконати аналіз сучасного стану розвитку систем контролю та моніторингу цифрових телекомунікаційних мереж;
- описати методологію аналізу характеристик надійності системи моніторингу ЦТМ;
- виконати безпосередню розробку системи контролю та моніторингу цифрових телекомунікаційних мереж.

Об'єктом дослідження є програмно-апаратні засоби та системи контролю та моніторингу цифрових телекомунікаційних мереж.

Предметом дослідження є процес розробки, впровадження та оптимізації програмно-апаратних засобів для контролю та моніторингу ЦТМ з метою забезпечення їх ефективності, надійності та безпеки.

Методи досліджень базуються на використанні теорії мереж та систем мобільного зв'язку, методах вимірювань та оптимізації параметрів цифрових телекомунікаційних систем та мереж.

Новизна одержаних результатів полягає в наступному:

- проведено докладний аналіз надійності доступних засобів контролю телекомунікаційних мереж.
- представлено методи оцінювання показників надійності програмного забезпечення систем моніторингу;
- запропоновано структуру та функціональні особливості первинного перетворювача системи моніторингу;
- описано обробку сигналів первинного цифрового потоку системи моніторингу;
- запропоновано загальну архітектуру системи.

Практичне значення розробки дозволяє здійснювати постійний моніторинг роботи ЦТМ, виявляти проблеми та недоліки в реальному часі. Це сприяє підвищенню ефективності роботи мережі та покращенню якості обслуговування, дозволяє виявляти потенційні загрози для безпеки мережі та мінімізувати ризики порушень безпеки, зберігати конфіденційність даних.

Апробація результатів роботи. Основні ідеї роботи доповідались і обговорювались на LIII науково-технічній конференції підрозділів Вінницького національного технічного університету у 2024 році.

1 АНАЛІЗ ХАРАКТЕРИТСИК ВІДОМИХ СИСТЕМ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

1.1 Загальна характеристика цифрових телекомунікаційних мереж

Цифрові телекомунікаційні мережі (ЦТМ) можна класифікувати за різними ознаками, такими як призначення мережі, метод передачі сигналу, спосіб експлуатації та режим передавання. Класифікація телекомунікаційних мереж представлена на рис. 1.1 [3].

Рисунок 1.1 - Класифікація цифрових телекомунікаційних мереж

Для забезпечення доступу абонентів до основних послуг електрозв'язку за сучасних умов, коли дальність зв'язку та обсяги передаваної інформації стають все більше і більше, створення окремих мереж передачі даних і їхнє незалежне використання є надто витратним. Як вирішення цієї проблеми, може бути введення загальної мережі, яка охоплює всі види зв'язку, через типові канали передачі та групові тракти, що об'єднують всі точки введення та виведення інформації [3].

Основна мета телекомунікаційних мереж – забезпечити багатьом користувачам одночасний доступ до обчислювальних ресурсів. Таку мережу можна описати як систему розподіленої обробки інформації, що складається з комп'ютерів, розташованих на відстані один від одного, і взаємодіють між собою через засоби зв'язку. Комп'ютери, що входять до складу такої мережі, виконують різноманітні завдання, зокрема: забезпечення доступу до мережі; керування передачею інформації; надання обчислювальних ресурсів і послуг користувачам мережі [1].

Транспортні мережі призначені для передавання великих обсягів даних. Серед найпоширеніших на сьогоднішній день є, наприклад, Frame Relay та IP з технологією SDH (синхронна цифрова ієрархія).

За призначенням ЦТМ можна розподілити на мережі зв'язку, комп'ютерні, транспортні та інтелектуальні мережі.

Концепція Інтелектуальної Мережі (ІМ) представляє собою ключовий напрямок в розвитку сучасних мереж зв’язку. Зацікавленість у ІМ має обґрунтовані підстави, оскільки оператори мереж і абоненти одержують ряд переваг при впровадженні послуг ІМ, які також називають «послугами для додаткових доходів». Крім цього, дана концепція сприяла розвитку ринку засобів зв’язку, охоплюючи не лише виробників комутаційного обладнання, але й провідних виробників обчислювальної техніки та сучасних засобів обробки інформації [2].

Концепція ІМ формується вже протягом понад тридцяти років, а після випуску пакета рекомендацій серії Q.1200 в 1997 році Міжнародним союзом електрозв'язку (ITU-T), вона стала визнаним міжнародним стандартом, що підтримується практично всіма основними організаціями стандартизації зв'язку, такими як ETSI, ANSI та інші [5].

Відповідно до рекомендації ITU-T I.312/Q.1201, інтелектуальна мережа (ІМ) описується наступним чином. ІМ – це концепція архітектури, спрямована на надання нових послуг зв'язку, що володіє такими ключовими характеристиками:

- використання сучасних методів обробки інформації;
- ефективне використання ресурсів мережі;
- модульність і універсальність мережевих функцій;
- можливість розробки та впровадження послуг за допомогою модульних мережевих функцій;
- стандартизована взаємодія мережевих функцій через незалежні від послуг мережеві інтерфейси;
- можливість керування певними аспектами послуг з боку абонентів та користувачів;
- стандартизоване управління логікою послуг [6].

Залежно від методу передачі сигналу, мережі зв'язку можуть бути провідними, оптичними волокнами або безпровідними. У безпровідних мережах варто відзначити супутникові, радіочастотні та мобільні системи. Вибір конкретного методу передачі сигналу зазвичай залежить від ряду факторів, таких як відстань передачі, швидкість передачі, якість сигналу, пропускна здатність каналів і економічна доцільність.

Згідно з методом експлуатації, мережі зв'язку можуть бути класифіковані як комутовані, де канали надаються абонентам лише на час передачі повідомлень, та некомутовані, де канали призначені для конкретних абонентів. Зазвичай використовуються обидва ці підходи разом. Комутовані лінії можуть бути

механічними, електронними або використовувати пакетну комутацію. Механічна комутація майже не використовується в сучасних мережах зв'язку. Впровадження електронної комутації призвело до зменшення витрат на експлуатацію, економії простору та можливості розширення і зниження вартості обладнання.

Мережі з пакетною комутацією відрізняються від мереж з комутацією каналів тим, що джерело та призначення не взаємодіють в реальному часі. У таких мережах повідомлення можуть бути доставлені з певною затримкою, оскільки вузол призначення може бути зайнятий або не може прийняти навантаження з будь-якої причини. Вони не вимагають визначення стану вузла перед передачею повідомлення, як це відбувається в мережах з комутацією каналів [3].

При пакетній комутації, до кожного пакета додається заголовок, що містить адресу та іншу керуючу інформацію. Кожен пакет пересилається через мережу зберігаючи на проміжних вузлах. Призначений вузол збирає пакети у неперервне початкове повідомлення, яке потім передається користувачу[2].

1.2 Особливості вимірювання та контролю параметрів цифрових телекомунікаційних систем

Для вирішення завдань контролю мереж СКС на основі концепції TMN на організація МСЕ запропонувала об’єднати пункти сигналізації СКС7 з прикладною підсистемою ОМАР. Проте, різноманітність можливих реалізацій, яка дозволяється рекомендацією щодо TMN, і складність протоколу CMIP, що лежить в основі ОМАР та пропозиції МСЕ щодо підтримки взаємодії між мережевими елементами і системами експлуатаційного управління, призвели до того, що виробники комутаційного обладнання використовують для контролю елементів мережі СКС7, а також для дистанційного керування ними, власні, більш прості, але несумісні між собою протоколи [3].

Зазвичай це робиться спеціально, щоб уникнути можливості несанкціонованого доступу до управління власним обладнанням. Це призводить до труднощів у забезпеченні єдиного центру експлуатаційного управління пунктами сигналізації від різних виробників. Крім того, комутаційне обладнання, яке перебуває в режимі перевантаження, може неправильно відображати стан керованих ним елементів мережі СКС7, але саме ці моменти представляють найбільший практичний інтерес під час технічної експлуатації мережі [2].

У зв'язку з цим системи розподіленого моніторингу мережевих елементів, які ґрунтуються на пасивному з'єднанні моніторів сигналізації з ланками СКС7, стали широко поширеними на практиці.

На сьогоднішній день існує низка систем моніторингу мережі, таких як AcceSS7 від Hewlett-Packard, Network Wide View-7 від General Signal Networks, і QUEST7 від GN Nettest. Ці системи подібні за своєю структурою і функціональністю. Однак їх вартість надзвичайно висока (за неофіційною інформацією приблизно 50 млн. доларів для мережі Deutsche Telecom) [5].

Найбільш оптимальним варіантом використання у мережі, будь якого, оператора є системи управління мережею провідних виробників комутаційного обладнання, таких як 1300NMC від Alcatel, ETNA-NEM та NMAS від Ericsson, O&MS від Siemens, Net Minder і MFOS від Lucent Technologies та інші. Дані центри представляють собою комплексні системи контролю і управління елементами мережі і транспортною мережею в цілому [8].

При цьому, актуальним для операторів є питання розробки власної концепції системи моніторингу та управління, яка буде повністю відповідати вашій технічній та бізнес-моделям мережі зв’язку.

1.3 Аналіз відомих систем контролю та моніторингу

Спільноканальна сигналізація (СКС) в Україні була запроваджена недавно, в порівнянні з США та країнами ЄС, але уже на даний момент становить всього приблизно 15–20% міського і міжміського комунікаційного трафіку. У мережі СКС України є особливість у використанні застарілих ліній у вигляді пучків витих пар з пропускною здатністю 2,048–8,192 Мбіт/с, а також оптичних ліній з пропускною здатністю до 600 Мбіт/с [1].

Лінії першого типу та оптичні лінії експлуатуються такими операторами як Укртелеком, Vodafone, Lifecell, Київстар. Проте лише частина обладнання в мережі представляє собою інтелектуальні системи, які здатні реалізувати протоколи СКС, а більшість комунікаційних систем виконана у вигляді кінцевих автоматів, таких як «ІКМ-120» [9].

На рис. 1.3 представлено узагальнену структуру інформаційно-вимірювальної системи (ІВС).

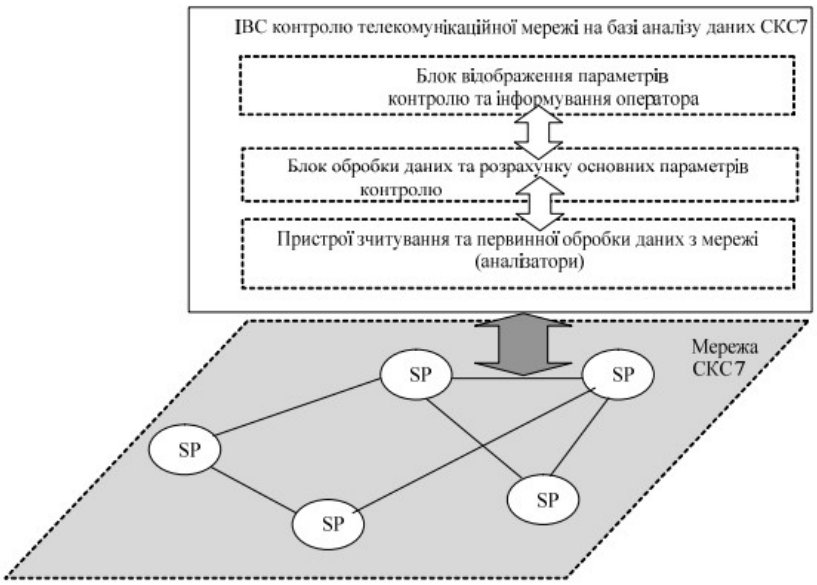

Рисунок 1.2 – Узагальнена структура ІВС

Нерівномірність обладнання, що вироблене з різними вимогами до параметрів, призводить до того, що основна мережа стає плезисинхронною, що в свою чергу породжує проблему синхронізації прийому даних у системі моніторингу для кожного контрольованого пункту сигналізації [8].

На відміну від комутаційних систем, де кожну помилку передачі можна виправити через повторну передачу, система моніторингу не може компенсувати похибки, спричинені короткочасною девіацією несучої частоти, за пасивного паралельного підключення. Тому вона повинна працювати асинхронно і мати здатність адаптуватися до кожного каналу передачі даних, який вона контролює. Хоча вона може повністю усунути помилки при втраті з'єднання в лінії, але такий метод, якщо немає нагальної необхідності через інші застосування, не є бажаним для використання у загальній комутаційній мережі [10].

Взаємодія між телекомунікаційними системами базується на обміні ініціюючими сигнальними пакетами, що містять запити на послуги, та сигнальними пакетами підтвердження, які містять позитивні або негативні відповіді на запити. Ускладнення визначення часу взаємодії сигнальних повідомлень та ідентифікації з'єднань системою моніторингу виникає з того, що як у локальних, так і в глобальних телекомунікаційних мережах ініціюючі пакети та пакети підтвердження можуть передаватися через віртуальні маршрути, які працюють на різних фізичних апаратних засобах.

Оскільки моніторинг і тестування можуть проводитися не лише на кінцевих пунктах повідомлень (у пунктах встановлення з'єднань), але й на транзитних пунктах мережі, для уникнення ситуацій, коли час реєстрації пакета підтвердження менший за час ініціюючого пакета, таймери пристроїв системи моніторингу на всіх сигналізаційних пунктах мережі повинні бути синхронізовані. Цю синхронізацію таймерів можна здійснювати на рівні обладнання, яке приймає сигналізаційні пакети, або на рівні серверів, які архівують і групують пакети за їх взаємозв'язком [3].

Максимальна допустима похибка визначення часу не повинна перевищувати часу реакції комутаційного обладнання на запит. При аналізі даних моніторингу з урахуванням зростання пропускної здатності комунікаційних систем і зростання швидкості передачі даних, похибка синхронізації не повинна перевищувати 1 мс, оскільки, наприклад, час взаємодії пакетів сигналізації СКС7 на найбільш розвинутому комутаційному обладнанні мобільних операторів може бути приблизно 3-5 мс [4].

На рис. 1.3 показано типову блок-схему роботи системи моніторингу [3].

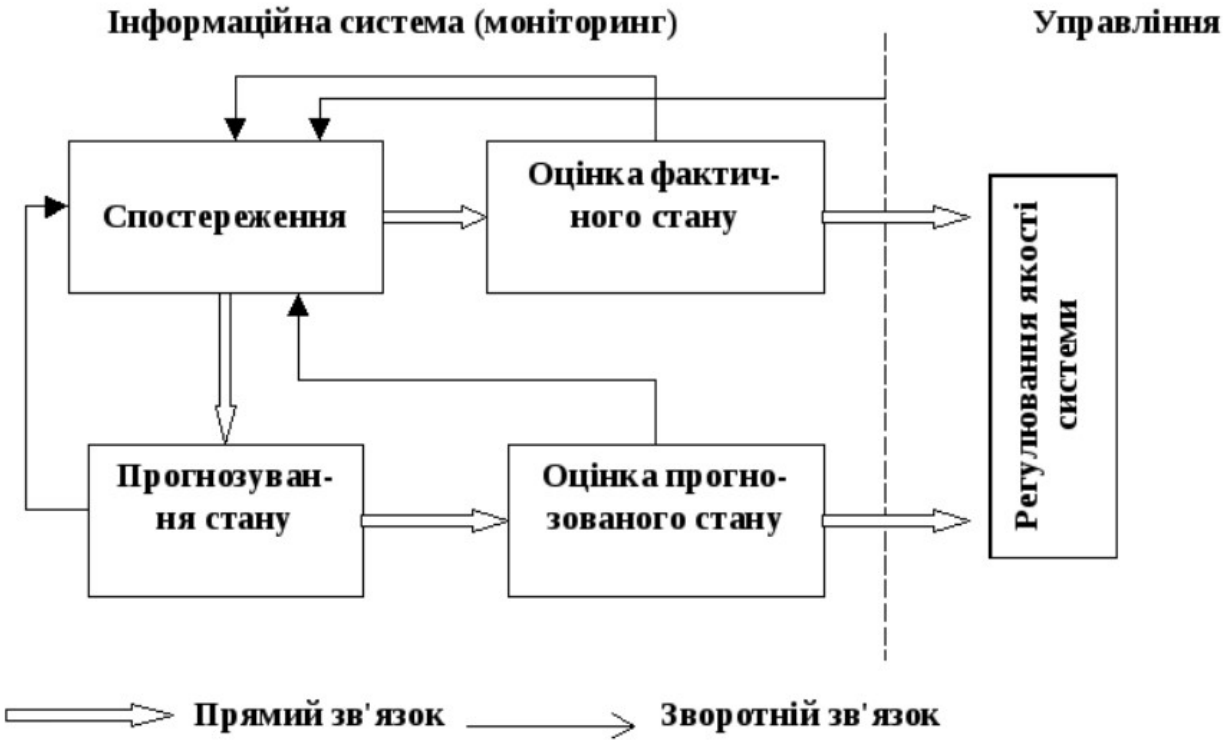

Рисунок 1.3 – Принцип роботи системи моніторингу

Існують спеціальні протоколи для синхронізації часу на рівні серверів, такі як NETworkTime. Проте доступ до первинних даних до сервера може включати кілька етапів обміну, що призводить до значної затримки, обумовленої

завантаженням обладнання та пріоритетністю виконуваних завдань. Тому краще визначати час за допомогою обладнання, яке реєструє дані. Для цього використовують приймачі GPS, які надають значення часу з точністю до секунди та сигнал синхронізації секунди 1PPS [3].

Точність визначення часу залежить від часу реакції на сигнал 1PPS. Цей сигнал передається приймачем через один із стандартних інтерфейсів, зазвичай RS232, що дозволяє йому бути доступним для прийому без будь-якого додаткового обладнання на будь-якому існуючому сервері. Таким чином, визначення часу прийому пакетів на рівні комп'ютера може мати велику похибку і не є прийнятним для системи моніторингу.

Одним з завдань моніторингу є проведення досліджень та аналізу ефективності топології мережі, а також її оптимізація на основі моделі передачі даних. Головним критерієм для оцінки моделі є середнє значення T_{Σ} та дисперсія σ_{Σ}^2 затримки сигнальних повідомлень у ланках мережі, визначені виразами (1.1 та 1.2) [3].

$$T_{\Sigma,}^{i,j} = \sum_{u_{kl} \in U(i,j)} \frac{1}{2}\left(T_{fkl} + \frac{a_{eff_{kl}}}{1 - a_{eff_{kl}}} \frac{T_{vir_{kl}}^{(2)}}{T_{vir_{kl}}^{(1)}} \right) + T_{vir_{kl}}^{(1)} - \left(T_{EK_{kl}} - T_{EП_{kl}} \right), . \qquad (1.1)$$

$$\sigma_{\Sigma,}^2 (i,j) = \sum_{u_{kl} \in U(i,j)} \left(\frac{T^2{}_{fkl}}{12} + \frac{1}{4}\left(\frac{a_{eff_{kl}}}{1 - a_{eff_{kl}}} \frac{T_{vir_{kl}}^{(2)}}{T_{vir_{kl}}^{(1)}}\right) \right)^2 + T_{vir_{kl}}^{(2)} + \frac{1}{31} \frac{a_{eff_{kl}}}{-a_{eff_{kl}}} \times$$
$$\times \frac{T_{vir_{kl}}^{(3)}}{T_{EK_{kl}} - T_{EП_{kl}}} - \left(T_{vir_{kl}}^{(1)} \right) + \left(T_{EK_{kl}} - T_{EП_{kl}} \right)^2 (1 - k_1). \qquad (1.2)$$

Очевидно, що модель може адекватно відображати динаміку взаємодії ланок сигналізації, що ураховується в умовах, коли відбуваються похибки в оцінках

часу передачі *і-м* пунктом сигналізації $(ПС_i)$ $\triangle t_i$ і прийому $(ПС_j)$ $\triangle t_j$ в сумі значно менші за T_Σ , тобто [3]:

$$t_i + t_j << T_\Sigma \ . \tag{1.3}$$

Для задоволення цієї умови, поставимо завдання визначення часу з певною похибкою, дисперсія якої буде визначена [3]:

$$\sigma^2_{\triangle t} + \sigma^2_\Sigma \ . \tag{1.4}$$

Отже, сформульовано дві основні вимоги до синхронізації даних та часу у системі моніторингу:

- прийом даних має відбуватися асинхронно з адаптацією до кожного з каналів окремо;

- визначення часу прийому даних і синхронізація його з мітками часу системи GPS має здійснюватися на рівні обладнання, що приймає дані і працює як кінцевий пристрій.

Давайте розглянемо відомі системи моніторингу та перевіримо їх відповідність зазначеним вимогам.

Компанія Inet Technologies, Inc. (США) є провідним розробником систем моніторингу. Наразі її системи широко використовуються багатьма телекомунікаційними операторами у США, Канаді, а також BundesTelecom та іншими. Системи цієї компанії реалізовані у вигляді мережі пристроїв GeoProbe. Загальна конструкція пристрою, яка представлена на рис. 1.5, є типовою для більшості подібних систем. Вона містить центральний процесор у форматі Industrial PC зі стандартним набором портів та інтерфейсів для зберігання та обміну даними, що відповідає за реєстрацію даних та служить сервером.

На рис. 1.4 представлено узагальнений склад пристрою для систем моніторингу [12].

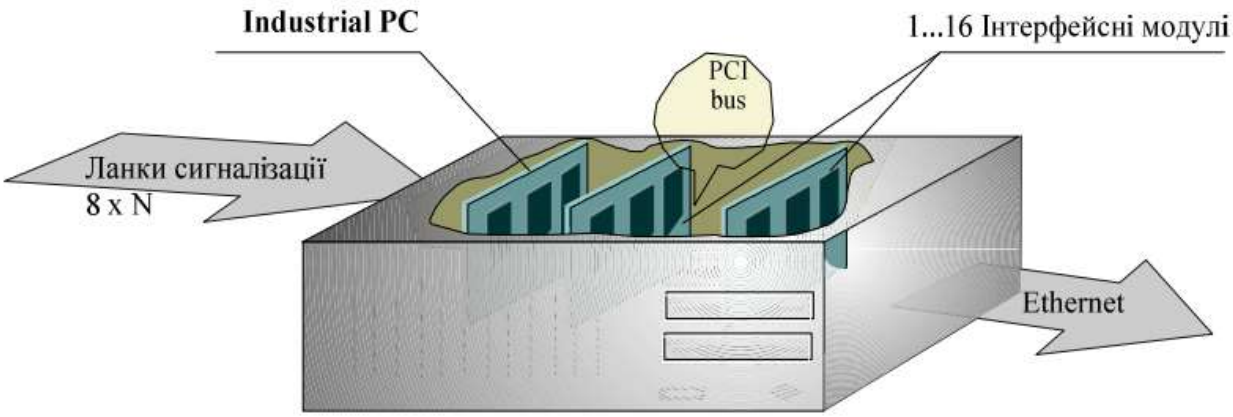

Рисунок 1.4 – Загальна компоновка пристрою для системи моніторингу

Крім того, до складу пристрою входить від одного до шістнадцяти інтерфейсних модулів (ІМ), які призначені для з'єднання з лініями зв'язку та з центральним процесором за допомогою стандартних інтерфейсів.

Інтерфейсні модулі відповідають за первинну обробку ПЦП, що полягає в вибірці пакетів даних. За допомогою об'єднувальної панелі та шини PCI ці модулі підключаються до центрального процесора. Залежно від кількості потоків E1/T1/J1 та їхнього місця розташування систему моніторингу конфігурують з використанням відповідного числа пристроїв. Пристрої об'єднуються в мережу за допомогою Ethernet-портів, що входять до складу центрального процесора.

Відома система моніторингу від компанії Telesoft-technologies (США) базується на мережі пристроїв ANSTY 4000 Monitoring Probe. Розглянемо детальний опис цього пристрою, оскільки його конструктивні особливості є спільними з GeoProbe від Inet та іншими системами. ANSTY-4000 складається з центрального процесора, який має порти Ethernet, RS232 і порт керування та відображення, а також від одного до шістнадцяти інтерфейсних модулів (ІМ)

MPAC2400, що з'єднані між собою та з центральним процесором за допомогою шини PCI.

Кожен інтерфейсний модуль включає в себе системний процесор і цифровий сигнальний процесор (DSP), восьмипортовий інтерфейсний блок для стандартів E1/T1 (E1/T1 Interface) і комутаційну матрицю (Switch matrix). Системний процесор, за допомогою шини адрес (AD) та блока мосту (PCI bridge), з'єднаний з системною шиною ЦП стандарту PCI, яка має формат Compact PCI. Зовнішні аналогові входи та виходи інтерфейсних блоків призначені для підключення до ліній E1/T1, що контролюється системою моніторингу. Цифрові входи та виходи підключені до першої групи виходів і входів комутаційної матриці, яка відповідає за комутацію канальних інтервалів E1/T1, до другої і третьої груп входів і виходів, які підключені до системного і сигнального процесорів [3].

Системний процесор включає в себе порт Ethernet і блок постійної пам'яті, що дозволяє використовувати цей інтерфейсний модуль як частину системи з декількома модулями, які керуються центральним процесором, так і у самостійному режимі, де він управляється через порт Ethernet. У самостійному режимі блок постійної пам'яті використовується для ініціалізації системного і сигнального процесорів. Сигнальний процесор відповідає за прийом та передачу сигнальних пакетів, тоді як системний процесор здійснює обробку цих пакетів за допомогою високорівневих протоколів (для СКС7 - MTP3, ISUP, TCAP, SCCP і інші, див. рекомендації ITU Q.704 - Q.780, MAP рекомендації GSM 09.02) [12].

Однією з недоліків цієї структури є можливість втрати даних, якщо частота синхронізації комутаційної матриці несправно відповідає частоті синхронізації вхідних потоків даних через дрейф (jitter).

Ще одним недоліком є те, що використання системного процесора в кожному ІМ призводить до ускладнення пристрою і збільшення витрат, оскільки системний процесор може бути надто продуктивним порівняно з системним та сигнальним процесорами. У даному пристрої, як системний процесор

використовується мікропроцесор MPC860, який працює на частоті 66 МГц, тоді як системний процесор може мати частоту 3000 МГц або більше, тому системний процесор необхідний лише у разі, якщо ІМ працює в автономному режимі.

Розподілення обробки протоколів високого рівня на системні процесори декількох ІМ також невиправдане, оскільки значна частина сигнальних потоків транспортується через віртуальні канали з використанням різних фізичних носіїв. Це може призвести до ситуацій, коли пакети одного з'єднання отримані різними ІМ, і для відновлення шляху з'єднання (CDR) потрібно організувати обмін даними між ІМ. Структура ІМ представлена на рис. 1.5 [3].

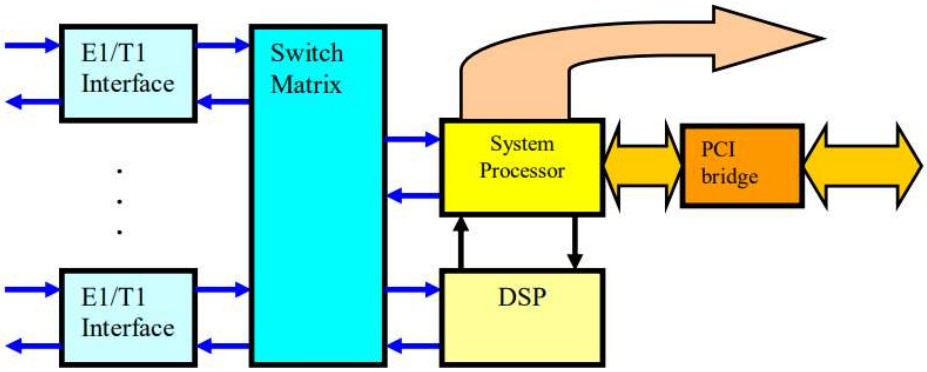

Рисунок 1.5 – Загальна структура інтерфейсних модулів пристроїв прототипів

Одним з основних недоліків розглянутих систем є відсутність жорсткої синхронізації часу прийому сигнальних повідомлень. Хоча час може бути синхронізований за допомогою приймачів точного часу, підключених до стандартних портів, що обслуговуються операційною системою, це може викликати значні помилки у визначенні моменту реєстрації сигнальних повідомлень, як показано вище. Ще одним важливим недоліком є те, що існуючі системи не були розроблені з урахуванням показників надійності центральної

системи управління трафіком (ЦТМ). Наразі відсутні методології надійного проектування інтегрованих вузлів системи ЦТМ, що стає необхідним, оскільки під час розробки інтегрованих вузлів системи необхідно враховувати високу надійність самої ЦТМ [3].

Висновок. На підставі огляду провідних наукових розробок можна визначити, що для розробки систем та пристроїв для моніторингу важливо вирішити наступні завдання:

- подолання впливу плезисинхронності телекомунікаційних мереж на точність прийому сигнальних повідомлень шляхом адаптації до параметрів кожного з вимірювальних каналів та розроблення програмно-апаратного розподілення процесів прийому даних та їх обробки незалежно від особливостей кожного каналу;

- забезпечення жорсткої синхронізації часу по всій системі моніторингу для уникнення помилок у формуванні маршрутів з'єднань у швидкодіючих комутаційних мережах за допомогою методу кінцевих автоматів, що працюють в реальному часі;

- врахування показників надійності роботи інтегрованої системи вузлів комутації при її проектуванні.

Використання наявних інструментів контролю цифрових телекомунікаційних мереж не забезпечує повного вирішення завдання контролю основних параметрів цифрової телекомунікаційної мережі. Це пояснюється наявністю їхніх недоліків та відсутністю урахування особливостей національної версії СКС7. З огляду на викладене, стає очевидним, що важливою та актуальною є задача розробки інтегрованої системи для контролю цифрової телекомунікаційної мережі, яка б забезпечила одночасне визначення основних параметрів мережі та врахування національної специфікації СКС7.

2 АНАЛІЗ ХАРАКТЕРИСТИК НАДІЙНОСТІ СИСТЕМ КОНТРОЛЮ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1 Надійність обчислювальних компонентів засобів контролю цифрових телекомунікаційних мереж

Надійність програмного забезпечення (ПЗ), як складової частини обчислювальної системи, визначається його безперебійним функціонуванням і здатністю до відновлення. Безперебійність ПЗ можна оцінити за середнім часом між виникненням відмов при його роботі, враховуючи, що обчислювальна система перебуває у справному стані. Під відмовкою ПЗ розуміється неприпустиме відхилення характеристик функціонування програми від встановлених вимог [3].

Період спостереження визначає час, необхідний для виконання задачі на електронно-обчислювальній машині (ЕОМ).

Основна відмінність програмного забезпечення (ПЗ) від апаратного полягає у тому, що програма не піддається зношуванню. Таким чином, надійність функціонування ПЗ залежить виключно від його якості, яка визначається процесом розробки. Вхідні дані не впливають на відмови апаратури, але значно впливають на роботу ПЗ. Інтенсивність відмов апаратури не залежить від тривалості експлуатації (після періоду пробного запуску) [14].

Підвищення надійності програми є результатом виявлення прихованих помилок програми під час її експлуатації. Відновлюваність ПЗ визначається часом, необхідним для усунення відмов та їх наслідків. Стійкість функціонування ПЗ полягає в його здатності обмежувати наслідки помилок або протистояти їм.

На рис. 2.1 представлено приклад виведення результатів оптимізації для випадку задання $T_{0\min}$.[15]

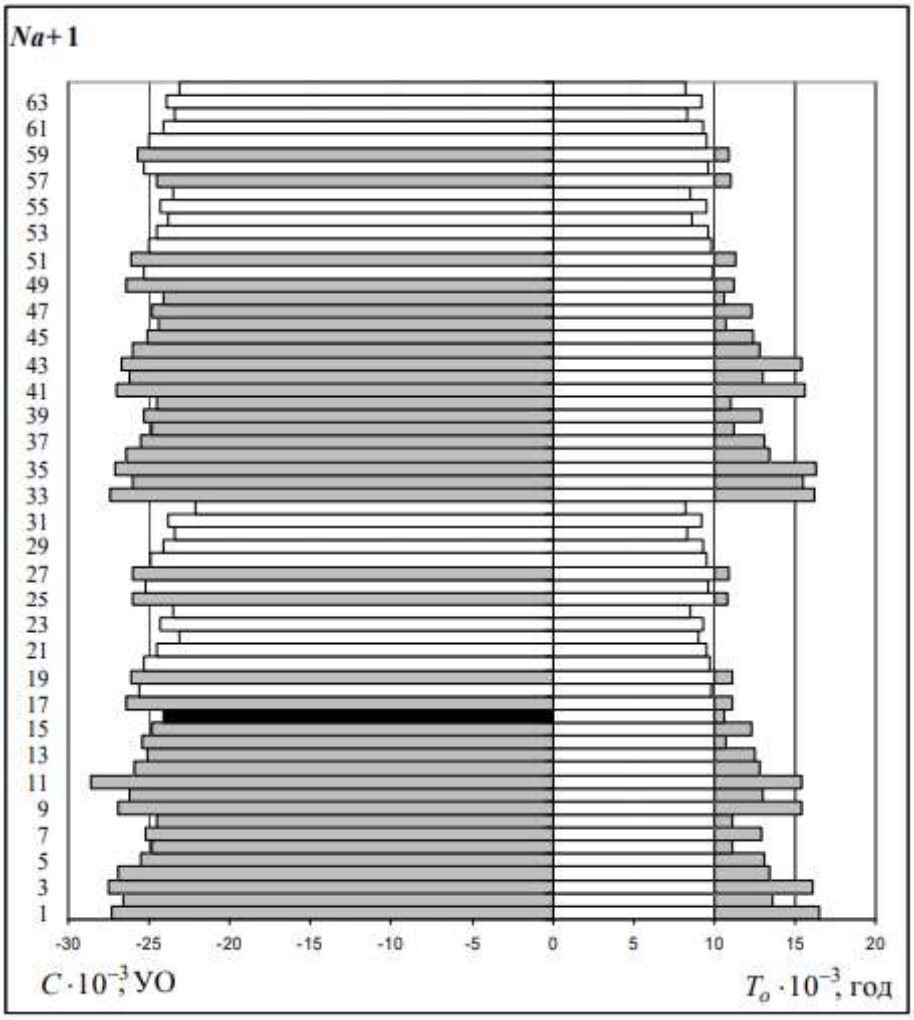

Рисунок 2.1 – Виведення результатів оптимізації

Результати оптимізації:

$T_{0\min} = 10^4$ *годин*,

$C_{\min} = 24080\,УО.$

Номер структури $N_a = 15$.

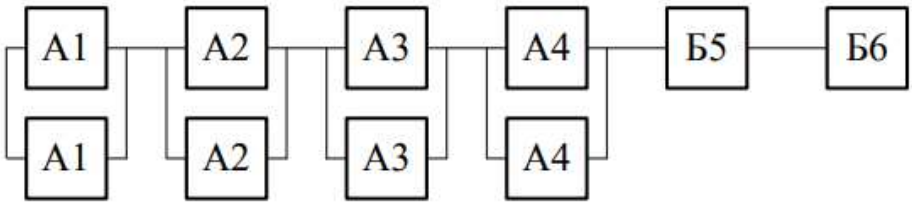

Рисунок 2.2 – Схема структури процесу оптимізації [16]

Як було відзначено раніше, завдання оцінки надійності програмного забезпечення включає наступні аспекти:

- оцінка та контроль статистичних властивостей вихідних текстів програми;
- створення аналітичної моделі надійності програми для оцінки показників надійності під час тестування;
- розробка моделі надійності для великих програмних комплексів.

2.2 Методи оцінки показників надійності програмно-апаратних комплексів моніторингу цифрових телекомунікаційних мереж

До статистичних параметрів, які впливають на складність розробки програмного забезпечення (ПЗ), входять довжина вихідного тексту програми, об'єм цього тексту, рівень якості ПЗ і використана мова програмування. Ці параметри визначають різні аспекти, такі як умовну робочу ємність для програмування, час, потрібний для розробки, інтелектуальний вміст програми, а також передбачувану кількість перших помилок у вихідних текстах програм і прогнозовану кількість помилок для нових програм. Оцінка характеристик надійності програм, базована на вихідних текстах, здійснюється на основі емпіричних даних, отриманих під час тестування програм [16].

Під час аналізу у програмах були виявлені типові види помилок, такі як помилки в обчисленнях, логічні помилки, помилки в операціях введення-

виведення, маніпулюванні даними, взаємодії, операції з базою даних та операційною системою. Також було встановлено розподіл помилок за їх типами, причому виявлено, що найбільша частка помилок пов'язана з проектуванням програм. Також, проведено аналіз залежності кількості помилок від розміру програмного модуля, з виявленням, що більші модулі містять більше помилок, при цьому оптимальна лінійна оцінка варіюється від 10 до 20 помилок на кожні 1000 операторів вихідного тексту. У джерелі також наводяться дані, що до початку системного тестування на кожну тисячу операторів у програмному забезпеченні припадає приблизно десять помилок [15].

Рівень прийнятної надійності для початку експлуатації вважається таким, коли на кожну тисячу операторів програмного коду припадає приблизно одна помилка, тобто $N_{пом} = 10^{-3} V_{оп}, де\, N_{пом}, V_{оп}$ - число помилок та операторів у програмі відповідно.

Отже, можливо визначити кількість помилок після розробки за виразом [3]:

$$N_{пом} = K_H V_{оп} \log_2(\eta_1 + \eta_2), \tag{2.1}$$

де $K_н$ – коеф. пропорційності; η_1, η_2 - число відмінних операторів та операндів у програмі.

Значання коефіцієнта $K_н$ залежить від виду програми, для лінійних програм $K_H = 1/3000,$ для розгалужених - $K_H = 1/750.$

Пропонується використовувати метод експертних оцінок для аналізу помилок програмного забезпечення. Суть цього методу полягає у тому, що кількість помилок визначається шляхом усереднення даних, отриманих за допомогою різних методик. Імовірність виявлення програмної помилки обчислюється за відповідною формулою [3]:

$$P_{пом} = 1 - \exp(-N_{пом}). \quad (2.2)$$

Імовірності невияву програмних помилок в програмних модулях:

$$P_{поі} = 1 - P_{пом} N_i / N_{пом}, \quad (2.3)$$

де N_i – кількість помилок в *і-му* програмному модулі.

Отримані дані використовуються як вихідна інформація для розробки стратегії тестування та вибору методів налагодження програмного забезпечення. Аналітичні моделі надійності програмного забезпечення формуються під час тестування. Потреба у їх створенні пояснюється тим, що емпіричні моделі є досить узагальненими. Різниця між прогнозованими кількостями помилок та фактичними результатами може бути значною. Крім того, емпіричні моделі не враховують динаміку обчислювального процесу під час експлуатації програми.

У практиці використовуються два типи аналітичних моделей для оцінки надійності програмного забезпечення: статистичні і імовірнісні. У статистичних моделях оцінка надійності програмного забезпечення також пов'язана з кількістю програмних помилок за допомогою відносних співвідношень, які визначаються статистичними методами, і при цьому не вносяться жодні припущення про розподіл.

Згідно з методом Мілса для розглянутого програмного забезпечення випадковим чином вводиться певна кількість відомих помилок, і припускається, що темп виявлення власних помилок у програмі та введених є однаковим. Тоді кількість власних помилок програмного забезпечення визначається:

$$N_{пом} = n_{пом} N_{вн} / n_{вн},$$

де $N_{вн}$ - кількість введених помилок, з яких виявлено $n_{вн}$; $n_{пом}$ - кількість виявлених власний помилок ПЗ.

Модель передбачає, що в програмному забезпеченні існує багато джерел програмних відмов, які пов'язані з різними видами помилок та мають різні імовірності появи. Основним аргументом цієї моделі є кількість прогонів програми, позначена як n. Відповідно до цього, оцінка надійності програмного забезпечення представляє собою формулу або вираз [17]:

$$R(n) = \left(n^{+} / n\right) + \sum_{k} \delta_k \left(n_{помк} - 1\right) / n, \tag{2.4}$$

де n^{+} - кількісь успішних прогнозів ПЗ; $n_{помк}$ - кількість знайдених помилок *к-го* типу, які можна усунути з ймовірністю p_k, причому

$$\delta_k = \begin{cases} \rho_k \, при \, n_{помк} > 0, \\ 0 \, при \, n_{помк} = 0. \end{cases} \tag{2.5}$$

Метод паралельного тестування включає участь двох незалежних груп спеціалістів, які кожна використовує власну стратегію для виявлення помилок. При цьому припускається, що множина помилок, виявлених обома групами $ERR = ERR1 \cup ERR2$, де $ERR1, ERR2$ - відповідно підмножини помилок, причому $ERR1 \setminus ERR2 = \varnothing$.

Показник ефективності тестування груп $E_1 = N_{пом1} / N_{пом}$ і $E_2 = N_{пом2} / N_{пом}$, де $N_{пом}$ - загальна кількість помилок, а $N_{пом1}$ та $N_{пом2}$ - потужності підмножин $ERR1, ERR2$ відповідно [3].

На підставі зазначених припущень отримуємо вираз [3]:

$$N_{пом} = N_{пом12} / E_1 E_2, \tag{2.6}$$

де $N_{пом12}$ - потужність множини $ERR1 \cap ERR2$.

У найбільш комплексних імовірнісних моделях розглядаються випадкові процеси виявлення та прояву дефектів та відмов програмного забезпечення. Основні умови в моделі Шумана можуть бути узагальнені таким чином:

1) При налагоджені ПЗ є E_T помилок. Протягом часу налагодження τ усувається $\varepsilon_c(\tau)$ помилок з розрахунку на 1-ну команду.

2) Припускається, що значення функції частоти відмов *z(t)* залежить від кількості помилок, що залишилися після часу налагодження τ, тобто $z(t) = c \cdot \varepsilon_r(\tau)$. Тоді імовірність безвідмовної роботи протягом інтервалу (*0,t*) дорівнює [3]:

$$R(t,\tau) = \exp\left\{-c\left[E_T / I_T - \varepsilon_c(\tau)\right]t\right\}. \tag{2.7}$$

У моделі Джелінського–Моранді припускається, що інтервали часу налагодження мають експоненційний розподіл, де частота помилок пропорційна кількості невиявлених дефектів. Функція щільності розподілу часу виявлення *i-ї* помилки має наступний вигляд [18]:

$$P(t_i) = \lambda_i \cdot e^{-\lambda_i t}, \tag{2.9}$$

де $\lambda_i = \Phi(N - i + 1), N$ - початкове число помилок.

Для визначення оцінок максимальної ймовірності N та Φ потрібно розв'язати наступну рівність[18]:

$$\begin{aligned} &\sum_{i=1}^{k}\left(\widehat{N}-i+1\right)^{-1}=k/\left(\widehat{N}+1-\theta k\right), \\ &\widehat{\Phi}=\frac{k/A}{\widehat{N}+1-\theta k}. \end{aligned} \tag{2.10}$$

Модель Муси відома як одна з провідних імовірнісних моделей, що базується на припущенні про експоненційний розподіл кількості помилок у програмі з плином часу. У цій моделі враховується загальний час функціонування τ, що визначається від моменту тестування програми до моменту, коли оцінюється її надійність. Припускається, що помилки у програмі є незалежними та виявляються з постійною інтенсивністю. Це означає, що інтервали між відмовами розподіляються за експоненційним законом, і параметр цього розподілу змінюється після виправлення помилки [3].

Основна відмінність даної моделі від попередніх полягає у тому, що інтенсивність відмов моделюється як неперервна функція, що спрощує математичне уявлення. Нехай $N_{пом}$ - кількість помилок в програмі перед тестуванням; $m(\tau)$ - кількість виправлених помилок; $m_0(\tau)$ - залишкові помилки. Тоді:

$$m_0(\tau)=N_{пом}-m(\tau). \tag{2.11}$$

Звідси робимо висновок, що інтенсивність відмов є пропорційною $m_0(\tau)$:

$$\lambda(\tau)=C\cdot m_0(\tau), \tag{2.12}$$

де С – коефіцієнт, який враховує швидкодію та кількість команд в програмі.

Якщо можливості щодо виправлення помилок *dm/dt* дорівнюють можливостям їх виявлення, то маємо:

$$dm/dt = \lambda(\tau) \tag{2.13}$$

Розв'язавши разом вирази 2.12 та 2.13, отримуємо:

$$(dm/dt) + Cm = CN_{пом}. \tag{2.14}$$

Середній час безвідмовної роботи після тестування протягом часу τ складає $\overline{T}_0 = 1/\lambda(\tau)$.

Таким чином:

$$\overline{T}_0 = (1/CN_{пом})\exp(-C_\tau). \tag{2.15}$$

Моделі обмежено через:

- обмежений доступ до інформації про налагодження програм та усунення помилок;

- низька інтенсивність програмних збоїв у випробуваннях, що ускладнює оцінку параметрів моделей;

- неможливість усунення всіх виявлених помилок на етапі супроводження;

- відсутність загального закону розподілу даних про програмні помилки з різних проектів.

Необхідність використання моделей надійності програмного забезпечення з системно незалежними аргументами виникає з того, що основою таких моделей, зокрема моделі Нельсона, є припущення про те, що область S_0 значень векторів

вхідних даних $Y^{(0)}$ складається з двох підмножин. $S_0 = S_0^+ U S_0^-$, *де* S_0^+ - дані, що спричиняють збій у роботі програми; S_0^- - решта.

Оскільки визначення набору $Y^{(0)}$ є по суті випадковим, то кожен m-ий прогін ПЗ з ймовірністю Q_m закінчується відмовою. При проведенні n прогонів програми формула ймовірності безвідмовного функціонування програмного забезпечення виглядає наступним чином [16] :

$$R(n) = \prod_{m=1}^{n} (1 - Q_m) = \exp\left\{ \sum_{m=1}^{n} \ln(1 - Q_m) \right\}. \quad (2.16)$$

Процес знаходження значення Q_m засновано на розрахунку функціонального розподілу програми – розподіл імовірності $\rho(i,m)$ для обрання певного вектору $Y^{(0)}$ під час виконання m-го прогону ПЗ [16]:

$$Q_m = \sum_{i=1}^{S_0} p(i,m) l_i. \quad (2.17)$$

Очевидно, що функціональний аспект програми визначається конкретними умовами її реального використання. Переваги моделі Нельсона, які роблять її корисною на завершальних етапах життєвого циклу програмного забезпечення, включають:

- врахування динаміки роботи програмного забезпечення в реальному операційному середовищі;

- відсутність припущень щодо характеристик операційного середовища та умов експлуатації ПЗ;

- відсутність припущень щодо причин програмних збоїв;

- необов'язковість мати інформацію про стан програмного забезпечення та динаміку процесів на початкових етапах його життєвого циклу;

- використання методів теорії ймовірностей лише у випадку відсутності можливості отримати детерміновані оцінки параметрів [3].

Одночасно з тим використання моделі Нельсона на практиці викликає певні складнощі пов'язані з знаходженням ймовірностей $p(i,m)$, а отже і Q_m, особливо для масштабних ПЗ.

Для прогнозування надійності великих програмних комплексів можна використовувати марківську модель. Надійність усього програмного комплексу визначається як функція надійності його складових частин. Мірою надійності програмного модуля є ймовірність його коректного виконання. Кожному набору вхідних даних, що надходить на вхід програми, відповідає певна послідовність модулів. Таким чином, надійність програмного комплексу залежить від послідовності виконуваних модулів та надійності кожного модуля.

2.3 Аналіз надійності програмного забезпечення

Для оцінки кількості помилок, що очікуються під час роботи ПЗ використовують модель Холстеда. Число помилок $N_{пом}$ в програмі визначається за формулою (2.1), а ймовірність появи даних програмних помилок – за (2.2). Імовірність відсутності програмних помилок у кожному окремому модулі програми за виразом (2.3) [3].

Для оцінки кількості помилок у програмному комплексі системи контролю потрібно виконати наступні кроки:

1. Введення даних. Число операторів та операндів в кожному програмному модулі V_{on}; кількість типів операторів і операндів $\eta 1$ і $\eta 2$; тип програми – лінійна або розгалужена.

2. Визначення кількості очікуваних помилок N_i в кожному модулі.

3. Визначення загального числа помилок в програмі за виразом $N_{пом} = \sum_{i=1}^{n} N_i$, де n – кількість програмних модулів в програмному комплексі.

Результати розрахунків наведені в табл. 2.1.

Таблиця 2.1 - Результати розрахунку кількості програмних помилок на основі статистичного аналізу

Параметр	Номер програмного модуля														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Кількість операторів і операндів $\times 10^{-3}$	85,2	2,01	1,13	16,1	16,4	3,99	24,9	31,9	16,1	16,4	11,3	3,99	18,9	31,9	12,6
Кількість типів операторів і операндів	120	65	50	100	100	60	120	120	100	100	80	60	65	120	50
Кількість помилок в програмному модулі	196	4	2	35	36	8	57	73	35	36	23	8	39	73	24
Кількість помилок в програмному комплексі	649														

Щільність розподілу часу виявлення *i*-ої помилки [3]:

$$P(t_i) = \lambda_i e^{-\lambda_i t_i}. \qquad (2.18)$$

Ймовірність відсутності помилок після завершення *i*-го інтервалу тестування [3]:

$$P(t_i) = 1 - e^{-\lambda_i t_i}, \tag{2.19}$$

де $\lambda_i = \Phi(T - i + 1)$ інтенсивність помилок після прояву *i*-ї помилки.

Для визначення параметрів Ф та N потрібно розв'язувати рівність [3]:

$$\Phi = \frac{K / A}{N + 1 - K\varnothing}, \tag{2.20}$$

$$\frac{K}{N + 1 - K\varnothing} = \sum_{i=1}^{M} \frac{M_i}{N - n_{i-1}}. \tag{2.21}$$

Модель Моранди – Джелінського:

$$A = \sum_{i=1}^{M} t_i, \tag{2.22}$$

$$B = \sum_{i=1}^{M} (n_{i-1} + 1) t_i. \tag{2.23}$$

Для моделі Волвертона вирази набувають вигляду:

$$A = \sum_{i=1}^{M} t_i (T_{i-1} + t_i / 2), \tag{2.24}$$

$$B = \sum_{i=1}^{M} (n_{i-1} + 1) t_i (T_{i-1} / t_i / 2). \tag{2.25}$$

Якщо всі часові інтервали дорівнюють t_0 , тоді вирази для розрахунків коефіцієнтів A та B набувають більш спрощеного вигляду. Модель Моранди – Джелінського [3]:

$$A = Mt_0, \tag{2.26}$$

$$B = t_0 \sum_{i=1}^{M} (n_{i-1} + 1). \tag{2.27}$$

Для моделі Волвертона вирази набувають вигляду [3]:

$$A = t^2{}_0 \sum_{i=1}^{M} (i - 0,5), \tag{2.28}$$

$$B = t^2{}_0 (n_{i-1} + 1)(i - 1). \tag{2.29}$$

На рис. 2.3 наведено графіки ймовірностей P(t_i) [15].

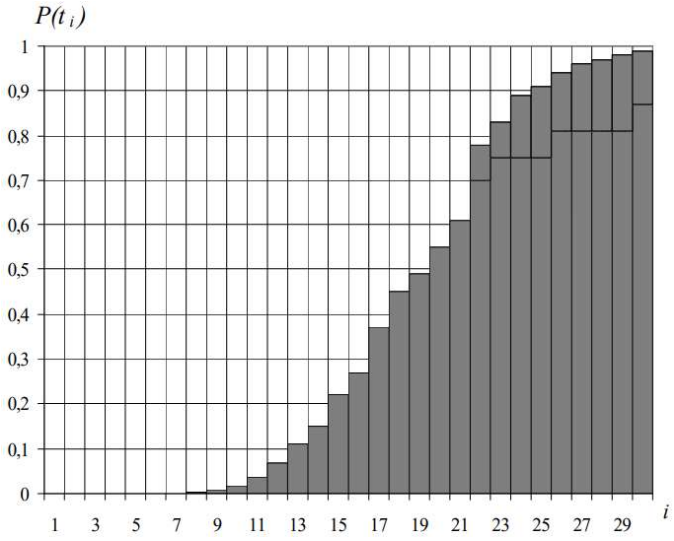

Рисунок 2.3 – Графіки ймовірностей P(t_i) при використанні моделі Джелінського-Моранди

Відповідно до описаної методики, було проведено розрахунок. Результати розрахунків наведено у табл. 2.2.

Таблиця 2.2 - Результати розрахунку показників надійності програмного комплексу з використанням моделі Джелінського – Моранди

Номер інтервалу i	Число відмов M_i	Інтенсивність λ_i	Імовірність $P(t_i)$	M_i після корекції	λ_i після корекції	$P(t_i)$ після корекції
1	30,00	1,500	0,000	30,00	1,510	0,000
2	23,00	1,800	0,000	23,00	1,280	0,000
3	19,00	1,120	0,000	19,00	1,120	0,000
4	17,00	0,990	0,000	17,00	0,990	0,000
5	16,00	0,870	0,000	16,00	0,870	0,000
6	14,00	0,750	0,000	14,00	0,750	0,000
7	13,00	0,660	0,001	13,00	0,660	0,001
8	12,00	0,570	0,003	12,00	0,570	0,003
9	12,00	0,480	0,008	12,00	0,480	0,008
10	10,00	0,400	0,018	10,00	0,400	0,018
11	9,00	0,330	0,036	9,00	0,330	0,036
12	7,00	0,270	0,067	7,00	0,270	0,067
13	5,00	0,220	0,110	5,00	0,220	0,110
14	4,00	0,190	0,150	4,00	0,190	0,150
15	4,00	0,150	0,220	4,00	0,150	0,220
16	3,00	0,130	0,270	3,00	0,130	0,270
17	3,00	0,100	0,370	3,00	0,100	0,370
18	2,00	0,080	0,450	2,00	0,080	0,450
19	2,00	0,070	0,490	2,00	0,070	0,490
20	1,00	0,060	0,550	1,00	0,060	0,550
21	2,00	0,050	0,610	2,00	0,050	0,610
22	1,00	0,035	0,700	1,44	0,025	0,780
23	0,00	0,028	0,750	1,00	0,018	0,830
24	0,00	0,028	0,750	0,74	0,012	0,890
25	1,00	0,028	0,750	0,53	0,009	0,910
26	0,00	0,021	0,810	0,38	0,006	0,940
27	0,00	0,021	0,810	0,28	0,004	0,960
28	1,00	0,021	0,810	0,20	0,003	0,970
29	0,00	0,021	0,810	0,14	0,002	0,980
30	0,00	0,014	0,870	0,10	0,001	0,990

У випадку однакових проміжків часу, інтенсивність помилок розраховується за певною формулою $\lambda_i = \Phi(N - n_{i-1})$.

Для обчислення показників надійності за допомогою моделі Джелінського – Моранди потрібно виконати такі кроки:

1) Ввести дані – результати тестування програми (моменти часу виникнення відмов програми).

2) Вибрати значення t_o.

3) Визначити кількість часових інтервалів $M = t_{mecm}/t_o$. t_{mecm} – тривалість періоду тестування.

4) Визначається К за формулою (2.30):

$$K = \sum_{i=1}^{M} M_i = n_M. \qquad (2.30)$$

5) Визначаються А і В за формулами (2.26) та (2.27).

6) Визначається $\theta = B / AK$.

7) Визначається кількість помилок в і-му інтервалі M_i.

8) Розраховуються коефіцієнти Ф та N.

9) Значення Ф та N підставляються в формулу розрахунку λ_i.

10) Розраховується значення $P(t_i)$ [15].

АСТС з використанням моделі Джелінського – Моранди використовує 30 часових інтервалів тривалістю t_0 = 20 годин. Розраховані параметри моделі: $\Phi = 0{,}007$, $N = 213$. Після завершення тестування імовірність безвідмовної роботи програми $P_{30} = 0{,}87$, що є незадовільним результатом. Пропонується використовувати апроксимацію кількості відмов після 21-го інтервалу. Апроксимаційна функція має вигляд $M_i = 2e^{-0{,}333(i-21)}, i = 21...30.$

На рис. 2.4 зображено граф, який відтворює структуру програмного комплексу системи контролю мережі СКС7 [3]. Цей комплекс складається з 15 програмних модулів і має один вхід та два виходи. Щоб спростити графічне зображення, на графі не відображені вхідні та вихідні стани, а також поглинаючий стан, який відповідає відмовам програмних модулів.

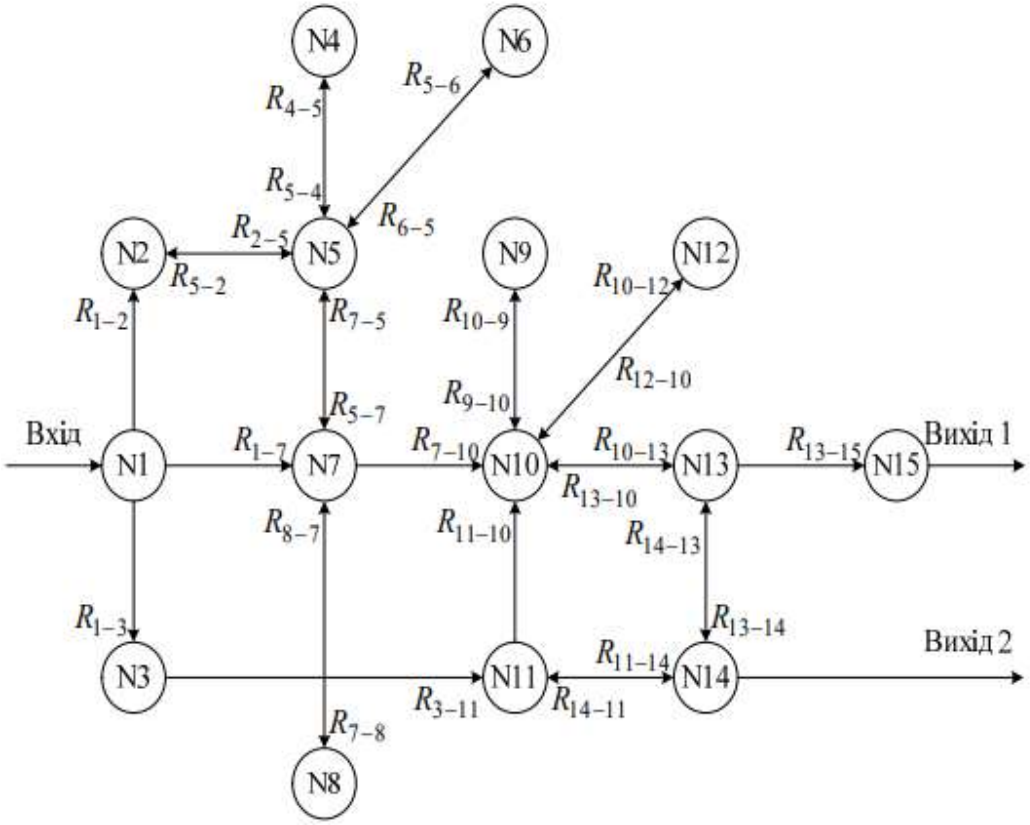

Рисунок 2.4 – Модель надійності програмного комплексу системи контролю

N1 – АСТС;
N2 – заповнювач БД;
N3 – концентратор;
N4, N9 – архіватор даних;
N5, N10 – СУБД;
N6,N12 – реплікатор;
N7 – адміністратор системи;
N8 – менеджер станів;
N11 – дисплей станів (сервер);
N13 – сервер звітів;
N14 – дисплей станів (клієнт);
N15 – сервер клієнтських звітів.

Переваги використання Марківської моделі для оцінки надійності великих програмних комплексів включають можливість поетапної оцінки надійності моделей під час їх розробки і налагодження, швидкого визначення надійності програмного комплексу завдяки паралельному тестуванню модулів, менші затрати часу і коштів при тестуванні окремих програмних модулів порівняно з тестуванням всього комплексу, а також можливість визначення внеску кожного модуля у надійність програмного комплексу та вжиття заходів для його поліпшення.

Висновок. Було ретельно вивчено параметри надійності обчислювальних компонентів засобів контролю цифрових телекомунікаційних мереж, а також методи оцінки показників надійності програмно-апаратних комплексів моніторингу цифрових телекомунікаційних мереж. Додатково проведено аналіз надійності програмного забезпечення. Ці аспекти спрямовані на забезпечення стабільності та безперебійності функціонування системи, що є критично важливим для забезпечення ефективної роботи цифрових телекомунікаційних мереж.

Після використання апроксимаційної моделі ймовірність безвідмовної роботи зросла з 0,87 до 0,99. Слід відзначити, що шкали часу для обох функцій неоднакові. Кожен інтервал екстраполюючої функції відповідає тривалості такої самої кількості інтервалів вихідної функції, в яких відбулася одна відмова програми. Зі збільшенням тривалості тестування різниця між функціями зменшується. Запропонований метод також дозволяє прогнозувати тривалість тестування програми при заданому рівні імовірності безвідмовної роботи.

3 РОЗРОБКА СИСТЕМИ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Один з загальних недоліків, що були визначені в розділі 1 щодо систем моніторингу, полягає в відсутності жорсткої синхронізації часу прийому сигнальних повідомлень. Для забезпечення синхронізації часу можна використовувати приймачі точного часу, які підключені до одного зі стандартних портів, що обслуговується операційною системою. Однак, як вже було вказано, це може призвести до значних похибок у визначенні моменту реєстрації сигнальних повідомлень.

Після аналізу провідних розробок та концепцій систем, які були описані раніше, можна сформулювати додаткові технічні задачі, необхідні для розробки системи та пристроїв моніторингу:

- подолання впливу плезисинхронності ЦТМ на точність прийому сигнальних повідомлень за допомогою адаптації параметрів вимірювальних каналів та створення програмно-апаратного розподілення процесів прийому даних та їх обробки, незалежно від індивідуальних властивостей каналів;

- забезпечення жорсткої синхронізації часу по всій системі моніторингу з метою уникнення збоїв у з’єднаннях швидкодіючих комутаційних мереж за допомогою методу кінцевих автоматів, що працюють в реальному часі [13].

3.1 Структурна організація та особливості роботи первинного перетворювача системи

Як було визначено раніше, для збору та первинної обробки даних в системі використовується аналізатор сигналізації телекомунікаційних систем (АСТС). АСТС реалізовано на основі індустріального комп’ютера, функції взаємодії з

ПЦП виконує розроблений контролер ланок сигналізації (КЛС) у вигляді інтерфейсного модуля, загальна структура якого представлена на рис. 3.1 [19].

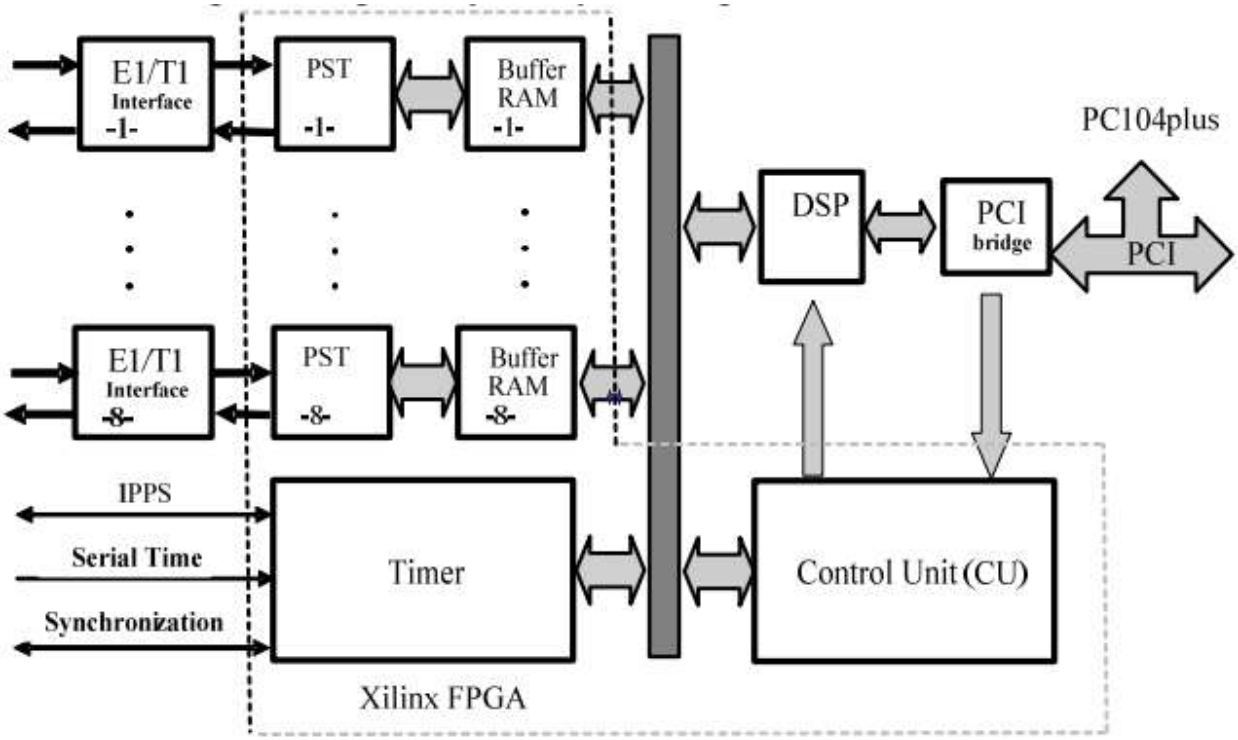

Рисунок 3.1 – Структура інтерфейсного модуля на основі КЛС

У відміну від існуючих пристроїв, контролер обробки даних ПЦП працює незалежно для кожного каналу, використовуючи блоки паралельно-послідовного перетворення (PST) та буферну оперативну пам'ять (Buffer RAM). Послідовні дані з ПЦП спочатку перетворюються блоком PST у паралельну форму і записуються у буферну пам'ять, яка складається з двох незалежних модулів. Один модуль призначений для запису з ПЦП, а другий – для читання. Функціонування цих модулів змінюється кожні 125 мікросекунд у фреймовому періоді, коли починається новий цикл послідовної передачі-прийому серії байтів [18].

Сигнали фреймової синхронізації, що визначаються блоками інтерфейсу ПЦП, передаються блокам PST, буферній пам'яті та блоку керування (CU), який відповідає за обробку переривань програми DSP згідно із фреймовими сигналами. Крім того, CU виконує функції управління обміном даних. За допомогою цього модуля та блока моста зі шиною PCI (PCI bridge), процесор (ЦП) забезпечує керування конфігурацією параметрів вхідних кіл блоків інтерфейсу ПЦП. Сигнальний процесор (DSP) може обробляти дані попереднього фрейму у будь-який момент наступного фрейму, що дозволяє незалежно від частоти кожного з каналів ПЦП обробляти дані [19].

Як показано на рис. 3.1, системний процесор відсутній в КЛС, і всі функції первинної обробки даних здійснюються DSP. Пакети, вилучені із ПЦП, передаються для подальшої обробки по протоколах високого рівня до ЦП.

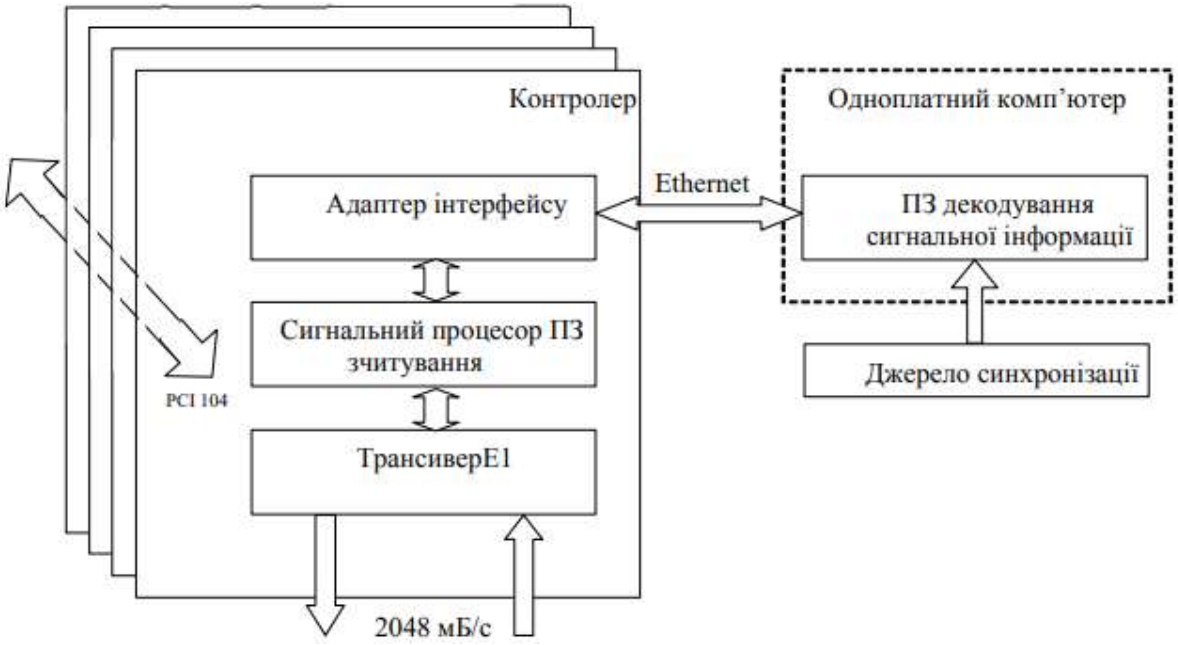

Рисунок 3.2 – Компоновка пристрою для моніторингу у форматі PC104 на основі КЛС

Для самостійної роботи ІМ можна підключити ЦП у стандарт PC104 за допомогою додаткового роз'єму, що суміщений з шиною PCI. Цей роз'єм має габаритні розміри близько 100x100x15 мм. Загальна структура пристрою у такому варіанті конфігурації показана на рис. 3.2 [3].

Один ЦП може бути підключений до чотирьох КЛС. Така конфігурація дозволяє зменшити вагу та розміри пристрою для моніторингу, що робить його більш привабливим для широкого кола користувачів. Більшість компонентів схеми реалізовані на одному кристалі програмованої логіки великої ємності з технологією FPGA від Xilinx, тому габаритні розміри КЛС не перевищують близько 160x100x10 мм. Загальний вигляд КЛС показано на рис. 3.3 [3].

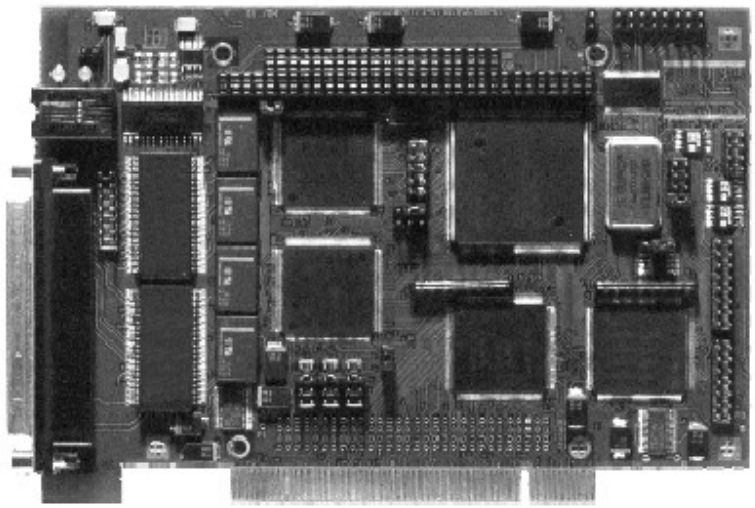

Рисунок 5.3 – Загальний вигляд контролера ланок сигналізації

Процедура роботи пристрою для моніторингу (ACTC) включає наступні кроки. Починаючи з запуску програми actc.exe, яка визначає підключені до системи КЛС і завантажує їх програмні модулі в пам'ять DSP. Після цього кожен КЛС підтверджує початок роботи програми та готовність до роботи. Потім програма actc.exe налаштовує вхідні канали блоків інтерфейсу та встановлює

з'єднання для обробки канальних інтервалів ПЦП, використовуючи конфігураційний файл, який був створений попередньою сесією або користувачем. Кожен КЛС постійно контролює стан підключених лінійних входів і повідомляє ЦП про всі випадки аварій. Програма actc.exe відображає дані про стан ліній на панелі індикаторів. Користувач може відкривати структуровані групи файлів, об'єднані в сесію, для реєстрації пакетів даних моніторингу [12].

Перший рівень бази даних моніторингу утворюють файли сесії, а верхній рівень створює інтегрована СУБД, що базується на продуктах від фірми Oracle. Ця система збирає дані від усіх пристроїв моніторингу через локальні та глобальні мережі, які з'єднують пристрої, що розташовані в різних місцях. В інтегрованій базі даних, за допомогою SQL-запитів, можна проводити пошук та відбір одного або групи сигнальних повідомлень, що пройшли через контрольовані пристрої. Зібрані дані можуть бути представлені у графічному форматі або у формі звіту, який включає параметри проходження сигнальних повідомлень в мережі.

3.2 Модель обробки даних первинного цифрового потоку та визначення часу подій в системі моніторингу

Період передачі даних в ПЦП складає $T_{\Phi} = 125\,мкс.$ Фреймова синхронізація визначається сигналом, який передається у першому (нульовому) байті 32-байтової послідовності. Блоки інтерфейсу стандарту E1/T1 виділяють цей сигнал і передають його разом з цифровими даними блокам PST. Внаслідок цього можливий зсув фаз між фреймовими сигналами на зовнішній аналоговій лінії та внутрішній цифровій лінії, який може складати половину періоду $\triangle\varphi_{\max} \le 0,5T_{\phi}$. Сигнали фреймової синхронізації через блоки PST, Buffer RAM та CU ініціюють переривання програми DSP [15].

Програма, яка відповідає за обробку цього переривання, реєструє, які ПЦП відбули оновлення даних, які необхідно обробити і передати на нижчий рівень бази даних. Час спрацювання переривання фіксується за допомогою таймера, тому момент прийому пакету сигнального повідомлення не залежить від моменту завершення обробки. Можливе затримування в реєстрації моменту спрацювання переривання може викликати інше переривання, що надійшло раніше. Тому програма DSP, яка обробляє переривання, налаштована таким чином, що здійснює фіксацію подій за мінімальний час за допомогою системи флагів (flag) і передає їх на обробку основній програмі. Основна програма перевіряє стан флагів і виконує відповідні дії, пов'язані зі спрацюванням прапорців. Як результат, максимальний час обробки переривань DSP з тактовою частотою 160 МГц не перевищує 2 мкс [3].

Встановлення моменту фреймового переривання проводиться шляхом зчитування значення таймера, який функціонує протягом однієї секунди з точністю до 1 мкс - $T_{mks} = 0…0,99999$ с. Даний час в сумі з часом, що надходить від приймача точного часу щосекунди T_{sec} , визначає астрономічний час прийому сигнального повідомлення як $T_{rec}=T_{sec}+T_{mks}$.

Операція таймера синхронізується за допомогою сигналу 1PPS (рис. 3.1). Інформація про номер секунди T_{sec} надходить від приймача точного часу через вхід блока таймера Serial Time. Вхід-вихід таймера Synchronization використовується для взаємної синхронізації КЛС в АСТС. Процедура синхронізації таймера діє наступним чином: якщо таймер досягає максимального значення перед надходженням наступного імпульсу сигналу 1PPS, він припиняє свою роботу, а при надходженні наступного сигналу 1PPS переходить в початковий режим. У випадку коли сигнал 1PPS надходить раніше, ніж досягнуте максимальне значення таймера, він повертається в початкове положення [15].

Інформація про T_{sec} надходить послідовно через з'єднання RS232 у відрізках часу між сигналами 1PPS, з відставанням від них на одну секунду. Ці дані

зберігаються в буфері таймера та з відправленням сигналу 1PPS стають наступними відліками астрономічного часу. Синхронізація таймера відбувається за допомогою кварцевого резонатора, стабільність якого не перевищує 30 PPM. За одну секунду його максимальне відхилення від номінального значення може складати до 30 мкс. Отже, середня похибка визначення T_{mks} протягом секунди становить приблизно 15 мкс. В такий спосіб, максимальна похибка визначення часу приймання сигнального повідомлення може бути розрахована [3]:

$$\triangle t = \triangle \varphi_{\max} + \triangle t_{\text{int}} + \triangle T_{mks} \le 79{,}5\, мкс, \qquad (3.1)$$

даний параметр менше встановленого вище граничного значення 0,1 мс.

Щоб зменшити похибку (3.1), передбачено можливість синхронізації частоти всіх таймерів інтерфейсних модулів $f_s = 2048\, МГц$, що виділена із одного з ПЦП і може бути підключена по входу-виходу Synchronization. У даному режимі, що встановлюється опціонально, кожні 125 мкс, синхронно з фронтом частоти f_s таймер збільшує своє значення на 125, а на протязі періоду f_s збільшує своє значення синхронно з частотою резонатора. В результаті похибка T_{mks} складає 3,75 нс і тому у виразі (3.1) $\Delta\ T_{mks}$ можна опустити, тоді $\Delta t<64,5$ мкс [21].

В разі втрати або відсутності сигналу 1PPS один із ІМ стає генератором секундної синхронізації – той же модуль, що генерує f_s . В даному випадку час T_{sec} може означати як абсолютну величину, так і відносну – з часу включення пристрою.

3.3 Загальна архітектура системи моніторингу та управління

Система моніторингу має ієрархічну структуру і складається з рівня збору даних та центру моніторингу.

В залежності від розміру та структури управління мережею СКС7, система моніторингу може бути організована на трьох рівнях, що включають регіональні центри моніторингу. На рис. 3.4 наведено трьохрівневу архітектуру системи [15].

Перший рівень, рівень збору даних, складають територіально розподілені локальні пункти моніторингу (ЛПМ). Кожен ЛПМ має територіально розподілені пристрої АСТС, які встановлені безпосередньо на сигнальних ланках. Кількість контрольованих сигнальних ланок може коливатися від одиниць до сотень. ЛПМ об'єднані мережею передачі даних, незалежною від мережі СКС7, яка використовується в якості корпоративної МПД. Крім пристроїв АСТС, склад ЛПМ включає:

- додаткові сервери баз даних;
- сервери програмного забезпечення;
- модуль для прийому архіву даних з локального рівня;
- програмно-апаратні модулі MTP, ISUP, загального управління [12].

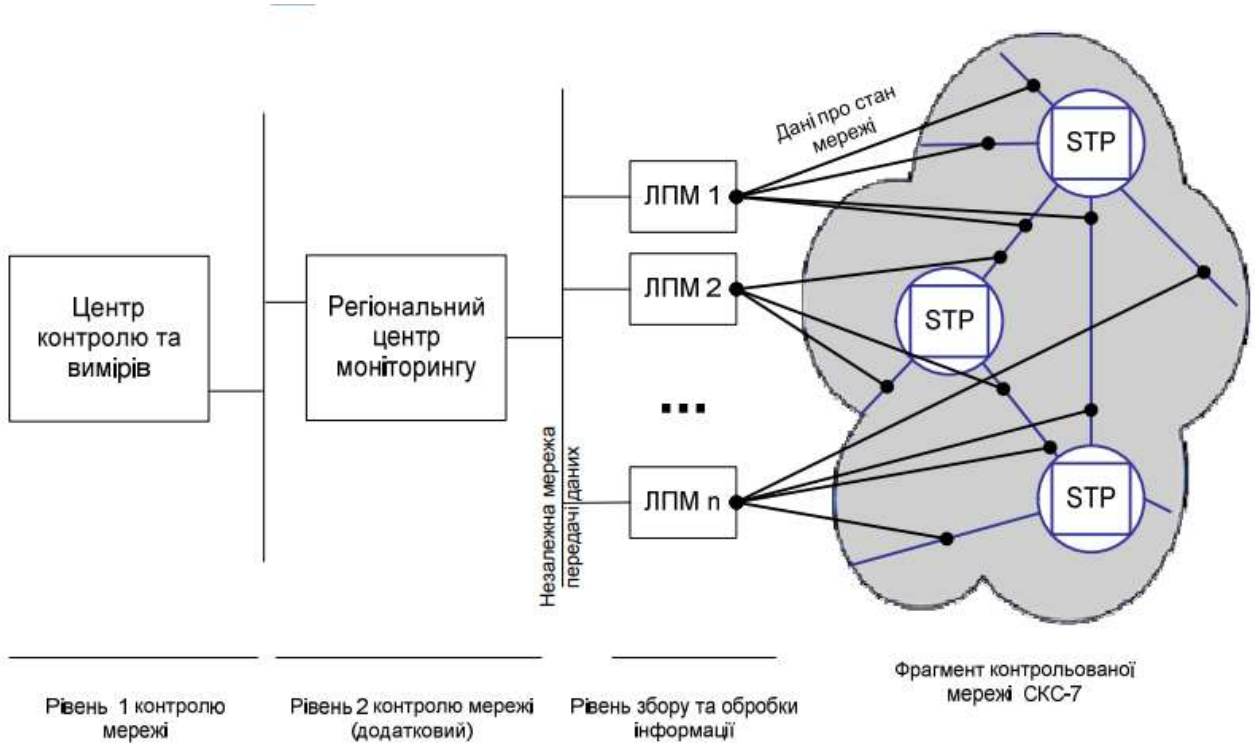

Рисунок 3.4 – Загальна архітектура системи моніторингу та управління

Програмне забезпечення локальних пунктів моніторингу (ЛПМ) аналізує інформацію з мережі СКС7 для формування статистичних даних щодо якості, трафіку, викликів, тощо.

Керування системою моніторингу здійснюється через центр моніторингу. Програмне забезпечення центру моніторингу дозволяє контролювати всю мережу СКС7 в режимі реального часу, адмініструвати систему моніторингу, аналізувати статистику, управляти правами користувачів та генерувати звіти. Функціонал центру обмежується встановленим програмним забезпеченням.

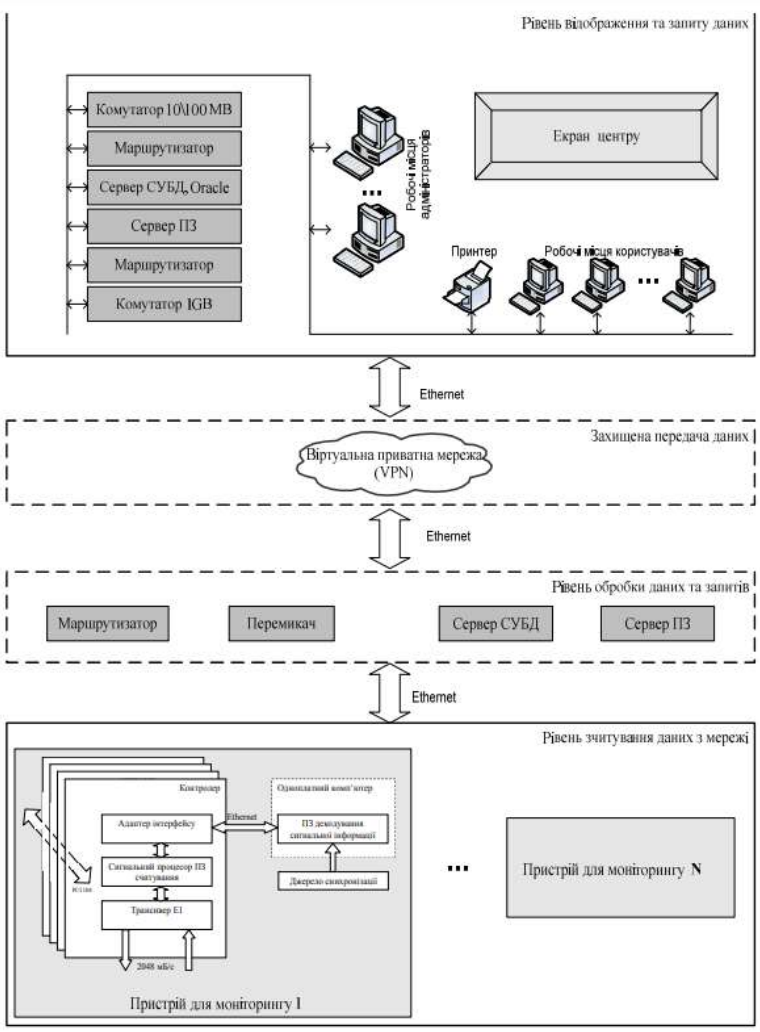

Рисунок 3.5 – Структурна схема ІВС

На рис. 3.5 наведено структурну схему ІВС контролю телекомунікаційних систем на базі аналізу даних СКС7. На рівні зчитування даних системи розташовані пристрої для моніторингу (АСТС), що підключені безпосередньо до потоків 2048 кбіт/с.

У режимі реального часу, дані щодо функціонування мережі СКС7 надходять на локальний рівень обробки даних та запитів через мережу передачі даних. Інформація про стан мережі зберігається на рівні сервера баз даних. На сервері програмного забезпечення встановлено програми, які відповідають за первинну обробку даних та взаємодію з сервером баз даних. Маршрутизатор забезпечує зв'язок між локальними пристроями моніторингу та VPN (корпоративною мережею), а перемикач дозволяє кільком комп'ютерам одночасно працювати з одним набором пристроїв введення-виведення. На цьому рівні також присутнє джерело синхронізації, яке зв'язане з еталоном часу для забезпечення єдиної системи часу.

Для безпечної передачі інформації використовується віртуальна приватна мережа (VPN). На рівні відображення та запиту даних розміщені спеціалізовані робочі місця, що об'єднані в межах локальної мережі, із розподіленим доступом для користувачів та адміністраторів інформаційно-виправних систем (ІВС). Ці робочі місця обладнані програмним забезпеченням, яке відповідає за вирішення поточних завдань. Крім того, на цьому рівні розташовані такі пристрої:

- маршрутизатор;
- комутатор зі швидкістю 1 Гбіт/с;
- комутатор зі швидкістю 10/100 Мбіт/с;
- сервери програмного забезпечення;
- сервери баз даних (СУБД).

Також на цьому рівні доступний широкий екран, на якому відображається інформація про конфігурацію та стан мережі СКС7.

3.4 Структура програмного забезпечення системи моніторингу та управління

Комп'ютери, які використовуються для програмного забезпечення «Аналізатор АСТС», містять у собі пристрої АСТС, які формують логічні та територіальні групи програмно-апаратних комплексів «АСТС». Кожне таке об'єднання може включати від одного до десяти АСТС. Функції цих пристроїв включають контроль за станом мережі сигналізації та передачею цієї інформації в реальному часі в центр керування, а також розрахунок статистичних показників трафіку та якості роботи мережі з подальшим передаванням цих даних в базу даних.

«Аналізатор АСТС» є критично важливим елементом інформаційно-виправних систем, оскільки його відмова, непрацездатність або недостатність ресурсів комп'ютера призводять до втрати даних. Більше того, цей елемент є масштабованим компонентом ІВС. АСТС виконує такі функції:

- автоматичний запуск при старті ОС або запуск по команді;
- автоматичну настройку у відповідності з конфігурацією ІВС та реконфігурацію по команді «Адміністратора програм»;
- автоматичне створювання/відкриття документа/сесії;
- динамічне підключення/відключення джерел даних в сесії;
- динамічне реконфігурування сесії у відповідності з конфігурацією ІВС;
- довготривалу буферизацію даних, що приймаються та підраховуються;
- підготовку даних для ІВС;
- автоматичну очистку дисків від застарілих даних;
- автоматичне підключення до «Концентратора» та підтримка з‘єднання;
- автоматичне підключення до «Заповнювача БД» та підтримка з‘єднання;
- підготовка та «змістовна» буферизація даних для відправлення (канал передачі даних у реальному часі).

На серверах ПЗ ЛМП розміщено програмне забезпечення, яке приймає дані від сервера зондів та надсилає їх у центр контролю у реальному часі. Також воно веде запис статистичної інформації на сервера баз даних ЛПМ.

Схему модулів та потоків даних на ЛПМ представлено на рис. 3.6 [20].

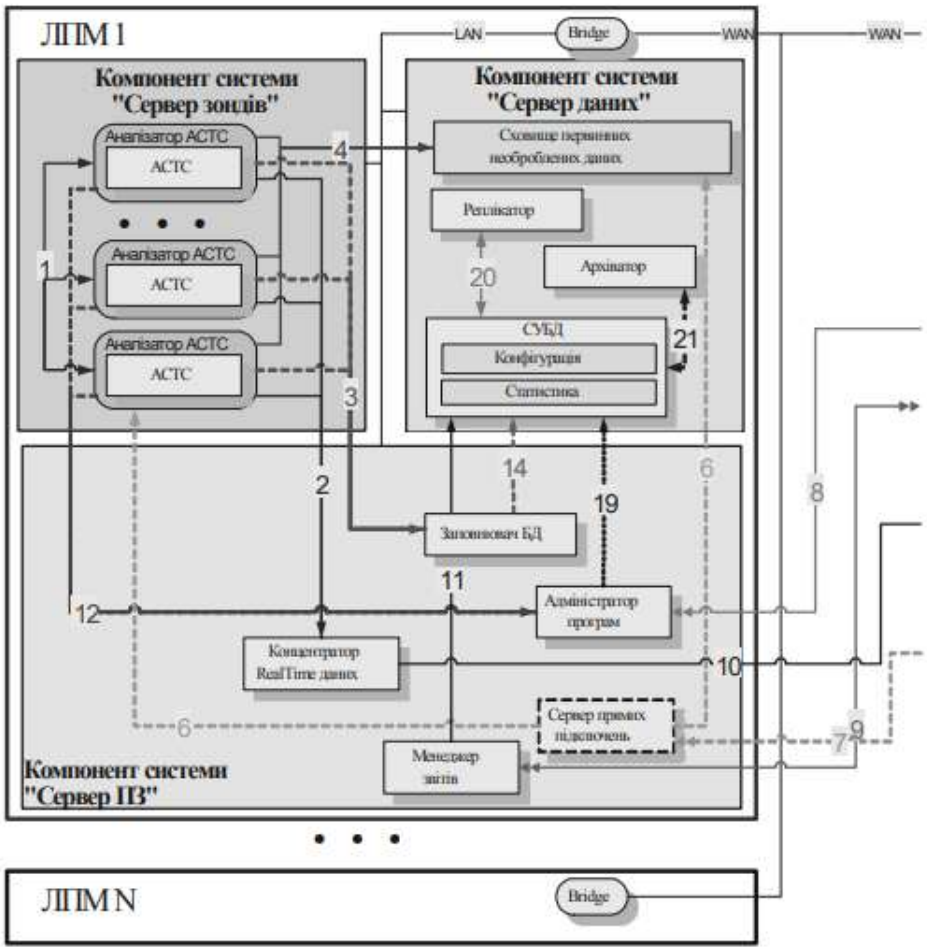

Рисунок 3.6 – Архітектура системи модулів та потоків даних ЛПМ

1 → *Socket* – АСТС-АСТС;

2 → *Socket* – АСТС - Концентратор ReallTime даних;

3 → *Socket* – АСТС - Заповнювач БД;

4 → *Files* – АСТС - Сховище первинних даних;

5 → *SQL* – Доступ до даних для вторинної обробки;

6 → *Files* – Сервер підключень - Сховище первинних даних;

7 → *Socket* – Дисплей стану(клієнт)-Сервер підключень;

8 → *CORBA* – Адміністратор -Адміністратор;

9 → *CORBA* – Менеджер звітів - Менеджер звітів;

10 → *Socket* – Концентратор ReallTime даних -Концентратор ReallTime даних;

11 → *SQL* – Менеджер звітів - СУБД(статистичні дані).

Сервер ЛПМ обладнаний програмним забезпеченням, яке надає доступ до статистичної інформації на сервері баз даних для створення звітів. Крім того, на серверах програмного забезпечення ЛПМ встановлено програмне забезпечення для автономного контролю ІВС.

Крім того, на сервері баз даних ЛПМ реалізовано програмне забезпечення для архівування застарілої статистичної інформації з метою оптимізації використання дискового простору.

У зв'язку з великим обсягом даних у центрі контролю (ЦК) є два сервери програмного забезпечення (ПЗ): один для конфігурування ІВС та постачання даних для звітів, інший - для надання інформації про стан об'єктів мережі СКС7 в реальному часі.

Висновок. Під час аналізу технічних аспектів системи було проведено глибоке дослідження вимог до неї, зокрема враховуючи структуру та функціональні особливості.

Було наведено моделі обробки даних первинного цифрового потоку, а також методи визначення часу подій у системі моніторингу. Загальна архітектура системи також була ретельно розглянута, враховуючи її складові елементи та їх взаємозв'язки. Не менш важливим етапом був аналіз структури програмного забезпечення, який визначив способи обробки та передачі даних у системі. Цей комплексний підхід дозволив забезпечити оптимальне функціонування системи та задовольнити вимоги її користувачів.

4 ОХОРОНА ПРАЦІ

Небезпечні та шкідливі виробничі фактори можуть мати вплив на проектувальника програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем в організмі людини наступні: підвищена чи понижена температура повітря робочої зони; недостатнє освітлення робочої зони; недостатність природного освітлення; підвищений рівень шуму на робочому місці; відсутність чи нестача природнього світла; фізичні перевантаження (статичні); нервово - психічні перевантаження (перенапруга аналізаторів, емоційні навантаження).

Відповідно до визначених факторів формуємо рекомендації щодо безпечних умов праці під час проектування програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем [24].

4.1 Технічні рішення щодо безпечного виконання роботи

Місце праці проектувальника, що обладнане ПК, має бути так розташоване, щоб забезпечити оптимальні умови для праці та комфорт користувача. Рекомендується відстань не менше 1,5 м від вікон, щоб уникнути надмірного освітлення або блисків на екрані. Від інших стін відстань повинна бути не менше 1 м, щоб забезпечити вільний доступ до робочого місця. Також важливо, щоб відстань до інших користувачів була не менше 1,5 м для забезпечення приватності та незалежності під час роботи. Щодо розташування відносно вікон, важливо, щоб природне світло падало на робоче місце збоку, переважно зліва, щоб уникнути надмірного відблиску на екрані [25].

При розташуванні елементів робочого місця користувача ПК слід враховувати:

- робочу позу користувача;
- простір для розміщення користувача;
- можливість огляду елементів робочого місця;
- розміщення документації і матеріалів, які використовуються користувачем.

Для забезпечення точного та швидкого зчитування інформації в зоні найкращого бачення площина екрана монітора повинна бути перпендикулярною нормальній лінії зору. При цьому повинна бути передбачена можливість переміщення монітора навколо вертикальної осі в межах ±30° (справа наліво) та нахилу вперед до 85° і назад до 105° з фіксацією в цьому положенні.

Клавіатура повинна бути розташована так, щоб на ній було зручно працювати двома руками. Клавіатуру слід розміщати на поверхні столу на відстані 100...300 мм від краю. Кут нахилу клавіатури до столу повинен бути в межах від 5 до 15°, зап’ястя на долонях рук повинні розташовуватись горизонтально до площини столу [26].

Для запобігання світлових відблисків від екрана, клавіатури в напрямку очей користувача від освітлювачів загального призначення або сонячних променів необхідно застосовувати антивідблискові сітки, спеціальні фільтри, захисні козирки, на вікнах регульовані жалюзі.

Принтер повинен бути розміщений у зручному для користувача положенні, так, що максимальна відстань від користувача до клавіш управління принтером не перевищувала довжину витягнутої руки користувача.

Конструкція робочого стола повинна забезпечувати можливість оптимального розміщення на робочій поверхні обладнання, що використовується, з врахуванням його кількості та конструктивних особливостей (розмір монітора, клавіатури, принтера, ПК та ін.) і документів, а також враховувати характер роботи, що виконується.

Згідно з вимог електробезпеки, під час проектування та експлуатації систем електропостачання для ПК необхідно дотримуватись вимог.

Під час проектування лінії живлення для комп'ютерів, периферійних пристроїв та обладнання для їх обслуговування, ремонту та налагодження, варто використовувати окрему групову трипровідну мережу, прокладаючи фазові, нульові робочі та нульові захисні провідники. Нульовий захисний провідник призначено для заземлення електричних пристроїв .

Категорія умов по небезпеці електротравматизму – без підвищеної небезпеки, у зв’язку з відсутністю факторів підвищеної небезпеки [12].

Для запобігання електротравмам у приміщенні здійснюються:

1) ізоляція нормально струмоведучих елементів електроустаткування відповідно з вимогами нормативів;

2) захисне заземлення із використанням природних заземлювачів;

3) систематичне проходження інструктажу з елетробезпеки [27].

Вимоги безпеки перед початком роботи:

1. Перевірити надійність встановлення апаратури на робочому столі.

2. Перевірити загальний стан апаратури, справність проводки електромережі, з’єднувальних шнурів, штепсельних вилок та розеток, заземлення захисного екрана.

3. Відрегулювати освітленість робочого місця.

4. Відрегулювати і зафіксувати висоту стільця (крісла), зручний для користувача нахил його спинки.

5. Увімкнути апаратуру ПК вмикачами на корпусах в такій послідовності: стабілізатор (або блок безперервного живлення), монітор, системний блок, принтер (якщо передбачається друкування).

6. Відрегулювати яскравість світіння екрану монітору, контрастність.

7. При появі несправностей комп’ютерної техніки повідомити керівника.

4.2 Технічні рішення з гігієни праці та виробничої санітарії

4.2.1 Мікроклімат

За енерговитратами проектування програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем згідно Гігієнічної класифікація праці [1] відноситься до категорії І б. Нормовані значення параметрів мікроклімату для цієї категорії наведені в табл. 4.1

Таблиця 4.1 - Нормовані параметри мікроклімату в робочій зоні

Період року	Категорія робіт	Допустимі		
		t, °C	W, %	V,м/с
Теплий	Легка І б	22-28	40-60	0,1-0,3
Холодний		20-24	75	0,2

Для забезпечення необхідних за нормативами параметрів мікроклімату здійснюються такі заходи:

1. Температура в приміщенні в холодний період року підтримується за допомогою системи центрального опалення.
2. Використовується передбачається припливна вентиляційна система.
3. Здійснюється систематичне вологе прибирання [28].

4.2.2. Склад повітря робочої зони

Забруднення повітря робочої зони регламентується граничнодопустимими концентраціями (ГДК) в мг/м3 [11]. ГДК шкідливих речовин, які знаходяться в досліджуваному приміщені, наведені в таблиці 4.2.

Таблиця 4.2 – ГДК шкідливих речовин у повітрі

Назва речовини	ГДК, мг/м^3		Клас небезпечності
	Максимально разова	Середньо добова	
Пил нетоксичний	0,5	0,15	4
Озон	0,16	0,03	1

Для забезпечення складу повітря робочої зони під час проектування приладу моніторингу серцевих скорочень слід використовувати механічну вентиляцію та забезпечити регулярне прибирання [29].

4.2.3 Виробниче освітлення

Природне освітлення повинно бути боковим, бажано одностороннім. Для уникнення засліплюючої дії сонячних променів найкраще, коли світлові отвори (вікна) зорієнтовані на північ чи північний схід. Коефіцієнт природної освітленості (КПО) повинен бути не нижче 1,5%.

Таблиця 4.3 - Норми освітленості в приміщенні

Характеристика зорової роботи	Найменший розмір об'єкта розрізнювання	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об'єкта розрізнення з фоном	Характеристика фона	Освітленість, Лк		КПО, $e_н$,%			
						Штучне освітлення		Природнє освітлення		Сумісне освітлення	
						Комбіноване	Загальне	Верхнє або верхнє	Бокове	Верхнє або верхнє і бокове	Бокове
Дуже високої точності	Від 0,15 до 0,3	II	г	великий	світлий	1000	300	7	2,5	4,2	1,5

У приміщенні, де проводиться розробка програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем використовується штучне та природне освітлення. Норми освітленості при штучному освітленні та КПО (для III пояса світлового клімату) при природному та сумісному освітленні зазначені у таблиці 4.3.

Для забезпечення достатнього освітлення передбачені такі заходи:

1) Максимальне використання бічного природного освітлення.

2) Систематичне очищення скла від бруду – не рідше двох разів на рік.

3) Штучне освітлення в приміщенні забезпечується світильниками типу РСП08×250 (однолампові) з лампами ДРЛ-250 [30].

4.2.4 Виробничий шум

У приміщеннях з ПК рівні звукового тиску, рівні звуку та еквівалентні рівні звуку на робочих місцях повинні відповідати ДСН 3.3.6.037-99 [10].

Рівні шуму на робочих місцях осіб, що працюють з ПК, визначені ДСанПіН 3.3.2-007-98 [9]. Допустимі значення звукового тиску під час проектування приладу моніторингу серцевих скорочень наведені в табл. 4.4 [31].

Таблиця 4.4 - Рівень звукового тиску

Характер робіт	Допустимі рівні звукового тиску (дБ) в стандартизованих октавних смугах з середньогеометричними частотами, Гц								
	32	63	125	250	500	1000	2000	4000	8000
Постійні робочі місця в промислових приміщеннях	107	95	87	82	78	75	73	71	69

Для зниження шуму в приміщенні, необхідно:

– безпосередньо біля джерел шуму використовувати звукопоглинаючі матеріали для покриття стелі, стін;

– для боротьби з вентиляційним шумом потрібно застосовувати мало шумові вентилятори.

4.2.5 Виробничі випромінювання

Рівні електромагнітного випромінювання та магнітних полів повинні відповідати вимогам. Рівні інфрачервоного випромінювання не повинні перевищувати граничних. Рівні ультрафіолетового випромінювання не повинні перевищувати допустимих [9].

Гранично допустима напруженість електростатичного поля на робочих місцях не повинна перевищувати рівнів [6].

Заходи щодо зменшення впливу на працівника електромагнітного випромінювання: оптимальна організація робочого місця, доцільне розміщення технологічного устаткування, дотримання гігієнічно-обгрунтованих режимів праці та відпочинку, зменшення часу перебування у зоні опромінення [32].

4.3 Розрахунок параметрів пожежної безпеки

Приміщення, де здійснюється розробка програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем відноситься до категорії пожежної безпеки В (табл.4.5).

Таблиця 4.5. Категорія приміщення за вибухопожежною і пожежною небезпекою

Категорія приміщення	Характеристика речовин і матеріалів, що знаходяться (обертаються) у приміщенні
В Пожежонебезпечна	Тверді горючі та важкогорючі речовини і матеріали, за умови, що приміщення, в яких вони знаходяться, не відносяться до категорій А, Б і питома пожежна навантага для твердих і рідких легкозаймистих та горючих речовин на окремих ділянках площею не менше 10 м2 кожна перевищує 180 МДж/м2.

Конструкція будівлі, де розміщено приміщення, відноситься до II-го ступеня вогнестійкості (будівля з несучою конструкцією з природних матеріалів або штучного каменю, бетону або залізобетону з застосуванням листових і плиткових негорючих матеріалів).

Згідно з правилами улаштування електроустановок, приміщення відноситься до класу П-IIа пожежної небезпеки (приміщенні, у якому знаходяться тверді горючі речовини та матеріали) [33].

4.3.1 Технічні рішення системи запобігання пожежі

До причин, що можуть спричинити пожежу в приміщенні, відносяться:

– короткі замикання;

– перевантаження електромережі і перегріву струму несучих частин та з’єднань;

– порушення правил техніки безпеки.

При виникненні аварійних ситуацій відбувається різке виділення теплової енергії, яка може стати причиною виникнення пожежі.

Заходи щодо запобігання пожежі:

– систематична перевірка на справність струмоведучих частин обладнання;

– систематичне проведення протипожежного інструктажу;

– дотримання вимог пожежної безпеки на робочому місці [34].

4.3.2. Технічні рішення системи протипожежного захисту

У приміщені можливе використання системи автоматичного пожежогасіння. Також потрібно використовувати установку порошкового пожежогасіння, що використовує у якості вогнегасної речовини спеціальний порошок, який є нетоксичним. Для подачі сигналів про пожежу у приміщенні встановлено пожежну сигналізацію.

Після закінчення роботи від усіх електроприладів, а також з мереж їх живлення повинна бути відключена напруга (за винятком протипожежних та охоронних установок). Електропроводи для підключення комп'ютерів, приладів повинні прокладатися по негорючих конструктивних елементах.

Згідно норм [7] на кожні 20 м^2 площі приміщення вказаних категорії та класу пожежо-вибухо-небезпеки та можливих класів пожеж – А, В і Е розміщується один порошковий або вуглекислотний вогнегасник з масою заряду від 3 до 5 кг. Крім того на поверсі, де знаходиться приміщення слід забезпечити наявність двох порошкових вогнегасники з масою заряду 10 кг.

Тому в приміщені буде розташовуватися два порошкових вогнегасники, які будуть розміщуватись в різних його кінцях, на висоті не більше 1,5 м від рівня підлоги до нижнього торця вогнегасника і на відстані від дверей, достатній для їх повного відчинення. Підходи до місця розташування вогнегасників мають бути завжди вільними. Для зазначення місцезнаходження вогнегасників буде встановлений вказівний знак. Знак розташовують на видних місцях на висоті 2,0 - 2,5 м від рівня підлоги [35].

ВИСНОВКИ

На основі аналізу передових наукових розробок встановлено, що для ефективної розробки систем та пристроїв моніторингу необхідно вирішити наступні завдання. Спочатку, необхідно подолати вплив плезисинхронності телекомунікаційних мереж на точність прийому сигнальних повідомлень. Це можна зробити шляхом адаптації до параметрів кожного з вимірювальних каналів та розроблення програмно-апаратного розподілення процесів прийому даних та їх обробки, незалежно від особливостей кожного каналу.

Далі, важливо забезпечити жорстку синхронізацію часу по всій системі моніторингу, щоб уникнути помилок у формуванні маршрутів з'єднань у швидкодіючих комутаційних мережах. Це можна досягти за допомогою методу кінцевих автоматів, що працюють в реальному часі.

Також, при проектуванні системи важливо врахувати показники надійності роботи інтегрованої системи вузлів комутації.

З огляду на викладене вище, було зроблено висновок, що важливою та актуальною є задача розробки інтегрованої системи для контролю цифрової телекомунікаційної мережі, яка б забезпечила одночасне визначення основних параметрів мережі та врахування національної специфікації СКС7.

Було ретельно вивчено параметри надійності обчислювальних компонентів засобів контролю цифрових телекомунікаційних мереж, а також методи оцінки показників надійності програмно-апаратних комплексів моніторингу цифрових телекомунікаційних мереж. Додатково проведено аналіз надійності програмного забезпечення. Ці аспекти спрямовані на забезпечення стабільності та безперебійності функціонування системи, що є критично важливим для забезпечення ефективної роботи цифрових телекомунікаційних мереж.

Після використання апроксимаційної моделі ймовірність безвідмовної роботи зросла з 0,87 до 0,99. Слід відзначити, що шкали часу для обох функцій неоднакові. Кожен інтервал екстраполюючої функції відповідає тривалості такої самої кількості інтервалів вихідної функції, в яких відбулася одна відмова програми. Зі збільшенням тривалості тестування різниця між функціями зменшується. Запропонований метод також дозволяє прогнозувати тривалість тестування програми при заданому рівні імовірності безвідмовної роботи.

Під час аналізу технічних аспектів системи було проведено глибоке дослідження вимог до неї, зокрема враховуючи структуру та функціональні особливості.

Було наведено моделі обробки даних первинного цифрового потоку, а також методи визначення часу подій у системі моніторингу. Загальна архітектура системи також була ретельно розглянута, враховуючи її складові елементи та їх взаємозв'язки.

Як один із найважливіших етапів було проведено аналіз структури програмного забезпечення, який визначив способи обробки та передачі даних у системі. Цей комплексний підхід дозволив описати умови для оптимального функціонування системи, щоб задовольнити вимоги її користувачів.

Також у роботі було проведено дослідження параметрів з охорони праці та безпеки в надзвичайних ситуаціях для заданих умов та параметрів навколишнього середовища. Зроблено необхідні висновки.

Отже, поставлені завдання щодо розробки програмно-апаратних засобів контролю та моніторингу ЦТС можна вважати виконаними у повному обсязі.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. М. Ю. Ільченко, С. О. Кравчук Телекомунікаційні системи // НАН України, Нац. техн. ун-т України «Київ. політехн. ін-т ім. Ігоря Сікорського», НДІ телекомунікацій. – Київ : Наук. думка, 2017. – 734, с.

2. Телекомунікаційні системи передачі : підручник / В. М. Кичак, О. М. Шинкарук, Г. Г. Бортник, І. І. Чесановський, О. В. Стальченко. – Хмельницький : Видавництво НАДГІСУ, 2016. – 424 с.

3. Методологія побудови систем контролю та моніторингу цифрових телекомунікаційних мереж / Р. Н. Квєтний, В. Г. Лисогор, В. П. Посвятенко та ін. – Вінниця : УНІВЕРСУМ Вінниця, 2006 .– 162 с.

4. Оптимізація та математичне моделювання мереж зв'язку [Текст] : навч. посіб. / В. М. Безрук, О. М. Буханько, Д. В. Чеботарьова ; Харків. нац. ун-т радіоелектроніки. - Харків : Компанія СМІТ, 2014. – 192 с.

5. Gundall M, Schneider J, Schotten HD, Aleksy M, Schulz D, Franchi N, et al. 5G as Enabler for Industrie 4.0 Use Cases: Challenges and Concepts. IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA): IEEE; 2018. p. 1401-8.

6. ITU-T Recommendation I.312/Q.1201 (10/92) - Principles of intelligent network architecture

7. Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації: Мережі, технології, безпека, економіка, управління. – К.: Азимут-Україна, 2013. – 608 с.

8. Alriksson F, Boström L, Sachs J, Wang Y-PE, Zaidi A. Ericsson Technology Review: Critical IoT Connectivity. Stockholm, Sweden – 2020 .

9. Бортник Г. Г. Методи та засоби первинного цифрового оброблення радіосигналів [Текст] : монографія / Г. Г. Бортник, М. В. Васильківський, В. М.

Кичак. - Вінниця : ВНТУ, 2016. – 168 с. - ISBN 978-966-641-678-3.

10. Кичак В. М. Основи радіоелектроніки [Текст] : навчальний посібник / В. М. Кичак, Ю. В. Крушевський, Д. В. Гаврілов. - Вінниця : ВНТУ, 2010. - 368 с.

11. Лисогор В.Г. Аналіз надійності системи контролю цифрової телекомунікаційної мережі по раптовим відмовам // Оптикоелектронні інформаційно-енергетичні технології. – 2004.– №2(8).–С. 186-193.

12. Batenkov, K. Batenkov, and A. Fokin, “Methods of formation of sets of states of telecommunication networks for various measures of connectivity”, in Proc. Of SPIIRAS, iss. 19, vol 3, pp. 644-673, 2020, doi: https://doi.org/10.15622/sp.2020.19.3.7.

13. Лисогор В.Г. Оптимізація систем контролю цифрових телекомунікаційних мереж за надійнисними критеріями // Вісник ВПІ. – 2005 .– №3. – С. 8–15.

14. Лисогор В.Г., Квєтний Р.Н. Посвятенко В.П. Математична модель затримок в ланці сигналізації // Вісник Хмельницького національного університету. – 2005.–№4 Ч1., Т.2 (68).– С. 201–206.

15. V. Romanyuk, “Directions for improving the efficiency of the functioning of tactful mobile radio networks”, in Proc. VIIIth scientific-practical seminar Priority areas of development of telecommunication systems and networks for special purpose, Kyiv, MITI of SUT, 2013, pp. 40-56.

16. Лисогор В.Г., Квєтний Р.Н., Посвятенко В.П. Моделі оцінки якості послуг в телекомунікаційних системах // Збірник тезисів докладів по матеріалам 10-ї Ювілейної міжнародної наукової конференції "ТЕОРІЯ І ТЕХНІКА ПЕРЕДАВАННЯ, ПРИЙМАННЯ ТА ОБРОБКИ ІНФОРМАЦІЇ". – Харків, ХНУРЕ– 2004.– Частина 2. – С. 122–123.

17. Лисогор В.Г., Квєтний Р.Н., Скидан О.Ю. Принципи побудови систем автоматизованого управління телекомунікаційними мережами // Оптико-електронні інформаційно-енергетичні технології. – 2003.–№1-2 (5-6).–С. 153-158.

18. Лисогор В.Г., Скидан Ю.А., Скидан О.Ю. Управління технологічними процесами, вимірювання параметрів сигналів, моніторинг та тестування мереж у розробках ІВП "ІнноВінн" // Матеріали VI міжнародної конференції КУСС-2001.–2001.–Том 2.– С. 82-84.

19. Пат. 5288 України, МКИ H04M1/24. Пристрій для системи моніторингу спільноканальної сигналізації. Лисогор В.Г., Скидан Ю.А., Качківський О.І., Буняк Ю.А. (Україна) - №20041008830; Заявл. 28.10.2004; Опубл. 15.02.2005; Бюл. №2.

20. Пат. 5289 України, МКИ H04M1/24. Спосіб керування навантаженням у телекомунікаційній мережі з спільноканальною сигналізацією. Лисогор В.Г., Скидан Ю.А., Батранін А.В., Буняк Ю.А. (Україна) - №20041008831; Заявл. 28.10.2004; Опубл. 15.02.2005; Бюл. №2.

21. ETSI Technical Report 003: Network Aspects (NA): Quality of Service and Network Performance. 10, 94.

22. G.703. ITU-T Recommendation G.703. Phisical/electrical characteristics of hierarchical digital interfaces. – Geneva, 1993. – 82 p.

23. ISO/IEC JTC1/SC33: Information Technology: Open Distributed Processing – Reference Model – Quality Of Service. 07, 98.

24. НАКАЗ №248 від 8.04.2014 Про затвердження Державних санітарних норм та правил «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу» URL: https://zakon.rada.gov.ua/laws/show/z0472-14#Text

25. ДСТУ OHSAS 18002:2015. Системи управління гігієною та безпекою праці. Основні принципи виконання вимог OHSAS 18001:2007 (OHSAS 18002:2008, IDT). К. : ГП «УкрНИУЦ», 2016. 21 с.

26. ДСНіП3.3.6.096-2002. Державні санітарні норми і правила при роботі з джерелами електромагнітних полів. URL: http://zakon2.rada.gov.ua/laws/show/z0203-03

27. НПАОП 40.1-1.32-01 Правила будови електроустановок. Електрообла днання спеціальних установок (Правила устройства электроустановок. Элект рооборудование специальных установок). URL: https://zakon.rada.gov.ua/ rada/show/v0272203-01#Text

28. ДСТУ EN 62305:2012 Блискавкозахист (європейський стандарт IEC 62305:2010). URL: https://tdsb.com.ua/ru/dstu-en-62305/

29. ДСТУБ В.2.5-82:2016. Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом. К. : ДП «УкрНДНЦ», 2016. 109 с

30. Наказ Міністерства внутрішніх справ України «Про затвердження Пра вил експлуатації та типових норм належності вогнегасників». URL: https://zakon.rada.gov.ua/laws/show/z0225-18#Text.

31. ДБН В.1.1-7:2016 Пожежна безпека об`єктів будівництва. Загальні ви моги. URL: http://www.poliplast.ua/doc/dbn _v.1.1-7-2002.pdf

32. НПАОП 0.00-7.15-18 Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями. URL: http://sop.zp.ua/norm_npaop _0 _ 00-7_ 15-18_01_ua.php

33. ДСН 3.3.6.037-99 Санітарні норми виробничого шуму, ультразвуку та інфразвуку. - [Електронний ресурс] - Режим доступу: http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvuku-nor4878.html

34. ДСН 3.3.6.042-99 Санітарні норми мікроклімату виробничих приміщень. - [Електронний ресурс] - Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972

35. Правила улаштування електроустановок - [Електронний ресурс] - Режим доступу: http://www.energiy.com.ua/PUE.html

Додаток А
(обов’язковий)

ІЛЮСТРАТИВНА ЧАСТИНА

РОЗРОБКА ПРОГРАМНО-АПАРАТНИХ ЗАСОБІВ КОНТРОЛЮ ТА МОНІТОРИНГУ ЦИФРОВИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

(назва бакалаврської дипломної роботи)

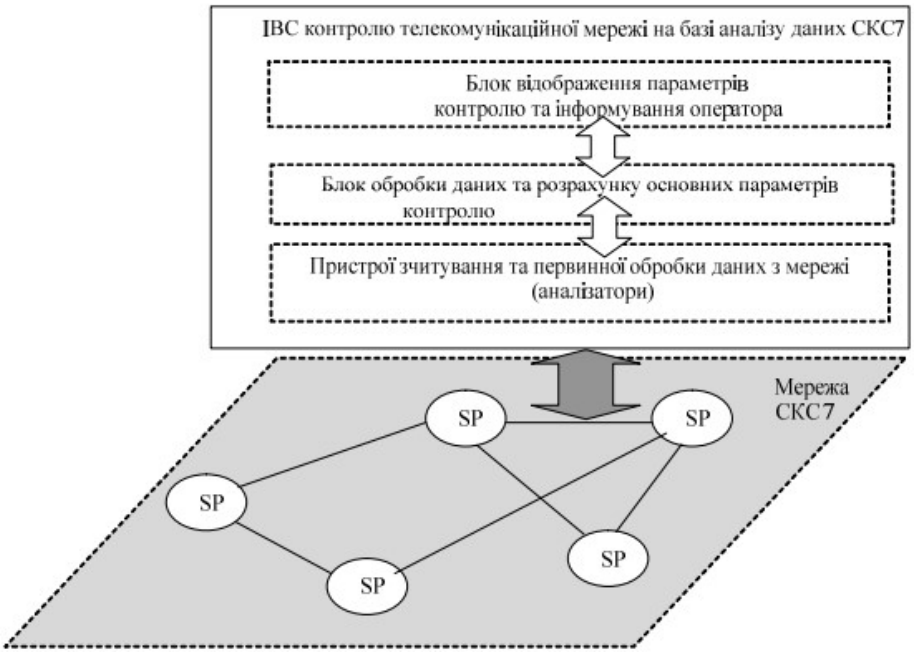

Рисунок А.1 – Узагальнена структура ІВС

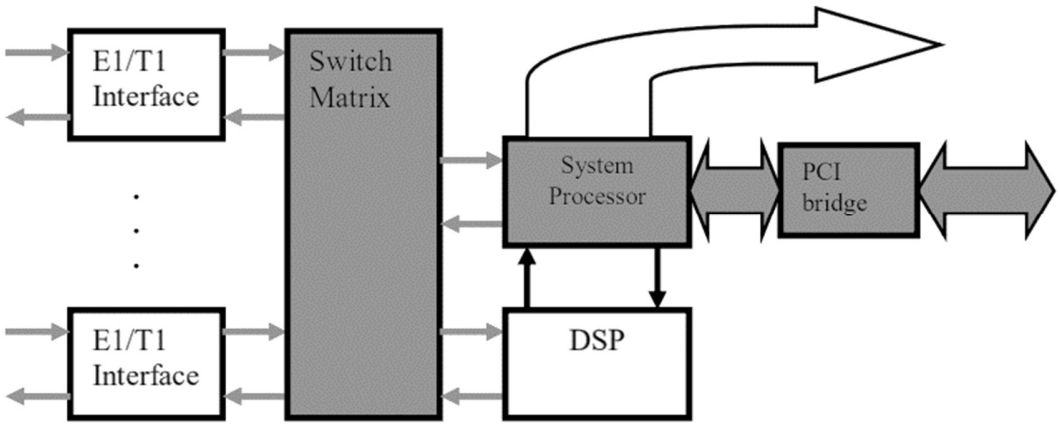

Рисунок А.2 – Загальна структура інтерфейсних модулів пристроїв прототипів

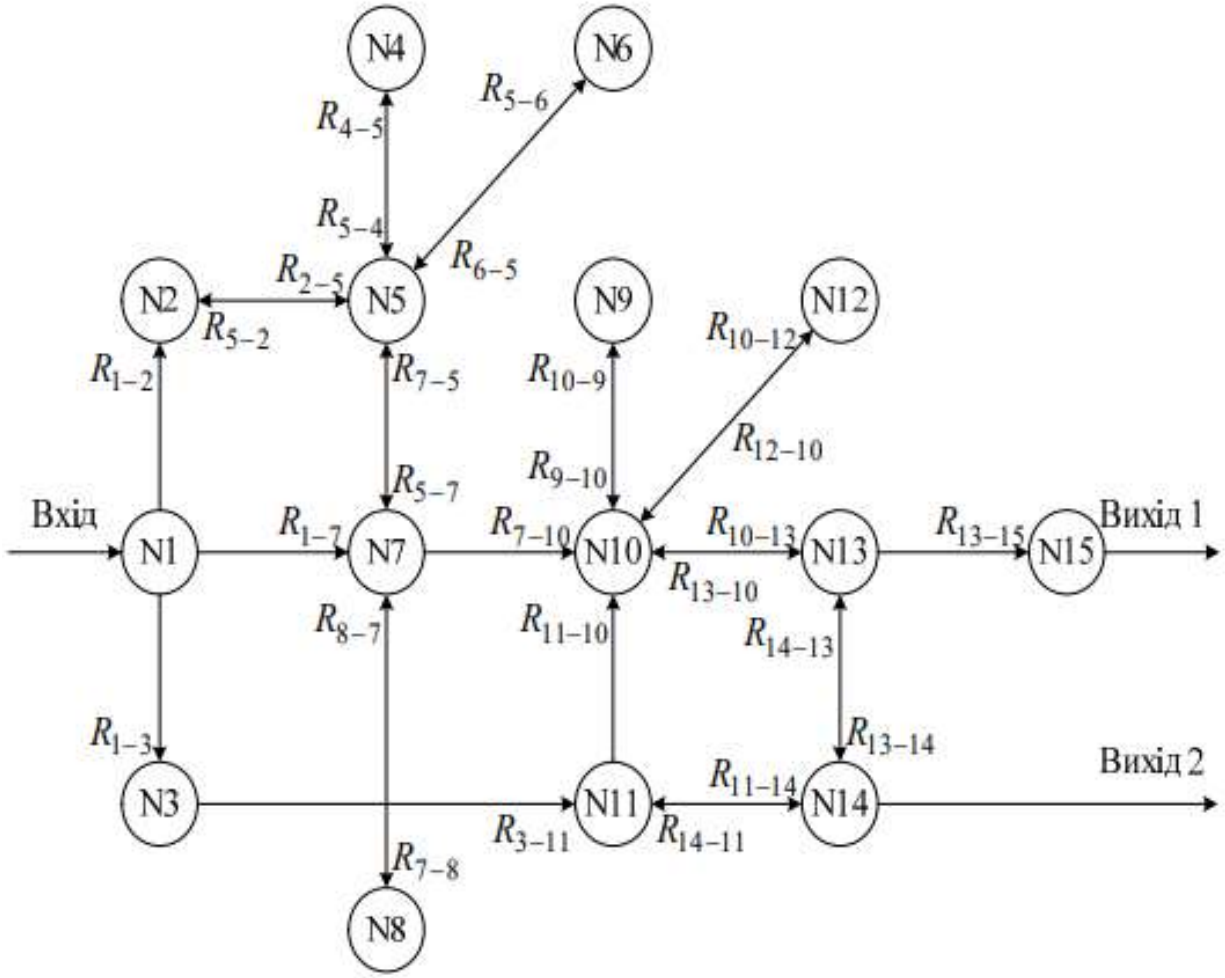

Рисунок А.3 – Модель надійності програмного комплексу системи контролю

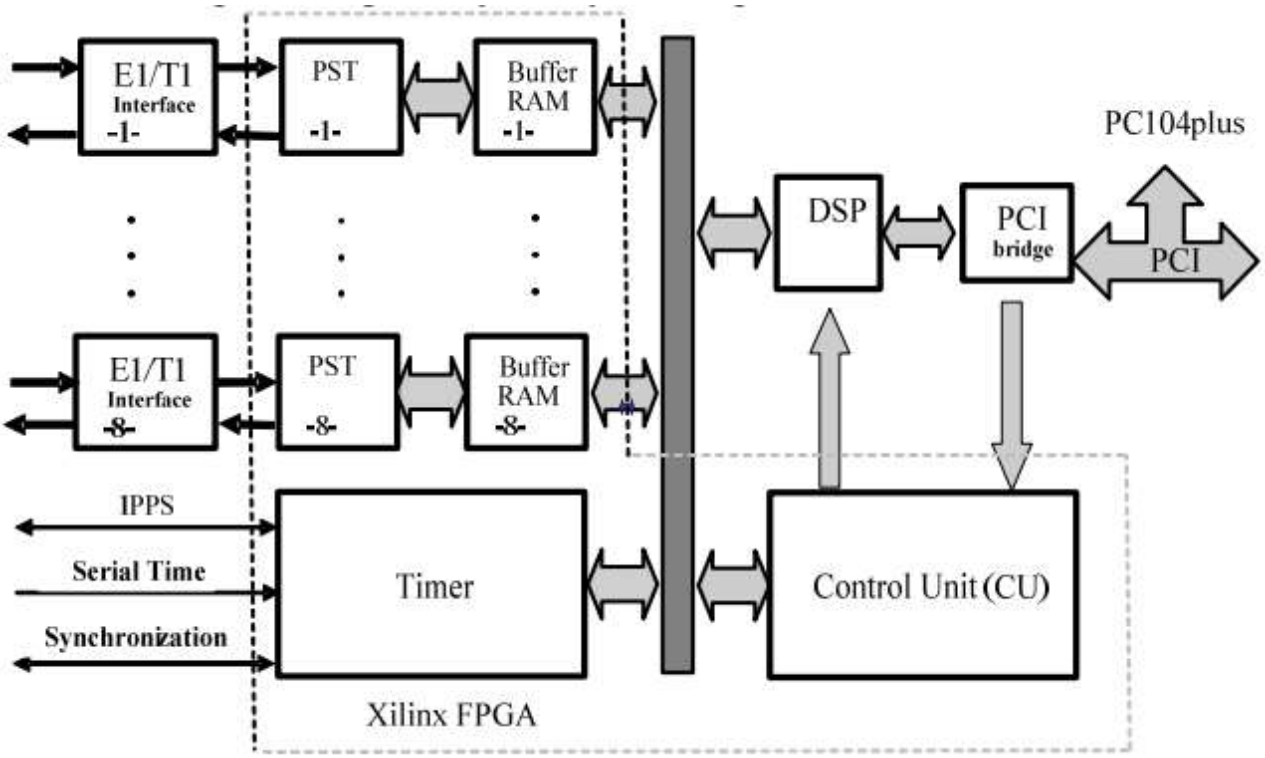

Рисунок А.4 – Структура інтерфейсного модуля на основі КЛС

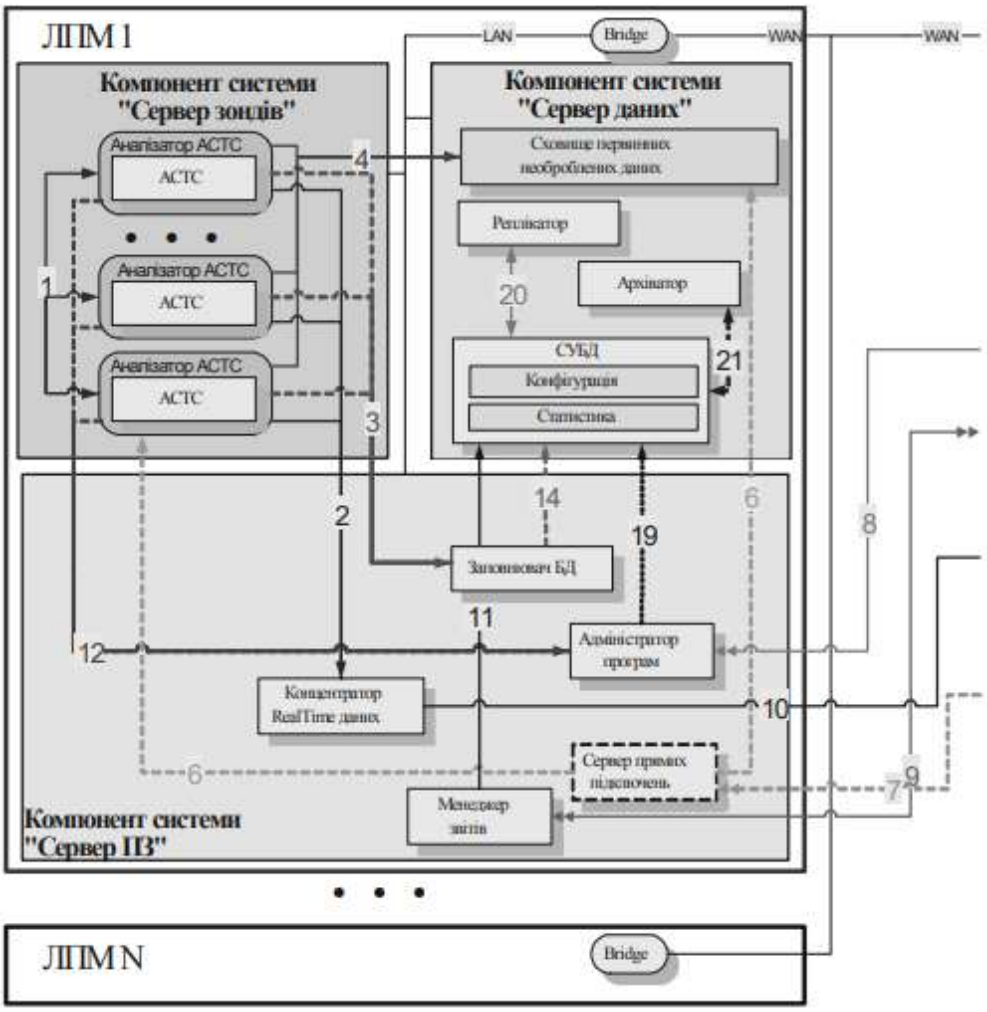

Рисунок А.5 – Архітектура системи модулів та потоків даних ЛПМ

Додаток Б
(обов`язковий)

ПРОТОКОЛ
ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ
НА НАЯВНІСТЬ ТЕКСТОВИХ ЗАПОЗИЧЕНЬ

Назва роботи: Розробка програмно-апаратних засобів контролю та моніторингу цифрових телекомунікаційних систем

Тип роботи: Бакалаврська дипломна робота
(БДР, МКР)

Підрозділ кафедра Інфокомунікаційних систем і технологій, факультет Інформаційних електронних систем
(кафедра, факультет)

Показники звіту подібності Unicheck

Оригінальність 92,52 % Схожість 7,48 %

Аналіз звіту подібності (відмітити потрібне):

■ 1. Запозичення, виявлені у роботі, оформлені коректно і не містять ознак плагіату.

☐ 2. Виявлені у роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і відсутності самостійності її виконання автором. Роботу направити на розгляд експертної комісії кафедри.

☐ 3. Виявлені у роботі запозичення є недобросовісними і мають ознаки плагіату та/або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень.

Особа відповідальна за перевірку _____ Васильківський М.В.
(підпис) (прізвище, ініціали)

Ознайомлені з повним звітом, який був згенерований системою Unicheck щодо роботи.

Автор роботи _____ Франчук О.В.
(підпис) (прізвище, ініціали)

Керівник роботи _____ Кичак В.М.
(підпис) (прізвище, ініціали)