МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
Факультет інженерії та енергетики
Кафедра електрифікації, автоматизації виробництва та інженерної екології

Кваліфікаційна робота
на правах рукопису

Олександрович Оксана Валеріївна

УДК 621.359.4

КВАЛІФІКАЦІЙНА РОБОТА

Аналіз будови найбільш важливих систем збору і передачі технологічної і діагностичної інформації в енергетиці
(тема роботи)

141 «Електроенергетика, електротехніка та електромеханіка»
(шифр і назва спеціальності)

Подається на здобуття освітнього ступеня магістр

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

Олександрович О. В.
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи

Рассадкіна Марина Валеріївна
(прізвище, ім'я, по батькові)
к.т.н., доцент кафедри вищої та прикладної математики
(науковий ступінь, вчене звання)

Житомир – 2023

АНОТАЦІЯ

Олександрович О. В. Аналіз будови найбільш важливих систем збору і передачі технологічної і діагностичної інформації в енергетиці. Кваліфікаційна робота на здобуття освітнього ступеня магістра за спеціальністю 141 – Електроенергетика, електротехніка та електромеханіка – Поліський національний університет, Житомир, 2023.

Метою роботи є аналіз способів розгортання систем діагностичного моніторингу високовольтних електроустановок за рахунок спільного використання каналів зв'язку пасивних волоконно-оптичних систем збору та передачі інформації та систем передачі діагностичної інформації установлюваних в системах безперервної технічної діагностики за основі побудови мережі на базі технології GPON.

Ключові слова: технічна діагностика, система передачі діагностичної інформації, пасивна оптична мережа, xPON , GPON, АСУТП.

ABSTRACT

Oleksandrovich O. V. Analysis of the structure of the most important systems of collection and transmission of technological and diagnostic information in the energy industry. Qualification work for obtaining a master's degree in specialty 141 - Electric power, electrical engineering and electromechanics - Polish National University, Zhytomyr, 2023.

The purpose of the work is to analyze the methods of deployment of diagnostic monitoring systems of high-voltage electrical installations due to the joint use of communication channels of passive fiber-optic information collection and transmission systems and diagnostic information transmission systems installed in continuous technical diagnostics systems based on the construction of a network based on GPON technology.

Keywords: technical diagnostics, diagnostic information transmission system, passive optical network, xPON, GPON, automated control system.

ЗМІСТ

ВСТУП

В останні десятиліття на зміну електромеханічним та статичним реле приходять системи та пристрої мікропроцесорного релейного захисту та автоматики (мікропроцесорні реле). Згідно з даними наведених статистик за встановленими мікропроцесорним реле у США на 2007 рік припадало від 30% (диференціальна захист шин) до 65% (захист генераторів) пристроїв [1]. За даними, наведеним в «Концепції розвитку релейний захисту і автоматики електромережевого комплексу» , в Україні на 2015 рік в експлуатації знаходиться 18,43% мікропроцесорних пристроїв загального числа пристроїв релейного захисту та автоматики (РЗА). Згідно з даними звіту прогнозу зростання ринку [2] мікропроцесорного релейного захисту з 2016 по 2021 очікується зростання за п'ять наступних років не менше ніж на 30% до 4,54 млрд. дол., що свідчить про тенденцію збільшення кількості мікропроцесорних реле, що зберігається. в складі систем релейної захисту і автоматики у всьому світі.

Сучасні мікропроцесорні реле являють собою не тільки пристрої, що забезпечують захист електроустановок різних класів напруги, але й мають можливістю виконувати функції систем контролю і управління, телемеханіки, моніторингу і контролю РЗА і протиаварійної автоматики (ПА). Дані функції реалізуються при опитуванні мікропроцесорних реле, що входять до системи збору та передачі інформації (СЗПІ), по окремим каналам зв'язку. Перспектива розвитку концепції «цифровий підстанції» визначає необхідність розгортання вже єдиної внутрішньооб'єктної СЗПІ для систем РЗА, SCADA та інших систем автоматизації згідно стандарту ПЕК 61850 [3].

На тлі зростання кількості виконуваних мікропроцесорними реле функцій, до обладнання і каналам зв'язку пред'являються все більше високі вимоги по надійності, швидкодії, резервування, а також по електромагнітній сумісності, аж до створення підстанційних мереж з нульовими втратами пакетів даних [4]. Економічний аспект також є важливим складником

можливості впровадження інноваційних рішень. У більшості випадків рішення, що приносять якісний технологічний ефект, але які призводять до подорожчання, тривалий час не можуть знайти широкого застосування. Тому **актуальним є напрямок** пошуку компромісних рішень, які містять в собі переваги нових технологій, усувають недоліки старих і надають додаткові функції, покращують продуктивність та надійність систем в загалом, при цьому є економічно обґрунтованими.

Найчастіше для об'єктів середнього класу напруги вартість розгортання СЗПІ співвідносна зі вартістю самих об'єктів. На об'єктах високого класу напруги вартість розгортання таких систем виправдана, оскільки аварійні ситуації і пов'язані з ними перерви в електропостачанні неприпустимі за вимогами надійності та якості електропостачання великих промислових та комунальних споживачів, вимогам забезпечення режимів роботи мережі, а також через супроводжуючого їх значного економічного шкоди.

Метою роботи є аналіз способів розгортання систем діагностичного моніторингу високовольтних електроустановок за рахунок спільного використання каналів зв'язку пасивних волоконно-оптичних систем збору та передачі інформації (СЗПІ) АСУТП та систем передачі діагностичної інформації (СПДІ) установлюваних в системах безперервної технічної діагностики за основі побудови мережі на базі технології GPON.

Ціллю роботи є аналіз організації та розробка основ стандартизації технології PON та активне виведення її на ринок для Ethernet та IP-трафіку.

Методи дослідження. Аналіз поточного стану об'єктів електромережевого комплексу, технічна діагностика, аналіз системи збору та передачі інформації, системи передачі діагностичної інформації, економічні способи розгортання систем діагностики та моніторгу.

Перелік публікацій автора за темою дослідження :

Гончаренко Ю. П., Олександрович О. В. РЕЛІЙНИЙ ЗАХИСТ ЧЕРЕЗ ПАКЕТНІ МЕРЕЖІ. ТЕСТУВАННЯ SDH-МУЛЬТИПЛЕКСОРА ДОСТУПУ

Матеріали VII Міжнародна науково-практичної конференції «Біоенергетичні системи» 15-17 листопада 2023 року. Житомир: Поліський національний університет, 2023.- С 47-49.

Гончаренко Ю. П., Олександрович О. В. АНАЛІЗ МОЖЛИВОСТЕЙ ПЕРЕХОДУ НА МЕРЕЖІ З ПАКЕТНОЮ ТЕХНОЛОГІЄЮ ПЕРЕДАЧІ СИГНАЛІВ РЕЛЕЙНОГО ЗАХИСТУ

Матеріали науково-практичної конференції науково-педагогічних працівників, докторантів, аспірантів та молодих вчених факультету інженерії та енергетики «НАУКОВІ ЧИТАННЯ – 2023». 25 жовтня 2023 р. Житомир: Поліський національний університет, 2023.- С 106-108.

Олександрович О. В. ОСНОВИ ТЕХНОЛОГІЇ ТА ОСОБЛИВОСТІ БУДОВИ GPON

Матеріали міжнародної науково-практичної конференції «Інженерні процеси та системи» 14-15 червня 2023 року. Житомир: Поліський національний університет, 2023.- С 47-51.

РОЗДІЛ 1
ТЕХНОЛОГІЇ ПЕРЕДАЧІ ДАНИХ У СУЧАСНИХ СИСТЕМАХ РЕЛІЙНОЇ ЗАХИСТИ І АВТОМАТИКИ І ЇХ ПОКАЗНИКИ ЯКОСТІ

Аналіз поточного стану об'єктів електромережевого комплексу країни показує, що на 2021 р. стан ЄЕС характеризується наступним обсягом обладнання із понаднормативним терміном служби: 59% для ПС (понад 25 років) та 49% для ЛЕП –18% [2].

Стан повітряних ліній Єдиної національної електричної мережі на 01.01.2021 р. характеризувався таким співвідношенням (за протяжністю):

- "Робочий" стан - 46%;
- "погіршений" стан - 52%;
- "передаварійний" стан - 2%.

Загальна частка технологічних порушень в електромережевому комплексі через причини, пов'язані зі старінням (зносом) обладнання, за підсумками 2020 року склала 24%.

Для продовження термінів служби дорогого високовольтного електрообладнання та підвищення надійності мережі загалом необхідно впроваджувати системи та пристрої технічної діагностики та безперервного моніторингу стану обладнання [2]. Технічна діагностика в режимі реального часу дозволяє оперативно виявити пошкодження та дефекти робочих частин електрообладнання на початкових етапах розвитку та запобігати виникненню аварійних ситуацій. Проте впровадження систем безперервної технічної діагностики та моніторингу сьогодні є дорогим заходом, особливо для найпоширеніших у міських, приміських та промислових електричних мережах електроустановок (ЕУ) середньої напруги (СН). Також актуальним завданням, у зв'язку зі складністю та дорожнечею заходів щодо дотримання вимог електромагнітної сумісності в ЕУ при застосуванні «мідних» каналів зв'язку в системах збору та передачі інформації (СЗПІ) в автоматизованих системах управління технологічним процесом в електроенергетиці.

1.1 Проблема електромагнітних впливів

– При розгортанні СЗПІ на об'єктах електроенергетики також необхідно враховувати вплив складною електромагнітної обстановки всередині високовольтного електроустаткування, через яке або поряд з якими прокладено канали зв'язку та встановлено обладнання СЗПІ. Згідно з даними статистики, зазначеними в «Концепції розвитку релейний захисту і автоматики електромережевого комплексу», в 2014 року зафіксовано порядка 1400 випадків неправильного спрацьовування релейного захисту та автоматики, з них по нез'ясованим причин зафіксовано 38 випадків, по неправильним вказівкам 6, за іншими – 198. Зазначені формулювання не дозволяють точно судити про те, що спричинило хибне спрацювання, проте очевидно: одним із факторів є вплив перешкод на канали зв'язку.

Незважаючи на те, що всі пристрої та канали зв'язку без перевірки на відповідність стандартам електромагнітної сумісності не вводяться в експлуатацію, повністю виключити вплив перешкод неможливо [5]. Ця проблема є актуальною у всьому світі. Наприклад, за даними японських компаній-виробників [6] ушкодження систем мікропроцесорних реле від електромагнітних впливів число тимчасових і постійних ушкоджень складає, в середньому, 6 випадків за рік.

Традиційно для організації передачі даних у СЗПІ на об'єктах енергетики різних класів напруги, в даний час у більшості випадків використовуються канали зв'язку з урахуванням *RS-485* і *Ethernet* , переважно на основі крученої пари. Однак усі частіше виробники, на вимогу замовника, встановлюють оптичні перетворювачі інтерфейсу для *RS-485* або високошвидкісні оптичні порти *Ethernet* . Дані рішення дозволяють використовувати переваги оптичних передавачів:

— надійність каналів зв'язку;
— висока швидкість передачі даних;
— завадозахищеність;
— широка смуга пропускання;

— можливість використання спектрального ущільнення (організація повнодуплексного зв'язку з використанням всього одного хвилеводу);

— пожежна безпека;

— гарантована пропускна здатність (при використанні синхронної/плезіохронної цифрової ієрархії мережі (*SDH/PDH*);

— можливість створення протяжних ліній зв'язку.

Незважаючи на очевидні переваги, для організації мережі на основі оптичних каналів зв'язку потрібне складне активне комунікаційне обладнання – оптичні комутатори, ціна яких у рази вища за їх традиційні аналоги, що обмежує широке застосування оптичних рішень, які підвищують надійність електропостачання, а також керованість енергооб'єктами в загалом.

Слід зазначити, що сьогодні економічно доцільним для об'єктів середнього напруги стає побудова систем релейний захисту або систем сигналізації не на основі окремих мікропроцесорних реле (захищаючих свій окремий фідер), а в якості єдиної для всього об'єкта централізованою системи управління, захисту і сигналізації, представляючою собою сукупність мікропроцесорних пристроїв приєднань, високонадійної СЗПІ і центрального управителя вузла. СЗПІ в такому випадку є основним вузлом, визначальним надійність, якість і функціонал роботи централізованою системи, що, в свою черга, пред'являє значні вимоги як до прокладених на об'єкті каналів зв'язку, так і до надійності та завадостійкості пристроїв СЗПІ.

Порівняння каналів передачі даних технологій зв'язку на підстанціях по виконується по двом параметрам:

— пінг - час, який потрібен пакету даних, щоб досягти вибраного пристрою через мережу, а потім прийти назад на вихідний пристрій;

— *BER (Bit Error Rate)* - співвідношення між правильно переданими бітами інформації і неправильно переданими.

1.2 Показники якості інтерфейсу *RS-485*

Інтерфейс *RS-485* - широко поширений інтерфейс зв'язку в промисловості

і енергетиці в зокрема, що обумовлюється його гнучкістю, простотою програмування та порівняно високою швидкістю передачі даних (до 10 Мбіт/с). Традиційна архітектура СЗПИ з урахуванням даного інтерфейсу показано на рис.1.1.

Існують фактори, що обмежують за певних умов можливості цього інтерфейсу:

- довжина кабелю;
- конструкція кабелю;
- імпеданс кабелю – ємність та індуктивність згладжують форму імпульсів, що підвищує ймовірність виникнення помилки при передачі даних;
- запас завадостійкості;
- швидкість наростання вхідної напруги драйвера;
- узгодження кінцевого навантаження – якісне узгодження зводить відображення сигналу до мінімуму, підвищуючи якість обміну в цілому.

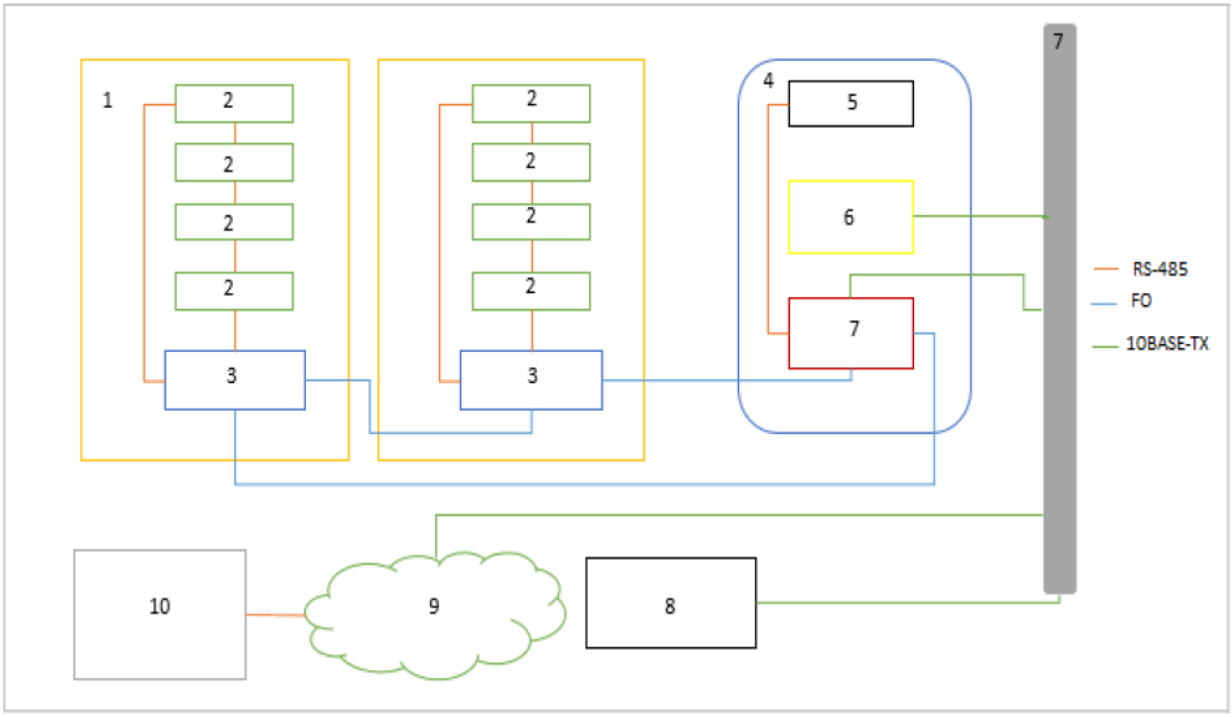

Рисунок 1.1. Архітектура підстанційної мережі з урахуванням RS-485: 1 – шафи польового рівня; 2 – модулі вхідних, вихідних дискретних сигналів, аналогових уніфікованих сигналів; 3 – медіаконвертер RS-485/FO; 4 – шафа комунікаційного рівня; 5 – GPS – модуль синхронізації; 6 – Ethernet-

комутатор; 7 – LAN – протокол DNP3; 8 – АРМ; 9 – протокол МЕК60870-5-104/5-101; 10 – диспетчерський центр, FO - ВОЛЗ

Розглянемо основні показники якості інтерфейсу RS-485:

1) Максимальний час обходу пакета основним шляхом T_{max} визначається за таким виразом [7]:

$$T_{\max} = \left(T_{пак} + T_{зат} + T_{шлях}\right) \cdot N_k = \left(\frac{N_p + 2}{10^6} + 10^{-3} + \frac{l \cdot 2}{3 \cdot 10^8}\right) \cdot N_k \ , \qquad (1.1)$$

де $T_{\text{пак}}$ - час відправлення пакета, с; $T_{\text{зат}}$ - час затримки в мультиплексорі (5 мкс); $T_{\text{шлях}}$ - час доставки повідомлення по оптоволокну, с; $N_{\text{р}}$ – розмір пакета повідомлення (байт): N_{k} – кількість вузлів у кільці; l - Отримані середня відстань між вузлами, м.

$$T_{\max} = \left(\frac{8+2}{10^6} + 10^{-3} + \frac{3 \cdot 2}{3 \cdot 10^8}\right) \cdot 5 = 0,005 \text{ с.}$$

Як очевидно з розрахунків, повна затримка залежить, переважно, від швидкодії вхідних регістрів, накладають основні обмеження використання інтерфейсу RS-485 в сучасних СЗПІ. Ця затримка є приємленою для доставки керуючих сигналів та сигналів автоматизованого опитування мікропроцесорних реле. Однак для каналів зв'язку ПА та для критичних повідомлень між мікропроцесорними реле цей поріг не повинен перевищувати 5-10 мс [8].

2) Джіттер та *BER*. Як приклад розглянемо дослідження показників максимальної продуктивності системи зв'язку з урахуванням інтерфейсу RS-485. Для випробування використовувалася кручена пара 5 категорії, передача велася на швидкості від 1 до 39 Мбіт/секунд при довжині кабелю від 90 до 270 метрів. За результатами випробувань, наведених у роботі [9] при дослідженні показників інтерфейсу RS-485 мережі RS-485 здатні забезпечувати швидкість обміну даними до 52 Мбіт/с при довжинах кабелю, що досягають сотні метрів без ретрансляторів або перетворювачів інтерфейсів.

Незважаючи на всі переваги інтерфейсу RS-485, вимоги до каналів та інтерфейсів зв'язку в енергетиці з кожним роком все вище. Ця тенденція

пов'язана з постійним збільшенням навантаження та ускладненням схем електричних мереж, появою множини щодо малопотужної генерації в різних точках мережі. Також спостерігається тенденція до появи нових протоколів зв'язку (наприклад, протоколи в рамках міжнародного стандарту МЕК 61850), що ведуть до ускладнення мікропроцесорних реле, удосконалення алгоритмів захисту та введення нових функцій. До того ж, помітний інтерес до підвищення «прозорості» та керованості електроенергетичних об'єктів, що неможливо здійснити при використанні усталених технологій, в першу чергу, через обмежену пропускну спроможність та вразливість їх до наявних на об'єктах електроенергетики електростатичних розрядів.

При ситуації, що склалася, актуальним є впровадження нових рішень, що дозволяють здійснювати надійний високошвидкісний обмін пакетами даних на енергооб'єктах різних класів напруги.

1.3 Показники якості *Ethernet*

Застосування технології мереж *Ethernet* на об'єктах енергетики для контролю та моніторингу режимів у реальному часі стало можливим завдяки розробці провідними виробниками мережного обладнання, здатного працювати в умовах жорсткої електромагнітної обстановки, та стандартів, що описують правила взаємодії елементів комунікаційних мереж. Комунікаційний протокол *Industrial Ethernet (IE)* було адаптовано під особливості пристроїв контролю, таких як *RTU*, мікропроцесорне реле, пристрої систем автоматизації енергооб'єктів. Внутрішньопідстанційна мережа на основі *Ethernet* показана на рис. 1.2.

Технологію *Industrial Ethernet* було обрано для реалізації стандарту МЕК 61850 в енергетиці. Однією з особливостей МЕК 61850 є так звана організація внутрішньостанційної шини техпроцесу, що поєднує польові пристрої, цифрові вимірювальні перетворювачі з мікропроцесорними реле, пристроями протиаварійної автоматики та системами автоматизації на підстанції, що є за термінологією стандарту - інтелектуальні електронні пристрої (IED) (рис.1.3).

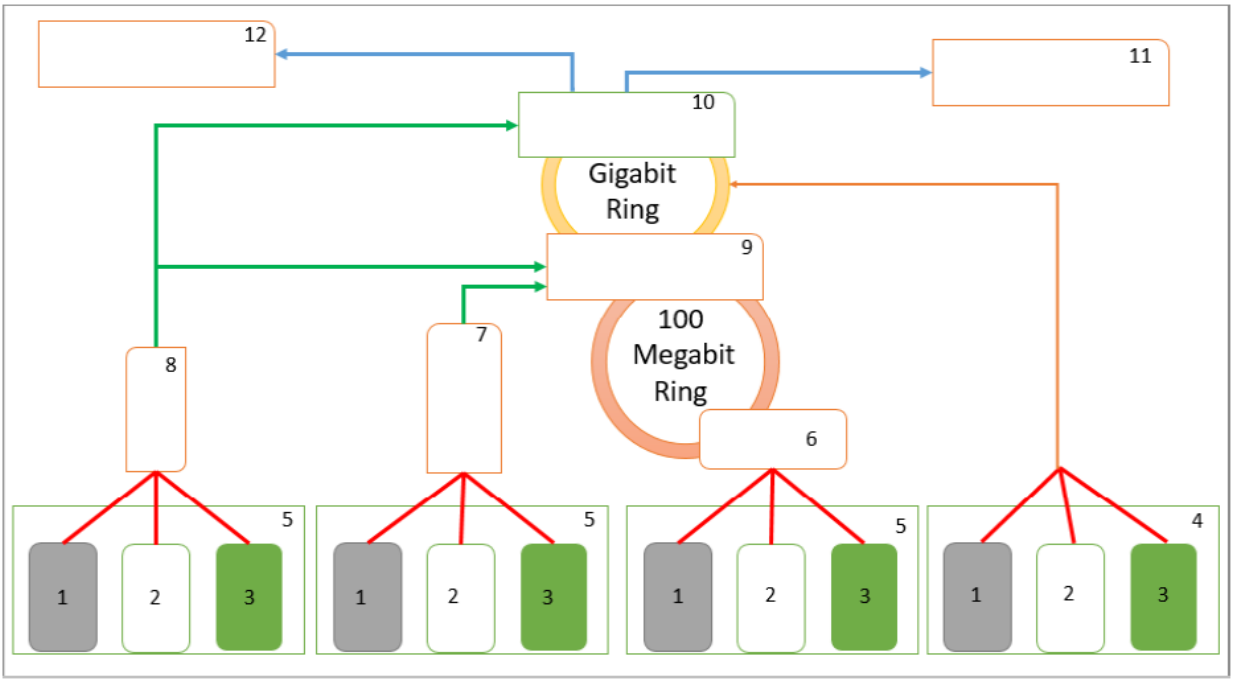

Рисунок 1.2 – Внутрішньооб'єктна СЗПІ на базе *Ethernet*: 1 – *Relay*; 2 – *RTU*; 3 – *IED*; 4 – МЕК 61850; 5 – *Не* МЕК 61850; 6 – *RS* 232/422/485 - *Ethernet* медіа конвертертер; 7 – комунікаційний шлюз; 8 – термінальний сервер; 9 – маршрутизатор другого рівня; 10 – маршрутизатор третього рівня; 11 – АРМ; 12 – *Scada HMI*

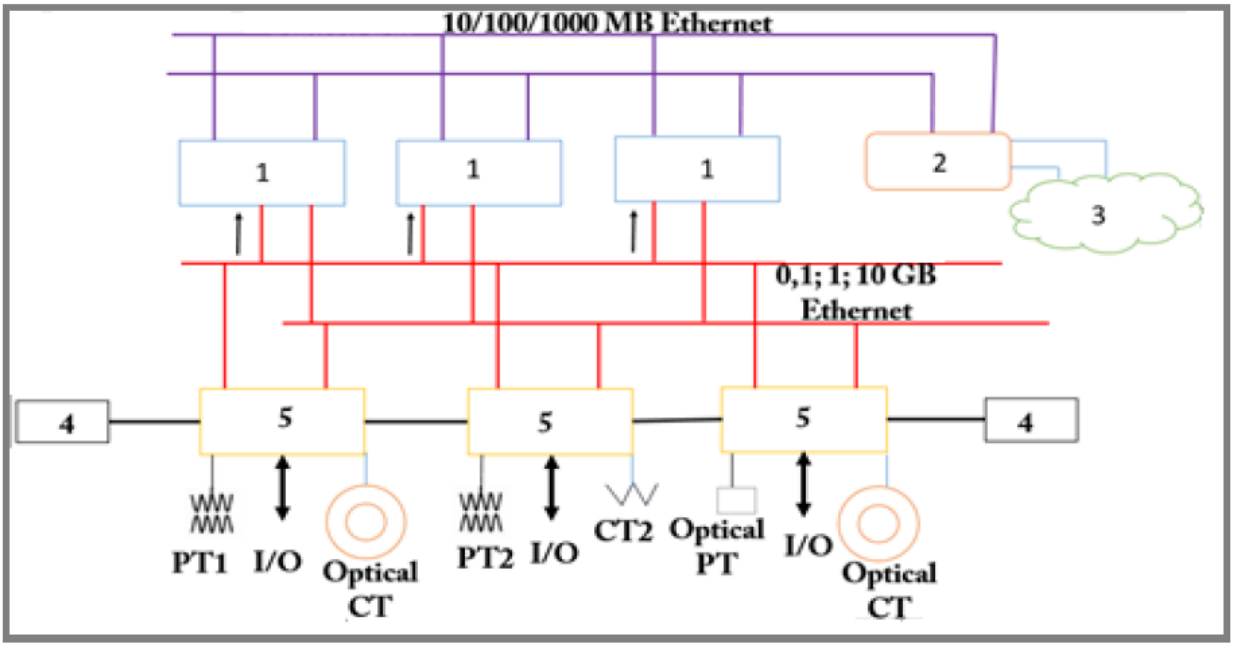

Рисунок 1.3 - Модель підстанції відповідно до МЕК61850: 1-реле; 2-сервер віддаленого доступу; 3 – зовнішня мережа; 4 – блок синхронізації; 5 – інтелектуальний електронний пристрій; РТ – силовий трансформатор; *Optical*

CT –оптичний трансформатор струму; *CT* – традиційний трансформатор струму

Розглянемо показники якості каналів зв'язку на основі Ethernet для найбільш вимогливої до надійності, пропускної спроможності та гарантованості доставки даних комунікаційної системи МЕК 61850:

1) Максимальний час обходу кільця основним шляхом $T_{\max}$ визначається за таким виразом [7]:

$$T_{\max} = \left(T_{пак} + T_{зат} + T_{шлях}\right) \cdot N_k = \left(\frac{N_p + 2}{10^6} + 10^{-3} + \frac{l \cdot n_{ov}}{3 \cdot 10^8}\right) \cdot N_k \ , \qquad (1.3)$$

де $T_{пак}$ - час відправлення пакета, с; $T_{зат}$ - час затримки в мультиплексорі (5 мкс); $T_{шлях}$ - час доставки повідомлення по оптоволокну, с; N_p – розмір пакета повідомлення (байт): N_k – кількість вузлів у кільці; l - Отримані середня відстань між вузлами, м; n_{ov} - показник заломлення оптоволокна (1,45-1,55).

Стандартна довжина пакетів *GOOSE* складає 1500 байт для пакетів *Sample Value* (*SV, IEC* 61850-9-2 *(LE)*) – 163 байт, кількість вузлів у кільці не перевищує 3 метри, середня відстань між вузлами l у межах підстанції становить 5 метрів.

Тоді передачі пакетів *SV* максимальний час складе $T_{\max}$ = 56 мкс; для *GOOSE* повідомлень: $T_{\max}$ = 377 мкс. Отримані значення є прийнятними у плані швидкодії оперативної реакції при аваріях, що відповідно до вимог стандарту МЕК-61850, має перевищувати 4 мс [8].

2) Згідно з даними лабораторії університету Нью Хемпшира [11], обладнання *Ethernet* стандартів *IEEE* 802.3 демонструє функціональні характеристики та припускає наявність помилок у пакетах, затверджених при їх розробці, з точністю 95%. Зокрема, показник якості *BER* і, відповідно, кількість неправильно переданих кадрів багато в чому залежить від конкретного обладнання, конфігурації мережі, захищеності каналів зв'язку та зовнішніх умов і лежить у межах 10-8-10-12. Проте механізм прямої корекції помилок *FEC (Forward Error Correction)*, реалізований у тому чи іншому вигляді, дозволяє звести і так їх мале число до нуля, знижуючи, однак,

загальну пропускну спроможність мережі. Відповідно до стандарту МЕК 61850 [3], механізм доставки *GOOSE*-повідомлень є передачею інформації в широкомовному діапазоні, а отримання адресатом повідомлення при цьому відсутня, тому *GOOSE*-повідомлення передаються з особливою періодичністю в встановленому режимі. Передача пакетів *SV* здійснюється так: при втраті будь-якого з пакетів дані не передаються повторно, а відновлюються вже у адресата завдяки алгоритму відновлення втрачених даних за допомогою лінійної інтерполяції [3]. Дані принципи доставки дозволяють знизити область використання *FEC*-механізму, підвищуючи при цьому потенційну пропускну спроможність мережі.

Порушення роботи мідних каналів зв'язку в умовах електромагнітної обстановки на підстанціях через наведення при попаданні блискавки в ОРУ або поруч із підстанцією, згідно з численними даними статистики [6], призводить до помилкових спрацьовувань пристроїв релейного захисту, неправильним показанням і нерідко – до необхідності заміни дорогого вторинного обладнання. У зв'язку з чим є тенденція використання оптичних медіаконвертерів, що підвищують складність та вартість СЗПІ в цілому не тільки в частині обладнання, але і при пуско-налагодженні, і надалі обслуговування системи.

Забезпечення надійного високошвидкісного зв'язку всередині підстанції на основі *Ethernet* на сьогоднішній день є вирішеним завданням, проте створення повноцінного мережі з усіма заходами безпеки, резервуванням і якістю даних, що передаються є дуже дорогим заходом, зокрема через високу ціну промислових комутаторів, маршрутизаторів та шлюзів.

1.4 Показники якості *GPON*

В даний час, у зв'язку з появою та поширенням у телекомунікаційній сфері більш дешевих рішень на основі технологій *xPON (Passive Optical Network; PON)*, побудова мереж з волоконно-оптичними лініями зв'язку стає більш доступною. Зокрема, одним із найуспішніших у цій сфері є стандарт *GPON (Gigabit PON)*. Ключовими особливостями *GPON* є використання тільки

одного приймально-передаючого пристрою *(Optical Linear Terminal)* для прийому та передачі інформації безлічі пристроїв, що приймають *(Optical Network Unit або Optical Network Terminal)*. При цьому, на відміну від традиційних мереж, побудованих на оптоволокні, немає необхідності встановлення активних пристроїв у вузлах мережі; замість них від основного кабелю робляться відгалуження за допомогою оптичних спліттерів, у зв'язку з чим топологія мережі є «деревом з пасивними вузлами».

Ключовими аспектами даної технології, що дозволяють впровадити її на об'єкти електроенергетики, є:

- можливість встановлення модульних компактних трансіверів у форматі стандарту *SFP (Small Form-factor Pluggable)* у мікропроцесорні реле або контролери приєднань *(bay-controller) SCADA* для організації каналів зв'язку СЗПІ;

- компактність спліттерів дозволяє їх розмістити в обмежених просторах, аж до відсіків РЗА в осередках середньої напруги;

- форматонезалежність кадрів, що передаються;

- маршрутизація пакетів реалізована в самих приймально-передаючих пристроях завдяки механізму управління даними *GTC*;

- стандарт *GPON* підтримує наступні швидкості: низхідний трафік (від *OLT*) транслюється на швидкості 1,25 – 2,5 Гбод, висхідний від *(ONT)* – на швидкостях 0,155 – 1,25 Гбод.

На рис. 1.4 показано архітектуру внутрішньопідстанційної СЗПІ на основі технології *GPON*. Як пристрій приєднання виступає вимірювальний багатофункціональний контролер ЕНІП-2, оскільки він представляється нам оптимальним варіантом за техніко-економічними показниками [4].

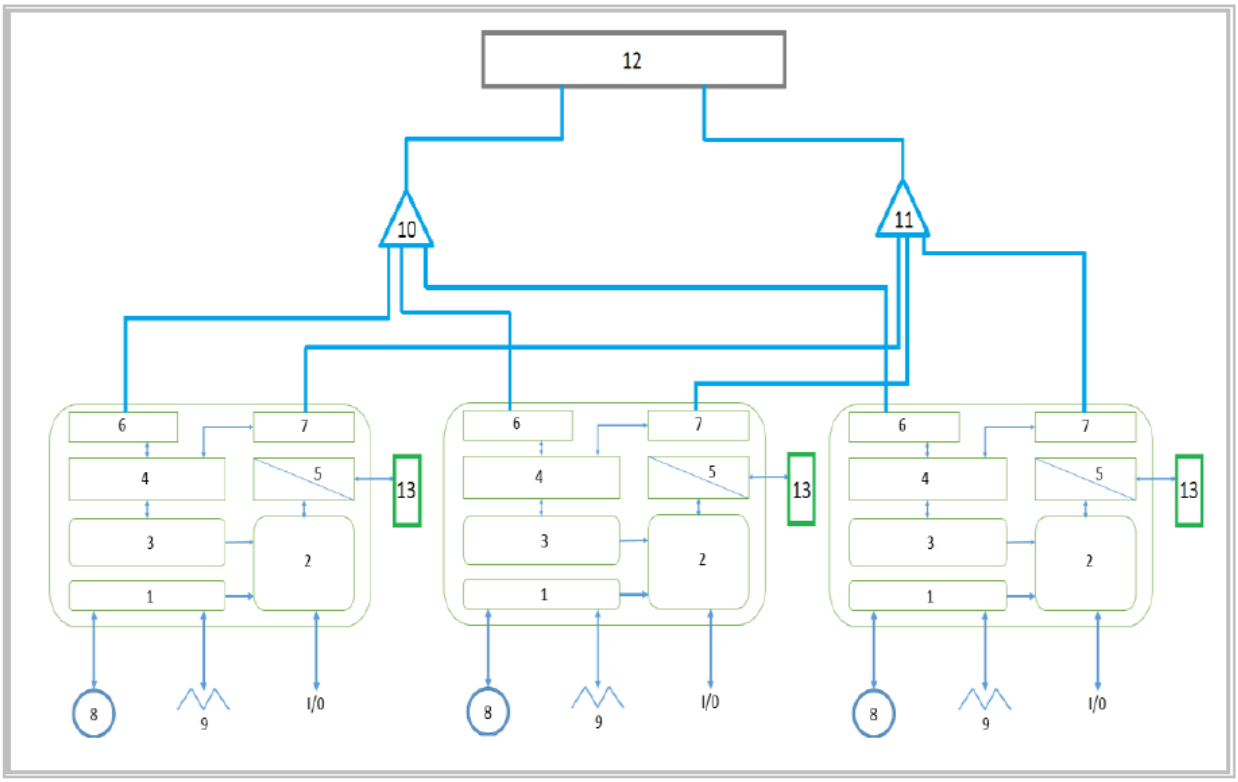

Рисунок 1.4 - Архітектура СЗПІ з урахуванням технології *GPON*: 1–АЦП, 2 – Сигнальний процесор; 3 - 1000 Мбод мікроконтролер *Ethernet*; 4 - медіаконвертер *RGMII-SGMII*; 5 – медіаконвертер *RS*-485; 6 – *SFP*-модуль *GPON (ONT)*; 7 – резервний *SFP*-модуль *GPON (ONT)*; 8 – трансформатор напруги; 9 – трансформатор струму; 10 - оптичний спліттер; 11 – резервний оптичний спліттер; 12 – комутатор із підтримкою *GPON (OLT)*; 13 – лічильник

Далі розглянемо показники якості каналів зв'язку внутрішньооб'єктної мережі з урахуванням технології *GPON*.

1. Затримка доставки повідомлень

а) Час доставки *GTC*-кадрів у низхідному напрямку $T_{\max}$, мкс визначається за формулою

$$T_{\max} = \left(T_{пак} + T_{зат} + T_{шлях}\right) \cdot N_k = \left(125 \cdot 10^{-9} + \left(25,7 + 70,7\right) \cdot 10^{-9} + \frac{l \cdot n_{ov}}{3 \cdot 10^8}\right) = 125 \ , (1.4)$$

де $T_{пак}$ - час відправлення пакета стандартної довжини 38880 байт (с), що дорівнює 125мкс; $T_{зат}$ - сторожовий інтервал, що формується з наступних значень: T_{lazer} - час перемикання лазера (25,7 нс) та T_{pad} - час обробки преабули (70,7 нс); $T_{шлях}$ - час доставки повідомлення по оптоволокну, с; l –відстань до

найдальшого приймача, м; n_{ov} – показник заломлення оптоволокна (1,5).

б) Час доставки *GTC*-кадрів у верххідному напрямку T_{max}, мкс визначається за формулою

$$T_{\max} = \left(T_{пак} + T_{зат} + T_{шлях}\right) \cdot N_k = \left(125 \cdot 10^{-9} + \left(25,7 + 70,7\right) \cdot 10^{-9} + \frac{l \cdot n_{ov}}{3 \cdot 10^8}\right) = 125 \ , \quad (1.5)$$

де $T_{пак}$ - час відправлення пакета стандартної довжини 19440 байт (с), що дорівнює 125 мкс; $T_{зат}$ - сторожовий таймер, що складається з T_{laser} - час перемикання лазера (25,7 нс) та T_{pad} - преамбула (70,7 нс); Тшляху - час доставки повідомлення по оптоволокну (с); l -відстань до найдальшого приймача, м; n_{ov} – показник заломлення оптоволокна (1,5).

Час затримки доставки повідомлення залежить від величини буфера: при малій величині буфера, наприклад 10 Мбайт, час затримки може досягати десятка мілісекунд, що показано в дослідженні динамічної лінії пропускання технології *GPON* [11].

Висновки по першому розділу

Застосування стандарту *Industrial Ethernet (IE)* у СЗПІ на підстанціях стрімко набирає своєї популярності, що можна судити з кількості рішень, представлених над ринком. Однак обмеження використання недосконалого, з погляду перешкодобезпеченості, *IE* на базі мідних каналів зв'язку та дорожнечі *IE* з використанням оптичних медіаконвертерів дозволяють зробити висновок про актуальність пошуку альтернативних рішень, що пропонують компроміс між ціною обладнання та перешкодозахищеністю каналів зв'язку.

Рішення на основі пасивних оптичних мереж є альтернативою, здатною вирішити цю проблему. Показники якості каналів зв'язку технології *GPON* задовольняють усім вимогам для використання каналів зв'язку в РЗА, *SCADA*-системах і системах моніторингу РЗА і ПА. Особливості *GTC*-механізму передачі даних дозволяють здійснити перехід на *GPON* без додаткових проблем, оскільки даний механізм багато в чому схожий на *SDH*-технологію, що вже успішно використовується в електроенергетиці.

Однією з переваг технології *GPON* є вбудована високоточна синхронізація та гарантія доставки повідомлення в межах 125 мкс, що є критично важливим для передачі аварійних сигналів, сигналів релейного захисту та збереження стійкості роботи електроенергетичної мережі в цілому. Особливо важливою перевагою даної технології є підтримка *SFP*-модулів різних конфігурацій, які підтримуються інтерфейсами сучасних пристроїв приєднань (наприклад, ЕНІП-2). Також існують конфігурації *SFP*-модулів, що дозволяють організовувати канали зв'язку як на одному оптоволокні за допомогою технології *WDM*, так і двох роздільних для низхідного і висхідного трафіку, що важливо для створення резервних каналів зв'язку.

Застосування технології *GPON* для побудови СЗПІ в централізованих системах управління, захисту та сигналізації на енергооб'єктах середнього класу напруги може забезпечити високонадійний, стійкий до перешкод і високошвидкісний обмін даними між пристроями приєднань і центральним вузлом, причому економічно доцільним способом .

РОЗДІЛ 2
ПОБУДОВА МЕРЕЖІ НА ОСНОВІ ТЕХНОЛОГІЇ GPON

Технологія пасивних оптичних мереж (PONs , Passive Optical Networks) починає свій розвиток з 1995 р., коли група з семи компаній (British Telecom, France Telecom, Deutsche Telecom, NTT, KPN, Telefonica та Telecom Italia) заснувала консорціум (FSAN, Full Service Access Network). Метою організації є розробка основ стандартизації технології *PON* та активне виведення її на ринок для Ethernet та IP-трафіку.

У дослідницької групи 15 ITU-T з'явилася серія базових рекомендацій, які детальніше обговорюються нижче.

G.984.1 – це документ, в якому описано архітектуру, а також викладено основні експлуатаційні характеристики та вимоги до продуктивності GPON-систем. Відповідно до G.984.1 при певних умов можна здійснювати також передачу інформації на далекі відстані (60 км) і забезпечувати високий рівень розгалуження (128 абонентських вузлів ONU), що виходить за межі можливостей PON-систем.

2.1 Основи технології та особливості будови GPON

Устаткування для передачі даних за технологією GPON складається тільки з оптичної лінії, яка орієнтовано на OLT (с англ.optical line terminal) і оптичні мережеві пристрої ONU (з англ. Optical network unit) [11]. На рис. 2.1 показана логічна архітектура мережі з варіантами використання різних типу кабелів та обладнання.

Починаючи з головного пристрою, тільки одне однорежимне оптичне волокно проходить через оптичний розгалужувач (спліттер), який ділить оптичну потужність на *n* частин. Число розділення оптичного сигналу може змінюватись від 2 до 64.

При цьому дальність передачі сигналу може досягати 20 км (див. рис.2.2).

Стандарти GPON дозволяють вибирати різні швидкості прийому та передачі даних. Наприклад, на передачу даних від 1,2 Гбіт/с та вище 2,4 Гбіт/с, на завантаження 1,9 Гбіт/с та вище 2,4 Гбіт/с.

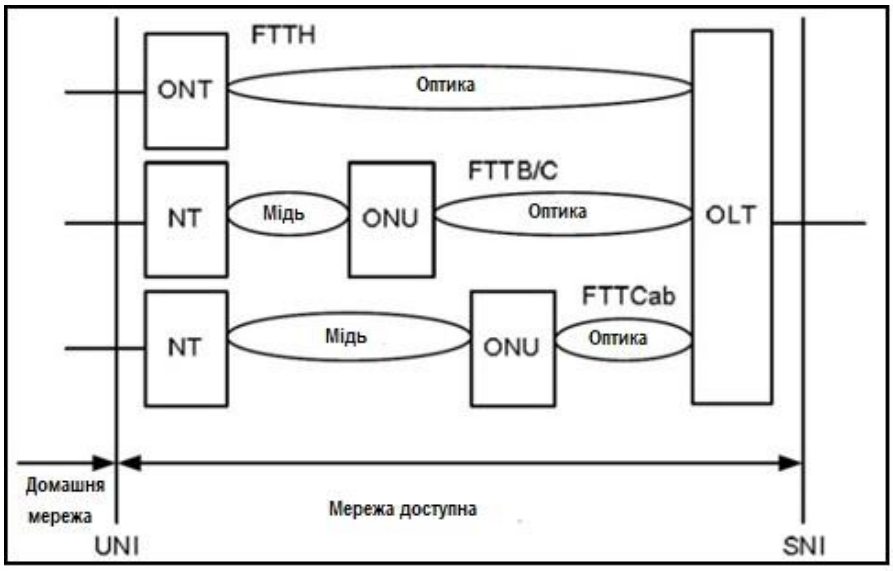

Рисунок 2.1 - Логічна архітектура мережі GPON

Діапазон робочих довжин хвиль 1480-1500 нм для передачі та 1260-1360 нм для прийому даних. У доповнення цього діапазон довжин хвиль 1550-1560 нм може використовуватися для поширення відео.

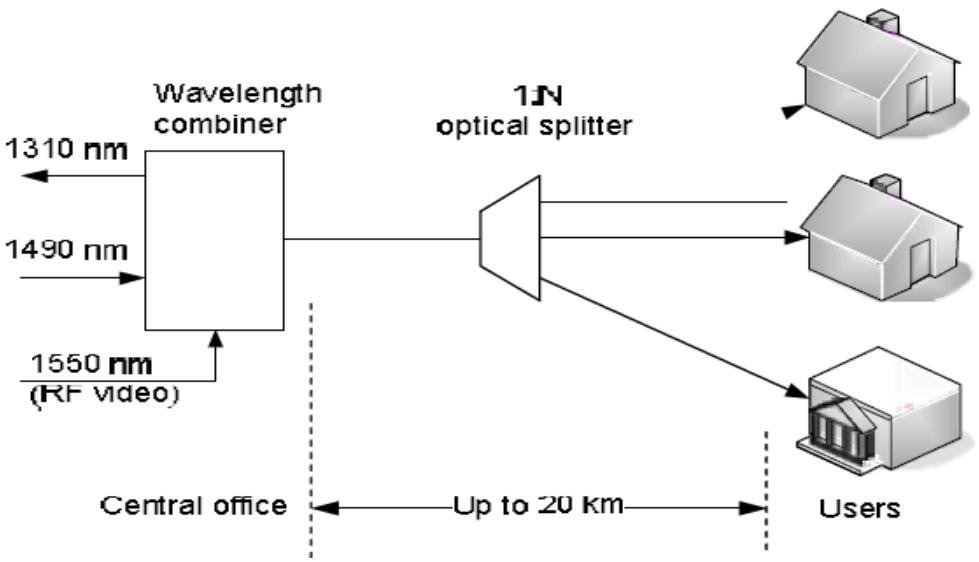

Рисунок 2.2 – Принципи передачі сигналу в системі GPON

Пряма корекція помилок (FEC) – математичний метод обробки сигналів, який кодує дані в такий спосіб, що помилки можуть бути виявлені та виправлені. У FEC надлишкова інформація передається разом із вихідною інформацією.

Кількість надлишкової інформації дуже мала і не впливає на роботу пристроїв. FEC призводить до збільшення бюджету лінії зв'язку приблизно 3-4 дБ (dB). Таким чином, може підтримуватися висока швидкість передачі та більше відстань від OLT до ONU, а також більше кількість розгалужень на одне дерево PON.

Трафік контейнери

Трафік контейнери (T-CONT) використовуються для керування смугою вихідного потоку даних у GPON [12]. Контейнери насамперед використовується для покращення пропускний здібності вихідного каналу . ONU посилає трафік , використовуючи один або кілька контейнерів , які дозволяють реалізувати QoS (англ . quality of service – якість обслуговування) для вихідного потоку даних .

Є п'ять типів контейнерів , які можуть бути призначені для користувачів :

1) гарантує фіксоване розподіл пропускної здібності для чутливого до часу додатків (VoIP);

2) гарантує фіксоване розподіл пропускної здібності для нечутливих до часу додатків ;

3) мінімум гарантованої смуги пропускання плюс додаткові негарантовані;

4) динамічний розподіл без будь - якої гарантованої пропускний здібності;

5) змішування всіх типів .

Динамічне розподілення смуги пропускання

Динамічний розподіл смуги пропускання (DBA) метод, який дозволяє швидко змінювати смугу пропускання користувача на основі поточного трафіку. DBA контролюється OLT, який розподіляє обсяг пропускної смуги для ONU. Це працює лише на передачу даних.

Щоб визначити, який пріоритет призначити ONU, OLT повинен знати інформацію про завантаженості контейнерів, пов'язаних з ONU.
ONU з трафіком передає значення статусу контейнерів, у якому вказується скільки пакетів залишилося в буфері даних.

Після того, як OLT отримує цю інформацію, він може перерозподілити пріоритет різним ONU залежно від завантаженості. Коли ONU не передає та не приймає інформацію, він переходить у режим очікування, надсилаючи порожню комірку даних, показуючи, що його буфер порожній. Це інформує OLT, що пріоритет для цього контейнера може бути присвоюватися іншим контейнерам. Якщо ONU має довгі черги очікування в буфері, то OLT може призначити кілька контейнерів для цього ONU.

Безпека

Основний особливістю GPON є те, що при завантаженні , дані передаються всім ONU, і кожен ONU виділяє час , коли дані належать йому (як TDM). Через це деякі несанкціоновані користувачі можуть перепрограмувати свій власний ONU і перехопити всі дані , що призначалися іншим ONU, які підключені до цього OLT. Для передачі GPON використовує з'єднання типу точка-точка тому весь трафік захищений від прослуховування . При передачі вся конфіденційна інформація може бути відправлено відкритим текстом. Таким чином, у GPON використовується рекомендація G.984.3, у якій описується механізм використання інформаційної безпеки для того, щоб користувачам був доступ тільки до даних , які призначені лише їм. При кодуванні використовується алгоритм шифрування Advanced Encryption Standard (AES) [3]. Його розмір дорівнює 128, 192, і 256 байт, що робить ключі шифрування конче важкими до лобової атаці . Ключ може періодично змінюватися, не порушуючи потік інформації з метою підвищення безпеки [4].

Захист

Захист у GPON застосовується для підвищення надійності функціонування мережі доступу . Воно розглядається як додатковий механізм , оскільки його реалізація залежить від бюджету компанії . Існують два типи захисту,

автоматичне перемикання та примусове . Перший спрацьовує при виявленні несправності , наприклад , при втраті сигналу , втрати кадру або погіршення сигналу . Другий за глобального зміні , наприклад заміна оптичного волокна .

Передача даних у GPON

GPON використовує GEM (GPON Encapsulation Метод) як спосіб , який інкапсулює дані у GPON. Хоча й будь-який тип даних може інкапсулюватися, фактично це залежить від службової ситуація . GEM забезпечує орієнтований на з'єднання зв'язок . Цей метод заснований на модифікованій версії рекомендації ITU-T.

Вхідний трафік транслюється із OLT до всіх ONU. Кожному ONU необхідно враховувати тільки кадри , призначені для нього . Тривалість кадру при вихідному потоці даних складає 125 мкс . поза залежно від пропускної можливості мережі в низхідному потоці (1,244 Гбіт /с або 2,488 Гбіт /с). Таким чином, кадр при швидкості 1,244 Гбіт / с з 19440 байтів , а при швидкості 2,488 Гбіт /с - з 38880 байтів . Довжина PCBd однакова для обох швидкостей і залежить від кількості блоків розподілу , що мають один і той самий ідентифікатор Allocation -ID в одному кадрі.

Формат кадру представлено на рис. 2. 3.

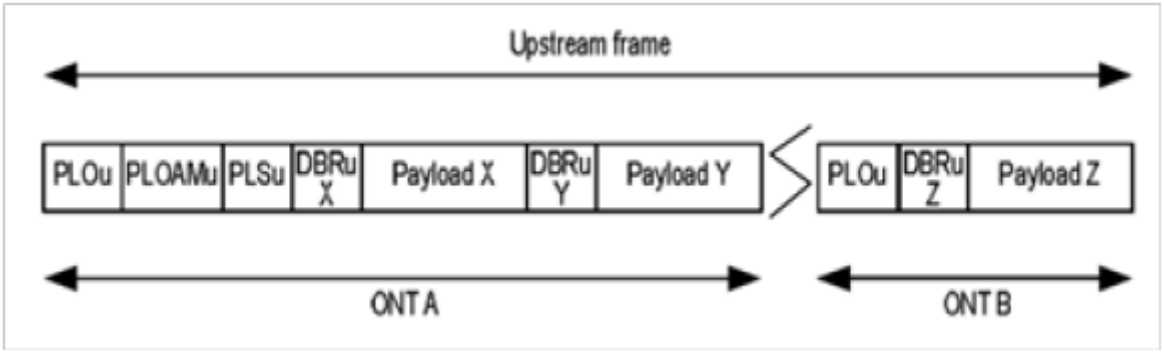

Рисунок 2.3 – Формат кадру

Для вихідного трафіку використовується TDMA, який контролюється OLT. OLT призначає певний тимчасовий інтервал , коли ONU робить запит на передачу даних . Формат кадру представлено на рис.2.4.

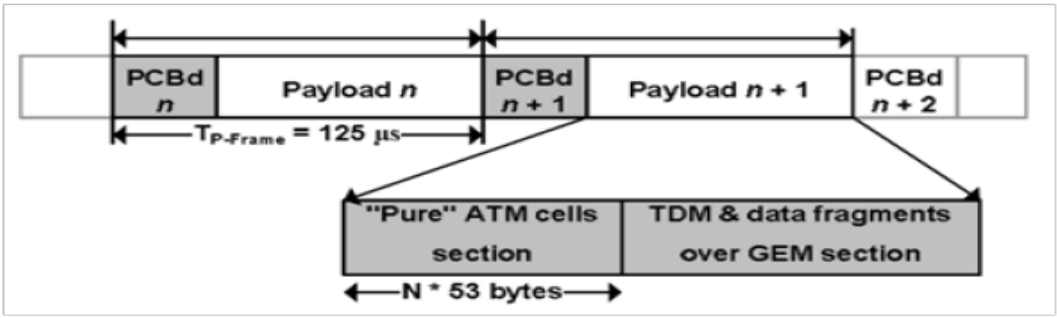

Рисунок 2.4 – Формат кадру

T-CONT

T-CONT – механізм для вихідного потоку QoS , в той час як методи обслуговування такого ж типу CoS .

При вихідних даних смуга пропускання для ONU залежить не тільки від типу трафіку конкретного ONU, а й від шаблонів трафіку на інші ONU в мережі. Коли середа ділиться різними ONU, будь-яка передача даних в ONU по власній ініціативи призведе до зіткнення та повторної передачі, викликаючи зниження продуктивності . Таким чином, ця загальна середа створена для множинних з'єднань точка-точка між ONU та OLT шляхом використання TDMA. OLT, будучи центральної точкою , повідомляє про пропускну можливості для кожного ONU. На основі шаблону трафіку на всіх ONU він надає доступ до ONU у фіксованому слоті щодо кадру вихідного потоку даних . Вихідний трафік кадр можна розглядати як розділений на різні типи контейнери . У GPON визначено п'ять типів .

Тип-1. T-CONT сервіс заснований на періодичних не запитаних дозволи на надання фіксованого розподілу корисний навантаження або потужності вимогам фіксованою смуги пропускання . Це статичний тип T-CONT, що не обслуговується DBA.

Тип-2. T-CONT призначений для змінної бітовий швидкості з обмеженою затримкою та вимогами до коливань як у передачі відео та голоси по IP.

Тип-3. T-CONT призначений для гарантованої затримки.

Тип-4. T-CONT – для максимально можливого трафіку .

Тип-5. T-CONT комбінується з двох або більше за інших чотирьох типів , визначених вище , і в цьому випадку індивідуальна пропускна здатність та призначення виробляються на ONU (див. рис.2. 5).

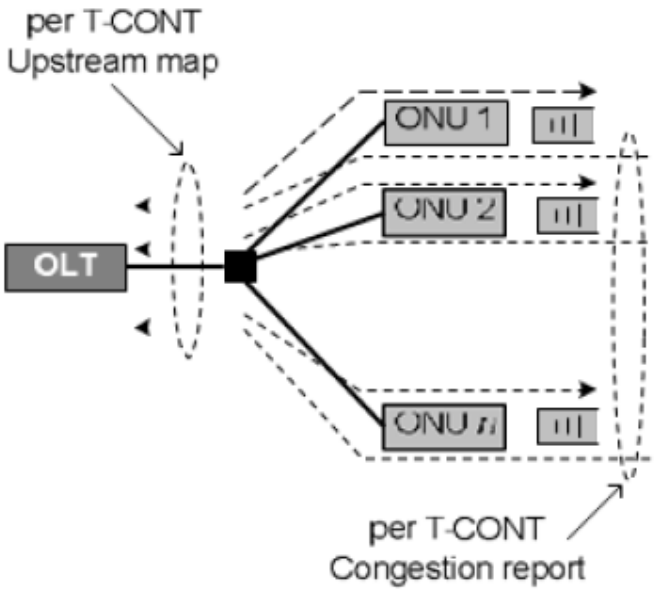

Рисунок 2.5 – Типи GPON

GEM сегмент

GPON підтримує два методи інкапсуляції: метод ATM та метод інкапсуляції GPON (GEM). При використанні GEM весь трафік відображається у мережі GPON у вигляді загальної процедури формування кадрів SONET/SDH (GFP). GEM підтримує вбудовану передачу голосу та даних без додаткового ATM або рівня інкапсуляції IP (див. рис. 6). GPON підтримує швидкість вихідного потоку 2.5 Гбіт/с та швидкості висхідного потоку від 155 Мбіт/с до 2.5 Гбіт/с.

Рисунок 2.6 – Структура GEM сегменту

Оптичний розгалужувач

Типова PON приєднує одне волокно від OLT до кількох пристроїв оптоволоконної мережі ONU. З'єднання крапка-багато точка між OLT і кілька ONU досягається завдяки використання одного чи кількох пасивних розгалужувачів.

У середині PON знаходиться пасивний оптичний розгалужувач. Цей пристрій має один вхід та кілька виходів. Як правило, кількістьство виходів дорівнює 2^n (наприклад, 2, 4, 8 і т.д.), а оптична потужність розподіляється рівномірно між виходами. За правилом оптична потужність на кожному виході зменшується по відношеннюня до входу на коефіцієнт $n \times 3.5$ дБ ($10\times\log2n = n\times10\times\log2$; 0.5 дБ додаються для включення втрат у розгалужувач).

Оптичний розгалужувач є двонаправним пристроєм. Через це його іноді називають розгалужувачем/спліттером. Оптичний сигнал згасає на ту ж величину ~ ($n \times 3.5$ дБ) для обох напрямків.

Втрати при розгалуженні

Одним із ключових параметрів для кожного FTTH-проектувальника мережі є досяжним проміжок між центральним офісом та абонентами, іншими словами, максимальний оптичний бюджет системи. Оптичний бюджет складається із загасання від з'єднувачів, волокна передачі та оптичних розгалужувачів. Оптичний розгалужувач на сьогоднішній день є самим вимогливим компонентом з точки зору втрат (втрати від типового 1×32 оптичного розгалужувачі можуть становити від 17 дБ до 18 дБ).

2.2 Архітектура та розрахунок параметрів мережі

При побудові мереж GPON у більшості випадків використовуються OLT та клієнтський пристрій ONU. Оптична розподілена мережа ODN є оптичним середовищем, яке підключене до OLT. До неї входять оптичні волокно, оптичні дільники, роз'єми тощо. Основними перевагами мереж GPON над

іншими вже існуючими мережами є швидкість передачі даних, а також можливість передавати дані на великі відстані. Щоб усе це працювало правильно, треба при побудові враховувати багато нюансів. Основною характеристикою оптичної мережі є згасання. Авторами експериментально встановлено, що загасання відбувається через те, що в ODN пристрій забирає собі частину сигналу, також загасання сигналу може відбуватися через неправильний монтаж.

Дальність передачі даних залежить від потужності передавача і приймача. Більшість організації обирають обладнання, яке дозволяє підтримувати швидкість 1244 Гбіт/с. Для цієї швидкості робочий бюджет обладнання складає 22-23 дБ.

Далі буде запропоновано приблизний розрахунок оптичного бюджету з урахуванням характеристик устаткування.

Розрахунок оптичного бюджету (P) при побудові PON дерева можна зробити за такою формулою:

$$P = FCA \cdot L + SL + SP,$$

де FCA –згасання оптичного волокна дБ/м, L-довжина волокна; SL = загасання сигналу у з'єднаннях волокна; SP = загасання сигналу в спліттерах.

Допустимо, ми будемо використовувати довжину хвилі 1550 нм . Розрахуємо приблизну довжину передачі:

$$\frac{23\text{дБ-}SL - 2 \cdot 0,5\text{дБ-}0,5\text{дБ}}{FCA\left[\frac{\text{дБ}}{\text{м}}\right]} = 20\text{км} .$$

У таблиці 2.1 представлені приблизні значення згасання щодо різних оптичних пристроїв [6].

Таблиця 2.1 – Значення згасання оптичних пристроїв

Пристрій	Затухання на 1 км
Волокно 1310 нм	0,1-0,2 дБ
Волокно 1310 нм	0,3 дБ
Оптичний конектор	0,3 дБ
Сплітер 1:2	3 дБ
Сплітер 1:4	7 дБ
Сплітер 1:8	10 дБ
Сплітер 1:16	13 дБ

Розрахуємо оптичну потужність та рівень сигналу на основі реальної мережі. Схема мережі зображено рисунку 7. Загальна довжина оптичної траси 9982 метри. Тестування проводилося обладнання Raisecom ISCOM 5508. Потужність SFP +3 дБм[5]. Розрахуємо оптичний бюджет та порівняємо з реальними показниками на устаткуванні. Дані будемо заносити до таблиці 2.

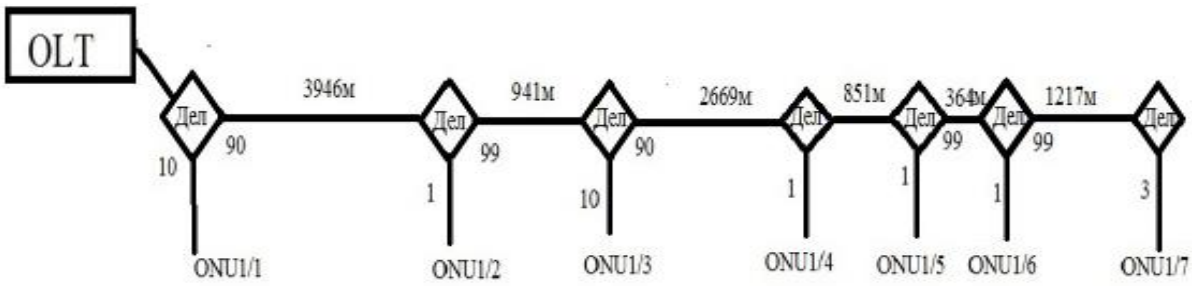

Рисунок 2.7 – Схема мережі для розрахунку

З даних видно, що показники можуть відрізнятися. Ці розбіжності можна пояснити тим, що оптичний канал дуже чутливий і втрати можуть виникнути внаслідок неправильного зварювання оптичного волокна або неправильного монтажу. Допустиме значення розбіжності має перевищувати 10%. Максимальне значення сигналу, у якому оптичне устаткування працюватиме коректно дорівнює -30дБм. Для правильної побудови мережі необхідно попередньо розрахувати оптичний бюджет та проводити виміри сигналу на кожній ділянці мережі.

Таблиця 2.2 – Порівняння показників сигналу в дБм

Номер Опі	Розрахункові показники	Реальні показники
1/1	-10	-10,1
1/2	-18,1	-19,5
1/3	18,6	-18,4
1/4	-20	-21,4
1/5	-24	-25,3
1/6	-25	-26,7
1/7	-18,7	-19,5

Висновоки по другому розділу

На сьогоднішній день GPON – найпрогресивніша і найперспективніша технологія доступу в інтернет, здатна забезпечити потреби, що стрімко зростають, у швидкості обміну інформацією. GPON не тільки повністю відповідає сучасним вимогам, але й має ресурси та потенціал для забезпечення розвитку технологій зв'язку в майбутньому.

Для порівняння за допомогою технології DSL максимальна швидкість досягає 20 МБ/с при максимальній дальності кабелю 5 км. Аналіз у статті показав, що характеристики GPON кілька разів більші.

Хоча є і свої недоліки, наприклад, оптичний кабель дуже чутливий до вигинів, дорожнеча обладнання, у багатьох випадках клієнтські пристрої не підтримують швидкість, яку їм надає провайдер. GPON підтримується і старими мережами, при цьому володіючи величезним технічним потенціалом.

РОЗДІЛ 3

ГІБРИДНИЙ ВАРІАНТ ЗВ'ЯЗОКУ ТА ПЕРЕДАЧІ ДАНИХ РЕЛЕЙНОГО ЗАХИСТУ В МЕРЕЖІ

Сучасні програми інноваційного розвитку потребують розробки технічних вимог до створення каналів зв'язку між цифровою підстанцією та іншими об'єктами та каналами передачі команд РЗ і ПА каналами зв'язку від цифрових підстанцій. Останні 20 років технологічні мережі зв'язку розвивалися головним чином шляхом заміни аналогового обладнання на цифрове, що використовує технологію PDH та SDH.

Сьогодні проектування нових технологічних мереж передачі (ТМПД), будуть базуватися в основному на пакетних технологіях, які набагато складніші, ніж ті що використовуються нині. [13]. Це пов’язано з передачею інформації від цифрових підстанцій до окремих типів технологічного обладнання, в першу чергу, існуючого обладнання релейного захисту та протиаварійної автоматики. Перехід від цифрових мереж (SDH та PDH) до пакетних мереж буде досить тривалим, і основною технологічною проблемою стане процес конвергенції мереж у цей період [14]. "Гарні" рішення, представлені в ряді проектів створення ТМПД, при найменшому відхиленні від низки вимог до пакетних мереж можуть призвести до катастрофічних наслідків для енергетики.

Досить докладний аналіз проблем переходу технологічного інформаційного обміну на пакетні мережі описаний у низці зарубіжних публікацій [15]. Розглянутий у цьому розділіі варіант створення гібридних мереж, що забезпечують поєднання різних технологій передачі інформації, дає можливість зберегти високу надійність при впровадженні нових зразків енергетичного обладнання на існуючих енергооб'єктах та забезпечити інформаційний обмін при спорудженні "цифрових підстанцій".

3.1 Аналіз переходу на мережі з пакетною технологією передачі сигналів релейного захисту

Сигнали релейного захисту – це найкритичніші дані, що передаються через технологічні телекомунікаційні мережі, і тому при виникненні аварійної ситуації повинен гарантуватися мінімальний час проходження інформації, точніше команди РЗ повинні передаватися з гарантованим часом доставки. Ці вимоги зберігаються під час переходу від мереж SDH/ SONET до мереж з пакетною технологією. Відповідно, проблема реалізації цих вимог є основною [16].

Види трафіка в перехідний період

В даний час основні мережі зв'язку для всіх додатків використовують технологію SDH/SONET, однак колишня інфраструктура та обладнання підстанції поступово скорочуються, поступаючись місцем сучасним, які підтримують протокол IEC 61850, що призводить до необхідності поетапного переходу на технологію передачі сигналів взаємодії через мережі Ethernet та IP. Рух до Smart Grid є ключовим фактором для цього процесу, оскільки пакетна транспортна мережа, яка має більшу пропускну спроможність і нижчу вартість, повинна обробляти велику кількість трафіку, що генерується сучасними технологічними програмами, що використовуються в інтелектуальних мережах електропостачання. SCADA на основі IP, вимірювальні системи WASA (wide area situation awareness), синхронізовані векторні вимірювання та новітні розробки в галузі автоматизації підстанцій, такі як стандарт IEC 61850, є прикладом нових додатків, що вимагають в системах передачі та розподілу електроенергії застосування пакетної передачі та використання можливостей технології Ethernet

Проблеми переходу

Енергетичні компанії, більшість з яких мають власні мережі, обережно сприймають перехід до IP. Будучи традиційно консервативними організаціями, енергетики не поспішають переходити до IP, якщо не бачать чітких параметрів забезпечення високої надійності та передбачуваності, як у мережах SDH/SONET. Однак виникають економічні проблеми, викликані

збільшенням капітальних витрат, пов'язаних із застосуванням нових технологій, за необхідності збереження мереж SDH/SONET на перехідний період. З технічної точки зору, реалізація інтелектуальних комунікацій на основі пакетних мереж повинна гарантувати безвідмовну роботу механізмів, що забезпечують низьку затримку при передачі сигналів, високу готовність і надійність при передачі важливих додатків у середовищі з комутацією пакетів. Для сигналів Релейного захисту потреба у швидкій і достовірній передачі інформації диктує необхідність низької симетричної затримки та мінімального джиттера. Обидва ці параметри становлять велику проблему для мереж із комутацією пакетів. Тим не менш, техніка Ethernet має різні механізми, щоб подолати ці проблеми та забезпечити необхідну продуктивність, що буде описано нижче. У той самий час перехід на пакетні мережі – процес тривалий і має низку неоднозначних чинників. Таким чином, збереження технології TDM дозволить забезпечити на час переходу необхідну надійність та безпеку передачі даних критично важливих програм.

Сьогодні типовою реалізацією передачі TDM трафіку, включаючи сигнали РЗ, через пакетні мережі є псевдопровідна емуляція (PWE). У майбутньому очікується поява нових методів, включаючи пряме відображення корисного навантаження на з'єднання Ethernet, без етапів обробки TDM та псевдопровідної інкапсуляції. Для реалізації сучасних релейних захистів використовують канали волоконно-оптичного зв'язку з інтерфейсом С37.94.

Передача сигналів РЗ зображена на рис. 3.1.

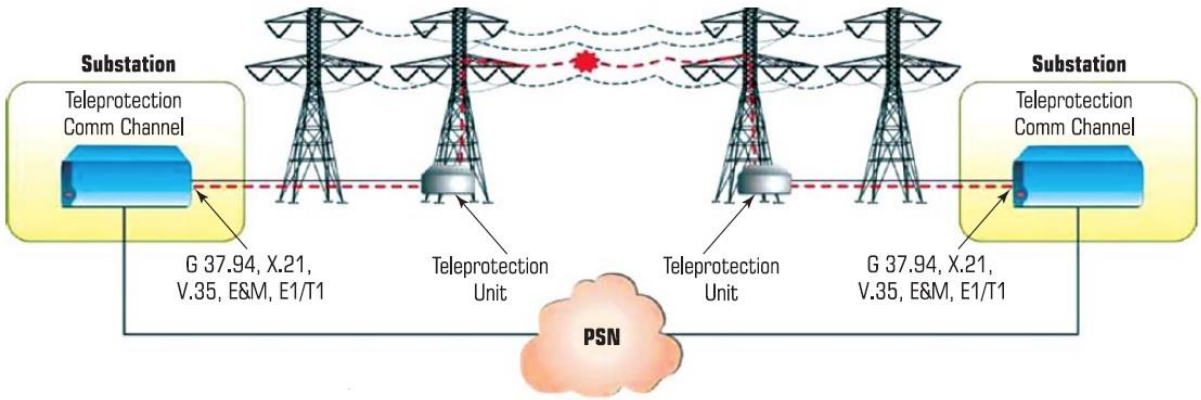

Рисунок 3.1 – Передача сигналів РЗ по пакетним мережам

3.1.1 Вимоги до телекомунікаційних мереж для передачі сигналів релейного захисту

Час передачі: Повний час роботи системи релейного захисту включає час для того, щоб ініціювати команду на передавальному кінці, час розповсюдження по телекомунікаційному каналу і час на прийняття рішення на приймальному кінці, включаючи додаткову затримку на захист від перешкод.

Надійність: можливість передати та отримати достовірні команди в умовах інтерференції та/або перешкод, мінімізуючи можливість пропадання команди (Pmc). Надійність визначається за заданої частоті передачі помилкових бітів (BER).

Безпека: можливість запобігти помилкам, що виникають внаслідок впливу шумів, мінімізуючи вірогідність помилкових команд. Параметри безпеки задаються для певної частоти передачі хибних бітів (BER).

Додаткові елементи, які впливають на характеристики передачі сигналів РЗ, включають вимоги до пропускної здатності, використовуваної системою РЗ, її стійкості до відмови і здатності відновлення. З вищезазначених критеріїв час передачі, вимоги до пропускної спроможності та надійність прямо відносяться до апаратури зв'язку та середовища передачі.

Розгляд значень часу затримки

Вимоги до часу затримки корпоративних мереж мають тенденцію змінюватися залежно від багатьох параметрів, включаючи тип устаткування релейного захисту. Більшість силового обладнання ліній електропередачі може витримати до п'яти циклів включення та вимикання живлення, перш ніж виникне незворотне погіршення або вплив на інші сегменти в мережі. У лініях 50 Гц визначає повний час усунення пошкодження 100 мс. Як міра безпеки, однак, час дії систем захисту обмежується 70 - 80% цього періоду, включаючи час на розпізнавання аварії, час передачі команди та час перемикання лінійного вимикача. Деякі компоненти системи, такі як великі

електромеханічні перемикачі, вимагають тривалого спрацьовування, що займає більшу частину повного часу виконання команди на конкретну дію, залишаючи вікно тільки 10 мс для передачі сигналів захисту.

Враховуючи серйозність проблеми, у нових мережах ці вимоги викладено у Стандарті Міжнародної електротехнічної комісії 61850: межі часу передачі сигналів для найкритичніших повідомлень становлять 5-10 Мс для силових ліній на 50 Гц.

Асиметрія затримки

Крім мінімальної затримки сигналів взаємодії диференціального захисту використовуваний канал зв'язку повинен бути симетричним, тобто мати симетричну затримку передачі і прийому. Як згадано вище, це потребує особливої уваги в пакетних мережах до значення джиттера. Для сигналів взаємодії РЗ оптимально мати нульову асиметричну затримку, переважно устаткування РЗ може витримувати розбіжності до 250 мкс. Основні інструменти, доступні для зниження зміни затримки нижче цього порога:
Jitter “buffer” на кожному кінці лінії може використовуватися для зміни затримки, ставлячи у чергу надіслані та отримані пакети. Довжина черг повинна компенсуватися збільшенням швидкості передачі, оскільки зі збільшенням буфера збільшується затримка.

Інструменти керування трафіком гарантують, що сигнали релейного захисту отримують найвищий пріоритет передачі і мінімізують кількість точок маршрутизації, в яких виникає джиттер.

Стандарт технології синхронізації для мережі комутації пакетів, такий як 1588-2008 Precision Time Protocol (PTP) та Синхронний Ethernet (Sync-E), допомагає підтримувати стійкість мережі.

Джерела затримки в релейному захисті

Важливо зрозуміти вплив мережевих обмежень, оскільки кожен елемент і процес обробки в системі захисту додається в сумарну затримку:

• *Затримка обладнання релейного захисту*: ця невід'ємна затримка включає ідентифікацію збоїв у силовому устаткуванні, ініціювання команди та час прийняття рішення.

Мультиплексор доступу (TDM interface): затримка в обладнанні мультиплексора – результат функцій, таких як час на reframe після втрати сигналу, виділення та формування часових інтервалів, буферизації при формуванні DS0 та E1, синхронізації та розсинхронізації, час перемикання в кільці SDH (PDH), час виявлення несправностей. Затримка мультиплексора мінімізується через оптимальні механізми ICs та функції крос-з'єднання DS0.

• "*Псевдопровідна" затримка інкапсуляції та пакетування*: процес перетворення TDM на пакети включають фіксовану затримку 1-5 мс, залежно від розміру пакета та числа TDM кадрів, які містить кожен пакет. Коротші пакети збільшують потребу в пропускній здатності, але зменшують затримку.

• *Мережеві елементи мережі комутації пакетів*: якщо обладнання релейного захисту з'єднується по пакетній мережі (рис. 1), кожен елемент уздовж шляху трафіку додає фіксовану та змінну затримку, як наслідок, відповідно, обробки інформації та організації черг. Змінна затримка становить велику загрозу продуктивності релейного захисту внаслідок високого рівня невизначеності, яку вона уявляє, що вимагає використання засобів управління трафіком.

3.1.2 Додаткові проблеми, що стосуються передачі сигналів релейного захисту

Надійність. Системи релейного захисту, враховуючи їх роль для вирішення відповідальних завдань, повинні бути забезпечені стійкими до відмов у разі неправильного функціонування будь-якого з компонентів системи. Багато додатків застосовують надлишкові методи підвищення надійності, так дистанційний і диференціальний захист використовують різні канали. З телекомунікаційної точки зору надійність може бути досягнута на багатьох рівнях:

Апаратна надмірність: надійність мультиплексора має бути заснована на захисті від відмов одиночних модулів з використанням апаратної надмірності та можливістю заміни блоків у гарячому режимі.

Лінійна надмірність: 1+1 топологія захисту з автоматичним перемиканням між трактами при виникненні дефектів обладнання або кабелю. Трафік, заснований на Ethernet, використовує схему Link Aggregation Group (LAG), IEEE 802.3-2005 LACP (Link Aggregation Control Protocol), в якому паралельні посилання прив'язуються до єдиного віртуального каналу.

Захист маршруту: стандарти промислового Ethernet забезпечують різні інструменти, щоб гарантувати високу доступність. Вони включають захисне перемикання ліній Ethernet (G 8031) - також механізми захисту, названі "EVC (Ethernet Virtual Connection)" і Ethernet Ring Protection Switching (G 8032 ERP), розроблені, щоб забезпечити "П'ять Дев'яток" (99.999%), надійність сервісів та швидке відновлення.

Управління трафіком і якостю обслуговування

Розвиток технології Ethernet дозволяє використовувати складні механізми, що надають сигналам релейного захисту детермінований рівень якості обслуговування та пріоритету, якого вони вимагають. Це є особливо критичним при проходженні інформаційних пакетів різних комутаторів та інших мережевих елементів, при цьому виникає потреба змінити значення таких параметрів, як затримка при організації черг. Керуючи ресурсом пропускної спроможності та пріоритетами передачі за допомогою механізмів CoS (Class of Service), багаторівневе ієрархічне управління трафіком дозволяє отримати передбачувану затримку та джиттер. Удосконалений набір інструментальних засобів включає наступне:

Класифікація вхідного трафіку в потоках, відповідно до типу та вимог QoS. Ethernet підтримує велику різноманітність критеріїв сортування, такі як VLAN-ID, P-bit marking, MAC/IP-адресація і т.д., що дозволяє ретельно поділяти трафік.

Ієрархічне планування трафіку визначає порядок відправлення різних потоків за допомогою двоступінчастого механізму планування, у результаті кожен потік отримує необхідний пріоритет. Таким чином, пріоритетний трафік обслуговується в першу чергу, водночас черга для трафіку з низьким пріоритетом також просувається. Розвинені способи керування чергами також служать для запобігання переповнень і забезпечення мінімальної затримки та джиттера навіть у ситуаціях, коли велика кількість нерівномірного трафіку передається по тому ж каналу. Формування трафіку дозволяє згладжувати викиди та уникнути переповнення буфера у наступних елементах мережі. Редагування пакетів передає вказівки щодо правильної їх обробки наступним елементам мережі та забезпечує цілісність даних.

Моніторинг виробництва та тестування

Технологія Ethernet операторського класу пропонує безліч інструментів для тестування, моніторингу та усунення збоїв у роботі ліній зв'язку. Повний набір службових пакетів Ethernet (OAM), методів вимірювання затримки, джиттера та втрати пакетів, діагностичні петлі та інші засоби можна застосовувати віддалено, автоматично виконуючи такі процедури:

- перевірка з'єднання;
- інтенсивне тестування;
- моніторинг продуктивності;
- визначення збою;
- передача повідомлення про збій та його локалізація.

Віддалене тестування, активний моніторинг та повна картина мережевих подій дозволяють адміністраторам мереж передбачати погіршення якості сервісу, забезпечити постійну продуктивність мережі та скоротити капіталовкладення.

Синхронізація сигналізації у пакетних мережах

Пакетні мережі не розроблялися із вбудованими механізмами синхронізації, і тому вимагають додаткових рішень передачі тактової частоти з точністю, необхідною для стабільної роботи мережі з передбачуваною

продуктивністю. В електроенергомережах це особливо необхідно для підтримки традиційного обладнання та додатків, чутливих до затримки та джиттера, таких як релейний захист, SCADA. Донедавна було прийнято використовувати GPS у кожному вузлі/пункті обслуговування, однак це призводить до значного зростання витрат.

Для синхронізації в пакетному середовищі на сьогодні застосовуються кілька способів:

Метод ITU-T Synchronous Ethernet (Sync-E) використовує фізичний рівень мережі Ethernet для точної передачі тактової частоти. Для цього потрібно, щоби кожен фізичний канал не переривався протягом усього маршруту.

Інший метод – адаптивне відновлення тактової частоти (Adaptive Clock Recovery, ACR) – спирається на час прибуття пакетів у псевдопровідному потоці TDM, незалежному від фізичного рівня. Протоколи IETF NTP та IEEE 1588-2008 Precision Time Protocol (PTP) обмінюються інформацією про тимчасові мітки в ієрархії пристроїв “ведучий-відомий”, щоб передати тактову частоту та дані TOD (Time of Day) таким чином, як це необхідно для нормальної роботи датчиків розподілених вимірів та попередження каскадних відключень. Використання протоколу PTP протягом усього мережного маршруту є гарною альтернативою GPS для синхронізації часу. Хоча за допомогою PTP можна передавати і тактову частоту і мітки часу, багато мережних операторів воліють використовувати фізичний рівень мережі передачі частоти (тобто. TDM чи Synchronous Ethernet), а сервіс PTP – лише з синхронізації часу. Більше того, оскільки на багатьох підстанціях пристрою, як і раніше, використовують тимчасові коди IRIG-B, необхідно надійне перетворення між PTP і IRIG-B для підключення традиційного обладнання до нових систем Smart Grid.

Стандарт IEC 61850 докладно розглядає потреби електроенергомереж у передачі сигналізації та синхронізації в пакетних мережах. Він посилається на стандартний профіль IEEE C37.238 для IEEE Std. 1588 Precision Time Protocol

у додатках для підстанцій та профіль 1588 PTP Telco для зв'язку між підстанціями по глобальній мережі.

Сучасні комунікаційні пристрої релейного захисту, які підтримують передачу точного часу, сприяють зниженню витрат, оскільки вони позбавляють необхідності купувати дорогі апаратні засоби або установки GPS.

3.1.3 Вибір правильної пакетної мережі

При переході електроенергетичних мереж до комунікацій нового покоління вибір пакетних технологій включає Ethernet операторського класу, IP, стандартний MPLS (Multi-Protocol Label Switching), MPLS-TE та новітній варіант MPLS-TP. Крім того, можна розглядати нове покоління комутації каналів (Circuit Switching, CS) на основі оптичних транспортних мереж OTN (Optical Transport Networks). Подібно до SDH/SONET, OTN можна використовувати як фізичний рівень для надійної передачі трафіку Ethernet або IP по оптоволокну на швидкостях від 50 Мбіт/с до понад 100 Гбіт/с. Кожна з перерахованих пакетних технологій здатна надійно доставляти інформацію, але має різні характеристики. Рішення про тип технології залежить від таких факторів як кількість вузлів, які будуть з'єднані, їх розміру, можливості обраного рішення забезпечити відповідну продуктивність, використовуючи різне середовище передачі, доступне кожному вузлі, і, звісно, вартості. Незважаючи на те, що сервіс VPLS (Virtual Private LAN Service), заснований на передачі Ethernet по MPLS може забезпечити необхідну стійкість для критичних додатків за допомогою захисного механізму FRR (Fast Re-Route) з низькою затримкою, у нього є кілька серйозних недоліків з точки зору захисту, що визначаються вбудовані засоби OAM для моніторингу мережі і висока ціна на порт . Поєднання доступу Layer 2 Ethernet з магістраллю MPLS дозволяє знизити ціну на порт, мати більший функціонал OAM та інструменти PM для з'єднань Layer 2 Ethernet та використовувати розвинені захисні механізми за допомогою Ethernet Ring Protection Switching та Ethernet Linear Protection Switching. Крім того, такий підхід дозволяє зберегти встановлену базу обладнання доступу і може бути оптимальним варіантом для великої кількості

розподілених енергооб'єктів, підключених по мідній, оптоволоконній та бездротовій
інфраструктури.

3.2 Релійний захист через пакетні мережі. Тестування SDH-мультиплексора доступу [15]

Для тестування розглянемо одну з мультисервісних платформ доступу (мультиплексор, що пройшов атестацію ФСК) як елемент мережі під час передачі сигналів релейного захисту під час використання пакетної технології. Тестування складалося з перетворення даних TDM, отриманих від модулів релейного захисту, пакети. Потім інкапсульований трафік був переданий по мережі Cisco MPLS з використанням статичної маршрутизації, щоб переконатися у сталості тракту, забезпечуючи вимоги до продуктивності мінімальної затримки сигналів релейного захисту (рис. 3.2).

Для тестування використовувалося обладнання диференціального захисту виробництва AREVA, ABB і Siemens, використовуючи наступні інтерфейси сполучення: G 703; X. 21; RS-232; C37.94. Мультиплексор, що тестується, успішно виконав ці вимоги, забезпечивши допустиму затримку та необхідну якість обслуговування для пріоритетних сигналів за допомогою інструментів формування та організації трафіку. Крім того, було забезпечено синхронізацію часу через мережу передачі. Одна з тестових схем включала дублювання на рівні E1 через створення двох псевдопровідних з'єднань для резервування E1 в мережі MPLS з різних трактів. У сценаріях, де мережа SDH/SONET зберігається як резерв, дублювання E1 може використовувати одне з'єднання як псевдопровідне по пакетній мережі, а інше по резервній мережі TDM.

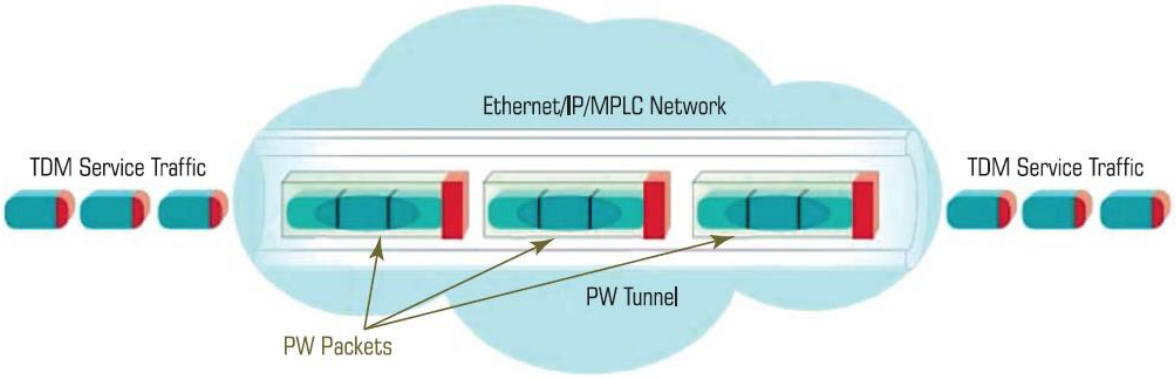

Рисунок 3.2 – Проходження TDM сигналів через пакетну мережу

Релійний захист за пакетними мережами

Механізми вирішення проблеми передачі сигналів РЗ через пакетні мережі, завдяки їх складності та різноманіттю, викликають обгрунтоване занепокоєння у “традиційних” зв'язківців та релейників. Розробка нових стандартів та рекомендацій для пакетних мереж, включаючи засоби захисту від всіляких загроз – процес постійний. Останні розробки технології SDN (Software-Defined Networking) та технології віртуалізації мережевих функцій NFV (Network Function Virtualization) дозволять створювати інтелектуальні мережі з високим рівнем гнучкості, уніфікувати обладнання, що виробляється, знизити витрати на впровадження нових сервісів. Природно, всі технології повинні проходити перевірку, тому до настання ери великої інтеграції необхідно сформулювати конкретні технічні вимоги до мереж, що створювалися вже сьогодні.

Усі розуміють, що один невірний крок чи недотримання всіх можливих і немислимих заходів мережевої безпеки може призвести до катастрофи. У будь-якому випадку "бігти попереду паровоза", як пропонують деякі ентузіасти прогресу, - заняття досить небезпечне, особливо в галузі електроенергетики.

Телекомунікаційні стандарти розроблялися на весь період експлуатації обладнання та, в основному, не змінювалися. Висока надійність, відсутність можливості несанкціонованого доступу – це рай відповідальних консерваторів. Використання цих властивостей технології SDH для передачі

лише критичних даних дозволить значно знизити витрати під час створення мереж.

Найкращий варіант для систем доступу, призначених для енергетичного ринку - це гібридне SDH і PSN в одному обладнанні.

Це дозволяє забезпечити роботу всіх при положень із виконанням усіх технічних вимог: надійності, швидкості тощо. За допомогою комбінації можливості промислового Ethernet та мереж TDM для додатків можуть бути обрані кращі маршрути, забезпечуючи передачу сигналів існуючих сервісів та інтерфейсів.

Це рішення дозволяє:

• з боку технології TDM:

– легке інтегрування інтелектуальних електронних пристроїв (IEDs) та NG сервісів та обладнання в існуючу інфраструктуру TDM – безперервність сервісу для існуючих програм та обладнання, навіть після того, як базова мережа замінюється на IP/MPLS;

– знайти рішення щодо емуляції схем, які ставлять під загрозу якість обслуговування чи величину затримки;

- численні засоби резервування для забезпечення заданої надійності;

• з боку технології PSN:

– гарантія певного QoS для служб NGN та передачі сучасних програм по пакетних мережах, що використовують мультипріоритетне управління трафіком, OAM, діагностику та контроль продуктивності;

з боку технології PSN:

– гарантія певного QoS для служб NGN та передачі сучасних додатків по пакетних мережах, використовую-

щим мультипріоритетне управління трафіком, OAM, діагностику та контроль продуктивності;

– перспективні рішення, розроблені для зв'язку в інтелектуальних системах Smart Grid та архітектури IEC-61850, включаючи надійні Ethernet сервіси з

малим часом затримки під час передачі даних між вузлами, що вимагають обміну повідомленнями у реальному часу, такими як GOOSE/GSSE;

– захист критично важливої інфраструктури та заснованих на IP систем SCADA від кібератак за допомогою протоколів автентифікації та забезпечення кібербезпеки, таких як SSH, SSL, SNMPv3 та RADIUS і т.д.

При використанні як транспортної мережі технології OTN або її окремих елементів тов (рис. 3.3), можливий ще ряд варіантів створення захищених гібридних мереж з мінімальними капітальними вкладеннями та гарантією надійності, яку забезпечує застосування обладнання SDH або PDH (рис.3.4).

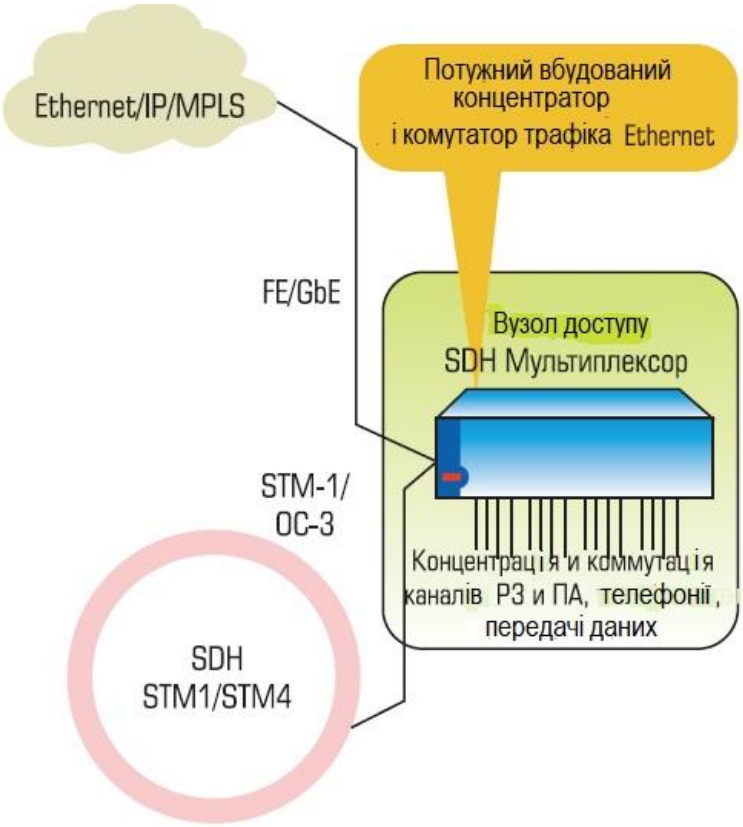

Рисунок 3.3 – Гібридний вузол доступу

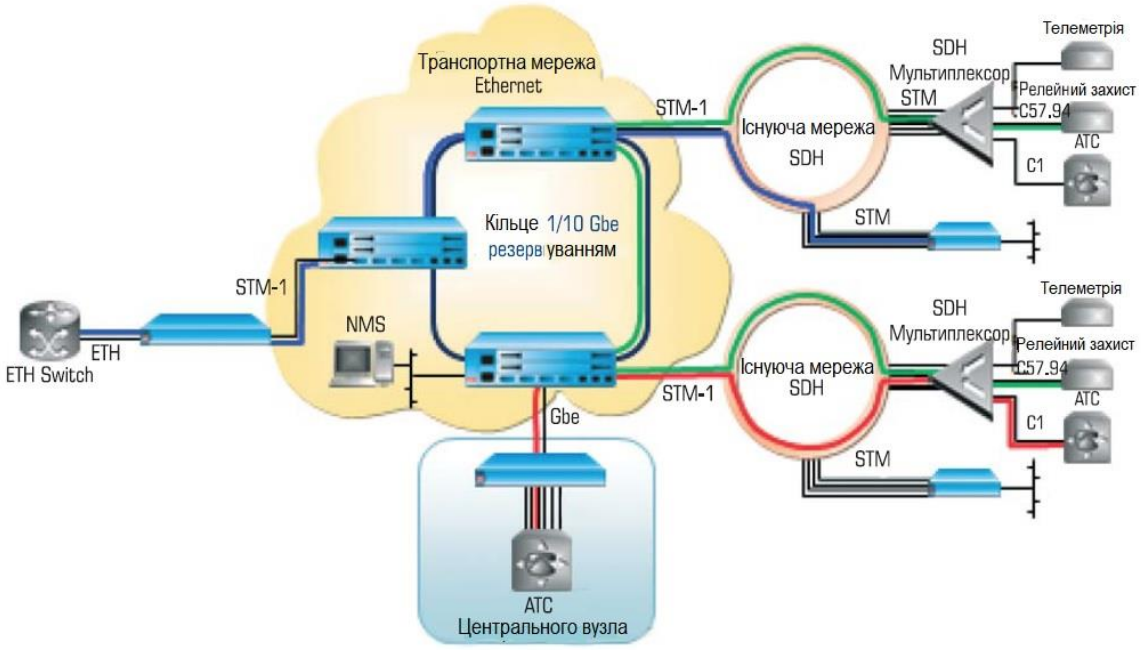

Рисунок 3.4 – Проек по з’єднанню вузлів підстанцій через транспортну мережу

Висновки по третьому розділу

Перехід до Smart Grid та мереж наступного покоління йде вже повним ходом, проте надзвичайно важливі програми, такі як релейний захист, потребують особливої уваги.

Тільки рішення, які забезпечують жорсткі вимоги технологічного обладнання: мінімальний час передачі, надійності та безпеки – можна розглядати як варіанти для реалізації.

Гібридний варіант, що включає технологію TDM та пакетні рішення, дозволяє енергетичним компаніям безболісно та вільно вибрати шлях переходу до нових технологій, що задовольняють їх потреби.

ВИСНОВКИ

У системі РЗА енергооб'єкта для забезпечення необхідного рівня надійності необхідне апаратно-незалежне троювання (основна дія з подвійним резервуванням, у тому числі з далеким).

Розподілена система мікропроцесорної РЗА підстанції 110-220 кВ, порівняно з електромеханічними та мікроелектронними аналогами, за кількістю необхідних панелей (шаф) немає явних переваг. У терміналах РЗА є суттєва апаратна та функціональна надмірність. Система РЗА ускладнюється з допомогою поперечних зв'язків між терміналами. Знижується огляд системи, підвищується ймовірність помилок при проектуванні, монтажі, налагодженні. Створення комбінованої системи, що виконує централізоване введення та розподіл сигналів у цифровій формі у поєднанні з розподіленою системою їх обробки у групах індивідуальних шаф кожного з приєднань, призводить до невиправданої апаратної та функціональної надмірності. Комбінована централізовано-розподілена система РЗА може розглядатися як проміжний етап переходу від традиційної розподіленої архітектури до централізованої.

При побудові розподіленої системи мікропроцесорної РЗА функцію третьої підсистеми посиленого резервування доцільно покласти прості польові термінали РЗА, виконують функції резервних щаблів з автоматичним прискоренням від централізованої системи РЗА і виправленням неселективних дій від АПВ. Такі термінали доцільно використовувати разом із резервними ємнісними накопичувачами для керування електромагнітами відключення вимикачів. При деякому зниженні функціональності надійність та стійкість системи РЗА може бути підвищена шляхом заміни терміналів автономними пристроями релейного захисту альтернативної електромеханічної елементної бази.

Слід вважати перспективними дослідження у сфері створення централізованої системи РЗА підстанції. Пропонується дубльована структура збору, передачі та обробки даних на основі мажорованої мультипроцесорної системи.

У КРУ 6-10-35 кВ доцільно зберегти традиційну розподілену архітектуру РЗА із застосуванням одного терміналу на приєднання. Окремі типи захисту можуть мати централізоване виконання.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Abdelkader Abdelmoumene, Hamid Bentarzi «Reliability assessment and improvement of digital protective relays». 2014.

2. [Электронный ресурс] Protective Relay Market worth 4.54 Billion USD by 2021 Режим доступа: http://www.marketsandmarkets.com/PressReleases/protective-relay.asp.

3. Drew Baigent, Mark Adamia, Ralph Mackiewicz, «Протокол МЕК 61850 Комунікаційні мережі і системи підстанцій. Загальний огляд для використання».

4. Marzio P. Pozzuoli, «Zero-Packet-Loss in the Substation». 2010.

5. Гуревич В.І. Проблема електромагнітних впливів на мікропроцесорні пристрої релейного захисту. 2010 року.

6. Toshio Matsumoto, Yasuhiro Kurosawa, Member, IEEE, Masaji Usui, Koji Yamashita, Member, IEEE, and Taisei Tanaka. «Experience of Numerical Protective Relays Operating in an Environment With High-Frequency Switching Surge in Japan». 1996.

7. Мукімов Ш.С., Бойко В.В. Розрахунок пропускної спроможності каналів зв'язку для корпоративних мереж. 2014;

8. Ліфшиц А.М. Перехід до Smart Grid та цифрових підстанцій. Гібридний варіант побудови мережі зв'язку та передачі даних. ТОВ «НВЦ Пріоритет» 2013 року.

9. Хьюлсман М., Він Ф. «Яких показників ми можемо досягти при використанні RS-485?». 2006;

10. University of New Hampshire InterOperability Laboratory. «Ethernet physical layer interoperability test suite version 2.4 technical document». 2007.

11. Björn Skubic, Ericsson Research «A Comparison of Dynamic Bandwidth Allocation for EPON, GPON, and Next-Generation TDM PON». 2009.

12. S.Srinath «Performance Analysis of 2.5 Gbps GPON». 2014.

13. Кобець Б.Б., Волкова І.О. Smart Grid в електроенергетиці / Енергетична політика, № 6, 2009.

14. Волобуєв В.В. Що таке Smart Grid? Ка-кові перспективи розвитку - http://www.rsci.ru/ sti/3755/208683.php.

15. RAD Data Communications Inc. 900 Corporate Drive Mahwah, NJ 07430 USA Tel: (201) 529-1100, Toll free: 1-800-444-7234 Fax: (201) 529-5777 E-mail: market@radusa. com <mailto:market@radusa.com>

16. Гуревич В.І. Інтелектуальні мережі: но- ві перспективи чи нові проблеми?