Форма № 11-9.02

Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування закладу вищої освіти)

Навчально-науковий інститут інформаційних технологій і робототехніки
(повне найменування інституту, назва факультету (відділення))

Кафедра автоматики, електроніки та телекомунікацій
(повна назва кафедри (циклової комісії))

Пояснювальна записка

до кваліфікаційної роботи

магістра
(ступінь вищої освіти)

на тему **Розробка мережі доступу підприємства критичної інфраструктури**

Виконав: студент 6 курсу, групи 6дТТ
спеціальності 172 «Електронні
комунікації та радіотехніка»
(шифр і назва напряму підготовки, спеціальності)

Поляков О.Л.
(прізвище та ініціали)

Керівник Лисечко В.П.
(прізвище та ініціали)

Рецензент Куст О.М.
(прізвище та ініціали)

Полтава - 2025 рік

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

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

З А В Д А Н Н Я

НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Полякову Олександру Леонідовичу

1. Тема проекту (роботи) **«Розробка мережі доступу підприємства критичної інфраструктури»**
керівник проекту (роботи) Лисечко Володимир Петрович, д.т.н., професор, затверджений наказом вищого навчального закладу від "09" 05 2024 року № 818-ф-ч
2. Строк подання студентом проекту (роботи) 19.12.2024 р.
3. Вихідні дані до проекту (роботи) Схема та характеристики підключення локальної мережі підприємства до електронної комунікаційної мережі загального користування, вимоги до послуги доступу до мережі Інтернет.
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд сучасних ліній зв'язку що використовуються для мереж доступу та їх резервування. Створення проекту удосконаленої мережі доступу та її резервування. Аналіз надійності запропонованих рішень. Рекомендації по впровадженню результатів.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових плакатів):
1) Схема мережі доступу діюча
2) Існуючи можливості підключення до мережі Інтернет
3) Модель мережі доступу що пропонується
4) Вибір обладнання
5) Схема мережі доступу з резервуванням

6) Забезпечення резервного живлення мережі доступу
7) Розрахунок надійності доступу до мережі Інтернет
8) Висновки

6. Дата видачі завдання 02.09.2024 р.

КАЛЕНДАРНИЙ ПЛАН

Пор. №	Назва етапів магістерської роботи	Термін та обсяг виконання етапів роботи			Примітка (плакати)
1	Вступ. Аналіз функціонування діючої мережі доступу в сучасних умовах.	07.10.24	I	10%	Пл. 1
2	Врахування вимог та рекомендацій споживача і керівних документів.	11.10.24		15%	
3	Огляд можливостей підключення до мережі Інтернет	16.10.24		25%	Пл. 2
4	Розробка моделі мережі доступу	05.11.24	II	40%	Пл. 3
5	Вибір електронного комунікаційного обладнання	12.11.24		50 %	Пл. 4
6	Розробка схеми мережі доступу з резервуванням	19.11.24		60%	Пл. 5
7	Вибір обладнання для резервного живлення.	26.11.24		70%	Пл. 6
8	Розрахунок надійності доступу до мережі Інтернет	11.12.24	III	90%	Пл. 7
9	Оформлення пояснювальної записки	19.12.24		100%	Пл. 8

Магістрант (підпис) Поляков О.Л.
(прізвище та ініціали)

Керівник роботи (підпис) Дисечко В.П.
(прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ [4], [8], [10]

ЕКМ – електронні комунікаційні мережі;

ЕКМЗК – електронні комунікаційні мережі загального користування;

WAN (Wide Area Network) – глобальна комп'ютерна мережа;

LAN (local area network) – локальна комп’ютерна мережа;

PON (Passive optical network) – технологія пасивних оптичних мереж, заснована на деревоподібній волоконно-кабельній архітектурі з пасивними оптичними розгалужувачами на вузлах;

GPON (Gigabit Passive Optical Network) – представник сімейства пасивних технологій оптичних мереж доступу PON.;

Opt – оптичний/оптична;

WEB – інтернет - простір;

DDoS (Distributed Denial of Service) - атаки розподіленої відмови в обслуговуванні;

СШД – станція широкосмугового доступу (обладнання точки широкосмугового доступу через мікрохвильовий радіоканал);

ССЗ – станція (термінал) супутникового зв’язку;

QoS (Quality of service) – якість обслуговування, у широкому значенні – якість послуг, які надає комунікаційна мережа.

Послуга доступу до мережі Інтернет - електронна комунікаційна послуга, що забезпечує доступ до мережі Інтернет і можливість логічного з’єднання з кінцевими точками мережі Інтернет незалежно від технології, що застосовується в електронній комунікаційній мережі, і кінцевого (термінального) обладнання, що використовується;

ВСТУП

В сучасних реаліях підприємства, організації та громадяни України постійно вирішують проблему стійкості зв’язку для забезпечення різноманітних потреб суспільства і держави [9]. Вплив російської агресії на інфраструктуру електронних комунікаційних мереж підприємств, установ та закладів України є значним і різноманітним. Це і фізичне знищення об'єктів, таких як базові станції, сервери та дата-центри, що призводить до пошкодження, або повного знищення ключових елементів електронних комунікаційних мереж, кібератаки, включаючи DDoS-атаки, націлені на системи зв'язку, викликали збої у роботі, що ускладнює доступ до інформації та послуг, вимкнення електрики через обстріли енергетичної інфраструктури також негативно позначається на функціонуванні електронних комунікаційних мереж. Додатково, зміна умов праці та евакуація спеціалістів призвели до дефіциту кадрів у галузі. Втрата фізичної інфраструктури вимусила операторів шукати альтернативні маршрути для трафіку, що може знизити якість обслуговування.

У цих умовах резервування мереж доступу стає критично важливим. Воно дозволяє забезпечити гарантований доступ до мережевих ресурсів, навіть у випадках збоїв чи фізичного пошкодження інфраструктури. Забезпечення високої якості обслуговування є важливим для критичних процесів, таких як комунікації, освіта та інші сервіси [2]. Резервування також забезпечує швидку адаптацію у разі зміни умов чи появи нових загроз, дозволяючи оперативно змінювати налаштування та перенаправляти ресурси для забезпечення безперервності роботи. Це допомагає знизити ризик втрати даних, або перерв у роботі підприємств, установ та закладів в умовах війни.

Крім того, наявність резервованих ресурсів дозволяє швидше відновлювати роботу після атак, або інших негативних впливів на інфраструктуру. Отже, резервування мереж доступу є важливим інструментом для забезпечення стійкості та надійності інфраструктури

електронних комунікаційних мереж в умовах агресії, що суттєво підвищує шанси на успішне функціонування. Також, що важливо, підприємство з резервованою мережею доступу має значну конкурентну перевагу, оскільки забезпечує безперервність роботи та високу якість обслуговування навіть в умовах непередбачуваних збоїв.

Резервування мереж доступу — це процес виділення та управління мережевими ресурсами для забезпечення гарантованого рівня обслуговування (QoS) для конкретних користувачів або додатків, що дозволяє забезпечити надійність та стабільність мережевих з'єднань, особливо в сучасних умовах.

Процес резервування мереж доступу включає в себе:

Вимоги: необхідно з'ясувати, які ресурси (швидкість, час доступу, сервери, тощо) необхідні для задоволення потреб [2], а також умови функціонування.

Доступність: перевірка завантаженості мережі, статусу обладнання, тощо.

Стратегія резервування: які ресурси резервуються для конкретних користувачів, та при яких умовах застосовуються (час, пріоритети, тощо).

Забезпечення механізмів резервування: протоколи та інструменти, які дозволяють автоматизувати процес резервування. Це можуть бути системи управління мережами, або програмне забезпечення для мережевого обладнання.

Резервування ресурсів: фактичне резервування, зафіксувавши ресурси за допомогою відповідних протоколів.

Моніторинг та управління: спостереження за використанням ресурсів і при необхідності коригування для оптимізації продуктивності мережі.

Відновлення штатної (повноцінної) роботи: після завершення критичної ситуації повернення до вихідного стану роботи мереж.

Вищезазначене дозволяє забезпечити необхідні ресурси для критично важливих мереж та підтримувати якість обслуговування.

1 АНАЛІЗ ТА ОГЛЯД

1.1 Аналіз функціонування діючої мережі доступу підприємства

Для того щоб провести аналіз функціонування діючої мережі доступу підприємства критичної інфраструктури необхідно спочатку ознайомитись з його узагальненими характеристиками.

Підприємство критичної інфраструктури, яке займається спеціалізованим виробництвом в інтересах сил оборони, має структуру, що відображає його обмежені розміри та вузькопрофільну діяльність. Основні характеристики підприємства:

Штат працівників: штат підприємства оцінюється в 20 – 25 посад та включає інженерів, виробничий персонал, технічних спеціалістів і адміністративних працівників. Деякі співробітники можуть виконувати кілька функцій одночасно, наприклад, інженер може відповідати як за технічне обслуговування обладнання, так і за контроль виробничих процесів.

Приміщення: підприємство займає кілька виробничих та адміністративних приміщень, розташованих у виробничій будівлі. Це спеціалізовані цехи для виробництва, складання та обробки продукції для сил оборони, а також офісні приміщення для управління та планування. Кожне виробниче приміщення обладнане необхідною технікою для забезпечення безперервного виробничого процесу. Будівля знаходиться в межах обласного центру, в промисловій зоні, поруч будівлі 2-9 ти поверхові. Поблизу (1-2 км.) кілька вузлів різних провайдерів забезпечених безперебійним живленням.

Обладнання: Підприємство використовує обладнання для виробництва, встановлене в основному у 2010-2020 роках, яке відповідає стандартам якості та безпеки. Комп'ютери, сервери та інші пристрої для управління виробництвом, адміністративної діяльності, зворотного зв'язку, тощо, з'єднані через комутатори в локальну мережу, що забезпечує виробничий процес.

Об'єднання інформаційного простору: Всі виробничі та адміністративні приміщення підприємства об'єднані локальною мережею,

що забезпечує швидкий і зручний доступ до даних про виробництво та управлінських ресурсів. Це дозволяє працівникам легко обмінюватися інформацією та оперативно керувати виробничими процесами. Локальна мережа включає в себе Wi-Fi мережу, що забезпечує швидке бездротове підключення нових пристроїв зі швидкістю до 100 Мбіт/с.

Комутатори та кабельна інфраструктура: На підприємстві використовуються комутатори зі швидкістю до 1 Гбіт/с для з'єднання виробничих пристроїв через Ethernet-кабелі CAT5e, що забезпечує стабільну швидкість передачі даних у внутрішній мережі.

Мережа доступу (WAN): Підключення до інтернету здійснюється через оптоволоконний модем зі швидкістю до 100 Мбіт/с. Підприємство використовує динамічні IP-адреси, що надаються провайдером, оскільки воно не має статичної IP-адреси.

Мережева безпека: Локальна мережа підприємства захищена базовими засобами, такими як брандмауери, антивірусні програми та система контролю доступу. Особлива увага приділяється безпеці даних, пов'язаних з розробкою нових рішень в інтересах виробництва для сил оборони [3].

Технічна підтримка: Технічна підтримка мережі та обладнання здійснюється внутрішніми IT-фахівцями, а також зовнішніми підрядниками, які забезпечують стабільність і обслуговування критичних систем мережі і обладнання.

Підприємство стабільно працювало та розвивалось в 2015-2022 роках. За період з 2022 року по теперішній час неодноразово виникали аварійні зупинки в виробництві, затримки відвантаження продукції, складнощі в логістичній і фінансовій діяльності. На фоні виникаючих ризиків та для подальшого розвитку керівництво підприємства прийняло рішення про удосконалення і резервування мережі доступу підприємства [5].

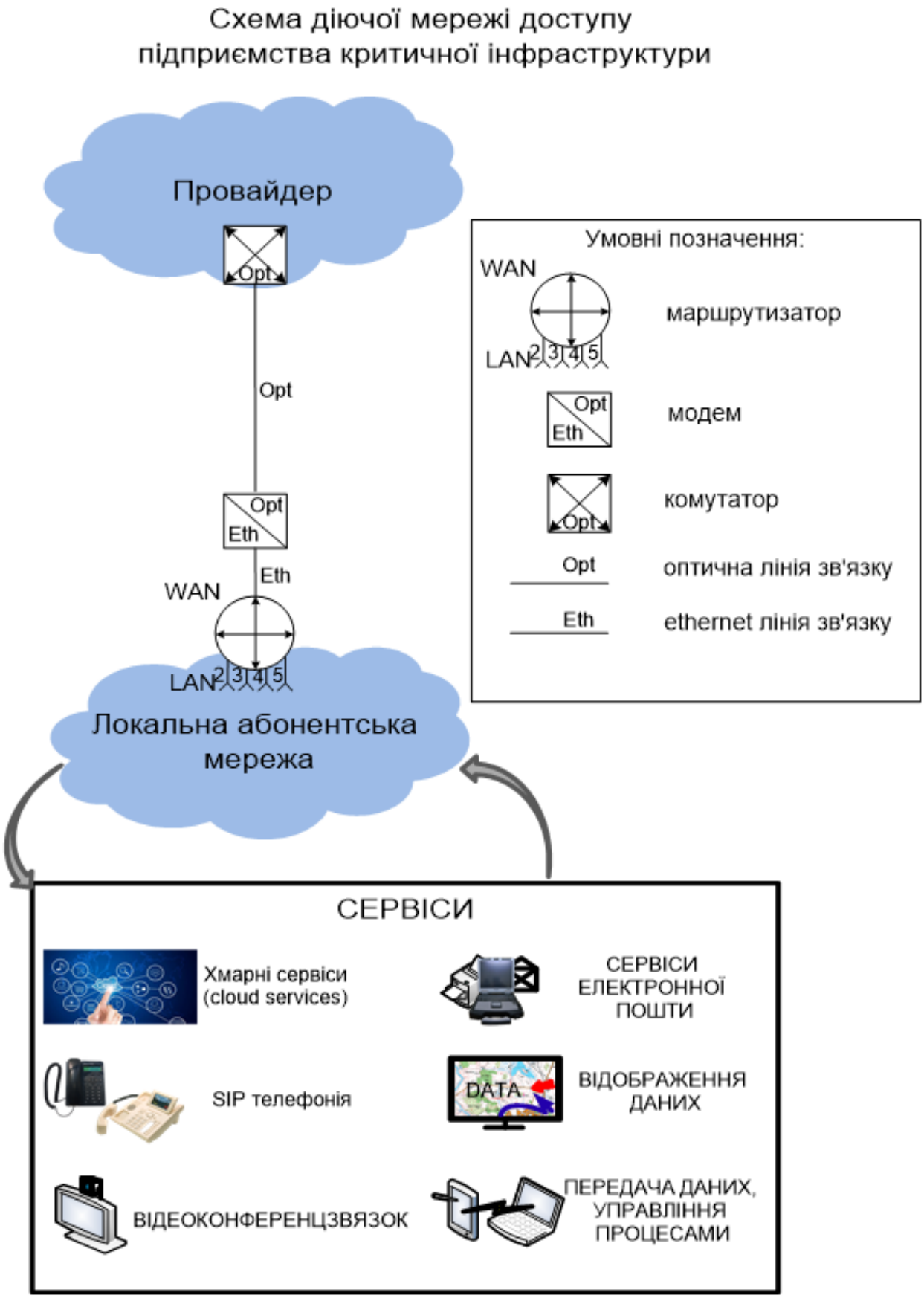


Рисунок 1.1 – Діюча мережа доступу

Структура мережі доступу підприємства складається з кількох ключових елементів, які забезпечують зв'язок та обмін даними.

На першому етапі розташована локальна мережа підприємства, що складається з комп'ютерів, серверів та інших пристроїв, з'єднаних між собою. Всі ці пристрої підключені до роутера, який виконує функцію маршрутизації трафіку всередині локальної мережі та забезпечує вихід в інтернет.

Роутер має Ethernet WAN-порт, який служить для підключення до зовнішніх мереж. Через цей порт роутер з'єднується з Ethernet-лінією, що забезпечує зв'язок з провайдером.

Далі Ethernet-лінія підключається до модему, який конвертує Ethernet-сигнал у формат, придатний для передачі через оптоволоконну лінію.

Оптична лінія звязку забезпечує високу швидкість передачі даних на великі відстані і є основою для з'єднання з мережею провайдера. Оптичний комутатор провайдера комутує трафік у електронну комунікаційну мережу загального користування.

Таким чином, структура мережі доступу підприємства включає локальну мережу, роутер з Ethernet WAN-портом, Ethernet-лінію, модем, оптичну лінію та оптичний комутатор провайдера, що забезпечує простий доступ до інтернету та інших мережевих ресурсів.

Така структура мережі доступу досить проста, але має ряд суттєвих недоліків:

Ця система може бути вразливою до збоїв на різних етапах. Наприклад, якщо модем, або роутер вийдуть з ладу, це призведе до втрати зв'язку. Також фізичні пошкодження Ethernet-лінії, або оптичної лінії можуть викликати серйозні перерви в обслуговуванні.

Хоча оптичні лінії забезпечують високу швидкість передачі даних, якість з'єднання може знижуватися на етапах перетворення сигналів

(наприклад, між Ethernet і оптикою) або через обмеження маршрутизації в роутері. Ці фактори можуть призвести до затримок у передачі даних.

Система повністю залежить від електропостачання. У разі відключення електроживлення всі елементи (роутер, модем, комутатор) перестануть працювати, що призведе до втрати доступу до мережі. Це робить підприємство вразливим до зовнішніх чинників, таких як аварії в енергомережах.

Загалом, хоча ця структура забезпечує функціональність, її недоліки в надійності, швидкості та енергонезалежності можуть впливати на стабільність роботи підприємства.

1.2 Вимоги підприємства як споживача електронних комунікаційних послуг [2], [9]

Підприємство критичної інфраструктури [5], яке займається спеціалізованим виробництвом висуває наступні вимоги до мережі доступу:

Висока пропускна здатність: Підприємству потрібна стабільна та швидка мережа з пропускною здатністю, достатньою для одночасного обслуговування виробничих процесів, передачі великих обсягів даних і підтримки зв’язку з підрядниками, або військовими установами. Швидкість підключення до інтернету має бути не менш ніж 100 Мбіт/с.

Надійність і безперервність роботи: Оскільки виробничі процеси можуть бути критичними для оборонної сфери, мережа повинна забезпечувати безперебійну роботу з мінімальними затримками і максимальною доступністю. Будь-які перебої можуть вплинути на безпеку та виробництво.

Безпека: Оскільки підприємство обслуговує сили оборони, мережа повинна бути захищена на найвищому рівні. Це передбачає використання брандмауерів, систем контролю доступу, VPN для безпечного з'єднання з віддаленими об'єктами, шифрування даних і

захист від кіберзагроз. Безпека інформації та виробничих даних є критично важливими [3], [6].

Можливість масштабування: мережа повинна мати гнучкість для швидкого масштабування, якщо виробничі потреби зростають. Це стосується як збільшення кількості підключених пристроїв, так і розширення пропускної здатності при зростанні обсягу переданих даних.

Можливість швидкої релокації: повинна бути можливість швидкого розгортання мережі доступу на новому місці в інтересах всього виробництва, або підрозділу підприємства, а також тимчасового швидкого розгортання/згортання в умовах польових випробувань продукції.

Захист від збоїв: Необхідне забезпечення захисту від збоїв та резервні канали зв'язку (наприклад, використання декількох провайдерів, або резервних ліній, резервування живлення та обладнання), щоб уникнути зупинки виробничих процесів у випадку технічних проблем.

Якість обслуговування (QoS): Мережа повинна забезпечувати пріоритезацію критично важливих даних та з'єднань. Це дозволить уникнути затримок у передачі важливої інформації, що має стратегічне значення для підприємства.

Мінімальні затримки (latency): Особливо важливо для підтримки реального часу під час управління процесами на віддалених локаціях або при обміні даними з оборонними відомствами.

Підтримка динамічних IP-адрес або статичних адрес при необхідності: Підприємство використовує динамічні IP-адреси, але в разі потреби у статичній IP-адресі для певних додатків або захищених з’єднань, має бути можливість налаштувати таку послугу.

Сумісність із наявним обладнанням: Мережеве обладнання, яке використовується на підприємстві (комутатори, маршрутизатори,

сервери), повинне бути сумісним з інфраструктурою мережі доступу, що дозволяє легко інтегрувати його у виробничі процеси.

Вимоги до удосконаленої мережі доступу можна перераховувати до нескінченості [7], але реалізація їх в повному обсязі можлива лише при нескінченому бюджеті. Необхідність реалізації рішень по удосконаленню мережі доступу буде ухвалена на підставі аналізу позитивних і негативних вірогідних наслідків для підприємства.

1.3 Вимоги та рекомендації діючих керівних документів

При прийнятті рішення по проектуванню та впровадженню удосконаленої мережі доступу та її резервуванні необхідно врахувати вимоги та бажано втілити рекомендації діючого законодавства, розпорядчих документів та концепцій розвитку галузі електронних комунікацій. Нижче приведено основні з них:

Закон України "Про електронні комунікації" [4].

Безперервність надання електронних комунікаційних послуг: Закон зобов’язує постачальників вживати технічних та організаційних заходів для забезпечення безперервності надання послуг, а також для захисту від несанкціонованого доступу до мережі та даних. Це включає заходи для забезпечення безпеки та сталості функціонування мереж.

Стійкість електронних комунікаційних мереж: Мережі повинні зберігати свої функції під впливом дестабілізуючих чинників (сталість електронної комунікаційної мережі). Це стосується резервування та захисту мережі від зовнішніх впливів, які можуть призвести до збоїв або перебоїв у наданні послуг.

Оперативне управління під час надзвичайних ситуацій: Закон вимагає забезпечення безперебійного управління електронними комунікаційними мережами під час надзвичайного стану, або воєнного стану, що є критично важливим для підприємств, які належать до критичної інфраструктури.

ДСТУ 2861-94 "Державний стандарт України Надійність техніки, аналіз надійності" Основні положення. [1]

Аналіз надійності: Стандарт передбачає необхідність оцінки надійності об'єкта, що включає перевірку ефективності запропонованих заходів щодо доопрацювання конструкції, технології виготовлення та стратегії технічного обслуговування для підвищення надійності систем, що можуть стосуватися мереж доступу (розділ 4.1).

Програма забезпечення надійності (ПЗН): Аналіз надійності передбачає заходи для забезпечення безвідмовності, довговічності та ремонтопридатності системи. Ці заходи також включають резервування компонентів або елементів системи для забезпечення їх стабільної роботи (розділ 5.1).

Методи забезпечення надійності: Стандарт описує можливість використання резервних або надлишкових шляхів функціонування системи, що дозволяє забезпечити стабільну роботу у разі відмови окремих компонентів або елементів (Додаток Б.3).

Таким чином, ДСТУ 2861-94 визначає необхідність аналізу надійності систем, що може включати резервування та заходи для забезпечення стабільної роботи мереж, особливо у критичних умовах.

"Стратегія розвитку сфери електронних комунікацій України на період до 2030 року" презентована Міністерством цифрової трансформації України 16 травня 2024 року. [7]

Безперебійне функціонування мереж електронних комунікацій є критично важливим для державних, військових та суспільних інтересів. Важливо формувати державну політику таким чином, щоб постійно підвищувати стійкість та безвідмовність функціонування електронних комунікаційних мереж. Необхідно розробити інструменти для забезпечення безперервності роботи електронних комунікаційних мереж, ухвалити Стратегію цифрової стійкості, затвердити технічні

вимоги до електронних комунікаційних мереж щодо їх сталості, а також проводити дослідження сталості мереж.

Необхідно забезпечити резервне живлення та впровадження систем аварійного відновлення електронних комунікаційних мереж для забезпечення неперервності роботи об'єктів критичної інфраструктури електронних комунікаційних мереж.

Ці пункти підкреслюють важливість резервування та підтримки стабільної роботи мереж для забезпечення безпеки та надійності в умовах сучасних викликів.

1.4 Огляд існуючих можливостей підключення до мережі Інтернет [4], [10]

Послуги доступу до мережі Інтернет провайдер до клієнта може забезпечувати різними способами будуючи лінії зв’язку за різними технологіями. Нижче приведені основні різновиди лінії зв’язку які використовуються для розгортання мереж доступу.

Кабельні лінії:

а.) Мідний кабель:

- Кручена пара (UTP, STP): Найпоширеніший тип для локальних мереж (LAN). Використовується для передачі даних на короткі відстані.

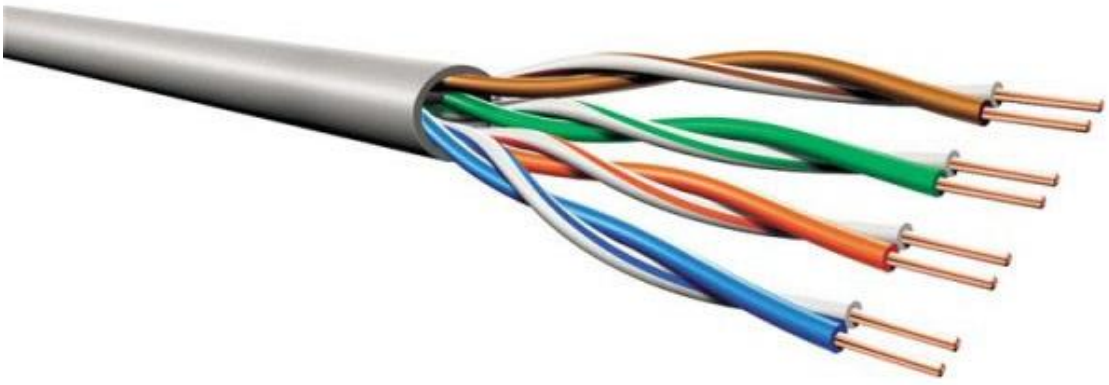


Рисунок 1.2 – Кручена пара UTP

- Коаксіальні кабелі: Використовуються для телевізійних мереж, інтернет-з'єднань та передавання даних на великі відстані. Їх використовували для доступу до мережі Інтернет раніше, на теперішній час

замінені іншими рішеннями.

Рисунок 1.3 – Коаксіальний кабель

- Чотирьох, або двох провідна лінія для DSL: вважається застарілою технологією порівняно з сучасними оптоволоконними мережами. Проте DSL лінії були основними засобами для забезпечення доступу до інтернету в минулому, до розповсюдження більш сучасних технологій. В деяких ситуаціях використовується і на даний час.

Рисунок 1.4 – Обладнання DSL лінії

- Силові кабелі з передачею даних: Використовуються у спеціальних системах для одночасної передачі електричної енергії та даних, наприклад, в системах інтелектуальних мереж (Smart Grids).

Рисунок 1.5 – Силовий кабель з можливістю передачі даних

b.) Оптоволоконний кабель:

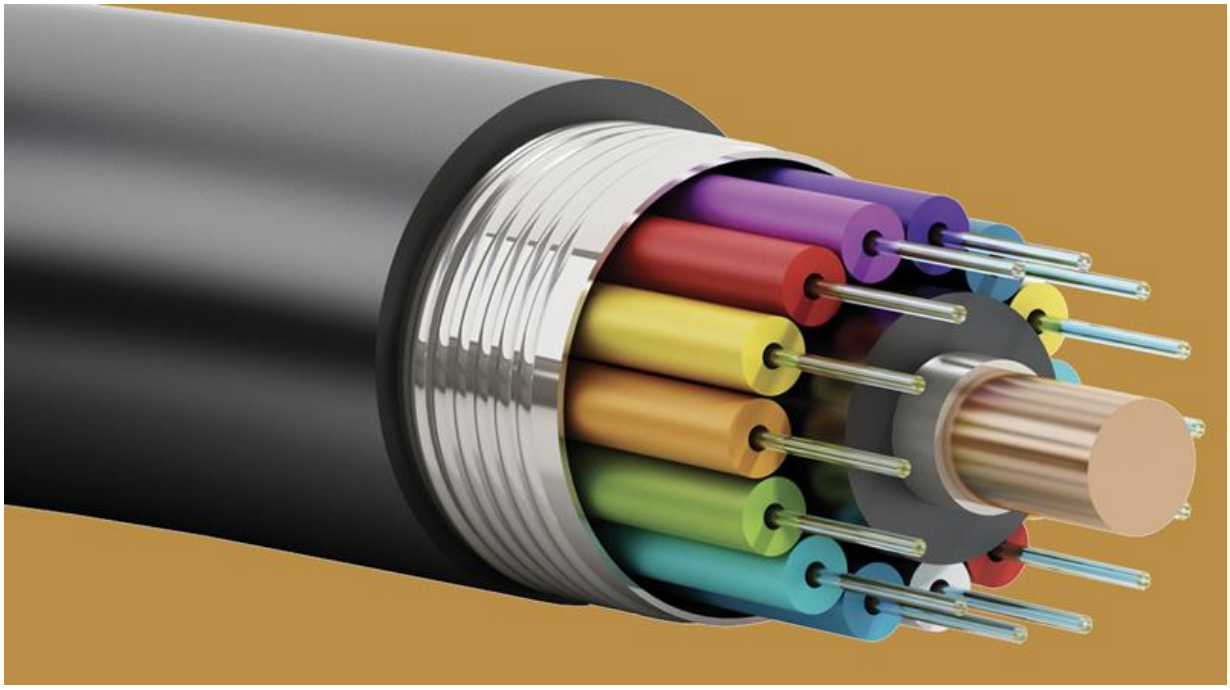
FTTx (Fiber to the x) — це загальний термін для різних типів оптоволоконних архітектур мереж доступу. Літера «x» в назві може замінюватися різними варіантами залежно від того, де закінчується оптичне волокно і як далі передаються дані. Найпоширеніші типи FTTx:

- FTTH (Fiber to the Home): Оптичне волокно підведене безпосередньо до абонента/користувача. Це найкращий варіант, оскільки повністю усуває мідні дроти та забезпечує максимальну швидкість.

- FTTB (Fiber to the Building/Business): Оптичне волокно підводять до будівлі або офісного центру, а всередині використовуються інші технології (наприклад, Ethernet або VDSL) для розподілу сигналу між користувачами.

- FTTC (Fiber to the Curb/Cabinet): Оптоволокно підводять до вуличного вузла або кабінету біля будівлі, після чого дані передаються через мідні або коаксіальні кабелі до кінцевого користувача.

- FTTN (Fiber to the Node/Neighborhood): Волокно підводять до сусіднього вузла, де сигнал переходить на мідні лінії для розподілу в житлові будинки. Ця технологія також має обмеження по швидкості на



останній ділянці мідної лінії.

Рисунок 1.6 – Оптичний кабель

PON (Passive Optical Network)

- **GPON (Gigabit Passive Optical Network)**: Широко використовується для побудови оптичних мереж доступу. Це пасивна оптична мережа, яка дозволяє використовувати одну оптичну лінію для обслуговування кількох абонентів. GPON підтримує передачу до 2,5 Гбіт/с на завантаження і до 1,25 Гбіт/с на відправлення.

- **EPON (Ethernet Passive Optical Network)**: Альтернативна технологія до GPON, базується на стандарті Ethernet. Вона також використовує пасивну інфраструктуру, але інтегрується в Ethernet-

мережі простіше. Швидкість досягає 1 Гбіт/с, а існує також і версія 10G-EPON для швидшої передачі даних.

Active Optical Network (AON): Це оптична мережа з активними елементами, де кожен користувач має індивідуальне оптоволоконне з'єднання. В AON використовуються активні комутатори або маршрутизатори для управління трафіком. AON забезпечує високу швидкість і більш контрольоване розподілення пропускної здатності,

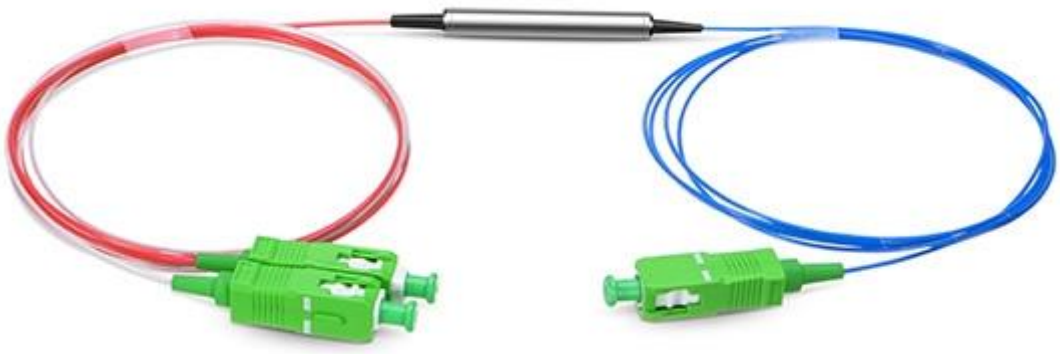
але потребує більше обладнання та енергетичних ресурсів порівняно з PON.

Рисунок 1.7 – Оптичний кабель для PON

WDM (Wavelength Division Multiplexing)

- CWDM (Coarse Wavelength Division Multiplexing): Технологія, яка дозволяє передавати кілька сигналів різних довжин хвиль по одному оптоволокну. Вона використовується для підвищення пропускної здатності на вже існуючих волокнах, що особливо актуально в мережах доступу, де необхідно масштабувати пропускну здатність.

- **DWDM (Dense Wavelength Division Multiplexing)**: Більш просунута технологія, яка дозволяє передавати ще більше каналів по



одному волокну з вищою щільністю. Використовується в магістральних мережах, але також може бути застосована на рівні мереж доступу для підвищення ємності.

Рисунок 1.8 – Оптичний кабель з мультиплексором

Радіо лінії:

Радіолінії для мереж доступу використовуються для бездротової передачі даних, особливо в тих випадках, коли побудова кабельних мереж є економічно невигідною, або технічно складною. Радіотехнології забезпечують швидкий доступ до мережі, особливо на великих відстанях, або в сільській місцевості. Основні типи радіоліній, які використовуються в мережах доступу:

а.) Мікрохвильові (надвисокочастотні) радіолінії

- Земні мікрохвильові лінії: Працюють у діапазонах від 6 ГГц до 38 ГГц. Вони використовують прямі лінії передачі між двома точками (точка-точка, Point-to-Point, PtP). Це високошвидкісні радіоканали, які забезпечують високу пропускну здатність на відстанях до кількох десятків кілометрів. Основні характеристики:

- Швидкість передачі даних може досягати 1 Гбіт/с і більше.
- Потребують прямої видимості між передавачем і приймачем.

- Використовуються для магістральних ліній і підключення базових станцій до основних мереж.

Рисунок 1.9 – Станції широкосмугового доступу

- Мікрохвильові радіорелейні системи: Використовуються для передачі сигналів на великі відстані, часто поєднуючи кілька проміжних станцій. Це популярний метод передачі даних у важкодоступних, або віддалених регіонах.

Рисунок 1.10 – Радіорелейна станція

b.) Wi-Fi (IEEE 802.11): Популярний стандарт бездротового доступу в локальних мережах (LAN), часто використовується для мереж доступу в міських і сільських районах.

- Працює в діапазонах 2,4 ГГц та 5 ГГц (Wi-Fi 6 — до 6 ГГц).
- Максимальна швидкість передачі даних досягає кількох Гбіт/с у новітніх версіях (Wi-Fi 6 і 6E).

- Використовується як для домашнього доступу до інтернету, так і для публічних бездротових мереж.
- Може використовуватись для організації бездротового підключення в сільській місцевості, або на великих територіях.

Рисунок 1.11 – Wi-Fi точки доступу

c.) WiMAX (Worldwide Interoperability for Microwave Access), (IEEE 802.16): Це технологія бездротового широкосмугового доступу, що забезпечує високошвидкісний доступ до інтернету на великих відстанях.

- Використовується в діапазонах 2,3, 2,5, 3,5 ГГц та інших.
- Підтримує передачу даних на відстані до 50 км.
- Швидкість передачі даних може досягати 70 Мбіт/с, а в деяких реалізаціях до 1 Гбіт/с.
- Використовується для підключення віддалених сільських районів, або організації муніципальних мереж.

Рисунок 1.12 – WiMAX обладнання

d.) 4G/5G

- 4G (LTE, Long-Term Evolution): Четверте покоління мобільного зв'язку, що забезпечує високошвидкісний інтернет доступ. LTE може досягати швидкості до 1 Гбіт/с.

- 5G: П'яте покоління мобільних мереж, яке значно підвищує швидкість і знижує затримки в порівнянні з 4G. Швидкість передачі може досягати кількох Гбіт/с, а відстань і якість покриття залежать від використовуваного частотного діапазону:

- Низькочастотні діапазони (600 МГц - 1 ГГц): Велике покриття і хороша проникність крізь перешкоди.
- Середньочастотні діапазони (1-6 ГГц): Компроміс між покриттям і швидкістю.
- Міліметрові хвилі (24 ГГц і вище): Забезпечують найвищі швидкості, але мають обмежене покриття і потребують прямої видимості.

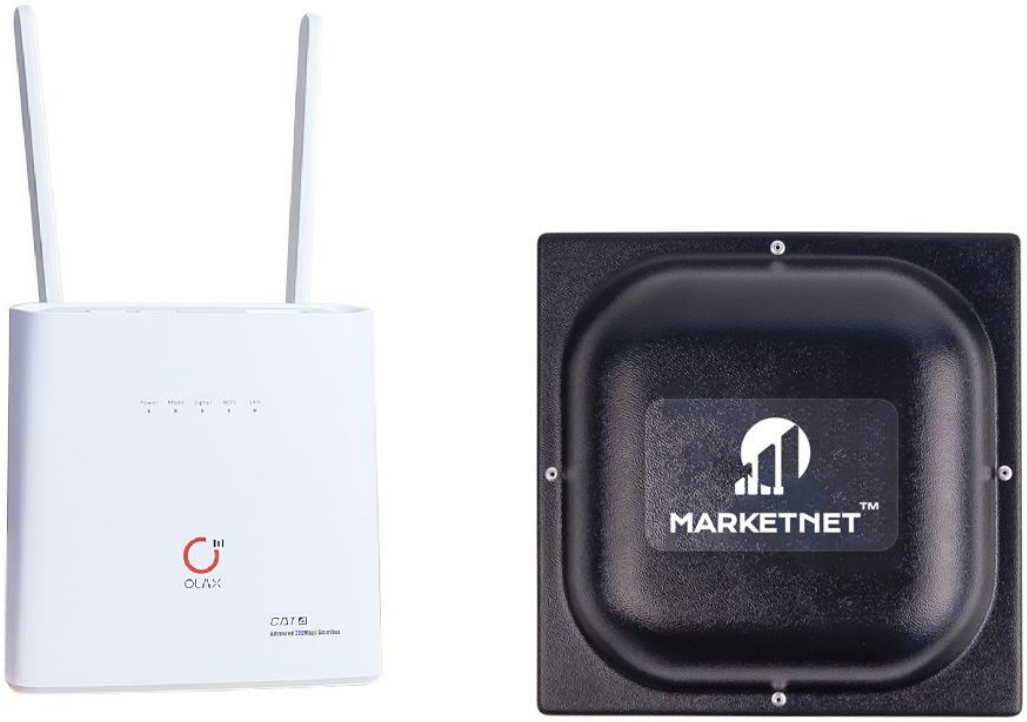


Рисунок 1.13 – 4G модем та антена

e.) MMDS (Multichannel Multipoint Distribution Service) - це технологія бездротового зв'язку, яка використовує мікрохвильові частоти (діапазони 2,5-2,7 ГГц) для передачі даних. Використовується для організації точка-багатоточка (Point-to-Multipoint**,** PtMP**) мереж.**

- Забезпечує бездротовий доступ до інтернету або телекомунікацій на великих територіях.
- Швидкість передачі даних може досягати 10-100 Мбіт/с.
- Використовується в основному для підключення віддалених регіонів, сільських мереж або розподілу контенту.

f.) Satellite Internet (Супутниковий Інтернет): Застосовується для забезпечення доступу до інтернету в дуже віддалених регіонах, де немає можливості прокладати кабелі або використовувати наземні радіолінії.

- Працює через геостаціонарні або низькоорбітальні супутники.
- Швидкість варіюється від 10 Мбіт/с до 100+ Мбіт/с (у нових супутникових системах, як Starlink).

- Недолік: велика затримка передачі даних, особливо на геостаціонарних супутниках.

Рисунок 1.14 – Термінал супутникового зв’язку (геостаціонарний)

g.) LMDS (Local Multipoint Distribution Service) використовує міліметрові хвилі (діапазон 28-31 ГГц) для організації широкосмугових мереж доступу, зазвичай в міських зонах.

- Принцип дії схожий на MMDS, але з використанням вищих частот.
- Підходить для організації бездротових широкосмугових мереж на обмежених територіях (наприклад, бізнес-центри або міські райони).

Переваги радіоліній для мереж доступу:

- **Гнучкість**: Можливість розгортання в будь-якій місцевості, незалежно від наявності кабельної інфраструктури.
- **Швидкість розгортання**: Радіолінії можна розгорнути набагато швидше, ніж прокласти кабелі.

- **Мобільність**: Бездротові рішення можна легко адаптувати до потреб мобільних користувачів або тимчасових рішень (наприклад, для забезпечення інтернету на великих подіях).

Однак радіолінії мають і свої недоліки, такі як обмежений радіус дії, потреба у прямій видимості та можливість перешкод від інших радіоджерел.

1.5 Приклади діючих мереж доступу

Нижче наведені приклади діючих мереж доступу від абонента до провайдера, які використовують різні типи ліній зв'язку — як кабельних, так і бездротових. Такі мережі забезпечують користувачам доступ до інтернету через різні технології, залежно від інфраструктури та умов покриття.

а.) Мережі на основі оптоволоконних ліній (FTTx)

- **FTTH (Fiber to the Home)**: Це найбільш передова і швидкісна технологія, де оптоволокно підводять безпосередньо до дому, офісу, або квартири користувача.
  - **Приклад**: У багатьох містах світу та в Україні мережі на основі FTTH активно розгортаються великими інтернет-провайдерами, такими як **Укртелеком**, **Київстар,** або **Vodafone Україна**. Вони пропонують інтернет на швидкості до 1 Гбіт/с, або більше для приватних користувачів і підприємств.
- **FTTB (Fiber to the Building)**: Волокно підводиться до будівлі, а всередині використовується Ethernet, або інша мідна технологія для підключення окремих квартир, або офісів.
  - **Приклад**: Мережі доступу в багатоповерхових будинках в українських містах, таких як Київ, Дніпро та Львів, які надають провайдери **Ланет**, **Triolan** та інші.

b.) Мережі на основі мідних ліній (DSL)

- **ADSL (Asymmetric DSL)**: Використовує звичайні телефонні лінії (мідні дроти) для передачі даних. Це більш стара технологія, але вона все ще популярна у віддалених районах.
  - **Приклад**: **Укртелеком** в Україні продовжує пропонувати ADSL-з'єднання в сільських і віддалених регіонах, де немає можливості прокладати оптоволокно. Швидкість таких з'єднань може досягати до 24 Мбіт/с на завантаження.
- **VDSL (Very High-Speed DSL)**: Використовує ті ж мідні лінії, але забезпечує більші швидкості на коротших відстанях.
  - **Приклад**: У містах України, наприклад, провайдер **Київстар** надає VDSL-з'єднання в місцях, де не можна встановити оптоволокно, забезпечуючи швидкість до 100 Мбіт/с.

c.) Кабельні мережі (DOCSIS)

- **DOCSIS (Data Over Cable Service Interface Specification)**: Технологія, що використовує коаксіальні кабелі, які зазвичай використовуються для телебачення, для надання широкосмугового інтернету.
  - **Приклад**: У багатьох європейських країнах і в Україні провайдери, такі як **Воля** (тепер під брендом **Vodafone Україна**), надають послуги інтернету через кабельні мережі DOCSIS, з можливістю підключення швидкості до 500 Мбіт/с і вище.

d.) Бездротові мережі (4G/5G)

- **4G (LTE)**: Використовується для надання мобільного інтернету в зонах, де немає проводового підключення. Швидкість LTE може досягати до 100 Мбіт/с.
  - **Приклад**: Оператори мобільного зв'язку в Україні — **Київстар**, **Vodafone Україна** та **lifecell** — надають послуги мобільного інтернету через 4G/LTE, забезпечуючи покриття по всій країні. Це особливо популярно в сільських і віддалених районах.

- **5G**: П'яте покоління мобільних мереж, яке дозволяє отримувати швидкість до кількох Гбіт/с і знижену затримку.
  - **Приклад**: В Україні технологія 5G ще в процесі впровадження, але в багатьох країнах Європи, таких як Німеччина чи Швеція, оператори вже надають комерційні 5G-послуги для приватних та бізнес-абонентів.

e.) Wi-Fi (Fixed Wireless Access)

- **Wi-Fi для домашніх мереж або муніципальних мереж доступу**: Це бездротові мережі, що використовуються для організації точка-точка або точка-многоточка з'єднань для доступу до інтернету.
  - **Приклад**: Провайдери можуть використовувати Wi-Fi для надання інтернету у важкодоступних місцях, де складно прокладати кабелі. Наприклад, у деяких сільських регіонах або на туристичних об'єктах Wi-Fi мережі використовуються як основний засіб доступу до інтернету.

f.) Мікрохвильові лінії зв'язку

- **Мікрохвильові радіорелейні лінії (точка-точка)**: Використовуються для забезпечення зв'язку між базовими станціями та інфраструктурою провайдера. Ця технологія застосовується для передачі великих обсягів даних на відстані кількох десятків кілометрів.
  - **Приклад**: Багато операторів мобільного зв'язку використовують мікрохвильові лінії для підключення базових станцій до магістральних оптоволоконних мереж. Наприклад, **Vodafone Україна** використовує такі лінії для забезпечення стабільного з'єднання в регіонах з недостатньою оптоволоконною інфраструктурою.

g.) Супутниковий інтернет

- **Супутниковий інтернет (Starlink, VSAT)**: Забезпечує доступ до інтернету через супутникові системи, що робить його особливо важливим у віддалених регіонах, де немає іншої інфраструктури.

- **Приклад**: Система **Starlink** від SpaceX вже активно використовується в Україні для забезпечення інтернету в місцях з пошкодженою інфраструктурою, або у віддалених регіонах. Також існують інші супутникові рішення **[14]**, такі як **VSAT (Very Small Aperture Terminal) — мала супутникова наземна станція, термінал з антеною, за міжнародною класифікацією до менше 2,5 метрів**, які використовуються в різних регіонах для доступу до інтернету, наприклад IDirect, або Tooway.

1.6 Висновки по першому розділу

Проектування та побудова мережі доступу для підприємства критичної інфраструктури на теперішній час в Україні є складним, але цікавим завданням, яке потребує врахування багатьох факторів: від технічних вимог і доступності технологій до безпеки та надійності інфраструктури. Виходячи з аналізу проведеного в першому розділі, можна зробити наступні висновки щодо наявності, доступності та порядку вибору мережевих рішень.

а.) Типи ліній зв'язку та технологій доступу

Сучасна інфраструктура в Україні пропонує широкий вибір технологій для побудови мереж доступу, які можуть бути використані підприємствами критичної інфраструктури:

- **Оптоволоконні лінії (FTTx)**: Найнадійніше та швидке рішення для передачі великих обсягів даних. В Україні розвиваються FTTH, FTTB та FTTC, забезпечуючи стабільний інтернет для критичної інфраструктури.
- **Мідні лінії (DSL)**: Застаріле, але тимчасове рішення для віддалених регіонів, де немає оптоволоконних мереж. Підходить для невеликих об'єктів із низькими потребами.

- **Кабельні мережі (DOCSIS)**: Може використовуватися там, де є коаксіальна інфраструктура, але менш надійні порівняно з оптоволокном.

- **Бездротові мережі (4G/5G, Wi-Fi, мікрохвильові лінії зв'язку, супутниковий доступ)**: Використовуються у мобільних або віддалених місцях, де неможливо прокласти кабель.

b.) Обладнання для мереж доступу

Залежно від обраної технології доступу, наявне в Україні обладнання дозволяє забезпечити надійний зв'язок для підприємств критичної інфраструктури. Наприклад:

- Для **оптоволоконних мереж** використовуються рішення від таких виробників, як **Huawei** та **ZTE** (OLT, ONT, сплітери), що забезпечують надійне та швидке підключення з високою пропускною здатністю.

- Для **бездротових мереж 4G/5G** можна використовувати обладнання типу **Huawei B535 4G CPE** або **ZTE MC801A 5G CPE**, що дозволяє організувати швидкий доступ до інтернету в місцях, де немає кабельної інфраструктури.

- Для **мікрохвильових ліній** застосовуються пристрої, такі як **Cambium Networks PTP 820**, що дозволяє забезпечити безперебійний зв'язок між віддаленими об'єктами.

- Для **супутникового зв'язку** використовується обладнання Starlink від SpaceX, або наприклад, термінали Tooway від ViaSat.

c.) Надійність і безпека мереж

Для підприємств критичної інфраструктури особливо важливі параметри **надійності** та **безпеки** мереж:

- **Оптоволоконні мережі** забезпечують високу надійність і захищеність від зовнішніх впливів, включно з електромагнітними перешкодами. Це робить їх найкращим вибором для критичних об'єктів, таких як енергетичні, транспортні, комунікаційні мережі та підприємства оборонного комплексу.

- Бездротові рішення можуть використовуватися як резервні канали зв'язку, забезпечуючи безперервну роботу підприємства в разі збоїв основної мережі. 4G мережі, наприклад, дозволяють передавати дані з відносно невеликою затримкою, що важливо для резервування систем контролю та моніторингу.

- Супутникові системи (Starlink, Tooway) можуть бути використані як резервні рішення для віддалених або стратегічних об'єктів, де інші типи з'єднань недоступні або ненадійні.

d.) Доступність інфраструктури в Україні

В Україні інфраструктура для побудови мереж доступу постійно розвивається, проте є певні відмінності залежно від регіону:

- У великих містах (Київ, Львів, Харків) доступні сучасні **FTTH/FTTB мережі** з високошвидкісним інтернетом і повноцінною інфраструктурою для побудови корпоративних мереж.

- У сільських та віддалених регіонах, та районах постраждалих при веденні бойових дій іноді використовуються застарілі **DSL, або 4G рішення**, однак це може бути ефективним для забезпечення тимчасового доступу або резервних ліній зв'язку.

e.) Порядок вибору та проектування мережі доступу

Проектування мереж доступу для підприємств критичної інфраструктури може проходити у кілька етапів:

a) **Оцінка потреб**: Визначення вимог до швидкості, стабільності, безпеки і резервування. Критичні підприємства зазвичай потребують високошвидкісного і захищеного з'єднання з резервними каналами зв'язку.

b) **Вибір технології**: Оптимальний варіант для критичної інфраструктури — **оптоволоконні рішення (FTTH, FTTB),** або **мікрохвильові лінії**, залежно від розташування об'єктів. Віддалені об'єкти можуть використовувати супутникові рішення.

c) **Проектування резервної мережі**: Для гарантії безперервної роботи варто проектувати не тільки основний канал, але й резервні — через інші технології (4G/5G, мікрохвильові, супутникові).

d) **Впровадження систем захисту**: Особливо важливою є **кібербезпека** мереж для підприємств критичної інфраструктури, що включає захист від DDoS-атак, шифрування даних та фізичну безпеку обладнання.

В Україні доступні різні технології побудови мереж доступу для підприємств критичної інфраструктури, зокрема оптоволоконні, мідні, бездротові та супутникові рішення. Найбільш надійними та перспективними є оптоволоконні мережі (FTTH/FTTB), які забезпечують високошвидкісний і надійний зв'язок, критично важливий для безперервної роботи. Для резервних або віддалених рішень можуть використовуватися мікрохвильові лінії, 5G або супутникові технології. Проектування мереж для критичних підприємств повинно враховувати вимоги до безпеки, надійності та резервування з'єднань.

2 ПОСТАНОВКА ЗАВДАННЯ ТА РОЗРОБКА СХЕМИ

2.1 Розробка моделі

Враховуючи вимоги до що ставляться до розглядаємого підприємства, існуючи можливості апаратного та програмного забезпечення, а також пропозиції ринку надання послуг електронних комунікацій пропоную наступну модель мережі доступу:

- основна оптоволоконна лінія доступу побудована на технології GPON, що дозволяє забезпечити достатню для повноцінної роботи швидкість та енергонезалежність, а також на ринку присутні 5-7 провайдерів, які надають дану послугу;
- резервування оптоволоконної лінії здійснити за допомогою Wi-Fi (IEEE 802.11), пропозицій на ринку безліч, в великих відстанях потреби немає (підприємство в межах обласного центру), швидкість достатня для резервування;
- резервування на випадок виходу з ладу обладнання провайдера та/або забезпечення функціонування віддаленого підрозділу підприємства здійснити за допомогою терміналу супутникового зв’язку, вибір на ринку достатній, але між пропозиціями велика різниця в технічних і економічних параметрах.

Вище приведена модель буде виглядати наступним чином [8]:

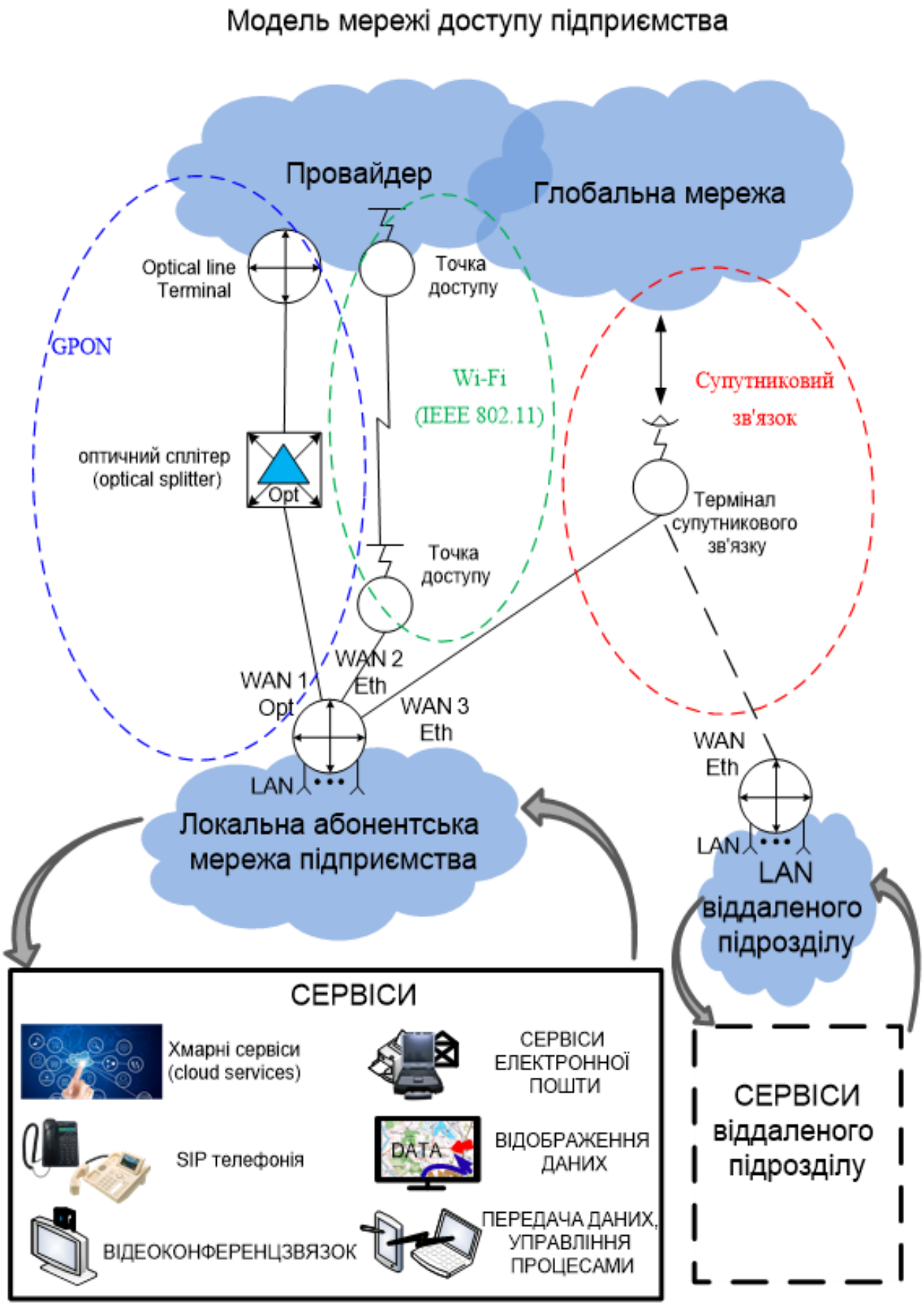


Рисунок 2.1 – Модель мережі доступу, що пропонується

2.2 Можливі варіанти, переваги і недоліки

Вибір основної лінії доступу побудований на технології **GPON** обумовлений наступними факторами:

- виконуються основні вимоги підприємства щодо забезпечення швидкості від 100 Мбіт/с та енергонезалежність обладнання (більшість провайдерів обіцяють підтримку енергоживлення свого обладнання на вузлах зв'язку під час критичних ситуацій, а сама лінія не потребує живлення) [9];
- дана технологія доступна на ринку, при чому вартість підключення та абонентська плата еквівалентна вже діючому підключенню.

Основним недоліком такої лінії є її фізична вразливість, проте поверхневий аналіз показав що всі провайдери мають аварійні бригади для ремонту пошкоджень, частина оптоволоконного кабелю прокладається по кабельним шахтам під землею, а вузли зв'язку знаходяться під охороною.

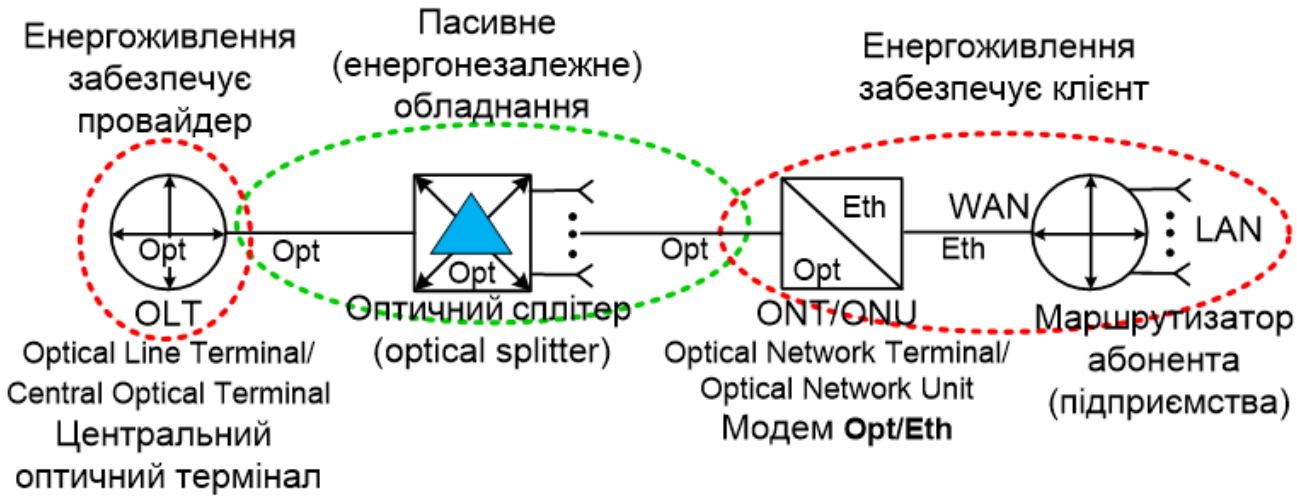


Рисунок 2.2 – GPON лінія

Оглядаючись на вищезазначене логічним вибором резервування основної лінії є одна з технологій широкосмугового радіозв'язку.

Найбільш дешевим та розповсюдженим варіантом є **Wi-Fi (IEEE 802.11)**.

Вибір цього варіанту випливає з наступних факторів:

- в діючий мережі доступу підприємство взагалі не має резервування, тому є сенс розвивати структуру поступово, і почати з найбільш доступного рішення;
- враховуючи відстані до вузлів провайдерів немає сенсу будувати повноцінну радіорелейну лінію з дорого вартісним обладнанням;
- даний варіант підключення передбачає обладнання з мінімальним споживанням енергоживлення і досить легко підключається до резервних акумуляторних батарей;
- точки доступу досить легко розташувати на новій локації, а також не складно розвинути мережу доступу змінивши топологію точка – точка на точка – багатоточка.
- хоча це і резервний варіант, сучасні зразки точок доступу дозволяють працювати на швидкостях до 300 Мбіт/с і більше.

Основними недоліками вищезазначеної радіолінії є необхідність пошуку відкритих інтервалів, що досить просто вирішується при наявності високих споруд. Також радіолінія вразлива до різного виду електромагнітних перешкод, що не є критичним для резервування.

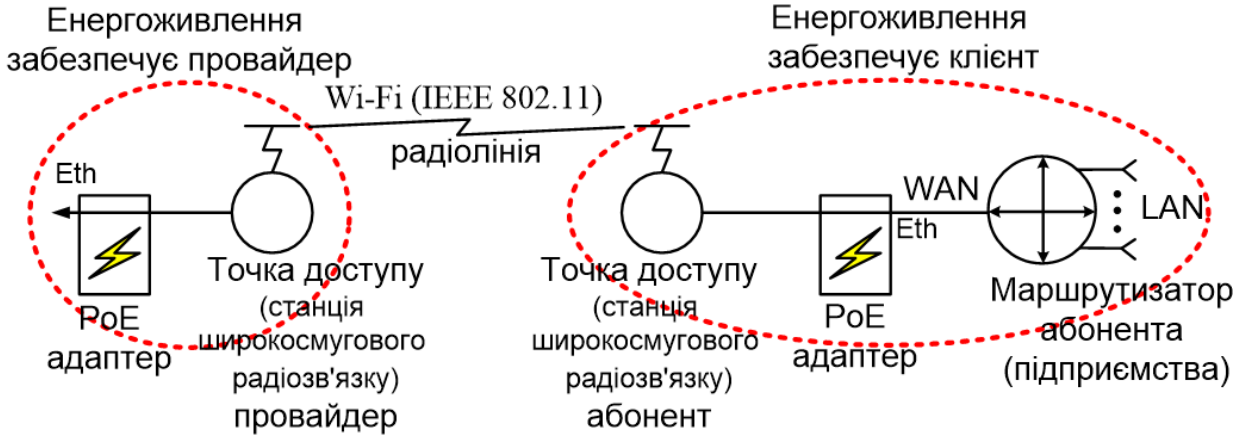


Рисунок 2.3 – Широкосмугова радіолінія

Основна лінія та її резервування розраховані на одного провайдера, з метою зменшення витрат та спрощення процедур підключення і обслуговування, тому логічним кроком для забезпечення резерву “останньої надії” буде підключення що орієнтується на іншого постачальника електронних комунікаційних послуг. Найкращим рішенням в даній ситуації буде взагалі відхід від місцевих провайдерів і забезпечення доступу до мережі інтернет від глобального постачальника за допомогою **систем супутникового зв’язку**.

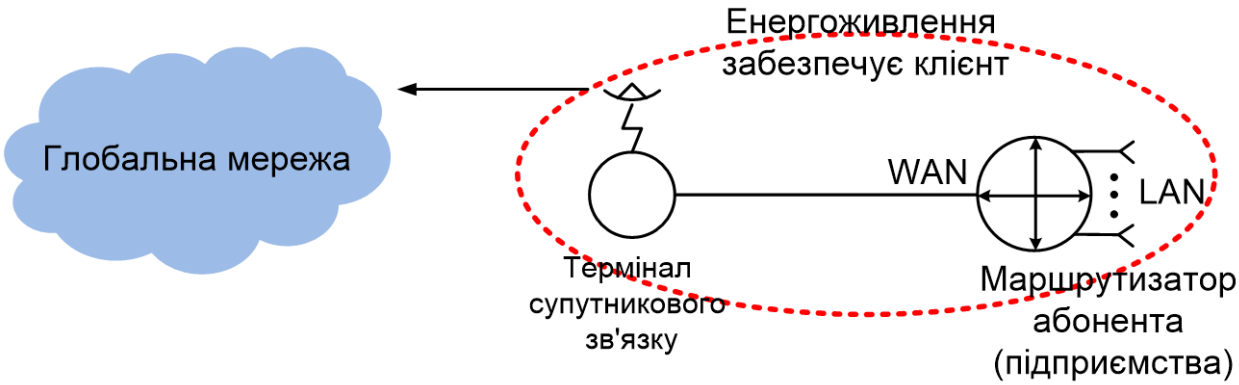


Рисунок 2.4 –Лінія супутникового зв’язку

В широкому доступі на ринку України присутні два види таких послуг: низькорбітальні та геостаціонарні системи [10], [11]. Головна перевага систем, що працюють з геостаціонарними супутниками в тому, що ціна на послуги доступу до мережі Internet та відповідне обладнання постійно падає і є доступною для підприємств. Проте аналізуючи характеристики такого підключення виявляється що у більшості провайдерів швидкість не перевищує 20 – 30 Мбіт/с, і найголовніше затримки (ping) можуть досягати 1000 – 1500 мс, що є неприйнятним у багатьох процесах управління виробництвом.

Серед представлених на ринку постачальників доступу до мережі Internet за допомогою низькоорбітальних систем по ряду факторів поза конкуренцією є Starlink від SpaceX. Можливо через кілька років, завдяки розвитку проектів OneWeb, Amazon Kuiper та інших аналогічних вибір на користь Starlink буде не на стільки очевидним.

2.3 Вибір обладнання

В даній роботі не розробляється локальна мережа підприємства, но для схеми мережі доступу необхідно визначити на чому будується локальна мережа підприємства. Так як штат працівників до 25 осіб, для розгортання локальної мережі буде достатньо маршрутизатора середнього цінового діапазону типу Mikrotik RB4011iGS+RM вартістю до 200$.

WAN порт: Gigabit Ethernet, 1xSFP.

LAN-порт: 10x10/100/1000.

Брандмауер (Firewall), NAT, VPN.

Живлення (PoE/адаптер).

Рисунок 2.5 Маршрутизатор Mikrotik RB4011iGS+RM

Вибір обладнання для побудови оптоволоконної лінії, як правило повністю задається провайдером, який її розгортає і підключає. Що стосується оптичного терміналу на стороні клієнта, це на мою думку пристрої BDCOM або PICOTEL, які рекомендують провайдери. Ціновий діапазон в даному випадку 30 - 50$. В даному випадку принципової різниці у виборі модему від різних виробників немає, так як любі сучасні рішення по своїм характеристикам перекривають вимоги від клієнта (підприємства).

BDCOM P1501DS

Інтерфейси:
1x10/100/1000Base-TX (RJ-45), 1xEPON.
Живлення:
зовнішній DC 12В/0,5А

Рисунок 2.6 Оптичний термінал BDCOM P1501DS

Для побудови широкосмугової радіолінії я підібрав Mikrotik SXT SA5ac з пропускною здатністю до 800 Мбіт/с, та ціною за одиницю в районі 100$. Плюсом цього рішення є той факт, що для розширення можливостей даного обладнання достатньо лише розширити ліцензію з Level 3 до Level 4. При аналізі різних пропозицій в мене виникли сумніви щодо вибору діапазону Wi-Fi. Так як пристрої будуть використовуватись зовні приміщень та в умовах прямої видимості я віддав перевагу більш високих частот і відповідно більшої швидкості. [10]

Mikrotik SXT SA5ac
Стандарт: 802.11ac (Wi-Fi 5)
Потужність передавача: 30 дБм
Діаграма направленості: 90°
Максимальна швидкість з'єднання: 866 Мбіт/с.

Рисунок 2.7 Точка доступу Mikrotik SXT SA5ac

Для забезпечення супутникового зв’язку я як оптимальний варіант обрав STARLINK Satellite Dish Kit v2 з вартістю обладнання 450$ та абонплатою за місяць 75$. Базової швидкості в 80 – 100 Мбіт/с достатньо для крайнього резерву, або для роботи віддаленого підрозділу, як тимчасове рішення.

Рисунок 2.8 Антенний пристрій терміналу STARLINK Satellite Dish Kit v2

2.4 Розробка схеми мережі доступу з резервуванням

На основі моделі мережі доступу та враховуючи обране обладнання розробляю схему мережі доступу підприємства критичної інфраструктури. Основна оптична лінія доступу виглядатиме наступним чином:

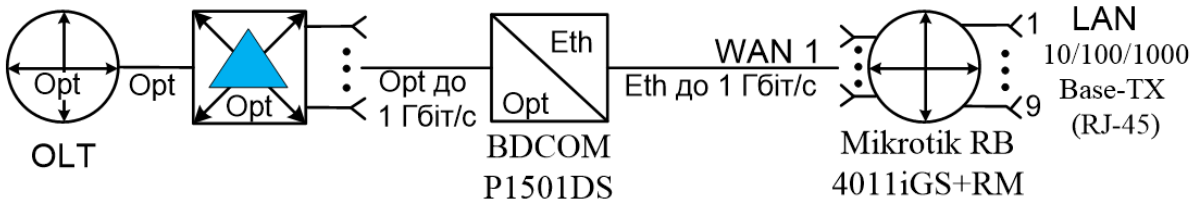


Рисунок 2.9 Оптична лінія мережі доступу

Маршрутизатор Mikrotik RB4011iGS+RM клієнта (підприємства) одним з WAN портів підключений до модема BDCOM P1501DS за допомогою Ethernet-кабелю CAT5e. Від оптичного модему за допомогою оптоволоконного кабелю в GPON мережі провайдера на лінійний термінал. Клієнту (підприємству) необхідно забезпечити живлення маршрутизатора та модема.

Резервування основної лінії за допомогою широкосмугової радіолінії на схемі буде зображено так:

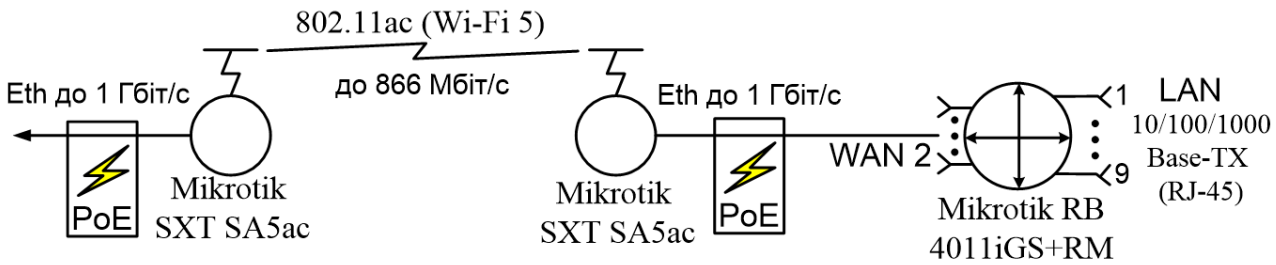


Рисунок 2.10 Широкосмугова радіолінія мережі доступу

Маршрутизатор Mikrotik RB4011iGS+RM клієнта (підприємства) другим WAN портом підключений до інжектору PoE за допомогою Ethernet-кабелю CAT5e, далі за допомогою такого ж кабелю трафік і живлення подається на точку доступу Mikrotik SXT SA5ac яка за допомогою радіолінії 802.11ac (Wi-Fi 5) обмінюється трафіком з такою ж на стороні провайдера.

Схема забезпечення третьої черги резервування за допомогою супутникового зв'язку на базі STARLINK виглядатиме так:

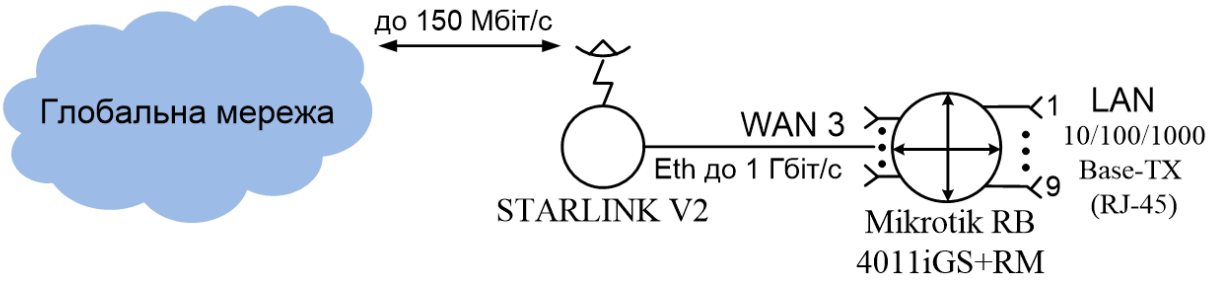


Рисунок 2.11 Лінія супутникового зв'язку мережі доступу

Маршрутизатор Mikrotik RB4011iGS+RM клієнта (підприємства) третім WAN портом підключений до роутера Starlink Ethernet-кабелем CAT5e. Хоча основний спосіб підключення абонентів до терміналу STARLINK це Wi-Fi мережа, в даному випадку надійніше використовувати кабель Ethernet.

На даному етапі, маючи модель мережі доступу, схеми ліній зв'язку, що формують мережу доступу досить просто узагальнити ці дані в повну схему мережі доступу підприємства. Необхідно зазначити якими засобами планується розгортання мережі доступу, з якими параметрами і коротко оцінити її переваги і недоліки.

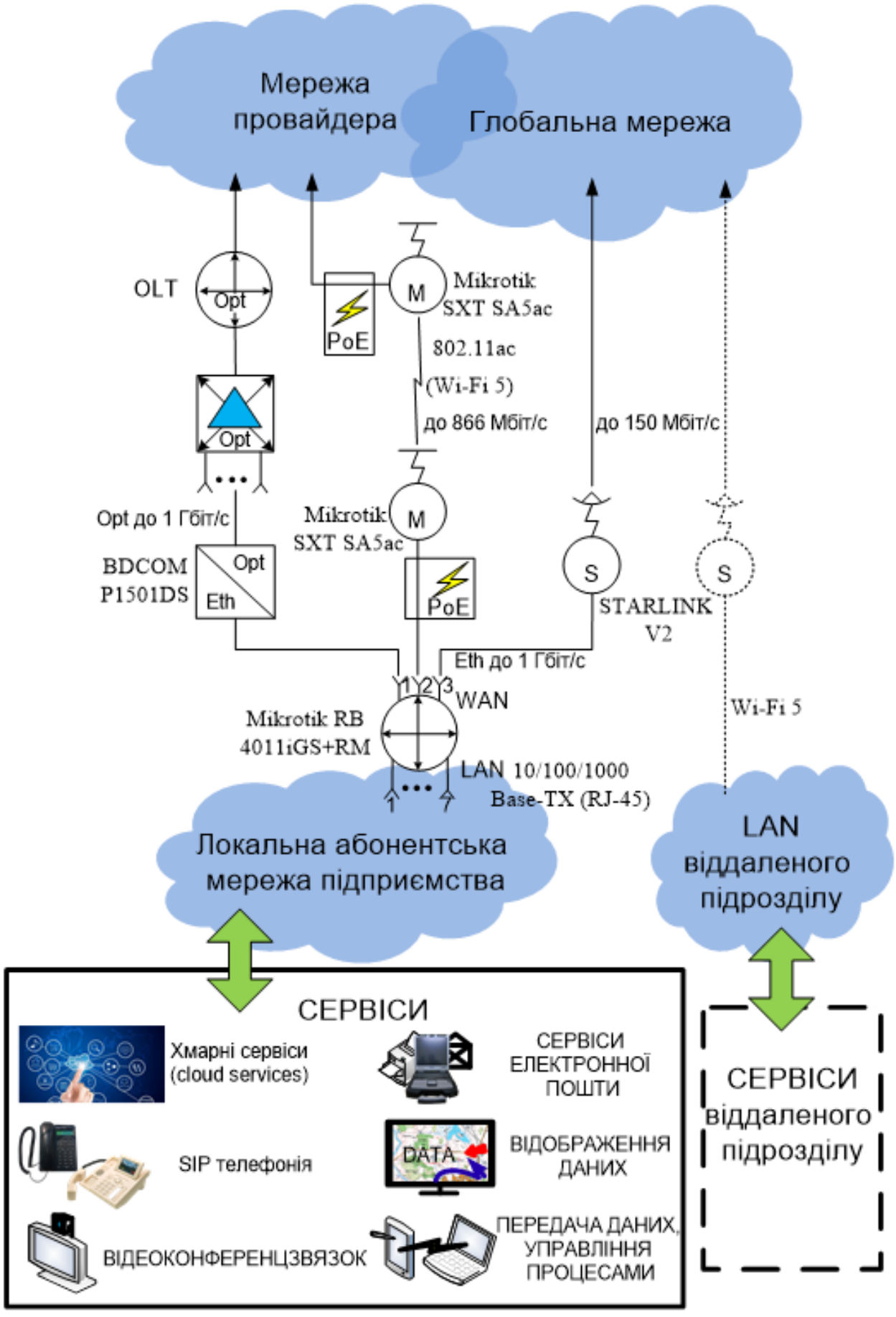


Рисунок 2.12 Схема мережі доступу підприємства

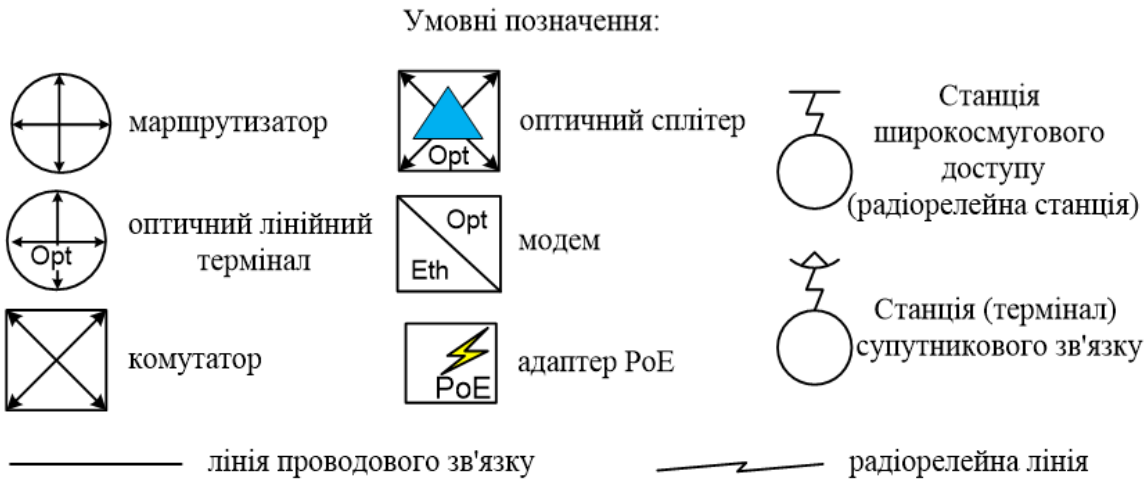


Рисунок 2.13 Умовні позначення

Короткий підсумок переваг та недоліків представленої схеми.

Переваги

a) **Багатоканальне резервування**:
   - Три різні канали доступу (GPON через BDCOM, Wi-Fi через Mikrotik SXT SA5ac та через Starlink) створюють надійний рівень резервування. Це підвищує стійкість мережі, адже у випадку збою одного з каналів дані зможуть передаватися через інші доступні.

b) **Різноманітність технологій доступу**:
   - Використання оптичної лінії (GPON) забезпечує високу швидкість і стабільність з’єднання з низькими затримками.
   - Starlink дає можливість підключення в місцях, де оптичний кабель або радіозв'язок можуть бути недоступними.
   - Радіоканал на основі Wi-Fi 5 (802.11ac) дозволяє забезпечити додатковий канал зв'язку на випадок перебоїв в інших каналах, хоч і з обмеженими швидкостями.

c) **Оптимальне управління живленням**:
   - Підключення до PoE інжектора дозволяє забезпечити живлення деяких пристроїв через Ethernet-кабель, що знижує кількість кабельних підключень та спрощує інфраструктуру.

Недоліки

a) **Залежність від окремих компонентів**:
   - Використання збільшеної кількості пристроїв означає додаткову точку відмови. Збій у будь-якому з цих пристроїв може порушити частину мережі.

b) **Обмеження швидкості Ethernet-кабелю CAT5e**:
   - Кабель CAT5e підтримує швидкість до 1 Гбіт/с. Хоча це зазвичай достатньо, для максимального використання сучасних високошвидкісних з'єднань (особливо в GPON-мережах, які можуть підтримувати понад 1 Гбіт/с) доцільніше було б використовувати CAT6 або вище.

c) **Вплив зовнішніх умов на радіозв'язок**:
   - Канал зв'язку між двома точками Mikrotik SXT SA5ac може зазнавати перешкод через різні умови умови, що потенційно знизить стабільність передачі даних через Wi-Fi 5.

d) **Складність налаштування та управління**:
   - Три канали з різними типами підключення потребують ретельного налаштування маршрутизації та балансування навантаження, що може ускладнити управління мережею, особливо в разі збою одного з каналів.

Ця схема є гнучкою та забезпечує високий рівень надійності, однак потребує ретельного підходу до налаштування мережевих параметрів для забезпечення безперебійної роботи та повного використання швидкостей.

2.5 Вибір обладнання для резервного живлення

В першу чергу необхідно визначитись з споживанням електроенергії обладнанням що забезпечує функціонування мережі доступу на стороні клієнта (підприємства).

З характеристик маршрутизатора Mikrotik RB4011iGS+RM відомо що в його комплект входить блок живлення 24 В на 1,5 А. Відповідно максимальна його споживаєма потужність розрахована на 36 Вт.

Модем BDCOM P1501DS живиться напругою 12 В струмом 0,5 А, що дає нам до 6 Вт.

До складу Mikrotik SXT SA5ac входить інжектор PoE 24 В на 0,8 А, при цьому в характеристиках вказано що максимальне споживання 16 Вт.

Термінал Starlink V2 споживає згідно його опису від 50 до 100 Вт. При цьому треба зауважити, що максимальне споживання обумовлене обігрівом поверхні антени при низьких температурах.

Для забезпечення безперебійної роботи мережі доступу в повному об’ємі необхідно джерело безперебійного живлення потужністю близько 160 Вт.

Аналіз роботи малих підприємств в умовах аварійних відключень живлення показує, що без втручання людини необхідно забезпечити автоматичне ввімкнення резервного джерела і забезпечити підтримку працездатності обладнання до прибуття фахівця який прийме рішення щодо подальших дій. Як правило цей термін не перевищує 24 годин. Резервне живлення може забезпечуватись від резервної лінії, від акумуляторних батарей та від генератора. В нашому випадку, при невеликій потужності оптимальним варіантом автоматичного резервного живлення є акумуляторні батареї. Резервна лінія не допоможе, якщо відключення електроенергії глобальне, а автоматичний запуск генератора не відбувається миттєво, що призведе до вимкнення та перезавантаження обладнання. До того ж налаштування автоматичного запуску генератора потребує дорожчого обладнання та складних змін в систему живлення.

Найоптимальнішою схемою підключення мережі доступу для невеликого підприємства на мою думку буде робота від акумуляторних батарей до 24 годин з ручним переходом на роботу від генератора. Для забезпечення такої роботи необхідне наступне обладнання:

- акумуляторні батареї ємністю 160 х 24 = 3840 Вт;
- інвертор DC 12 (24) В / АС 220 В потужністю більше 160 Вт. На ринку оптимальна ціна на даний час за 1 – 2 кВт інвертори;
- зарядний пристрій для АКБ DC 12 (24) від 10 (5) А;
- генератор потужністю від 1 кВт (менші не раціонально).

Все це обладнання крім генератора можна замінити одним пристроєм на кшталт EcoFlow, або Bluetti. Основний мінус одного пристрою це ціна. Пристрій ємністю від 3,8 кВт/год коштує від 2500 $. Якщо забезпечити комплект інвертор, зарядний пристрій, АКБ то приблизно буде так:

- інвертор 1 – 2 кВт 50 – 100$;
- зарядний пристрій DC 12 В 10А – від 25$;
- акумулятор LiFePO4 ємністю від 3,8 кВт/год найдорожчий елемент системи, ціна на даний час стартує від 750 $.

Загалом вибір на користь окремих пристроїв дешевше в два рази, як мінімум.

Щодо вибору генератора, то при невеликій потужності, 1 – 2 кВт, найбільший вибір і найдешевше обладнання в сегменті бензинових генераторів. Ціна стартує від 300 $.

На мою думку вибір резервного живлення в основному це питання ціни. На користь системи з окремими елементами також виступає можливість подальшої модернізації і нарощування можливостей.

Схема підключення резервного живлення у двох варіантах виглядатиме наступним чином:

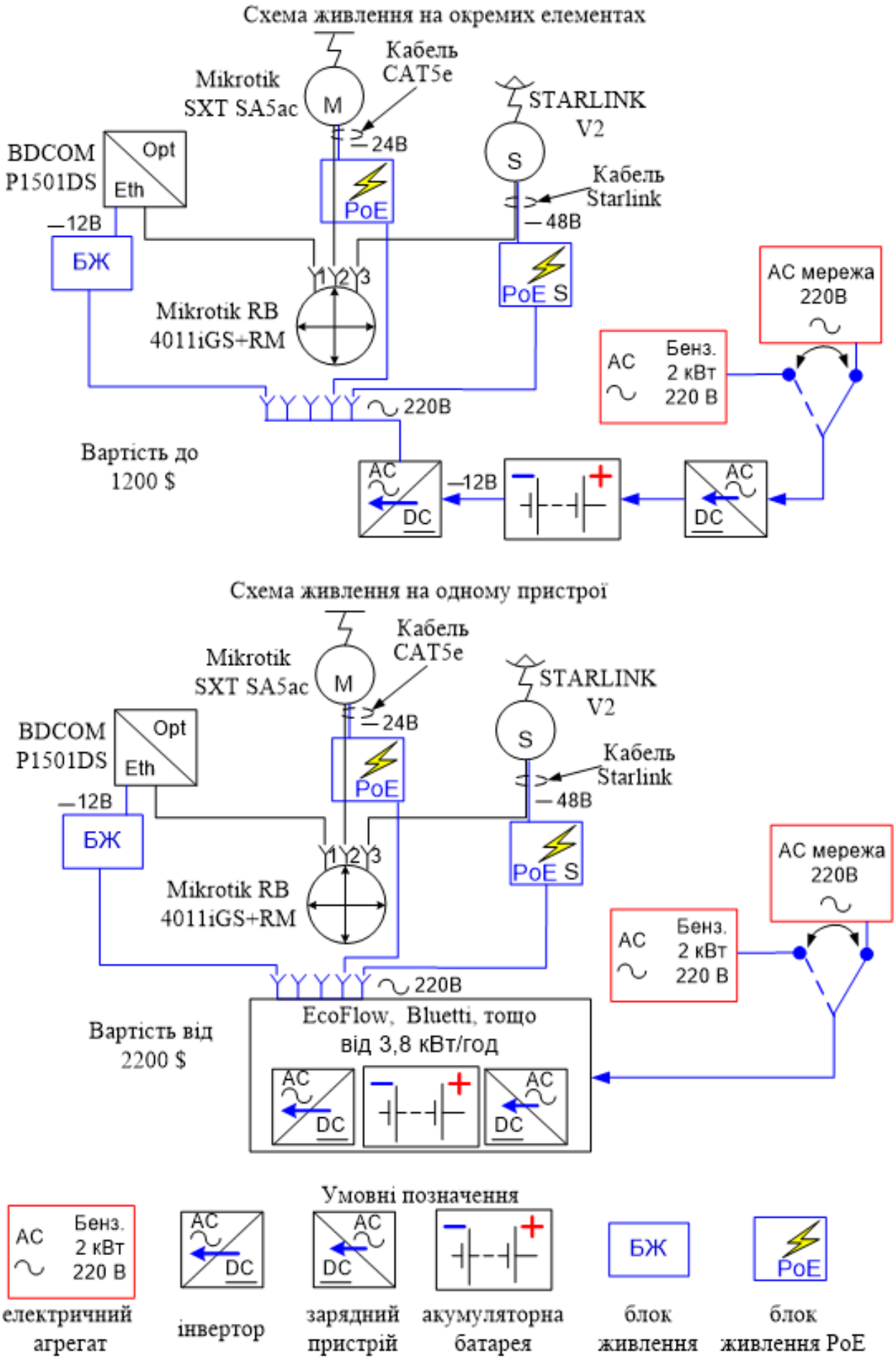


Рисунок 2.14 Схеми резервного живлення

2.6 Опис роботи мережі доступу з резервуванням

В даному розділі буде розроблено і описано алгоритм роботи мережі доступу підприємства критичної інфраструктури в різних ситуаціях, але перед цим необхідно визначитись, що усе обладнання постійно ввімкнене і забезпечує оперативне резервування, а також не потребує негайного втручання оператора (працівника) під час аварійної ситуації.

Штатна робота

Основна оптоволоконна лінія забезпечує доступ для всіх абонентів через WAN 1. Абоненти в повному обсязі працюють через. Радіолінія ввімкнена, підключена до маршрутизатора через WAN 2 але трафік користувачів через неї не здійснюється. Термінал супутникового зв’язку налаштований, роутер Starlink підключений на WAN 3, користувацький трафік через неї також не здійснюється. Живлення всіх пристроїв мережі доступу абонентської сторони здійснюється від інвертора, який працює від акумулятора, той в свою чергу знаходиться в буферному режимі від зарядного пристрою. Зарядний пристрій працює від штатної мережі 220В. [12]

Аварія на оптичній лінії зв’язку

Під час аварії на основній лінії із за виходу з ладу обладнання оптичної лінії трафік перемикається на радіолінію, яка забезпечує достатню швидкість для всіх абонентів. Проте можливі деякі незначні обмеження тому трафік з розповсюджується через VLAN “РЕЗЕРВНИЙ” де кількість абонентів, або характеристики їх доступу можна обмежити. Живлення абонента працює штатно.

Комплексна аварія у провайдера

При припиненні роботи основного провайдера за будь яких причин передача трафіку перемикається на WAN 3 і доступ користувачів здійснюється через VLAN “ОБМЕЖЕНИЙ” до якого доступ будуть мати критичні користувачі та сервіси, а решта має бути обмежена. Живлення абонента працює штатно.

Аварійне вимкнення живлення

При аварійному вимкненні живлення акумуляторна батарея буде на протязі до 24 годин підтримувати живлення обладнання мережі доступу, за цей час черговий працівник повинен запустити електричний генератор, потужності якого достатньо щоб підтримувати живлення апаратури і зарядити резервний акумулятор. Єдиний нюанс, працівник повинен вручну відключити обладнання живлення від змінної мережі 220В і підключити до генератору, при цьому в запропонованій схемі перерв в роботі обладнання електронних комунікацій не буде.

Комплексна аварія на стороні клієнта

В залежності від ситуації обладнання радіолінії на стороні клієнта може бути релоковане в певних межах, термінал Starlink взагалі можна розгорнути майже всюди, обладнання живлення також дозволяє працювати одразу після переміщення та/або при відсутності стаціонарної мережі живлення.

Нижче приведений короткий алгоритм дій, що забезпечують безперебійну роботу мережі доступу:

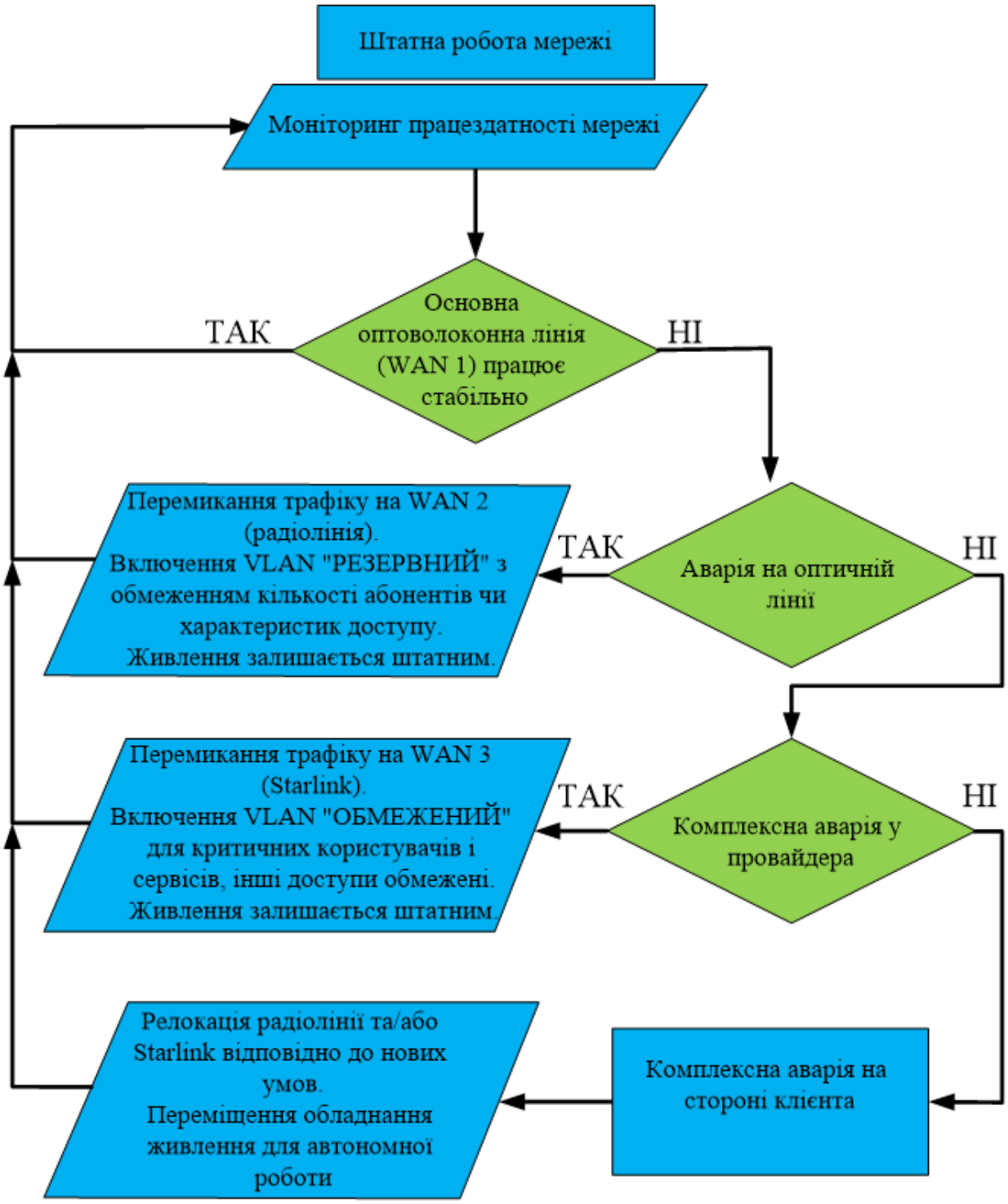


Рисунок 2.15 Алгоритм дій по забезпеченню роботи мережі доступу

2.7 Висновки по другому розділу

Приведений в другому розділі порядок розробки схеми мережі доступу дозволяє наглядно оцінити велику кількість складових і обрати оптимальний варіант. Обрана конфігурація обладнання і його взаємодія має ряд переваг та недоліків які висвітлені вище. Головним завданням яке необхідно було виконати в даному розділі при розробці схеми мережі доступу це порівняти негативні і позитивні сторони конкретного вибору саме для невеликого підприємства критичної інфраструктури, що і було виконано. Запропонована схема дозволяє забезпечити головну мету завдання, а саме забезпечення стійкості мережі доступу в сучасних умовах. Також варто зазначити, що запропонований набір обладнання та порядок його роботи легко піддається зміні, масштабуванню, вдосконаленню та трансформації, так як вся схема побудована на доступних та розповсюджених комплектуючих [10].

Треба зазначити, що застосування розробленої схеми, на мою думку, не потребує утримання в обмеженому штаті підприємства окремих фахівців, є лише необхідність разових залучень фахівців основного провайдера та короткої підготовки (інструктажу) одного/двох працівників, які згідно додаткових обов’язків будуть виконувати певний алгоритм в аварійних ситуаціях[10].

3 РОЗРАХУНОК НАДІЙНОСТІ

3.1 Порядок визначення

В світовій практиці існує низка параметрів визначення надійності ліній зв'язку, що в свою чергу складають електронні комунікаційні мережі. Основні джерела визначення такої надійності це [1]:

- ISO/IEC 27001 — міжнародний стандарт в галузі IT, назва якого «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги». («Information technology — Security techniques — Information security management systems — Requirements»). ISO / IEC 27001 встановлює вимоги до створення, впровадження, підтримки та постійного поліпшення системи менеджменту інформаційної безпеки в контексті організації. Він також включає в себе вимоги до оцінки і обробки ризиків інформаційної безпеки з урахуванням потреб організації.

- Рекомендація ITU-T Y.1564 стандартизує методику проведення вимірювань, необхідні перевірки якості сервісів, переданих через Ethernet. В результаті вимірювань, виконаних за цією методикою, для кожного сервісу можна визначити: гарантовану швидкість передачі даних (CIR), допустиме перевищення гарантованої швидкості (EIR), затримку пакетів (FTD), джиттер пакетів (FDV), коефіцієнт втрати пакетів (FLR) та низку інших важливих параметрів.

Основні параметри визначення надійності:

а. Коефіцієнт готовності (Availability)

- Відображає відсоток часу, протягом якого лінія зв'язку працює без збоїв.

A=MTBF/(MTBF+MTTR)x100%

MTBF (Mean Time Between Failures) — середній час між відмовами.

MTTR (Mean Time to Repair) — середній час відновлення.

Приклад: Якщо MTBF = 10000 годин, а MTTR = 1 година:

A = 10000/(10000+1)x100% = 99.99%

b. Імовірність безвідмовної роботи (Reliability)

- Ймовірність того, що лінія зв’язку працюватиме безвідмовно протягом певного часу t:

$R(t)=e^{-\lambda t}$

λ — інтенсивність відмов (λ = 1/MTBF).

Приклад: Якщо MTBF = 10 000 годин і t=100 годин:

λ = 1/10000 = 0,00001

$R(100) = e^{-0.0001x100} = 0,99$

c. Час між відмовами (Mean Time Between Failures, MTBF)

- Середній час між двома послідовними збоями в системі.
- Високий MTBF вказує на стабільну і надійну роботу.

d. Пропускна здатність (Bandwidth Stability)

- Стабільність швидкості передачі даних без суттєвих падінь пропускної здатності. Це важливо для уникнення перевантажень.

e. Затримка (Latency)

- Час, необхідний для передачі даних між кінцевими точками. Оптимальною вважається затримка до 50 мс для більшості додатків.

f. Ймовірність втрати пакетів (Packet Loss)

- Вимірює, який відсоток даних втрачається під час передачі. Значення повинно бути не більше 1% для високонадійних мереж.

g. Резервування (Redundancy)

- Наявність резервних каналів зв’язку для забезпечення безперебійної роботи у разі відмови основної лінії.

для розрахунку комбінованої доступності для резервованих ліній використовується наступна формула:

$A_{заг}=1-(1-A_1)(1-A_2)\ldots(1-A_n)$

Де: A_1, A_2,…A_n — доступність основного і резервних каналів.

Врахування типу резервування

- **Active-Active** (активно-активне): обидва канали працюють одночасно.
- **Active-Passive** (активно-пасивне): резервний канал активується лише у разі відмови основного.

Треба зазначити, що резервні канали будуть мати різний MTTR в залежності від того в якому режимі вони працюють.

Визначення будь яких вихідних даних для обчислення параметрів надійності можна зробити двома основними способами, або їх комбінацією [1]:

a. Можна розрахувати MTBF (середній час між відмовами) та MTTR (середній час на відновлення) для лінії зв'язку, маючи дані по обладнанню, з якого вона складається. Наприклад:

- Для MTBF можна взяти гарантійне напрацювання модему, або дані про безвідмовну роботу оптичної лінії. Якщо модем має гарантійне напрацювання 50000 годин, то це буде загальним часом роботи. Якщо оптична лінія може забезпечити безвідмовну роботу протягом 10 років (експлуатаційний термін), то це також буде загальний час роботи.

Можна оцінити кількість відмов, використовуючи оцінки від виробника обладнання, або ж орієнтуючись на дані, зібрані з подібних систем інших виробників.

- Для розрахунку MTTR необхідні дані про час, витрачений на ремонт, або відновлення обладнання після відмов. Це може бути середній час відновлення, базуючись на наявній документації. Наприклад, якщо фахівець з ремонту надає дані що для модему середній час ремонту становить 2 години, а оптична лінія відновлюється за 5 годин після відмови, можна взяти ці значення для MTTR.

Отже, маючи дані по окремому обладнанню, з якого складається лінія зв'язку, можна обчислити MTBF і MTTR для всієї системи.

b. Другий спосіб отримання даних це статистичний. Необхідно проаналізувати роботу лінії зв’язку за певний проміжок часу і визначити таким чином необхідні дані. Інформація про відмови є і у провайдерів і у клієнтів.

Статистичний спосіб отримання даних вважається набагато точнішим і простішим у використанні. Основний недолік такого способу це необхідність мати інформацію про відмови за значний проміжок часу, що не завжди є можливим. Я в своїй роботі розглядаю технології доступу, які широко використовуються вже більше двох років, тому проблем з напрацюванням статистики немає. Більш того, завжди можна зробити комбіновану перевірку надійності, використовуючи обидва підходи.

І найголовніше, в даній роботі я розглядаю не абсолютні значення надійності, а те як запропонована мною схема збільшить надійність роботи мережі доступу.

3.2 Розрахунок

Для розрахунку кількості збоїв і порушень в роботі діючий мережі доступу підприємства я скористався двома джерелами даних. Перше джерело це безпосередньо від клієнта за останній рік дані по дням коли відбувались відмови і скільки годин мережа доступу не працювала, в тому числі і по лог-файлам маршрутизатору. Другий тип даних це графіки відключень електроенергії від Полтаваобленерго [13]. Статистика представлена на діаграмах:

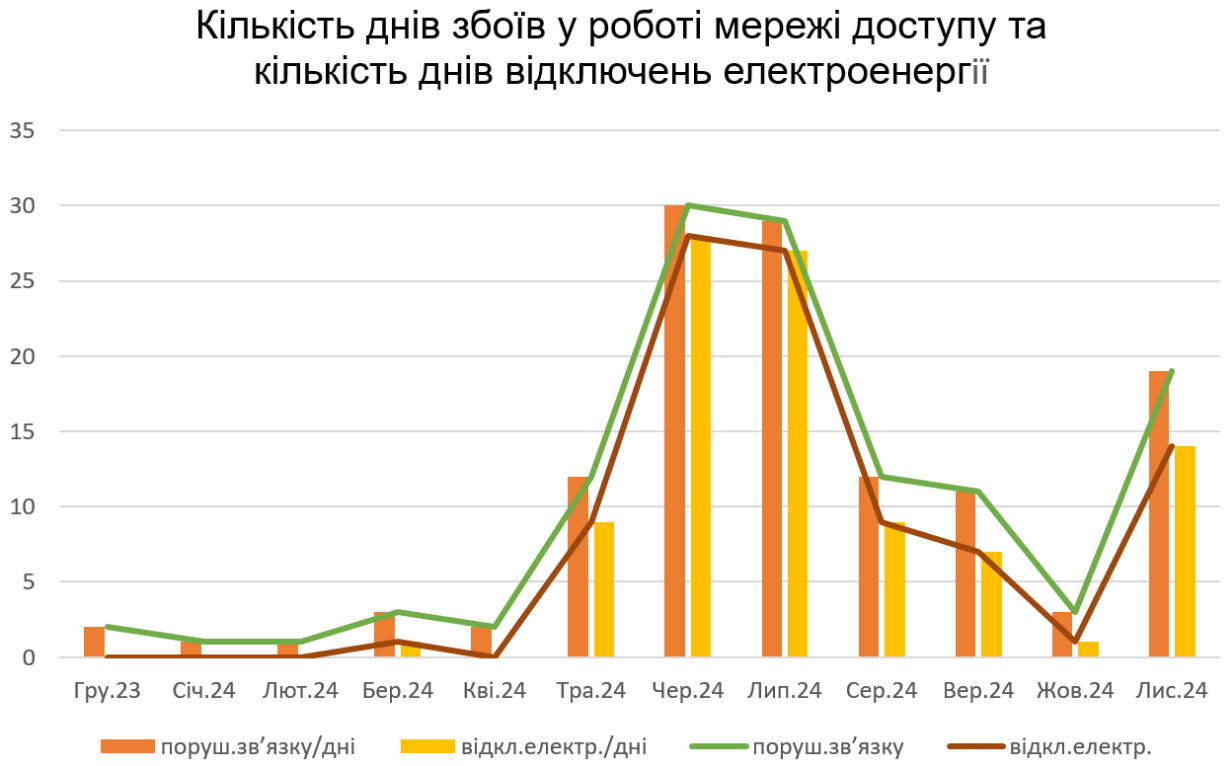


Рисунок 3.1 Порівняння днів збоїв роботи мережі доступу і відключень електроенергії

За рік 125 днів збоїв роботи мережі доступу (загальна кількість збоїв обчислена приблизно як 340, з яких не по причині відсутності живлення 13) з них 96 днів, з високою вірогідністю із за відсутності електроживлення. Так як на добу зв'язок міг бути відсутнім і пару хвилин, і всю добу, ця інформація не підходить для розрахунку надійності мережі доступу, але дає загальне уявлення про загрози відмов в сучасних реаліях.

Для розрахунку необхідно врахувати саме години непрацездатності мережі доступу і відштовхуватись від цієї інформації.

Згідно статистичних даних за рік мережа доступу була непрацездатною 738 годин, з них 655 годин, з високою вірогідністю із за відсутності електроживлення.

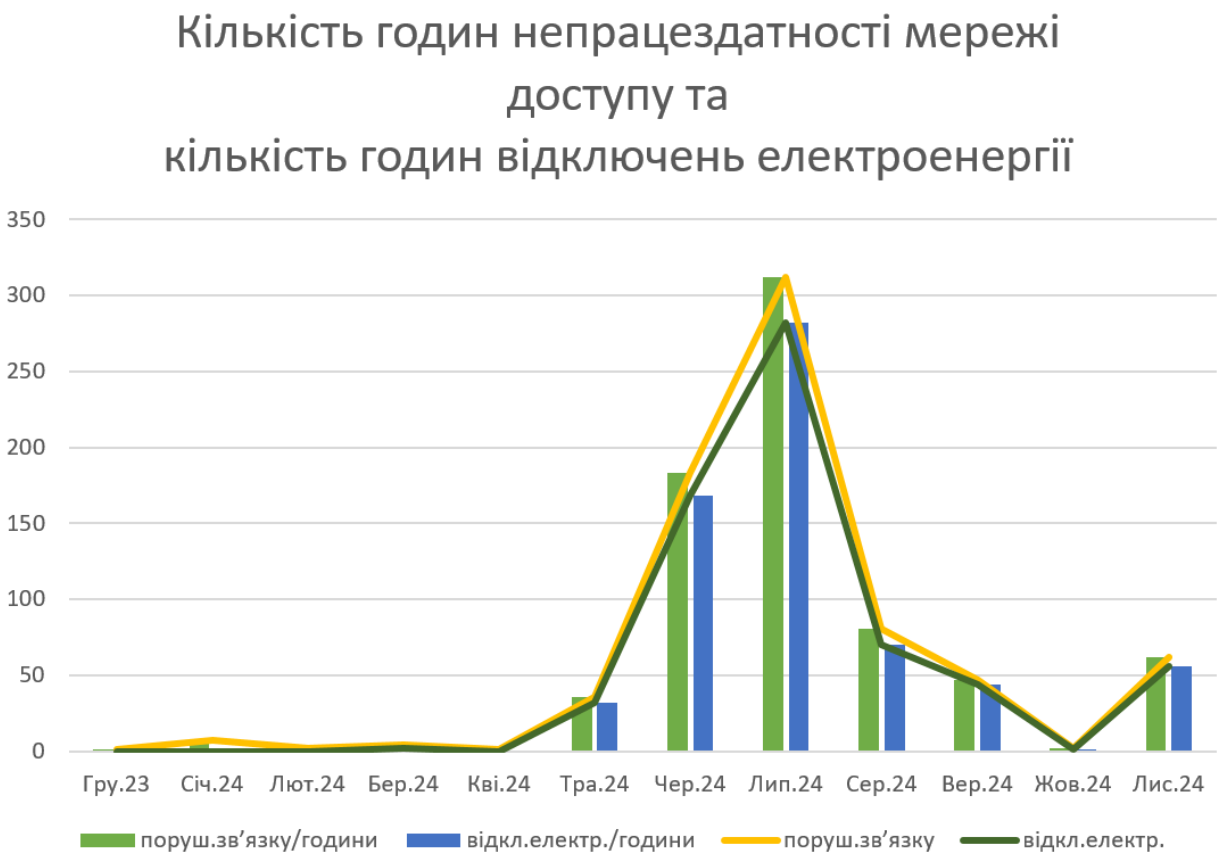


Рисунок 3.2 Порівняння годин збоїв роботи мережі доступу і відключень електроенергії

За рік 738 годин непрацездатності мережі доступу з них 655 годин, з високою вірогідністю із за відсутності електроживлення.

Маючи вищезазначені дані обчислюємо надійність діючої мережі доступу підприємства за формулою визначення коефіцієнта готовності: A=MTBF/(MTBF+MTTR)x100%. Вирахуємо за рік на який маємо дані.

MTTR = 738 годин за рік (статистика).

MTBF (годин) = (365 днів х 24 години – 738 годин непрацездатності)/340 = 8022 години/340 = 23,59.

A = 23,59/(23,59+738) х100% ≈ 3,097%

Таким чином коефіцієнт готовності (Availability) діючої мережі доступу дуже низький із за частих відключень електроенергії.

Також визначимо ймовірність того, що лінія зв'язку працюватиме безвідмовно протягом певного часу (100 годин): $R(t)=e^{-\lambda t}$

λ **(**інтенсивність відмов) = 1/MTBF = 1/23,59 = 0,04239084

t=100 годин. e = 2,71828.

$R(100 \text{ год.}) = 2{,}71828^{-0{,}04239084 \times 100} = 1{,}44\%$, результат наближений до нуля із за великої кількості відмов.

В результаті з урахуванням відключень електроенергії ми маємо коефіцієнт готовності 3 % та ймовірність безвідмовної роботи протягом 100 годин наближений до нуля:

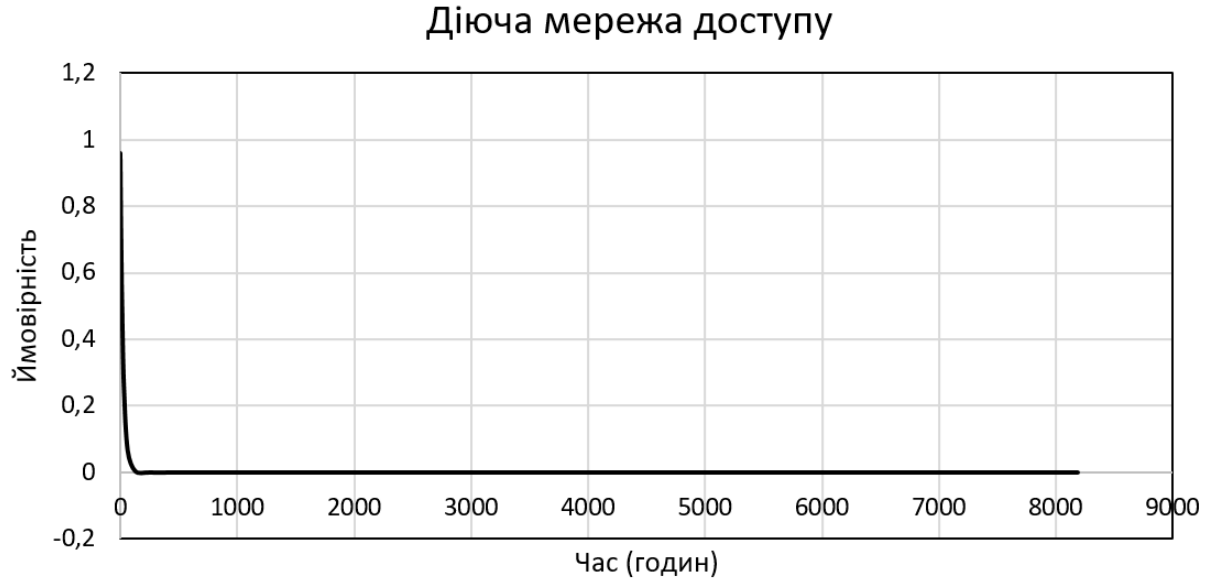


Рисунок 3.3 Ймовірність безвідмовної роботи діючої мережі

Якщо не враховувати енергоживлення, то відповідні дані вже можна врахувати при порівнянні: MTTR = 738 – 655 = 83 години за рік. MTBF

(годин) = (365 днів х 24 години – 83 години непрацездатності)/13 = 667,46 годин, при цьому А = 667,46 /(667,46 +83) х100% ≈ 88,93%

R(100 год.) = $2{,}71828^{-0{,}0014982 \text{x} 100}$ = 86,086 % що теж доволі мала величина для 100 годин роботи, але, що важливо, підходить для подальшого аналізу.

Відстежити залежність імовірності безвідмовної роботи від часу можна на графіку:

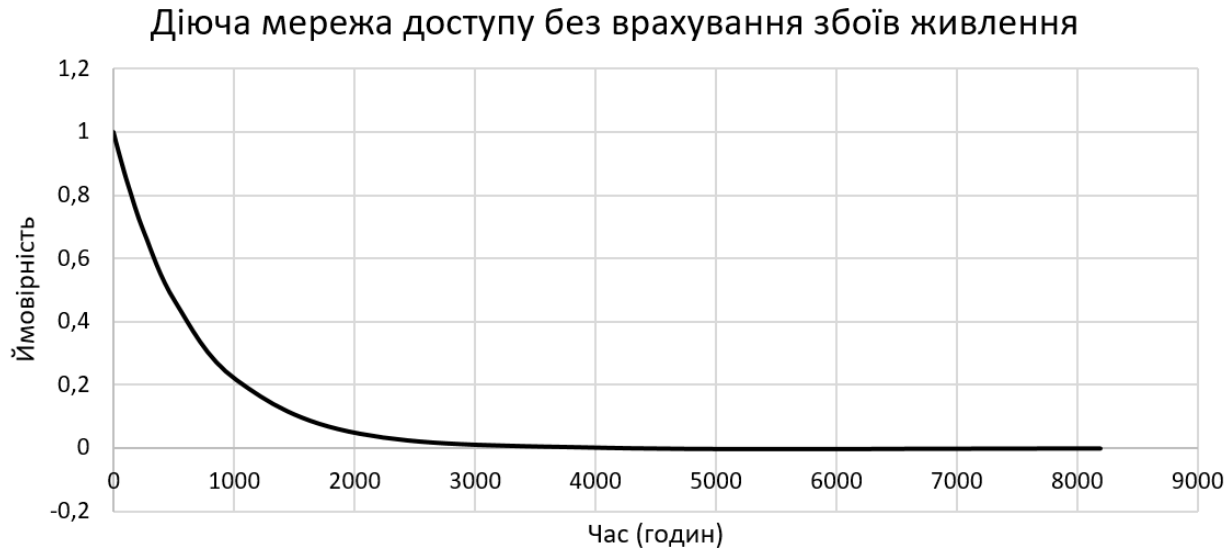


Рисунок 3.4 Ймовірність безвідмовної роботи діючої мережі при резервуванні живлення

При плануванні резервованої мережі доступу ми будемо використовувати три типи ліній зв’язку, і вираховувати їх загальний показник.

Для спрощення обчислень, знаючи що оптична лінія GPON більш надійна ніж лінія з активними елементами я залишив її показники як у діючій лінії мережі доступу. Враховуючи те що ми забезпечили енергонезалежність розробленої схеми мережі доступу A_{pon} = 88,93%, а R_{pon} (100 годин) = 86,1 %.

При розрахунку вищезазначених параметрів для роботи терміналу Starlink я використав напрацювання по місцю роботи, в тому числі API телеметрію на інформаційній панелі Starlink. Так як супутниковий термінал використовувався не в цілодобовому режимі, а також з частим (2-3 рази на добу) рзгортанням/підключенням, то статистика буде точно не завищена в кращу сторону.

Приблизні статистичні дані:

За 91 календарну добу 261 година в роботі. Час на встановлення зв'язку загалом склав 8 годин. З робочих годин після встановлення зв'язку і початку надання сервісу доступу до глобальної мережі Інтернет з приблизно 253 годин час перерв в роботі за різних причин (оновленні програмного забезпечення, збої з падінням швидкості, тощо) склав 14 годин. Статистика представлена на діаграмі:

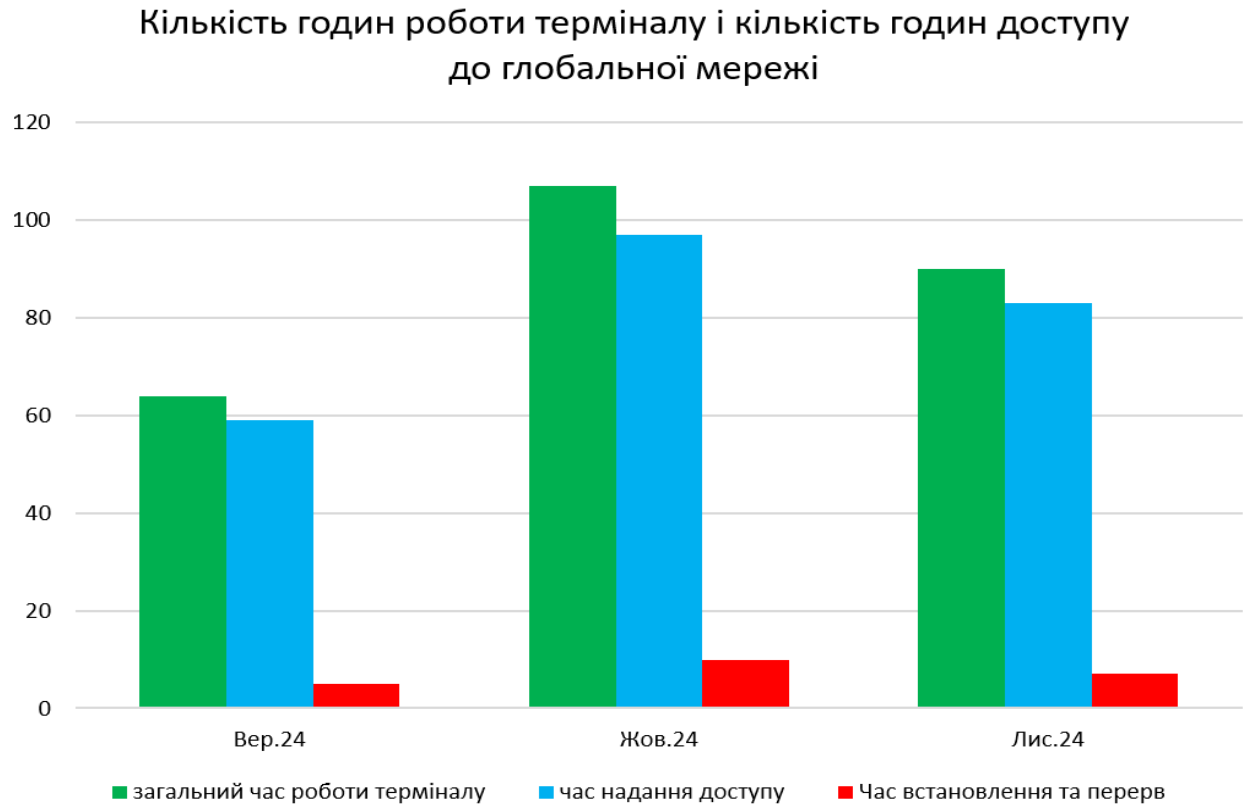


Рисунок 3.5 Оцінка роботи терміналу Starlink

При цьому збоїв в роботі було 5 за весь період. Відповідно для лінії низькоорбітального супутникового зв'язку при частому процесі

розгортання A_{str} = 47,8 / (47,8 + 22) x 100% = 68,48%,

R_{str} (100 год) = $2{,}71828^{-0{,}00418410042x100}$ = 65,8%.

Треба зазначити що прямого впливу відключень живлення на статистику немає, так як термінали Starlink розгортались по потребі і якщо стаціонарне живлення було відсутнє, то використовувалось автономне. Також застосування автономного живлення терміналів Starlink під час відключень електроенергії незначно (5 - 10%) збільшує час на розгортання.

Для мікрохвильового зв'язку доступну для себе статистику я знайшов для двох ліній 480 та 1700 метрів, за 8 і 10 місяців відповідно. На обох лініях використовуються Mikrotik SXT 2 (RBSXTG-2HnD), і хоча ми використовуємо набагато більш нову модель, загальний розрахунок надійності можна буде використати для уявлення порядку значень.

Для радіолінії 480 м з 01.03.2020 року по 31.10.2020 року відбулось 17 збоїв роботи обладнання з загальним часом відновлення 38 годин.

Діаграма:

Рисунок 3.6 Оцінка роботи радіолінії №1

Для радіолінії 1700 м з 01.12.2020 року по 31.09.2021 року відбулось 28 збоїв роботи обладнання з загальним часом відновлення 65 годин. Діаграма:

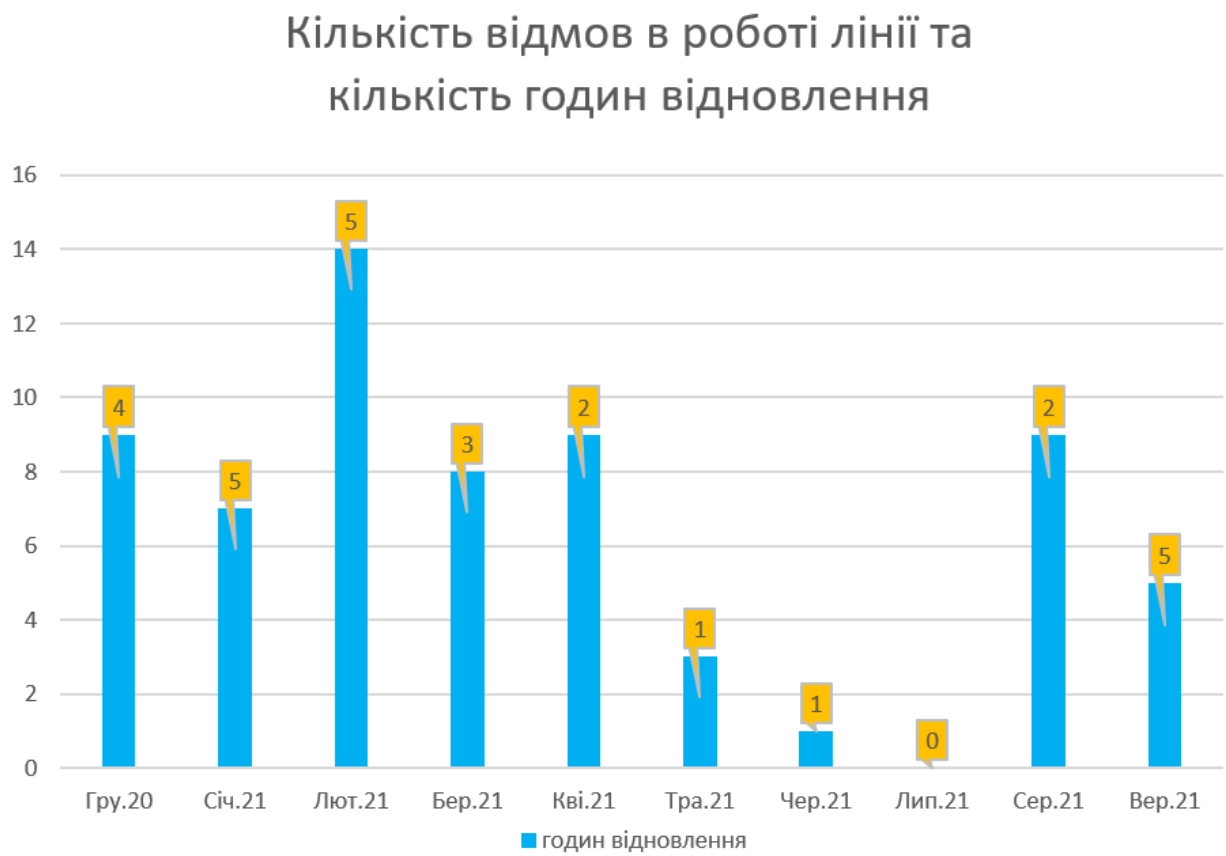


Рисунок 3.7 Оцінка роботи радіолінії №2

Відповідно вищезазначеним даним розрахуємо загальні характеристики для обох радіоліній щоб отримати опосередковане значення:

Для першої радіолінії загальний час спостережень 5880 годин, відновлення 38 годин, час працездатності відповідно 5842 години.

Для другої радіолінії загальний час спостережень 7296 годин, відновлення 65 годин, час працездатності відповідно 7231 година.

Загалом по двом радіолініям разом час відновлення 103 години при працездатності 13073 години і кількість збоїв 45.

A_{rl} = 290,51 / (290,51 + 65) x 100% = 81,72%,

R_{rl} (100 год.) = $2{,}71828^{-0{,}0034422223x100}$ = 70,88%.

Маючи тепер дані коефіцієнтів готовності та ймовірність безвідмовної роботи по трьом лініям мережі доступу з резервуванням можемо розрахувати тепер загальні її параметри надійності.

Для нашого випадку коефіцієнт готовності розраховується по формулі: $A_{мер}$= 1−(1− A_{pon})(1− A_{str})(1− A_{rl}) = 99,3621625%

Ймовірність безвідмовної роботи по трьом лініям (параметр ймовірності того що хоч одна лінія буде працювати) на протязі 100 годин:

$R_{мер}$= 1−(1− R_{pon})(1− R_{str})(1− R_{rl}) = 1−(1− 0,861)(1− 0,658)(1− 0,7088)

$R_{мер}$= 98,62 % (для 100 годин).

Ймовірність безвідмовної роботи по трьом лініям на протязі місяця (30 діб) буде складати 90,2163059%. При цьому залежність від часу представлена на графіку:

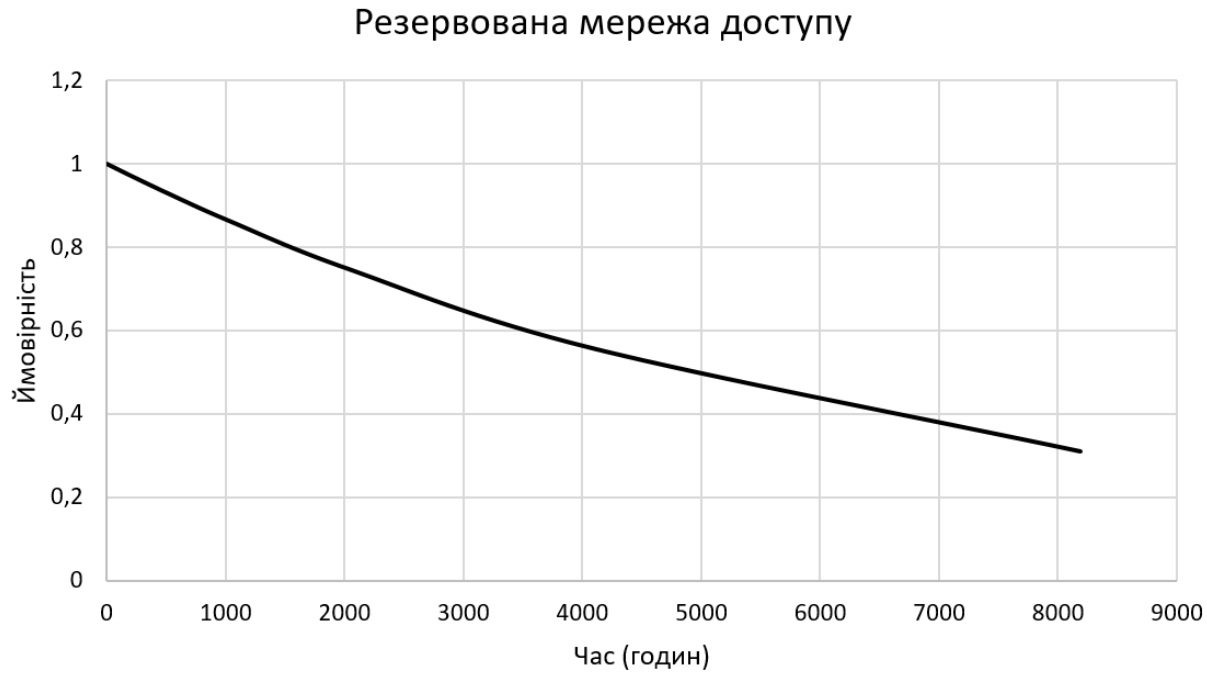


Рисунок 3.8 Ймовірність безвідмовної роботи резервованої мережі доступу

3.3 Порівняння та підсумок по третьому розділу

Відповідно зібраних даних та проведених розрахунків оцінюємо надійність роботи мережі доступу діючої, мережі доступу діючої з безперебійними джерелами живлення, та розроблену резервовану мережу доступу.

Коефіцієнт готовності для діючої мережі - A=3,097%

Коефіцієнт готовності для діючої мережі з резервним живленням на стороні провайдера і клієнта - A=88,93%

Коефіцієнт готовності для розробленої резервованої мережі доступу - A=99,36%.

A=3,097% проти A=99,36%

Ймовірність безвідмовної роботи на протязі 100 годин для діючої мережі - R = 1,44%

Ймовірність безвідмовної роботи на протязі 100 годин для діючої мережі з резервованим живленням - R = 86,086 %

Ймовірність безвідмовної роботи на протязі 100 годин для розробленої резервованої мережі доступу - R = 90,22%.

$R_{100\ год}$ = 1,44% проти $R_{100\ год}$ = 90,22%

Краще ймовірність безвідмовної роботи показано на графіку залежності від часу всіх трьох варіантів (Ряд1 – діюча мережа, Ряд2 – діюча мережа без урахування перебоїв живлення, Ряд3 – резервована мережа):

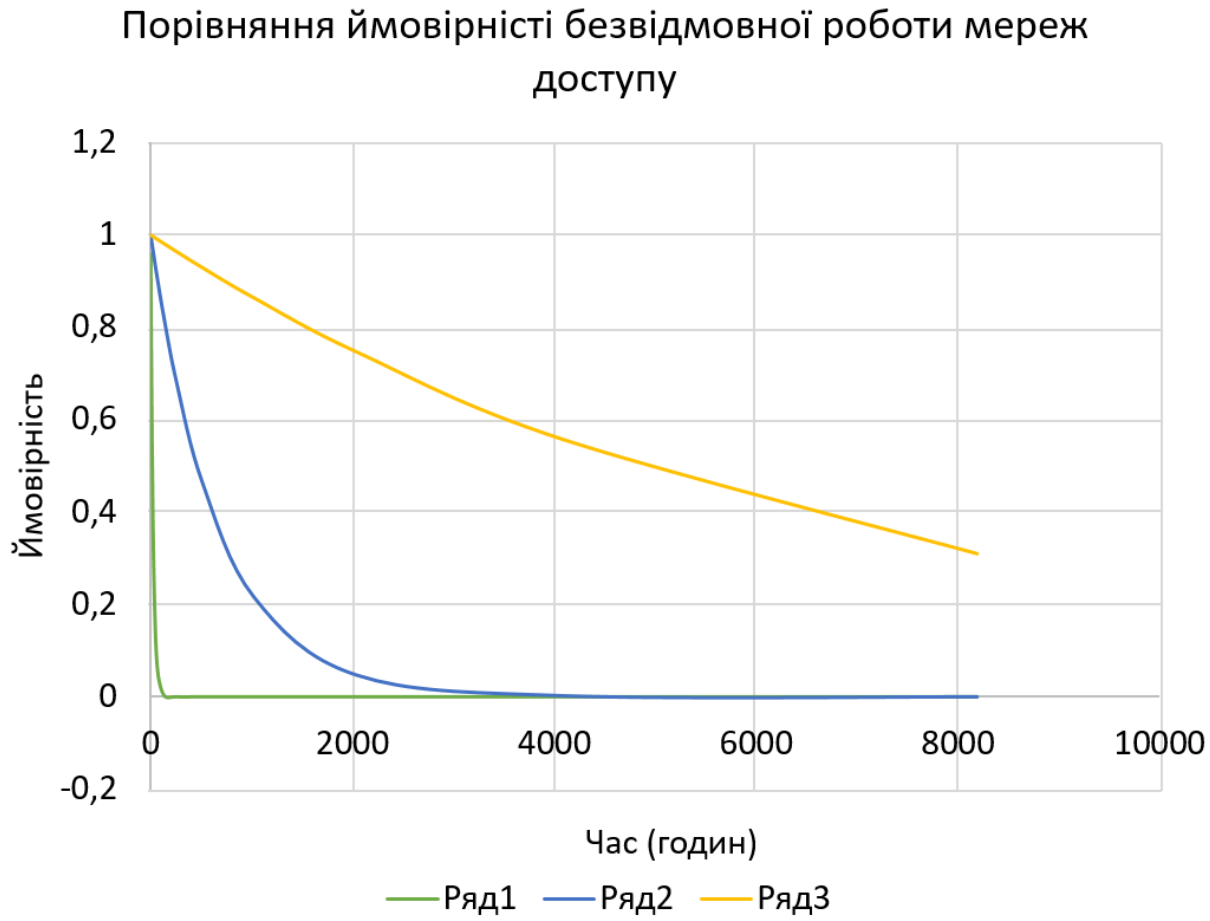


Рисунок 3.9 Порівняння ймовірність безвідмовної роботи

Статистичні дані і розрахунки показали, що в сучасних реаліях надійність мереж доступу критично низька із-за перебоїв живлення. Встановлення системи безперебійного живлення на стороні клієнта та на стороні провайдера, а також резервована мережа доступу дозволяє досягти високих показників надійності.

ВИСНОВКИ

Наслідки російської агресії на інфраструктуру електронних комунікацій в Україні приводять до критичного рівня надійності мереж, перебоїв у роботі підприємств, установ та організацій. Забезпечення стабільності зв'язку є однією із пріоритетних задач як для Держави так і для користувачів електронних комунікацій.

В дипломній роботі проаналізовано деструктивний вплив російської агресії на роботу мереж доступу та запропоновано шляхи нівелювання цього впливу. З метою модернізації проведено аналіз сучасних способів та засобів побудови ліній зв’язку та їх безперебійного живлення, обґрунтовано конкретний вибір. Запропонований шлях модернізації та резервування ліній зв’язку мережі доступу та забезпечення безперебійного живлення дозволяє збільшити коефіцієнт готовності з 3 до 99 відсотків, а ймовірність безвідмовної роботи на протязі певного часу зростає на порядки. Також запропонований варіант мережі доступу надає для підприємства критичної інфраструктури ряд додаткових можливостей, наприклад, швидке розгортання мережі доступу в інтересах віддаленого підрозділу, або швидке забезпечення доступу при релокації. Такий підхід до організації роботи підприємства не вимагає збільшення штатної кількості працівників і потребує мінімальних затрат на підготовку працівників.

Економічне обґрунтування реалізації запропонованої моделі не розглядалося в межах даної роботи, проте елементи конкретних рішень вже більше двох років широко використовуються як в цивільній, так і в військовій сфері і показують що відношення фінансових затрат до збільшення ефективності робочого процесу досить вигідне. Наявність надійної резервованої мережі доступу дає підприємству конкурентні

переваги, зменшує кіберзагрози, стабілізує робочий процес та економить кошти на усуненні наслідків кризових ситуацій.

Основна мета роботи, яка полягала в покращенні надійності мережі доступу досягнута, а основна задача роботи, яка полягала в удосконаленні структури мережі доступу вирішена.

СПИСОК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Державний стандарт України ДСТУ 2861-94 Надійність техніки. Аналіз надійності.

2. Постанова Національної комісії, що здійснює державне регулювання у сферах електронних комунікацій, радіочастотного спектра та надання послуг поштового зв’язку 20 квітня 2022 року № 30. ОРІЄНТОВНИЙ ПЕРЕЛІК видів електронних комунікаційних послуг.

3. Закон України "Про захист інформації в автоматизованих системах".

4. Закон України "Про електронні комунікації".

5. Закон України "Про критичну інфраструктуру".

6. Закон України "Про основні засади забезпечення кібербезпеки України".

7. Міністерство цифрової трансформації Стратегія розвитку сфери електронних комунікацій України – 2030, Опубліковано 24 травня 2024.

8. STANAG 5042 (Видання 1) Військові телекомунікації – схематичні позначення, 1978. – 25с.

9. Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації від 29.12.2022 № 849 Технічні вимоги до електронних комунікаційних мереж щодо їх сталості в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.

10. Довідник “сержанта-зв’язківця” ЗВП 6-00(26).62, липень 2024.

11. [Електронний ресурс] База даних для потреб ЗСУ: https://flashbase.com.ua

12. [Електронні ресурси] Військова бібліотека: https://www.ukrmilitary.com, https://mil.in.ua/uk/articles/militarna-biblioteka

13. [Електронний ресурс] Сайт Полтаваобленерго https://www.poe.pl.ua/disconnection/power-outages.

14. [Електронний ресурс] Вікіпедія https://uk.wikipedia.org/wiki/VSAT

ДОДАТКИ

ДОДАТОК 1

1.5 Examples of active access networks

Below are examples of active subscriber-to-provider access networks that use different types of communication lines — both cable and wireless. Such networks provide users with access to the Internet through various technologies, depending on the infrastructure and coverage conditions.

a.) Networks based on fiber optic lines (FTTx)

- **FTTH (Fiber to the Home):** This is the most advanced and high-speed technology, where optical fiber is brought directly to the user's home, office, or apartment.
  - **Example:** In many cities of the world and in Ukraine, FTTH-based networks are actively deployed by large Internet providers, such as **Ukrtelecom**, **Kyivstar**, or **Vodafone Ukraine**. They offer Internet speeds of up to 1 Gbit/s or more for private users and businesses.
- **FTTB (Fiber to the Building)**: Fiber is brought to the building, and inside it Ethernet or other copper technology is used to connect individual apartments or offices.
  - **Example:** Access networks in high-rise buildings in Ukrainian cities, such as Kyiv, Dnipro and Lviv, provided by providers **Lanet, Triolan** and others.

b.) Networks based on copper lines (DSL).

- **ADSL (Asymmetric DSL)**: Uses regular telephone lines (copper wires) for data transmission. This is an older technology, but it is still popular in remote areas.
  - **Example:** Ukrtelecom in Ukraine continues to offer ADSL connections in rural and remote regions where it is not possible to lay optical fiber. The speed of such connections can reach up to 24 Mbit/s per download.

- **VDSL (Very High-Speed DSL)**: Uses the same copper lines, but provides faster speeds over shorter distances.
  - **Example**: In the cities of Ukraine, for example, the **Kyivstar** provider provides VDSL connections in places where optical fiber cannot be installed, providing speeds of up to 100 Mbit/s.

c.) Cable networks (DOCSIS)

- **DOCSIS (Data Over Cable Service Interface Specification):** A technology that uses coaxial cables, commonly used for television, to provide broadband Internet.
  - **Example:** In many European countries and in Ukraine, providers such as **Volya** (now under the **Vodafone Ukraine** brand) provide Internet services through DOCSIS cable networks, with the possibility of connection speeds up to 500 Mbit/s and higher.

d.) Wireless networks (4G/5G)

- **4G (LTE)**: It is used to provide mobile Internet in areas where there is no wired connection. LTE speed can reach up to 100 Mbps.
  - **Example:** Mobile operators in Ukraine — **Kyivstar**, **Vodafone Ukraine** and **lifecell** — provide mobile Internet services via 4G/LTE, providing coverage throughout the country. This is especially popular in rural and remote areas.
- **5G**: The fifth generation of mobile networks, which allows you to get speeds up to several Gbps and reduced latency.
  - **Example:** In Ukraine, 5G technology is still in the process of being implemented, but in many European countries, such as Germany or Sweden, operators already provide commercial 5G services for private and business subscribers.

e.) Wi-Fi (Fixed Wireless Access)

- **Wi-Fi for home networks or municipal access networks:** These are wireless networks used to organize point-to-point or point-to-multipoint connections for Internet access.

- **Example:** ISPs can use Wi-Fi to provide Internet access in hard-to-reach places where cabling is difficult. For example, in some rural regions or at tourist sites, Wi-Fi networks are used as the main means of accessing the Internet.

f.) Microwave communication lines

- **Microwave radio relay lines (point-to-point):** Used to provide communication between base stations and the provider's infrastructure. This technology is used to transmit large amounts of data at a distance of several tens of kilometers.
  - **Example:** Many mobile operators use microwave lines to connect base stations to fiber backbone networks. For example, **Vodafone Ukraine** uses such lines to ensure a stable connection in regions with insufficient fiber optic infrastructure.

g.) Satellite Internet

- **Satellite Internet (Starlink, VSAT)**: Provides access to the Internet through satellite systems, which makes it especially important in remote regions where there is no other infrastructure.
  - **Example:** The Starlink system from SpaceX is already actively used in Ukraine to provide Internet in places with damaged infrastructure or in remote regions. Other satellite solutions also exist **[14]**, such as **VSAT** (**Very Small Aperture Terminal) — small satellite ground station, terminal with antenna, according to international classification up to less than 2.5 meters**, which are used in different regions to access the Internet, such as **IDirect** or **Tooway**.

ДОДАТОК 2

Міністерство освіти і науки України
Національний університет «Полтавська політехніка імені Юрія Кондратюка» (Україна)
Інститут телекомунікацій та глобального інформаційного простору Національної академії наук України (Україна)
Національний технічний університет «Дніпровська політехніка» (Україна)
Лодзький університет, Лодзь (Польща)
Лодзька політехніка, Лодзь (Польща)
Білостоцька політехніка, Білосток (Польща)
Європейський інститут безперервної освіти EIDV (Словенія)
Коледж бізнесу Коггін, Університет Північної Флориди, Джексонвіль (США)

МАТЕРІАЛИ
Міжнародної науково-практичної конференції

Digital Economy and IT: Trends and Perspectives 2024

28-29 листопада 2024 року

Полтава 2024

[8] R. Oliveto, F. Khomh, G. Antoniol, and Y.-G. Guéhéneuc, “Numerical signatures of antipatterns: An approach based on b-splines,” in Proceedings of the 14th Conference on Software Maintenance and Reengineering, IEEE Computer Society Press, 2019.
[9] R. Peters and A. Zaidman, “Evaluating the lifespan of code smells using software repository mining,” in Proceedings of the European Conference on Software Maintenance and Reengineering, 2020, pp. 411–416.
[10] T. Kamiya, S. Kusumoto, and K. Inoue, “CCfinder: a multilinguistic token-based code clone detection system for large scale source code,” Transactions on Software Engineering, no. 4, 2018.
[11] F. Khomh, S. Vaucher, Y.G. Guéhéneuc, and H. Sahraoui, “A Bayesian Approach for the Detection of Code and Design Smells”, in Proceedings of the 9th International Conference on Quality Software, 2021.
[12] I. D. Baxter, A. Yahin, L. Moura, M. Sant’Anna, and L. Bier, “Clone detection using abstract syntax trees,” in Proceedings of the International Conference on Software Maintenance, 2019, pp. 368–377.
[13] G. Canfora, L. Cerulo, and M. Di Penta, “Identifying changed source code lines from version repositories,” in Proceedings of 4th International Workshop on Mining Software Repositories. Minneapolis, Minnesota, USA: IEEE CS Press, 2018, pp. 14–21.
[14] B. Caprile and P. Tonella, “Restructuring program identifier names,” in Proceedings of the International Conference on Software Maintenance, 2021, pp. 97–107.

Варіативність і Доступність Мереж Доступу для Бізнесу та Промисловості, як Основа Досягнення Надійності Роботи Сервісів Електронних Комунікацій.

Олександр Поляков[a]

[a] *Військовий коледж сержантського складу Військового інституту телекомунікацій та інформатизації імені Героїв Крут, м. Полтава, 36000, Україна*

Анотація

Безперебійне функціонування мереж електронних комунікацій є критично важливим для бізнесу і промисловості. Для підприємств існує потреба постійно підвищувати стійкість та безвідмовність функціонування електронних комунікаційних мереж доступу. Працюючий у критичних ситуаціях бізнес не тільки конкурентний, но і є економічною базою виживання держави. За допомогою сучасних технологій є можливість відносно дешево забезпечити надійність мереж доступу і підвищити їх функціонал. Для забезпечення процесу резервування необхідно розробити модель з заданими параметрами і підібрати обладнання. Для розгортання ліній зв’язку і їх налаштування до послуг промисловості та бізнесу велика кількість локальних і глобальних провайдерів на ринку України та у світі.

Ключові слова

Надійність, електронні комунікації, підприємство, мережа доступу

Вступ

В сучасних реаліях підприємства, організації та суспільство України постійно вирішує проблему стійкості зв’язку для забезпечення різноманітних потреб. Вплив російської агресії на інфраструктуру електронних комунікаційних мереж підприємств, установ та закладів України є

Digital Economy and IT: Trends and Perspectives 2024, November 28-29, 2024, Poltava, Ukraine
equator255equator@gmail.com (O. Poliakov)
0009-0007-1447-226X (O. Poliakov)

значним і різноманітним. Це і фізичне знищення об'єктів, таких як базові станції, сервери та дата-центри, що призводить до пошкодження, або повного знищення ключових елементів електронних комунікаційних мереж, кібератаки, включаючи DDoS-атаки, націлені на системи зв'язку, викликали збої у роботі, що ускладнює доступ до інформації та послуг, вимкнення електрики через обстріли енергетичної інфраструктури також негативно позначається на функціонуванні електронних комунікаційних мереж. Додатково, зміна умов праці та евакуація спеціалістів призвели до дефіциту кадрів у галузі. Втрата фізичної інфраструктури вимусила операторів шукати альтернативні маршрути для трафіку, що може знизити якість обслуговування. В той же час за останнє десятиліття значно збільшились можливості розгортання мереж електронних комунікацій, з'явились нові та покращились старі способи підключень бізнесу та промисловості до електронних комунікаційних мереж загального користування[4].

Постановка задачі

Враховуючи вищезгадані загрози та маючи доступні на ринку технічні можливості резервування мереж доступу стає критично важливим. Воно дозволяє забезпечити гарантовану надійність доступ до мережевих ресурсів, навіть у випадках збоїв чи фізичного пошкодження інфраструктури. Забезпечення високої надійності обслуговування є важливим для критичних процесів, таких як комунікації, промисловість, освіта та інші сервіси. Резервування також забезпечує швидку адаптацію у разі зміни умов чи появи нових загроз, дозволяючи оперативно змінювати налаштування та перенаправляти ресурси для забезпечення безперервності роботи. Це допомагає знизити ризик втрати даних, або перерв у роботі підприємств, установ та закладів в умовах війни [1], [3].

Підприємство з резервованою мережею доступу має значну конкурентну перевагу, оскільки забезпечує безперервність роботи та високу якість обслуговування навіть в умовах непередбачуваних збоїв.

Послуги доступу до мережі Інтернет провайдер до клієнта може забезпечувати різними способами будуючи лінії зв'язку за різними технологіями.

Нижче приведені основні різновиди лінії зв'язку які використовуються для розгортання мереж доступу[4], а саме: кабельні лінії (мідний кабель: кручена пара (UTP, STP); коаксіальні кабелі; чотирьох, або двох провідна лінія для DSL; силові кабелі з передачею даних; оптоволоконний кабель: FTTx (Fiber to the x); PON (Passive Optical Network); Active Optical Network (AON); WDM (Wavelength Division Multiplexing); радіо лінії (мікрохвильові (надвисокочастотні) радіолінії: земні мікрохвильові лінії; мікрохвильові радіорелейні системи; Wi-Fi (IEEE 802.11); WiMAX; 4G/5G; MMDS (Multichannel Multipoint Distribution Service); Satellite Internet (Супутниковий Інтернет); LMDS (Local Multipoint Distribution Service)).

Проєктування та побудова мережі доступу для підприємств та бізнесу на теперішній час в Україні є складним, але необхідним завданням, яке потребує врахування багатьох факторів (від технічних вимог і доступності технологій до безпеки та надійності інфраструктури).

При існуючій насиченості ринку електронних комунікаційних послуг підприємства промисловості можуть дозволити забезпечити підвищення надійності роботи сервісів багатократним резервування за відносно невелику ціну.

Вибір моделі мережі доступу

Для підприємств критичної інфраструктури особливо важливі параметри надійності та безпеки мереж[4]:

- Оптоволоконні мережі забезпечують високу надійність і захищеність від зовнішніх впливів, включно з електромагнітними перешкодами. Це робить їх найкращим вибором для критичних об'єктів, таких як енергетичні, транспортні, комунікаційні мережі та підприємства оборонного комплексу.

- Бездротові рішення можуть використовуватися як резервні канали зв'язку, забезпечуючи безперервну роботу підприємства в разі збоїв основної мережі. 4G мережі, наприклад,

дозволяють передавати дані з відносно невеликою затримкою, що важливо для резервування систем контролю та моніторингу.

- Супутникові системи (Starlink, Tooway) можуть бути використані як резервні рішення для віддалених або стратегічних об'єктів, де інші типи з'єднань недоступні або ненадійні.

Як приклад наведена модель для мережі доступу невеликого підприємства на рис.1 [2].

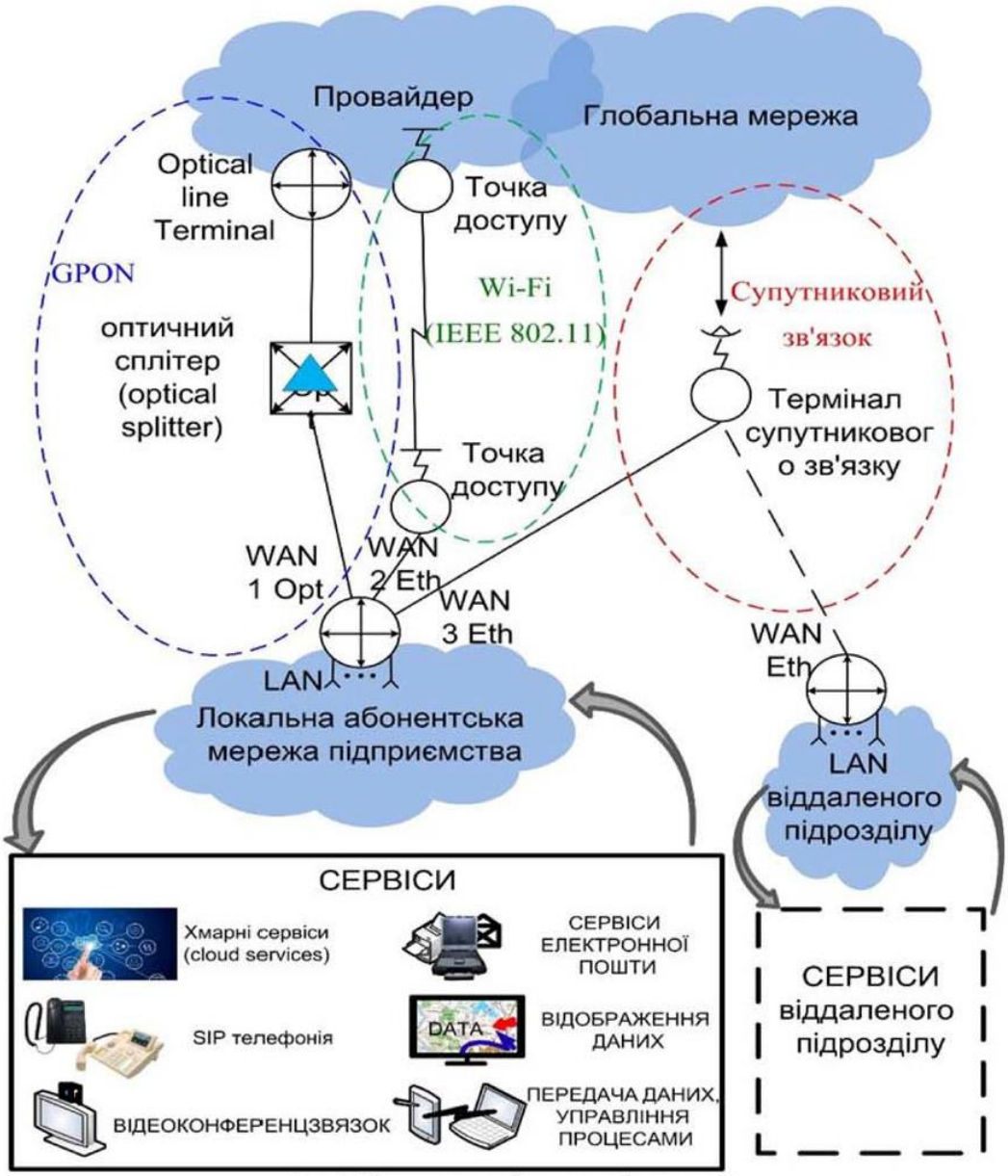


Рис.1. Модель мережі доступу підприємства

Вибір основної лінії доступу побудований на технології GPON обумовлений наступними факторами:

- виконуються основні вимоги підприємства щодо забезпечення швидкості та енергонезалежність обладнання (більшість провайдерів обіцяють підтримку енергоживлення свого обладнання на вузлах зв’язку під час критичних ситуацій, а сама лінія не потребує живлення);
- дана технологія доступна на ринку і представлена багатьма провайдерами.

Логічним вибором резервування основної лінії є одна з технологій широкосмугового радіозв’язку. Найбільш дешевим та розповсюдженим варіантом є Wi-Fi (IEEE 802.11).

Вибір цього варіанту випливає з наступних факторів:

- в діючий мережі доступу підприємство взагалі не має резервування, тому є сенс розвивати структуру поступово, і почати з найбільш доступного рішення;
- даний варіант підключення передбачає обладнання з мінімальним споживанням енергоживлення і досить легко підключається до резервних джерел живлення;
- точки доступу досить легко розташувати на новій локації, а також не складно розвинути мережу доступу змінивши топологію точка – точка на точка – багатоточка.
- хоча це і резервний варіант, сучасні зразки точок доступу дозволяють працювати на швидкостях до 300 Мбіт/с і більше.

Основними недоліками вищезазначеної радіолінії є необхідність пошуку відкритих інтервалів, що досить просто вирішується при наявності високих споруд. Також радіолінія вразлива до різного виду електромагнітних перешкод, що не є критичним для резервування.

Основна лінія та її резервування розраховані на одного провайдера, з метою зменшення витрат та спрощення процедур підключення і обслуговування, тому логічним кроком для забезпечення резерву “останньої надії” буде підключення що орієнтується на іншого постачальника електронних комунікаційних послуг. Найкращим рішенням в даній ситуації буде взагалі відхід від місцевих провайдерів і забезпечення доступу до мережі інтернет від глобального постачальника за допомогою систем супутникового зв’язку. В широкому доступі на ринку України присутні два види таких послуг: низькорбітальні та геостаціонарні системи. Головна перевага систем, що працюють з геостаціонарними супутниками в тому, що ціна на послуги доступу до мережі Internet та відповідне обладнання постійно падає і є доступною для підприємств. Проте аналізуючи характеристики такого підключення виявляється що у більшості провайдерів швидкість не перевищує 20 – 30 Мбіт/с, і найголовніше затримки (ping) можуть досягати 1000 – 1500 мс, що є неприйнятним у багатьох процесах управління виробництвом. Серед представлених на ринку постачальників доступу до мережі Internet за допомогою низькоорбітальних систем по ряду факторів поза конкуренцією є Starlink від SpaceX. Можливо через кілька років, завдяки розвитку проектів OneWeb, Amazon Kuiper та інших аналогічних вибір на користь Starlink буде не на стільки очевидним.

Висновки

Дана модель, як приклад, дозволяє показати які можливості забезпечення стійкості мережі доступу існують на даний час. Також варто зазначити, що наведений приклад моделі піддається зміні, масштабуванню, вдосконаленню та трансформації, так як всі елементи побудовані на доступних та розповсюджених комплектуючих.

Вважається, що застосування такої моделі для невеликого підприємства не потребує утримання в обмеженому штаті окремих фахівців, є лише необхідність разових залучень фахівців основного провайдера та короткої підготовки (інструктажу) одного (декількох) працівників, які згідно додаткових обов’язків будуть виконувати певний алгоритм в аварійних ситуаціях.

Література

[1] "Стратегія розвитку сфери електронних комунікацій України на період до 2030 року" презентована Міністерством цифрової трансформації України 16 травня 2024 року.
[2] STANAG 5042 (Видання 1) Військові телекомунікації – схематичні позначення, 1978.
[3] Наказ Адміністрації Державної служби спеціального зв'язку та захисту інформації від 29.12.2022 № 849 Технічні вимоги до електронних комунікаційних мереж щодо їх сталості в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.
[4] Климаш М. М. Телекомунікаційні системи передавання інформації: навч. посібник / М.М. Климат, Р.С. Колодій. — Львів: Видавництво Львівської політехніки, 2018.

ДОДАТОК 3

ISU
INTERNATIONAL SCIENTIFIC UNITY

CERTIFICATE
of conference participant

it is hereby certified, that

ОЛЕКСАНДР ПОЛЯКОВ

took part in the XII International Scientific and Practical Conference
«SCIENTIFIC THEORIES AND PRACTICES AS AN ENGINE
OF MODERN DEVELOPMENT»

February 28 - March 1, 2024, Bratislava, Slovakia
12 Hours of Participation
(0,4 ECTS credits)

Head of the
organizing committee

Viktoriia Tsiundyk