ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ»

на здобуття освітнього ступеня магістра
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

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

_____ Віталій БУРЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-61
Віталій БУРЧЕНКО
Ім'я, ПРІЗВИЩЕ

Керівник: Юрій МЕЛЬНИК
д.т.н., професор *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка _____
Освітньо-професійна програма _____Телекомунікаційні системи та мережі_____

ЗАТВЕРДЖУЮ
Завідувач кафедри __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бурченку Віталію Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Захист каналів зв'язку в критичних інфраструктурах
керівник кваліфікаційної роботи Юрій МЕЛЬНИК, д.т.н., професор
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «30» 10. 2025 р. № 467

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1. Волоконно-оптичні лінії зв'язку.
2. Вразливості оптоволоконних каналів зв'язку.
3. Захист від DDoS атак.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Волоконно-оптичні лінії зв'язку: класифікація, особливості та застосування компонентів.
2. Вразливості оптоволоконних каналів зв'язку.
3. Приховані канали зв'язку.
4. Захист від DDoS атак.

5. Перелік ілюстративного матеріалу: ___презентація на____слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	15.10.2025	Викон.
2	Розробка першого розділу	23.10.2025	Викон.
3	Розробка другого розділу	03.11.2025	Викон.
4	Розробка третього розділу	13.11.2025	Викон.
5	Розробка четвертого розділу	23.11.2025	Викон.
6	Висновки, вступ, реферат	03.12.2025	Викон.
7	Розробка презентації	13.12.2025	Викон.

Здобувач вищої освіти _____ Віталій БУРЧЕНКО
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Юрій МЕЛЬНИК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Бурченко В.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «Захист каналів зв'язку в критичних інфраструктурах»

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач Бурченко Віталій Миколайович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Бурченка Віталія Миколайовича на оцінку «відмінно» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Юрій МЕЛЬНИК
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Бурченко В.М. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедри телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 20___ року

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Бурченка Віталія Миколайовича
(прізвище, ім'я, по батькові)
на тему «Захист каналів зв'язку в критичних інфраструктурах»

Актуальність.
Сучасні телекомунікаційні системи є критично важливими для функціонування державних, військових, фінансових, енергетичних та корпоративних структур. Передавання більшості стратегічних даних здійснюється саме через волоконно-оптичні лінії зв'язку, які традиційно вважалися майже недоступними для перехоплення. Однак розвиток технологій, поява високочутливих сенсорів, нових типів мікрозгинань, евансцентних підключень, оптичних спліттерів та методів розсіювання показали, що фізичний рівень ВОЛЗ не є абсолютно захищеним. В умовах гібридних загроз, інформаційних операцій та зростання частки шифрованих сервісів особливої ваги набуває питання фізичної безпеки оптоволоконних ліній. Захист від інтрузивних і неінтрузивних атак стає не менш важливим, ніж криптографічні механізми. Саме тому дослідження методів перехоплення, моделювання втрат при згинанні, аналіз фізичних уразливостей та розробка практичних рекомендацій із захисту оптичних каналів є актуальним, практично значущим і стратегічно важливим завданням.
Позитивні сторони.
1. У роботі досліджено повний перелік реальних методів атаки на ВОЛЗ, включно з рідкісними неінтрузивними технологіями.
2. У роботі наведено реальні кейси перехоплення оптоволоконних каналів у міжнародній практиці.
Недоліки.
1. Недостатньо таблиць і порівняльних узагальнень для систематизації матеріалу.
2. Моделювання представлене без детального опису параметрів та умов експерименту.

Відзначені зауваження не впливають на загальну позитивну оцінку магістерської кваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "відмінно", а здобувач Бурченко Віталій Миколайович заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 82 стор., 21 рис., 1 табл., 20 джерел.

Мета роботи – аналіз вразливостей оптоволоконних каналів зв'язку, дослідження фізичних методів перехоплення інформації та розробка рекомендацій щодо підвищення стійкості оптичних ліній до інтрузивних і неінтрузивних атак.

Об'єкт дослідження – волоконно-оптичні лінії зв'язку як частина телекомунікаційної інфраструктури.

Предмет дослідження – фізичні вразливості оптоволоконних каналів та методи їх несанкціонованого підключення, включно з мікрозгинами, макрозгинами, оптичним розщепленням, евансцентним підключенням і розсіюванням сигналу.

Короткий зміст роботи: у кваліфікаційній роботі досліджено захист каналів зв'язку в критичних інфраструктурах з акцентом на фізичні та мережеві загрози, включно з DDoS-атаками та перехопленням трафіку в оптоволоконних лініях (мікрозгини, макрозгини, optical splitting, evanescent coupling). Показано, що навіть ВОЛЗ потребують додаткових інженерних і криптографічних заходів безпеки. Проаналізовано ризики, пов'язані з технологіями WDM/DWDM, та узагальнено сучасні методи протидії DDoS, які потребують автоматизації та багаторівневого підходу. Зроблено висновок про необхідність комплексного захисту, що поєднує технічні, програмні й організаційні рішення.

КЛЮЧОВІ СЛОВА: ЗАХИСТ КАНАЛІВ ЗВ'ЯЗКУ, КРИТИЧНА ІНФРАСТРУКТУРА, ОПТОВОЛОКОННІ ЛІНІЇ, ПЕРЕХОПЛЕННЯ ТРАФІКУ, МІКРОЗГИНИ, МАКРОЗГИНИ, OPTICAL SPLITTING, EVANESCENT COUPLING, WDM, DWDM, DDOS-АТАКИ, МЕРЕЖЕВІ ЗАГРОЗИ, ШИФРУВАННЯ, МОНІТОРИНГ ЦІЛІСНОСТІ, ФІЗИЧНА БЕЗПЕКА

ABSTRACT

Text part of the master's qualification work: 82 pages, 21 figures, 1 table, 20 sources.

The purpose of the work is to analyze the vulnerabilities of fiber-optic communication channels, study physical methods of information interception and develop recommendations for increasing the resistance of optical lines to intrusive and non-intrusive attacks.

Object of the study is fiber-optic communication lines as part of the telecommunications infrastructure.

Subject of the study is the physical vulnerabilities of fiber-optic channels and methods of their unauthorized connection, including microbends, macrobends, optical splitting, evanescent coupling and signal scattering.

Summary of the work: the qualification work investigates the protection of communication channels in critical infrastructures with an emphasis on physical and network threats, including DDoS attacks and interception of traffic in fiber-optic lines (microbends, macrobends, optical splitting, evanescent coupling). It is shown that even FOCLs require additional engineering and cryptographic security measures. The risks associated with WDM/DWDM technologies are analyzed and modern methods of countering DDoS, which require automation and a multi-level approach, are summarized. The conclusion is made about the need for comprehensive protection, combining technical, software and organizational solutions.

KEYWORDS: PROTECTION OF COMMUNICATION CHANNELS, CRITICAL INFRASTRUCTURE, FIBER OPTIC LINES, TRAFFIC INTERCEPTION, MICRO-BENDS, MACRO-BENDS, OPTICAL SPLITTING, EVANESCENT COUPLING, WDM, DWDM, DDOS ATTACKS, NETWORK THREATS, ENCRYPTION, INTEGRITY MONITORING, PHYSICAL SECURITY

ЗМІСТ

ВСТУП 9
РОЗДІЛ 1 ВОЛОКОННО-ОПТИЧНІ ЛІНІЇ ЗВ'ЯЗКУ: КЛАСИФІКАЦІЯ, ОСОБЛИВОСТІ ТА ЗАСТОСУВАННЯ КОМПОНЕНТІВ 11
1.1 Історія та основні положення 11
1.2 Вікна прозорості та поняття модовості 19
1.3 З’єднання та мультиплексування в каналх зв’язку 24
РОЗДІЛ 2 ВРАЗЛИВОСТІ ОПТОВОЛОКОННИХ КАНАЛІВ ЗВ’ЯЗКУ 30
2.1 Методи атаки на оптоволоконні канали зв’язку 30
2.2 Моделювання методів 35
2.3 Подальші сценарії 40
РОЗДІЛ 3 ПРИХОВАНІ КАНАЛИ ЗВ’ЯЗКУ 46
3.1 Абстрактні анонімні мережі 46
3.2 Основні підходи до реалізації 51
3.3 Створення архітектур 56
РОЗДІЛ 4 ЗАХИСТ ВІД DDOS АТАК 62
4.1 Основні компоненти захисту 62
4.2 Способи впровадження компонентів захисту 67
4.3 Підходи до реалізації рішеть захисту від DDoS 71
ВИСНОВКИ 81
ПЕРЕЛІК ПОСИЛАНЬ 83
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ 85

ВСТУП

Сучасне суспільство неможливо уявити без розгалужених комунікаційних систем, які забезпечують стабільну роботу енергетики, транспорту, фінансових структур, охорони здоров'я, органів державного управління та інших сфер, що належать до критичної інфраструктури. Усі ці системи залежать від надійних каналів зв'язку, адже навіть короткочасне порушення їх функціонування може призвести до серйозних економічних збитків, соціальної дестабілізації або створення загрози національній безпеці.

Разом із тим, розвиток телекомунікацій, впровадження волоконно-оптичних ліній зв'язку, технологій спектрального ущільнення (CWDM, DWDM), а також поширення безпроводових і мобільних мереж п'ятого та шостого поколінь створює нові виклики для забезпечення їх захищеності. Канали зв'язку, які ще донедавна вважалися майже недоступними для перехоплення, сьогодні піддаються складним атакам: від використання методів оптичного підключення (мікро- та макроізгини, розщеплення сигналу, брегівські решітки) до впровадження паразитичних та прихованих каналів.

Не менш критичними є і кіберзагрози, пов'язані з атаками на рівні мережевих протоколів та прикладних сервісів. Зокрема, DoS та DDoS-атаки вже давно перестали бути інструментом окремих зловмисників і перетворилися на глобальну проблему, здатну паралізувати діяльність навіть найбільших дата-центрів та хмарних платформ. Використання ботнетів із сотень тисяч вузлів, зловживання уразливостями web-додатків, зростання частки шифрованого трафіку (SSL/TLS) ускладнюють процес виявлення та блокування загроз. У цьому контексті постає потреба в інтегрованих підходах, які поєднують як локальні CPE-рішення, так і потужні хмарні сервіси з можливістю масштабування та автоматичного реагування.

Важливим є і те, що канали зв'язку в критичних інфраструктурах мають забезпечувати не лише захист від зовнішніх атак, але й від внутрішніх загроз. Йдеться про можливість компрометації користувачів, зловживання доступом, створення прихованих каналів у вже наявних мережах. Саме тому актуальним стає

впровадження криптографічних механізмів з теоретично доведеною анонімністю, багаторівневої системи моніторингу та поведінкового аналізу користувачів.

Отже, актуальність дослідження захисту каналів зв’язку в критичних інфраструктурах зумовлена сукупністю факторів: стрімким розвитком технологій зв’язку, зростанням обсягів і швидкості передачі даних, ускладненням методів атак і підвищенням вимог до безпеки. Метою даної роботи є комплексне дослідження сучасних методів та засобів захисту, аналіз архітектурних рішень для забезпечення стійкості до атак, а також розробка практичних рекомендацій щодо побудови ефективної системи безпеки каналів зв’язку для критичних об’єктів.

1 ВОЛОКОННО-ОПТИЧНІ ЛІНІЇ ЗВ'ЯЗКУ: КЛАСИФІКАЦІЯ, ОСОБЛИВОСТІ ТА ЗАСТОСУВАННЯ КОМПОНЕНТІВ

1.1 Історія та основні положення

XX століття стало не лише епохою стрімкого науково-технічного прогресу, а й періодом справжнього прориву у сфері комунікацій. Технології передавання інформації зазнали глибоких змін: телеграф поступово еволюціонував у більш досконалі рішення на основі витої пари, а радіозв’язок — у потужні мобільні мережі, що згодом перетворилися на невід’ємну частину життя суспільства. Саме в цей час починається історія створення та розвитку волоконно-оптичних ліній зв’язку (ВОЛЗ), які стали фундаментом сучасної телекомунікаційної інфраструктури.

Витоки цієї технології сягають середини XX століття, коли науковці розробили теоретичні засади, що пояснювали природу явища повного внутрішнього відбиття світла. Ця теорія відкрила можливість використовувати світлові хвилі як носій інформації. У 1950-х роках було висунуто перші ідеї застосування скляних волокон для створення світловодів. Попри це, технологія на початковому етапі мала суттєві обмеження: низька якість матеріалів і значні оптичні втрати не дозволяли використовувати їх для ефективної передачі даних на практиці.

Справжній прорив відбувся у 1960-х роках завдяки дослідженням компанії Corning Glass Works. Її фахівці змогли створити скло високого рівня чистоти й однорідності, що значно знизило рівень втрат сигналу під час його поширення. Цей результат відкрив шлях до використання волокон для передавання світла на великі відстані. Водночас у лабораторіях Bell Telephone було розроблено перші напівпровідникові лазери з характеристиками, придатними для роботи у волоконно-оптичних системах. Таким чином, з’явився симбіоз двох ключових технологій — досконалих світловодів і стабільних лазерних джерел.

У 1970-х роках були прокладені перші експериментальні ВОЛЗ, що підтвердили перспективність нової технології. Уже у 1980-х роках вона здобула міжнародне визнання, а телекомунікаційні оператори почали масово впроваджувати волоконно-оптичні лінії у власні мережі. Надалі розвиток технології відбувався у напрямку зниження втрат у волокнах, вдосконалення лазерних передавачів та підвищення швидкості передавання даних.

Сьогодні волоконно-оптичні лінії є основою глобальної телекомунікаційної індустрії. Вони забезпечують не лише надзвичайно високу пропускну здатність, а й виняткову надійність під час передавання інформації на міжконтинентальні відстані. Саме завдяки ВОЛЗ функціонують сучасний Інтернет, міжнародна та міжміська телефонія, кабельне телебачення, а також численні інформаційні мережі. Сьогодні важко уявити будь-яку сферу життєдіяльності без технології, яка з моменту свого створення стала символом еволюції комунікацій, та відкрила шлях до нової цифрової епохи.

Основний принцип

Ключовий принцип роботи волоконно-оптичних ліній зв’язку повністю відображений у їхній назві: інформація передається за допомогою світлових хвиль, що поширюються в оптичному волокні. Завдяки цьому досягається надзвичайно висока швидкість і пропускна здатність, що робить технологію основою сучасних телекомунікаційних систем. Конструктивно будь-який оптичний канал складається з двох взаємопов’язаних елементів — оптичного волокна, яке виступає фізичним середовищем поширення сигналу, та трансивера, що забезпечує перетворення і відновлення інформації.

Оптичне волокно є ключовою частиною всієї системи. Воно складається з кількох шарів, кожен з яких виконує важливу функцію. Центральна частина — скляна або кварцова сердцевина, по якій поширюється світловий сигнал. Вона оточена оболонкою з меншим показником заломлення, завдяки чому реалізується ефект повного внутрішнього відбиття. Це явище дозволяє світловим променям рухатися всередині сердцевини навіть при згинах кабелю, не виходячи за межі волокна. Зовні вся конструкція вкрита захисним шаром, що запобігає механічним пошкодженням,

впливу вологи, температурних коливань та інших негативних факторів навколишнього середовища. Додатково в сучасних кабелях використовують армувальні елементи, що підвищують стійкість до розтягування та зовнішніх навантажень.

Не менш важливою складовою є трансивер — спеціальний приймально-передавальний модуль, який виконує перетворення сигналів. Під час передавання він трансформує електричні коливання у світлові імпульси за допомогою лазерного діода або світлодіода. При прийманні відбувається зворотний процес: оптичний сигнал перетворюється фотодетектором на електричний, після чого відновлюється початковий потік даних. Таким чином, трансивер виступає своєрідним "мостом" між електронною частиною телекомунікаційної системи та оптичним середовищем передавання інформації.

У поєднанні ці два елементи забезпечують унікальні можливості волоконно-оптичних ліній: мінімальні втрати сигналу навіть на відстанях у сотні кілометрів, нечутливість до електромагнітних завад, високу швидкість і стабільність передавання даних. Саме завдяки цьому волоконно-оптичні технології стали базисом сучасного Інтернету, глобальних телекомунікаційних мереж, кабельного телебачення та багатьох інших інформаційних сервісів.

Оптоволокно

Оптичне волокно є фундаментальним елементом сучасних телекомунікаційних систем, адже саме воно забезпечує передавання інформації зі швидкістю, що відповідає потребам цифрової епохи. За своїми характеристиками волокна поділяють на дві головні групи — одномодові (Single Mode, SM) та багатомодові (Multi Mode, MM). Основна відмінність між ними полягає у діаметрі сердцевини та використанні різних діапазонів довжин хвиль світла, що визначає сфери їхнього практичного застосування.

У випадку одномодового волокна діаметр сердцевини становить у середньому 7–9 мкм, що дозволяє пропускати лише один мод світлового променя. Це дає змогу уникнути ефекту багатомодової дисперсії та забезпечити стабільність сигналу навіть на надвеликих відстанях. Для передавання інформації в таких

системах використовуються довжини хвиль у діапазоні 1 310–1 550 нм, що вважаються оптимальними через мінімальне поглинання та низьке затухання сигналу.

Багатомодове волокно, навпаки, має сердцевину значно більшого діаметра — 50–62,5 мкм, що дає змогу одночасно передавати багато мод світла. Це робить обладнання дешевшим і менш вимогливим до точності, але призводить до значніших втрат та обмежує максимальну відстань передавання. Як правило, багатомодові системи працюють з довжинами хвиль у діапазоні 850–1 300 нм. Через відносну дешевизну та простоту використання їх найчастіше застосовують у локальних мережах, для з'єднання обладнання всередині будівель, у корпоративних дата-центрах, де відстань між вузлами не перевищує кількох сотень метрів.

Водночас одномодове волокно демонструє зовсім інші характеристики. Воно забезпечує мінімальні втрати сигналу (затухання може становити менш ніж 0,2 дБ/км) і дозволяє передавати дані на десятки та сотні кілометрів без використання підсилювачів. Це робить його незамінним у магістральних каналах зв'язку, міжміських та міжнародних оптоволоконних лініях, а також у глобальній інфраструктурі Інтернету. Завдяки можливості підтримувати надвисокі швидкості обміну даними — 10G, 40G, 100G Ethernet і більше — одномодові системи стають основою мереж наступних поколінь. Єдиним недоліком є висока вартість обладнання (трансиверів, лазерів, фотодетекторів), що потребує високої точності налаштування.

Слід зазначити, що в межах кожної з двох категорій існують додаткові стандартизовані підтипи волокон, які відрізняються характеристиками та сферою застосування. Так, багатомодові кабелі поділяють на класи OM1, OM2, OM3, OM4 та OM5. Вони розраховані на роботу з різними джерелами випромінювання та підтримують різні швидкості передавання: наприклад, OM3 і OM4 широко використовуються у дата-центрах для 40G і 100G Ethernet на відстанях до 300–400 метрів. Одномодові волокна поділяються на класи OS1 та OS2: перший орієнтований на прокладання всередині приміщень, другий — на роботу в

магістральних мережах із мінімальним затуханням та здатністю передавати сигнал на відстань у сотні кілометрів.

Таким чином, поділ оптоволокон на одномодові та багатомодові має практичне значення й зумовлений специфічними потребами різних сфер використання. Якщо багатомодове волокно є економічним рішенням для коротких відстаней і внутрішніх комунікацій, то одномодове забезпечує критично важливу основу для глобальних мереж і високошвидкісних систем передавання даних. Саме їхнє взаємне доповнення дозволяє створювати сучасні телекомунікаційні інфраструктури, що відповідають вимогам як локальних, так і глобальних користувачів.

Види та стандарти оптичних волокон

У сучасних телекомунікаційних системах важливу роль відіграє правильна класифікація оптоволокон, адже від їхніх характеристик залежать швидкість, якість та дальність передавання даних. Загалом виділяють дві великі групи: багатомодові та одномодові волокна.

Багатомодові волокна (OM)

Для багатомодових оптичних волокон прийнято використовувати п’ять класифікаційних категорій — OM1, OM2, OM3, OM4, OM5 (де OM походить від *Optical Multimode*). Вони відрізняються діаметром сердцевини, смугою пропускання, а також сферою застосування.

Таблиця 1.1

Класифікації категорій

Категорія	Діаметр сердцевини, мкм	Діаметр оболонки, мкм	Колір оболонки	Джерело світла	Смуга пропускання, МГц·км	Застосування
OM1	62,5	125	помаранчевий	LED	200	Застарілий стандарт, використовується у старих мережах Ethernet 10BASE-F і 100BASE-FX. Підтримує 1 Гбіт/с Ethernet на відстані до 275 м.
OM2	50	125	помаранчевий	LED	500	Також застарілий стандарт, але з більшою пропускною здатністю, ніж OM1. Підтримує 1 Гбіт/с Ethernet на відстані до 550 м.
OM3	50	125	бірюзовий	VCSEL	2 000	Оптимізований для використання з лазерними джерелами світла. Підтримує 10 Гбіт/с Ethernet до 300 м, 40 Гбіт/с Ethernet до 100 м та 100 Гбіт/с Ethernet до 70 м (за умови паралельної передачі по кількох волокнах).
OM4	50	125	бірюзовий або фіолетовий	VCSEL	4 700	Удосконалена версія OM3 з більшою пропускною здатністю. Підтримує 10 Гбіт/с Ethernet до 550 м, 40 Гбіт/с Ethernet до 125 м та 100 Гбіт/с Ethernet до 125 м (за умови паралельної передачі по кількох волокнах).
OM5	50	125	яскраво-зелений з жовтуватим відтінком	VCSEL	див. прим.	Оптимізований для технології SWDM (Short Wavelength Division Multiplexing), яка дозволяє передавати кілька оптичних сигналів на різних довжинах хвиль по одному волокну. Підтримує високошвидкісні застосування (40, 100, 400 Гбіт/с) на більших відстанях у порівнянні з OM3 та O

Смуга пропускання для багатомодових волокон зазвичай вимірюється на довжині хвилі 850 нм, за винятком OM5, де використовують ширший діапазон — 850–953 нм. Це дозволяє застосовувати сучасні методи мультиплексування й досягати вищих швидкостей передавання даних на більших відстанях.

Одномодові волокна (OS)

Одномодові оптичні волокна мають власну класифікацію — OS1 та OS2, яка ґрунтується на вимогах стандарту *ITU-T G.652*.

- **OS1** — це ранній стандарт одномодового волокна, який спочатку був розроблений для прокладання всередині приміщень: у будівлях або між поверхами. Характеризується низьким затуханням у діапазонах довжин хвиль 1310 нм та 1550 нм, однак не був оптимізований для високих потужностей та передавання сигналів на великі відстані. На сьогодні OS1 вважається застарілим, хоча все ще може зустрічатися у локальних інфраструктурах.
- **OS2** — вдосконалений варіант, який використовується для зовнішнього прокладання між будівлями, у магістральних мережах та під час створення міжміських каналів зв’язку. Він має ще нижчі показники затухання порівняно з OS1, особливо на довжині хвилі 1550 нм, і добре підходить для високошвидкісної передачі на відстані у десятки та сотні кілометрів. OS2 також оптимізований для роботи з системами DWDM (Dense Wavelength Division Multiplexing — щільне спектральне мультиплексування), що робить його стандартом вибору для глобальних мереж та підводних кабелів.

Технологія DWDM

DWDM стала одним із найважливіших етапів розвитку телекомунікацій. Її сутність полягає у здатності передавати кілька незалежних оптичних сигналів по одному волокну, де кожен сигнал має свою довжину хвилі. Завдяки цьому відбувається багаторазове збільшення пропускної здатності без необхідності прокладання нових кабелів.

У системах DWDM зазвичай застосовується крок між каналами 100 або 50 ГГц, але у сучасних мережах перевага віддається сітці з кроком 50 ГГц, яка дозволяє

ефективніше використовувати спектр. Передавання здійснюється у «вікнах прозорості» оптичного волокна:

- **C-діапазон** (*Conventional band*, 1530–1565 нм),
- **S-діапазон** (*Short band*, 1460–1530 нм),
- **L-діапазон** (*Long band*, 1565–1625 нм).

Завдяки такому підходу сучасні мережі отримали можливість передавати сотні каналів із сукупною пропускною здатністю у терабіти на секунду.

Міжнародні стандарти одномодових волокон

Класифікація одномодових волокон базується на рекомендаціях ITU-T, серед яких особливе місце займають стандарти G.652, G.655 та G.657.

- **G.652 (Standard Single Mode Fiber)** — найпоширеніший стандарт, що охоплює як OS1, так і OS2, а також має підтипи A, B, C та D.
    - *G.652.A* і *G.652.B* оптимізовані для роботи на довжині хвилі **1310 нм**.
    - *G.652.C* і *G.652.D* відзначаються зменшеними втратами на довжині хвилі 1383 нм (так звана «водяна піка»), що дозволяє їх ефективне застосування у ширшому діапазоні 1310–1625 нм.
- **G.657** описує волокна, стійкі до вигинів. Вони створені спеціально для використання у приміщеннях, де кабель може мати малий радіус вигину або укладатися у петлі. Це значно полегшує монтаж у щільних кабель-каналах чи обмеженому просторі. Існують підтипи G.657, які відрізняються допустимим мінімальним радіусом вигину без значних втрат сигналу.
- **G.655** визначає волокна зі зміщеною дисперсією. Вони оптимізовані для довжини хвилі 1550 нм і використовуються у системах DWDM, де важливо мінімізувати вплив дисперсії під час передавання сигналів на великі відстані. Такі волокна стали базою для розвитку міжнародних магістральних каналів і підводних кабелів.

1.2 Вікна прозорості та поняття модовості

Вікна прозорості

Одним із ключових параметрів, що визначає ефективність роботи оптичного волокна, є довжина хвилі світла, яка використовується для передавання інформації. У технічних характеристиках вона завжди вказується з особливою точністю, адже саме цей показник суттєво впливає на якість та дальність передавання сигналу. Постає логічне питання: чому використовуються лише певні значення довжин хвиль і чим це зумовлено?

Відповідь була знайдена під час численних експериментів, у ході яких з’ясувалося, що затухання світлових хвиль залежить від їхньої довжини. Деякі хвилі втрачають інтенсивність значно швидше, тоді як інші здатні поширюватися у волокні з мінімальними втратами. На підставі цих досліджень було сформовано поняття «вікон прозорості» — спектральних діапазонів, у яких коефіцієнт затухання є мінімальним. Саме ці області використовуються для побудови телекомунікаційних систем. Виділяють три основні вікна прозорості: 850 нм, 1 310 нм та 1 550 нм.

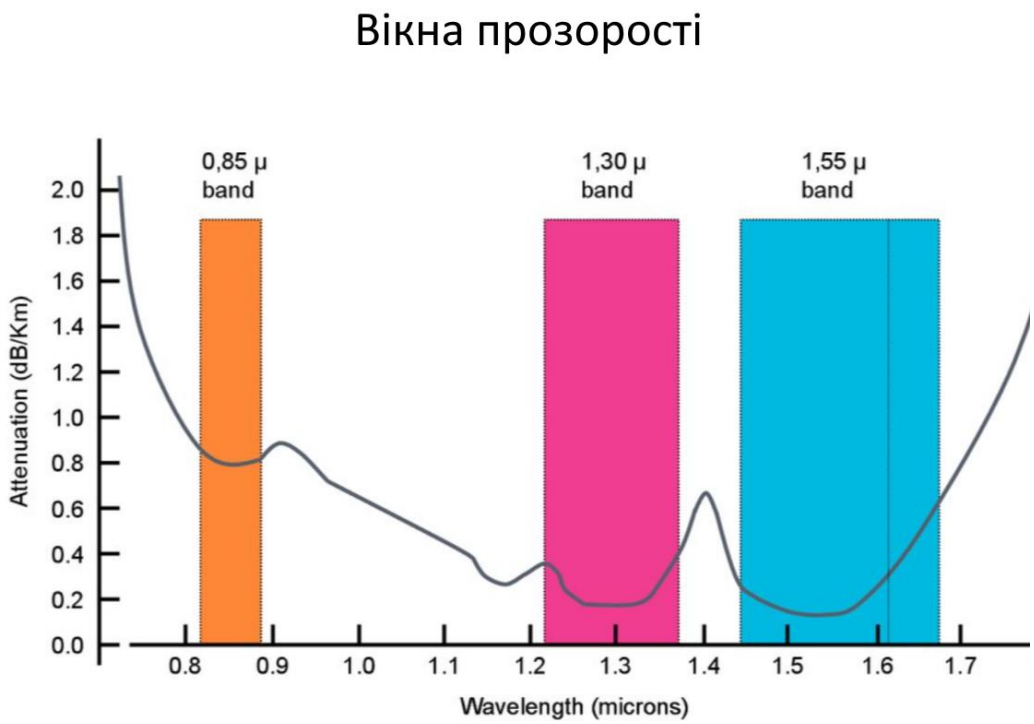


Рис. 1.1 Три основні вікна прозорості

Оптимальні діапазони та їх застосування

- **850 нм** — це найкоротше з базових вікон прозорості, яке здебільшого використовується у багатомодовому оптичному волокні. Через відносно високий рівень затухання (близько 2,5–3 дБ/км) воно підходить лише для передавання на короткі відстані, зазвичай у межах одного будинку або кампусу. Попри цей недолік, діапазон 850 нм зберігає популярність завдяки доступності та низькій вартості джерел випромінювання, особливо лазерів **VCSEL** (Vertical-Cavity Surface-Emitting Laser), що широко використовуються у локальних мережах та дата-центрах.
- **1 310 нм** — проміжне вікно прозорості, яке застосовується переважно в одномодовому волокні. Воно характеризується мінімальною хроматичною дисперсією, тобто світлові імпульси не розтягуються у часі, зберігаючи чіткість і форму навіть при передаванні на значні відстані. Саме тому діапазон 1 310 нм став основним вибором для побудови телекомунікаційних систем середнього масштабу, що забезпечують стабільне передавання сигналів на відстанях у десятки кілометрів.
- **1 550 нм** — найдовше та водночас найважливіше вікно прозорості. Воно забезпечує рекордно низьке затухання (менше 0,2 дБ/км), що робить його оптимальним для побудови магістральних ліній зв’язку, підводних кабелів та міжміських каналів. Додатковою перевагою цього діапазону є його сумісність із технологіями **DWDM (Dense Wavelength Division Multiplexing)**, які дозволяють передавати сотні незалежних каналів одночасно по одному оптичному волокну. Завдяки цьому саме діапазон 1 550 нм став основою сучасних глобальних телекомунікаційних систем, де критично важливими є великі відстані й висока пропускна здатність.

Наукове та практичне значення

Використання вікон прозорості стало одним із ключових чинників розвитку оптичних технологій. Якщо на початкових етапах оптоволокно обмежувалося короткими відстанями й низькими швидкостями, то з відкриттям цих спектральних

діапазонів вдалося створити сучасні високопродуктивні системи передавання даних.

- Діапазон **850 нм** забезпечив поширення волоконно-оптичних мереж у локальних комунікаціях.
- Діапазон **1 310 нм** дозволив значно розширити можливості одномодових систем, забезпечивши передачу сигналів без суттєвих втрат якості.
- Діапазон **1 550 нм** фактично став символом епохи високошвидкісних магістральних мереж і нині вважається «золотим стандартом» оптичного зв'язку.

Таким чином, саме завдяки концепції вікон прозорості телекомунікаційна галузь отримала можливість досягти сучасного рівня розвитку. Вибір оптимальної довжини хвилі для конкретної мережі дає змогу збалансувати вартість обладнання, швидкість передавання, якість сигналу та максимальну дальність.

Поняття модовості

У волоконно-оптичних системах поняття **моди** описує можливі шляхи, якими світловий промінь може поширюватися крізь оптичне волокно. Інакше кажучи, мода — це певний просторовий або геометричний напрямок руху фотонів усередині сердцевини волокна.

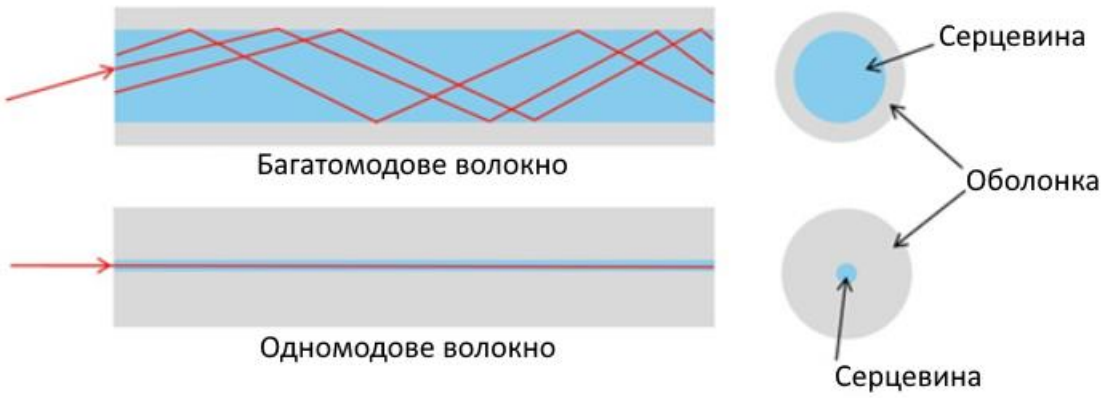


Рис. 1.2 Багатомодове та одномодове волокна

Усередині оптоволоконного кабелю світло здатне поширюватися як прямолінійно вздовж осі сердцевини, так і складними зигзагоподібними

траєкторіями, багаторазово відбиваючись від межі між сердцевиною та оболонкою. Така різноманітність шляхів призводить до того, що окремі промені проходять неоднакові відстані та, відповідно, приходять до приймального кінця кабелю у різний час. В результаті світловий імпульс «розтягується» у часі, стає менш чітким, а інформаційний сигнал спотворюється. Це явище отримало назву модової дисперсії.

Модова дисперсія є серйозним обмежувальним фактором для багатомодових систем, оскільки вона зменшує швидкість і якість передавання даних. Чим довша відстань поширення та чим вища швидкість передавання, тим сильніше помітний негативний ефект. Саме тому у високошвидкісних мережах часто застосовують одномодові волокна, де поширюється лише одна мода і відсутні часові спотворення через різницю шляхів.

Проте повна відмова від багатомодових волокон є недоцільною, адже вони значно дешевші у виробництві та простіші в експлуатації. Для покращення їхніх характеристик було розроблено технологію створення градієнтного профілю показника заломлення у сердцевині. На відміну від стандартних волокон із «ступінчастим» профілем, де межа між сердцевиною і оболонкою є різкою, у градієнтному волокні показник заломлення поступово зменшується від центру до периферії.

Завдяки цьому фізичному ефекту промінь, що рухається зигзагоподібно, частину шляху проходить у зовнішніх шарах волокна, де швидкість поширення світла вища (оскільки показник заломлення нижчий). Водночас промені, які рухаються майже прямолінійно по центру сердцевини, долають свій шлях із дещо меншою швидкістю. У результаті час прибуття сигналів вирівнюється, і модова дисперсія суттєво зменшується.

Таким чином, градієнтний профіль дозволяє значно покращити якість роботи багатомодових волокон, забезпечуючи можливість передавання сигналу на більші відстані без критичного спотворення. Ця технологія є компромісом між дешевизною багатомодових систем та високими характеристиками одномодових, і

тому широко використовується у тих випадках, коли застосування одномодових волокон з економічних чи технічних причин є недоцільним.

Ще однією важливою проблемою, характерною для багатомодових оптичних волокон, є додаткове ослаблення сигналу, спричинене особливостями поширення світла. У багатомодових кабелях промені світла рухаються складними зигзагоподібними траєкторіями, багаторазово відбиваючись від межі між сердцевиною та оболонкою. Кожне таке відбиття супроводжується невеликими, але постійними втратами енергії: частина світлової хвилі проникає в оболонку й розсіюється. У підсумку, що довший шлях і що більше відбиттів відбувається, то помітнішими стають втрати сигналу та спотворення переданих даних.

Важливою закономірністю є те, що чим менше можливих траєкторій поширення світла всередині волокна, тим нижчий рівень таких втрат. Саме тому у волокнах із меншою кількістю мод сигнал зберігає свою потужність і форму значно краще, ніж у широкосердцевинних багатомодових кабелях. Цей принцип пояснює, чому одномодові волокна, де фактично існує лише один шлях для поширення світлового імпульсу, демонструють найкращі характеристики за якістю та дальністю передавання.

Щоб краще зрозуміти вплив модової дисперсії та додаткового ослаблення, наводять приклади волокон із різними діаметрами сердцевини. Наприклад, у кабелях типу HCS/PCS із діаметром сердцевини 200 мкм кількість можливих мод є надзвичайно великою. Це означає, що промені світла долають різні за довжиною траєкторії, прибувають до приймача в різний час, а при кожному відбитті втрачають частину своєї енергії. У результаті виникає комбінація двох негативних явищ: значної модової дисперсії та підвищеного рівня затухання.

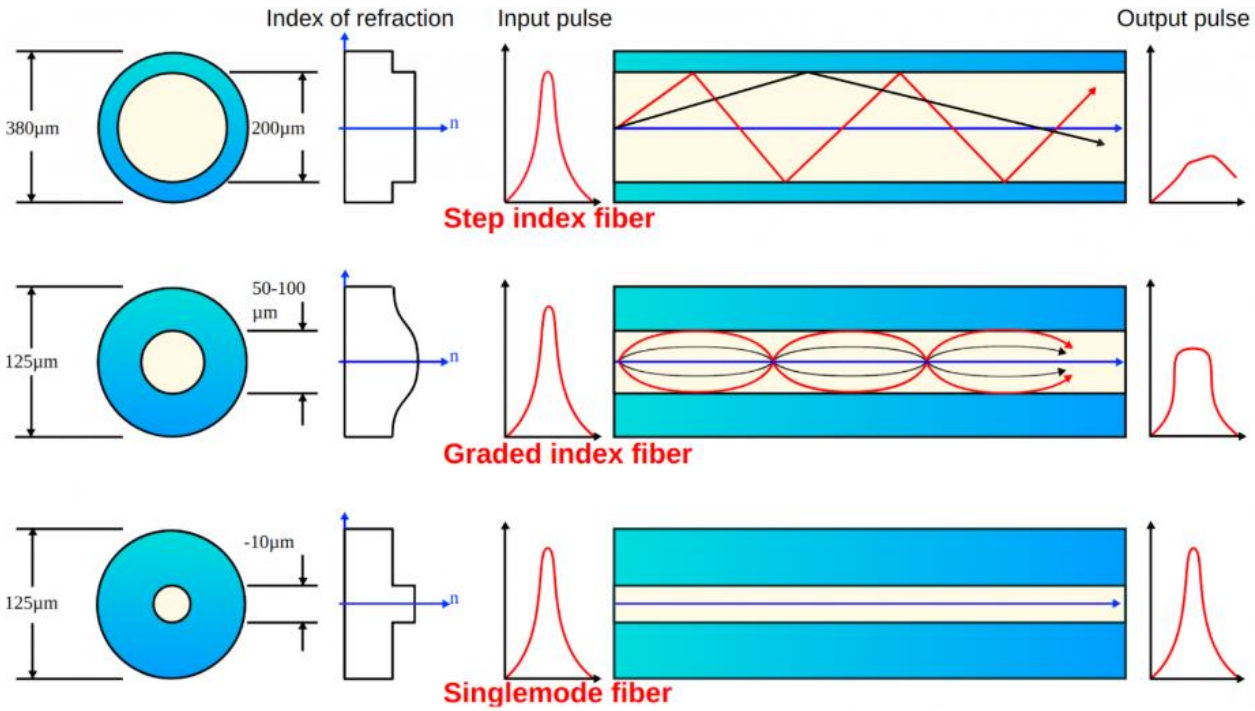


Рис. 1.3 Поширення світла у волокнах трьох розмірів

Для сучасних високошвидкісних телекомунікацій це є критичною проблемою, оскільки якість передавання безпосередньо залежить від стабільності сигналу. Тому багатомодові кабелі з великою сердцевиною сьогодні практично не використовуються у магістральних мережах, обмежуючись лише локальними інсталяціями з невеликими відстанями.

1.3 З’єднання та мультиплексування в каналх зв’язку

У волоконно-оптичних системах якість сигналу визначається не лише характеристиками самого волокна, але й точністю обробки на його кінцях. Під час з’єднання двох відрізків кабелю завжди виникають додаткові втрати, пов’язані з мікроскопічною повітряною прошаркою на стику та ефектом зворотного відбиття світла. Частина сигналу повертається у бік передавача, що призводить до шумів, зниження рівня потужності та можливих спотворень. Ці втрати особливо відчутні у високошвидкісних мережах, де навіть незначне погіршення параметрів може суттєво вплинути на якість передавання даних.

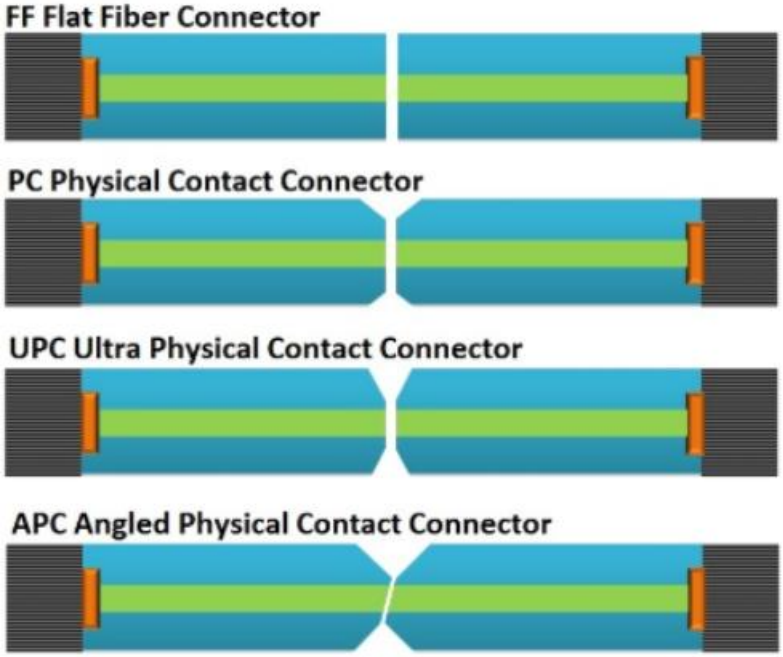


Рис. 1.4 Види торців оптоволокна

Щоб мінімізувати ці негативні явища, у практиці застосовують технології полірування торців волокон, які забезпечують максимально щільний контакт та правильне проходження світлового сигналу. Залежно від вимог до системи та умов експлуатації використовуються різні варіанти полірування: PC, SPC, UPC та APC.

- **PC (Physical Contact, фізичний контакт)** — базова технологія полірування, яка з'явилася першою. Кінці волокон шліфуються так, щоб утворювати сферичну поверхню. Це забезпечує безпосередній контакт сердцевин, але не гарантує мінімізації відбиттів. Для PC характерні відносно високі зворотні втрати, тому сьогодні цей тип майже не використовується в нових інсталяціях, але може зустрічатися у старих мережах.
- **SPC (Super Physical Contact, суперфізичний контакт)** — удосконалення PC-полірування. Завдяки більш ретельному шліфуванню торці стають гладшими, що значно зменшує коефіцієнт зворотного відбиття. Цей тип з'єднань вважається надійнішим і довговічнішим, особливо для систем середнього рівня вимог.
- **UPC (Ultra Physical Contact, ультрафізичний контакт)** — подальший розвиток технології PC. Торці волокон обробляються з максимальною точністю, забезпечуючи практично ідеальну геометрію та ще менші відбиття.

Рівень зворотних втрат у UPC-поліруванні значно нижчий, ніж у PC і SPC. Саме ця технологія стала найпоширенішою у сучасних волоконно-оптичних лініях зв’язку, оскільки поєднує високу якість сигналу та відносну економічність.

- **APC (Angled Physical Contact, кутовий фізичний контакт)** — найбільш досконала технологія. На відміну від інших типів, полірування виконується під кутом (зазвичай 8°). Завдяки цьому відбитий сигнал не повертається у сердцевину, а відводиться в оболонку волокна, повністю усуваючи ефект повторного попадання сигналу на джерело. Це забезпечує мінімальні зворотні втрати серед усіх типів полірування. APC-з’єднання використовуються у найвідповідальніших сферах — кабельному телебаченні (CATV), аналогових системах передавання сигналів, оптичних сенсорах та в усіх додатках, де критично важливий контроль над відбиттям.

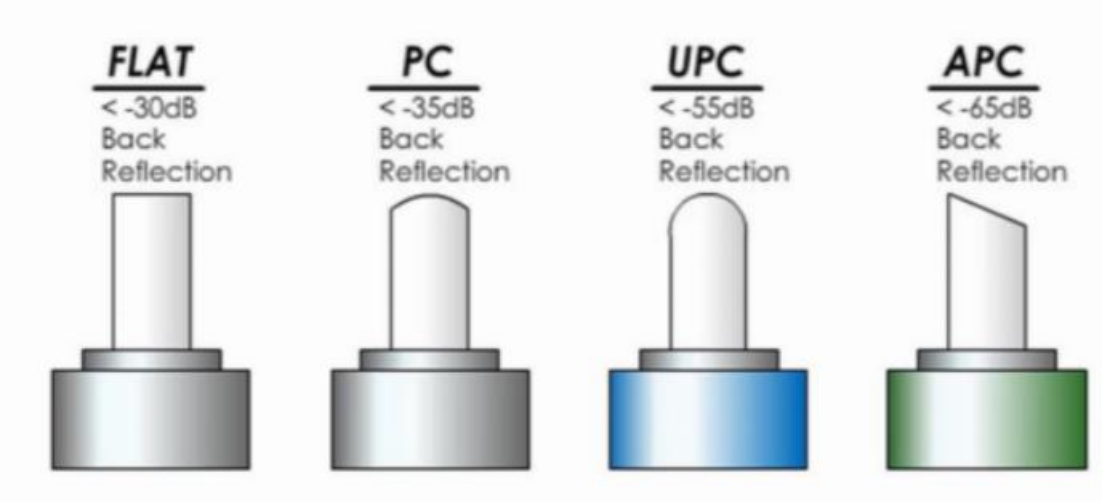


Рис. 1.5 Види торців оптоволокна

Завдяки розвитку цих технологій стало можливим забезпечити стабільність і довговічність роботи волоконно-оптичних систем. Якщо UPC сьогодні є стандартом для більшості телекомунікаційних мереж, то APC вважається спеціалізованим рішенням для високоточних систем. Таким чином, правильний вибір типу полірування дозволяє досягти балансу між вартістю обладнання, якістю сигналу та вимогами конкретної мережі.

Технологія спектрального ущільнення каналів (WDM)

Технологія WDM (Wavelength Division Multiplexing — спектральне ущільнення каналів) стала однією з ключових у розвитку волоконно-оптичних систем зв’язку. Вона дозволяє значно підвищити ефективність використання одного оптоволокна завдяки передаванню кількох незалежних світлових сигналів одночасно, кожен з яких має власну довжину хвилі. По суті, WDM перетворює одне волокно на багатоканальне середовище, здатне обслуговувати десятки чи навіть сотні паралельних потоків даних.

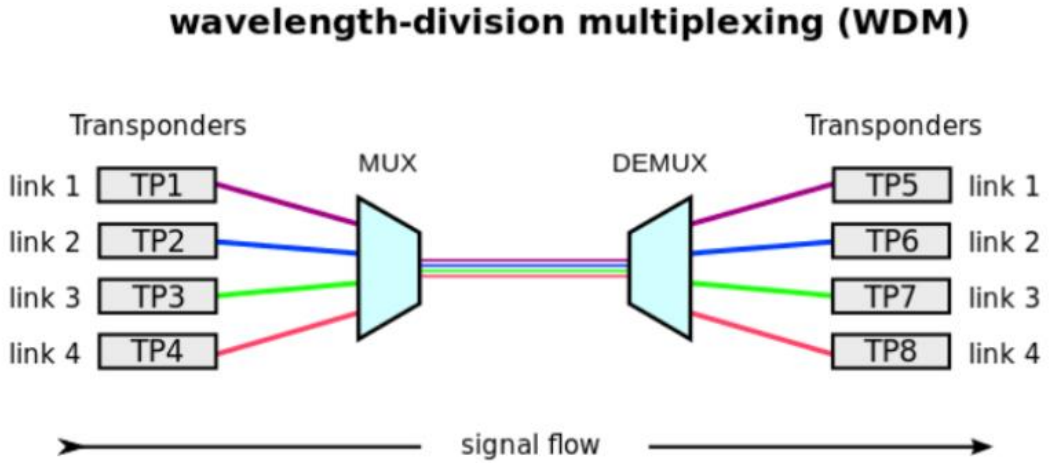


Рис. 1.6 Технологія WDM

Принцип дії технології полягає в тому, що у складі трансиверів встановлюються транспондери, які формують світлові сигнали на заданих довжинах хвиль. Далі мультиплексор об’єднує всі ці сигнали в єдиний оптичний потік, який передається по волокну. На приймальній стороні демультиплексор виконує зворотну операцію — розділяє загальний потік на окремі канали, відновлюючи їх у первинному вигляді. Завдяки такому підходу з’явилася можливість багаторазово збільшувати пропускну здатність мереж без необхідності прокладання додаткових кабелів.

Різновиди технології WDM

На сучасному етапі розвитку телекомунікацій виділяють кілька основних варіантів спектрального ущільнення:

- **Базове WDM**

  Це початковий варіант технології, який дозволяє передавати два незалежні канали з довжинами хвиль 1310 нм та 1550 нм. Найчастіше його застосовують

для організації двонаправленого зв’язку по одному волокну. Окрім цього, базове WDM може використовуватись для збільшення пропускної здатності існуючих систем без суттєвих змін інфраструктури.

- **CWDM (Coarse WDM — грубе спектральне ущільнення)**
  Є наступним етапом розвитку базового WDM. Завдяки цій технології весь спектр ділиться на 18 каналів у діапазоні від 1270 до 1610 нм із кроком між каналами 20 нм. Хоча CWDM не забезпечує дуже великої дальності через підвищене затухання, воно є вигідним рішенням для міських і регіональних мереж, де важливим є баланс між вартістю обладнання та збільшенням пропускної здатності.
- **DWDM (Dense WDM — щільне спектральне ущільнення)**
  Найбільш сучасна й продуктивна технологія. У системах DWDM відстань між несучими довжинами хвиль становить 50 або 100 ГГц (близько 0,8–0,4 нм). Це дозволяє розмістити у спектрі від 48 до 96 каналів, а в деяких випадках — ще більше. Завдяки такій щільності каналів досягається надзвичайно висока пропускна здатність, що робить DWDM базовим стандартом для магістральних мереж, міжконтинентальних каналів зв’язку та підводних кабелів.

Значення WDM у сучасних мережах

Впровадження WDM стало переломним моментом у розвитку телекомунікацій. Якщо на початкових етапах волоконно-оптичні системи могли передавати лише один канал по одному волокну, то завдяки спектральному ущільненню їхня ефективність зросла у десятки та сотні разів.

- **Базове WDM** стало поштовхом до розширення можливостей існуючих ліній без необхідності масштабної заміни інфраструктури.
- **CWDM** забезпечило створення відносно недорогих багатоканальних систем, що знайшли широке застосування у міських та корпоративних мережах.
- **DWDM** перетворило оптичні системи на основний інструмент глобальної комунікації, зробивши можливим передавання терабітних потоків даних на великі відстані з мінімальними втратами.

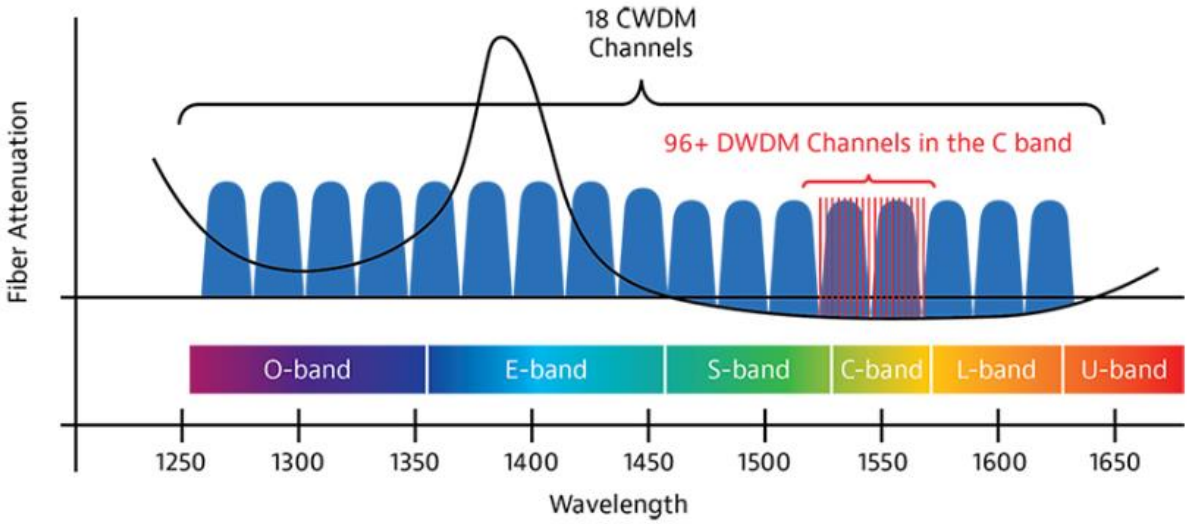


Рис. 1.7 Завдяки високій щільності каналів DWDM ефективно використовує ресурси оптоволокна

Завдяки WDM сьогоднішні телекомунікаційні мережі можуть масштабуватися майже необмежено, а пропускна здатність одного волокна використовується максимально ефективно. Саме тому ця технологія вважається основою сучасної та майбутньої інфраструктури Інтернету.

2 ВРАЗЛИВОСТІ ОПТОВОЛОКОННИХ КАНАЛІВ ЗВ'ЯЗКУ

2.1 Методи атаки на оптоволоконні канали зв'язку

Існує поширене уявлення, що оптичні волокна є повністю захищеним середовищем передавання даних. Однак на практиці це не зовсім так: волоконно-оптичні канали зв'язку уразливі до підключень і прослуховування. Сьогодні через них передається величезний обсяг конфіденційної інформації — від державних і військових комунікацій до фінансових операцій та корпоративних даних. І хоча ймовірність втручання невелика, ризик потрапляння такої інформації до сторонніх осіб із відповідними технічними ресурсами й обладнанням є цілком реальним.

Підключення до оптоволокна (fiber tapping) — це метод компрометації каналу, коли частина світлового сигналу вилучається для подальшого аналізу. Залежно від технічної реалізації розрізняють два типи:

- **Інтрузивне підключення** — вимагає фізичного втручання у волокно: його розрізають, а потім під'єднують до спеціального пристрою зчитування. Такий метод залишає сліди втручання і є відносно легшим для виявлення, проте він забезпечує повний доступ до даних.
- **Неінтрузивне підключення** — виконується без порушення цілісності волокна та без зупинки роботи сервісу. У цьому випадку сигнал знімається завдяки фізичним явищам, наприклад мікрозгинанню чи використанню ефектів розсіювання. Саме ці технології вважаються найбільш небезпечними, адже їх практично неможливо виявити звичайними засобами моніторингу.

Попри те, що такі втручання рідко документуються у відкритих джерелах, історія знає кілька підтверджених випадків, які показують реальність загрози:

- **2000 рік** — в аеропорту Франкфурта (Німеччина) виявлено несанкціоновані підключення до трьох магістральних ліній компанії **Deutsche Telekom**.
- **2003 рік** — на оптоволоконній мережі компанії **Verizon** знайдено підслуховуючий пристрій, що дозволяв знімати дані.

- **2005 рік** — підводний човен ВМС США **USS Jimmy Carter** був спеціально модернізований для здійснення прихованих підключень до підводних кабелів, що підтверджує зацікавленість державних структур у подібних методах контролю.

Ці приклади демонструють, що хоча оптичні мережі вважаються високозахищеним середовищем передавання даних, їх безпека не є абсолютною. Особливо складним є завдання виявлення місця підключення: навіть при інтрузивному втручанні сигнал втрачає мінімальну частку потужності, що в реальних мережах часто не сприймається як аномалія. Для неінтрузивних методів виявлення ще складніше, адже вони майже не впливають на якість каналу.

Сьогодні розробляються різні підходи до захисту волоконно-оптичних мереж від несанкціонованих підключень. Серед них:

- використання систем моніторингу цілісності волокна, які здатні фіксувати найменші зміни параметрів сигналу,
- застосування спеціальних протоколів шифрування, що роблять перехоплені дані непотрібними для зловмисника,
- розвиток технологій виявлення вторгнень на основі аналізу відбитих хвиль та розсіювання.

Таким чином, хоча випадки «прослуховування» оптоволокон залишаються поодинокими, загроза є реальною і потребує постійної уваги. Для забезпечення надійного захисту інформації в оптоволоконних мережах необхідне не лише використання сучасних методів шифрування, а й удосконалення фізичного рівня безпеки, який досі залишається однією з найвразливіших ланок системи.

Методи підключення до оптоволокна

А. Використання згинання волокна

Одним із найбільш поширених методів несанкціонованого підключення до оптоволоконних ліній є навмисне згинання волокна. Для його реалізації кабель розбирається до рівня оптичного волокна, після чого здійснюється контрольований вплив на його геометрію. Принцип дії цього способу базується на фізиці поширення світла всередині волокна, а саме на явищі повного внутрішнього відбиття. У

нормальних умовах промінь світла відбивається від межі сердцевини та оболонки під кутом, більшим за критичний, і не виходить за межі волокна. Якщо ж цей кут стає меншим від критичного, частина світлової енергії починає проникати крізь оболонку назовні, створюючи умови для перехоплення даних.

Штучне згинання оптичного волокна якраз і використовується для того, щоб змінити траєкторію руху світла, зменшити кут падіння і викликати витік інформації. За своєю природою це явище може мати два основні різновиди:

1. Мікрозгин

Мікрозгини виникають унаслідок локального прикладення зовнішнього зусилля, яке створює різке, але дуже мале за масштабом викривлення поверхні волокна. Такі деформації вимірюються мікронами і практично непомітні для людського ока. Незважаючи на малі розміри, вони викликають зсуви світлових променів та часткове розсіювання світла в оболонку. У результаті через таку «мікродеформацію» частина сигналу витікає і може бути використана спеціальними сенсорами для зняття інформації.

Мікрозгини особливо небезпечні тим, що вони можуть створюватися навіть без серйозного пошкодження кабелю — достатньо акуратно натиснути на оболонку або змінити її структуру. Це робить метод зручним для прихованих підключень, які складно виявити при звичайному контролі.

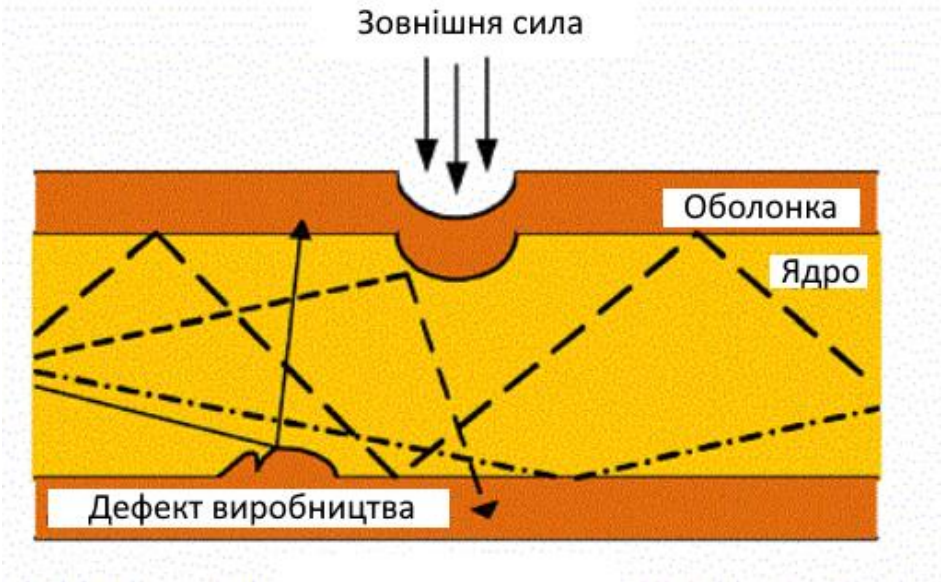


Рис 2.1 Мікрозгин

2. Макрозгин

На відміну від мікрозгинів, макрозгини являють собою помітніші деформації волокна, при яких його вигинають на певному радіусі. Для кожного типу оптичного волокна існує параметр, що визначає мінімально допустимий радіус згину, при якому передача сигналу відбувається без значних втрат. Якщо ж волокно зігнути сильніше, тобто зменшити цей радіус, відбувається вихід частини світлової енергії за межі сердцевини.

Цей витік світла можна зареєструвати й використати для зняття інформації. Наприклад, для одномодового волокна мінімальний радіус згину зазвичай становить 6,5–7,5 см (за винятком спеціалізованих моделей, стійких до вигинів). Для багатомодових волокон цей показник є ще меншим — приблизно 3,8 см. Таким чином, макрозгин дозволяє створити відносно стабільний канал витоку сигналу без порушення цілісності оптичної лінії.

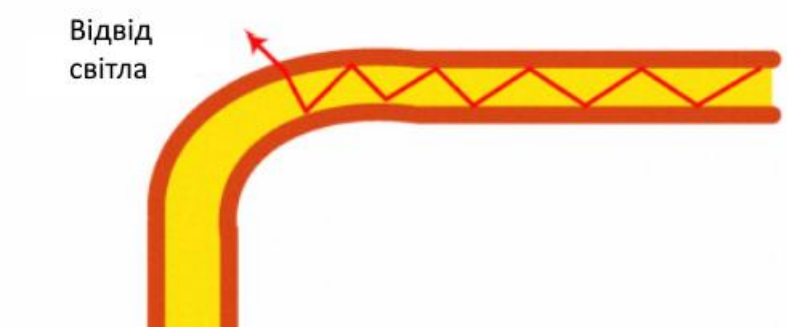


Рис. 2.2 Макрозгин

В. Оптичне розщеплення

Одним із класичних методів отримання доступу до сигналу є використання оптичного спліттера. Волокно розрізається та вбудовується у пристрій, який відводить частину світлового потоку. Цей спосіб належить до категорії інтрузивних методів, адже потребує порушення цілісності волокна. У більшості випадків це призводить до короткочасних збоїв у роботі каналу, що може бути зафіксовано системами моніторингу.

Попри це, належним чином виконане підключення такого типу може залишатися непоміченим протягом багатьох років, працюючи стабільно та без

явних слідів компрометації. Оптичне розщеплення часто використовується у легальних цілях, наприклад для організації розподілу сигналу, однак у випадку несанкціонованого застосування становить серйозну загрозу інформаційній безпеці.

C. Використання неоднорідних хвиль (Evanescent Coupling)

Цей метод є більш витонченим і належить до неінтрузивних технологій, хоча його реалізація є доволі складною. Принцип базується на явищі еванесцентного поля — слабкого електромагнітного випромінювання, яке поширюється за межами сердцевини волокна.

Для перехоплення сигналу оболонки волокна-джерела та волокна-приймача ретельно полірують до рівня сердцевини, після чого з'єднують їх максимально щільно. Частина світлової енергії із першого волокна завдяки еванесцентному полю передається у друге, створюючи можливість знімати дані.

У лабораторних умовах цей метод показує хороші результати, однак у реальних мережах він складний у виконанні через необхідність високоточного обладнання та делікатної механічної обробки.

D. V-подібний виріз (V-Groove Cut)

Ще один спосіб полягає у створенні спеціальної V-подібної виїмки в оболонці оптичного волокна. Виріз розташовують максимально близько до сердцевини й формують під таким кутом, що умови поширення світла змінюються. У результаті кут падіння променя відносно проекції вирізу перевищує критичне значення, що спричиняє порушення повного внутрішнього відбиття.

Частина світлового сигналу виходить через оболонку у ділянці вирізу та може бути зчитана відповідним обладнанням. Метод вважається інвазивним, адже потребує фізичної модифікації волокна, але він є відносно простим у реалізації й тому використовується як у легальних інженерних рішеннях, так і у прихованих підключеннях.

E. Використання розсіювання

Ще одним методом перехоплення інформації є експлуатація явища розсіювання світла в оптичному волокні. Для цього в сердцевині створюють

спеціальну періодичну структуру — Breггівську решітку. Вона формується шляхом впливу ультрафіолетових лазерних променів, які накладаються під певним кутом і створюють інтерференційну картину.

Breггівська решітка змінює показник заломлення сердцевини по довжині, що призводить до часткового відбиття світлового потоку назад або вбік. Отриманий відбитий сигнал може бути використаний для зчитування інформації.

Хоча цей метод потребує високоточного обладнання й більше підходить для лабораторних або дослідницьких умов, його потенційна небезпека полягає в тому, що він здатний забезпечувати довготривале перехоплення сигналу без суттєвого впливу на основний канал.

2.2 Моделювання методів

A. Методологія

Для проведення високоточної оцінки втрат, що виникають при згинанні оптичного волокна типу SMF-28, застосовується сучасний підхід, заснований на використанні повновекторного частотного розв’язувача рівнянь Максвелла. Даний метод реалізується на основі скінченно-елементного аналізу високого порядку та передбачає можливість адаптації граничних умов завдяки використанню спеціальних поглинаючих шарів. Це дозволяє максимально точно моделювати процес поширення світлових хвиль у деформованому хвилеводі та оцінювати їх взаємодію з навколишнім середовищем.

У ході моделювання були отримані векторні розподіли електричних полів мод, а також значення констант поширення для різних сценаріїв деформації волокна. Особлива увага приділяється аналізу фундаментальної моди, яка визначає основні характеристики передавання сигналу. Рівень втрат обчислюється на основі уявної складової константи поширення цієї моди, що дозволяє кількісно оцінити зниження потужності сигналу при згині.

Загальні втрати системи розраховуються як сума втрат, обумовлених як базовою, так і ортогональною модою. Це дає змогу отримати більш повну картину

впливу згинання на параметри передавання. Проведені експерименти та порівняння з відомими результатами показали, що застосований метод забезпечує високу точність розрахунків і може використовуватися як достовірний інструмент для аналізу втрат у волоконно-оптичних лініях

B. Вихідні дані для моделювання

Для виконання чисельного аналізу використовувались параметри стандартного одномодового оптичного волокна SMF-28, що широко застосовується у телекомунікаційних мережах. Основні характеристики такі:

- сердцевина волокна: радіус — 4,15 мкм; показник заломлення — 1,4493;
- оболонка волокна: радіус — 62,25 мкм; показник заломлення — 1,444;
- зовнішнє середовище (повітря): коефіцієнт заломлення приймається рівним 1.

Ці параметри були покладені в основу математичної моделі та дозволили дослідити вплив геометричних і фізичних властивостей волокна на рівень втрат у випадку згину.

C. Розрахунок втрат потужності

У процесі моделювання було враховано, що радіус кривизни волокна задається відносно осі **x**, тоді як поляризація моди відбувається вздовж осі **y**, а поширення сигналу здійснюється по осі **z**. Такий підхід дозволяє детально відобразити просторові особливості поведінки світлового сигналу у викривленому хвилеводі та оцінити закономірності його затухання.

Схематична ілюстрація конфігурації згину волокна наведена на рисунку 2.3. Вона демонструє розташування осей, напрямок поширення сигналу та геометрію деформації, що безпосередньо впливає на параметри дисперсії та величину втрат.

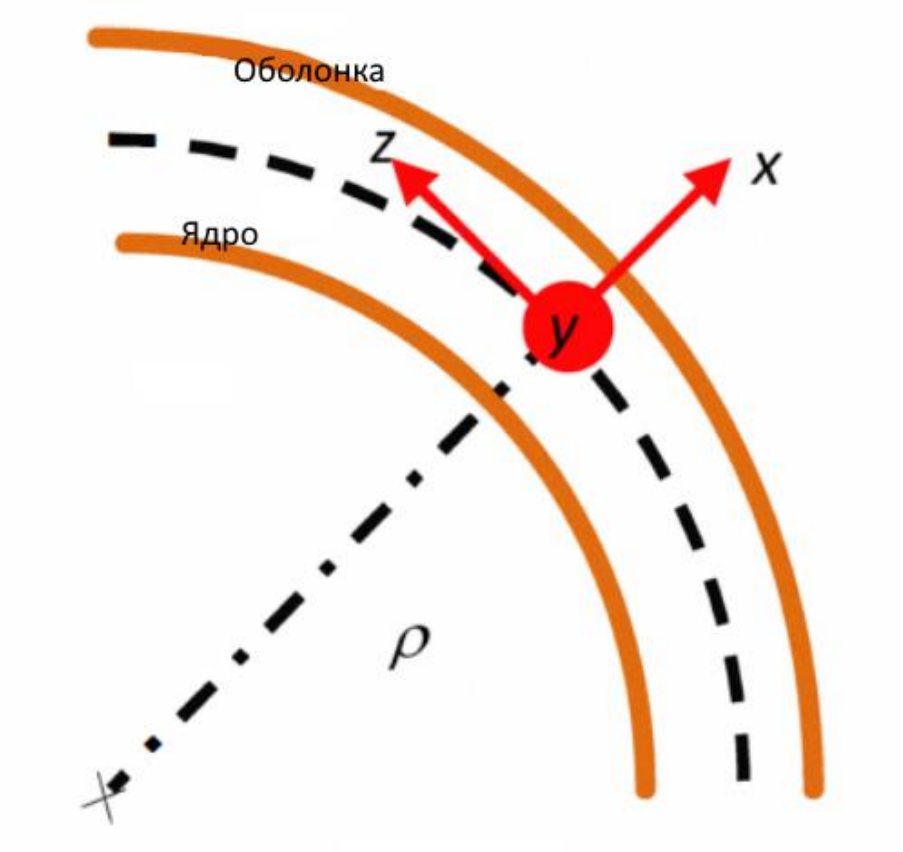


Рис. 2.3 Конфігурація згину волокна

Розраховані дані дозволяють встановити залежність між радіусом згину, параметрами мод і рівнем енергетичних втрат. Це, у свою чергу, дає можливість оптимізувати проєктування оптичних ліній зв’язку, враховуючи обмеження на мінімально допустимі радіуси вигину для забезпечення надійності й стабільності передавання сигналу.

Рисунок 2.4 демонструє залежність рівня втрат оптичного сигналу при згині від величини радіуса викривлення для відрізка волокна довжиною один метр. З аналізу результатів спостерігається чітка логарифмічна залежність: при зменшенні радіуса згину інтенсивність втрат зростає експоненціально, тоді як зі збільшенням радіуса — різко знижується.

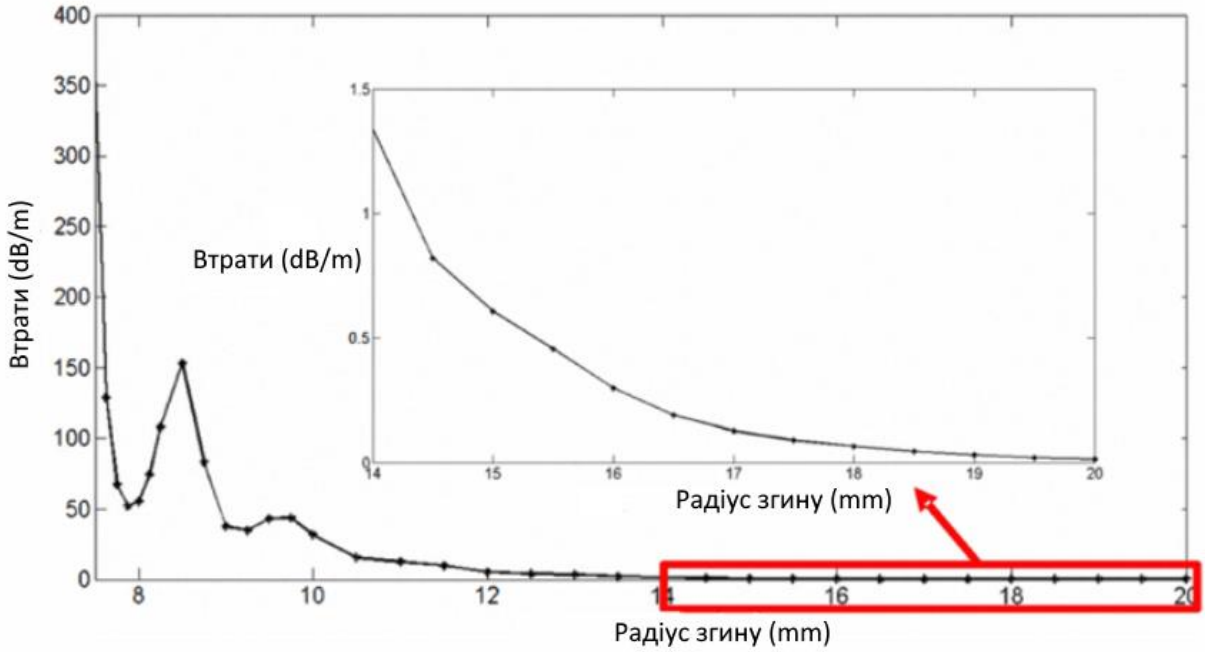


Рис. 2.4 Чисельна оцінка втрати на вигині, як функції від радіусу згину

При дуже малих радіусах кривизни (ρ < 10 мм) втрати перевищують 40 дБ/м, що фактично унеможливлює якісну передачу сигналу. У таких умовах оптичне випромінювання масово виходить за межі сердцевини, переходячи в оболонку та розсіюючись у навколишнє середовище. Це явище супроводжується різким падінням потужності сигналу, появою шумів і зниженням пропускної здатності лінії.

Для середніх і великих радіусів викривлення ситуація істотно змінюється. При значеннях (ρ > 15 мм) втрати стають мінімальними та не перевищують 1 дБ/м, що відповідає нормальним експлуатаційним умовам. Саме тому у специфікаціях до волоконно-оптичних кабелів завжди вказуються допустимі радіуси вигину, які забезпечують баланс між гнучкістю кабелю та стабільністю передавання сигналу.

З практичної точки зору, ця залежність має критичне значення для проєктування та прокладання волоконно-оптичних ліній зв’язку (ВОЛЗ). Умови експлуатації — прокладання у кабель-каналах, колекторах чи під землею — часто вимагають вигинання кабелю. Якщо ці вигини не врахувати або виконати їх із порушенням мінімальних радіусів, мережа може зазнати серйозних втрат пропускної здатності й швидкості передавання.

Мета і загальна ідея.

Метою дослідження було показати на рівні концепції, наскільки теоретично можлива витік інформації з оптичного каналу та які типи даних у такому випадку можуть бути відновлені. Робота розглядає логічні етапи — фіксацію частини оптичного потоку, перетворення сигналу в електричну форму, розпізнавання протоколів і програмну обробку для відновлення прикладних даних (наприклад, фрагментів відеопотоку). Це опис аналітичного характеру, а не інструкція з реалізації втручання.

Опис експериментальної схеми.

У лабораторних умовах моделювали канал «джерело — середовище передачі — приймач» і в межах контрольованої ділянки фіксували частину переданого оптичного сигналу. Захоплений трафік зберігався у форматі дампу (.pcap) і підлягав подальшому аналізу: розпізнаванню рівнів мережевих протоколів, виділенню потоків і реконструкції прикладових даних за допомогою доступних інструментів. У звіті розглянуто, який обсяг інформації та яких типів може бути витягнутий при сприятливих умовах.

Процедура обробки зібраних даних.

Захоплені мережеві кадри аналізувалися для виділення MAC- і IP-адрес, ідентифікації протоколів та екстракції пакетів прикладного рівня. Отримані дампи використовувалися для спроби відновлення мультимедійного потоку та інших об’єктів, причому оцінювалися фактори, що впливають на якість реконструкції (співвідношення сигнал/шум, втрачені пакети, синхронізація).

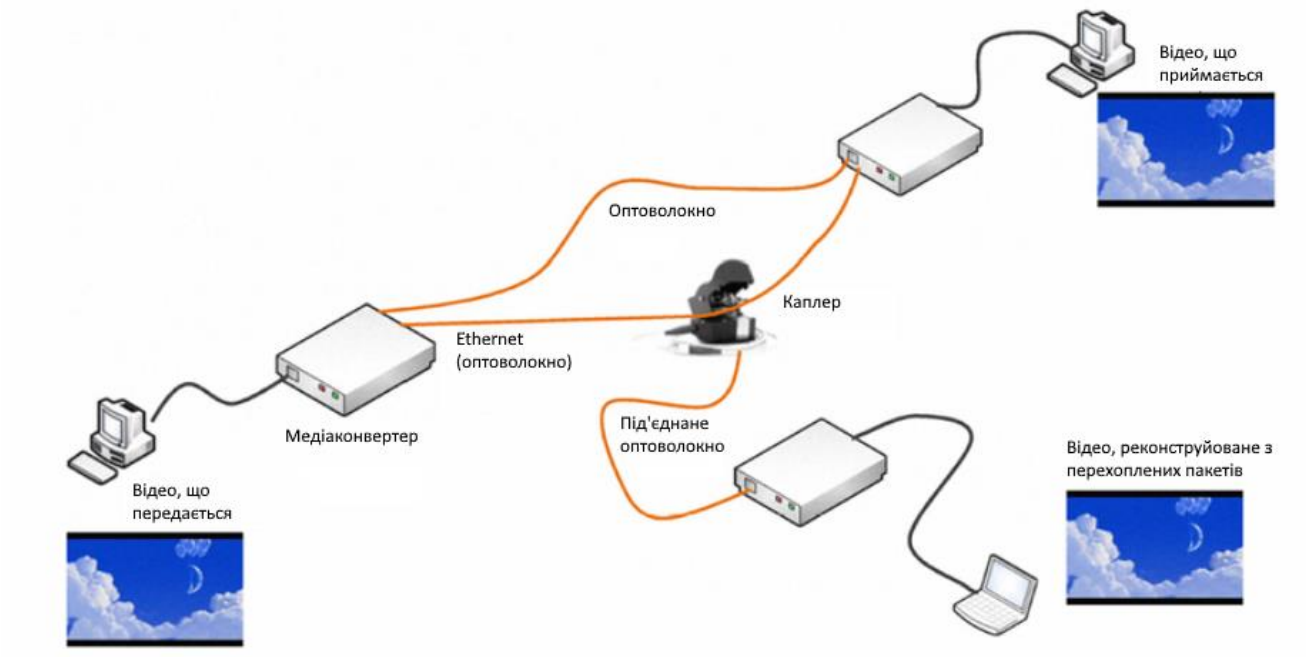


Рис. 2.5 Експериментальна схема для приєднання до волокна методом зигину

Результати і обмеження.

Експеримент показав, що за сприятливих умов частина прикладних даних (наприклад, фрагменти відеопотоку) може бути реконструйована з дампів трафіку, а також вилучені метадані (адреси, сигнальна інформація). Водночас якість і повнота відновлення значною мірою залежать від рівня захопленого сигналу та ступеня його пошкодження: у реальних мережах фрагментарність і фонові шумові явища часто ускладнюють коректну реконструкцію. Також підкреслено, що тривале і непомітне перехоплення на практиці ускладнене фізичними й експлуатаційними факторами.

Можливі наслідки.

Аналіз демонструє потенційну загрозу витоку конфіденційної інформації через уразливості фізичного рівня зв’язку, що робить актуальними заходи з підвищення фізичної безпеки каналів та застосування наскрізного шифрування.

2.3 Подальші сценарії

Експеримент, описаний у цьому розділі, виконувався з використанням компонентів Ethernet через їхню найбільшу доступність і простоту застосування.

Водночас деякі сценарії, що можуть трапитися у реальних умовах, цілком можуть мати вигляд, поданий нижче:

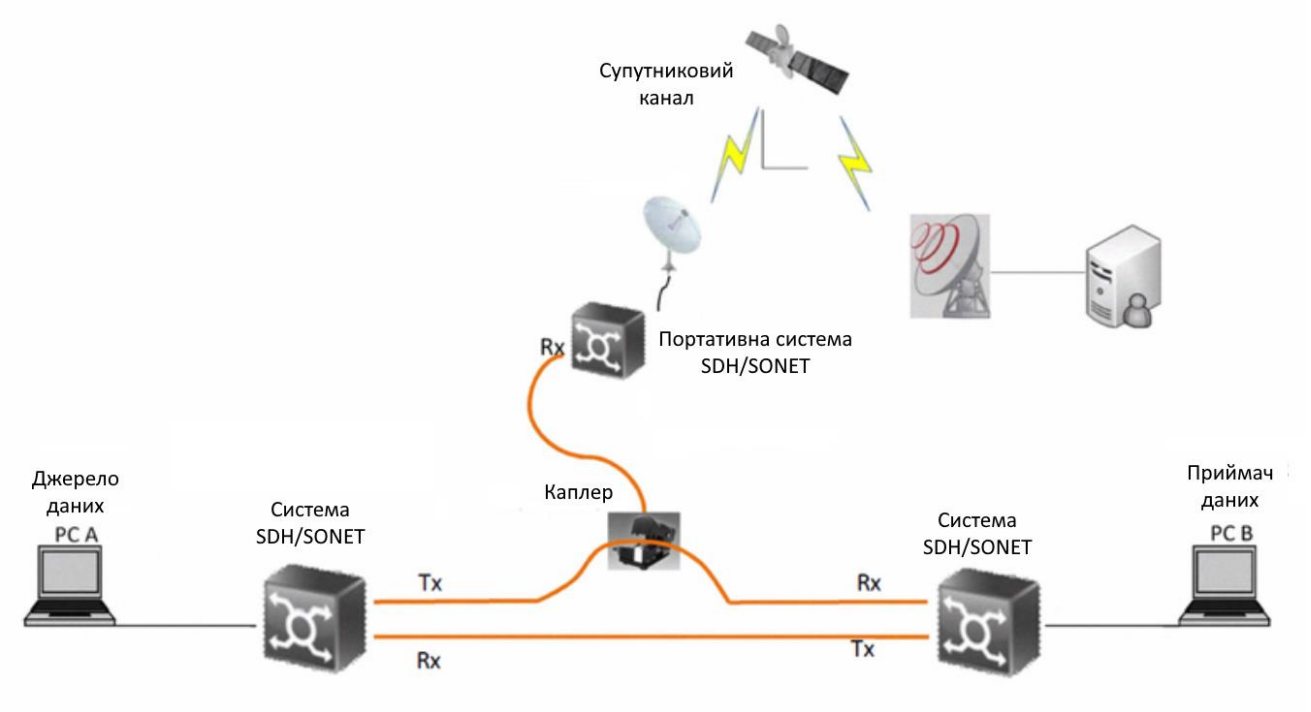


Рис. 2.6 Сценарій підключення з віддаленою обробкою

У магістральних і метромережах значний обсяг критичного трафіку проходить через стандарти SDH/SONET. Завдяки структурі мультиплексування (наприклад, контейнерам VC-4) з оптичного потоку теоретично можна виділяти нижчі рівні трафіку, хоча їхнє збереження й подальша обробка ускладнені через дуже високу пропускну здатність каналів. Для таких випадків доцільно використовувати віддалену обробку даних, яка вирішує дві ключові проблеми: по-перше, потребу у значних сховищах, адже захоплені потоки на швидкостях у кілька Гбіт/с швидко заповнюють диски; по-друге, можливість централізувати роботу мережевих фахівців, які замість польових умов отримують доступ до даних у спеціалізованому центрі з необхідними ресурсами.

Сценарії віддаленої обробки можуть реалізовуватися в різних формах:

1. **Використання бездротових каналів.** При застосуванні Wi-Fi або інших локальних бездротових технологій комп’ютер для збору даних може розташовуватися за межами будівлі чи в окремому транспортному засобі, а експерт працює дистанційно, маючи доступ до потрібних ресурсів.

2. **Передача через мікрохвильові чи супутникові лінії.** У модифікованих схемах дані можуть бути переадресовані на супутниковий або інший високошвидкісний канал для подальшої пересилки в центр обробки (*Рисунок 6*). Це зручно в умовах ізоляції або обмеженого доступу до наземної інфраструктури.
3. **Теоретичне введення або модифікація сигналу.** Наукові роботи описують можливість впливу на оптичний канал шляхом розсіювання або ін’єкції контрольованого сигналу. Такі сценарії важливі для аналізу ризиків, адже можуть стосуватися створення перешкод або навіть спроби модифікації передаваних даних.

Разом з тим, усі ці варіанти обмежені низкою факторів: потребою у високій пропускній здатності для передавання великих масивів інформації, ризиком фрагментарності та шуму у вилучених потоках, а також наявністю сучасних систем моніторингу (OTDR, аналіз відбиттів), що робить непомітне втручання малоймовірним. Саме тому першочергову увагу слід приділяти профілактичним заходам: наскрізному шифруванню трафіку, постійному контролю цілісності волокон, використанню броньованих кабелів і тампер-детекторів, організації централізованих систем збору з логуванням доступу, а також регулярним аудитам і навчанню персоналу.

Підключення з віддаленою обробкою

Існує два ключові чинники, які роблять віддалену обробку даних доцільною при підключенні до віддалених високошвидкісних каналів (кілька Гбіт/с). По-перше, роль сховища стає критично важливою: захоплені пакети дуже швидко заповнюють дисковий простір. По-друге, залучення мережевих експертів для роботи в польових умовах часто дорого й незручно — набагато ефективніше організувати глибоку аналітику в віддаленому центрі обробки, де є спеціалізоване обладнання й великі обчислювальні та дискові ресурси.

За допомогою уяви можна побудувати різні сценарії віддаленої обробки. Наприклад:

1. **Використання бездротового інтернету.** При застосуванні Wi-Fi комп’ютер для збору даних може розташовуватися в іншій кімнаті або в окремому фургоні за межами будівлі, де знаходиться кабель. Фахівець у віддаленому центрі отримує доступ до ресурсів і працює віддалено з накопиченими даними.
2. **Переадресація через мікрохвильовий або супутниковий канал.** В експериментальній схемі трафік може бути спрямований на захищений супутниковий або інший радіоканал для подальшої пересилки в центр обробки.
3. **Інжекція сигналу (теоретично).** Теоретично, на основі методів розсіяння можна уявити пристрої, які вводять у волокно контрольовані сигнали або шуми шляхом модифікованих схем оптичного каплінгу (coupling). Такі сценарії розглядаються в науковому дискурсі як потенційні загрози або тестові методи оцінки стійкості мережі — їхня практична реалізація вимагає значних технічних ресурсів і має підлягати строгим етичним і правовим обмеженням.

Захист від підключень

Існують три основні категорії методів, що дозволяють запобігати несанкціонованим підключенням або зменшувати їхній вплив.

А. Спостереження за кабелем і моніторинг

1. **Моніторинг контрольних сигналів у додаткових волокнах.**

   Виробляють кабелі з однією або кількома резервними нитками, по яких постійно передається спеціальний контрольний сигнал. Будь-яка спроба згину або механічного втручання викликає зміну або втрату цього сигналу, що призводить до генерації тривоги. Недолік — підвищена вартість таких кабелів.
2. **Електричні провідники в конструкції кабелю.**

   Вбудовування електричних жил у структуру кабелю дозволяє фіксувати порушення оболонки: зміна електричної ємності або провідності між жилами може слугувати тригером для сигналізації про пошкодження.

3. **Моніторинг розподілу потужності по модах.**

   У багатомодових волокнах рівень затухання залежить від моди, в якій поширюється світло. Спроба підключення зазвичай впливає на певні моди й одночасно змінює енергетичний баланс між провідними й непровідними модами. Аналіз зміни співвідношення потужностей у серцевині та оболонці може бути використаний як індикатор стороннього втручання.

4. **Вимірювання оптично значимої потужності.**

   Постійний контроль рівня оптичної потужності у волокні дозволяє виявляти відхилення від очікуваного значення. Для цього корисно передавати по кабелю службовий (пілотний) сигнал або підтримувати певний постійний рівень потужності, що робить аномалії більш помітними. Такий підхід вимагає спеціальної кодування/структури сигналу.

5. **Оптичні рефлектометри (OTDR).**

   Оскільки підключення забирає частину оптичного потоку або змінює оптичні відбиття, за допомогою OTDR можна визначити місце, де спостерігається падіння рівня сигналу або аномальна рефлексія по трасі. Це дозволяє локалізувати потенційні місця втручання.

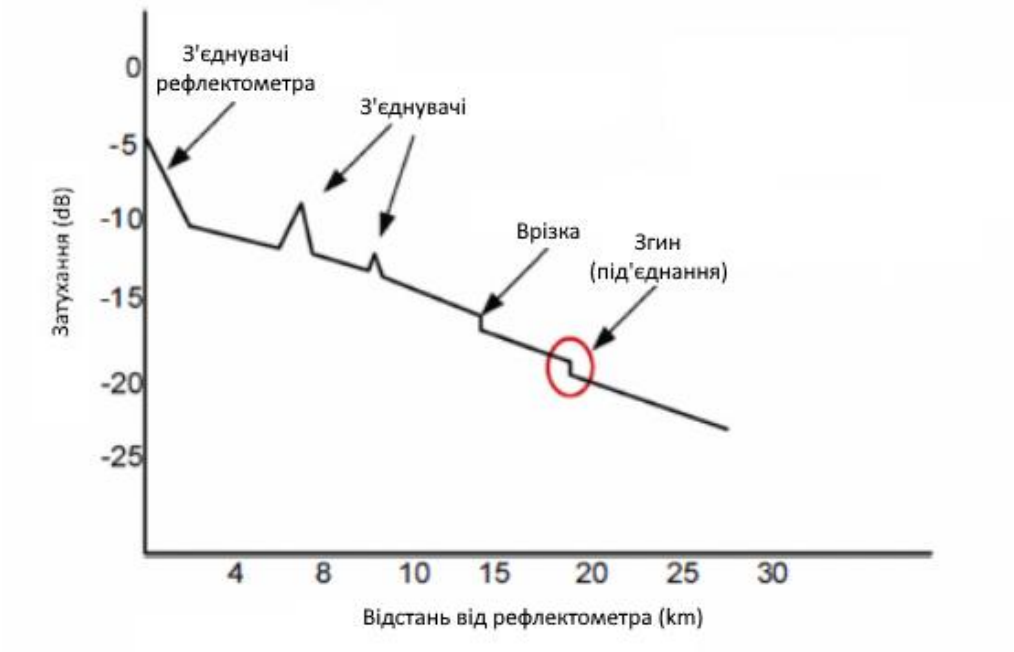


Рис. 2.7 Пошук підключення на оптичній трасі за допомогою оптичного рефлектометра

6. **Методи з використанням пілотного тону.**

   Пілотні тони передаються по волокну разом із комунікаційними даними і можуть застосовуватися для виявлення порушень у передачі. Однак якщо супутні частоти пілотних тонів не зачіпаються під час атаки, цей метод виявиться неефективним; факт підключення можна судити по суттєвому погіршенню рівня пілотного тону.

B. Волокно з підвищеною стійкістю до згинів (bend-insensitive fiber)

Спеціальні типи оптичного волокна, стійкі до сильного згину, зменшують втрати при механічних впливах (згин, натяг, перекручування), ускладнюючи отримання корисного витоку світла шляхом простих маніпуляцій. Існують також інші технології та конструкції, що підвищують механічну стійкість і знижують чутливість до зовнішніх впливів.

C. Шифрування

Шифрування саме по собі не перешкоджає фізичному підключенню до волокна, але робить перехоплені дані практично марними для зловмисника без ключів. Шифрування умовно ділять на рівні:

1. **Шифрування третього рівня (наприклад, IPsec).**

   Реалізується на кінцевих пристроях або на транспортному/мережевому рівні й забезпечує захист прикладного трафіку. Недоліки — додаткові затримки та складність впровадження при великій кількості мережевих елементів.

2. **Шифрування другого рівня.**

   Виконується нижче рівня мережі (наприклад, на канальному рівні). Одне із можливих рішень — оптичні варіанти CDMA (O-CDMA), які в деяких умовах підвищують складність коректного відновлення даних з точки зору атак методом грубої сили. Проте ефективність таких методів сильно залежить від системного дизайну, співвідношення сигнал/шум та параметрів реалізації; покращення коду може підвищити складність злому, але не робить систему абсолютно невразливою.

3 ПРИХОВАНІ КАНАЛИ ЗВ’ЯЗКУ

3.1 Абстрактні анонімні мережі

Сучасне суспільство неможливо уявити без сервісів зв’язку та цифрових платформ, що фактично перетворилися на складову критичної інформаційної інфраструктури. Соціальні мережі, месенджери, електронна пошта, хмарні сховища — усе це є інструментами повсякденного використання, від яких залежить функціонування бізнесу, державних структур і приватного сектору. Водночас саме вони акумулюють величезні масиви чутливої інформації, що робить їх стратегічними об’єктами для контролю, моніторингу та потенційного зловживання.

У цьому контексті формується своєрідна подвійність: користувачі отримують зручність і продуктивність, а сервіси — дані, що перетворюються на економічний і політичний ресурс. Такий взаємозв’язок уже не можна розглядати лише як симбіоз — він набуває ознак паразитизму, де сторони взаємно залежать, але водночас виснажують одна одну. На початкових етапах розвитку цифрової екосистеми користувачі справді виступали споживачами ресурсів сервісів. Проте сучасна модель взаємодії свідчить про інше: саме сервіси централізують контроль і формують монопольні структури, що починають жити за рахунок клієнтів, використовуючи їхній цифровий слід як базовий ресурс.

Цей процес має небезпечні наслідки для критичної інфраструктури. Сервіси об’єднують дані між собою, створюючи закриті «екосистеми», які нагадують картелі. Користувацька інформація може циркулювати від одного постачальника до іншого практично безконтрольно, що призводить до зростання ризиків витоку, маніпуляцій та інформаційних атак. Відомими є випадки, коли теми приватних розмов в офлайн-середовищі швидко відображалися у вигляді реклами в онлайн-сервісах, або коли переписка в одній соціальній мережі призводила до появи цільового контенту в іншій. Така інтеграція становить реальну загрозу інформаційній безпеці держави, бізнесу та громадян.

Особливо небезпечним є поступове зрощування економічної потужності цих платформ із політичним впливом. Централізовані сервіси, перетворюючись на монополістів, отримують можливість формувати громадську думку, розширювати сфери контролю та інтегруватися з державними інститутами. Це створює умови, за яких критична інфраструктура втрачає незалежність, а надмірна концентрація інформації в руках обмеженого кола компаній загрожує як національній безпеці, так і правам користувачів.

У підсумку можна стверджувати, що сучасні комунікаційні сервіси є не лише ключовою частиною цифрової екосистеми, але й джерелом стратегічних ризиків. Вони фактично стали «паразитами» у глобальному масштабі, оскільки, забезпечуючи базові потреби користувачів, одночасно акумулюють і монетизують дані, створюючи залежність, з якої складно вийти.

Єдиним шляхом зниження цих ризиків є впровадження захисних механізмів критичної інфраструктури: застосування клієнт-безпечних сервісів зі сквозним шифруванням, використання анонімних мереж і прихованих каналів зв’язку, а також розробка національних і наднаціональних стратегій кібербезпеки, спрямованих на захист цифрового простору від надмірної концентрації даних і потенційних загроз.

Альтернативи та можливі рішення

Попри відсутність повноцінних замін централізованим сервісам, існує низка технологічних рішень, які можуть суттєво знизити рівень ризиків для критичної інформаційної інфраструктури.

1. **Клієнт-безпечні застосунки.**

   Вони забезпечують захист комунікацій за рахунок шифрування і автентифікації виключно на стороні клієнта. Це означає, що навіть якщо дані передаються через сервер або зберігаються на ньому, сервіс не здатен їх розшифрувати чи модифікувати. Найбільш відомим прикладом є застосування наскрізного (end-to-end) шифрування. Такі рішення вже реалізовані у програмному забезпеченні на кшталт RetroShare, Freenet, Bitmessage.

2. **Анонімні мережі.**

   Їх головна перевага — приховування як факту передачі даних між вузлами, так і самого зв’язку між відправником і отримувачем. На відміну від клієнт-безпечних застосунків, анонімні мережі зосереджені виключно на маршрутизації. Проте їхня ефективність зростає у поєднанні з end-to-end шифруванням, що забезпечує одночасно і анонімність, і конфіденційність. Прикладами є Tor, I2P, Mixminion.

3. **Приховані канали зв’язку.**

   Вони не є самостійним рішенням, а виступають як надбудова над клієнт-безпечними застосунками чи анонімними мережами. Їхня ключова особливість — можливість інтегруватися у вже існуючі канали зв’язку, роблячи їх стійкішими до атак та перехоплення. Класичним прикладом є використання PGP/GPG: інформація шифрується локально і передається через централізовані сервіси, але в захищеному вигляді. Ще цікавішою є комбінація прихованих каналів із анонімними мережами, що відкриває нові перспективи для розвитку безпечних комунікацій у масштабах критичної інфраструктури.

У сучасних дослідженнях телекомунікацій приховані канали зв’язку часто розглядаються як ефективний інструмент підвищення захищеності вже існуючих комунікаційних систем — як централізованих, так і децентралізованих. Вони дозволяють інтегрувати додатковий рівень конфіденційності без радикальної зміни архітектури мережі. Проте виникає логічне питання: чи можливо створити настільки універсальну систему, яка забезпечувала б не лише збереження даних, а й повну анонімізацію трафіку, незалежно від зовнішніх умов функціонування мережі?

Відповідь на це запитання лежить у концепції так званих абстрактних анонімних мереж. На відміну від традиційних рішень, що мають чіткі обмеження за кількістю вузлів, вимогами до маршрутизації чи залежністю від IP-адрес, абстрактна анонімна мережа гіпотетично ігнорує такі чинники. Для неї не є критичними:

1. рівень централізації чи децентралізації мережевої структури;
2. відкритість або відомість IP-адрес користувачів;
3. наявність або відсутність класичної маршрутизації;
4. кількість вузлів у мережі та їхня топологія;
5. відключення або вихід з ладу окремих вузлів;
6. варіації швидкості передавання трафіку.

З погляду сучасних технологій, поєднання всіх перелічених властивостей видається практично недосяжним. Проте гіпотетичне існування таких мереж відкриває нові горизонти у сфері захисту критичної інфраструктури.

Завдяки своїй абстрактності такі мережі здатні функціонувати не лише у класичних середовищах комунікації, а й інтегруватися у приховані канали зв'язку, що дозволяє видозмінювати сам спосіб взаємодії між суб'єктами. Інакше кажучи, абстрактні анонімні мережі потенційно здатні відтворювати стійкий канал зв'язку в будь-якому середовищі, де є мінімальна можливість обміну інформацією. Це може бути як стандартна інтернет-мережа, так і допоміжні канали — від радіохвиль до стеганографічних методів передавання даних.

На відміну від сучасних анонімних мереж (Tor, I2P тощо), які залежать від великої кількості проміжних вузлів і мають свої обмеження щодо швидкості чи масштабованості, абстрактна модель пропонує універсальний підхід. Вона поєднує можливість анонімізації з повною незалежністю від фізичної інфраструктури, створюючи базу для формування наступного покоління систем безпечного зв'язку.

У такій перспективі абстрактні анонімні мережі можна розглядати як концептуальну надбудову над існуючими технологіями, яка здатна радикально змінити парадигму захисту інформації. Вони відкривають шлях до створення середовищ, де ані централізація, ані наявність чи відсутність класичних маршрутів, ані навіть кількість учасників не впливатимуть на рівень конфіденційності. Саме ці властивості роблять концепцію надзвичайно цінною для критичної інформаційної інфраструктури, яка вимагає максимальної стійкості до зовнішніх загроз і гнучкості у відповідь на нові виклики.

Проєктування абстрактних мереж

Попри уявну складність, проєктування та реалізація абстрактних анонімних мереж не є завданням, яке неможливо виконати. Навпаки, сучасні підходи дають змогу створювати такі мережі на основі вже існуючих технологій, доповнюючи їх математичною строгістю та новими методами анонімізації. Ключовою умовою у цьому процесі є те, що анонімність повинна бути не лише практично досягнутою, а й теоретично доведеною, що значно підвищує рівень довіри до системи.

Одним із прикладів є DC-мережі, побудовані на відомій криптографічній задачі «обідаючих криптографів» (Dining Cryptographers). Її суть полягає у створенні такої системи передавання повідомлень, де неможливо визначити, хто саме є відправником, навіть якщо факт передавання очевидний для всіх учасників. Таким чином забезпечується високий рівень анонімності, який не залежить від кількості спостерігачів. Окрім цього, у наукових колах набувають популярності й інші моделі — зокрема ті, що базуються на чергах повідомлень. У таких системах анонімність досягається шляхом «змішування» повідомлень у часових проміжках і контрольованого розподілу їх між отримувачами. Подібні механізми ускладнюють навіть глобальне спостереження, оскільки втрачається можливість кореляції часу надсилання та отримання даних.

Теоретично доведена анонімність

Мережі з теоретично доведеною анонімністю визначаються як замкнені та повністю контрольовані системи, у яких будь-які пасивні атаки виявляються безрезультатними. Це стосується навіть сценаріїв, коли існує глобальний спостерігач, здатний аналізувати весь трафік у системі. У таких умовах неможливо деанонімізувати:

- факт надсилання чи отримання повідомлення;
- зв’язок між конкретним відправником і одержувачем;
- часову кореляцію між подіями у мережі.

Єдиною умовою функціонування таких систем залишається наявність певної кількості вузлів, які не перебувають у змові. Саме вони створюють «криптографічний шум», що забезпечує рівномірний розподіл ймовірностей і гарантує, що будь-які знання, отримані зловмисником після аналізу трафіку

(апостеріорні), будуть рівнозначними тим, що він мав до початку спостереження (апріорним). Інакше кажучи, ймовірність деанонімізації завжди залишається рівною для всіх учасників мережі.

Це забезпечує фундаментальний рівень стійкості системи до пасивних атак і робить її унікальною серед усіх відомих підходів до анонімізації трафіку. На відміну від більшості практичних рішень (Tor, I2P, Mixminion), які уразливі до глобальних атак кореляції, теоретично доведені мережі формують **нову парадигму безпеки**.

Перспективи для критичної інфраструктури

Застосування абстрактних анонімних мереж у сфері критичної інфраструктури може стати революційним кроком. Їх можна використати у:

- **урядових і військових системах управління**, де важлива не лише секретність даних, а й приховування самих комунікаційних зв’язків;
- **фінансових мережах**, де передача транзакцій повинна бути захищена від глобального спостереження;
- **аварійних каналах зв’язку**, які повинні функціонувати навіть у разі перехоплення чи спроби блокування;
- **системах енергетики та транспорту**, де стійкість до кібератак є питанням національної безпеки.

Таким чином, концепція абстрактних анонімних мереж поєднує у собі практичні механізми анонімізації та теоретичну обґрунтованість, формуючи перспективний напрям для розвитку безпечних комунікацій у глобальному масштабі.

3.2 Основні підходи до реалізації

Проблема «обідаючих криптографів» та її роль у проєктуванні анонімних мереж

Проблема «обідаючих криптографів» (Dining Cryptographers Problem, DC-problem) є однією з базових моделей у криптографії, яка демонструє можливість

досягнення анонімності у групових комунікаціях. Вона описує ситуацію, у якій група учасників мережі прагне забезпечити передавання інформації так, щоб усі знали про сам факт передачі, але при цьому ніхто, окрім відправника, не міг встановити його особу.

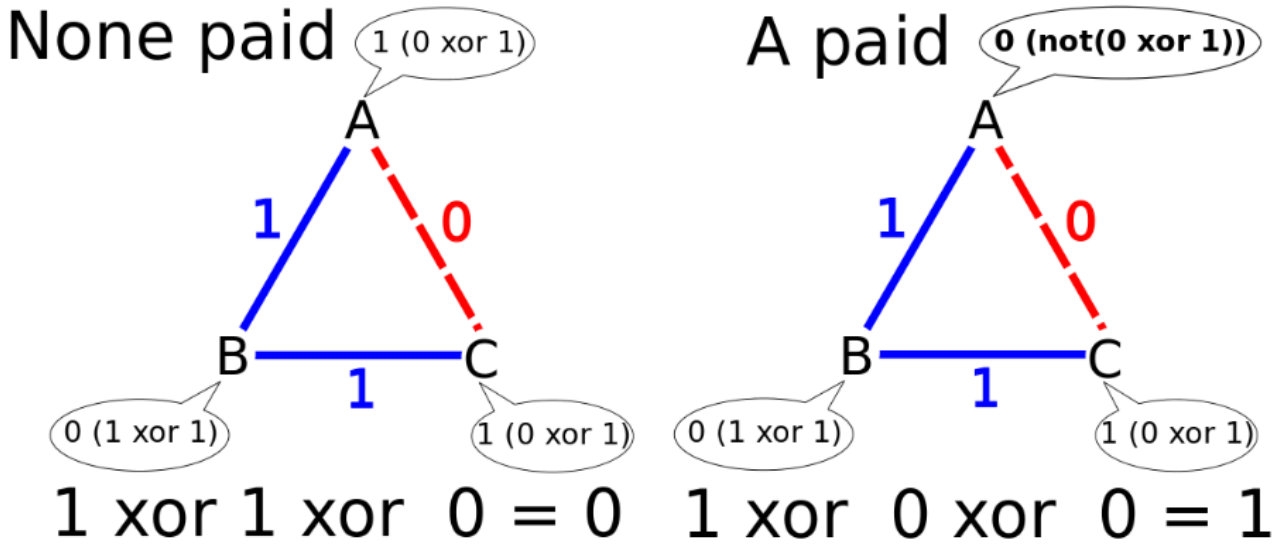


Рис. 3.1 Dining Cryptographers Problem

У класичному прикладі розглядаються три учасники {A, B, C}, які з'єднані між собою захищеними каналами. Кожен із них у визначений момент часу *T* генерує випадковий біт, який узгоджується з сусідами. Припустимо, що учасники домовилися про такі значення: {A, B} = 1, {B, C} = 0, {C, A} = 1. Далі кожен виконує операцію XOR над бітами, отриманими зі своїх каналів: A = 1 ⊕ 1 = 0, B = 1 ⊕ 0 = 1, C = 0 ⊕ 1 = 1. Результати публікуються та знову комбінуються операцією XOR усіма учасниками: 0 ⊕ 1 ⊕ 1 = 0. Це означає, що інформаційний біт дорівнює «0». Якщо ж учасник A хоче передати «1», він додає операцію заперечення (¬), отримуючи значення 1 замість 0. Після повторного обміну усі прийдуть до результату 1 ⊕ 1 ⊕ 1 = 1. У такий спосіб забезпечується передавання одного біта даних, при якому анонімність відправника зберігається на рівні 50/50 для інших суб'єктів.

З точки зору внутрішнього спостерігача (B чи C), деанонімізувати відправника практично неможливо без змови з іншим учасником, оскільки знання лише власних секретів недостатньо. Для глобального спостерігача ситуація не

змінюється — він бачить лише передачу зашифрованих бітів через захищені канали у момент часу *T*, але не може ідентифікувати джерело повідомлення. Саме це робить DC-проблему одним із небагатьох прикладів систем із теоретично доведеною анонімністю.

Водночас класичні DC-мережі мають обмеження. Вони потребують високого рівня централізації та прямого з'єднання між кожною парою учасників за схемою «один-до-одного». Якщо змінити архітектуру на «усі-до-одного», то вузол, який об'єднує всі комунікації, фактично стає точкою вразливості та джерелом можливої деанонімізації.

Щоб усунути цю проблему, пропонується відмовитися від суворої моделі «один-до-одного» і перейти до архітектури, де кожен учасник заздалегідь погоджує ключі з усіма іншими, а центральний вузол виконує лише функцію ретранслятора. Таким чином, ключові дані не зосереджуються в одному місці, а відтак ризик деанонімізації значно зменшується. Для полегшення узгодження ключів доцільно використовувати асиметричну криптографію, яка дозволяє кожному суб'єкту обмінюватися відкритими ключами та уникати складних процедур прямої синхронізації.

Окремої уваги заслуговує питання масштабованості. У початковій постановці задача розглядалася для трьох учасників, проте сучасні дослідження дозволяють поширити цей підхід на десятки чи навіть сотні вузлів. Чим більше учасників, тим складніше зловмиснику виконати атаку кореляції чи змови, що суттєво підвищує рівень анонімності. Це відкриває перспективи використання DC-мереж не лише у дослідницьких моделях, а й у реальних системах, зокрема у сфері захищених комунікацій критичної інфраструктури.

Таким чином, проблема «обідаючих криптографів» не лише демонструє фундаментальний принцип анонімізації трафіку, але й наближає нас до концепції абстрактних анонімних мереж. Вона підтверджує, що можливо створити систему, у якій такі параметри, як кількість вузлів, відкритість IP-адрес чи швидкість трафіку, не є критичними для збереження конфіденційності. Єдиною умовою залишається

правильна організація архітектури та усунення надмірної централізації, що робить дану модель перспективною основою для побудови майбутніх анонімних мереж.

Задача на основі черг

Задача на основі черг є розвитком ідей DC-протоколів («обідаючих криптографів»), проте вона має принципові відмінності, які роблять її більш прикладною та придатною для практичного використання в анонімних мережах. Якщо DC-модель орієнтована на широкомовну передачу даних між усіма учасниками групи, то задача на основі черг передбачає побудову динамічної структури взаємопов'язаних вузлів, де реалізовано наскрізне (E2E) шифрування та механізм керованого обміну повідомленнями.

Уявімо систему з кількома учасниками, наприклад {A, B, C}. Кожен із них має власне внутрішнє сховище типу FIFO (First In — First Out), яке працює за принципом «першим прийшов — першим вийшов». Це сховище фактично є чергою повідомлень, у якій можуть накопичуватися як справжні дані, так і фіктивні пакети. Додатково кожен вузол має узгоджений часовий інтервал *T*, у межах якого він зобов'язаний генерувати повідомлення.

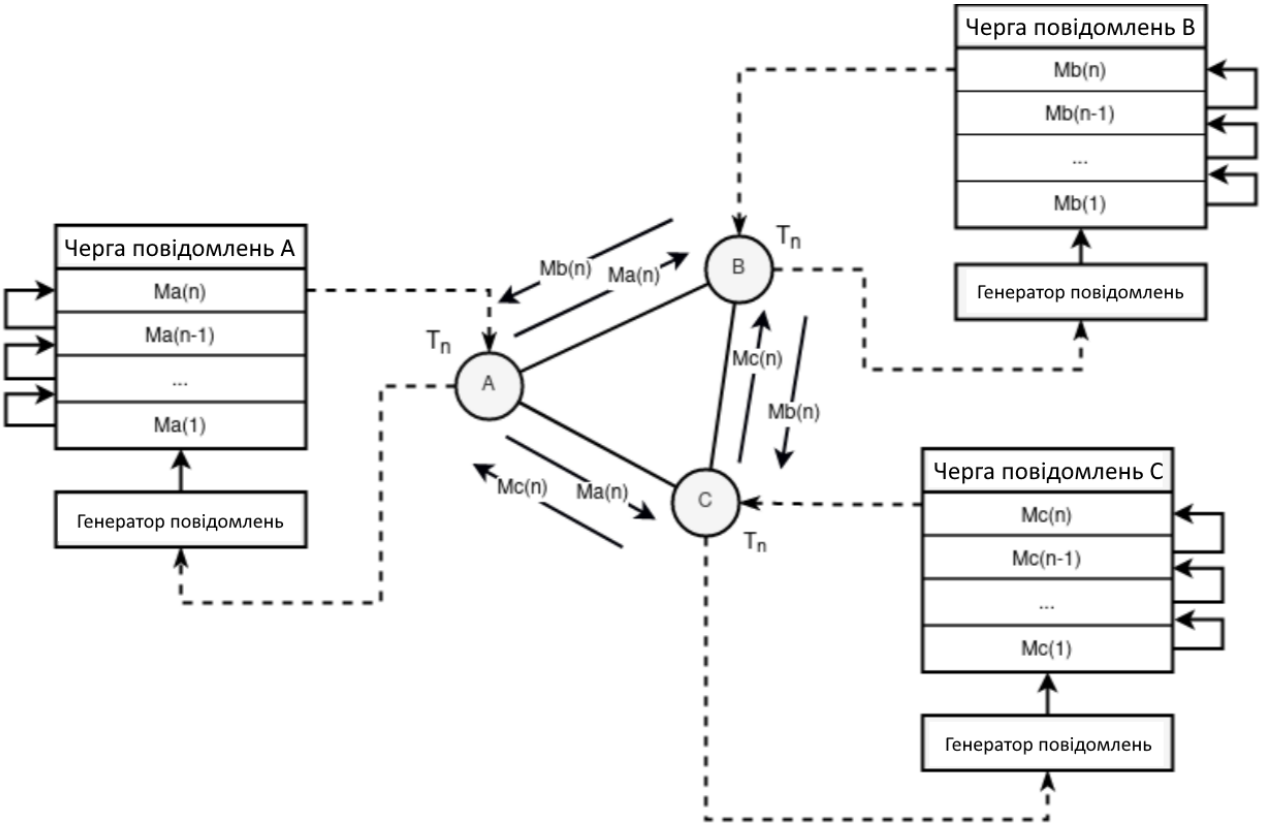


Рис. 3.2 Завдання на базі черг

Кожного разу в момент часу *T* вузол створює пакет, який може мати один із двох варіантів:

- **істинне повідомлення** — це запит або відповідь, адресовані конкретному учаснику, що містять корисну інформацію;
- **хибне повідомлення** — фіктивний пакет, наповнений випадковими бітами, який не несе жодного смислового навантаження.

Важливо, що учасник не може надіслати повідомлення раніше чи пізніше визначеного інтервалу *T*, оскільки це зруйнувало б принцип синхронності, який забезпечує анонімність. Якщо у вузла накопичується кілька справжніх повідомлень, він поміщає їх у свою чергу, а далі, згідно з порядком FIFO, відправляє їх у наступні часові такти.

Таким чином, формується не одна черга, як у DC-протоколі, а мережа з множиною взаємопов’язаних черг, що робить систему більш стійкою до атак аналізу трафіку та дозволяє гнучко масштабувати її на більшу кількість учасників.

Для глобального спостерігача така мережа виглядає максимально непрозорою: він бачить лише регулярну відправку пакетів усіма вузлами у моменти часу *T*. При цьому неможливо визначити, які з цих повідомлень є реальними, а які — фіктивними. Внутрішні пасивні учасники також не здатні розкрити комунікацію між іншими вузлами, оскільки повідомлення зашифровані наскрізно, а їхній вміст не дає жодних даних про відправника чи одержувача.

Завдяки такій архітектурі задача на основі черг забезпечує теоретично доведену анонімність. Вона позбавляє систему тих обмежень, які притаманні DC-мережам: залежності від топології «один-до-одного», високого рівня централізації чи проблем із масштабованістю.

Сьогодні існують і практичні реалізації цієї моделі:

- **HLS** (Hidden Loop System) — ядро анонімної мережі з теоретично доведеною анонімністю, побудоване на базі черг;
- **HLM** (Hidden Loop Messenger) — анонімний месенджер, створений поверх HLS, який демонструє можливість безпечного обміну повідомленнями без розкриття комунікаційних зв’язків;

- **HLT** (Hidden Loop Traffic) — додаток для збереження та повторного розподілу трафіку, що функціонує у складі HLS.

Перспективність задачі на основі черг полягає у її універсальності. Вона може застосовуватися у критичній інформаційній інфраструктурі, зокрема в урядових, військових або фінансових системах, де надзвичайно важливим є не лише захист змісту даних, а й приховування самого факту комунікації. Така модель дозволяє будувати системи, стійкі до глобальних атак спостереження, атак кореляції та навіть спроб виявлення взаємозв'язків між користувачами.

Отже, задача на основі черг є не лише математичною моделлю, а й практичною платформою для створення мереж майбутнього, у яких анонімність та безпека будуть забезпечуватися не окремими алгоритмами, а самою структурою архітектури комунікацій.

3.3 Створення архітектур

Комбінація «таємний канал зв'язку + абстрактна анонімна мережа»

Поєднання таємного каналу зв'язку з абстрактною анонімною мережею відкриває можливість підтримувати приховану комунікацію з високим рівнем анонімності, використовуючи при цьому ресурси вже існуючих централізованих сервісів. Основна ідея полягає в тому, що зашифровані повідомлення не зберігаються у спеціально виділених вузлах, а ховаються всередині масових інфраструктур, застосовуючи їх у якості сховищ та каналів розповсюдження даних. Така модель має очевидні риси «паразитичності», адже фактично використовує чужі обчислювальні та мережеві ресурси не за прямим призначенням, створюючи прихований рівень зв'язку поверх традиційних сервісів.

Головна перевага такого підходу полягає у відсутності потреби створювати «чисті» вузли, що виконують лише функцію ретрансляції анонімного трафіку. Оскільки абстрактні анонімні мережі часто обмежені кількістю вузлів та страждають від низької продуктивності, їх виживання напряму залежить від здатності інтегруватися в уже готові системи. У результаті ці мережі стають

життєздатними завдяки масштабності централізованих платформ, у яких їхній трафік маскується під звичайну діяльність користувачів. Така інтеграція забезпечує маскування, економію ресурсів та гнучкість, однак водночас робить систему залежною від політик і стабільності зовнішніх сервісів.

Архітектуру такого підходу зручно пояснити на прикладі проєкту Hidden Lake, який складається з трьох ключових компонентів: HLS (service), HLM (messenger) і HLT (traffic). Усі вони взаємодіють між собою для перетворення повідомлень і їх прихованого розміщення у сторонніх сервісах. Основні терміни при цьому виглядають так: Payload — відкриті дані в незашифрованому вигляді; Message — зашифрований формат повідомлення; F(Message) — спеціальна оболонка, яка дозволяє адаптувати зашифровані повідомлення до формату стороннього сервісу.

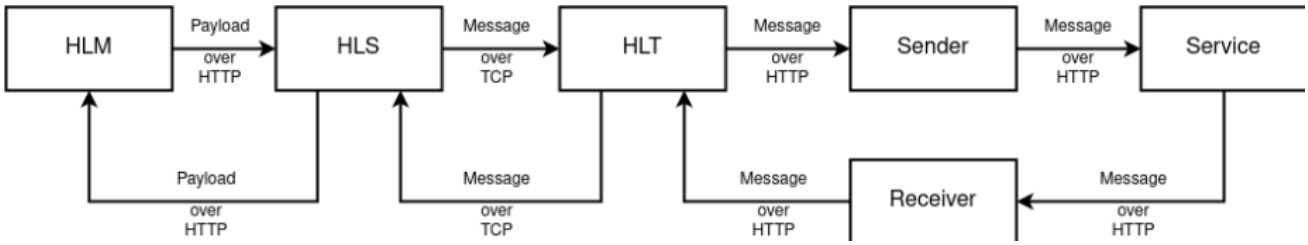


Рис. 3.3 Архітектура таємного каналу зв'язку при використанні HLS, HLM та HLT

Розподіл функцій між компонентами виглядає наступним чином:

1. **HLS (ядро сервісу)** працює з TCP у зовнішній мережі та HTTP у внутрішній, зберігаючи лише хеш-значення повідомлень без вмісту, що знижує ризик витоку.
2. **HLM (месенджер)** виконує функції графічного інтерфейсу та зберігає Payload, забезпечуючи шифрування повідомлень перед відправленням і розшифрування після отримання.
3. **HLT (сервіс трафіку)** імітує поведінку HLS та здійснює перерозподіл повідомлень, упакованих у F(Message), у зовнішні сервіси.
4. **Sender** перетворює Message у F(Message) для подальшого збереження у Service, а **Receiver** виконує зворотну операцію, відновлюючи Message з оболонки.

5. **Service** виступає у ролі зовнішнього сховища, що зберігає F(Message) як звичайні дані, не маючи можливості отримати доступ до їх змісту.

У такій архітектурі дані рухаються наступним чином: користувач у HLM формує Payload, який шифрується у Message та надсилається через HLT у форматі F(Message) до зовнішнього сервісу. Receiver періодично перевіряє наявність оновлень, витягує F(Message), перетворює його назад у Message, після чого HLM розшифровує повідомлення у Payload для користувача.

До переваг цієї моделі належать:

- адаптація до масової інфраструктури з використанням її масштабності та глобальної доступності;
- приховування трафіку серед звичайних користувацьких дій;
- економія ресурсів за рахунок відмови від побудови власної глобальної інфраструктури;
- гнучкість у виборі форматів F(Message), що дозволяє застосовувати різні сервіси.

Разом із тим існують компроміси та ризики:

- залежність від сторонніх сервісів та їх політики;
- юридичні й етичні обмеження використання чужих ресурсів;
- можливість виявлення через аналіз поведінкових патернів;
- небезпека витоку метаданих при поганій реалізації F(Message);
- ризики операційної нестабільності (наприклад, видалення даних або блокування сервісом).

Для забезпечення безпеки важливо дотримуватися таких принципів:

- використання стійких криптографічних алгоритмів, що гарантують цілісність та конфіденційність;
- мінімізація збереження метаданих у HLS та HLT;
- диверсифікація зовнішніх сервісів для зменшення ризику централізованого блокування;
- постійний моніторинг змін у зовнішніх сервісах і адаптація до них.

З етичної та правової точки зору використання централізованих платформ у прихованих цілях викликає серйозні питання, оскільки може підпадати під законодавство про несанкціонований доступ і порушення умов користування. Тому подібні системи доречно розглядати переважно в контексті досліджень критичної інфраструктури, як об’єкт для розробки методів виявлення прихованих каналів і підвищення захисту телекомунікаційних мереж.

У представленій моделі архітектуру системи можна порівняти з початковими підходами до анонімізації трафіку, де весь процес базувався виключно на так званих «чистих» з’єднаннях. Такі з’єднання являли собою прямий обмін повідомленнями між вузлами без участі зовнішніх сервісів зв’язку чи використання прихованих каналів. Подібна схема є відносно простою за реалізацією та зрозумілою за логікою роботи: інформація передається від відправника до отримувача без проміжних шарів інтеграції, що у свою чергу зменшує кількість потенційних точок відмови або компрометації даних.

Однак у той же час подібна «чиста» архітектура має суттєві обмеження. Вона вимагає постійної підтримки власної інфраструктури, яка повинна функціонувати як окрема мережа з визначеною кількістю вузлів і достатньою пропускною здатністю. Це створює додаткове навантаження на ресурси та значно знижує масштабованість системи. У випадку з невеликими мережами та обмеженою кількістю користувачів така модель ще може бути ефективною, проте в умовах високонавантажених систем або при необхідності глобального розгортання вона стає надто громіздкою.

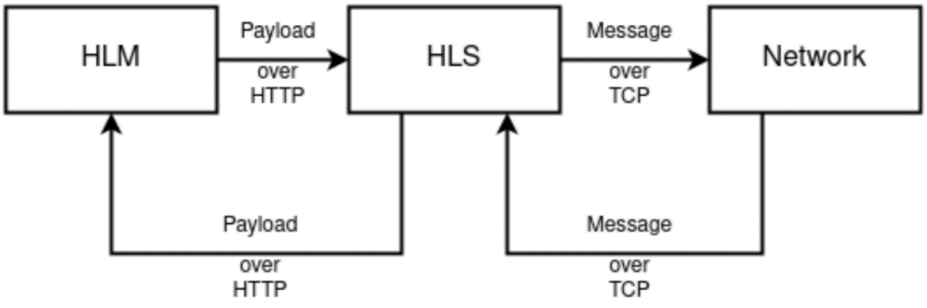


Рис. 3.4 Архітектура анонімізації трафіку при використанні HLS та HLM

Схема, у якій реалізується анонімізація за допомогою компонентів HLS та HLM, має принципово інший характер. Тут Network може бути представлена у вигляді сукупності модулів (HLT + Sender + Receiver + Service), що дозволяє будувати більш гнучку і абстрактну модель комунікації. Така модульність забезпечує можливість легкого переходу між базовою архітектурою та її розширеною версією з використанням HLT. Завдяки цьому користувач або адміністратор може налаштовувати роботу системи відповідно до конкретних вимог: у мінімальній конфігурації застосовується лише HLS і HLM, а за необхідності масштабування чи прихованої інтеграції додається HLT разом із відповідними адаптерами.

Особливої уваги заслуговує роль Sender та Receiver, які можна розглядати як універсальні адаптери. Вони виконують критично важливе завдання трансформації одного типу повідомлення в інший: Sender «упаковує» зашифроване повідомлення у формат, сумісний із зовнішнім сервісом (Message → F(Message)), тоді як Receiver здійснює зворотну операцію (F(Message) → Message). Таким чином, система отримує гнучкий механізм перетворення даних, що дозволяє інтегруватися із різними платформами та маскувати анонімний трафік під звичайну користувацьку активність.

Ще однією важливою рисою є відносна замінюваність клієнтського застосунку HLM. Якщо уважно проаналізувати логіку архітектури, стає очевидним, що HLM виконує лише роль інтерфейсу для користувача та збереження відкритої інформації (Payload). Тобто його можна без суттєвих змін замінити на будь-який інший застосунок — наприклад, файловий сервіс, поштовий клієнт або корпоративну систему обміну даними. Загальна архітектура при цьому залишиться незмінною, адже сам механізм анонімізації та формування прихованого каналу зв’язку реалізується на рівні HLS, HLT та адаптерів.

Завдяки такій гнучкості та абстрагуванню архітектура набуває ознак універсальності. Вона не прив’язана до конкретного сервісу або типу даних, а виступає як інфраструктурний «шар», який можна накласти практично на будь-яке

середовище. Це суттєво підвищує її життєздатність, особливо в умовах змінної мережевої топології, обмежених ресурсів або потреби у швидкому масштабуванні.

У підсумку можна зазначити, що порівняння «чистої» архітектури та схеми з використанням HLS/HLM демонструє еволюцію підходів до анонімізації трафіку. Якщо перший варіант забезпечує простоту, але обмежений у масштабуванні та продуктивності, то другий дозволяє досягти значно більшої гнучкості, розширюваності та адаптивності за рахунок модульної побудови та використання сторонніх сервісів. Саме тому подібна архітектура є більш перспективною для використання у критично важливих системах, де безпека та стійкість комунікацій мають пріоритетне значення.

4 ЗАХИСТ ВІД DDOS АТАК

4.1 Основні компоненти захисту

У сучасному світі, де майже всі сфери життя переходять у цифровий формат, питання кіберзахисту набуває вирішального значення. Однією з найбільш небезпечних та поширених загроз є **DDoS-атаки (Distributed Denial of Service)**, що становлять реальну загрозу для функціонування як бізнесу, так і державної критичної інфраструктури. Їхня головна мета полягає у створенні штучного перевантаження системи, яке унеможливлює або значно ускладнює доступ легітимних користувачів до ресурсів. У результаті організація-мішень зазнає значних фінансових та репутаційних втрат, а іноді й ставить під загрозу національну безпеку.

Масштаби та наслідки атак

DDoS-атаки мають унікальну особливість: вони можуть бути спрямовані проти будь-якої організації, незалежно від її розміру чи галузі діяльності. Під удар потрапляють як маленькі компанії, так і транснаціональні корпорації, як приватні освітні сервіси, так і урядові портали чи медіа-платформи. Зафіксовані випадки, коли навіть великі хмарні провайдери з потужними ресурсами ставали жертвами атак обсягом у кілька терабіт за секунду. Наприклад, у 2021 році мережа Microsoft Azure повідомила про атаку потужністю понад 3,4 Тбіт/с, що стала однією з найбільших в історії. У 2022–2023 роках масові атаки відбувалися проти фінансових установ Європи та Азії, державних ресурсів України, США та країн ЄС.

Економічні наслідки атак вимірюються мільйонами доларів. За даними міжнародних досліджень, середні збитки від однієї масштабної DDoS-атаки для середнього бізнесу сягають 120–150 тис. доларів за годину простою. Для великих корпорацій ці втрати обчислюються десятками мільйонів. Але фінанси — не єдиний аспект. Порушення роботи державних порталів чи енергетичних компаній може призвести до соціальної паніки, підриву довіри громадян і навіть до політичної дестабілізації.

Технологічна еволюція атак

Із середини 2000-х років DDoS-атаки значно еволюціонували. Якщо раніше вони будувалися здебільшого на простих механізмах flood-трафіку (UDP flood, SYN flood), то сьогодні це вже комбіновані, багаторівневі сценарії, що одночасно зачіпають різні рівні моделі OSI. Виділяють кілька основних категорій:

- **Об'ємні атаки (Volumetric attacks)** — спрямовані на перевантаження каналів зв'язку величезними обсягами трафіку. Типові приклади: UDP flood, ICMP flood, amplification-атаки через DNS або NTP.
- **Протокольні атаки (Protocol attacks)** — експлуатують вразливості у механізмах встановлення з'єднання, перевантажуючи серверні ресурси або мережеве обладнання. Приклади: SYN flood, Smurf, Ping of Death.
- **Атаки прикладного рівня (Application Layer attacks)** — найнебезпечніші через складність виявлення. Вони маскуються під легітимний користувацький трафік, але паралізують роботу додатків. Приклади: HTTP flood, Slowloris, атаки на бази даних.

Особливу загрозу становлять так звані Low and Slow-атаки, де шкідливий трафік надходить у дуже малих обсягах, але надовго утримує серверні ресурси. Такі атаки важко відрізнити від звичайної активності, тому традиційні системи часто пропускають їх. Ще більш небезпечними є атаки «нульового дня», що експлуатують невідомі вразливості і протидія яким можлива лише через адаптивні та інтелектуальні системи виявлення.

Сценарії застосування ботнетів

Для організації масштабних DDoS-кампаній зловмисники зазвичай використовують ботнети — розподілені мережі заражених пристроїв. Якщо раніше основу таких ботнетів складали персональні комп'ютери, то нині найбільш вразливими стали IoT-пристрої (смарт-камери, маршрутизатори, датчики). Вони часто мають слабкий захист, стандартні паролі та застаріле ПЗ, що робить їх легкою здобиччю для зловмисників. Відомий приклад — ботнет Mirai, який у 2016 році здійснив масштабну атаку на провайдера DNS-послуг Dyn, внаслідок чого були паралізовані сервіси Twitter, Netflix, Reddit та інші великі ресурси.

Архітектура захисту: універсальна система фільтрації атак

Умовна «універсальна система фільтрації атак» має працювати одночасно на кількох рівнях ISO/OSI (з 2-го по 7-й), забезпечуючи комплексний захист як мережевої інфраструктури, так і прикладних сервісів. Вона включає:

1. **Апаратно-програмний комплекс боротьби з DDoS.**
    - обробка трафіку у режимі реального часу з пропускною здатністю сотні Гбіт/с;
    - інтеграція алгоритмів машинного навчання для виявлення аномалій;
    - SSL/TLS offloading для аналізу зашифрованих потоків;
    - можливість перенаправлення трафіку у зовнішні центри очищення (провайдерські чи хмарні).
2. **Web Application Firewall (WAF).**
    - захист від атак прикладного рівня: SQL-ін’єкції, XSS, CSRF, Command Injection;
    - створення сигнатур «на льоту»;
    - поведінковий аналіз запитів та фільтрація підозрілих HTTP/HTTPS-сеансів.
3. **Системи моніторингу, управління та аналітики.**
    - централізований моніторинг усіх інцидентів;
    - інтеграція з SIEM-платформами для кореляції подій;
    - прогнозування можливих атак на основі Threat Intelligence feeds.
4. **Організаційний компонент — служба підтримки.**
    - доступність у режимі 24/7/365;
    - допомога у налаштуванні та фільтрації;
    - розробка сигнатур під час складних атак.

Додаткові механізми захисту

Окрім базових рішень, таких як апаратно-програмні комплекси для боротьби з DDoS та системи веб-екранів (WAF), сучасна архітектура кіберзахисту активно інтегрує додаткові технології, що виконують функції підсилення основних механізмів безпеки. Їхнє завдання полягає у зниженні ризиків, підвищенні

надійності системи, а також у створенні багаторівневого захисту, де зловмиснику надзвичайно складно обійти всі ланки оборони.

1. **Anycast-routing.**

   Технологія Anycast передбачає можливість використання однієї IP-адреси для кількох географічно розподілених серверів. Це означає, що запити користувачів автоматично маршрутизуються до найближчого вузла, що забезпечує не лише підвищення швидкості обслуговування, а й рівномірний розподіл навантаження. У випадку DDoS-атаки трафік зловмисників також «розтягується» між різними центрами обробки даних, що суттєво знижує ймовірність виведення з ладу всієї інфраструктури. Anycast використовується у глобальних сервісах — наприклад, у системі **DNS Cloudflare** чи **Google Public DNS**, де відбувається балансування мільйонів запитів щосекунди.

2. **Load Balancing.**

   Балансування навантаження є ще одним ключовим елементом захисту. За допомогою спеціалізованих алгоритмів (Round Robin, Least Connections, IP Hash тощо) система рівномірно розподіляє запити між кількома серверами. Це дозволяє уникнути перевантаження окремих вузлів і зберегти працездатність навіть під час сплесків трафіку. Крім того, сучасні балансувальники підтримують **автоматичне виявлення відмови** (failover) та миттєве перенаправлення запитів на резервні сервери, що гарантує безперервність роботи критичних сервісів.

3. **Honeypots.**

   «Медові пастки» (honeypots) — це спеціально створені віртуальні системи, які імітують справжні сервери або сервіси, але не мають реальної бізнес-цінності. Їхнє основне завдання — привернути увагу зловмисників та відволікти їх від критичних елементів інфраструктури. При цьому кожна дія атакуючого ретельно фіксується, що дозволяє дослідникам кібербезпеки отримувати цінну інформацію про тактики, техніки та процедури (TTPs) зловмисників. Honeypots часто інтегруються з більш складними системами

honeynets, що складаються з декількох взаємопов’язаних пасток і створюють повну ілюзію справжньої мережі.

4. **User Behavior Analytics (UBA/UEBA).**

   Технології аналітики поведінки користувачів стали надзвичайно актуальними завдяки розвитку машинного навчання. Вони дозволяють виявляти відхилення у діях користувачів та систем, які можуть свідчити про бот-активність або компрометацію акаунтів. Наприклад, різке зростання кількості запитів від одного користувача, підозріла геолокація або спроби доступу до нетипових сервісів можуть сигналізувати про атаку. Системи UBA/UEBA часто поєднуються з SIEM-рішеннями, утворюючи єдиний аналітичний простір для моніторингу та реагування.

5. **Threat Intelligence Feeds.**

   Служби потоків розвідданих про кіберзагрози (Threat Intelligence Feeds) забезпечують надходження актуальної інформації про відомі атаки, IP-адреси ботнетів, зловмисні домени чи сигнатури шкідливого коду. Завдяки інтеграції таких даних система може оперативно блокувати підозрілий трафік ще до того, як він спричинить шкоду. Розвіддані можуть надходити як від комерційних постачальників (наприклад, Recorded Future, FireEye, IBM X-Force), так і від відкритих спільнот (наприклад, Abuse.ch). У поєднанні з технологіями машинного аналізу ці дані дозволяють будувати прогностичні моделі атак і завчасно готувати інфраструктуру до можливих загроз.

Для секторів, що належать до критичної інформаційної інфраструктури (банки, енергетика, транспорт, державні сервіси), DDoS-атаки є особливо небезпечними. Відмова таких систем навіть на кілька годин може мати катастрофічні наслідки. Тому провідні країни світу інтегрують DDoS-захист у національні стратегії кібербезпеки, створюють державні CERT-команди, фінансують розвиток центрів очищення трафіку та стимулюють співпрацю між приватним і державним секторами.

4.2 Способи впровадження компонентів захисту

«В розрив» (Inline)

Метод встановлення системи захисту «в розрив» передбачає інтеграцію відповідного обладнання або програмно-апаратного комплексу безпосередньо у тракт проходження трафіку. Іншими словами, увесь інформаційний потік, що рухається між мережею користувача та глобальною мережею, обов'язково проходить крізь пристрій фільтрації. Такий підхід вважається одним із найбільш ефективних у сфері протидії DDoS-атакам, оскільки забезпечує повний контроль над усіма пакетами даних. Разом із тим він має певний ризик: у випадку виходу з ладу компонента захисту можливе повне припинення передавання трафіку. Саме тому при використанні «inline»-схеми слід заздалегідь передбачати резервування обладнання або ж реалізувати режим bypass (автоматичне пропускання трафіку напряму без фільтрації у разі несправності системи).

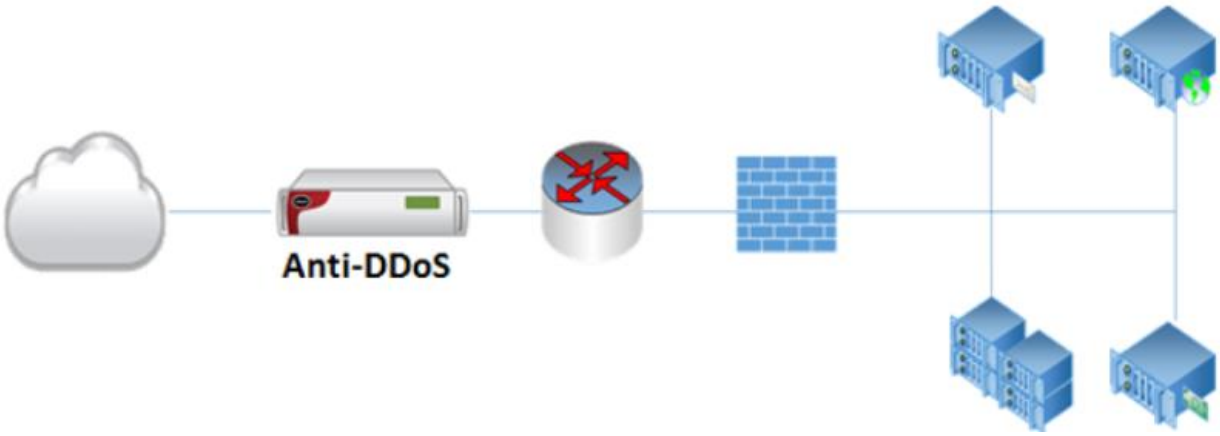


Рис. 4.1 Метод встановлення «в розрив»

Переваги розміщення «в розрив»

Установка системи захисту безпосередньо на шляху трафіку забезпечує одразу кілька ключових позитивних ефектів:

- можливість проводити інспектування всього трафіку в реальному часі, що дозволяє виявляти як відомі, так і нові типи атак;

- захист усіх елементів мережевої інфраструктури компанії, починаючи від прикладних сервісів і закінчуючи мережевим обладнанням, від DDoS-активності як із зовнішніх, так і з внутрішніх джерел.

Особливості реалізації

Варто враховувати, що більшість маршрутизаторів та міжмережевих екранів використовують зовнішні «білі» IP-адреси, інформація про які є відносно легко доступною для атакуючих. Це відкриває можливість здійснення розвідки: визначення відкритих портів, виявлення версій операційних систем і сервісів, а надалі — експлуатації відомих вразливостей стеку TCP/IP. У таких випадках саме система захисту, встановлена «в розрив», виконує функцію бар'єра, здатного своєчасно ідентифікувати й відбити атаку, не допускаючи пошкодження всієї мережевої інфраструктури.

Архітектура роботи системи

Функціонування модуля протидії DDoS-атакам у такій схемі зазвичай реалізується у вигляді двох паралельних фаз, які працюють незалежно одна від одної.

Фаза 1 — навчання контрольним характеристикам.

До початку атаки система формує еталонний профіль трафіку, який описує нормальну структуру та динаміку передавання даних у мережі. На основі цих параметрів надалі відбувається розпізнавання аномалій. Під час навчання створюються контрольні значення, що дозволяють визначати відхилення у структурі, обсягах та швидкості трафіку. У випадку фіксації ознак атаки процес навчання негайно зупиняється, а система переходить у режим активного захисту.

Фаза 2 — аналіз і фільтрація аномального трафіку.

На постійній основі здійснюється аналіз усього трафіку, що проходить через систему, а також контроль поведінки захищеної інфраструктури. Якщо виявляється аномалія, система автоматично ідентифікує її джерело. У разі, якщо аномалія має зовнішнє походження та створює загрозу для функціонування сервісів, генерується набір динамічних фільтрів, які адаптуються до поточного стану мережі та конкретного типу атаки. Таким чином, процес фільтрації триває доти, доки

аномальний трафік не буде усунутий. При цьому легітимні користувачі продовжують працювати без відчутних перерв у доступі (за винятком випадків, коли канал повністю перевантажено).

Після завершення атаки відновлюється процес навчання, що дозволяє системі адаптуватися до можливих змін у структурі нормального трафіку та підготуватися до майбутніх загроз.

«Out-of-path»

Метод «out-of-path» розглядається як альтернативний підхід до розгортання систем протидії DDoS-атакам, коли обладнання для очищення трафіку не вбудовується безпосередньо у тракт його проходження, а працює паралельно поза основним маршрутом. Подібна схема застосування вважається більш типовою для операторів телекомунікаційних послуг, які володіють значними обчислювальними ресурсами і великими каналами зв'язку, та менш актуальною для корпоративних центрів обробки даних, де критично важливим є мінімізація затримок і безперервність обробки запитів.

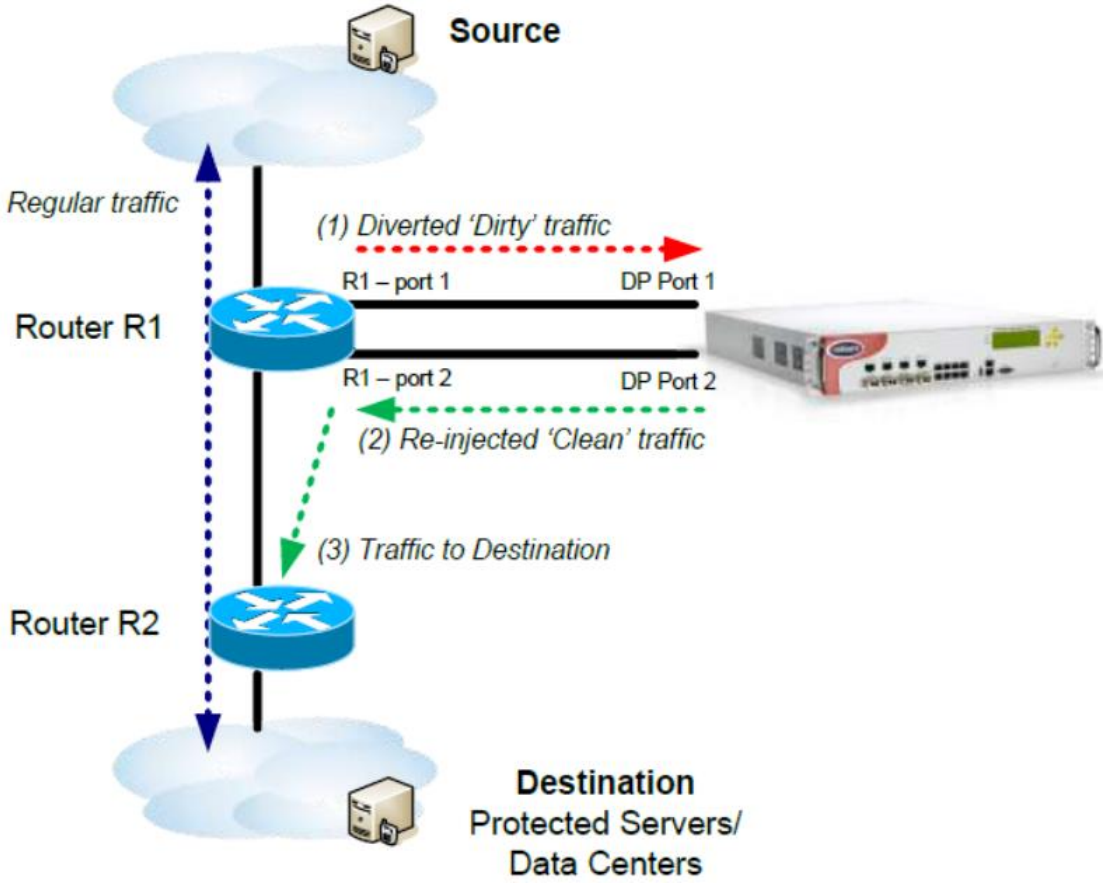


Рис. 4.2 Метод встановлення «out-of-path»

Суть підходу полягає у тому, що маршрутизатор організації у разі виявлення загрози перенаправляє увесь вхідний трафік на спеціалізований пристрій очищення, де відбувається відсів шкідливих пакетів та формування «чистого» потоку даних. Після цього очищений трафік повертається на інший маршрутизатор і далі рухається по мережі за призначенням. Завдяки тому, що обидва маршрутизатори взаємопов'язані, адміністратори мають змогу в будь-який момент перевести маршрутизацію у режим bypass, повністю оминаючи пристрій очищення, наприклад, у випадку його несправності або перевантаження.

Попри очевидні переваги такої архітектури, пов'язані з гнучкістю та можливістю інтеграції на рівні магістральних операторів, у неї є і суттєві недоліки. Найперше, це відносно триваліший час реагування на атаку: для виявлення загрози потрібно активувати механізми моніторингу, задіяти сенсори або детектори та перенаправити увесь трафік на центри очищення. У багатьох випадках для цього застосовуються напівавтоматичні чи навіть ручні процедури, що знижує ефективність захисту у перші критичні хвилини атаки. Також існують сценарії, коли увесь трафік постійно пропускається через центри очищення, але це тягне за собою додаткові затримки та підвищене навантаження на інфраструктуру.

Ще однією слабкою стороною підходу є обмеженість у боротьбі з певними видами атак. Зокрема, рішення «out-of-path» не здатні повноцінно нейтралізувати загрози, що використовують SSL/TLS-шифрування, включно з потужними Pingback DDoS-атаками. Причина криється у широкому впровадженні сучасними вебсервісами механізму Perfect Forward Secrecy (PFS), який передбачає використання ефемерних ключів протоколу Діффі-Геллмана. Завдяки цьому, навіть маючи закритий ключ сервера, неможливо розшифрувати вже узгоджений сесійний ключ. Передача ж приватного ключа на зовнішній пристрій очищення суперечить вимогам безпеки і фактично позбавляє «out-of-path»-рішення можливості аналізувати зашифрований трафік.

Водночас цей метод не слід вважати марним, адже він може ефективно працювати у складі гібридних систем захисту. Наприклад, модуль боротьби з DDoS-атаками може бути встановлений безпосередньо «у розрив» для аналізу і

блокування трафіку, тоді як модуль Web Application Firewall розгортається поза основним маршрутом, тобто «out-of-path». За умови якісної інтеграції між цими компонентами можлива побудова комплексної системи, де WAF виявляє спроби шкідливих дій на прикладному рівні і передає інформацію про них у модуль DDoS-захисту, який уже реалізує необхідні заходи фільтрації. Таким чином, досягається подвійний ефект: з одного боку — блокується небажаний трафік, з іншого — усувається додаткова точка відмови в інфраструктурі.

4.3 Підходи до реалізації рішеть захисту від DDoS

Гібридні підходи до архітектури захисту від DDoS

Розуміння архітектури захисту від DDoS — ключова передумова для вибору правильного рішення під потреби конкретної організації. Особливо це стосується великих структур, де критично важлива одночасно й швидкість реагування, й здатність витримувати масштабні потокові атаки. Одним із найпоширеніших і практично найбільш життєздатних підходів є гібридна архітектура, що поєднує локальні CPE-пристрої (Customer Premises Equipment) і хмарні/провайдерські сервіси очищення трафіку. Мета такої комбінації — компенсувати недоліки кожного підходу окремо і максимально використовувати їхні переваги.

Нижче — детальне роз'яснення двох основних моделей гібридизації: комбінування і резервування, їхні операційні особливості, сценарії застосування, а також практичні обмеження і рекомендації.

Комбінований (роздільний) підхід

Суть. При комбінованому підході завдання по фільтрації розподіляються між локальним CPE і хмарою за профілем атак:

- **хмара** відповідає за фільтрацію великих об’ємних (volumetric) атак — amplification, UDP/ICMP flood і т.п., які спрямовані на вичерпання пропускної здатності каналів;
- **CPE** — за детекцію та блокування атак транспортного (SYN flood, нестандартні TCP-сценарії) та прикладного рівнів (HTTP-flood, атаки на

логіку веб-додатків), де важлива глибока інспекція пакетів, швидка реакція та збереження приватності (наприклад, SSL-інспекція локально).

Практичні переваги:

1. **Економія**: порівняно з розгортанням повноцінного CPE-парку з надмірною пропускною здатністю, комбінований підхід часто дешевший — частина «широкосмугової» роботи знімає хмара.
2. **Захист приватності**: критичні ключі чи конфіденційні дані не передаються в хмару — шифровані з'єднання розшифровуються та аналізуються локально.
3. **Цільова фільтрація**: локальні модулі можуть ефективніше боротися зі «тонкими» прикладними атаками, що імітують легітимний трафік (Low&Slow), а хмара — з «грубою силою» пропускної здатності.

Операційні виклики та обмеження:

1. **Залежність від лінку між CPE і хмарою.** Пропускна здатність і SLA такого каналу повинні проектуватися з урахуванням не лише нормального трафіку, а й потенційної хвилі атак транспортного рівня, що може вимагати десятків — сотень Гбіт/с. Якщо канал виявиться вузьким, хмара не допоможе.
2. **Складність масштабування CPE.** При зростанні потужності атак локальні пристрої доведеться розгортати додатково, що вимагає інвестицій у устаткування й операційну підтримку.
3. **Необхідність висококваліфікованого персоналу.** Навіть при сильній автоматизації потрібні оператори та інженери, які розуміють політики фільтрації, налаштування SSL-інспекції, тонкощі мережевої маршрутизації і процедури перемикання.
4. **Операційні латентності.** Хоча хмара чудово справляється з великими хвилями, перенаправлення трафіку і налаштування політик вимагають часу; у некоректно налаштованих системах це може призвести до простою.

Рекомендації при проектуванні комбінованої архітектури:

- Планувати резервну пропускну здатність каналу між CPE і хмарою, виходячи з прогнозованого «worst case» при транспортних атаках.

- Встановити автоматичні тригери (thresholds) для початку перенаправлення трафіку у хмару — щоб уникнути ручного реагування.
- Забезпечити логічну сегментацію фільтрації: задіювати локальні політики для критичних внутрішніх ресурсів, а хмару — для «глобального очищення».
- Проводити регулярні вправи з ескалації (tabletop exercises) і тестові перенаправлення, щоб відпрацювати процедури переключення.

Підхід резервування (failover / on-demand)

Суть. Універсальна схема, у якій CPE діє як первинний захисний шар у штатному режимі, а хмарне рішення підключається тільки при виявленні, коли CPE не справляється: трафік «вкл/викл» переводиться через центри очищення. Це дозволяє зберегти нормальну роботу з мінімальними латентностями у звичайному режимі й одночасно мати механізм для критичного сценарію.

Переваги:

- **Автономність у штатному режимі.** Організація не залежить від хмари під час повсякденної роботи.
- **Економія ресурсів.** Хмарні потужності зазвичай оплачуються за використання; використовувати їх постійно не обов’язково.
- **Можливість очищення великих хвиль** при виникненні надзвичайних атак.

Недоліки та ризики:

- **Час переходу та можливі розриви сервісу.** Переключення маршруту може тривати від кількох секунд до хвилин, і в цей інтервал частина сервісів може бути тимчасово недоступна.
- **Організаційні витрати.** Підтримка двох паралельних рішень — дорожча у плані людських ресурсів і операційних процедур.
- **Потреба в передачі ключів** для активної інспекції SSL у хмарі, якщо хмара виконує розшифрування; це може бути неприйнятно з точки зору політики безпеки.
- **Необхідність регулярних тестів.** Щоб під час реальної атаки перемикання відбувалось без проблем, слід проводити перевірки й адаптації навчальних моделей.

Поради щодо впровадження резервного підходу:

- Організувати **автономний «канал» зв'язку** між хмарою і локальною мережею або передбачити багаторівневі маршрути для зниження ризику виявлення й атак на сам канал.
- Встановити **цілі SLA** з провайдером хмарних послуг: час початку очищення, пропускна здатність у режимі аварії, можливість миттєвого масштабування.
- Розробити чіткий **playbook** на випадок перемикання, включно з ролями, контактами 24/7 та процедурою повернення до штатного режиму.

Коли поєднувати комбінування і резервування

В реальних інфраструктурах часто застосовують гібридні стратегії, що комбінують обидва підходи. Наприклад:

- CPE відповідає за постійну фільтрацію прикладних атак;
- Хмара виконує «масове очищення» під час великих volumetric атак;
- Резервний канал дозволяє перемикатися повністю на хмару, якщо CPE не справляється.

Такий мікс дає можливість отримати гнучкість і надійність, але одночасно ускладнює операційну експлуатацію: зростає кількість компонентів, їх треба інтегрувати, тестувати політики і відпрацьовувати процедури переключення.

Операційні та безпекові нюанси, що потрібно врахувати

1. **SLA і час реагування.** Перевіряйте контрактну гарантію — важливо не лише теоретичне «очищення», а й швидкість початку дій (time to mitigation). Ідеал — реакція за секунди; реальність — багато провайдерів дають гарантії лише щодо доступності в «спокійному» стані.
2. **SSL/TLS-інспекція.** Якщо захист передбачає аналіз зашифрованого трафіку, потрібно продумати: де відбуватиметься розшифрування (локально чи в хмарі) і як зберігатимуться приватні ключі. PFS (Perfect Forward Secrecy) значно ускладнює розшифровку «на стороні», тому багато організацій залишають SSL-інспекцію локально.

3. **Логування і звітність.** Консолідація даних з усіх компонентів у єдиній системі моніторингу / SIEM — обов'язкова. Це пришвидшує розслідування і дає можливість кореляції інцидентів.
4. **Тестування і тренування персоналу.** Регулярні симуляції атак, тести перемикань і оновлення «еталонних» профілів трафіку — необхідні для підтримки працездатності систем у реальному житті.
5. **Масштабованість.** Проєктуйте архітектуру з урахуванням можливості швидкого додавання фільтраційних ресурсів — вертикально (потужніші пристрої) і горизонтально (додаткові вузли).
6. **Невидимість механізмів фільтрації.** Щоб сама система фільтрації не стала мішенню, рекомендується мінімізувати видимість її інтерфейсів (наприклад, відсутність IP-конфігурацій на інспектованих портах у CPE-рішеннях).

Приклад практичної імплементації

Організація з дата-центром і веб-фронтом:

- Розгортає CPE-кластер з WAF і IPS біля пограничного маршрутизатора; це дає миттєву інспекцію L7 і відсікання більшості прикладних атак.
- Має підписку на хмарний DDoS-чистильник з гарантованим «on-demand» каналом 500 Гбіт/с.
- Налаштовує автоматичні тригери: при збільшенні аномальної хвилі трафіку > X Gbps або при виявленні > Y IP з високою частотою помилкових запитів — маршрутизація всього зовнішнього трафіку через хмару.
- Проводяться щоквартальні вправи з переключення з контролем часу перемикання і перевіркою коректності політик.

Ефективність реагування на DoS/DDoS-атаки

Одним із ключових параметрів при виборі рішень для протидії DoS/DDoS-атакам є їхня реальна ефективність, яка зазвичай визначається умовами SLA (Service Level Agreement — угоди про рівень послуг). У таких документах фіксується опис послуг, права й обов'язки сторін, рівень якості сервісу (зокрема час реагування на інциденти) та санкції у випадку невиконання домовленостей.

Аналізуючи договори більшості постачальників хмарних сервісів із захисту від DoS/DDoS, можна помітити, що гарантії високої доступності часто діють лише доти, доки атака відсутня. Тобто клієнт фактично не отримує підтверджень, що під час самої атаки буде забезпечена безперебійна робота чи гарантовано швидка реакція на інцидент.

Ще один суттєвий момент полягає у тому, що в контрактах, як правило, міститься закритий список типів атак, від яких провайдер готовий захищати клієнта. У разі появи нових, невідомих чи нетипових методів впливу жодних гарантій захисту вже не надається. Зважаючи на динамічність та еволюцію DDoS-методик, це створює серйозний ризик.

Не менш важливим є і питання оперативності технічної підтримки. На практиці перша реакція на повідомлення клієнта може сягати півгодини і більше. Для DDoS-атаки це надто великий проміжок часу: ресурс може стати недоступним, а збитки — відчутними.

Таким чином, часто виникає ситуація, коли саме замовник першим виявляє факт атаки та змушений інформувати провайдера. Від моменту звернення й до фактичних дій з боку постачальника проходить певний час, протягом якого зловмисники можуть кілька разів змінити тактику чи вектор атаки. Це суттєво ускладнює ручне або напівавтоматичне фільтрування трафіку, адже на аналіз і створення сигнатур витрачається набагато більше часу, ніж триває сама зміна характеру атаки.

Звідси випливає головна вимога: системи захисту від DDoS повинні діяти автоматично та майже миттєво. Виявлення аномалій та створення динамічних фільтрів має відбуватися протягом секунд, а не хвилин. Лише за таких умов можна говорити про реальну ефективність рішень.

Варто зазначити, що більшість провідних постачальників хмарних сервісів сьогодні вже використовують автоматизовані алгоритми аналізу й блокування шкідливого трафіку. Такі системи здатні швидко відсікати найпоширеніші види атак у режимі реального часу. Однак клієнтам усе одно необхідно уважно ознайомлюватися з умовами SLA та вимагати чітко прописаних гарантій швидкодії,

оскільки навіть незначна затримка може обернутися серйозними фінансовими та репутаційними втратами.

Комплексний підхід до впровадження засобів протидії атакам та вторгненням

Для того щоб забезпечити належний рівень захисту від сучасних кіберзагроз, незалежно від того, яку архітектуру рішення обрала компанія, необхідно дотримуватись комплексного підходу. Його суть полягає у створенні багаторівневої системи, де кожен елемент виконує власну роль, а разом вони формують єдиний цілісний контур безпеки.

Засоби захисту від мережевих атак, спрямованих на виснаження ресурсів серверів чи мережевого обладнання, доцільно встановлювати перед прикордонним маршрутизатором ЦОД. Це дає змогу убезпечити всю корпоративну інфраструктуру від потужних DDoS-атак, які здатні паралізувати роботу критичних сервісів. Якщо використовується зовнішній або хмарний сервіс, подібний захист реалізується автоматично, що значно знижує навантаження на внутрішні ресурси.

Важливо також мати окремий рівень протидії атакам на прикладному рівні. Такі системи повинні бути розташовані після модуля мережевого захисту, щоб надійно фільтрувати трафік, що надходить безпосередньо до серверів. Це дозволяє знизити ризик експлуатації вразливостей у web-додатках або службових протоколах, а також вчасно виявляти повільні та малопомітні атаки.

Значну роль відіграє IPS (Intrusion Prevention System). Його основне завдання полягає у блокуванні атак невеликого масштабу та спроб використання відомих вразливостей. У комплексі з іншими рішеннями IPS підвищує рівень захисту, оскільки здатний виявляти загрози ще на початкових етапах їх прояву.

Надзвичайно важливим елементом є WAF (Web Application Firewall), що відповідає за безпеку web-додатків і захист від атак рівня L7, включаючи ті, які описані в OWASP TOP-10. WAF може бути розміщений у двох варіантах: у тісному поєднанні з модулем прикладного захисту або безпосередньо перед серверами. В обох випадках він виступає критично необхідним бар’єром проти SQL-ін’єкцій, XSS-атак, обходу механізмів автентифікації та інших складних методів злому.

Багаторівнева архітектура дозволяє протистояти переважній більшості відомих атак. Єдиним винятком залишаються загрози, пов’язані з маніпуляціями протоколом BGP, для яких досі не існує універсальних рішень захисту.

Загалом комплексна система може включати такі ключові складові:

- **Cloud DDoS protection** – хмарні сервіси для очищення трафіку;
- **DDoS protection (CPE-рішення)** – обладнання, що встановлюється безпосередньо в інфраструктурі компанії;
- **Behavioral analysis** – інструменти поведінкового аналізу, зокрема IPS та WAF, які здатні виявляти аномалії у роботі користувачів і систем.

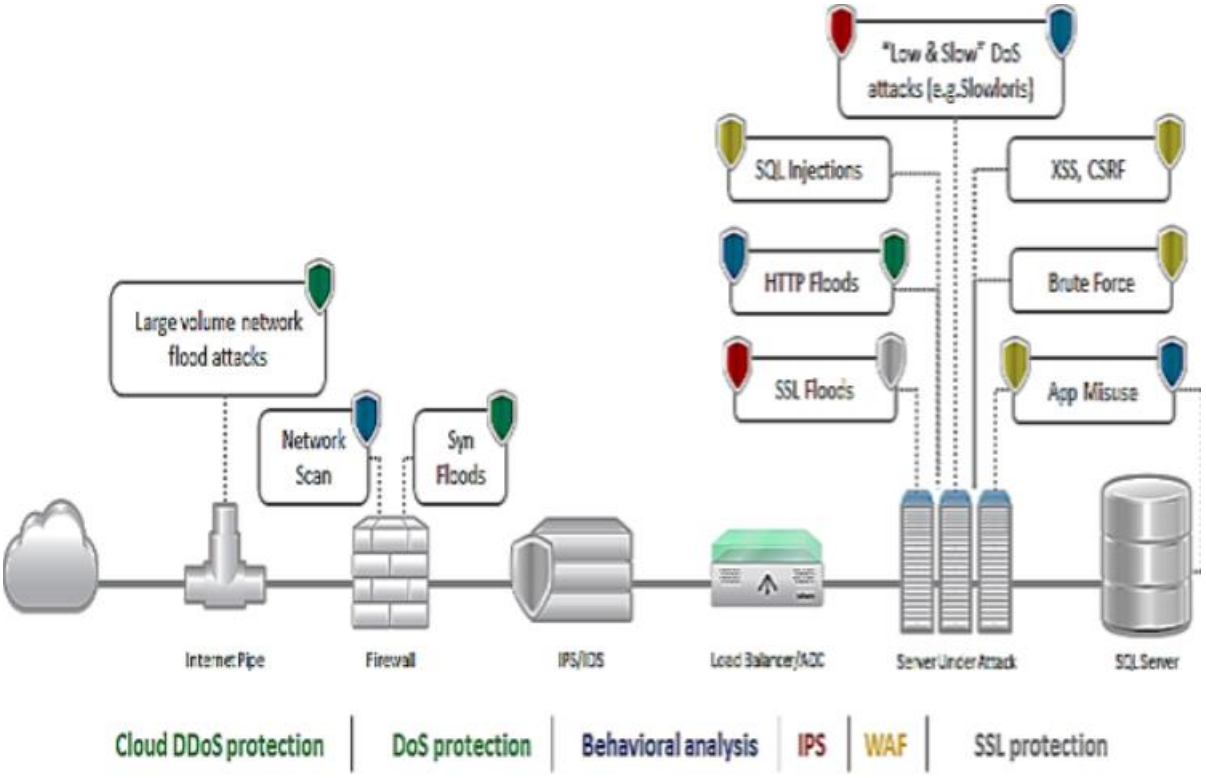


Рис. 4.3 Орієнтовна архітектура рішення захисту від DDoS

Поєднання цих компонентів забезпечує формування стійкої системи кіберзахисту, яка здатна витримати як масштабні автоматизовані атаки, так і цілеспрямовані загрози, спрямовані проти конкретної інфраструктури.

Час реагування на атаку

Сучасні можливості зловмисників дозволяють здійснювати атаки з динамічно змінюваним вектором впливу. Тип атаки, її масштаб та інтенсивність можуть змінюватися буквально за кілька хвилин, що особливо характерно для великих

ботнет-мереж, керованих централізовано. У такій ситуації використання лише ручних або навіть напівавтоматичних методів протидії втрачає сенс, оскільки швидкість роботи людини істотно нижча за темпи зміни атакуючої інфраструктури. Для аналізу трафіку, визначення характеру атаки, розробки сигнатур чи правил фільтрації потрібен час, якого у більшості випадків просто немає.

Отже, протидія має здійснюватися автоматизовано, в режимі реального часу. Система фільтрації повинна реагувати протягом секунд, а не хвилин, і робити це без необхідності втручання фахівців з інформаційної безпеки. Лише в такому випадку можна гарантувати ефективне стримування DDoS-атак та забезпечення безперебійної роботи критичних сервісів.

Захист web-додатків: виклики підтримки та супроводу

Сучасні веб-додатки постійно змінюються: додаються нові функції, розділи чи інтеграції. Це створює додаткові можливості для бізнесу, але водночас значно ускладнює завдання їх захисту. Наприклад, нова функція, здатна збільшити прибутки, може стати джерелом нових уразливостей, якщо її не супроводити адекватними заходами безпеки.

Тому сучасні рішення повинні надавати можливість оперативно адаптувати політики захисту. Найефективніший підхід — це внесення змін у режимі реального часу, що підтримує безперервний цикл оновлення програмних продуктів. Для цього застосовуються два методи: постійний моніторинг трафіку та інтеграція з системами Dynamic Application Security Testing (DAST).

WAF має автоматично виявляти будь-які зміни у веб-додатку та пропонувати нові правила безпеки. Якщо ж використовується інтеграція з DAST, то такі системи можуть сканувати оновлені зони застосунку, виявляти уразливості та створювати «віртуальні патчі» для їхнього закриття. Це дозволяє значно знизити ризики без необхідності негайного втручання у програмний код.

Мінімізація впливу на легітимних користувачів

Одним з головних завдань сучасних систем протидії атакам є збереження стабільної роботи легітимних користувачів навіть у випадку активної атаки. Якщо клієнти не можуть скористатися сервісом або швидкість його роботи значно

знижується, то фактично ціль атаки досягається, навіть якщо технічно вона блокується.

Тому системи повинні гарантувати мінімізацію негативного впливу на легальний трафік. Це означає, що користувачі не мають відчувати помітних затримок чи переривань у роботі навіть у період пікового навантаження, спричиненого атакою. Використання таких засобів, як CAPTCHA або додаткові JavaScript-тести, допустиме лише як виняток, адже вони створюють зайві бар'єри для клієнтів і можуть знизити їхню лояльність.

Моніторинг та звітність

Ефективна протидія атакам передбачає не лише фільтрацію, але й повний контроль за ситуацією. Для цього потрібні системи централізованого моніторингу та звітності, які забезпечують видимість усіх атак у режимі реального часу. Єдина консоль управління дозволяє адміністраторам контролювати роботу захисних механізмів, оцінювати ефективність застосованих фільтрів та швидко реагувати на нові інциденти.

Важливим є й об'єднання інформації з кількох вузлів чи центрів очищення в єдині панелі та звіти. Це дає змогу уникнути дублювання інструментів і забезпечує повну картину поточного стану інфраструктури. Зібрані дані можна використовувати не лише для оперативного реагування, але й для подальшого аналізу та удосконалення політик безпеки.

ВИСНОВКИ

У процесі дослідження теми захисту каналів зв’язку в критичних інфраструктурах було всебічно проаналізовано сучасні підходи, технології та архітектурні рішення, спрямовані на забезпечення надійності та безпеки інформаційного обміну в умовах зростаючих кіберзагроз. Розглянуті матеріали доводять, що комунікаційні системи, які становлять основу роботи об’єктів критичної інфраструктури, залишаються вразливими як до традиційних атак (DoS, DDoS, експлуатація відомих уразливостей), так і до нових високотехнологічних загроз, включно з перехопленням трафіку на оптоволоконних лініях, застосуванням складних методів підключення (bending, optical splitting, evanescent coupling тощо), а також використанням паразитичних каналів зв’язку та схем прихованого впливу.

Важливим результатом роботи стало узагальнення особливостей фізичного та логічного захисту мережевих з’єднань. Було показано, що навіть такі надійні технології, як волоконно-оптичні лінії, не є повністю захищеними від несанкціонованого доступу. Методи підключення до волокон (мікро- та макроізгини, V-подібні вирізи, брегівські решітки) демонструють, що витік інформації може відбуватися без фізичного пошкодження каналу. Це вимагає застосування додаткових інженерних і криптографічних заходів — від правильного полірування з’єднувачів (PC, UPC, APC) до активного моніторингу цілісності оптичної лінії, використання рефлектометрів та систем спостереження за параметрами сигналу.

Окрему увагу було приділено технологіям спектрального ущільнення (WDM, CWDM, DWDM), які дозволяють значно збільшити пропускну здатність каналів, але водночас створюють нові вектори загроз. У роботі акцентовано, що паралельно зі зростанням швидкості та ємності мережі зростають і вимоги до її захисту: необхідно контролювати роботу кожного каналу, захищати систему мультиплексування та забезпечувати надійну синхронізацію.

Проаналізовано методи протидії DDoS-атакам, які залишаються одними з найбільш руйнівних для критичної інфраструктури. Встановлено, що класичні

ручні та напівавтоматичні механізми не в змозі забезпечити своєчасну фільтрацію аномального трафіку. Сучасні системи повинні працювати в автоматичному режимі з реакцією протягом секунд, застосовувати багаторівневу архітектуру (CPE-рішення, хмарні платформи та гібридні моделі), інтегрувати механізми WAF, IPS, UEBA та системи поведінкового аналізу. Важливим є також використання Anycast-маршрутизації, балансувальників навантаження, honeypot-технологій, аналітики користувацької поведінки та потоків Threat Intelligence для раннього виявлення ботнетів.

У роботі показано, що для досягнення стійкості інфраструктурних систем недостатньо лише встановити окремі рішення — необхідний комплексний підхід. Його ключовими складовими є: шифрування даних на транспортному та прикладному рівнях, постійний моніторинг і звітність, адаптивні механізми реагування на загрози, а також організаційні заходи — підготовка персоналу, чітко прописані SLA між замовником і провайдером захисних послуг, здатність до масштабування та інтеграції нових технологій.

Таким чином, можна зробити висновок, що захист каналів зв’язку в критичних інфраструктурах є багаторівневим завданням, яке потребує одночасного поєднання інженерних рішень, сучасних програмно-апаратних засобів і організаційних механізмів. Лише гармонійна інтеграція цих елементів дозволить мінімізувати ризики витоку інформації, знизити ймовірність успішних атак і забезпечити безперебійну роботу критично важливих сервісів для суспільства та держави.

ПЕРЕЛІК ПОСИЛАНЬ

1. Krutz, R. L. Securing SCADA Systems. Wiley, 2006. – Практичний огляд безпеки каналів та протоколів у SCADA.
2. Radvanovsky, R., Brodsky, J. Handbook of SCADA/Control Systems Security. CRC Press, 2016. – Повний довідник із захисту комунікацій у системах управління.
3. Colbert, E. J. M., Kott, A. (eds.) Cyber-security of SCADA and Other Industrial Control Systems. Springer, 2016. – Міжнародна збірка наукових статей.
4. Knapp, E. D., Langill, J. T. Industrial Network Security. Syngress, 2nd Ed., 2015. – Охоплює SCADA, Smart Grid та канали зв’язку.
5. Wiles, J., Claypoole, T., Drake, P. Techno Security’s Guide to Securing SCADA. Syngress, 2008. – Прикладні підходи до захисту каналів SCADA.
6. Kogut, Yu. Кібервійна та безпека об’єктів критичної інфраструктури. Сідкон, 2021.
7. Babayev, D., et al. SCADA Security: Protecting Critical Infrastructure. Artech House, 2022. – Новітні підходи до безпеки SCADA.
8. Manoj, K. S. Industrial Automation with SCADA. Notion Press, 2019. – Про SCADA – комунікації та їх захист.
9. Fries, S., Falk, R. Ensuring Secure Communication in Critical Infrastructures. – ResearchGate, 2016.
10. Khalili, A., et al. SCADA Communication Protocols: Vulnerabilities, Attacks and Possible Mitigations. – International Journal of Critical Infrastructure Protection, 2013.
11. Beigi, M. R., et al. Secure and Reliable Communications for SCADA Systems. – International Journal of Communications, 2012.
12. Henze, M., et al. Securing Wireless Communication in Critical Infrastructure: Challenges and Opportunities. – IEEE Communications Magazine, 2023.
13. Srivastava, A., et al. Stealthy Deception Attacks Against SCADA Systems. – arXiv preprint arXiv:1706.09303, 2017.

14. Srivastava, A., Hahn, A. Cybersecurity for SCADA Systems. – IEEE Security & Privacy, 2015.
15. Amin, S., et al. Impact Assessment of Cyberattacks on Power Systems. – IEEE Transactions on Smart Grid, 2018.
16. Voyiatzis, A. G. A Survey on Security Challenges in SCADA Networks. – IEEE Access, 2019.
17. NIST SP 800-82 Rev.3 – Guide to Operational Technology (OT) Security. NIST, 2022.
18. IEC 62351 Series – Power systems management and associated information exchange – Data and communications security. IEC, 2007-2023.
19. ENISA Report (European Union Agency for Cybersecurity) – Communication Network Interdependencies in Critical Infrastructures, 2020.
20. OECD Report – Protection of Critical Information Infrastructures: Communication Networks Security, 2019.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

КВАЛІФІКАЦІЙНА РОБОТА

ЗАХИСТ КАНАЛІВ ЗВ’ЯЗКУ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ

Виконав:
студент групи ТСДМ-61
Віталій БУРЧЕНКО

МЕТА РОБОТИ ТА АКТУАЛЬНІСТЬ

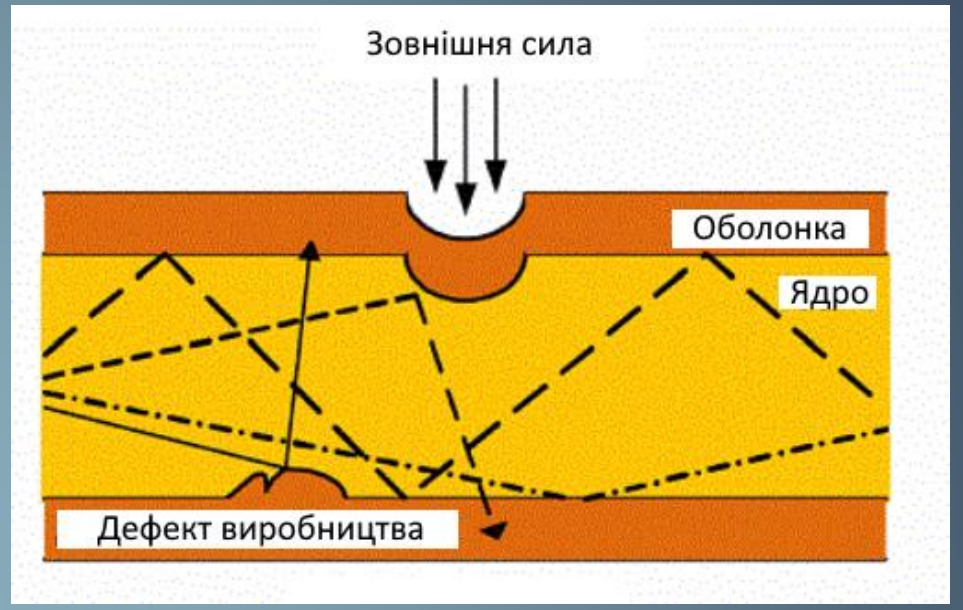
- Мета роботи – аналіз вразливостей оптоволоконних каналів зв’язку, дослідження фізичних методів перехоплення інформації та розробка рекомендацій щодо підвищення стійкості оптичних ліній до інтрузивних і неінтрузивних атак.
- Об’єкт дослідження – волоконно-оптичні лінії зв’язку як частина телекомунікаційної інфраструктури.
- Предмет дослідження – фізичні вразливості оптоволоконних каналів та методи їх несанкціонованого підключення, включно з мікрозгинами, макрозгинами, оптичним розщепленням, евансцентним підключенням і розсіюванням сигналу.

Актуальність.

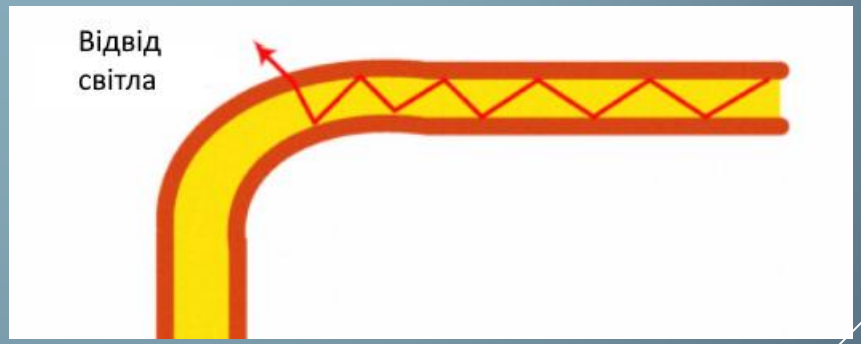
- Сучасні телекомунікаційні системи є критично важливими для функціонування державних, військових, фінансових, енергетичних та корпоративних структур. Передавання більшості стратегічних даних здійснюється саме через волоконно-оптичні лінії зв’язку, які традиційно вважалися майже недоступними для перехоплення. Однак розвиток технологій, поява високочутливих сенсорів, нових типів мікрозгинань, евансцентних підключень, оптичних спліттерів та методів розсіювання показали, що фізичний рівень ВОЛЗ не є абсолютно захищеним. В умовах гібридних загроз, інформаційних операцій та зростання частки шифрованих сервісів особливої ваги набуває питання фізичної безпеки оптоволоконних ліній. Захист від інтрузивних і неінтрузивних атак стає не менш важливим, ніж криптографічні механізми. Саме тому дослідження методів перехоплення, моделювання втрат при згинанні, аналіз фізичних уразливостей та розробка практичних рекомендацій із захисту оптичних каналів є актуальним, практично значущим і стратегічно важливим завданням.

МЕТОДИ АТАКИ НА ОПТОВОЛОКОННІ КАНАЛИ ЗВ’ЯЗКУ

- Оптичні волокна не є повністю захищеним середовищем — їх можна перехоплювати як інтрузивними, так і неінтрузивними методами. Найнебезпечнішими є непомітні способи, зокрема мікро- та макрозгини, що змінюють умови повного внутрішнього відбиття й спричиняють витік світла. Інші методи включають оптичне розщеплення, еванесцентне з’єднання, V-подібні вирізи та використання розсіювання (Бреггівські решітки). Історичні інциденти свідчать, що такі втручання реальні та складні для виявлення. Основні засоби протидії: моніторинг цілісності волокна, контроль оптичних параметрів, OTDR та обов’язкове застосування наскрізного шифрування.



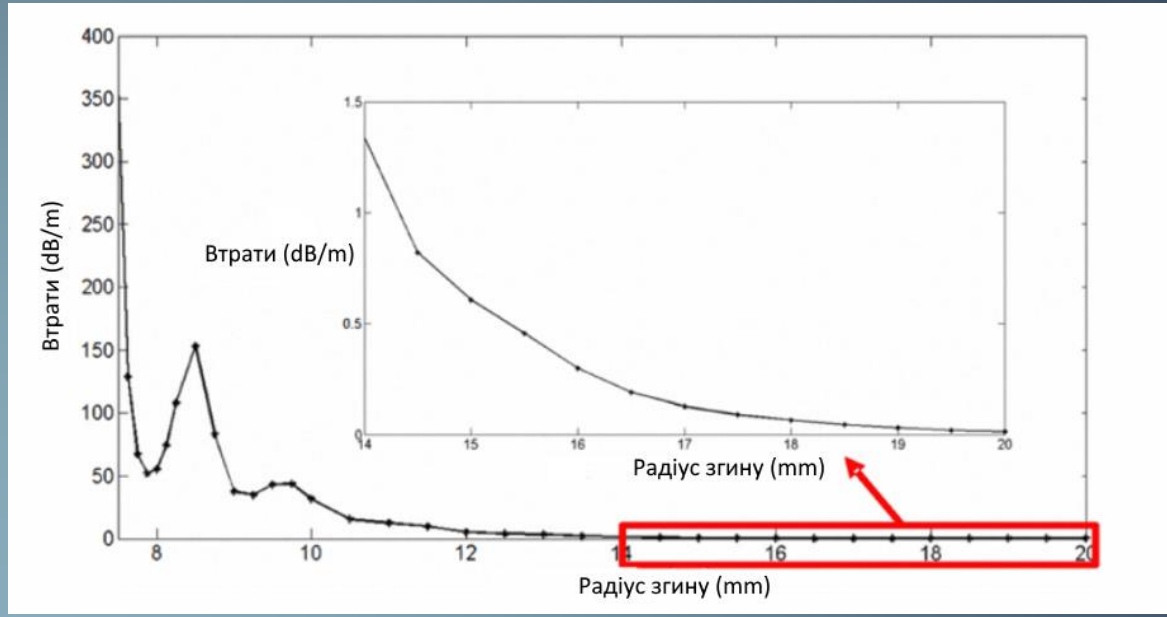
Мікрозгин



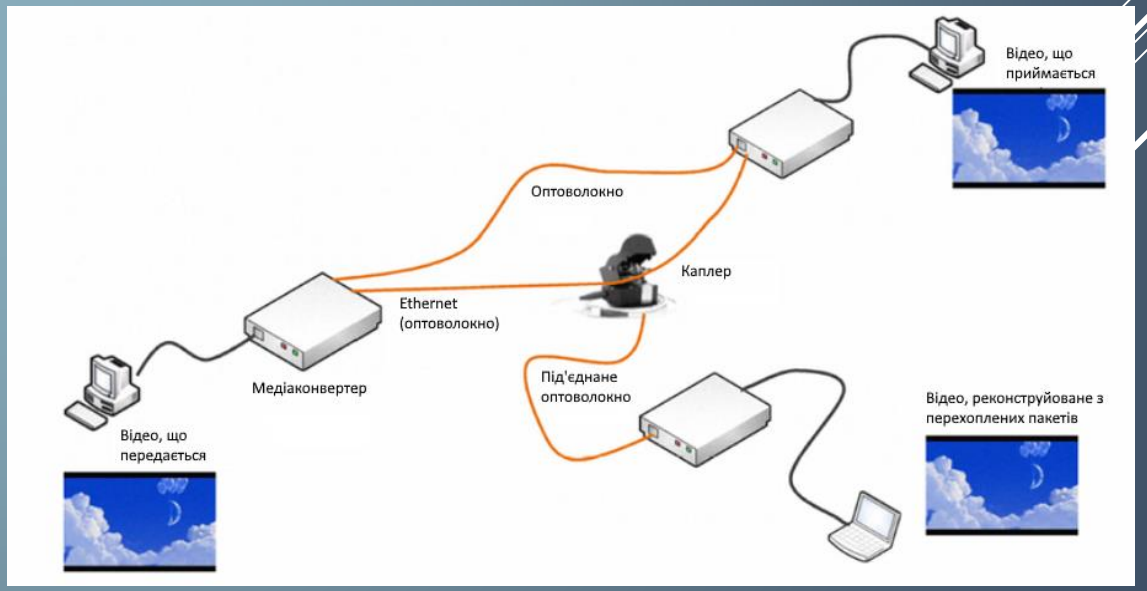
Макрозгин

МОДЕЛЮВАННЯ МЕТОДІВ

- Для оцінки втрат при згинанні SMF-28 застосовано повновекторний FEM-розв’язувач рівнянь Максвелла, що дозволило змоделювати поведінку фундаментальної моди та визначити залежність втрат від радіуса згину. Показано, що при $\rho < 10$ мм втрати різко зростають, а при $\rho > 15$ мм залишаються мінімальними.
- Експериментально досліджено можливість перехоплення частини оптичного сигналу через згин волокна. Отримані .pcap-дампи дали змогу частково відновити метадані й фрагменти прикладових даних, хоча якість залежала від шумів і неповноти потоку. Це підтверджує необхідність фізичного захисту ліній і наскрізного шифрування.



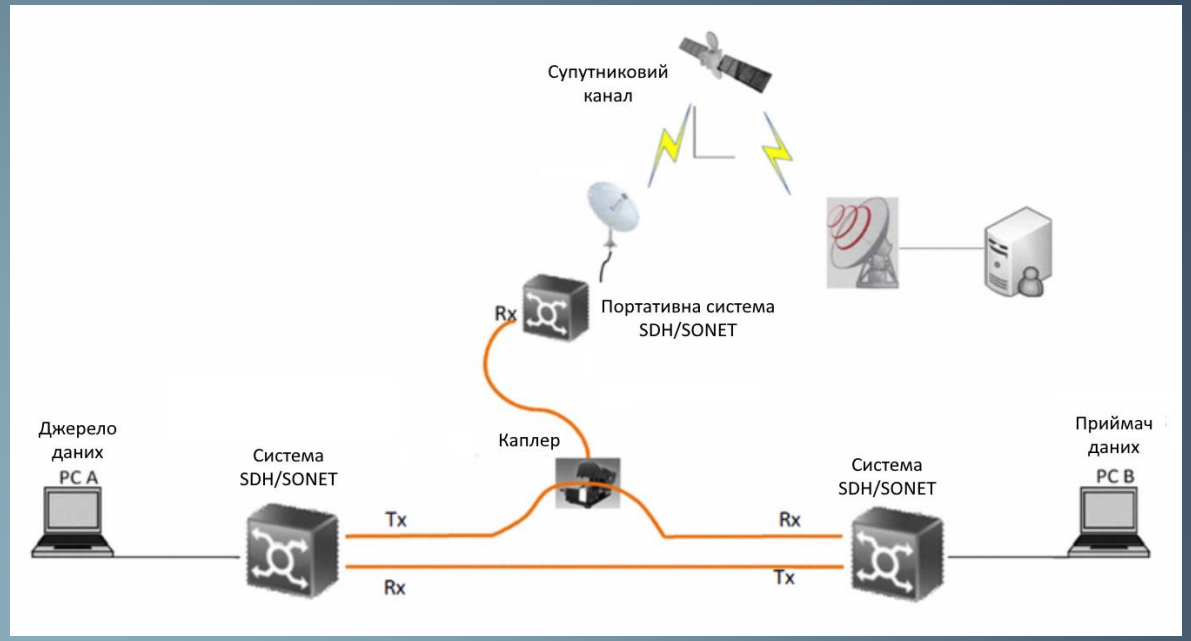
Чисельна оцінка втрати на вигині, як функції від радіусу згину



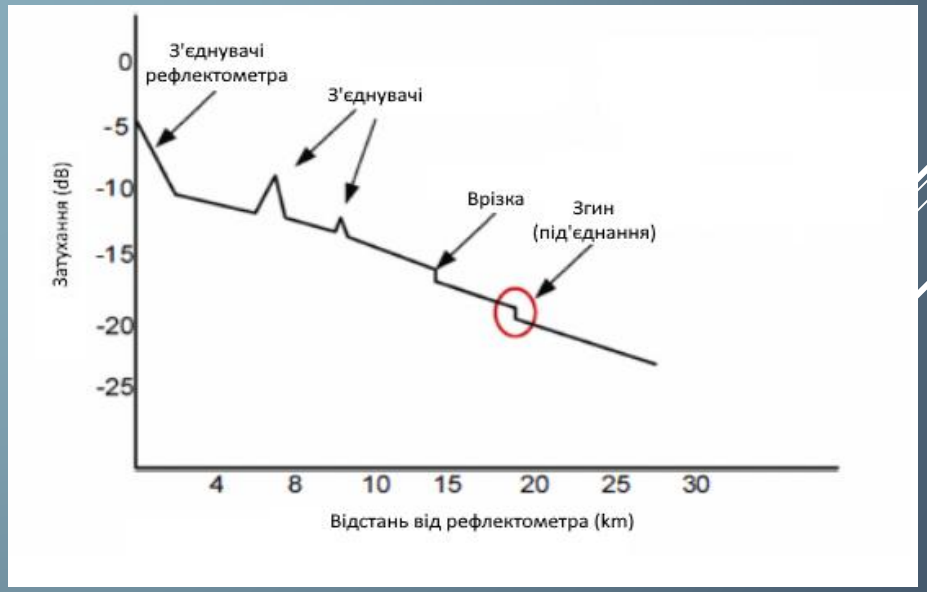
Експериментальна схема для приєднання до волокна методом зигину

ПОДАЛЬШІ СЦЕНАРІЇ

- Експеримент проводився на Ethernet-компонентах, але в реальних мережах можливі сценарії з використанням SDH/SONET, де через високу швидкість потоків доцільна віддалена обробка. Вона дозволяє уникнути швидкого заповнення сховищ та дає експертам можливість аналізувати дані у спеціалізованому центрі. Сценарії включають бездротове підключення, передачу через мікрохвильові або супутникові канали та теоретичне введення сигналу. Захист забезпечують моніторинг волокон (резервні нитки, електричні датчики, аналіз мод, OTDR), використання bend-insensitive fiber та шифрування (IPsec, канальний рівень). Такі методи ускладнюють непомітне втручання та підвищують стійкість оптичних ліній.

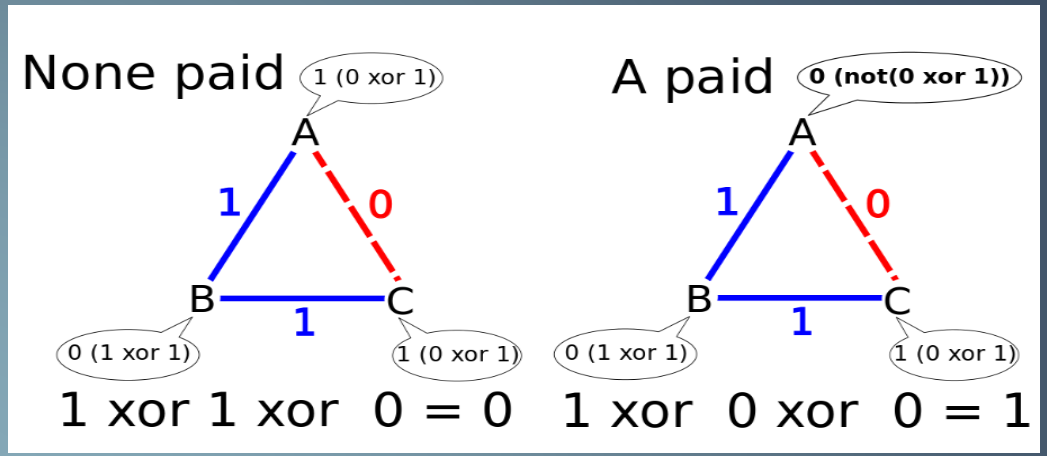


Сценарій підключення з віддаленою обробкою

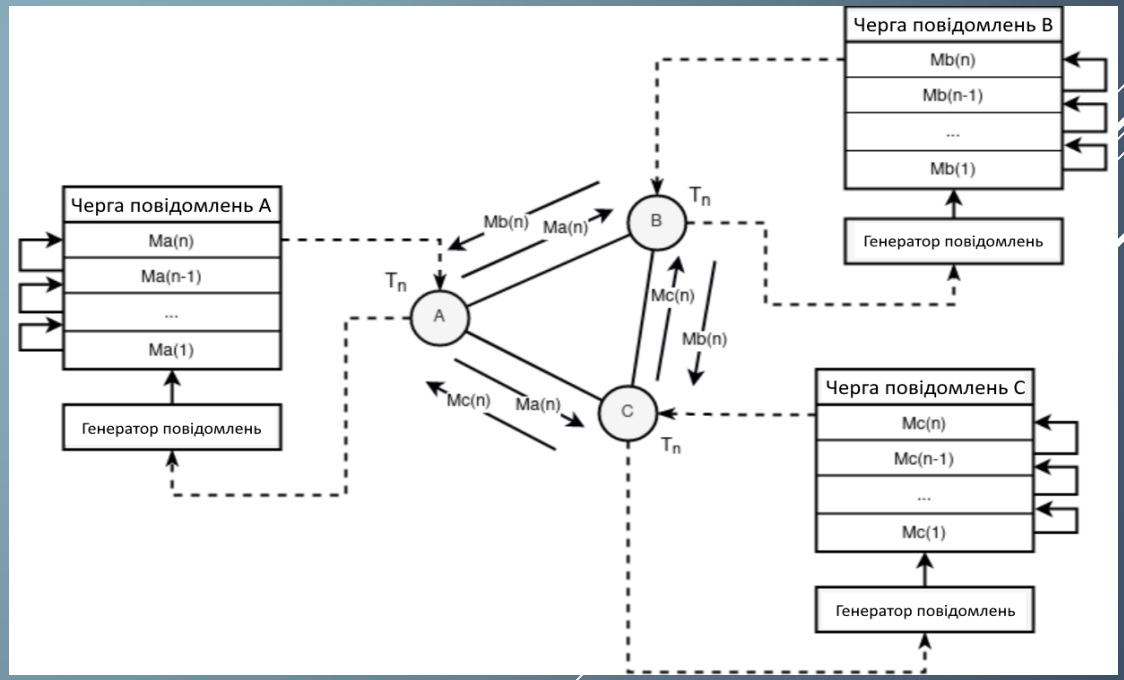


Пошук підключення на оптичній трасі за допомогою оптичного рефлектометра

- Сучасні цифрові сервіси стали ключовою частиною критичної інфраструктури, але їхня централізація створює ризики монополізації, витоку даних і зовнішнього контролю. Користувацька інформація циркулює між платформами, формуючи залежність і загрожуючи безпеці держави та бізнесу. Зменшити ризики допомагають клієнт-безпечні застосунки з E2E-шифруванням, анонімні мережі та приховані канали зв'язку. Перспективним напрямом є абстрактні анонімні мережі, незалежні від топології, IP-адрес чи маршрутизації. Моделі на основі DC-проблеми та черг забезпечують теоретично доведену анонімність і можуть стати основою майбутніх безпечних комунікацій у критичній інфраструктурі.
- Проблема «обідаючих криптографів» демонструє спосіб анонімної передачі даних у групі без розкриття відправника, однак класична модель має обмеження масштабованості та потребує прямого з'єднання між усіма учасниками. Розвитком цієї ідеї є задача на основі черг, де кожен вузол надсилає справжні або фіктивні повідомлення у фіксовані моменти часу, формуючи мережу FIFO-черг із наскрізним шифруванням. Така архітектура забезпечує стійкість до аналізу трафіку, знімає централізаційні обмеження та використовується в системах HLS/HLM/HLT для створення масштабованих анонімних мереж.



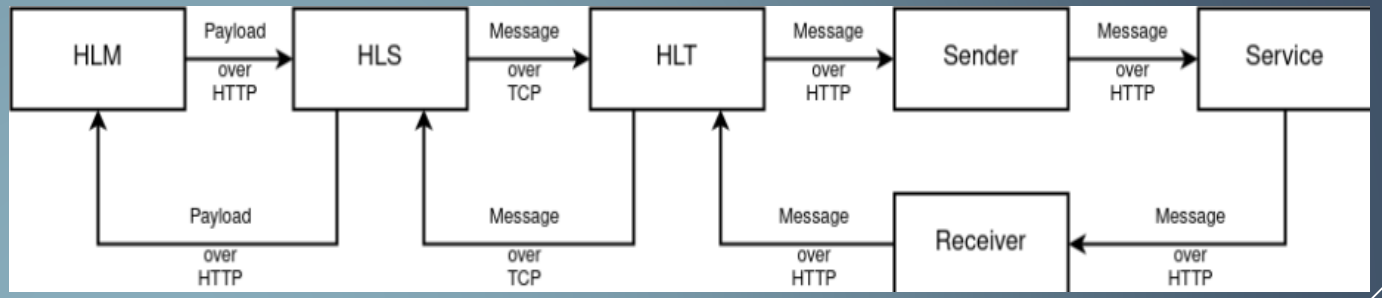
Dining Cryptographers Problem



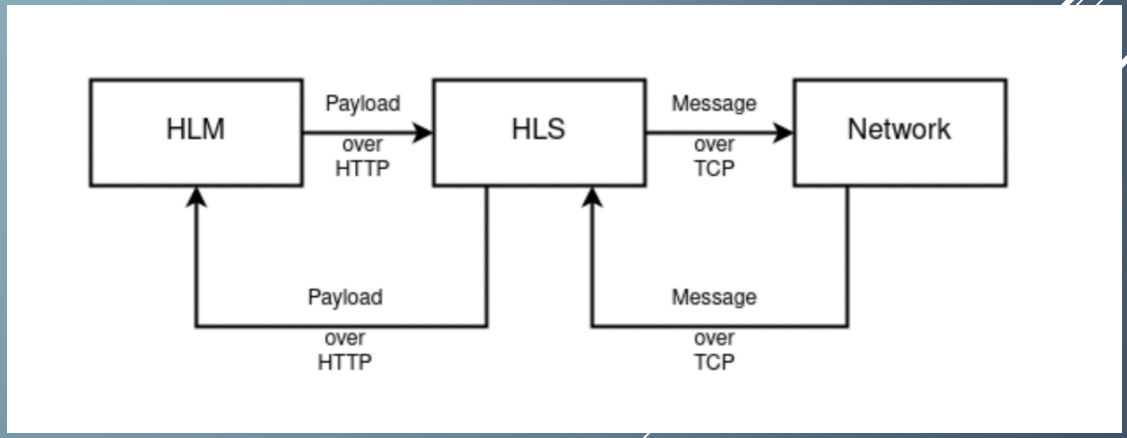
Завдання на базі черг

СТВОРЕННЯ АРХІТЕКТУР

- Комбінація таємного каналу зв’язку з абстрактною анонімною мережею дозволяє приховано передавати зашифровані повідомлення, маскуючи їх у великих централізованих сервісах. У моделі Hidden Lake модулі HLS, HLM і HLT перетворюють Payload у Message та далі у F(Message), який зберігається як звичайні дані у сторонньому сервісі, звідки Receiver витягує й розшифровує його. Переваги підходу — маскування трафіку, економія ресурсів і масштабованість; ризики — залежність від зовнішніх платформ, можливість виявлення за поведінковими ознаками та юридичні обмеження. Модульність архітектури забезпечує гнучкість і адаптивність.



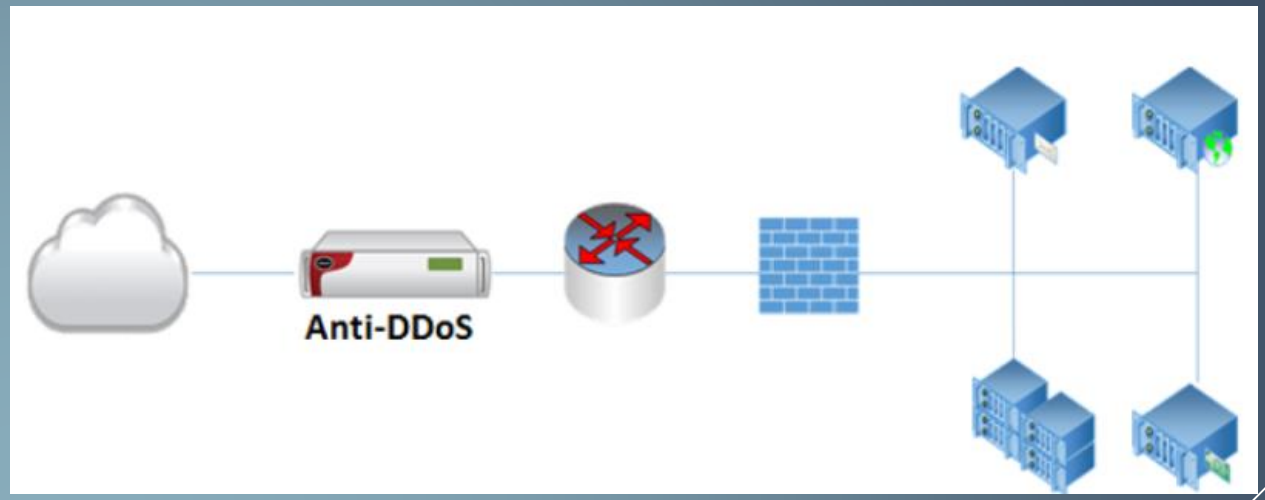
Архітектура таємного каналу зв'язку при використанні HLS, HLM та HLT



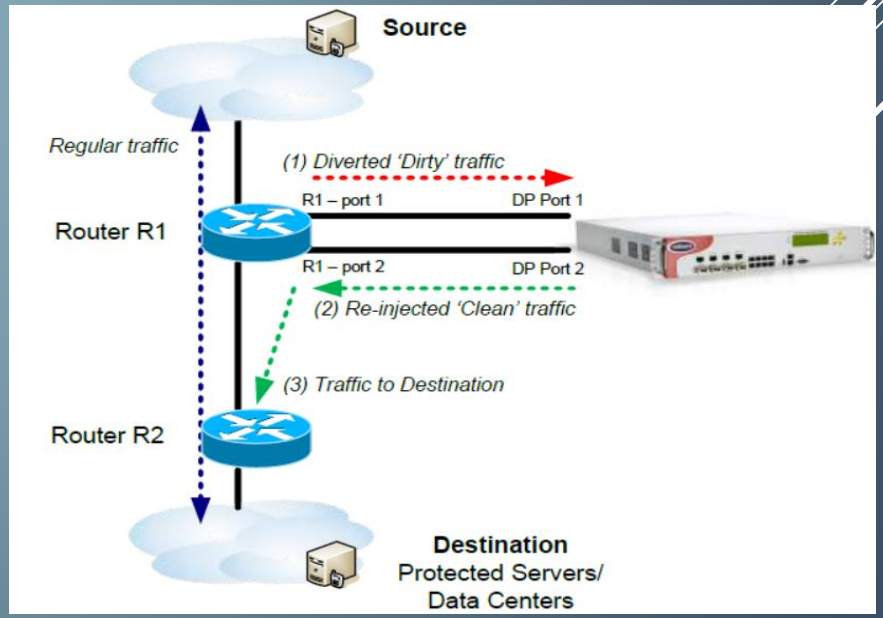
Архітектура анонімізації трафіку при використанні HLS та HLM

СПОСОБИ ВПРОВАДЖЕННЯ КОМПОНЕНТІВ ЗАХИСТУ

- Метод встановлення «в розрив» передбачає пропуск усього трафіку через систему фільтрації, що забезпечує максимальний контроль над атаками, але створює ризик зупинки сервісів у разі збою, тому потребує резервування або режиму bypass. Такий підхід дозволяє інспектувати трафік у реальному часі, формувати профілі нормальної активності, виявляти аномалії та динамічно блокувати шкідливі запити. Альтернативна схема «out-of-path» працює поза основним маршрутом і передбачає перенаправлення трафіку на зовнішні центри очищення, що забезпечує гнучкість, але має більші затримки, залежить від процедур переадресації та неефективна проти зашифрованих атак через обмеження SSL/TLS і PFS. Обидва методи часто поєднуються в гібридних рішеннях для досягнення балансу між контролем, безпекою та відмовостійкістю.



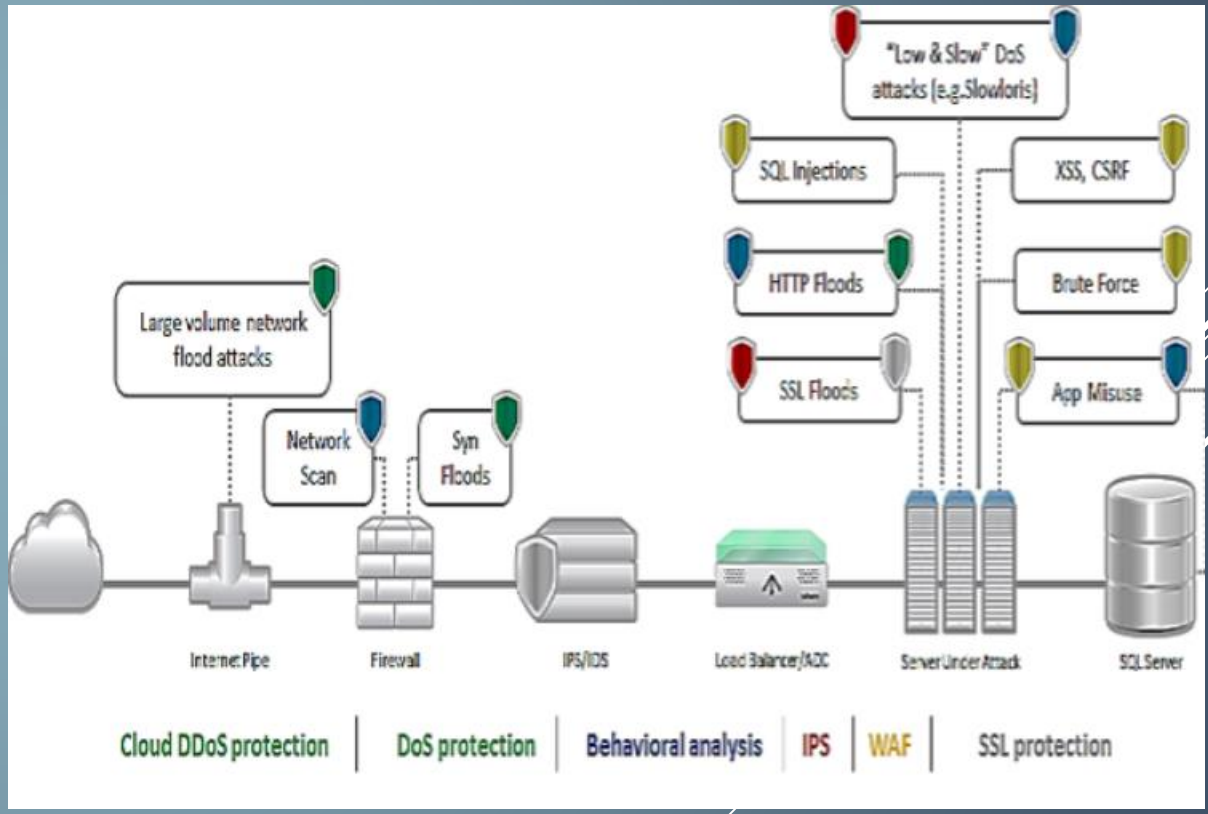
Метод встановлення «в розрив»



Метод встановлення «out-of-path»

ПІДХОДИ ДО РЕАЛІЗАЦІЇ РІШЕТЬ ЗАХИСТУ ВІД DDOS

- Гібридна архітектура захисту від DDoS поєднує можливості локальних CPE-рішень і хмарних сервісів, забезпечуючи швидку реакцію на прикладні атаки та високу стійкість проти масових volumetric-ударів. У моделі комбінування локальний CPE фільтрує транспортні та L7-атаки, тоді як хмара нейтралізує хвилі великої інтенсивності; у моделі резервування хмара підключається лише тоді, коли локальна система не справляється. Обидва підходи мають переваги та обмеження, пов'язані зі SLA, пропускною здатністю, часом перемикання, інспекцією SSL та потребою в автоматизації. Ефективний захист передбачає багаторівневу архітектуру з CPE-фільтрацією, хмарним очищенням, IPS/WAF, поведінковим аналізом, постійним моніторингом і мінімальним впливом на легітимних користувачів. Ключовим чинником успіху є автоматичне виявлення й блокування атак у режимі реального часу, регулярне тестування та коректно визначені SLA, що гарантують швидкодію та надійність захисних механізмів.



Орієнтовна архітектура рішення захисту від DDoS

ВИСНОВКИ

- У роботі комплексно досліджено питання захисту каналів зв’язку в критичних інфраструктурах, проаналізовано сучасні загрози на фізичному та мережевому рівнях, включаючи DDoS-атаки, експлуатацію уразливостей та високотехнологічні методи перехоплення даних на оптоволоконних лініях (мікро- й макрозгини, optical splitting, evanescent coupling, брегівські решітки).
- Показано, що навіть високонадійні ВОЛЗ залишаються вразливими без додаткових інженерних, криптографічних та організаційних заходів.
- Узагальнено сучасні методи протидії DDoS-атакам, які потребують автоматизації, багаторівневого підходу та використання хмарних, CPE- і гібридних рішень.
- Підкреслено необхідність комплексного підходу до захисту, що включає шифрування, моніторинг, поведінкову аналітику, організаційні процедури та адаптивні системи реагування.
- Зроблено висновок, що лише інтеграція технічних, програмних та організаційних засобів забезпечує стійкість критичних комунікаційних систем.

ДЯКУЮ ЗА УВАГУ!

Протокол аналізу звіту подібності науковим керівником

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

Автор: Віталій БУРЧЕНКО

Назва: ЗАХИСТ КАНАЛІВ ЗВ’ЯЗКУ В КРИТИЧНИХ ІНФРАСТРУКТУРАХ

Координатор: Юрій МЕЛЬНИК

Підрозділ: ННІТ

Коефіцієнт подібності 1:0.3

Коефіцієнт подібності 2:0

Тривога: 0

Після аналізу Звіту подібності констатую наступне:

☐ виявлені в роботі запозичення є сумлінними і не мають ознак плагіату. Тому робота визнається самостійною і допускається до захисту;

☐ виявлені в роботі запозичення не мають ознак плагіату, але їх надмірна кількість викликає сумніви щодо цінності роботи і самостійності її автора. Роботу направити на доопрацювання;

☐ виявлені в роботі запозичення є недобросовісними і мають ознаки плагіату або в ній містяться навмисні спотворення тексту, що вказують на спроби приховування недобросовісних запозичень. У зв'язку з чим, робота не допускається до захисту.

…… ……

Дата *Підпис Наукового керівника*