ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «Побудова захищеної та відмовостійкої корпоративної мережевої інфраструктури»

на здобуття освітнього ступеня бакалавра
зі спеціальності 123 Комп'ютерної інженерії
(код, найменування спеціальності)
освітньо-професійної програми Комп'ютерна інженерія
(назва)

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

	Григорій НІКІТЧЕНКО
(підпис)	*Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. КСЗ-51
Григорій НІКІТЧЕНКО
Ім'я, ПРІЗВИЩЕ
Керівник: Ірина КУЗЬМІЧ
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ
Рецензент:
науковий ступінь, вчене звання Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій

Кафедра Комп'ютерної інженерії

Ступінь вищої освіти бакалавр

Спеціальність 123 – Комп'ютерної інженерії

Освітньо-професійна програма Комп'ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувач кафедри
Комп'ютерної інженерії
_____ Наталія ЛАЩЕВСЬКА
_____
«_____» _____ 2025р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Нікітченко Григорій Олександрович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Побудова захищеної та відмовостійкої корпоративної мережевої інфраструктури
керівник кваліфікаційної роботи Ірина КУЗЬМІЧ,
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «24» лютого 2025р. № 56
2. Строк подання кваліфікаційної роботи «5» червня 2024р.
3. Вихідні дані до кваліфікаційної роботи: науково-технічна література; технології FTTH та PON; маршрутизація трафіку з використанням адміністративної відстані (AD); топологія мережі, логічна топологія (Layer 3), фізична топологія (Layer 2); VPN-тунелі; термінал ONU; модем ADSL; мережеві протоколи: PPPoE, DHCP, L2TP;
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Поняття інформаційної безпеки сучасності
2. Побудова відмовостійкої корпоративної комп'ютерної мережі
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання «24» лютого 2025р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Збір даних	25.02-30.03.2025	Виконано
2	Обробка матеріалу	30.03-07.04.2025	Виконано
3	Розробка теоретичної частини	07.04-14.04.2025	Виконано
4	Розробка моделі мережі	14.04-25.04.2025	Виконано
5	Висновки за результатами аналізу	25.04-15.05.2025	Виконано
6	Оформлення пояснювальної записки	15.05-20.05.2025	Виконано
7	Розробка презентації	21.05-25.05.2025	Виконано
8	Передзахист	27.05-29.05.2025	Виконано
9	Здача в деканат	29.05-04.06.2025	Виконано

Здобувач вищої освіти _____ Григорій НІКІТЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Ірина КУЗЬМІЧ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня бакалавра: 40 стор., 10 рис., 3 табл., 34 джерел.

Мета роботи – Побудова захищеної та відмовостійкої корпоративної мережевої інфраструктури

Об'єкт дослідження – Система мережевої безпеки корпоративної інфраструктури, що забезпечує функціонування мережі як єдиного цифрового середовища.

Предмет дослідження – Процеси, концептуальні моделі та методи модернізації архітектури корпоративної мережевої інфраструктури з метою підвищення її стійкості до мережевих загроз

Короткий зміст роботи: Інформаційна безпека та відмовостійкість мережі, є невід'ємними компонентами, будь-якої, корпоративної мережевої інфраструктури. Не дивлячись на те, що більшість можливих векторів атак на мережу компанії, або ж організації, вже досить давно відомі фахівцям з кібербезпеки, мережевим та комп'ютерним інженерам, завжди залишається шанс того, що втручання відбудеться не за допомогою впливу на інфраструктуру ззовні, а з причини необачності людини, що працює в компанії, або ж належить до тої чи іншої організації. Для зменшення можливості виникнення подібних інцидентів, є досить важливим, проведення ознайомчих зустрічей та/або тренінгів з кібер-гігієни, для співробітників, фахівцями відділів IT та Кібербезпеки.

Окремим пунктом можна виділити відмовостійкість мережі, оскільки від цього на пряму залежить дохід, працездатність, та збереження даних клієнтів та співробітників компанії. Зазвичай, для цього використовується обладнання з можливістю підключення одразу двох провайдерських підключень (ISP), пристрої резервного живлення обладнання, динамічна маршрутизація, Site-to-Site VPN-тунелі, та використання, хоч і застарілих, але все ще працюючих та

стабільних методів підключення до мережі Інтернет.

Під час проведення дослідження, було побудовано, повністю відмовостійку мережеву інфраструктуру між головним офісом та 12 філіями туристичної фірми, з використанням FTTH, PON, VPN-тунелів, ADSL, та адміністративних відстаней для автоматичної зміни маршруту трафіку, для мінімізації часу простою, та максимального аптайму, незалежно від збоїв на стороні провайдера.

КЛЮЧОВІ СЛОВА: КОРПОРАТИВНА МЕРЕЖА, VPN-ТУНЕЛЬ, L2TP, ISP, ІНФОРМАЦІЙНА БЕЗПЕКА, АДМІНІСТРАТИВНА ВІДСТАНЬ, МАРШРУТИЗАЦІЯ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ..... 9
ВСТУП..... 10
1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ МЕРЕЖЕВОЇ БЕЗПЕКИ..... 11
1.1 Поняття мережевої безпеки: генезис, сучасність..... 11
1.2 Способи реалізації безпеки підприємств 17
2 АНАЛІТИЧНО-ДОСЛІДНИЦЬКЕ РІШЕННЯ.....24
2.1 Провідні фактори впливу на безпеку підприємства 24
2.2 Проблематика та постановка завдання..... 25
2.3 SWOT-аналіз безпеки до модернізації……26
2.4 Варіанти вирішення та їх порівняння…….....28
2.5 Методика оцінки ефективності після модернізації……30
3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ ТА ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ 32
3.1 Об'єкт дослідження..... 32
3.2 Механізми модернізації корпоративної мережевої інфраструктури туристичної фірми..... 37
3.3 Верифікація результатів дослідження..... 41
3.4 Порівняльний аналіз ризиків до та після модернізації корпоративної мережевої інфраструктури……47
ВИСНОВКИ..... 49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ..... 51
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ..... 55

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД	бази даних
ІБ	інформаційна безпека
ІС	інформаційна система
КМ	корпоративна мережа
ПЗ	програмне забезпечення
СМ	сегментація мережі
EDMS	Electronic Document Management Systems

ВСТУП

З огляду на те, що ефективність функціонування мережі визначається такими параметрами, як продуктивність, масштабованість, надійність, керованість, вартість та рівень захисту інформації, проектування корпоративної інфраструктури повинно здійснюватися на основі системного аналізу альтернативних архітектурних рішень. Особливої актуальності набуває питання вибору раціональної структурної схеми з урахуванням специфіки підприємства, особливостей його предметної області та потенційних загроз, пов’язаних з витоком, модифікацією чи блокуванням критично важливої інформації. На практиці це ставить перед розробниками завдання оптимізації мережі за заданими критеріями функціональності, із одночасним дотриманням принципів інформаційної безпеки.

У досліджуваному випадку, необхідно розробити та впровадити відмовостійку інфраструктуру туристичної фірми, яка складатиметься з центрального офісу та 12-ти відокремлених філій, яким необхідний прямий зв’язок із центральним сервером.

1 ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Поняття мережевої безпеки: генезис, сучасність

У реаліях цифрової трансформації, що охопила сучасний глобалізований світ, питання мережевої безпеки вийшло на передній план як один із критичних чинників стабільної діяльності підприємств. Організаціям необхідно гарантувати безпечний, постійний доступ співробітників до внутрішніх ресурсів незалежно від місця чи часу, що вимагає цілісної, адаптивної та динамічної стратегії безпеки. Така стратегія має враховувати не лише нарощування надійності мережевої інфраструктури, але й забезпечення оперативного управління ризиками, а також проактивний захист від нових, постійно вдосконалюваних кіберзагроз.

Особливої актуальності це набуває в умовах зростання популярності гібридних моделей зайнятості та широкого використання персональних пристроїв – смартфонів, ноутбуків, планшетів – для виконання службових обов’язків. Такий підхід, хоча й підвищує мобільність та продуктивність працівників, водночас створює нові вектори атаки та збільшує площу потенційних вразливостей. Хакерські угруповання користуються цим, застосовуючи дедалі витонченіші методи проникнення, соціальної інженерії та маскування.

У дослідженні, проведеному Slashdotmedia, у якому брали участь фахівці з IT та керівники підрозділів мережевої безпеки, на запитання «Коли ви обираєте рішення з мережевої безпеки, які чинники є найважливішими для вашої компанії?» майже половина респондентів (приблизно 50%) на перше місце поставили надійність обраного рішення, вказуючи на зростання ролі довіри до технологій у період цифрової вразливості.

Ігнорування чи недооцінка загроз, пов’язаних із безпекою мережі, може мати ланцюгову реакцію негативних наслідків. Компрометація інформаційних

систем здатна спричинити втрату або витік чутливих даних, перебої у роботі сервісів, блокування доступу працівників і клієнтів до необхідних ресурсів, а також відтік клієнтської бази через втрату довіри. У перспективі це може призвести до зменшення ринкової частки компанії та зростання витрат на відновлення репутації.

До того ж, наслідки порушення мережевої безпеки не обмежуються лише інформаційними втратами. Наприклад, недоступність веб-сайту у годину-пік може не тільки позбавити компанію прибутку за рахунок втраченої транзакційної активності, але й спровокувати хвилю негативного піару, який в довгостроковій перспективі матиме куди масштабніші наслідки для продажів. В окремих галузях, зокрема у фінансовому секторі, охороні здоров'я чи критичній інфраструктурі, законодавчо встановлені високі вимоги до доступності послуг. Їх порушення здатне спричинити регуляторні санкції, штрафи або навіть тимчасову втрату ліцензії на діяльність.

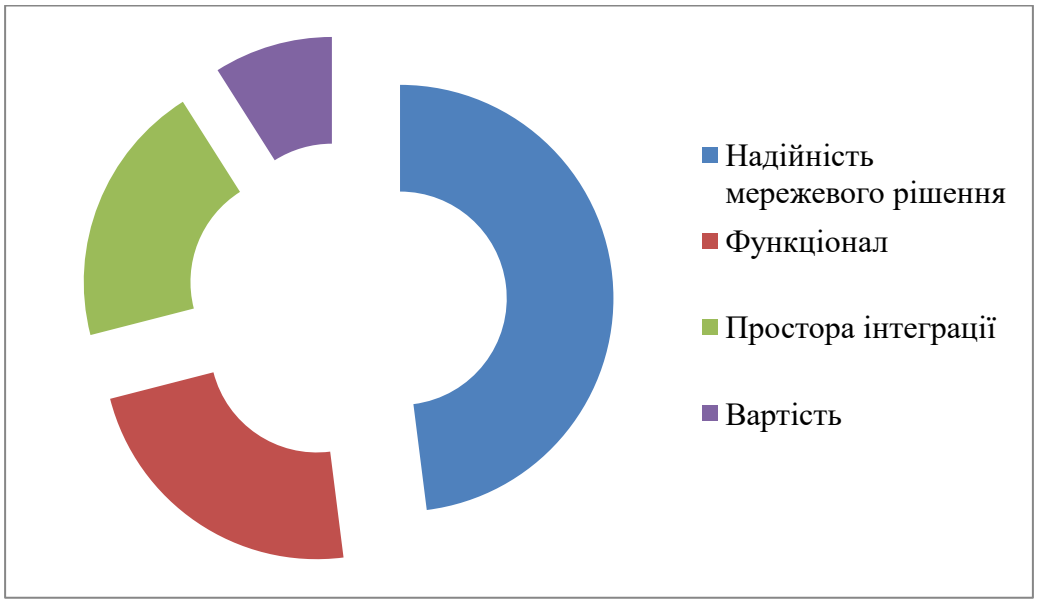


Рисунок 1.1 – Діаграма відповідей на поставлене запитання: Коли ви вибираєте рішення з мережевої безпеки, які фактори найбільш важливі для вашої компанії?

Поруч із надійністю рішень, яка була визнана найважливішою майже 48% респондентів, на перший план виходить і низка інших важливих чинників, що безпосередньо впливають на вибір стратегії мережевої безпеки в умовах обмежених ресурсів. Зокрема, близько 23% IT-фахівців звернули увагу на вартість впровадження рішень як на критичну проблему, що впливає на здатність компаній ефективно захищатися в умовах суттєво скорочених IT-бюджетів останніх років.

Ще приблизно 20% опитаних вказали на простоту інтеграції рішень у наявну інфраструктуру як один із визначальних чинників. Це свідчить про посилений тиск на IT-відділи, яким доводиться забезпечувати комплексний захист, працюючи в умовах постійного дефіциту часу, персоналу та фінансування. В умовах таких викликів компанії прагнуть обирати рішення, які не лише забезпечують захист, а й можуть бути швидко впроваджені без значного реінжинірингу системи.

Варто наголосити, що лише 9% респондентів окремо виділили мережеві функції (функціонал) як ключовий критерій. Це вказує на те, що більшість компаній орієнтується насамперед на загальну ефективність та стабільність рішення, а не лише на набір функціональних можливостей. Проте цей показник також підкреслює важливість гнучкості платформи, здатної адаптуватися до специфіки корпоративного середовища.

У межах того ж дослідження IT-фахівцям було поставлено запитання: «Який тип мережевих атак найбільше впливає вашу IT-організацію?»

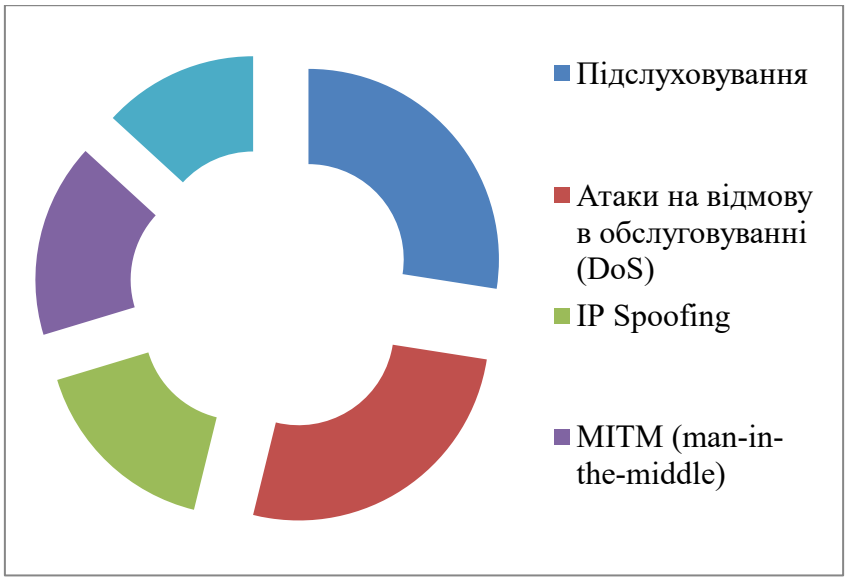


Рисунок 1.2 – Діаграма відповідей на поставлене запитання: Який тип мережевих атак найбільше впливає вашу IT організацію?

Сьогодні хакери використовують різноманітні методи атаки на мережі компаній. Дослідження показало, що IT-фахівці найбільш стурбовані двома конкретними типами атак: атаки на відмову в обслуговуванні (DoS) і підслуховування (Eavesdropping) - ці атаки вказані як найбільш небезпечні і пріоритетні приблизно у 25% респондентів. І по 15% респондентів вибрали в якості ключових загроз атаки типу IP Spoofing і MITM (man-in-the-middle). Решта типів загроз виявилися пріоритетні менш ніж для 12% респондентів.

Сучасні кіберзлочинці застосовують широкий арсенал методів для атак на корпоративні мережі, постійно вдосконалюючи як технічні, так і соціотехнічні засоби впливу. Результати опитування IT-фахівців засвідчили, що найбільше занепокоєння викликають два конкретні типи атак: атаки на відмову в обслуговуванні (DoS) та підслуховування трафіку (Eavesdropping). Ці загрози були названі найнебезпечнішими і найпріоритетнішими приблизно для 25% респондентів, що свідчить про високу обізнаність щодо ризиків порушення доступності сервісів та витоку конфіденційної інформації.

Крім того, по 15% опитаних вказали серед головних загроз IP Spoofing (підробка IP-адреси для несанкціонованого доступу) та атаки типу "людина

посередині" (MITM), які дозволяють перехоплювати або змінювати трафік між учасниками комунікації.

Варто зазначити, що решта типів атак – включаючи фішинг, DNS-спуфінг, атак на внутрішні протоколи тощо – були відзначені як критичні менш ніж для 12% респондентів, що не применшує їхньої небезпеки, але вказує на відносно нижчу частоту чи ймовірність таких інцидентів у порівнянні з основними загрозами.

Наступне запитання, яке було поставлено під час опитування, звучало так:

«У контексті мобільних вразливостей, що є найбільшим предметом занепокоєння для вашої IT-команди?»

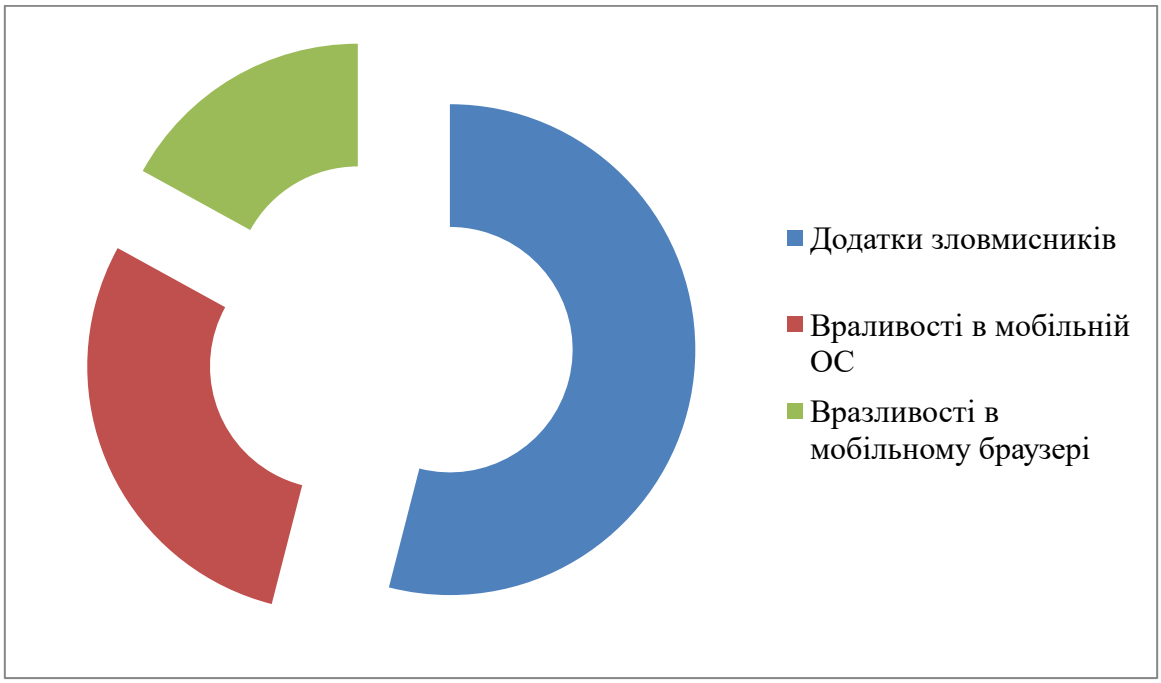


Рисунок 1.3 – Діаграма відповідей на поставлене запитання: У контексті мобільних вразливостей, що є найбільшим предметом занепокоєння для вашої IT-команди?

Сьогодні все більше компаній впроваджують політику використання персональних пристроїв для службових цілей (BYOD). Така трансформація суттєво ускладнює завдання захисту мережевої інфраструктури, оскільки створює додаткові точки входу для потенційних загроз. У цьому контексті особливо

небезпечним є стрімке зростання кількості уразливих мобільних додатків, що активно використовуються в корпоративному середовищі.

Серед найважливіших вимог до сучасних систем забезпечення мережевої безпеки можна виділити такі ключові характеристики:

– підтримка сьомого рівня OSI-моделі, що дозволяє аналізувати трафік на рівні додатків;

– можливість ідентифікації конкретного користувача у зв’язку зі змістом його мережевої активності;

– інтеграція системи виявлення і запобігання вторгненням (IPS) безпосередньо в архітектуру рішення;

– наявність вбудованого захисту від DoS-атак і атак типу прослуховування;

– загальна висока надійність системи.

Окрему увагу слід приділити специфіці національного контексту. Більшість українських компаній, незалежно від галузі, мають справу з обробкою персональних даних фізичних осіб (як мінімум, своїх співробітників), що автоматично накладає на них юридичні зобов’язання відповідно до чинного законодавства України в сфері інформаційної безпеки. Використання організаційно-технічних засобів захисту інформації регламентується національними стандартами ІБ та керівними документами.

Дотримання вимог перевіряється державними органами, які проводять як планові, так і раптові інспекції. Порушення норм може призвести не лише до серйозних фінансових збитків і репутаційних втрат, а й до притягнення керівників компаній до кримінальної відповідальності.

На тлі ускладнення кіберзагроз, зростання рівня технічної витонченості атак та використання хакерами нових схем зламу, компанії змушені переглядати свої стратегії безпеки. Актуальними стають рішення, які поєднують високу надійність, оптимальну вартість володіння, а також здатність до інтеграції з іншими IT-системами підприємства.

Таким чином, боротьба з сучасними кіберзагрозами вимагає комплексного підходу до побудови мережевої безпеки. Йдеться не лише про впровадження технічних інструментів, а й про переосмислення самої стратегії захисту – з урахуванням змін у поведінці користувачів, нових технологій, законодавчого поля та динаміки атак. В сучасних умовах ігнорування питань інформаційної безпеки є не просто помилкою – це пряма загроза стабільності, легальності та життєздатності бізнесу. Тому відповідь на нові виклики має полягати у впровадженні інноваційних підходів, нових засобів захисту та гнучких політик реагування на інциденти.

1.2 Способи реалізації безпеки підприємств

Конфіденційна інформація, що має критичне значення для бізнесу, традиційно перебуває у фокусі підвищеної зацікавленості з боку конкурентів. Особливий інтерес до неї виявляють недобросовісні учасники ринку, корупційні структури та інші зловмисні суб’єкти, які прагнуть отримати несанкціонований доступ до корпоративних даних з метою отримання переваги або нанесення шкоди. У цьому контексті найбільш вразливими є відомості щодо структури управління підприємства, його внутрішніх процесів, стратегічних цілей та поточного фінансового стану. Наявність доступу до такої інформації, а тим паче можливість її змінити або викрасти, створює потенційно руйнівні ризики для економічної безпеки компанії. У практиці корпоративного шпигунства достатньо навіть часткового витоку даних, аби завдати серйозної шкоди. У деяких випадках компрометація навіть однієї п’ятої (20%) обсягу конфіденційної інформації може стати тригером фінансової нестабільності, втрати активів або ринкових позицій. Причини таких витоків можуть мати як технічний, так і людський характер. Особливої уваги заслуговують випадки, коли відсутність належної системи

інформаційної безпеки унеможливлює вчасне виявлення порушень або дійсно дозволяє виникнення інцидентів через необізнаність чи неуважність персоналу. Недостатня кваліфікація, недотримання процедур захисту, відсутність навчання – усе це створює сприятливий ґрунт для випадкових, але не менш небезпечних, витоків.

Інформаційна безпека – це комплексний підхід до захисту даних, що забезпечує їхню цілісність, конфіденційність та доступність виключно для уповноважених користувачів. Ефективна система захисту інформації розглядається не лише як сукупність технічних рішень, а як результат зваженої управлінської політики, спрямованої на виявлення та нейтралізацію зовнішніх і внутрішніх загроз для стабільної роботи організації.

Надійна система інформаційної безпеки повинна створювати сприятливі умови для функціонування бізнесу в умовах нестабільності, передбачати захист комерційних інтересів від протиправних дій з боку конкурентів, а також гарантувати юридичну можливість захисту прав підприємства в разі спроб інформаційного втручання. Окрім того, сучасна парадигма безпеки зосереджується також на фізичному захисті персоналу та охороні майнових активів. Пріоритетними завданнями системи стає не лише запобігання розкраданню інформації або матеріальних ресурсів, а й боротьба зі спробами спотворення даних, несанкціонованого розголошення комерційно чутливої інформації, порушення виробничого процесу або цілеспрямованого знищення майна підприємства.

Забезпечення інформаційної безпеки повинно реалізовуватись одночасно в кількох вимірах – виробничому, комерційному, інформаційному та кадровому. У виробничому контексті це означає запобігання втратам матеріальних ресурсів; у комерційній площині – належне юридичне супроводження договірних відносин і забезпечення економічної доцільності співпраці з партнерами; в інформаційній сфері – встановлення контролю над обігом і збереженням цінної інформації, яка становить об’єкт інтересу з боку конкурентів. Водночас, у кадровому аспекті йдеться про належну перевірку співробітників та формування надійного

персонального складу, який буде дотримуватись норм інформаційної гігієни й політики безпеки компанії.

Не менш важливим є дотримання чинного законодавства у сфері захисту персональних даних та інтелектуальної власності. Для українських підприємств це має особливе значення, оскільки більшість з них так чи інакше обробляють інформацію про фізичних осіб. Закон зобов'язує впроваджувати відповідні організаційно-технічні заходи, регламентовані як національними стандартами, так і спеціальними керівними документами з інформаційної безпеки. Виконання вимог контролюється державними органами шляхом проведення планових і позапланових перевірок, результати яких можуть мати юридичні наслідки для посадових осіб, включно з притягненням до кримінальної відповідальності в разі грубих порушень.

Система забезпечення інформаційної безпеки організації повинна ґрунтуватися на низці фундаментальних принципів, які визначають її структурну логіку, функціональну ефективність та адаптивність до потенційних загроз. Одним із ключових є принцип комплексності, який передбачає необхідність врахування повного спектру можливих загроз – як зовнішніх, так і внутрішніх – із допущенням їх потенційної реалізації в будь-який момент. При цьому кожен можливий канал доступу до інформації, зокрема й закритий, має бути захищений відповідними технічними та організаційними засобами. Захист не може бути фрагментарним: застосовані заходи мають утворювати взаємопов'язану багаторівневу систему, у якій усі компоненти функціонують синхронно, доповнюючи одне одного в межах цілісної архітектури інформаційної безпеки.

Наступним концептуальним підґрунтям є принцип ешелонування, що передбачає побудову захисної системи за зональною логікою. Згідно з цим принципом, інформаційна безпека реалізується через послідовне розташування кількох рівнів захисту, кожен з яких утворює власну зону безпеки. Найвища концентрація захисних механізмів при цьому формується у внутрішньому периметрі системи, де зберігається критично важлива інформація, доступ до якої суворо обмежено. Таким чином, створюється багатошарова структура оборони,

що ускладнює шлях потенційного порушника і значно підвищує рівень стійкості системи в умовах реальних загроз.

Важливою умовою є також дотримання принципу надійності, що вимагає забезпечення однакового рівня захищеності для всіх сегментів системи безпеки. Незалежно від їхньої ієрархічної значущості, усі зони повинні відповідати єдиному стандарту захисту, з урахуванням імовірності реалізації конкретних загроз. Відсутність слабких ланок, навіть у другорядних ділянках інформаційної системи, дозволяє гарантувати збалансовану безпеку, де компрометація однієї частини не призводить до обвалу всієї системи.

З огляду на ресурсні обмеження, реалізація вказаних підходів повинна ґрунтуватися на принципі розумної достатності, який передбачає раціональне співвідношення між рівнем безпеки, витратами на її забезпечення та потенційними наслідками можливого інциденту. Створення абсолютно захищеної системи в умовах практики є економічно недоцільним і технологічно надлишковим. Тому, проєктуючи систему захисту, необхідно орієнтуватися на досягнення оптимального рівня безпеки, достатнього для стримування реальних загроз, при якому вартість захисних заходів не перевищує обґрунтовану межу очікуваних втрат.

Завершальним і не менш важливим є принцип безперервності, відповідно до якого всі елементи системи інформаційної безпеки повинні функціонувати постійно, без тимчасових відключень або пауз. Безперервна робота систем спостереження, контролю та реагування є критичною умовою своєчасного виявлення і нейтралізації загроз у режимі реального часу. Перерви у роботі захисних механізмів створюють «вікна вразливості», якими можуть скористатися зловмисники, тому концепція безпеки повинна включати підтримку цілодобового моніторингу, резервування каналів та відмовостійкість системних компонентів.

Служба безпеки в межах сучасного підприємства виконує широкий спектр завдань, пов’язаних із захистом майна, персоналу, інформації та фінансових інтересів організації. Її функціонування може бути організоване за різними структурними моделями залежно від масштабу підприємства, його фінансових

можливостей та специфіки діяльності. У найпоширенішому варіанті служба безпеки входить безпосередньо до внутрішньої структури підприємства, фінансується з його бюджету та підпорядковується керівництву. Така модель найчастіше зустрічається у компаніях, які прагнуть інтегрувати функції безпеки в загальну систему управління, маючи стабільне фінансове становище й достатній кадровий ресурс.

Забезпечення інформаційної безпеки в організації базується на комплексному підході, що охоплює низку функціональних напрямків, кожен із яких спрямований на мінімізацію ризиків для критично важливих інтересів підприємства. Однією з основних передумов є своєчасне формування захисної інфраструктури, здатної протидіяти загрозам, які можуть виникати як із боку кримінальних структур, так і з боку конкурентних організацій. У таких випадках особливу роль відіграють методи превентивного аналізу, зокрема ділова розвідка та аналітичне прогнозування розвитку ситуацій, що дозволяє підприємству не лише реагувати на загрози, а й передбачати їх на етапі формування.

Інформаційно-комерційна безпека, як третій ключовий вектор, включає в себе захист інформаційних ресурсів, технічних каналів передачі даних і прав на інтелектуальну власність. У свою чергу, охорона персоналу, умов праці, екологічної й санітарної безпеки, а також дотримання стандартів внутрішніх комунікацій, формують ще один важливий рівень захисної стратегії підприємства. Незважаючи на всю багатогранність цих заходів, слід визнати, що універсального й водночас абсолютно ефективного методу інформаційного захисту на сьогоднішній день не існує, проте потреба в комплексному, якісному захисті залишається беззаперечною, а в умовах підвищеного ризику – критично необхідною.

У рамках загальної архітектури інформаційного захисту застосовуються кілька методологічних підходів. Метод перешкоди передбачає фізичне унеможливлення доступу до конфіденційної інформації шляхом ізоляції інформаційних носіїв та апаратного обладнання. Управління доступом реалізується через автоматизовані системи з функціями ідентифікації,

аутентифікації, перевірки повноважень, фіксації звернень та реагування на несанкціоновані спроби. Маскування забезпечується криптографічними засобами, які унеможливлюють прочитання даних без відповідного ключа. Регламентація полягає в точному визначенні прав доступу до інформації та суворому дотриманні процедур її зберігання й обміну.

Окрім технічних і нормативних засобів, використовуються також поведінкові методи, зокрема примус, що передбачає впровадження санкцій у разі порушення політики безпеки, та спонукання, що базується на етичних і моральних принципах, які мотивують персонал дотримуватися встановлених правил без потреби зовнішнього тиску. Всі ці елементи, об’єднані в єдину систему, створюють багаторівневу платформу захисту, яка дозволяє організації функціонувати впевнено, зберігаючи стратегічну стійкість у середовищі постійно зростаючих інформаційних загроз.

Фізичні засоби забезпечення інформаційної безпеки традиційно асоціюються із зовнішнім рівнем захисту, що охоплює територіальний контроль, пропускний режим, пожежну безпеку, відеоспостереження, сигналізацію, охорону приміщень і блокування несанкціонованого фізичного доступу до обладнання. Сучасні системи фізичної безпеки включають не лише механічні рішення, які потребують участі людини, але й автоматизовані електронні системи, що функціонують на основі мережі датчиків, мікропроцесорів, біометричних сканерів та електронних ключів.

Окрему категорію становить захист від витоків через електромагнітні канали, який реалізується завдяки впровадженню екранувальних матеріалів у структуру приміщень, використанню поглинаючих елементів, магнітних пасток у вентиляційних системах, діелектричних розділювачів на трубопроводах і установці пристроїв контролю змінної напруги з функцією тривожного сповіщення та автоматичного запису інциденту за допомогою відеофіксації.

Поряд із фізичними, в структурі безпеки важливу роль відіграють апаратні засоби, які функціонують як вбудовані електронні чи електромеханічні компоненти в межах інформаційно-обчислювальних систем. Їхнє основне

завдання полягає у запобіганні несанкціонованому доступу до терміналів, процесорів, ліній зв’язку, периферійних пристроїв та внутрішніх каналів передачі даних. Апаратні рішення відповідають за надійний захист файлових систем, цілісність баз даних, безпечне функціонування програмних продуктів під час збоїв або аварійних вимкнень, а також забезпечують реалізацію процедур автентифікації, ідентифікації, визначення повноважень та реєстрації дій користувача. У разі необхідності, для зберігання конфіденційної інформації можуть використовуватись спеціалізовані фізичні носії з обмеженим доступом і властивостями, що унеможливлюють її зчитування без авторизації.

Третім компонентом системи виступають програмні засоби, які або інтегруються у програмне забезпечення автоматизованої системи, або функціонують у взаємодії з апаратною інфраструктурою. Їх застосування охоплює широкий діапазон функцій – від забезпечення контролю доступу до конфіденційних даних за допомогою ідентифікаторів, паролів і кодів до обмеження доступу до окремих компонентів системи, захисту користувацьких процесів, виявлення і нейтралізації вірусного ПЗ, а також автоматичного очищення оперативної пам’яті від залишкових слідів роботи з чутливими файлами.

Таким чином, система забезпечення інформаційної безпеки сучасної організації є багаторівневою й гетерогенною за своєю структурою, поєднуючи фізичні, апаратні та програмні рішення у єдину захисну екосистему. Вона не лише технічно блокує доступ до критичної інформації, а й забезпечує правове, адміністративне й економічне підґрунтя для її стійкого функціонування, зокрема в умовах глобалізації, цифровізації й загострення проблеми інтелектуального піратства.

2 АНАЛІТИЧНО-ДОСЛІДНИЦЬКЕ РІШЕННЯ

2.1 Провідні фактори впливу на безпеку підприємства

Одним із найбільш вагомих зовнішніх чинників, що загрожують стабільності інформаційної безпеки підприємства, виступає економічна політика держави, яка, за умови нестабільності або надмірного втручання в ринкові процеси, може створювати серйозні системні ризики. Маніпулятивне використання таких інструментів, як валютний курс, облікова ставка, податкове навантаження чи митне регулювання, нерідко породжує протиріччя в управлінні фінансами, виробничими та комерційними процесами підприємств. Особливу небезпеку становлять ситуації, коли адміністративні бар'єри для виходу на ринок чи участі в зовнішньоекономічній діяльності супроводжуються обмеженням прав власності, доступу до інформаційних ресурсів або втручанням державних органів у внутрішній інформаційний простір компаній. Така практика веде не лише до порушення ринкових механізмів, а й до зниження довіри суб’єктів господарювання до інститутів державного управління. У ще більш загрозливому вигляді проявляється державна політика, що має форму запровадження санкцій чи обмежень економічної взаємодії, яка створює атмосферу недовіри, дестабілізує ділове середовище та підриває фундаментальні принципи захисту інформації.

Особливу загрозу для інформаційної безпеки становить той факт, що пропозиції за доступ до конфіденційних даних у деяких випадках у багато разів перевищують заробітну плату працівника, що підвищує спокусу імовірної зради корпоративним інтересам, а отже – знижує ефективність превентивних заходів, таких як підписка про нерозголошення. Іще більш небезпечною стає ситуація, коли недобросовісна конкуренція виходить за межі інформаційного чи економічного поля і трансформується у фізичний тиск.

Таким чином, ефективне забезпечення інформаційної безпеки вимагає від підприємства не лише внутрішньої дисципліни, технічної підготовленості та правового супроводу, а й постійного моніторингу державної політики, економічної ситуації, конкурентного середовища та глобальних фінансових процесів. Лише у випадку багаторівневої інтеграції захисних механізмів на тлі усвідомлення системних зовнішніх загроз можна забезпечити стабільність, стійкість і довготривалу безпеку інформаційного простору організації.

2.2 Проблематика та постановка завдання

Стрімкий розвиток інформаційних технологій та їх проникнення у всі сфери господарської діяльності створили умови, за яких комп'ютерна інформація набуває не лише функціонального значення, але й значної економічної цінності. У нових умовах цифрової трансформації підприємств захист інформаційних ресурсів стає не просто технологічним викликом, а ключовою умовою забезпечення стабільності, конкурентоспроможності та репутаційної цілісності організації. Відтак, однією з пріоритетних проблем у межах впровадження інформаційних технологій у корпоративне середовище є формування ефективної системи інформаційної безпеки, здатної протидіяти широкому спектру загроз.

Реалізація цієї мети вимагає глибокого опрацювання теоретичних засад та практичних механізмів виявлення, аналізу та запобігання небезпекам у сфері обігу інформації, що передбачає не лише визначення форм та каналів витоку даних, але й розробку інструментів захисту, а також створення системи управління інформаційною безпекою відповідно до особливостей функціонування конкретного підприємства. Зокрема, ключовим напрямком є вивчення й адаптація способів і засобів протидії загрозам, які безпосередньо пов'язані з інфраструктурою підприємства, а також організацією доступу до інформаційних ресурсів.

Основною загрозою, на яку спрямовані заходи захисту, є витік конфіденційної інформації, що трактується як будь-які відомості, доступ до яких обмежений їхнім володарем і які підлягають правовому захисту відповідно до чинного законодавства. У сучасній практиці розрізняють кілька категорій конфіденційної інформації, серед яких можна виділити службову таємницю, персональні дані, адвокатську, нотаріальну, комерційну, банківську, лікарську, податкову, професійну таємницю, таємницю зв'язку, відомості, що становлять сутність винаходу до моменту його опублікування, а також інформацію слідчого або судового характеру. Втрата або несанкціоноване розголошення таких даних може мати як правові, так і фінансові наслідки для підприємства, аж до повної дестабілізації його діяльності.

У межах даного дослідження об'єктом аналізу виступає корпоративна мережа з високим рівнем інформаційної взаємозалежності між підрозділами та складною структурою інформаційних потоків. Для таких суб'єктів господарювання збереження цілісності та конфіденційності інформації.

З огляду на вищезазначене, у межах цієї роботи поставлено завдання розробити комплексну та дієву систему забезпечення мережевої безпеки для корпоративної інформаційної інфраструктури, яка дозволить не лише локалізувати існуючі загрози, але й сформувати механізми превентивного реагування, управління доступом і протидії несанкціонованим впливам у цифровому середовищі. Особливу увагу буде приділено аспектам функціонування мережевих архітектур, а також специфіці зберігання, обробки й передачі інформації у багаторівневій системі.

У підсумку проведеного дослідження було окреслено фундаментальні аспекти мережевої безпеки, здійснено уточнення понятєво-категоріального апарату, розкрито зміст та типологію інформаційних загроз, характерних для функціонування сучасного підприємства в умовах цифрової трансформації. Особливу увагу приділено виокремленню актуальних загроз витоку конфіденційної інформації в межах корпоративної мережі, а також узагальненню

сучасних підходів до запобігання таким загрозам у контексті внутрішньої інфраструктури підприємства.

У подальшому планується провести методологічне обґрунтування дослідження, в межах якого планується детально розробити структурні й функціональні компоненти системи мережевої безпеки, з урахуванням специфіки корпоративної інфраструктури. Основний акцент буде зроблено на формуванні моделі інформаційного захисту, що охоплює технічні, організаційні та програмні механізми протидії витокам даних, а також принципи їх взаємодії в умовах розгалуженої цифрової екосистеми підприємства.

2.3 SWOT-аналіз безпеки до модернізації

У рамках аналізу вихідного стану корпоративної мережевої інфраструктури було проведено SWOT-аналіз, який дозволив виявити сильні та слабкі сторони, можливості для вдосконалення, а також зовнішні загрози, що впливають на безпеку системи:

Таблиця 2.1 – Аналіз абревіатури SWOT

Категорія	Приклад
S (Strengths)	Наявність власної мережевої інфраструктури, централізоване управління, стандартизоване обладнання
W (Weaknesses)	Відсутність резервування, спільний VLAN, ручне перемикання між каналами, відсутність моніторингу
O (Opportunities)	Впровадження багаторівневої маршрутизації, автоматизація, інтеграція VPN, використання Zabbix
T (Threats)	Збої з боку провайдерів, кібератаки, витік даних, людський фактор, порушення законодавства

Детальніше аналізуючи категорії загроз (T), варто звернути увагу на посилення інтенсивності та складності сучасних кіберзагроз, які значно збільшили ймовірність несанкціонованого доступу до конфіденційної інформації. В умовах відсутності сегментації мережі та недостатнього контролю за міжфілійним трафіком це створює серйозні вектори атаки, особливо за використання фішингових схем, шкідливого ПЗ або атак типу «людина посередині» (MITM).

У категорії слабких сторін (W) важливим аспектом є також технічна залежність від одного провайдера, що унеможливлює гнучке перемикання каналів у разі збоїв. Це суттєво знижує відмовостійкість мережі та створює ризики повного припинення зв’язку між філіями й головним офісом.

Щодо можливостей (O), компанія має усі передумови для впровадження сучасної моделі інформаційної безпеки, оскільки вже володіє певною мережею філій, уніфікованим обладнанням та централізованою IT-службою. Це дозволяє реалізувати масштабовані рішення з єдиним адмініструванням та моніторингом, а також створити резервні канали та VPN-зв’язки між об’єктами інфраструктури.

Загалом, результати SWOT-аналізу підтвердили необхідність комплексної модернізації з фокусом на підвищення стабільності мережі, створення систем резервування, впровадження засобів автоматизації та забезпечення інформаційної безпеки згідно з сучасними стандартами. Цей аналіз став основою для обґрунтування вибору напрямів модернізації корпоративної мережі.

2.4 Варіанти вирішення та їх порівняння

У ході дослідження були розглянуті альтернативні підходи до модернізації корпоративної мережі. Їх порівняльна характеристика представлена в таблиці нижче.

Таблиця 2.2 – Порівняльний аналіз варіантів вирішення проблеми

Підхід	Вартість	Надійність	Гнучкість	Складність впровадження
VPN на MikroTik	$	Висока	Висока	Низька
MPLS через провайдера	$$$$	Дуже висока	Низька	Висока
SD-WAN рішення	$$$	Висока	Висока	Середня

Перевагою VPN-рішення на базі MikroTik є відносна дешевизна, можливість повного контролю з боку IT-відділу, а також легка масштабованість. Такий підхід забезпечує створення логічно ізольованих тунелів зв’язку між філіями та центральним офісом з використанням шифрування, автентифікації та резервування каналів. Крім того, пристрої MikroTik підтримують розширені можливості маршрутизації, скриптування та централізованого моніторингу, що дозволяє оперативно реагувати на інциденти та збої.

MPLS-технологія (Multiprotocol Label Switching), хоча і пропонує високий рівень надійності та якості обслуговування (QoS), є значно дорожчою, потребує залучення зовнішнього провайдера та не завжди доступна для середніх за розміром компаній. Вона краще підходить для великих корпоративних середовищ із жорсткими вимогами до SLA.

SD-WAN (Software-Defined Wide Area Network) — це сучасний підхід, який забезпечує високий рівень керованості та автоматизації з’єднань між офісами, однак вимагає спеціального програмного забезпечення та складнішого налаштування. Попри це, він дозволяє ефективно поєднувати декілька каналів зв’язку, забезпечуючи балансування навантаження та адаптивну маршрутизацію залежно від якості лінії.

Таким чином, з урахуванням технічних та фінансових можливостей туристичної фірми, VPN-рішення на базі MikroTik було визнано оптимальним як за ефективністю, так і за економічною доцільністю.

2.5 Методика оцінки ефективності після модернізації

Для об’єктивної оцінки ефективності модернізованої інфраструктури було визначено такі ключові індикатори ефективності (KPI):

- *MTTR (Mean Time to Recovery)***.** Середній час відновлення з’єднання після збою;
- *Uptime*. Рівень доступності сервісів, вимірюваний у відсотках до загального часу;
- *Кількість аварійних інцидентів на місяць*. Порівняння до та після впровадження;
- *Затримка передачі даних*. Середній ping між філіями та головним офісом;
- *Швидкість перемикання каналів зв’язку*. Час, необхідний для переходу на резервний маршрут;
- *Кількість спрацювань автоматичного резервування.* Частота використання систем резервного доступу;
- *Інтенсивність broadcast-трафіку*. Рівень широкомовного навантаження після сегментації;
- *Навантаження на мережеві інтерфейси*. Середнє і пікове використання пропускної здатності;
- *Час реагування на інцидент*. Середній інтервал між виявленням і усуненням проблеми.

Збирання даних для вищезазначених показників здійснюється за допомогою системи моніторингу Zabbix, NetWatch, логів маршрутизаторів MikroTik та email-сповіщень, що надсилаються при зміні стану з’єднання або переході на резервний маршрут. Для аналізу використовується візуалізація графіків з розбивкою по філіях і часових відрізках.

Крім кількісних показників, у якості якісного індикатора використовується рівень задоволеності персоналу філій, який оцінюється шляхом опитування IT-користувачів щодо зниження кількості збоїв і швидкості відновлення доступу.

На основі аналізу цих показників буде надано висновок про досягнутий рівень підвищення безпеки, стабільності та відмовостійкості корпоративної мережі, що дозволяє оцінити рентабельність інвестицій у модернізацію інфраструктури та спрогнозувати ефективність її масштабування в майбутньому.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ЗАХИЩЕНОЇ ТА ВІДМОВОСТІЙКОЇ КОРПОРАТИВНОЇ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

3.1 Об'єкт дослідження

Об’єктом дослідження у межах даної кваліфікаційної роботи виступає локальна корпоративна система, що об’єднує мережеву інфраструктуру дванадцяти філій туристичної фірми та центрального офісу в єдину інформаційно-комунікаційну структуру. З технічної точки зору, топологія системи реалізована провайдером інтернет-послуг (ISP) шляхом виділення окремого VLAN у межах магістральної мережі оператора. Це дозволяє забезпечити логічну ізоляцію трафіку мережі філій туристичної фірми від інших абонентів та надати їй окремий рівень обслуговування.

На момент дослідження, підключення філій туристичної фірми до інтернету реалізовано за допомогою волоконно-оптичних каналів зв’язку, із використанням двох технологій доступу – FTTH (Fiber to the Home) та PON (Passive Optical Network). Згідно з поточною мережею, у двох філіях та центральному офісі впроваджено підключення на основі FTTH, що дозволяє отримувати високошвидкісний Ethernet-зв’язок безпосередньо через оптичну лінію. У решті дев’яти філій туристичної фірми використовується архітектура PON, з розгортанням терміналів Huawei моделі HG810, які функціонують як ONU (Optical Network Unit) на стороні абонента.

Особливістю застосовуваного обладнання є наявність вбудованих функцій, які, хоча і є корисними для архітектури провайдера у частині масштабованості та безпеки доступу, можуть створювати небажані обмеження для корпоративних клієнтів. Зокрема, в мережах, побудованих на базі Huawei PON, за замовчуванням реалізується політика ізоляції трафіку між усіма ONU, які підключені до одного OLT (Optical Line Terminal). Така політика, орієнтована на типові сценарії

масового доступу, блокує горизонтальний обмін даними між підрозділами одного підприємства, що унеможливлює повноцінне функціонування корпоративної мережі філій туристичної фірми.

З метою вирішення цієї проблеми було впроваджено спеціалізовані профілі VLAN, що дозволяють налаштувати обхід обмеження через механізми службової конфігурації ONU. Це рішення дозволило відновити комунікацію між всіма вузлами корпоративної мережі філій туристичної фірми у рамках одного логічного VLAN, не порушуючи загальної політики безпеки провайдера.

Схематичне відображення поточної конфігурації мережевої інфраструктури філій туристичної фірми до моменту модернізації подано на рисунку 3.1. У подальших етапах роботи буде проведено аналіз функціональних обмежень існуючої архітектури, а також запропоновано структурні зміни, спрямовані на підвищення рівня мережевої безпеки та ефективності системи обміну даними в корпоративному середовищі філій туристичної фірми.

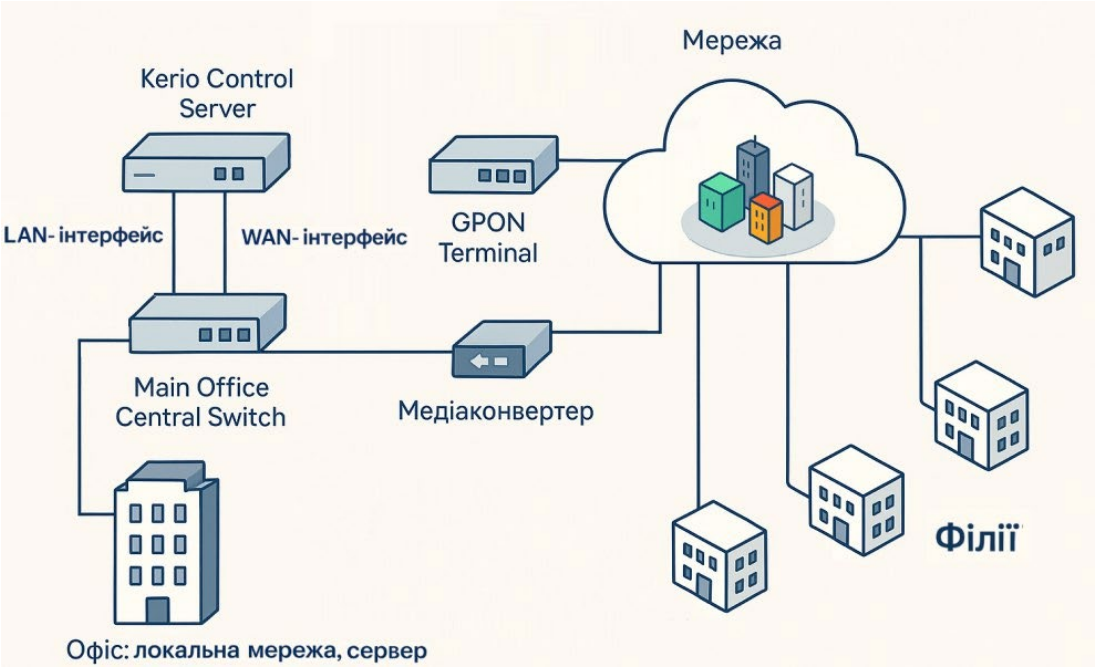


Рисунок 3.1 – Схема мережі філій туристичної фірми до модернізації

До моменту проведення модернізації корпоративна мережа філій туристичної фірми являла собою плоску, некеровану інфраструктуру, об’єднану в межах одного великого VLAN, виділеного інтернет-провайдером. Усі філії – всього 12 об’єктів, - були підключені до мережі провайдера за допомогою оптичних каналів зв’язку з використанням технологій FTTH (Ethernet) у центральному офісі та двох філіях, а також PON (Passive Optical Network) у решті дев’яти точках. У випадку PON використовувалося обладнання Huawei HG810, що виконує функції ONU (Optical Network Unit) у топології доступу.

Ця конфігурація мала низку критичних обмежень, обумовлених особливостями архітектури PON. Зокрема, за замовчуванням ONU блокує передавання DHCP-пакетів від абонента до мережі провайдера, що унеможливлює роботу DHCP-сервера, розташованого у центральному офісі, з вузлами в інших філіях. Навіть за наявності фізичного з’єднання, механізм автоматичної адресації не функціонує, що критично для роботи пристроїв у віддалених точках.

Аналогічні обмеження стосуються і Multicast-трафіку – пакети такого типу не проходять через ONU, що унеможливлює реалізацію протоколів широкомовної доставки, зокрема для синхронізації даних чи відеоспостереження. Водночас інші типи трафіку проходили без затримок чи фільтрації, що свідчить про наявність вбудованих обмежувальних політик на рівні ONU, спрямованих на типовий сценарій масового доступу, але не придатних для корпоративного середовища.

Загальна архітектура мережі функціонувала під керуванням єдиного шлюзу – Kerio Control Server, через який маршрутизувався весь трафік. Внаслідок такої централізації, всі IP-пристрої в усіх філіях туристичної фірми перебували в одному широкомовному домені. Таблиці FDB на комутаторах провайдера містили понад 350 активних записів MAC-адрес, що суттєво перевищує оптимальний рівень навантаження й ускладнює процеси комутації. Наявність надмірного broadcast-трафіку, а також відсутність логічної сегментації спричиняли збої, що негативно впливали на стабільність роботи мережі та функціонування ключових процесів.

Особливу загрозу становили аварійні ситуації на стороні провайдера, зокрема – у вузлах електроживлення, які обслуговують головний офіс. У разі знеструмлення будівель, де розміщувався вузол доступу провайдера, центральний офіс втрачав зв’язок з усією мережею, що призводило до повної дестабілізації бізнес-процесів. У такі періоди філії туристичної фірми залишалися без можливості проводити синхронізацію цін та пропозицій турів та готелів, виконувати ревізії турів, а головне – приймати безготівкові платежі, що паралізує роботу касових вузлів і викликає прямі фінансові втрати.

Для часткового вирішення проблеми було запроваджено резервний канал зв’язку через лінію PON, заведений у головний офіс туристичної фірми як альтернативний до Ethernet-лінії. Однак через блокування DHCP-пакетів з боку ONU цей канал міг використовуватись лише для обмежених завдань, і перемикання між каналами здійснювалося вручну, що не відповідало вимогам до високодоступної інфраструктури.

Таким чином, наявна мережева архітектура філій туристичної фірми, хоча і забезпечувала фізичний зв’язок між усіма об’єктами, не відповідала базовим вимогам до корпоративної надійності, масштабованості та інформаційної безпеки, і потребувала негайної модернізації з урахуванням сегментації, резервування, автоматизації перемикань та оновлення політик обробки трафіку в інфраструктурі доступу.

3.2 Механізми модернізації корпоративної мережевої інфраструктури туристичної фірми

Механізми модернізації локальної корпоративної мережі туристичної фірми, що об’єднує центральний офіс та дванадцять філій, спрямовані на підвищення її надійності, керованості та стійкості до відмов. Запропоновані зміни реалізуються шляхом комплексного оновлення архітектури із впровадженням

багаторівневої маршрутизації, резервування каналів зв’язку, а також централізованого моніторингу.

Передусім, виконано сегментацію єдиної широкомовної інфраструктури з розділенням її на окремі ізольовані broadcast-домени для кожної філії та центрального офісу туристичної фірми. Такий підхід дозволив локалізувати вплив помилок або перевантаження у будь-якому з сегментів і запобігти їхньому поширенню мережею.

З метою підвищення доступності міжфіліального зв’язку, впроваджено механізм автоматичного перемикання між основним і резервним каналами зв’язку в центральному офісі. У разі втрати доступу до магістралі Ethernet або відмови PON-лінії, маршрутизатор здійснює миттєве перемикання маршруту без втрати сесії. Аналогічний підхід застосовано на рівні кожної філії: якщо основне з’єднання з ISP (через FTTH або PON) недоступне, активується резервний канал через другого провайдера.

Окрім того, реалізовано механізм моніторингу стану каналів зв’язку, що дозволяє системі виявляти втрату доступності офісної мережі або Інтернету в будь-якому з вузлів. У разі виявлення аварії, відповідальний персонал негайно інформується через вбудовану систему оповіщень.

У якості системи моніторингу було обрано Zabbix, яка дозволяє контролювати ключові параметри роботи мережі в режимі реального часу, зокрема: доступність каналів, навантаження на інтерфейси, час відповіді маршрутизаторів, статус VPN-тунелів тощо.

Мережеву інфраструктуру оновлено із використанням обладнання MikroTik. У центральному офісі встановлено модель RB1100AHx2, яка забезпечує достатню обчислювальну потужність для маршрутизації, балансування навантаження та роботи з VPN-з’єднаннями. У кожному з дванадцяти філій туристичної фірми встановлено пристрої MikroTik hEX (RB750Gr3), які підтримують резервування маршрутів, IPSec-тунелі та моніторинг.

Усі об’єкти додатково підключено до другого провайдера – Діанет, що надає доступ до Інтернету. У центральному офісі реалізовано FTTH-з’єднання, у

філіях – ADSL через модеми, які працюють у режимі bridge для передачі PPPoE-сесії безпосередньо на маршрутизатори MikroTik.

Система адресації побудована за принципом розподіленої топології. Для локальних підмереж використовується такий діапазон:

– 192.168.1.0/24 – мережа центрального офісу;

– 192.168.2.0/24 до 192.168.13.0/24 – локальні мережі кожної з дванадцяти філій.

Для організації VPN-зв'язку між маршрутизаторами передбачено використання двох службових підмереж:

– 10.10.10.0/24 – трафік основного каналу (Ethernet до головного офісу);

– 10.10.20.0/24 – трафік резервного каналу (PON-лінія до головного офісу).

Центральний офіс отримує доступ до Інтернету через три незалежні канали, що дозволяє реалізувати повноцінне балансування та відмовостійкість:

– ISP1-A – основний канал через Ethernet, IP-адреса за схемою /30: 100.100.100.2/30;

– ISP1-B – резервний канал через PON, IP-адреса: 101.101.101.2/30;

– ISP2 (Дianет) – канал PPPoE, динамічна IP-адреса, умовно dynamic-IP/PPPoE.

```
[admin@MAIN-BORDER-ROUTER] > ip address export
/ip address
add address=10.10.10.1/24 comment="ISP-LOCAL-ADDRESS" interface=eth-1
network=10.10.10.0
add address=10.10.20.1/24 comment="ISP-RESERVE-LOCAL-ADDRESS" interface=eth-
2 network=10.10.20.0
add address=1.1.1.1/30 comment="ISP1-MAIN-INET-ADDRESS" interface=eth-1
network=1.1.1.0
add address=2.2.2.2/30 comment="ISP1-RESERVE-INET" interface=eth-2
network=2.2.2.0
add address=192.168.1.1/24 comment="OFFICE-LOCAL-ADDRESS" interface=bridge-
MAIN-OFFICE network=192.168.1.0
```

Рисунок 3.2 – Налаштування адресації

У випадку PPPoE, що належить другому провайдеру, проводяться налаштування зображені на рисунку 3.3:

```
interface pppoe-client print
0    R  name="RT-PPPoE"  max-mtu=1480  max-mru=1480  mrru=1600  interface=eth-3
user="U" password="P"
      profile=default keepalive-timeout=30 service-name="" ac-name=""
      add-default-route=no dial-on-demand=no use-peer-dns=no
      allow=pap,chap,mschap1,mschap2
```

Рисунок 3.3 – Налаштування PPPoE підключення другого провайдера

Для забезпечення стабільної роботи віддалених філій у випадках втрати з'єднання з провайдером ISP-1, на головному маршрутизаторі в офісі було налаштовано по два окремих VPN-акаунти для кожної точки. Це дозволяє кожній філії підтримувати одночасно два активних VPN-з'єднання через Інтернет – до двох різних зовнішніх IP-адрес, що належать провайдерам офісної мережі.

З метою розмежування трафіку для обох VPN-напрямках додатково впроваджено дві службові підмережі:

– 10.20.30.0/24 – для тунелів, які встановлюються через IP-адресу ISP-1;

– 10.30.40.0/24 – для тунелів, які проходять через зовнішню ISP-2;

На маршрутизаторі офісу активовано L2TP-сервер, після чого створено користувацькі профілі для кожної філії (по одному для кожного VPN-шляху).

За допомогою команди /interface l2tp-server у розділі PPP реалізується жорстке зіставлення VPN-підключень із конкретними філіями. Такий підхід дозволяє однозначно ідентифікувати кожну філію за її VPN-іменем, а також визначати, через який саме канал зв'язку (основний чи резервний) відбувається передача трафіку. Це спрощує моніторинг, облік і налагодження маршрутизації в корпоративній мережі.

У результаті такої побудови формуються чотири окремі підмережі, які використовуються для обміну трафіком між офісом і філіями:

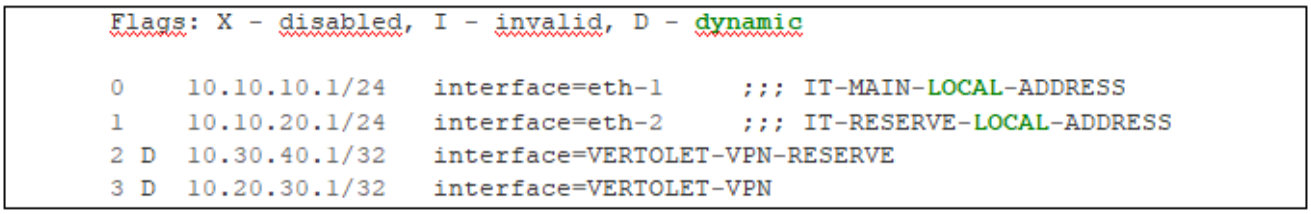


Рисунок 3.4 – Список підмереж, які сформувалися під час налаштування ISP

З метою оптимізації адміністрування та забезпечення прогнозованої логіки маршрутизації, запроваджено схему, в якій усі IP-підмережі віддалених філій отримують фіксовані IP-адреси в різних зонах маршрутизації. Зокрема, мережа філії 192.168.15.0/24 буде доступна з головного офісу через такі адреси залежно від каналу зв’язку:

– 10.10.10.15 – у випадку з'єднання через основний фізичний канал (Ethernet, ISP-1);

– 10.10.20.15 – у разі використання резервного фізичного каналу (PON/ADSL, ISP-2);

– 10.20.30.15 – при з'єднанні через основний VPN-тунель (через зовнішню IP ISP-1);

– 10.30.40.15 – при роботі через резервний VPN-тунель (через зовнішню IP ISP-2).

Для забезпечення автоматичного вибору найоптимальнішого маршруту до філій у різних ситуаціях, у конфігурації маршрутизатора використовуються різні значення адміністративної відстані (AD) для кожного маршруту. Такий підхід дозволяє системі самостійно перемикатись між доступними шляхами залежно від їхньої доступності.

У штатному режимі, коли всі канали працюють коректно, трафік до мережі філії 192.168.15.0/24 прямує через IP-адресу 10.10.10.15, оскільки маршрут через цю адресу має найнижчу адміністративну відстань – 10. Цей маршрут проходить через інтерфейс eth-1, що відповідає основному Ethernet-каналу провайдера ISP-1.

У випадку, якщо зв’язок по eth-1 буде втрачено, маршрутизатор автоматично перемикає трафік на резервний канал через eth-2, тобто через PON-

з’єднання до тієї ж IP-адреси (наприклад, 10.10.20.15) з більш високим значенням адміністративної відстані, наприклад 20.

Якщо ж і цей маршрут стає недоступним, система активує VPN-резервування – через PPPoE-з’єднання провайдера ISP-2. У такому випадку маршрут проходить через IP-адреси 10.20.30.15 або 10.30.40.15 з ще вищими значеннями AD – наприклад, 30 та 40 відповідно.

Таким чином, реалізується багаторівнева відмовостійка маршрутизація, що дозволяє автоматично зберігати зв'язок із філіями туристичної фірми навіть у разі критичних збоїв кількох ліній зв’язку.

Схема підключення офісної мережі з урахуванням усіх маршрутів подана на рисунку 3.5 нижче.

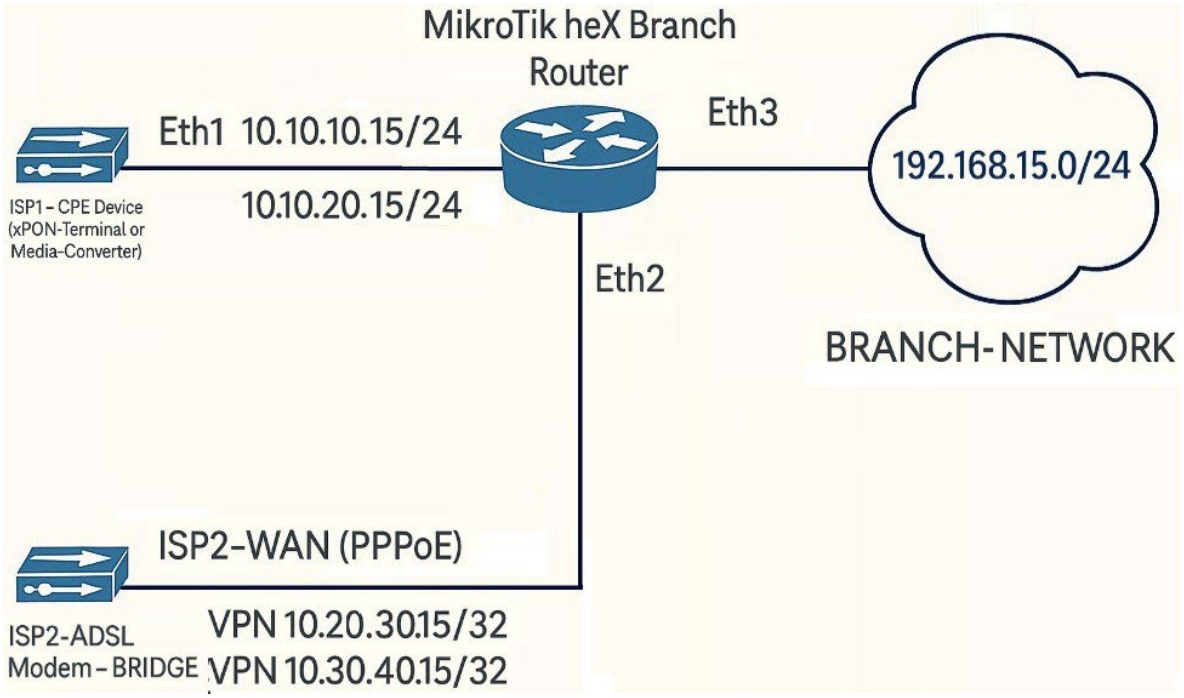


Рисунок 3.5 – Схема підключення мережі в центральному офісі туристичної фірми

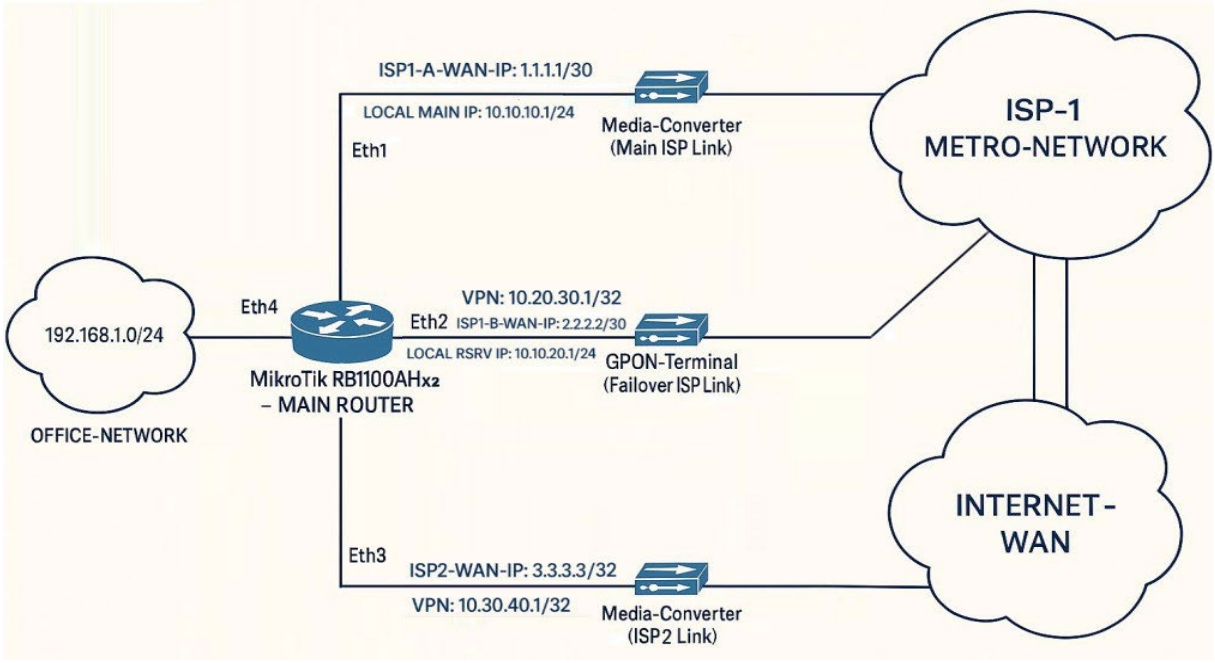


Рисунок 3.6 – Схема підключення філії туристичної фірми

Схематичне підключення філії зображено на рисунку 3.6.

У випадку, якщо інтерфейс ether1 у віддаленій філії втрачає зв’язок (наприклад, через збій з боку ISP-1), звичайні локальні маршрути до офісу, що проходять через IP-адреси 10.10.10.1 та 10.10.20.1, стають недоступними. У такій ситуації автоматично активується обхідний шлях через VPN-з'єднання, які постійно підтримуються активними через резервний інтернет-канал філії (ISP-2).

Зокрема, з’єднання з офісом у такому випадку забезпечується за допомогою VPN-тунелів через IP-адреси:

– 10.20.30.1 – основний VPN-канал до офісу через ISP-2;

– 10.30.40.1 – резервний VPN-канал до офісу через ISP-2.

3.3 Верифікація результатів дослідження

У рамках побудови надійної мережевої інфраструктури для філії туристичної фірми було реалізовано розширену схему маршрутизації, яка

забезпечує відмовостійкий зв’язок з головним офісом через кілька незалежних каналів зв’язку. Основна мета цієї конфігурації – гарантувати постійний доступ до офісних сервісів навіть у разі повного виходу з ладу основного провайдера або маршрутизатора, а також забезпечити стабільну роботу VPN-тунелів.

Для початку створено окрему таблицю маршрутизації, яка відповідає за передавання трафіку через резервний інтернет-канал провайдера ISP-2. У цю таблицю додано маршрут, що використовує інтерфейс RT-INET-Reserve як шлюз. Маршрут має адміністративну відстань 1 та застосовується до трафіку, позначеного міткою ISP2-Reserve. Щоб VPN-трафік був чітко ізольований від загального трафіку і не потрапляв на інші канали, були створені спеціальні правила маршрутизації, які змушують пакети, адресовані на IP VPN-серверів офісу (2.2.2.2 та 3.3.3.3), шукати маршрути виключно в таблиці ISP2-Reserve. Таким чином, VPN-канали залишаються активними та стабільними незалежно від того, через який інтерфейс у поточний момент працює інтернет у філії.

VPN-з'єднання між офісом і філією завжди піднімається саме через резервний інтернет-канал. Це дозволяє тунелю бути постійно готовим до обробки трафіку, навіть коли основне з’єднання неактивне. Такий підхід дозволяє організувати швидке та безперервне перемикання маршрутизації трафіку філії на VPN у разі втрати основного з'єднання без ручного втручання.

Оскільки за замовчуванням загальний інтернет у філії працює через основний канал ISP-1, у конфігурації маршрутизатора створено дві окремі таблиці маршрутизації: одна відповідає за основний доступ через адресу офісного шлюзу 10.10.10.1 (таблиця ISP1-A), інша – за резервний доступ через 10.10.20.1 (таблиця ISP1-B). Для кожної таблиці створено окремий маршрут із пріоритетною відстанню 1 та вказаною вихідною адресою (pref-src), що забезпечує коректну роботу NAT і зворотних відповідей на запити.

Щоб уникнути некоректного спрямування трафіку на IP-адреси головного офісу (зокрема 10.10.10.1 та 10.10.20.1) через дефолтний маршрут, який може повернути відповіді через невірний інтерфейс, були створені правила маршрутизації, що змушують шукати маршрути до цих IP-адрес тільки в таблицях

ISP1-A та ISP1-B відповідно. Це дозволяє досягти симетричності з'єднання, що особливо критично для коректної роботи NAT та VPN.

Завершальним етапом конфігурації стало створення основних маршрутів до корпоративної мережі офісу туристичної фірми – 192.168.1.0/24. Було налаштовано чотири маршрути з різними адміністративними відстанями: через основний канал (AD=10), через резервний канал ISP-1 (AD=20), через основний VPN-тунель (AD=30), і через резервний VPN-тунель (AD=40). Завдяки такій градації, маршрутизатор автоматично перемикає маршрут у разі виявлення непрацездатності поточного шляху, забезпечуючи безперервний доступ до офісної мережі.

Налаштування механізму автоматичного та швидкого перемикання між каналами зв'язку у даній мережі є логічним продовженням реалізації багаторівневої відмовостійкої маршрутизації. На цьому етапі, після створення таблиць маршрутів і маршрутних правил, необхідно реалізувати контроль доступності каналів зв'язку з можливістю динамічного оновлення їх адміністративних пріоритетів (AD), що і досягається за допомогою спеціального скрипта моніторингу.

Для реалізації перемикання каналів створено спеціальний скрипт, який виконує постійний моніторинг доступності основних маршрутів. Принцип його роботи простий: кожен з каналів зв'язку (зокрема, основні два локальні й один через інтернет) тестується за допомогою пінгів до відповідних інтерфейсів головного офісу. Для кожного каналу виконується сім запитів із великим розміром пакету – 1500 байт. Результат вважається позитивним, якщо успішно повертається не менше п'яти відповідей. Такий метод дозволяє виявити не лише повну втрату зв'язку, а й часткову деградацію каналу, що в умовах корпоративної мережі має критичне значення.

Залежно від результатів перевірки, скрипт змінює адміністративну відстань відповідного маршруту. У разі виявлення проблем зв'язку, значення AD маршруту підвищується на 100 одиниць, що автоматично виводить його з числа пріоритетних, і система переходить на резервний шлях. Такий підхід забезпечує

миттєве реагування на втрату зв’язку без втручання адміністратора та без потреби повного перерахунку таблиць маршрутизації.

У ситуації, коли стають недоступними всі три канали, пов’язані з основним провайдером (два локальних і один через інтернет), скрипт ініціює додаткову логіку: викликається окремий сценарій, який може надіслати сповіщення системному адміністратору про аварію або відновлення, а також переключити зв’язок на останній резервний шлях – зовнішній VPN-тунель через ISP-2, який завжди має фіксоване значення AD = 40.

Необхідно зазначити, що перевірка виконується лише для трьох маршрутів. Останній, четвертий, VPN через ISP-2, не перевіряється свідомо – з міркувань економії часу та тому, що його статус завжди стабільний, оскільки не залежить від внутрішніх інтерфейсів основного провайдера. Таким чином, забезпечується ефективне балансування навантаження та повна автономність мережевого резервування у філіях.

NetWatch налаштовано на постійний моніторинг офісного шлюзу з IP-адресою 10.10.10.1 з інтервалом 10 секунд та тайм-аутом 2 секунди. У разі втрати доступності цього вузла система миттєво змінює адміністративну відстань відповідного маршруту, підвищуючи її на 100, що автоматично виводить маршрут із активного використання.

Одночасно запускається додатковий скрипт, який здійснює глибшу перевірку стану з'єднання. Якщо виявиться, що відмова була хибною (наприклад, через короткочасну нестабільність), скрипт повертає маршруту попередній пріоритет. Якщо ж обидва локальні канали зв'язку дійсно вийшли з ладу, скрипт відправляє повідомлення адміністраторам про аварію.

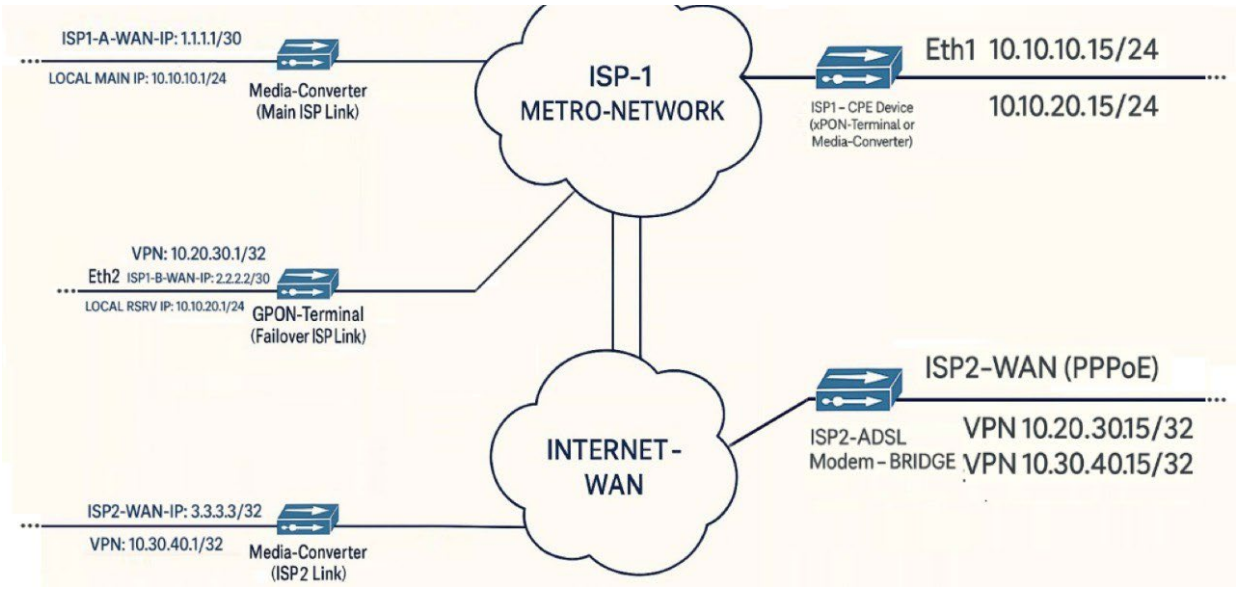


Рисунок 3.7 – Загальна схема підключення офісу і однієї філії туристичного агентства

У випадку, коли пінг знову починає відповідати, NetWatch не повертає маршрут до активного автоматично. Натомість повторно викликається той самий перевірочний скрипт, який аналізує стан каналів і приймає рішення щодо доцільності повернення на основний маршрут.

Подібні записи NetWatch реалізовано для всіх трьох критичних внутрішніх адрес у мережі провайдера ISP-1. Вони постійно пінгуються з обох боків – з офісу та філій, і у випадку порушення зв’язку виконують миттєве перевизначення маршруту через зміну AD і активацію глибшої перевірки. Це дозволяє забезпечити високу адаптивність та оперативність перемикання каналів без ручного втручання.

Скрипт EMAIL-IT-FAIL, який запускається на маршрутизаторі у разі втрати з'єднання філії з центральним офісом. Скрипт надсилає сповіщення на електронну пошту адміністратора, повідомляючи про аварійну ситуацію та автоматичний перехід на VPN-режим.

Скрипт, що відповідає за фіксацію відновлення зв’язку, повністю повторює структуру попереднього сценарію, за винятком зміненого тексту повідомлення. Основна його функція – автоматичне інформування адміністратора про те, що

з'єднання між філією і головним офісом відновлено і пристрої повернулись до штатного каналу передачі даних, минаючи резервний VPN.

З урахуванням усіх попередньо описаних технічних заходів, було здійснено повноцінну верифікацію результатів проєктування модернізованої корпоративної мережевої інфраструктури туристичної фірми. Аналіз проведено на основі впроваджених етапів сегментації мережі, побудови резервних каналів зв’язку, впровадження VPN-з’єднань із використанням L2TP, побудови складної структури маршрутів із використанням окремих таблиць маршрутизації та розумного перерозподілу адміністративних відстаней. Особливу увагу приділено автоматизації перемикання між основними та резервними каналами зв’язку, реалізованої через механізми Netwatch у поєднанні з користувацькими скриптами перевірки доступності, а також розгорнутій системі сповіщень адміністраторів за допомогою email-алертів про втрату або відновлення зв’язку.

Додатково було впроваджено статичне резервування VPN-тунелів через альтернативного провайдера ISP-2, із постійно піднятими з’єднаннями, що дозволило забезпечити повну мережеву доступність навіть у випадку одночасної відмови основних фізичних каналів. Кожна філія туристичної фірми має жорстку маршрутизовану прив’язку до офісної мережі через окремі логічні канали, що повністю усуває ефект широкомовного домену й дозволяє оптимізувати навантаження на мережеву інфраструктуру.

Також проведено повне конфігурування адресної структури, логічне впорядкування підмереж та маршрутизованих напрямків трафіку з чітким поділом ролей: офіс, основний канал, резерв, зовнішній VPN. Завдяки цьому вдалося мінімізувати ризики дублювання маршрутів, виключити маршрутизаційні конфлікти та підвищити предиктивність мережевої поведінки при аваріях.

3.4 Порівняльний аналіз ризиків до та після модернізації корпоративної мережевої інфраструктури

З метою оцінки ефективності впроваджених змін у мережевій інфраструктурі туристичної фірми було здійснено порівняльний аналіз ключових ризиків, які існували до модернізації, та їх поточного стану після впровадження відмовостійких рішень. У таблиці нижче наведено основні загрози, їх характеристики до змін та стан після технічної реалізації оновленої інфраструктури.

Таблиця 3.1 – Аналіз ризиків до та після модернізації

№	Категорія ризику	Стан до впровадження	Стан після впровадження	Зміна рівня ризику
1	Відмова зв’язку з філіями	Втрата зв’язку при збої в головному офісі або на стороні провайдера	Багаторівнева маршрутизація, резервні канали зв'язку	Значне зниження
2	Єдиний широкомовний домен	Високе навантаження, збої через broadcast-трафік	Сегментація на окремі VLAN для кожної філії	Знижено
3	Блокування DHCP / multicast	ONU блокують пакети; не працюють автоматичні сервіси	Обхід політик ONU, VLAN-конфігурація	Частково знижено
4	Нестабільна маршрутизація	Відсутність автоматичного перемикання між провайдерами	AD-пріоритети, VPN-зв’язки, скрипти	Значно знижено

Продовження таблиці 3.1 – Аналіз ризиків до та після модернізації

5	Недоступність офісних сервісів	Переривання доступу до баз даних, кас, синхронізації	VPN, резервні IP, автоматичне перемикання	Значно знижено
6	Відсутність моніторингу	Аварії виявлялись вручну, зі спізненням	Zabbix, NetWatch, email-сповіщення	Знижено
7	Перехоплення/втрата конфіденційності	Спільний VLAN – підвищений ризик	Сегментація, VPN, шифрування	Знижено
8	Відсутність централізованого контролю	Немає єдиної точки спостереження	Zabbix – моніторинг усіх вузлів	Знижено
9	Людський фактор у перемиканні	Перехід між каналами вручну	Автоматизація через скрипти	Знижено
10	Загальна інформаційна уразливість	Відсутність принципів багаторівневої ІБ	Впроваджено VPN, IPSec, сегментацію, контроль доступу	Знижено

На підставі проведеного аналізу можна стверджувати, що впроваджені технічні, організаційні та програмні рішення значною мірою підвищили стійкість мережі до збоїв, атак та людських помилок. Найбільший ефект досягнуто за рахунок резервування каналів зв’язку, впровадження багаторівневої маршрутизації та автоматизованого моніторингу з активним сповіщенням про інциденти. Це дозволяє гарантувати безперервність бізнес-процесів навіть у складних умовах експлуатації.

ВИСНОВКИ

У межах даної кваліфікаційної роботи було всебічно досліджено процес модернізації мережевої безпеки корпоративної мережевої інфраструктури туристичної фірми із фокусом на підвищення надійності, адаптивності та рівня контролю інфраструктури. На основі розгорнутого технічного аналізу сформовано цілісний підхід до перебудови локальної мережі, орієнтований на типову структуру підприємства з територіально розподіленими вузлами, зокрема з центральним офісом та дванадцятьма філіями, з'єднаними оптоволоконними каналами через FTTH та PON.

Корпоративна мережа розглядається як складна динамічна система, що забезпечує синхронізований обмін даними між критично важливими сервісами, зокрема інформаційними базами, програмними модулями, а також інфраструктурою доступу. На відміну від простих локальних мереж, вона вимагає впровадження структурованих принципів побудови – ізольованих сегментів, гнучких маршрутів, захищених каналів передачі даних, систем глибокого моніторингу та швидкого реагування на аварійні події.

У межах роботи було реалізовано обраний підхід конфігурації СМ3 * ЗВВ1 * ІБ2, що включає сегментацію на основі комутаторів, забезпечення зв'язку через виділену лінію з резервуванням, а також впровадження міжмережевого екранування на основі фільтрації пакетів. Завдяки проведеному аналізу щільності ймовірності трафіку підтверджено, що фактичне навантаження не перевищує 10 Мбіт/с у жодному з сегментів мережі. Це гарантує достатню пропускну здатність при використанні обладнання стандарту Ethernet 100 Мбіт/с та вище, із дотриманням нормативного обмеження до 40% використання пропускної спроможності каналу.

У процесі модернізації особливу увагу було приділено побудові логічної адресації та структури VLAN-ів у мережі провайдера. Кожна філія має власну ізольовану підмережу, що дозволяє уникнути конфліктів і впливу широкомовного

трафіку. Одним із ключових технічних рішень стала побудова резервної архітектури доступу – впроваджено L2TP-з'єднання з головним офісом через VPN, де кожна філія підтримує два активних тунелі до двох IP-адрес офісного маршрутизатора, що належать двом різним провайдерам.

Для автоматизації маршрутизації та швидкого перемикання між каналами у разі аварії було реалізовано політично керовану маршрутизацію (Policy-Based Routing), багаторівневу структуру маршрутів із розподілом адміністративної відстані (AD), створено окремі таблиці маршрутизації для кожного каналу зв'язку, а також розгорнуто механізми динамічного моніторингу їх доступності через Netwatch і контрольні скрипти з логікою оповіщення. Система виявлення подій та автоматичного реагування надсилає електронні листи з повідомленнями про втрату або відновлення з'єднання, чим гарантує оперативне реагування з боку IT-відділу.

Таким чином, модернізована корпоративна мережева інфраструктура туристичної фірми повністю перевершила попередню за всіма параметрами – від продуктивності та надійності до безпеки і керованості. Отримані результати свідчать про високу якість проєктних рішень і технічну доцільність впровадження подібної архітектури у реальному середовищі для забезпечення сталого функціонування критичної IT-інфраструктури туристичного бізнесу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Антонюк Л.В., Ситніков В.О. Інформаційна безпека підприємства: навч. посібник. Київ: КНЕУ, 2018.

2. Бібліографічний покажчик "Інформаційна безпека підприємства" / Уклад.: І. О. Іванов, О. В. Петрова, В. М. Сидоренко. Київ: Видавництво "Інформаційна безпека", 2019. 120 с.

3. Бібліографічний покажчик "Управління інформаційною безпекою підприємства" / Уклад.: І. М. Коваленко, М. В. Сергієнко, О. В. Шевченко. – Харків: Видавництво "Наукова думка", 2020. 180 с.

4. Богуславський В. І. Управління інформаційною безпекою підприємств: проблеми та перспективи розвитку / В. І. Богуславський, Л. М. Кравченко, В. М. Лагодюк. - Київ: НАУ, 2017. - 198 с.

5. Бондар В.І. Кібербезпека підприємства: навч. посібник. Київ: Центр учбової літератури, 2020.

6. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби : посібник / [В. Л. Бурячок, С. В. Толюпа, В. В. Семко та ін.]. – К. : ДУТ-КНУ, 2016. 178 с.

7. Гринчук А.М., Лисобей Л.В., Черняк В.А. Математична модель управління інформаційною безпекою установи. Збірник матеріалів проблемної наукової міжгалузевої конференції «Кібербезпека та комп’ютерно-інтегровані технології» (КБКІТ-2022). Тернопіль, 2022. С.43-45.

8. Гринчук А.М., Пилипів С.І., Войтенко О.О., Черняк В.А. Структура центру управління інформаційною безпекою для протидії загрозам. Збірник матеріалів проблемної наукової міжгалузевої конференції «Автоматизація та комп’ютерно-інтегровані технології» (АКІТ-2022). Тернопіль, 2022. С.88-90.

9. Грищук Р.В., Даник Ю.Г. Основи кібернетичної безпеки: Монографія. Житомир: ЖНАЕУ, 2016. 636 с.

10. Дузь-Крятченко О. П., Грицай П. М., Грищенко В. П., Клименко В. С. та ін. Основи стратегії національної безпеки та оборони держави: підруч. К. : НУОУ ім. Івана Черняховського, 2015. 620 с.

11. Єгорова-Гудкова Т.І., Шепитко Г.І. Економічна безпека держави в умовах цифровізації економіки та інваріант технологічного укладу. Вісник ОНУ. Серія: Економіка. 2020. № 5. С. 51-56

12. Журавльов І. В. Системний підхід до управління інформаційною безпекою підприємства / І. В. Журавльов, Н. О. Кондратюк, Л. М. Кравченко. Київ: Видавництво НАУ, 2019. 192 с.

13. ибальченко Л.В., Косиченко О.О. Проблеми безпеки персональних даних в Україні / Регіональна економіка / Запоріжжя. 2019. С.57-62

14. Іванов, І. О. Інформаційна безпека підприємства / І. О. Іванов, О. В. Петрова, В. М. Сидоренко. – Київ: Видавництво "Інформаційна безпека", 2019.

15. Іванов, П. С. Управління інформаційною безпекою підприємства: дисертація на здобуття наукового ступеня доктора економічних наук. Київський національний економічний університет імені Вадима Гетьмана,2018. 300 с.

16. Інформаційна безпека: навчальний посібник/ Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник, А. П. Бондарєв та інші; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І.В. Горбатого. Львів : Видавництво Львівської політехніки, 2019. 580 с.

17. Ключові цифри та тренди актуальні кіберзагрози: IV квартал 2022 року https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q4/

18. Коваленко, І. М. Управління інформаційною безпекою підприємства / І. М. Коваленко, М. В. Сергієнко, О. В. Шевченко. – Харків: Видавництво "Наукова думка", 2020.

19. Ковальчук, В. І. Управління інформаційною безпекою підприємства. Київ: Видавництво "Наукова думка", 2020. 200 с.

20. Лагодюк В. М. Моделі та методи управління інформаційною безпекою підприємства / В. М. Лагодюк, Л. М. Кравченко, В. І. Богуславський. Київ:

Видавничий центр НАУ, 2018. 230 с.

21. Литвиненко К. О., Філатова М. О. Системний аналіз управління людськими ресурсами сучасної ІТ-компанії. Ринкова економіка: сучасна теорія і практика управління. 2022. Т. 21 Вип. 1 (50). С. 111-128. URL: http://rinek.onu.edu.ua/issue/archive

22. Лісовська Ю. Кібербезпека. Ризики та заходи. К.: Кондор, 2019. 272 с.

23. Olena Sadchenko, Hanna Obykhod, Ivan Yaroshenko, Ludmyla Levkovska, Oleksandr Deineha, Tetiana Dombrovska Management of the Economy in the Field of Environmental Management and Energy Security as Components of Sustainable Development. J Sustain Res. (Journal of Sustainability Research) 2022;4(2):e220008. https://doi.org/10.20900/jsr20220008

24. Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. унт внутріш. справ, 2020. 144 с

25. Пількевич І.А., Лобанчикова Н.М.,. Молодецька К.В. Захист інформації в автоматизованих системах управління: посібник. Житомир: Вид-во ЖДУ ім. І. Франка, 2015. 226 с.

26. Посунько М.С., Черкасова В.Ю. Управління інформаційною безпекою підприємства: навч. посібник. Харків: Національний технічний університет "Харківський політехнічний інститут", 2019.

27. Правові засади інформаційної безпеки України: монографія / П.Д. Біленчук, Л.В. Борисова, І.М. Неклонський., В.О. Собина; за ред. П.Д. Біленчука – Харків: 2018. 289 с. [Електронний ресурс]. – Режим доступу: https://cutt.ly/5ugjj6s

28. Савенко О.С., Кльоц Ю.П., Лисенко С.М. Системне програмне забезпечення. – Хмельницький: ХНУ, 2016. 403с.

29. Сільченко О.В., Корчевна О.М., Корчевний С.Ю. Інформаційна безпека підприємства: навч. посібник. Київ: КНЕУ, 2019.

30. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. К.: КПІ ім. Ігоря Сікорського, 2018. 162 с. Режим доступу до ресурсу: https://ela.kpi.ua/bitstream/123456789/23896/1/ TZI_book.pdf

31. Теоретичні аспекти формування та функціонування системи забезпечення інформаційної безпеки України, https://pidru4niki.com/14051003/politologiya/teoretichni_aspekti_formuvannya_funktsionuvannya_sistemi_zabezpechennya_informatsiynoyi_bezpeki_ukrayini

32. Управління інформаційною безпекою. Конспект лекцій [Електронний ресурс] : навчальний посібник для студентів спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського ; уклад.: С. О. Носок, О. М. Фаль, В. М. Ткач. Електронні текстові дані. Київ : КПІ ім. Ігоря Сікорського, 2021. 258 с.

33. 50+Статистичних даних,фактів і тенденцій кібербезпеки на 2023 рік. https://www.websiterating.com/ru/research/cybersecurity-statistics-facts/

34. Boc K. , Vaculik J. , Vidrikova D. Fuzzy approach to risk analysis and its advantages against the qualitative approach // Proceedings of the 12th International Conference “Reliability and Statistics in Transportation and Communication” // Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia

Додаток А

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(ПРЕЗЕНТАЦІЯ)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Інформаційних технологій
Кафедра Комп'ютерної інженерії

КВАЛІФІКАЦІЙНА РОБОТА
НА ЗДОБУТТЯ ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВРА
на тему: «Побудова захищеної та відмовостійкої корпоративної мережевої інфраструтури»

Виконав студент групи КСЗ-51
Нікітченко Григорій Олександрович

Керівник кваліфікаційної роботи:
Кузьміч Ірина Богданівна, заступник директора ННІІТ

Київ – 2025

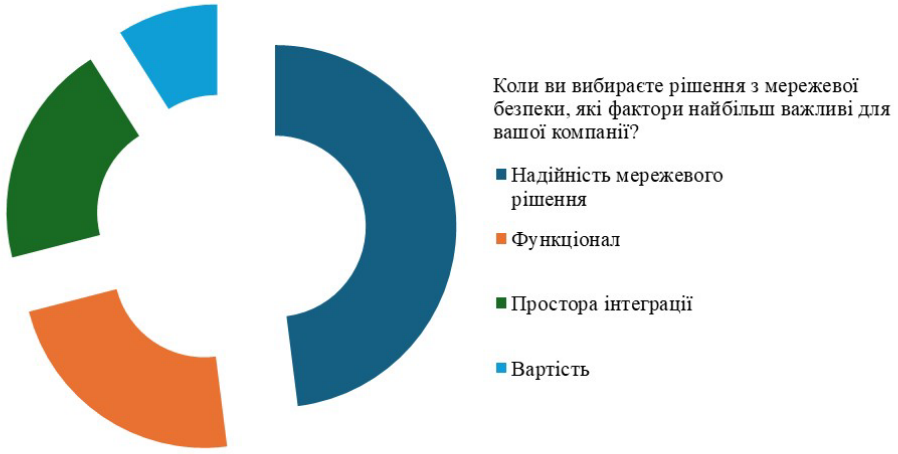
Мета, об'єкт та предмет дослідження

- *Мета роботи* – Побудова захищеної та відмовостійкої корпоративної мережевої інфраструктури
- *Об'єкт дослідження* – Система мережевої безпеки корпоративної інфраструктури, що забезпечує функціонування мережі як єдиного цифрового середовища.
- *Предмет дослідження* – Процеси, концептуальні моделі та методи модернізації архітектури корпоративної мережевої інфраструктури з метою підвищення її стійкості до мережевих загроз

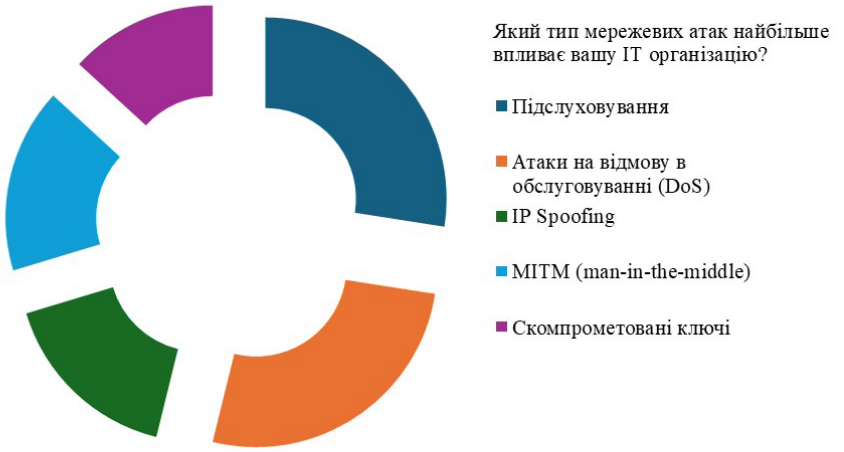
Актуальність дослідження

- З огляду на те, що ефективність функціонування мережі визначається такими параметрами, як продуктивність, масштабованість, надійність, керованість, вартість та рівень захисту інформації, проектування корпоративної інфраструктури повинно здійснюватися на основі системного аналізу альтернативних архітектурних рішень. Особливої актуальності набуває питання вибору раціональної структурної схеми з урахуванням специфіки підприємства, особливостей його предметної області та потенційних загроз, пов'язаних з витоком, модифікацією чи блокуванням критично важливої інформації. На практиці це ставить перед розробниками завдання оптимізації мережі за заданими критеріями функціональності, із одночасним дотриманням принципів інформаційної безпеки.

Діаграма відповідей на поставлене запитання

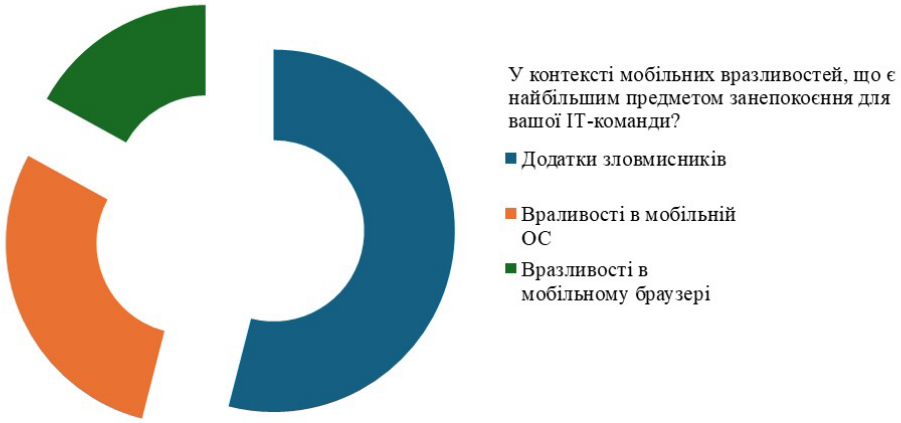


Діаграма відповідей на поставлене запитання



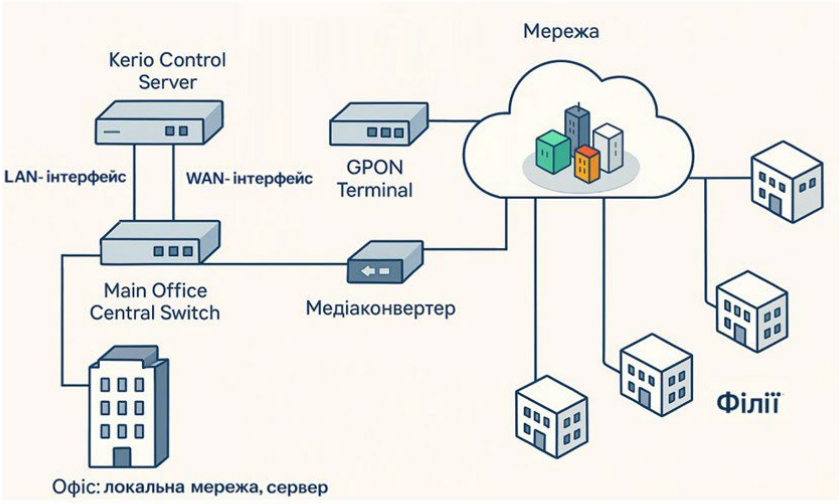
5

Діаграма відповідей на поставлене запитання



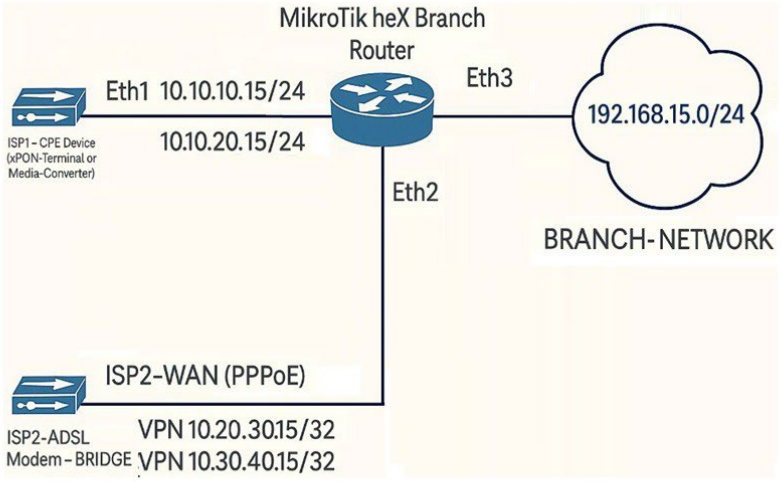
6

Схема мережі філій туристичної фірми до модернізації



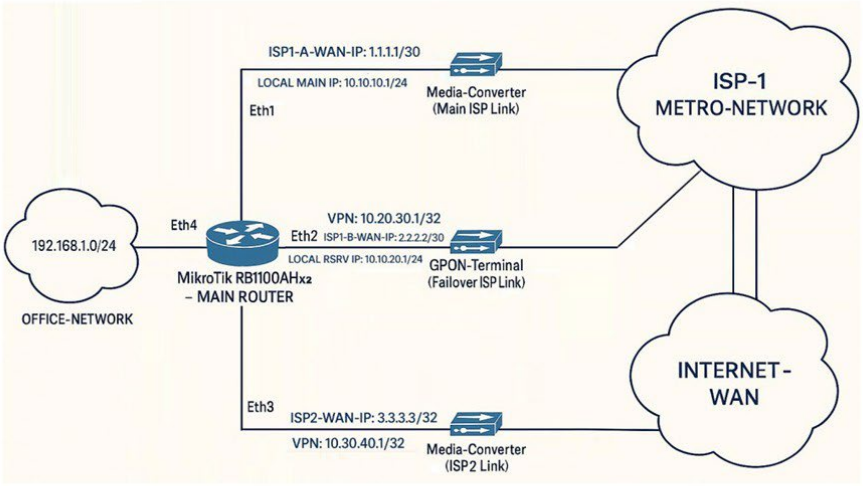
7

Схема підключення мережі в центральному офісі туристичної фірми

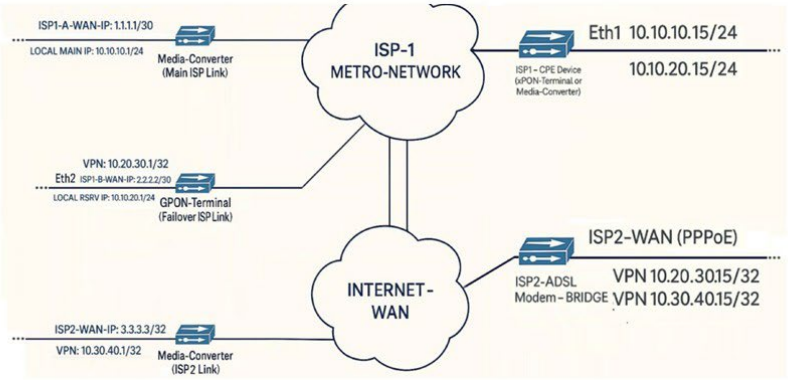


8

Схема підключення філії туристичної фірми



Загальна схема підключення офісу і однієї філії туристичного агентства



ВИСНОВКИ

- У процесі модернізації особливу увагу було приділено побудові логічної адресації та структури VLAN-ів у мережі провайдера. Кожна філія має власну ізольовану підмережу, що дозволяє уникнути конфліктів і впливу широкомовного трафіку. Одним із ключових технічних рішень стала побудова резервної архітектури доступу – впроваджено L2TP-з'єднання з головним офісом через VPN, де кожна філія підтримує два активних тунелі до двох IP-адрес офісного маршрутизатора, що належать двом різним провайдерам.
- Для автоматизації маршрутизації та швидкого перемикання між каналами у разі аварії було реалізовано політично керовану маршрутизацію (Policy-Based Routing), багаторівневу структуру маршрутів із розподілом адміністративної відстані (AD), створено окремі таблиці маршрутизації для кожного каналу зв'язку, а також розгорнуто механізми динамічного моніторингу їх доступності через Netwatch і контрольні скрипти з логікою оповіщення. Система виявлення подій та автоматичного реагування надсилає електронні листи з повідомленнями про втрату або відновлення з'єднання, чим гарантує оперативне реагування з боку IT-відділу.
- Таким чином, модернізована корпоративна мережева інфраструктура туристичної фірми повністю перевершила попередню за всіма параметрами – від продуктивності та надійності до безпеки і керованості. Отримані результати свідчать про високу якість проєктних рішень і технічну доцільність впровадження подібної архітектури у реальному середовищі для забезпечення сталого функціонування критичної IT-інфраструктури туристичного бізнесу.