ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНФОРМАЦІЙНИХ СИСТЕМ ТА ТЕХНОЛОГІЙ

КВАЛІФІКАЦІЙНА РОБОТА
на тему: «КОРПОРАТИВНА МЕРЕЖА НА БАЗІ ТЕХНОЛОГІЙ MIKROTIK ROUTEROS»

на здобуття освітнього ступеня бакалавр
зі спеціальності 126 Інформаційні системи та технології
(код, найменування спеціальності)
освітньо-професійної програми Інформаційні системи та технології
(назва)

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

_____ Роман ГРИГОР'ЄВ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: здобувач вищої освіти гр. ІСД-42
Роман ГРИГОР'ЄВ
Ім'я, ПРІЗВИЩЕ

Керівник:
доктор філософії Ольга ЖИДКА
Ім'я, ПРІЗВИЩЕ

Рецензент:
Ім'я, ПРІЗВИЩЕ

Київ 2026

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інформаційних систем та технологій

Ступінь вищої освіти Бакалавр

Спеціальність 126 Інформаційні системи та технології

Освітньо-професійна програма Інформаційні системи та технології

ЗАТВЕРДЖУЮ
Завідувач кафедрою ІСТ
Каміла СТОРЧАК
«_____» _____ 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Григор'єв Роман Віталійович
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Корпоративна мережа на базі технологій MikroTik RouterOS

керівник кваліфікаційної роботи Ольга ЖИДКА, доктор філософії,
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «20» лютого 2026р. №51

2. Строк подання кваліфікаційної роботи «01» червня 2026 р.

3. Вихідні дані до кваліфікаційної роботи: науково-технічна література, захищена корпоративної мережі на базі технологій MikroTik RouterOS.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

визначення вимог до побудови сучасної захищеної корпоративної мережі, аналіз потреб організації у безпечному передаванні даних .

розробка архітектури корпоративної мережі, вибір мережевих технологій і протоколів маршрутизації, побудова логічної та фізичної структури мережі.

5. Перелік графічного матеріалу: *презентація*

6. Дата видачі завдання «20» лютого 2026 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Визначення потреб та вимог до побудови захищеної корпоративної мережі. Формулювання мети та обґрунтування вибору технологій MikroTik RouterOS	15.04.2026 р.	Виконано
2	Аналіз наукової та технічної літератури з питань побудови корпоративних мереж та забезпечення їх інформаційної безпеки	20.04.2026 р.	Виконано
3	Огляд, порівняння та аналіз мережевих технологій і засобів захисту корпоративних мереж (VPN, IPsec, GRE, міжмережеві екрани, маршрутизація)	25.04.2026 р	Виконано
4	Проєктування архітектури захищеної корпоративної мережі. Розробка логічної та фізичної структури, IP-плану адресації та політик маршрутизації	30.04.2026 р.	Виконано
5	Реалізація корпоративної мережі на базі MikroTik RouterOS та аналіз результатів тестування у віртуальному середовищі	05.05.2026 р.	Виконано
6	Розробка демонстраційних матеріалів (схеми мережі, конфігурації, результати тестування)	15.05.2026 р.	Виконано
7	Розробка демонстраційних матеріалів	25.05.2026 р.	Виконано
8	Підготовка доповіді до захисту.	30.05.2026 р.	Виконано

Здобувач вищої освіти _____ Роман ГРИГОР'ЄВ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Ольга ЖИДКА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина бакалаврської роботи: 64 сторінки, 31 рисунок, 29 джерел.

Об'єкт дослідження – корпоративна комп'ютерна мережа підприємства, що функціонує в умовах розподіленої інфраструктури та потребує забезпечення високого рівня захищеності, надійності й доступності мережевих сервісів.

Предмет дослідження – технології побудови, захисту та адміністрування корпоративних мереж на базі операційної системи MikroTik RouterOS.

Мета роботи – розроблення та впровадження сучасної захищеної корпоративної мережі з використанням технологій MikroTik RouterOS.

Короткий зміст роботи:

У бакалаврській кваліфікаційній роботі розглянуто питання розробки та впровадження захищеної корпоративної комп'ютерної мережі з використанням технологій MikroTik RouterOS. Проаналізовано сучасні підходи до побудови мережевої інфраструктури, систем виявлення вторгнень та технологій захисту мережевої взаємодії (VPN, IPsec, GRE).

Практична частина роботи присвячена проєктуванню логічної топології, плану IP-адресації, розгортанню прототипу мережі в середовищі EVE-NG, налаштуванню маршрутизації OSPF, резервування VRRP та Dual ISP failover. Отримані результати підтверджують відмовостійкість розробленої архітектури, високу ефективність міжмережевого екранування та надійність шифрування міжфілійного трафіку.

КЛЮЧОВІ СЛОВА: MIKROTIK ROUTEROS, КОРПОРАТИВНА МЕРЕЖА, МЕРЕЖЕВА БЕЗПЕКА, VPN, IPSEC, GRE, МАРШРУТИЗАЦІЯ, МІЖМЕРЕЖЕВИЙ ЕКРАН, ФІЛЬТРАЦІЯ ТРАФІКУ, EVE-NG, ЗАХИСТ ІНФОРМАЦІЇ

ЗМІСТ

ВСТУП

Актуальність дослідження. У сучасних умовах цифровізації бізнес-процесів корпоративні комп'ютерні мережі відіграють ключову роль у забезпеченні безперервної діяльності організацій, обміну даними та доступу до інформаційних ресурсів. Одночасно зі зростанням масштабів і складності мережевих інфраструктур стрімко збільшується кількість і різноманіття кіберзагроз, зокрема несанкціонованого доступу, перехоплення трафіку, атак типу DoS/DDoS, а також внутрішніх загроз, пов'язаних із помилками конфігурації або зловживанням правами доступу.

Забезпечення належного рівня захищеності корпоративної мережі вимагає впровадження комплексного підходу, що поєднує сучасні технології маршрутизації, сегментації трафіку, віртуальних приватних мереж, міжмережевих екранів та механізмів контролю доступу. При цьому особливої актуальності набуває питання вибору мережевих рішень, які є не лише функціонально потужними, але й економічно доцільними, гнучкими в налаштуванні та здатними до масштабування відповідно до потреб організації.

Операційна система MikroTik RouterOS є одним із поширених рішень для побудови корпоративних мереж різного рівня складності, оскільки поєднує широкий набір мережевих і безпекових функцій, підтримку сучасних протоколів маршрутизації та засобів захисту інформації. Водночас практична імплементація захищених корпоративних мереж на базі MikroTik RouterOS потребує ґрунтовного аналізу архітектурних підходів, обґрунтованого проєктування та перевірки ефективності впроваджених рішень у наближених до реальних умовах.

У зв'язку з цим дослідження, присвячене імплементації сучасної захищеної корпоративної мережі з використанням технологій MikroTik RouterOS, є актуальним і має практичну цінність, оскільки дозволяє обґрунтувати вибір архітектури мережі, продемонструвати можливості платформи MikroTik у забезпеченні інформаційної безпеки та сформувати рекомендації щодо побудови надійної й масштабованої корпоративної мережевої інфраструктури.

Предмет дослідження – технології побудови, захисту та адміністрування корпоративних мереж на базі операційної системи MikroTik RouterOS.

Мета роботи – розроблення та впровадження сучасної захищеної корпоративної мережі з використанням технологій MikroTik RouterOS.

Наукові завдання:

1. аналіз сучасних технологій та методів побудови корпоративних комп'ютерних мереж, зокрема архітектурних підходів, протоколів маршрутизації та механізмів забезпечення інформаційної безпеки;
2. дослідження мережевих платформ і програмних засобів для реалізації захищених корпоративних мереж, зокрема можливостей операційної системи MikroTik RouterOS та її інструментів;
3. визначення ключових вимог до захищеної корпоративної мережі з урахуванням надійності, безпеки передавання даних, масштабованості, керованості та продуктивності мережевої інфраструктури;
4. реалізація захищеної корпоративної мережі на базі MikroTik RouterOS із використанням механізмів міжмережевого екрану, VPN-з'єднань, NAT та засобів контролю трафіку;
5. оцінка ефективності функціонування розробленої мережевої інфраструктури шляхом проведення тестування її працездатності, безпеки та продуктивності;
6. формулювання практичних рекомендацій щодо впровадження та експлуатації сучасних захищених корпоративних мереж на базі технологій MikroTik RouterOS.

Методи дослідження:

1. аналіз літературних та технічних джерел – вивчення сучасних підходів до побудови корпоративних мереж, принципів мережевої безпеки та можливостей обладнання mikrotik.
2. методи системного аналізу та проєктування – розроблення архітектури корпоративної мережі, визначення її логічної та фізичної топології, планування ір-адресації та сегментації мережі.

3. методи конфігурації та програмної реалізації – налаштування маршрутизаторів і комутаторів mikrotik, реалізація vpn-з’єднань, міжмережевого екранування, механізмів маршрутизації та фільтрації трафіку.

4. експериментальні методи – моделювання роботи корпоративної мережі в середовищі eve-ng, перевірка працездатності та надійності мережі, оцінка рівня її захищеності від мережевих загроз.

Наукова новизна одержаних результатів. У ході дослідження розроблено комплексну модель відмовостійкої розподіленої корпоративної мережі на базі операційної системи MikroTik RouterOS, яка передбачає інтеграцію механізмів динамічної маршрутизації OSPF із протоколом резервування шлюзу VRRP та балансуванням Dual ISP. Запропоновано оптимізовану схему периметрового захисту та Policy-Based Routing (PBR/PCC) у межах Packet Flow, що дозволяє підвищити рівень захищеності ізольованих IoT-сегментів і корпоративних даних без втрати загальної продуктивності. Результати моделювання в середовищі EVE-NG демонструють мінімальний час відновлення зв'язку та стійкість захищених VPN-тунелів до мережевих відмов.

Практична значущість одержаних результатів. Запропонована система забезпечує ефективне рішення для віддаленого увімкнення, вимкнення та контролю стану комп’ютерів у корпоративних мережах. Реалізоване рішення дозволяє зменшити витрати на обслуговування IT-інфраструктури, підвищити енергоефективність та забезпечити централізоване управління пристроями. Система може бути використана в організаціях різного масштабу для автоматизації процесів адміністрування та підтримки комп’ютерної техніки.

Апробація результатів. Основні положення та результати дослідження пройшли апробацію на:

1. III Всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» (Київ, ДУІКТ, 18 листопада 2025 р.). Тези доповіді на тему «Технологічні інновації в сучасній освіті: аналіз та перспективи впровадження» опубліковані у збірнику матеріалів конференції (стор. 305).

2. VII Всеукраїнській науково-технічній конференції «Сучасний стан та перспективи розвитку IoT» (Київ, ДУІКТ, 20 квітня 2026 р.). Тези доповіді на тему «Сучасні інформаційні технології в україні та світі: глобальні тренди та макроекономічний вплив» опубліковані у збірнику матеріалів конференції (стор. 29).

1 АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ЗАХИЩЕНИХ КОРПОРАТИВНИХ МЕРЕЖ

1.1 Сучасні архітектурні підходи до побудови корпоративних комп'ютерних мереж

З розвитком інформаційних технологій ефективне функціонування підприємств значною мірою залежить від використання інформаційних систем та мережевих інфраструктур. Одним із елементів такої інфраструктури є корпоративна комп'ютерна мережа, яка забезпечує обмін даними між користувачами, серверами та інформаційними системами організації.

Корпоративна мережа – це сукупність апаратних і програмних засобів, об'єднаних у єдину інформаційно-комунікаційну систему, що забезпечує передачу, обробку та зберігання даних у межах організації. Така мережа може об'єднувати робочі станції співробітників, сервери, мережеве обладнання, системи зберігання даних, а також різноманітні програмні сервіси, які використовуються для забезпечення бізнес-процесів підприємства.

Основною метою корпоративної мережі є створення єдиного інформаційного середовища для забезпечення ефективної взаємодії між підрозділами організації, оптимізації роботи з інформаційними ресурсами та підвищення продуктивності праці співробітників. Завдяки використанню корпоративної мережі підприємство отримує можливість централізовано керувати інформаційними ресурсами, контролювати доступ до даних, забезпечувати резервування інформації та підтримувати стабільну роботу критично важливих сервісів [1].

Для підприємств корпоративні мережі виконують низку важливих функцій. По-перше, вони забезпечують швидкий обмін інформацією між працівниками та структурними підрозділами організації. По-друге, дозволяють організувати спільний доступ до інформаційних ресурсів, таких як бази даних, файлові

сервери, корпоративні інформаційні системи та інші програмні сервіси. По-третє, корпоративні мережі забезпечують централізоване адміністрування та управління інформаційною інфраструктурою підприємства. Крім того, вони дозволяють реалізувати механізми захисту інформації, контролю доступу, шифрування трафіку та моніторингу мережевої активності.

Архітектура корпоративної мережі визначає спосіб організації мережевої інфраструктури, взаємодію між її елементами та принципи обробки мережевого трафіку. Від правильного вибору архітектури мережі залежить ефективність її роботи, масштабованість, надійність та рівень захищеності. У сучасних інформаційних системах застосовується декілька основних архітектурних підходів до побудови корпоративних мереж.

Модель клієнт-серверної архітектури мережі, зосереджена на спеціалізованих серверах, які обслуговують запити клієнтських пристроїв – це одна з найпоширених моделей. Клієнтами виступають робочі станції користувачів або інші пристрої, які звертаються до серверів для отримання доступу до даних або виконання певних операцій [2]. Такий підхід забезпечує централізоване управління ресурсами, підвищує рівень безпеки та дозволяє ефективно контролювати доступ до інформації.

Ієрархічна архітектура мережі, передбачає поділ мережевої інфраструктури на декілька рівнів, кожен з яких виконує певні функції. Зазвичай виділяють три основні рівні: рівень доступу (Access Layer), рівень розподілу (Distribution Layer) та магістральний рівень (Core Layer). Рівень доступу забезпечує підключення кінцевих пристроїв користувачів до мережі. Рівень розподілу виконує функції агрегації трафіку, маршрутизації та застосування політик безпеки. Магістральний рівень відповідає за високошвидкісну передачу даних між сегментами мережі та забезпечує її відмовостійкість.

Також у сучасних корпоративних мережах використовується багаторівнева (three-tier) архітектура інформаційних систем. У такій моделі мережеві сервіси розподіляються між трьома основними рівнями: рівнем представлення, рівнем прикладної логіки та рівнем зберігання даних. Рівень представлення відповідає за

взаємодію з користувачем, рівень прикладної логіки обробляє запити та реалізує бізнес-логіку системи, а рівень зберігання даних забезпечує доступ до баз даних та інших інформаційних ресурсів.

У великих організаціях використовується архітектура розподілених корпоративних мереж, із декількома територіально віддаленими офісами. У такій моделі мережа об’єднує декілька локальних мереж, що розташовані у різних географічних точках, за допомогою захищених каналів зв’язку, зокрема VPN-з’єднань. Це дозволяє створити єдину інформаційну інфраструктуру підприємства незалежно від місця розташування його підрозділів.

Можна сказати, що корпоративна мережа забезпечує ефективний обмін інформацією, централізоване управління ресурсами та підтримку бізнес-процесів організації. Використання сучасних архітектурних підходів до побудови корпоративних мереж дозволяє підвищити продуктивність роботи мережі, забезпечити її масштабованість, надійність та належний рівень інформаційної безпеки.

Як писалось вище, однією з базових моделей є архітектура Client–Server (рис. 1.1). У цій моделі мережеві ресурси та сервіси розміщуються на центральних серверах, які обслуговують запити клієнтських пристроїв. Клієнтами можуть виступати робочі станції користувачів, мобільні пристрої або інші комп’ютери, які звертаються до серверів для отримання доступу до файлів, баз даних або програмних сервісів. Основною перевагою цієї моделі є централізоване управління ресурсами, спрощене адміністрування та можливість реалізації політик безпеки на серверному рівні.

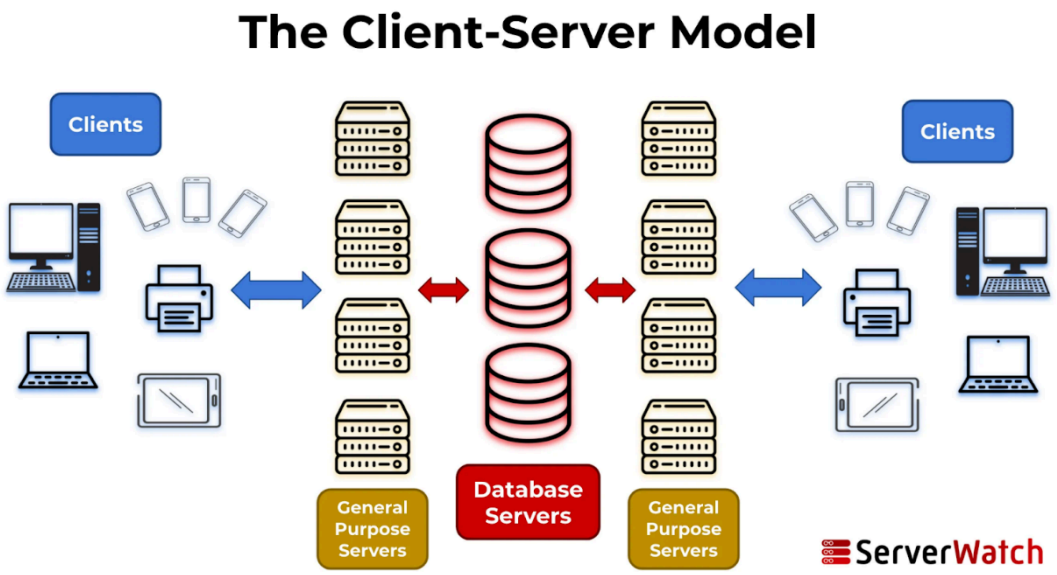


Рис. 1.1 – Архітектура Client–Server

Іншою поширеною моделлю є three-tier architecture (трирівнева архітектура). У цій моделі система поділяється на три логічні рівні: рівень представлення, рівень прикладної логіки та рівень даних [3]. Рівень представлення відповідає за взаємодію користувача з інформаційною системою. Рівень прикладної логіки забезпечує виконання бізнес-процесів і обробку запитів. Рівень даних відповідає за зберігання інформації у базах даних. Такий підхід дозволяє підвищити масштабованість системи, спростити її модифікацію та забезпечити більш ефективний розподіл навантаження між компонентами системи.

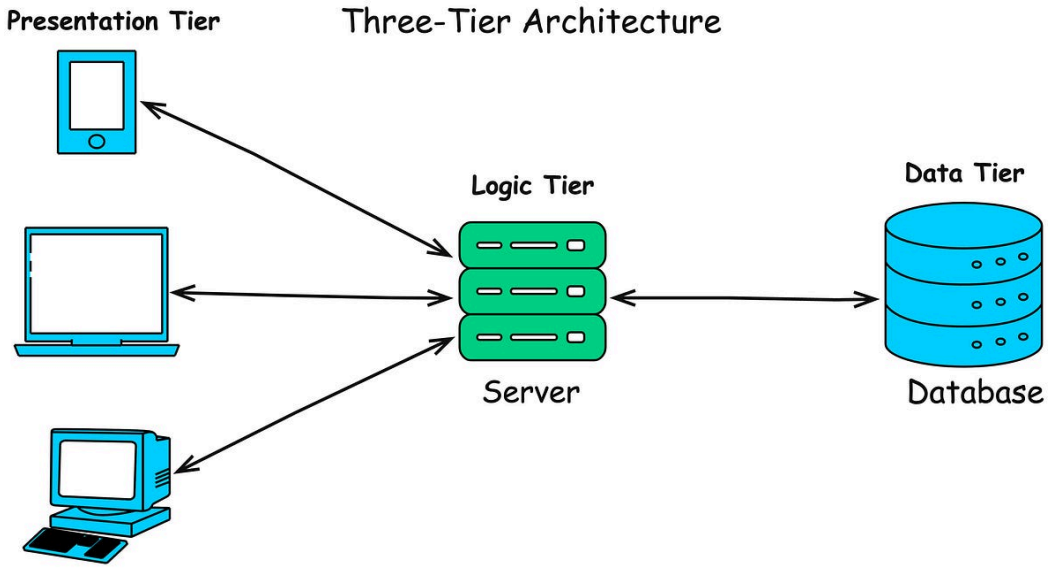


Рис. 1.2 – Трирівнева архітектура (Three-Tier Architecture)

Для великих організацій часто використовується модель Campus Network. Вона застосовується для побудови мереж у межах одного підприємства або комплексу будівель, наприклад університету, бізнес-центру або великого офісного кампусу. Така мережа об’єднує різні локальні сегменти, забезпечуючи централізоване управління доступом, сегментацію трафіку за допомогою VLAN та використання високошвидкісних магістральних каналів для передачі даних між підрозділами.

Data Center Network, використовується для організації мережевої інфраструктури центрів обробки даних. У такій архітектурі основна увага приділяється високій пропускній здатності, масштабованості та відмовостійкості мережі. Центри обробки даних забезпечують роботу серверів, систем зберігання даних та хмарних сервісів, що обслуговують як внутрішні потреби організації, так і зовнішніх користувачів [4].

З розвитком хмарних технологій значного поширення набули Cloud та Hybrid Cloud архітектури. У хмарній моделі частина або всі інформаційні ресурси організації розміщуються у хмарних дата-центрах постачальників хмарних сервісів. Гібридна модель поєднує локальну інфраструктуру підприємства з хмарними сервісами, що дозволяє гнучко масштабувати ресурси, зменшити витрати на обладнання та забезпечити високий рівень доступності сервісів.

Основні архітектурні моделі корпоративних мереж представлено у вигляді порівняльної табл. 1.1.

Таблиця 1.1 – Основні моделі архітектури корпоративних мереж

Модель архітектури	Основна характеристика	Переваги	Сфера застосування
Client–Server	Центральні сервери обслуговують запити клієнтів	централізоване управління, контроль доступу, просте адміністрування	корпоративні системи, файлові сервери, бази даних

Продовження таблиці 1.1

Three-tier architecture	Поділ системи на три рівні: представлення, логіка, дані	масштабованість, розподіл навантаження, гнучкість	веб-додатки, корпоративні інформаційні системи
Campus Network	Мережа, що об'єднує декілька будівель або підрозділів	висока швидкість, сегментація мережі, централізоване управління	університети, великі офіси, підприємства
Data Center Network	Мережа для центрів обробки даних	висока продуктивність, масштабованість, відмовостійкість	дата-центри, хмарні сервіси
Cloud / Hybrid Network	Використання хмарної або змішаної інфраструктури	гнучкість, масштабованість, економія ресурсів	хмарні платформи, сучасні IT-інфраструктури

1.2 Класифікація систем виявлення вторгнень

Зі зростанням кількості кіберзагроз, таких як несанкціонований доступ до інформаційних ресурсів, мережеві атаки, шкідливе програмне забезпечення та спроби перехоплення даних, виникає необхідність застосування спеціалізованих засобів захисту мережевої інфраструктури. Одним із таких засобів є системи виявлення вторгнень (Intrusion Detection Systems, IDS) [5].

Система виявлення вторгнень – це програмно-апаратний комплекс, призначений для моніторингу мережевого трафіку або активності комп’ютерних систем з метою виявлення підозрілих дій, спроб несанкціонованого доступу або інших проявів кіберзагроз. Основним завданням таких систем є аналіз подій у мережі або на окремих вузлах та своєчасне повідомлення адміністратора про можливі інциденти інформаційної безпеки.

Системи виявлення вторгнень дозволяють підвищити рівень захищеності корпоративної мережі шляхом постійного контролю мережевого трафіку, аналізу поведінки користувачів та виявлення потенційно небезпечних дій. Вони можуть

працювати як самостійні інструменти моніторингу або бути інтегрованими до комплексних систем забезпечення інформаційної безпеки.

Залежно від способу розміщення та принципу роботи системи виявлення вторгнень поділяються на декілька основних типів.

Першим типом є мережеві системи виявлення вторгнень (Network-based Intrusion Detection System, NIDS). Такі системи аналізують мережевий трафік, що проходить через мережеву інфраструктуру. Вони розміщуються у ключових точках мережі, наприклад на прикордонних маршрутизаторах або мережевих сегментах, де здійснюється інтенсивний обмін даними. NIDS дозволяє аналізувати пакети даних, виявляти підозрілу активність та фіксувати спроби атак на мережеві сервіси.

Другим типом є системи виявлення вторгнень на рівні вузла (Host-based Intrusion Detection System, HIDS). Такі системи встановлюються безпосередньо на комп’ютерах або серверах і здійснюють моніторинг їхньої внутрішньої активності. Вони аналізують журнали подій, зміни системних файлів, спроби доступу до ресурсів та інші події, що можуть свідчити про несанкціоноване втручання у роботу системи [6].

Окрім систем виявлення вторгнень, у сучасних мережах також застосовуються системи запобігання вторгненням (Intrusion Prevention Systems, IPS). На відміну від IDS, які лише виявляють потенційні загрози та повідомляють адміністратора, IPS здатні автоматично реагувати на підозрілу активність. Такі системи можуть блокувати шкідливий трафік, розривати з’єднання або застосовувати інші механізми захисту для запобігання атакам.

Системи виявлення та запобігання вторгненням можуть використовувати різні методи аналізу мережевої активності. Сигнатурний метод один із найпоширеніших, передбачає порівняння мережевого трафіку з базою відомих сигнатур атак. Якщо система знаходить відповідність між трафіком і сигнатурою атаки, вона фіксує інцидент безпеки.

Іншим методом є поведінковий або аномальний аналіз, який базується на визначенні нормальної поведінки мережі або користувачів. У разі виявлення

відхилень від звичайної активності система сигналізує про можливу загрозу. Такий підхід дозволяє виявляти нові або невідомі типи атак, які ще не мають сигнатур у базі даних.

Також використовується гібридний метод, який поєднує сигнатурний аналіз та аналіз поведінки. Це дозволяє підвищити ефективність виявлення атак та зменшити кількість помилкових спрацювань системи.

У сучасних корпоративних мережах системи IDS та IPS часто інтегруються з іншими засобами мережевої безпеки, такими як міжмережеві екрани, системи керування подіями інформаційної безпеки (SIEM), системи контролю доступу та засоби моніторингу мережі. Комплексний підхід дозволяє створити багаторівневу систему захисту інформаційної інфраструктури організації.

Системи виявлення вторгнень IDS/IPS дозволяють своєчасно виявляти спроби атак, контролювати мережеву активність та підвищувати рівень захищеності інформаційних ресурсів підприємства [7].

Для кращого розуміння особливостей функціонування систем виявлення вторгнень доцільно розглянути їх класифікацію залежно від місця встановлення та принципу роботи. Різні типи таких систем дозволяють контролювати як мережевий трафік, так і активність окремих комп’ютерних вузлів, що забезпечує комплексний підхід до захисту інформаційної інфраструктури підприємства.

Залежно від архітектури та способу аналізу інформації системи виявлення вторгнень поділяються на декілька основних типів, серед яких найбільш поширеними є мережеві системи виявлення вторгнень (NIDS), системи виявлення вторгнень на рівні вузла (HIDS) та системи запобігання вторгненням (IPS). Основні характеристики цих систем наведено в табл. 1.2.

Таблиця 1.2 – Класифікація систем виявлення вторгнень

Тип системи	Опис	Місце встановлення
NIDS	Аналізує мережевий трафік і виявляє підозрілу активність	мережеві сегменти, маршрутизатори

Продовження таблиці 1.2

HIDS	Контролює активність окремого комп’ютера або сервера	робочі станції, сервери
IPS	Автоматично блокує або запобігає атакам	мережеві шлюзи, міжмережеві екрани

На рис. 1.3 представлено приклад організації периметрового захисту корпоративної мережі підприємства. У цій архітектурі зовнішня мережа Інтернет підключається через провайдера (ISP), після чого мережевий трафік надходить до прикордонного мережевого обладнання. На межі між зовнішньою та внутрішньою мережею розміщується міжмережевий екран (Firewall), який виконує функції фільтрації трафіку, контролю доступу та захисту внутрішніх ресурсів від несанкціонованого доступу.

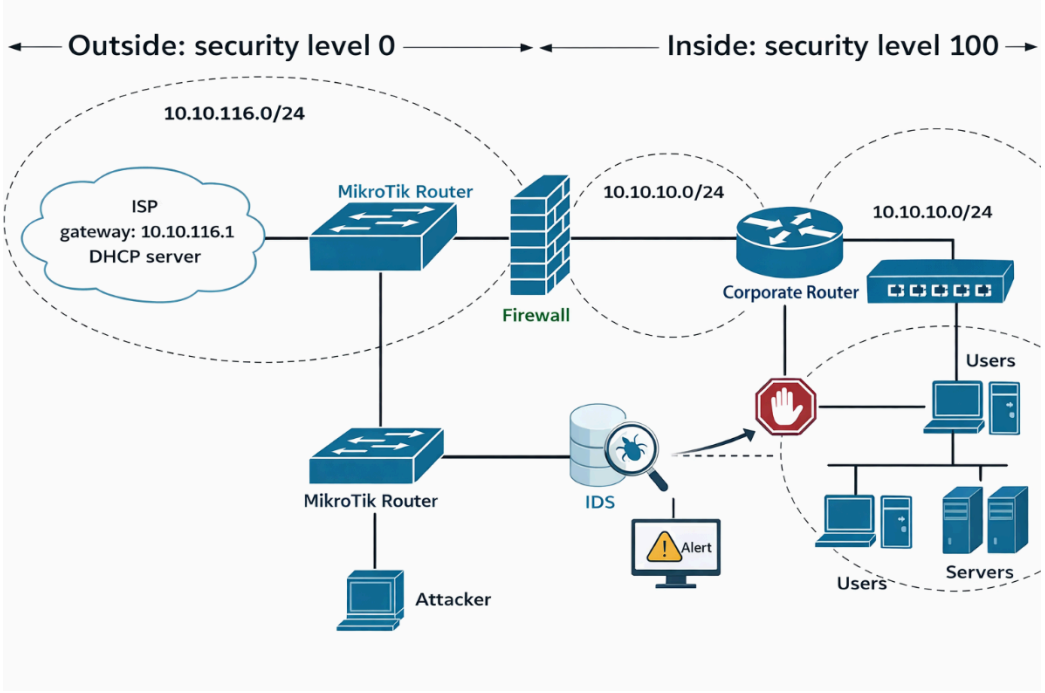


Рис. 1.3 – Схема периметрового захисту корпоративної мережі із застосуванням міжмережевого екрана

Після проходження через міжмережевий екран трафік спрямовується до внутрішнього маршрутизатора, який забезпечує маршрутизацію пакетів у межах локальної мережі підприємства. Внутрішній сегмент мережі містить користувацькі пристрої та серверні ресурси, доступ до яких контролюється

політиками безпеки. Такий підхід дозволяє ізолювати внутрішню інфраструктуру підприємства від зовнішніх загроз та забезпечити багаторівневий захист корпоративної мережі.

1.3 Технології захисту мережевої взаємодії (GRE, IPsec, site-to-site VPN)

У сучасних корпоративних мережах важливим завданням є забезпечення безпечної передачі даних між різними сегментами мережі, а також між віддаленими офісами підприємства. З розвитком інформаційних технологій та збільшенням кількості віддалених підключень виникає необхідність використання спеціалізованих технологій, які дозволяють захищати мережевий трафік від несанкціонованого доступу, перехоплення або модифікації. До таких технологій належать віртуальні приватні мережі (VPN), протоколи тунелювання GRE та протоколи шифрування IPsec.

Віртуальна приватна мережа (Virtual Private Network, VPN) – це технологія, яка дозволяє створювати захищені з’єднання поверх відкритих або незахищених мереж, таких як Інтернет. VPN забезпечує конфіденційність, цілісність і автентичність переданих даних шляхом використання механізмів шифрування та аутентифікації [8]. Завдяки використанню VPN організації можуть об’єднувати свої віддалені підрозділи в єдину корпоративну мережу незалежно від географічного розташування.

Одним із найпоширеніших типів VPN є site-to-site VPN, який використовується для організації захищеного з’єднання між двома або більше локальними мережами. Такий тип VPN дозволяє створити захищений канал зв’язку між офісами підприємства через мережу Інтернет. У цьому випадку маршрутизатори або шлюзи безпеки на кожному боці тунелю виконують функції шифрування та дешифрування трафіку. Для користувачів така мережа виглядає як єдина локальна мережа, хоча фізично вона може бути розподілена між різними містами або навіть країнами.

Для реалізації захищених VPN-з’єднань широко використовується протокол IPsec (Internet Protocol Security). IPsec є набором протоколів і стандартів, призначених для забезпечення захисту мережевого трафіку на мережевому рівні моделі OSI. Основними функціями IPsec є шифрування даних, перевірка автентичності сторін з’єднання та контроль цілісності переданих пакетів.

IPsec може працювати у двох основних режимах: transport mode та tunnel mode. У транспортному режимі шифрується лише корисне навантаження пакета, тоді як заголовок IP залишається незмінним. Такий режим зазвичай використовується для захисту з’єднання між окремими вузлами. У тунельному режимі шифрується весь IP-пакет, який інкапсулюється в новий пакет із новим заголовком. Саме цей режим найчастіше використовується для побудови VPN між мережами.

Ще однією технологією тунелювання є GRE (Generic Routing Encapsulation). GRE є протоколом, який дозволяє інкапсулювати різні типи мережевих протоколів у IP-пакети та передавати їх через мережу. Основною перевагою GRE є можливість передавати різні типи трафіку, включаючи маршрутизаційні протоколи, через тунель між двома мережевими пристроями.

На відміну від IPsec, GRE сам по собі не забезпечує шифрування даних. Тому у практичних мережевих рішеннях часто використовується комбінація GRE over IPsec, у якій GRE відповідає за тунелювання мережевого трафіку, а IPsec забезпечує його шифрування та захист. Такий підхід дозволяє поєднати гнучкість GRE із високим рівнем безпеки IPsec.

У корпоративних мережах технології VPN, IPsec та GRE широко використовуються для організації захищених каналів зв’язку між центральним офісом і віддаленими підрозділами, для забезпечення доступу співробітників до внутрішніх ресурсів підприємства, а також для захисту передачі конфіденційної інформації через публічні мережі. Використання таких технологій дозволяє значно підвищити рівень інформаційної безпеки організації та забезпечити надійну роботу корпоративної мережевої інфраструктури [9].

Таким чином, застосування технологій VPN, IPsec та GRE є важливим елементом побудови сучасних захищених корпоративних мереж. Вони забезпечують безпечну передачу даних між різними сегментами мережі, дозволяють об’єднувати віддалені офіси підприємства та створюють надійну основу для функціонування корпоративних інформаційних систем.

Таблиця 1.3 – Порівняння технологій захисту мережевої взаємодії

Технологія	Основне призначення	Переваги
VPN	створення захищених каналів зв’язку	захист трафіку, віддалений доступ
IPsec	шифрування мережевого трафіку	високий рівень безпеки
GRE	тунелювання мережевих протоколів	гнучкість та підтримка різних типів трафіку

На рисунку 1.4 представлено приклад організації захищеного з’єднання між декількома віддаленими мережами за допомогою технології VPN. У цій архітектурі центральний вузол мережі розташований у головному офісі (Head Office) та виконує роль основного маршрутизатора або шлюзу, через який здійснюється взаємодія між усіма підключеними сегментами мережі.

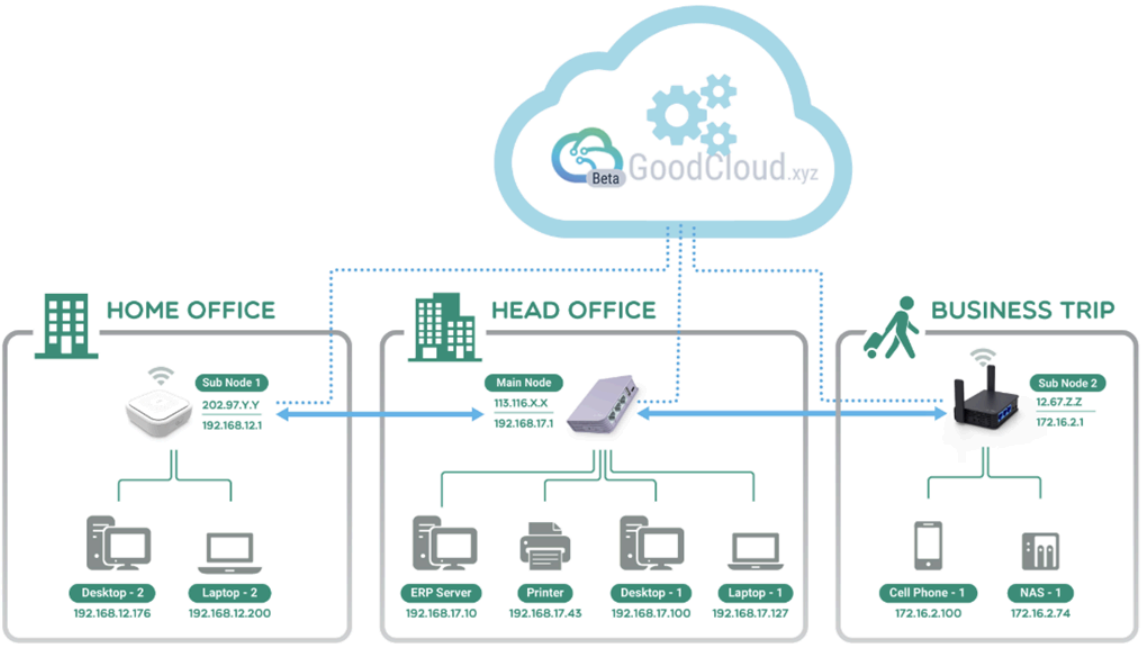


Рис. 1.4 – Схема організації захищеного з’єднання між віддаленими мережами за допомогою VPN

Віддалені мережі, такі як домашній офіс (Home Office) або мобільний вузол під час службових поїздок (Business Trip), підключаються до головного офісу через захищені VPN-тунелі, які проходять через публічну мережу Інтернет. Перед передачею через Інтернет мережевий трафік інкапсулюється та шифрується, що забезпечує конфіденційність, цілісність і автентичність переданої інформації.

Завдяки використанню VPN-тунелів усі віддалені сегменти мережі можуть взаємодіяти між собою так, ніби вони знаходяться в одній локальній мережі. Це дозволяє співробітникам отримувати доступ до внутрішніх ресурсів підприємства, серверів і корпоративних сервісів незалежно від їхнього фізичного розташування.

Таким чином, використання технології VPN дозволяє організувати безпечну взаємодію між центральним офісом і віддаленими підрозділами підприємства, забезпечуючи захист даних під час їх передачі через публічні мережі.

1.4 Особливості мережевого обладнання для корпоративних мереж

Ефективне функціонування корпоративної комп’ютерної мережі значною мірою залежить від правильно обраного мережевого обладнання. Саме мережеві

пристрої забезпечують передачу даних між вузлами мережі, організацію доступу до інформаційних ресурсів, керування мережевим трафіком та реалізацію механізмів інформаційної безпеки. У корпоративних мережах застосовується широкий спектр мережевого обладнання, яке виконує різні функції залежно від архітектури мережі та вимог до її продуктивності й захищеності.

До основних типів мережевого обладнання, що використовуються у корпоративних мережах, належать маршрутизатори, комутатори, міжмережеві екрани, точки бездротового доступу та інші спеціалізовані пристрої. Кожен із цих елементів виконує свою роль у забезпеченні стабільної та безпечної роботи мережевої інфраструктури підприємства.

Основним завданням маршрутизатора є передача пакетів даних між різними мережами або підмережами. Маршрутизатори аналізують адреси призначення пакетів та визначають оптимальний маршрут для їх передачі. У корпоративних мережах маршрутизатори також можуть виконувати функції міжмережевого екрану, реалізовувати VPN-з’єднання, забезпечувати трансляцію мережевих адрес (NAT) та здійснювати контроль доступу до мережевих ресурсів [10].

На рисунку 1.5 представлено приклад використання маршрутизатора у корпоративній мережі. Маршрутизатор виконує функцію з’єднання різних мереж або підмереж та забезпечує передачу пакетів даних між ними. Він аналізує IP-адресу призначення кожного пакета та визначає оптимальний маршрут його доставки.

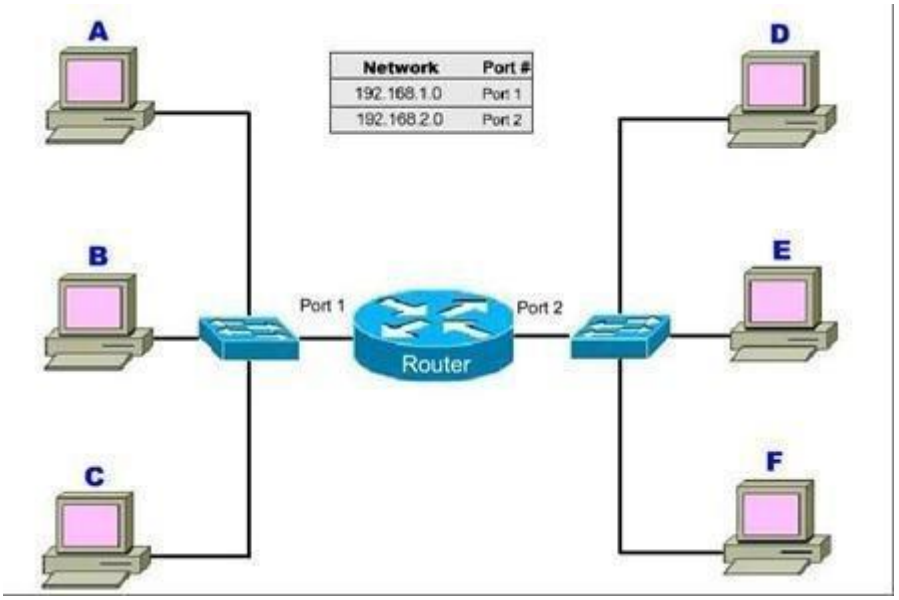


Рис. 1.5 – Використання маршрутизатора у корпоративній мережі

Комутатори забезпечують передачу даних між пристроями всередині локальної мережі (LAN). Вони працюють на канальному рівні моделі OSI та використовують MAC-адреси для визначення адресатів мережевих пакетів. У корпоративних мережах широко застосовуються керовані комутатори, які підтримують функції сегментації мережі за допомогою технології VLAN, керування трафіком, моніторингу мережевої активності та забезпечення якості обслуговування (QoS) [11].

На рисунку 1.6 показано принцип роботи комутатора у локальній мережі. Комутатор забезпечує з’єднання різних пристроїв, таких як комп’ютери, сервери або мережеві принтери, у межах однієї локальної мережі. Передача даних здійснюється на основі MAC-адрес пристроїв, що дозволяє ефективно направляти пакети лише до потрібного отримувача.

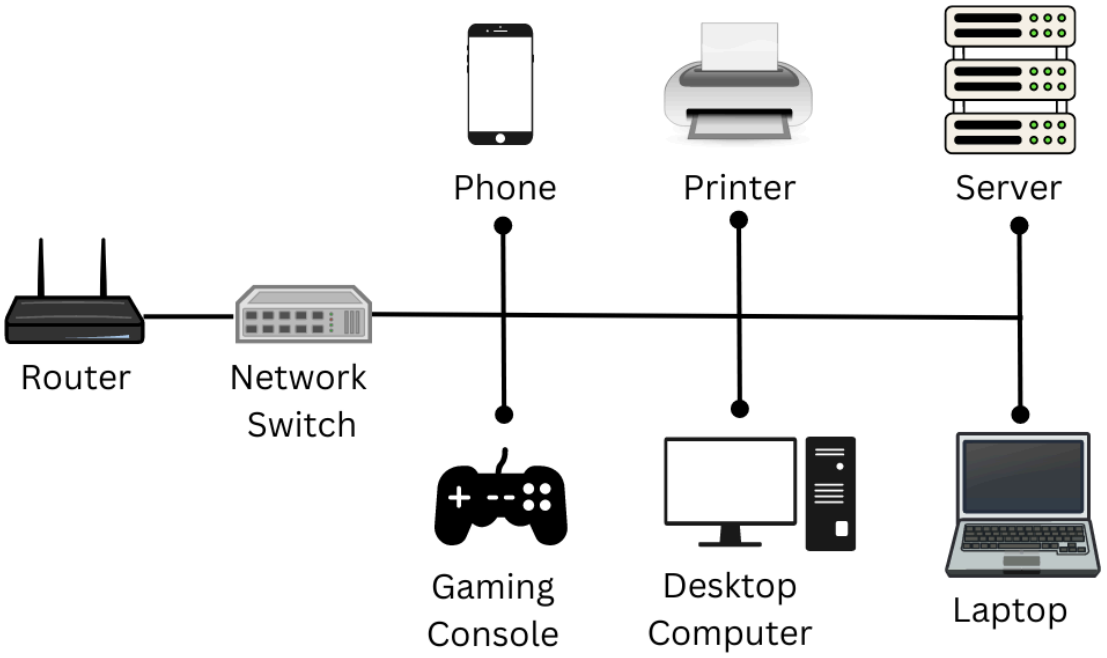


Рис. 1.6 – Робота комутатора в локальній мережі

Для забезпечення захисту мережі від зовнішніх загроз використовуються міжмережеві екрани (firewalls). Основною функцією міжмережевого екрана є фільтрація мережевого трафіку на основі встановлених правил безпеки. Firewall дозволяє контролювати доступ до внутрішніх ресурсів підприємства, блокувати підозрілий трафік, запобігати несанкціонованому доступу та захищати мережу від різних типів атак.

На рисунку 1.7 показано принцип роботи комутатора у локальній мережі. Комутатор забезпечує з’єднання різних пристроїв, таких як комп’ютери, сервери або мережеві принтери, у межах однієї локальної мережі. Передача даних здійснюється на основі MAC-адрес пристроїв, що дозволяє ефективно направляти пакети лише до потрібного отримувача.

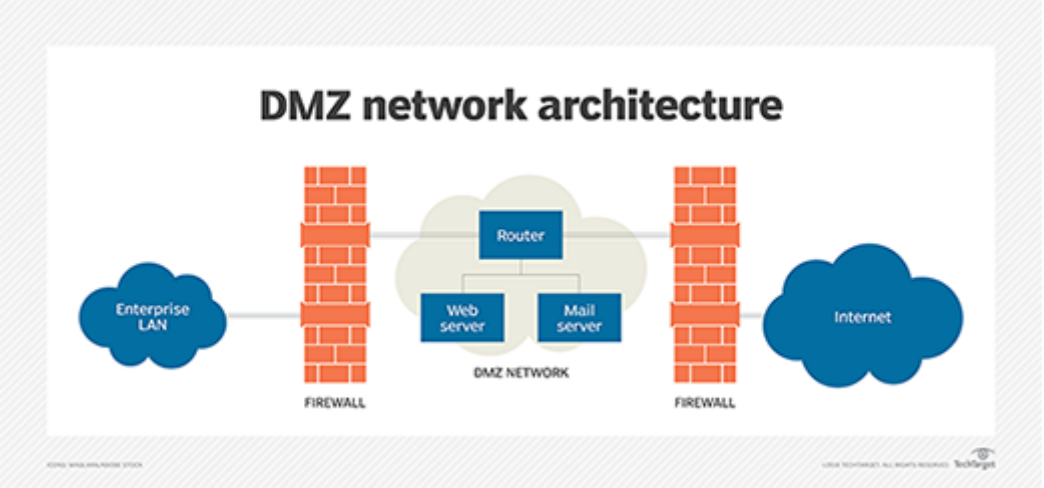


Рис. 1.7 – Використання міжмережевого екрана для захисту корпоративної мережі

У сучасних корпоративних мережах також широко використовуються точки бездротового доступу (access points), які забезпечують підключення мобільних пристроїв до мережі за допомогою технологій Wi-Fi. Бездротові мережі дозволяють підвищити мобільність користувачів та спростити організацію доступу до мережевих ресурсів. При цьому важливо забезпечити належний рівень безпеки бездротових мереж шляхом використання сучасних методів шифрування та автентифікації користувачів.

Особливістю мережевого обладнання для корпоративних мереж є підтримка розширених функцій керування та безпеки. До таких функцій належать підтримка протоколів маршрутизації, створення віртуальних локальних мереж (VLAN), балансування навантаження, реалізація VPN-з’єднань, а також засоби моніторингу та адміністрування мережі. Використання таких функцій дозволяє забезпечити ефективне управління мережею, підвищити її надійність та захищеність.

Корпоративні мережі також потребують високої масштабованості та відмовостійкості. Тому мережеве обладнання повинно підтримувати механізми резервування, автоматичного відновлення з’єднань та балансування трафіку між різними каналами зв’язку. Це дозволяє забезпечити безперервність роботи інформаційних систем підприємства навіть у разі відмови окремих компонентів мережі.

Від правильного вибору та налаштування мережевих пристроїв залежить продуктивність, надійність та рівень безпеки корпоративної мережі. Використання мережевого обладнання з підтримкою розширених функцій управління та захисту дозволяє створити ефективну і масштабовану мережеву інфраструктуру, здатну забезпечити стабільну роботу інформаційних систем підприємства.

Таблиця 1.4 – Основні типи мережевого обладнання корпоративних мереж

Тип обладнання	Основне призначення	Основні функції
Маршрутизатор	передача пакетів між мережами	маршрутизація, NAT, VPN
Комутатор	з’єднання пристроїв у локальній мережі	VLAN, QoS, керування трафіком
Firewall	захист мережі	фільтрація трафіку, контроль доступу
Access Point	бездротовий доступ	Wi-Fi підключення, шифрування

1.5 Аналіз можливостей MikroTik RouterOS у задачах побудови захищених мереж

У корпоративній мережах важливе використання надійних програмно-апаратних рішень, які забезпечують ефективне керування мережевим трафіком, реалізацію механізмів захисту інформації та підтримку різних мережевих сервісів. Одним із таких рішень є операційна система MikroTik RouterOS, яка широко використовується для побудови мережевої інфраструктури підприємств різного масштабу.

MikroTik RouterOS – це спеціалізована мережева операційна система, розроблена компанією MikroTik, яка встановлюється на мережеві пристрої та забезпечує виконання функцій маршрутизатора, міжмережевого екрана, VPN-шлюзу, комутатора та інших мережевих сервісів. Вона використовується як у

невеликих локальних мережах, так і у великих корпоративних інфраструктурах завдяки широкому набору функцій і можливостей налаштування.

Рис. 1.8 – Логотип MikroTik RouterOS

Однією з основних переваг RouterOS є підтримка широкого спектра мережевих протоколів та технологій. Система підтримує різні протоколи маршрутизації, зокрема статичну маршрутизацію, OSPF, BGP та RIP, що дозволяє ефективно організовувати маршрутизацію трафіку між різними сегментами мережі. Завдяки цьому MikroTik RouterOS може використовуватися як у простих локальних мережах, так і у складних розподілених мережевих інфраструктурах.

Функціональною можливістю RouterOS є підтримка віртуальних приватних мереж (VPN). Система дозволяє реалізовувати різні типи VPN-з’єднань, зокрема IPsec, L2TP, PPTP, SSTP та OpenVPN. Використання таких технологій дозволяє організовувати захищені канали зв’язку між віддаленими офісами підприємства або забезпечувати безпечний доступ співробітників до внутрішніх ресурсів мережі через Інтернет [12].

RouterOS також має потужні механізми мережевого захисту. До них належать функції міжмережевого екрану (Firewall), фільтрації пакетів, контролю з’єднань, обмеження доступу до ресурсів та захисту від різних типів мережевих атак. Firewall у RouterOS дозволяє створювати детальні правила фільтрації трафіку, що забезпечує ефективний контроль доступу до мережевих ресурсів і захист корпоративної мережі від несанкціонованого доступу.

MikroTik RouterOS є підтримує NAT (Network Address Translation), яка дозволяє транслювати приватні IP-адреси внутрішньої мережі у публічні адреси при доступі до мережі Інтернет. Це дозволяє ефективно використовувати адресний простір та підвищує рівень безпеки внутрішньої мережі.

RouterOS також підтримує технології VLAN, які дозволяють логічно сегментувати мережу та розділяти різні типи трафіку між підрозділами

організації. Такий підхід дозволяє підвищити рівень безпеки мережі, спростити її адміністрування та оптимізувати використання мережевих ресурсів.

Крім того, RouterOS має розвинуті засоби моніторингу та керування мережею. Адміністратор може використовувати інструменти аналізу трафіку, системи журналювання подій, засоби контролю пропускної здатності каналів та інші механізми, які дозволяють контролювати роботу мережі та своєчасно виявляти можливі проблеми або загрози безпеці. MikroTik RouterOS є гнучкість налаштування та відносно невисока вартість обладнання порівняно з іншими корпоративними мережевими рішеннями. Завдяки цьому MikroTik широко використовується у малому та середньому бізнесі, освітніх установах, а також у великих корпоративних мережах [13].

Аналіз можливостей MikroTik RouterOS показує, що ця система має широкий набір функцій для побудови захищених корпоративних мереж. Вона забезпечує підтримку сучасних протоколів маршрутизації, реалізацію VPN-з’єднань, фільтрацію мережевого трафіку, сегментацію мережі та інші механізми забезпечення інформаційної безпеки. Використання MikroTik RouterOS дозволяє створювати гнучкі, масштабовані та надійні мережеві інфраструктури, що відповідають сучасним вимогам до захисту інформації (табл. 1.5).

Таблиця 1.5 – Основні функції MikroTik RouterOS

Функція	Призначення
Маршрутизація	передача пакетів між мережами
Firewall	фільтрація мережевого трафіку
VPN	створення захищених каналів зв’язку
NAT	трансляція IP-адрес
VLAN	сегментація мережі
Моніторинг	контроль роботи мережі

2 ПРОЄКТУВАННЯ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ НА БАЗІ MIKROTIK ROUTEROS

2.1 Вибір та обґрунтування мережевого обладнання MikroTik

Під час проєктування корпоративної комп'ютерної мережі важливим етапом є вибір мережевого обладнання, яке забезпечуватиме стабільну передачу даних, ефективне керування трафіком та належний рівень інформаційної безпеки. Вибір обладнання повинен здійснюватися з урахуванням вимог до продуктивності мережі, масштабованості інфраструктури, рівня захисту даних та економічної доцільності впровадження.

Для реалізації проєктованої мережевої інфраструктури у даній роботі було обрано обладнання компанії MikroTik, яке працює під керуванням операційної системи RouterOS. Продукція MikroTik широко використовується для побудови локальних та корпоративних мереж завдяки поєднанню широкого функціоналу, гнучкості налаштування та відносно невисокої вартості у порівнянні з іншими мережевими рішеннями корпоративного класу [14].

Основною перевагою обладнання MikroTik є підтримка великої кількості мережевих технологій, таких як маршрутизація, міжмережевий екран, створення VPN-з'єднань, сегментація мережі за допомогою VLAN, балансування навантаження та контроль пропускної здатності каналів. Це дозволяє використовувати один пристрій для виконання функцій декількох мережевих компонентів, що значно спрощує адміністрування мережі та зменшує витрати на її впровадження.

У корпоративних мережах обладнання MikroTik може використовуватися у різних ролях, зокрема як прикордонний маршрутизатор, VPN-шлюз, комутатор або центральний мережевий вузол. Залежно від масштабу мережі та вимог до продуктивності використовуються різні серії пристроїв MikroTik.

Однією з таких серій є MikroTik CCR (Cloud Core Router), пристрої цієї серії призначені для використання у великих мережах з високими вимогами до продуктивності. Вони оснащені потужними багатоядерними процесорами та здатні обробляти значні обсяги мережевого трафіку. CCR часто використовуються у дата-центрах, великих корпоративних мережах або мережах провайдерів Інтернету.

Іншою поширеною серією є MikroTik RB (RouterBoard). Пристрої цієї серії є універсальними маршрутизаторами, які широко застосовуються у малих та середніх корпоративних мережах. Вони підтримують усі основні функції RouterOS, включаючи маршрутизацію, VPN, NAT, фільтрацію трафіку та керування мережею. Завдяки компактності та доступній вартості RouterBoard є популярним рішенням для побудови локальних мереж підприємств.

MikroTik CRS (Cloud Router Switch), пристрої цієї серії поєднують функції маршрутизатора та комутатора і призначені для використання у мережах з великою кількістю підключених пристроїв. CRS підтримує високошвидкісні мережеві інтерфейси, VLAN, агрегацію каналів та інші функції керування мережевим трафіком.

Під час вибору конкретного мережевого обладнання для корпоративної мережі необхідно враховувати декілька основних критеріїв.

Першим критерієм є продуктивність пристрою. Мережеве обладнання повинно забезпечувати достатню пропускну здатність для обробки мережевого трафіку без затримок та втрати пакетів.

Другим критерієм є кількість мережевих портів, яка визначає кількість пристроїв або сегментів мережі, що можуть бути підключені до маршрутизатора або комутатора.

Третім критерієм є підтримка VPN-технологій, які дозволяють організовувати захищені канали зв’язку між віддаленими мережами або користувачами. Наявність підтримки таких протоколів, як IPsec, L2TP або OpenVPN, є важливою вимогою для корпоративних мереж.

MikroTik має значну перевагу в вартості обладнання, оскільки пропонує широкий функціонал за відносно доступною ціною. Порівняльну характеристику основних серій обладнання MikroTik наведено в табл. 2.1.

Таблиця 2.1 – Порівняльна характеристика основних серій обладнання MikroTik

Серія пристроїв	Основне призначення	Рівень продуктивності	Кількість портів	Підтримка VPN	Переваги
MikroTik CCR	використання у великих корпоративних мережах, дата-центрах, мережах із високим навантаженням	високий	середня або велика, залежно від моделі	повна підтримка IPsec, L2TP, SSTP, OpenVPN, WireGuard	висока обчислювальна потужність, стабільна робота під великим навантаженням, підтримка складної маршрутизації
MikroTik RB (RouterBoard)	використання у малих та середніх корпоративних мережах	середній	невелика або середня	повна підтримка основних VPN-протоколів	універсальність, доступна ціна, простота впровадження, достатній функціонал для більшості задач
MikroTik CRS	використання у мережах, де важлива комутація та велика кількість підключень	середній	велика	обмежено або як додаткова функція залежно від моделі	велика кількість портів, підтримка VLAN, зручність побудови комутаційного рівня

З урахуванням зазначених критеріїв для реалізації проєктованої корпоративної мережі було обрано маршрутизатор MikroTik серії RB, який працює

під керуванням операційної системи RouterOS та забезпечує реалізацію функцій маршрутизації, захисту мережевого трафіку, створення VPN-з’єднань та керування мережею підприємства.

Таким чином, використання обладнання MikroTik дозволяє створити ефективну, масштабовану та економічно доцільну мережеву інфраструктуру, що відповідає сучасним вимогам до побудови захищених корпоративних мереж.

2.2 Архітектура та проходження трафіку в операційній системі MikroTik RouterOS

У використанні обладнання MikroTik функції маршрутизації трафіку, обробкою пакетів та реалізацією політик безпеки займається операційна система RouterOS, яка забезпечує комплексне керування мережевими сервісами та взаємодією між різними сегментами мережі.

MikroTik RouterOS має модульну архітектуру, що дозволяє реалізовувати широкий спектр мережевих функцій, включаючи маршрутизацію пакетів, фільтрацію трафіку, організацію VPN-з’єднань, трансляцію мережевих адрес (NAT), сегментацію мережі за допомогою VLAN та контроль пропускної здатності каналів. Завдяки такій архітектурі один пристрій може виконувати функції декількох мережевих компонентів одночасно, що спрощує побудову та адміністрування корпоративної мережі [15].

RouterOS є чітко визначена схема обробки мережевих пакетів, яка отримала назву Packet Flow. Ця схема визначає порядок проходження трафіку через різні модулі системи, включаючи правила міжмережевого екрана, механізми NAT, маршрутизацію та інші функції керування мережею. Розуміння процесу обробки пакетів є важливим для правильного налаштування політик безпеки та оптимізації роботи мережі.

Під час надходження мережевого пакета до маршрутизатора RouterOS він проходить декілька етапів обробки. Спочатку пакет потрапляє до мережевого інтерфейсу пристрою, після чого система визначає тип трафіку та напрямок його

подальшої передачі. На цьому етапі здійснюється перевірка правил фільтрації та можливе застосування механізмів маркування пакетів.

Далі пакет передається до модуля Firewall, який виконує аналіз мережевого трафіку відповідно до встановлених правил безпеки. Firewall у RouterOS дозволяє контролювати вхідний, вихідний та транзитний трафік, блокувати підозрілі з’єднання та запобігати несанкціонованому доступу до внутрішніх ресурсів мережі.

Після обробки правил міжмережевого екрана пакет може бути переданий до модуля NAT, якщо для даного типу трафіку передбачено трансляцію мережевих адрес. NAT використовується для перетворення приватних IP-адрес внутрішньої мережі у публічні адреси під час доступу до мережі Інтернет, а також для організації доступу до внутрішніх сервісів із зовнішніх мереж [16].

Наступним етапом є маршрутизація пакета, під час якої RouterOS визначає оптимальний шлях передачі даних до кінцевого вузла. Для цього використовується таблиця маршрутизації, що містить інформацію про доступні мережі та маршрути до них. У разі необхідності пакет може бути переданий до іншого мережевого сегмента або відправлений через зовнішній інтерфейс до мережі Інтернет.

Після визначення маршруту пакет передається на відповідний мережевий інтерфейс, через який він надсилається до наступного мережевого пристрою або безпосередньо до кінцевого отримувача. У разі використання додаткових функцій, таких як VPN або VLAN, пакет може проходити додаткові етапи інкапсуляції або маркування.

На рисунку 2.1 представлено спрощену схему проходження мережевого трафіку через маршрутизатор, що працює під керуванням операційної системи MikroTik RouterOS. Мережевий трафік надходить із зовнішньої мережі Інтернет до маршрутизатора, де проходить через механізми перевірки правил міжмережевого екрана (Firewall).

Після перевірки правил безпеки трафік може бути оброблений модулем трансляції мережевих адрес (NAT), який виконує перетворення IP-адрес внутрішньої мережі для забезпечення доступу до мережі Інтернет. Далі

маршрутизатор визначає маршрут передачі пакета відповідно до таблиці маршрутизації та передає його до відповідного сегмента локальної мережі.

Такий механізм обробки пакетів дозволяє забезпечити ефективне керування мережевим трафіком, реалізувати політики безпеки та контролювати доступ до ресурсів корпоративної мережі.

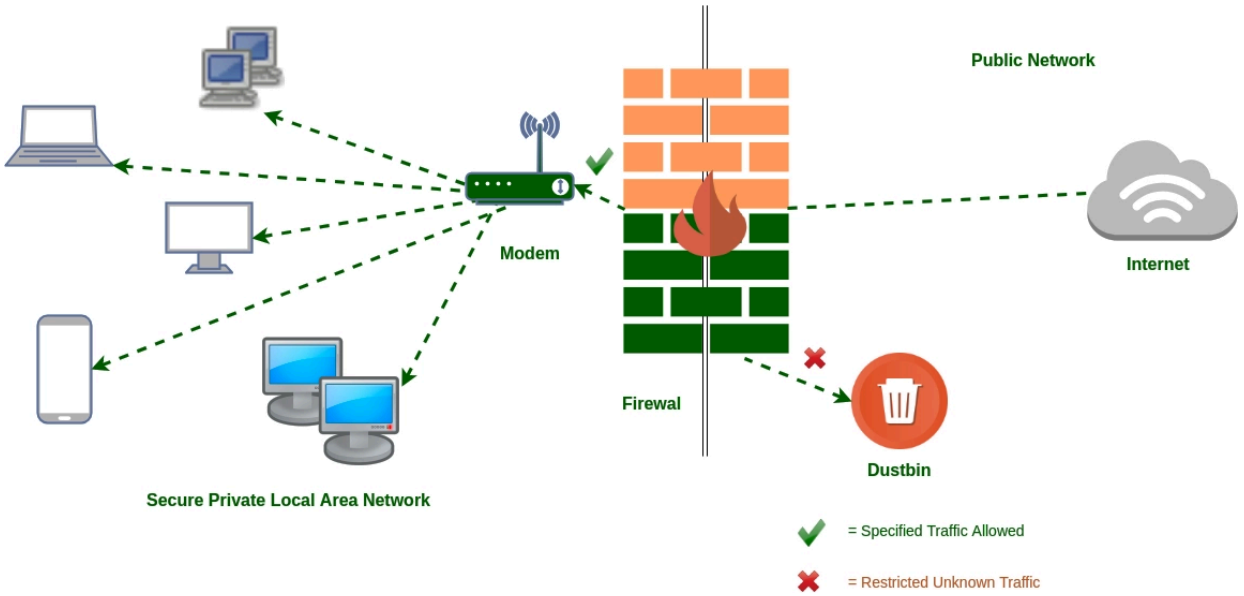


Рис. 2.1 – Спрощена схема проходження мережевого трафіку в MikroTik RouterOS

Архітектура MikroTik RouterOS забезпечує послідовну та ефективну обробку мережевого трафіку, що дозволяє реалізовувати складні політики безпеки, контролювати доступ до мережевих ресурсів та оптимізувати роботу корпоративної мережевої інфраструктури. Розуміння принципів проходження трафіку у RouterOS є необхідним для правильного налаштування мережевих пристроїв та забезпечення стабільної роботи корпоративної мережі.

2.3 Проєктування структури корпоративної мережі

Розроблення корпоративної мережі підприємства зазвичай розпочинається зі створення структурних схем. Такі схеми дають змогу представити мережу як сукупність взаємопов’язаних компонентів або логічних елементів, які на початковому етапі розглядаються на узагальненому рівні [17]. Хоча подальше проєктування передбачає детальнішу специфікацію кожного елемента, саме початкові структурні моделі дозволяють сформувати цілісне уявлення про принципи функціонування мережі та взаємодію її складових.

На рисунку 2.2 подано структурну модель мережі, яка відображає основні елементи мережевої інфраструктури та взаємозв’язки між ними. У цій схемі представлені такі складові:

- головний офіс підприємства;
- віддалені філії, що використовують ті самі канали провайдерського зв’язку, що і центральний офіс;
- окремі філії, які підключаються лише до глобальної мережі Інтернет;
- сегменти захищених мереж IoT, що функціонують через міжмережеві екрани;
- канали зв’язку, які забезпечують взаємодію між усіма компонентами мережевої інфраструктури.

Завдяки такій структурній схемі можна наочно оцінити організацію мережі підприємства, визначити ключові вузли взаємодії та зрозуміти загальні принципи побудови корпоративної мережевої архітектури.

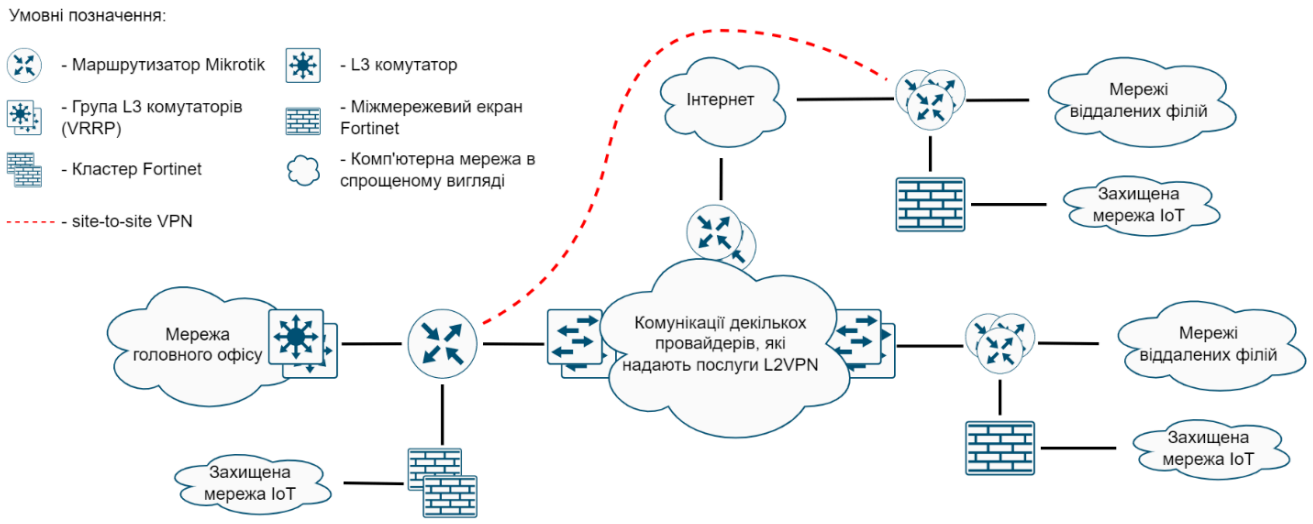


Рис. 2.2 – Структурна схема мережевої архітектури прототипу

На рисунку 2.3 представлено структурну схему захищеної мережевої інфраструктури, у якій основна увага приділяється організації взаємодії між елементами мережі з точки зору міжмережевих екранів. Така схема демонструє принципи побудови захищених каналів зв’язку між різними сегментами корпоративної мережі.

Під час формування захищеної мережі із використанням загальних комунікаційних каналів міжмережеві екрани фактично розглядають мережеву інфраструктуру провайдера як своєрідну «чорну скриньку», яка виконує функцію транспортування зашифрованого мережевого трафіку від одного вузла захисту до іншого. У такій архітектурі основною задачею комунікаційного середовища є забезпечення надійної передачі зашифрованих пакетів між міжмережевими екранами, що формують захищений периметр мережі.

Важливими вимогами до такої інфраструктури є надійність та висока доступність мережевих сервісів. Досягнення цих характеристик забезпечується шляхом резервування критично важливих елементів мережевого обладнання, а також організацією резервних каналів зв’язку між філіями підприємства. Такий підхід дозволяє підтримувати стабільність функціонування мережі навіть у випадку відмови окремих компонентів або каналів передачі даних.

Слід зазначити, що у структурних схемах як приклад розглядаються міжмережеві екрани виробництва Fortinet. Проте детальний розгляд їх конфігурації, так само як і повне налаштування інфраструктури мереж Інтернету речей, виходить за межі даного дослідження. З цієї причини під час створення експериментального прототипу мережі було використано мережеве обладнання MikroTik, яке дозволяє реалізувати необхідні функції маршрутизації, фільтрації трафіку та організації захищених з'єднань.

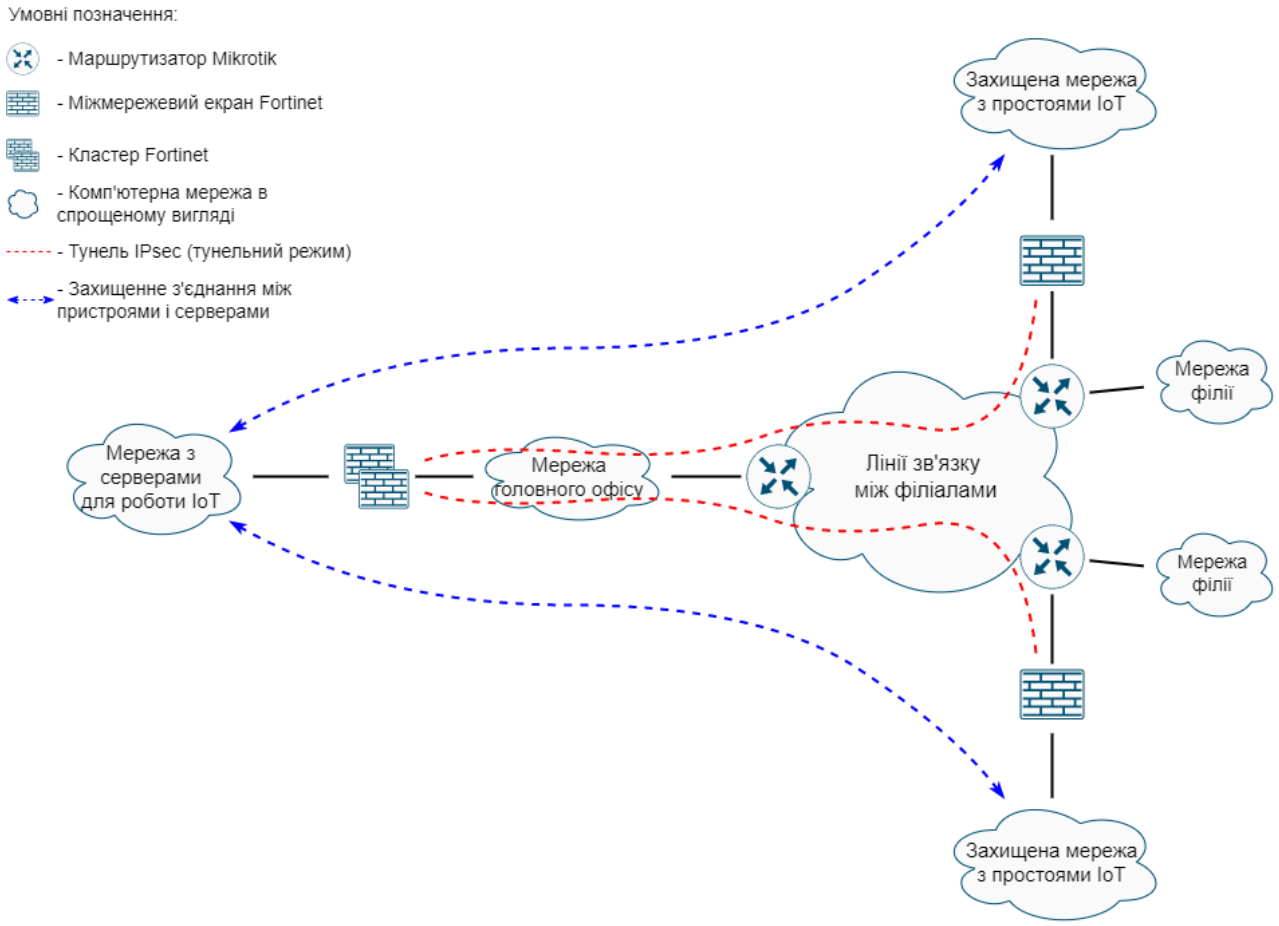


Рис. 2.3 – Структурна модель захищеної мережі, реалізованої на базі загальної мережі

2.4 Розробка плану IP-адресації та логічної топології

У процесі проєктування мережевої інфраструктури підприємства розроблення плану IP-адресації зазвичай виконується паралельно з формуванням

логічної схеми мережі. Однак у межах даної роботи цей процес було розпочато з аналізу спрощеної організаційної структури підприємства та подальшого створення відповідного плану IP-адресації.

Як основу для внутрішньої адресації було обрано приватний діапазон адрес 10.0.0.0/8, який дозволяє створити значну кількість підмереж для різних сегментів корпоративної інфраструктури. Відповідно до структури підприємства та потреб мережі цей адресний простір було поділено на кілька підмереж, кожна з яких призначена для окремих мережевих сегментів або сервісів [18].

Для ілюстрації структури плану адресації розглянемо фрагмент таблиці IP-адрес, що стосується комунікацій із першим провайдером (табл. 2.1). Усі наступні таблиці побудовані за аналогічним принципом. Їх детальний опис наведено у цьому підрозділі, тоді як повні таблиці, з огляду на їх значний обсяг.

Структура таблиці 2.1 включає такі основні поля:

- порядковий номер підмережі;
- назву підмережі та ідентифікацію відповідних хостів, яким призначено IP-адреси;
- перелік IP-адрес;
- маску підмережі, представлену як у скороченому, так і в повному форматі;
- номер VLAN та його назву;
- поле для додаткових приміток або коментарів.

Застосування такої структури таблиць дозволяє систематизувати інформацію про мережеву адресацію та забезпечує зручність подальшого адміністрування мережевої інфраструктури.

Таблиця 2.1 – Частина таблиці, що містить інформацію про провайдерські підключення

ISP1					
№	**Хост**	**IP адреса**	**Маска**	**VLAN**	**Коментар**
1	**2**	**3**	**4**	**5**	**6**
1	**Point-to-Point to ISP1**	100.64.0.0	30	p-to-p-ISP1	З'єднання з ISP1. Через цю підмережу прописаний маршрут до пулу глобальних адрес
	ISP1-GW	100.64.0.1	30	545	
	HQ-R-border	100.64.0.2			
	Broadcast	100.64.0.3	255.255.255.252		
2	**Global pool ISP1**	100.64.1.0	29	-	
			29	-	
	Остання адреса	100.64.1.8	255.255.255.248		
3	**ISP1 VLAN for branch**	10.1.0.0	24	ISP1-district-VLAN	
	HQ-R-border	10.1.0.1	24	544	
	Branch1-R	10.1.0.2			
	Branch2-R	10.1.0.3			
	Резерв	10.1.0.4			
	Broadcast	10.1.0.255	255.255.255.0		

Підприємство має підключення до двох інтернет-провайдерів, кожен з яких надає два адресні простори. Перший призначений для організації з'єднання з провайдерським шлюзом і має розмір /30, а другий використовується підприємством для власних мережевих потреб та має розмір /29.

Крім того, для забезпечення взаємодії між віддаленими філіями підприємства було створено дві окремі підмережі, які використовуються для організації зв'язку за допомогою технології L2VPN.

Перший провайдер надав адресний простір 100.64.0.0/30 для підключення до свого шлюзу, а також 100.64.1.0/29, який використовується для внутрішніх потреб підприємства. Для організації зв'язку між філіями через комунікаційну інфраструктуру цього провайдера використовується підмережа 10.1.0.0/24.

Другий провайдер, у свою чергу, надав простори адрес 100.65.0.0/30 та 100.65.1.0/29, а для забезпечення взаємодії між філіями використовується мережа 10.2.0.0/24.

У мережевій інфраструктурі також передбачено використання loopback-адрес для маршрутизаторів та комутаторів третього рівня, які застосовуються для стабільного встановлення з'єднання з цими пристроями. Окрім цього, визначено адресний простір, що використовується для взаємодії між окремими мережевими пристроями, наприклад між прикордонним маршрутизатором і міжмережевим екраном, а також адресацію, що застосовується всередині VPN-тунелів.

Адресний простір головного офісу підприємства умовно поділено на чотири основні сегменти: ISP, DMZ, LAN та IoT [19].

Сегмент ISP містить адреси, які використовуються для керування мережевим обладнанням, розташованим між прикордонним маршрутизатором і мережами провайдерів.

Сегмент DMZ призначений для організації демілітаризованої зони, у якій розміщено мережу керування та серверний сегмент. У цьому сегменті функціонують серверні ресурси підприємства, зокрема DNS-сервер.

Сегмент LAN містить адресацію для кінцевих пристроїв різних структурних підрозділів підприємства. У межах цього сегмента передбачено мережі для адміністрування мережевого обладнання та серверів, серверну підмережу, мережу IT-відділу, а також окремі мережі для інших департаментів організації.

Сегмент IoT відповідає за захищений мережевий простір, у якому розміщується серверна частина систем Інтернету речей.

Адресація філій підприємства має подібну структуру і складається з двох основних частин: LAN та IoT.

У сегменті LAN визначено адресацію для мережі керування та для мереж різних підрозділів підприємства.

Сегмент IoT призначений для ізольованої та захищеної мережі пристроїв Інтернету речей, у якій розташовані кінцеві IoT-пристрої та інші пов’язані елементи інфраструктури.

3 РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ПРОТОТИПУ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Розгортання прототипу мережі в середовищі EVE-NG

Перед розгортанням прототипу корпоративної мережі необхідно врахувати низку важливих факторів, які пов’язані з особливостями використання віртуальної лабораторії EVE-NG, специфікою функціонування операційної системи RouterOS у середовищі віртуальних машин, а також загальними технічними умовами реалізації проєкту. У зв’язку з цим під час створення прототипу було прийнято певні припущення, спрощення та обмеження, що наведені нижче.

1. Віртуальний маршрутизатор MikroTik CHR має технічні обмеження щодо швидкості роботи мережевих інтерфейсів, яка становить до 1 Мбіт/с. Крім того, дана версія не підтримує реалізацію ACL (Access Control List) на рівні комутаторів, що обмежує можливості моделювання деяких механізмів фільтрації трафіку.

2. Мережі провайдерів, а також глобальна мережа Інтернет, у лабораторному середовищі були змодельовані із застосуванням віртуальних маршрутизаторів MikroTik CHR. При цьому замість реальної глобальної адресації використано спільний адресний простір, який зазвичай застосовується провайдерами для реалізації NAT операторського рівня (Carrier-Grade NAT) [20].

3. У рамках даного прототипу питанням інформаційної безпеки не приділено детального опрацювання. Реалізовано лише базові елементи захисту, зокрема використання міжмережевих екранів та прикордонного маршрутизатора. Повноцінне впровадження механізмів захисту потребує детального врахування

політик безпеки конкретного підприємства та комплексного налаштування відповідних засобів захисту.

4. Підсумкова конфігурація прототипу може відрізнятися від реальної мережевої інфраструктури підприємства. Це пов’язано з тим, що топологія рівня L2 значною мірою визначається фізичною організацією каналів зв’язку, тоді як логічна структура рівня L3 залежить від внутрішньої організаційної структури підприємства. Разом із тим, завдяки модульному принципу побудови мережі та її масштабованості, основні архітектурні підходи і принципи функціонування мережі залишаються незмінними.

3.2 Налаштування L2 та L3 комутаторів

Комутатори MikroTik мають певну особливість у процесі налаштування комутаційних функцій. У випадку, коли конфігурація пристрою відсутня або була видалена, після запуску обладнання всі мережеві інтерфейси функціонують у режимі маршрутизатора, а не комутатора. Тому для реалізації базових можливостей комутації необхідно виконати початкове налаштування мережевої структури.

Зокрема, для активації комутаційного режиму потрібно створити логічний міст (bridge) та додати до нього всі фізичні інтерфейси, які планується використовувати для комутації мережевого трафіку [26].

Для забезпечення коректної роботи VLAN на комутаторах було виконано таку послідовність дій:

1) створено логічний інтерфейс bridge;

```
1 /interface bridge
2 add name=bridge1
```

2) до створеного bridge було додано всі необхідні мережеві інтерфейси. Для магістральних (trunk) портів встановлено параметр frame-types=admit-only-vlan-tagged, що забезпечує передачу виключно тегованих кадрів VLAN. Для портів доступу було застосовано параметр

frame-types=admit-only-untagged-and-priority-tagged, який визначає інтерфейс як access-порт. У цьому випадку порт автоматично прив'язується до відповідного VLAN, номер якого задається через параметр pvid.

```
/interface bridge port
add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged \
    ingress-filtering=yes interface=ether1 pvid=3
add bridge=bridge1 frame-types=admit-only-untagged-and-priority-tagged \
    ingress-filtering=yes interface=ether2 pvid=999
add bridge=bridge1 frame-types=admit-only-vlan-tagged ingress-filtering=yes \
    interface=ether9
add bridge=bridge1 frame-types=admit-only-vlan-tagged ingress-filtering=yes \
    interface=ether10
```

3) магістральні інтерфейси, а також сам bridge (який використовується для VLAN керування), було додано до таблиці bridge vlan у режимі тегованих портів. Для них відповідно визначено ідентифікатори VLAN, що забезпечує передачу тегованого трафіку через магістральні з'єднання та коректну роботу керуючої VLAN [21].

```
/interface bridge vlan
add bridge=bridge1 tagged=ether10,ether9 vlan-ids=3
add bridge=bridge1 tagged=ether10,ether9,bridge1 vlan-ids=256
```

4) для забезпечення роботи механізму VLAN на комутаторі відповідну функціональність було увімкнено безпосередньо на інтерфейсі bridge.

```
/interface bridge
set 0 frame-types=admit-only-vlan-tagged ingress-filtering=yes vlan-filtering=yes
```

Для організації керування комутатором було створено VLAN-інтерфейс, через який здійснюється доступ до пристрою. На цьому інтерфейсі було призначено IP-адресу, після чого налаштовано маршрут за замовчуванням, що забезпечує можливість мережевої взаємодії з іншими сегментами мережі.

```
/interface vlan
add interface=bridge1 name=bridge1.256 vlan-id=256
/ip address
add address=10.4.0.7/24 interface=bridge1.256
/ip route
add distance=1 gateway=10.4.0.254
```

Налаштування функціональності L3 на комутаторах MikroTik ґрунтується на попередньо виконаній коректній конфігурації L2-рівня, зокрема механізмів VLAN.

Після завершення налаштування комутаційної частини було створено низку VLAN-інтерфейсів, які базуються на логічному інтерфейсі bridge. Приклад такої конфігурації наведено нижче.

```
/interface vlan
add comment=Server_Managment interface=bridgeMain name=bridgeMain.2 vlan-id=2
add comment=Servers interface=bridgeMain name=bridgeMain.3 vlan-id=3
add comment=Dep-1 interface=bridgeMain name=bridgeMain.4 vlan-id=4
add comment=Dep-2 interface=bridgeMain name=bridgeMain.5 vlan-id=5
add comment=Dep-3 interface=bridgeMain name=bridgeMain.6 vlan-id=6
add comment=Network_Managment interface=bridgeMain name=bridgeMain.256 vlan-id=256
add comment=IT-dep interface=bridgeMain name=bridgeMain.257 vlan-id=257
add comment=To_HQ-L3SW-Core2 interface=bridgeMain name=bridgeMain.258 vlan-id=258
```

Після створення VLAN-інтерфейсів наступним етапом є призначення їм IP-адрес, що забезпечує можливість виконання функцій маршрутизації між підмережами. Як приклад, нижче наведено конфігурацію адресації, яка була виконана на комутаторі HQ-L3SW-Core1.

```
/ip address
add address=10.255.1.2/30 comment=To_HQ-R-Border interface=ether10
add address=10.4.2.1/24 comment=Server_Managment interface=bridgeMain.2
add address=10.4.3.1/24 comment=Servers interface=bridgeMain.3
add address=10.4.4.1/24 comment=Dep-1 interface=bridgeMain.4
add address=10.4.5.1/24 comment=Dep-2 interface=bridgeMain.5
add address=10.4.6.1/24 comment=Dep-3 interface=bridgeMain.6
add address=10.4.0.1/24 comment=Network_Managment interface=bridgeMain.256
add address=10.4.1.1/24 comment=IT-dep interface=bridgeMain.257
add address=10.255.0.254 interface=Bridge_loopback
add address=10.255.1.9/30 comment=To_HQ-L3SW-Core2 interface=bridgeMain.258
```

Для забезпечення резервування мережевого з’єднання на комутаторах HQ-L3SW-Core1 та HQ-L3SW-Core2 було налаштовано протокол VRRP [27]. У процесі конфігурації створеним віртуальним інтерфейсам було призначено відповідні IP-адреси, а також визначено значення пріоритетів для протоколів VRRP і RSTP. Таке налаштування дозволяє у штатному режимі спрямовувати мережевий трафік оптимальним маршрутом через комутатор HQ-L3SW-Core1, тоді як другий комутатор виконує роль резервного вузла.

```
/interface vrrp
add name=VRRP_bridgeMain.2 interface=bridgeMain.2
add name=VRRP_bridgeMain.3 interface=bridgeMain.3
add name=VRRP_bridgeMain.4 interface=bridgeMain.4
add name=VRRP_bridgeMain.5 interface=bridgeMain.5
add name=VRRP_bridgeMain.6 interface=bridgeMain.6
add name=VRRP_bridgeMain.256 interface=bridgeMain.256
add name=VRRP_bridgeMain.257 interface=bridgeMain.257
```

Для реалізації динамічної маршрутизації за протоколом OSPF як на L3-комутаторах, так і на маршрутизаторах було виконано конфігурування відповідних параметрів і елементів протоколу. Зокрема, було налаштовано основні компоненти, необхідні для коректної роботи протоколу маршрутизації.

1) задано ідентифікатор процесу OSPF, який використовується для ідентифікації та функціонування відповідного екземпляра протоколу маршрутизації.

```
/routing ospf instance
set [ find default=yes ] router-id=10.255.0.254
```

2) інтерфейси було налаштовано таким чином, що ті з них, які підключені до мереж кінцевих користувачів, працюють у режимі passive, тоді як інтерфейси, що з’єднують мережеве обладнання між собою, сконфігуровано для взаємодії з протоколом BFD, що забезпечує швидке виявлення відмов з’єднання.

```
/routing ospf interface
add passive=yes
add interface=ether10 use-bfd=yes
add interface=bridgeMain.258 use-bfd=yes
```

3) визначено адресні діапазони, на основі яких протокол OSPF автоматично визначає інтерфейси, на яких необхідно активувати його роботу.

```
/routing ospf network
add area=backbone network=10.255.1.0/30
add area=backbone network=10.4.2.0/24
add area=backbone network=10.4.3.0/24
add area=backbone network=10.4.4.0/24
add area=backbone network=10.4.5.0/24
add area=backbone network=10.4.6.0/24
add area=backbone network=10.4.0.0/24
add area=backbone network=10.4.1.0/24
add area=backbone network=10.255.0.254/32
add area=backbone network=10.255.1.8/30
```

3.3 Налаштування маршрутизаторів та прикордонного вузла

Налаштування маршрутизаторів, розташованих у філіях підприємства, передбачало створення VLAN-інтерфейсів, а також конфігурацію IP-адресації як для внутрішніх інтерфейсів локальної мережі, так і для інтерфейсів, що забезпечують підключення до мереж інтернет-провайдерів. Крім цього, було реалізовано підтримку динамічної маршрутизації за протоколом OSPF. Усі зазначені конфігураційні операції виконувались із дотриманням підходів і рекомендацій, що були розглянуті у попередніх розділах роботи.

З метою автоматизації процесу отримання мережевих параметрів клієнтськими пристроями в головному офісі було розгорнуто DHCP-сервер. Для мережевого обладнання, через яке здійснюється підключення кінцевих користувачів, було налаштовано механізм DHCP Relay, що забезпечує передачу DHCP-запитів від клієнтів до центрального DHCP-сервера. Конфігурація цього механізму виконана наступним чином [22].

```
/ip dhcp-relay
add dhcp-server=10.4.3.10 disabled=no interface=ether1.2 local-address=\
    10.7.2.1 name=Dep1
add dhcp-server=10.4.3.10 disabled=no interface=ether1.3 local-address=\
    10.7.3.1 name=Dep2
```

Для організації з’єднання з головним офісом через мережу Інтернет було реалізовано використання GRE-тунелів у поєднанні з протоколом IPsec. Конфігурація включала виконання таких дій:

- створено GRE-тунелі до головного офісу та призначено відповідну IP-адресацію на цих тунельних інтерфейсах;

```
/interface gre
add allow-fast-path=no local-address=100.66.0.4 mtu=1450 name=GRE_ISP1_HQ \
    remote-address=100.64.0.2
add allow-fast-path=no local-address=100.66.0.4 mtu=1450 name=GRE_ISP2_HQ \
    remote-address=100.65.0.2
/ip address
add address=10.255.2.2/30 interface=GRE_ISP1_HQ network=10.255.2.0
add address=10.255.2.6/30 interface=GRE_ISP2_HQ network=10.255.2.4
```

- виконано конфігурацію першої фази протоколу IPsec (IKE Phase 1), що забезпечує встановлення захищеного каналу для подальшого обміну криптографічними параметрами між вузлами.

```
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 hash-algorithm=sha512 name=\
    PH1-GRE
```

- виконано конфігурацію другої фази протоколу IPsec (IKE Phase 2), у межах якої визначено параметри захисту та шифрування трафіку, що передається через встановлений тунель.

```
/ip ipsec proposal
add auth-algorithms=sha512 enc-algorithms=aes-256-cbc name=PH2-GRE pfs-group=\
   modp2048
```

- виконано налаштування IPsec peer, а також визначено параметри взаємної автентифікації між вузлами для встановлення захищеного з’єднання.

```
/ip ipsec peer
add address=100.65.0.2/32 exchange-mode=ike2 local-address=100.66.0.4 name=\
    ISP2_HQ profile=PH1-GRE
add address=100.64.0.2/32 exchange-mode=ike2 local-address=100.66.0.4 name=\
    ISP1_HQ profile=PH1-GRE
/ip ipsec identity
add peer=ISP1_HQ secret=Very_Strong_Key
add peer=ISP2_HQ secret=Very_Strong_Key
```

- сформовано та налаштовано політики IPsec, які визначають правила застосування механізмів шифрування і захисту для мережевого трафіку.

```
/ip ipsec policy
add dst-address=100.64.0.2/32 peer=ISP1_HQ proposal=PH2-GRE protocol=gre \
    src-address=100.66.0.4/32
add dst-address=100.65.0.2/32 peer=ISP2_HQ proposal=PH2-GRE protocol=gre \
    src-address=100.66.0.4/32
```

3.4 Реалізація міжмережевого екранування та VPN-з’єднань

Налаштування IP-адресації, а також конфігурація GRE/IPsec-тунелів і протоколу OSPF виконувались за аналогічними принципами, що були описані у попередніх підрозділах.

На прикордонному маршрутизаторі було реалізовано функціональність міжмережевого екрана, який здійснює фільтрацію трафіку, що надходить з боку мережі провайдера. Основним завданням цього механізму є обмеження небажаних підключень із зовнішньої мережі та забезпечення контрольованого доступу до ресурсів корпоративної інфраструктури.

Зокрема, налаштовані правила фільтрації дозволяють:

- проходження відповідного (зворотного) трафіку для вже встановлених з’єднань;
- встановлення з’єднань із використанням протоколу IPsec;
- обробку службових повідомлень ICMP;
- передачу трафіку, який надходить після дешифрування IPsec-з’єднання.

Крім цього, було реалізовано фільтрацію транзитного трафіку, яка дозволяє проходження лише тих пакетів, що є відповіддю на з’єднання, ініційовані з внутрішньої мережі підприємства. Такий підхід підвищує рівень захищеності мережі та запобігає небажаним підключенням із зовнішнього середовища.

```
/ip firewall filter
add action=accept chain=input comment=IN_accept_established connection-state=\
    established
add action=accept chain=input comment=IN_accept_related connection-state=\
    related
add action=accept chain=input comment=IN_accept_untracked connection-state=\
    untracked
add action=jump chain=input comment=Jump_to_IN_ISP in-interface-list=ISP \
    jump-target=IN_ISP
add action=accept chain=forward comment=\
    "FWD_accept_established related untracked" connection-state=\
    established,related,untracked
add action=accept chain=forward comment="FWD_ISP_accept dst-nat" \
    connection-nat-state=dstnat in-interface-list=ISP
add action=drop chain=forward in-interface-list=ISP
add action=accept chain=IN_ISP comment=\
    "IN_ISP_accept_IPsec encrypted traffic" ipsec-policy=in,ipsec
add action=accept chain=IN_ISP comment=IN_ISP_accept_ICMP protocol=icmp
add action=accept chain=IN_ISP comment="IN_ISP_accept_IPsec ESP" protocol=\
    ipsec-esp
add action=accept chain=IN_ISP comment="IN_ISP_accept_IPsec IKE" dst-port=500 \
    protocol=udp
add action=accept chain=IN_ISP comment="IN_ISP_accept_IPsec NAT-T or IKEv2" \
    dst-port=4500 protocol=udp
add action=drop chain=IN_ISP comment=IN_ISP_drop_all
```

З метою спрощення адміністрування та налаштування Firewall було сформовано список IP-адрес, які не належать до глобального адресного простору та не можуть використовуватися як публічні адреси. Це дозволяє ефективніше застосовувати правила фільтрації та спростити подальшу конфігурацію міжмережевого екрана.

```
/ip firewall address-list
add address=0.0.0.0/8 comment="\"This\" Network" list=BOGONS
add address=10.0.0.0/8 comment="Private-Use Networks" list=BOGONS
add address=100.64.0.0/10 comment="Shared Address Space. RFC 6598" list=\
    BOGONS
add address=127.0.0.0/8 comment=Loopback list=BOGONS
add address=169.254.0.0/16 comment="Link Local" list=BOGONS
add address=172.16.0.0/12 comment="Private-Use Networks" list=BOGONS
add address=192.0.0.0/24 comment="IETF Protocol Assignments" list=BOGONS
add address=192.0.2.0/24 comment=TEST-NET-1 list=BOGONS
add address=192.168.0.0/16 comment="Private-Use Networks" list=BOGONS
add address=198.18.0.0/15 comment=\
    "Network Interconnect Device Benchmark Testing" list=BOGONS
add address=198.51.100.0/24 comment=TEST-NET-2 list=BOGONS
add address=203.0.113.0/24 comment=TEST-NET-3 list=BOGONS
add address=224.0.0.0/4 comment=Multicast list=BOGONS
add address=192.88.99.0/24 comment="6to4 Relay Anycast" list=BOGONS
add address=240.0.0.0/4 comment="Reserved for Future Use" list=BOGONS
add address=255.255.255.255 comment="Limited Broadcast" list=BOGONS
```

Для реалізації політики маршрутизації на основі правил (Policy-Based Routing, PBR) необхідно виконати налаштування кількох параметрів, зокрема організувати маркування мережевого трафіку та визначити окремі маршрути для кожного інтернет-провайдера. Початковим етапом стало впровадження механізму маркування пакетів, що було реалізовано відповідно до таких конфігурацій:

- створено правила, спрямовані на запобігання виникненню петель маршрутизації, що забезпечує коректну обробку трафіку під час застосування політики маршрутизації.

```
/ip firewall mangle
add action=accept chain=prerouting comment="Loop prevention for ISP1" \
    dst-address=100.64.0.0/30 in-interface-list=!ISP
add action=accept chain=prerouting comment="Loop prevention for ISP2" \
    dst-address=100.65.0.0/30 in-interface-list=!ISP
```

- виконано налаштування маркування вхідних з'єднань, що дозволяє ідентифікувати трафік під час його обробки та забезпечити коректне застосування політики маршрутизації.

```
add action=mark-connection chain=prerouting comment="Connmark in from ISP1" \
    connection-mark=no-mark in-interface=ether1.545 new-connection-mark=\
    conn_isp1 passthrough=no
add action=mark-connection chain=prerouting comment="Connmark in from ISP2" \
    connection-mark=no-mark in-interface=ether1.453 new-connection-mark=\
    conn_isp2 passthrough=no
```

- виконано маркування маршрутів для пакетів, що належать до з'єднань із попередньо встановленою міткою, що дозволяє застосовувати відповідну політику маршрутизації для такого трафіку.

```
add action=mark-routing chain=prerouting comment=\
    "Routemark transit out via ISP1" connection-mark=conn_isp1 \
    dst-address-type=!local in-interface-list=!ISP new-routing-mark=to_isp1 \
    passthrough=no
add action=mark-routing chain=prerouting comment=\
    "Routemark transit out via ISP2" connection-mark=conn_isp2 \
    dst-address-type=!local in-interface-list=!ISP new-routing-mark=to_isp2 \
    passthrough=no
add action=mark-routing chain=output comment="Routemark local out via ISP1" \
    connection-mark=conn_isp1 dst-address-type=!local new-routing-mark=\
    to_isp1 passthrough=no
add action=mark-routing chain=output comment="Routemark local out via ISP2" \
    connection-mark=conn_isp2 dst-address-type=!local new-routing-mark=\
    to_isp2 passthrough=no
-   налаштовано балансування вихідного трафіку з допомогою PCC;
add action=mark-routing chain=prerouting comment="PCC routermark via ISP1" \
    connection-mark=no-mark dst-address-list=!BOGONS dst-address-type=!local \
    in-interface-list=!ISP new-routing-mark=to_isp1 passthrough=no \
    per-connection-classifier=src-address:2/0
add action=mark-routing chain=prerouting comment="PCC routermark via ISP2" \
    connection-mark=no-mark dst-address-list=!BOGONS dst-address-type=!local \
    in-interface-list=!ISP new-routing-mark=to_isp2 passthrough=no \
    per-connection-classifier=src-address:2/1
```

Для реалізації окремих таблиць маршрутизації для кожного з інтернет-провайдерів було виконано відповідні команди конфігурації, що забезпечують використання різних маршрутів залежно від обраної політики маршрутизації.

```
/ip route
add comment="Marked ISP1 via ISP1 Main" distance=1 gateway=8.8.8.8 \
    routing-mark=to_isp1 target-scope=11
add comment="Marked ISP1 via ISP2 (Backup1)" distance=2 gateway=8.8.4.4 \
    routing-mark=to_isp1 target-scope=11
add comment="Marked ISP2 via ISP2 Main" distance=1 gateway=8.8.4.4 \
    routing-mark=to_isp2 target-scope=11
add comment="Marked ISP2 via ISP1 (Backup1)" distance=2 gateway=8.8.8.8 \
    routing-mark=to_isp2 target-scope=11
add check-gateway=ping comment="Unmarked via ISP1" distance=1 gateway=8.8.8.8 \
    target-scope=11
add check-gateway=ping comment="Unmarked via ISP2" distance=2 gateway=8.8.4.4 \
    target-scope=11
add comment="Emergency route" distance=254 gateway=Bridge_loopback
add check-gateway=ping comment="For recursion via ISP2" distance=1 \
    dst-address=8.8.4.4/32 gateway=100.65.0.1 scope=11
add check-gateway=ping comment="For recursion via ISP1" distance=1 \
    dst-address=8.8.8.8/32 gateway=100.64.0.1 scope=11
/ip route rule
add comment="From ISP1 IP to Inet" src-address=100.64.0.2/32 table=to_isp1
add comment="From ISP2 IP to Inet" src-address=100.65.0.2/32 table=to_isp2
```

На міжмережевих екранах було виконано налаштування IP-адресації, визначено маршрути за замовчуванням, а також реалізовано роботу протоколу

IPsec, який використовується для встановлення захищених з'єднань між сегментами мережі у філіях підприємства. Крім того, було налаштовано Firewall, що забезпечує обмеження доступу до захищеного мережевого сегмента та контролює проходження трафіку.

Конфігурація адресації та маршрутів на міжмережевому екрані головного офісу була виконана наступним чином:

```
/ip address
add address=10.255.1.14/30 comment=to_HQ-R-border interface=ether1
add address=192.168.0.1/24 comment=IoT-servers interface=ether2
/ip route
add gateway=10.255.1.13@main
```

Для організації захищеного з'єднання між міжмережевими екранами було реалізовано використання протоколу IPsec. Конфігурація включала виконання таких кроків:

- виконано налаштування першої фази IPsec (IKE Phase 1), яка забезпечує встановлення захищеного каналу для подальшого узгодження параметрів шифрування між вузлами.

```
/ip ipsec profile
add dh-group=modp2048 enc-algorithm=aes-256 hash-algorithm=sha512 name=\
    PH1-FW_IoT
```

- створено та налаштовано IPsec peer для кожної з віддалених філій, що забезпечує встановлення захищеного з'єднання між міжмережевими екранами.

```
/ip ipsec peer
add add=10.255.1.18/32 exchange-mode=ike2 name=to_Branch1-FW-IoT profile=PH1-FW_IoT
add add=10.255.1.22/32 exchange-mode=ike2 name=to_Branch2-FW-IoT profile=PH1-FW_IoT
add add=10.255.1.26/32 exchange-mode=ike2 name=to_Branch3-FW-IoT profile=PH1-FW_IoT
```

- виконано налаштування другої фази протоколу IPsec, у межах якої визначено параметри шифрування та правила захисту трафіку, що передається через встановлене VPN-з'єднання.

```
/ip ipsec proposal
add auth-algorithms=sha512 enc-algorithms=aes-256-cbc name=PH2-FW_IoT pfs-group=\
    modp2048
```

- визначено та налаштовано параметри автентифікації, що використовуються для підтвердження справжності віддалених філій під час встановлення захищеного з'єднання.

```
/ip ipsec identity
add peer=to_Branch1-FW-IoT secret=Very_Strong_Key
add peer=to_Branch2-FW-IoT secret=Very_Strong_Key
add peer=to_Branch3-FW-IoT secret=Very_Strong_Key
```

- сформовано окремі політики IPsec для кожної філії, що визначають правила шифрування та обробки трафіку в межах відповідних захищених з'єднань.

```
/ip ipsec policy
add dst-address=192.168.1.0/24 peer=to_Branch1-FW-IoT proposal=PH2-FW_IoT protocol=all \
    src-address=192.168.0.0/24 tunnel=yes
add dst-address=192.168.2.0/24 peer=to_Branch2-FW-IoT proposal=PH2-FW_IoT protocol=all \
    src-address=192.168.0.0/24 tunnel=yes
add dst-address=192.168.3.0/24 peer=to_Branch3-FW-IoT proposal=PH2-FW_IoT protocol=all \
    src-address=192.168.0.0/24 tunnel=yes
```

Для забезпечення захисту мережевих сегментів, розташованих за міжмережевим екраном, а також для підвищення рівня безпеки самого пристрою було виконано налаштування Firewall.

З метою захисту безпосередньо міжмережевого екрана було обмежено всі вхідні з'єднання, за винятком тих, які необхідні для коректної роботи протоколу IPsec. Крім того, було дозволено обробку та передачу трафіку, що надходить після дешифрування IPsec-з'єднань.

Для захисту внутрішніх мереж, які знаходяться за міжмережевим екраном, реалізовано правила фільтрації, що блокують будь-який трафік, окрім того, який відповідає визначеним політикам IPsec. Такий підхід дозволяє забезпечити передачу даних лише через встановлені захищені канали зв'язку [23].

Варто зазначити, що налаштовані правила безпеки є уніфікованими для всіх міжмережевих екранів у мережевій інфраструктурі підприємства. Приклад відповідної конфігурації наведено нижче.

```
/ip firewall filter
add action=accept chain=input comment=IN_accept_established connection-state=\
    established
add action=accept chain=input comment=IN_accept_related connection-state=\
    related
add action=accept chain=input comment=IN_accept_untracked connection-state=\
    untracked
add action=jump chain=input comment=Jump_to_IN_WAN in-interface-list=WAN \
    jump-target=IN_WAN
add action=accept chain=IN_WAN comment="IN_ISP_accept_IPsec encrypted traffic" \
    ipsec-policy=in,ipsec
add action=accept chain=IN_WAN comment=IN_WAN_accept_ICMP protocol=icmp
add action=accept chain=IN_WAN comment="IN_WAN_accept_IPsec ESP" protocol=\
    ipsec-esp
add action=accept chain=IN_WAN comment="IN_WAN_accept_IPsec IKE" dst-port=500 \
    protocol=udp
add action=accept chain=IN_WAN comment="IN_WAN_accept_IPsec NAT-T or IKEv2" \
    dst-port=4500 protocol=udp
add action=drop chain=IN_WAN comment=IN_WAN_drop_all
add action=accept chain=forward comment=\
    "FWD_accept_established related untracked" connection-state=\
    established,related,untracked
add action=accept chain=forward comment="FWD_accept_encrypted IPsec out" \
    connection-state="" ipsec-policy=out,ipsec
add action=accept chain=forward comment="FWD_accept_encrypted IPsec in" \
    connection-state="" ipsec-policy=in,ipsec
add action=drop chain=forward comment="FWD_drop_ all from WAN" \
    in-interface-list=WAN
add action=drop chain=forward comment="FWD_drop_ all from ether2 to WAN" \
    in-interface=ether2 out-interface-list=WAN
```

3.5 Перевірка працездатності та надійності мережі

Для перевірки працездатності мережевої інфраструктури було проведено тестування механізму резервування каналу доступу до мережі Інтернет, реалізованого в прототипі. Перевірка виконувалася шляхом одночасного запуску команди ping на двох клієнтських пристроях, які здійснювали вихід до Інтернету через різних провайдерів [25].

На рисунку 3.1 відображено реакцію мережі у випадку відмови другого інтернет-провайдера. Під час переключення на резервний канал зв’язку перший клієнтський комп’ютер тимчасово втратив з’єднання та не отримав 16 відповідей на ICMP-запити, що відповідає приблизно 16 секундам переривання зв’язку до моменту відновлення стабільного маршруту.

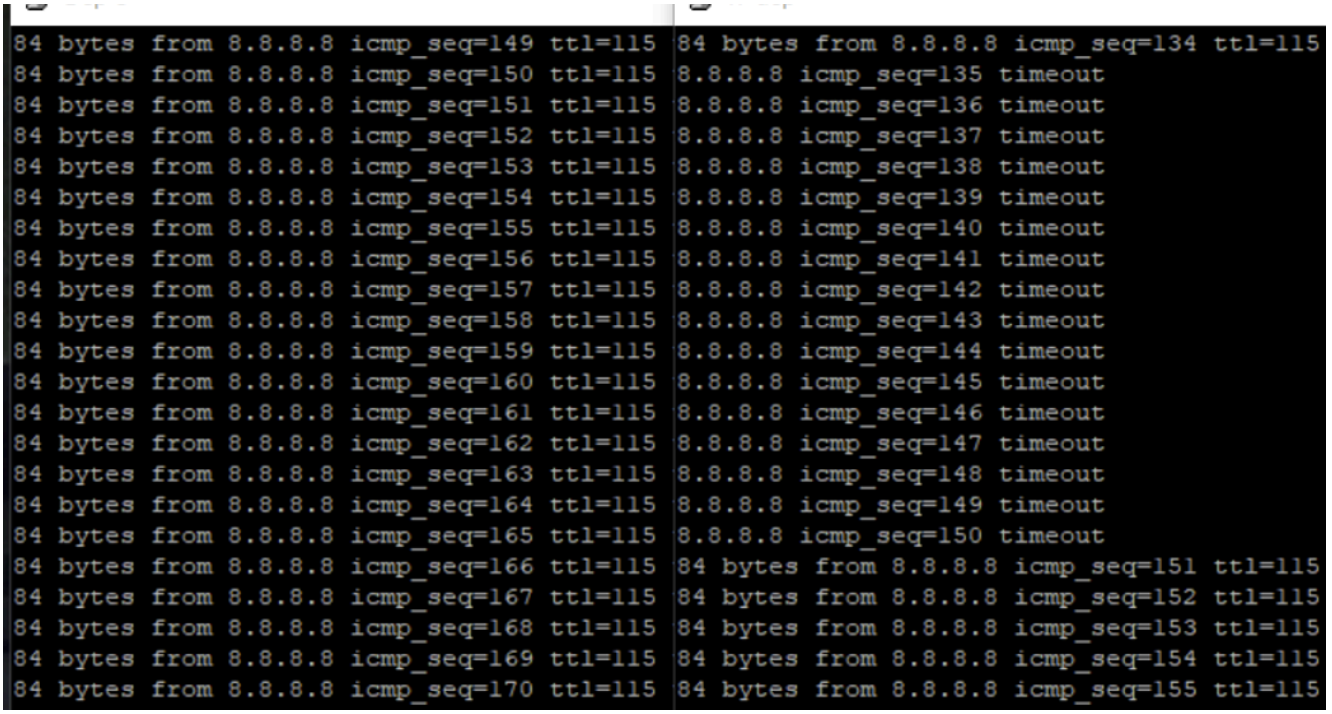


Рис. 3.1 – Демонстрація перемикання на резервний канал доступу до Інтернету

Наступним етапом було проведено тестування надійності роботи мережевої архітектури рівня ядра та розповсюдження, розгорнутої в головному офісі підприємства. Для цього на двох клієнтських комп’ютерах одночасно було виконано команду ping, а в якості цільового вузла було обрано локальний DNS-сервер.

Під час моделювання відмови першого L3-комутатора (рис. 3.2) спостерігалося тимчасове переривання зв’язку: було втрачено три відповіді на ICMP-запити, що відповідає приблизно чотирьом секундам до повного відновлення передачі даних.

На рисунку 3.3 продемонстровано реакцію мережі на відмову одного з каналів зв’язку між рівнями ядра/розповсюдження та доступу. У цьому випадку час відновлення зв’язку склав близько трьох секунд, після чого мережевий трафік автоматично було перенаправлено альтернативним шляхом.

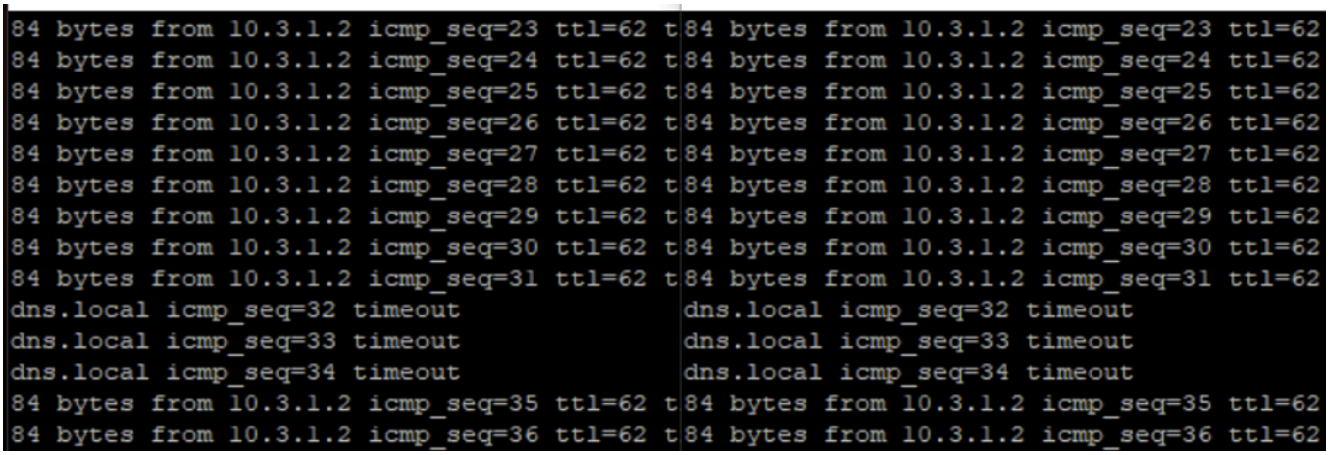


Рис. 3.2 – Результати тестування мережі при відмові L3-комутатора

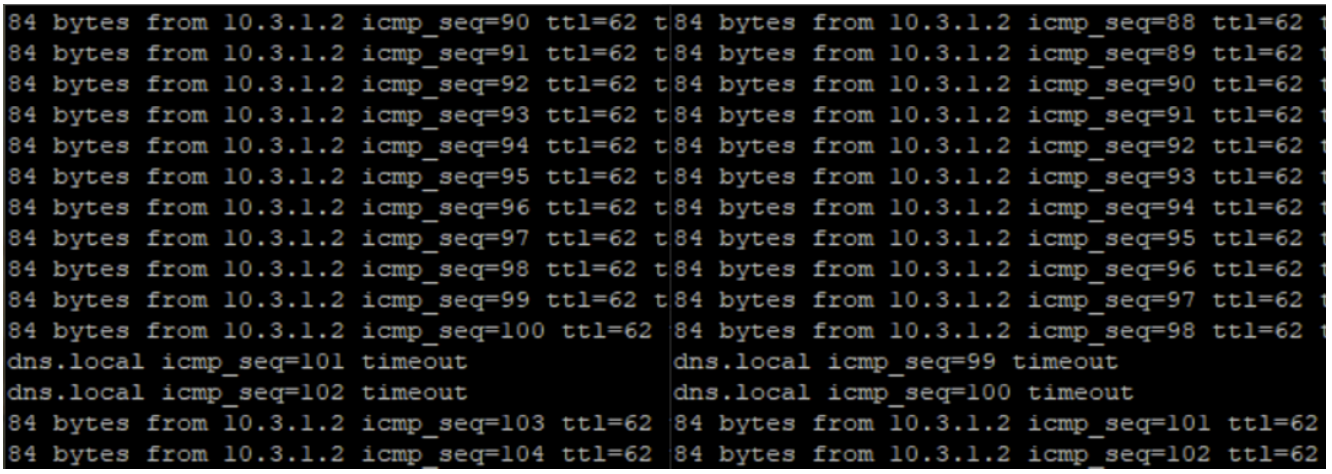


Рис. 3.3 – Тестування мережі при відмові каналу між комутаторами рівнів L3 та L2

Після завершення перевірки надійності функціонування прототипу в межах головного офісу було проведено додаткове тестування стійкості зв’язку між філією підприємства та центральним офісом.

На рисунку 3.4 представлено реакцію мережевої інфраструктури на відмову другого інтернет-провайдера, який забезпечував з’єднання між головним офісом та третьою філією. У процесі переключення на резервний канал було втрачено два ICMP-запити, що свідчить про короткочасне переривання зв’язку. Таким чином, час відновлення мережевого з’єднання склав приблизно дві секунди.

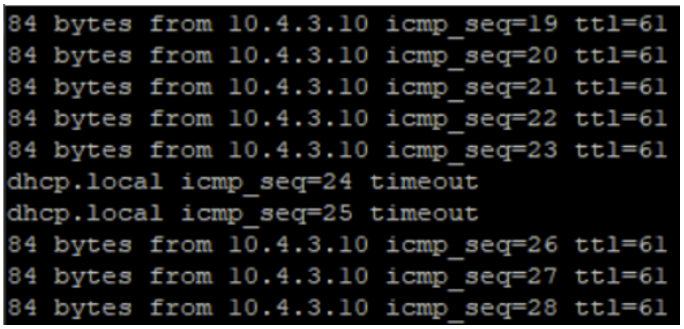


Рис. 3.4 – Перевірка роботи мережі у випадку відмови з’єднання між третьою філією та головним офісом

3.6 Аналіз рівня захищеності корпоративного сегменту

З метою перевірки захищеності мережевих комунікацій між міжмережевими екранами було виконано тестування шляхом встановлення з’єднання між сервером та пристроєм IoT, а також аналізу мережевого трафіку, перехопленого на різних ділянках мережі.

Захоплення пакетів здійснювалося у кількох контрольних точках мережевої інфраструктури:

- перед входом трафіку до міжмережевого екрана, розташованого у головному офісі (рис. 3.5);
- після виконання шифрування та виходу трафіку з міжмережевого екрана головного офісу (рис. 3.6);
- перед надходженням зашифрованого трафіку до міжмережевого екрана, встановленого у першій філії (рис. 3.7);
- після виконання процедури дешифрування та виходу трафіку з міжмережевого екрана першої філії (рис. 3.8).

Аналіз отриманих даних показав, що протокол ICMP, який використовується утилітою ping, передається між кінцевими мережевими пристроями у відкритому вигляді. Водночас трафік, що передається між міжмережевими екранами, проходить через канал уже у зашифрованому вигляді, що підтверджує коректну роботу механізмів захисту [26].

Для додаткової перевірки того, що трафік, представлений на рис. 3.6 та рис. 3.7, дійсно належить до з'єднання між пристроями HQ-FW-IoT та Branch1-FW-IoT, було визначено значення SPI (Security Parameter Index) безпосередньо на міжмережевому екрані (рис. 3.9). Після цього отримані значення було порівняно з відповідними параметрами у перехопленому трафіку. Значення 27212ffg та 3beece81 повністю співпадають у обох випадках, що підтверджує належність зафіксованого трафіку до відповідного IPsec-з'єднання.

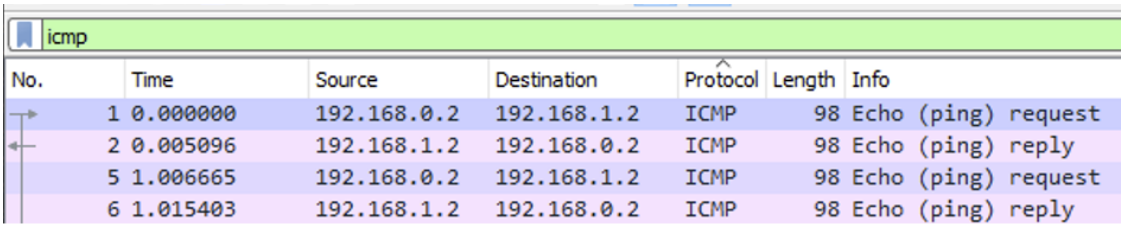


Рис. 3.5 – Мережевий трафік перед обробкою міжмережевим екраном HQ-FW-IoT

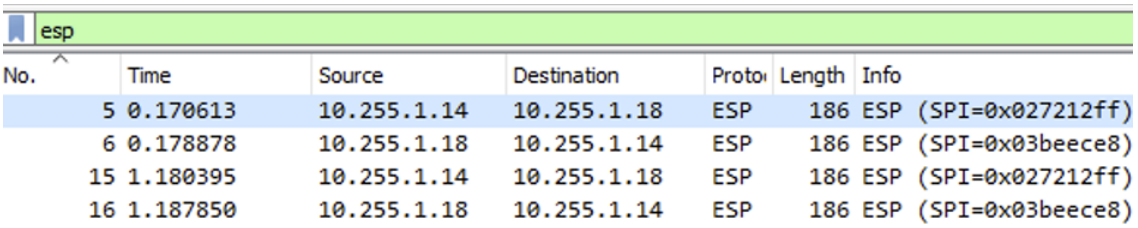


Рис. 3.6 – Мережевий трафік після обробки міжмережевим екраном HQ-FW-IoT

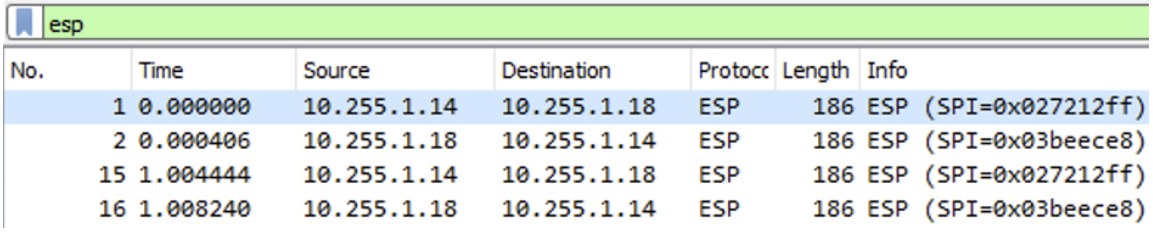


Рис. 3.7 – Мережевий трафік перед надходженням до міжмережевого екрана Branch1-FW-IoT

icmp

No.	Time	Source	Destination	Protoco	Length	Info
1	0.000000	192.168.0.2	192.168.1.2	ICMP	98	Echo (ping) request
2	0.000059	192.168.1.2	192.168.0.2	ICMP	98	Echo (ping) reply
5	1.005295	192.168.0.2	192.168.1.2	ICMP	98	Echo (ping) request
6	1.005388	192.168.1.2	192.168.0.2	ICMP	98	Echo (ping) reply

Рис. 3.8 – Мережевий трафік після обробки міжмережевим екраном Branch1-FW-IoT

IPsec

Policies | Proposals | Groups | Peers | Identities | Profiles | Active Peers | Mo

Flush

	SPI	Src. Address	Dst. Address	Auth. ...	Encr. A...	Encr. ...
E	27212ff	10.255.1.14	10.255.1.18	sha512	aes cbc	256
E	3beece8	10.255.1.18	10.255.1.14	sha512	aes cbc	256

Рис. 3.9 – Перелік активних IPsec-з’єднань на міжмережевому екрані

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було досліджено сучасні підходи до побудови захищених корпоративних комп'ютерних мереж та розроблено прототип мережевої інфраструктури на базі технологій MikroTik RouterOS.

У першому розділі роботи було проведено аналіз теоретичних основ побудови корпоративних мереж. Розглянуто сучасні архітектурні підходи до організації мережевої інфраструктури підприємств, зокрема клієнт-серверну, трирівневу та кампусну архітектури. Проаналізовано роль систем виявлення та запобігання вторгненням (IDS/IPS) у забезпеченні мережевої безпеки. Також досліджено основні технології захисту мережевої взаємодії, зокрема VPN-з'єднання, протоколи GRE та IPsec, які забезпечують конфіденційність і цілісність передавання даних у корпоративних мережах. Окрему увагу приділено аналізу мережевого обладнання та можливостей операційної системи MikroTik RouterOS у задачах побудови захищених мереж.

У другому розділі було виконано проєктування корпоративної мережі на базі обладнання MikroTik. Проведено вибір та обґрунтування мережевого обладнання з урахуванням критеріїв продуктивності, масштабованості, вартості та підтримки сучасних мережевих технологій. Досліджено архітектуру операційної системи MikroTik RouterOS та принципи обробки мережевого трафіку в межах механізму Packet Flow. Розроблено логічну структуру корпоративної мережі, визначено основні сегменти інфраструктури, а також сформовано план IP-адресації та принципи взаємодії між мережевими вузлами.

У третьому розділі було реалізовано прототип захищеної корпоративної мережі у віртуальному середовищі EVE-NG. Виконано налаштування мережевих пристроїв, реалізовано маршрутизацію трафіку між сегментами мережі, впроваджено механізми міжмережевого екранування та організовано захищені VPN-з'єднання між вузлами мережі. Проведено тестування працездатності мережевої інфраструктури, що дозволило перевірити коректність функціонування

мережевих сервісів, стабільність передавання даних та ефективність застосованих механізмів захисту.

Результати проведеного дослідження підтвердили, що використання обладнання MikroTik та операційної системи RouterOS дозволяє створювати ефективні, гнучкі та економічно доцільні рішення для побудови корпоративних мереж. Завдяки широкому набору функцій, таким як підтримка протоколів маршрутизації, реалізація VPN-з’єднань, фільтрація трафіку, NAT та сегментація мережі, MikroTik RouterOS забезпечує високий рівень керованості та захищеності мережевої інфраструктури.

Практична цінність роботи полягає у розробленні моделі корпоративної мережі, яка може бути використана як основа для впровадження мережевої інфраструктури підприємств малого та середнього бізнесу. Запропоновані рішення можуть застосовуватися під час проєктування та модернізації корпоративних мереж з урахуванням сучасних вимог до інформаційної безпеки, продуктивності та масштабованості мережевих систем.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cisco Systems. Enterprise Campus Architecture Design Guide [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/solutions/enterprise/design-zone-campus/index.html (дата звернення: 13.03.2026).
2. Stallings W. Network Security Essentials: Applications and Standards. – 6th ed. – Pearson Education, 2017. – 480 p.
3. Tanenbaum A., Wetherall D. Computer Networks. – 5th ed. – Pearson, 2011. – 960 p.
4. MikroTik. RouterOS Documentation [Електронний ресурс]. – Режим доступу: https://help.mikrotik.com/docs/ (дата звернення: 13.03.2026).
5. MikroTik. Manual: Packet Flow in RouterOS [Електронний ресурс]. – Режим доступу: https://help.mikrotik.com/docs/display/ROS/Packet+Flow (дата звернення: 13.03.2026).
6. NIST. Guide to Intrusion Detection and Prevention Systems (IDPS) [Електронний ресурс]. – Режим доступу: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (дата звернення: 13.03.2026).
7. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – NIST Special Publication 800-94. – National Institute of Standards and Technology, 2007.
8. RFC Editor. IP Security Architecture for the Internet Protocol (RFC 4301) [Електронний ресурс]. – Режим доступу: https://www.rfc-editor.org/rfc/rfc4301 (дата звернення: 13.03.2026).
9. RFC Editor. Generic Routing Encapsulation (GRE) – RFC 2784 [Електронний ресурс]. – Режим доступу: https://www.rfc-editor.org/rfc/rfc2784 (дата звернення: 13.03.2026).
10. Oppenheimer P. Top-Down Network Design. – 3rd ed. – Cisco Press, 2011. – 624 p.

11. Comer D. Internetworking with TCP/IP: Principles, Protocols and Architecture. – 6th ed. – Pearson, 2015. – 640 p.

12. Cisco Systems. Introduction to Virtual Private Networks (VPN) [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/index.html (дата звернення: 13.03.2026).

13. Cloudflare. What is VPN? [Електронний ресурс]. – Режим доступу: https://www.cloudflare.com/learning/network-layer/what-is-a-vpn/ (дата звернення: 13.03.2026).

14. Fortinet. What is Intrusion Detection System (IDS)? [Електронний ресурс]. – Режим доступу: https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system (дата звернення: 13.03.2026).

15. Cisco Systems. Cisco Networking Fundamentals [Електронний ресурс]. – Режим доступу:
https://www.netacad.com/ (дата звернення: 13.03.2026).

16. Rekhter Y., Moskowitz B., Karrenberg D., de Groot G., Lear E. Address Allocation for Private Internets (RFC 1918) [Електронний ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc1918 (дата звернення: 13.03.2026).

17. Farinacci D., Li T., Hanks S., Meyer D., Traina P. Generic Routing Encapsulation (GRE) (RFC 2784) [Електронний ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc2784 (дата звернення: 13.03.2026).

18. Frankel S., Krishnan S. IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap (RFC 6071) [Електронний ресурс]. URL: https://datatracker.ietf.org/doc/html/rfc6071 (дата звернення: 13.03.2026).

19. Cisco Systems. Cisco Catalyst 9200 Series Switches Data Sheet [Електронний ресурс]. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9200-series-switches/nb-06-cat9200-ser-data-sheet-cte-en.html (дата звернення: 13.03.2026).

20. Extreme Networks. ExtremeSwitching 200 Series Data Sheet

[Електронний ресурс]. URL: https://www.extremenetworks.com/product/200-series/ (дата звернення: 13.03.2026).

21. Edge-Core Networks. ECS4100 Series Switches Data Sheet [Електронний ресурс]. URL: https://www.edge-core.com/_upload/images/2022-ECS4100_series-DS_R02-20220218.pdf (дата звернення: 13.03.2026).

22. MikroTik. CRS3xx, CRS5xx, CCR2116, CCR2216 Switch Chip Features [Електронний ресурс]. URL: https://help.mikrotik.com/docs/display/ROS/CRS3xx%2C+CRS5xx%2C+CCR2116%2C+CCR2216+switch+chip+features (дата звернення: 13.03.2026).

23. Cisco Systems. Cisco Catalyst 9500 Series Switches Data Sheet [Електронний ресурс]. URL: https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html (дата звернення: 13.03.2026).

24. Extreme Networks. ExtremeSwitching X460-G2 Series Data Sheet [Електронний ресурс]. URL: https://www.extremenetworks.com/product/x460-g2/ (дата звернення: 13.03.2026).

25. Edge-Core Networks. ECS4620 Series L3 Gigabit Ethernet Stackable Switch Data Sheet [Електронний ресурс]. URL: https://www.edge-core.com/_upload/images/2022-ECS4100_series-DS_R02-20220218.pdf (дата звернення: 13.03.2026).

26. MikroTik. L3 Hardware Offloading in RouterOS [Електронний ресурс]. URL: https://help.mikrotik.com/docs/display/ROS/L3+Hardware+Offloading (дата звернення: 13.03.2026).

27. Noor-A-Rahim M., John J., Zorbas D., Firyaguna F. Wireless Communications for Smart Manufacturing and Industrial IoT: Existing Technologies, 5G, and Beyond. 2022. 21 p.

28. Jay. EZ, AP & QR Code Setup Modes for Wi-Fi based IoT [Електронний ресурс]. Petoneer. URL: https://petoneer.com (дата звернення: 13.03.2026).

29. ДСТУ ISO/IEC 27001:2015 Інформаційні технології – Методи захисту

– Системи управління інформаційною безпекою. Київ: ДП «УкрНДНЦ», 2015.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА ІНЖЕНЕРІЇ ПЗ АВТОМАТИЗОВАНИХ СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА

«Корпоративна мережа на базі технологій MikroTik RouterOS»

Виконав: здобувач вищої освіти гр. ІСД-42 Роман ГРИГОР'ЄВ

Керівник: викладач кафедри Олександр БОНДАРЧУК

Київ – 2026

МЕТА, ОБ'ЄКТ ТА ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета роботи

Розроблення та впровадження сучасної захищеної корпоративної мережі з використанням технологій MikroTik RouterOS.

Об'єкт дослідження

Корпоративна комп'ютерна мережа підприємства, що функціонує в умовах розподіленої інфраструктури та потребує забезпечення високого рівня захищеності, надійності й доступності мережевих сервісів.

Предмет дослідження

Технології побудови, захисту та адміністрування корпоративних мереж на базі операційної системи MikroTik RouterOS.

НАУКОВІ ЗАВДАННЯ ТА МЕТОДИ ДОСЛІДЖЕННЯ

3

Наукові завдання:

1. Аналіз сучасних технологій і методів побудови корпоративних мереж та архітектурних підходів

2. Дослідження можливостей MikroTik RouterOS у задачах побудови захищених мереж

3. Визначення ключових вимог до мережі: надійність, безпека, масштабованість, продуктивність

4. Реалізація мережі з міжмережевим екраном, VPN-з'єднаннями, NAT та контролем трафіку

5. Оцінка ефективності мережі шляхом тестування працездатності та безпеки у EVE-NG

6. Формулювання рекомендацій щодо впровадження захищених мереж MikroTik RouterOS

Методи дослідження:

- Аналіз технічних джерел та мережевих технологій MikroTik
- Системний аналіз та проєктування мережевої архітектури
- Налаштування маршрутизаторів, VPN, firewall, NAT
- Моделювання мережі у середовищі EVE-NG
- Тестування надійності, безпеки та продуктивності

АРХІТЕКТУРНІ МОДЕЛІ КОРПОРАТИВНИХ МЕРЕЖ

4

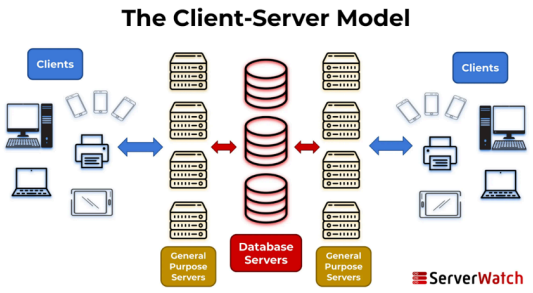


Рисунок 1 – Архітектура Client-Server

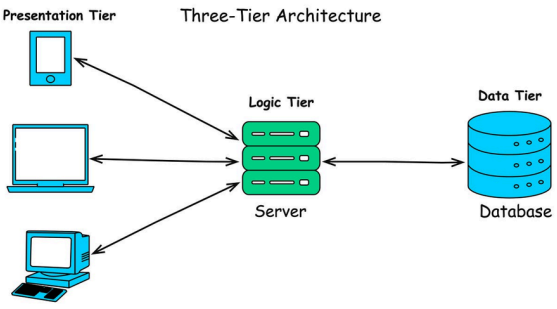


Рисунок 2 – Трирівнева архітектура (Three-Tier)

ТЕХНОЛОГІЇ ЗАХИСТУ МЕРЕЖЕВОЇ ВЗАЄМОДІЇ

5

Таблиця 1 – Порівняння технологій захисту мережевої взаємодії

Технологія	Рівень OSI	Тип захисту	Переваги	Недоліки
GRE	3 (мережевий)	Тунелювання	Простота, підтримка multicast	Немає власного шифрування
IPsec	3 (мережевий)	Шифрування + автентифікація	Високий рівень безпеки, AH/ESP	Складність налаштування
Site-to-Site VPN	3–7	Захищений тунель між офісами	Прозора взаємодія мереж	Залежить від продуктивності
Firewall	2–7	Фільтрація трафіку	Гнучкі правила, контроль	Не шифрує трафік
GRE over IPsec	3 (мережевий)	Тунелювання + шифрування	Поєднує переваги обох	Вища складність конфігурації

МОЖЛИВОСТІ MIKROTIK ROUTEROS ДЛЯ КОРПОРАТИВНИХ МЕРЕЖ

6

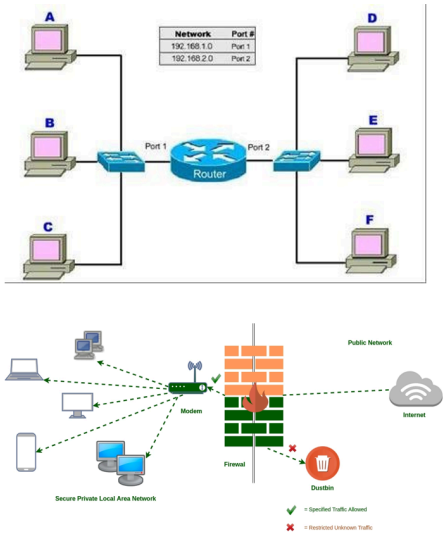


Рисунок 3 – Корпоративна мережа підприємства із застосуванням MikroTik RouterOS

Функція	Опис
Маршрутизація	OSPF, BGP, статична маршрутизація, policy routing
VPN	IPsec, GRE, L2TP, PPTP, OpenVPN, WireGuard
Firewall	Stateful пакетний фільтр, NAT, mangle, address list
Управління трафіком	QoS, shaping, queuing, HTB
VLAN / Bridge	IEEE 802.1Q, trunk/access портів, STP/RSTP
Моніторинг	Winbox, The Dude, SNMP, Syslog, Netflow
Висока доступність	VRRP, failover, dual ISP, load balancing

Таблиця 2 – Основні функції MikroTik RouterOS

ПРОЄКТУВАННЯ АРХІТЕКТУРИ КОРПОРАТИВНОЇ МЕРЕЖІ

7

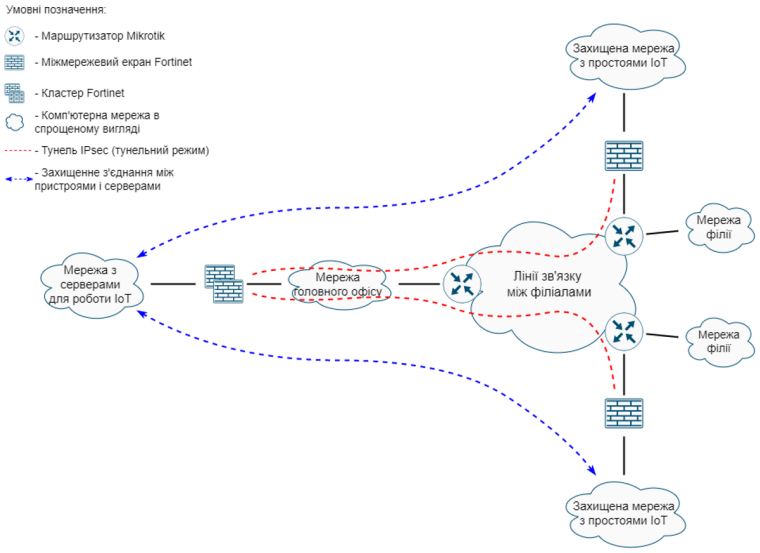


Рисунок 4 – Структурна модель захищеної мережі на базі MikroTik

ПЛАН IP-АДРЕСАЦІЇ ТА ЛОГІЧНА ТОПОЛОГІЯ

8

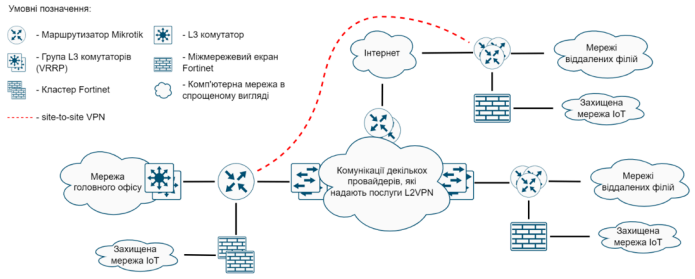


Рисунок 5– Частина плану IP-адресації (провайдерські підключення та VLAN-сегменти)

Головний офіс (HQ)
OSPF-ядро, L3/L2 комутатори, ISP1/ISP2 dual-homing, VLAN 24/256/544

Філія 1 (Branch1)
VPN-з'єднання через ISP1, L2-сегментація, IPsec тунель до HQ-FW-IoT

Філія 2 (Branch2)
VPN-з'єднання через ISP2, аналогічна структура з резервним каналом

IoT-сегмент
Ізольований сегмент із фільтрацією через міжмережеві екрани HQ-FW-IoT та Branch-FW-IoT

РОЗГОРТАННЯ ПРОТОТИПУ У СЕРЕДОВИЩІ EVE-NG

9

ISP1					
№	Хост	IP адреса	Маска	VLAN	Коментар
1	2	3	4	5	6
1	**Point-to-Point to ISP1**	100.64.0.0	30	p-to-p-ISP1	З'єднання з ISP1. Через що підмережу прописаний маршрут до пулу глобальних адрес
	ISP1-GW	100.64.0.1	30	545	
	HQ-R-border	100.64.0.2			
	Broadcast	100.64.0.3	255.255.255.252		
2	**Global pool ISP1**	100.64.1.0	29	-	
			29	-	
	Остання адреса	100.64.1.8	255.255.255.248		
3	**ISP1 VLAN for branch**	10.1.0.0	24	ISP1-district-VLAN	
	HQ-R-border	10.1.0.1	24	544	
	Branch1-R	10.1.0.2			
	Branch2-R	10.1.0.3			
	Резерв	10.1.0.4			
	Broadcast	10.1.0.255	255.255.255.0		

Компоненти середовища:

- EVE-NG — платформа для мережевого моделювання на базі Linux
- RouterOS CHR — віртуальні маршрутизатори MikroTik
- Головний офіс: 2×L3, 4×L2-комутатори, 2 ISP, HQ-FW-IoT
- Філія 1 та Філія 2: по 1 маршрутизатору, локальні комутатори
- 3 філії з'єднані з HQ через шифровані IPsec-тунелі
- Dual ISP (failover) на рівні HQ-Border
- OSPF-маршрутизація між сегментами головного офісу
- VRRP — резервування шлюзу за замовчуванням

РЕАЛІЗАЦІЯ МІЖМЕРЕЖЕВОГО ЕКРАНУВАННЯ ТА VPN-З'ЄДНАНЬ

10

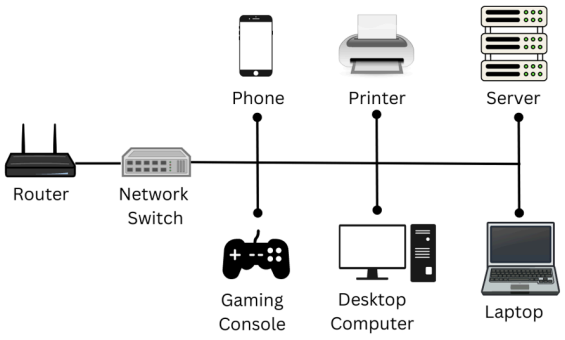


Рисунок 6 – DMZ-архітектура мережевого периметру

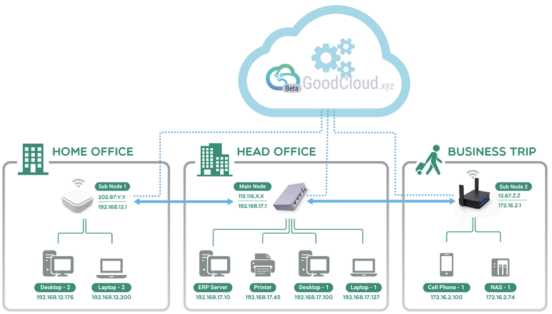
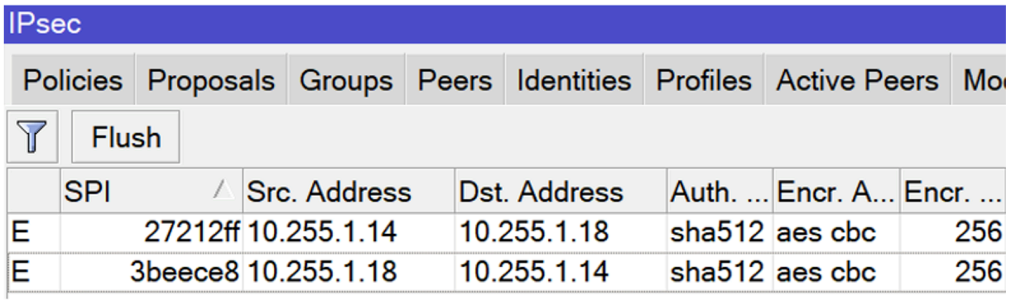


Рисунок 7 – Схема IPsec VPN між HQ та філіями

АНАЛІЗ РІВНЯ ЗАХИЩЕНОСТІ КОРПОРАТИВНОГО СЕГМЕНТУ

11



	SPI	Src. Address	Dst. Address	Auth. ...	Encr. A...	Encr. ...
E	27212ff	10.255.1.14	10.255.1.18	sha512	aes cbc	256
E	3beece8	10.255.1.18	10.255.1.14	sha512	aes cbc	256

Рисунок 8 – Активні IPsec-з'єднання (SPI 27212ff, 3beece81 підтверджують шифрування)

ВИСНОВКИ

12

1. Досліджено сучасні архітектурні підходи до побудови корпоративних мереж (Client-Server, Three-Tier, Campus Network), проаналізовано роль IDS/IPS, технологій GRE, IPsec та VPN у забезпеченні мережевої безпеки.

2. Обґрунтовано вибір MikroTik RouterOS як платформи для реалізації захищеної корпоративної мережі завдяки широкому функціоналу, гнучкості налаштування та економічній доцільності.

3. Розроблено архітектуру трирівневої корпоративної мережі (ядро/розподіл/доступ) з головним офісом та трьома філіями, визначено план IP-адресації та принципи сегментації VLAN.

4. Реалізовано прототип мережі у середовищі EVE-NG: налаштовано OSPF, VRRP, dual ISP failover, GRE-over-IPsec тунелі між HQ та філіями, firewall з address lists та NAT.

5. Тестування підтвердило відмовостійкість: відновлення при відмові L3-комутатора — ~4 с; при відмові ISP-каналу — ~2 с; автоматичне перемикання на резервний маршрут.

6. Аналіз захищеності підтвердив коректне шифрування міжфілійного трафіку: збіг SPI-значень (27212ff, 3beece81) у Wireshark та конфігурації IPsec підтверджує цілісність тунелю.

7. Практична цінність роботи — готова модель захищеної мережі для підприємств малого та середнього бізнесу з рекомендаціями щодо впровадження MikroTik RouterOS-інфраструктури.

АПРОБАЦІЯ:
1.III Всеукраїнській науково-технічній конференції «Технологічні горизонти: дослідження та застосування інформаційних технологій для технологічного прогресу України і світу» (Київ, ДУІКТ, 18 листопада 2025 р.).
Тези доповіді на тему «Технологічні інновації в сучасній освіті: аналіз та перспективи впровадження»
опубліковані у збірнику матеріалів конференції (стор. 305).

2.VII Всеукраїнській науково-технічній конференції «Сучасний стан та перспективи розвитку IoT» (Київ, ДУІКТ, 20 квітня 2026 р.).
Тези доповіді на тему «Сучасні інформаційні технології в Україні та світі: глобальні тренди та макроекономічний вплив»
опубліковані у збірнику матеріалів конференції (стор. 29).

ДЯКУЮ ЗА УВАГУ!