МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ
Циклова комісія комп’ютерної інженерії та інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему

ОПТИМІЗАЦІЯ ДОМАШНЬОЇ WI-FI МЕРЕЖІ З ВИКОРИСТАННЯМ VLAN І ГОСТЬОВОГО ДОСТУПУ

Виконав:
студент групи 1К-22
Спеціальності
123 «Комп’ютерна інженерія»
Владислав МУХА
Керівник:
Маргарита МЕДОЛИЗ

Черкаси 2026

ЧЕРКАСЬКИЙ ДЕРЖАВНИЙ ФАХОВИЙ БІЗНЕС-КОЛЕДЖ

Циклова комісія комп’ютерної інженерії та інформаційних технологій

Спеціальність 123 «Комп’ютерна інженерія»

Освітня програма Комп’ютерна інженерія

ЗАТВЕРДЖУЮ
Завідувачка циклової комісії КІ та ІТ
_____Наталя ФАЛЬЧЕНКО
(підпис)
«_____» _____2025 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Мухі Владиславу Сергійовичу

1. Тема кваліфікаційної роботи «Оптимізація домашньої Wi-Fi мережі з використанням VLAN і гостьового доступу»
   Керівник роботи Медолиз Маргарита Миколаївна, викладач вищої категорії, затверджені наказом закладу передвищої освіти від 06.10.2025 р № 84/1у
2. Строк подання студентом кваліфікаційної роботи 08.06.2026
3. Вихідні дані до кваліфікаційної роботи: технічна документація для програмованого мережевого обладнання, характеристики домашніх комп’ютерних мереж, засоби для моделювання комп’ютерних мереж, стандарти бездротових мереж, стандарти технології VLAN, програмне середовище Cisco Packet Tracer
4. Зміст кваліфікаційної роботи: Аналіз принципів побудови домашніх Wi-Fi мереж; класифікація методів оптимізації бездротових мереж;дослідження технології VLAN та її застосування; моделювання домашньої мережі з використанням VLAN та гостьового доступу
5. Дата видачі завдання 15.10.2025 р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Терміни виконання етапів	Примітка про виконання
1	Вступ	14.10.2025	
2	Розділ 1 Основи побудови домашніх wi-fi мереж	09.12.2025	
3	Розділ 2 Оптимізація домашньої wi-fi мережі	10.03.2026	
4	Розділ 3 Практична реалізація та оцінка ефективності мережі	28.04.2026	
5	Висновки	12.05.2026	
6	Оформлення кваліфікаційної роботи (чистовий варіант)	26.05.2026	
7	Перевірка кваліфікаційної роботи на наявність ознак плагіату (за 10 днів до захисту)	05.06.2026	
8	Подання кваліфікаційної роботи на затвердження завідувачу ЦК (за 7 днів до захисту)	08.06.2026	

Студент _____ Владислав МУХА
(підпис)

Керівник роботи _____ Маргарита МЕДОЛИЗ
(підпис)

АНОТАЦІЯ

Кваліфікаційна робота присвячена дослідженню та оптимізації домашньої Wi-Fi мережі шляхом впровадження технології VLAN та організації гостьового доступу. Актуальність теми зумовлена зростанням кількості бездротових пристроїв у домашніх мережах, та необхідністю забезпечення стабільної роботи мережі в умовах віддаленої роботи.

У роботі проаналізовано принципи функціонування Wi-Fi мереж, сучасні стандарти бездротового зв'язку IEEE 802.11, основні проблеми домашніх бездротових мереж та можливості їх усунення за допомогою сегментації трафіку.

У практичній частині виконано проектування та моделювання оптимізованої домашньої мережі в середовищі GNS3. Розроблено логічну структуру мережі з поділом на окремі VLAN для робочих, домашніх, IoT та гостьових пристроїв. Для реалізації проєкту обрано маршрутизатор MikroTik. Також використано програмні засоби Wireshark та RouterOS sniffer для аналізу трафіку та оцінювання продуктивності мережі.

Проведено тестування розробленої моделі та виконано оцінку ефективності впроваджених рішень. Отримані результати підтвердили, що використання VLAN та гостьового доступу дозволяє підвищити рівень інформаційної безпеки, зменшити вплив широкомовного трафіку, покращити керованість мережі та забезпечити стабільну роботу пристроїв різного призначення.

КЛЮЧОВІ СЛОВА: WI-FI, VLAN, IEEE 802.1Q, МАРШРУТИЗАЦІЯ, СЕГМЕНТАЦІЯ МЕРЕЖІ, ГОСТЬОВИЙ ДОСТУП, MIKROTIK, GNS3, WIRESHARK, ІНФОРМАЦІЙНА БЕЗПЕКА, БЕЗДРОТОВА МЕРЕЖА.

ABSTRACT

The qualification work is devoted to the study and optimization of a home Wi-Fi network by implementing VLAN technology and organizing guest access. The relevance of the topic is due to the growth in the number of wireless devices in home networks, and the need to ensure stable network operation in remote work conditions.

The work analyzes the principles of operation of Wi-Fi networks, modern IEEE 802.11 wireless communication standards, the main problems of home wireless networks and the possibility of eliminating them using traffic segmentation.

In the practical part, the design and modeling of an optimized home network in the GNS3 environment was performed. A logical network structure was developed with division into separate VLANs for work, home, IoT and guest devices. A MikroTik router was selected for the project. Wireshark and RouterOS sniffer software were also used to analyze traffic and evaluate network performance.

The developed model was tested and the effectiveness of the implemented solutions was assessed. The results obtained confirmed that the use of VLAN and guest access allows to increase the level of information security, reduce the impact of broadcast traffic, improve network manageability and ensure stable operation of devices for various purposes.

KEYWORDS: WI-FI, VLAN, IEEE 802.1Q, ROUTING, NETWORK SEGMENTATION, GUEST ACCESS, MIKROTIK, GNS3, WIRESHARK, INFORMATION SECURITY, WIRELESS NETWORK.

ЗМІСТ

ВСТУП

У сучасному світі безпровідні технології стали невід'ємною частиною щоденного життя. Домашні Wi-Fi мережі застосовуються для доступу до Інтернету, роботи, навчання, дозвілля, а також для з'єднання великої кількості приладів, включаючи смартфони, комп’ютери , телевізори та пристрої Інтернету речей (IoT). Проте зі зростанням кількості підключених пристроїв та обсягів переданих данних виникають проблеми, пов'язані зі зниженням швидкості, нестабільністю з'єднання та недостатнім рівнем захисту мережі.

Особливо важливою є проблема несанкціонованого доступу до домашньої мережі, а також відсутність поділу між приладами різного призначення. У більшості випадків домашні користувачі задіюють одну мережу для усіх пристроїв, що створює ризики витоку даних та зменшення продуктивності. Одним із дієвих способів вирішення цієї проблеми є використання технологій сегментації мережі, зокрема VLAN, а також влаштування гостьово годоступу.

Питання вдосконалення безпровідних мереж досліджувалися багатьма інженерами та фахівцями у сфері комп'ютерних мереж. Питання оптимізації бездротових мереж активно досліджувалися в межах великих підприємств і корпоративних інфраструктур, де забезпечення стабільності, продуктивності та безпеки мережі є критично важливим. У таких середовищах широко застосовується технологія VLAN, яка дозволяє ефективно сегментувати мережу, ізолювати трафік та підвищувати рівень контролю доступу.

Водночас у домашніх умовах застосування VLAN залишається недостатньо дослідженим і використовується значно рідше, незважаючи на зростання кількості підключених пристроїв та вимог до безпеки. Особливої актуальності це питання набуло у зв’язку зі збільшенням кількості працівників, які працюють віддалено та використовують домашні мережі для доступу до корпоративних ресурсів. У таких умовах домашня мережа

фактично стає частиною корпоративної інфраструктури, що підвищує ризики несанкціонованого доступу, витоку даних і зниження продуктивності.

Саме тому дослідження можливостей впровадження VLAN у межах домашньої Wi-Fi мережі є актуальним і доцільним, оскільки дозволяє адаптувати ефективні корпоративні рішення до побутового використання та підвищити якість роботи мережі.

Метою роботи є оптимізація домашньої Wi-Fi мережі шляхом впровадження технології VLAN та організації гостьового доступу для підвищення її продуктивності та безпеки.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- проаналізувати принципи роботи домашніх Wi-Fi мереж;

- дослідити технологію VLAN, її принципи роботи та можливості застосування у домашніх мережах;

- обґрунтувати доцільність використання VLAN у домашніх умовах для забезпечення сегментації та безпеки;

- провести аналіз існуючої домашньої мережі та виявити її недоліки (продуктивність, безпека, навантаження);

- розробити оптимізовану структуру домашньої мережі з урахуванням розподілу на VLAN (основна, гостьова, IoT тощо);

- реалізувати налаштування VLAN і гостьового доступу з урахуванням захисту корпоративних даних при віддаленій роботі;

- оцінити ефективність запропонованих рішень за показниками продуктивності, стабільності та безпеки.

Об’єктом дослідження є домашня Wi-Fi мережа.

Предметом дослідження є методи оптимізації домашньої мережі з використанням технології VLAN-сегментації та механізмів організації гостьового доступу.

Практичне значення цієї роботи полягає в тому, що оптимізація домашньої Wi-Fi мережі за допомогою VLAN та гостьового доступу дозволяє одночасно підвищити рівень безпеки й ефективність використання ресурсів.

Ізоляція різних сегментів трафіку забезпечує захист основної мережі від потенційних загроз, а створення окремого каналу для гостей робить користування більш зручним і контрольованим. Цінність роботи полягає у створенні реальних умов для безпечного, продуктивного та комфортного використання домашньої мережевої інфраструктури.

РОЗДІЛ 1 ОСНОВИ ПОБУДОВИ ДОМАШНІХ WI-FI МЕРЕЖ

1.1 Поняття та принцип роботи Wi-Fi мереж

Wi-Fi – це торгова марка Wi-Fi Alliance та загальновживана назва для набору стандартів IEEE 802.11, що описують передавання цифрових потоків даних через радіоканали.

Це найбільш розповсюджена технологія для побудови бездротових локальних мереж (WLAN), яка дозволяє пристроям з'єднуватися та обмінюватися даними без використання кабелів

Wi-Fi мережа – це технологія бездротового доступу до локальної мережі та Інтернету. Основою роботи Wi-Fi є передача інформації за допомогою радіохвиль, зазвичай у діапазонах 2,4 ГГц та 5 ГГц, а в сучасніших стандартах також 6 ГГц.

У типовій домашній мережі головним компонентом є бездротовий маршрутизатор або точка доступу. Він виступає посередником між пристроями користувача та інтернет-провайдером. Коли пристрій підключається до Wi-Fi, він обмінюється даними з маршрутизатором, який потім пересилає ці дані до локальної мережі або в Інтернет [1].

Основні поняття :

- WLAN (Wireless Local Area Network): Локальна мережа, де для зв’язку замість дротів використовуються радіохвилі

- Точка доступу (Access Point): Основа бездротової мережі, яка підключається до дротової інфраструктури (зазвичай інтернет-провайдера) і транслює радіосигнал.

- Хот-спот (Wi-Fi зона): Територія радіусом 50–100 метрів навколо точки доступу, у межах якої можливе підключення до мережі.

- SSID (Service Set Identifier): Унікальний ідентифікатор , назва мережі, який точка доступу транслює для виявлення її клієнтськими пристроями.

Принцип роботи Wi-Fi базується на використанні радіочастотних технологій для двосторонньої комунікації між приймачами та передавачами в

мережевих пристроях. Точка доступу кожні 100 мс передає спеціальні сигнальні пакети зі своїм SSID на мінімальній швидкості 0,1 Мбіт/с. 0,1 Мбіт/с – найменша швидкість передавання даних для Wi-Fi.

Клієнтський пристрій , потрапляючи в зону покриття, виявляє доступні мережі за їхніми SSID і надсилає запит на підключення. При потраплянні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на основі даних про рівень сигналу.

Дані передаються у визначених частотних діапазонах. Найпоширенішими є 2,4 ГГц (краще долає перешкоди, але повільніший) та 5 ГГц (швидший, але має менший радіус дії). Новітні стандарти, такі як Wi-Fi 6E та Wi-Fi 7, використовують також діапазон 6 ГГц для зменшення завад та збільшення ємності мережі

Бездротові мережі можуть функціонувати у кількох різних режимах, кожен із яких має власну логіку організації та історичний контекст розвитку. Найбільш поширеним є інфраструктурний режим, у якому вся взаємодія між пристроями відбувається через центральний вузол – точку доступу. Така схема легко масштабується: достатньо додати нові точки доступу, щоб розширити мережу, і саме тому вона стала стандартом для більшості сучасних Wi-Fi систем.

Інший підхід, відомий як ad-hoc або «точка-точка», передбачає пряме з’єднання між пристроями без участі центрального керуючого елемента. Цей режим був характерним для ранніх версій Wi-Fi, але вимагав ручного налаштування параметрів – від імені мережі до IP-адресації. З часом він втратив актуальність: сучасні операційні системи або значно обмежують його використання, або взагалі не підтримують, що фактично зробило технологію застарілою.

На зміну ad-hoc прийшла більш сучасна концепція – Wi-Fi Direct. Її офіційно запровадив Wi-Fi Alliance у 2010 році як сертифікаційну програму. У цьому випадку мережа будується за принципом групи, де один із пристроїв автоматично стає керуючим – так званим Group Owner, виконуючи функції

точки доступу. Головна перевага полягає в автоматичному налаштуванні: пристрої самостійно конфігурують параметри, отримують IP-адреси та встановлюють захищене з’єднання. Цікаво, що для створення такої мережі достатньо, аби стандарту Wi-Fi Direct відповідав лише один із пристроїв, що значно спрощує процес і робить технологію доступною для широкого використання.

Таким чином, еволюція режимів роботи Wi-Fi демонструє поступовий перехід від ручних і громіздких рішень до автоматизованих і гнучких систем, які відповідають потребам сучасних користувачів.

Важливою характеристикою Wi-Fi мережі є її пропускна здатність і стабільність сигналу. На ці параметри впливають різні фактори: відстань до точки доступу, наявність перешкод , кількість підключених пристроїв, а також завади від інших мереж, що працюють на тих самих частотах. Наприклад, у багатоквартирних будинках часто виникає перевантаження діапазону 2,4 ГГц, що призводить до зниження швидкості з’єднання [2].

Щоб уникнутии цих проблем у спільному ефірі, Wi-Fi використовує спеціальний протокол CSMA/CA. Його логіка проста : перед тим як відправити дані, пристрій перевіряє ефір на вільність. Якщо канал зайнятий іншим передавачем, пристрій чекає випадковий проміжок часу і пробує знову.

1.2 Аналіз стандартів бездротового зв’язку

Розвиток сучасних бездротових технологій нерозривно пов'язаний з еволюцією стандартів сімейства IEEE 802.11, які в побуті ми називаємо Wi-Fi. Ці стандарти фактично є набором правил і протоколів, що визначають, як саме дані перетворюються на радіохвилі та передаються між пристроями [1].

Історія стандартів почалася ще в 1997 році з оригінального IEEE 802.11, який забезпечував швидкість лише до 2 Мбіт/с.

Справжній прорив стався у 1999 році з появою 802.11b, який працював на частоті 2,4 ГГц і став першим масовим стандартом, що популяризував бездротовий зв’язок

Паралельно з'явився 802.11a для діапазону 5 ГГц, який хоч і був швидшим (до 54 Мбіт/с), мав значно менший радіус дії через фізичні особливості високих частот погано долати перешкоди.

У 2003 році стандарт 802.11g об’єднав переваги обох попередників, запропонувавши 54 Мбіт/с на вже звичному діапазоні 2,4 ГГц, що зробило Wi-Fi невіддільною частиною офісного та домашнього життя.

Сучасна ера бездротового зв'язку почалася з впровадження стандарту 802.11n у 2009 році, який офіційно отримав назву Wi-Fi 4.

На сьогоднішній день старіші версії, такі як 802.11g, сьогодні практично не використовуються, поступившись місцем 802.11n і стандартам вище .

На зміну йому прийшов 802.11ac , який фокусувався виключно на діапазоні 5 ГГц, пропонуючи гігабітні швидкості .

Сьогодні найактуальнішим для впровадження в домашніх умовах є стандарт 802.11ax, відомий як Wi-Fi 6. Особливої уваги заслуговує розширення Wi-Fi 6E, яке відкриває доступ до нового діапазону 6 ГГц. Це дозволяє уникнути зашумленості ефіру, яку створюють сусідські мережі на частотах 2,4 та 5 ГГц.

Розвиток стандартів бездротового зв’язку відбувався не лише за рахунок збільшення номінальної швидкості передачі даних, а й завдяки впровадженню нових технологічних рішень. Одним із важливих параметрів Wi-Fi мережі є ширина каналу. У ранніх стандартах, таких як 802.11b та 802.11g, використовувалася фіксована ширина каналу 20 МГц. З появою 802.11n стало можливим об’єднання каналів до 40 МГц, що фактично подвоювало пропускну здатність. У стандарті 802.11ac ця ідея отримала подальший розвиток –підтримуються канали шириною 80 та навіть 160 МГц [3].З одного боку, це дозволяє значно збільшити швидкість передачі даних, але з іншого – підвищує ризик перешкод, особливо в умовах щільної забудови.

Не менш важливу роль відіграє модуляція сигналу – спосіб кодування інформації в радіохвилях. У сучасних стандартах, зокрема 802.11ac та 802.11ax, використовується високоефективна квадратурна амплітудна

модуляція (QAM), наприклад 256-QAM або 1024-QAM. Модуляція визначає, скільки біт даних "пакується" в один радіосигнал. Це дозволяє значно підвищити швидкість, однак потребує кращої якості сигналу, оскільки така модуляція є більш чутливою до завад.

Також ключовою технологічною відмінністю стандартів IEEE 802.11ax від попередніх поколінь є перехід від методу ортогонального частотного мультиплексування (OFDM) до множинного доступу з ортогональним частотним поділом (OFDMA). У стандартах Wi-Fi 4 та Wi-Fi 5 технологія OFDM передбачає виділення всього частотного каналу лише одному користувачу в конкретний момент часу. Натомість OFDMA дозволяє розділяти один канал на декілька підканалів. Це забезпечує можливість одночасної комунікації точки доступу з кількома клієнтськими пристроями в межах одного кадру, що суттєво підвищує ефективність та мінімізує затримки.

Ще однією вагомою технолонією стала системам багатокнального вводу-виводу (MIMO). Технологія MIMO, впроваджена у стандарті Wi-Fi 4, використовує кілька антен для одночасної передачі декількох потоків даних одному клієнту, що дозволяє кратно збільшити швидкість з’єднання в межах одного частотного каналу. Наступним кроком став перехід до MU-MIMO (Multi-User MIMO), вперше реалізованого у Wi-Fi 5 для низхідного каналу (Downlink), а у Wi-Fi 6 – і для висхідного (Uplink). На відміну від базового MIMO, який обслуговує лише одного користувача в конкретний проміжок часу , технологія MU-MIMO дозволяє точці доступу формувати просторово розділені промені для одночасного обміну даними з декількома незалежними клієнтами.

Узагальненну інформацію щодо характеристик кожного стандарту можна побачити на порівняльній таблиці (табл. 1.1). Розвиток стандартів бездротового зв’язку, який відображено у таблиці, спрямований на підвищення швидкості передачі даних, зменшення затримок і покращення стабільності роботи мережі в умовах великої кількості підключених пристроїв.

Таблиця 1.1 – Порівняльна таблиця стандартів IEEE 802.11

Характеристика	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 6E
Дата випуску	2009[4]	2014[4]	2019[4]	2021[4]
Стандарт IEEE	802.11n	802.11ac	802.11ax	802.11ax
Макс. швидкість	1.2 Гбіт/с	3.5 Гбіт/с	9.6 Гбіт/с	9.6 Гбіт/с
Діапазони частот	2.4 ГГц та 5 ГГц	5 ГГц	2.4 ГГц та 5 ГГц	6 ГГц
Безпека	WPA 2	WPA 2	WPA 3	WPA 3
Ширина каналу	20, 40 МГц	20, 40, 80, 80+80,160 МГц	20, 40, 80, 80+80, 160 МГц	20, 40, 80, 80+80,160 МГц
Модуляція	64-QAM OFDM	256-QAM OFDM	1024-QAM OFDMA	1024-QAM OFDMA
MIMO	4x4 MIMO	4x4 MIMO, DL MU-MIMO	8x8 UL/DL MU-MIMO	8x8 UL/DL MU-MIMO

Виконаний аналіз показує, що використання новітніх стандартів є важливою умовою для побудови стабільної та продуктивної домашньої Wi-Fi мережі, особливо в умовах віддаленої роботи та активного використання мультимедійних сервісів.

1.3 Основні проблеми функціонування домашніх Wi-Fi мереж

Функціонування домашніх бездротових мереж у сучасних реаліях часто супроводжується низкою технічних та експлуатаційних викликів, які безпосередньо впливають на якість користувацького досвіду. Попри те, що технологія Wi-Fi стала стандартом де-факто для доступу до інтернету, її природа як радіоефірного середовища зумовлює певні вроджені обмеження.

Однією з найбільш відчутних проблем є фізичні перешкоди та обмежена дальність передавання сигналу. Поширення радіохвиль залежить від потужності передавача, типу антен та характеристик навколишнього середовища. Особливо це актуально для діапазону 5 ГГц, який хоч і забезпечує вищу швидкість, проте значно гірше долає об’єкти на шляху сигналу, такі як товсті стіни чи меблі, порівняно з частотою 2,4 ГГц.

Ще одна серйозна проблема полягає у неоднорідності парку клієнтських пристроїв. У типовій домашній мережі одночасно працюють сучасний смартфон з підтримкою Wi-Fi 6 та, наприклад, старий ноутбук або дешевий датчик температури, що використовує застарілий стандарт. Оскільки точка доступу змушена підтримувати зворотну сумісність, робота повільного пристрою може суттєво гальмувати всю мережу. Це явище називають «проблемою повільного клієнта»: поки старий гаджет передає свій невеликий пакет даних на низькій швидкості, швидкі пристрої простоюють в очікуванні вільного ефіру. Без логічного поділу трафіку за допомогою гостьових мереж або окремих VLAN, один такий застарілий девайс може нівелювати переваги дорогого маршрутизатора.

Іншим критичним фактором є спектральна перевантаженість та інтерференція. У багатоквартирних будинках десятки роутерів одночасно намагаються транслювати сигнал на тих самих частотах, що створює значний рівень шуму. Додаткові завади створюють побутові прилади, наприклад, мікрохвильові печі або Bluetooth-пристрої, що працюють у популярному діапазоні 2,4 ГГц.

На практиці проблеми також можуть створювати безпровідні девайси які працюють безпосередньо близько до Wi-Fi адаптера. Це призводить до нестабільності з'єднання та різкого падіння швидкості, оскільки точка доступу змушена постійно конкурувати за вільний ефір.

Нарешті, суттєвий вплив має неправильне налаштування та адміністрування мережі. Використання статичних радіоканалів у динамічному середовищі часто призводить до конфліктів із сусідськими мережами, тоді як відсутність моніторингу трафіку не дозволяє вчасно виявити аномальну активність чи перевантаження.

Саме для вирішення цих проблем у роботі пропонується впровадження VLAN, що дозволяє ізолювати гостьові пристрої та IoT-ґаджети від основного сегмента мережі, підвищуючи як безпеку, так і загальну керованість системою.

1.4 Технологія VLAN як засіб сегментації мережі

У сучасній практиці побудови локальних мереж одним із найважливіших етапів є забезпечення логічного розподілу ресурсів та ізоляції трафіку. Традиційні мережі, які досі часто зустрічаються в домашніх умовах, становлять собою єдиний логічний сегмент. У такій структурі будь-який пристрій, відправивши широкомовний запит може «бачити» всі інші активні вузли в мережі. Це створює не лише надмірне навантаження на канал зв'язку, а й серйозну вразливість: зловмисник, отримавши доступ до однієї точки, може вільно переміщуватися всередині периметра та атакувати критично важливі системи. Технологія VLAN покликана розв'язати цю проблему шляхом логічної сегментації єдиної фізичної інфраструктури на декілька незалежних віртуальних мереж

Концепція віртуальних локальних мереж виникла як відповідь на обмеженість фізичної інфраструктури. У традиційному розумінні, щоб розділити дві групи пристроїв удома, потрібно було б будувати дві окремі фізичні мережі з власними кабелями та комутаторами. VLAN дозволяє обійти це обмеження, створюючи декілька ізольованих логічних мереж поверх одного фізичного обладнання. У контексті домашнього Wi-Fi це означає, що один маршрутизатор може обслуговувати основні робочі станції та гостьові смартфони так, ніби для кожної з цих груп виділено окремий персональний пристрій.

Технічним фундаментом для роботи віртуальних мереж є стандарт IEEE 802.1Q . Суть процесу полягає в тому, що в кожен Ethernet-кадр додається спеціальний 4-байтний ідентифікатор – тег, що містить номер віртуальної мережі (VLAN ID число від 1 до 4094) [3].Коли пакет проходить через комутатор, що підтримує цей стандарт , пристрій зчитує тег і точно знає, до якого сегмента належать дані та на які порти їх можна передавати. При виході з мережі на кінцевий пристрій, який «не знає» про VLAN, тег видаляється, і пакет набуває стандартного вигляду.

Розглядаючи способи побудови VLAN, визначається належність пристроїв до віртуальної мережі. Існують два базові підходи: один передбачає статичне закріплення портів чи параметрів конфігурації, що робить структуру передбачуваною та простою для адміністрування. Інший орієнтується на динамічне приєднання обладнання, коли роль у мережі визначається автоматично – наприклад, за характеристиками трафіку або ідентифікаційними даними користувача. Така різниця демонструє еволюцію від жорстко фіксованих схем до більш гнучких і адаптивних рішень, які відповідають вимогам сучасних систем із високим рівнем мобільності та масштабованості.

Важливою перевагою використання VLAN у домашніх умовах є можливість гнучкого налаштування прав доступу між сегментами. Сама по собі сегментація лише розділяє пристрої, але за допомогою маршрутизації між VLAN користувач може створювати складні сценарії взаємодії. Наприклад, можна налаштувати мережу так, щоб основний ноутбук міг бачити lot пристрої в іншому сегменті, але самі пристроїї при цьому не мали жодного доступу до ноутбука чи виходу в інтернет. Такий підхід на рівні домашньої інфраструктури робить її стійкою до атак.

Підсумовуючи, використання VLAN для сегментації домашньої мережі дозволяє перетворити її з хаотичного середовища на структуровану систему з чіткими межами безпеки. Це не лише обмежує поширення широкомовного «сміття», підвищуючи загальну продуктивність, а й гарантує, що конфіденційні дані власника залишаться недоступними для випадкових гостей чи скомпрометованих IoT-пристроїв.

1.5 Організація гостьового доступу та методи забезпечення інформаційної безпеки

Організація гостьового доступу в сучасній Wi-Fi мережі є одним із найбільш критичних аспектів забезпечення інформаційної безпеки. Традиційні мережі часто будуються в одному логічному елементі так званому

широкомовному домені як оголошувалося в минулому пункті. Така архітектура базується на хибному припущенні, що зовнішнього брандмауера достатньо для стримування загроз , але це не так. Як тільки пристрій підключається до мережі в межах хот-споту , він отримує повний доступ до всіх ресурсів мережі, що робить її надзвичайно вразливою до внутрішніх атак.

Для розв'язання цієї проблеми використовується логічна сегментація через гостьовий VLAN. Це дозволяє створити ізольоване середовище, де гості мають доступ виключно до інтернету, не «бачачи» при цьому приватних серверів, систем зберігання даних чи розумних пристроїв власника. З технічного погляду це реалізується шляхом трансляції окремого ідентифікатора мережі (SSID), який жорстко прив'язаний до конкретного тегу VLAN. Таким чином, навіть якщо гість спробує просканувати мережу, його ARP-запити ніколи не покинуть межі гостьового сегмента, що суттєво звужує поверхню атаки.

Більш просунутим методом захисту є використання Private VLAN (PVLAN). Ця технологія дозволяє не лише ізолювати гостей від основної мережі, а й заборонити пристроям у межах самої гостьової мережі спілкуватися між собою. Це ідеальний сценарій для безпеки: навіть якщо один із гостьових гаджетів інфікований шкідливим програмним забезпеченням, воно не зможе поширитися на інші пристрої в тому ж сегменті. Такий підхід перетворює мережу на набір ізольованих портів, які можуть взаємодіяти лише з центральним шлюзом , що зазвичай підключений до маршрутизатора.

Методи автентифікації також відіграють ключову роль. Для домашніх мереж стандартом є використання протоколу WPA3, який забезпечує індивідуальне шифрування даних для кожного користувача та надійний захист від підбору паролів методом брутфорс.

Додатковими, але не менш важливими методами захисту є MAC-фільтрація та Ingress Filtering. Хоча MAC-адресу можна підробити, її використання як додаткового бар'єра ускладнює завдання для недосвідченого зловмисника. Вхідна фільтрація, відповідно гарантує, що пакети, які

надходять до мережі, дійсно походять із заявлених адрес, запобігаючи спробам підміни IP-адрес для обходу правил брандмауера.

Нарешті, ефективна безпека неможлива без моніторингу та управління. Використання контролерів дозволяє централізовано налаштовувати політики доступу та оперативно виявляти аномальну активність, наприклад, спроби DoS-атак або появу фальшивих точок доступу. Програмні інструменти, такі як Arpwatch, можуть автоматично сповіщати адміністратора про появу нових пар IP/MAC адрес у гостьовому сегменті, що дозволяє вчасно реагувати на потенційні інциденти.

РОЗДІЛ 2 ПРОЄКТУВАННЯ ТА МОДЕЛЮВАННЯ ДОМАШНЬОЇ WI-FI МЕРЕЖІ

2.1 Аналіз вимог до домашньої мережі в умовах віддаленої роботи

Поширення дистанційної роботи суттєво змінило вимоги до домашніх комп'ютерних мереж. Раніше домашній Wi-Fi використовувався переважно для перегляду веб-сторінок або перегляду відео, але зараз він перетворився на повноцінний робочий простір. Відеоконференції, передача великих обсягів даних, використання хмарних сервісів та віддалений доступ до корпоративних ресурсів – все це вимагає стабільної, безпечної та надійної мережі.

Першочерговою вимогою є забезпечення високої пропускної здатності та мінімальних затримок. Якщо для перегляду соціальних мереж достатньо базової швидкості, то професійна діяльність зазвичай передбачає роботу з «важким» мультимедійним контентом, постійну синхронізацію з хмарними сховищами та участь у відеоконференціях високої чіткості. Для підтримки якісного голосу через IP мережа повинна забезпечувати затримку не більше ніж 150 мс та мати пріоритезацію трафіку. В умовах багатоквартирних будинків, де ефір перевантажений сусідськими роутерами, критично важливою стає підтримка стандартів Wi-Fi 5 або Wi-Fi 6/6E, які використовують ширші канали та нові частотні діапазони для уникнення інтерференції.

Наступним важливим пунктом є стабільність та здатність мережі обслуговувати велику кількість пристроїв одночасно. У типовому будинку кількість підключених ґаджетів: від робочих ноутбуків до побутової техніки, постійно зростає. Крім того, сучасна мережа має забезпечувати впевнене покриття у всіх зонах помешкання, щоб користувач міг вільно переміщуватися без втрати зв’язку.

Найбільш важливим для домашньої мережі у контексті віддаленої роботи є забезпечення конфіденційності та ізоляції робочих даних. Традиційні домашні мережі мають суттєвий недолік: усі пристрої в них перебувають в

одному широкомовному домені та «довіряють» один одному. Це означає, що потенційна вразливість у дешевій смарт-лампі або ігровій консолі може стати «вхідними дверима» для зловмисника, який отримає доступ до корпоративного пристрою з конфіденційною інформацією. Отже, виникає гостра потреба у логічній сегментації мережі.

Не менш важливим є питання надійності обладнання. Бюджетні маршрутизатори часто не розраховані на постійне навантаження та велику кількість одночасних підключень. У результаті можливі перегрівання, зависання або автоматичні перезавантаження пристрою. Саме тому для організації ефективної домашньої мережі в умовах віддаленої роботи важливо обирати обладнання з достатнім запасом продуктивності та підтримкою сучасних мережевих технологій.

2.2 Порівняльний аналіз середовищ мережевого моделювання

Порівняльний аналіз середовищ мережевого моделювання дозволяє виділити три основні платформи, які найчастіше використовуються інженерами та студентами: Cisco Packet Tracer, GNS3 та Cisco Modeling Labs. Кожне з цих середовищ має власні особливості, переваги та обмеження, що впливають на доцільність їх використання для навчання, тестування або побудови складних мережевих сценаріїв.

Cisco Packet Tracer є одним із найпопулярніших інструментів для початкового вивчення комп’ютерних мереж. Його головною перевагою є простота використання та невисокі вимоги до апаратних ресурсів комп’ютера. Середовище дозволяє швидко створювати топології, налаштовувати базові мережеві протоколи та моделювати роботу маршрутизаторів, комутаторів і бездротових пристроїв. Packet Tracer широко використовується в освітніх закладах, оскільки має зрозумілий графічний інтерфейс і підходить для освоєння базових принципів роботи мереж. Проте його основним недоліком є обмежена функціональність. Оскільки програма використовує спрощену

емуляцію пристроїв Cisco, вона не завжди підтримує сучасні технології або реальну поведінку мережевого обладнання.

Більш функціональним середовищем є GNS3, яке орієнтоване на емуляцію реального мережевого обладнання. На відміну від Packet Tracer, GNS3 дозволяє запускати справжні образи операційних систем маршрутизаторів і комутаторів, зокрема Cisco IOS, MikroTik RouterOS та інших платформ. Завдяки цьому користувач отримує середовище, максимально наближене до реальної мережевої інфраструктури.

GNS3 активно використовується для тестування складних мережевих сценаріїв, налаштування VLAN, VPN, динамічної маршрутизації та систем безпеки. Крім того, платформа підтримує інтеграцію з віртуальними машинами, що дозволяє створювати повноцінні лабораторії з серверами та клієнтськими системами.

Ще одним професійним середовищем є Cisco Modeling Labs – офіційна платформа Cisco для мережевого моделювання. Вона створена переважно для професійного тестування та підготовки мережевих спеціалістів. CML забезпечує високу точність емуляції та підтримує сучасні мережеві технології, які використовуються у реальних корпоративних мережах. Однак використання CML потребує ліцензії, а також достатньо потужного обладнання, що обмежує можливість її застосування для моделювання у навчальних лабораторіях або приватного використання.

При порівнянні зазначених платформ можна зробити висновок, що кожна з них орієнтована на різний рівень підготовки та різні задачі. Cisco Packet Tracer є оптимальним вибором для початкового навчання та ознайомлення з базовими мережевими концепціями. GNS3 забезпечує значно ширші можливості для практичного моделювання та наближений до реальних умов експлуатації мереж. У свою чергу, Cisco CML орієнтований переважно на професійне середовище та складні корпоративні сценарії.

2.3 Вибір середовища моделювання

Під час дослідження та оптимізації комп’ютерних мереж важливу роль відіграє використання спеціалізованого програмного середовища для моделювання. Такі системи дозволяють створювати віртуальні мережеві топології, тестувати налаштування обладнання та аналізувати поведінку мережі без необхідності використання великої кількості фізичних пристроїв. Для виконання даної роботи необхідно було обрати середовище, яке забезпечує підтримку сучасних мережевих технологій, зокрема VLAN, бездротових сегментів і гостьового доступу, а також дозволяє максимально наблизити модель до реальних умов функціонування домашньої Wi-Fi мережі.

На відміну від спрощених симуляторів, платформа GNS3 (Graphical Network Simulator-3) є потужним емулятором, що дозволяє запускати реальні образи операційних систем мережевих пристроїв. Це забезпечує максимальну близькість до поведінки справжнього обладнання, оскільки в GNS3 емулюється не просто логіка роботи протоколу, а весь процес обробки даних процесором пристрою. Для роботи з VLAN маршрутизацією це критично важливо: використання реальних образів гарантує, що стандарт тегування трафіку IEEE 802.1Q працюватиме без спотворень, які іноді трапляються в спрощених програмних моделях.

Однією з головних переваг GNS3 у межах цього проєкту є можливість глибокої інтеграції з реальними хостами та стороннім програмним забезпеченням. Програма дозволяє підключати до віртуальної топології віртуальні машини (VM), що виступають як реальні клієнти або сервери. Наприклад, при моделюванні гостьового доступу ми можемо запустити повноцінну ОС Linux або Windows у віртуальному середовищі, щоб перевірити, як саме працюють механізми автентифікації та чи справді гостьовий сегмент ізольований від основного домашнього сегмента на канальному рівні. Такий рівень деталізації перетворює модель з теоретичної схеми на реальний випробувальний стенд.

Крім того, GNS3 забезпечує безшовну інтеграцію з аналізатором трафіку Wireshark. Це дозволяє захоплювати пакети на будь-якому інтерфейсі віртуальної мережі та детально розбирати їхню структуру. Для дослідження безпеки сегментації це неоціненно: можна наочно побачити, як додається тег VLAN до кадру, або переконатися, що ARP-запити з гостьової мережі не проникають у захищений робочий сегмент. Можливість моніторингу трафіку в режимі реального часу дозволяє виявляти потенційні вразливості та аномальну активність, що є основою сучасної мережевої безпеки.

Звісно, робота з GNS3 вимагає значних обчислювальних ресурсів та глибших знань у налаштуванні серверів віртуалізації.Але використання GNS3 дає змогу не лише розробити архітектуру мережі, а й підготувати повний набір конфігураційних файлів, які в подальшому можуть бути завантажені безпосередньо на фізичне обладнання без змін.

Таким чином, вибір GNS3 як середовища моделювання є обґрунтованим з точки зору функціональності, гнучкості та наближеності до реальних умов експлуатації мережі. Платформа дозволяє реалізувати всі необхідні технології для дослідження домашньої Wi-Fi мережі, включаючи VLAN, сегментацію трафіку та організацію гостьового доступу, що робить її оптимальним інструментом для виконання даної роботи.

2.4 Розробка структури мережі із застосуванням VLAN

Розробка структури сучасної мережі, особливо в контексті домашньої інфраструктури, що обслуговує потреби віддаленої роботи, вимагає відходу від застарілих «плоских» моделей на користь логічної сегментації. Традиційна архітектура, де всі пристрої перебувають в одному широкомовному домені, створює надмірне навантаження на канал та значні ризики безпеки, оскільки компрометація одного вразливого IoT-пристрою дає зловмиснику доступ до всієї мережі.

При проектуванні структури мережі першочерговим завданням є визначення функціональних сегментів. Для домашнього середовища доцільно виділити щонайменше чотири типи VLAN: робочий (для корпоративних пристроїв), домашній (для персональних ґаджетів), сегмент «розумного будинку» (IoT) та гостьовий доступ. Всі VLAN з'єднуються в єдину мережу за допомогою бездротового з'єднання, окрім домашнього VLAN, який комбінує в собі дротове підключення для персонального комп'ютера [5].

Такий розподіл базується на принципі найменших привілеїв: наприклад, гостьовий сегмент повинен мати доступ лише до інтернету, не «бачачи» при цьому приватних серверів чи робочих ноутбуків власника. На практиці це реалізується шляхом трансляції різних SSID на точці доступу, де кожна бездротова мережа прив'язана до відповідного тегу VLAN [6].

Важливу роль у структурі мережі відіграє правильний розподіл IP-адрес. Для кожного VLAN використовується окрема підмережа, що спрощує адміністрування та дозволяє чітко контролювати мережевий трафік. Наприклад в межах роботи буде ір адреси будуть розподіленні так – робоча мережа має використовувати діапазон 192.168.10.0/24, а основна 192.168.20.0/24 , IoT-пристроїв – 192.168.30.0/24, гостьова – 192.168.40.0/24. Такий підхід полегшує ідентифікацію пристроїв та подальше налаштування правил безпеки. Загальну структуру схеми VLAN наведено на рисунку 2.1.

Також при розробці структури варто приділити безпеці магістральних каналів (транків). Оскільки транкові порти передають трафік багатьох VLAN одночасно, вони є критичними точками інфраструктури. Для захисту від атак типу «VLAN hopping» необхідно дотримуватися правил гігієни конфігурації:, призначати всі невикористовувані порти в ізольований «dummy» VLAN та змінювати стандартний Native VLAN (зазвичай це VLAN 1) на інший, унікальний ідентифікатор. Це гарантує, що нетегровані кадри не будуть помилково спрямовані в управлінський чи робочий сегменти [7]. Схему розподілу VLAN на оптимізованій мережі можна побачтити на рис. 2.1

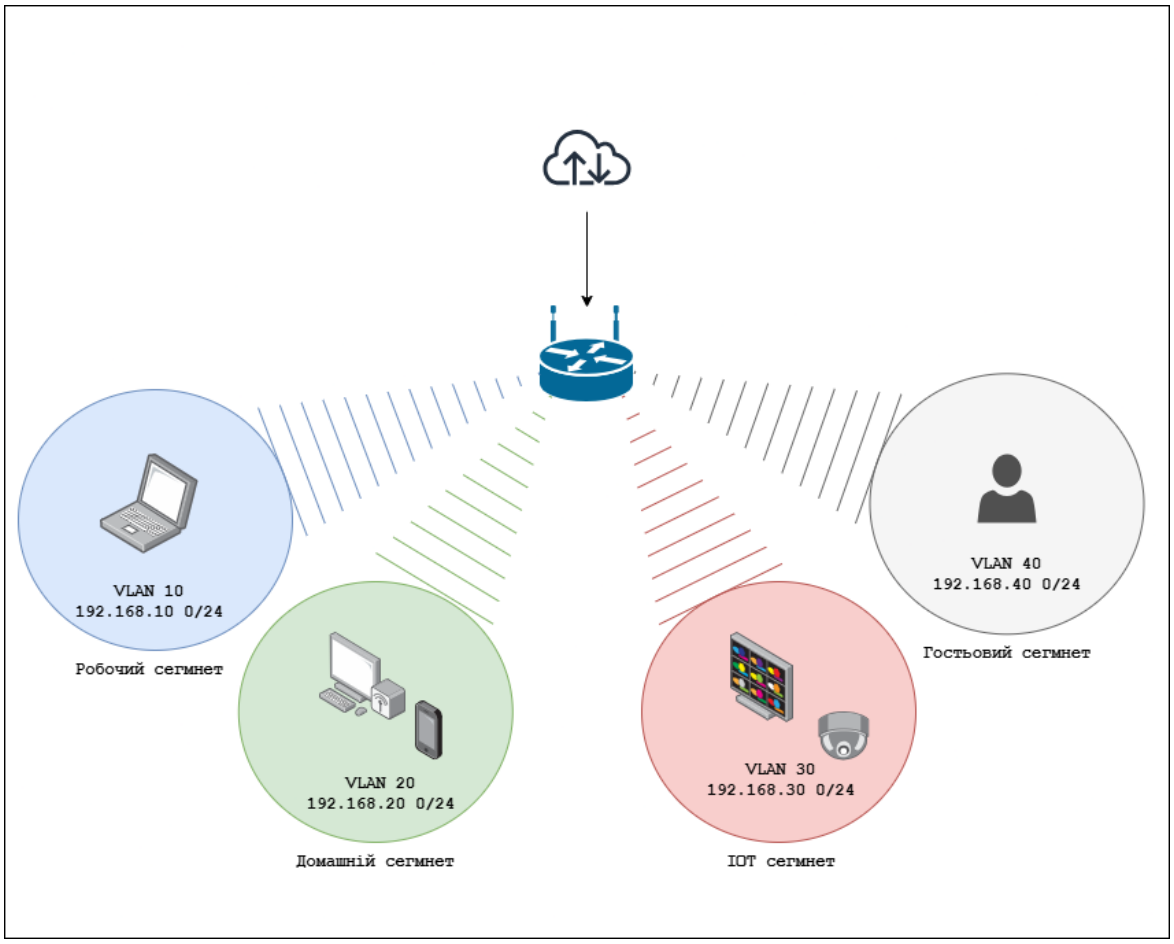

Рисунок 2.1 - Приклад оптимізованої структури VLAN

Розробка структури мережі на основі VLAN є обов'язковим кроком для оптимізації сучасного цифрового простору. Такий підхід забезпечує не лише надійну ізоляцію критичних даних та локалізацію широкомовного трафіку, а й створює гнучку основу для масштабування мережі в майбутньому.

2.5 Вибір мережевого обладнання та програмних засобів реалізації

Вибір апаратного та програмного забезпечення є фундаментом реалізації проєкту, оскільки саме технічні можливості обладнання визначають межі реалізації політик сегментації та безпеки. Для оптимізації домашньої мережі з використанням VLAN та гостьового доступу критично важливо обирати пристрої, які підтримують стандарт тегування трафіку IEEE 802.1Q та можливість трансляції кількох незалежних бездротових мереж (Multi-SSID).

Найбільш доцільним є використання інтегрованих пристроїв, що поєднують у собі функції маршрутизатора, комутатора, точки доступу та брандмауера.

Як основний мережевий пристрій було обрано маршрутизатор серії MikroTik. Обладнання цього виробника широко використовується як у невеликих офісах, так і в домашніх мережах завдяки поєднанню функціональності, стабільності та відносно невисокої вартості. Головною перевагою маршрутизаторів MikroTik є операційна система RouterOS, яка забезпечує підтримку великої кількості мережевих функцій, зокрема VLAN, QoS, VPN, гостьових мереж та механізмів фільтрації трафіку.

Для реалізації даної роботи доцільним є використання маршрутизатора MikroTik hAP ax3. Дана модель підтримує стандарт Wi-Fi 6 (802.11ax), що дозволяє ефективніше працювати з великою кількістю одночасно підключених пристроїв. Крім цього, маршрутизатор має багатоядерний процесор і достатній обсяг оперативної пам’яті для реалізації міжмережевої маршрутизації, VLAN та механізмів QoS без суттєвого зниження продуктивності.

Важливою перевагою обладнання MikroTik є гнучкість налаштування. За допомогою RouterOS можна створювати окремі VLAN для різних категорій пристроїв, налаштовувати міжсегментну маршрутизацію, обмежувати швидкість для гостьового сегмента та реалізовувати пріоритезацію трафіку. Наприклад, робочі пристрої можуть отримувати вищий пріоритет обслуговування порівняно з мультимедійним або гостьовим трафіком.

Для створення та тестування мережевої структури у роботі використовується середовище GNS3. Дана платформа дозволяє емулятувати роботу реального мережевого обладнання та перевіряти налаштування без використання фізичної інфраструктури.

Для аналізу мережевого трафіку використовується Wireshark. Програма дозволяє виконувати перехоплення та аналіз пакетів у реальному часі, що дає можливість перевіряти коректність роботи VLAN, тегування кадрів за

стандартом IEEE 802.1Q та ефективність механізмів QoS. Аналіз трафіку також допомагає виявляти перевантаження мережі або помилки конфігурації.

Для тестування продуктивності мережі можуть застосовуватись утиліти типу iPerf3, які дозволяють вимірювати швидкість передачі даних між сегментами мережі та оцінювати вплив навантаження на роботу системи. Це особливо важливо при перевірці ефективності механізмів пріоритезації трафіку та оцінці роботи мережі під час віддаленої роботи або потокової передачі даних.

Отже, оптимальним вибором для реалізації проєкту є використання, яке підтримує повний стек протоколів тегування та ізоляції трафіку. Програмний комплекс, що включає GNS3 для моделювання та Wireshark для діагностики, створює надійну базу для підтвердження правильності концепції роботи мережі.

2.6 Розробка логічної та фізичної схеми мережі

Після вибору мережевого обладнання та визначення структури VLAN наступним етапом стала розробка логічної та фізичної схеми мережі. Побудова таких схем є важливою частиною проєктування мережевої інфраструктури, оскільки дозволяє наочно відобразити взаємодію між пристроями, принципи сегментації мережі та структуру підключення обладнання. Крім цього, наявність чіткої схеми значно спрощує процес налаштування, подальшого адміністрування та пошуку можливих несправностей.

Логічна схема мережі відображає структуру взаємодії між сегментами та принцип маршрутизації трафіку незалежно від фізичного розташування пристроїв. У межах даної роботи логічна структура побудована на основі використання VLAN, що дозволяє розділити домашню мережу на окремі функціональні сегменти. Основний VLAN призначений для персональних і робочих пристроїв користувача, які потребують доступу до внутрішніх ресурсів мережі та мають підвищений рівень довіри.

План адресації розробляється на основі приватного простору IPv4 згідно з RFC 1918. Для зручності адміністрування кожному VLAN призначається окрема підмережа, де третій октет IP-адреси відповідає ідентифікатору VLAN ID. Наприклад, підмережа 192.168.10.0/24 буже відповідати VLAN 10. Керування адресацією здійснюється через DHCP-сервер, налаштований на центральному маршрутизаторі, який динамічно виділяє адреси пристроям залежно від порту підключення або SSID.

Центральним елементом логічної схеми є маршрутизатор MikroTik hAP ax3, який виконує функції міжмережевої маршрутизації, DHCP-сервера та контролю доступу між VLAN. Загальну структуру логічної схеми мережі наведено на рисунку 2.2.

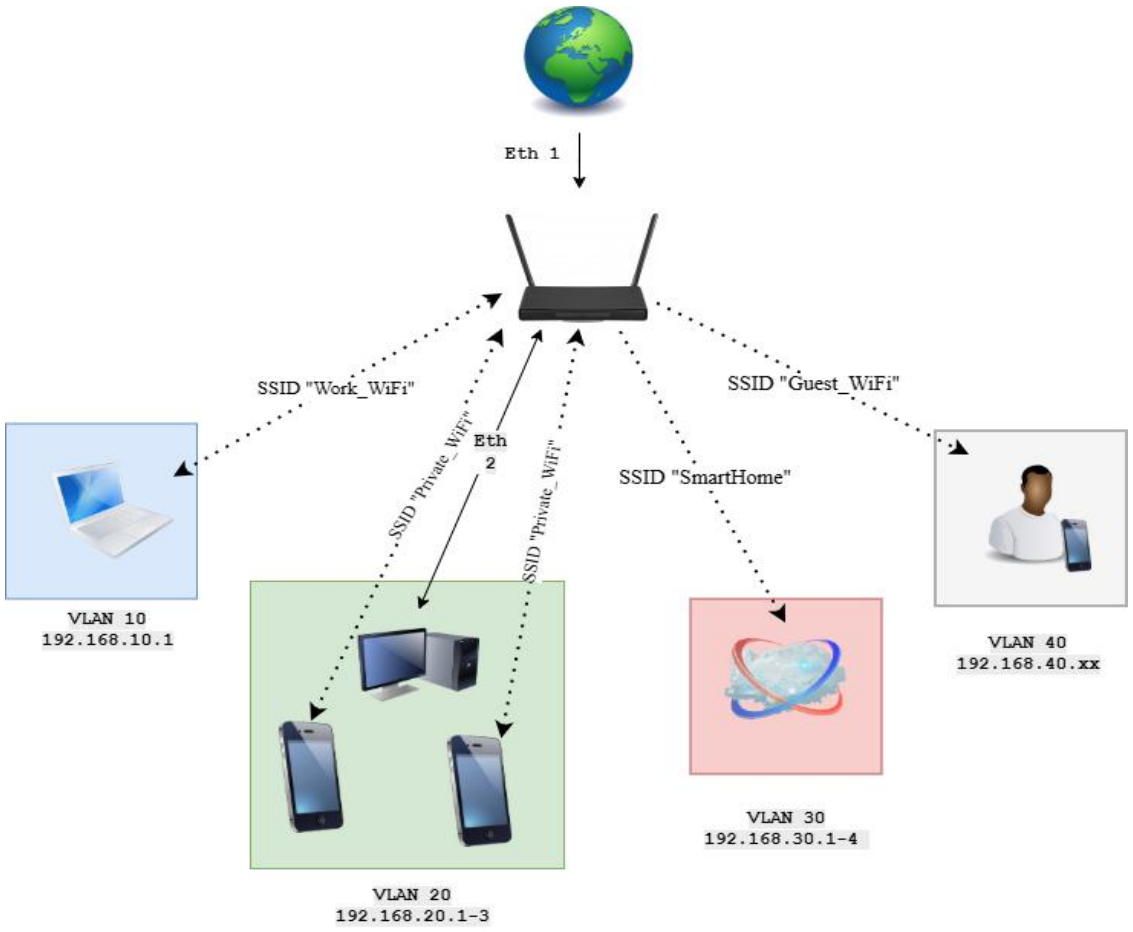

Рисунок 2.2 – Загальна структура логічної схеми мережі

Фізична структура мережі визначає реальне розміщення обладнання та типи кабельних з'єднань. Найбільш стійкою та масштабованою для домашніх умов є топологія «Зірка», де всі кінцеві вузли та точки доступу підключаються до центрального комутаційного вузла.

Під час розробки фізичної схеми мережі за основу було обрано один із найпоширеніших типів панельних квартир. Такий підхід дозволив наблизити результати моделювання до реальних умов використання домашньої Wi-Fi мережі, оскільки саме панельні будинки становлять значну частину житлового фонду.

Центральним елементом фізичної схеми є маршрутизатор MikroTik hAP ax3, який забезпечує маршрутизацію трафіку, підтримку VLAN, DHCP та бездротовий доступ до мережі. Для забезпечення максимально рівномірного покриття маршрутизатор було розташовано у центральній частині квартири. Таке розташування дозволяє мінімізувати кількість зон зі слабким сигналом та покращити стабільність бездротового з’єднання.

До маршрутизатора через Ethernet-порти підключаються окремі сегменти мережі відповідно до налаштованих VLAN. А саме саціонарні пристрої, такі як персональні комп’ютери або телевізори, використовують дротове підключення для забезпечення стабільнішої швидкості передачі даних. Мобільні пристрої та IOT підключаються через Wi-Fi, використовуючи окремі SSID для різних сегментів мережі, зокрема основної та гостьової мережі.

Фізичне середовище передавання даних базується на мідній витій парі категорій 5e або 6, що забезпечує швидкість до 1 Гбіт/с а безротові пристрої використовують частоту 5 Ггц для робочого VLAN та 2,4 Ггц для інших. Наглядне фізичне розташування пристроїв по приміщенню можна побачити на рис. 2.3.

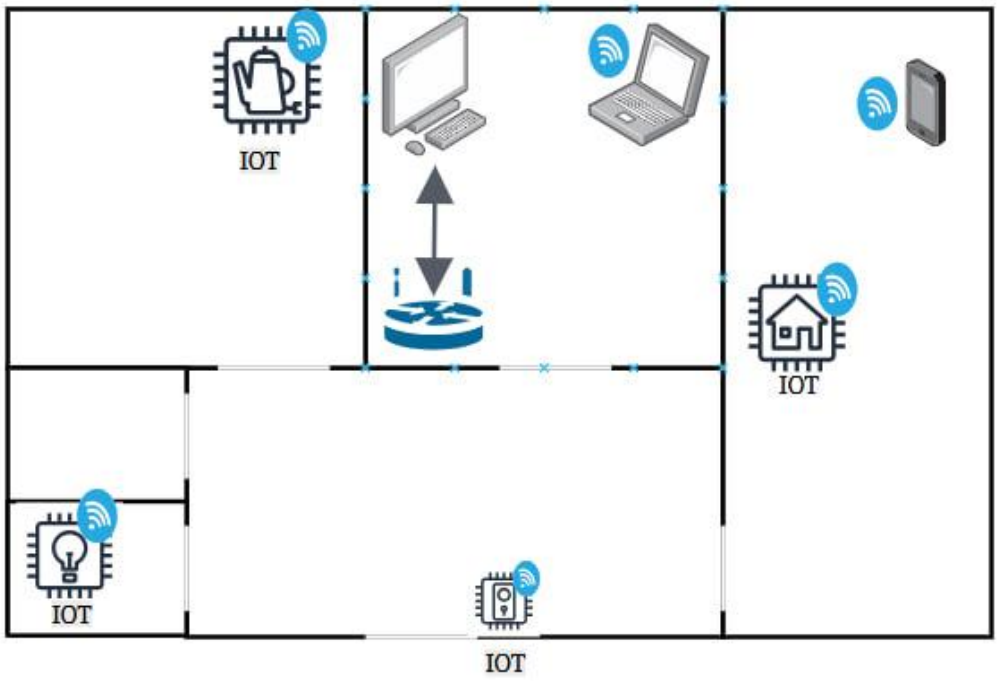

Рисунок 2.3 - Загальна структура фізичної схеми мережі

У межах даного розділу було розроблено логічну та фізичну схеми домашньої Wi-Fi мережі з використанням технології VLAN. Логічна схема дозволила реалізувати сегментацію мережі на окремі функціональні зони, зокрема основний, гостьовий та IoT-сегменти, що забезпечило підвищення рівня безпеки та більш ефективний розподіл мережевого трафіку.

Фізична схема мережі була побудована з урахуванням особливостей типового панельного житла, що дало можливість наблизити модель до реальних умов експлуатації. Таким чином, розроблена фізична схема мережі забезпечує ефективне розташування обладнання, стабільне Wi-Fi покриття та можливість реалізації сегментації мережі за допомогою VLAN. Це створює основу для ефективної та безпечної роботи домашньої мережі в умовах сучасного навантаження та активного використання цифрових сервісів.

РОЗДІЛ 3 ПРАКТИЧНА РЕАЛІЗАЦІЯ ТА ОЦІНКА ЕФЕКТИВНОСТІ МЕРЕЖІ

3.1 Реалізація мережевої моделі в середовищі GNS3

Реалізація мережевої моделі в середовищі моделювання є ключовим етапом, який дозволяє перевірити працездатність обраних рішень як «підтвердження концепції» перед їхнім впровадженням у реальну експлуатацію. Використання емулятора GNS3 забезпечує високу точність моделювання, оскільки він дозволяє запускати реальні образи операційних систем, що мінімізує розбіжності між віртуальною моделлю та фізичною мережею.

Для симуляції центрального вузла мережі, відповідального за сегментацію та маршрутизацію трафіку, було використано MikroTik RouterOS, запущений через гіпервізор QEMU. Використання QEMU дозволяє емулювати апаратне забезпечення, необхідне для повноцінної роботи RouterOS, що дає змогу налаштовувати тегування трафіку за стандартом IEEE 802.1Q та правила брандмауера для кожного VLAN. Це гарантує, що логіка розподілу трафіку між робочим, приватним та гостьовим сегментами буде ідентичною тій, що використовується на фізичних пристроях MikroTik .

Моделювання кінцевих пристроїв було реалізовано за допомогою різних інструментів, залежно від їхньої ролі в мережі:

Для симуляції персональних комп'ютерів (ПК) використано вбудовані вузли VPCS (Virtual PC Simulator). Ці легковагі вузли є ідеальними для перевірки базової мережевої зв’язності, налаштування статичних IP-адрес або перевірки отримання адрес через DHCP, а також для тестування маршрутизації за допомогою команд ping та traceroute .

Для симуляції мобільних телефонів застосовано образи TinyCore Linux із попередньо встановленим браузером Firefox. Такий підхід дозволив максимально точно змоделювати роботу сучасних смартфонів, оскільки вони

використовуються користувачами переважно для вебсерфінгу та доступу до хмарних застосунків через браузер.

Для моделювання пристроїв «розумного будинку» використано Alpine Linux у поєднанні з Python-скриптами. Оскільки реальні IoT-ґаджети зазвичай виконують обмежений набір автоматизованих функцій, запуск Python-скриптів дозволив імітувати їхню типову активність – відправку телеметричних даних або періодичні запити до серверів. Це дозволило проаналізувати вплив IoT-трафіку на мережу та підтвердити його надійну ізоляцію від робочих сегментів. На рисунку 3.1 можна побачити побудовану схему в середовищі GNS3:

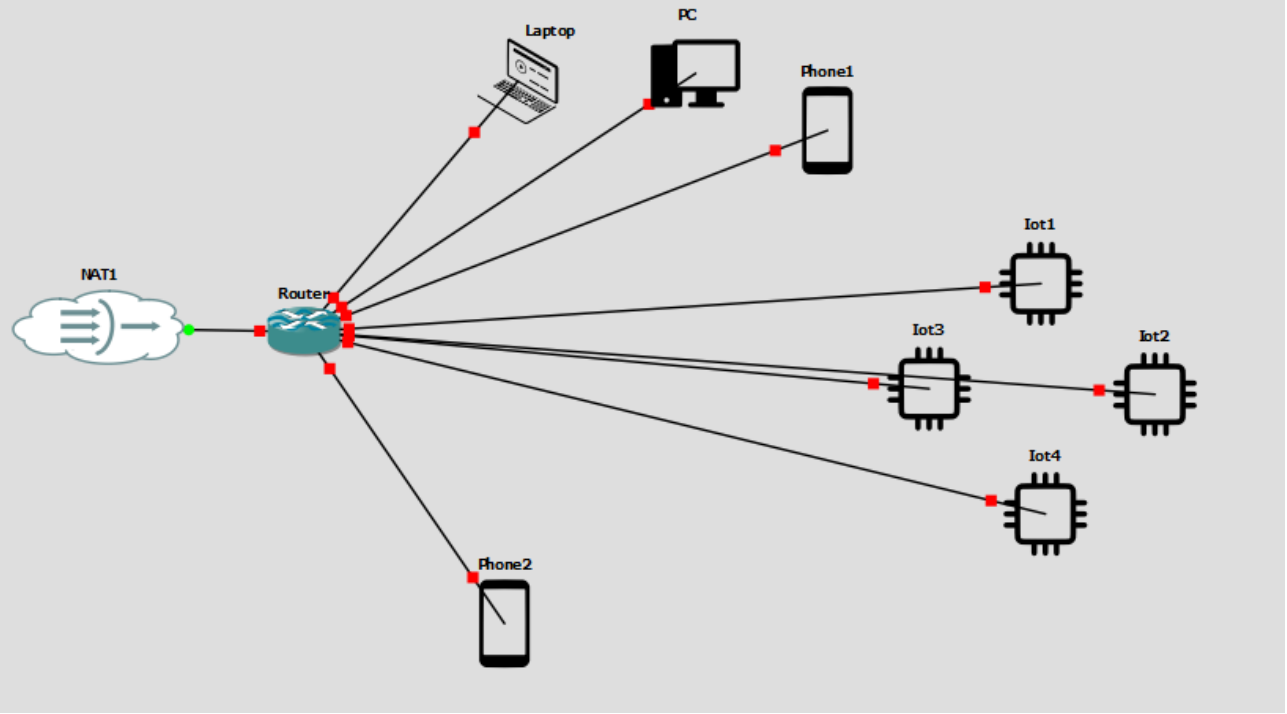

Рисунок 3.1 – Приклад мережі в середовищі GNS3.

Підсумовуючи, створення такого середовища в GNS3 дозволило не лише візуалізувати топологію, а й детально проаналізувати взаємодію різних типів пристроїв у межах сегментованої мережі.

3.2 Налаштування VLAN та сегментації мережі

Одним із ключових етапів реалізації домашньої Wi-Fi мережі стало налаштування VLAN та сегментації мережевого середовища. Основною метою даного процесу було розділення мережі на окремі логічні сегменти для підвищення рівня безпеки, зменшення широкомовного трафіку та забезпечення більш ефективного керування мережевими ресурсами. У межах цього етапу налаштування виконувалося на базі операційної системи MikroTik RouterOS, яка надає гнучкі інструменти для керування віртуальними мережами та безпекою на рівні ядра системи .

Процес налаштування розпочався з базової підготовки пристрою та організації доступу до зовнішньої мережі. Першим кроком було активовано DHCP-клієнт на інтерфейсі ether1, що дозволило роутеру автоматично отримати публічну IP-адресу від інтернет-провайдера.По замовчуванню цей DHCP-клієнт уже розгорнутий на інтерйвейсі ether1 , але якщо є якісь несправності його можна розгорнути за допомогою команди зображеної у лістингу 3.1.

```
/ip dhcp-client add interface=ether1 disabled=no
```

Лістинг 3.1 – Налаштування WAN-інтерфейсу

Після цього було створено програмний комутатор bridge1 із увімкненим режимом vlan-filtering. Bridge у RouterOS виконує роль внутрішнього комутатора та об’єднує фізичні інтерфейси в єдине комутаційне середовище. Увімкнення параметра vlan-filtering дозволяє реалізувати підтримку VLAN та виконувати фільтрацію трафіку відповідно до правил сегментації.

На наступному етапі LAN-порт ether2 та wlan порти були додані до bridge1. Це дало можливість використовувати їх як порти внутрішнього комутатора та надалі прив’язати кожен із них до окремого VLAN. Такий підхід

дозволяє фізично розділити мережеві сегменти між різними групами пристроїв.

```
# Створення bridge
/interface bridge
add name=bridge1 vlan-filtering=yes
# Додавання LAN-портів до bridge
/interface bridge port
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=wlan1
add bridge=bridge1 interface= wlan2
add bridge=bridge1 interface= wlan3
add bridge=bridge1 interface= wlan3
add bridge=bridge1 interface= wlan3
add bridge=bridge1 interface= wlan3
add bridge=bridge1 interface=wlan4
```

Лістинг 3.2 – Створення bridge та додавання LAN-портів до bridge

Далі було створено логічні VLAN-інтерфейси: vlan10, vlan20, vlan30 та vlan40. Кожен із них отримав власний VLAN ID і був прив’язаний до bridge1. Завдяки цьому маршрутизатор зміг обробляти трафік окремо для кожного сегмента мережі. У межах даної роботи VLAN використовувалися для розділення домашньої мережі за функціональним призначенням пристроїв, наприклад робочого сегмента, IoT-пристроїв або гостьового доступу.

Після створення VLAN було налаштовано IP-адресацію. Кожен VLAN отримав власну IP-підмережу та адресу шлюзу за замовчуванням. Наприклад, для vlan10 використовувалася мережа 192.168.10.0/24 із шлюзом 192.168.10.1. Такий підхід забезпечує логічну ізоляцію сегментів і спрощує подальше адміністрування мережі.

Наступним кроком стало налаштування правил VLAN на bridge. Для кожного фізичного порту було визначено відповідний VLAN ID у режимі untagged.

```
#Створення VLAN-інтерфейсів
/interface vlan
add name=vlan10_work interface=bridge1 vlan-id=10
add name=vlan20_main interface=bridge1 vlan-id=20
add name=vlan30_iot interface=bridge1 vlan-id=30
add name=vlan40_guest interface=bridge1 vlan-id=40
#Налаштування IP-адрес VLAN
/ip address
add address=192.168.10.1/24 interface=vlan10
add address=192.168.20.1/24 interface=vlan20
add address=192.168.30.1/24 interface=vlan30
add address=192.168.40.1/24 interface=vlan40
# Прив’язка VLAN до фізичних портів
/interface bridge vlan
add bridge=bridge1 vlan-ids=10 untagged=wlan1
add bridge=bridge1 vlan-ids=20 untagged=ether2,wlan2
add bridge=bridge1 vlan-ids=30 untagged=wlan3
add bridge=bridge1 vlan-ids=40 untagged=wlan4
```

Лістинг 3.3 – Створення VLAN-інтерфейсів ,налаштування IP-адрес VLAN та прив’язка VLAN до портів.

Паралельно налаштовано системний DNS-сервер (8.8.8.8) для коректного розв'язання доменних імен. Заключним етапом стала автоматизація адресації: для кожного VLAN створено окремі пули адрес та сервери DHCP. Тепер будь-який ґаджет при підключенні до порту або

відповідного SSID автоматично отримує коректну IP-адресу, маску підмережі та адресу шлюзу, що відповідає його рівню доступу.

```
# Налаштування DNS-серверів
/ip dns
set servers=8.8.8.8,1.1.1.1 allow-remote-requests=yes
# Створення пулів IP-адрес для DHCP
/ip pool
add name=pool10 ranges=192.168.10.10-192.168.10.254
add name=pool20 ranges=192.168.20.10-192.168.20.254
add name=pool30 ranges=192.168.30.10-192.168.30.254
add name=pool40 ranges=192.168.40.10-192.168.40.254
# Налаштування DHCP-серверів
/ip dhcp-server
add name=dhcp10 interface=vlan10 address-pool=pool10
add name=dhcp20 interface=vlan20 address-pool=pool20
add name=dhcp30 interface=vlan30 address-pool=pool30
add name=dhcp40 interface=vlan40 address-pool=pool40
#Налаштування DHCP network
/ip dhcp-server network
add address=192.168.10.0/24 gateway=192.168.10.1 dns-server=8.8.8.8
add address=192.168.20.0/24 gateway=192.168.20.1 dns-server=8.8.8.8
add address=192.168.30.0/24 gateway=192.168.30.1 dns-server=8.8.8.8
add address=192.168.40.0/24 gateway=192.168.40.1 dns-server=8.8.8.8
```

Лістинг 3.4 Повна схема налаштування DHCP-серверів для роздачі адрес VLAN сегиентам.

Наведена послідовність кроків дозволила трансформувати звичайний роутер MikroTik на потужний вузол безпеки. Використання механізму vlan-filtering у поєднанні з автоматизацією DHCP забезпечує надійну ізоляцію

критичних даних. Такий підхід гарантує, що гостьовий трафік або потенційно вразливі IoT-пристрої залишатимуться в межах своїх логічних кордонів.

3.3 Конфігурація гостьового доступу

Налаштування брандмауера (firewall) є завершальним і критично важливим етапом налаштування мережі, оскільки сама по собі сегментація через VLAN лише розділяє широкомовні домени, але не забороняє маршрутизацію трафіку між ними. Наведені вами команди MikroTik RouterOS реалізують стратегію «найменших привілеїв», перетворюючи гостьовий сегмент на ізольовану мережу.

Налаштування доступу відбуваються на консолі маршрутизатора за допомогою вбудованого файрволу.

Першим правилом дозволяється вихід гостьових пристроїв у глобальну мережу Інтернет через WAN-інтерфейс ether1. Це забезпечує базову функціональність гостьового доступу, дозволяючи користувачам використовувати веб-сервіси, месенджери та інші онлайн-ресурси.

Другим правилом реалізується заборона доступу до внутрішніх підмереж локальної мережі. Для цього використовується блокування трафіку з гостьової підмережі 192.168.40.0/24 до адресного простору 192.168.0.0/16. Такий підхід гарантує повну ізоляцію гостьового сегмента від основної мережі та пристроїв користувача, що є важливим елементом інформаційної безпеки.

Третє правило обмежує доступ гостьових пристроїв безпосередньо до самого маршрутизатора. Це означає, що користувачі гостьової мережі не можуть отримати доступ до адміністративних сервісів, змінювати налаштування або використовувати внутрішні служби управління. Це запобігає спробам гостей підібрати пароль до роутера (брутфорс), сканувати порти пристрою або втручатися в його конфігурацію.

Всі правила зображено на лістингу 3.5 та 3.6.

```
/ip firewall filter
add chain=forward src-address=192.168.40.0/24 out-interface=ether1
action=accept
```

Лістинг 3.5 – Правило яке дає доступ гостьовим користувачам до інтернету.

```
#Друге правило
/ip firewall filter
add chain=forward src-address=192.168.40.0/24 dst-address=192.168.0.0/16
action=drop
#Третє правило
/ip firewall filter
add chain=input src-address=192.168.40.0/24 action=drop
```

Лістинг 3.6 – Правила які обмежують доступ до локальної мережі та роутеру.

Реалізована конфігурація гостьового доступу забезпечує баланс між зручністю використання та рівнем безпеки. Гостьові користувачі отримують можливість підключення до Інтернету без обмежень на рівні сервісів, проте повністю ізольовані від внутрішньої інфраструктури мережі.

3.4 Проведення тестування мережі

Після завершення налаштування VLAN, гостьового доступу та механізмів маршрутизації було проведено тестування розробленої мережі з метою перевірки її працездатності, коректності сегментації та ефективності ізоляції трафіку.

Першим етапом тестування стала перевірка базової зв’язності між пристроями в межах одного VLAN. Для цього використовувався стандартний інструмент ICMP (ping). Результати показали, що пристрої всередині одного сегмента успішно обмінюються пакетами без втрат і з мінімальною затримкою.

Далі було проведено тестування гостьового сегмента мережі. З гостьового пристрою виконувалася перевірка доступу до зовнішніх ресурсів за допомогою ping до публічних IP-адрес, зокрема шлюзу провайдера та DNS-серверів. Результати підтвердили, що мережа має повноцінний доступ до Інтернету.

Окремо було виконано перевірку ізоляції гостьового VLAN від внутрішньої мережі. Для цього з гостьового сегмента здійснювалися спроби ping до адрес інших внутрішніх підмереж (192.168.10.0/24, 192.168.20.0/24). У всіх випадках запити не отримували відповіді, що підтверджує коректну роботу правил firewall та повну ізоляцію гостьового доступу.

Оскільки у віртуальній та лабораторній моделі відсутній фізичний мережевий аналізатор на рівні комутатора , для захоплення пакетів застосовувався вбудований інструмент MikroTik Sniffer. Це дозволило виконати перехоплення трафіку безпосередньо на маршрутизаторі та проаналізувати структуру кадрів.

За допомогою Sniffer було підтверджено правильність тегування VLAN. Додатково було проаналізовано проходження ICMP-пакетів між VLAN та їх маршрутизацію через центральний маршрутизатор.

Такий підхід дозволив підтвердити, що гостьовий трафік справді маркується відповідним ідентифікатором VLAN ID та не змішується з іншими потоками даних у магістральному каналі, забезпечуючи високий рівень інформаційної безпеки .

3.5 Порівняльний аналіз параметрів мережі до та після оптимізації

Порівняльний аналіз параметрів мережі виконувався з метою оцінки ефективності впровадження VLAN-сегментації та механізмів оптимізації трафіку. Основна увага приділялася зміні характеру мережевого навантаження, кількості широкомовних пакетів , а також загальній стабільності передачі даних у мережі до та після налаштування.

Для проведення аналізу використовувалися інструменти моніторингу та захоплення трафіку. У режимі аналізу без VLAN застосовувався Wireshark, який дозволив дослідити загальний потік пакетів у мережі та визначити характер взаємодії пристроїв у спільному широкомовному домені. Після впровадження VLAN додатково використовувався вбудований інструмент MikroTik Sniffer на маршрутизаторі MikroTik, що дало можливість проаналізувати трафік безпосередньо на рівні мережевого обладнання, включно з маркуванням VLAN та розподілом пакетів між сегментами.Також для фіксування швидкості передачі даних та кількості перевідправлених пакетів використовувалася утиліта iPerf3.

Результати тестування до оптимізації показали високу кількість широкомовних пакетів у мережі. У середньому фіксувалося близько 130 пакетів за 30 секунд, значна частина яких припадала на broadcast-трафік.Середня пропускна здатність становила близько 1,17 Мбіт/с, при цьому зафіксовано 219 повторних передач пакетів. Велика кількість повторних передач свідчить про наявність перевантаження мережі, виникнення колізій та необхідність повторної відправки пакетів через втрати під час передачі даних.

Після впровадження VLAN ситуація суттєво змінилася. Завдяки логічному поділу мережі на окремі сегменти кількість широкомовних пакетів у кожному VLAN зменшилася приблизно до 30 пакетів за 30 секунд. Це свідчить про значне скорочення broadcast-домену та більш ефективну локалізацію трафіку в межах відповідних сегментів.

Результати вимірювання за допомогою iPerf3 показали середню швидкість передачі на рівні 1,29 Мбіт/с для передавальної сторони та 1,17 Мбіт/с для приймальної сторони. При цьому кількість повторних передач зменшилася до 27 пакетів, що майже у вісім разів менше порівняно з початковими показниками.

Окрім аналізу мережевого трафіку, було виконано моніторинг завантаження центрального процесора маршрутизатора під час тестування. До впровадження сегментації мережі середнє завантаження CPU становило

близько 27 %, що було пов’язано з обробкою широкомовного трафіку та передачею даних у межах одного широкомовного домену. Після реалізації VLAN і розподілу пристроїв між окремими сегментами завантаження процесора знизилося до 19 % тобто на 8 процентних пунктів. Отримані результати свідчать про зменшення навантаження на маршрутизатор приблизно на 30 %, що пояснюється локалізацією широкомовного трафіку та більш ефективною організацією передачі даних між мережевими сегментами. Зниження використання процесорних ресурсів також створює додатковий запас продуктивності для подальшого розширення мережі та впровадження додаткових сервісів без необхідності модернізації обладнання.Загальні зміни в роботі мереж продемонстровано на порівняльній таблиці 3.1

Таблиця 3.1 – Порівняльна таблиця мереж після та до оптимізації

Характеристика	Плоска мережа	Оптимізована мережа
Кількість широкомовних пакетів за 30 с.	130	30
Швидкість передачі Мбіт/с	1.17 Мбіт/с	1.29 Мбіт/с
Кількість повторних передач	219	27
Навантаженість CPU маршрутизатора	27%	19%

Аналіз за допомогою Wireshark та MikroTik Sniffer також показав, що після оптимізації трафік чітко розподіляється між VLAN та містить відповідні мітки IEEE 802.1Q. Це підтверджує коректність роботи механізму сегментації та правильність конфігурації мережевого обладнання. Результати тестування за допомогою iPerf3 підтверджують позитивний вплив впроваджених рішень на якість передачі даних. Найбільш показовим результатом стало значне зменшення кількості повторних передач пакетів – з 219 до 27, що свідчить про підвищення стабільності мережі та більш ефективне використання доступної пропускної здатності каналу.

3.6 Оцінка ефективності впроваджених рішень

На основі проведеного моделювання, конфігурації та тестування мережевої інфраструктури, можна зробити висновок, що впроваджені рішення забезпечили комплексне досягнення поставлених цілей: підвищення рівня безпеки, покращення продуктивності та забезпечення масштабованості домашньої мережі для потреб віддаленої роботи. Перехід від традиційної «плоскої» архітектури до сегментованої мережі на основі VLAN дозволив кардинально покращити параметри середовища передавання даних.

Локалізація широкомовного трафіку: Впровадження VLAN розділило єдиний великий широкомовний домен на чотири ізольовані логічні сегменти. Це дозволило обмежити поширення службових кадрів (ARP, DHCP) межами конкретного VLAN.

Використання VLAN у поєднанні з правилами брандмауера створило багаторівневу систему захисту:

Налаштовані правила action=drop у ланцюжку forward MikroTik RouterOS гарантують, що пристрої в гостьовому VLAN 40 мають доступ лише до інтернету і не можуть ініціювати з'єднання з робочим або приватним сегментами. Це повністю нівелює загрозу «латерального переміщення» зловмисника всередині мережі.

Блокування доступу до IP-адрес роутера (ланцюжок input) для гостьової та IoT-мереж запобігає спробам несанкціонованої зміни конфігурації .

У разі потреби додавання нових функціональних зон, це реалізується програмно через створення нового VLAN ID без закупівлі додаткового апаратного забезпечення.

Розгортання окремих DHCP-серверів для кожного сегмента спростило адміністрування та забезпечило автоматичне призначення пристроїв у відповідні зони довіри залежно від SSID підключення.

Використання технології віртуалізації локальної мережі дозволило замінити кілька фізичних пристроїв одним потужним багатофункціональним

маршрутизатором MikroTik, що суттєво знизило капітальні витрати на побудову інфраструктури.

На основі проведених тестів в минулому розділі можна побачити вагомий приріст в ефективності передачі пакетів, а саме зменшення широкомовних запитів та повторних передач пакетів, детальну інформацію щодо ефективності впроваджених рішень в відсотках можна побачити на рис.3.2.

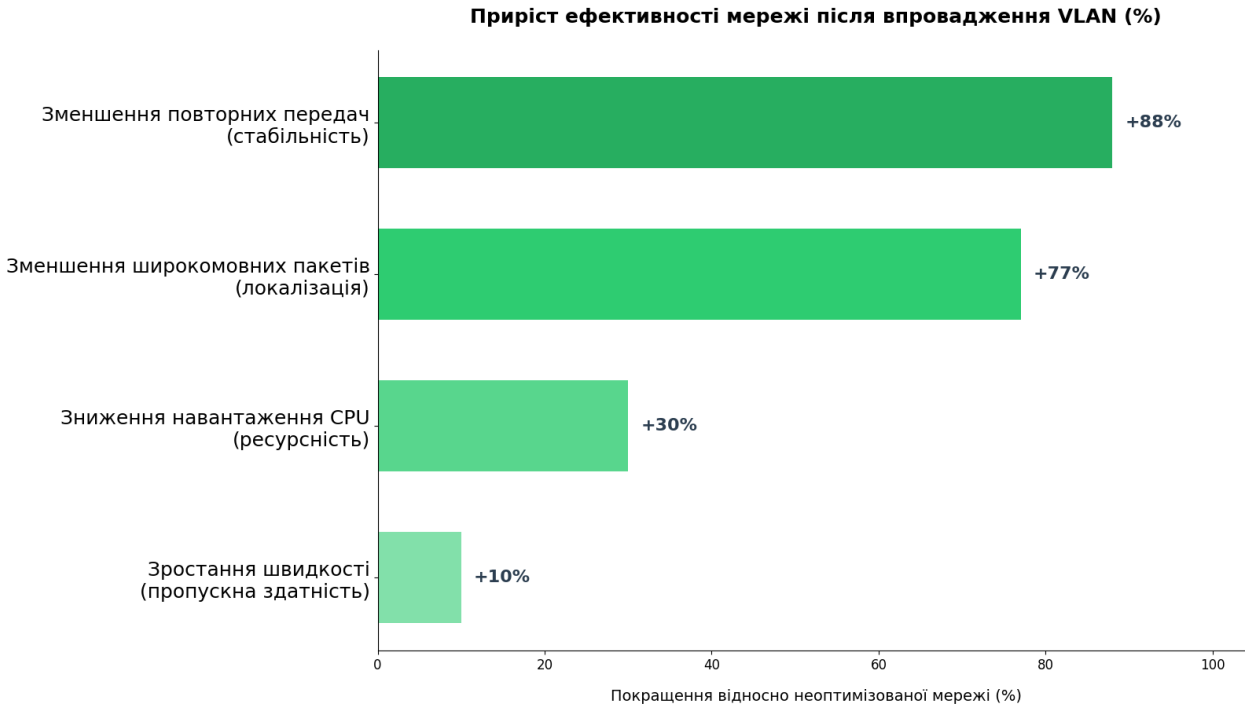

Рисунок 3.2 – Графік приросту ефективності відносно звичайної мережі.

Можна зробити висновок, що впроваджені рішення є ефективними та доцільними для використання в умовах сучасної домашньої Wi-Fi мережі. Поєднання VLAN-сегментації, гостьового доступу та базових механізмів контролю трафіку дозволяє підвищити продуктивність, стабільність та безпеку мережевої інфраструктури без суттєвого ускладнення її експлуатації.

ВИСНОВКИ

У ході виконання роботи було досліджено особливості проєктування та оптимізації домашніх бездротових мереж для забезпечення стабільної та безпечної роботи користувачів в умовах віддаленої роботи. Актуальність обраної тематики обумовлена стрімким зростанням кількості мережевих пристроїв у домашніх мережах, збільшенням обсягів передаваних даних та підвищенням вимог до інформаційної безпеки.

У результаті проведеного аналізу сучасних технологій бездротового доступу було розглянуто принципи побудови домашніх Wi-Fi мереж, основні стандарти бездротового зв’язку, механізми маршрутизації та засоби забезпечення мережевої безпеки.

Для перевірки запропонованих рішень було виконано моделювання роботи оптимізованої домашньої мережі із застосуванням сучасних програмних засобів. У середовищі GNS3 створено повноцінний випробувальний стенд, який включає маршрутизатор MikroTik RouterOS, комутаційне обладнання та кінцеві вузли різних категорій. Побудована модель дозволила максимально наблизити умови тестування до реальної мережевої інфраструктури та провести практичну перевірку ефективності розроблених рішень.

У процесі моделювання було реалізовано сегментацію мережі за допомогою технології VLAN, що забезпечило логічне розділення користувацьких пристроїв, IoT-обладнання, гостьових клієнтів та адміністративного сегмента. Такий підхід дозволив зменшити кількість широкомовного трафіку, підвищити рівень інформаційної безпеки та спростити управління мережевими ресурсами. Крім того, сегментація забезпечила можливість гнучкого масштабування мережі без необхідності суттєвої зміни її структури.

Особливу увагу було приділено питанням мережевої безпеки. На базі операційної системи MikroTik RouterOS розроблено рекомендації щодо

налаштування міжмережевого екрана Firewall із застосуванням принципу найменших привілеїв. Запропоновані правила фільтрації забезпечують контроль доступу між VLAN-сегментами, захист від несанкціонованих підключень та обмеження потенційних загроз з боку зовнішніх і внутрішніх джерел. Реалізація таких механізмів дозволяє суттєво підвищити рівень захищеності домашньої мережі та мінімізувати ризики компрометації інформаційних ресурсів.

На основі проведеного аналізу та результатів моделювання також сформовано практичні рекомендації щодо вибору мережевого обладнання для побудови сучасної домашньої Wi-Fi мережі. Визначено доцільність використання керованих комутаторів, маршрутизаторів із підтримкою VLAN та сучасних точок доступу, що забезпечують високу продуктивність, масштабованість і можливість централізованого управління мережею.

Отримані результати підтвердили ефективність використання сегментації мережі, механізмів міжмережевого екранування та сучасних підходів до проєктування домашніх Wi-Fi мереж. Запропоновані рішення дозволяють підвищити рівень безпеки, покращити стабільність бездротового зв’язку, зменшити вплив широкомовного трафіку та забезпечити більш ефективне використання мережевих ресурсів.

Практичне значення роботи полягає в можливості використання розроблених рекомендацій під час проєктування, модернізації та адміністрування домашніх і малих офісних бездротових мереж. Запропоновані підходи можуть бути адаптовані до різних сценаріїв використання та забезпечують основу для подальшого розвитку мережевої інфраструктури відповідно до сучасних вимог продуктивності та інформаційної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. 8th ed. Hoboken : Pearson, 2021. 800 p..

2. Все, що потрібно знати про бездротові мережі WLAN: побудова, безпека та керування. Netwave : веб-сайт. URL: https://netwave.ua/blog/vse-shcho-potribno-znaty-pro-bezdrotovi-merezhi-wlan-pobudova-bezpeka-ta-keruvannya/ (дата звернення: 10.01.2026).

3. IEEE 802.11. Runmodule : веб-сайт. URL: https://runmodule.com/2026/05/05/ieee-802-11/ (дата звернення: 10.06.2026).

4. The Most Common Wi-Fi Standards and Types, Explained. How-To Geek : веб-сайт. URL: https://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/ (дата звернення: 15.01.2026).

5. Switching, Routing, and Wireless Essentials Companion Guide (CCNAv7). Hoboken : Cisco Press, 2020. 640 p..

6. Kallatsa M. Strategies for network segmentation : a systematic literature review : Master thesis. University of Jyväskylä, 2024. URL: https://jyx.jyu.fi/jyx/Record/jyx_123456789_92952# (дата звернення: 10.02.2026).

7. Бездротовий маршрутизатор] Що таке VLAN і як налаштувати його в бездротовому маршрутизаторі ASUS? ASUS Україна. 9 лип. 2025. URL: https://www.asus.com/ua-ua/support/faq/1049415/ (дата звернення: 14.03.2026).

8. Toivakka J. Network segmentation : Bachelor’s thesis. South-Eastern Finland University of Applied Sciences, 2018. 35 p. URL: https://www.theseus.fi/bitstream/handle/10024/158766/Toivakka_Jussi_opinnaytetyo.pdf (дата звернення: 31.03.2026).