Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування закладу вищої освіти)

Факультет комп'ютерних та інформаційних технологій
(повне найменування факультету)

Кафедра комп'ютерної інженерії та кібербезпеки
(повне найменування кафедри)

КВАЛІФІКАЦІЙНА РОБОТА ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «БАКАЛАВР»

КОМП'ЮТЕРНА МЕРЕЖА З БЕЗПРОВОДОВИМ СЕГМЕНТОМ

COMPUTER NETWORK WITH A WIRELESS SEGMENT

спеціальність 123 Комп'ютерна інженерія
(шифр і назва спеціальності)

освітня програма Комп'ютерна інженерія
(назва освітньої програми)

Виконав: здобувач вищої освіти групи КІс-21
Гальчун Роман Олександрович

(підпис)

Керівник:
Керівник: к.е.н., доцент
Гордєєва Дар'я Валеріївна

(підпис)

Кваліфікаційну роботу
допущено до захисту
« _____ » червня 2023 р.
Гарант освітньої програми:
к.т.н., доцент
Лавренчук Світлана Василівна

(підпис)

Луцьк – 2023 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *комп'ютерних та інформаційних технологій*
Кафедра *комп'ютерної інженерії та кібербезпеки*
Ступінь вищої освіти: *бакалавр*
Галузь знань: *12 Інформаційні технології*
Спеціальність: *123 Комп'ютерна інженерія*
Освітня програма: *«Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ проф. Н.Чернящук
« _____ » _____ 2023 р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧУ ВИЩОЇ ОСВІТИ

Гальчуну Роману Олександровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи *Комп'ютерна мережа з безпроводовим сегментом*

Керівник роботи *к.е.н., доцент Гордєєва Дар'я Валеріївна*

затверджені наказом закладу вищої освіти від «28» грудня 2022 року № 982/01-02
2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 01.06.2023р.

3. Вихідні дані до роботи *Джерелом розробки є науково-технічна література та публікації в періодичних виданнях з даного питання, опубліковані зарубіжні та вітчизняні роботи в даній області та різні інтернет-ресурси технічного спрямування*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити):
Вступ
Аналіз сучасного стану проблеми, існуючих методів та засобів для систем аутентифікації за допомогою візуальної криптографії, розробка та тестування прототипу, оцінка результатів дослідження.
Висновки

5. Перелік графічного (ілюстративного) матеріалу:

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис	
		завдання видав	завдання прийняв
Аналіз проблеми за темою роботи та постановка завдань дослідження	*Гордєєва Д.В., доцент*		
Теоретичне дослідження та практична реалізація	*Гордєєва Д.В., доцент*		
Проєктування комп'ютерної мережі з безпроводовим сегментом	*Гордєєва Д.В., доцент*		
Висновки	*Гордєєва Д.В., доцент*		

7. Дата видачі завдання 01.11.2022 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	*Розділ 1 Аналітична частина*	До 15.11.2022 р.	
2.	*Розділ 2 Проєктування комп'ютерної мережі з безпроводовим сегментом*	До 15.12.2022 р.	
3.	*Розділ 3 Реалізація та дослідження ефективності мережі*	До 02.03.2023 р.	
4.	*Висновки та пропозиції*	До 02.04.2023 р.	
5.	*Формування списку використаних джерел*	До 15.04.2023 р.	
6.	*Формування додатків*	До 02.05.2023 р.	
7.	*Оформлення ілюстративного матеріалу*	До 15.05.2023 р.	
8.	*Нормоконтроль*	До 25.05.2023 р.	
9.	*Інструментальна перевірка на академічний плагіат*	До 01.06.2023 р.	
10.	*Представлення кваліфікаційної роботи бакалавра до захисту*	До 07.06.2023 р.	

Здобувач вищої освіти _____ Гальчун Р.О.
(підпис) (прізвище, ініціали)

Керівник кваліфікаційної роботи _____ Гордєєва Д.В.
(підпис) (прізвище, ініціали)

АНОТАЦІЯ

Гальчун Р.О. Комп’ютерна мережа з безпроводовим сегментом. Рукопис.

Кваліфікаційна робота бакалавра ОП «Комп’ютерна інженерія» спеціальності 123 Комп’ютерна інженерія. Луцький національний технічний університет. Луцьк, 2023.

Кваліфікаційна робота складається з вступу, трьох розділів, висновків, списку використаних джерел, додатків.

У першому розділі здійснено аналіз основних принципів побудови комп’ютерних мереж, сучасних мережевих стандартів, протоколів передавання даних та технологій безпроводового доступу.

У другому розділі проведено проєктування комп’ютерної мережі з безпроводовим сегментом, включаючи розробку фізичної та логічної структури, вибір мережевого обладнання, планування IP-адресації, VLAN-сегментацію та розміщення точок доступу Wi-Fi.

У третьому розділі здійснено практичну реалізацію спроєктованої мережі, налаштування активного мережевого обладнання та механізмів захисту безпроводового сегмента.

Об’єкт дослідження – локальна комп’ютерна мережа з інтегрованим безпроводовим сегментом.

Предмет дослідження – методи проєктування, реалізації та забезпечення ефективної й безпечної роботи комп’ютерних мереж із безпроводовим доступом.

Метою роботи є проєктування та практична реалізація комп’ютерної мережі з безпроводовим сегментом, яка забезпечує необхідний рівень продуктивності, надійності та інформаційної безпеки, а також оцінювання її ефективності в реальних умовах експлуатації.

Ключові слова: комп’ютерна мережа, безпроводовий сегмент, Wi-Fi, VLAN, IP-адресація, мережева безпека, WPA3, маршрутизація, моніторинг мережі.

ABSTRACT

Galchun R. Computer network with a wireless segment. Manuscript.

Qualification work of the bachelor of the specialty "Computer Engineering" specialty 123 Computer Engineering. Lutsk National Technical University. Lutsk, 2025.

The qualification work consists of an introduction, three chapters, conclusions, a list of sources used, and appendices.

The first section analyzes the basic principles of building computer networks, modern network standards, data transmission protocols and wireless access technologies.

The second section designs a computer network with a wireless segment, including the development of a physical and logical structure, the selection of network equipment, planning IP addressing, VLAN segmentation and placement of Wi-Fi access points.

The third section implements the practical implementation of the designed network, configures active network equipment and wireless segment protection mechanisms.

The object of the study is a local computer network with an integrated wireless segment.

The subject of the study is methods for designing, implementing and ensuring the effective and secure operation of computer networks with wireless access.

The purpose of the work is to design and practical implementation of a computer network with a wireless segment, which provides the required level of performance, reliability and information security, as well as to evaluate its effectiveness in real operating conditions.

Keywords: computer network, wireless segment, Wi-Fi, VLAN, IP addressing, network security, WPA3, routing, network monitoring.

ЗМІСТ

ВСТУП

Сучасний етап розвитку інформаційних технологій характеризується стрімким розширенням цифрових сервісів, інтенсивним зростанням обсягів переданих даних та інтеграцією інформаційних систем у практично всі сфери діяльності людини. У цьому контексті комп’ютерні мережі виступають ключовим елементом інформаційної інфраструктури, забезпечуючи обмін даними, доступ до ресурсів, сервісів та віддалених систем. Особливої актуальності набувають дослідження та розробка мережевих архітектур, що включають безпроводові сегменти, оскільки вони забезпечують мобільність, масштабованість, швидке розгортання та адаптивність мережі без необхідності фізичної кросової інфраструктури. Бездротові мережі стали базовою складовою корпоративних, навчальних, муніципальних та домашніх систем, а їх ефективне проєктування є критично важливим для забезпечення надійного функціонування сучасних цифрових платформ.

Підвищені вимоги до пропускної здатності, стабільності роботи, кіберзахищеності, мінімізації затримок та доступності каналів зв’язку зумовлюють необхідність формування оптимальних підходів до побудови мережевих рішень, які поєднують дротову та бездротову інфраструктуру. У результаті від фахівців очікується не лише опанування класичних принципів мережевої інженерії, а й здатність застосовувати сучасні технічні стандарти, протоколи безпеки, інструменти моніторингу, сканування трафіку та реакції на загрози. Тому розробка комп’ютерної мережі з безпроводовим сегментом є актуальною науково-практичною задачею, що має важливе значення як для теорії, так і для практики побудови інфраструктурних рішень у сфері інформаційних технологій.

Об’єктом дослідження є комп’ютерна мережа як комплексна система передавання, обробки, маршрутизації та доступу до інформаційних ресурсів.

Предметом дослідження є методи, технічні рішення, моделі, архітектурні підходи та інструменти побудови комп’ютерної мережі з безпроводовим сегментом, що забезпечують її ефективність, масштабованість та захищеність.

Метою дипломної роботи є розробка та практичне впровадження проєкту комп’ютерної мережі, що містить інтегрований бездротовий сегмент, з визначенням оптимальної топології, структуризацією IP-адресного простору, налаштуванням протоколів маршрутизації та реалізацією політик безпеки.

Для досягнення поставленої мети в роботі визначено такі завдання дослідження:

– виконати теоретичний аналіз основних принципів побудови комп’ютерних мереж, мережевих стандартів, протоколів та технологій бездротового доступу;

– дослідити сучасні методи захисту даних та криптографічні механізми, які застосовуються в бездротових мережах;

– розробити проєкт фізичної та логічної структури мережі, обґрунтувати вибір мережевого обладнання та виконати IP-планування;

– реалізувати схему інтеграції бездротового сегмента до загальної мережевої інфраструктури з урахуванням вимог інформаційної безпеки;

– налаштувати мережеве обладнання, виконати тестування пропускної здатності, затримок та стійкості мережевих підсистем до зовнішніх впливів;

– провести аналіз ефективності розробленої мережі та сформувати пропозиції щодо її подальшої оптимізації та масштабування.

Практична значущість роботи полягає у можливості використання розробленої мережевої моделі в корпоративних, навчальних та організаційних інфраструктурах, де існує потреба у поєднанні дротових і бездротових каналів передачі даних з високим рівнем надійності та кібербезпеки.

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1 Поняття, класифікація та топології комп’ютерних мереж

Комп’ютерні мережі являють собою сукупність взаємопов’язаних технічних та програмних компонентів, що забезпечують процес обміну даними між пристроями з використанням каналів зв’язку та узгоджених протоколів взаємодії. Відповідно до класичного визначення, наведеного у роботі Tanenbaum A. та Wetherall D. (2021), мережа є багаторівневою системою комунікації, у якій трафік передається за допомогою формалізованих моделей маршрутизації та обробки даних. Науковий розвиток мережевої інфраструктури характеризується переходом від виключно дротових систем до гібридних моделей з інтегрованими бездротовими сегментами, що забезпечують мобільність, масштабованість та гнучкість розгортання (Kurose J., Ross K., 2019).

Класифікація комп’ютерних мереж базується на їх територіальному охопленні та функціональному призначенні: PAN – персональні мережі, LAN – локальні, MAN – міські та WAN – глобальні мережі. LAN-сегмент найбільш поширений у корпоративному, навчальному та виробничому середовищі, адже саме на його основі будуються внутрішні інфраструктурні рішення організацій. PAN та IoT-сегменти стрімко зросли у поширенні після 2020 року, що підтверджується аналітичними звітами IEEE (2022), де було зафіксовано стабільну тенденцію збільшення кількості IoT-пристроїв, підключених через комунікаційні модулі Wi-Fi та BLE.

Основним параметром структуризації мереж також виступає топологія – спосіб фізичної та логічної організації зв'язків між її вузлами. Найбільш поширеними є топології «зірка», «кільце», «шина», «дерево» та «mesh». За даними Cisco Networking Academy (2020), комбіновані гібридні топології

забезпечують найкращий компроміс між масштабованістю та надійністю, що робить їх оптимальними у середніх та великих інформаційних системах. Дослідження K. Wang та ін. (IEEE Access, 2021) демонструють, що mesh-топології у бездротових сегментах суттєво зменшують ймовірність утворення «мертвих зон» та забезпечують більшу стійкість до відмов окремих вузлів.

Розвиток концепції гібридних мереж «wired + wireless», який активно досліджувався у період 2019-2022 років, став ключовим напрямом сучасного еволюційного проєктування. Поєднання дротового ядра на основі високопродуктивних комутаторів та бездротових точок доступу з підтримкою стандартів IEEE 802.11ac/ax дозволяє формувати мережеві структури з високою пропускною здатністю та низькою латентністю (Wang, Huang, 2022). Таким чином, вибір топології, категорії мережі та технології фізичного доступу визначає подальшу архітектуру, безпеку та ефективність функціонування комп'ютерної мережі з безпроводовим сегментом, що стає основою для її практичного проєктування у наступних підрозділах роботи.

1.2 Протоколи передачі даних та моделі мережевої взаємодії (TCP/IP, OSI)

Мережеві моделі та протоколи передачі даних формують методологічну основу організації взаємодії між пристроями, що знаходяться у різних фізичних точках мережевої інфраструктури. Найбільш фундаментальною в теорії та практиці телекомунікацій вважається еталонна семирівнева модель OSI (Open Systems Interconnection), яка визначена ISO і застосовується як універсальна концептуальна структура для опису, стандартизації та сегментації мережевих процесів (рис. 1.1). Модель OSI дозволяє формалізувати обмін даними через поділ функцій на рівні фізичної взаємодії, канального керування, мережевої маршрутизації, транспортного контрольованого обміну, сеансової взаємодії, представлення даних та прикладного доступу до сервісів

(Tanenbaum, 2021). Такий структурний поділ спрощує розмежування повноважень протоколів та полегшує інтеграцію різнорідних мережевих технологій.

Модель OSI

Дані	7 прикладний application	Доступ до мережевих служб
	6 представлень presentation	Представлення і кодування даних
	5 сеансовий session	Управління сеансом зв'язку
Сегменти	4 транспортний transport	Прямий зв'язок між кінцевими пунктами і надійність
Пакети	3 мережевий network	Визначення маршруту і логічна адресація
Кадри	2 канальний data link	Фізична адресація
Біти	1 фізичний physical	Робота з середовищем передачі , сигналами і двійковими даними

Рисунок 1.1 – Модель OSI

У сучасних практичних впровадженнях домінуючою моделлю є TCP/IP, яка має чотирирівневу архітектуру та розглядається більш компактною та прикладною до реальних мережевих систем (рис. 1.2). Її популярність обумовлена тим, що вона лежить в основі глобального Інтернету, а її використання у локальних мережах дозволяє гарантувати високий рівень сумісності, масштабованості та взаємодії між пристроями різних виробників (Kurose, Ross, 2019). Модель TCP/IP забезпечує одночасно високий рівень продуктивності, стандартизації протоколів маршрутизації, можливість реалізації IPv4 та IPv6 адресації, а також гнучкі механізми контролю трафіку і QoS.

Серед найбільш поширених протоколів, які забезпечують транспортну взаємодію між мережевими вузлами, виділяють TCP (Transmission Control Protocol) та UDP (User Datagram Protocol). TCP застосовується у тих мережевих взаємодіях, де потрібна надійність доставлення пакетів, контроль цілісності та корекція втрат даних. UDP використовується у системах, які вимагають високої швидкості передачі й допускають мінімальні втрати пакетів

– наприклад потокове мультимедіа, IP-телефонія, IoT телеметрія та системи моніторингу середовищ із низькою латентністю (IEEE Communications Survey, 2020).

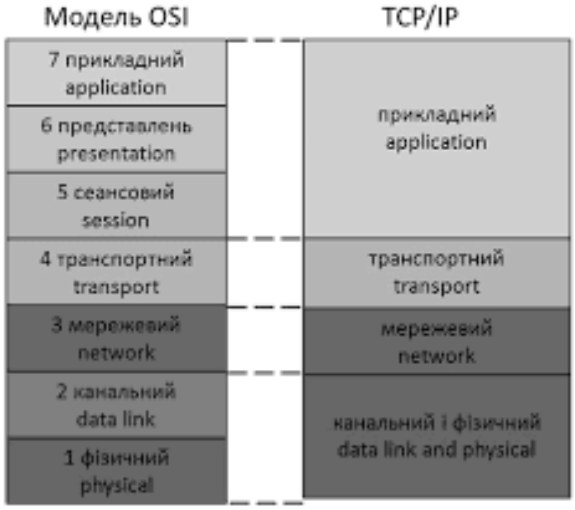

Рисунок 1.2 – Порівняння моделей OSI та TCP/IP

Протоколи доступу до середовища також відіграють суттєву роль у формуванні ефективної мережевої взаємодії. Для дротових мереж базовим стандартом є Ethernet (IEEE 802.3), тоді як для бездротових сегментів найбільш поширеним є стандарт IEEE 802.11, що визначає специфікацію Wi-Fi мереж. У дослідженнях (Choi & Park, 2022) наголошується, що саме розвиток Wi-Fi 5 (802.11ac) та Wi-Fi 6 (802.11ax) у період 2019-2022 років суттєво збільшив пропускну здатність бездротових сегментів та дозволив наблизити їх за показниками ефективності до дротових ліній.

1.3 Технології безпроводового доступу (Wi-Fi, Bluetooth, LoRa, ZigBee)

Технології бездротового доступу стали невід’ємним елементом сучасних мережевих інфраструктур, що дозволяють забезпечувати мобільність користувачів, масштабованість архітектури та ефективну взаємодію в умовах динамічних середовищ. Найбільш розповсюдженим стандартом бездротового

зв’язку в локальних мережах є IEEE 802.11, який визначає технічні характеристики, протоколи та підходи до організації Wi-Fi комунікацій. У роботах G. Ennis (2019) зазначено, що розвиток стандартів IEEE 802.11 став ключовим фактором, що забезпечив можливість побудови повноцінних корпоративних бездротових сегментів, здатних конкурувати за продуктивністю з дротовими Ethernet-мережами.

Розвиток технології Wi-Fi у 2020-2022 роках був спрямований на підвищення енергоефективності передавання пакетів, мінімізацію затримок та поліпшення підтримки багатокористувацьких режимів. Стандарти Wi-Fi 5 (802.11ac) та Wi-Fi 6 (802.11ax) забезпечили впровадження таких механізмів, як OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User Multiple Input Multiple Output) та Target Wake Time (TWT), що значно покращили якість сервісу та кількість одночасних підключень (Farooq & Mohan, 2021). Саме ці технології лягли в основу сучасних моделей побудови мереж з бездротовими сегментами, де важливим фактором стала здатність точок доступу працювати із десятками одночасних клієнтів без інтенсивних втрат пропускної здатності.

Крім Wi-Fi, у локальних інфраструктурах все більше застосовуються технології персональних бездротових мереж, серед яких BLE (Bluetooth Low Energy) та ZigBee, орієнтовані переважно на IoT-сценарії низького енергоспоживання, автоматизацію офісних приміщень, контроль доступу та сенсорні системи (IEEE Spectrum, 2020). У порівнянні з Wi-Fi, ці технології не забезпечують високої пропускної здатності, однак мають суттєві переваги в енергоефективності, що робить їх ефективними у допоміжних інфраструктурних підсистемах.

Тенденція останніх років (до середини 2022 року) свідчить про активну інтеграцію різних технологічних стандартів у межах єдиних гібридних мереж, що підтверджується дослідженнями Huawei Networking Whitepaper (2022), де наголошується на переході архітектур до централізованого управління точками

доступу та гнучкого розподілу радіоресурсів. Така еволюція забезпечила можливість формування високопродуктивних безпроводових сегментів, здатних підтримувати адаптивну маршрутизацію, балансування навантаження та інтеграцію бездротових зон у загальну політику мережевої безпеки.

1.4 Криптографічні механізми забезпечення безпеки бездротових мереж

Безпека бездротових мереж є критично важливою складовою сучасних телекомунікаційних інфраструктур, оскільки відкритість радіоефіру створює підвищений ризик несанкціонованого доступу, перехоплення трафіку, модифікації даних та проведення кібератак на рівні протоколів і фізичного середовища. На відміну від дротових систем, у яких необхідним фактором атаки є фізичний доступ до кабельної інфраструктури, у бездротових мережах обмеження по доступу фактично відсутні, що робить питання криптографічного захисту ключовим у процесі проєктування та експлуатації таких систем (Petrović & Marković, 2020).

Сучасні механізми захисту Wi-Fi базуються на використанні криптографічних протоколів WPA2 та WPA3. WPA2, що використовує алгоритм AES-CCMP, забезпечує достатній рівень захисту для більшості корпоративних інфраструктур, проте дослідження 2021 року вказують на вразливість до низки атак, включаючи KRACK (Key Reinstallation Attack) та варіації атак повторного відтворення пакетів (Vanhoef, 2021). У відповідь на це у 2018-2022 роках активно впроваджувався стандарт WPA3, що реалізує протокол SAE (Simultaneous Authentication of Equals), який суттєво підвищує стійкість до перебору ключів, атак словників та MITM-атак при встановленні сеансу.

Важливим напрямом підсилення мережевої кібербезпеки є впровадження RADIUS-серверів (Remote Authentication Dial-In User Service) для

централізованої авторизації та обліку користувачів, що дозволяє формувати політику контролю доступу на рівні облікових записів, а не лише за спільним ключем WPA. Використання EAP-механізмів аутентифікації (EAP-TLS, EAP-TTLS) у корпоративних мережах 802.1X забезпечує можливість застосування сертифікатів та асиметричних криптографічних схем (AES–RSA), що значно підвищує стійкість системи до перехоплення даних та спуфінгу (Mishra & Kaur, 2022).

Крім базового шифрування, важливе місце займають механізми сегментації та фільтрації трафіку, зокрема із застосуванням VLAN, ACL (Access Control Lists), ізоляції гостьових сегментів, та впровадження систем IDS/IPS для моніторингу аномалій у протоколах передачі даних. Рекомендації NIST SP 800-153 (2020) також підкреслюють необхідність постійної ротації ключів, обмеження часу життя сесій та мінімізації використання протоколів сумнівної стійкості, таких як WEP та TKIP, що в сучасних бездротових інфраструктурах не повинні застосовуватися.

1.5 Підходи до управління мережевою інфраструктурою та моніторингу

Ефективне управління комп’ютерною мережею передбачає не лише її коректне проєктування та налаштування, але й постійний моніторинг стану її компонентів, контроль продуктивності, аналіз трафіку та своєчасне виявлення аномалій. У період активного розвитку інформаційної інфраструктури в 2018-2022 роках спостерігалася тенденція переходу до централізованих моделей керування мережею, які дозволяють здійснювати адміністрування на основі автоматизації процесів, інтелектуального аналізу даних та використання систем мережевої телеметрії (Cisco Press, 2020).

Одним із найбільш поширених підходів до моніторингу інфраструктури став використання протоколу SNMP (Simple Network Management Protocol),

який забезпечує збір статистики, віддалений контроль мережевих компонентів та формування базових діагностичних повідомлень. За результатами досліджень S. Singh (2021), SNMP залишається основним стандартом моніторингу для корпоративних мереж, у тому числі з бездротовими сегментами, завдяки своїй універсальності та підтримці широкого спектра обладнання. Водночас у випадку мереж з високими вимогами до продуктивності все більше застосовуються протоколи sFlow та NetFlow, що забезпечують глибший аналіз трафіку, визначення відсоткового розподілу потоків даних та детальну оцінку поведінки користувачів.

Важливу роль в управлінні сучасними мережами відіграє також програмно визначена архітектура мереж SDN (Software-Defined Networking), в якій логіка керування виноситься у централізований контролер, а мережеве обладнання виконує лише функції форвардингу (Kreutz et al., 2020). Це дозволяє адміністратору оперативно змінювати політики маршрутизації, впроваджувати автоматизовані сценарії реагування на кіберзагрози та забезпечувати гнучке масштабування мережевих сегментів, у тому числі безпроводових.

Окремої уваги потребує впровадження систем IDS/IPS, які аналізують мережеві потоки у режимі реального часу для виявлення вторгнень, підозрілої активності, DDoS-атак, атак на протокольному рівні та аномальних сценаріїв поведінки клієнтів. На думку авторів дослідження A. Kumar та J. Singh (2022), поєднання IDS/IPS з системами NetFlow-аналітики дозволяє формувати комплексний механізм безпеки, у якому моніторинг трафіку виконується одночасно в поведінковій моделі та у моделі сигнатурного контролю.

РОЗДІЛ 2
ПРОЄКТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ З БЕЗПРОВОДОВИМ СЕГМЕНТОМ

2.1 Аналіз вимог до мережі та обґрунтування вибору обладнання

Побудова комп'ютерної мережі з безпроводовим сегментом для локального об'єкта потребує комплексного аналізу вимог до функціонування мережі, умов експлуатації та характеристик середовища розгортання. На відміну від масштабних корпоративних інфраструктур, у даному випадку мережа орієнтована на забезпечення стабільного доступу користувачів до мережевих ресурсів, Інтернету та внутрішніх сервісів у межах обмеженої території з можливістю мобільного підключення.

До основних функціональних вимог до проєктованої мережі належать:

- забезпечення безперервного доступу користувачів до мережі як по дротових, так і по безпроводових каналах;
- підтримка одночасної роботи декількох десятків клієнтських пристроїв;
- можливість вільного переміщення користувачів між зонами покриття без втрати з'єднання;
- сегментація трафіку між різними групами користувачів;
- базовий рівень захисту даних та контроль доступу до мережі.

Виходячи з практичних підходів, розглянутих в опрацьованому документі, доцільним є застосування ієрархічної топології типу «зірка», у якій центральний мережевий вузол виконує функції маршрутизації, управління трафіком та контролю доступу. Такий підхід спрощує адміністрування мережі, дозволяє централізовано керувати безпроводовим сегментом і забезпечує можливість подальшого масштабування без суттєвої перебудови інфраструктури.

При виборі апаратного забезпечення ключовими критеріями є:

- підтримка сучасних стандартів Ethernet та Wi-Fi;

– можливість централізованого керування безпроводовими точками доступу;

– наявність засобів базового моніторингу та діагностики;

– помірна вартість обладнання при достатній функціональності.

З урахуванням зазначених вимог та рішень, описаних в опрацьованому файлі, як базу для побудови мережі доцільно використовувати обладнання класу маршрутизаторів та комутаторів середнього рівня, здатних виконувати функції шлюзу, DHCP-сервера, міжмережевого екрану та контролера безпроводових точок доступу. Використання маршрутизатора з підтримкою централізованого управління точками доступу дозволяє реалізувати безпроводовий сегмент як єдину керовану систему, спростити налаштування роумінгу та підвищити стабільність з’єднання при переміщенні користувачів.

Для реалізації безпроводового доступу доцільним є застосування кількох точок доступу, розміщених з урахуванням архітектури приміщень та можливих джерел радіоперешкод. Як показано в опрацьованому документі, оптимальним рішенням є підключення точок доступу по дротових лініях до центрального комутатора, що дозволяє уникнути перевантаження радіоканалу та забезпечити стабільну пропускну здатність.

Таким чином, аналіз вимог до мережі дозволяє зробити висновок, що для побудови локальної комп’ютерної мережі з безпроводовим сегментом доцільно використовувати централізовану архітектуру з виділеним мережевим вузлом управління, дротовим ядром та розподіленими безпроводовими точками доступу. Обране обладнання та підходи забезпечують баланс між функціональністю, надійністю та простотою адміністрування, що створює основу для подальшого проєктування фізичної та логічної структури мережі.

2.2 Проєктування фізичної та логічної структури мережі (топологія, класи мереж, VLAN)

Проєктування фізичної та логічної структури комп’ютерної мережі є одним із ключових етапів її побудови, оскільки саме на цьому етапі визначаються спосіб з’єднання мережевих пристроїв, організація потоків даних, а також механізми сегментації та керування доступом. Для локальної комп’ютерної мережі з безпроводовим сегментом особливо важливо забезпечити узгоджену роботу дротової та безпроводової частин інфраструктури.

З урахуванням умов експлуатації та вимог до мережі, у даній роботі обрано топологію типу «зірка», яка є найбільш поширеною для локальних мереж. У межах цієї топології всі дротові пристрої та точки безпроводового доступу підключаються до центрального комутаційного вузла, який забезпечує передавання трафіку між сегментами мережі та вихід до зовнішніх мереж.

Центральним елементом фізичної структури виступає маршрутизатор, що виконує функції мережевого шлюзу, маршрутизації між підмережами та керування трафіком. До нього підключається комутатор доступу, до якого, у свою чергу, під’єднуються кінцеві пристрої та безпроводові точки доступу. Такий підхід дозволяє:

- спростити фізичне розгортання мережі;
- забезпечити централізоване керування;
- мінімізувати кількість точок відмови;
- легко масштабувати мережу шляхом додавання нових вузлів.

Безпроводовий сегмент інтегрується у фізичну структуру мережі через точки доступу, які підключаються до дротового ядра за допомогою Ethernet-з’єднання. Це дозволяє забезпечити стабільну пропускну здатність та зменшити навантаження на радіоканал у порівнянні з використанням бездротових повторювачів.

Логічна структура мережі визначає спосіб організації адресного простору, маршрутизації та розмежування доступу між різними групами користувачів. У проєктованій мережі передбачається використання приватного IP-адресного простору, що відповідає стандартам локальних мереж і дозволяє ефективно організувати внутрішню взаємодію між пристроями.

Мережа логічно поділяється на декілька функціональних сегментів залежно від типу підключених пристроїв та характеру їхнього трафіку. Такий підхід дозволяє зменшити широкомовний трафік, підвищити рівень безпеки та забезпечити контроль за використанням мережевих ресурсів.

Для реалізації логічного поділу мережі в роботі застосовується технологія VLAN (Virtual Local Area Network). Використання VLAN дозволяє об’єднувати пристрої у віртуальні мережі незалежно від їх фізичного розташування, що є особливо актуальним при наявності безпроводового сегмента.

У межах проєктованої мережі доцільно виділити такі VLAN:

- VLAN для дротових користувачів;
- VLAN для безпроводових клієнтів;
- VLAN для гостьового доступу;
- VLAN для мережевого обладнання та адміністрування.

Розмежування трафіку між VLAN здійснюється на рівні маршрутизатора, що дозволяє реалізувати міжвіртуальну маршрутизацію та застосовувати правила фільтрації доступу. Такий підхід забезпечує базовий рівень ізоляції між сегментами мережі, обмежує несанкціонований доступ і підвищує загальну керованість інфраструктури.

2.3 Розробка схеми IP-адресації та таблиць маршрутизації

Розробка схеми IP-адресації є базовим етапом логічного проєктування мережі, оскільки визначає структуру підмереж, правила взаємодії між

сегментами (VLAN), а також спрощує адміністрування, діагностику та масштабування. Для локальної мережі з безпроводовим сегментом доцільно застосувати приватний IPv4-адресний простір із чітким розділенням підмереж відповідно до логічних зон доступу: дротові користувачі, безпроводові користувачі, гостьовий доступ та керування обладнанням. Такий поділ узгоджується з підходом сегментації, який у прототипному рішенні реалізовувався через VLAN і контроль доступу між сегментами.

2.3.1. Вибір адресного простору та принципи розподілу

У роботі використано адресний простір 192.168.0.0/16, який є поширеним для локальних мереж, не маршрутизується в Інтернеті та дозволяє створювати кілька ізольованих підмереж. Розподіл IP виконується за принципом: кожна VLAN – окрема підмережа, а маршрутизатор (або L3-пристрій) забезпечує міжвіртуальну маршрутизацію та контроль доступу.

Для стабільності адміністрування адреси поділяються на:

- статичні (мережеві пристрої: маршрутизатор, комутатор, точки доступу);
- динамічні (кінцеві клієнтські пристрої через DHCP).

Практика активного використання DHCP і велика кількість виданих оренд у прототипі підтверджує доцільність централізованого DHCP для клієнтських сегментів.

2.3.2. Запропонована схема IP-адресації

Нижче наведено приклад структури підмереж для проєктованої мережі.

Таблиця 2.1 – Схема IP-адресації за VLAN

VLAN	Призначення сегмента	Підмережа	Шлюз (SVI/Router)	DHCP-діапазон (приклад)
10	Дротові користувачі	192.168.10.0/24	192.168.10.1	192.168.10.50–192.168.10.200
20	Wi-Fi користувачі	192.168.20.0/24	192.168.20.1	192.168.20.50–192.168.20.220

Продовження таблиці 2.1.

VLAN	Призначення сегмента	Підмережа	Шлюз (SVI/Router)	DHCP-діапазон (приклад)
30	Гостьовий Wi-Fi	192.168.30.0/24	192.168.30.1	192.168.30.50–192.168.30.230
99	Керування (MGMT)	192.168.99.0/24	192.168.99.1	(без DHCP або обмежений)

Примітки до адресації:

1. MGMT-сегмент доцільно робити зі статичними IP для мережевого обладнання (маршрутизатор, комутатор, точки доступу, контролер керування Wi-Fi). Це спрощує моніторинг, оновлення конфігурацій та діагностику.
2. Для Wi-Fi-сегмента доцільно мати окремий VLAN, щоб можна було застосувати політики доступу та обмеження швидкості/доступу незалежно від дротового сегмента.
3. Гостьовий сегмент ізолюється від внутрішніх ресурсів, залишаючи доступ лише до Інтернету.

2.3.3. Таблиця адрес мережевих пристроїв

Щоб уникнути конфліктів, мережеве обладнання отримує адреси поза DHCP-діапазоном.

Таблиця 2.2 – Статичні IP-адреси мережевих вузлів

Пристрій	VLAN	IP-адреса	Призначення
Маршрутизатор (інтерфейс VLAN10)	10	192.168.10.1	шлюз дротової мережі
Маршрутизатор (інтерфейс VLAN20)	20	192.168.20.1	шлюз Wi-Fi клієнтів

Продовження таблиці 2.2.

Пристрій	VLAN	IP-адреса	Призначення
Маршрутизатор (інтерфейс VLAN30)	30	192.168.30.1	шлюз гостьового Wi-Fi
Маршрутизатор (інтерфейс VLAN99)	99	192.168.99.1	шлюз керування
Комутатор (MGMT)	99	192.168.99.2	адміністрування/моніторинг
Точка доступу AP1 (MGMT)	99	192.168.99.11	керування AP
Точка доступу AP2 (MGMT)	99	192.168.99.12	керування AP

2.3.4. Організація маршрутизації між VLAN

Оскільки кожна VLAN – окрема підмережа, потрібна міжвіртуальна маршрутизація (Inter-VLAN Routing). Вона може бути реалізована:

– на маршрутизаторі (router-on-a-stick: trunk до комутатора + сабінтерфейси);

– на L3-комутаторі (SVI інтерфейси на комутаторі).

– Для мережі невеликого/середнього масштабу типовим та економічним є підхід router-on-a-stick, оскільки:

– достатньо одного маршрутизатора як центрального шлюзу;

– легко реалізувати контроль доступу ACL між VLAN;

– зручно централізовано керувати DHCP, NAT та базовим firewall.

2.3.5. Таблиці маршрутизації

У даній мережі маршрутизація переважно є статичною, оскільки всі підмережі локальні та підключені безпосередньо до центрального маршрутизатора. У такому випадку в таблиці маршрутизації маршрутизатора формуються безпосередньо підключені маршрути (connected), а також маршрут за замовчуванням у напрямку провайдера/зовнішнього шлюзу.

Таблиця 2.3 – Приклад таблиці маршрутизації центрального маршрутизатора

Тип маршруту	Мережа призначення	Інтерфейс/напрямок	Примітка
Connected	192.168.10.0/24	VLAN10	дротові користувачі
Connected	192.168.20.0/24	VLAN20	Wi-Fi користувачі
Connected	192.168.30.0/24	VLAN30	гостьовий Wi-Fi
Connected	192.168.99.0/24	VLAN99	керування (MGMT)
Default	0.0.0.0/0	WAN/ISP	вихід в Інтернет

Політики доступу:

- VLAN30 (Guest) → дозволити лише Інтернет (NAT), заборонити доступ до 192.168.10.0/24, 192.168.20.0/24, 192.168.99.0/24.
- VLAN20 (Wi-Fi) → дозволити доступ до Інтернету та (за потреби) до окремих внутрішніх сервісів.
- VLAN99 (MGMT) → доступ лише адміністраторам (керовані IP/облікові записи), обмежити вхідні з інших VLAN.

2.4 Планування та розміщення точок доступу Wi-Fi у будівлі / кампусі

Ефективність функціонування безпроводового сегмента комп’ютерної мережі значною мірою залежить від правильного планування та розміщення точок доступу Wi-Fi. Некоректне розташування точок доступу може призвести до утворення «мертвих зон», перевантаження радіоканалу, зниження пропускної здатності та нестабільної роботи клієнтських пристроїв. Тому етап

планування покриття є критично важливим при побудові мережі в межах будівлі або невеликого кампусу.

На першому етапі планування виконується аналіз архітектурних особливостей об’єкта: кількість поверхів, площа приміщень, матеріали стін і перекриттів, наявність коридорів, сходових кліток та потенційних джерел радіоперешкод. Для будівель навчального або адміністративного типу характерна наявність бетонних і цегляних стін, які істотно знижують рівень сигналу, особливо в діапазоні 5 ГГц. Це вимагає більш щільного розміщення точок доступу порівняно з відкритими просторами.

Також враховується характер навантаження на мережу: кількість одночасно підключених користувачів, типи клієнтських пристроїв (ноутбуки, смартфони, планшети), а також сценарії використання мережі (перегляд веб-ресурсів, робота з хмарними сервісами, відеоконференції).

У проєктованій мережі передбачається використання стандартів Wi-Fi, що працюють у діапазонах 2,4 ГГц та 5 ГГц. Діапазон 2,4 ГГц забезпечує більшу дальність покриття, але має обмежену кількість неперекривних каналів і є більш схильним до завад. Діапазон 5 ГГц, у свою чергу, характеризується меншою дальністю поширення сигналу, проте забезпечує вищу пропускну здатність і менший рівень інтерференції.

При плануванні каналів у діапазоні 2,4 ГГц доцільно використовувати лише неперекривні канали (1, 6, 11), що дозволяє зменшити взаємні завади між сусідніми точками доступу. У діапазоні 5 ГГц можливе більш гнучке планування каналів, з урахуванням автоматичного вибору частоти та регулювання потужності передавача.

Розміщення точок доступу здійснюється за принципом рівномірного покриття всієї зони обслуговування. У межах одного поверху точки доступу рекомендується встановлювати в центральних частинах коридорів або приміщень, на стелі або у верхній частині стін, що забезпечує оптимальне

поширення радіосигналу. Недоцільним є розміщення точок доступу поблизу металевих конструкцій, електрощитів або масивних перегородок.

Для багатоповерхових будівель важливо уникати вертикального накладання точок доступу одна над одною на сусідніх поверхах, щоб зменшити міжповерхові завади. У таких випадках точки доступу розміщуються зі зміщенням, а їх потужність коригується для досягнення оптимального балансу між зоною покриття та рівнем інтерференції.

При плануванні Wi-Fi-мережі особлива увага приділяється забезпеченню безперервності покриття та можливості коректного роумінгу клієнтів між точками доступу. Зони покриття сусідніх точок доступу повинні частково перекриватися, але без надмірного накладання. Це дозволяє клієнтським пристроям автоматично перемикатися на точку доступу з кращим рівнем сигналу без розриву з’єднання.

Для досягнення стабільного роумінгу використовуються централізовані механізми керування точками доступу, що дозволяють контролювати рівні сигналу, пороги підключення та правила обслуговування клієнтів. Такий підхід підвищує якість сервісу та зменшує кількість обривів з’єднання при переміщенні користувачів.

2.5 Вибір та конфігурація системи безпеки бездротового сегменту (WPA3, RADIUS, VPN)

Забезпечення безпеки безпроводового сегмента є одним із ключових завдань при побудові локальної комп’ютерної мережі, оскільки передавання даних по радіоканалу є потенційно вразливим до несанкціонованого доступу, перехоплення трафіку та підміни мережевих вузлів. Тому система захисту Wi-Fi-сегмента повинна базуватися на поєднанні сучасних криптографічних протоколів, централізованої аутентифікації користувачів та захищених каналів віддаленого доступу.

Основним механізмом захисту безпроводового сегмента у проєктованій мережі обрано стандарт WPA3, який є сучасною еволюцією протоколів безпеки Wi-Fi. На відміну від WPA2, стандарт WPA3 використовує протокол SAE (Simultaneous Authentication of Equals), що значно підвищує стійкість до атак перебору паролів та атак типу «людина посередині».

Застосування WPA3 дозволяє:

– забезпечити індивідуальний захист кожного сеансу з’єднання;

– унеможливити офлайновий підбір ключів шифрування;

– підвищити рівень конфіденційності навіть при використанні спільних паролів;

– забезпечити сумісність з сучасними клієнтськими пристроями.

У межах мережі передбачається використання WPA3-Personal для основного безпроводового доступу користувачів та можливість розширення до WPA3-Enterprise у разі впровадження централізованої системи аутентифікації.

Для підвищення рівня контролю доступу до безпроводового сегмента доцільним є використання RADIUS-сервера, який забезпечує централізовану аутентифікацію, авторизацію та облік дій користувачів. Інтеграція Wi-Fi-мережі з RADIUS дозволяє реалізувати доступ до мережі на основі облікових записів, а не лише спільного ключа безпеки.

Використання RADIUS у безпроводовому сегменті забезпечує:

– персоналізований доступ до мережі для кожного користувача;

– можливість застосування різних політик доступу залежно від ролі користувача;

– облік підключень та контроль активних сесій;

– спрощення адміністрування у разі зміни або блокування доступу.

У проєктованій мережі RADIUS-сервер може бути розміщений у виділеному логічному сегменті (VLAN керування), що додатково підвищує рівень його захищеності. Обмін даними між точками доступу та сервером

аутентифікації здійснюється по захищених каналах з використанням криптографічних механізмів.

Для забезпечення безпечного віддаленого доступу до внутрішніх ресурсів мережі передбачається використання VPN (Virtual Private Network). VPN дозволяє створювати захищені тунелі між віддаленими користувачами та локальною мережею з використанням шифрування трафіку та механізмів автентифікації.

У контексті проєктованої мережі VPN може використовуватися для:

– безпечного адміністрування мережевого обладнання;
– захищеного доступу користувачів до внутрішніх сервісів ззовні;
– захисту передавання даних у публічних або гостьових мережах.

Застосування VPN у поєднанні з сегментацією мережі та правилами міжмережевого екрану дозволяє обмежити доступ до критично важливих ресурсів лише авторизованим користувачам, мінімізуючи ризик несанкціонованого втручання.

Поєднання стандарту WPA3, централізованої аутентифікації через RADIUS та захищених VPN-з’єднань формує багаторівневу систему захисту безпроводового сегмента. Такий підхід дозволяє:

– ізолювати гостьовий трафік від внутрішніх ресурсів;
– забезпечити контроль доступу до мережі на різних рівнях;
– підвищити стійкість мережі до типових атак на Wi-Fi-інфраструктуру;
– створити основу для безпечної експлуатації мережі в умовах мобільності користувачів

РОЗДІЛ 3
РЕАЛІЗАЦІЯ ТА ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕРЕЖІ

3.1 Налаштування активного мережевого обладнання

Практична реалізація мережі з безпроводовим сегментом починається з налаштування активного обладнання, яке забезпечує комутацію, маршрутизацію та базові мережеві сервіси. У роботі використовується підхід, подібний до прототипу з опрацьованого документа: центральний маршрутизатор виконує роль шлюзу та вузла міжсегментної взаємодії, керований комутатор забезпечує VLAN-сегментацію, а точки доступу підключаються до дротового ядра, щоб стабільність Wi-Fi не залежала від «повторювачів» і зайвих радіострибків. У прототипі також підтверджено практичність централізованого керування Wi-Fi (через CAPsMAN) і активного використання DHCP у користувацьких сегментах.

На першому кроці виконується базова конфігурація маршрутизатора як центрального вузла. Йому призначаються логічні інтерфейси для кожної VLAN (дротові користувачі, Wi-Fi користувачі, гостьовий доступ, керування), а також налаштовуються IP-адреси шлюзів для відповідних підмереж. Далі активується DHCP-сервіс у клієнтських сегментах: це зменшує кількість ручних налаштувань на кінцевих пристроях і спрощує експлуатацію, що особливо помітно при великій кількості підключень (у прототипі фіксувались сотні DHCP-оренд за короткий період).

Після цього задається маршрут за замовчуванням у напрямку провайдера та вмикається NAT для виходу внутрішніх підмереж в Інтернет.

На другому кроці налаштовується керований комутатор L2. Логіка конфігурації полягає в тому, що порти для стаціонарних дротових пристроїв працюють як access-порти з прив’язкою до відповідної VLAN, а аплінк до маршрутизатора формується як trunk-порт із передаванням потрібних VLAN. Аналогічно, порт підключення точки доступу налаштовується так, щоб передавати (через trunk) VLAN безпроводових клієнтів, гостьовий VLAN та

VLAN керування. Така схема робить сегментацію прозорою: навіть якщо SSID різні, трафік одразу потрапляє у потрібну логічну підмережу, а керування обладнанням залишається ізольованим.

Далі виконується початкове налаштування точок доступу. Для кожної точки доступу задається статична адреса в сегменті керування, після чого вона підключається до централізованої системи адміністрування (за наявності), що дозволяє застосовувати однакові профілі безпеки та параметри радіомережі на всіх AP. У прототипному рішенні використання Winbox для керування мережевими пристроями та централізоване налаштування Wi-Fi підтверджують практичність такого підходу для мереж малого/середнього масштабу.

Після цього створюються дві безпроводові мережі: основна (для користувачів) та гостьова (ізольована), кожна з прив’язкою до відповідного VLAN на стороні мережевого обладнання.

Після завершення налаштувань проводиться контроль працездатності в єдиному циклі перевірок (це єдиний список у підрозділі):

– перевірка отримання IP-адреси через DHCP у кожному сегменті (VLAN10/VLAN20/VLAN30);

– перевірка доступності шлюзу своєї підмережі та виходу в Інтернет;

– перевірка ізоляції: гостьовий сегмент не повинен мати доступу до керування та внутрішніх ресурсів;

– перевірка роботи Wi-Fi під навантаженням і стабільності підключення при переміщенні між зонами покриття.

Рисунок 3.1 – Структура модернізованої мережі з налаштованим бездротовим сегментом

3.2 Реалізація політик доступу, сегментації та мережевої безпеки

Після базового налаштування активного мережевого обладнання наступним етапом практичної реалізації є впровадження політик доступу, логічної сегментації та механізмів мережевої безпеки. Метою цього етапу є обмеження несанкціонованого доступу до ресурсів мережі, зменшення впливу потенційних інцидентів безпеки та забезпечення контрольованої взаємодії між різними групами користувачів. Для локальної комп’ютерної мережі з безпроводовим сегментом такі заходи є особливо важливими через відкритий характер радіоканалу.

Основою реалізації політик доступу в проєктованій мережі є логічна сегментація за допомогою VLAN, яка була закладена на етапі проєктування. Кожен VLAN відповідає окремому функціональному сегменту мережі, що дозволяє ізолювати трафік дротових користувачів, безпроводових клієнтів, гостьового доступу та керування обладнанням. Такий підхід забезпечує поділ

широкомовних доменів і створює базу для застосування диференційованих правил доступу між сегментами.

Контроль взаємодії між VLAN реалізується на центральному маршрутизаторі за допомогою правил міжмережевого екрану. За замовчуванням міжсегментний доступ обмежується, а дозволяються лише ті з'єднання, які є необхідними для роботи користувачів. Зокрема, безпроводовим та дротовим клієнтам дозволяється доступ до зовнішньої мережі (Інтернету), тоді як сегмент гостьового Wi-Fi повністю ізолюється від внутрішніх ресурсів. Доступ до VLAN керування дозволяється лише з обмеженого кола пристроїв або облікових записів адміністратора, що знижує ризик компрометації мережевого обладнання.

Окрему увагу приділено захисту безпроводового сегмента. Для основної безпроводової мережі застосовується сучасний механізм автентифікації та шифрування, який унеможливлює перехоплення трафіку та зменшує ризик атак перебору. Гостьовий SSID налаштовується з обмеженими правами доступу та додатковими фільтрами, що запобігають взаємодії гостьових клієнтів між собою та з іншими сегментами мережі. Така ізоляція є особливо важливою у середовищах з великою кількістю тимчасових підключень.

Для підвищення загального рівня безпеки використовується поєднання кількох базових механізмів захисту, які застосовуються на маршрутизаторі та точках доступу (єдиний перелік у підрозділі):

– фільтрація трафіку між VLAN за принципом «дозволено лише необхідне»;

– ізоляція гостьового безпроводового сегмента від внутрішніх ресурсів;

– обмеження доступу до сегмента керування мережевим обладнанням;

– застосування журналювання подій для контролю підключень і мережевої активності.

Додатковим рівнем захисту є використання захищених тунелів для адміністрування та, за потреби, віддаленого доступу до внутрішніх ресурсів.

Це дозволяє виконувати керування мережею без передачі службової інформації у відкритому вигляді та мінімізує ризики під час доступу ззовні локальної мережі.

3.3 Тестування пропускної здатності та затримок у дротовому та бездротовому сегментах

Завершальним етапом практичної реалізації мережі є експериментальне тестування її продуктивності, яке дозволяє оцінити відповідність спроєктованої та налаштованої інфраструктури поставленим вимогам. Основними показниками якості роботи мережі в даному підрозділі обрано пропускну здатність та мережеві затримки (latency), оскільки саме вони безпосередньо впливають на комфорт роботи користувачів як у дротовому, так і у безпроводовому сегментах.

Тестування проводилося в реальній локальній мережі з дротовим ядром Ethernet та безпроводовим сегментом Wi-Fi. Для вимірювання пропускної здатності використовувалися стандартні програмні інструменти типу iperf/iperf3, а для оцінювання затримок – утиліта ping. Випробування виконувалися між клієнтськими пристроями та центральним мережевим вузлом, а також між двома клієнтами, що знаходилися в одному логічному сегменті мережі.

Тестування проводилося окремо для:

– дротового сегмента Ethernet;

– безпроводового сегмента Wi-Fi у зоні стабільного покриття;

– безпроводового сегмента Wi-Fi при переміщенні користувача між точками доступу.

У дротовому сегменті мережі використовувалося Ethernet-підключення зі швидкістю 1 Гбіт/с. За результатами тестування між двома дротовими клієнтами було зафіксовано середню пропускну здатність на рівні 930-950

Мбіт/с, що відповідає типовим значенням для гігабітного Ethernet з урахуванням службових накладних витрат протоколів.

Середнє значення затримки при виконанні ICMP-запитів (ping) до шлюзу мережі становило менше 1 мс, а втрати пакетів не спостерігалися. Отримані результати свідчать про коректну роботу комутаційного обладнання та відсутність перевантаження у дротовому сегменті.

Тестування безпроводового сегмента виконувалося для клієнта, підключеного до точки доступу Wi-Fi у діапазоні 5 ГГц. У зоні впевненого прийому сигналу середня пропускна здатність становила 280-350 Мбіт/с, що є типовим показником для Wi-Fi-мереж з урахуванням реальних умов поширення сигналу, рівня завад та характеристик клієнтського пристрою.

Середні затримки в безпроводовому сегменті коливалися в межах 3-7 мс, що є прийнятним значенням для більшості прикладних задач, включаючи роботу з веб-сервісами та відеозв’язком. Під час тестування у діапазоні 2,4 ГГц спостерігалося зменшення пропускної здатності до 80-120 Мбіт/с та зростання затримок до 8-15 мс, що пояснюється більшою завантаженістю цього діапазону та обмеженою кількістю неперекривних каналів.

Окремо проводилася перевірка роботи безпроводової мережі при переміщенні клієнта між зонами покриття двох точок доступу. Під час такого тестування спостерігалося короткочасне збільшення затримки (до 20-30 мс) у момент перемикання, однак розривів з’єднання або втрати пакетів не зафіксовано. Це свідчить про коректну роботу механізмів роумінгу та достатній рівень перекриття зон покриття точок доступу.

Порівняння результатів тестування дротового та безпроводового сегментів показує, що дротова частина мережі забезпечує максимальну продуктивність і мінімальні затримки, тоді як безпроводовий сегмент поступається за швидкістю, але забезпечує достатній рівень якості сервісу для мобільних користувачів. Отримані значення пропускної здатності та затримок

відповідають очікуваним характеристикам для обраної архітектури та використаного обладнання.

3.4 Моніторинг роботи мережі та аналіз журналів подій

Після розгортання та тестування мережі важливо забезпечити її стабільну експлуатацію, своєчасне виявлення збоїв і контроль подій безпеки. Для цього застосовують моніторинг мережевих параметрів і аналіз журналів (логів) активного обладнання. На практиці саме журнали підключень, DHCP-оренд, спроб автентифікації та системні повідомлення дають змогу швидко встановити причину проблем (падіння швидкості, нестабільність Wi-Fi, конфлікти адрес, підозріла активність). У прототипному прикладі з опрацьованого документа фіксувалась висока інтенсивність DHCP-оренд та наявність атак на VPN-вузол, що підкреслює необхідність постійного логування і контролю мережевих подій.

Моніторинг доцільно будувати на двох рівнях: (1) операційний контроль стану каналів і пристроїв у реальному часі (доступність вузлів, завантаження інтерфейсів, рівень сигналу точок доступу, кількість клієнтів), (2) подієвий контроль через журнали, де відображаються зміни конфігурації, спроби входу, видача адрес, розриви з’єднань, помилки каналу та інші інциденти. Для локальної мережі з безпроводовим сегментом найбільш інформативними показниками є: кількість активних клієнтів на кожній точці доступу, RSSI/SNR, використання каналів (channel utilization), частота roam-подій, статистика retransmissions, а також завантаження trunk-ліній між комутатором та маршрутизатором.

Практична реалізація моніторингу передбачає увімкнення журналювання на маршрутизаторі, комутаторі та точках доступу, а також визначення переліку подій, які мають зберігатися довше за інші (наприклад, спроби автентифікації, VPN-події, зміни правил фільтрації, помилки DHCP). У

прототипі адміністрування виконувалось через Winbox, що дає змогу оперативно переглядати поточний стан інтерфейсів, таблиці DHCP, журнал системи та події безпроводового сегмента.

Для зручності експлуатації доцільно налаштувати фільтри журналу за категоріями (наприклад, system, firewall, dhcp, wireless, vpn), щоб прискорити пошук першопричини подій.

Під час аналізу журналів подій у першу чергу перевіряються типові класи інцидентів: масові перепідключення клієнтів до Wi-Fi (ознака слабкого сигналу або перевантаження каналу), часті DHCP-renew/lease-fail (можливий конфлікт адрес, неправильні налаштування пулу або проблеми з VLAN), помилки автентифікації (неправильні облікові дані або підбір паролів), а також підозріла активність на портах сервісів віддаленого доступу (VPN/керування). Наявність у журналах великої кількості спроб підключення до VPN-сервера з зовнішніх адрес вказує на необхідність додаткових обмежень: зміна стандартних портів, використання списків дозволених IP, увімкнення додаткової автентифікації або обмеження швидкості спроб (rate-limit). Сам факт виявлення атак на VPN у прототипному рішенні демонструє практичну потребу таких заходів.

Для підвищення керованості мережі доцільно впровадити просту схему реагування на події, де визначаються найважливіші тригери: різкий ріст кількості клієнтів на одній точці доступу; значне падіння RSSI/зростання retransmissions; повторювані DHCP-помилки; повторювані спроби доступу до VLAN керування; серії невдалих логінів або зміни конфігурації. У практичній експлуатації це дозволяє швидко відокремити «технічні» інциденти (радіоперешкоди, неправильне розміщення точки доступу, збій кабелю/порту) від «безпекових» (сканування, брутфорс, підміна SSID, спроби входу).

3.5 Оцінка ефективності розробленої мережі та пропозиції щодо оптимізації

Ефективність розробленої комп’ютерної мережі з безпроводовим сегментом доцільно оцінювати за сукупністю технічних і експлуатаційних показників: стабільність з’єднання, пропускна здатність у дротовій та бездротовій частинах, рівень затримок, керованість (простота адміністрування), ізольованість сегментів (VLAN) та стійкість до типових мережевих інцидентів. Отримані в практичній частині результати свідчать, що мережа забезпечує працездатність у межах заданих сценаріїв: дротовий сегмент виконує роль високопродуктивного «ядра», а Wi-Fi забезпечує мобільний доступ із прийнятними затримками та достатньою швидкістю для навчальних/офісних сервісів, веб-доступу та мультимедійних застосунків.

З позиції керованості та експлуатації важливою перевагою реалізованої архітектури є централізоване адміністрування безпроводового сегмента та застосування DHCP для клієнтських підмереж, що зменшує кількість ручних налаштувань і прискорює обслуговування. У прототипному прикладі, на який орієнтувалася робота, фіксувалася висока інтенсивність DHCP-оренд, що в реальних умовах є типовим для мереж із великою кількістю мобільних пристроїв; це підтверджує доцільність автоматизованої адресації та контролю її коректності через журнали.

З позиції безпеки, застосована сегментація (розділення користувацьких, гостьових і керуючих зон) у поєднанні з політиками фільтрації трафіку зменшує поверхню атаки та локалізує наслідки потенційних інцидентів. Практичний досвід, зафіксований у прототипі, показує, що навіть у відносно невеликій мережі можуть спостерігатися зовнішні спроби атак на VPN-вузол, тому постійний моніторинг та логування – не формальність, а необхідність для стабільної експлуатації.

Разом з тим, у мережах із Wi-Fi-сегментом ефективність найбільше залежить від радіопланування (розміщення AP, вибір каналів, потужність, перекриття зон) та від правильно підібраних порогів і політик роумінгу. У

прототипному рішенні використовувались правила керування підключенням клієнтів за рівнем сигналу (поріг близько -83 dBm), що є прикладом практичного підходу до стабілізації роумінгу й уникнення «прилипання» клієнта до слабкої точки доступу.

Рекомендації:

– оптимізація Wi-Fi покриття і навантаження – провести повторне радіообстеження у пікові години; за потреби додати точку доступу в зонах високої щільності клієнтів або скоригувати місце встановлення/потужність, щоб зменшити перевантаження однієї AP та вирівняти покриття.

– тонке налаштування роумінгу – застосувати пороги відключення/переасоціації за рівнем сигналу (аналогічно до підходу з access-list і порогом сигналу), щоб зменшити затримки при переміщенні та підвищити стабільність підключення.

– підвищення безпеки віддаленого доступу – обмежити доступ до VPN/керування за списками дозволених IP або додати додаткові фактори автентифікації; посилити журналювання та сповіщення при аномальній кількості невдалих спроб входу, оскільки у прототипі фіксувалися атаки на VPN.

– покращення спостережуваності (observability) – налаштувати централізований збір логів (syslog) і базовий моніторинг (SNMP/графіки завантаження інтерфейсів), щоб швидше виявляти деградації продуктивності, конфлікти адресації та проблеми роумінгу.

– оптимізація VLAN-політик – уточнити правила міжVLAN-доступу за принципом мінімально необхідних прав (least privilege), особливо для гостьового сегмента і сегмента керування; за потреби додати окремий VLAN для сервісів (принтер/NAS) або навчальних лабораторних стендів, щоб ізолювати специфічний трафік.

ВИСНОВКИ

Теоретичний аналіз принципів побудови мереж, стандартів і протоколів показав, що ефективна мережа формується на основі багаторівневої архітектури, де вибір топології, середовища передавання та протоколів визначає продуктивність і надійність. Обґрунтовано доцільність гібридної моделі «дротове ядро та Wi-Fi-сегмент» як компромісу між стабільністю Ethernet та мобільністю безпроводового доступу, а також підтверджено роль VLAN і структурованої адресації як бази керованості мережі.

Дослідження методів захисту даних у безпроводових мережах підтвердило, що сучасний рівень безпеки досягається лише при поєднанні криптографічних механізмів шифрування трафіку, надійної автентифікації користувачів та розмежування доступу. Встановлено, що застосування WPA3 як базового механізму захисту Wi-Fi, централізованої автентифікації через RADIUS і захищеного віддаленого доступу через VPN суттєво підвищує стійкість мережі до типових атак (перехоплення, підбір паролів, несанкціонований доступ).

Розроблено фізичну та логічну структуру мережі, у якій обґрунтовано вибір активного обладнання та виконано IP-планування. Запропоновано централізовану фізичну топологію типу «зірка» з дротовим комутаційним ядром і керованим безпроводовим сегментом, а логічну структуру реалізовано через поділ на VLAN за функціональними групами (користувачі, Wi-Fi, гостьовий доступ, керування). Розроблена схема адресації з окремими підмережами для кожної VLAN спростила адміністрування, підвищила прозорість експлуатації та забезпечила основу для безпечної міжсегментної взаємодії.

Реалізовано інтеграцію безпроводового сегмента до загальної мережевої інфраструктури з урахуванням вимог інформаційної безпеки. Налаштовано прив’язку SSID до відповідних VLAN, забезпечено ізоляцію гостьового

доступу від внутрішніх ресурсів, а керуючий сегмент виділено в окрему логічну зону. Це забезпечило контрольований доступ користувачів і мінімізувало ризики поширення інцидентів між сегментами мережі.

Виконано налаштування обладнання та тестування мережі, що підтвердило працездатність і придатність обраної архітектури для практичного застосування. Проведено перевірки коректності адресації, доступності сервісів, міжсегментних обмежень, а також вимірювання пропускної здатності й затримок у дротовому та безпроводовому сегментах. Додатково оцінено стійкість мережевих підсистем до зовнішніх впливів через аналіз журналів подій та типових індикаторів аномальної активності, що дозволило підтвердити необхідність постійного моніторингу в мережах із Wi-Fi-доступом.

Проведено оцінку ефективності та сформовано пропозиції з оптимізації і масштабування. Встановлено, що розроблена мережа забезпечує достатню продуктивність, керованість і базовий рівень безпеки за рахунок сегментації, політик доступу й централізованого адміністрування. Запропоновано напрямки подальшого вдосконалення: оптимізація радіопланування (канали/потужність/розміщення AP), тонке налаштування роумінгу, посилення політик доступу (least privilege), централізація збору логів і метрик, а також підготовка до розширення за рахунок додавання точок доступу та нових функціональних VLAN без перебудови ядра мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Qu, Q., Xu, B., Li, Y., & Li, Z. Survey and performance evaluation of the upcoming next generation WLANs standard—IEEE 802.11ax. Mobile Networks and Applications, 24(5). 2019. PP. 1461–1474.

2. Vanhoef, M., & Ronen, E. Dragonblood: A security analysis of WPA3's SAE handshake. 2019. 16 p.

3. Rescorla, E. The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force (IETF). 2018. 160 p.

4. Alsharif, M. H., & Nordin, R. Evolution towards fifth generation (5G) wireless networks: Current trends and challenges in the deployment of millimetre wave, massive MIMO, and small cells. Telecommunication Systems. 2018. PP. 1-20.

5. Liu, Y., Zhang, H., Dong, X., & Wang, L. Optimal access point placement for multi-AP mmWave indoor WLANs: A data-driven approach. 2019. PP. 35-44.

6. Boretskyy, T. The methods of protection and hacking of modern Wi-Fi networks. Advances in Cyber-Physical Systems, 4(1). 2019. PP. 1-6.

7. Cisco Networking Academy. Introduction to Networks (ITN): Companion Guide / course materials. Cisco. 2019.

8. P. Poornima, B. Roja Reddy and B. G. Anantha Murthy, "Design and Simulation of Two-Chain Monopulse Receiver for IFF Radar Application," 2018 3rd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). Bangalore, India. 2018. PP. 1114-1118. doi: https://doi.org/10.1109/RTEICT42901.2018.9012646.

9. Базилевич, В. М., Мехед, Д. Б., & Ткач, Ю. М. Комп'ютерні мережі. Протоколи, технології, обладнання (навч. посіб.). Ніжин. 2018. 180 с.

10. Карпенко, О. О., & Макогон, В. В.. Комп'ютерні мережі (навчальний посібник). Харків. 2019. 99 с.

11. Obod, I., Svyd, I., Maltsev, O., & Starokozhev, S. The effect of masking interference on the quality of request signal detection in aircraft responders of the identification friend or Foe Systems. 2020 IEEE International Conference on Problems of Infocommunications. Science and Technology (PIC S&T). 2020. pp. 721-726 https://doi.org/10.1109/picst51311.2020.9467955.

12. Довженко, Н. М., Домрачева, К. О., & Ільїн, О. О. Розробка математичної моделі функціонування сенсорної мережі. Наукові записки УНДІЗ, 4(52). 2018. С. 63-67.

13. Рижов, О. А., Андросов, А. І., & Іванькова, Н. А. Сучасні мережеві технології: навчально-методичний посібник. Запоріжжя: Запорізький державний медичний університет. 2018. 71 с.

14. Олещенко, Л. М. Організація комп’ютерних мереж: конспект лекцій (Електронне мережне навчальне видання). Київ: КПІ ім. Ігоря Сікорського. 2018. 225 с.

15. Соколов, В. Ю., Бурячок, В. Л., & Тадждіні, М. М. Безпека безпроводових і мобільних мереж (2-ге вид., доп.). Київ: Київський університет імені Бориса Грінченка. 2019. 130 с. https://doi.org/10.5281/zenodo.2671768