Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет комп'ютерної інженерії та управління
(повна назва)

Кафедра електронних обчислювальних машин
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

Рівень вищої освіти перший (бакалаврський)

Налаштування та оптимізація мережі з використанням VLAN у корпоративному середовищі

(тема)

Виконав:
здобувач 4 року навчання,
групи КІУКІ-21-2
Артур ЗІНОВ'ЄВ
(власне ім'я, прізвище)

Спеціальність
123 «Комп'ютерна інженерія»
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма
Комп'ютерна інженерія
(повна назва освітньої програми)

Керівник: ас. Артем МОРОЗ
(посада, власне ім'я, прізвище)

Допускається до захисту

Завідувач кафедри ЕОМ _____ Андрій КОВАЛЕНКО
(підпис) (власне ім'я, прізвище)

2025 р.

Харківський національний університет радіоелектроніки

Факультет комп’ютерної інженерії та управління

Кафедра електронних обчислювальних машин

Рівень вищої освіти перший (бакалаврський)

Спеціальність 123 «Комп’ютерна інженерія»
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма Комп’ютерна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
“____” _____ 20__ р.

ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Зінов’єву Артуру Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Налаштування та оптимізація мережі з використанням VLAN у корпоративному середовищі

затверджена наказом по університету від “ 26 ” травня 2025 р. № 424 Ст

2. Термін подання здобувачем роботи до екзаменаційної комісії 17 червня 2025 р.

3. Вхідні дані до роботи

1. Розробка комп'ютерної мережі підприємства
2. Опис організаційної структури підприємства
3. Вимоги до швидкості передачі інформації в мережі
4. Перелік використаних програмних засобів: ОС Windows 11

4. Перелік питань, що потрібно опрацювати у роботі

1. Теоретичні основи технології vlan та її застосування в корпоративних мережах
2. Аналіз поточного стану та вимог до мережі підприємства
3. Проєктування корпоративної мережі з використанням vlan

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій 14 слайдів

6. Консультанти розділів роботи (заповнюється за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / терміни виконання етапів роботи	Примітка
1	Аналіз проблеми та огляд існуючих рішень	27.05.25 – 30.05.25	
2	Вибір технології розробки та інструментальних	31.05.25 – 02.06.25	
	засобів		
3	Розробка алгоритмічного забезпечення	03.06.25 – 05.06.25	
4	Розробка та відлагодження програмного	06.06.25 – 09.06.25	
5	Оформлення матеріалів кваліфікаційної роботи	10.06.25 – 11.06.25	
6	Подання кваліфікаційної роботи керівникові	12.06.25 – 13.06.25	
	та її попередній захист		
7	Подання кваліфікаційної роботи на	14.06.25 – 16.06.25	
	рецензування		

Дата видачі завдання " 26 " травня 2025 р.

Здобувач _____
(підпис)

Керівник роботи _____ ас. Артем МОРОЗ
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 64 с., 2 рис., 0 табл., 1 дод., 12 джерел.

КОМП’ЮТЕРНА МЕРЕЖА, ІНТЕРНЕТ, МАРШРУТИЗАТОР, ПРОТОКОЛ, СЕРВЕР, ШЛЮЗ, FIREWALL, WI-FI, WLAN.

Метою кваліфікаційної роботи є розробка теоретичних і практичних засад щодо налаштування та оптимізації корпоративної мережі на основі технології VLAN. Для досягнення цієї мети передбачається виконати такі завдання: провести аналіз сучасних стандартів і методів впровадження VLAN у корпоративному середовищі; дослідити існуючий стан та основні проблеми мережевої інфраструктури підприємства; визначити вимоги до інформаційної безпеки, продуктивності та масштабованості мережі; обґрунтувати вибір оптимальної топології та підходів до сегментації; розробити рекомендації щодо впровадження, адміністрування й моніторингу VLAN для підвищення ефективності роботи та захисту корпоративної інформації.

ABSTRACT

Bachelor’s thesis: 64 pages, 2 figures, 0 tables, 1 appendix, 12 references.

COMPUTER NETWORK, INTERNET, ROUTER, PROTOCOL, SERVER, GATEWAY, FIREWALL, WI-FI, WLAN.

The aim of the qualification thesis is to develop theoretical and practical foundations for configuring and optimizing a corporate network based on VLAN technology. To achieve this goal, the following tasks are outlined: analyze modern standards and methods for implementing VLANs in a corporate environment; examine the current state and key issues of the enterprise’s network infrastructure; determine requirements for information security, performance, and scalability of the network; justify the selection of an optimal topology and segmentation approaches; and develop recommendations for the implementation, administration, and monitoring of VLANs to enhance operational efficiency and protect corporate information.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

ACL — Access Control List — список контролю доступу

CPU — Central Processing Unit — центральний процесор

DHCP — Dynamic Host Configuration Protocol — протокол динамічного налаштування хостів

DNS — Domain Name System — система доменних імен

HSRP — Hot Standby Router Protocol — протокол резервування маршрутизаторів

IP — Internet Protocol — протокол інтернету

IPSec — Internet Protocol Security — захист IP-даних

LAN — Local Area Network — локальна мережа

MAC — Media Access Control — фізична адреса пристрою в мережі

NIC — Network Interface Card — мережева карта

OSPF — Open Shortest Path First — протокол маршрутизації

PoE — Power over Ethernet — передача живлення через Ethernet

QoS — Quality of Service — якість обслуговування

RAM — Random Access Memory — оперативна пам’ять

SNMP — Simple Network Management Protocol — протокол керування мережею

SSID — Service Set Identifier — ідентифікатор бездротової мережі

VLAN — Virtual Local Area Network — віртуальна локальна мережа

VoIP — Voice over IP — передача голосу через IP-мережі

ВСТУП

У сучасних умовах цифрової трансформації бізнесу інформаційна інфраструктура відіграє ключову роль у забезпеченні ефективності, гнучкості й безпеки роботи підприємств. Зростання обсягів даних, впровадження хмарних сервісів, поява мобільних і віддалених робочих місць, а також підвищення вимог до конфіденційності й цілісності інформації формують нові виклики для корпоративних мереж. Однією з базових технологій, яка дозволяє вирішити проблеми ізоляції, оптимізації та захисту трафіку, є концепція віртуальних локальних мереж (VLAN). Використання VLAN забезпечує гнучке логічне розділення мережевої інфраструктури, підвищує рівень інформаційної безпеки, спрощує адміністрування та підтримує масштабованість корпоративних мереж.

Актуальність дослідження обумовлена необхідністю модернізації традиційних мережевих архітектур для задоволення вимог сучасного бізнесу. Багато підприємств стикаються з такими проблемами, як недостатня сегментація трафіку, ускладнення керування великою кількістю пристроїв, обмежена гнучкість при розширенні мережі та зростання ризиків кібербезпеки. У зв’язку з цим питання впровадження VLAN-сегментації, правильного планування та оптимізації мережі набуває особливого значення для організацій різних масштабів і галузей.

Метою цієї кваліфікаційної роботи є розробка теоретичних і практичних засад щодо налаштування та оптимізації корпоративної мережі на основі технології VLAN. Для досягнення цієї мети передбачається виконати такі завдання: провести аналіз сучасних стандартів і методів впровадження VLAN у корпоративному середовищі; дослідити існуючий стан та основні проблеми мережевої інфраструктури підприємства; визначити вимоги до інформаційної безпеки, продуктивності та масштабованості мережі; обґрунтувати вибір оптимальної топології та

підходів до сегментації; розробити рекомендації щодо впровадження, адміністрування й моніторингу VLAN[1] для підвищення ефективності роботи та захисту корпоративної інформації.

Таким чином, виконання цієї роботи дозволить сформувати комплексний підхід до проєктування та модернізації корпоративних мереж із використанням VLAN, що відповідає сучасним вимогам безпеки, продуктивності й гнучкості, а також забезпечує готовність підприємства до подальшого розвитку й масштабування.

1 ТЕОРЕТИЧНІ ОСНОВИ ТЕХНОЛОГІЇ VLAN ТА ЇЇ ЗАСТОСУВАННЯ В КОРПОРАТИВНИХ МЕРЕЖАХ

1.1 Концепція віртуальних локальних мереж (VLAN)

Віртуальні локальні мережі (VLAN) стали одним із ключових інструментів сучасної мережевої архітектури, які дають змогу подолати традиційні обмеження фізичної топології і зробити мережу максимально гнучкою, масштабованою та безпечною. Концепція VLAN передбачає створення логічних груп пристроїв, незалежно від їх фактичного розташування у структурі фізичної мережі[2]. Це означає, що користувачі одного департаменту, які розташовані в різних корпусах або навіть будівлях, можуть взаємодіяти так, ніби підключені до однієї й тієї ж мережі, при цьому залишаючись ізольованими від інших відділів. Подібна ізоляція стає можливою завдяки створенню окремих широкомовних доменів, у межах яких трафік залишається локалізованим і не потрапляє до інших сегментів мережі. Це, у свою чергу, не лише покращує безпеку, але й зменшує кількість зайвих широкомовних повідомлень, підвищуючи ефективність використання мережевих ресурсів.

Основна ідея VLAN полягає у логічному об’єднанні мережевих пристроїв на основі організаційних, функціональних або безпекових принципів, а не фізичної близькості чи підключення до конкретних портів мережевого обладнання. Таке розмежування дає мережевим адміністраторам безпрецедентну гнучкість у керуванні доступом, зміні структури мережі та впровадженні нових політик без необхідності перепідключення кабелів чи переустановлення обладнання. Зміни у структурі компанії, переїзди співробітників, злиття підрозділів чи поява нових робочих груп більше не потребують трудомістких маніпуляцій з фізичною інфраструктурою: достатньо змінити налаштування VLAN на комутаторі, і пристрої

автоматично потрапляють у потрібний логічний сегмент.

Впровадження VLAN у корпоративному середовищі забезпечує низку важливих переваг. По-перше, йдеться про ефективну сегментацію трафіку, яка дозволяє не лише ізолювати трафік певних груп користувачів, а й значно скоротити кількість широкомовних розсилок у загальному мережевому просторі. Це особливо актуально для великих організацій, де широкомовні домени, що охоплюють сотні пристроїв, можуть суттєво впливати на пропускну здатність мережі. По-друге, VLAN підвищує рівень безпеки корпоративної інфраструктури. Розділення трафіку на рівні комутаторів дозволяє обмежити потенційні атаки та витоки інформації. Наприклад, якщо зловмисник підключиться до фізичної мережі компанії, він все одно не отримає доступу до критичних сервісів чи конфіденційних даних інших підрозділів, якщо ці ресурси знаходяться у різних VLAN. По-третє, гнучкість адміністрування мережі значно зростає, оскільки тепер адміністратор має можливість оперативно змінювати налаштування доступу для груп пристроїв, не змінюючи фізичну топологію.

Окрім ізоляції трафіку й підвищення безпеки, впровадження VLAN сприяє оптимізації використання мережевих ресурсів. Завдяки логічній структурі можна мінімізувати кількість необхідного обладнання, уникнути дублювання мережевих сегментів і, відповідно, знизити експлуатаційні витрати. Масштабованість є ще однією суттєвою перевагою: додавання нових пристроїв або робочих груп відбувається шляхом простого внесення змін у конфігурацію комутаторів, а не шляхом закупівлі нових фізичних пристроїв чи перекладання кабельних трас. У сучасних корпоративних мережах важливою є також підтримка централізованої реалізації політик доступу та контролю. VLAN дозволяє застосовувати ці політики на логічному рівні: наприклад, адміністратор може задати різні правила доступу до ресурсів мережі для різних підрозділів, навіть якщо співробітники працюють у спільному офісному просторі.

Існує декілька основних принципів формування VLAN у

корпоративних мережах. Найбільш поширеним підходом є використання портових VLAN (port-based VLAN), коли кожен фізичний порт комутатора жорстко призначається до певної VLAN. Цей спосіб найбільш простий в адмініструванні, проте не завжди гнучкий, особливо у динамічних середовищах, де робочі місця та пристрої можуть змінюватись досить часто. Для більш гнучкого керування мережевою інфраструктурою існують також протокольні VLAN (protocol-based VLAN)[3,4], які формуються на основі мережевого протоколу, що використовується пристроєм. Ще один підхід — MAC-based VLAN, коли розподіл у VLAN відбувається на основі MAC-адреси пристрою, що дозволяє організовувати сегментацію незалежно від того, який порт використовується. Для середовищ, де ключову роль відіграє адресний простір, актуальним є підхід subnet-based VLAN, коли об’єднання віртуальних сегментів ґрунтується на IP-підмережах.

Особливістю VLAN є також розподіл на статичні та динамічні типи. У статичних VLAN призначення портів до певної VLAN виконується вручну і залишається незмінним, поки адміністратор самостійно не внесе зміни. Це підходить для середовищ зі стабільною структурою. У динамічних VLAN розподіл відбувається автоматично, на основі певних правил або спеціальних протоколів — наприклад, GVRP (GARP VLAN Registration Protocol) або VTP (VLAN Trunking Protocol), що дає змогу масштабувати мережу без зайвих витрат часу та зусиль.

Порівняння VLAN з традиційними підходами до організації локальних мереж яскраво ілюструє суттєву різницю у можливостях масштабування, гнучкості та безпеки. Традиційна мережа побудована за принципом фізичної ізоляції: для кожної робочої групи чи підрозділу створюється окремий фізичний сегмент, що потребує прокладання додаткових кабельних трас, використання окремих комутаторів і часто — дублювання обладнання. У випадку зростання компанії або зміни структури організації, подібний підхід стає малоефективним, оскільки будь-які зміни потребують фізичного втручання і можуть призвести до збоїв у роботі мережі. Крім того, у

традиційній архітектурі широкомовний трафік не ізольований між різними сегментами, що призводить до перевантаження мережі й зниження продуктивності.

Впровадження VLAN дає змогу побудувати логічно ізольовані сегменти у межах однієї фізичної мережі, завдяки чому трафік між різними підрозділами чи групами користувачів не змішується, і зловмисник із одного сегменту не може легко атакувати пристрої іншого. Масштабування мережі, додавання нових пристроїв або переміщення робочих місць перетворюється з проблеми на просту адміністративну задачу. Адміністратор змінює лише логічну конфігурацію на комутаторах, а не фізичне підключення пристроїв.

Сучасний підхід до побудови корпоративних мереж ґрунтується саме на принципах логічної сегментації за допомогою VLAN. Це дозволяє компаніям оперативно реагувати на зміни в організаційній структурі, легко масштабувати ресурси і впроваджувати нові сервіси, а також забезпечувати належний рівень інформаційної безпеки, що є критичним для бізнесу в умовах постійного зростання кіберзагроз.

Окрім базової ізоляції, VLAN відкриває широкі можливості для централізованого контролю та застосування розширених політик управління доступом, що робить цю технологію незамінною у сучасних мережевих інфраструктурах. Логічна сегментація дозволяє не лише ізолювати мережевий трафік, але й реалізовувати різні рівні доступу до ресурсів, застосовувати окремі правила контролю для окремих груп чи навіть окремих пристроїв, що підвищує рівень безпеки корпоративної мережі загалом.

Підсумовуючи, можна стверджувати, що концепція VLAN докорінно змінила підхід до організації локальних мереж у корпоративному середовищі, дозволивши поєднати гнучкість, безпеку, ефективність та простоту адміністрування. Саме завдяки VLAN сучасні організації мають можливість динамічно адаптувати мережеву інфраструктуру під свої поточні та майбутні бізнес-потреби без значних фінансових та часових витрат, що забезпечує конкурентні переваги та підвищує стійкість до зовнішніх та

внутрішніх викликів.

1.2 Технічні аспекти реалізації VLAN

Технологічна основа для впровадження віртуальних локальних мереж у корпоративних середовищах базується на ретельно розроблених стандартах, протоколах і апаратних рішеннях, які взаємодіють між собою для створення єдиного логічного простору з високим рівнем ізоляції, масштабованості та безпеки. Еволюція цієї технології почалася наприкінці 90-х років, коли класичні фізичні схеми побудови мереж вичерпали свій потенціал щодо масштабованості та ефективного розмежування трафіку. Виникнення великої кількості підрозділів, нових офісних локацій та бізнес-вимог щодо ізоляції і контролю потоків даних вимагало абсолютно нового підходу до побудови мережевої інфраструктури.

Ключовим кроком стало створення міжнародного стандарту IEEE 802.1Q[5], який визначив формат тегування Ethernet-кадрів з метою логічної ідентифікації належності трафіку до конкретної VLAN. У традиційному Ethernet-кадрі немає жодної інформації про логічний сегмент, до якого він належить. Стандарт 802.1Q додає до кожного кадру чотирибайтовий тег, який включає поле Tag Protocol Identifier (TPID)[6], що дорівнює 0x8100, а також поле Tag Control Information (TCI), де міститься VLAN ID (12 біт), пріоритет (3 біти) та службова інформація. Таким чином, будь-який кадр, що мандрує мережею, може бути однозначно віднесений до певної логічної мережі незалежно від маршруту його проходження. Сучасні комутатори, що підтримують 802.1Q, автоматично додають і зчитують цей тег, виконуючи розподіл, фільтрацію й маршрутизацію кадрів відповідно до поточних політик безпеки й адміністрування.

Стандарт 802.1Q зробив можливим функціонування десятків і навіть сотень VLAN на одній фізичній інфраструктурі, оскільки 12 біт дозволяють ідентифікувати до 4096 окремих віртуальних мереж. Однак у реальних

мережах зазвичай використовується набагато менше VLAN, оскільки це обмежується структурою організації, кількістю підрозділів, типом додатків і політиками безпеки. Класична модель побудови VLAN ґрунтується на двох типах портів комутаторів: access-порти та trunk-порти. Access-порт підключає кінцевий пристрій (комп'ютер, принтер, камеру спостереження тощо) до лише однієї конкретної VLAN і не пропускає тегований трафік. Усі кадри, що надходять із access-порту, автоматично маркуються як належні до певної VLAN, і навпаки — всі кадри, що виходять на такий порт, надходять до пристрою у стандартному, нетегованому вигляді. Trunk-порт, на відміну від access, передає між комутаторами або між комутатором і маршрутизатором трафік багатьох VLAN. На trunk-порту всі кадри, крім трафіку Native VLAN, мають тег 802.1Q. Це дозволяє ефективно об'єднувати велику кількість логічних сегментів в єдиній фізичній інфраструктурі, зберігаючи ізоляцію трафіку та можливість централізованого адміністрування.

Особливу увагу слід приділити концепції Native VLAN, яка виникла як компроміс між необхідністю тегування і сумісністю з обладнанням, що не підтримує 802.1Q. Якщо на trunk-порту надійшов нетегований кадр, комутатор інтерпретуєйцц його як кадр, що належить до Native VLAN. За замовчуванням це VLAN 1, але з міркувань безпеки в сучасних мережах її змінюють і виділяють для цього окрему неадміністративну VLAN. Однак така функціональність може стати об'єктом атак, зокрема VLAN Hopping, коли зловмисник намагається через некоректно налаштовані trunk-порти проникнути в інші логічні сегменти. Тому розробка політик управління Native VLAN та суворе обмеження її використання належить до найважливіших аспектів побудови безпечної мережі.

Ще одним базовим елементом технічної реалізації VLAN є протоколи динамічного адміністрування та розповсюдження інформації про віртуальні мережі. У мережах з великим числом комутаторів ручне налаштування VLAN на кожному пристрої стає малоефективним, схильним до помилок і

важким для масштабування. Для спрощення цього процесу в обладнанні Cisco був реалізований протокол VLAN Trunking Protocol (VTP), який дозволяє централізовано створювати, редагувати й видаляти VLAN на одному комутаторі з автоматичною синхронізацією змін по всіх пристроях у межах одного VTP-домену. Аналогічну функцію у мультивендорних середовищах виконує GVRP (GARP VLAN Registration Protocol)[7], що дозволяє комутаторам різних виробників динамічно реєструвати інформацію про наявні VLAN, автоматично додаючи чи видаляючи відповідні конфігурації. Втім, ці протоколи несуть і потенційні ризики: помилкове або несанкціоноване видалення VLAN на одному пристрої призведе до втрати доступу до цього сегменту по всій мережі, тому критично важливими є обмеження прав адміністраторів і регулярне резервне копіювання конфігурацій.

Велику роль у забезпеченні ефективної роботи VLAN відіграє також ретельне планування топології та розподілу портів, особливо в ієрархічних мережах з великою кількістю рівнів комутації. На практиці доступні підходи до організації портів можуть комбінуватися залежно від типу мережі: у дата-центрах часто використовують одночасно access-, trunk- і навіть hybrid-порти, що дозволяють адаптуватися до різних типів трафіку й політик безпеки. Окремо варто згадати таке поняття, як Private VLAN (PVLAN), що дозволяє створити додаткові рівні ізоляції навіть у межах однієї VLAN — наприклад, щоб сервери могли бачити шлюз, але не мали прямого доступу один до одного. Це особливо актуально для хмарних сервісів, хостинг-провайдерів і корпоративних центрів обробки даних.

Не менш важливою є і проблема сумісності мережевого обладнання, яка іноді стає стримуючим чинником для впровадження VLAN у гетерогенних інфраструктурах. Хоча більшість сучасних комутаторів і маршрутизаторів підтримують 802.1Q і відповідні механізми тегування, на практиці трапляються ситуації з неповною або специфічною реалізацією протоколів, що потребує додаткового тестування й уніфікації політик у

багатовендорних середовищах.

Варто зазначити, що створення й підтримка складних ієрархічних мереж на базі VLAN вимагає не лише коректної конфігурації, а й постійного моніторингу стану мережі, журналювання змін, проведення аудиту налаштувань і своєчасного оновлення програмного забезпечення мережевих пристроїв. Для цього використовуються спеціалізовані системи управління й автоматизації (наприклад, Cisco DNA Center, SolarWinds, PRTG)[8], що дозволяють централізовано відслідковувати статус VLAN, оперативно реагувати на відмови чи аномалії у передачі трафіку, а також виконувати аналіз широкомовних штормів і інших типових проблем.

Нарешті, окремим важливим аспектом залишається питання відповідності технічної реалізації VLAN вимогам інформаційної безпеки підприємства. VLAN дає змогу чітко відмежовувати внутрішній службовий трафік, гостьовий доступ, робочі групи й критично важливі сервіси (наприклад, бухгалтерія чи сервери обліку) в окремі логічні домени, для яких можна впроваджувати різні політики доступу, списки контролю доступу (ACL), додаткові заходи моніторингу і шифрування даних. Це не лише мінімізує ризики витоку або компрометації інформації, а й полегшує проведення розслідувань інцидентів, ізоляцію джерел атак і впровадження сучасних систем виявлення вторгнень (IDS/IPS).

Таким чином, технічна реалізація VLAN — це багаторівневий процес, що базується на гармонійному поєднанні міжнародних стандартів, апаратних рішень, протоколів керування та гнучких сценаріїв адміністрування. Грамотне впровадження цієї технології забезпечує не лише ефективну сегментацію мережевого простору, але й створює фундамент для майбутнього розвитку корпоративної інфраструктури в умовах цифрової трансформації, масштабування й підвищених вимог до кібербезпеки.

1.3 Інтеграція VLAN з іншими мережевими технологіями

Інтеграція віртуальних локальних мереж із сучасними мережевими технологіями відкриває перед корпоративною інфраструктурою новий рівень функціональності, безпеки та керованості. Сьогодні VLAN уже не сприймається як ізольований інструмент для простої сегментації трафіку — ця технологія органічно вплітається у складну екосистему корпоративних мереж, взаємодіє з протоколами маршрутизації, системами забезпечення якості обслуговування, засобами централізованого керування і автоматизації, а також з хмарними й віртуалізованими платформами.

Однією з ключових задач у побудові сучасної корпоративної мережі є організація взаємодії між різними VLAN. За своєю природою VLAN працюють на канальному рівні моделі OSI, забезпечуючи ізоляцію трафіку, але часто виникає необхідність забезпечити комунікацію між різними сегментами. Для цього застосовується міжвланова маршрутизація, яку реалізують як за допомогою класичних маршрутизаторів, так і через багатофункціональні Layer 3 комутатори. Найбільш типовий сценарій — це використання так званої схеми “Router-on-a-Stick”, коли маршрутизатор через trunk-інтерфейс приймає трафік з різних VLAN, обробляє його та здійснює маршрутизацію відповідно до заданих політик. Однак із розвитком мережевого обладнання з’явилися Layer 3 комутатори, які виконують функції маршрутизації безпосередньо на рівні комутатора, забезпечуючи більшу швидкість і гнучкість, що особливо важливо для великих та навантажених мереж.

У сучасних мережах VLAN часто поєднується із системами забезпечення якості обслуговування — Quality of Service (QoS). Це критично важливо для додатків із підвищеними вимогами до затримок і стабільності з’єднання, наприклад, для IP-телефонії, відеоконференцій, потокового відео чи хмарних сервісів. Впровадження VLAN дозволяє сегментувати мережу таким чином, щоб трафік “чутливих” додатків ізолювався від масового

трафіку (наприклад, web-серфінгу чи пересилання великих файлів), а завдяки тегуванню 802.1p можна призначити різні пріоритети для різних класів трафіку, що дає змогу ефективно керувати пропускною здатністю, уникати перевантажень та гарантувати якість сервісу. Адміністратор отримує можливість задати правила для кожної VLAN — наприклад, зарезервувати смугу пропускання для телефонії, обмежити максимум для гостьового Wi-Fi або впровадити політику “zero trust” для підозрілих сегментів.

Особливе місце у розвитку мережевої архітектури займають сучасні концепції автоматизації та централізованого керування, такі як Software-Defined Networking (SDN). У SDN архітектурі VLAN стає не просто способом ізоляції трафіку, а елементом гнучкої логічної структури, яку централізовано контролює SDN-контролер. Це забезпечує високий рівень адаптивності: додавання, зміна чи видалення VLAN може виконуватися в реальному часі на сотнях пристроїв без втручання людини — достатньо змінити відповідну політику на контролері. За допомогою API, скриптів (наприклад, на Python чи Ansible) та інтеграції із зовнішніми системами моніторингу можна впроваджувати складні сценарії автоматичного масштабування, балансування навантаження або реагування на інциденти безпеки. У великих дата-центрах та хмарних платформах VLAN дозволяє створювати багатокористувацькі середовища з ізольованими мережевими просторами, динамічно змінювати топологію мережі, оперативно реагувати на зростання чи зменшення навантаження та підвищувати рівень обслуговування відповідно до бізнес-вимог.

Віртуальні мережі відіграють надзвичайно важливу роль у забезпеченні інформаційної безпеки корпоративної мережі. Логічна сегментація дозволяє ізолювати критичні сервіси (наприклад, бухгалтерію, сервери домену, внутрішні додатки) від менш захищених або зовнішніх зон (гостьовий Wi-Fi, публічні сервери, IoT-пристрої). Це мінімізує ризики несанкціонованого доступу, стрімкого поширення шкідливого програмного забезпечення, атак типу “man-in-the-middle” та інших кіберзагроз. Додатково у VLAN-

структурах впроваджують списки контролю доступу (Access Control Lists, ACL)[9], правила firewall, багаторівневу аутентифікацію, моніторинг аномальної активності та інші засоби захисту. Адміністратор має можливість тонко налаштовувати політики маршрутизації, дозволяючи чи забороняючи певні типи трафіку між окремими сегментами мережі відповідно до принципу “найменших повноважень”. У поєднанні з механізмами Private VLAN (PVLAN), ізоляція може бути реалізована навіть усередині одного великого сегменту, наприклад, для клієнтів у хмарній інфраструктурі.

Інтеграція VLAN із сучасними мережевими технологіями також актуальна для гібридних інфраструктур, де ресурси компанії розподілені між локальними дата-центрами, публічними та приватними хмарами. Хмарні платформи активно використовують VLAN для сегментації клієнтських середовищ, ізоляції сервісів, організації тунелів для захищеного доступу та динамічного розподілу ресурсів. Завдяки гнучкості цієї технології можливо будувати єдиний керований простір із заданими політиками доступу, незалежно від того, де фізично розташовані сервери чи користувачі.

Таким чином, VLAN не лише забезпечує базову ізоляцію трафіку, а й слугує фундаментом для розгортання складних, масштабованих, безпечних і динамічних мереж, де важливе місце займають автоматизація, захист, якість сервісу та централізований контроль. Віртуальні мережі інтегруються із системами маршрутизації, протоколами динамічного управління, хмарними платформами й сучасними технологіями автоматизації, утворюючи інноваційну архітектуру, що відповідає сучасним бізнес-викликам та вимогам інформаційної безпеки.

1.4 Сучасні тенденції розвитку VLAN-технологій

Сучасний розвиток технології VLAN відображає загальні тенденції еволюції корпоративних мереж і поступово виводить концепцію логічної сегментації трафіку на якісно новий рівень. Традиційна ідея ізоляції трафіку

на базі віртуальних мереж поступово збагачується новими протоколами, автоматизованими механізмами керування та можливістю гнучкої інтеграції з хмарними й віртуалізованими середовищами. Це відповідає новим викликам цифрової трансформації бізнесу, де пріоритетом стають масштабованість, швидкість розгортання сервісів, кібербезпека та централізоване управління інфраструктурою.

Першим великим кроком у розвитку VLAN стала поява стандарту IEEE 802.1Q, що забезпечив можливість паралельного функціонування сотень логічних сегментів у межах однієї фізичної мережі. Але з часом вимоги корпоративних мереж ускладнювались, і з’явилась потреба не лише ізолювати трафік, а й створювати багаторівневі структури, розширювати масштабованість і керованість віртуальних мереж. На цю потребу відповів стандарт IEEE 802.1ad (Q-in-Q), який дозволяє вкладати одну VLAN у іншу. Це дало змогу провайдерам і великим організаціям створювати багатокористувацькі або багаторівневі мережеві інфраструктури, де логічний розподіл зберігається навіть на рівні орендарів або різних сервісів. Q-in-Q особливо актуальний у хмарних середовищах, у дата-центрах, а також у мультиорендованих мережах, де ізоляція клієнтських потоків є критично важливою для безпеки та стабільності.

Інтеграція VLAN із хмарними та гібридними інфраструктурами стала наступним етапом розвитку технології. Зростання популярності IaaS, PaaS і SaaS-рішень обумовило необхідність гнучко та швидко ізолювати мережевий трафік різних користувачів чи додатків, незалежно від їхнього місцезнаходження. Хмарні провайдери (AWS, Azure, Google Cloud, VMware Cloud Foundation тощо) активно використовують VLAN для організації ізольованих віртуальних мереж для кожного клієнта чи проєкту, гарантуючи безпечний та прогнозований рівень сервісу. На практиці це дозволяє створювати, масштабувати й видаляти цілі мережеві топології буквально за кілька хвилин або навіть секунд, повністю через програмні інтерфейси керування. У таких архітектурах VLAN стає не просто логічним

роздільником, а ключовим інструментом для побудови ізольованих середовищ розробки, тестування, експлуатації та підтримки критичних бізнес-сервісів.

Сучасні тенденції розвитку VLAN-технологій тісно пов’язані з автоматизацією та оркестрацією мережевих ресурсів. Впровадження підходів на кшталт Network as Code (мережа як код), використання скриптів на Python, систем управління конфігураціями (Ansible, Puppet, SaltStack), а також спеціалізованих платформ (Cisco DNA Center, Juniper Contrail, Arista CloudVision) дозволяє централізовано й автоматично створювати, змінювати та видаляти VLAN у масштабах усієї організації. Це значно знижує людський фактор, зменшує час на розгортання нових сервісів та оперативно реагує на зміну бізнес-потреб. Автоматизація також підвищує якість документації, дозволяє створювати резервні копії конфігурацій, швидко відновлювати інфраструктуру у разі збоїв чи кібератак, що особливо актуально у середовищах із високими вимогами до безпеки й відмовостійкості.

Окремою тенденцією стає поєднання VLAN з технологіями Software-Defined Networking (SDN), де мережеве обладнання перетворюється на керовану інфраструктуру, а логічні сегменти створюються й змінюються централізовано через SDN-контролер. У SDN-мережах адміністратор керує всією топологією, політиками доступу, балансуванням трафіку й безпековими правилами через єдиний інтерфейс — як у локальних дата-центрах, так і у хмарі. Це дає змогу динамічно реагувати на атаки, змінювати маршрутизацію, впроваджувати нові сервіси або масштабувати інфраструктуру без втручання у фізичну топологію. У таких сценаріях VLAN використовується для побудови ізольованих віртуальних мереж для клієнтів, підрозділів чи додатків, для відділення службових і користувацьких потоків, а також для реалізації багаторівневого доступу до ресурсів.

Варто підкреслити, що сучасний розвиток VLAN супроводжується зростанням вимог до кібербезпеки. Віртуальні мережі дедалі частіше стають не просто інструментом ізоляції, а базовою складовою комплексних систем

захисту корпоративної інфраструктури. У поєднанні з Private VLAN, міжмережевими екранами нового покоління, системами IDS/IPS та засобами мікросегментації, VLAN дозволяє створювати мережі з принципово новим рівнем контролю трафіку й доступу. Це особливо важливо для критичних секторів, банків, державних структур, дата-центрів і великих компаній.

У майбутньому розвиток VLAN-технологій тісно пов’язаний із подальшою інтеграцією із сервісами штучного інтелекту для автоматичного моніторингу й аналізу аномалій, застосуванням принципів Zero Trust, а також із поєднанням традиційних підходів сегментації з сучасними методами контейнеризації, багаторівневого шифрування й політик динамічного доступу. Дедалі більшої популярності набувають рішення, що дозволяють автоматично створювати й знищувати логічні мережі “на льоту”, залежно від потреб проєктів, робочих навантажень чи поведінки користувачів. Нові стандарти й підходи, такі як EVPN (Ethernet VPN), VXLAN (Virtual Extensible LAN), спрямовані на подолання традиційних обмежень VLAN щодо масштабування у великих хмарних середовищах та побудову truly глобальних віртуальних мереж.

Підсумовуючи, можна стверджувати, що сучасна технологія VLAN вже давно вийшла за межі класичного розуміння віртуальних мереж. Вона стала гнучким, масштабованим, керованим та захищеним інструментом, без якого неможливе існування сучасних корпоративних, хмарних та гібридних інфраструктур. Її розвиток продовжує визначати стандарти цифрової трансформації, оркестрації сервісів, кібербезпеки та інноваційної архітектури майбутніх мереж.

2 АНАЛІЗ ПОТОЧНОГО СТАНУ ТА ВИМОГ ДО МЕРЕЖІ ПІДПРИЄМСТВА

2.1 Огляд існуючої інфраструктури підприємства

Сучасна корпоративна мережа — це складна багаторівнева система, яка інтегрує численні апаратні й програмні компоненти з різними функціональними ролями, забезпечуючи безперервну та безпечну взаємодію між користувачами, сервісами, серверними й периферійними пристроями. Аналізуючи існуючу інфраструктуру підприємства, слід враховувати всі аспекти її побудови: топологію, інвентаризацію обладнання, фізичний рівень, засоби керування й моніторингу, а також загальний стан підтримки стандартів сучасних мереж.

На фундаментальному рівні топологія корпоративної мережі найчастіше будується за принципом трирівневої ієрархії. Ядро мережі або Core Layer — це центральна артерія, через яку проходить основний трафік організації. Тут розташовані найбільш продуктивні комутатори із резервуванням усіх ключових вузлів, що забезпечує не лише гігабітну або навіть багатогігабітну швидкість передавання даних, але й мінімальні затримки, відмовостійкість і надмірність, завдяки чому мережа залишається доступною навіть у разі збоїв. Усе обладнання цього рівня повинно відповідати найсучаснішим стандартам і підтримувати стекування, віртуалізацію, маршрутизацію третього рівня, розвинену роботу з таблицями MAC-адрес, а також забезпечувати високу пропускну здатність backplane для роботи з трафіком великих обсягів.

Від ядра відгалужуються рівні розподілу (Distribution Layer) і доступу (Access Layer). Рівень розподілу відіграє роль проміжного вузла між ядром та “краєм” мережі, агрегації трафіку від безлічі підключених до Access Layer комутаторів. Саме тут реалізуються політики безпеки, маршрутизації між

VLAN, QoS, фільтрація трафіку та балансування навантаження. Розподільчі комутатори, на відміну від доступових, мають потужніші процесори, підтримку динамічних протоколів маршрутизації, гнучке впровадження ACL (Access Control Lists) та засобів traffic shaping. Вони часто мають модульну конструкцію й здатність до розширення, що полегшує масштабування мережі при зростанні кількості користувачів або додаткових сервісів.

Рівень доступу безпосередньо забезпечує підключення кінцевих пристроїв: комп'ютерів, телефонів, принтерів, камер відеоспостереження, IoT-пристроїв тощо. Саме тут формується найбільша щільність портів, забезпечується підтримка PoE (Power over Ethernet) для живлення активних пристроїв без додаткових джерел електроенергії, впроваджуються засоби VLAN-сегментації та контроль автентифікації користувачів. Доступові комутатори, окрім кількості портів, повинні забезпечувати стабільну роботу із засобами захисту, підтримку технологій аутентифікації 802.1X, можливість централізованого управління й моніторингу через SNMP, а також інтеграцію з голосовими VLAN для IP-телефонії.

Щоб точно оцінити поточний стан інфраструктури, необхідна повна інвентаризація обладнання, що використовується на кожному рівні. Для ядра це потужні комутатори з розширеною підтримкою Layer 3, стекуванням, великим розміром таблиць MAC/ARP, широким набором SFP+/QSFP портів для гігабітних і багатогігабітних підключень. Рівень розподілу включає модульні або stackable Layer 2/3 комутатори з підтримкою різних протоколів маршрутизації (OSPF, EIGRP, BGP), multicast-функціоналом, ACL, портовою безпекою й QoS. Access Layer комутатори характеризуються найбільшою кількістю портів, підтримкою PoE/PoE+, функціями автентифікації на портах, можливістю швидкої VLAN-конфігурації, управлінням через web-інтерфейс і SNMP.

Окремої уваги заслуговують маршрутизатори, які забезпечують підключення до зовнішніх мереж (Інтернет, MPLS, VPN). Вони повинні підтримувати широкий спектр WAN-інтерфейсів, функціонал NAT і firewall,

гнучкі політики маршрутизації, шифрування (IPSec, SSL VPN), а також високу пропускну здатність, що відповідає зростаючим обсягам корпоративного трафіку. У складі інфраструктури також широко використовуються бездротові точки доступу з підтримкою сучасних стандартів Wi-Fi (802.11ac, 802.11ax), множинних SSID та VLAN, централізованим керуванням, автентифікацією WPA2/WPA3-Enterprise і PoE-живленням[10].

Фізичний рівень мережі неможливо ігнорувати під час аналізу — якість і стан кабельної системи безпосередньо визначають можливості впровадження сучасних мережевих сервісів. У типовій корпоративній мережі виділяють два основних види кабелів: магістральні, які з’єднують між собою будівлі, поверхи чи віддалені точки, і горизонтальні — для підключення робочих місць до шаф. Магістралі виконуються, як правило, на основі оптоволокна (OM3, OM4, одномодові кабелі), що дозволяє отримати високу швидкість і мінімальні втрати сигналу навіть на великих відстанях. Для горизонтальної підсистеми найчастіше використовують мідні кабелі категорії 5e, 6 або 6A, що забезпечують гігабітні й навіть 10-гігабітні швидкості на відстанях до 100 метрів. Якість патч-кордів, стан комутаційних панелей, акуратність маркування — усе це впливає на надійність та продуктивність мережі. Обов’язковим є регулярне тестування пропускної здатності, виявлення обривів, коротких замикань, перевірка відповідності міжнародним стандартам (TIA/EIA, ISO/IEC), а також наявність детальної документації всіх з’єднань. Телекомунікаційні шафи і стійки повинні бути правильно організовані: забезпечене ефективне охолодження, надійне електроживлення з резервуванням, фізичний захист від несанкціонованого доступу.

Ще однією критичною складовою інфраструктури є системи управління та моніторингу. Вони виконують функцію “нервової системи” корпоративної мережі, дозволяючи в реальному часі отримувати інформацію про стан обладнання, навантаження на інтерфейси, аномалії в роботі пристроїв, зміни конфігурацій та інциденти безпеки. Найбільш поширеними

технологіями є SNMP для збору статистики, NetFlow та sFlow для аналізу трафіку, а також syslog для централізованого збору подій. Через такі системи адміністратори можуть аналізувати продуктивність мережі, бачити структуру трафіку, джерела пікового навантаження, швидко реагувати на відмови, блокувати підозрілу активність і планувати модернізацію. Використання систем централізованого управління (NMS) забезпечує графічне відображення топології, автоматизацію рутинних задач, централізоване налаштування обладнання, контроль версій конфігурацій, генерацію звітів та інші інструменти для підтримки стабільної роботи мережі. Автоматизація резервного копіювання та відновлення конфігурацій після збоїв значно скорочує час простою та втрати для бізнесу.

Інфраструктура сучасного підприємства — це не лише сукупність фізичних пристроїв, кабелів і програмних засобів, а й чітко організований механізм управління, що забезпечує гнучкість, масштабованість, високу продуктивність та захищеність корпоративної мережі у динамічних умовах розвитку бізнесу. Саме детальний і системний аналіз поточного стану цієї інфраструктури закладає основу для ефективного планування, впровадження сучасних технологій VLAN, автоматизації, підвищення рівня інформаційної безпеки та якості обслуговування мережевих сервісів.

2.2 Вимоги до інформаційної безпеки та сегментації трафіку

Вимоги до інформаційної безпеки та сегментації трафіку у сучасних корпоративних мережах обумовлені широким спектром загроз, зростаючою складністю архітектури, а також необхідністю дотримання суворих міжнародних і національних регуляторних норм. Інформаційна безпека стала критично важливою не лише для захисту інтелектуальної власності чи комерційних таємниць, а й для збереження репутації компанії, забезпечення безперервності бізнесу та уникнення фінансових втрат у разі інцидентів. Сучасна корпоративна мережа стикається як із зовнішніми, так і з

внутрішніми загрозами. З одного боку, працівники компанії можуть випадково або навмисно ініціювати витік або компрометацію даних через несумлінне дотримання політик безпеки, слабкі паролі, відсутність многофакторної автентифікації, використання особистих пристроїв, інсталювання несанкціонованого програмного забезпечення або спробу отримати доступ до інформації, яка виходить за межі їх посадових обов'язків. З іншого боку, організація піддається постійному ризику зовнішніх атак: це сканування мережі, експлуатація відомих вразливостей, фішингові кампанії, розповсюдження вірусів та шкідливого програмного забезпечення, атаки типу "brute force", а також складні багаторівневі атаки Advanced Persistent Threats, які можуть тривати роками та бути спрямовані на цілеспрямований витік інформації або саботаж.

Особливу увагу в корпоративних мережах приділяють специфічним ризикам, що виникають при впровадженні VLAN. Хоча віртуальна сегментація дозволяє суттєво підвищити ізоляцію, існують технології і атаки, які спрямовані на обхід логічних меж — такі як VLAN Hopping, Switch Spoofing, Double Tagging чи MAC Flooding. Вони дозволяють зловмиснику отримати доступ до трафіку інших сегментів або перехопити пакети з різних VLAN, якщо обладнання або політики неправильно налаштовані чи не оновлені.

Для ефективного захисту організації політики безпеки повинні базуватися на комплексному багаторівневому підході. Важливо впроваджувати принцип найменших привілеїв, коли кожен користувач чи пристрій має лише ті права, які необхідні для виконання службових завдань. Сегментація на рівні VLAN дає змогу чітко розмежувати доступ між різними групами: наприклад, адміністративний персонал, фінансовий відділ, технічна підтримка, розробка, відділ продажів та маркетингу мають окремі сегменти з суворо регламентованою можливістю міжвланового обміну, що реалізується через міжмережеві екрани, ACL або проксі. Аналогічно серверна інфраструктура виділяється у власні VLAN для веб-серверів, баз даних,

файлових ресурсів, систем резервного копіювання чи тестового середовища. Додатково, для специфічних задач впроваджуються спеціальні сегменти: Voice VLAN для IP-телефонії, Guest VLAN для відвідувачів, Management VLAN для адміністрування обладнання, DMZ VLAN для публічних сервісів.

Архітектура безпеки сучасної мережі має відображати поділ інфраструктури на різнорівневі зони довіри. Зона високої довіри (Trusted Zone) призначена для найкритичніших систем, які містять конфіденційні дані та сервіси з підвищеним рівнем захисту. В цю зону потрапляють сервери управління, сервери резервного копіювання, системи моніторингу безпеки, і доступ до них суворо обмежується ідентифікованими адміністраторами. Напівдовірена зона (Semi-Trusted Zone)[11,12] містить робочі місця користувачів, файлові сервери підрозділів, принтери, і доступ до них контролюється відповідно до ролей і службових функцій. Низькодовірена зона (Untrusted Zone) охоплює гостьові мережі, публічні точки Wi-Fi, демілітаризовану зону для зовнішніх сервісів, і тут діють максимальні обмеження, ізоляція та суворий моніторинг.

Особливої ваги набуває мікросегментація — деталізований поділ навіть усередині однієї зони для ізоляції окремих додатків, служб чи навіть індивідуальних пристроїв. Це дозволяє впроваджувати Zero Trust архітектуру, де жоден користувач або сервіс не отримує довіру за замовчуванням, а кожен сеанс перевіряється незалежно. Мікросегментація стає все більш актуальною у віртуалізованих і хмарних середовищах, де кількість сервісів і взаємозв’язків постійно зростає.

Для організації ефективної сегментації й контролю доступу застосовують Network Access Control (NAC) — системи, які здійснюють автентифікацію пристроїв при підключенні, перевіряють їхню відповідність політикам безпеки, динамічно призначають VLAN, ізолюють пристрої у карантин у разі невідповідності вимогам. Централізоване управління обліковими записами, контроль життєвого циклу користувача, багатофакторна автентифікація і Single Sign-On реалізуються через системи

Identity and Access Management (IAM). Важливо не лише впровадити захист, а й забезпечити постійний моніторинг — збір і аналіз логів (SIEM), аналіз мережевого трафіку в реальному часі (NDR), кореляція подій, форензичний аналіз і автоматичне реагування на інциденти.

Крім технологічних заходів, корпоративна мережа повинна відповідати вимогам міжнародних і галузевих стандартів, таких як ISO/IEC 27001/27002, NIST Cybersecurity Framework, PCI DSS, HIPAA, SOX, а також національним законам на кшталт GDPR. Це означає впровадження жорстких політик ізоляції, шифрування, моніторингу, аудиту доступу до критичних ресурсів, а також організацію процесів управління інцидентами, відновлення після атак і забезпечення прав громадян на захист персональних даних.

Інформаційна безпека та сегментація трафіку — це не разова дія, а безперервний процес, який включає аналіз загроз, розробку й актуалізацію політик безпеки, впровадження технологічних і організаційних рішень, підвищення обізнаності персоналу, постійний моніторинг і аудит, дотримання стандартів та своєчасну реакцію на інциденти. Тільки комплексний підхід дозволяє ефективно захистити мережеву інфраструктуру підприємства в умовах зростаючих загроз, динамічних змін бізнесу і стрімкого розвитку інформаційних технологій.

2.3 Оцінка навантаження і типових сценаріїв використання мережі

Оцінка навантаження та типових сценаріїв використання мережі є критично важливою передумовою для проектування ефективної VLAN-структури й побудови оптимальної політики керування корпоративним трафіком. У сучасних умовах саме дані про реальні обсяги й характер трафіку, паттерни використання різними категоріями користувачів, сезонні та часові особливості роботи сервісів дозволяють обґрунтовано визначати вимоги до пропускної здатності, планувати модернізацію обладнання та забезпечувати необхідний рівень якості обслуговування (QoS) для критично

важливих бізнес-додатків.

Детальний аналіз трафіку проводиться із застосуванням спеціалізованих систем збору й обробки даних — таких як NetFlow, sFlow, SNMP, а також засобів глибокої інспекції пакетів. Flow-based аналіз дозволяє отримати інформацію про основних споживачів ресурсів, ідентифікувати найактивніші додатки, виявити аномальні сесії, підозрілі потоки чи потенційні загрози безпеки. SNMP моніторинг дає змогу контролювати завантаження портів, канали зв’язку, якість роботи інтерфейсів, виявляти втрати пакетів, оцінювати стан обладнання й ресурсів. Packet capture аналіз застосовується для глибокої діагностики складних інцидентів, розслідування атак або проблем із продуктивністю — тут фіксуються й досліджуються окремі пакети для виявлення причин затримок, помилок чи некоректної поведінки додатків.

Типові паттерни трафіку в корпоративному середовищі демонструють залежність від робочого часу, днів тижня, сезону, а також бізнес-циклів компанії. Під час робочих годин спостерігається максимальне навантаження на канали зв’язку — активно використовуються ERP, CRM, системи документообігу, корпоративна пошта, бізнес-аналітика, відбувається велика кількість автентифікацій, синхронізацій, відеоконференцій. У періоди обідньої перерви та позаробочий час частка ділового трафіку зменшується, натомість може зростати використання розважальних сервісів, соціальних мереж, потокового відео. У вихідні дні навантаження падає, натомість зростає інтенсивність планових робіт, резервного копіювання, оновлення програмного забезпечення. Особливості мережевого трафіку проявляються також у сезонних піках: кінець фінансового року — це збільшення активності у бухгалтерських і аналітичних системах, у періоди масштабних маркетингових кампаній чи запуску нових продуктів зростає трафік на веб-сервіси, портали самообслуговування, B2B ресурси. У географічно розподілених компаніях трафік між філіями суттєво впливає на магістральні канали, і саме тут виникає потреба у WAN-оптимізації, плануванні

пропускної здатності з урахуванням часових поясів, специфіки локальних і міжнародних операцій.

Ефективна VLAN-сегментація базується на чіткому розумінні ролі та критичності кожного додатку, сервісу, категорії користувачів для бізнесу. Критичні додатки — ERP, системи управління фінансами, основні операційні бази даних, корпоративна пошта, засоби миттєвої комунікації й відеозв'язку — повинні мати виділені ресурси, ізольовані сегменти, пріоритетний трафік, мінімальні затримки й високу доступність. Для цих сервісів актуальні вимоги до 99.9% доступності, підтримки цілісності даних, захисту від втрат і джиттера. Бізнес-важливі додатки — CRM, документообіг, корпоративні портали, B2B сервіси — мають забезпечувати стабільну продуктивність, надійний доступ і безпечну роботу, хоча можуть обслуговуватися в спільних сегментах з іншими бізнес-додатками. Стандартні додатки — офісні пакети, файлові сервіси, принт-сервіси — не потребують особливих умов, але мають гарантуватися у рамках загальної інфраструктури. Некритичні додатки — розважальний контент, особисте використання співробітників, соціальні мережі — мають обмежуватись за пропускною здатністю, отримувати найнижчий пріоритет, а іноді й блокуватися залежно від політики компанії.

Планування пропускної здатності каналів і ресурсів відбувається з урахуванням як поточних рівнів використання, так і прогнозованого зростання — як по кількості користувачів, так і по кількості сервісів. Збір історичних даних, аналіз піків і середніх значень дозволяють ідентифікувати "пляшкові горлечка", побачити тенденції росту й сезонні коливання. Для кожної VLAN визначаються нормативні значення: середнє використання для користувацьких сегментів, коефіцієнти перевикористання, пікове навантаження, резерви для зростання. Серверні VLAN розраховуються з урахуванням вимог основних сервісів, резервування каналів для backup-трафіку, обмеження коефіцієнтів перевантаження для критичних серверів. Voice VLAN для IP-телефонії вимагає суворого контролю затримок, втрат пакетів, джиттера та резерву пропускної здатності під кожен дзвінок.

Процес планування апгрейдів інфраструктури передбачає поетапну модернізацію: спочатку оновлення й резервування критичних вузлів, збільшення пропускної здатності магістралей, впровадження високопродуктивних комутаторів ядра, потім поступове оновлення обладнання на рівні розподілу (Layer 3, 10GbE uplink, маршрутизація між VLAN), і, нарешті, заміну комутаторів доступу, впровадження PoE+, розширення gigabit-портів. Бюджетування включає як капітальні витрати (закупівля обладнання, ліцензії, монтаж, навчання), так і операційні (сервіс, електроенергія, зарплати адміністраторів, оновлення ПЗ). Розрахунок повернення інвестицій базується на підвищенні продуктивності співробітників, зменшенні простоїв, економії на адмініструванні, покращенні комплаєнсу й безпеки.

Окремо слід враховувати поведінкові паттерни користувачів різних груп. Топ-менеджмент потребує мобільного доступу, пріоритетного трафіку, високої конфіденційності та можливості працювати з усіма корпоративними ресурсами з будь-якої точки. Менеджери середньої ланки інтенсивно використовують email, звіти, CRM/ERP, активно користуються мобільними пристроями, мають регулярний доступ до аналітики. Фінансовий персонал працює з великими обсягами даних, сезонними піками, критичними файлами та вимогами до аудиту. IT-персонал має адміністративний доступ, використовує специфічні інструменти, часто працює в нестандартний час, потребує високої пропускної здатності для задач адміністрування та моніторингу. Звичайні працівники — основний масив користувачів офісних програм, файлообміну, друку, мають обмежені права доступу до ресурсів.

Часові паттерни визначають піки та спади трафіку: ранкові години супроводжуються масовою автентифікацією, завантаженням пошти й синхронізацією файлів, вдень — інтенсивною роботою із бізнес-додатками, під час обідньої перерви — зростанням розважального трафіку, увечері — початком процедур backup та планових робіт IT-служби. Особливості BYOD і мобільної роботи створюють нові виклики: необхідність в ізольованих

гостьових VLAN, захищених VPN, підтримці широкого спектра пристроїв і підвищених вимог до безпеки.

Комплексний аналіз цих факторів дозволяє створити гнучку, масштабовану, продуктивну мережу, що здатна адаптуватися до змін бізнес-процесів, забезпечити якість обслуговування для критичних додатків і безпеку для всієї організації.

2.4 Визначення проблем і вузьких місць у наявній мережі

Аналіз продуктивності корпоративної мережі завжди є відправною точкою для виявлення слабких місць та визначення напрямків подальшої оптимізації. Систематичний моніторинг каналів зв’язку допомагає визначити сегменти з перевищенням критичних рівнів завантаження, наприклад, коли утилізація портів і інтерфейсів перевищує 70-80%. Особливої уваги потребують ті канали, де перевищення навантаження спостерігається протягом значної частини робочого дня або де фіксується асиметричний трафік, що може свідчити про нераціональний розподіл ресурсів чи неправильну маршрутизацію. Водночас рівень затримок, втрати пакетів і варіація затримки (джиттер) є ключовими показниками для забезпечення якості сервісу, особливо для real-time додатків — відеоконференцій, IP-телефонії, систем онлайн-обслуговування клієнтів. Аналіз проводиться як “end-to-end”, так і поетапно для кожного хопу, що дозволяє виявити окремі проблемні пристрої чи сегменти. Підвищені затримки, непередбачуваний джиттер або зростання втрат пакетів безпосередньо впливають на зниження якості користувацького досвіду та часто є симптомом перевантаження обладнання чи некоректної конфігурації.

Детальний аудит також дозволяє виявити вузькі місця, пов’язані з широкомовним трафіком — broadcast storms, які виникають через надмірний ARP-трафік, DHCP-запити чи широкомовні повідомлення службового характеру (наприклад, NetBIOS). Неправильна конфігурація комутаторів або

петлі у топології часто призводять до лавиноподібного розповсюдження broadcast-пакетів, що перевантажує процесори мережевих пристроїв і негативно впливає на роботу критично важливих сервісів. Впровадження VLAN дає змогу ефективно обмежити розповсюдження широкомовного трафіку, ізолювати проблемні сегменти та підвищити загальну стабільність мережі. Не менш важливою є сегментація для запобігання латеральному поширенню загроз — malware, несанкціонований доступ, витоки інформації можуть поширюватися мережею у разі відсутності ізоляції, особливо у “плоских” мережах без логічного поділу на зони. Крім цього, моніторинг уніфікованого трафіку складніший, а forensic-аналіз інцидентів ускладнюється через відсутність чіткої видимості та структурованості потоків.

Зі зростанням організації й кількості пристроїв виникають виклики масштабованості та управління, які є типовими для традиційних мережевих архітектур. Серед основних обмежень — фізична кількість портів на комутаторах, недостатність кабельної інфраструктури, складність додавання нових сегментів чи перепідключення користувачів через прив’язку до конкретного порту. Мануальне налаштування кожного інтерфейсу не тільки займає багато часу, але й підвищує ризики помилок та ускладнює документування конфігурацій. В умовах швидкої зміни організаційної структури та мобільності співробітників такі обмеження негативно впливають на гнучкість і адаптивність мережі. Відсутність централізованої системи управління призводить до неузгодженості конфігурацій, складнощів із резервуванням та відновленням, а також ускладнює масштабування команди адміністраторів і передачу знань у разі кадрових змін.

З економічної точки зору, традиційна мережа супроводжується значними капітальними та операційними витратами. До прямих витрат належать закупівля та ліцензування мережевого обладнання, монтаж кабельної інфраструктури, підтримка електроживлення й охолодження. Операційні витрати включають оплату праці IT-персоналу, витрати на

електроенергію, сервісне обслуговування, модернізацію. Додатково виникають непрямі витрати: втрати продуктивності через простої або повільну роботу додатків, затримки доступу до ресурсів, погіршення якості обслуговування клієнтів, а також ризики безпеки, які можуть призвести до серйозних фінансових збитків, штрафів, витрат на відновлення після інцидентів і втрату репутації. До витрат належать і час адміністрування, діагностики, внесення змін та навчання персоналу.

Порівняльний аналіз показує, що впровадження VLAN дозволяє істотно оптимізувати як капітальні, так і операційні витрати. Ефективніше використання наявного обладнання, уникнення дублювання інфраструктури, централізоване управління й автоматизація рутинних задач суттєво знижують витрати на масштабування та підтримку. VLAN також підвищують продуктивність і якість сервісів за рахунок гнучкішої сегментації, поліпшення показників доступності, оптимізації пропускної здатності та підвищення якості обслуговування real-time сервісів.

Аналізуючи ризики, пов’язані із поточною архітектурою, важливо враховувати як технічні, так і бізнес- та фінансові аспекти. Одиночні точки відмови, відсутність резервування, залежність від окремих критичних вузлів чи постачальників, вузькі місця у маршрутизації, перевантаження окремих сегментів, відсутність балансування навантаження — усе це створює загрозу збоїв та довгого відновлення після аварій. Плоска архітектура без сегментації ускладнює моніторинг, контроль доступу, створює ризики латерального поширення атак, не дозволяє впроваджувати принцип найменших привілеїв і швидко ізолювати скомпрометовані сегменти. Додатково, регуляторні вимоги щодо захисту персональних даних, ведення аудиту та відповідності стандартам compliance можуть залишатися невиконаними, що загрожує штрафами та санкціями. Бізнес-ризики пов’язані з операційною залежністю від ключових фахівців, складністю швидких змін, відсутністю гнучкості при організаційних трансформаціях чи інтеграції нових підрозділів.

Для мінімізації ризиків рекомендується поступова модернізація мережі:

впровадження моніторингу, створення інвентарю критичних компонентів, планування аварійного відновлення й навчання персоналу основам безпеки в короткостроковій перспективі. У середньостроковій перспективі доцільно поетапно впроваджувати VLAN-сегментацію, модернізувати критичні вузли, впроваджувати резервування й формалізувати політики безпеки. У довгостроковій — проводити повну модернізацію інфраструктури, автоматизувати управління, інтегрувати хмарні сервіси та розвивати експертизу команди у сфері сучасних мережевих технологій. Такий комплексний підхід дозволяє не лише знизити витрати й ризики, а й створити стійку, адаптивну та конкурентоспроможну мережу для розвитку бізнесу.

3 ПРОЕКТУВАННЯ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ VLAN

3.1 Проектування архітектури VLAN для корпоративної мережі

Проектування ефективної архітектури VLAN у корпоративній мережі розпочинається зі створення продуманої логічної схеми сегментації, що враховує специфіку організаційної структури, бізнес-процеси, вимоги до інформаційної безпеки, особливості географічного розташування підрозділів та технічні можливості наявного обладнання. На першому етапі визначається стратегія побудови VLAN — функціональна, рольова, географічна чи гібридна. Функціональний підхід передбачає виділення окремих VLAN для кожного підрозділу, наприклад, адміністрації, фінансів, HR, IT-відділу, продажів, і створення спеціалізованих сегментів для критичних серверів, відеоспостереження, гостьового доступу, IP-телефонії. Рольова сегментація зручна для компаній із матричною структурою або проектною діяльністю, дозволяючи організувати мережу відповідно до ролей і рівнів доступу, незалежно від приналежності до відділів. Географічний підхід застосовується для оптимізації трафіку у компаніях із розподіленою інфраструктурою — офіси, філії, дата-центри отримують окремі VLAN. Найбільшої гнучкості досягає гібридна модель, яка поєднує різні типи сегментації для оптимального балансу між продуктивністю, безпекою та простотою управління.

Архітектурно логічна схема часто оформлюється як ієрархія: критичні серверні VLAN розташовані на верхньому рівні, далі йдуть користувацькі VLAN для підрозділів, а на нижньому рівні — спеціалізовані VLAN для сервісів, таких як голос, відео чи гостьовий доступ. Це дозволяє чітко розмежувати рівні довіри, організувати контроль доступу та централізовано впроваджувати політики безпеки. Плоскі схеми використовуються в простих

або невеликих мережах, але з ростом компанії стають малокерованими. У зональній моделі до кожної групи VLAN застосовуються уніфіковані політики залежно від рівня довіри: наприклад, корпоративна зона, DMZ, зона гостьового доступу.

Важливою складовою проектування є стратегія нумерації VLAN і IP-адресації. Для кожного типу сегментів виділяється окремий діапазон VLAN ID та підмереж: системні VLAN, серверні, користувацькі для офісу й філій, спеціалізовані для voice, video, гостьового доступу й резерву на майбутнє. Наприклад, адміністрація отримує VLAN 210 (10.2.10.0/24), фінанси — VLAN 220 (10.2.20.0/24), IT — VLAN 230 (10.2.30.0/24), HR — VLAN 240 (10.2.40.0/24), продажі — VLAN 250 (10.2.50.0/24). Кожен сегмент має власний пул адрес і унікальні правила доступу. Сервери та інфраструктурні сервіси розміщуються у VLAN із підвищеним рівнем контролю: наприклад, для серверів використовується VLAN 110 (10.1.10.0/24), а для окремих категорій серверів (БД, додатки, backup) — підмережі 111, 112, 113, 114 відповідно. Для управління обладнанням виділяється окрема Management VLAN з максимально обмеженим доступом (наприклад, VLAN 90, 10.0.90.0/24). Для телефонії налаштовується Voice VLAN з максимальним QoS-пріоритетом, а для гостьового доступу — Guest VLAN, яка дозволяє лише вихід в Інтернет і обмежується за пропускною здатністю та часом сесії.

Особливу увагу під час проектування приділяють вимогам кожного підрозділу: для адміністрації — максимальна захищеність, контроль дій, двофакторна автентифікація; для фінансів — відповідність стандартам, повна ізоляція, спеціальні backup та аудит; для IT — розширені права на моніторинг і управління, доступ до management VLAN; для HR — захист персональних даних, інтеграція з системами контролю доступу; для продажів — пріоритет CRM, мобільний доступ, VoIP. Серверні VLAN ізолюються від користувацьких, до Management VLAN мають доступ лише адміністратори, а Guest VLAN не перетинається з жодною із внутрішніх підмереж.

Коли логічна схема затверджена, розробляється архітектура

міжвланової маршрутизації. В сучасних мережах використовується як централізована, так і розподілена маршрутизація. Централізований підхід передбачає використання одного або декількох маршрутизаторів/Layer 3-комутаторів, які обробляють увесь міжвлановий трафік — це спрощує контроль доступу, політик QoS, аудит, але створює можливе вузьке місце й одиночну точку відмови. Розподілена маршрутизація передбачає, що Layer 3-комутатори на рівні розподілу самостійно здійснюють маршрутизацію між локальними VLAN, що зменшує затримки й підвищує відмовостійкість, розподіляє навантаження й оптимізує локальний трафік. Найчастіше обирається гібридний варіант, коли локальний трафік обробляється на рівні розподілу, а міжсайтовий проходить через ядро. Для маршрутизації використовується OSPF (через підтримку ієрархії, VLSM, відкритий стандарт), EIGRP (у Cisco-мережах), а у простих топологіях — статичні маршрути для DMZ чи резервних ліній. Route summarization зменшує розмір таблиць маршрутів, прискорює конвергенцію й підвищує стабільність.

Проектування високої доступності та резервування охоплює всі рівні — від обладнання до каналів зв’язку й протоколів маршрутизації. Для цього використовують стекування комутаторів (Cisco StackWise, HPE IRF), віртуалізацію комутаторів (Cisco VSS, HPE VSF), що дозволяє об’єднати декілька фізичних пристроїв у логічну структуру, спростити керування, забезпечити автоматичне переключення при відмові й балансування навантаження. Для каналів зв’язку застосовуються EtherChannel та LAG — агрегація кількох ліній підвищує пропускну здатність і забезпечує автоматичне відновлення у разі відмови. Spanning Tree Protocol (RSTP, MSTP, PVST+) використовується для уникнення петель і забезпечення швидкого відновлення шляхів. Layer 3 резервування реалізується протоколами HSRP, VRRP або GLBP, які дають змогу створити віртуальний шлюз для клієнтів VLAN, автоматично перемикати трафік при відмові маршрутизатора та балансувати навантаження між декількома пристроями. Регулярний моніторинг стану обладнання й каналів зв’язку, автоматичне

резервування й контроль версій конфігурацій, а також тестування failover-сценаріїв та disaster recovery-процедур забезпечують стабільність та готовність мережі до нештатних ситуацій.

Комплексний підхід до проектування VLAN включає не лише розподіл IP-адрес, визначення підмереж, побудову маршрутної архітектури й резервування, а й організацію централізованого моніторингу, автоматизації управління, політик безпеки й документообігу. Такий підхід дає змогу забезпечити високий рівень доступності, гнучкість масштабування, мінімізувати ризики збоїв та кіберзагроз, підтримати розвиток організації й швидко адаптувати мережу під нові бізнес-вимоги.

3.2 Конфігурація мережевого обладнання для підтримки VLAN

Конфігурація мережевого обладнання для підтримки VLAN є одним із ключових етапів практичної реалізації сучасної корпоративної мережі. Цей процес включає налаштування всіх рівнів мережевої ієрархії, починаючи з комутаторів доступу і закінчуючи маршрутизаторами, а також забезпечення ефективної взаємодії між різними VLAN і централізоване управління мережею.

На першому етапі особливу увагу приділяють комутаторам рівня доступу, оскільки саме вони забезпечують підключення кінцевих пристроїв співробітників, принтерів, точок доступу Wi-Fi, IP-телефонів до логічно сегментованої мережі. Кожен порт комутатора налаштовується як access-порт, який асоціюється з конкретною VLAN, визначеною відповідно до функціональної чи організаційної структури компанії. У випадку, коли через один порт підключаються декілька пристроїв (наприклад, комп’ютер і VoIP-телефон), використовують механізм голосової VLAN, який дозволяє виділити голосовий трафік у окремий пріоритетний сегмент. Кожній VLAN надається унікальний ідентифікатор та описова назва, що суттєво спрощує управління великою кількістю сегментів у розподіленій інфраструктурі.

Надійність і безпека починається з налаштування Port Security — обмеження кількості дозволених MAC-адрес на порту, автоматичного блокування чи повідомлення про порушення. Також активується захист від несанкціонованих DHCP-серверів через функцію DHCP Snooping, яка дозволяє розмежувати trusted та untrusted порти і блокувати підроблені DHCP-пакети. Це особливо важливо для запобігання атак типу DHCP spoofing та зловмисного отримання IP-адрес у внутрішній мережі.

Наступним кроком є налаштування trunk-з'єднань між комутаторами для підтримки передачі трафіку кількох VLAN через одне фізичне з'єднання. В основі цього процесу лежить стандарт IEEE 802.1Q, що дозволяє тегувати Ethernet-кадри спеціальним заголовком, у якому зберігається ідентифікатор VLAN та інша службова інформація. Тільки завдяки коректній конфігурації trunk-портів стає можливою підтримка цілісної VLAN-структури на різних ділянках мережі, особливо якщо обладнання розміщене у різних комутаційних шафах чи навіть у віддалених офісах. На trunk-портах чітко визначається перелік VLAN, які допускаються до передачі, а також налаштовується native VLAN для нетегованого трафіку, яка має бути однаковою на обох кінцях з'єднання. Додатково для оптимізації використання пропускної здатності впроваджується механізм VLAN pruning, який обмежує трафік тільки активними VLAN, мінімізуючи розповсюдження широкомовного трафіку.

Для організації комунікації між різними VLAN необхідна участь пристрою третього рівня — маршрутизатора або Layer 3-комутатора. Існує декілька методів реалізації міжVLAN-маршрутизації: класичний (на окремих фізичних інтерфейсах маршрутизатора), субінтерфейсний (на одному фізичному порту з використанням логічних підінтерфейсів із відповідними IP-адресами шлюзу для кожної VLAN) та через SVI (Switch Virtual Interface) на багаторівневих комутаторах. Сучасні корпоративні рішення найчастіше використовують субінтерфейси чи SVI, що дозволяє більш гнучко керувати маршрутами, масштабувати мережу та зменшувати кількість необхідних

фізичних інтерфейсів. На рівні маршрутизатора або Layer 3-комутатора впроваджуються політики безпеки за допомогою списків контролю доступу (ACL), які чітко визначають, які типи трафіку дозволені або заборонені між різними VLAN, які підмережі мають право доступу до критичних ресурсів, а які — лише до Інтернету.

Для централізованого управління конфігураціями VLAN у великих мережах використовується протокол VTP (VLAN Trunking Protocol), що автоматично поширює інформацію про створені VLAN між усіма комутаторами у домені. Це зменшує ймовірність помилок при ручному налаштуванні, прискорює впровадження нових VLAN і спрощує адміністрування. BTP підтримує три режими: серверний (де створюються та поширюються VLAN), клієнтський (який лише приймає і застосовує конфігурацію), та прозорий, коли комутатор не бере участі у розповсюдженні, але може мати власні локальні VLAN. Надійність роботи VTP забезпечується налаштуванням доменного імені, пароля та контролем версій. З міркувань безпеки слід обмежувати кількість серверних пристроїв і ретельно документувати зміни, адже помилка на одному сервері може призвести до втрати всіх VLAN у домені.

Розгортання такої системи включає не лише технічну конфігурацію, а й розробку політик резервування та моніторингу: backup налаштувань, автоматичний аудит змін конфігурацій, періодичне тестування failover-сценаріїв, впровадження syslog і SNMP для відстеження інцидентів та стану обладнання. В цілому, грамотна й поетапна конфігурація мережевого обладнання — це фундамент надійної, масштабованої, безпечної корпоративної мережі, яка готова до подальшого розвитку та впровадження сучасних сервісів

3.3 Схема комп’ютерної мережі з використанням VLAN

На схемі (рисунок 3.1) відображено комплексну ієрархічну архітектуру корпоративної мережі, яка реалізована із застосуванням технології VLAN та відповідає сучасним принципам побудови розподілених і захищених корпоративних інфраструктур. Основу мережі складає поділ на окремі логічні сегменти відповідно до функціонального, сервісного та безпекового призначення кожного підрозділу й сервісу, що дозволяє досягти максимальної ізоляції, керованості та масштабованості.

Верхній рівень структури складає рівень ядра (Core Layer), де розташовано центральний комутатор (Core Switch), який забезпечує високошвидкісну магістральну комутацію між усіма сегментами мережі. Саме через цей комутатор відбувається агрегація трафіку від різних підрозділів та серверних зон. На кордоні мережі встановлено потужний firewall або маршрутизатор з адресою 10.0.0.1, який відповідає за фільтрацію вхідного й вихідного трафіку, захист від зовнішніх атак і реалізацію політик доступу до Інтернету та зовнішніх мереж. Така побудова дозволяє централізовано контролювати зовнішні з’єднання й забезпечує безпеку периметру.

Ліва частина схеми присвячена серверній зоні, яка складається з кількох ізольованих VLAN, кожна з яких має своє призначення. VLAN 110 (10.1.10.0/24) використовується для загальних серверів підприємства, VLAN 111 (10.1.11.0/24) — для серверів баз даних, що забезпечує фізичну й логічну ізоляцію критичних даних. Окрема VLAN 112 (10.1.12.0/24) виділена для серверів додатків, що дозволяє впроваджувати специфічні політики QoS і безпеки для аплікаційного трафіку. Веб-сервери розміщуються у VLAN 113 (10.1.13.0/24), що спрощує керування доступом до публічних ресурсів і реалізацію DMZ-архітектури. Для backup-серверів, які відповідають за резервування даних, виділена VLAN 114 (10.1.14.0/24), що дозволяє ізолювати трафік резервного копіювання від основного робочого трафіку та

уникати негативного впливу на продуктивність мережі під час backup-вікон.

Особливу роль відіграють спеціалізовані VLAN. VLAN 90 (10.0.90.0/24) призначена для управління мережевим обладнанням — це Management VLAN, доступ до якої суворо обмежений лише адміністраторам і здійснюється ізольовано від робочого трафіку. Окремий сегмент VLAN 410 (10.10.10.0/24) відведений для IP-телефонії — це Voice VLAN із пріоритетом QoS, мінімальними затримками та підтримкою PoE для підключення телефонних апаратів. Гостьовий доступ організований через VLAN 420 (10.20.10.0/24) — ізольовану мережу з доступом лише до Інтернету та суворими обмеженнями на пропускну здатність і тривалість сесій.

Користувацькі VLAN структуровано за функціональними підрозділами компанії, кожен з яких отримує власний ізольований сегмент. VLAN 210 (10.2.10.0/24) призначена для адміністрації, де підключено комп’ютери, IP-телефони та інші пристрої персоналу через Access Switch. Така ізоляція забезпечує високий рівень безпеки та пріоритетний доступ до корпоративних ресурсів, електронної пошти та систем документообігу. VLAN 220 (10.2.20.0/24) обслуговує фінансовий відділ із окремим Access Switch і робочими станціями, що дозволяє суворо контролювати доступ до фінансових систем, підтримувати відповідність галузевим стандартам та вести аудит транзакцій.

VLAN 230 (10.2.30.0/24) організована для IT-відділу, тут підключаються як дротові пристрої, так і Wi-Fi точки доступу, оскільки IT-персонал часто використовує мобільні рішення та потребує підвищених прав адміністрування. Робочі станції адміністраторів та фахівців з мережевого обслуговування виділені в межах власного сегменту, що дозволяє забезпечити доступ до Management VLAN, моніторингових систем та систем логування. VLAN 240 (10.2.40.0/24) використовується відділом кадрів (HR), де основний акцент зроблено на захисті персональних даних співробітників та інтеграції з системами контролю доступу. VLAN 250 (10.2.50.0/24) створена для відділу продажів: тут також реалізовано підключення Wi-Fi

точок доступу, оскільки співробітники часто використовують мобільні пристрої, CRM-системи, VoIP-телефонію та відеоконференції для спілкування з клієнтами.

Ключовими особливостями цієї архітектури є функціональна сегментація, яка забезпечує чітку ізоляцію трафіку кожного підрозділу, що значно підвищує безпеку та спрощує контроль доступу. Серверна зона побудована за принципом ізольованих VLAN для різних типів серверів, що дозволяє застосовувати гнучкі політики доступу й захисту даних. Впровадження безпровідного доступу у VLAN IT та Sales підрозділів підвищує мобільність працівників і забезпечує безперервність бізнес-процесів. Voice VLAN гарантує якість IP-телефонії, виділяючи трафік голосових сервісів у пріоритетний сегмент, що зменшує затримки й втрати пакетів. Гостьовий доступ повністю ізольований, не має виходу до корпоративних ресурсів і реалізований через фільтрацію та обмеження пропускної здатності. Для адміністрування всієї мережі використовується централізований Management VLAN, що дозволяє управляти обладнанням незалежно від користувацьких сегментів.

Загалом, така мережна схема забезпечує не лише високу безпеку і продуктивність, а й зручність масштабування, легкість адміністрування й гнучкість подальшого розвитку корпоративної мережі, дозволяє ефективно розмежовувати політики доступу, оптимізувати трафік та забезпечувати високу відмовостійкість та оперативне реагування на бізнес-запити організації.

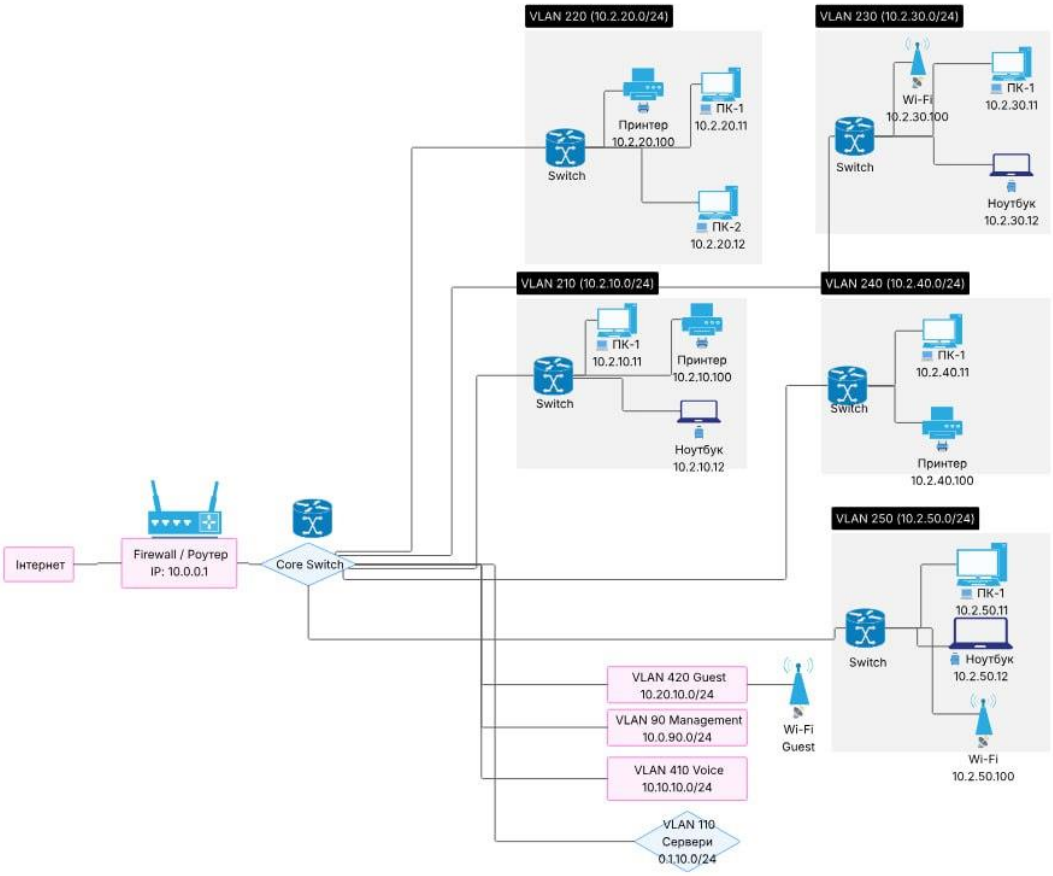

Рисунок 3.1 – Схема спроектовоної ККМ

3.4 Мережеве обладнання, використане при побудові ККМ з VLAN

У сучасній корпоративній мережі, що базується на технології VLAN, ключовим елементом, який забезпечує цілісність, масштабованість і стабільну роботу всієї інфраструктури, є ядерний комутатор. Його роль не обмежується лише передачею даних — він виступає як головна магістраль, що об'єднує всі підрозділи організації, серверні зони, пристрої безпеки, а також забезпечує ефективну маршрутизацію між логічно розділеними сегментами мережі. Найбільш показовим прикладом такого пристрою є Cisco Catalyst 9500 — високопродуктивний фіксований комутатор корпоративного класу, спеціально розроблений для ядра мережі з підтримкою сучасних технологій віртуалізації, безпеки та автоматизації.

Cisco Catalyst 9500 вирізняється винятковою продуктивністю, надійністю та широкими можливостями для інтеграції в мережі великого масштабу. Його архітектура побудована на основі чіпсету Cisco UADP (Unified Access Data Plane), що забезпечує апаратне прискорення комутації та маршрутизації, а також дозволяє гнучко обробляти політики доступу, шифрування, сегментацію та QoS в режимі реального часу. Завдяки модульній операційній системі Cisco IOS XE, комутатор підтримує не лише класичні протоколи маршрутизації та комутації, а й функції автоматизованого розгортання, REST API, NetConf, а також інтеграцію з системами програмно-визначеної мережі (SDN) через Cisco DNA Center.

У типовому сценарії Cisco Catalyst 9500 (рисунок 3.2) виконує агрегацію трафіку від усіх комутаторів доступу та розподілу, з'єднується з міжмережевими екранами, серверами резервного копіювання, IP-телефонією та шлюзами до зовнішніх ресурсів. Наприклад, в корпоративній мережі з сегментацією VLAN по підрозділах — адміністрація, фінанси, IT, HR, гостьовий доступ — саме на цьому комутаторі відбувається міжVLAN-маршрутизація. Кожна VLAN підключена через trunk-з'єднання, трафік тегується згідно з IEEE 802.1Q, а маршрутизація виконується на основі віртуальних інтерфейсів (SVI), налаштованих у комутаторі.

Цей пристрій підтримує швидкість комутації до 960 Гбіт/с, що дозволяє обробляти великі об'єми трафіку без затримок, навіть при значному навантаженні. Комутатор може бути обладнаний портами 10G, 25G, 40G і 100G Ethernet, що дозволяє йому працювати в середовищі дата-центру або у розподіленій корпоративній мережі з великою кількістю серверів, точок доступу, VoIP-систем та відеоконференційних сервісів. Його багатий функціонал дозволяє одночасно впроваджувати політики безпеки, контролювати пріоритети трафіку, блокувати потенційно небезпечні пакети, а також реалізовувати багаторівневе резервування за допомогою протоколів HSRP або VRRP.

З точки зору безпеки, Cisco Catalyst 9500 забезпечує надійний perimeter

defense — комутатор підтримує Access Control Lists (ACL), DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, що унеможливлює базові атаки на рівні 2-3 моделей OSI. Крім того, завдяки інтеграції з Cisco TrustSec, можна впроваджувати політично-керовану сегментацію та контроль доступу не за IP, а за ідентифікатором користувача або роллю, що особливо актуально у Zero Trust-архітектурі.

Практичне використання Cisco Catalyst 9500 можна проілюструвати на прикладі компанії з понад 500 співробітниками, що має центральний офіс та віддалені філії. У цьому випадку Catalyst 9500 служить центральним комутаційним хабом, до якого підключаються комутатори доступу (наприклад, Cisco 2960X), сервери ERP-систем, телефонна інфраструктура, точки доступу Wi-Fi 6, міжмережевий екран Cisco Firepower і вихід у глобальну мережу. Комутатор одночасно виконує функцію маршрутизатора між VLAN, фільтрує доступ до серверів за допомогою ACL, виконує балансування навантаження та автоматично повідомляє Cisco DNA Center про аномалії в трафіку або відмови портів.

Таким чином, Cisco Catalyst 9500 — це не просто комутатор, а високотехнологічна платформа для побудови масштабованої, безпечної та інтелектуальної мережі корпоративного рівня з глибокою сегментацією через VLAN.

Рисунок 3.2 – Cisco Catalyst 9500

У корпоративній мережі з розгалуженою структурою надзвичайно важливу роль відіграють комутатори рівня розподілу, які виступають проміжною ланкою між комутаторами рівня доступу та ядерним комутатором. Їх основна функція полягає в агрегації трафіку з кількох комутаторів доступу, реалізації між VLAN-маршрутизації, впровадженні політик безпеки, фільтрації, управлінні пріоритетами трафіку через механізми QoS, а також забезпеченні резервування для підвищення надійності інфраструктури. Вони, як правило, мають розширені можливості третього рівня (Layer 3), що дозволяє їм ефективно працювати з маршрутизованим трафіком між віртуальними сегментами. Завдяки високій продуктивності та підтримці таких функцій, як протоколи динамічної маршрутизації (OSPF, BGP), політики доступу (ACL), а також віртуальні інтерфейси (SVI), ці пристрої забезпечують гнучку конфігурацію та швидкий обмін даними між підрозділами підприємства. Одним із яскравих прикладів таких комутаторів є HPE Aruba 6000R — модульний, масштабований пристрій, який поєднує надійність, високу щільність портів і підтримку технологій віртуалізації та централізованого управління. Його гнучка архітектура дозволяє адаптувати конфігурацію під потреби конкретного підприємства, забезпечуючи при цьому можливість гарячої заміни модулів, балансування навантаження та автоматичне перемикання при збої ліній зв’язку або живлення. Aruba 6000R часто встановлюється в основних кросах будівель або поверхів, де відбувається консолідація трафіку від локальних access switch'ів і подальша передача на рівень ядра.

Водночас комутатори рівня доступу безпосередньо обслуговують кінцеві пристрої користувачів та формують базовий шар мережевої інфраструктури. Саме на цьому рівні реалізується первинна VLAN-сегментація — кожен порт комутатора асоціюється з певною VLAN відповідно до функціонального призначення підключеного пристрою. Комутатори доступу повинні підтримувати основні механізми безпеки та керованості, такі як Port Security, який обмежує кількість MAC-адрес на

порту, DHCP Snooping для запобігання атакам через підроблені DHCP-сервери, а також підтримку PoE або PoE+ для живлення точок доступу, IP-телефонів та камер відеоспостереження. У типовому офісі ці пристрої встановлюються у телекомунікаційних шафах і обслуговують користувацькі ПК, принтери, SIP-телефони, термінали обліку часу або POS-обладнання. Одним із популярних представників цього класу є HPE Aruba 2530/2540 — недорогі, енергоефективні, керовані комутатори, що мають широкий набір функцій для малого та середнього бізнесу. Вони підтримують Web-інтерфейс, CLI, SNMP, дозволяють гнучко налаштовувати VLAN, здійснювати моніторинг портів, будувати дзеркальні з'єднання для відлагодження мережі, а також інтегруються в централізовану систему управління Aruba AirWave або Aruba Central. З їхньою допомогою адміністратор може легко забезпечити надійне підключення користувачів, одночасно дотримуючись політик безпеки та контролю доступу.

Таким чином, комутатори рівня розподілу та доступу працюють у тісному тандемі, формуючи логічну й фізичну основу корпоративної мережі з сегментацією на основі VLAN. Вони забезпечують масштабованість, гнучкість та ефективність передачі даних, дозволяючи ізолювати трафік між різними підрозділами, контролювати доступ до ресурсів, реалізовувати балансування навантаження та впроваджувати стратегії безпеки на різних рівнях організації.

У сучасній корпоративній мережі міжмережевий екран (firewall) відіграє ключову роль у забезпеченні безпеки, виступаючи як перший рубіж захисту між внутрішнім інформаційним середовищем підприємства та зовнішнім простором Інтернету. Firewall може бути реалізований як у вигляді апаратного пристрою, встановленого в мережевій шафі, так і у вигляді віртуального рішення, розгорнутого на серверній інфраструктурі. Його головна задача — це фільтрація трафіку за заданими правилами, запобігання несанкціонованому доступу, виявлення аномалій, блокування атак та забезпечення шифрованих каналів зв'язку через VPN. Однією з

найпотужніших функцій є підтримка глибокої інспекції пакетів (Deep Packet Inspection), яка дозволяє аналізувати вміст трафіку не лише за IP-адресою чи портом, а й за сигнатурами потенційно шкідливих дій або порушень політики. Більшість сучасних firewall'ів, таких як Cisco Firepower, FortiGate або Palo Alto, мають вбудовані системи виявлення та запобігання вторгненням (IDS/IPS), інтегруються з централізованими системами управління політиками, підтримують сегментацію внутрішньої мережі через зони безпеки та забезпечують підключення до DMZ — демілітаризованих зон для сервісів, які мають бути доступними ззовні, таких як веб-сервери або поштові шлюзи. Firewall також виступає шлюзом між окремими VLAN, дозволяючи застосовувати політики контролю доступу між сегментами, особливо якщо йдеться про доступ до серверів чи адміністративної частини мережі.

Серверна інфраструктура, яка логічно розміщена в окремих VLAN, виконує критично важливі функції обслуговування корпоративних сервісів. У типовій організації це окремі сервери або віртуальні машини, які виконують ролі серверів додатків (Application Server), баз даних (Database Server), веб-серверів (Web Server) та систем резервного копіювання (Backup Server). Розміщення серверів у виділених VLAN забезпечує їхню ізоляцію від користувацького трафіку та дозволяє реалізувати специфічні політики доступу, що підвищує рівень безпеки. Сервери зазвичай підключаються до високопродуктивних комутаторів рівня ядра або серверних комутаторів із підтримкою високошвидкісних портів 10/40/100 Гбіт/с, а також резервованих шляхів. У великих інфраструктурах використовуються віртуалізаційні платформи типу VMware vSphere або Microsoft Hyper-V, що дозволяє гнучко керувати ресурсами, балансувати навантаження та реалізовувати механізми відновлення після збоїв. Сервери баз даних, наприклад, можуть бути налаштовані з використанням кластеризації та реплікації, щоб гарантувати безперервність бізнес-процесів, а backup-сервери — інтегровані з хмарними сховищами або системами віддаленого зберігання для забезпечення

надійного відновлення в разі кібератаки чи збою обладнання.

Точки доступу Wi-Fi (Wireless Access Points) завершують інфраструктуру бездротового зв’язку та дозволяють кінцевим користувачам підключатися до мережі за допомогою мобільних пристроїв, ноутбуків чи планшетів. Вони стратегічно розміщуються в офісних приміщеннях, зонах спільного користування, конференц-залах або навіть складах, якщо потрібно покриття для мобільного обладнання. Сучасні точки доступу підтримують виділення декількох SSID, кожен з яких асоційований із окремою VLAN — наприклад, одна VLAN для співробітників, інша для гостьового доступу, третя — для IoT-пристроїв або телефонії. Точки доступу повинні інтегруватися з протоколами автентифікації типу RADIUS та підтримувати захищені методи шифрування (WPA3 Enterprise), що дозволяє реалізувати політики контролю доступу на основі облікових записів користувачів. Серед найбільш популярних пристроїв — моделі Ubiquiti UniFi, які вирізняються високою продуктивністю, зручною централізованою системою управління через UniFi Controller, підтримкою Wi-Fi 6 та автоматичним балансуванням навантаження між точками. Вони дозволяють забезпечити стабільне покриття навіть у складних радіоумовах, реалізовувати гостьові портали, відстежувати трафік та інтегрувати бездротовий сегмент в єдину VLAN-архітектуру корпоративної мережі.

Отже, firewall, сервери та точки доступу створюють критично важливе оточення для підтримки функціональності, безпеки та мобільності в межах VLAN-структури сучасної корпоративної мережі. Їх правильне розгортання, налаштування та управління безпосередньо впливають на надійність і захищеність всієї IT-інфраструктури підприємства.

ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було досягнуто поставлену мету — розроблено теоретично обґрунтовану та практично реалізовану модель корпоративної комп’ютерної мережі з використанням технології VLAN. Проведений аналіз сучасного стану інформаційної інфраструктури підприємств підтвердив актуальність впровадження логічної сегментації мережевого трафіку як ефективного способу підвищення безпеки, керованості та продуктивності мережі.

На основі дослідження сучасних стандартів і практик побудови VLAN-сегментованих мереж було розроблено оптимальну топологію мережі, яка враховує вимоги до інформаційної безпеки, гнучкого масштабування та ефективної взаємодії між структурними підрозділами підприємства. У роботі обґрунтовано вибір активного мережевого обладнання, описано процес конфігурації VLAN, IP-адресації, а також розроблено рекомендації з подальшого адміністрування й моніторингу мережі.

Отримані результати демонструють практичну цінність впровадження VLAN у корпоративне середовище — зокрема, завдяки підвищенню рівня ізоляції між сервісами, зниженню ризику несанкціонованого доступу, спрощенню технічного супроводу та забезпеченню готовності мережі до подальшого масштабування.

Таким чином, дана кваліфікаційна робота не лише підтвердила доцільність застосування технології VLAN у сучасних корпоративних мережах, а й сформувала методичну та практичну базу для подальших досліджень і впроваджень у цій сфері.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі: принципи, технології, протоколи. – 2006. – 958 с.

2. Столлінгс В. Комп'ютерні мережі, протоколи і технології Інтернету. –.: BHV, 2005. – 832 с.

3. Таненбаум Е. С., Уезеролл Д. Дж. Комп'ютерні мережі: підручник. – 5-те вид. – К.: Видавництво «Вільямс», 2012. – 880 с.

4. Річардс Д. Основи локальних мереж. – К.: Діалектика, 2004. – 416 с.

5. Бех М.О., Ярошенко О.О. Технології побудови структурованих кабельних систем: навчальний посібник. – Х.: ХНУРЕ, 2019. – 135 с.

6. Каток В.Б., Руденко І.Є. Сучасні технології з'єднань волоконних світловодів зі складу оптичних кабелів зв'язку // Інформатизація та нові технології. – 1996, №1. – С. 41–43.

7. IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 3: CSMA/CD Access Method and Physical Layer Specifications. IEEE Std 802.3-2018.

8. RFC 1918 Address Allocation for Private Internets [Електронний ресурс]. – Режим доступу: https://datatracker.ietf.org/doc/html/rfc1918

9. Ubiquiti Inc. EdgeRouter – User Guide [Електронний ресурс]. – Режим доступу: https://help.ui.com/hc/en-us/articles/204959174-EdgeRouter-User-Guide

10. Cisco Systems. IP Addressing and Subnetting for New Users [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/13788-3.html

11. Synology Inc. NAS User's Guide [Електронний ресурс]. – Режим доступу: https://kb.synology.com/en-

global/DSM/help/DSM/AdminCenter/system_information

12. Yealink SIP-T21P E2 IP Phone – User Manual [Електронний ресурс]. – Режим доступу: https://support.yealink.com/