Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Кібербезпеки
(повна назва)

Кафедра Інформаційно-мережної інженерії
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

Проектування локальної мережі підприємства
(тема)

Виконав:
Здобувач четвертого року навчання,
групи ТРІМІ-22-1
Анна Колатиріна
(власне ім'я, прізвище)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма Інформаційно-мережна інженерія
(повна назва освітньої програми)

Керівник *доц. Юлія Скорик*
(посада, власне ім'я, прізвище)

Допускається до захисту

В.о. Завідувача кафедри _____ _____ *Дарія Чеботарьова*
(підпис) (власне ім'я, прізвище)

2026

Харківський національний університет радіоелектроніки

Факультет Кібербезпеки

Кафедра Інформаційно-мережної інженерії

Рівень вищої освіти перший (бакалаврський)

Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)

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

Освітня програма Інформаційно-мережна інженерія
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«2» 06 2026 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачеві Колатиріной Анні Владиславівні
(прізвище, ім'я, по батькові)

1. Тема роботи Проектування локальної мережі підприємства
затверджена наказом університету від 2 06 2026 р. № 466Ст
2. Термін подання здобувачем роботи до екзаменаційної комісії 12 07 2026 р.
3. Вихідні дані до роботи *Проектування локальної мережі підприємства з розробки програмного забезпечення WorkDataNet. Розрахунок мережного обладнання. Проектування логічної організації підприємства в Packet Tracer.*

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Вступ
1. Вибір структури та топології організації
2. Структурована кабельна система організації
3. Вибір мережного обладнання
4. Логічна організація ЛМЗ
Висновки

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
Слайди у форматі Power Point (назва, вступ і актуальність кваліфікаційної роботи, Локальна мережа, Підприємство WorkDataNet, Класифікація локальних мереж, Топологія локальної мережі, Структурована кабельна система, Організація будівлі компанії WorkDataNet, Вибір мередного обладнання, Апаратні та програмні інструменти захисту, Протоколи інформаційної безпеки різних рівнів, Ієрархічне розбиття мережі на підмережі, Налаштування центрального маршрутизатора, Конфігурування комутаційного обладнання, висновки та результати роботи).

6. Консультанти розділів роботи (п.6 включається до завдання 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
Основна частина	доц. Скорик Ю.В.		11.07.2026

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Строк / термін виконання етапів роботи	Примітка
1	Ознайомлення із завданням. Уточнення ТЗ	02.06-04.06.2026	виконано
2	Підбір літератури за темою роботи	05.06-08.06.2026	виконано
3	Виконання розділу 1	09.06-11.06.2026	виконано
4	Виконання розділу 2	12.06-15.06.2026	виконано
5	Виконання розділу 3	16.06-20.06.2026	виконано
6	Виконання розділу 4	21.06-05.07.2026	виконано
7	Оформлення презентаційного матеріалу	06.07-09.07.2026	виконано
8	Підготовка до захисту у ЕК	10.07-12.07.2026	виконано

Дата видачі завдання __2___ _____06_____2026 р.

Здобувач _____
(підпис)

Керівник роботи _____ __*доц. Юлія Скорик*_____
(підпис) (посада, власне ім'я, прізвище)

РЕФЕРАТ

Пояснювальна записка: 59 стор. формату А4, 6 рис., 6 табл., 10 посилань.

Об’єкт дослідження – локальні комп'ютерні мережі.

Мета роботи – проектування локальної обчислювальної мережі, показати особливості локальної комп'ютерної мережі: структуру, класифікацію, призначення, топологію, технічну підтримку.

Показані теоретичні і практичні сторони побудови локальної комп’ютерної мережі підприємства на прикладі компанії «WorkDataNet». Були проаналізовані літературні джерела на предмет класифікації локальних комп'ютерних мереж, запропоноване мережне обладнання за відібраними характеристиками та надані рекомендації з налаштування для кожного з елементів локальної комп’ютерної мережі підприємства «WorkDataNet». Здійснено ознайомлення з інструментами для забезпечення захисту інформації та комерційної таємниці локальної мережі, а саме: брандмауери, проксі-сервери, VPN та протоколи. Проведена кількісна і якісна оцінка мережного обладнання, задля швидкого обміну даними між окремими підрозділами чи співробітниками та значної економії коштів.

ЛОКАЛЬНА МЕРЕЖА ЗВ’ЯЗКУ, ТОПОЛОГІЯ, TP-LINK, МЕРЕЖА, ДАНІ, МАРШРУТИЗАТОР, КОМУТАТОР, MAC-АДРЕС.

ABSTRACT

Explanatory note: 59 pp. format A4, 6 Fig., 10 reference, 6 tab.

Object of research – local area networks.

Purpose of the work – to design a local area network and demonstrate the specific features of a LAN, including its structure, classification, purpose, topology, and technical support.

The theoretical and practical aspects of designing a local area network (LAN) for an enterprise are considered, using the "WorkDataNet" company as a case study. Literature sources on the classification of local area networks are analyzed, network equipment is proposed based on the selected characteristics, and recommendations for configuring each element of the "WorkDataNet" enterprise LAN are provided. An overview of tools for ensuring information security and protecting trade secrets within the local network is carried out, specifically focusing on firewalls, proxy servers, VPNs, and protocols. Finally, a quantitative and qualitative assessment of the network equipment was conducted to ensure rapid data exchange between individual departments or employees, while achieving significant cost savings.

LOCAL AREA NETWORK, TOPOLOGY, TP-LINK, NETWORK, DATA, ROUTER, SWITCH, MAC ADDRESS.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ..... 8
ВСТУП..... 13
1 ВИБІР СТРУКТУРИ ТА ТОПОЛОГІЇ ОРГАНІЗАЦІЇ.....14
1.1 Концептуалізація локальних обчислювальних мереж.....14
1.2 Структурна організація локальних комп'ютерних мереж.....15
1.3 Класифікація локальних комп'ютерних мереж.....17
1.4 Топологічні структури локальних обчислювальних мереж.....19
ВИСНОВКИ ДО РОЗДІЛУ 1.....24
2 ПРОЄКТУВАННЯ СТРУКТУРОВАНОЇ КАБЕЛЬНОЇ СИСТЕМИ ПІДПРИЄМСТВА.....25
2.1 Концептуальні засади та архітектура СКС.....25
2.2 Функціональний аналіз підсистем СКС компанії.....25
2.2.1 Підсистема робочого простору.....25
2.2.2 Горизонтальна підсистема та просторова організація поверхів.....26
2.2.3 Вертикальна (магістральна) підсистема будівлі.....28
ВИСНОВКИ ДО РОЗДІЛУ 2.....31
3 ОБГРУНТУВАННЯ ТА ВИБІР АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ І СИСТЕМ МЕРЕЖНОЇ БЕЗПЕКИ.....32
3.1 Критерії вибору мережного обладнання.....32
3.2 Технічний опис та специфікація обраного обладнання.....33
3.2.1 Центральний бізнес-маршрутизатор ЛОМ.....33
3.2.2 Магістральний керований комутатор 3-го рівня (L3/L2+).....34
3.2.3 Поверхові комутатори з підтримкою технології PoE+.....35
3.2.4 Середовище передачі даних.....36

3.3 Комплексна безпека локальної обчислювальної мережі.....37
3.3.1 Апаратні та програмні інструменти захисту.....38
3.3.2 Протоколи інформаційної безпеки різних рівнів.....38
3.3.3 Захист протоколів маршрутизації.....39
ВИСНОВКИ ДО РОЗДІЛУ 3.....40
4 ЛОГІЧНА ОРГАНІЗАЦІЯ ТА СИМУЛЯЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ ПІДПРИЄМСТВА.....41
4.1 Адресний план та ієрархічне розбиття мережі на підмережі.....41
4.2 Конфігурування активного мережного обладнання.....42
4.2.1 Налаштування центрального маршрутизатора.....42
4.2.2 Конфігурування комутаційного обладнання.....43
4.3 Аналіз та обгрунтування використаних канальних технологій.....44
4.3.1 Технологія Fast Ethernet (стандарт IEEE 802.3u) 45
4.3.2 Технологія Gigabit Ethernet (стандарт IEEE 802.3z / IEEE 802.3ab) 46
ВИСНОВКИ ДО РОЗДІЛУ 4.....47
ВИСНОВКИ.....48
ПЕРЕЛІК ПОСИЛАНЬ.....50
ДОДАТОК А. Логічна схема локальної мережі організації.....51
ДОДАТОК Б. Слайди презентації.....52

ПЕРЕЛІК СКОРОЧЕНЬ

ACL (Access Control List) – список контролю доступу;

ADSL (Asymmetric Digital Subscriber Line) – асиметрична цифрова абонентська лінія;

AI (Artificial Intelligence) – штучний інтелект;

ARP (Address Resolution Protocol) – протокол розв'язання адрес;

ATM (Asynchronous Transfer Mode) – асинхронний режим передачі даних;

BGP (Border Gateway Protocol) – протокол граничного шлюзу для маршрутизації між автономними системами в Internet;

CAM (Content Addressable Memory) – таблиця асоціативної пам’яті комутатора, що зберігає прив’язки MAC-адрес до портів;

CapEx (Capital Expenditure) – капітальні витрати на придбання обладнання та побудову мережі;

CCA (Copper-Clad Aluminium) – алюмінієвий дріт, покритий тонким шаром міді;

CIDR (Classless Inter-Domain Routing) – безкласова міждоменна маршрутизація для ефективного розподілу IP-адрес;

CoS (Class of Service) – технологія пріоритезації трафіку на канальному рівні моделі OSI;

DAI (Dynamic ARP Inspection) – функція динамічної перевірки пакетів ARP для захисту від спуфінгу;

DHCP (Dynamic Host Configuration Protocol) – протокол автоматичного призначення IP-адрес та налаштувань мережі хостам;

DMZ (Demilitarized Zone) – демілітаризована зона, ізольований сегмент мережі для загальнодоступних серверів;

DNS (Domain Name System) – система доменних імен для перетворення символьних адрес у числові IP-адреси;

DoS / DDoS (Denial of Service) – мережна атака, спрямована на перевантаження та зупинку роботи сервісів;

DSCP (Differentiated Services Code Point) – код диференційованих послуг для пріоритезації трафіку на мережному рівні;

EAP (Extensible Authentication Protocol) – розширюваний протокол автентифікації користувачів;

FTP (Foiled Twisted Pair) – кабельна кручена пара із загальним захисним екраном з алюмінієвої фольги;

IEEE (Institute of Electrical and Electronics Engineers) – міжнародний інститут інженерів з електротехніки та електроніки;

IP (Internet Protocol) – базовий міжмережний протокол для передачі пакетів даних;

IPSec (Internet Protocol Security) – набір протоколів захисту та шифрування мережного IP-трафіку;

IPTV (Internet Protocol Television) – технологія цифрового телебачення за протоколом IP;

ISO (International Organization for Standardization) – міжнародна організація зі стандартизації;

L2 / L3 (Layer 2/Layer 3) – канальний та мережний рівні еталонної моделі OSI;

LSZH (Low Smoke Zero Halogen) – вогнестійкий матеріал оболонки кабелю з низьким рівнем виділення диму;

MAC (Media Access Control) – унікальна фізична адреса пристрою, що закладається виробником;

MD5 (Message Digest 5) – алгоритм обчислення 128-бітного хешу для верифікації та автентифікації даних;

MITM (Man-in-the-Middle) – атака типу «людина посередині» з метою перехоплення або модифікації трафіку;

MMF (Multi-mode Optical Fiber) – багатомодове оптичне волокно;

MU-MIMO (Multi-User Multiple-Input Multiple-Output) – технологія бездротової передачі даних із використанням кількох антен;

NAT (Network Address Translation) – механізм перетворення мережних адрес між приватними та глобальними інтерфейсами;

OpEx (Operational Expenditure) – операційні витрати на поточне обслуговування та адміністрування мережі;

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, заснований на відстеженні стану каналів;

OSI (Open Systems Interconnection) – еталонна семирівнева модель взаємодії відкритих систем;

PAM-5 (Pulse Amplitude Modulation 5) – п'ятирівнева імпульсно-амплітудна модуляція для гігабітних мереж;

PGP (Pretty Good Privacy) – протокол прикладного рівня для шифрування та захисту електронної пошти;

PoE / PoE+ (Power over Ethernet) – технологія одночасної передачі живлення та даних через кабель крученої пари;

QoS (Quality of Service) – комплекс методів пріоритезації мережного трафіку для важливих додатків;

RFC (Request for Comments) – технологічний стандарт або документ Інженерної ради Інтернету (IETF);

RIP (Routing Information Protocol) – динамічний протокол маршрутизації, заснований на дистанційно-векторному алгоритмі;

SFP / SFP+ (Small Form-factor Pluggable) – компактний модульний трансивер для підключення магістральних кабелів;

SMF (Single-mode Optical Fiber) – одномодове оптичне волокно;

SPI (Stateful Packet Inspection) – технологія фільтрації пакетів із глибокою перевіркою стану активного з'єднання;

SSL (Secure Sockets Layer) – протокол захищених сокетів для створення безпечного каналу зв'язку;

SVI (Switched Virtual Interface) – віртуальний інтерфейс комутатора третього рівня для адміністрування VLAN;

TCP / IP (Transmission Control Protocol) – головний ієрархічний стек мережних протоколів сучасних комп'ютерних мереж;

TLS (Transport Layer Security) – протокол захисту транспортного рівня, криптографічний наступник SSL;

UPnP (Universal Plug and Play) – універсальна архітектура спрощеного підключення пристроїв до мережі;

USB (Universal Serial Bus) – універсальна послідовна шина для підключення периферії;

UTP (Unshielded Twisted Pair) – неекранована кручена пара, тип кабелю без захисних металевих екранів;

VPN (Virtual Private Network) – технологія створення зашифрованих захищених тунелів поверх відкритих каналів;

WAN (Wide Area Network) – глобальна комп'ютерна мережа, зовнішній інтерфейс підключення до Інтернет;

WEP / WPA / WPA2 / WPA3 (Wi-Fi Protected Access) – стандарти та криптографічні протоколи безпеки для бездротових мереж Wi-Fi;

ВОЛЗ – Волоконно-оптична лінія зв'язку;

ІБ – Інформаційна безпека;

ІТ – Інформаційні технології;

ЛОМ – Локальна обчислювальна мережа;

ПК – Персональний комп'ютер;

ПЗ – Програмне забезпечення;

СКС – Структурована кабельна система.

ВСТУП

Становлення та еволюція мережних технологій забезпечили принципово новий, надійний і високоефективний інструментарій для інформаційної взаємодії. Аналогічно до інших інновацій у галузі ІТ, комп'ютерні мережі першочергово впроваджувалися для вирішення науково-дослідних завдань, після чого інтегрувалися практично в усі сфери людської діяльності.

Тематика цієї кваліфікаційної роботи присвячена процесу проєктування локальної обчислювальної мережі (ЛОМ). Дослідження зазначеного напряму є високоактуальним, оскільки ЛОМ забезпечує об'єднання обчислювальних потужностей і створює умови для спільного використання апаратних ресурсів, а також підключеного периферійного обладнання (принтерів, плотерів, дискових масивів тощо).

Актуальність теми дослідження зумовлена повсюдною інтеграцією мережних архітектур у сучасні соціально-економічні та виробничі процеси: від освітнього сектору до автоматизованих систем управління підприємствами. З одного боку, сучасні мережі є специфічним різновидом розподілених обчислювальних систем, а з іншого – виступають ефективним засобом трансферу даних на великі відстані. Для забезпечення цього процесу в мережних структурах використовуються передові методи кодування та мультиплексування даних, запозичені й адаптовані з телекомунікаційних систем.

З огляду на це, у цій роботі буде досліджено та реалізовано процес проєктування локальної обчислювальної мережі для забезпечення функціональних потреб підприємства «WorkDataNet».

1 ВИБІР СТРУКТУРИ ТА ТОПОЛОГІЇ ОРГАНІЗАЦІЇ

1.1 Концептуалізація локальних обчислювальних мереж

Локальна обчислювальна мережа (ЛОМ) є сукупністю технічних і програмних засобів обміну даними, що перебуває у власності та під безпосереднім управлінням єдиної організації. У науково-практичному контексті ЛОМ визначається як інтегрована інформаційна система, функціонал якої спрямований на спільне використання ресурсів корпоративного середовища та оптимізацію бізнес-процесів. За функціональним призначенням ЛОМ класифікують на установчі (офісні мережі комерційних компаній, органів адміністративного управління тощо) та мережі автоматизованого керування технологічними процесами (АСУ ТП) на виробництві.

Переважна більшість ЛОМ інтегрує в єдиний простір робочі станції та персональні комп'ютери. Кожен мережний вузол функціонує на базі власного процесора, що забезпечує автономне виконання програмних застосунків, маючи при цьому санкціонований доступ до загальних баз даних та апаратних ресурсів у межах мережної архітектури. Це дозволяє організувати колективний доступ до периферійного обладнання (наприклад, мережевих принтерів) і спільних інформаційних масивів. Окрім цього, ЛОМ виступає платформою для забезпечення внутрішньокорпоративної комунікації користувачів через сервіси електронної пошти та системи миттєвого обміну повідомленнями [1].

Практична реалізація та проєктування ЛОМ у межах цієї кваліфікаційної роботи здійснюється на базі інфраструктури міжнародної компанії WorkDataNet.

WorkDataNet є міжнародною сервісною аутстаффінговою компанією, ключовий вектор діяльності якої спрямований на розгортання в Україні центрів

досліджень і розробок (R&D), формування профільних проєктних груп для IT-індустрії, а також надання офшорних і наземних технологічних рішень з метою задоволення глобального попиту на висококваліфіковані IT-кадри. Компанія забезпечує формування індивідуальних проєктних команд, повністю адаптованих під специфіку конкретних завдань, що сприяє створенню інноваційних програмних продуктів. Для забезпечення довгострокового партнерства із закордонними контрагентами залучаються профільні експерти високого кваліфікаційного рівня, які розробляють конкурентоспроможні рішення у таких високотехнологічних доменах, як:

– 3D modelling;
– Artificial Intelligence (AI);
– App Development;
– E-commerce;
– UI/UX Design;
– Data Analysis;
– Machine Learning;
– Data Science.

Один із ключових філіалів компанії територіально розташований у центральній частині м. Харкова, займає три поверхи та розрахований на 30 постійних робочих місць.

1.2 Структурна організація локальних комп'ютерних мереж

Формування архітектури ЛОМ, крім кінцевих користувацьких пристроїв, базово передбачає інтеграцію трьох ключових компонентів: мережних адаптерів, фізичного середовища передачі даних (кабельної системи) та відповідного

програмного забезпечення. У межах розробки кваліфікаційної роботи класифікацію ЛОМ доцільно представити через призму таких базових ознак:

– Топологія: просторова та геометрична конфігурація розташування вузлів і з'єднань у мережі (наприклад, лінійна або кільцева топології).

– Протоколи: стандартизовані правила та специфікації кодування, що регламентують процес трансляції даних (найбільш поширеним є стек протоколів TCP/IP у середовищі Ethernet). Мережні протоколи також детермінують архітектурний тип мережі – одноранговий (Peer-to-Peer) або клієнт-серверний (Client-Server).

– Середовище передачі (носій): фізичні канали зв'язку, представлені симетричним кабелем (кручена пара), коаксіальним або волоконно-оптичним кабелем.

Апаратну взаємодію в ЛОМ, що регулюється програмним забезпеченням, забезпечують спеціалізовані інтерфейси – блоки доступу до мережі. Дані пристрої інтегруються безпосередньо в материнські плати обчислювальних машин у вигляді мережних карт. Їх функціонал полягає у встановленні фізичного зв'язку, моніторингу доступності каналу, буферизації та регулюванні швидкості передачі масивів даних, мінімізації та усуненні помилок і колізій під час трансляції, а також в агрегації даних із ЛОМ у структурованому вигляді [1, 2].

Метод доступу до ресурсів мережі базується на адресації абонента за його мережевим ідентифікатором із використанням комутації каналів у вузлі комунікації (ВК). Дана технологія передбачає встановлення безперервного фізичного або логічного з'єднання між абонентами через ВК на час сесії передачі інформаційного пакета. При цьому архітектура ВК дозволяє гнучко налаштовувати пріоритетність доступу окремих абонентів до загального мережного ресурсу [1].

Серед ключових переваг ЛОМ такого типу слід виділити:

– Економічну ефективність та відносну простоту процедури інтеграції нових користувачів.

– Ергономічність та спрощену структуру адміністрування й керування мережними процесами.

– Можливість оперативного підключення або виведення з експлуатації окремих абонентських вузлів без порушення стабільності функціонування всієї системи.

До основних недоліків відносяться:

–Деградація швидкості передачі повідомлень залежно від динамічного зростання кількості активних абонентів, інтенсивності трафіку та безпосередньої пропускної здатності ВК.

– Пряма залежність загальної відмовостійкості та надійності мережі від працездатності центрального ВК.

– Значна сумарна протяжність ліній зв'язку та порівняно низький коефіцієнт корисного використання фізичного середовища трансляції сигналів.

З метою нівелювання зазначених недоліків та підвищення рівня відмовостійкості системи, сучасні ВК проєктуються за модульним принципом, який передбачає функціонування дубльованих (робочих і резервних) модулів. Інтегрована підсистема автоматизованої діагностики безперервно оцінює параметри життєдіяльності активного модуля і, в разі фіксації критичних помилок або апаратних збоїв, здійснює миттєве перемикання мережної інфраструктури на роботу з резервним блоком [2].

1.3 Класифікація локальних комп'ютерних мереж

Локальні комп'ютерні мережі можливо класифікувати за ознаками, які приведені в табл. 1.1.

Таблиця 1.1 – Класифікація локальних мереж

Ознака класифікації	Типи ЛОМ	Стисла характеристика та функціональне призначення
За архітектурою управління (організацією взаємодії)	Однорангові (Peer-to-Peer)	Усі вузли мають рівні права; адміністрування децентралізоване.
	Клієнт-серверні (Client-Server)	Виділено один або кілька серверів, які керують ресурсами та безпекою.
За топологією	Шина (Bus)	Спільний канал передачі; вразливий до обриву кабелю.
	Кільце (Ring)	Послідовне з'єднання вузлів у замкнене коло.
	Зірка (Star)	Усі вузли підключені до центрального комутатора (найпопулярніша).
	Гібридні (Tree/Mesh)	Поєднання кількох топологій (наприклад, зірково-шинна).
За середовищем передачі даних	Дротові (кабельні)	Використовують кручену пару, коаксіал або волоконно-оптичний кабель.
	Бездротові (Wireless)	Передача даних через радіоканал (Wi-Fi, Bluetooth).
За технологією передачі (протоколами)	Ethernet / Fast Ethernet / Gigabit Ethernet	Найбільш поширені стандарти провідного зв'язку (до 10-100 Гбіт/с).
	Wi-Fi (стандарти IEEE 802.11)	Технології бездротового пакетного обміну даними.

Прожовження таблиці 1.1.

За швидкістю передачі даних	Низькошвидкісні (до 10 Мбіт/с)	Застарілі системи або спеціалізовані промислові мережі.
	Середньошвидкісні (до 100 Мбіт/с)	Стандартні мережі для невеликих офісів.
	Високошвидкісні (понад 1 Гбіт/с)	Сучасні корпоративні мережі з високою інтенсивністю трафіку.
За призначенням (сферою застосування)	Установчі (офісні)	Інтеграція робочих місць співробітників, автоматизація документообігу.
	Промислові (виробничі / АСУ ТП)	Управління технологічним обладнанням, станками, датчиками.
	Науково-дослідні	Обробка великих масивів даних, моделювання, інженерні розрахунки.

1.4 Топологічні структури локальних обчислювальних мереж

Під мережною топологією (архітектурною конфігурацією, просторовою структурою) розуміють геометричне та фізичне взаєморозташування обчислювальних вузлів, а також спосіб їх інтеграції за допомогою ліній зв'язку. Слід зазначити, що детерміноване поняття топології є базовим саме для локальних мереж, де архітектуру з'єднань можна чітко простежити та зафіксувати. Натомість у глобальних мережах (WAN) топологічна структура є динамічною та прихованою від кінцевого користувача, оскільки кожен окремий сеанс зв'язку та маршрутизація пакетів даних можуть здійснюватися за унікальними індивідуальними траєкторіями [1].

У телекомунікаційній практиці виділяють такі базові топології ЛОМ:

– Шина (Bus) – архітектурна схема, в якій усі робочі станції паралельно підключаються до єдиного спільного каналу передачі даних (рис. 1.1).

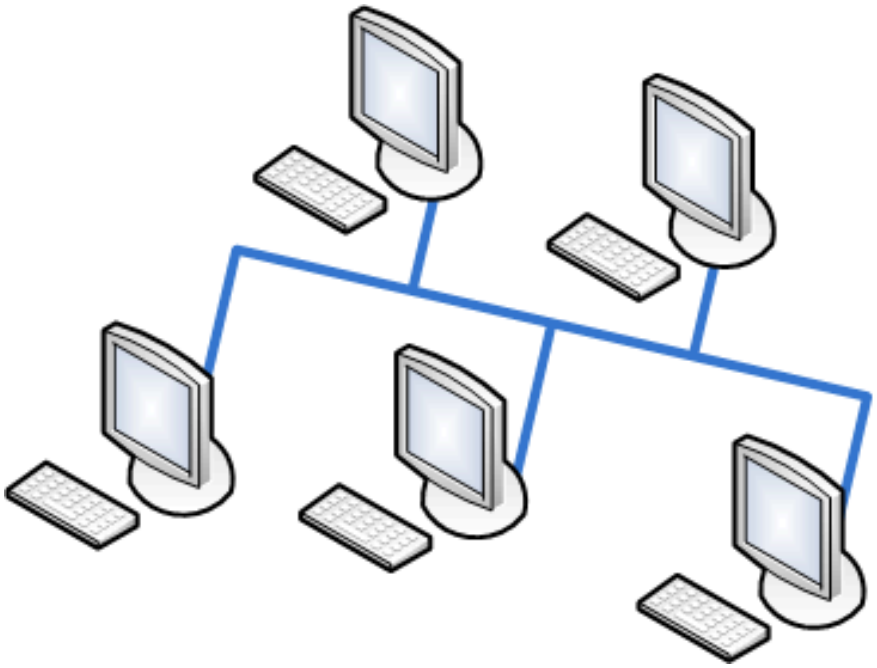


Рисунок 1.1 – Мережна топологія шина

– Зірка (Star) – конфігурація, яка за принципом централізації поділяється на два основні підвиди:

– Активна зірка – класична схема, де в ролі центрального інтегруючого елемента виступає головна обчислювальна машина (хост/сервер), яка безпосередньо приймає та обробляє потоки даних (рис. 1.2).

– Пасивна зірка – сучасна реалізація, де центральним вузлом є спеціалізоване мережне обладнання – комутатор (світч) або концентратор, що здійснює комутацію каналів або пакетів без безпосереднього аналізу вмісту програмного коду (рис. 1.3).

– Кільце (Ring) – топологія, за якої всі робочі станції послідовно об'єднуються в замкнене кільцеве середовище передачі сигналів (рис. 1.4).

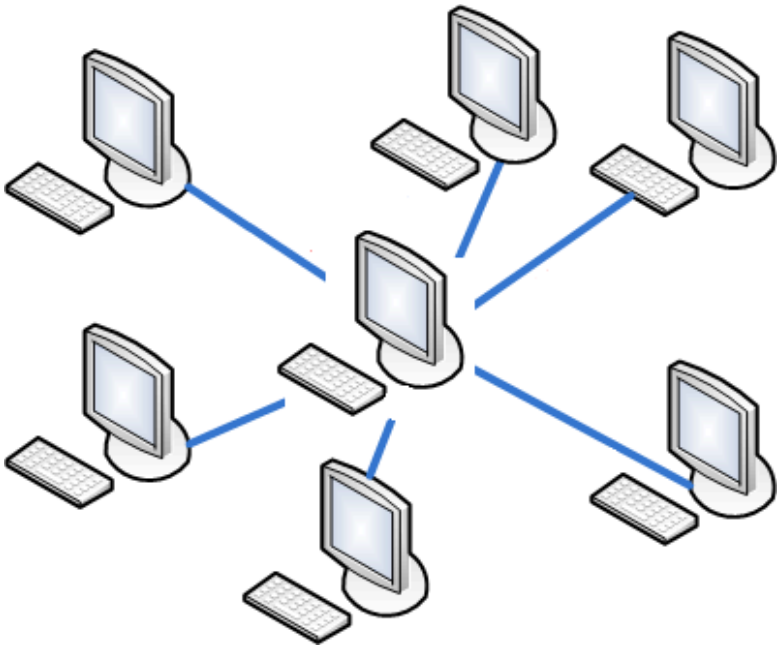


Рисунок 1.2 – Активна зірка

Вибір конкретного топологічного рішення є критично важливим етапом проєктування, оскільки він системно визначає ключові техніко-економічні та експлуатаційні характеристики майбутньої мережі, зокрема:

– Склад, номенклатуру та специфікацію необхідного мережного обладнання.

– Пропускну здатність та інтегральні характеристики кінцевих пристроїв.

– Потенціал масштабованості та можливості подальшого розширення мережної інфраструктури.

– Методологію адміністрування та загального управління мережними процесами.

Для реалізації завдання цієї кваліфікаційної роботи було обрано топологію «пасивна зірка». Історично концепція зіркоподібної топології походить від архітектури мейнфреймів, де центральний комп'ютер виконував роль активного вузла обробки всієї периферійної інформації [2].

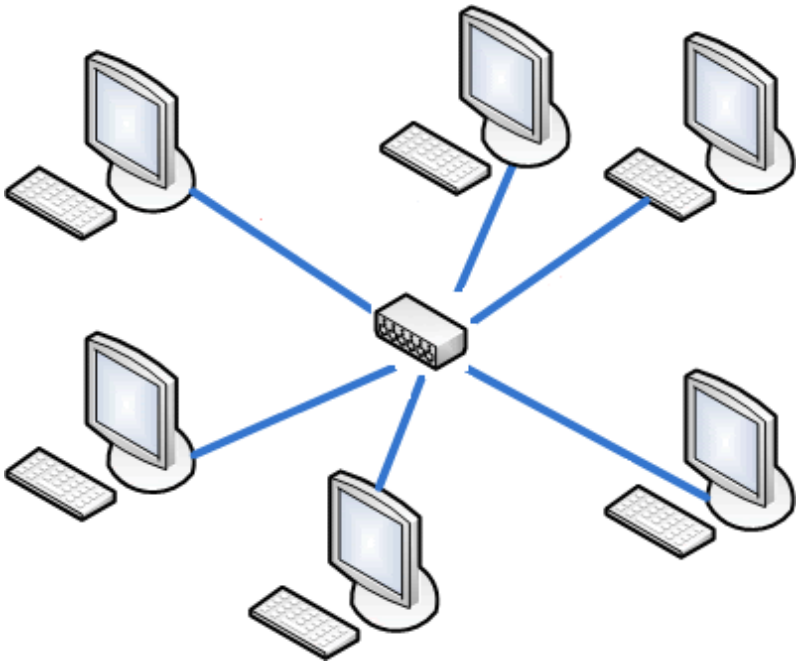


Рисунок 1.3 – Пасивна зірка

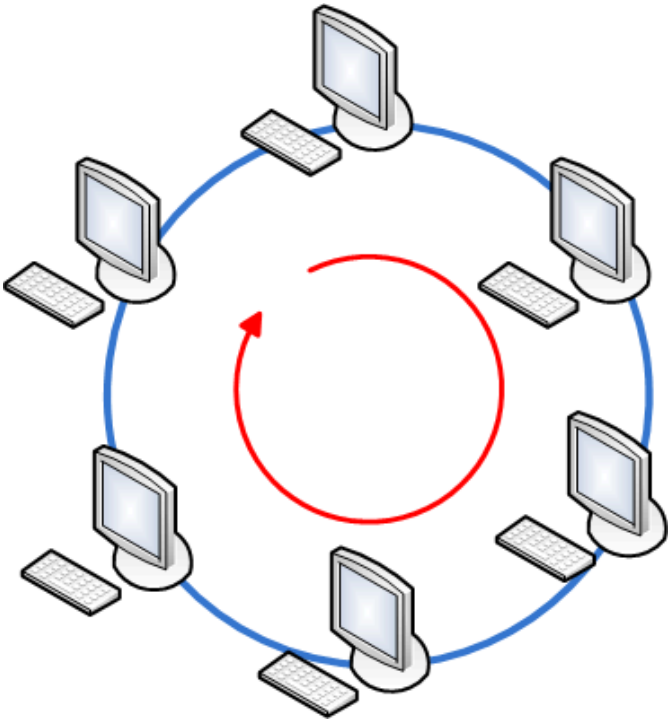


Рисунок 1.4 – Мережна топологія кільце

У сучасних системах передачі даних цей принцип адаптовано: трансляція інформаційних потоків між двома периферійними робочими станціями обов'язково здійснюється через центральний комутаційний вузол мережі.

Зіроподібна топологія демонструє найвищі показники продуктивності серед базових конфігурацій обчислювальних мереж. Це зумовлено тим, що обмін даними між кінцевими вузлами відбувається через високопродуктивний центральний комутатор за допомогою виділених ліній зв'язку, які експлуатуються виключно цими робочими станціями. Завдяки такій структурі частота виникнення колізій та затримок при взаємних запитах є мінімальною порівняно з іншими топологічними схемами.

Додатковою перевагою мереж із топологією «зірка» є простота їх модифікації та високий рівень локальної відмовостійкості. У разі апаратного або програмного збою на одній із робочих станцій (або пошкодження її індивідуального кабельного сегмента), вся інша мережна інфраструктура продовжує функціонувати в штатному режимі. З ладу виходить лише той вузол, який зазнав пошкодження.

З огляду на вищезазначене, для об'єкта проєктування (компанії WorkDataNet) топологію «зірка» було обрано на основі таких системних критеріїв [2]:

– Необхідність забезпечення стабільного функціонування значної кількості індивідуальних робочих місць.

– Оптимальне співвідношення фінансових витрат на розгортання та підсумкової ефективності мережі.

– Простота і висока технологічність монтажу, пусконалагоджувальних робіт та подальшої експлуатації.

– Високий потенціал для швидкої модернізації та гнучкого масштабування мережі у разі розширення штату підприємства.

ВИСНОВКИ ДО РОЗДІЛУ 1

У першому розділі кваліфікаційної роботи виконано комплексний теоретико-методологічний аналіз принципів побудови та функціонування локальних обчислювальних мереж (ЛОМ), а також визначено ключові архітектурні рішення для об'єкта проєктування.

За результатами аналізу науково-технічних джерел встановлено, що сучасна ЛОМ є складним інтегрованим середовищем, ефективність якого залежить від системного поєднання апаратних інтерфейсів, фізичного носія та мережевих протоколів. Розглянуто класифікацію ЛОМ та здійснено порівняльний аналіз базових топологій (шина, кільце, зірка). Визначено, що для корпоративного сегмента найбільш оптимальною є клієнт-серверна архітектура з використанням топології «зірка» на базі центрального комутатора. Дане рішення мінімізує частоту колізій, спрощує адміністрування та забезпечує високу локальну відмовостійкість системи.

Практичну частину дослідження орієнтовано на інфраструктуру Харківського офісу міжнародної IT-компанії «WorkDataNet», що налічує 30 робочих місць. Враховуючи специфіку діяльності компанії (розробка ПЗ, AI, Data Science), яка вимагає високої пропускної здатності та захищеності каналів зв'язку, обґрунтовано доцільність проєктування високошвидкісної ЛОМ із топологією «пасивна зірка». Обраний підхід дозволить створити масштабовану та економічно ефективну мережну інфраструктуру, повністю адаптовану до високих вимог сучасного IT-підприємства.

2 ПРОЄКТУВАННЯ СТРУКТУРОВАНОЇ КАБЕЛЬНОЇ СИСТЕМИ ПІДПРИЄМСТВА

2.1 Концептуальні засади та архітектура СКС

Структурована кабельна система (СКС) являє собою універсальну, інтегровану та ієрархічну кабельну інфраструктуру будівлі або комплексу споруд, яка розрахована на тривалий період експлуатації без необхідності проведення капітальної перебудови чи модернізації фізичного середовища. Проєктування СКС виконується відповідно до міжнародних та національних стандартів (зокрема ISO/IEC 11801 та ANSI/TIA/EIA-568), що гарантує мультипротокольність, тобто здатність системи підтримувати одночасну передачу різноридних сигналів (цифрових даних, мовного трафіку, відеопотоків, сигналів систем безпеки) [3].

Головна перевага СКС полягає у її надлишковості та гнучкості: конфігурація робочих місць і сервісів може змінюватися виключно шляхом комутації на кросс-панелях без прокладання нових кабельних ліній. Відповідно до архітектурних стандартів, у структурі СКС офісу компанії «WorkDataNet» виділено чотири ключові функціональні підсистеми:

– Підсистема робочих груп;

– Горизонтальна кабельна підсистема;

– Магістральна підсистема будівлі (вертикальна підсистема);

– Підсистема телекомунікаційних приміщень та адміністрування.

2.2 Функціональний аналіз підсистем СКС компанії

2.2.1 Підсистема робочого простору

Даний компонент призначений безпосередньо для підключення термінального обладнання кінцевих користувачів (персональних комп'ютерів, графічних станцій, мережних принтерів, IP-телефонів, точок доступу Wi-Fi) до телекомунікаційної інфраструктури через інформаційні розетки (RJ-45). До складу підсистеми робочого простору входять:

– Інформаційні модульні розетки, інтегровані в кабельні канали або безпосередньо в елементи меблів.

– Комутаційні кабелі (патч-корди) фабричного виробництва, що забезпечують безпосереднє з'єднання інтерфейсу ПК із розеткою.

– Адаптери та узгоджувальні пристрої (за потреби підключення специфічного обладнання).

Ефективне функціонування СКС безпосередньо гарантує стабільність фізичного з'єднання на рівні робочого простору, де критично важливим є використання сертифікованих компонентів для запобігання затуханню сигналу [3].

2.2.2 Горизонтальна підсистема та просторова організація поверхів

Горизонтальна підсистема охоплює простір від інформаційної розетки робочого місця до горизонтального крос-з'єднання (патч-панелі), розташованого в телекомунікаційній шафі на поточному поверсі. Основними компонентами є горизонтальні кабельні лінії, розетки та комутаційне обладнання в шафі.

Згідно з вимогами стандартів проектування (ISO/IEC 11801):

– Довжина горизонтального кабелю на ділянці від інформаційної розетки до крос-панелі не повинна перевищувати 90 метрів, незалежно від типу середовища передачі. Додатково допускається використання до 10 метрів сумарної довжини патч-кордів для комутації.

– На кожне організоване робоче місце необхідно передбачити не менше 2-х ліній горизонтального кабелю (одна для передачі даних, інша – для телефонії або як резерв/альтернативний канал) [4].

Розподіл робочих зон на поверхах компанії відображено на схематичному плані (рис. 2.1).

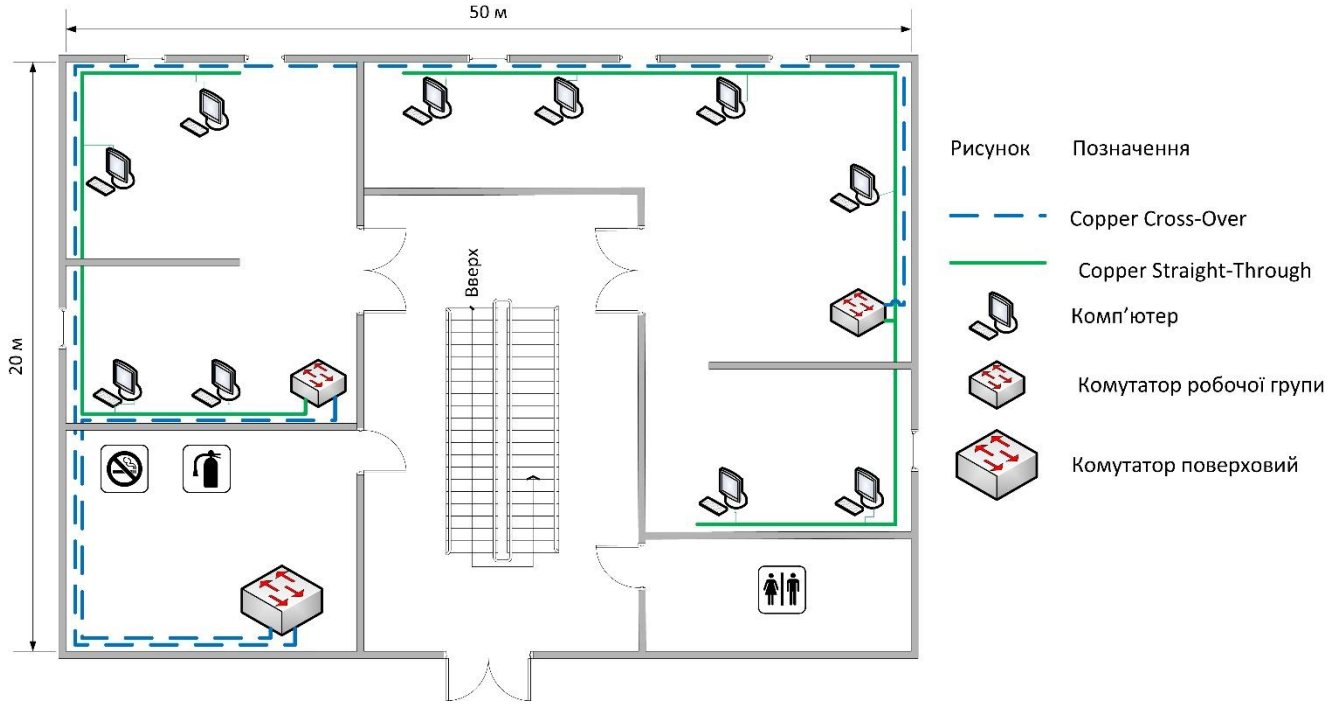


Рисунок 2.1 – Організація поверхів

Для оптимізації кабельного господарства та забезпечення високих експлуатаційних характеристик в умовах офісу впроваджено такі рішення:

– Розрахунок матеріалів: Середня витрата кабелю типу «кручена пара» становить орієнтовно 240 метрів на один поверх будівлі.

– Вибір середовища передачі: Застосовано неекрановану кручену пару категорії 5e (UTP Cat. 5e), що задовольняє вимогам технології Fast Ethernet (100BASE-TX) на поточному етапі, а також містить закладений технічний

потенціал (надлишковість) для переходу на технологію Gigabit Ethernet (1000BASE-T) у процесі подальшого розвитку корпоративної мережі.

– Кабельні траси: Монтаж кабельних ліній виконується вздовж стінових поверхонь у спеціалізованих захисних пластикових коробах (кабель-каналах), що захищає провідники від механічних пошкоджень та мінімізує вплив електромагнітних завад. Міжповерховий тракт прокладається у вертикальних технологічних шахтах, розташованих поблизу сходового отвору.

– Апаратна оптимізація: З метою раціонального використання бюджету проєкту та оптимізації кількості активного обладнання було прийнято рішення розгорнути 2 комутатори для обслуговування 5 робочих груп. Локально для кожної робочої групи реалізовано топологію «зірка» з комутатором у центрі, що гарантує високу ізоляцію відмов на рівні кінцевих сегментів [4].

2.2.3 Вертикальна (магістральна) підсистема будівлі

Магістральна підсистема будівлі є вертикальним ядром СКС, яке забезпечує консолідацію та розподіл інформаційних потоків по всій споруді. Її першочергове призначення – функціональне об'єднання поверхових розподільних пунктів (горизонтальних підсистем) між собою, а також їх підключення до головного комутаційного вузла організації та підсистеми адміністрування.

Базою для побудови вертикальної магістралі виступають багатопарні мідні кабелі підвищених категорій або волоконно-оптичні лінії зв'язку (ВОЛЗ), які доповнюються металевими лотками, гільзами та закладними трубами для міжповерхового переходу. Схематична структура вертикальної інтеграції 3-поверхового офісу компанії «WorkDataNet» представлена на рис. 2.2.

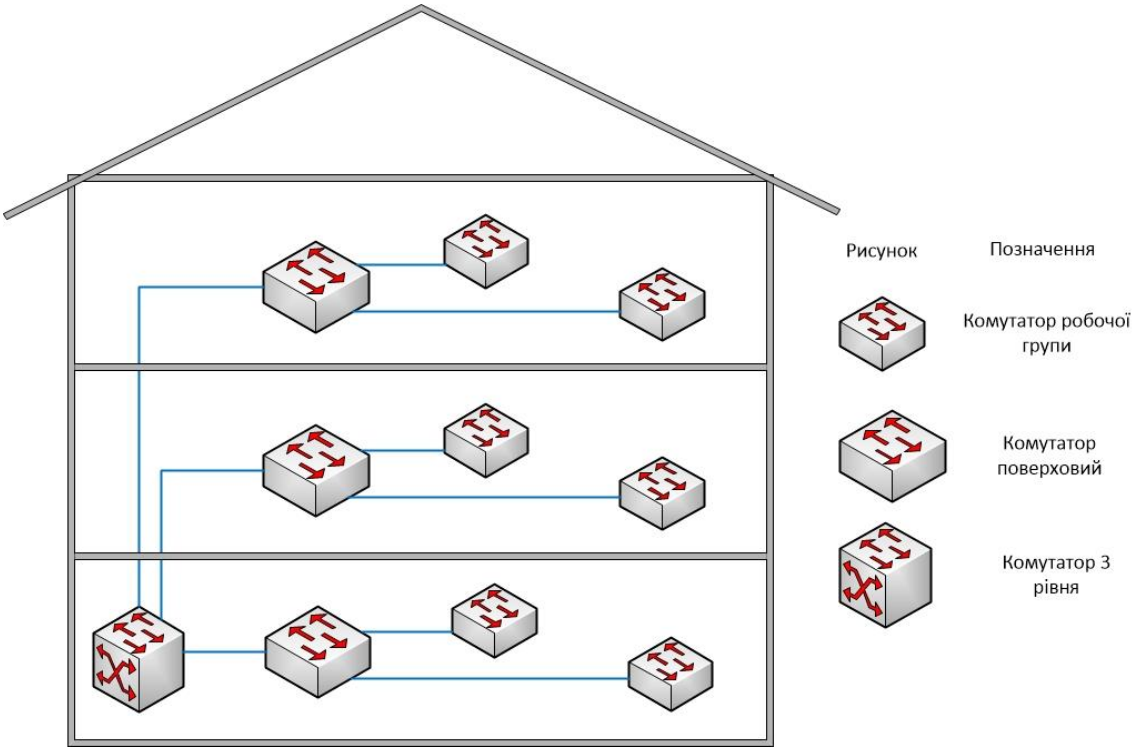


Рисунок 2.2 – Організація будівлі компанії

Організація магістрального середовища характеризується такими параметрами:

– Метраж: сумарний обсяг кабелю для побудови міжповерхових з'єднань у триповерховому корпусі становить близько 730 метрів.

– Магістральний носій: для вертикальної комутації використано високоякісний мідний кабель категорії UTP Cat. 5e. Взаємодія між поверховими комутаційними вузлами реалізована за стандартом 100BASE-TX (Fast Ethernet), що забезпечує стабільну швидкість магістрального обміну на рівні 100 Мбіт/с із можливістю агрегації каналів у майбутньому.

– Топологічна структура: з'єднання горизонтальних підсистем між собою виконано за ієрархічною топологією «зірка». Центральним елементом і ядром всієї мережі виступає комутатор 3-го рівня (Layer 3) моделі OSI. Використання L3-комутатора є архітектурно виправданим для компанії, оскільки воно дозволяє не

лише здійснювати високошвидкісну комутацію пакетів, а й реалізувати міжмережну маршрутизацію (між різними VLAN робочих груп), забезпечити впровадження політик безпеки (ACL) та керувати пріоритезацією трафіку (QoS), що вкрай важливо для розробників ПЗ та інженерів Data Science [4].

ВИСНОВКИ ДО РОЗДІЛУ 2

У другому розділі кваліфікаційної роботи було здійснено практичне проєктування та розрахунок структурованої кабельної системи (СКС) для триповерхового офісу компанії «WorkDataNet».

На основі міжнародних стандартів (ISO/IEC 11801) додано чотирирівневу архітектуру СКС, яка включає підсистеми робочого простору, горизонтальну та вертикальну магістральні підсистеми, а також вузли адміністрування. Під час проєктування горизонтального сегмента обгрунтовано впровадження неекранованої крученої пари категорії UTP Cat. 5e та визначено витрату кабелю в обсязі 240 метрів на один поверх з дотриманням правила обмеження довжини променя до 90 метрів. Для підвищення локальної відмовоїйкості та економічної оптимізації проєкту реалізовано топологію «зірка» на базі двох комутаторів для обслуговування п'яти робочих груп.

У межах вертикальної підсистеми розраховано магістральний тракт загальною протяжністю 730 метрів. Ключовим архітектурним рішенням стало використання на магістральному рівні високопродуктивного комутатора 3-го рівня (Layer 3) моделі OSI. Це забезпечує не лише стабільну роботу технології Fast Ethernet, а й створює надійну базу для впровадження міжмережної маршрутизації (VLAN), політик безпеки та пріоритезації трафіку. Спроєктована СКС має високий рівень гнучкості, капітальної надлишковості та повністю готова до інтеграції активного мережного обладнання.

3 ОБГРУНТУВАННЯ ТА ВИБІР АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ І СИСТЕМ МЕРЕЖНОЇ БЕЗПЕКИ

3.1Критерії вибору мережного обладнання

Процес підбору активного та пасивного мережного обладнання для розгортання локальної обчислювальної мережі (ЛОМ) підприємства є багатокритеріальним завданням. Техніко-економічне обгрунтування вибору комутаторів, маршрутизаторів та кабельної продукції в межах цього проєкту базується на таких ключових чинниках:

– Пропускна здатність та швидкісні характеристики: забезпечення гігабітних швидкостей (10/100/1000 Мбіт/с) на рівні кінцевих пристроїв та магістральних ліній зв'язку.

– Технологічна сумісність: повна відповідність обладнання мережним стандартам та канальним технологіям (Fast/Gigabit Ethernet, PoE/PoE+, стандарти Wi-Fi 6).

– Керованість та масштабованість: наявність інструментів централізованого адміністрування, підтримка стеків протоколів L2/L3 моделей OSI, можливість гнучкого розширення мережі.

– Економічна доцільність: оптимальне співвідношення капітальних витрат на придбання обладнання (CapEx) до його продуктивності, відмовостійкості та вартості подальшого обслуговування (OpEx) [5, 6].

3.2 Технічний опис та специфікація обраного обладнання

Для побудови корпоративної мережі Харківського філіалу ІТ-підприємства було обрано лінійку професійного бізнес-обладнання від компанії TP-Link (серія Omada та JetStream) [7].

3.2.1 Центральний бізнес-маршрутизатор ЛОМ

Для забезпечення периметра безпеки, маршрутизації та організації бездротового сегмента обрано сучасний гігабітний VPN-маршрутизатор TP-Link Omada ER706W (або аналог серії ER7206) з підтримкою Wi-Fi 6, що прийшов на заміну застарілим домашнім рішенням. У табл. 3.1 наведені технічні характеристики маршрутизатора TP-Link Omada [7].

Таблиця 3.1 – Технічні характеристики маршрутизатора TP-Link Omada

Група параметрів	Назва характеристики	Значення та опис параметра
Бездротова мережа	Стандарти зв'язку	IEEE 802.11ax/ac/n/a (5 ГГц), IEEE 802.11ax/n/b/g (2.4 ГГц) – Wi-Fi 6
	Швидкість Wi-Fi	До 2402 Мбіт/с (5 ГГц) + до 574 Мбіт/с (2.4 ГГц)
	Антени	3 зовнішні знімні антени з підтримкою MU-MIMO
Провідна мережа	Інтерфейси	гігабітний порт SFP WAN/LAN, 1 гігабітний порт WAN, 4 гігабітні порти LAN/WAN

Продовження таблиці 3.1

	Процесор	Двоядерний процесор із тактовою частотою 1.2 ГГц
	Оперативна пам'ять	512 MB DDR3 + 128 MB NAND Flash
Мережна безпека	Шифрування Wi-Fi	WEP, WPA, WPA2, WPA3-Enterprise
	Міжмережний екран	SPI Firewall, захист від DoS/DDoS атак, фільтрація IP/MAC/URL
	Функції захисту	Multi-SSID, ізоляція пристроїв, прив'язка IP-MAC, DHCP Snooping
VPN та Протоколи	Підтримувані VPN-тунелі	WireGuard, IPsec VPN, OpenVPN, PPTP, L2TP
	Підтримувані VPN-тунелі	IPv4, IPv6, VLAN (802.1Q), Мережна маршрутизація (Static, RIP, OSPF)

3.2.2 Магістральний керований комутатор 3-го рівня (L3/L2+)

Для забезпечення центральної комутації на рівні будівлі, міжмережної маршрутизації та агрегації каналів обрано керований комутатор TP-Link JetStream TL-SG3428X (заміна застарілим некерованим моделям). У табл. 3.2 наведені технічні характеристики магістрального комутатора JetStream [7].

Таблиця 3.2 – Характеристики магістрального комутатора JetStream

Назва характеристики	Значення та функціональний опис
Інтерфейси підключення	24 гігабітні порти RJ45 (10/100/1000 Мбіт/с) + 4 розрядні слоти 10G SFP+ для високошвидкісних магістралей
Комутаційна здатність	128 Гбіт/с (неблокуюча архітектура масиву)
Швидкість пересилання пакетів	95.23 млн пакетів за секунду (Mpps)
Функції 3-го рівня (L3)	Статична маршрутизація (Static Routing), IPv4/IPv6 IPv4/IPv6 Static Routing, DHCP Server, DHCP Relay
Функції безпеки та управління	IP-MAC-Port Binding, Access Control Lists (ACL), 802.1Q VLAN, Port Security, Storm Control, інструмент захисту від DoS

3.2.3 Поверхові комутатори з підтримкою технології PoE+

Для безпосереднього підключення робочих груп, живлення IP-телефонів та точок доступу Wi-Fi на поверхах застосовано керований комутатор TP-Link JetStream TL-SG3428MP. У табл. 3.3 наведені технічні характеристики поверхового PoE+ комутатора [7].

Таблиця 3.3 – Характеристики поверхового PoE+ комутатора

Назва характеристики	Значення та опис параметра
Портова конфігурація	24 гігабітні порти RJ45 з підтримкою PoE+ (802.3at/af) + 4 гігабітні SFP-слоти
Бюджет потужності PoE	384 Вт сумарно (до 30 Вт на один порт), що дозволяє живити будь-яку периферію

Продовження таблиці 3.3.

Функції QoS	Пріоритезація трафіку за стандартами 802.1p CoS/DSCP, 8 черг пріоритетів
Пріоритезація трафіку за стандартами 802.1p CoS/DSCP, 8 черг пріоритетів	16 000 записів (16K), підтримка кадрів Jumbo до 9 Кбайт

3.2.4 Середовище передачі даних

З метою повної відповідності стандартам проєктування та забезпечення надійної передачі даних, замість бюджетного алюмінієвого кабелю (CCA) обрано екранований мідний кабель FTP Cat. 6 Solid Copper (табл. 3.4) [7, 8].

Таблиця 3.4 – Технічні параметри кабелю передачі даних

Параметр	Технічний опис та значення
Тип кабелю / Категорія	FTP (Foiled Twisted Pair) – екранована кручена пара / Категорія 6
Матеріал провідника	Чиста електротехнічна мідь (Solid Bare Copper), калібр провідника 23 AWG
Екранування	Загальний екран з алюмінієвої фольги зі дренажним провідником для захисту від наведень
Швидкісні стандарти	Повна підтримка 100BASE-TX, 1000BASE-T та перспектива 10GBASE-T (до 55 метрів)
Оболонка кабелю	LSZH (Low Smoke Zero Halogen) – вогнестійкий пластик із низьким виділенням диму

3.3Комплексна безпека локальної обчислювальної мережі

Забезпечення інформаційної безпеки (ІБ) в умовах сучасного ІТ-підприємства є безперервним інженерно-організаційним процесом, спрямованим на захист конфіденційності, цілісності та доступності корпоративних даних. До основних загроз та векторів мережних атак у середовищі ЛОМ належать:

– Сніффінг (Sniffing): несанкціоноване перехоплення мережного трафіку за допомогою переведення мережевих адаптерів у нерозбірливий режим (promiscuous mode). Зловмисники використовують аналізатори пакетів (сніффери) для зчитування конфіденційних даних (паролів, сесій).

– ARP-спуфінг (ARP Spoofing/ARP Poisoning): атака типу «людина посередині» (Man-In-The-Middle – MITM), під час якої у локальну мережу надсилаються фальшиві ARP-повідомлення. Це призводить до зв'язування MAC-адреси зловмисника з IP-адресою легітимного вузла (наприклад, шлюзу за замовчуванням), що дозволяє повністю перехоплювати та модифікувати трафік [5].

– DHCP Spoofing (Rogue DHCP): розгортання зловмисником несанкціонованого DHCP-сервера в мережі, який видає користувачам підроблені мережні налаштування (зокрема, хибні адреси DNS-серверів або шлюзів) для реалізації фішингу та MITM-атак.

– MAC-флудинг (MAC Flooding): лавинне розсилання підроблених MAC-адрес з метою переповнення таблиці комутатора (CAM-таблиці). Це змушує комутатор перейти в режим роботи хаба (транслювати трафік на всі порти), полегшуючи сніффінг.

– DoS/DDoS атаки: генерація аномального трафіку (наприклад, SYN-флуд) для виведення з ладу мережних сервісів [8].

3.3.1 Апаратні та програмні інструменти захисту

Для нейтралізації вищеперелічених загроз у спроєктованій мережі «WorkDataNet» на базі обраного керованого обладнання TP-Link реалізуються такі захисні механізми:

– DHCP Snooping: функція комутатора, яка розділяє порти на «довірені» (де підключено легітимний DHCP-сервер) та «недовірені» (користувацькі). Усі DHCP-відповіді з недовірених портів автоматично блокуються, що унеможливлює атаку Rogue DHCP.

– Dynamic ARP Inspection (DAI): технологія, яка перехоплює всі ARP-запити та відповіді на недовірених портах і звіряє їх із базою даних, сформованою процесом DHCP Snooping. Пакети з невалідними парами IP-MAC негайно відкидаються, повністю нівелюючи загрозу ARP-спуфінгу [4].

– Портова безпека (Port Security): обмеження кількості MAC-адрес, які можуть бути вивчені на одному фізичному порту комутатора, що запобігає атакам типу MAC-флудинг.

– Сегментація мережі через VLAN (IEEE 802.1Q): ізоляція трафіку різних робочих груп та відділів підприємства на канальному рівні [6, 8].

3.3.2 Протоколи інформаційної безпеки різних рівнів

Для захисту даних під час трансляції через відкриті та внутрішні канали зв'язку використовуються криптографічні протоколи, інтегровані в різні рівні моделі OSI/TCP-IP:

– Прикладний рівень (PGP): Протокол Pretty Good Privacy застосовується для автентифікації, шифрування та забезпечення цілісності повідомлень електронної пошти за допомогою цифрових підписів та асиметричної криптографії.

– Транспортний рівень (SSL/TLS): Протокол Transport Layer Security (наступник SSL) функціонує між транспортним і прикладним рівнями. Він забезпечує захист сесій обміну даними (наприклад, HTTPS) через механізм рукостискання (handshake), під час якого сторони верифікують одна одну та генерують симетричний сесійний ключ для шифрування.

– Мережний рівень (IPSec): Набір протоколів Internet Protocol Security забезпечує прозоре шифрування та автентифікацію всього IP-трафіку. Він є базою для побудови безпечних корпоративних VPN-тунелів між філіалами компанії [6].

3.3.3 Захист протоколів маршрутизації

Динамічні протоколи маршрутизації (RIP, OSPF, BGP) є вразливими до ін'єкцій хибних маршрутів. Для захисту від DoS-атак та перехоплення маршрутів у роботі реалізовано криптографічний захист відповідно до стандарту RFC-2082.

Замість передачі паролів відкритим текстом застосовується автентифікація на основі односторонніх хеш-функцій (алгоритм MD5). Секретний ключ, відомий лише суміжним маршрутизаторам, змішується з тілом пакета маршрутизації, після чого обчислюється унікальний хеш. Сам ключ ніколи не передається по мережі. Одержувач проводить аналогічне обчислення, і в разі незбігу хеш-значень пакет маршрутизації миттєво відхиляється, що гарантує цілісність таблиць маршрутизації підприємства [8, 9].

ВИСНОВКИ ДО РОЗДІЛУ 3

У третьому розділі кваліфікаційної роботи виконано комплексне обгрунтування та підбір активного обладнання і засобів мережної безпеки для локальної обчислювальної мережі IT-компанії «WorkDataNet».

На основі розроблених критеріїв продуктивності, керованості та економічної доцільності, застаріле побутове обладнання було замінено на сучасні рішення бізнес-класу від компанії TP-Link (серії Omada та JetStream). Для забезпечення периметра мережі та маршрутизації обрано гігабітний VPN-маршрутизатор Omada ER706W з підтримкою стандарту Wi-Fi 6 та шифрування WPA3-Enterprise. Рівень агрегації та магістральної комутації реалізовано на базі керованого комутатора 3-го рівня JetStream TL-SG3428X з портами 10G SFP+, а рівень доступу робочих груп – на базі поверхових PoE+ комутаторів TL-SG3428MP. Специфіковано використання високоякісного мідного екранованого кабелю FTP Cat. 6 Solid Copper, що повністю відповідає чинним стандартам СКС.

У межах побудови системи захисту ЛОМ проаналізовано ключові загрози (сніффінг, DoS, ARP/DHCP-спуфінг) та впроваджено комплексні апаратні механізми захисту, такі як DHCP Snooping, Dynamic ARP Inspection (DAI) та сегментація трафіку через VLAN. Розглянуто застосування криптографічних протоколів різних рівнів моделі OSI (TLS, IPSec, PGP) та захист динамічної маршрутизації за допомогою алгоритму автентифікації MD5 (RFC-2082). Запропонований комплекс рішень гарантує високу пропускну здатність, відмовостійкість та захищеність корпоративної інформації відповідно до вимог сучасної IT-індустрії.

4 ЛОГІЧНА ОРГАНІЗАЦІЯ ТА СИМУЛЯЦІЙНЕ МОДЕЛЮВАННЯ МЕРЕЖІ ПІДПРИЄМСТВА

Розробка та реалізація проєкту потребують побудови чіткої логічної структури мережної інфраструктури, яка відображатиме взаємодію активного обладнання та кінцевих вузлів на мережному й канальному рівнях моделі OSI.

Для проектування, візуалізації та верифікації працездатності розробленої архітектури використано спеціалізоване середовище імітаційного моделювання Cisco Packet Tracer. Застосування цього програмного комплексу дозволяє виконати попереднє тестування мережних протоколів, перевірити коректність маршрутизації та налаштування політик безпеки в реальному часі. Графічний план розміщення обладнання та загальна схема симуляції представлені у Додатку А.

4.1 Адресний план та ієрархічне розбиття мережі на підмережі

Для організації внутрішнього інформаційного простору триповерхового офісу компанії було прийнято рішення використати діапазон приватних IP-адрес (так званих «сірих» адрес) класу C. Базовим простором визначено мережу 192.168.0.0/24.

Оскільки адміністративна будівля складається з 3 поверхів, а загальна кількість хостів становить 30 одиниць (по 10 робочих місць на поверх), вихідний адресний простір необхідно оптимізувати та розділити на ізольовані підмережі за допомогою механізму безкласової маршрутизації (CIDR).

У вихідній мережі префікс /24 означає, що перші три октети (192.168.0.) ідентифікують мережеву частину, а останній октет виділено для адресації хостів. Для створення ізольованих сегментів (VLAN) для кожного поверху використано

маску підмережі з префіксом /28 (маска 255.255.255.240). Це дозволяє розбити мережу на підмережі з кроком у 16 адрес, де кожна підмережа здатна обслуговувати до 14 легітимних IP-адрес кінцевих вузлів, що повністю задовольняє поточні потреби офісу (10 хостів на поверх) та забезпечує необхідний резерв для масштабування [5, 6].

Деталізований адресний план ЛОМ підприємства представлено в табл. 4.1.

Таблиця 4.1 – Схема розподілу адресного простору та віртуальних мереж (VLAN)

Номер поверху	Ідентифікатор віртуальної мережі	Адреса підмережі та маска (CIDR)	Маска підмережі в десятковому форматі	Діапазон адрес для кінцевих вузлів
1 поверх	VLAN 10	192.168.0.0/28	255.255.255.240	192.168.0.2 – 192.168.0.14
2 поверх	VLAN 20	192.168.0.16/28	255.255.255.240	192.168.0.18 – 192.168.0.30
3 поверх	VLAN 30	192.168.0.32/28	255.255.255.240	192.168.0.34 – 192.168.0.46

4.2 Конфігурування активного мережного обладнання

4.2.1 Налаштування центрального маршрутизатора

Для реалізації міжмережного обміну між ізольованими поверховими підмережами (VLAN) на маршрутизаторі застосовано технологію Router-on-a-Stick. На фізичному гігабітному інтерфейсі налаштовуються логічні підінтерфейси (subinterfaces) для кожної віртуальної мережі з інкапсуляцією трафіку за стандартом IEEE 802.1Q [6].

Нижче наведено фрагмент конфігураційного скрипту для першого поверху (VLAN 10):

```
interface GigabitEthernet0/0.10
 description Gateway_for_Floor_1
 encapsulation dot1Q 10
 ip address 192.168.0.1 255.255.255.240
exit
```

Аналогічно налаштовуються підінтерфейси GigabitEthernet0/0.20 з IP 192.168.0.17 та GigabitEthernet0/0.30 з IP 192.168.0.33.

Для автоматизації процесу призначення мережних налаштувань кінцевим робочим станціям на маршрутизаторі розгорнуто та активовано службу DHCP (Dynamic Host Configuration Protocol). З метою запобігання виникненню IP-конфліктів, адреси шлюзів за замовчуванням попередньо вилучаються з пулу динамічного розподілу:

```
service dhcp
ip dhcp excluded-address 192.168.0.1
ip dhcp excluded-address 192.168.0.17
ip dhcp excluded-address 192.168.0.33

ip dhcp pool VLAN10_Floor1
network 192.168.0.0 255.255.255.240
default-router 192.168.0.1
domain-name worknest.local exit
```

4.2.2 Конфігурування комутаційного обладнання

На центральному комутаторі 3-го рівня (L3), який здійснює агрегацію трафіку, виконується налаштування магістральних портів (Trunk) для трансляції маркованих кадрів усіх поверхових VLAN, а також створюються віртуальні інтерфейси керування (SVI):

```
vlan 10,20,30
exit


interface TenGigabitEthernet0/1
```

```
 description Trunk_to_Core_Router
 switchport trunk encapsulation dot1q
 switchport mode trunk
exit

interface GigabitEthernet0/1
 description Trunk_to_Floor1_Switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
exit
```

На поверхових комутаторах рівня доступу (L2) магістральний порт налаштовується в режим Trunk для зв'язку з ядром мережі, а користувацькі порти переводяться в режим Access із жорсткою прив'язкою до відповідного ідентифікатора VLAN:

```
interface GigabitEthernet0/1
 description Trunk_to_L3_Core
 switchport mode trunk
exit

interface GigabitEthernet0/2
 description Connect_to_PC_Floor1
 switchport mode access
 switchport access vlan 10
 spanning-tree portfast
exit
```

4.3 Аналіз та обгрунтування використаних канальних технологій

Основою для побудови фізичного та канального рівнів спроєктованої мережі є стандарти сімейства Ethernet, а саме технології Fast Ethernet та Gigabit Ethernet, що стандартизовані інститутом IEEE.

4.3.1 Технологія Fast Ethernet (стандарт IEEE 802.3u)

Технологія Fast Ethernet є еволюційним розвитком класичного стандарту Ethernet, який дозволив збільшити пропускну здатність фізичних сегментів до 100 Мбіт/с. Ключовими перевагами інтеграції цього стандарту є:

– Збереження базового методу доступу до середовища передачі (CSMA/CD) та структури кадру.

– Підтримка повнодуплексного режиму роботи, що повністю нівелює ризик виникнення колізій у комутованих мережах.

– Спадкоємність архітектурних рішень та збереження топології «зірка», що дозволяє використовувати традиційні кабельні системи на основі крученої пари та оптоволокна.

Стандарт IEEE 802.3u визначає три ключові специфікації фізичного рівня для різних типів носіїв [9]:

– 100BASE-TX: функціонує на базі двох пар неекранованої крученої пари (UTP) категорії 5/5e або екранованої кабельної системи (STP) з максимальною довжиною сегмента до 100 метрів. Це базовий стандарт для підключення периферійних пристроїв та робочих станцій в офісі «WorkDataNet».

– 100BASE-T4: специфікація для використання чотирьох пар кабелю UTP категорій 3, 4 або 5 (на сьогодні вважається застарілою та практично не застосовується).

– 100BASE-FX: стандарт передачі даних через багатомодовий волоконно-оптичний кабель, що забезпечує високу завадостійкість та гальванічну ізоляцію між сегментами.

4.3.2 Технологія Gigabit Ethernet (стандарт IEEE 802.3z / IEEE 802.3ab)

Технологія Gigabit Ethernet забезпечує пропускну здатність на рівні 1000 Мбіт/с (1 Гбіт/с), зберігаючи повну зворотну сумісність із попередніми стандартами 10/100 Мбіт/с. Це дозволяє організувати прозору ієрархічну структуру мережі без необхідності конвертації протоколів та переформатування кадрів між сегментами з різною швидкістю.

Впровадження гігабітних каналів у сучасній IT-компанії є критично необхідним для забезпечення потреб швидкісних систем розробки, обробки великих масивів даних (Data Science) та обміну внутрішньокорпоративним трафіком. Номенклатура фізичних інтерфейсів Gigabit Ethernet включає такі основні специфікації:

– 1000BASE-SX: оптичний сегмент, що використовує багатомодове волокно (MMF) і трансляцію світлового сигналу на довжині хвилі 850 нм (максимальна відстань до 550 м).

– 1000BASE-LX: оптичний сегмент для одномодового (SMF, до 5000 м) або багатомодового (до 550 м) кабелю з довжиною хвилі 1300 нм. Оптимальний для побудови вертикальних магістралей у великих будівлях.

– 1000BASE-CX: застаріла специфікація для екранованої крученої пари на надкороткі відстані (до 25 м), яка повністю витіснена мідними стандартами.

– 1000BASE-T (стандарт IEEE 802.3ab): найбільш масове та економічно ефективне рішення, що забезпечує передачу даних на швидкості 1 Гбіт/с через чотирипару неекрановану або екрановану кручену пару категорії 5e або 6 на відстань до 100 метрів. Передача реалізується дуплексно по кожній із чотирьох пар одночасно, що вимагає застосування складних методів кодування (PAM-5) та ехокомпенсації. Цей стандарт обрано як основний для побудови горизонтальної та вертикальної підсистем ЛОМ компанії [9, 10].

ВИСНОВКИ ДО РОЗДІЛУ 4

У четвертому розділі кваліфікаційної роботи було детально розроблено та верифіковано логічну структуру локальної обчислювальної мережі для Харківського офісу компанії «WorkDataNet».

Для наочного представлення та тестування архітектури мережі використано програмне середовище імітаційного моделювання Cisco Packet Tracer, у якому побудовано та перевірено віртуальну модель взаємодії всього спектра обладнання. У межах організації адресного простору приватних IP-адрес класу C (192.168.0.0/24) здійснено оптимальне безкласове розбиття мережі (CIDR) на три ізольовані підмережі з префіксом /28 (маска 255.255.255.240), що відповідає структурі поверхів будівлі та забезпечує кожну робочу групу з 10 хостів необхідним технологічним резервом адрес.

Наведено та обгрунтовано програмну конфігурацію активного обладнання Cisco/TP-Link. На центральному маршрутизаторі реалізовано технологію міжмережевого обміну Router-on-a-Stick за стандартом інкапсуляції IEEE 802.1Q та розгорнуто службу DHCP для автоматичного призначення мережевих параметрів. На комутаторах ядра (L3) та доступу (L2) виконано налаштування магістральних портів (Trunk) та користувацьких інтерфейсів (Access) із прив'язкою до відповідних поверхових VLAN. Техніко-економічний аналіз канальних технологій Fast Ethernet (IEEE 802.3u) та Gigabit Ethernet (IEEE 802.3ab) підтвердив правильність вибору стандарту 1000BASE-T на базі крученої пари категорії 6, що забезпечує гігабітні швидкості, відсутність колізій та високу продуктивність корпоративної мережі підприємства.

ВИСНОВКИ

У кваліфікаційній роботі на основі системного аналізу вихідних даних, сучасних технологічних стандартів та загальних принципів побудови телекомунікаційних систем було успішно розроблено проєкт локальної обчислювальної мережі (ЛОМ) для Харківського офісу міжнародної ІТ-компанії «WorkDataNet».

Під час виконання роботи здійснено комплексний аналіз поняття локальних комп'ютерних мереж, їхньої класифікації, архітектурних особливостей та базових топологій. На основі специфіки об'єкта проєктування (інтенсивний обмін даними, розробка ПЗ, Data Science) обгрунтовано доцільність впровадження клієнт-серверної архітектури та ієрархічної топології «зірка», що забезпечує максимальну відмовостійкість та мінімізує затримки трафіку.

Розроблено та розраховано чотирирівневу структуровану кабельну систему (СКС) для триповерхової адміністративної будівлі компанії, яка обслуговує 3 структурні підрозділи (по 10 робочих місць на кожному поверсі, загалом 30 вузлів). Розраховано параметри горизонтальної та вертикальної магістральних підсистем із використанням екранованого мідного кабелю FTP Cat. 6 у вогнестійкій оболонці LSZH, що повністю відповідає стандарту ISO/IEC 11801 та забезпечує капітальну надлишковість інфраструктури.

В роботі виконано техніко-економічне обгрунтування та специфікацію активного мережного обладнання бізнес-класу компанії TP-Link (лінійки Omada та JetStream), яке демонструє оптимальне співвідношення продуктивності, функціональності та капітальних витрат. Рівень доступу та магістральної агрегації реалізовано на базі керованих гігабітних комутаторів 2-го та 3-го рівнів (Layer

2/Layer 3) моделей OSI з підтримкою технології PoE+, а периметр мережі захищено високопродуктивним VPN-маршрутизатором із підтримкою стандарту Wi-Fi 6.

У середовищі імітаційного моделювання Cisco Packet Tracer розроблено та успішно протестовано логічну структуру мережі. Створено гнучкий адресний план на основі приватного простору IPv4 (192.168.0.0/24) із використанням безкласової маршрутизації (CIDR) та префікса /28. Це дозволило сегментувати мережу на ізольовані віртуальні підмережі (VLAN) для кожного поверху. Наведено лістинги програмного конфігурування інтерфейсів, маршрутизації Router-on-a-Stick та автоматичного розподілу адрес через службу DHCP.

Організовано комплексну систему захисту ЛОМ від поширених векторів атак (сніффінг, DoS, ARP/DHCP-спуфінг). Захист реалізовано шляхом активації апаратних функцій комутаторів (DHCP Snooping, Dynamic ARP Inspection), впровадження криптографічних протоколів різних рівнів (TLS, IPSec) та налаштування автентифікації повідомлень динамічної маршрутизації за алгоритмом MD5 (RFC-2082).

Розроблена ЛОМ повністю задовольняє сучасні технічні вимоги щодо швидкості, надійності та безпеки, є економічно ефективною, простою в адмініструванні та містить високий потенціал для подальшого масштабування у разі розширення штату підприємства «WorkDataNet». Накопичений під час проєктування та конфігурування пристроїв практичний досвід дозволяє ефективно вирішувати завдання з розгортання та модернізації сучасних корпоративних мереж.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров Є. В. Комп’ютерні мережі: підручник для студентів вищих навчальних закладів. – Львів : Магнолія-2006, 2021. – 416 с.

2. Оліфер В. Г. Комп'ютерні мережі. Принципи, технології, протоколи : навч. посібник. – К. : Юніор, 2011. – 944 с.

3. Павлов В. Г., Коваленко В.Г. Проєктування та монтаж структурованих кабельних систем (СКС) : навчальний посібник. – Харків : ХНУРЕ, 2019. – 188 с.

4. ISO/IEC 11801-1:2017. Information technology Generic cabling for customer premises – Part 1: General requirements. – Geneva: International Organization for Standardization, 2017. – 154 p.

5. Kurose J. F., Ross K. W. Computer Networking: A Top-Down Approach. – 8th ed. – Hoboken: Pearson, 2021. – 812 p.

6. Tanenbaum A. S., Wetherall D. J., Feamster N. Computer Networks. – 6th ed. – New York: Pearson, 2021. – 944 p.

7. Офіційний сайт компанії TP-Link в Україні [Електронний ресурс]: Каталог бізнес-обладнання (маршрутизатори Omada, комутатори JetStream). – Режим доступу: https://www.tp-link.com/uk-ua/business-networking/

8. Deering S., Hinden R. RFC 8200. Internet Protocol, Version 6 (IPv6) Specification. – Internet Engineering Task Force (IETF), 2017.

9. Malkin G. RFC 2453. RIP Version 2. – Internet Engineering Task Force (IETF), 1998.

10. Antunes M., Silva M. Computer Networks and Cybersecurity: Principles and Technologies. – Berlin: Springer, 2023. – 310 p.