Форма № Н-9.02

Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя»

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту корпоративної мережі логістичного підприємства "Global-Express" з використанням VPN-технологій для об'єднання філій**

Виконав: студент VII курсу, групи КІб-703

Спеціальності **123 Комп'ютерна інженерія**

(шифр і назва спеціальності)

_____ Максим ГРИЦИШИН

(ім'я та прізвище)

Керівник _____ Андрій ЮЗЬКІВ

(ім'я та прізвище)

Рецензент _____ _____

(ім'я та прізвище)

Тернопіль – 2026

ВІДОКРЕМЛЕНИЙ СТРУКТУРНИЙ ПІДРОЗДІЛ
«ТЕРНОПІЛЬСЬКИЙ ФАХОВИЙ КОЛЕДЖ
ТЕРНОПІЛЬСЬКОГО НАЦІОНАЛЬНОГО ТЕХНІЧНОГО УНІВЕРСИТЕТУ
імені ІВАНА ПУЛЮЯ»

Відділення **інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян**
Циклова комісія **комп'ютерної інженерії**
Освітньо-професійний ступінь **фаховий молодший бакалавр**
Освітньо-професійна програма: **Обслуговування комп'ютерних систем і мереж**
Спеціальність: **123 Комп'ютерна інженерія**
Галузь знань: **12 Інформаційні технології**

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"18" травня 2026 року

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

Грицишину Максиму Володимировичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту корпоративної мережі логістичного підприємства "Global-Express" з використанням VPN-технологій для об'єднання філій**

керівник роботи Юзьків Андрій Васильович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 18.05.2026р №4/9-252.

2. Строк подання студентом роботи: 22 червня 2026 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проєктування, стандарти ANSI/EIA/TIA 568 - "Commercial Building Telecommunications Wiring Standart" і ANSI/EIA/TIA 569 - "Commercial Building Standart for Telecommunications Pathwais and Spaces

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити): Загальний розділ. Розробка технічного та робочого проєкту. Спеціальний розділ. Економічний розділ. Охорона праці та безпека життєдіяльності.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- модель мережі
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Ірина ЛЕЩИК методист, викладач		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	18.05	
2	Збір і узагальнення інформації	21.05	
3	Написання першого розділу	25.05	
4	Розробка технічного та робочого проекту	1.06	
5	Написання спеціального розділу	8.06	
6	Розрахунок економічної частини	11.06	
7	Написання розділу охорони праці	12.06	
8	Виконання графічної частини	14.06	
9	Оформлення проекту	18.06	
10	Погодження нормоконтролю	19.06	
11	Попередній захист роботи	22.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 18 травня 2026 року

Студент _____ Максим ГРИЦИШИН
(підпис) (ім'я та прізвище)

Керівник роботи _____ Андрій ЮЗЬКІВ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Грицишин М.В. Розробка проєкту корпоративної мережі логістичного підприємства "Global-Express" з використанням VPN-технологій для об'єднання філій: кваліфікаційна робота на здобуття освітнього ступеня бакалавр за спеціальністю «123 – Комп'ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2026. 111 с.

У кваліфікаційній роботі розроблено проєкт сучасної мережевої інфраструктури для логістичного підприємства «Global-Express». Рішення базується на стандартах Gigabit Ethernet (IEEE 802.3ab), Wi-Fi 5 (IEEE 802.11ac) та віртуалізації каналів згідно з IEEE 802.1Q. Проведено детальне планування адресного простору та сегментацію мережі на віртуальні підмережі (VLAN) для оптимізації трафіку. Практична цінність роботи полягає у розробці комплексних інструкцій з налаштування серверної частини, організації захищених VPN-каналів між головним офісом та філіями, а також конфігурації шлюзів доступу до Інтернету. Створено моделі у Cisco Packet Tracer.

Ключові слова: комп'ютерна мережа, сервер, точка доступу, VPN, маршрутизатор, комутатор, віртуальна мережа, VLAN, Cisco Packet Tracert

ANNOTATION

Hrytsyshyn M.V. Development of a corporate network project for the logistics enterprise "Global-Express" using VPN technologies to connect branches: qualification work for obtaining a bachelor's degree in the specialty "123 - Computer Engineering". Ternopil: VSP "TFK TNTU", 2026. 111 p.

The qualification work developed a project of a modern network infrastructure for the logistics enterprise "Global-Express". The solution is based on the standards Gigabit Ethernet (IEEE 802.3ab), Wi-Fi 5 (IEEE 802.11ac) and channel virtualization according to IEEE 802.1Q. Detailed planning of the address space and network segmentation into virtual subnetworks (VLAN) were carried out to optimize traffic. The practical value of the work lies in the development of comprehensive instructions for configuring the server side, organizing secure VPN channels between the head office and branches, as well as configuring Internet access gateways. Models were created in Cisco Packet Tracer.

Keywords: computer network, server, access point, VPN, router, switch, virtual network, VLAN, Cisco Packet Tracert

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DNS (Domain Name System) – сервер доменних імен.

ERP (Enterprise Resource Planning) – програмне забезпечення для комплексного управління бізнес-процесами

IDS (Intrusion Detection System) – пасивна система моніторингу мережі, що аналізує трафік і сповіщає про загрози

IEEE 802.3ab – стандарт Gigabit Ethernet на витій парі UTP 5e, 6.

IEEE 802.3z – стандарт Gigabit Ethernet на оптоволоконному кабелі.

IEEE 802.3ac – стандарт, що пребачає збільшення максимального розміру фрейму до 1522 байт.

IP (Internet Protocol) – Інтернет-протокол.

IPS (Intrusion Prevention System) – активна система моніторингу мережі, що аналізує трафік і сповіщає про загрози.

IPSec (Internet Protocol Security) – це набір протоколів, які забезпечують безпеку даних, що передаються по IP-мережах.

LAN (Local Area Network) – локальна мережа.

NAT (Network Address Translation) –технологія в мережах TCP/IP, яка дозволяє маршрутизатору змінювати IP-адреси в заголовках пакетів

OU (Organization Unit) – організаційна одиниця групових політик безпеки.

TCP/IP (Transmission Control Protocol/Internet Protocol) – протокол управління передачею/Інтернет протокол

SQL (Structured Query Language) – декларативна мова програмування, що використовується для створення, модифікації, керування та отримання даних у реляційних базах даних.

VPN (Virtual Private Network) – узагальнена назва клієнт-серверних технологій, які дають змогу створювати віртуальні захищені мережі поверх інших мереж із нижчим рівнем довіри

ОС – операційна система.

ВСТУП

Розвиток транспортно-логістичної галузі в Україні вимагає від підприємств впровадження високоефективних цифрових рішень для координації вантажопотоків. Для тернопільського підрозділу компанії «Global-Express», що спеціалізується на міжнародних та внутрішніх перевезеннях, стабільність мережевої інфраструктури є стратегічним пріоритетом. Оскільки компанія має офіс у м. Тернопіль та мережу регіональних складів, виникає гостра потреба у створенні захищеного корпоративного середовища для оперативного доступу до бази даних товарів, обліку вантажів та митної документації.

Специфіка роботи логістичного терміналу в Тернополі полягає у великій інтенсивності обміну даними між офісними працівниками та складськими підрозділами. Використання технології Site-to-Site VPN (IPsec) дозволяє об’єднати ці територіально розподілені об’єкти в єдину логічну мережу через публічні канали Internet, забезпечуючи при цьому конфіденційність трафіку на рівні банківських стандартів. Впровадження динамічної маршрутизації OSPF та резервних каналів зв’язку гарантує безперебійну роботу системи навіть у разі відмови основного провайдера, що є критичним для запобігання простоям у логістичних ланцюгах.

Мета роботи – проєктування та реалізація відмовостійкої корпоративної мережі для тернопільського підрозділу компанії «Global-Express», яка забезпечує безпечне об’єднання центрального офісу з регіональними складами та гарантує безперервний доступ до корпоративних сервісів.

Наукова новизна та практичне значення полягає у створенні комплексної моделі мережі для логістичного оператора м. Тернопіль, яка інтегрує механізми автоматичного перемикання на резервні канали та багаторівневу систему шифрування даних. Розроблені інструкції з конфігурації обладнання можуть бути безпосередньо впроваджені в роботу «Global-Express» для підвищення ефективності управління вантажними перевезеннями.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

У даній кваліфікаційній роботі необхідно розробити захищену корпоративну мережу Тернопільського регіонального підрозділу логістичного оператора «Global-Express». Основним об’єктом розробки є комплексна інформаційно-телекомунікаційна система, що забезпечує автоматизацію основних бізнес-процесів підприємства в межах Тернопільської області та координацію взаємодії з віддаленими складськими терміналами.

Область застосування результатів даного проєкту охоплює внутрішню інфраструктуру логістичного хабу в м. Тернопіль, який виступає центральною точкою збору та обробки інформації. Проєктна документація регламентує створення єдиного цифрового контуру, що об’єднує адміністративний офіс, де функціонує 30 персональних комп'ютерів, із трьома географічно розподіленими підрозділами, кожен з яких обслуговує від 10 до 15 робочих місць. Окрім стандартних робочих станцій, область застосування розширюється на мобільні сегменти мережі, зокрема термінали збору даних, що працюють у складських зонах і потребують безперебійного доступу до центральної бази даних.

Технічні рішення, описані в роботі, спрямовані на вирішення прикладних завдань логістичної галузі, таких як моніторинг перевезень у реальному часі, управління залишками товарів на складах та митне супроводження вантажів. Оскільки «Global-Express» оперує конфіденційною інформацією про клієнтів та маршрути, розроблена система знаходить своє застосування у сфері кібербезпеки підприємства, впроваджуючи механізми захисту трафіку через публічні канали зв'язку.

Застосування проєкту дозволяє перевести тернопільський підрозділ на якісно новий рівень інформаційної взаємодії, де кожен віддалений склад стає

повноцінною частиною внутрішньої мережі (LAN). Це досягається завдяки використанню технології Site-to-Site VPN, що нівелює географічні бар'єри між офісом у центрі міста та складськими об'єктами, розташованими на периферії. Таким чином, розроблена мережа є фундаментом для подальшого впровадження систем електронного документообігу та автоматизованих систем управління логістикою, забезпечуючи необхідну пропускну здатність та відмовостійкість для безперервного циклу вантажоперевезень.

1.1.2 Призначення розробки

Головне призначення даної розробки полягає у створенні цілісного, захищеного та високопродуктивного інформаційного середовища для тернопільського регіонального підрозділу логістичної компанії «Global-Express». Проєктована мережа виступає технологічним фундаментом для повної автоматизації операційного циклу підприємства, що включає реєстрацію вантажів, контроль за їх переміщенням у реальному часі та оперативну синхронізацію складських залишків. Система призначена для забезпечення безперебійного доступу адміністративного персоналу центрального офісу та операторів віддалених складів до єдиної корпоративної бази даних товарів, що дозволяє уникнути дублювання інформації та мінімізувати помилки при оформленні транспортних накладних.

Важливою функціональною складовою розробки є реалізація механізмів безпеки, спрямованих на захист комерційної таємниці та персональних даних клієнтів компанії. Оскільки обмін інформацією між тернопільським офісом та трьома регіональними складами відбувається через публічні канали мережі Інтернет, проєкт призначений для створення зашифрованих віртуальних тунелів на основі стеку протоколів IPsec. Це дозволяє нівелювати загрози несанкціонованого перехоплення трафіку або кібератак на мережевий периметр, перетворюючи географічно розрізнені локальні мережі (LAN) у єдиний безпечний віртуальний простір із централізованою політикою доступу.

Окрім безпекового аспекту, розробка має на меті забезпечення високого рівня відмовостійкості мережевої інфраструктури. Впровадження протоколу динамічної маршрутизації призначене для автоматичного керування потоками даних та миттєвої адаптації мережі до змін у топології. У разі виникнення технічних несправностей на лініях основного провайдера, система повинна автоматично перенаправляти критично важливий логістичний трафік на резервні канали зв'язку. Це гарантує безперервність роботи терміналів збору даних та систем електронного документообігу, що є важливим для дотримання жорстких графіків доставки вантажів у межах Тернопільської області та за її межами.

Додатковим призначенням розробки є оптимізація внутрішнього мережевого трафіку шляхом впровадження технології віртуальних локальних мереж (VLAN). Це дозволяє логічно розділити потоки даних між різними відділами підприємства – адміністрацією, бухгалтерією та складськими службами, що підвищує загальну продуктивність мережі та спрощує процес адміністрування. Таким чином, проєкт є комплексним інструментом, призначеним для трансформації IT-інфраструктури «Global-Express» у сучасну масштабовану систему, здатну підтримувати зростаючі обсяги вантажоперевезень та забезпечувати високу якість логістичного сервісу в західному регіоні України.

1.1.3 Вимоги до апаратного і програмного забезпечення

Формування вимог до технічного та програмного базису мережі логістичного підприємства «Global-Express» ґрунтується на необхідності створення відмовостійкої архітектури, здатної підтримувати інтенсивний обмін даними між тернопільським офісом та регіональними складами. Апаратне забезпечення центрального вузла повинно відповідати високим стандартам продуктивності, оскільки саме тут зосереджується основне навантаження з обробки VPN-трафіку та маршрутизації потоків даних від 30 робочих станцій. Ключовою вимогою до центрального маршрутизатора є наявність апаратної підтримки шифрування за стандартом AES, що необхідно для стабільної роботи IPsec-тунелів без деградації

швидкості з’єднання. Комутаційне обладнання офісу має підтримувати технологію віртуальних локальних мереж (VLAN) та мати достатню кількість портів Gigabit Ethernet для забезпечення внутрішньої швидкості обміну даними на рівні 1 Гбіт/с.

Для складських підрозділів вимоги до апаратного забезпечення зміщуються в бік надійності та підтримки бездротових технологій. Оскільки робота на складах передбачає використання терміналів збору даних, мережеве обладнання філій повинно включати точки доступу з підтримкою стандарту IEEE 802.11ac (Wi-Fi 5) для стабільного покриття всієї площі приміщень. Маршрутизатори на складах мають бути сумісними з протоколом OSPF для коректної роботи в загальній системі динамічної маршрутизації. Клієнтські робочі станції (персональні комп'ютери та ноутбуки) повинні мати апаратні характеристики, достатні для комфортної роботи з сучасним логістичним ПЗ та CRM-системами, включаючи об’єм оперативної пам'яті не менше 8 ГБ та швидкісні SSD-накопичувачі.

Вимоги до програмного забезпечення охоплюють як системний, так і прикладний рівень функціонування мережі. На серверному обладнанні в Тернополі передбачається розгортання операційної системи сімейства Windows Server (рекомендується версія 2025 для забезпечення максимальної безпеки та підтримки нових протоколів), яка виконуватиме ролі доменного контролера (AD DS), DNS та DHCP серверів. Програмне забезпечення мережевих пристроїв повинно мати актуальні оновлення безпеки та підтримувати розширені функції моніторингу трафіку (наприклад, за протоколом SNMP або NetFlow). Для захисту кінцевих точок мережі обов’язковим є використання ліцензійного антивірусного ПЗ із централізованим управлінням, а для забезпечення віддаленого доступу адміністраторів – захищених протоколів SSH та HTTPS. Таке поєднання апаратних та програмних засобів дозволить створити надійну IT-екосистему, адаптовану до специфічних потреб логістичного оператора «Global-Express».

1.1.4 Вимоги до документації

Процес розробки та впровадження корпоративної мережі для логістичного підприємства «Global-Express» має супроводжуватися формуванням повного пакету технічної документації, що відповідає державним стандартам та внутрішнім корпоративним регламентам. Основна вимога до документального супроводу полягає у забезпеченні прозорості архітектури мережі для IT-персоналу, що дозволить мінімізувати час на діагностику несправностей та полегшить подальше масштабування системи. До складу звітної документації обов'язково повинні входити детальні схеми фізичної та логічної топології мережі, де відображено розташування всіх комутаційних вузлів у тернопільському офісі та на регіональних складах, а також шляхи проходження основних та резервних каналів зв'язку.

Окремий блок вимог стосується документування мережевих параметрів та конфігурацій активного обладнання. Для кожного маршрутизатора та комутатора має бути створений технічний паспорт, що містить актуальні версії вбудованого програмного забезпечення, таблиці призначення інтерфейсів та архівні копії конфігураційних файлів. Важливою частиною документації є регламент адресації, у якому чітко зафіксовано розподіл IP-адрес у межах створених віртуальних підмереж (VLAN) для адміністративного персоналу, логістів та складських працівників. Це дозволить уникнути конфліктів адрес при підключенні нового обладнання та забезпечить коректну роботу політик доступу в межах VPN-тунелів IPsec.

Додатково технічна документація повинна включати інструкції з експлуатації та плани дій у аварійних ситуаціях. Зокрема, мають бути розроблені покрокові керівництва для системних адміністраторів щодо відновлення зв'язку між тернопільським хабом та філіями у разі критичного збою, а також методики перевірки цілісності зашифрованих з'єднань. Для кінцевих користувачів підприємства передбачається створення коротких пам'яток щодо правил безпечної роботи у корпоративній мережі та використання ресурсів віддаленого доступу. Завершальним етапом документування є підготовка акту виконаних

робіт та протоколів успішного тестування мережі в середовищі моделювання, що підтверджують відповідність розробленої інфраструктури вимогам замовника.

1.1.5 Техніко-економічні показники

Впровадження проєкту модернізації корпоративної мережі для тернопільського підрозділу «Global-Express» обґрунтовується низкою техніко-економічних показників, що свідчать про високу ефективність капіталовкладень. Основним економічним показником є значне зниження операційних витрат на оренду виділених ліній зв'язку між офісом у м. Тернопіль та регіональними складами. Завдяки використанню технології Site-to-Site VPN поверх публічних каналів мережі Інтернет, підприємство отримує захищений канал передачі даних, вартість експлуатації якого є в кілька разів нижчою за вартість оренди приватних каналів L2-рівня, при цьому рівень безпеки завдяки шифруванню IPsec залишається максимально високим [1].

Технічна ефективність розробки виражається у зростанні продуктивності праці персоналу логістичного вузла. Мінімізація затримок при доступі до центральної бази даних товарів та автоматизація обміну інформацією між складами дозволяють скоротити час на обробку однієї вантажної одиниці. Показник надійності системи, що забезпечується протоколом динамічної маршрутизації OSPF та резервуванням каналів зв'язку, дозволяє уникнути фінансових втрат, пов'язаних із простоями складських терміналів. Розрахунковий час окупності проєкту базується на зменшенні кількості помилок ручного введення даних та виключенні ризиків, пов'язаних із втратою критично важливої комерційної інформації внаслідок кібератак.

Додатковим економічним чинником є висока масштабованість запропонованого рішення. Архітектура мережі спроектована таким чином, що підключення нових логістичних точок у Тернопільській області потребує лише мінімальних витрат на придбання кінцевого обладнання, не вимагаючи докорінної зміни структури центрального ядра мережі. Використання сучасного енергое-

фективного обладнання та хмарних технологій адміністрування дозволяє зменшити витрати на енергоспоживання та підтримку штату системних адміністраторів. Таким чином, сукупність техніко-економічних переваг підтверджує доцільність впровадження даного проєкту як засобу підвищення конкурентоспроможності компанії «Global-Express» на ринку логістичних послуг західного регіону України.

1.1.6 Стадії та етапи розробки

Процес створення та впровадження комплексної мережевої інфраструктури для тернопільського підрозділу компанії «Global-Express» базується на суворому дотриманні послідовних етапів проектування, що гарантує цілісність системи та її відповідність бізнес-вимогам логістичного оператора. Початкова стадія розробки зосереджена на глибокому передпроєктному аналізі, який включає детальне технічне обстеження об’єктів у м. Тернопіль та трьох регіональних складських терміналів. На цьому етапі проводиться аудит існуючих кабельних систем, оцінка електроживлення серверних вузлів та аналіз спектру радіочастот для розгортання бездротового сегменту Wi-Fi на складах. Важливим аспектом цієї стадії є збір даних про обсяги трафіку, який генерують 30 робочих станцій офісу та мобільні термінали збору даних, що дозволяє сформувати чітке технічне завдання з врахуванням масштабування компанії [2].

Друга стадія розробки присвячена етапу логічного та фізичного проектування IT-інфраструктури. Тут виконується побудова ієрархічної моделі мережі (рівні ядра, розподілу та доступу), розробляється детальна схема IP-адресації для всього тернопільського підрозділу та визначаються межі віртуальних локальних мереж (VLAN). На цьому ж етапі здійснюється проектування архітектури динамічної маршрутизації на базі протоколу OSPF, що забезпечує швидку збіжність мережі при зміні топології. Особлива увага приділяється проектуванню захищеного периметра: розраховуються параметри криптографічного захисту для Site-to-Site VPN (IPsec) тунелів, обираються

алгоритми шифрування та хешування, а також розробляються правила міжмережевого екранування для шлюзів доступу до мережі Інтернет.

Наступна стадія – це етап віртуального моделювання та верифікації проектних рішень. Перед закупівлею дороговартісного обладнання Cisco, розроблена топологія відтворюється у середовищі імітаційного моделювання Cisco Packet Tracer. Це дозволяє протестувати працездатність складних конфігурацій, перевірити коректність роботи протоколу OSPF між офісом та філіями, а також симулювати критичні сценарії відмови основних ліній зв'язку. Етап моделювання є критично важливим, оскільки він дозволяє виявити та усунути потенційні помилки в логіці маршрутизації або політиках безпеки ще до початку фізичного монтажу обладнання в Тернополі.

Завершальна стадія розробки включає безпосередню реалізацію проєкту, що складається з етапів монтажу, налаштування та пусконалагоджувальних робіт. Після інсталяції активного обладнання проводиться конфігурування маршрутизаторів та комутаторів згідно з проектними специфікаціями. Окремим підпунктом виділяється етап інтеграції серверного програмного забезпечення (Windows Server) та налагодження централізованих служб ідентифікації.

Після завершення технічних робіт починається етап дослідної експлуатації, під час якого здійснюється моніторинг стабільності VPN-з'єднань під навантаженням та проводиться інструктаж персоналу щодо правил безпечної роботи в оновленій мережі. Весь життєвий цикл розробки закінчується стадією підготовки виконавчої документації та передачею системи у промислову експлуатацію, що забезпечує «Global-Express» надійною платформою для розвитку логістичних сервісів у західному регіоні.

1.1.7 Порядок контролю та прийому

Процедура контролю якості та офіційного прийому розробленої мережевої інфраструктури тернопільського підрозділу «Global-Express» є багатоетапним процесом, спрямованим на підтвердження повної відповідності системи технічному завданню та стандартам безпеки. Контроль починається ще на етапі

моделювання, де проводиться первинна верифікація логіки маршрутизації та конфігурацій VPN-тунелів у середовищі Cisco Packet Tracer. На цій стадії розробник демонструє здатність мережі до самовідновлення при імітації розриву основних каналів зв'язку та стабільність роботи протоколу OSPF, що фіксується у відповідних звітах тестування.

Основним етапом є проведення комплексних випробувань на реальному обладнанні, встановленому в тернопільському офісі та на регіональних складах. Порядок контролю передбачає перевірку пропускної здатності каналів зв'язку між філіями, де ключовим показником є відсутність деградації швидкості при повному завантаженні IPsec-шифрування. Приймання системи включає обов'язковий етап аудиту безпеки, під час якого проводиться сканування вразливостей вузлів та тестування політик доступу віртуальних підмереж (VLAN). Замовник здійснює контроль за коректністю розподілу адресного простору та перевіряє доступність центральної бази даних з кожного робочого місця на віддалених складах.

Завершальна фаза прийому розробки полягає у проведенні дослідної експлуатації протягом встановленого терміну (зазвичай від 72 годин до одного робочого тижня). У цей період ведеться моніторинг стабільності роботи VPN-шлюзів та терміналів збору даних в умовах реального логістичного навантаження. Процес прийому завершується підписанням акту впровадження, що можливе лише за умови надання повного пакету виконавчої документації, включаючи актуальні конфігураційні файли, схеми топології та інструкції для системних адміністраторів. Тільки після успішного проходження всіх контрольних точок та підтвердження цілісності зашифрованих каналів зв'язку, мережа вважається офіційно прийнятою в промислову експлуатацію тернопільським підрозділом «Global-Express».

1.2 Аналіз інформаційних потреб та структури підприємства

Для якісного проектування корпоративної мережі необхідно проаналізувати організаційно-штатну структуру тернопільського регіонального підрозділу логістичної компанії «Global-Express» та визначити специфічні інформаційні

потреби кожного з її відділів. Загальна інфраструктура підприємства розділена на дві основні логічні та фізичні зони: центральний офіс управління (м. Тернопіль) та три територіально віддалені складські термінали.

Основна діяльність тернопільського підрозділу «Global-Express» зосереджена на наданні повного спектру логістичних послуг, що включають приймання, консолідацію, тимчасове зберігання та магістральне перевезення вантажів. Організаційна структура побудована таким чином, щоб забезпечити безперебійний цикл обробки посилок у режимі 24/7. Центральний офіс виконує функцію координаційного центру, де зосереджено стратегічне управління та фінансовий контроль. Тут працюють логісти-диспетчери, які в реальному часі керують рухом власного та найманого автотранспорту, формуючи оптимальні маршрути для мінімізації витрат пального та дотримання термінів доставки. Бухгалтерський підрозділ забезпечує супровід усіх транзакцій, працюючи з великими обсягами електронних документів та банківськими системами, що вимагає високої стабільності мережевих каналів для уникнення затримок у розрахунках з контрагентами.

Виробничий процес на складських терміналах починається з моменту прибуття транспортного засобу на рампу. Кожна одиниця вантажу проходить обов'язкову процедуру сканування, під час якої дані про габарити, вагу та кінцевий пункт призначення миттєво передаються до центральної бази даних. На головному сортувальному хабі, що розташований на об'їзній дорозі Тернополя, відбувається розподіл потоків: частина вантажів спрямовується на палетне зберігання, а інша – на лінію крос-докінгу для негайного перевантаження в автомобілі, що прямують до інших регіонів України. Оскільки компанія спеціалізується на швидкій доставці, швидкість обміну інформацією між сканером комірника та сервером в офісі є важливим показником. Будь-яка мережева затримка призводить до простою техніки та персоналу, що безпосередньо впливає на пропускну здатність усього терміналу.

Важливою складовою діяльності є забезпечення високого рівня сервісу для клієнтів. Це досягається шляхом інтеграції складських процесів із системою

онлайн-трекінгу. Кожна зміна статусу посилки на складі – від «прийнято» до «відправлено» – має негайно відображатися в особистому кабінеті замовника. Це створює додаткове навантаження на інформаційну інфраструктуру, оскільки мережа повинна підтримувати тисячі одночасних запитів до бази даних без втрати продуктивності. Крім того, діяльність підприємства передбачає постійну взаємодію з кур'єрами, які використовують мобільні додатки для звітності. Таким чином, «Global-Express» функціонує як єдиний цифровий організм, де фізичне переміщення вантажів повністю синхронізоване з потоками даних у корпоративній мережі.

Центральний офіс, розташований на вулиці Бродівській, є головним інформаційним вузлом, де розміщено серверне обладнання та консолідовано процеси управління компанією. Робочі місця (30 ПК) розподілені між наступними структурними підрозділами:

- відділ транспортної логістики та диспетчеризації включає 12 ПК. Найбільший і найбільш навантажений підрозділ. Працівники цього відділу відповідають за побудову маршрутів, моніторинг руху транспорту через GPS-трекери та координацію роботи водіїв. Основними інформаційними потребами є безперервний доступ до корпоративної системи управління транспортом (TMS), картографічних сервісів та баз даних складських залишків. Трафік цього відділу потребує високої пропускної здатності та пріоритезації (QoS), оскільки затримки в оновленні даних можуть призвести до логістичних збоїв;

- бухгалтерія та фінансовий відділ включає 4 ПК. Цей підрозділ відповідає за фінансовий облік, нарахування заробітної плати, оплату рахунків та взаємодію з податковими органами. Основною інформаційною потребою є максимальний рівень мережевої безпеки. Робочі станції бухгалтерії повинні бути ізольовані від загального інтернет-трафіку підприємства за допомогою технології VLAN. Критично важливим є захищений доступ до систем «Клієнт-Банк» та внутрішнього ERP-сервера;

- відділ по роботі з клієнтами та продажу послуг. В цьому підрозділі розташовано 7 ПК. Відділ по роботі з клієнтами та продажу послуг здійснює

прийом заявок, консультування клієнтів та оформлення договорів. Інформаційні потреби: Стабільний доступ до CRM-системи, IP-телефонії (VoIP) та електронної пошти. Цей відділ генерує значний обсяг зовнішнього інтернет-трафіку, який повинен фільтруватися на корпоративному шлюзі безпеки;

- адміністративно-управлінський персонал – це директор філії (1 ПК), секретар (1 ПК), інженер з охорони праці (1 ПК), юрист (1 ПК) та HR-менеджер (1 ПК). Разом 5 комп'ютерів. Основною інформаційною потребою є консолідований доступ до звітів усіх підрозділів, систем електронного документообігу та інструментів відеоконференцзв'язку для нарад із головним офісом компанії;

- IT-відділ (2 ПК) – системні адміністратори, що забезпечують працездатність інфраструктури. Основні інформаційні потреби включають повний, але суворо регламентований доступ до управління мережевим обладнанням (маршрутизатори, комутатори), серверами та системами моніторингу трафіку.

Крім головного офісу підприємство включає три регіональних складських термінали (3 об'єкти, 37 пристроїв загалом). Складські комплекси відповідають за фізичну обробку вантажів: приймання, сортування, пакування (фулфілмент) та відвантаження. Інформаційна інфраструктура складів суттєво відрізняється від офісної і базується переважно на бездротових технологіях.

- склад №1 "Вантажний термінал" (розташовано 15 пристроїв) Орієнтований на обробку великогабаритних вантажів. Включає 5 стаціонарних ПК для операторів складу (оформлення накладних) та 10 мобільних терміналів збору даних, підключених через мережу Wi-Fi;

- склад №2 "Фулфілмент та електронна комерція" (12 пристроїв). Він орієнтований на дрібні відправлення. Включає 5 стаціонарні ПК для друку етикеток та 7 мобільних сканерів штрих-кодів;

- склад №3 "Крос-докінг" (розташовано 10 пристроїв). На цьому складі виконується швидке перевантаження без тривалого зберігання. Обслуговується 3 стаціонарними ПК, 7 терміналів збору даних та 4 IP-камери відеонагляду. Для під'єднання безпровідних пристроїв слід використати 4 точки доступу.

Аналіз бізнес-процесів «Global-Express» виявляє ключову проблему: склади не можуть функціонувати автономно. Усі термінали збору даних та ПК операторів на складах повинні в режимі реального часу взаємодіяти з центральною системою управління складом та базою даних, що фізично розміщені на серверах у тернопільському офісі.

Це формує такі жорсткі вимоги до проєктованої мережі:

- конфіденційність транзакцій. Оскільки обмін даними між офісом і трьома складами відбувається через географічно розподілену інфраструктуру (мережу Інтернет), комерційна інформація про вантажі та клієнтів є вразливою до перехоплення. Це зумовлює необхідність використання Site-to-Site VPN з шифруванням трафіку за протоколом IPsec;

- безперервність процесів (Відмовостійкість). Відключення зв'язку між складом та офісом навіть на 10 хвилин призводить до повної зупинки відвантажень, черг вантажівок та фінансових втрат. Відповідно, мережа вимагає впровадження резервних каналів зв'язку та протоколу динамічної маршрутизації OSPF для миттєвого та автоматичного перемикання трафіку у разі аварії на лінії основного провайдера;

- ізоляція трафіку. Для забезпечення безпеки та зменшення широкомовного навантаження, інформаційні потоки різних відділів (наприклад, бухгалтерії та складських сканерів) повинні бути логічно розділені на рівні комутаторів за допомогою VLAN.

Деталізуємо основні інформаційні потоки на підприємстві.

Перший ключовий інформаційний потік виникає в центральному офісі, коли клієнт здійснює замовлення. У цей момент дані вносяться в CRM-систему, створюючи нову електронну накладну. Ця інформація миттєво стає доступною для відділу логістики, який через внутрішню мережу передає дані на сервер бази даних.

Щойно вантаж прибуває на один із трьох складів, починається другий етап – фізичний облік. Працівник складу використовує термінал збору даних, який через бездротову мережу Wi-Fi та захищений тунель Site-to-Site VPN звертається

до сервера в офісі. Система має в реальному часі підтвердити отримання вантажу, змінити його статус та автоматично сформувати чергу на відвантаження або сортування. Будь-яка затримка на цьому етапі через нестабільність VPN-з’єднання призводить до накопичення транспорту на території складу та затримок у клієнтському сервісі.

Наступний важливий сегмент інформаційних потоків пов’язаний із внутрішньою координацією та безпекою. Крім обліку товарів, через корпоративну мережу постійно проходить управлінський трафік. Це включає обмін фінансовою документацією між бухгалтерією в Тернополі та складськими терміналами для друку актів та супровідних листів.

Окрему частку трафіку займає потік відеоданих із систем спостереження, що передається зі складів до центрального офісу для моніторингу збереження вантажів. Оскільки відеопотік є дуже об'ємним, він не повинен перекривати пріоритетні запити від терміналів збору даних. Саме тому в проекті важливо передбачити механізми, які б розпізнавали різні типи даних і забезпечували "зелений коридор" для критично важливих логістичних операцій, тоді як менш термінові дані можуть передаватися з меншим пріоритетом

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Аналіз та обґрунтування вибору топології та технології мережі

Для вибору архітектури мережі «Global-Express» необхідно провести порівняльний аналіз класичних топологій, оцінюючи їхню придатність для сучасного логістичного середовища, де надійність та швидкість передачі даних є визначальними факторами.

Вибір топології корпоративної мережі для логістичного підприємства «Global-Express» обумовлений територіальною розрізненістю його підрозділів та важливістю безперервного зв'язку між ними. На макрорівні (між об'єктами) обрано топологію «зірка» (Star), де центральним вузлом виступає офіс у м. Тернопіль, а променями – три віддалені склади. Така структура дозволяє централізовано керувати безпекою та ресурсами, оскільки всі основні сервери та бази даних зосереджені в одному місці, а філії отримують доступ до них через зашифровані VPN-тунелі. Це значно спрощує адміністрування та дозволяє впроваджувати єдині політики безпеки для всього підприємства одночасно.

Топологія «шина» передбачає використання спільного каналу передачі даних для всіх вузлів мережі. Незважаючи на мінімальні витрати на кабельну інфраструктуру, вона є абсолютно неприйнятною для сучасного підприємства через низьку відмовостійкість: обрив центрального кабелю призводить до зупинки всієї мережі, а пошук несправностей у такій структурі є надзвичайно складним [2].

Топологія «кільце» забезпечує послідовну передачу сигналу між пристроями, де кожен вузол працює як ретранслятор. Хоча вона краще впорядковує трафік, вихід із ладу одного комп'ютера або мережевої карти розриває коло зв'язку, що створює великі ризики для складських операцій, де обладнання працює в умовах підвищеного пилу та вологості.

Топологія «зірка» є значним кроком вперед, оскільки передбачає підключення кожного робочого місця до центрального комутатора. Це значно підвищує

надійність системи: пошкодження кабелю до одного ПК логіста ніяк не впливає на роботу бухгалтерії чи складу. Проте для великої компанії з територіально розрізненими об’єктами, як у «Global-Express», класична «зірка» стає занадто громіздкою та дорогою в обслуговуванні, оскільки вимагає прокладання величезної кількості кабелів до єдиного центрального вузла, що технічно неможливо реалізувати між різними районами Тернополя.

Більш надійна «повнозв’язна» топологія, де кожен вузол з’єднаний з усіма іншими, забезпечує найвищий рівень живучості, але її вартість та складність налаштування є економічно недоцільними для логістичного бізнесу середнього масштабу.

У результаті аналізу для реалізації проекту було обрано ієрархічну модель мережі, яка є вдосконаленим варіантом розширеної зірки. Даний вибір обґрунтовується необхідністю чіткого структурування інформаційних потоків та забезпечення високої пропускної здатності. Ця модель розділяє мережу на три логічні рівні: рівень ядра (Core Layer), рівень розподілу (Distribution Layer) та рівень доступу (Access Layer) (див. рис. 1.1).

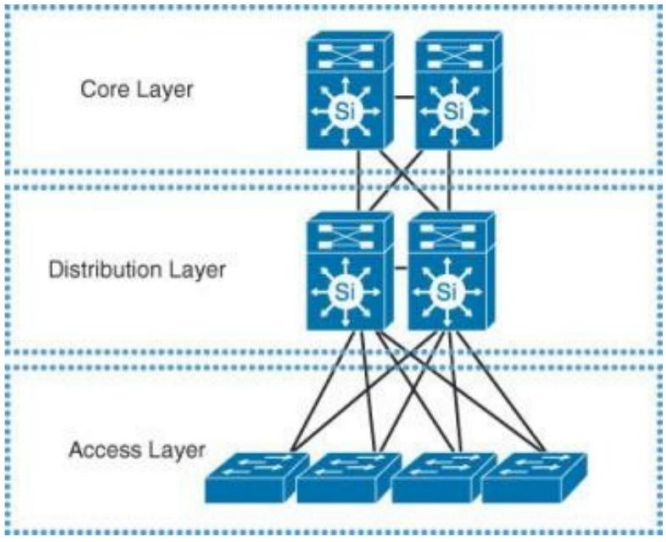


Рисунок 1.1 – Трирівнева модель корпоративної мережі

Рівень ядра забезпечує максимально швидку комутацію трафіку всередині будівлі. Рівень розподілу відповідає за агрегацію каналів та впровадження політик

безпеки через віртуальні підмережі (VLAN). Рівень доступу безпосередньо з'єднує кінцеві пристрої – робочі станції логістів, бухгалтерів, принтери та точки доступу для складських терміналів збору даних. Такий підхід гарантує, що вихід із ладу одного комутатора на поверсі або в окремому цеху не призведе до зупинки всієї мережі підприємства.

Окрему увагу при виборі топології приділено фактору відмовостійкості. Оскільки стандартна «зірка» має вразливість – залежність від центрального вузла та каналів зв'язку – проект передбачає впровадження елементів топології «часткова комірка» (Partial Mesh) на логічному рівні. Завдяки протоколу динамічної маршрутизації OSPF, мережа здатна автоматично перенаправляти потоки даних у разі обриву основного каналу. Якщо зв'язок між офісом та головним складом на об'їзній дорозі пошкоджується, система миттєво активує резервний канал (наприклад, через 4G/LTE шлюз або альтернативного провайдера), зберігаючи цілісність логічної структури та забезпечуючи безперервність бізнес-процесів.

Таким чином, комбінація ієрархічної побудови локальних мереж та зіркоподібної структури глобальної мережі із впровадженням динамічного резервування є найбільш раціональним рішенням для «Global-Express». Це забезпечує оптимальний баланс між вартістю обладнання, простотою обслуговування та високою надійністю, яка необхідна для оперативного обліку вантажів і фінансової звітності. Обрана топологія створює масштабовану платформу, яка дозволяє в майбутньому легко інтегрувати нові складські приміщення або офісні відділи без необхідності докорінної зміни архітектури всієї системи.

Зважаючи на масштаби підприємства та відносно невелику кількість кінцевих вузлів у кожному сегменті, у межах даного проєкту реалізовано модифіковану ієрархічну модель мережі. Для оптимізації апаратних ресурсів та спрощення адміністрування було прийнято рішення про логічне об'єднання рівнів ядра (Core) та розподілу (Distribution).

Функції цих двох рівнів покладено на високопродуктивні маршрутизатори з інтегрованими сервісами безпеки. Такий підхід дозволяє централізувати керування трафіком та забезпечити наступні функції в межах одного пристрою:

- міжсегментна маршрутизація (Inter-VLAN routing) – обробка потоків даних між відділами (офіс, склад, бухгалтерія) на швидкостях локальної мережі;

- організація захищеного WAN-периметра – побудова шифрованих Site-to-Site VPN-тунелів на базі протоколу IPsec між центральним офісом у Тернополі та віддаленими складськими терміналами;

- динамічне керування маршрутами – використання протоколу OSPF для автоматичного перемикання між основним та резервним каналами зв'язку.

Використання маршрутизаторів як комбінованих вузлів ядра та розподілу є економічно ефективним рішенням для «Global-Express», оскільки воно зменшує кількість активних одиниць обладнання, знижує енергоспоживання та спрощує діагностику мережі. При цьому потужності обраного обладнання (Cisco ISR) цілком достатньо для забезпечення гігабітної швидкості комутації та надійного шифрування VPN-трафіку в реальному часі. це рішення робить мережу простішою в обслуговуванні, але при цьому зберігається можливість майбутнього масштабування. Логічна топологія мережі представлена на рисунку 2.1.

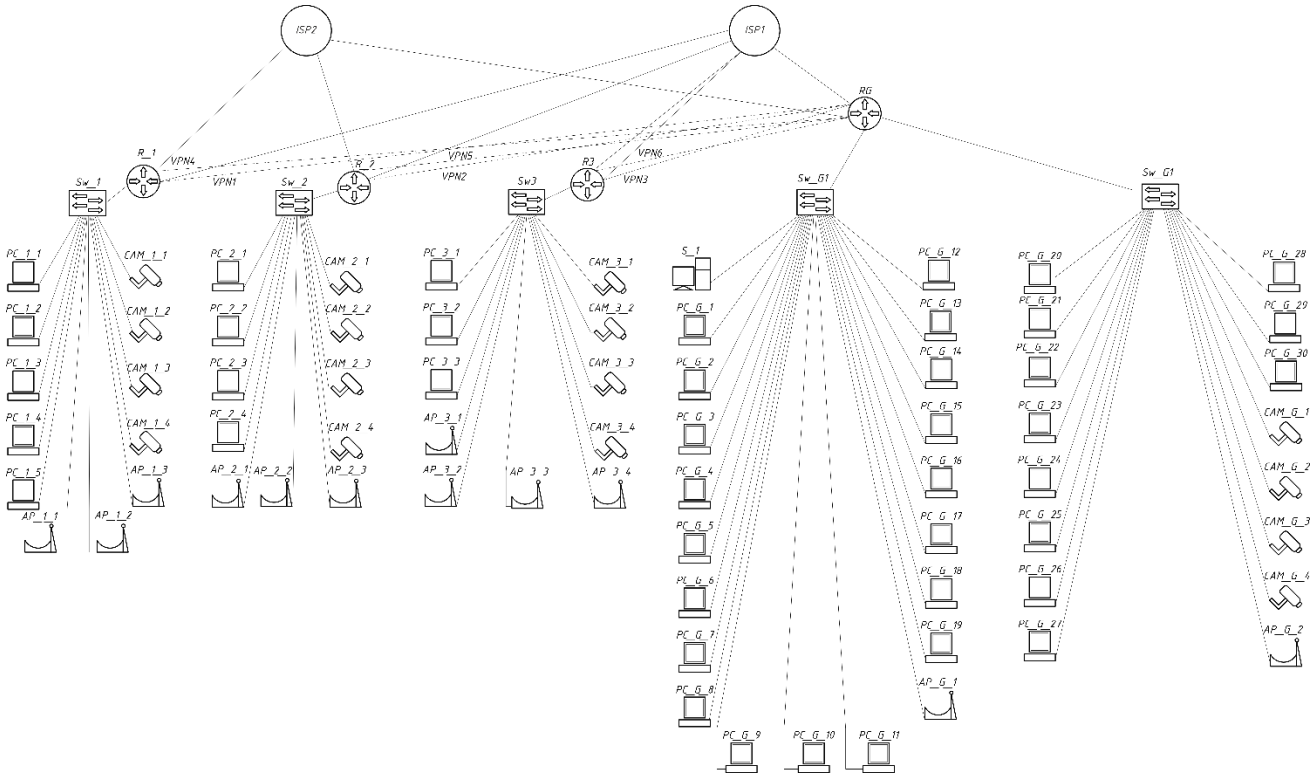


Рисунок 2.1 – Логічна топологія проектованої мережі

2.2 Аналіз та обґрунтування вибору технології мережі

Вибір технологічного базису для мережі «Global-Express» обумовлений необхідністю побудови захищеного, відмовостійкого та продуктивного середовища в умовах використання публічних каналів зв'язку. Першочерговим завданням є організація безпечного з’єднання між центральним офісом у Тернополі та віддаленими складськими терміналами. Розгляд альтернатив, таких як оренда виділених ліній (Leased Lines) або використання технології MPLS, показав їхню високу вартість та обмежену гнучкість при розширенні бізнесу. Тому для реалізації проекту обрано технологію Site-to-Site VPN на основі набору протоколів IPsec. Даний вибір дозволяє створити захищені віртуальні тунелі поверх звичайного інтернет-з’єднання. Використання стійких алгоритмів шифрування (AES-256) та автентифікації гарантує конфіденційність логістичних даних та фінансової звітності бухгалтерії, нівелюючи ризики перехоплення інформації зловмисниками.

Для забезпечення динамічної стійкості мережі та автоматизації процесів пересилання пакетів обрано протокол маршрутизації OSPF (Open Shortest Path First). На відміну від статичної маршрутизації, яка вимагає ручного втручання при кожній зміні в мережі, OSPF дозволяє маршрутизаторам самостійно обмінюватися інформацією про топологію. У складних умовах роботи «Global-Express», де можливі обриви ліній зв’язку у провайдерів, OSPF забезпечує миттєву переконфігурацію маршрутів. Якщо основний канал зв’язку зі складом на об’їзній дорозі стає недоступним, протокол за лічені секунди перенаправить трафік на резервний канал, що дозволить уникнути зупинки роботи терміналів збору даних та зриву графіків відвантаження.

Важливим аспектом внутрішньої організації мережі є впровадження технології віртуальних локальних мереж – VLAN (IEEE 802.1Q). Оскільки в офісі та на складах працюють різні групи користувачів (адміністрація, бухгалтерія, складські оператори), використання VLAN дозволяє логічно ізолювати їхній трафік один від одного на рівні комутаторів. Це суттєво підвищує безпеку,

оскільки обмежує можливість розповсюдження вірусів та несанкціонованого доступу до серверів з фінансовими даними. Крім того, сегментація мережі зменшує широкомовне навантаження (broadcast), що критично важливо для стабільної роботи бездротових точок доступу на складах, де велика кількість терміналів збору даних постійно генерує короткі та часті запити до бази даних.

Для забезпечення високої якості обслуговування у проекті передбачено впровадження механізмів QoS. Це технологічне рішення дозволяє призначати пріоритети для різних типів трафіку. У мережі логістичної компанії найвищий пріоритет надається трафіку IP-телефонії та запитам від систем управління складом, оскільки затримки в цих сервісах суттєво впливають на бізнес. Менш пріоритетний трафік, як-от оновлення програмного забезпечення або загальний доступ до мережі Інтернет, обробляється за залишковим принципом у моменти пікових навантажень. Комплексне використання IPsec, OSPF, VLAN та QoS дозволяє перетворити розрізнені підрозділи в Тернополі на єдину, стабільну та захищену інформаційну інфраструктуру, готову до масштабування та високих експлуатаційних навантажень.

Важливою складовою фізичного та канального рівнів проектованої мережі є впровадження технології Gigabit Ethernet (IEEE 802.3ab) як основного стандарту передачі даних. Вибір цієї технології замість застарілої Fast Ethernet обґрунтовується необхідністю створення високої пропускної здатності (до 1 Гбіт/с) на рівні ядра та розподілу мережі. У сучасних умовах роботи «Global-Express» обсяг внутрішнього трафіку значно зріс через використання систем відеоспостереження високої чіткості, що моніторять зони навантаження, та необхідність швидкого бекапування великих баз даних ERP-системи. Використання Gigabit Ethernet дозволяє усунути «вузькі місця» в мережі, забезпечуючи миттєвий відгук серверних додатків навіть у моменти пікового навантаження, коли офіс та всі склади одночасно здійснюють операції з вантажами.

Окрім чистої швидкості, вибір Gigabit Ethernet зумовлений переходом на сучасну кабельну інфраструктуру категорії Cat 5e або Cat 6. Це забезпечує кращу стійкість до перешкод та наведень, що особливо важливо в умовах складських

терміналів, де працює велика кількість промислового обладнання, двигунів та систем освітлення. Впровадження цієї технології також є інвестицією в масштабованість: вона дозволяє підтримувати технологію Power over Ethernet (PoE) на швидкостях гігабітного рівня, що необхідно для живлення сучасних точок доступу Wi-Fi та IP-камер без прокладання додаткових силових ліній. Таким чином, Gigabit Ethernet стає тим «швидкісним шосе», яке дозволяє всім іншим технологіям, таким як VPN та VLAN, функціонувати без затримок та втрат пакетів.

2.3 Вибір пасивного мережевого обладнання

Ефективність роботи гігабітної мережі безпосередньо залежить від якості пасивної інфраструктури, тому вибір кабельного середовища для тернопільського підрозділу базується на вимогах стандарту TIA/EIA-568. Основним середовищем передачі даних для внутрішніх локальних мереж обрано неекрановану кручену пару U/UTP категорії 6 (Cat 6). На відміну від категорії 5e, кабель шостої категорії має жорсткіші допуски щодо перехресних завад і системних шумів, що дозволяє стабільно підтримувати швидкість 1 Гбіт/с на відстані до 100 метрів. Це важливо для складських приміщень «Global-Express», де велика площа терміналів вимагає прокладання довгих сегментів кабелю від комутаційної шафи до віддалених точок доступу Wi-Fi та IP-камер.

Побудова територіально розподіленої мережі для компанії «Global-Express» базується на гібридному підході до організації каналів зв’язку. Враховуючи економічну доцільність та необхідність швидкого масштабування, для з’єднання віддалених складських терміналів із центральним офісом (сегмент WAN) було прийнято рішення використовувати інфраструктуру публічних інтернет-провайдерів. Безпека передачі даних у цьому загальнодоступному середовищі забезпечується шляхом створення криптографічно захищених VPN-тунелів. Такий підхід дозволяє уникнути значних капітальних витрат на прокладання власних магістральних ліній через усе місто, забезпечуючи при цьому гнучкість у виборі постачальників послуг зв’язку в кожній окремій точці присутності.

Для організації внутрішнього кабельного середовища (сегмент LAN) було проведено ретельний аналіз ринку пасивного мережевого обладнання. Основним компонентом фізичного рівня обрано кабель U/UTP Cat.6 4Pr від провідного вітчизняного виробника «Одескабель». Вибір даної продукції обґрунтований її високими експлуатаційними характеристиками: використання м'якого мідного дроту діаметром 0,57 мм (відповідно до стандарту 23 AWG) забезпечує низький опір та стабільну передачу гігабітного сигналу. Кожна жила провідника захищена поліетиленовою ізоляцією, що збільшує загальний діаметр до 1,05 мм, мінімізуючи ризик механічного пошкодження при протяжці кабелю в лотках. Даний тип кабелю пройшов сертифікацію на відповідність суворим міжнародним стандартам, таким як ISO/IEC 11801 та ANSI/TIA/EIA-568-B.2, що гарантує підтримку необхідної смуги пропускання для роботи складських терміналів та офісних станцій протягом наступних 10-15 років.

Якість фізичних з'єднань у проекті забезпечується використанням конекторів ATCOM RJ45 CAT.6 UTP 8P8C. Ці компоненти спеціально розроблені для роботи з кабелями шостої категорії, що мають товстіші жили, та забезпечують надійний електричний контакт без втрат пакетів на високих частотах. Для зручності адміністрування та створення естетичного робочого середовища, підключення кінцевого обладнання – від персональних комп'ютерів логістів до стаціонарних сканерів на складах – реалізується через настінні мережеві розетки стандарту 8P8C.

Для забезпечення термінального підключення робочих станцій та мережевого обладнання в межах розробленого проєкту було обрано накладну мережеву розетку моделі Cablexpert RJ45x1 UTP Cat.6 (див. рис. 2.2). Вибір даної моделі зумовлений її високими експлуатаційними характеристиками та конструктивною адаптивністю до умов швидкого розгортання IT-інфраструктури. Використання розеток зовнішнього типу монтажу є найбільш раціональним рішенням для офісних та складських приміщень компанії «Global-Express», оскільки вони дозволяють мінімізувати трудовитрати на інсталяцію та уникати складних робіт із руйнування стін для прихованої проводки.

Рисунок 2.2 – Мережева розетка Cablexpert RJ45x1 UTP cat.6

Дане технічне рішення забезпечує легкий доступ до комутаційного вузла для технічного обслуговування або модернізації мережі в майбутньому. Корпус розетки Cablexpert виготовлений із міцного пластику, що захищає внутрішні контакти від пилу та механічних пошкоджень, а повна відповідність категорії 6 гарантує стабільну передачу даних на гігабітних швидкостях без виникнення паразитних наведень чи втрат пакетів. Таким чином, обраний компонент стає надійним інтерфейсом між пасивною кабельною системою та активним обладнанням підприємства.

Комутація між розеткою та пристроєм виконується за допомогою заводських патч-кордів відповідної категорії, що дозволяє оперативно змінювати конфігурацію робочих місць без необхідності перемонтування кабельної лінії.

Враховуючи насиченість сучасного ринку мережевих компонентів та необхідність забезпечення високої ергономіки робочих місць, для фінальної комутації обладнання було обрано готові патч-корди промислового виробництва довжиною 1,5 метра. Такий розмір є оптимальним для підключення персональних комп'ютерів логістів та офісних працівників до настінних розеток, оскільки дозволяє уникнути надмірного накопичення кабелю та його випадкового пошкодження.

Конкретним технічним рішенням для проєкту стала модель 2E CAT6 UTP RJ-45 26AWG, яка характеризується високою гнучкістю провідників та надійним захистом фіксатора конектора від заломів. Використання патч-кордів шостої категорії з калібром провідника 26AWG гарантує стабільну роботу гігабітного інтерфейсу та мінімізує згасання сигналу на коротких ділянках, що є критично важливим для підтримки високої швидкості обміну даними між кінцевими пристроями та комутаційною інфраструктурою підприємства.

Інфраструктура логістичної компанії охоплює чотири відокремлені об'єкти, кожен з яких розташований у власній одноповерховій будівлі або займає функціональну частину поверху. Детальні плани приміщень із нанесеними зонами розташування обладнання наведені у додатку А. Проєктування топології передбачає впровадження ієрархічної моделі з чіткою централізацією обчислювальних потужностей та систем зберігання даних, що є критично важливим для стабільності та безпеки логістичних операцій.

У центральному офісі ключовою точкою концентрації ресурсів визначено серверне приміщення. Воно спроєктоване як спеціалізована гермозона з обмеженим фізичним доступом, оснащена кліматичним контролем, системами пожежної безпеки та джерелами безперебійного живлення з подвійним перетворенням. У серверній консолідується активне обладнання: сервери бази даних ERP, файлові сховища, контролери домену, сервер IP-телефонії та реєстратори відеоспостереження. Також тут інсталюється маршрутизатор (Firewall), який забезпечує термінацію VPN-каналів від віддалених складів та захист зовнішнього інтернет-периметра. Локальна комутація здійснюється за допомогою обладнання рівня доступу з використанням мідного кабелю Cat 6.

Для забезпечення мобільності персоналу на об’єктах розгортається бездротова мережа. Точки доступу Wi-Fi розміщуються стратегічно в центральних частинах приміщень для забезпечення рівномірного покриття. Живлення точок доступу та IP-камер реалізується за технологією PoE безпосередньо від комутаторів рівня доступу, що спрощує кабельну інфраструктуру та підвищує надійність системи. Кожна філія (складський термінал) обладнується локальним комутаційним вузлом, який розміщується в захищеній настінній шафі. Це дозволяє локалізувати мережевий трафік підрозділу та забезпечити надійне з’єднання з центральним офісом через VPN-шлюз.

Для розміщення активного та пасивного мережевого обладнання на всіх об'єктах передбачено використання спеціалізованих телекомунікаційних шаф. Вибір конструктивів базувався на комплексному аналізі наступних технічних параметрів:

- розрахунок висоти в юнітах (U) проводився з урахуванням поточного наповнення та обов'язкового резерву (20–30%) для майбутньої модернізації;

- наявність пасивної перфорації та можливість встановлення блоків примусової вентиляції для відведення тепла від активного обладнання;

- використання сталевого корпусу з надійною системою замків на передніх дверях та бічних панелях для запобігання несанкціонованому втручанню.

- наявність органайзерів для впорядкованого укладання патч-кордів, що полегшує діагностику та обслуговування мережі;

- відповідність корпусу умовам експлуатації, зокрема захист від пилу в складських зонах.

За сукупністю технічних характеристик та критерієм вартості, для реалізації проєкту обрано настінні комутаційні шафи Hypernet WMNC-9U-FLAT (див. рис. 2.3). Ця модель забезпечує оптимальну висоту 9U для розміщення комутатора, патч-панелі, полиці з маршрутизатором та блоку джерела безперебійного живлення, зберігаючи при цьому компактні габарити для монтажу в обмеженому просторі офісних та складських приміщень.

Рисунок 2.3 – Комутаційна шафа Hypernet WMNC-9U-FLAT

Вибрана комутаційна шафа слугує базовою платформою для інтеграції ключових елементів мережевої інфраструктури, зокрема: блоків патч-панелей, активних комутаторів, систем кабельного менеджменту та засобів гарантованого електроживлення. Для захисту обладнання від нестабільності в електромережі та забезпечення автономної роботи вузлів у разі аварійних відключень, передбачено встановлення джерела безперебійного живлення APC Back-UPS Pro 1500VA. Це

рішення з лінійно-інтерактивною топологією дозволяє не лише підтримувати живлення, а й стабілізувати напругу, що критично важливо для збереження працездатності маршрутизаторів та серверів бази даних у режимі 24/7.

Комутація горизонтальних кабельних ліній у шафі реалізується за допомогою патч-панелі Panduit 19" на 24 порти (Категорія 6). Даний компонент обрано через його високу надійність та повну відповідність міжнародному стандарту EIA/TIA 568 B.2-1, що гарантує збереження характеристик гігабітного каналу на всьому шляху проходження сигналу. Конструктивною особливістю панелі Panduit є інтегрована система термінації, яка не потребує спеціалізованого ударного інструменту, оскільки використовує механізм автоматичного прорізання ізоляції при закритті модулів.

Для підтримання порядку всередині шафи та запобігання надмірному натягу провідників, панель комплектується професійними елементами кріплення та нейлоновими хомутами Colring. Це дозволяє сформувати акуратні кабельні пучки та забезпечити правильні радіуси вигину крученої пари категорії 6. Використання такої зв’язки обладнання (APC та Panduit) створює професійне та відмовостійке середовище, яке спрощує подальше адміністрування мережі та мінімізує ризик виникнення фізичних несправностей у комутаційних вузлах підприємства.

2.4 Вибір активного мережевого обладнання

Ефективність функціонування IT-інфраструктури компанії «Global-Express» безпосередньо залежить від коректного підбору активного мережевого обладнання, що має забезпечити високу пропускну здатність, багаторівневу безпеку та відмовостійкість. Процес вибору апаратної бази ґрунтується на раніше визначеній ієрархічній моделі та детальному аналізі інформаційних потоків (див. розділ 1.2), що проходять між центральним офісом у Тернополі та віддаленими складськими терміналами.

Як вже відмічалось в розділі 2.1, враховуючи масштаби підприємства та відносно невелику кількість кінцевих вузлів у кожному сегменті, у межах даного

проєкту реалізовано модифіковану ієрархічну модель мережі. Для оптимізації апаратних ресурсів та спрощення адміністрування було прийнято рішення про логічне об'єднання рівнів ядра та розподілу за допомогою високопродуктивного маршрутизатора з інтегрованими сервісами безпеки.

Маршрутизатор виконує роль інтелектуального центру мережі «Global-Express», поєднуючи в собі функції шлюзу безпеки, пристрою ядра та вузла розподілу трафіку. Він забезпечує не лише високошвидкісний доступ локальної мережі до ресурсів Інтернету, а й відповідає за маршрутизацію пакетів між віртуальними підмережами (Inter-VLAN routing), що дозволяє ізолювати трафік різних відділів на логічному рівні без втрати продуктивності.

Оскільки підключення до зовнішнього інтернет-провайдера реалізується через волоконно-оптичну лінію зв'язку, ключовою вимогою до пристрою є наявність комбінованих SFP-портів. Це дозволяє організувати пряму передачу світлового сигналу від провайдера до маршрутизатора без використання додаткових медіаконвертерів, що суттєво підвищує надійність з’єднання. Аналогічно, магістральний канал (Uplink) від комутатора рівня доступу до маршрутизатора також виконується за допомогою оптоволокна, що мінімізує вплив електромагнітних наведень та забезпечує стабільну роботу ядра мережі.

Фундаментальною вимогою при виборі апаратної платформи стала підтримка апаратного шифрування та стеку протоколів IPsec. Це необхідно для побудови стійких Site-to-Site VPN-тунелів, які об'єднують територіально віддалені складські термінали з головним офісом у Тернополі в єдину захищену корпоративну мережу. Завдяки інтегрованим сервісам безпеки, маршрутизатор здатен обробляти зашифрований трафік у реальному часі, не створюючи затримок для критично важливих логістичних додатків.

На основі детального аналізу технічних вимог та розрахункового навантаження, для реалізації проєкту було обрано маршрутизатор Cisco ISR4321/K9. Дана модель серії Integrated Services Routers (ISR) відрізняється високою модульністю, наявністю необхідних гігабітних SFP-інтерфейсів та

потужним процесором для обробки VPN-з'єднань. Зовнішній вигляд пристрою представлений на рисунку 2.4.

Рисунок 2.4 – Зовнішній вигляд маршрутизатора Cisco ISR4221/K9

Апаратна архітектура обраного маршрутизатора базується на модульній платформі, що забезпечує гнучкість при побудові мережевих вузлів. Базова конфігурація пристрою включає два комбіновані порти, які можуть працювати як у режимі SFP, так і в режимі Gigabit Ethernet (RJ-45). Для розширення функціональних можливостей передбачено два слоти під інтерфейсні модулі нового покоління (NIM). У межах проєкту планується інсталяція додаткових SFP-модулів у ці слоти, що дозволить організувати високошвидкісне оптичне з'єднання з комутаторами рівня доступу, мінімізуючи затримки всередині ядра мережі.

Маршрутизатор Cisco ISR4321/K9 спроєктований для обробки мультисервісного трафіку з високою інтенсивністю. Його обчислювальна потужність підкріплена 4 ГБ оперативної пам'яті (з можливістю модернізації до 16 ГБ), що дозволяє пристрою стабільно тримати великі таблиці маршрутизації OSPF та підтримувати численні одночасні VPN-сесії без деградації продуктивності. Для надійного зберігання образів операційної системи Cisco IOS-XE та складних конфігураційних файлів передбачено 4 ГБ флеш-пам'яті.

Такий технічний потенціал робить ISR 4321 оптимальним рішенням для «Global-Express», оскільки він поєднує в собі функції маршрутизації, захисту даних та глибокого аналізу трафіку в одному компактному корпусі. Зведені технічні характеристики та експлуатаційні параметри моделі представлено в таблиці 2.1.

Таблиця 2.1 – Основні характеристики Cisco ISR4321/K9 [17]

Характеристика	Значення
1	2
Серія продукту	4000
Модель продукту	4321
Кількість вбудованих портів GE SFP	2
Кількість вбудованих портів RJ-45 GE	2
Кількість слотів NIM розширення	2
Розмір	43,7 x 32,2 x 25,4 мм
Вага	3,22 кг
Живлення	230 В

Маршрутизатор Cisco ISR 4321/K9 виступає надійним фундаментом для побудови територіально розподіленої інфраструктури завдяки розширеній підтримці криптографічних сервісів та інтелектуальних протоколів маршрутизації. Апаратне забезпечення моделі оптимізоване для розгортання масштабованих VPN-архітектур, що дозволяє об’єднати віддалені склади в єдиний безпечний контур.

Функціональні можливості пристрою охоплюють повний стек сучасних мережевих технологій:

- NAT (Network Address Translation): забезпечує трансляцію внутрішніх адрес підмереж у публічний IP-простір, що не лише економить адресний ресурс, а й приховує топологію локальної мережі від зовнішніх загроз;

- динамічна маршрутизація (OSPF, EIGRP, BGP, RIP): підтримка цих протоколів дозволяє мережі «самовідновлюватися». Зокрема, протокол OSPF у межах проекту відповідає за миттєвий обмін інформацією про стан каналів зв'язку між офісом та філіями, автоматично перенаправляючи трафік у разі аварійних ситуацій;

- PBR (Policy-Based Routing): механізм маршрутизації на основі політик дозволяє гнучко керувати потоками даних. Наприклад, критично важливий трафік ERP-системи можна спрямувати через основний швидкісний канал, а загальний інтернет-трафік — через резервний;

- PfR (Performance Routing): інтелектуальна технологія, що аналізує затримки та джиттер у реальному часі, обираючи найкращий шлях для передачі пакетів на основі поточної продуктивності каналів провайдерів.

Завдяки інтегрованій операційній системі Cisco IOS-XE, маршрутизатор пропонує гнучкі інструменти для реалізації різних типів віртуальних приватних мереж – від класичних Site-to-Site IPsec VPN до складних DMVPN (Dynamic Multipoint VPN). Це гарантує, що конфіденційні логістичні дані, які передаються між центральним офісом у Тернополі та складськими терміналами, будуть надійно захищені від перехоплення чи спотворення на всьому шляху прямування.

Реалізація політик безпеки на маршрутизаторі здійснюється за допомогою розширених списків контролю доступу (Extended ACLs). Ці інструменти дозволяють адміністратору мережі детерміновано керувати трафіком на основі адрес джерела та призначення, типів протоколів та номерів портів. У контексті логістичного підприємства це дає змогу:

- ізолювати критичні сегменти (наприклад, сервер з базою даних ERP) від загального доступу з інтернету;

- обмежувати доступ до певних сервісів для віддалених складів, залишаючи відкритими лише необхідні порти для роботи систем обліку.

- запобігати несанкціонованим спробам проникнення в корпоративну мережу через публічні канали зв'язку.

Використання вбудованого міжмережевого екрана в моделі ISR 4321 дозволяє відмовитися від придбання окремих апаратних файрволів для невеликих філій, що значно оптимізує бюджет на побудову IT-інфраструктури. При цьому апаратна архітектура Cisco IOS-XE гарантує, що фільтрація трафіку через ACL не призведе до відчутного зниження швидкості передачі даних, підтримуючи високу продуктивність мережі в реальному часі.

Наступним компонентом активного мережевого обладнання архітектури мережі логістичної компанії «Global-express» є комутатори рівня доступу.

Комутатори рівня доступу (Access Layer) виступають фундаментальними вузлами в архітектурі підприємства, забезпечуючи первинне підключення кінцевого обладнання до загальнокорпоративної мережі. На ці пристрої покладається функція агрегації трафіку від робочих станцій логістів, систем IP-відеоспостереження та іншої периферії з подальшою передачею даних до центрального комутатора або маршрутизатора ядра.

Процедура підбору комутаторів базується на критичному аналізі двох параметрів: щільності портів та реальної пропускної здатності внутрішньої шини. Враховуючи необхідність забезпечення кожному співробітнику «Global-Express» гарантованого каналу в 1 Гбіт/с, обов'язковою умовою є підтримка стандарту Gigabit Ethernet на всіх інтерфейсах. Це дозволяє уникнути виникнення затримок при роботі з об'ємними базами даних та потоковим відео у високій якості.

Для визначення оптимальної конфігурації обладнання ми орієнтуємося на найбільш завантажений сегмент мережі – центральний офіс. Згідно з логічною схемою (Додаток Б), цей сегмент налічує 22 активні хости. Таким чином, комутатор повинен бути оснащений щонайменше 23 портами: 22 інтерфейси для кінцевих вузлів та 1 високошвидкісний Uplink-порт для зв'язку з маршрутизатором.

Проте, наявність гігабітних портів не гарантує високу продуктивність без відповідної внутрішньої комутаційної спроможності (Switching Capacity або Backplane Bandwidth). Цей показник характеризує здатність апаратної частини пристрою одночасно обробляти потоки даних зі всіх портів у режимі повного дуплексу без втрати пакетів. Розрахунок мінімально необхідної продуктивності для найзавантаженішого вузла виконується за формулою [4]:

$$C = N \cdot S \cdot 2 \quad (2.1)$$

де:

C – внутрішня комутаційна спроможність;

N – загальна кількість задіяних портів;

S – номінальна швидкість порту (1 Гбіт/с);

2 – коефіцієнт, що враховує повнодуплексний режим (одночасне приймання та передача).

Для офісного сегмента з 22 активними вузлами отримуємо наступне значення:

$$21 \cdot 1 \text{ Гбіт/с} \cdot 2 = 42 \text{ Гбіт/с}$$

На основі отриманих розрахунків, а також враховуючи необхідність підтримки технології PoE для живлення Wi-Fi точок доступу та камер, для впровадження обрано керований комутатор Cisco Catalyst 2960L-24PS-LL. Дана модель володіє необхідним запасом продуктивності та функціоналом для забезпечення стабільної роботи мережі. Зовнішній вигляд пристрою наведено на рисунку 2.5.

Рисунок 2.5 – Комутатор Cisco Catalyst 2960L-24PS-LL

Інтеграція обраного керованого комутатора другого рівня (L2) у структуру «Global-Express» дозволяє сформувати високопродуктивне середовище передачі даних. Завдяки повній підтримці стандарту Gigabit Ethernet на кожному клієнтському порту, забезпечується мінімальна затримка при зверненні до серверних ресурсів, а виділені аплінк-інтерфейси гарантують стабільність магістральних каналів зв'язку. Така архітектурна побудова дозволяє комутатору ефективно обробляти мультисервісний трафік (дані, голос, відео) без виникнення черг або втрат пакетів.

Апаратна конфігурація пристрою включає 24 LAN-інтерфейси стандарту RJ-45 з підтримкою швидкостей 10/100/1000 Мбіт/с, що повністю покриває потреби в підключенні кінцевих вузлів офісного чи складського сегмента. Особливу увагу приділено надійності магістральних з'єднань: наявність чотирьох додаткових SFP-слотів (1000 Мбіт/с) дозволяє організувати високошвидкісні

канали зв'язку з маршрутизатором ядра або іншими вузлами мережі за допомогою волоконно-оптичних ліній. Це рішення є критично важливим для створення відмовостійкої опорної мережі підприємства.

Одним із вирішальних факторів вибору даної моделі є її комутаційна спроможність, що становить 56 Гбіт/с. Цей показник суттєво перевищує розрахований мінімальний поріг у 44 Гбіт/с, забезпечуючи значний експлуатаційний запас. Такий надлишок продуктивності нівелює ризики перевантаження внутрішньої шини пристрою під час пікової активності користувачів або при проведенні резервного копіювання великих масивів даних. Детальні технічні специфікації та експлуатаційні параметри обраного комутатора систематизовано у таблиці 2.2.

Таблиця 2.2 – Основні характеристики Cisco Catalyst 2960L-24PS-LL [17]

Характеристика	Значення
Тип пристрою	Комутатор другого рівня L2
Порти LAN	24 x 10/100/1000 Мбіт/с PoE+
Порти Uplink	4 x 10G SFP+,
Пропускна здатність	56 Гбіт/с
Швидкість обробки пакетів	46,67 млн пакетів/сек
Буфер пам’яті	512 Мб
Підтримка VLAN	8192
Розмір, мм	440 x 265 x 445
Вага, кг	3,46
Підтримка PoE	IEEE 802.3af/at (PoE+)

Відповідно до розробленої архітектури, бездротовий сегмент мережі компанії «Global-Express» базується на використанні точок доступу бізнес-серії TP-LINK EAP225 (див. рис. 2.6). Для забезпечення рівномірного покриття та мінімізації зон із низьким рівнем сигналу, пристрої монтуються в геометричному

центрі торгівельних та адміністративних залів. Таке позиціонування дозволяє ефективно обслуговувати мобільні термінали збору даних (ТЗД) та клієнтські пристрої по всій площі приміщення.

Рисунок 2.6 – Точка доступу TP-LINK EAP225

Вибір моделі EAP225 обґрунтований низкою технічних та експлуатаційних переваг [14]:

- підтримка стандарту 802.11ac (Wave 2) – використання технології MU-MIMO дозволяє точці доступу одночасно обмінюватися даними з декількома клієнтами, що критично важливо при інтенсивній роботі складського персоналу;
- дводіапазонний режим (Dual-Band) – робота на частотах 2.4 ГГц та 5 ГГц забезпечує сумарну швидкість передачі даних до 1350 Мбіт/с, що гарантує стабільність високонавантажених сервісів;
- конструктивне виконання корпусу дозволяє здійснювати швидку інсталяцію на стелю або стіни за допомогою спеціальних кріплень, що входять до комплекту. Це забезпечує гармонійну інтеграцію пристрою в інтер'єр без порушення естетики офісного простору;
- підтримка програмного контролера Omada дозволяє адміністратору мережі дистанційно моніторити стан точок доступу та налаштовувати безшовний роумінг між ними.

Важливою особливістю є підтримка технології 802.3af PoE, що дозволяє живити точки доступу безпосередньо від обраного раніше комутатора Cisco Catalyst через кабель крученої пари. Це значно спрощує розгортання мережі,

оскільки зникає потреба в прокладанні додаткових силових ліній до місць встановлення обладнання.

Ще однією перевагою серії EAP225 у контексті логістичного підприємства є розширена підтримка механізмів автентифікації користувачів. Використання протоколу WPA2/WPA3-Enterprise у поєднанні з RADIUS-сервером дозволяє адміністраторам «Global-Express» здійснювати індивідуальний контроль доступу до бездротового середовища. Це нівелює ризики несанкціонованого проникнення в корпоративну мережу через Wi-Fi сегмент, забезпечуючи високий рівень конфіденційності даних та можливість детального аудиту підключень кожного клієнтського пристрою.

Для реалізації комплексної системи відеоспостереження на складських терміналах та в офісних зонах обрано передову IP-камеру Reolink RLC-1224A (див. рис. 2.7). Дана модель є оптимальним рішенням для інтеграції в сучасну кабельну інфраструктуру компанії, оскільки вона підтримує стандарт передачі даних по крученій парі та повноцінне живлення за технологією PoE (802.3af). Це дозволяє підключати камеру безпосередньо до обраного комутатора Cisco одним кабелем Cat 6, що значно знижує витрати на монтаж та підвищує надійність системи живлення вузла спостереження.

Рисунок 2.7 – Зовнішній вигляд IP-камери Reolink RLC-1224A

Вибір моделі RLC-1224A також обґрунтований її високою роздільною здатністю (12 Мп) та інтелектуальними функціями детекції людей та транспортних засобів. Це критично важливо для логістичного центру, оскільки дозволяє автоматизувати моніторинг зон розвантаження та забезпечити високу деталізацію при ідентифікації номерних знаків або облич. Таким чином, обрані

компоненти Wi-Fi та відеоспостереження створюють синергію між мобільністю персоналу та фізичною безпекою об'єктів підприємства.

Технічний потенціал камери Reolink RLC-1224A базується на використанні сучасної матриці з роздільною здатністю 12 Мп (4096 x 3072), що забезпечує виняткову деталізацію та чіткість зображення. Це дозволяє системі безпеки компанії «Global-Express» ідентифікувати дрібні деталі, такі як маркування вантажів або обличчя відвідувачів, на значній відстані. Для цілодобового моніторингу пристрій оснащений адаптивною системою інфрачервоного (ІЧ) підсвічування з ефективним радіусом дії до 30 метрів, що гарантує отримання контрастного монохромного зображення навіть за умов нульової освітленості на складах.

Інтелектуальна складова моделі представлена алгоритмами детекції руху з функцією розпізнавання об'єктів (людина/транспортний засіб). Впровадження цієї технології дозволяє мінімізувати кількість хибних тривог, спричинених тваринами чи природними явищами, та точно фіксувати критичні події в зоні спостереження. Завдяки повній підтримці стандарту Power over Ethernet (PoE), інсталяція камер інтегрується безпосередньо в раніше спроєктовану кабельну систему на базі Cat 6.

За результатами проведеного аналізу та обґрунтування, формування специфікації активного та пасивної обладнання для мережі логістичної компанії повністю завершено. Обрана апаратна база на основі рішень Cisco, TP-Link, Reolink та кабельної продукції «Одескабель» створює цілісну, масштабовану та захищену інфраструктуру, що відповідає всім сучасним вимогам бізнесу.

2.5 Вибір серверного обладнання

Для центрального офісу компанії «Global-Express» важливо забезпечити безперебійний доступ до ERP-системи, бази даних SQL та корпоративних поштових сервісів у режимі 24/7.

Вибір серверного обладнання базувався на принципах відмовостійкості, можливості масштабування та високої щільності обчислювальних ресурсів. Для

реалізації поставлених завдань обрано сервер Dell PowerEdge R450 (див. рис. 2.8) у стійковому виконанні (Rack-mount 1U). Ця платформа оптимізована для роботи в сучасних мережах і забезпечує ідеальний баланс між потужністю та енергоспоживанням.

Рисунок 2.8 – Сервер Dell PowerEdge R450

Основними технічними критеріями, що зумовили вибір даної моделі, є:

- побудований на базі процесорів Intel Xeon Silver, що забезпечує високу швидкість обробки багатопотокових запитів від користувачів ERP-системи та складських терміналів;

- оснащується апаратним RAID-контролером. Конфігурація передбачає використання масиву RAID 10 на базі швидкісних SSD-накопичувачів, що поєднує високу швидкість запису/читання із дзеркальним резервуванням даних;

- наявність вбудованих гігабітних портів та підтримка додаткових мережевих адаптерів дозволяє інтегрувати сервер у ядро мережі за допомогою агрегованих каналів (EtherChannel), що виключає появу «вузьких місць» при пікових навантаженнях;

- підтримує встановлення двох блоків живлення з можливістю гарячої заміни (Hot-Plug Redundant Power Supplies), що в поєднанні з раніше обраним ДБЖ APC гарантує стабільну роботу при збоях у системі електропостачання;

Для оптимізації використання апаратних ресурсів на базі обраного сервера планується впровадження технології віртуалізації (наприклад, VMware ESXi або Microsoft Hyper-V). Це дозволить розгорнути декілька логічно ізольованих віртуальних серверів на одній фізичній машині:

- контролер домену (Active Directory) – для керування правами доступу користувачів;

- сервер баз даних та ERP – для обліку логістичних операцій;
- файловий сервер – для зберігання документації та звітів;
- сервер відеоспостереження – для керування потоками з IP-камер Reolink.

Такий підхід значно спрощує процедуру резервного копіювання, знижує витрати на обслуговування та дозволяє гнучко перерозподіляти потужність процесора та пам'яті між сервісами залежно від поточних потреб підприємства. Таким чином, серверна платформа Dell PowerEdge стає надійним фундаментом для стабільної роботи всіх підрозділів «Global-Express».

2.6 Особливості монтажу мережі та розташування мережевих вузлів

Фізична топологія мережі логістичної компанії «Global-Express» спроєктована з урахуванням архітектурних особливостей чотирьох об'єктів: Головного офісу та трьох складських терміналів (Склад №1, Склад №2, Склад №3). Розташування активного обладнання, периферійних пристроїв та кабельних трас відображено на планах приміщень представлених на додатку В.

Розташування вузлів мережі розраховано таким чином, щоб довжина жодного горизонтального сегмента кабелю не перевищувала критичну межу в 90 метрів, визначену стандартами для мідних ліній. У центральному офісі вузол комутації розташовується в ізольованому приміщенні з обмеженим доступом, що дозволяє централізувати керування трафіком. На складах вузли розміщуються у настінних комутаційних шафах, які захищають активне обладнання від пилу та випадкових механічних впливів, характерних для складської логістики. Таке розташування вузлів та вибір високоякісного кабельного середовища «Одескабель» створюють відмовостійкий фізичний рівень, здатний витримувати інтенсивний обмін даними між усіма структурними підрозділами підприємства.

Розташування вузлів мережі спроектовано за принципом максимальної доступності та безпеки. У центральному офісі на вулиці Бродівській облаштовується окреме серверне приміщення, що виконує роль головного вузла комутації. Тут встановлюється телекомунікаційна шафа висотою 9U, в якій

розміщується сервер, центральний маршрутизатор та комутатори рівня доступу центрального офісу. Серверна обладнується системою прецизійного кондиціювання та джерелами безперебійного живлення з подвійним перетворенням, що гарантує роботу ядра мережі навіть при короткочасних відключеннях електроенергії в місті.

Усі робочі місця офісу (30 ПК) підключаються до цього вузла за топологією «ієрархічна зірка», де довжина кожної кабельної лінії не перевищує 60-70 метрів для забезпечення максимального запасу потужності сигналу.

На складських терміналах (Склад №1 на об'їзній, Східний та Південний склади) розгортаються розподільчі вузли (ІС). Через специфіку складських приміщень – велику висоту стель та наявність металевих стелажів – комутаційні вузли розміщуються у настінних антивандальних шафах висотою 9U. Ці шафи розташовуються в адміністративних побутовках складів, що мають обмежений доступ. Кожен складський вузол включає комутатор з підтримкою PoE+ (Power over Ethernet), що дозволяє живити точки доступу та камери спостереження безпосередньо через кабель крученої пари. Таке розташування вузлів мінімізує довжину горизонтальних кабельних трас до терміналів збору даних та принтерів етикеток, а також забезпечує зручність обслуговування мережі технічним персоналом без зупинки логістичних процесів.

Прокладання горизонтальної підсистеми кабелів (Cat 6) організовано за магістральним принципом:

- головна траса проходить крізь стіни коридорного типу, забезпечуючи підключення кабінетів адміністративного блоку («ІТ-відділ», «Керівник», «Юрист», «Інженер з охорони праці»);

- окремі відгалуження спрямовані до «Бухгалтерії», кабінету «HR-менеджера» та «Відділу по роботі з клієнтами»;

- найбільша концентрація робочих місць спостерігається у «Відділі транспортної логістики», де до кожного ПК підведено дротове з'єднання. Точки бездротового доступу (AP_G_1, AP_G_2) розміщені геометрично по центру

великих приміщень для рівномірного покриття. IP-камери встановлені по кутах робочих зон для забезпечення максимального кута огляду без «сліпих зон».

На кожному з трьох складів архітектура мережі побудована за єдиним стандартом. Роль локальної серверної (комутаційного вузла) виконує кабінет Головного менеджера складу. Саме туди заведено оптичний канал від провайдера Інтернету та встановлено настінну шафу з локальним маршрутизатором і комутатором доступу.

- основні лінії прокладаються вздовж капітальних стін, з'єднуючи кімнати персоналу, складські зони та зони експедиції (на плані складу №3 представлено у на додатку В – зона приймання/видачі);

- у великих складських приміщеннях (наприклад, «Складське приміщення №1» та «№2») слід рівномірно розподілити по 2-4 безпровідні точки доступу. Це гарантує безшовний роумінг для терміналів збору даних під час переміщення комірників;

- завдяки використанню технології PoE від комутаторів у кабінетах менеджерів, до IP-камер та точок доступу підведено лише по одному кабелю «кручена пара», що значно пришвидшило монтажні роботи у високих складських приміщеннях.

В межах проекту зв'язок між територіально розрізненими об'єктами здійснюється через канали провайдерів (WAN-порт маршрутизатора), тому оптичне середовище використовується переважно всередині серверної для з’єднання ядра мережі з комутатрами рівня доступу. Таким чином, обрана комбінація кабельної інфраструктури Cat 6 та стратегічне розміщення комутаційних вузлів створюють надійну структуровану кабельну систему для стабільної роботи всіх логістичних сервісів компанії.

З огляду на різні умови експлуатації в адміністративних та промислових зонах, проєктом передбачено диференційований підхід до захисту кабельних трас. У приміщеннях Головного офісу магістральні лінії прокладаються у прихованому просторі за фальшстелею, а вертикальні спуски до робочих місць організовані за допомогою естетичних настінних пластикових коробів.

Натомість у складських терміналах (Склад №1, №2, №3), де існує підвищений ризик механічних пошкоджень від роботи вантажно-розвантажувальної техніки, магістральні кабелі монтуються у підвісних металевих лотках під стелею.

Усі спуски до IP-камер та точок доступу додатково захищаються гнучкими пластиковими гофротрубами. Таке рішення гарантує довговічність мережевої інфраструктури та відповідає чинним нормам пожежної безпеки.

2.7 Розподіл адресного простору мережевих вузлів

Планування адресного простору – це важливий етап проєктування, оскільки правильна IP-адресація забезпечує порядок у мережі та спрощує налаштування безпеки (VPN, ACL).

Для логістичної мережі такого масштабу найкраще підходить використання приватного діапазону класу C (192.168.0.0/24). Це дозволить виділити окремі підмережі (VLAN) для кожного об'єкта та відділу.

У проектовані мережі необхідно призначити IP-адреси не лише комп'ютерам, але й камерам відеонагляду, сканери штрих-кодів (термінали збору даних) та сервер. Щоб трафік від камер відеоспостереження (який дуже об'ємний) не заважав роботі ERP-системи чи бухгалтерії його необхідно ізолювати. Також поділ на підмережі дозволить впровадити списки контролю доступу (ACL). Наприклад, водії в гостьовому Wi-Fi не зможуть навіть «побачити» сервер із фінансовими даними. Виходячи із цих міркувань мережу слід розділити на логічні підмережі шляхом поділу на VLAN.

Поділ на підмережі вирішено здійснити за структурними підрозділами підприємства:

- Admin – підмережа адміністративно-управлінський персоналу це директор філії (1 ПК), секретар (1 ПК), інженер з охорони праці (1 ПК), юрист (1 ПК) та HR-менеджер (1 ПК). Разом 5 комп'ютерів;
- Finansy – бухгалтерія та фінансовий відділ включає 4 ПК;
- Clients – відділ по роботі з клієнтами та продажу послуг - 7 ПК;

- Logist – відділ транспортної логістики та диспетчеризації включає 12 ПК;
- IT – IT-відділ (2 ПК);
- Cam_G – камери відеонагляду головного офісу кількістю 4 шт;
- Guest_G – гостьова Wi-Fi мережа головного офісу розрахована максимально на 10 гостьових пристроїв;
- Sklad_1 – пристрої складу №1. Підмережа включає 5 стаціонарних ПК для операторів складу (оформлення накладних) та 10 мобільних терміналів збору даних, підключених через мережу Wi-Fi. Разом 15 адрес;
- Cam_1 – підмережа камер відеонагляду складу №1 кількістю 4 шт;
- Guest_1 – гостьова Wi-Fi мережа складу №1 розрахована максимально на 10 адрес;
- Sklad_2 – пристрої складу №2. Включає 5 стаціонарних ПК для операторів складу (оформлення накладних) та 7 мобільних сканерів штрих-кодів, підключених через мережу Wi-Fi. Разом 12 адрес;
- Cam_2 – підмережа камер відеонагляду складу №2 кількістю 4 шт;
- Guest_2 – гостьова Wi-Fi мережа складу №2 розрахована максимально на 10 адрес;
- Sklad_3 – пристрої складу №3. Включає 3 стаціонарних ПК для операторів складу (оформлення накладних) та 7 мобільних сканерів штрих-кодів, підключених через мережу Wi-Fi. Разом 10 адрес;
- Cam_3 – підмережа камер відеонагляду складу №3 кількістю 4 шт;
- Guest_3 – гостьова Wi-Fi мережа складу №3 кількістю 10 адрес;
- Serv – підмережа серверного обладнання. З метою підвищення безпеки та зручного формування ACL-списків доступу вирішено сервер ізолювати в окрему підмережу, яка розрахована на дві адреси – сам сервер та шлюз;
- VPN1, VPN2 та VPN3 – віртуальні підмережі VPN-тунелів між головним офісом та підмережами складів відповідно №1, №2 та №3. Відповідно до принципів VPN ці мережі організовані за принципом “точка-точка” і включають лише по дві IP-алреси;

- VPN4, VPN5 та VPN6 – віртуальні підмережі резервних VPN-тунелів, організованих через канал з'єднання із резервним Інтернет-провайдером між головним офісом та підмережами складів відповідно №1, №2 та №3. Які і в попередньому випадку включають лише по дві IP-алреси.

Оскільки, кожна із підмереж включає різну кількість кінцевих вузлів, то класичний поділ на рівні за розміром підмережі буде не економних щодо використання адресного простору. Із цієї причини вирішено використати технологію масок змінної довжини VLSM. Маршрутизатори Cisco працюватимуть швидше, бо замість десятків дрібних записів вони оперуватимуть одним компактним блоком адрес для цілої філії. Крім цього, використання безкласової адресації та VLSM дозволяє нам у будь-який момент додати нову групу пристроїв (наприклад, розумні датчики на складі чи нову систему контролю вантажівок), не переробляючи всю схему IP-адресації з нуля.

При проектуванні за методом VLSM спочатку необхідно відсортувати мережі за спаданням кількості вузлів від найбільшої до найменшої, це дозволяє уникнути накладання адрес та забезпечує логічну структуру.

Для розподілу на адресного простору використовується наступний алгоритм [5]:

- визначити кількість необхідних адрес для кожного сегмента (враховуючи пристрої, додаткову адресу для шлюз, через який здійснюється вихід із підмережі (призначається відповідному інтерфейсу маршрутизатора), широкомовну адресу та адресу самої підмережі). Разом три додаткові адреси;
- посортувати перелік підмереж у порядку спадання необхідної кількості адрес;
- підібрати найменшу можливу маску, яка покриває цю кількість;
- розрахувати діапазони, вказавши адресу підмережі, після якої діапазон адрес вузлів і остання адреса – широкосмугова. Для зручності складання таблиць адресації останню адресу діапазону буде виділено як адресу шлюзу.

В таблиці 2.1 представлено посортований у порядку спадання кількості адрес список підмереж мережі та обчислення значення мережевої маски.

Таблиця 2.1 – Обчислення маски підмереж

№	Підрозділ / Сегмент	Назва VLAN	Кількість адрес для підмекрежі	Кількість біт в адресі для хостів	Обчислення маски	Значення маски
1	2	3	4	5	6	7
1	Склад №1 (ПК+ТЗД)	Sklad_1	15+3=18	5	2^5=32 > 18 24+(8-5)=27	/27
2	Відділ логістики	Logist	12+3=15	4	2^4=16 > 15 24+(8-4)=28	/28
3	Склад №2 (ПК+ТЗД)	Sklad_2	12+3=15	4	2^4=16 > 15 24+(8-4)=28	/28
4	Склад №3 (ПК+ТЗД)	Sklad_3	10+3=13	4	2^4=16 > 13 24+(8-4)=28	/28
5	Гостьовий Wi-Fi Офіс	Guest_G	10+3=13	4	2^4=16 > 13 24+(8-4)=28	/28
6	Гостьовий Wi-Fi Склад 1	Guest_1	10+3=13	4	2^4=16 > 13 24+(8-4)=28	/28
7	Гостьовий Wi-Fi Склад 2	Guest_2	10+3=13	4	2^4=16 > 13 24+(8-4)=28	/28
8	Гостьовий Wi-Fi Склад 3	Guest_3	10+3=13	4	2^4=16 > 13 24+(8-4)=28	/28
9	Відділ клієнтів	Clients	7+3=10	4	2^4=16 > 10 24+(8-4)=28	/28
10	Адміністрація	Admin	5+3=8	4	2^4=16 > 8 24+(8-4)=28	/28
11	Бухгалтерія	Finansy	4+3=10	3	2^3=8 > 7 24+(8-3)=29	/29
12	Камери Головний офіс	Cam_G	4+3=10	3	2^3=8 > 7 24+(8-3)=29	/29

Продовження таблиці 2/1

1	2	3	4	5	6	7
13	Камери Склад 1	Cam_1	4+3=10	3	2^3=8 > 7 24+(8-3)=29	/29
14	Камери Склад 2	Cam_2	4+3=10	3	2^3=8 > 7 24+(8-3)=29	/29
15	Камери Склад 3	Cam_3	4+3=10	3	2^3=8 > 7 24+(8-3)=29	/29
16	IT-відділ	IT	2+3=5	3	2^3=8 > 5 24+(8-3)=29	/29
17	VPN-мережі	VPN1–VPN6	2+2=4	2	2^2=4 ≥ 2 24+(8-2)=30	/30

Відповідно до обчисленої в таблиці 2.1 мережевої маски на наступному кроці алгоритму послідовно розрахуємо адреси підмереж, вузлів, шлюзів та бродкестів. Результати розрахунку представлено в таблицях 2.2 та 2.3.

Таблиця 2.2 – План IP-адресації підрозділів мережі логістичної компанії “Global-Express”

Назва підмер.	Адреса підмережі	Маска	Діапазон адрес вузлів	Шлюз	Широкосмугова адреса
1	2	3	6	7	8
Sklad_1	192.168.0.0 /27	255.255.255.224	192.168.0.1 – 192.168.0.29	192.168.0.30	192.168.0.31
Logist	192.168.0.32 /28	255.255.255.240	192.168.0.33 – 192.168.0.45	192.168.0.46	192.168.0.47
Sklad_2	192.168.0.48 /28	255.255.255.240	192.168.0.49 – 192.168.0.61	192.168.0.62	192.168.0.63
Sklad_3	192.168.0.64 /28	255.255.255.240	192.168.0.65 – 192.168.0.77	192.168.0.78	192.168.0.79
Guest_G	192.168.0.80 /28	255.255.255.240	192.168.0.81 – 192.168.0.93	192.168.0.94	192.168.0.95
Guest_1	192.168.0.96 /28	255.255.255.240	192.168.0.97 – 192.168.0.109	192.168.0.110	192.168.0.111

Продовження таблиці 2.2

1	2	3	6	7	8
Guest_2	192.168.0.112 /28	255.255.255.240	192.168.0.113– 192.168.0.125	192.168.0.126	192.168.0.127
Guest_3	192.168.0.128 /28	255.255.255.240	192.168.0.129– 192.168.0.141	192.168.0.142	192.168.0.143
Clients	192.168.0.144 /28	255.255.255.240	192.168.0.145– 192.168.0.157	192.168.0.158	192.168.0.159
Admin	192.168.0.160 /28	255.255.255.240	192.168.0.161– 192.168.0.173	192.168.0.174	192.168.0.175
Finansy	192.168.0.176 /29	255.255.255.248	192.168.0.177– 192.168.0.181	192.168.0.182	192.168.0.183
Cam_G	192.168.0.184 /29	255.255.255.248	192.168.0.185– 192.168.0.189	192.168.0.190	192.168.0.191
Cam_1	192.168.0.192 /29	255.255.255.248	192.168.0.193– 192.168.0.197	192.168.0.198	192.168.0.199
Cam_2	192.168.0.200 /29	255.255.255.248	192.168.0.201– 192.168.0.205	192.168.0.206	192.168.0.207
Cam_3	192.168.0.208 /29	255.255.255.248	192.168.0.209– 192.168.0.213	192.168.0.214	192.168.0.215
IT	192.168.0.216 /29	255.255.255.248	192.168.0.217– 192.168.0.221	192.168.0.222	192.168.0.223
Serv	192.168.0.224 /30	255.255.255.252	192.168.0.225	192.168.0.226	192.168.0.227

Таблиця 2.3 – План IP-адресації підмереж VPN-тунелів мережі логістичної компанії “Global-Express”

Назва підмер.	Адреса підмережі	Маска	Адреса VPN-клієнта	Адреса VPN-сервера	Широкосму-гова адреса
VPN1	192.168.0.228 /30	255.255.255.252	192.168.0.229	192.168.0.230	192.168.0.231
VPN2	192.168.0.232 /30	255.255.255.252	192.168.0.233	192.168.0.234	192.168.0.235
VPN3	192.168.0.236 /30	255.255.255.252	192.168.0.237	192.168.0.238	192.168.0.239
VPN4	192.168.0.240 /30	255.255.255.252	192.168.0.241	192.168.0.242	192.168.0.243
VPN5	192.168.0.244 /30	255.255.255.252	192.168.0.245	192.168.0.246	192.168.0.247
VPN6	192.168.0.248 /30	255.255.255.252	192.168.0.249	192.168.0.250	192.168.0.251

Виділення окремих адресних блоків для основних та резервних VPN-тунелів створює базу для налаштування динамічної маршрутизації, що гарантує безперебійний зв'язок між Головним офісом та складськими терміналами навіть у разі відмови одного з каналів зв’язку.

2.9 Тестування та налагодження мережі

Після завершення монтажних робіт та програмної конфігурації активного обладнання проводиться поетапна перевірка працездатності мережі «Global-Express». Метою цієї фази розробки є виявлення можливих помилок у комутації, підтвердження коректності маршрутизації та перевірка систем безпеки. Процес тестування та налагодження мережі включає декілька етапів.

На етапі тестування структурованої кабельної системи здійснюється верифікація кожної кабельної лінії Cat 6 від комутаційних шаф у серверній до кінцевих точок підключення в офісах та на складах. Використання професійних кабельних аналізаторів дозволяє не лише підтвердити відсутність розривів чи перехресних наведень, а й сертифікувати кожну лінію на відповідність стандарту Gigabit Ethernet. Окрему увагу приділяють перевірці бюджету потужності PoE (Power over Ethernet), що вкрай важливо для стабільного живлення камер Reolink та точок доступу TP-Link, особливо на віддалених ділянках складських приміщень, де велика довжина кабелю.

Після підтвердження цілісності фізичного рівня переходяться до налагодження логічної структури та верифікації розробленого плану адресації VLSM. На маршрутизаторах Cisco ISR проводиться конфігурація інтерфейсів та субінтерфейсів для кожної з підмереж, після чого виконується тестування внутрішньої маршрутизації між VLAN. Процес налагодження включає перевірку роботи DHCP-серверів, які повинні коректно видавати IP-адреси пристроям у межах їхніх функціональних груп (наприклад, термінали збору даних на Складі №1 мають отримувати адреси виключно з діапазону 192.168.0.10 – 192.168.0.29). За допомогою утиліт діагностики трафіку, таких як Traceroute та розширений Ping,

відстежується шлях проходження пакетів, що дозволяє переконатися у відсутності петель маршрутизації та коректній роботі шлюзів за замовчуванням.

Дуже важливим етапом налагодження є конфігурація та тестування захищених VPN-тунелів, що об’єднують головний офіс із віддаленими складами. Оскільки проєкт передбачає наявність основних та резервних каналів зв’язку (VPN1 – VPN6), особлива увага приділяється механізмам відмовостійкості та динамічного перемикання маршрутів. Під час тестування імітуються аварійні ситуації, такі як обрив каналу від основного провайдера, для перевірки швидкості реакції маршрутизатора та автоматичного підняття резервного тунелю. Успішним результатом вважається збереження активних сесій у логістичній базі даних та мінімальна затримка при передачі відеопотоку з камер спостереження віддалених філій, що підтверджує надійність криптографічного захисту та стабільність тунелів з маскою /30.

Завершальна стадія налагодження зосереджена на оптимізації бездротового середовища та впровадженні політик безпеки. Виконуючи радіообстеження (Site Survey) на території складів, інженери аналізують зони перекриття сигналу точок доступу TP-Link EAP225 для забезпечення безшовного роумінгу. Це гарантує, що комірники з мобільними сканерами зможуть безперервно працювати під час переміщення між стелажами, автоматично перемикаючись між точками доступу без розриву зв'язку.

Паралельно з цим проводиться аудит налаштованих списків контролю доступу (ACL). Шляхом спроб несанкціонованого сканування мережі з гостьових Wi-Fi зон перевіряється ефективність ізоляції серверної підмережі та бухгалтерії. Лише після того, як кожен сегмент мережі демонструє повну відповідність матриці доступів та вимогам продуктивності, складається підсумковий протокол тестування, і мережа передається в промислову експлуатацію.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування комутації та маршрутизації між VLAN

3.2.1 Інструкції з конфігурування комутаторів рівня доступу

Конфігурування комутаторів рівня доступу є важливим етапом, що забезпечує фізичне розділення мережі на функціональні підмережі (VLAN) згідно з розробленою структурою підрозділів та планом IP-адресації. Процес налаштування розпочинається з базової ініціалізації пристрою, яка включає встановлення імені хоста, паролів доступу до консолі та режиму привілейованого доступу, а також налаштування IP-адреси управління в спеціальному сегменті для IT-відділу. Це дозволяє адміністраторам здійснювати подальший моніторинг та керування обладнанням дистанційно через захищений протокол SSH, мінімізуючи необхідність фізичної присутності в серверній кімнаті чи на віддалених складах.

Процес налаштування розпочинається з комутатора Sw_G_1, розміщеного в серверній кімнаті головного офісу. Даний пристрій є вузловим для забезпечення мережевої зв’язності підрозділів адміністрації (VLAN Admin) та транспортної логістики (VLAN Logist), згідно з розробленою топологією (Додаток В).

На початковому етапі організовується консольний доступ до пристрою з подальшою активацією режиму користувача. Процедура присвоєння мережевого імені (hostname) для ідентифікації вузла здійснюється згідно з лістингом команд, представленим на рисунку 3.1.

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#hostname Sw_G_1
Sw_G_1(config)#
```

Рисунок 3.1 – Присвоєння мережевого імені комутатора

Далі необхідно реалізувати комплексну систему розмежування прав доступу. Для запобігання несанкціонованому втручанню в роботу комутатора

впроваджується багаторівнева модель безпеки, що охоплює основні вектори входу до системи керування:

- захист локального термінала (Console port). Встановлення пароля на фізичний інтерфейс управління дозволяє контролювати доступ безпосередньо в серверній кімнаті, блокуючи спроби входу через консольний кабель;

- контроль дистанційного керування (VTY lines). Налаштування паролів для віртуальних ліній є обов'язковим для фільтрації віддалених сесій адміністрування (через протоколи SSH/Telnet), що забезпечує безпечне керування обладнанням через локальну мережу;

- авторизація привілейованого режиму (Enable mode). Цей рівень захисту є дуже важливим, оскільки він обмежує доступ до команд зміни системної конфігурації та перегляду чутливих даних;

- криптографічне приховування паролів. Використання функції глобального шифрування (service password-encryption) дозволяє перетворити всі паролі, що зберігаються у текстовому вигляді, на хешовані послідовності. Це нівелює ризик компрометації облікових даних при перегляді конфігураційних файлів сторонніми особами.

Особлива увага приділяється захисту доступу до режиму розширених прав. Відповідно до сучасних стандартів мережевої безпеки, пріоритетним є використання команди enable secret. На відміну від застарілих методів, дана команда за замовчуванням застосовує стійкі алгоритми хешування (наприклад, MD5 або SHA-256), що робить пароль практично неможливим для зворотного декодування.

Технічна реалізація захисту фізичного консольного порту передбачає перехід до спеціалізованого режиму конфігурування ліній (line console 0). Після призначення секретного коду за допомогою директиви password, важливим є застосування команди login. Саме вона активує механізм автентифікації, ініціюючи запит пароля при кожній спробі встановлення сесії.

Наочне представлення синтаксису команд та послідовність налаштування привілейованого доступу разом із консольним інтерфейсом наведено у лістингу на рисунку 3.2.

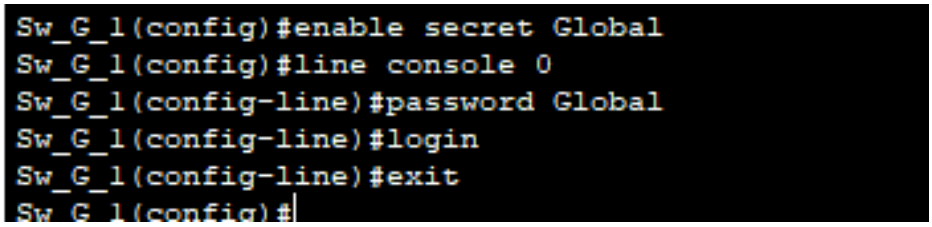


Рисунок 3.3 – Налаштування паролю на привілейований режим

Реалазіація безпеки при віддаленому адмініструванні комутатора через мережеві протоколи (SSH або Telnet) базується на регламентації доступу до віртуальних термінальних ліній – VTY (Virtual Teletype). Ці логічні інтерфейси виконують функцію первинного захисту, запобігаючи несанкціонованим спробам входу до операційної системи пристрою через зовнішні цифрові канали.

Сучасне мережеве обладнання Cisco підтримує багатокористувацьку модель управління, що реалізується шляхом активації групи ліній (зазвичай у діапазоні 0 –15). Такий підхід дозволяє організувати паралельні сесії для кількох адміністраторів одночасно.

Для активації захисту на віртуальних інтерфейсах виконується перехід до режиму групового конфігурування ліній. Основним етапом є призначення стійкої парольної комбінації та обов'язкове застосування директиви login, яка ініціює перевірку облікових даних при кожному запиті на встановлення сесії. Варто зазначити, що для максимального рівня безпеки в корпоративних мережах рекомендується надавати перевагу протоколу SSH, оскільки він, на відміну від Telnet, забезпечує повне шифрування трафіку адміністрування. Telnet передає автентифікаційні дані та системні команди у відкритому текстовому вигляді, що робить їх легкою ціллю для перехоплення (sniffing). Тому, важливим етапом налаштування захисту є повне виключення можливості доступу до пристрою через сервіси Telnet. Для цього використовується команда transport input ssh, яка виконує роль фільтра на рівні віртуальних термінальних ліній (VTY) та чітко визначаючи перелік дозволених протоколів для встановлення сесій дистанційного керування. В даному випадку лише SSH.

Для підвищення загального рівня безпеки та захисту конфіденційної інформації в системі використовується глобальна директива service password-encryption. Її функціональне призначення полягає в автоматичній зміні формату зберігання всіх паролів у поточному конфігураційному файлі пристрою (running-config).

Замість вразливого відкритого тексту, який може бути легко прочитаний при випадковому перегляді екрана або несанкціонованому доступі до файлів конфігурації, команда перетворює паролі на зашифровані хеш-послідовності. Це створює додатковий бар'єр безпеки, унеможливлюючи пряме копіювання облікових даних з налаштувань ліній VTY, консолі чи паролів привілейованого доступу.

Вичерпний перелік команд, необхідних для розгортання парольного захисту на інтерфейсах віддаленого доступу, а також приклад їх синтаксису, наведено у лістингу на рисунку 3.3.

```
Sw_G_1(config)# line vty 0 15
Sw_G_1(config-line)#password Global
Sw_G_1(config-line)#login
Sw_G_1(config-line)#transport input ssh
Sw_G_1(config-line)#exit
Sw_G_1(config)#service password-encryption
Sw_G_1(config)#
```

Рисунок 3.3 – Налаштування парольного захисту на відділений доступ по SSH

У даній інструкції для ілюстрації процесу конфігурування використано демонстраційний пароль «Global». Проте для впровадження системи у реальне виробниче середовище логістичного центру цей параметр має бути замінений на криптостійку комбінацію символів.

Останнім кроком у побудові системи захищеного управління є створення локального облікового запису адміністратора. Це необхідно для коректної роботи протоколу SSH, який вимагає обов'язкової автентифікації користувача за логіном та паролем. Процес передбачає генерацію локальної бази даних у пам'яті комутатора, що дозволяє індивідуалізувати доступ до обладнання.

Конкретний синтаксис команд для створення користувача з відповідними рівнями привілеїв та послідовність кроків для активації SSH-авторизації детально візуалізовано на рисунку 3.4.

```
Sw_G_1(config)# username root privilege 15 secret Global
Sw_G_1(config)#ip domain name globalexpress.local
Sw_G_1(config)#crypto key generate rsa
The name for the keys will be: Sw_G_1.globalexpress.local
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 512
% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

Sw_G_1(config)#
```

Рисунок 3.4 – Створення користувача для віддаленого доступу

Після налаштування аутентифікації можна приступати до розгортання ієрархічної структури віртуальних локальних мереж (VLAN) на комутаційному обладнанні.

Процес конфігурування полягає у створенні логічних сегментів, що чітко відповідають організаційній структурі та плану адресації «Global-Express», представленому в таблицях 2.2 та 2.3. Це дозволяє не лише впорядкувати мережевий трафік, а й забезпечити суворе розмежування потоків даних між функціональними підрозділами компанії, мінімізуючи ризики несанкціонованого міжсегментного обміну інформацією. Також, він гарантує, що трафік від систем відеоспостереження або гостьових бездротових точок доступу залишатиметься в межах своїх логічних кордонів, не створюючи надлишкового навантаження на канали зв'язку критично важливих бізнес-підрозділів.

Кожен сегмент отримує унікальний числовий ідентифікатор (VLAN ID) та описову назву, що спрощує подальший моніторинг та адміністрування мережі. Повний перелік ідентифікаторів, закріплених за конкретними структурними підрозділами, а також їхнє територіальне розміщення згідно з планами, систематизовано у таблиці 3.1 та додатку В.

Таблиця 3.1 – Ідентифікатори віртуальних підмереж

Назва VLAN	VLAN ID	Назва VLAN	VLAN ID
Sklad_1	101	Admin	110
Logist	102	Finansy	111
Sklad_2	103	Cam_G	112
Sklad_3	104	Cam_1	113
Guest_G	105	Cam_2	114
Guest_1	106	Cam_3	115
Guest_2	107	IT	116
Guest_3	108	Serv	117
Clients	109		

Процес розгортання логічної структури на комутаційному обладнанні розпочинається з переходу до режиму глобального конфігурування. Безпосереднє створення нового мережевого сегмента реалізується через активацію директиви vlan <ID>, де ключовим аргументом виступає унікальний числовий ідентифікатор, заздалегідь визначений у плані адресації представленому у таблиці 3.1. Кожен такий ідентифікатор відповідає окремому підрозділу або функціональній зоні логістичного підприємства.

Для спрощення подальшої експлуатації мережі, проведення діагностики та швидкої ідентифікації трафіку в консолі керування, кожній віртуальній мережі присвоюється змістовна текстова мітка за допомогою команди name. Це дозволяє адміністратору миттєво розрізняти потоки даних між різними відділами, уникаючи плутанини з цифровими індексами.

Повна послідовність операцій з ініціалізації та іменування сегментів на прикладі комутатора Sw_G_1, детально візуалізовано у лістингу команд представленому на рисунку 3.5.

Після завершення етапу формування віртуальних мереж (VLAN) критично важливим є коректне визначення функціональних ролей кожного фізичного порту комутатора. Це забезпечує правильну обробку трафіку та дотримання політик ізоляції.

```
Sw_G_1(config)#vlan 101
Sw_G_1(config-vlan)#name Sklad_1
Sw_G_1(config-vlan)#vlan 102
Sw_G_1(config-vlan)#name Logist
Sw_G_1(config-vlan)#vlan 103
Sw_G_1(config-vlan)#name Sklad_2
Sw_G_1(config-vlan)#vlan 104
Sw_G_1(config-vlan)#name Sklad_3
Sw_G_1(config-vlan)#vlan 105
Sw_G_1(config-vlan)#name Guest_G
Sw_G_1(config-vlan)#vlan 106
Sw_G_1(config-vlan)#name Guest_1
Sw_G_1(config-vlan)#vlan 107
Sw_G_1(config-vlan)#name Guest_2
Sw_G_1(config-vlan)#vlan 108
Sw_G_1(config-vlan)#name Guest_3
Sw_G_1(config-vlan)#vlan 109
Sw_G_1(config-vlan)#name Clients
Sw_G_1(config-vlan)#vlan 110
Sw_G_1(config-vlan)#name Admin
Sw_G_1(config-vlan)#vlan 111
Sw_G_1(config-vlan)#name Finansy
Sw_G_1(config-vlan)#vlan 112
Sw_G_1(config-vlan)#name Cam_G
Sw_G_1(config-vlan)#vlan 113
Sw_G_1(config-vlan)#name Cam_1
Sw_G_1(config-vlan)#vlan 114
Sw_G_1(config-vlan)#name Cam_2
Sw_G_1(config-vlan)#vlan 115
Sw_G_1(config-vlan)#name Cam_3
Sw_G_1(config-vlan)#vlan 116
Sw_G_1(config-vlan)#name IT
Sw_G_1(config-vlan)#vlan 117
Sw_G_1(config-vlan)#name Serv
```

Рисунок 3.5 – Створення бази даних VLAN на комутаторі Sw_G_1

У розробленій мережевій архітектурі «Global-Express» використовуються два базові типи логічних інтерфейсів [3]:

- порти доступу (Access-ports) – призначені для підключення кінцевого периферійного обладнання. Кожен такий порт жорстко закріплюється за однією конкретною VLAN, що гарантує потрапляння пристрою у відповідний сегмент;
- магістральні порти (Trunk-ports) – відіграють роль агрегаційних каналів і використовуються для під'єднання комутаторів до маршрутизатора Cisco ISR. Головною особливістю транкових портів є підтримка інкапсуляції IEEE 802.1Q, що дозволяє передавати трафік усіх наявних VLAN через один фізичний кабель.

Керуючись схемою топології (див. додаток Б), налаштування інтерфейсів комутатора Sw_G_1 проводиться в режимі глобальної конфігурації. Деталізований лістинг команд, що застосовувалися для програмування інтерфейсів Sw_G_1, представлений у графічній формі на рисунку 3.6.

```
Sw_G_1(config)#interface range gigabitethernet1/0/1-gigabitethernet1/0/21
Sw_G_1(config-if-range)#switchport mode access
Sw_G_1(config-if-range)#interface gigabitethernet1/0/1
Sw_G_1(config-if)#switchport access vlan 117
Sw_G_1(config-if)#interface range gigabitethernet1/0/2-gigabitethernet1/0/3
Sw_G_1(config-if-range)#switchport access vlan 116
Sw_G_1(config-if-range)#interface range gigabitethernet1/0/4-gigabitethernet1/0/8
Sw_G_1(config-if-range)#switchport access vlan 110
Sw_G_1(config-if-range)#interface range gigabitethernet1/0/9-gigabitethernet1/0/21
Sw_G_1(config-if-range)#switchport access vlan 102
Sw_G_1(config-if-range)#interface gigabitethernet1/1/1
Sw_G_1(config-if)#switchport mode trunk
Sw_G_1(config-if)#switchport trunk allowed vlan 102,110,116,117
Sw G 1(config-if)#exit
```

Рисунок 3.6 – Налаштування інтерфейсів комутатора Sw1

Додатковий рівень захисту мережі на другому рівні моделі OSI (Layer 2) реалізується за допомогою технології Port Security. Даний інструментарій дозволяє жорстко регламентувати доступ до мережевих ресурсів на основі унікальних фізичних MAC-адрес кінцевих пристроїв. Впровадження цієї технології нівелює ризики, пов'язані з несанкціонованим фізичним підключенням стороннього обладнання до вільних або робочих портів у офісних та складських приміщеннях.

Процедура активації та детальний синтаксис команд для налаштування режимів безпеки на інтерфейсах доступу наведені на рисунку 3.7.

```
Sw_G_1(config-if-range)#interface range gigabitethernet1/0/1-gigabitethernet1/0/21
Sw_G_1(config-if-range)#switchport port-security
Sw_G_1(config-if-range)#switchport port-security maximum 1
Sw_G_1(config-if-range)#switchport port-security mac-address sticky
Sw_G_1(config-if-range)#switchport port-security violation shutdown
Sw_G_1(config-if-range)#exit
```

Рисунок 3.7 – Налаштування захисту портів

Даний блок команд встановлює обмеження кількість дозволеної кількості MAC-адрес до одного пристрою на порт (maximum 1), дозволяє комутатору динамічно вивчати адресу підключеного пристрою і автоматично записувати її в поточний конфігураційний файл (метод sticky) та автоматично блокує порт у випадку доступу іншої MAC-адреси (режим shutdown).

Після успішного відпрацювання алгоритму налаштування інтерфейсів на комутаторі Sw_G_1, аналогічний комплекс операцій реалізується для всіх інших комутаторів рівня доступу, включаючи пристрої Sw_G_2, Sw_1, Sw_2 та Sw_3.

Для забезпечення прозорості адміністрування та запобігання помилкам при фізичному підключенні обладнання, в таблиці 3.2 наведено зведену специфікацію розподілу інтерфейсів.

Таблиця 3.2 – Налаштування інтерфейсів комутаторів рівня доступу

Комутатор	Інтерфейси комутатора	Режими портів	Команда визначення інтерфейсу
Sw_G_1	Gig1/0/1	access	switchport access vlan 117
	Gig1/0/2 – Gig1/0/3	access	switchport access vlan 116
	Gig1/0/4 – Gig1/0/8	access	switchport access vlan 110
	Gig1/0/9 – Gig1/0/21	access	switchport access vlan 102
	Gig1/1/1	trunk	switchport trunk allowed vlan 102,110,116,117
Sw_G_2	Gig1/0/1 – Gig1/0/4	access	switchport access vlan 111
	Gig1/0/5 – Gig1/0/11	access	switchport access vlan 109
	Gig1/0/12–Gig1/0/15	access	switchport access vlan 112
	Gig1/0/16	access	switchport access vlan 105
	Gig1/1/1	trunk	switchport trunk allowed vlan 105,109,111,112
Sw_1	Gig1/0/1 – Gig1/0/5	access	switchport access vlan 101
	Gig1/0/6 – Gig1/0/9	access	switchport access vlan 113
	Gig1/0/10–Gig1/0/12	access	switchport access vlan 106
	Gig1/1/1	trunk	switchport trunk allowed vlan 101,106,113
Sw_2	Gig1/0/1 – Gig1/0/4	access	switchport access vlan 103
	Gig1/0/5 – Gig1/0/8	access	switchport access vlan 114
	Gig1/0/9–Gig1/0/11	access	switchport access vlan 107
	Gig1/1/1	trunk	switchport trunk allowed vlan 103,107,114
Sw_3	Gig1/0/1 – Gig1/0/3	access	switchport access vlan 104
	Gig1/0/4 – Gig1/0/7	access	switchport access vlan 115
	Gig1/0/8–Gig1/0/11	access	switchport access vlan 108
	Gig1/1/1	trunk	switchport trunk allowed vlan 104,108,115

Заключним кроком у процесі налаштування комутаторів є перенесення поточної конфігурації з оперативної пам'яті (RAM) до енергонезалежного сховища (NVRAM) командою wr.

3.2.2 Інструкції з налаштування машртутизації між VLAN

Завершальною стадією базової підготовки активної мережевої інфраструктури є конфігурування маршрутизатора. Цей вузол відіграє роль центрального шлюзу для віртуальних локальних мереж (VLAN) у межах головного офісу та територіально розподілених складів, забезпечуючи безперебійну маршрутизацію трафіку між ізольованими сегментами мережі.

Підготовка маршрутизатора розпочинається з його системної ініціалізації: присвоєння унікального мережевого ідентифікатора (hostname), впровадження комплексної політики парольного захисту та генерації локального облікового запису для організації захищених сесій віддаленого адміністрування за протоколом SSH. Алгоритм виконання цих безпекових налаштувань є тотожним до процесу конфігурування комутаторів рівня доступу (відповідні лістинги команд наведено на рисунках 3.1–3.4).

Після затвердження параметрів доступу здійснюється перехід до налаштування логічної маршрутизації. Цей процес передбачає розділення одного магістрального фізичного інтерфейсу на кілька віртуальних субінтерфейсів. Кожен із них закріплюється за окремою VLAN та починає функціонувати як шлюз за замовчуванням для відповідної складської чи офісної підмережі. Детальний синтаксис команд для розгортання субінтерфейсів на прикладі маршрутизатора Складу №1 проілюстровано на рисунку 3.8.

```
R_1(config)#interface gigabitethernet0/0/0
R_1(config-if)#interface gigabitethernet0/0/0.101
R_1(config-subif)#encapsulation dotlq 101
R_1(config-subif)#ip address 192.168.0.30 255.255.255.224
R_1(config-subif)#no shutdown
R_1(config-subif)#interface gigabitethernet0/0/0.113
R_1(config-subif)#encapsulation dotlq 113
R_1(config-subif)#ip address 192.168.0.198 255.255.255.248
R_1(config-subif)#no shutdown
R_1(config-subif)#interface gigabitethernet0/0/0.106
R_1(config-subif)#encapsulation dotlq 106
R_1(config-subif)#ip address 192.168.0.109 255.255.255.240
R_1(config-subif)#no shutdown
R_1(config-subif)#exit
```

Рисунок 3.8 – Налаштування віртуальних підінтерфейсів маршрутизатора

Процес забезпечення маршрутизації між ізольованими віртуальними мережами базується на логічному розділенні одного фізичного порту на декілька віртуальних каналів (субінтерфейсів). Ініціалізація такого логічного шлюзу здійснюється за допомогою команди “interface <тип_інтерфейсу>.<VLAN_ID>”.

Важливим етапом, який передує призначенню мережевої адреси, є активація механізму розпізнавання тегованого трафіку. Для цього на кожному субінтерфейсі застосовується директива “encapsulation dot1Q <VLAN_ID>”. Вона вказує маршрутизатору стандарт інкапсуляції пакетів (IEEE 802.1Q), що дозволяє коректно обробляти дані, які надходять від комутаторів. Лише після цього віртуальному інтерфейсу присвоюється роль шлюзу за замовчуванням за допомогою команди “ip address <адреса> <маска>’. Відповідні IP-адреси шлюзів та ідентифікатори віртуальних мереж інтегруються згідно з розробленими раніше таблицями 2.2 та 3.1.

Аналогічні налаштування необхідно здійснити на інших маршрутизаторах мережі. Необхідно лише врахувати, що для маршрутизатора R_G використовується два фізичні інтерфейси: GigabitEthernet0/0/0, для створення підінтерфейсів “.102”, “.110”, “.116”, “.117” та GigabitEthernet0/0/1 – “.105”, “.109”, “.111”, “.112”. Повна специфікація створених логічних шлюзів для всієї мережі систематизована у таблиці 3.3.

Таблиця 3.3 – Налаштування віртуальних підінтерфейсів маршрутизаторів

Назва	Підінтерфейси	Команда encapsulation dot1q	Команда ip address
1	2	3	4
R_1	GigabitEthernet0/0/0.101	101	192.168.0.30 255.255.255.224
	GigabitEthernet0/0/0.106	106	192.168.0.109 255.255.255.240
	GigabitEthernet0/0/0.113	113	192.168.0.234 255.255.255.224
R_2	GigabitEthernet0/0/0.103	103	192.168.0.94 255.255.255.224
	GigabitEthernet0/0/0.107	107	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/0.114	114	192.168.0.234 255.255.255.224

Продовження таблиці 3.3

1	2	3	4
R_3	GigabitEthernet0/0/0.104	104	192.168.0.126 255.255.255.224
	GigabitEthernet0/0/0.108	108	192.168.0.158 255.255.255.224
	GigabitEthernet0/0/0.115	115	192.168.0.234 255.255.255.224
R_G	GigabitEthernet0/0/0.102	102	192.168.0.46 255.255.255.240
	GigabitEthernet0/0/0.110	110	192.168.0.174 255.255.255.240
	GigabitEthernet0/0/0.116	116	192.168.0.222 255.255.255.248
	GigabitEthernet0/0/0.117	117	192.168.0.226 255.255.255.248
	GigabitEthernet0/0/1.105	105	192.168.0.94 255.255.255.240
	GigabitEthernet0/0/1.109	109	192.168.0.158 255.255.255.240
	GigabitEthernet0/0/1.111	111	192.168.0.182 255.255.255.248
	GigabitEthernet0/0/1.112	112	192.168.0.190 255.255.255.248

Для забезпечення автоматичної IP-адресації клієнтів у бездротових сегментах мережі, на відповідних віртуальних субінтерфейсах необхідно налаштувати функцію перенаправлення DHCP-запитів. Оскільки маршрутизатори за замовчуванням блокують широкомовний (broadcast) трафік, запити від нових пристроїв не зможуть самостійно досягти сервера конфігурації, якщо він знаходиться в іншій підмережі.

Згідно з архітектурою проєкту, роль централізованого DHCP-сервера виконує виділений вузол на базі операційної системи Microsoft Windows Server 2025, якому призначено статичну IP-адресу 192.168.0.225. Вказування цієї адреси на логічних шлюзах бездротових мереж дозволяє маршрутизатору інкапсулювати широкомовні запити клієнтів в одноадресні (unicast) пакети та направляти їх безпосередньо до сервера. Приклад синтаксису для налаштування адреси DHCP-сервера на маршрутизаторі R_1 проілюстровано на рисунку 3.9.

```
R_1(config)#interface gigabitethernet0/0/0.106
R_1(config-subif)#ip helper-address 192.168.0.225
```

Рисунок 3.9 – Встановлення адреси DHCP-сервера на шлюзі маршрутизатора

Ангалогічні команди слід ввести на віртуальних підінтерфейсах:

– GigabitEthernet0/0/0.107 маршрутизатора R_2;

– GigabitEthernet0/0/0.108 маршрутизатора R_3;

– GigabitEthernet0/0/0.102 та GigabitEthernet0/0/1.105 маршрутизатора R_G.

3.2 Інструкції з налаштування сервера мережі

3.2.1 Інструкції з розгортання та налаштування доменного контролера

Для створення єдиного середовища керування користувачами, впровадження групових політик (GPO) та розмежування прав доступу до мережевих ресурсів логістичної компанії реалізується доменна архітектура. Функції головного контролера домену (DC) покладено на серверну платформу Microsoft Windows Server 2025. Процес розгортання розпочинається з базової підготовки операційної системи, а подальше управління всіма сервісами та ролями здійснюється через інтегровану консоль Server Manager (див. рис. 3.10).

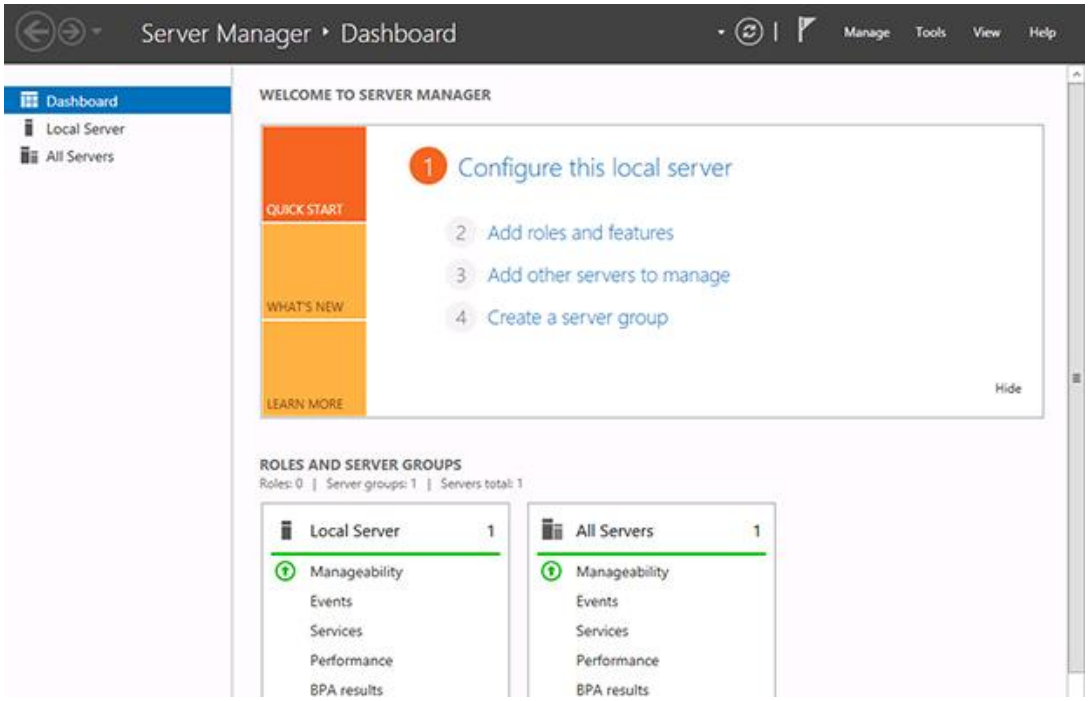


Рисунок 3.10 – Вікно Server Manger

Оскільки функціонування служб каталогів AD DS нерозривно пов'язане з системою доменних імен (DNS) для коректної локалізації ресурсів, даний сервер суміщатиме ролі контролера домену та внутрішнього DNS-вузла. Перед інсталяцією відповідних ролей необхідно виконати налаштування:

– серверу призначається статична IP-адреса 192.168.0.225 та шлюз 192.168.0.225 із маскою 255.255.255.248 відповідно до плану адресації, представленого в таблиці 2.2;

– у параметрах IPv4 як основний DNS-сервер вказується Loopback-адреса (127.0.0.1). Це дозволяє системі звертатися до власної бази даних для реєстрації та пошуку службових записів Active Directory. Для забезпечення доступу до зовнішніх мережевих ресурсів як альтернативний DNS вказується публічний вузол 8.8.8.8;

– з метою дотримання проєктної документації, системне ім'я сервера змінюється з автоматично згенерованого на Serv.

Процес перетворення сервера на контролер домену розпочинається з інсталяції необхідних компонентів через майстер Add Roles and Features. У розділі вибору ролей активуються служби Active Directory Domain Services (AD DS) та DNS Server. Система автоматично додає до переліку встановлення допоміжні адміністративні інструменти, зокрема оснастки AD та модулі PowerShell, що є критичним для подальшого керування об'єктами мережі.

Після завершення копіювання бінарних файлів у консолі Server Manager ініціюється процедура підвищення ролі сервера (Promote this server to a domain controller). Оскільки мережа логістичного оператора «Global-Express» створюється вперше, у майстрі конфігурації обирається розгортання нового лісу (Add a new forest). Для внутрішньої ідентифікації призначається корінь globalexpress.local. Використання суфікса .local є загальноприйнятим стандартом для приватних корпоративних середовищ, оскільки це унеможливлює конфлікти імен із публічними інтернет-доменами.

Під час налаштування параметрів обрано найвищий функціональний рівень лісу та домену – Windows Server 2025. Це відкриває доступ до сучасних криптог-

рафічних алгоритмів Kerberos та посилених методів захисту автентифікації. Окремо встановлюється пароль режиму відновлення служб каталогів (DSRM), необхідний для аварійної регенерації бази даних NTDS.dit. Попередження про відсутність делегування DNS на етапі перевірки вимог ігнорується, оскільки даний сервер є первинним авторитетним джерелом для своєї зони.

Наступним кроком після перезавантаження сервера є побудова ієрархії об'єктів у консолі Active Directory Users and Computers (ADUC). Для впорядкування ресурсів створюються організаційні підрозділи (Organizational Units – OU), що дозволяють групувати користувачів та обладнання за їхнім функціональним призначенням:

– Administration — для апарату управління та IT-відділу;

– Logistics_Ops — для персоналу, що забезпечує операційну діяльність;

– Accounting — для фінансового департаменту;

– Computers — окремий контейнер для робочих станцій, що дає змогу гнучко застосовувати різні групові політики безпеки до заліза.

Процедура реєстрації персоналу в системі супроводжується дотриманням суворих стандартів безпеки. При створенні облікового запису користувача (User) призначається унікальне ім'я входу (Logon name). На етапі встановлення пароля активується обов'язкова вимога «User must change password at next logon». Це гарантує конфіденційність: адміністратор генерує лише тимчасовий шифр, а користувач створює особистий пароль під час першої авторизації.

Для оптимізації управління правами доступу замість індивідуального призначення привілеїв використовуються Групи безпеки (Security Groups). Зокрема, у відповідних підрозділах створюються групи (наприклад, G_Logistics_Staff) із областю дії Domain Local. Такий підхід дозволяє масштабувати мережу, просто додаючи нових працівників до відповідних груп, які вже мають доступ до необхідних мережевих папок чи принтерів.

Далі необхідно налашутвтаи групи безпеки із обмеженнями окремих групп користувачів до певних ресурсів.

3.2.2 Інструкції з розгортання та налаштування доменного контролера

Хоча основна частина мережевої інфраструктури (сервери, комутатори, принтери) використовує статичну адресацію для забезпечення постійної доступності, робота мобільних сегментів потребує динамічного підходу. Для гостьових Wi-Fi зон, терміналів збору даних комірників та резервних робочих станцій відділу логістики передбачено розгортання ролі DHCP-сервера на базі Windows Server 2025.

Першим кроком є додавання відповідного функціонала до операційної системи. Це робиться через знайомий нам інтерфейс:

– у Server Manager (див. рис. 3.10) потрібно вибрати меню Manage, а в ньому Add Roles and Features;

– у розділі Server Roles відмітити пункт DHCP Server;

– підтвердити встановлення додаткових інструментів керування та завершити роботу майстра.

Після встановлення сервер ще не працює. У верхній частині Server Manager з’явиться жовтий трикутник (сповіщення). Необхідно натиснути на сповіщення та обрати Complete DHCP configuration.

Відкриється майстер, де потрібно натиснути Commit. Це створить дві групи безпеки (DHCP Administrators та DHCP Users) і авторизує сервер в Active Directory. Якщо сервер не авторизований, служба DHCP просто не запуститься, щоб не створювати конфліктів у домені.

На наступному кроці потрібно створити "пули" адрес для кожної підмережі. Для цього необхідно завантажити консоль DHCP, вибравши у Server Manager (див. рис. 3.10) пункт меню Tools, а в ньому DHCP.

Далі необхідно розгорнути дерево сервера, натиснути правою кнопкою миші на IPv4 і обрати New Scope.

Для кожної VLAN зі списку вказаного в таблиці 3.4 виконати наступні параметри (див. рис. 3.11):

– Name – назву пулу;

– IP Address Range – початкову адресу та кінцеву адресу пулу;

– Subnet Mask – мережева маска.

Таблиця 3.4 – Налаштування DHCP-пулів

Назва VLAN	Діапазон IP-адрес	Маска	Шлюз (Default Gateway)
Guest_G	192.168.0.81 – 192.168.0.92	28	192.168.0.94
Guest_1	192.168.0.97 – 192.168.0.109	29	192.168.0.110
Guest_2	192.168.0.113 – 192.168.0.125	29	192.168.0.126
Guest_3	192.168.0.129 – 192.168.0.141	29	192.168.0.142
Logist	192.168.0.40 – 192.168.0.45	28	192.168.0.46
Sklad_1	192.168.0.6 – 192.168.0.29	27	192.168.0.30
Sklad_2	192.168.0.54 – 192.168.0.61	28	192.168.0.62
Sklad_3	192.168.0.68 – 192.168.0.77	28	192.168.0.78

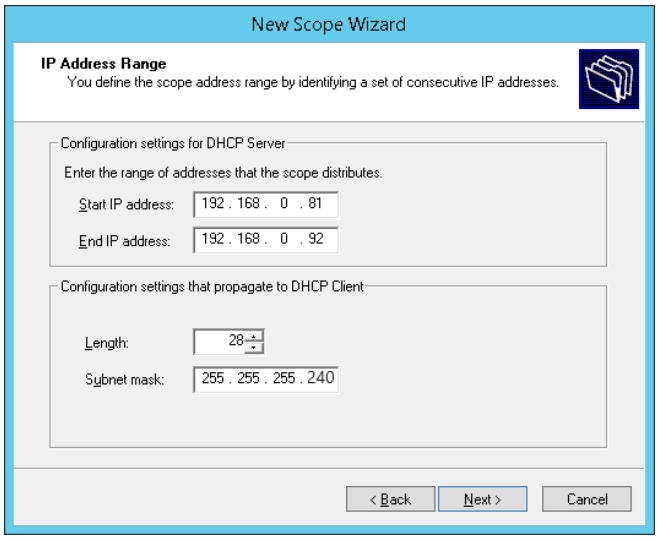


Рисунок 3.11 – Налаштування DHCP-пулу

У наступному вікні с Lease Duration необхідно вказати час оренди адреси. За замовчуванням прийнято 8 днів, але для гостьового Wi-Fi краще ставити 2 години. В останньому вікні відмітити опцію «Yes, I want to configure these options now» та вибрати кнопку Finish.

3.3 Інструкції по налаштуванню VPN-тунелів та NAT

Для забезпечення доступу хостів із внутрішніх сегментів VLAN (див. табл. 2.2) до глобальної мережі Інтернет, на межовому маршрутизаторі реалізовано механізм NAT. На першому етапі конфігурування необхідно чітко розмежувати зони довіри, визначивши ролі фізичних та логічних інтерфейсів:

– внутрішній інтерфейс (Inside) – порт GigabitEthernet0/0/0 для маршрутизаторів складів та GigabitEthernet0/0/0 і GigabitEthernet0/0/1 – головного офісу. Для нього встановлюється директива “ip nat inside”, що ідентифікує його як вхідну точку для локального трафіку;

– зовнішні інтерфейси (Outside) – порти, які під’єднують обладнання до каналів основного та резервного провайдерів. Для них застосовується команда “ip nat outside”, яка визначає ці інтерфейси як точки виходу в глобальну мережу.

Наступним кроком є створення списків контролю доступу (ACL), які дозволяють механізму NAT ідентифікувати трафік, що підлягає трансляції. До даного списку включено всі робочі та гостьові підмережі підприємства. Для раціонального використання публічних IP-адрес застосовано технологію PAT (Port Address Translation) з параметром overload. Це дозволяє групі внутрішніх пристроїв одночасно виходити в мережу через одну зовнішню адресу, розрізняючи сесії за номерами TCP/UDP портів.

Детальний лістинг команд для ініціалізації інтерфейсів та активації правил трансляції для маршрутизатора R_1 наведено на рисунку 3.12.

```
R_1(config)#interface gigabitethernet0/0/0
R_1(config-if)#ip nat inside
R_1(config-if)#interface range gigabitethernet0/0/1-gigabitethernet0/0/2
R_1(config-if-range)#ip nat outside
R_1(config-if-range)#exit
R_1(config)#access-list 100 permit ip 192.168.0.0 0.0.0.31 any
R_1(config)#access-list 100 permit ip 192.168.0.96 0.0.0.15 any
R_1(config)#access-list 100 permit ip 192.168.0.192 0.0.0.7 any
R_1(config)#ip nat inside source list 100 interface gigabitethernet0/0/0
R_1(config)#ip nat inside source list 100 interface gigabitethernet0/0/0 overload
R_1(config)#no ip nat inside source list 100 interface gigabitethernet0/0/0 overlo
R_1(config)#ip nat inside source list 100 interface gigabitethernet0/0/1 overload
R_1(config)#ip nat inside source list 100 interface gigabitethernet0/0/2 overload
```

Рисунок 3.12 – Налаштування NAT на маршрутизаторі R_1

Для забезпечення безперебійного доступу до мережі Інтернет на маршрутизаторі налаштовано два паралельні механізми NAT, що відповідають основному та резервному провайдерам. Вибір активного каналу передачі даних визначається станом маршруту за замовчуванням у таблиці маршрутизації. Для пріоритезації трафіку через основний канал зв'язку встановлюється статичний маршрут із параметром track 1, тоді як для резервного каналу призначається нижчий пріоритет через збільшення адміністративної дистанції до значення 10.

Ключовим елементом системи відмовостійкості є впровадження механізму IP SLA (Service Level Agreement) у поєднанні з функцією Object Tracking. Цей підхід дозволяє автоматично перемикати трафік на резервного провайдера навіть у тих випадках, коли фізичний інтерфейс основного каналу залишається в активному стані («Up»), але фактичний доступ до мережі відсутній через проблеми на стороні оператора.

Принцип роботи IP SLA полягає у безперервному генеруванні тестового ICMP-трафіку (запитів) до зовнішніх еталонних вузлів, таких як публічний DNS-сервер Google (8.8.8.8). На основі аналізу відповідей від цих вузлів маршрутизатор об’єктивно оцінює реальну доступність та якість Інтернет-з'єднання. Якщо контрольні пакети не повертаються протягом встановленого часу, система ідентифікує канал як непрацездатний і миттєво активує резервний маршрут.

Повний перелік команд, що забезпечують ініціалізацію сервісу IP SLA, налаштування параметрів відстеження та конфігурацію плаваючих статичних маршрутів, представлено на рисунку 3.13.

```
R1(config)#ip route 0.0.0.0 0.0.0.0 100.100.100.1 1
R1(config)#ip route 0.0.0.0 0.0.0.0 200.200.200.1 10
R1(config)#ip sla 1
R1(config-ip-sla)#icmp-echo 8.8.8.8 source-interface GigabitEthernet1/0
R1(config-ip-sla-echo)# exit
R1(config)#ip sla schedule 1 life forever start-time now
R1(config)#track 1 ip sla 1 reachability
```

Рисунок 3.13 – Налаштування маршруту за замовчуванням та моніторингу каналу зв’язку із провайдером

Для створення єдиного захищеного інформаційного простору між центральним офісом та трьома територіально віддаленими складськими комплексами впроваджується технологія віртуальних приватних мереж (VPN). Використання VPN-тунелів дозволяє здійснювати конфіденційний обмін даними через публічну мережу Інтернет, логічно об'єднуючи всі філії в спільну корпоративну інфраструктуру.

Згідно з розробленим планом адресації (див. табл. 2.2-2.3), для функціонування логічних каналів зв'язку виділено спеціалізовані адресні простори, представлені в таблиці 2.3. Процес конфігурування розпочинається з ініціалізації віртуального інтерфейсу Tunnel 1 на центральному маршрутизаторі R_G. Відповідно до проєктних розрахунків, цьому інтерфейсу призначається IP-адреса 192.168.0.229. Детальний процес призначення адреси та активації інтерфейсу продемонстровано на рисунку 3.14.

```
R_G(config-if)#ip address 192.168.0.229 255.255.255.252
R_G(config-if)#tunnel source gigabitethernet0/0/2
R_G(config-if)#tunnel destination 175.199.19.10
R_G(config-if)#exit
R_G(config)#R G
```

Рисунок 3. 14 – Налаштування віртуального тунелю на маршрутизаторі R_G

Відповідно до розробленої топології (див. рис. 3.16), за зовнішнім інтерфейсом маршрутизатора віддаленого офісу закріплено публічну IP-адресу 175.199.19.10. Наступним етапом є налаштування обладнання на боці віддаленого складу №1. Конфігурація виконується за аналогією з головним маршрутизатором, проте з урахуванням специфіки адресації точок термінації тунелю.

Зокрема, під час ініціалізації віртуального інтерфейсу на боці філії, як адресу призначення тунелю (tunnel destination) необхідно вказати зовнішній IP-інтерфейс головного маршрутизатора R1 – 172.103.102.2. Це забезпечить встановлення логічного зв'язку між центральним офісом та віддаленим об'єктом.

За аналогічним алгоритмом здійснюється розгортання VPN-каналів для решти територіально віддалених складів компанії. Повний перелік IP-адрес, що

використовуються для побудови тунельних з'єднань між усіма вузлами мережі «Global-Express», систематизовано у таблиці 3.5.

Таблиця 3.5 – Адреси фізичних та віртуальних інтерфейсів у VPN-тунелях

Номер тунелю	Віддалений склад	Фізичні IP-адреси на маршрутизаторах		IP-адреси VPN	
		клієнт	сервер	клієнт	сервер
1	1	175.199.19.10	100.100.100.2	192.168.0.230	192.168.0.231
2	1	178.22.12.21	200.200.200.2	192.168.0.234	192.168.0.235
3	2	175.199.19.10	100.100.100.2	192.168.0.238	192.168.0.239
4	2	178.103.21.18	200.200.200.2	192.168.0.242	192.168.0.243
5	3	175.199.39.45	100.100.100.2	192.168.0.246	192.168.0.247
6	3	178.121.14.11	200.200.200.2	192.168.0.250	192.168.0.251

На основі даних, наведених у таблиці 3.5, здійснюється конфігурування віртуальних інтерфейсів VPN-тунелів на периферійних маршрутизаторах R1, R2 та R3. Це дозволяє створити кінцеві точки зв'язку з боку територіальних підрозділів. Оскільки базові GRE-тунелі не мають вбудованих засобів криптографічного захисту, для забезпечення конфіденційності даних поверх них розгортається протокол IPSec.

У даному проєкті обрано транспортний режим функціонування IPSec, що дозволяє ефективно інкапсулювати корисне навантаження вище мережевого рівня моделі OSI, зберігаючи оригінальний IP-заголовок без змін. Впровадження захисту реалізується у два послідовні етапи на обох вузлах зв'язку.

Перший етап передбачає налаштування політик ISAKMP (Internet Security Association and Key Management Protocol). У режимі глобальної конфігурації визначаються ключові параметри безпеки, такі як алгоритми шифрування та хешування, і створюється відповідна політика вузла. Детальний перелік команд, необхідних для реалізації цього етапу, наведено на рисунку 3.15.

```
RG(config)#crypto isakmp policy 1
RG(config-isakmp)#encryption 3des
RG(config-isakmp)#hash md5
RG(config-isakmp)#authentication pre-share
RG(config-isakmp)#group 2
RG(config-isakmp)#lifetime 86400
RG(config-isakmp)#exit
RG(config)#crypto isakmp key chudoostriv address 178.98.17.101
RG(config)#
```

Рисунок 3.15 – Налаштування політики ISAKMP

Згідно з конфігурацією, наведеною на рисунку 3.15, для забезпечення конфіденційності передачі даних обрано алгоритм симетричного блочного шифрування 3DES, а цілісність інформації гарантується використанням хеш-функції MD5. Процедура автентифікації вузлів базується на застосуванні попередньо узгодженого спільного ключа (pre-shared key). Для генерації секретних ключів активовано другу групу алгоритму Діффі-Геллмана, а параметр lifetime регламентує часовий інтервал дії сеансового ключа.

У процесі налаштування встановлено ідентифікатор ключа «chudoostriv», який прив'язано до публічної IP-адреси віддаленого шлюзу відповідно до даних таблиці 3.3. Критично важливою умовою для встановлення з'єднання є повна ідентичність цього ключа на обох сегментах VPN-тунелю. Це забезпечує успішне проходження першої фази встановлення захищеного каналу.

Переходячи до другої фази налаштування IPSec, на пристроях формується набір перетворень (Transform Set), що отримав назву «TS». Даний набір визначає конкретні методи захисту корисного навантаження, які детально представлені на рисунку 3.16. Важливим етапом конфігурування є переведення IPSec у транспортний режим, що дозволяє оптимізувати роботу тунелю та зменшити накладні витрати на передачу заголовків пакетів.

```
RG(config)#crypto ipsec transform-set TS esp-3des esp-md5-hmac
RG(cfg-crypto-trans)# mode transport
RG(cfg-crypto-trans)# exit
```

Рисунок 3.16 – Налаштування траснпортного режиму роботи IPSec

Далі слід здійснити конфігурування захищеного каналу зв'язку є інтеграція протоколу IPSec із GRE-тунелем. Цей процес реалізується за допомогою механізму криптографічних карт (Crypto Map). У межах даного проєкту створюється карта з ідентифікатором MY_CRYPTO_MAP та індексом пріоритетності 10. Використання порядкових номерів забезпечує гнучкість налаштування, дозволяючи маршрутизатору послідовно обробляти декілька записів у межах однієї структури.

Процес налаштування, деталізований на рисунку 3.17, передбачає перехід у режим специфічної конфігурації Crypto Map для визначення параметрів пірингу. На цьому етапі жорстко задається IP-адреса віддаленого вузла (peer) — 175.199.19.10, яка, згідно з таблицею 3.3, є публічною адресою шлюзу на протилежному боці VPN-тунелю.

```
RG(config)#crypto map MY_CRYPTO_MAP 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
RG(config-crypto-map)#set peer 178.98.17.101
RG(config-crypto-map)#set transform-set MY TRANS SET
```

Рисунок 3.17 – Налаштування Crypto Map

Останнім кроком конфігурування є асоціація раніше створеного набору перетворень (Transform Set) із даною криптографічною картою. Це створює цілісну логічну схему, де маршрутизатор точно знає, до якого трафіку застосовувати шифрування та з яким віддаленим пристроєм встановлювати захищене з'єднання.

Для забезпечення коректного функціонування схеми GRE over IPsec необхідно реалізувати криптографічний захист саме того трафіку, що передається між публічними інтерфейсами маршрутизаторів. З цією метою створюється спеціалізований список контролю доступу (ACL), який ідентифікує пакети протоколу GRE (номер протоколу 47), що курсують між IP-адресами, визначеними у таблиці 3.5.

Після ідентифікації трафіку в ACL виконується фінальне налаштування об'єкта Crypto Map:

– створений список доступу прив'язується до криптографічної карти;

– карта активується безпосередньо на фізичному зовнішньому інтерфейсі маршрутизатора.

Після завершення конфігурування центрального вузла аналогічні налаштування впроваджуються на другому маршрутизаторі тунелю. При цьому забезпечується повна дзеркальність параметрів безпеки. Зокрема, у команді crypto isakmp key як цільова адреса вказується публічний інтерфейс головного офісу – 100.100.100.2. Такий підхід гарантує успішну взаємну автентифікацію та встановлення стабільного захищеного з’єднання.

Аналогічний алгоритм розгортання шифрування застосовується для всіх інших віртуальних тунелів мережі «Global-Express». Після встановлення захищених VPN-каналів реалізується схема статичної маршрутизації. Це критично важливо для забезпечення повноцінного обміну даними між центральним офісом та внутрішніми сегментами (VLAN) віддалених підрозділів, оскільки дозволяє маршрутизаторам коректно визначати шлях до цільових підмереж через створені логічні інтерфейси

3.4 Інструкції по налаштуванню динамічної маршрутизації

Для автоматизації обміну маршрутною інформацією між центральним офісом та віддаленими філіями впроваджено протокол динамічної маршрутизації OSPF. Вибір даного протоколу обумовлений його здатністю до швидкої збіжності мережі при зміні топології, що важливо у випадку аварійного розриву з’єднання із основним Інтрнет-провайдером, підтримкою ієрархічної структури та використанням алгоритму найкоротшого шляху.

Процес конфігурування розпочинається з ініціалізації процесу OSPF на кожному маршрутизаторі мережі, де кожному пристрою призначається унікальний ідентифікатор Router ID.

Основним етапом налаштування є визначення переліку мереж, які будуть брати участь у процесі динамічного обміну. За допомогою команди network вказуються адреси локальних підмереж (VLAN) та інтерфейсів VPN-тунелів разом із їхніми інверсними масками (wildcard masks). Усі сегменти мережі «Global-Express» включені до магістральної зони Area 0, що мінімізує затримки при передачі службової інформації та спрощує структуру маршрутизації між центральним офісом і віддаленими складами.

Особлива увага приділяється взаємодії OSPF із раніше створеними тунелями. Оскільки VPN-канали є логічними інтерфейсами, протокол OSPF сприймає їх як прямі з'єднання між маршрутизаторами. Це дозволяє центральному маршрутизатору автоматично отримувати маршрути до всіх внутрішніх підмереж складів через захищені канали, не потребуючи ручного оновлення статичних записів. Для оптимізації трафіку та підвищення безпеки на інтерфейсах, де відсутні інші OSPF-сусіди (наприклад, у клієнтських VLAN), активовано режим passive-interface, що запобігає розсиланню зайвих службових повідомлень усередину локальної мережі.

Повний перелік команд налаштування маршрутизації на маршрутизаторі головного офісу представлено на рисунку 3.18.

```
R_G(config)#router ospf 1
R_G(config-router)#router-id 1.1.1.1
R_G(config-router)#network 192.168.0.32 0.0.0.15 area 0
R_G(config-router)#network 192.168.0.80 0.0.0.15 area 0
R_G(config-router)#network 192.168.0.144 0.0.0.15 area 0
R_G(config-router)#network 192.168.0.160 0.0.0.15 area 0
R_G(config-router)#network 192.168.0.176 0.0.0.7 area 0
R_G(config-router)#network 192.168.0.184 0.0.0.7 area 0
R_G(config-router)#network 192.168.0.216 0.0.0.7 area 0
R_G(config-router)#network 192.168.0.224 0.0.0.3 area 0
R_G(config-router)#network 192.168.0.228 0.0.0.3 area 0
R_G(config-router)#network 192.168.0.236 0.0.0.3 area 0
R_G(config-router)#network 192.168.0.240 0.0.0.3 area 0
R_G(config-router)#network 192.168.0.244 0.0.0.3 area 0
R_G(config-router)#network 192.168.0.248 0.0.0.3 area 0
R_G(config-router)#passive-interface GigabitEthernet0/0/0
R_G(config-router)#passive-interface GigabitEthernet0/0/1
R_G(config-router)#exit
```

Рисунок 3.18 – Налаштування OSPF-маршрутизації на прикладі маршрутизатора R_G

3.5 Моделювання мережі

Етап практичного впровадження спроєктованої архітектури здійснюється шляхом побудови імітаційної моделі в спеціалізованому середовищі Cisco Packet Tracer. Процес розгортання топології реалізується за наступним алгоритмом:

– формування апаратної бази. Використовуючи панель компонентів, на робочій області розміщуються всі пристрої, що визначені специфікацією проєкту (маршрутизатори, комутатори, сервери та кінцеві станції);

– фізична комутація. На панелі елементів проводиться підбір типів кабелів (мідна «вита пара» прямого або перехресного типу) відповідно до стандартів Ethernet;

– конфігурування з'єднань. Встановлення зв’язку виконується через вибір конкретних фізичних портів на інтерфейсах обох вузлів. Комутація обладнання здійснюється у суворій відповідності до логічної схеми з’єднань, наведеної у додатку Б.

На другому етапі реалізації мережевої моделі проводиться індивідуальне налаштування кожної робочої станції. Процес передбачає виклик вікна налаштувань пристрою, де у вкладці Desktop через застосунок IP Configuration впроваджуються параметри мережевого рівня.

На другому етапі для кожної робочої станції необхідно викликати вікно налаштування пристрою і у меню Desktop застосунку IP Configuration впроваджуються параметри мережевого рівня. Зокрема, встановлюються статичні значення IPv4-адреси, маски підмережі та основного шлюзу згідно з розрахунковою таблицею 2.2. Для забезпечення коректної роботи доменних імен вказується адреса DNS-сервера – 192.168.0.225.

Черговим етапом реалізації проєкту є конфігурування засобів візуального моніторингу в середовищі Cisco Packet Tracer. Для забезпечення стабільної роботи камер відеоспостереження виконується призначення мережевих параметрів, що

відповідають виділеному сегменту. Усі налаштування здійснюються згідно з планом адресації, наведеним у таблиці 2.2.

Практична реалізація системи візуального моніторингу в симуляторі розпочинається з індивідуального налаштування кожної IP-камери. Для цього у вікні властивостей пристрою використовується вкладка Config, яка надає доступ до параметрів апаратних інтерфейсів. У навігаційній панелі обирається інтерфейс GigabitEthernet 0, що є точкою підключення камери до комутаційної інфраструктури мережі.

Безпосереднє встановлення мережевих параметрів передбачає введення статичної IPv4-адреси та відповідної маски підмережі, що належать до діапазону CAM_G, CAM_1, CAM_2, CAM_3 відповідно до приміщення. Такий підхід гарантує логічну ізоляцію трафіку відеоспостереження від загальних потоків даних. Весь процес ієрархічного призначення адрес для компонентів системи безпеки, що забезпечує їхню ідентифікацію в мережі, ілюструється на рисунку 3.19

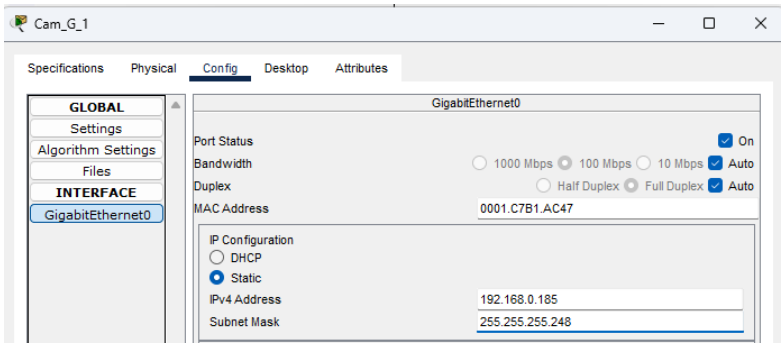


Рисунок 3.19 – Приклад налаштування IPv4 адреси камері відеоспостереження

Адресу шлюзу (для підмережі камер відеоспостереження), потрібно вказати в розділі Settings цієї ж вкладки Config.

Останній етап розгортання інфраструктури в середовищі Cisco Packet Tracer полягає у безпосередньому конфігуруванні активних компонентів – маршрутизаторів та комутаторів. Для взаємодії з операційною системою пристроїв використовується консольний інтерфейс (CLI), що імітує реальні умови адміністрування.

Загальний вигляд та логічна архітектура повністю сформованої мережі, що готова до експлуатації, представлені у додатку Г.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР

Визначення сукупних витрат часу, необхідних для успішного виконання науково-дослідної роботи (НДР), здійснюється шляхом детального структурування технологічного циклу на окремі стадії. Часові показники для кожного етапу розробки, а також їхня послідовність, представлені у таблиці 4.1.

Таблиця 4.1 – Середній час виконання НДР та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4
1.	Постановка задачі, формування технічного завдання на проект локальної мережі. Узгодження майбутнього розміщення мережевих розеток.	Керівник проекту	15
2.	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі логістичного підприємства «Global-Express». Вибір оптимальної логічної та фізичної топології. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення. Врахування структури підприємства для сегментування локальної мережі на підмережі.	Інженер	30

Продовження таблиці 4.1

1	2	3	4
3.	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання. Перевірка СКС локальної мережі на відповідність вибраній технології.	Технік	45
4.	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	30
5.	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
		Разом	125

Сумарний час виконання операцій технологічного процесу проектування мережі становить 125 години, з них 15 годин – робота керівника проекту, 65 години – інженера, 45 години – техніка.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

У системі економічних відносин підприємства оплата праці розглядається як грошовий еквівалент вартості та ціни специфічного товару – робочої сили. Вона виступає у формі винагороди, яку роботодавець виплачує персоналу за фактично виконаний обсяг робіт або відпрацьований час. При цьому рівень індивідуального заробітку працівника безпосередньо корелює з підсумковими показниками ефективності діяльності суб'єкта господарювання.

Для цілей даного проєкту загальний фонд оплати праці (ФОП) розраховується як сукупність основної та додаткової заробітної плати всіх залучених фахівців.

Основна заробітна плата розраховується за формулою:

$$З_{осн} = Т_с \cdot К_г, \quad (4.1)$$

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо таку ставку для керівник проекту – 250 грн, інженера – 200 грн./год. а для техніка – 160 грн./год.

Отже, основна заробітна плата для:

- керівника проекту – $З_{осн1} = 15 \cdot 250 = 3750$ грн.
- інженера – $З_{осн2} = 65 \cdot 200 = 13000$ грн.
- техніка – $З_{осн3} = 35 \cdot 160 = 5600$ грн.

Сумарна основна заробітна плата становить

$$З_{осн}=3750 +13000 + 5600 =22350 \text{ грн.}$$

Додаткова заробітна плата становить 10 –15 % від суми основної заробітної плати.

$$З_{дод} = З_{осн} \cdot К_{допл}, \quad (4.2)$$

де $К_{допл}$. – коефіцієнт додаткових виплат працівникам, 0,1– 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника $З_{дод1}=3750 \cdot 0,12= 450$ грн.
- інженера $З_{дод1}=13000 \cdot 0,12= 1560$ грн.
- техніка $З_{дод3}=5600 \cdot 0,12= 672$ грн.

Сумарна додаткова заробітна плата становить:

$$З_{дод}=450 + 1560 + 672 = 2682 \text{ грн.}$$

Звідси загальні витрати на оплату праці ($В_{о.п.}$) визначаються за формулою:

$$В_{о.п} = З_{осн} + З_{дод} \quad (4.3)$$

Отже, загальні витрати на оплату праці становлять:

$$В_{о.п.}= 22350 + 2682 = 25032 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи. Відрахування на соціальні заходи становлять 22%. Отже, сума відрахувань на соціальні заходи буде становити:

$$B_{с.з.} = ФОП \cdot 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з} = 25032 \cdot 0,22 = 5507,04 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 – Зведені розрахунки витрат на оплату праці

№ п/	Категорія працівників	Основна заробітна плата, грн.			Додатк. заробітна плата, грн.	Нарах. на ФОП, грн.	Всього витрати на оплату праці, грн
		Тарифна ставка, грн.	К-сть відпрац. год.	Фактично нарах. з/пл., грн.			
1	Керівник	250	15	3750	450	-	-
2	Інженер	200	65	13000	1560	-	-
3	Технік	160	45	5600	672	-	-
			Разом	22350	2682	5507,04	30539,04

Отже, загальні витрати на оплату праці становлять 30539,04 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{BI} = q_i \cdot P_i \quad (4.5)$$

де q_i – кількість витраченого матеріалу і-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} \sum M_{B_i} \quad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 – Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Кількість	Ціна, грн.	Сума, грн.
1	2	3	4	5	6
1	Комутаційна шафа Hypernet WMNC-18U-FLAT	шт.	4	4650	18600
2	Патчпанель 24 порти, кат. 6	шт.	6	1200	6720
3	Розетка RJ-45 (категорія 6)	шт.	40	120	4800
4	Розетка підлогова RJ-45 (категорія 6)	шт.	4	180	720
5	Роз’єм 8P8C (100 шт)	шт.	1	590	590
6	Короб (середня ціна)	м.	110	115	14260
7	Короб металічний (середня ціна)	м.	240	160	38400
8	Кабель UTP (кат. 6) (бухта)	шт.	3	5353	16059
9	Патчкорди (кат. 6)	шт.	44	56	2464
10	Патчкорди (оптоволокно)	шт.	1	85	85
11	Конектор SC	шт.	4	38	152
12	Гофрована трубка	м.	26	45	1170
13	Маршрутизатор Cisco ISR4221/K9	шт.	4	34225	136900
14	Комутатор рівня доступу Cisco Catalyst 2960L-24PS-LL	шт.	5	45256	226280
15	Точка доступу TP-LINK EAP225	шт.	12	3499	41988
16	Сервер Dell PowerEdge R450	шт.	1	72110	72110
17	Камера Reolink RLC-1224A	шт.	12	4590	55080
18	ДБЖ APC Back-UPS Pro 1500VA	шт.	2	4680	9360
Р а з о м			-	-	645738

Отже, загальна сума матеріальних витрат на розробку мережі становить 645738 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання визначаються за формулою:

$$З_е = W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 10 годин, споживана потужність – 0,5 кВт/год, вартість 1 кВт електроенергії – 9 грн. Тому витрати на електроенергію будуть становити:

$$З_е = 0,5 \cdot 10 \cdot 9 = 45 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8–10% від загальної суми матеріальних затрат.

$$Т_в = З_{м.в} \cdot 0,08..0,1, \quad (4.8)$$

де $Т_В$ – транспортні витрати.

Отже,

$$Т_В = 645738 \cdot 0,08 = 51659,04 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

В процесі використання основних фондів виконуються заходи що до їх відновлення. Для відновлення засобів праці у натуральному виразі необхідне їх

відшкодування у вартісній формі, яке здійснюється шляхом амортизації. Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення. Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Мінімально допустимі строки їх використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$A = \frac{Б_в \cdot Н_А}{100\%} \cdot T \quad (4.9)$$

де А – амортизаційні відрахування за звітний період, грн.;

$Б_в$ – балансова вартість групи основних фондів на початок звітного періоду, грн.;

$Н_А$ – норма амортизації, %;

Т – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 10 год., балансова вартість ПК - 26000 грн., тому, то амортизаційні відрахування становлять:

$$A = \frac{25000 \cdot 0{,}04}{150} \cdot 10 = 66{,}67 \text{ грн}$$

4.7 Обчислення накладних витрат

Накладні витрати – це витрати, не пов'язані безпосередньо з технологічним процесом виготовлення продукції, а утворюються під впливом певних умов роботи по організації, управлінню та обслуговуванню виробництва.

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20–60 % від суми основної та додаткової заробітної плати працівників.

$$H_в = B_{о.п.} \cdot 0{,}2...0{,}6,, \quad (4.10)$$

де H_B – накладні витрати.

$$H_B = 25032 \cdot 0{,}4 = 10012{,}8 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Кошторис витрат являє собою зведений план усіх витрат підприємства на майбутній період виробничо-фінансової діяльності.

Результати проведених вище розрахунків зведемо у таблиці 4.4, де зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	в % до загального
Витрати на оплату праці (основну і додаткову заробітну плату)	25032	3,39
Відрахування на соціальні заходи	5507,04	0,75
Матеріальні витрати	645738	87,49
Витрати на електроенергію	45	0,01
Транспортні витрати	51659,04	7
Амортизаційні відрахування	66,67	0,01
Накладні витрати	10012,8	1,36
Собівартість	738060,55	100

В таблиці 4.4 зазначено наступні види витрат: витрати на оплату праці, відрахування на соціальні заходи, матеріальні витрати, витрати на електроенергію, транспортні витрати, амортизаційні відрахування, накладні витрати, тобто собівартість ($С_в$) НДР розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.п.} + З_{м.в.} + З_е + Т_в + А + Н_в \quad (4.11)$$

Отже, собівартість дорівнює $С_В$=738060,55 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = C_в \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \quad (4.12)$$

де $P_{рен.}$ – рівень рентабельності;

ПДВ – ставка податку на додану вартість, (20 %).

Отже, ціна НДР становить:

$$Ц = 738060{,}55 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 1151374{,}46 \text{ грн}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

де *П* – прибуток;

C_B – собівартість;

$$П = 1151374{,}46 - 738060{,}55 = 413313{,}91 \text{ грн}$$

Економічна ефективність (Ер) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою:

$$E_p = \frac{П}{С_в} = \frac{413313{,}91}{738060{,}55} = 0{,}56 \quad (4.14)$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень $Т_р$:

$$T_p = \frac{1}{E_р} \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку:

$$T_p = \frac{1}{0{,}56} = 1{,}8$$

Всі дані внесемо в зведену таблицю 4.5 економічних показників.

Таблиця 4.5 – Економічні показники НДР

№п/п	Показник	Значення
1.	Собівартість, грн.	738060,55 грн.
2.	Плановий прибуток, грн.	413313,91 грн.
3.	Ціна, грн.	1151374,46 грн.
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

Загальна вартість розробленої комп'ютерної мережі логістичної компанії «Global-Express» становить 1151374,46 грн. Зважаючи на високі показники економічної ефективності – 0,56, кошти, вкладені в проведення проектних робіт окупляться за 1,8 року.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

5.1 Дотримання вимог пожежної безпеки в логістичному підприємстві "Global-Express"

Пожежна безпека є одним із найважливіших елементів загальної системи охорони праці на логістичному підприємстві «Global-Express», оскільки функціонування його сучасної інформаційно-комунікаційної мережі безпосередньо пов’язане з експлуатацією великої кількості електрообладнання, серверних систем, комутаційних вузлів та протяжних кабельних ліній.

Забезпечення належного рівня пожежної безпеки в приміщеннях підприємства здійснюється відповідно до вимог Кодексу цивільного захисту України, Кодексу законів про працю України, «Правил пожежної безпеки в Україні» (НАПБ А.01.001-2014) [10] та ДБН В.2.5-56:2014 «Системи протипожежного захисту» [9].

Основним завданням пожежної профілактики в межах розробленого проєкту є повне виключення можливості виникнення загоряння, а у випадку його виникнення – мінімізація негативних наслідків, швидка локалізація джерела вогню, захист життя і здоров’я персоналу, а також збереження коштовної мережевої інфраструктури та інформаційних ресурсів підприємства.

Аналіз умов праці та технічної специфіки розробленої корпоративної мережі показує, що основними джерелами пожежної небезпеки є приміщення центральної серверної та робочі місця офісних працівників філій, де зосереджено значну кількість комп'ютерної техніки, периферійних пристроїв, а також продуктивні комутатори Cisco Catalyst серії C9300.

Згідно з чинною класифікацією за вибухопожежною та пожежною небезпекою, офісні приміщення та серверні вузли належать переважно до категорії В, що обумовлює необхідність впровадження комплексних попереджувальних заходів. Пожежна небезпека в таких приміщеннях характеризується наявністю значної кількості горючих матеріалів у вигляді

пластикових елементів корпусів техніки, оплетки кабелів, а також постійною присутністю потенційних джерел запалювання, якими можуть виступати електричні дуги, іскри або зони критичного перегріву компонентів унаслідок коротких замикань, струмових перевантажень чи підвищеного перехідного опору в контактних з'єднаннях [3].

Для мінімізації зазначених ризиків у проєкті передбачено використання високоякісного мережевого кабелю типу U/UTP категорії 6 виробництва підприємства «Одескабель», який має покращені показники вогнестійкості та низький рівень виділення токсичного диму під час термічного впливу.

Всі кабельні траси всередині будівлі прокладаються у спеціальних негорючих металевих лотках або захисних пластикових коробах, що суттєво перешкоджає поширенню полум'я у разі випадкового пошкодження ізоляції.

Електропостачання серверного обладнання та ключових комутаційних вузлів організовано через потужні системи безперебійного живлення із вбудованим захистом від сплесків напруги, а розподільні щити оснащені надійними автоматичними вимикачами та пристроями захисного відключення, які миттєво знеструмлюють аварійну ділянку мережі при перевищенні допустимих параметрів струму.

Крім того, у приміщенні серверної передбачено встановлення прецизійної автономної системи кондиціонування повітря для підтримки стабільного температурного режиму та запобігання перегріву активного обладнання.

Важливою складовою системи протипожежного захисту логістичного підприємства є автоматична пожежна сигналізація, яка інтегрована в загальну систему безпеки «Global-Express».

Робочі кабінети, коридори та серверний вузол обладнуються високочутливими димовими пожежними сповіщувачами, які здатні виявити загоряння на найранішій стадії за появи перших ознак тління ізоляційних матеріалів. Сигнал від сповіщувачів надходить на головний приймально-контрольний прилад, що забезпечує автоматичне сповіщення чергового

персоналу, запуск світлозвукової системи оповіщення про евакуацію та негайну передачу сигналу на пульт централізованого спостереження пожежної охорони.

Для гасіння пожеж у приміщеннях з комп'ютерною технікою та електроустановками під напругою суворо заборонено використання води або хімічної піни, тому серверна кімната додатково оснащується газовою або порошковою автономною системою пожежогасіння, яка ефективно ліквідує вогонь без завдання шкоди електронним модулям.

У разі виникнення аварійної чи пожежонебезпечної ситуації успішна евакуація персоналу логістичного центру залежить від чіткої організації, узгодженості дій та наочності шляхів виходу з будівлі. З цією метою для офісу логістичного підприємства «Global-Express» було детально розроблено плани евакуації на випадок пожежі та схеми оптимального розміщення первинних засобів пожежогасіння, які винесені у графічну частину дипломного проєкту (див. рис. Д.1–Д.4, додатку Д).

На цих схемах чітко позначено основні та запасні евакуаційні шляхи, графічні напрямки руху людей, місця розташування внутрішніх пожежних кранів, а також спеціальні зони розміщення вуглекислотних вогнегасників типу ОУ-3 та ОУ-5, які є найбільш ефективними для локалізації загорянь класу Е, тобто електроустановок під напругою.

Всі шляхи евакуації суворо утримуються вільними від сторонніх предметів чи меблів, а двері на виходах обладнані легкодоступними замками типу «антипаніка», що відкриваються зсередини без використання ключа.

Додатково вздовж коридорів та безпосередньо над виходами встановлюються світлові покажчики «Вихід» з автономними акумуляторами, які гарантують видимість напрямку руху навіть при повному аварійному знеструмленні підприємства.

Організаційні заходи пожежної безпеки на підприємстві «Global-Express» передбачають обов'язкове призначення відповідальних осіб за пожежний стан кожного окремого кабінету, проведення регулярних інструктажів із

працівниками та організацію практичних тренувань з евакуації не рідше ніж двічі на рік.

Кожен співробітник при прийомі на роботу проходить вступний та первинний інструктажі на робочому місці, де детально ознайомлюється з правилами безпечної експлуатації комп'ютерної техніки, порядком дій під час спрацювання сигналу тривоги та правилами застосування вогнегасників згідно з розробленими планами евакуації.

Дотримання комплексу цих технічних, конструктивних та організаційних рішень дозволяє створити максимально безпечні умови для повсякденного функціонування корпоративної мережі логістичного підприємства та мінімізувати ймовірність виникнення будь-яких пожежонебезпечних ситуацій.

5.2 Санітарно-гігієнічні вимоги до серверних приміщень та робочих місць операторів логістичного центру

Забезпечення належних санітарно-гігієнічних умов у приміщеннях логістичного підприємства «Global-Express» є базовою умовою для підтримки високої працездатності персоналу, зниження рівня професійних захворювань та гарантування безвідмовної роботи складного мережевого й серверного обладнання.

Особливу увагу в межах розробленого проєкту приділено центральному серверному вузлу та залам роботи операторів логістичного центру, де спостерігається найбільша концентрація засобів обчислювальної техніки та активних пристроїв корпоративної мережі.

Організація виробничого середовища в цих зонах здійснюється у суворій відповідності до Закону України «Про забезпечення санітарного та епідемічного благополуччя населення», нормативно-правового акта з охорони праці НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту

здоров’я працівників під час роботи з екранними пристроями» [11], а також чинних державних санітарних норм і будівельних стандартів України.

Комплексний підхід до оптимізації мікроклімату, освітлення, шуму та ергономіки дозволяє мінімізувати шкідливий вплив виробничих факторів на організм працівників логістичного хабу.

Параметри мікроклімату в робочих зонах операторів та в серверному приміщенні суттєво відрізняються через різне функціональне призначення та технологічні вимоги до експлуатації техніки. Для робочих місць операторів «Global-Express», чия діяльність за формою організації праці та рівнем енерговитрат належить до категорії легких фізичних робіт (категорія Іа), згідно з ДСанПіН 3.3.6.042-99 підтримуються оптимальні параметри повітряного середовища [12].

У холодний період року температура повітря в офісних приміщеннях операторів становить 22–24 градуси Цельсія, а в теплий період року підтримується в межах 23–25 градусів Цельсія при відносній вологості 40–60 відсотків та швидкості руху повітря не більше 0,1 метра за секунду. На противагу цьому, у приміщенні серверної кімнати, де функціонують високопродуктивні комутатори Cisco Catalyst серії C9300 та сервери обробки даних, вимоги до мікроклімату орієнтовані на запобігання термічному перегріву напівпровідникових компонентів та накопиченню статичної електрики.

Температурний режим у серверній жорстко фіксується прецизійними системами кондиціонування у діапазоні 20–22 градусів Цельсія, а вологість утримується на рівні 50 відсотків, оскільки падіння вологості нижче 40 відсотків різко підвищує ризик електростатичних розрядів, здатних вивести з ладу порти GigabitEthernet та інтерфейсні модулі.

Раціональне проектування природного та штучного освітлення безпосередньо впливає на зорову функцію операторів логістичного центру,

які впродовж усієї зміни здійснюють моніторинг транспортних потоків та комунікують за допомогою програмного забезпечення VoIP. Відповідно до вимог ДБН В.2.5-28:2018 «Природне і штучне освітлення» [13], робочі місця операторів забезпечуються суміщеним освітленням, при якому природне світло з вікон доповнюється системою загального рівномірного штучного освітлення.

Оптимальна освітленість на поверхні робочих столів у зоні розміщення клавіатури та документації становить не менше 400 люкс, а безпосередньо на екранах моніторів – у межах 200–300 люкс [3].

Для виключення появи прямих і відбитих бліків, які викликають швидку втому очей та зниження гостроти зору, люмінесцентні або сучасні світлодіодні світильники загального освітлення комплектуються спеціальними дзеркальними растрами або дифузними розсіювачами.

Робочі столи операторів розміщуються таким чином, щоб природне світло падало з лівого боку, а вікна обладнуються регульованими сонцезахисними жалюзі для контролю інсоляції у сонячні дні. У серверному приміщенні штучне освітлення виконується лише у вигляді загального із рівнем освітленості 200 люкс, що є цілком достатнім для проведення періодичного технічного обслуговування, огляду кабельних з'єднань та моніторингу світлодіодних індикаторів на лицьових панелях комутаторів.

Основними джерелами шуму в корпоративній мережі є вентилятори охолодження серверних стійок та блоків живлення комутаційного обладнання, сумарний рівень звукового тиску від яких у серверній кімнаті може досягати 65–70 дБА. З метою захисту операторів від цього шкідливого чинника, серверний вузол проектується як повністю ізольоване приміщення з масивними стінами та звукоізоляційними дверима, що повністю виключає проникнення повітряного шуму в суміжні кабінети.

На робочих місцях самих операторів логістичного центру «Global-Express» еквівалентний рівень шуму відповідно до санітарних норм не перевищує 50 дБА, що досягається використанням малошумної офісної техніки, оздобленням стін і стелі звукопоглинальними матеріалами, а також раціональним плануванням робочих зон із достатньою питомою площею на одного працівника.

Ергономічна організація безпосереднього робочого місця оператора базується на вимогах індивідуального підбору та регулювання елементів меблевого гарнітура для зниження статичного напруження опорно-рухового апарату працівника.

Висота робочої поверхні столу встановлюється в межах 725 міліметрів, а під робочим столом забезпечується вільний простір для ніг висотою не менше 600 міліметрів та шириною не менше 500 міліметрів [3].

Робоче крісло оператора обов’язково обладнується підйомно-поворотним механізмом, що дозволяє регулювати висоту сидіння, кут нахилу спинки та висоту підлокітників для забезпечення фізіологічно правильної посадки протягом зміни.

Відеодисплейний термінал розміщується на оптимальній відстані 600–700 міліметрів від очей оператора, причому верхній край екрана повинен знаходитися трохи нижче рівня очей, щоб кут зору становив приблизно 15–20 градусів до горизонталі, що суттєво зменшує навантаження на шийний відділ хребта.

Оскільки праця операторів логістичного центру пов’язана з постійним нервово-емоційним напруженням та монотонними рухами кистей рук, внутрішнім розпорядком «Global-Express» впроваджується раціональний режим праці та відпочинку, який передбачає надання регламентованих перерв тривалістю 10 хвилин через кожні дві години роботи для виконання комплексів виробничої гімнастики та вправ для зняття зорової втоми..

ВИСНОВКИ

У ході виконання кваліфікаційної роботи було розроблено та теоретично обґрунтовано проєкт сучасної захищеної корпоративної мережі для логістичного підприємства «Global-Express». Впровадження даного проєкту дозволило створити єдину інформаційну інфраструктуру, яка об’єднує центральний офіс у місті Тернопіль із трьома регіональними складськими терміналами.

На основі аналізу інформаційних потреб підприємства була обрана та реалізована ієрархічна модель мережі, що базується на топології «зірка» на макрорівні та трирівневій моделі (ядро, розподіл, доступ) всередині об’єктів. Це забезпечило високу масштабованість та зручність адміністрування системи.

Мережа побудована з використанням сучасних стандартів Gigabit Ethernet та Wi-Fi 5, що гарантує необхідну пропускну здатність для роботи логістичного програмного забезпечення, систем ERP та передачі об’ємного відеопотоку. Впровадження технології VLAN дозволило логічно сегментувати мережу, відокремивши трафік адміністрації, логістів та систем безпеки, що суттєво підвищило загальний рівень продуктивності та безпеки.

Для з’єднання в єдину мережу віддалених складів реалізовано технології Site-to-Site VPN на основі протоколів IPsec. Використання протоколу динамічної маршрутизації OSPF у поєднанні з резервними каналами зв’язку гарантує безперебійність логістичних процесів навіть у разі відмови основного провайдера.

Працездатність розробленої архітектури було успішно верифіковано за допомогою імітаційного моделювання у середовищі Cisco Packet Tracer.

Розрахунки економічної частини показали, що загальна вартість проєкту становить 1 151 374,46 грн. Завдяки відмові від дорогих орендованих ліній на користь VPN та автоматизації процесів, очікуваний термін окупності капітальних вкладень становить 1,8 року, що підтверджує високу ефективність запропонованого рішення.

Останній розділ роботи описує питання охорони праці, та техніки безпеки, які є важливими для безпечної праці користувачів комп’ютерної техніки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Атаманчук П. С. Охорона праці в галузі: навч. посіб. / П. С. Атаманчук, В. В. Мендерецький, О. П. Панчук, Р. М. Білий. – К.: Центр учбової літератури, 2017. – 322

2. Буров Є., Митник М. Комп'ютерні мережі.(у 2-х томах) Львів, Магнолія, 2018.

3. Грибан В. Г., Фоменко А. Є., Казначеєв Д. Г. Безпека життєдіяльності та охорона праці : підруч. / В. Г. Грибан, А. Є. Фоменко, Д. Г. Казначеєв. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. 388 с

4. Єфіменко А. А. Основи побудови локальних комп'ютерних мереж Ethernet на базі керованих комутаторів компанії Cisco : навчальний посібник. – Житомир : Житомирська політехніка, 2021. – 116 с.\

5. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2016 р.) - 500 с.

6. Комп'ютерні мережі / О. Д. Азаров, С. М. Захарченко, О. В. Кадук, М. М. Орлова, В. П. Тарасенко // Навчальний посібник. – Вінниця: ВНТУ, 2013./МОНУ (Лист №1/11 – 8260 від 15.05 2015 р.) – 500 с.

7. Технології захисту локальних мереж на основі обладнання CISCO : навч. посібник / Т. І. Коробейнікова, С. М. Захарченко. – Львів: Видавництво Львівської політехніки, 2021. – 188 с.

8. Базові поняття мережевих технологій. URL: http://um.co.ua/8/8-17/8-1748.html. Дата звернення: 6.06.2026.

9. ДБН В.2.5-56:2014 "Системи протипожежного захисту". URL: https://dbn.co.ua/load/normativy/dbn/dbn_v_2_5_56_2014_sistemi_protipozhezhnogo_zakhistu/1-1-0-1204. (Дата звернення: 7.06.2026)

10. Правила пожежної безпеки в Україні : НАПБ А.01.001-2014: зат. наказом Міністерства внутрішніх справ України від 30.12.2014 р. № 1417: зареєстр. в Мін-ві юстиції України 05.03.2015 р. за № 252/26697. Київ: МВС

України, 2015. 114 с НПАОП 0.00-7.15-18

11. Державні санітарні норми мікроклімату виробничих приміщень : ДСанПіН 3.3.6.042-99 : постанова Головного державного санітарного лікаря України від 01.12.1999 р. № 42. URL: https://zakon.rada.gov.ua/laws/show/va042282-99 (дата звернення: 05.06.2026).

12. App.Diagrams сайт для створення схем URL: https://app.diagrams.net. (Дата звернення: 9.06.2026)

13. Одескабель Cat.6 URL: https://odeskabel.com/ua/products/katalog-lan/lan-kabeli-kategorii-6/uutp-4pr-indoor.html. (Дата звернення: 2.06.2026)

14. Південкабель ОПТ-24А4 URL: https://www.yuzhcable.info/edata/mrr/501001090120072144/lang/en. (Дата звернення: 1.06.2026)

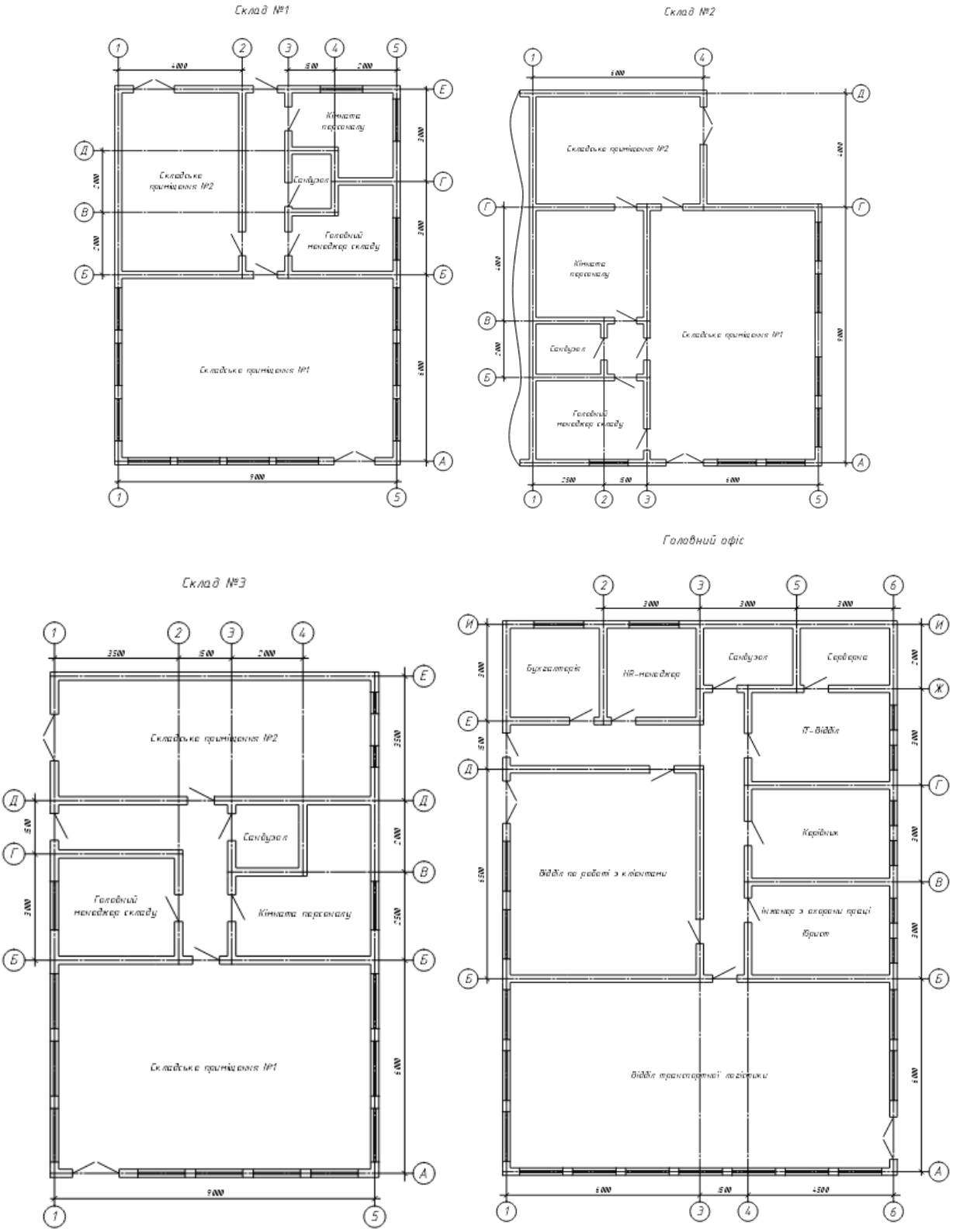
15. Комутатор Cisco Catalyst C9300-24S URL: https://stack-systems.com.ua/kommutator-cisco-ws-c9300-24s (Дата звернення: 2.06.2026)

16. Комутатор Cisco Catalyst C9200L-24P-4X URL: https://stack-systems.com.ua/kommutator-cisco-ws-c9200-24p-4x (Дата звернення: 2.06.2026)

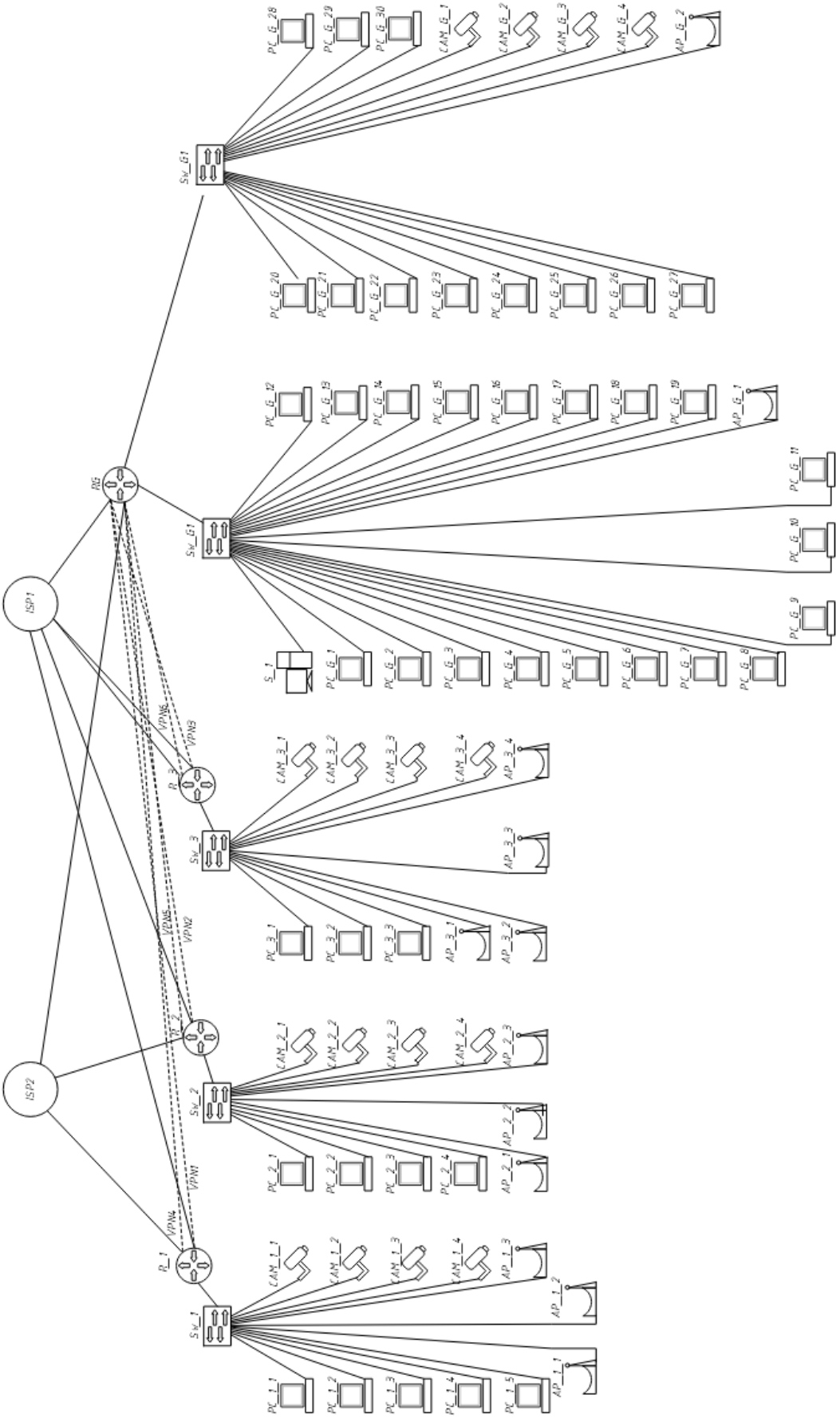
17. PowerEdge R760 Rack Server URL: https://www.dell.com/en-us/shop/cty/pdp/spd/poweredge-r760/pe_r760_tm_vi_vp_sb (Дата звернення: 3.06.2026)

ДОДАТКИ

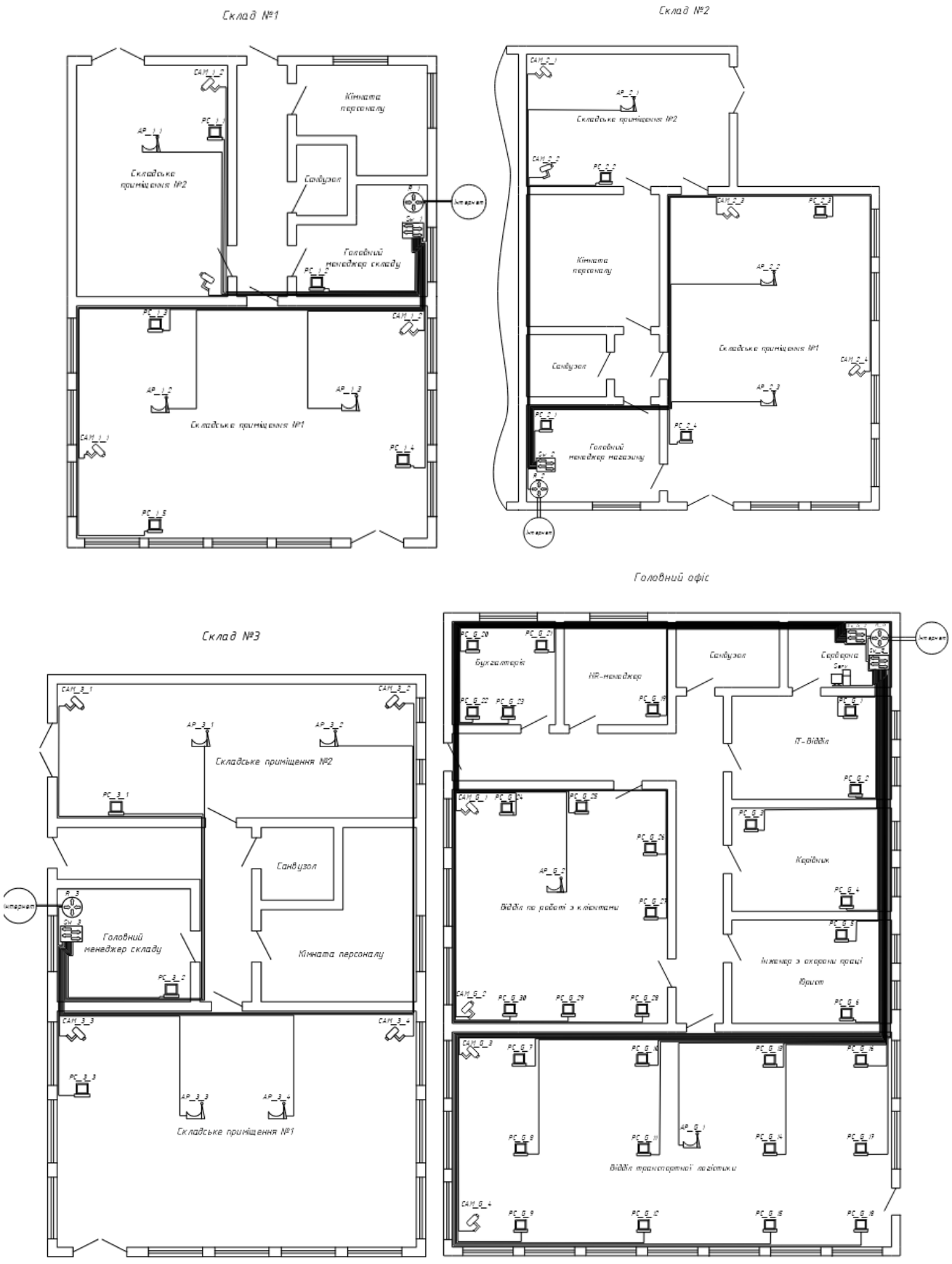
Додаток А. План приміщень будівель головного офісу та складських приміщень логістичної компанії «Global-Express»



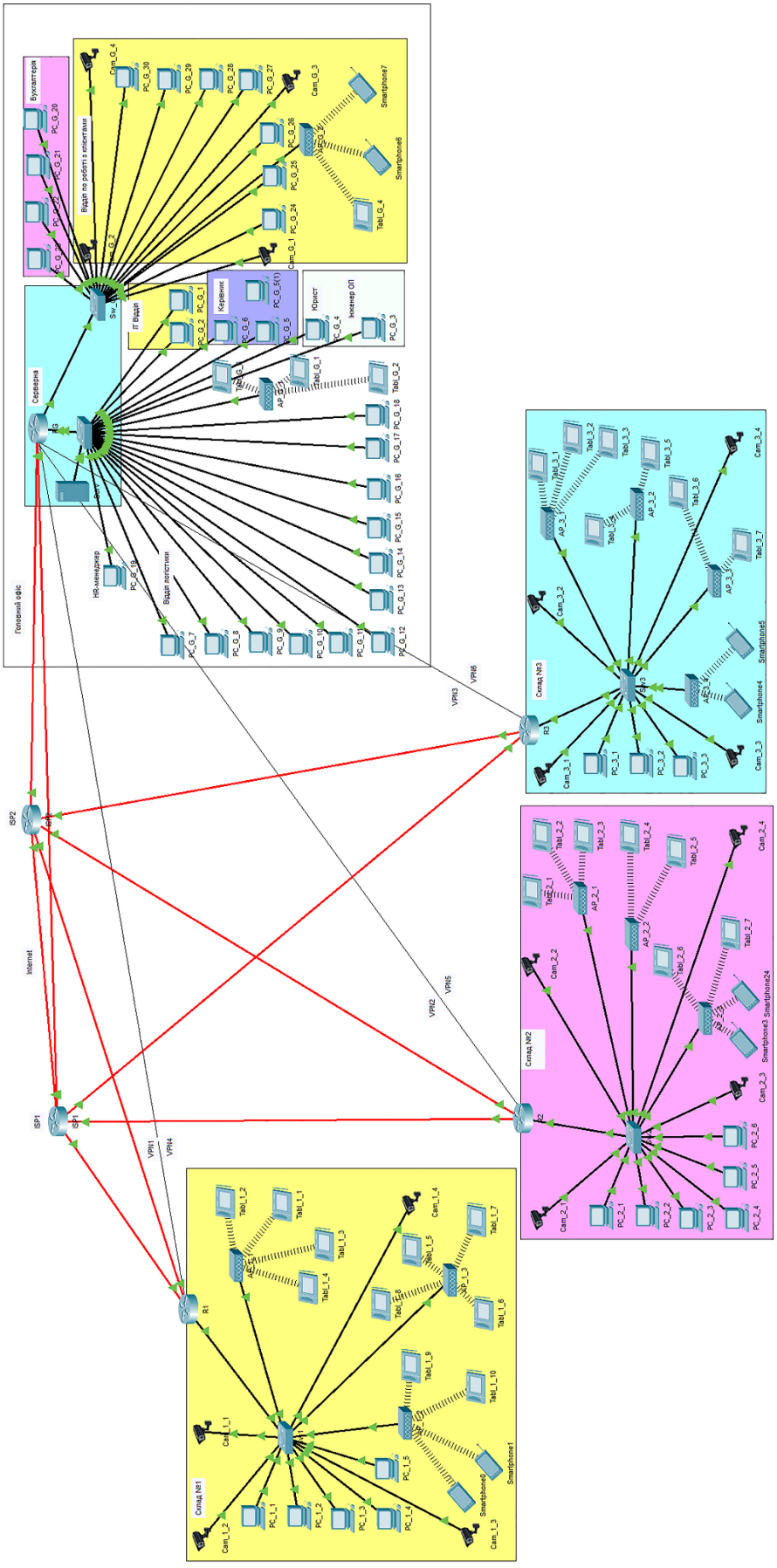
Додаток Б. Логічна топологія мережі логістичної компанії «Global-Express»



Додаток В. Схема прокладання мережевих кабелів в будівлях логістичної компанії «Global-Express»



Додаток Г. Модель мережі в Cisco Packet Tracer



Додаток Д. План евакуації на випадок пожежі

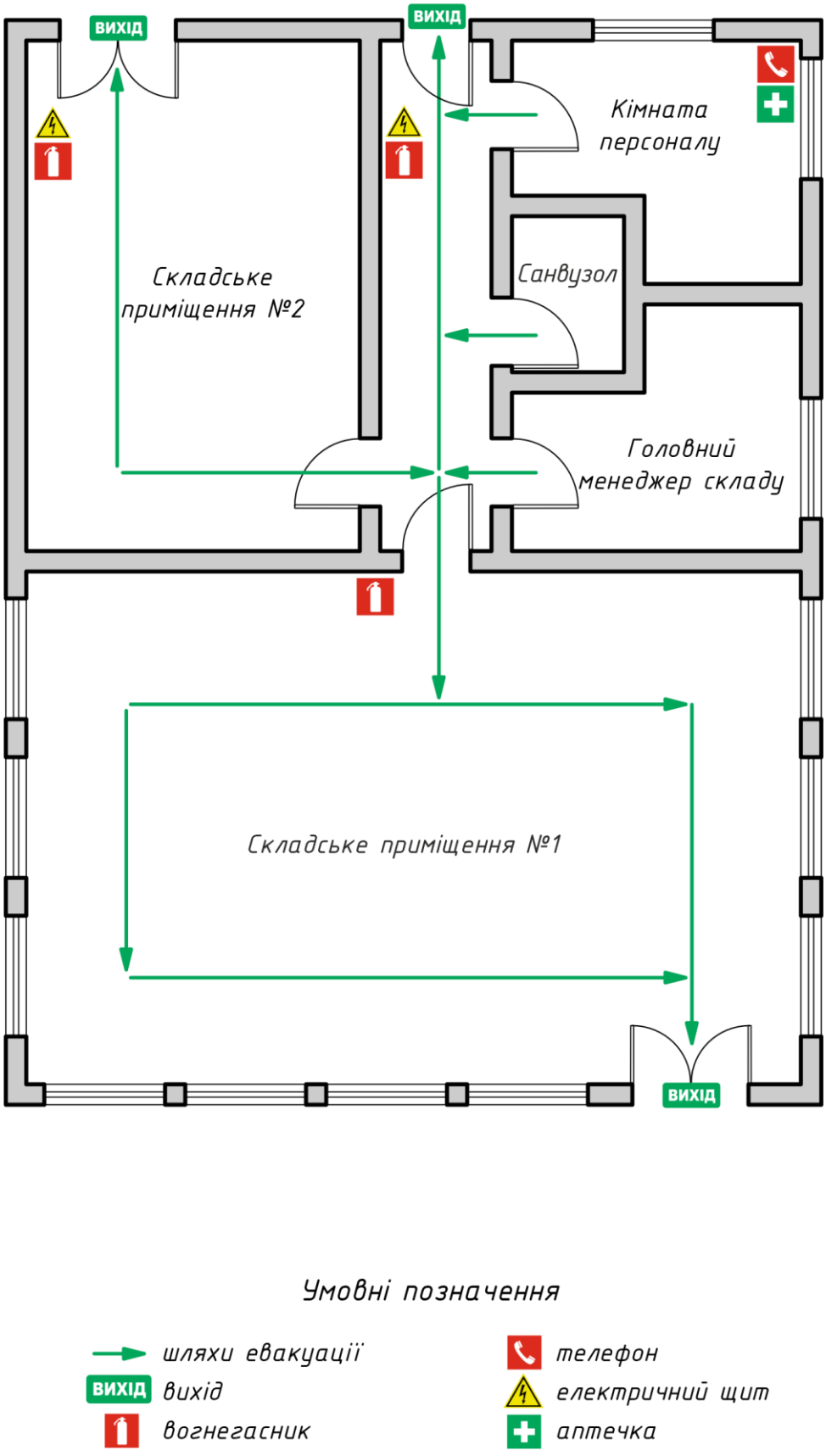


Рисунок Д.1 – План евакуації на випадок пожежі зі складу №1

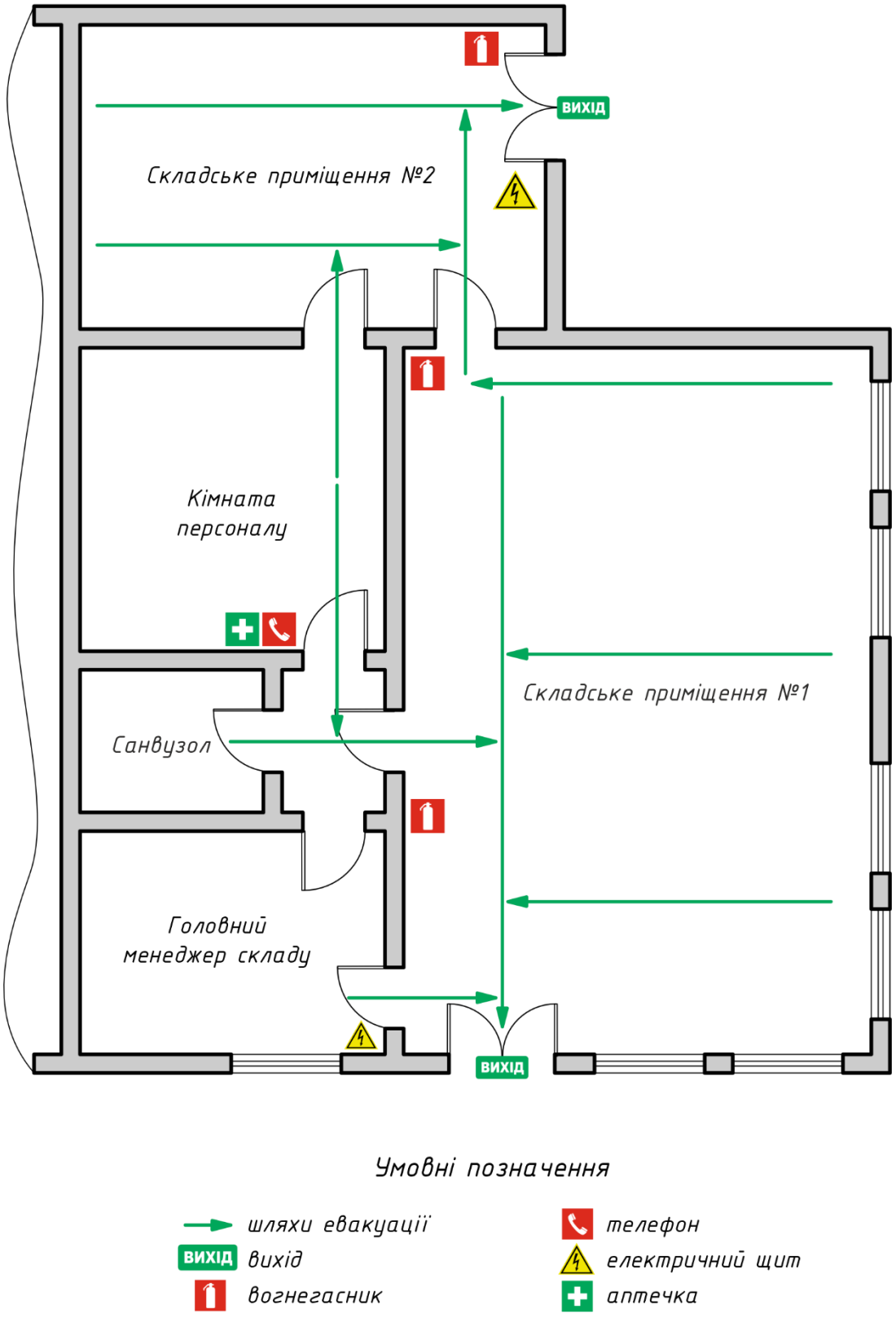


Рисунок Д.2 – План евакуації на випадок пожежі зі складу №2

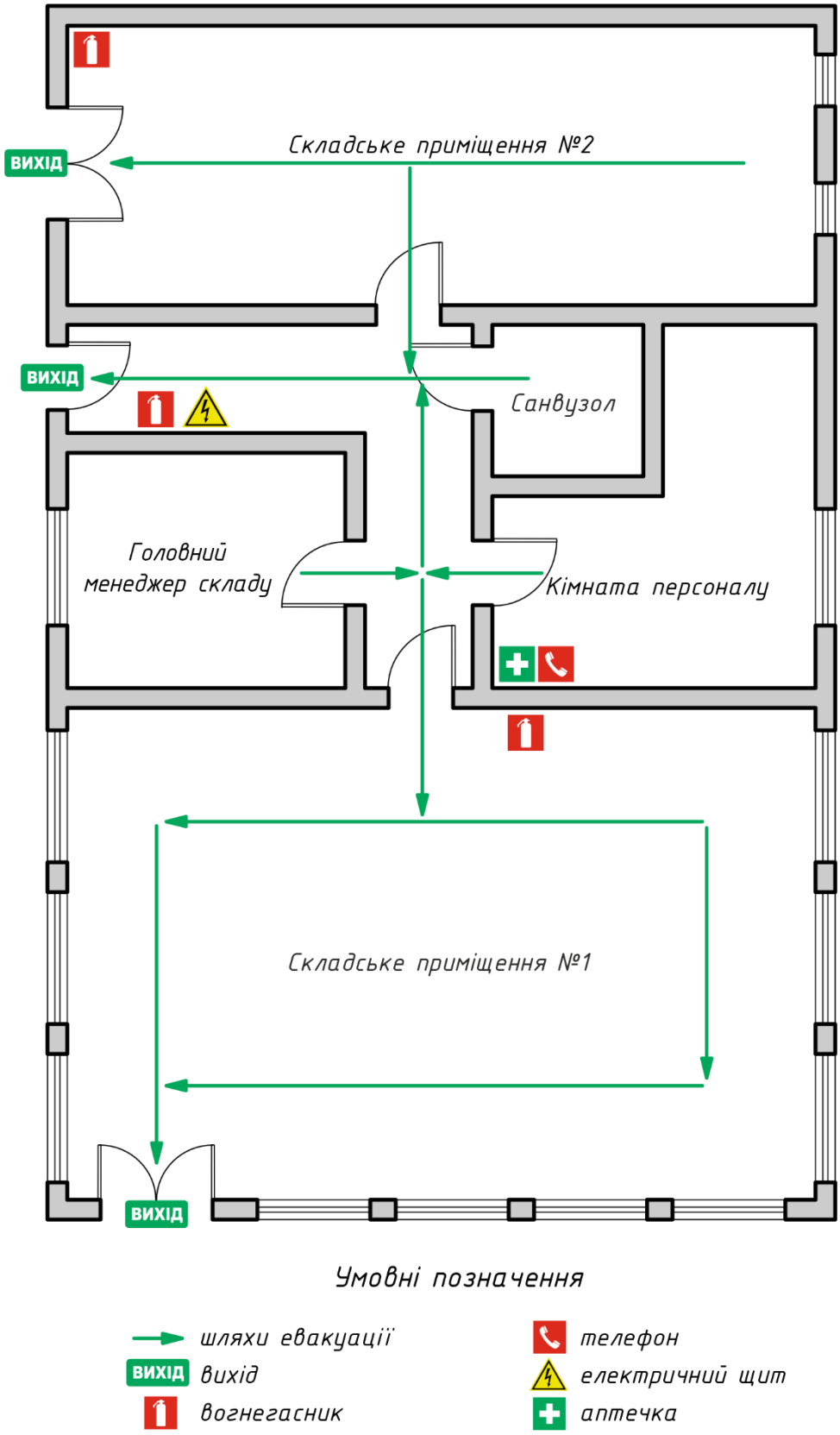


Рисунок Д.3 – План евакуації на випадок пожежі зі складу №3

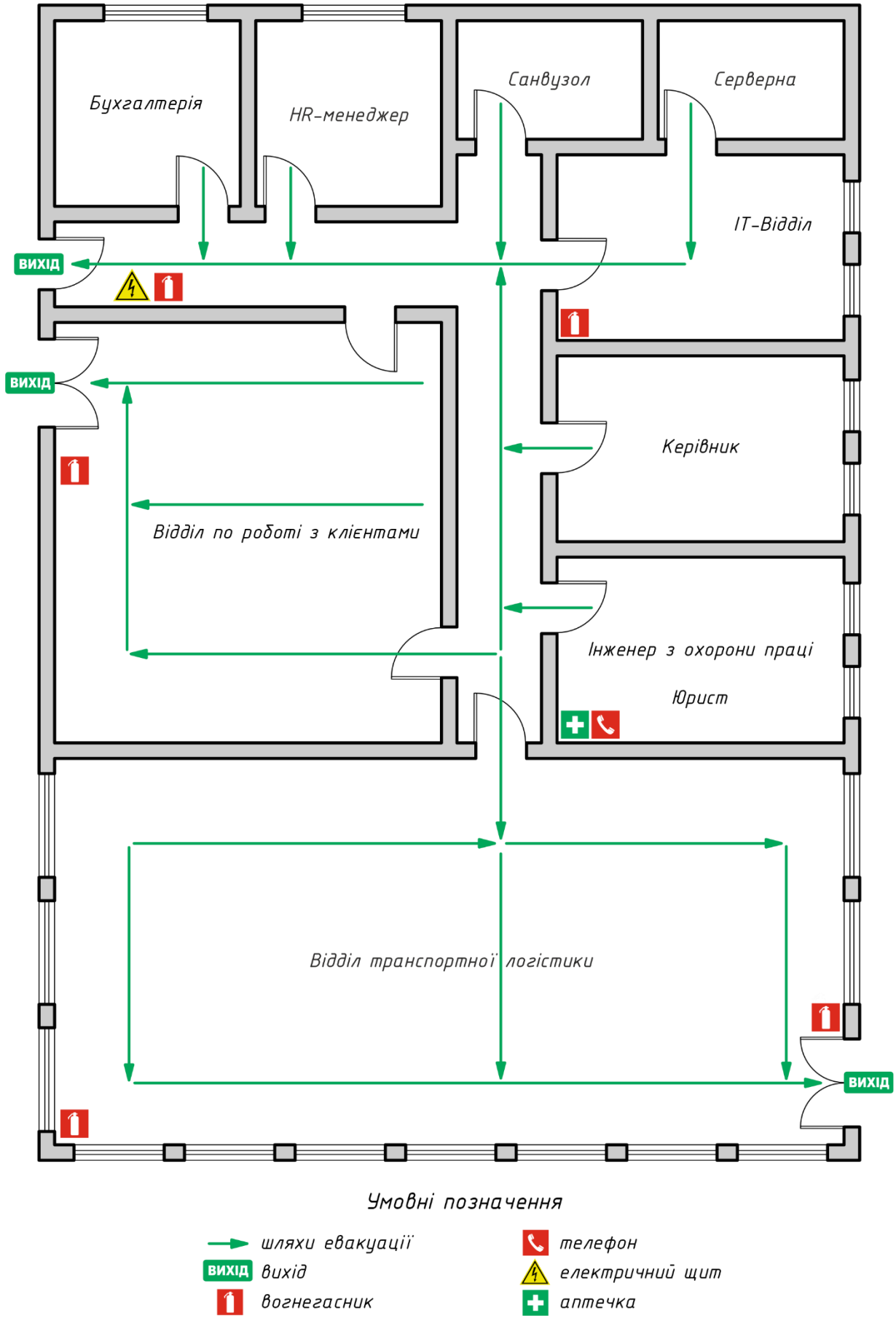


Рисунок Д.4 – План евакуації на випадок пожежі із головного офісу