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

фахового молодшого бакалавра
(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі супермаркетів "Торба"**

Виконав: студент IV курсу, групи КІ-412

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

_____ Назарій КОРВАЧ
(ім'я та прізвище)

Керівник Ігор КАПАЦІЛА
(ім'я та прізвище)

Рецензент _____
(ім'я та прізвище)

Тернопіль – 2025

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
"31" березня 2025 року

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

Корвачу Назарію Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі супермаркетів "Торба"**

керівник роботи Капаціла Ігор Богданович
(прізвище, ім'я, по батькові)

Затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університету імені Івана Пулюя» від 28.03.2025р № 4/9-166а.

2. Строк подання студентом роботи: 13 червня 2025 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;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Богдана МАРТИНЮК викладач		
Охорона праці та безпека життєдіяльності	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	05.05	
3	Написання першого розділу	16.05	
4	Розробка технічного та робочого проекту	23.05	
5	Написання спеціального розділу	30.05	
6	Розрахунок економічної частини	2.06	
7	Написання розділу охорони праці	4.06	
8	Виконання графічної частини	9.06	
9	Оформлення проєкту	11.06	
10	Погодження нормоконтролю	12.06	
11	Попередній захист роботи	13.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 01 квітня 2025 року

Студент _____ Назарій КОРВАЧ
(підпис) (ім'я та прізвище)

Керівник роботи _____ Ігор КАПАЦІЛА
(підпис) (ім'я та прізвище)

ЗМІСТ

АНОТАЦІЯ 6

Вступ 9

1 Загальний розділ 10

1.1 Технічне завдання 10

1.1.1 Найменування та область застосування 10

1.1.2 Призначення розробки 10

1.1.3 Вимоги до програмного забезпечення**Ошибка! Закладка не определена.**

1.1.4 Вимоги до програмної документації**Ошибка! Закладка не определена.**

1.1.5 Техніко-економічні показники ..... **Ошибка! Закладка не определена.**

1.1.6 Стадії та етапи розробки ..... **Ошибка! Закладка не определена.**

1.1.7 Порядок контролю та прийому..... **Ошибка! Закладка не определена.**

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі..... **Ошибка! Закладка не определена.**

2 **РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ** 21

2.1 Опис та обґрунтування вибору логічного типу мережі 21

2.2 Розробка схеми фізичного розташування кабелів та вузлів: 26

2.2.1 Типи кабельних з’єднань та їх прокладка**Ошибка! Закладка не определена.**

2.2.2 Будова вузлів та необхідність їх застосування 28

2.3 Обґрунтування вибору обладнання для мережі (пасивного та активного**)** 30

2.4 Особливості монтажу мережі 33

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі 34

2.6 Тестування та налагодження мережі .. **Ошибка! Закладка не определена.**

3 Спеціальний розділ 39

3.1 Інструкція з налаштування програмного забезпечення серверів 39

3.2 Інструкції з налаштування активного комутаційного обладнання..... 41

3.3 Інструкція з використання тестових наборів та тестових програм 52
3.4 Інструкція по налаштуванню засобів захисту мережі 58
3.5 Інструкція з експлуатації та моніторингу в мережі 61
4 ЕКОНОМІЧНА ЧАСТИНА 64
4.1 Визначення стадій технологічного процесу та загальної тривалості розробки та реалізації проекту комп'ютерної мережі супермаркетів "Торба"65
4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи 65
4.3 Розрахунок матеріальних витрат 67
4.4 Розрахунок витрат на електроенергію 69
4.5 Розрахунок суми амортизаційних відрахувань 69
4.6 Обчислення накладних витрат 70
4.7 Складання кошторису витрат та визначення собівартості ндр 70
4.8 Розрахунок ціни ндр 71
4.9 Визначення економічної ефективності і терміну окупності капітальних вкладень 71
5 Охорона праці, техніка безпеки та екологічні вимоги 73
5.1 Державні нормативні акти про охорону праці 73
5.2 Дії працівників у випадку виникнення пожежі 75
5.3 Засоби захисту людини від шкідливих речовин 76
Висновки 788
Перелік посилань 800
ДОДАТОК А 82

АНОТАЦІЯ

Корвач Н.М. Розробка проєкту комп'ютерної мережі супермаркетів "Торба": кваліфікаційна робота на здобуття освітньо-професійного ступеня фаховий молодший бакалавр за спеціальністю «123 – Комп’ютерна інженерія». Тернопіль: ВСП «ТФК ТНТУ», 2025. 92 с., рис. – 3, табл. – 11, кресл. – 4, додат. – 1.

Ключові слова: локальна мережа, віртуальні підмережі, VLAN, сервери, активні комутаційні пристрої, налаштування.

Кваліфікаційна робота присвячена розробці мережевої системи для мережі супермаркетів «Торба» .

В результаті аналізу потенційного інформаційного трафіку між відділами мережі супермаркетів «Торба» було сформовано технічне завдання на проектування локальної комп’ютерної мережі. Проаналізовано можливі варіанти та обрано топологію та архітектуру для побудови мережі. Визначено місця розташування та моделі активного комутаційного устаткування. Проведено поділ адресного простору на підмережі. Розроблено фізичну та логічну топології. Вибрано операційні системи серверного обладнання та робочих станцій. Подано інструкції для налаштування серверів та комутаторів компанії. Для перевірки коректності налаштувань розроблено модель мережі.

ANNOTATION

Korvach N.M. Development of a network system for the supermarket chain «TOR-BA»: qualification work for the educational and professional degree of professional junior bachelor in the specialty «123 – Computer engineering». Ternopil: VSP «TFK TNTU», 2025. 92 p., fig. – 3, table. – 11, fig. – 4, appendix. – 1 .

Keywords: DEVOPS, TERRAFORM, JENKINS,AWS, local network, virtual subnets, VLAN, servers, active switching devices, settings.

The qualification work is devoted to the development of a network system for the supermarket chain «TOR-BA» .

As a result of the analysis of potential information traffic between departments of the supermarket chain «TOR-BA»

terms of reference for the design of a local computer network were formed. Possible options were analyzed and the topology and architecture for building the network were selected. Locations and models of active switching equipment have been determined. The address space was divided into subnets. Physical and logical topologies have been developed. Operating systems of server equipment and workstations are selected. Instructions for configuring the company's servers and switches are provided. A network model has been developed to check the correctness of the settings.

ПЕРЕЛІК СКОРОЧЕНЬ

CLI – Command Line Interface;

DHCP – Dynamic Host Configuration Protocol;

DNS – Domain Name System;

IEEE – Institute of Electrical and Electronics Engineers;

MAC – Media Access Control;

PoE - Power over Ethernet;

RMON – Remote Network MONitoring;

SNMP – Simple Network Management Protocol;

SSH – Secure Shell;

USB – Universal Serial Bus;

VLAN – Virtual Local Area Network;

ВДТ – відео-диспдейний термінал;

ЛОМ – локальна обчислювальна мережа;

НДР – науково-дослідні роботи;

ПЗ – програмне забезпечення;

ПТОВ – пункт технічного обслуговування вогнегасників;

СКС – структурована кабельна система.

АРМ – автоматизоване робоче місце;

КС – комп’ютерна система;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

Ethernet – технологія передачі даних по мережі

ВСТУП

Сьогодні триває епоха бурхливого розвитку обчислювальних мереж. Границі між локальними та глобальними мережами постійно стираються, багато в чому завдяки появі локальних каналів зв'язку, що не поступаються за швидкістю кабельним системам локальних мереж. Глобальні мережі надають такі ж зручні та прозорі сервіси доступу до ресурсів, як і локальні мережі. Локальні мережі теж зазнають змін. З’явилася велика кількість різноманітних комунікаційних пристроїв, на кшталт комутаторів, маршрутизаторів та шлюзів. Ці пристрої дозволили зводити великі корпоративні мережі зі складними структурами, які об’єднують тисячі комп’ютерів.

Також спостерігається дуже важлива тенденція, яка однаково вплинула як на локальні, так і на глобальні мережі. Вони почали обробляти інформацію, яка раніше ніколи не опрацьовувалась в комп’ютерних мережах, наприклад, голос, відеопотоки та зображення. Це вимагало змін у протоколах, мережевих операційних системах та комунікаційному обладнанні. Поява трафіку реального часу кинула нові виклики, оскільки традиційні послуги комп'ютерних мереж, наприклад, передача файлів та електронна пошта, генерують трафік, нечутливий до затримок, і всі елементи мережі були спроектовані, щоб справлятися саме з ним.

На сьогоднішній день ці проблеми вирішуються різними способами за допомогою технологій, розроблених спеціально для передачі різних типів трафіку. Проте, у цій галузі ще багато роботи для досягнення довгоочікуваної мети - конвергенції всіх інформаційних мережевих технологій, зокрема комп'ютерів, телефонів і телебачення, а також локальних та глобальних мереж.

Під час виконання кваліфікаційної роботи бакалавра передбачається розробка мережі для компанії «ТОРБА». Завдання полягає у розробці проекту мережі, здатної ефективно та надійно передавати всі види інформації, як в межах локальної мережі, так і через Інтернет. Цей проект базуватиметься на сучасних досягненнях у галузі розробки комп’ютерних мереж.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання:

1.1.1 Найменування та область застосування

Найменування проєкту — Розробка проєкту комп'ютерної мережі супермаркетів "Торба"

Область застосування — даний проєкт призначений для створення масштабованої, безпечної та високопродуктивної комп’ютерної інфраструктури, яка охоплює всі філії торгової мережі “Торба” у межах міста та/або регіону. Розроблена мережа має забезпечити:

- безперервний обмін даними між центральним офісом та віддаленими торговими точками;
- централізовану обробку транзакцій, логістику товарообігу та підтримку POS-терміналів;
- доступ до внутрішніх інформаційних систем і баз даних з урахуванням політик безпеки;
- можливість розширення мережі без потреби в повному переоснащенні інфраструктури.

Сфера застосування охоплює повсякденну діяльність супермаркетів: облік товарів, автоматизацію касових операцій, підтримку відеоспостереження, телефонного зв’язку та корпоративної електронної пошти. Система також повинна бути адаптована до вимог майбутньої інтеграції з CRM/ERP-системами та резервного копіювання даних.

1.1.2 Призначення розробки

Призначенням даної розробки є створення комплексного технічного рішення з проєктування комп’ютерної мережі для супермаркетів торгової мережі «Торба»,

що дозволить забезпечити надійну, захищену та ефективну передачу даних між усіма структурними підрозділами підприємства.

Розробка спрямована на:

- забезпечення сталого функціонування автоматизованих робочих місць касирів, адміністраторів, бухгалтерів та керівного складу;
- організацію інтегрованої локальної мережі з можливістю віддаленого адміністрування та централізованого контролю ресурсів;
- оптимізацію внутрішніх бізнес-процесів шляхом впровадження мережевих технологій для обміну інформацією, управління залишками товарів, проведення фінансових операцій;
- створення платформи для впровадження додаткових інформаційних сервісів — відеоспостереження, IP-телефонії, внутрішнього чату та резервного копіювання даних;
- зменшення ризиків інформаційних втрат, несанкціонованого доступу та мережевих збоїв завдяки побудові резервованої та захищеної архітектури мережі.

Таким чином, проєкт виконує роль ключового етапу цифрової трансформації мережі супермаркетів «Торба» та створює надійну основу для подальшої автоматизації торговельної діяльності.

1.1.3 Вимоги до апаратного та програмного забезпечення

Для реалізації комп’ютерної мережі супермаркетів «Торба» висуваються технічні вимоги до апаратного та програмного забезпечення, які гарантують стабільну, безпечну та масштабовану роботу всієї мережевої інфраструктури.

Апаратне забезпечення

Мережеве обладнання повинно забезпечувати підтримку сучасних стандартів передачі даних, мати високий рівень надійності та можливість централізованого адміністрування:

- Комутатори: керовані комутатори рівня L2/L3 із підтримкою VLAN,

QoS, STP/RSTP, SNMP (наприклад, TP-Link JetStream, Cisco Catalyst);

- Маршрутизатори: із підтримкою VPN, DHCP, NAT, фаєрволом, інтерфейсами Gigabit Ethernet (наприклад, MikroTik, Ubiquiti EdgeRouter);
- Точки доступу Wi-Fi: з підтримкою стандартів IEEE 802.11ac/ax (для забезпечення бездротового зв'язку в торгових залах і службових приміщеннях);
- Сервери: для централізованого зберігання даних, доступу до баз даних, контролю доступу (рекомендовано — з процесорами Intel Xeon, 32+ ГБ ОЗП, RAID-масивами);
- Робочі станції: ПК з мінімум 8 ГБ ОЗП, SSD, мережевою картою 1Gbps;
- Джерела безперебійного живлення (UPS) для захисту критичних вузлів мережі від збоїв електроживлення;
- Кабельна інфраструктура: категорія не нижче Cat 6, патч-панелі, розетки, кроси, організатори кабелю.

Програмне забезпечення

Програмні компоненти повинні забезпечити управління, безпеку та ефективність мережевих процесів:

- Операційні системи: Windows Server або Linux-дистрибутиви (Ubuntu Server, CentOS) для серверів; Windows 10/11 або Linux Mint для робочих станцій;
- Системи віртуалізації: Proxmox, VMware ESXi або VirtualBox для створення ізольованих середовищ;
- Системи резервного копіювання: Veeam, Bacula, Acronis Backup;
- Мережеве ПЗ: утиліти для моніторингу (Nagios, Zabbix), адміністрування (WinBox, Putty, SSH);
- Антивірусне програмне забезпечення: корпоративні рішення (наприклад, ESET Endpoint Security, Kaspersky Endpoint Security);
- Системи обліку товарів та касового обслуговування: сумісні з локальною мережею рішення з підтримкою хмарної або локальної бази (наприклад, Comarch ERP, BAS Роздріб);
- Фаєрвол/UTM-рішення: для захисту від зовнішніх загроз (наприклад, pfSense, FortiGate).

Усі компоненти повинні бути сумісними між собою, забезпечувати гнучку масштабованість та мінімальний час простою при модернізації або відновленні. Програмне забезпечення має бути ліцензійним або з відкритим вихідним кодом.

1.1.4 Вимоги до документації

Комплексна документація, що супроводжує проєкт комп'ютерної мережі супермаркетів «Торба», повинна забезпечувати повну технічну, експлуатаційну та супровідну інформацію для всіх етапів — від проєктування до впровадження та обслуговування.

Документація має відповідати вимогам чинних нормативів і включати такі основні компоненти:

- Пояснювальна записка — текстовий супровід до проєктного рішення, що містить обґрунтування вибору апаратного й програмного забезпечення, опис логіки побудови мережі, визначення функціонального призначення підсистем;
- Мережева структура — схема логічної та фізичної топології мережі із зазначенням типів з'єднань, IP-адресації, VLAN-розподілу та зв'язків між вузлами;
- Специфікація обладнання — перелік необхідних апаратних засобів з детальними технічними характеристиками, марками, кількістю та місцем встановлення;
- Конфігураційна документація — інструкції з налаштування маршрутизаторів, комутаторів, серверів, точок доступу, опис параметрів безпеки, NAT, VPN, DHCP, DNS;
- Інструкція користувача — рекомендації для персоналу щодо використання інформаційних ресурсів мережі, доступу до внутрішніх сервісів та правил взаємодії з технічною підтримкою;
- Регламент обслуговування та моніторингу — переліки планових технічних дій, графіки перевірок працездатності, резервного копіювання, оновлення ПЗ, а також дії у разі аварійних ситуацій;
- Журнал змін і оновлень — контроль версій конфігурацій, фіксація змін

у мережевій інфраструктурі та оновлення програмних компонентів.

Уся документація повинна бути структурована, уніфікована за форматом, оформлена згідно з вимогами технічного діловодства та придатна для використання в умовах подальшої експлуатації та масштабування мережі.

1.1.5 Техніко-економічні показники

Техніко-економічні показники проєкту комп'ютерної мережі супермаркетів «Торба» відображають доцільність його впровадження з огляду на технічну ефективність, фінансову обґрунтованість та потенційну рентабельність у довгостроковій перспективі.

Основні показники включають:

Технічна ефективність

- Пропускназдатність мережі: не менше 1 Гбіт/с для внутрішньої локальної мережі та щонайменше 100 Мбіт/с для зовнішнього з'єднання з мережею Інтернет;
- Час відгуку внутрішніх сервісів: не більше 2 мс у межах філії, до 10 мс між торговими точками;
- Кількість підтримуваних робочих місць: проєктована мережа здатна обслуговувати від 50 до 150 одночасно підключених пристроїв у кожній торговій точці;
- Наявність резервування: включає резервне живлення, дублювання каналів зв'язку та серверного зберігання для уникнення втрати даних.

Економічна доцільність

- Орієнтовна вартість впровадження: залежно від масштабу (від однієї філії до всієї мережі), вартість реалізації базового варіанту проєкту становить приблизно 120 000 – 250 000 грн;
- Термін окупності: завдяки автоматизації обліку, зменшенню простоїв обладнання та підвищенню швидкості обслуговування клієнтів очікуваний період окупності становить 12–18 місяців;

- Зменшення експлуатаційних витрат: впровадження моніторингу та централізованого адміністрування дозволяє зменшити витрати на технічне обслуговування до 30% порівняно з неавтоматизованими точками;
- Підвищення продуктивності персоналу: за рахунок зменшення часу обробки інформації та збоїв — орієнтовно на 15–20%.

Інтеграційний потенціал

- Мережева структура передбачає подальше розширення без радикального переобладнання;
- Підтримка сучасних технологій (хмарні сервіси, IP-телефонія, відеоспостереження) — гарантує актуальність інфраструктури протягом наступних 5–7 років.

Таким чином, проєкт не лише вирішує актуальні технічні завдання, а й демонструє значний економічний ефект для підприємства, сприяючи підвищенню конкурентоспроможності торговельної мережі «Торба».

1.1.6 Стадії та етапи розробки

Процес розробки проєкту комп'ютерної мережі супермаркетів «Торба» поділяється на низку логічних стадій, кожна з яких включає визначені етапи з чітко сформульованими цілями, завданнями та очікуваними результатами. Такий підхід забезпечує послідовність реалізації проєкту, знижує ризики помилок і підвищує ефективність впровадження.

Стадія 1: Аналітична та підготовча

Етап 1.1. Вивчення структури підприємства та потреб користувачів Аналіз організаційної схеми супермаркетів, кількості робочих місць, особливостей облікових систем, обміну даними, географічного розміщення торгових точок.

Етап 1.2. Оцінка існуючих IT-ресурсів Інвентаризація наявного обладнання, каналів зв'язку, програмного забезпечення, визначення критичних вузлів і вузьких місць у поточній інфраструктурі.

Стадія 2: Проєктування мережі

Етап 2.1. Розробка логічної структури мережі Побудова топології, визначення сегментів, IP-адресації, маршрутів, політик доступу.

Етап 2.2. Вибір апаратного і програмного забезпечення Обґрунтований підбір маршрутизаторів, комутаторів, серверного обладнання, ПЗ для керування та моніторингу.

Етап 2.3. Підготовка проєктної документації Складання специфікацій, схем, інструкцій для подальшого монтажу та налаштування.

Стадія 3: Впровадження

Етап 3.1. Закупівля і встановлення обладнання Монтаж мережевих пристроїв, прокладка кабельної інфраструктури, встановлення серверів і робочих станцій.

Етап 3.2. Конфігурація і тестування мережі Налаштування маршрутизації, бездротових точок доступу, серверних служб, перевірка працездатності з'єднань.

Етап 3.3. Проведення пілотного запуску Тестування системи в умовах реального навантаження, виявлення та усунення недоліків.

Стадія 4: Завершальна та супровід

Етап 4.1. Документування результатів розробки Оновлення технічної документації відповідно до фактичної реалізації.

Етап 4.2. Навчання персоналу та передача об’єкта в експлуатацію Проведення інструктажу для працівників, передача інструкцій та схем обслуговування.

Етап 4.3. Підготовка до подальшої підтримки та масштабування Визначення процедур супроводу, переліку критичних оновлень та каналів технічної підтримки.

1.1.7 Порядок контролю та прийому

Контроль якості виконання робіт та приймання проєкту комп'ютерної мережі супермаркетів «Торба» здійснюється відповідно до затверджених етапів розробки, технічних вимог і нормативних документів, що регламентують побудову інформаційних систем.

1. Контроль розробки та реалізації

На кожному з етапів проєкту проводиться внутрішній технічний контроль відповідності результатів встановленим вимогам:

Контроль проєктної документації — перевірка на повноту, відповідність стандартам, логічну цілісність схем та обґрунтованість обраного обладнання;

Контроль монтажу та конфігурації — інспектування якісного виконання прокладки кабелів, підключення обладнання, правильності налаштувань комутаторів, маршрутизаторів, серверних служб;

Функціональне тестування — перевірка працездатності мережі: зв'язність між вузлами, коректність маршрутизації, безперебійність доступу до внутрішніх сервісів, стабільність бездротового з'єднання;

Перевірка безпеки — тестування фаєрволу, VPN-підключень, обмеження прав доступу, захищеність внутрішньої інформації.

2. Порядок приймання

Остаточне приймання мережі до експлуатації проводиться комісією, яка складається з представників технічного відділу, адміністрації та, за потреби, зовнішнього аудитора. Приймання здійснюється в такій послідовності:

3. Ознайомлення з проєктною та звітною документацією;

4. Проведення натурних випробувань мережі згідно з контрольними сценаріями;

5. Фіксація результатів у протоколі приймання з вказанням зауважень (якщо такі є);

6. Підписання акту здачі-передачі мережі в експлуатацію;

7. Передача комплекту технічної документації та інструкцій персоналу

замовника.

У разі виявлення недоліків під час перевірки розробник зобов'язується усунути їх у встановлений строк без додаткових витрат з боку замовника. Тільки після повного усунення зауважень система вважається прийнятою.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства, для якого створюється проект мережі

Мережа супермаркетів «ТОРБА» заснована на українському ринку рітейлів в 2011 році. На сьогоднішній день є сорок маркетів, що представлені у Івано-франківській, Чернівецькій, Тернопільській, Волинській, Рівненській, Миколаєвській, Херсонській та у Львівський області! В Торбі висока якість, помірна ціна, повний асортимент, простота у придбанні товару. ТОРБА – це вигідні покупки. Їхня перевага – максимальне скорочення «відстані» від виробника до споживача, щоб клієнти могли купувати товари за вигідною ціною. Сотні виробників, постачальників і працівників мережі турбуються, щоб товари були доступними та вигідними для всіх покупців, а програма лояльності допомагає купувати з розумом. Автономність кожного магазину Кожний із 40 магазинів мережі має свою систему акцій, що задовольняє потреби місцевого населення у всіх регіонах. Усі постачальники прагнуть, щоб їх товар став вашим улюбленим, тому регулярно розігрують приємні подарунки. Також вони працють з місцевими виробниками, яких так люблять покупці кожного регіону. Кілька форматів ТОРБА – мережа різних форматів! Свою роботу спершу вони розпочали з великих склад-маркетів із суцільним торговим залом та загальною площею від 1900 до 2500 м. кв. Такі магазини чудово підходять для великих щотижневих закупів, однак через великий розмір маркету не у всіх містах вдавалося розмістити його якомога ближче до центру. Тому було знайдено ідеальне рішення – експрес-маркет - новий компактний формат (площа від 400 до 1200 м. кв.), який ідеально підходить для спальних районів і щоденних покупок.

Супермаркети мережі «ТОРБА»

Супермаркети мережі «ТОРБА» у більшості представлені на західній Україні.

Знайти їх можна за такими адресами:

1. Чернівецька обл., м.Чернівці, пров. Складський, 1 (08.00 – 22.00)

2. Івано-Франківська обл., м. Івано-Франківськ, вул. Максимовича, 15 (08.00 – 22.00)

3. Івано-Франківська обл., м. Івано-Франківськ, вул. Коновальця, 100 (08.00 – 22.00)

4. Івано-Франківська обл., м. Коломия, вул. Русина,4а (08.00 – 20.00)

5. Івано-Франківська обл., м. Коломия, вул. Шухевича, 59 (08.00 – 22.00)

6. Івано-Франківська обл., м. Калуш, бульвар Незалежності, 2б (08.00 – 20.00)

7. Івано-Франківська обл., м. Надвірна, вул. Соборна, 165 (08.00 – 21.00)

8. Львівська область., м. Стрий, вул. Симона Петлюри, 103 (08.00 – 20.00)

9. Тернопільська обл., м. Тернопіль, вул Стуса, 1 (08.00 – 22.00)

10. Рівненська обл., м. Рівне, вул. Київська, 67 (08.00 – 22.00)

11. Рівненська обл., м. Рівне, вул. Коновальця, 1б (08.00 – 22.00)

12. Рівненська обл., м. Рівне, вул. Вербова, 1а (08.00 – 22.00)

13. Волиньська обл., м. Луцьк, вул Єршова, 11 (08.00 – 22.00)

14. Миколаївська обл., м. Миколаїв, вул. Космонавтів, 81 (08.00 – 22.00)

15. Херсонська обл., м. Нова Каховка, вул. Першотравнева, 17 (08.00 – 22.00)

16. Івано-Франківська обл., м. Коломия, вул. Романа Шухевича, 59 (08.00 – 22.00)

17. Львівська обл, м. Львів., вул. Зубрівська, 3 (08.00 – 22.00)

В супермаркетах виділяють три основні зони для торговельних залів:

1. Вхідна зона – це зона де знаходиться вхід у супермаркет, розташований відразу ж за вхідними дверима магазина. Це те саме місце, де відвідувач має перемикати свою головну увагу з того, що було зовні магазину, на вулиці, на те, що знаходиться в приміщенні супермаркету. Ця зона має обережно підводити відвідувачів до покупки продуктів з перших же секунд відвідування магазину,

викликати особливий інтерес і почуття комфорту від відвідування магазину. Як правило тут розміщують найбільш привабливі товари, як за ціною, так і за зовнішнім виглядом: різноманітні новинки, сучасні сезонні пропозиції та різноманітні за планом акції, продукти миттєвого попиту, товари розпродажу.

2. Касова зона – це завжди жвава та «гаряча» зона, де покупці масово простоюють в черзі на ту чи іншу касу, та дуже часто схильні до розсіювання своєї основної увагу на непотрібні їм та зайві товари, та здійснювати спонтанні непотрібні їм покупки. Тут, як правило, розміщують стелажі з різноманітними солодощами, батарейками, запальничками, сірниками, жуйками, стікерами кави, серветками, журналами та іншими популярними товарами спонтанного та імпульсного попиту.

Зона основного потоку – це, найбільш важлива та значуща зона в торговому приміщенні супермаркету, тобто те що відповідає за кількість зроблених та можливих в наступному покупок основного асортименту товарів супермаркету. Для магазинів з площею понад 1 000 м^2 важливо, щоб вона працювала дуже ефективно, тому використовують різноманітне маркування, особливі вказівники та інші візуально–ефективні засоби для виділення та особливого впорядкування основних маршрутних магістралей торгівельного залу супермаркету.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Загальна структура комп'ютерної мережі, спроектованої відповідно до вимог технічного завдання для супермаркету «ТОРБА», відображена на схемі, поданій на рисунку 2.1.

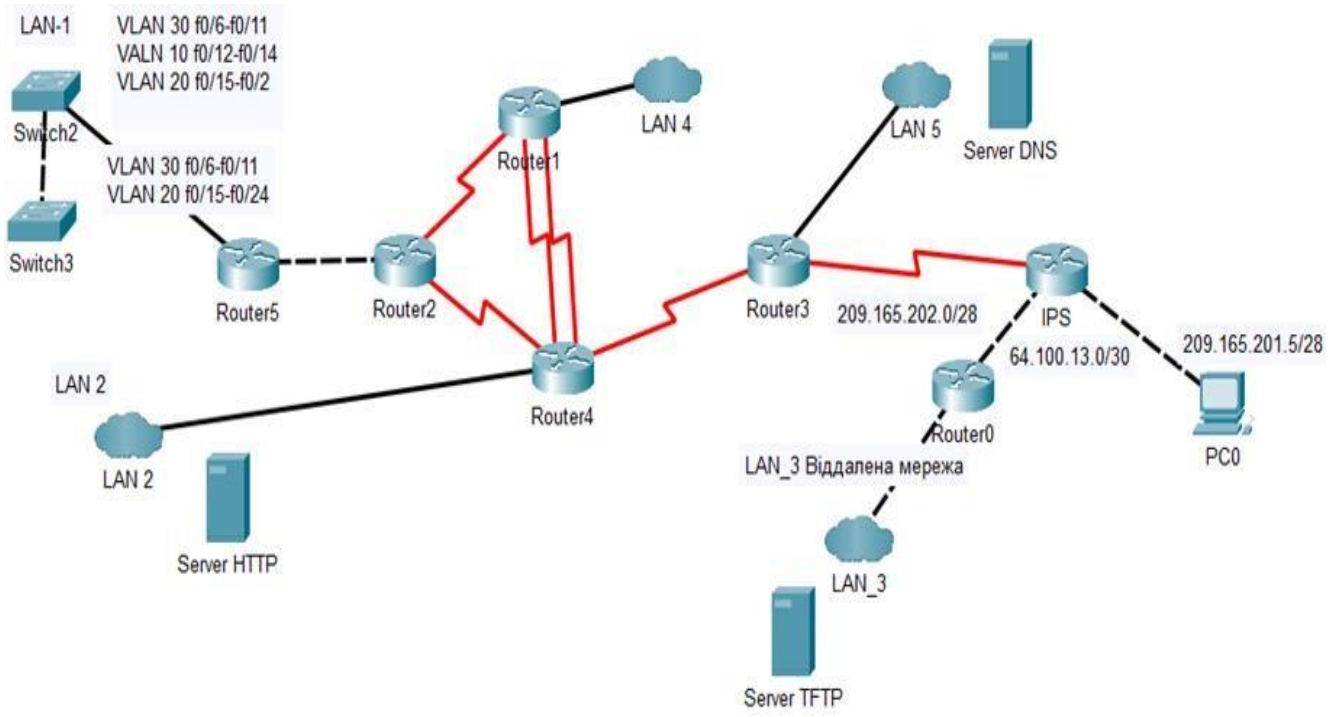

Рисунок 2.1 – Топологічна схема мережевої інфраструктури супермаркету «ТОРБА»

Основні параметри підмереж, які були визначені при проєктуванні локальної мережі цього торгового закладу, мають такі значення:

- виділений блок IP-адрес для подальшого поділу: 10.24.IPn.0/21;
- значення змінної IPn для даного блоку адрес: IPn = 24;
- очікувана кількість хостів у сегменті LAN1: 31 пристрій;
- кількість вузлів у підмережі LAN2: 97 одиниць;
- мережеві пристрої в сегменті LAN3: 31;

- підключення до підмережі LAN4: 70 клієнтів;
- сегмент LAN5 включає 23 пристрої;
- максимальна інтенсивність трафіку в мережі: 203 кадри за секунду.

Загалом, проектна кількість активних пристроїв у всіх підмережах складає 252 (31 + 97 + 31 + 70 + 23).

Для організації IP-адресації комп'ютерної мережі супермаркету «ТОРБА» використано IP-діапазон 10.24.24.0/21. З метою раціонального розподілу адресного простору було застосовано підхід VLSM (Variable Length Subnet Masking) — методику, що передбачає використання змінної довжини маски підмережі.

Цей метод дозволяє оптимально формувати підмережі відповідно до реальної потреби у кількості хостів. VLSM — це розширення концепції CIDR (Classless Inter-Domain Routing), що забезпечує гнучке керування IP-ресурсами. На відміну від класичних схем із фіксованими масками, використання VLSM дає змогу застосовувати індивідуальні маски до різних підмереж в межах одного IP-діапазону. Завдяки цьому забезпечується більш ефективне використання адресного простору без зайвих витрат IP-адрес, що особливо важливо при великій кількості дрібних сегментів у мережі.

Таким чином, підхід на основі VLSM дозволив адаптувати кожну підмережу до конкретної кількості пристроїв у ній, що зробило структуру мережі супермаркету не лише логічною, але й технологічно оптимізованою.

Таблиця 2.1 – Вихідні дані КС магазинів «ТОРБА»

LAN1	LAN2	LAN3	LAN4	LAN5
31	97	31	70	23

Отримані дані табл. 2.2 застосовані для виконання адресації пристроїв в підмережах підприємства «ТОРБА». Результат розподілу IP-арес наведений в табл. 2.3

Таблиця 2.2 – Схема адресації мереж КС «ТОРБА»

Назва підмережі	Розмір	Адреса	Десяткова маска	Діапазон доступних адрес
LAN2	126	10.24.24.0/25	255.255.255.128	10.24.24.1 - 10.24.24.126
LAN4	126	10.24.24.128/25	255.255.255.128	10.24.24.129 - 10.24.24.254
LAN1	62	10.24.25.0/26	255.255.255.192	10.24.25.1 - 10.24.25.62
LAN3	62	10.24.25.64/26	255.255.255.192	10.24.25.65 - 10.24.25.126
LAN5	30	10.24.25.128/27	255.255.255.224	10.24.25.129 - 10.24.25.158
WAN1	2	10.10.3.0	255.255.255.252	10.10.3.1 - 10.10.3.2
WAN2	2	10.10.3.4	255.255.255.252	10.10.3.5 - 10.10.3.6
WAN3	2	10.10.3.8	255.255.255.252	10.10.3.9 - 10.10.3.10
WAN4	2	10.10.3.12	255.255.255.252	10.10.3.13 - 10.10.3.14
WAN5	2	10.10.3.16	255.255.255.252	10.10.3.17 - 10.10.3.18
WAN IPS	2	209.165.202.0	255.255.255.252	209.165.202.1- 209.165.202.2
WAN Remout	2	64.100.13.0	255.255.255.252	64.100.13.1- 64.100.13.2
LAN IPS	2	209.165.201.0	255.255.255.240	209.165.200.1 - 209.165.200.16

Логічна структура мережі, яка реалізується в межах торговельної мережі магазинів «ТОРБА», охоплює п’ять окремих підмереж. Її архітектура сформована відповідно до внутрішньої організаційної будови компанії та враховує специфіку функціонування кожного підрозділу.

Попри можливі відмінності у фізичному розміщенні обладнання, логічна побудова мережі передбачає деревоподібну топологію на рівні глобального сегменту WAN (Wide Area Network). Така схема дозволяє ефективно організувати маршрути обміну даними між різними ділянками інфраструктури. Водночас локальні сегменти LAN (Local Area Network), що обслуговують окремі підрозділи або робочі групи, реалізовані за класичною топологією "зірка", яка забезпечує

централізоване управління та високу надійність з'єднань.

Всі ці підмережі об’єднані за допомогою комутаційного обладнання, що взаємодіє з маршрутизаторами через інтерфейси типу Serial та GigabitEthernet. Комунікація між маршрутизаторами відбувається із використанням протоколу динамічної маршрутизації EIGRP (Enhanced Interior Gateway Routing Protocol), який дозволяє автоматично визначати найефективніші маршрути передавання інформації.

Особливу роль у загальній схемі виконує Філія №1, яка функціонує як віддалений сегмент мережі. Вона забезпечує постійний канал зв'язку з головним офісом та синхронізацію даних із центральними ресурсами, що гарантує цілісність інформаційного простору підприємства.

Таблиця 2.3 – Схема адресації маршрутизаторів

Ім'я пристрою	Інтерфейс	IP-адреса	Маска	Шлюз	VLAN	Інтерфейс підключеного пристрою
1	2	3	4	5	6	7
Korvach_R1	G0/1	10.24.24.129	/25	-	--	G0/1
	S0/0/1	10.10.3.2	/30	-	-	S0/1/0
	S0/0/0	10.10.3.9	/30	-	-	S0/0/0
	S0/1/0	10.10.3.13	/30	-	-	S0/1/0
Korvach _R2	S0/0/1	10.10.3.1	/30	-	-	S0/0/1
	S0/0/0	10.10.3.5	/25	-	-	S0/0/0
Korvach _R5	G0/0	10.10.3.22	/30	-	-	G0/0
	G0/1.13	10.24.24.1	/27	-	13	G0/1.13
	G0/1.23	10. 24.24.33	/27	-	23	G0/1.23
	G0/1.33	10. 24.24.65	/27	-	33	G0/1.33
	G0/1.99	10. 24.24.96	/28		99	G0/1.99

Продовження таблиці 2.3

1	2	3	4	5	6	7
Korvach _R0	G0/2	10.24.25.64	/26	-	-	G0/2
	G0/0	64.100.13.2	/30	-	-	G0/0
Wireless_R0	Internet	10.24.25.66	/26	10.24.25.66	-	F0/24
DCL-100	Internet	10.24.25.67	/27	10.24.25.66	-	F0/23
Korvach _R3	S0/1/0	10.10.3.18	/30	-	-	S0/1/0
	G0/1	10.24.25.129	/27	-	-	G0/1
	S0/2/0	209.165.202.2	/30	-	-	S0/2/0
Rout_IPS	S0/2/0	209.165.202.1	/28	-	-	S0/2/0
	G0/0	64.100.13.1	/30	-	-	G0/0
	G0/1	209.165.201.1	/28	-	-	G0/1
Korvach _R4	G0/1	10.24.24.1	/25	-	-	G0/1
	S0/1/0	10.10.3.10	/30	-	-	S0/1/0
	S0/0/0	10.10.3.6	/30	-	-	S0/0/0
	S0/0/1	10.10.3.14	/30	-	-	S0/1/0
	S0/1/1	10.10.3.17	/30	-	-	S0/1/1
Korvach _Sw11	Vlan99	10.24.24.98	/28	10.24.24.97	99	G0/2
Korvach _Sw12	Vlan99	10.24.24.99	/28	10.24.24.97	99	G0/2
Korvach _Sw2	Vlan1	10.24.24.2	/25	10.24.24.1	-	G0/1
Korvach _Sw3	Vlan1	10.24.25.66	/26	10.24.25.65	-	G0/1
Korvach _Sw4	Vlan1	10.24.24.130	/25	10.24.24.129	-	G0/1
Korvach _Sw5	Vlan1	10.24.25.130	/27	10.24.25.129	-	G0/2

У структурі комп’ютерної мережі торговельної мережі «ТОРБА» реалізовано п’ять логічно розмежованих підмереж. Загальна архітектура побудована відповідно до внутрішньої організації підприємства, де кожна підмережа обслуговує певний функціональний або адміністративний підрозділ.

Передача даних між окремими частинами мережі здійснюється за логічною топологією типу "дерево", яка реалізована у сегменті WAN (Wide Area Network). Така структура дозволяє централізовано керувати потоками інформації, водночас зберігаючи гнучкість у масштабуванні. В локальних сегментах (LAN — Local Area

Network), що об’єднують робочі станції, касові термінали та периферійне обладнання в межах окремих магазинів чи офісів, застосовано топологію "зірка", що забезпечує зручне адміністрування та високу надійність з’єднання.

Міжсегментне з’єднання реалізовано через мережеві комутатори, які фізично підключаються до маршрутизаторів за допомогою кабельних інтерфейсів типу Serial та GigabitEthernet. Обмін даними між маршрутизаторами здійснюється з використанням EIGRP (Enhanced Interior Gateway Routing Protocol) — протоколу внутрішньої динамічної маршрутизації, що дозволяє оптимально формувати таблиці маршрутів відповідно до змін у мережевій топології.

Особливе значення має філіал №1, який функціонує як віддалений вузол загальної мережевої інфраструктури. Його головним завданням є підтримка стабільного з’єднання з головним офісом і забезпечення безперервного обміну інформацією з центральними системами компанії.

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.2.1 Типи кабельних з’єднань та їх прокладка

У межах побудови фізичної структури комп’ютерної мережі супермаркетів «Торба» основну роль відіграє правильний вибір типів кабелів, способів їх прокладки та монтажу. Від цих рішень залежать стабільність з’єднання, швидкість передачі даних, зручність обслуговування та перспективи масштабування мережі.

Використані типи кабельних з’єднань

Вита пара (UTP Cat 6)

Основний тип кабелю, застосований для з’єднання робочих станцій, касових апаратів, принтерів, серверного обладнання та мережевих комутаторів. Обрана категорія 6 забезпечує швидкість передачі до 1 Гбіт/с з можливістю подальшого оновлення до 10 Гбіт/с на коротких відстанях.

Оптичне волокно (Single-mode / Multi-mode)

Використовується для міжповерхового або міжбудинкового з’єднання

(наприклад, між серверною та торговим залом), де необхідна передача на великі відстані без втрати якості сигналу. Оптоволоконні лінії забезпечують високу пропускну здатність та захист від електромагнітних завад.

Коаксіальний кабель

Обмежено застосовується для систем відеоспостереження, якщо використовуються аналогові камери (у разі гібридної архітектури мережі), але в нових реалізаціях перевага надається IP-камерам із живленням по Ethernet.

Кабелі живлення (електроживлення обладнання)

Прокладаються окремо, з дотриманням електробезпеки та норм відстані до інформаційних кабелів для запобігання наведенням та перешкодам.

Способи прокладки кабелів

Підвісна прокладка в коробах (кабель-каналах) — найбільш поширений варіант для офісів, касових зон і технічних приміщень. Забезпечує естетику, легкий доступ для обслуговування та модернізації.

Прокладка під фальшпідлогою або в підвісній стелі — актуально для залів із високими вимогами до інтер'єру. Кабелі ховаються у спеціальних трасах з додатковим маркуванням.

Прокладка в гофрованих трубах або металорукавах — використовується в місцях із високою вологістю або де можливі механічні навантаження (склади, технічні кімнати).

Вертикальна прокладка стояками — між поверхами або зонами через телекомунікаційні шахти із кріпленням до стін або стояків.

Загальні вимоги до монтажу

Забезпечення мінімальної довжини кабелю без зниження якості сигналу;

Уникнення натягу, перегинів і різких кутів кабелів;

Обов'язкове маркування обох кінців кожного кабелю;

Відокремлення силових ліній від сигнальних (мінімум 30 см);

Організація кабелів у патч-панелях, кабельних органайзерах та шафах для впорядкованості й легкого обслуговування.

Таким чином, обрані типи кабелів і методи прокладки відповідають сучасним

стандартам і забезпечують ефективну роботу мережі з урахуванням вимог до швидкості, надійності та можливості розширення.

2.2.2 Будова вузлів та необхідність їх застосування

У структурі комп'ютерної мережі супермаркетів «Торба» ключовими елементами є мережеві вузли, які забезпечують функціональність, керованість і стійкість інформаційного середовища. Кожен вузол виконує конкретні завдання в межах локальної та розподіленої мережевої архітектури.

1. Центральний комутаційний вузол (ядро мережі)

Будова:

Керований комутатор рівня L3 (наприклад, Cisco Catalyst);

Основний маршрутизатор з підтримкою VPN, NAT, Firewall;

Сервер резервного копіювання і файловий сервер;

Джерело безперебійного живлення (UPS);

19-дюймова серверна шафа для розміщення обладнання;

Система охолодження (вентиляція або кондиціонер).

Необхідність застосування:

Цей вузол є центром усіх обчислювальних і комунікаційних процесів. Він забезпечує маршрутизацію між VLAN-сегментами, доступ до Інтернету, взаємодію з базами даних, обмін між касами та центральним обліком, а також забезпечує централізоване адміністрування.

2. Локальні вузли у торгових точках

Будова:

Невеликий керований або некерований комутатор (8–24 порти);

Точка доступу Wi-Fi для персоналу або клієнтів;

Каса/робочі місця підключені через виту пару;

Локальний принтер або сканер;

IP-камера (у разі потреби відеоспостереження);

Джерело безперебійного живлення на 500–1000 ВА.

Необхідність застосування:

Забезпечують підключення всіх пристроїв у межах торгової зали до загальної мережі. Дають можливість незалежного функціонування кожного магазину навіть при тимчасовій втраті зв’язку з центральним вузлом, з подальшою синхронізацією після відновлення.

3. Вузол бездротового доступу (Wi-Fi)

Будова:

Потужна точка доступу стандарту 802.11ac/ax;

PoE-інжектор або PoE-комутатор;

Антенне обладнання (залежно від розміщення).

Необхідність застосування:

Забезпечує мобільність співробітників, роботу зі сканерами штрихкодів, планшетами, POS-терміналами. Також — організацію гостьового доступу для покупців з обмеженням швидкості та доступу до внутрішніх ресурсів.

4. Серверний вузол (локальний або центральний)

Будова:

Сервер баз даних (PostgreSQL);

Сховище даних RAID (NAS/SAN);

Програмне забезпечення ERP або облікової системи;

Операційна система (Windows Server / Linux);

Системи моніторингу та журналювання (Zabbix).

Необхідність застосування:

Обробка транзакцій, ведення бази товарів, клієнтів, звітів, журналів касових операцій. Централізує управління інформаційними потоками, дозволяє вести аналітику та забезпечує зберігання критичних даних.

5. Вузли відеоспостереження (опційно)

Будова:

IP-камери з PoE або автономним живленням;

Мережевий відеореєстратор (NVR);

Сховище на HDD (2–4 ТБ);

Веб-інтерфейс доступу для адміністратора.

Необхідність застосування:

Контроль касових зон, складів, входів/виходів; підвищення безпеки; можливість перегляду архіву подій у разі конфліктних ситуацій або порушень.

Таким чином, побудова мережі базується на гнучкій архітектурі вузлів, які можуть масштабуватися та адаптуватися під потреби супермаркетів. Розділення на локальні, центральні та спеціалізовані вузли дозволяє досягти стабільності, безпеки та зручності в обслуговуванні всієї мережі.

2.3 Обґрунтування вибору обладнання для мережі (пасивного та активного)

Підбір головного комутатора наведено в таблиці 2.4. Вибір виконується із наявного на даний час обладнання на ринку. Для забезпечення достатнього рівня захисту передбачається використання шифрованого каналу передачі інформації та фільтрування трафіку по MAC адресі.

Обрано комутатор Cisco Catalyst C1000-24T-4G-L , який забезпечить високу надійність та якість роботи мережі

Рисунок 2.2 - Комутатор Cisco Catalyst C1000-24T-4G-L

Таблиця 2.4 - Порівняльна таблиця комутаторів для центрального вузла мережі

Параметр	Cisco Catalyst C1000-24T-4G-L	MikroTik CRS326-24G-2S+RM	TP-Link JetStream T2600G-28TS	Ubiquiti UniFi Switch USW-Pro-24
Кількість портів RJ-45 (1G)	24	24	24	24
Порти SFP / SFP+	4 x SFP (1G)	2 x SFP+ (10G)	4 x SFP (1G)	2 x SFP+ (10G)
Пропускна здатність	56 Gbps	64 Gbps	56 Gbps	128 Gbps
Продуктивність (пересилання)	41.67 Mpps	95.2 Mpps	41.7 Mpps	95.23 Mpps
Рівень управління	L2 (із базовим L3)	L3 (статична маршрутизація)	L2+ (статична маршрутизація)	L2+
Підтримка VLAN, QoS, STP, SNMP	Так	Так	Так	Так
Веб-інтерфейс / CLI / SSH	CLI, SNMP, Web	Web, CLI, WinBox	Web, CLI, SNMP	UniFi Controller (Web/Cloud)
Споживання енергії	~20 Вт	~21 Вт	~23 Вт	~25 Вт
Резервне живлення / UPS-порт	Ні	Ні	Ні	Так (через SmartPower)
Ціна (орієнтовно)	≈ 14 000–17 000 грн	≈ 7 500–9 000 грн	≈ 10 000–12 000 грн	≈ 13 000–16 000 грн
Переваги	Надійність, сумісність з Cisco	Потужність, SFP+, гнучке ПЗ	Доступний, простий в керуванні	Інтеграція з екосистемою UniFi
Недоліки	Висока ціна	Менш відома ОС (SwOS/RouterOS)	Обмеження по Layer 3	Потребує UniFi Controller

Також в даній мережі передбачається підключення клієнтів за допомогою точки доступу DIR-2150 (див. рисунок 2.3) вибраної виходячи з таблиці 2.2.

Таблиця 2.4 – Порівняльна таблиця вибору точки доступу

Модель	D-Link DIR-2150	Edimax EW-7206PDG	TP-LINK TL-Archer C90
Ціна			243грн
Версія протоколу Wi-Fi	802.11ac, 802.11g, 802.11n	802.11b, 802.11g	802.11ac, 802.11g, 802.11n
Режими роботи	Точка доступу / міст	AP Station Bridge	AP Mode AP Client Mode AP+ Bridge mode
Швидкість передачі даних (Мбіт/с)	2100	300	1800
Додаткові можливості	64/128-бітне WEP-шифрування Wi-Fi Protected Access (WPA/WPA2) WPS (PIN/PBC) Web-інтерфейс	Шифрування WEP, WPA і WPA2 Підтроимка Radius серверів с EAP-MD5	—
Гарантія	12 міс	36 міс	12 міс

Рисунок 2.3 - Зовнішній вигляд точки доступу DAP-1155

Характеристики точки доступу наступні:

DAP-1155 – багатофункціональна безпровідна точка доступу для мереж підприємств. Точка доступу розроблена для установки в приміщеннях і надає

розширені функції, включаючи Турбо-режим із швидкістю з'єднання до 108 Мбіт/с, функції безпеки і якості обслуговування (QOS), а також підтримку декількох режимів роботи дозволяючи розгортати керовані і надійні безпровідні мережі.

2.4 Особливості монтажу мережі

Монтаж кабельної інфраструктури виконується відповідно до норм, встановлених стандартом EIA/TIA-569, із дотриманням вимог до топології та розміщення комутаційних вузлів.

1. У зв’язку з тим, що мережа охоплює два окремі приміщення, у кожному з них передбачено встановлення окремого проміжного комутаційного вузла.

2. Довжина ліній з’єднання між головним комутаційним центром, проміжними вузлами та горизонтальними кабельними сегментами не повинна перевищувати граничні значення, зазначені в таблиці 2.5.

Таблиця 2.5 – Максимально допустимі довжини кабельних ліній для різних середовищ передачі

№	Тип кабельного середовища	Горизонтальний кабель ↔ Горизонтальний комут. вузол	Горизонтальний кабель ↔ Проміжний комут. вузол	Проміжний комут. вузол ↔ Горизонтальний комут. вузол
1	Багатомодовий оптоволоконний	2000 м	500 м	1500 м
2	Одномодовий оптоволоконний	3000 м	500 м	2500 м
3	Вита пара (для передачі голосу)	800 м	500 м	300 м
4	Вита пара (для передачі даних)	90 м	90 м	90 м

3. Для головного мережевого вузла відведене окреме технічне приміщення, розташоване в кабінеті №113.

4. Всі приміщення, що задіяні під розміщення мережевого обладнання, відповідають нормам електробезпеки та вимогам пожежної безпеки. У них

підтримується стабільна температура на рівні 21°C, вологість — 30–50%, рівень освітлення становить 500 люкс на висоті 2,6 метра. Розетки для живлення встановлено по дві на кожні 1,8 м лінійної стіни.

5. Забезпечено вільний доступ до всіх елементів мережі, включаючи монтажні шафи, проміжні вузли та головний комутаційний центр.

6. Двері до комутаційного приміщення мають ширину 90 см, відкриваються назовні та гарантують контрольований доступ відповідно до вимог інформаційної безпеки.

7. Устаткування розміщується на відстані не менше 50 см від стін. Монтажна шафа — стандартна модель Master Group MGW125FM-B (габарити 500×620×610 мм, 12U, чорного кольору), перед якою залишено щонайменше 80 см вільного простору для обслуговування.

8. Для організації захищеної прокладки кабелів використовуються кабельні короби Marshall Tufflex, що відповідають вимогам до механічного захисту та естетики.

2.5 Обґрунтування вибору операційних систем та програмного забезпечення для серверів та робочих станцій в мережі

Вибір операційних систем і прикладного програмного забезпечення для інформаційної інфраструктури супермаркетів «Торба» обумовлюється вимогами до стабільності, масштабованості, безпеки та зручності обслуговування мережевих ресурсів.

Серверна частина: Ubuntu Linux 22.04 LTS

На серверному обладнанні обґрунтовано використано операційну систему Ubuntu Linux 22.04 LTS (Long Term Support), яка поєднує високу продуктивність, стабільність, гнучкість налаштування та підтримку з боку світової спільноти.

Переваги такого вибору:

Безкоштовна ліцензія з відкритим кодом, що зменшує загальну вартість впровадження мережі;

Довгострокова підтримка (до 2027 року) з оновленнями безпеки та виправленнями, що важливо для критичних систем;

Сумісність із популярним серверним програмним забезпеченням, таким як Samba, OpenSSH, Apache/Nginx, PostgreSQL, а також із системами віртуалізації (KVM, Docker, Proxmox);

Знижена вразливість до вірусів та шкідливого ПЗ завдяки гнучкій політиці прав доступу та потужним вбудованим засобам захисту (AppArmor, UFW);

Широкий набір CLI-інструментів для автоматизації резервного копіювання, моніторингу та адміністрування мережі.

Ubuntu Linux 22.04 дозволяє централізовано керувати ресурсами, розгортати служби з мінімальними витратами апаратних ресурсів та забезпечує гнучке масштабування інфраструктури у майбутньому.

Робочі станції: Windows 10/11 Professional

У якості операційної системи на користувацьких пристроях використано Windows 10 або Windows 11 (редакція Professional), що забезпечує сумісність з широким спектром прикладного програмного забезпечення для торгівлі, документообігу, обліку товарів та інтеграції з периферійними пристроями.

Обґрунтування такого вибору:

Повна підтримка касового ПЗ, драйверів для сканерів штрих-коду, принтерів чеків, POS-терміналів, які часто не мають стабільних версій під Linux. Вбудовані засоби захисту (BitLocker, Windows Defender, контроль доступу на основі облікових записів Active Directory). Інтеграція з хмарними сервісами Microsoft (OneDrive, Office 365), що дає можливість роботи з документами в реальному часі . Звичний інтерфейс для персоналу без необхідності додаткового навчання, що пришвидшує адаптацію нових працівників. Можливість централізованого адміністрування за допомогою групових політик (GPO), що полегшує розгортання політик безпеки.

2.6 Тестування та налагодження мережі

Після того, як усі елементи мережі змонтовані, підключені та попередньо налаштовані, настає один із найважливіших етапів – тестування та налагодження. Саме цей етап дозволяє переконатися, що система працює коректно, усі пристрої "бачать" один одного, обмінюються даними без затримок і помилок, а мережа здатна витримувати необхідне навантаження.

Перевірка фізичної цілісності мережі

Насамперед перевіряється правильність прокладки кабелів. Для цього використовуються кабельні тестери, які дозволяють виявити:

- обриви або короткі замикання в жилах кабелю;
- неправильний порядок обжимки конекторів (що може спричинити помилки передачі даних);
- відстань до проблемної ділянки, якщо така є.

Це просте, але критично важливе тестування, адже навіть найкраще налаштована мережа не працюватиме, якщо є фізичні несправності.

Налаштування адресації та перевірка зв’язку

Далі переходять до логічної перевірки — призначаються IP-адреси для всіх пристроїв, налаштовуються підмережі, маршрутизація, DHCP-сервер (або статичне IP, залежно від сегменту). Після цього за допомогою команд ping, tracert (Windows) або traceroute (Linux) перевіряється:

- чи всі пристрої доступні в межах локальної мережі;
- чи є стабільний маршрут до шлюзу;
- чи коректно працює DNS (перевіряється через команду nslookup).

Якщо пінг проходить без втрат пакетів і затримки в межах норми — це добрий знак, що базова маршрутизація працює.

Тестування швидкості та навантаження

На цьому етапі проводиться перевірка продуктивності мережі. Для цього застосовуються утиліти на кшталт:

iPerf3 — для вимірювання реальної швидкості між вузлами.

LAN Speed Test — для оцінки швидкості запису/читання у мережевих сховищах.

Wireshark — для аналізу трафіку та виявлення потенційних затримок, дублювання або втрат пакетів.

Якщо результати відповідають проектним очікуванням (наприклад, 1 Гбіт/с на внутрішньому сегменті), можна переходити далі.

Тестування доступу до ресурсів

Після перевірки інфраструктурної частини проводиться тестування доступу користувачів до сервісів:

- чи відкривається спільна папка на сервері;
- чи працює касове програмне забезпечення, яке потребує з'єднання з базою;
- и функціонують принтери, сканери, відеоспостереження;
- чи коректно працює Wi-Fi (як для внутрішнього персоналу, так і для гостей, якщо передбачено).

Також перевіряється, чи немає несанкціонованого доступу між ізольованими сегментами мережі (наприклад, між службовим Wi-Fi та гостьовим).

Тестування безпеки. Щоб переконатися, що мережа захищена від зовнішніх та внутрішніх загроз, виконуються такі дії: перевірка відкритих портів за допомогою Nmap, перевірка коректної роботи фаєрволів, симуляція доступу з підозрілих IP для перевірки блокування, тест доступу до адміністративних панелей лише з дозволених пристроїв.

Налагодження: виправлення та оптимізація

Якщо під час тестування виявлено проблеми — вони усуваються. Наприклад:

при нестабільній роботі Wi-Fi — змінюються канали, збільшується потужність точки доступу;

Ппри повільній передачі файлів — оптимізується QoS або перевіряються налаштування Jumbo Frame. При конфліктах IP — коригуються діапазони DHCP або перевіряється статична адресація.

Також на цьому етапі оновлюється прошивка обладнання, активуються

засоби моніторингу (Zabbix), встановлюються логуючі системи для відстеження активності.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкція з налаштування програмного забезпечення серверів

Налаштування програмного забезпечення серверів є ключовим етапом побудови будь-якої сучасної комп'ютерної мережі. Встановити серверну операційну систему — це лише початок. Щоб сервер виконував свої завдання, працював стабільно, безпечно та ефективно, його потрібно правильно налаштувати. Це схоже на будівництво будинку: сам фундамент (операційна система) ще не робить його житловим — потрібні внутрішні системи, захист, доступ, комфорт.

Щоб сервер виконував свою функцію в мережі

Кожен сервер у мережі має чітке призначення: хтось відповідає за зберігання файлів, інший — за базу даних, третій — за маршрутизацію запитів або авторизацію користувачів. Налаштування програмного забезпечення дозволяє:

Запустити необхідні служби (наприклад, Samba для файлового сервера, PostgreSQL або MySQL для баз даних, Apache/Nginx для веб-додатків).

Забезпечити доступ користувачів і клієнтських пристроїв до потрібних ресурсів.

Організувати автоматичні резервні копії, синхронізацію даних та обмін інформацією між вузлами.

Для забезпечення безпеки даних

Сервер — це центральне сховище критичних даних, таких як звіти про продажі, облікові записи, налаштування касових терміналів тощо. Без грамотного налаштування програмного забезпечення сервер буде вразливим до:

Несанкціонованого доступу (наприклад, через відкриті порти або слабкі паролі). Зовнішніх атак (віруси, зловмисники, ботнети). Втрати даних через збої, якщо не налаштовано резервне копіювання або моніторинг стану.

Для цього конфігурується фаєрвол (UFW, iptables), створюються окремі облікові записи з різними рівнями доступу, шифруються з'єднання (SSL),

обмежується доступ до адміністративних панелей.

Для оптимальної продуктивності

Навіть якісний сервер може працювати повільно або нестабільно, якщо програмне забезпечення не налаштоване відповідно до потреб. Оптимізація дозволяє: раціонально використовувати оперативну пам’ять і процесор; зменшити час відгуку сервісів, щоб клієнтські пристрої не "гальмували"; уникнути перевантажень при пикових навантаженнях (наприклад, у години найбільшої кількості покупок).

Налаштовуються параметри кешування, логування, автоматичного перезапуску служб, пріоритети процесів, робочі потоки, обмеження одночасних з’єднань.

Для спрощення адміністрування

У майбутньому адміністратору під час експлуатації системи треба буде оновлювати систему, додавати нові користувачів, моніторити навантаження, шукати й усувати помилки.

Налаштування відповідного ПЗ (Zabbix) дасть змогу:

- бачити в реальному часі стан системи;
- отримувати сповіщення про проблеми;
- дистанційно керувати всіма аспектами роботи сервера.

Для автоматизації процесів

Одна з переваг серверного ПЗ — можливість автоматизації. Завдяки налаштуванням можна:

- регулярно робити резервні копії без участі людини;
- оновлювати систему за розкладом;
- відправляти звіти на пошту відповідальним особам;
- моніторити стан мережі й оперативно реагувати на збої.

Це економить час і знижує ризик людських помилок.

3.2 Інструкція з налаштування активного комутаційного обладнання

Інструкція з налаштування активного комутаційного обладнання для мережі магазинів "Торба"

Центральний комутатор Cisco Catalyst C1000-24T-4G-L

Початкове підключення та налаштування

Підключення до комутатора

Підключення через консольний кабель

Налаштування терміналу: 9600 baud, 8 data bits, no parity, 1 stop bit

Використання minicom в Linux

sudo minicom -D /dev/ttyUSB0 -b 9600

Або використання screen

screen /dev/ttyUSB0 9600

Перше підключення та скидання до заводських налаштувань

При першому вході в систему

Натисніть Enter для початку

Скидання до заводських налаштувань (якщо потрібно)

Switch> enable

Switch# write erase

Switch# delete flash:vlan.dat

Switch# reload

Початкова конфігурація

Вхід в режим конфігурації

Switch> enable

Switch# configure terminal

Встановлення імені комутатора

Switch(config)# hostname TRB-C-SW01

Встановлення паролю enable

TRB-C-SW01(config)# enable secret TRBCoreEn@ble2025

Налаштування доменного імені

TRB-C-SW01(config)# ip domain-name TRB.local

Відключення DNS lookup

TRB-C-SW01(config)# no ip domain-lookup

Базова конфігурація системи

2.1 Налаштування управління

Створення локального користувача

TRB-C-SW01(config)# username TRB-admin privilege 15 secret TRBAdmin@2025

TRB-C-SW01(config)# username TRB-tech privilege 5 secret TRBTech@2025

Налаштування консолі

TRB-C-SW01(config)# line console 0

TRB-C-SW01(config-line)# login local

TRB-C-SW01(config-line)# exec-timeout 10 0

TRB-C-SW01(config-line)# logging synchronous

TRB-C-SW01(config-line)# exit

Налаштування VTY ліній (Telnet/SSH)

TRB-C-SW01(config)# line vty 0 15

TRB-C-SW01(config-line)# login local

TRB-C-SW01(config-line)# transport input ssh

TRB-C-SW01(config-line)# exec-timeout 10 0

Налаштування SSH

Генерація RSA ключів

TRB-C-SW01(config)# crypto key generate rsa general-keys modulus 2048

Налаштування SSH

TRB-C-SW01(config)# ip ssh version 2

TRB-C-SW01(config)# ip ssh time-out 60

TRB-C-SW01(config)# ip ssh authentication-retries 3

Налаштування часу та NTP

Встановлення часового поясу

TRB-C-SW01(config)# clock timezone EET 2

TRB-C-SW01(config)# clock summer-time EEST recurring last Sun Mar 3:00 last Sun Oct 4:00

Налаштування NTP

TRB-C-SW01(config)# ntp server 0.ua.pool.ntp.org prefer

TRB-C-SW01(config)# ntp server 1.ua.pool.ntp.org

TRB-C-SW01(config)# ntp server time.google.com

Налаштування VLAN

3.1 Створення VLAN для різних сегментів мережі

VLAN для управління

TRB-C-SW01(config)# vlan 10

TRB-C-SW01(config-vlan)# name MANAGEMENT

TRB-C-SW01(config-vlan)# exit

VLAN для серверів

TRB-C-SW01(config)# vlan 20

TRB-C-SW01(config-vlan)# name SERVERS

TRB-C-SW01(config-vlan)# exit

VLAN для POS терміналів

TRB-C-SW01(config)# vlan 30

TRB-C-SW01(config-vlan)# name POS-TERMINALS

TRB-C-SW01(config-vlan)# exit

VLAN для офісних комп'ютерів

TRB-C-SW01(config)# vlan 40

TRB-C-SW01(config-vlan)# name OFFICE-PCs

TRB-C-SW01(config-vlan)# exit

VLAN для гостьового WiFi

TRB-C-SW01(config)# vlan 50

TRB-C-SW01(config-vlan)# name GUEST-WIFI

TRB-C-SW01(config-vlan)# exit

VLAN для камер відеоспостереження

TRB-C-SW01(config)# vlan 60

TRB-C-SW01(config-vlan)# name SECURITY-CAMERAS

TRB-C-SW01(config-vlan)# exit

VLAN для принтерів

TRB-C-SW01(config)# vlan 70

TRB-C-SW01(config-vlan)# name PRINTERS

TRB-C-SW01(config-vlan)# exit

Налаштування SVI (Switch Virtual Interface)

Інтерфейс управління

TRB-C-SW01(config)# interface vlan 10

TRB-C-SW01(config-if)# ip address 192.168.10.2 255.255.255.0

TRB-C-SW01(config-if)# no shutdown

TRB-C-SW01(config-if)# description Management Interface

TRB-C-SW01(config-if)# exit

Налаштування шлюзу за замовчуванням

TRB-C-SW01(config)# ip default-gateway 192.168.10.1

Конфігурація портів

Налаштування портів для серверів (Gi1/0/1-4)

Порт для основного сервера

TRB-C-SW01(config)# interface GigabitEthernet1/0/1

TRB-C-SW01(config-if)# description TRB-MAIN-SERVER

TRB-C-SW01(config-if)# switchport mode access

TRB-C-SW01(config-if)# switchport access vlan 20

TRB-C-SW01(config-if)# switchport port-security

TRB-C-SW01(config-if)# switchport port-security maximum 2

TRB-C-SW01(config-if)# switchport port-security violation restrict

TRB-C-SW01(config-if)# spanning-tree portfast

TRB-C-SW01(config-if)# no shutdown

TRB-C-SW01(config-if)# exit

Порт для резервного сервера

TRB-C-SW01(config)# interface GigabitEthernet1/0/2

TRB-C-SW01(config-if)# description TRBBACKUP-SERVER

TRB-C-SW01(config-if)# switchport mode access

TRB-C-SW01(config-if)# switchport access vlan 20

TRB-C-SW01(config-if)# switchport port-security

TRB-C-SW01(config-if)# switchport port-security maximum 2

TRB-C-SW01(config-if)# switchport port-security violation restrict

TRB-C-SW01(config-if)# spanning-tree portfast

TRB-C-SW01(config-if)# no shutdown

TRB-C-SW01(config-if)# exit

4.2 Налаштування портів для POS терміналів (Gi1/0/5-12)

Групове налаштування портів для POS

TRB-C-SW01(config)# interface range GigabitEthernet1/0/5-12

TRB-C-SW01(config-if-range)# description POS-TERMINALS

TRB-C-SW01(config-if-range)# switchport mode access

TRB-C-SW01(config-if-range)# switchport access vlan 30

TRB-C-SW01(config-if-range)# switchport port-security

TRB-C-SW01(config-if-range)# switchport port-security maximum 1

TRB-C-SW01(config-if-range)# switchport port-security violation shutdown

TRB-C-SW01(config-if-range)# spanning-tree portfast

TRB-C-SW01(config-if-range)# spanning-tree bpduguard enable

TRB-C-SW01(config-if-range)# no shutdown

TRB-C-SW01(config-if-range)# exit

4.3 Налаштування портів для офісних комп'ютерів (Gi1/0/13-18)

Порти для офісних комп'ютерів

TRB-C-SW01(config)# interface range GigabitEthernet1/0/13-18

TRB-C-SW01(config-if-range)# description OFFICE-COMPUTERS

TRB-C-SW01(config-if-range)# switchport mode access

TRB-C-SW01(config-if-range)# switchport access vlan 40

TRB-C-SW01(config-if-range)# switchport port-security

TRB-C-SW01(config-if-range)# switchport port-security maximum 2

TRB-C-SW01(config-if-range)# switchport port-security violation restrict

TRB-C-SW01(config-if-range)# spanning-tree portfast

TRB-C-SW01(config-if-range)# no shutdown

TRB-C-SW01(config-if-range)# exit

4.4 Налаштування портів для принтерів та периферії (Gi1/0/19-22)

Порти для принтерів

TRB-C-SW01(config)# interface range GigabitEthernet1/0/19-22

TRB-C-SW01(config-if-range)# description PRINTERS

TRB-C-SW01(config-if-range)# switchport mode access

TRB-C-SW01(config-if-range)# switchport access vlan 70

TRB-C-SW01(config-if-range)# spanning-tree portfast

TRB-C-SW01(config-if-range)# no shutdown

TRB-C-SW01(config-if-range)# exit

4.5 Налаштування порту для WiFi точки доступу (Gi1/0/23)

Порт для WiFi AP з trunk конфігурацією

TRB-C-SW01(config)# interface GigabitEthernet1/0/23

TRB-C-SW01(config-if)# description WIFI-ACCESS-POINT

TRB-C-SW01(config-if)# switchport mode trunk

TRB-C-SW01(config-if)# switchport trunk native vlan 40

TRB-C-SW01(config-if)# switchport trunk allowed vlan 40,50

TRB-C-SW01(config-if)# no shutdown

TRB-C-SW01(config-if)# exit

Налаштування uplink порту (Gi1/0/24)

Uplink до основного маршрутизатора

TRB-C-SW01(config)# interface GigabitEthernet1/0/24

TRB-C-SW01(config-if)# description UPLINK-TO-ROUTER

TRB-C-SW01(config-if)# switchport mode trunk

TRB-C-SW01(config-if)# switchport trunk native vlan 10

TRB-C-SW01(config-if)# switchport trunk allowed vlan 10,20,30,40,50,60,70

TRB-C-SW01(config-if)# no shutdown

TRB-C-SW01(config-if)# exit

Налаштування безпеки

5.1 Налаштування port security

Глобальне налаштування port security

TRB-C-SW01(config)# errdisable recovery cause psecure-violation

TRB-C-SW01(config)# errdisable recovery interval 300

Налаштування aging для MAC адрес

TRB-C-SW01(config)# interface range GigabitEthernet1/0/5-12

TRB-C-SW01(config-if-range)# switchport port-security aging time 60

TRB-C-SW01(config-if-range)# switchport port-security aging type inactivity

TRB-C-SW01(config-if-range)# exit

Налаштування DHCP Snooping

Увімкнення DHCP snooping

TRB-C-SW01(config)# ip dhcp snooping

TRB-C-SW01(config)# ip dhcp snooping vlan 30,40,50

Налаштування trusted портів

TRB-C-SW01(config)# interface GigabitEthernet1/0/24

TRB-C-SW01(config-if)# ip dhcp snooping trust

TRB-C-SW01(config-if)# exit

Налаштування rate limit

TRB-C-SW01(config)# interface range GigabitEthernet1/0/5-18

TRB-C-SW01(config-if-range)# ip dhcp snooping limit rate 10

TRB-C-SW01(config-if-range)# exit

Налаштування Spanning Tree

Налаштування Rapid PVST+

TRB-C-SW01(config)# spanning-tree mode rapid-pvst

Налаштування priority для VLAN

TRB-C-SW01(config)# spanning-tree vlan 10,20,30,40,50,60,70 priority 4096

Налаштування PortFast та BPDU Guard

TRB-C-SW01(config)# spanning-tree portfast default

TRB-C-SW01(config)# spanning-tree portfast bpduguard default

Налаштування Storm Control

Налаштування storm control на access портах

TRB-C-SW01(config)# interface range GigabitEthernet1/0/5-22

TRB-C-SW01(config-if-range)# storm-control broadcast level 10.00

TRB-C-SW01(config-if-range)# storm-control multicast level 10.00

TRB-C-SW01(config-if-range)# storm-control unicast level 10.00

TRB-C-SW01(config-if-range)# storm-control action shutdown

TRB-C-SW01(config-if-range)# exit

Управління та моніторинг

Налаштування SNMP

Налаштування SNMP v3

TRB-C-SW01(config)# snmp-server group TRB-ADMINS v3 priv

TRB-C-SW01(config)# snmp-server user TRB-monitor TRB-ADMINS v3 auth sha TRBMonAuth@2025 priv aes 128 TRBMonPriv@2025

Налаштування SNMP v2c (для сумісності)

TRB-C-SW01(config)# snmp-server community TRBRead@2025 RO

TRB-C-SW01(config)# snmp-server community TRBWrite@2025 RW

Налаштування SNMP параметрів

TRB-C-SW01(config)# snmp-server location "TRB Store Central Office"

TRB-C-SW01(config)# snmp-server contact "IT Department: it@TRB.ua"

TRB-C-SW01(config)# snmp-server enable traps

6.2 Налаштування Syslog

Налаштування syslog сервера

TRB-C-SW01(config)# logging host 192.168.20.10

TRB-C-SW01(config)# logging trap informational

TRB-C-SW01(config)# logging facility local0

TRB-C-SW01(config)# logging source-interface vlan 10

Налаштування локального логування

TRB-C-SW01(config)# logging buffered 32768 informational

TRB-C-SW01(config)# logging console warnings

Налаштування EEM (Embedded Event Manager)

Скрипт для автоматичного відновлення портів після err-disable

TRB-C-SW01(config)# event manager applet RECOVERY-PORTS

TRB-C-SW01(config-applet)# event timer watchdog time 600

TRB-C-SW01(config-applet)# action 1.0 cli command "enable"

TRB-C-SW01(config-applet)# action 2.0 cli command "show interface status err-disabled"

TRB-C-SW01(config-applet)# action 3.0 cli command "configure terminal"

TRB-C-SW01(config-applet)# action 4.0 cli command "interface range gi1/0/5-22"

TRB-C-SW01(config-applet)# action 5.0 cli command "shutdown"

TRB-C-SW01(config-applet)# action 6.0 wait 5

TRB-C-SW01(config-applet)# action 7.0 cli command "no shutdown"

TRB-C-SW01(config-applet)# action 8.0 cli command "end"

TRB-C-SW01(config-applet)# exit

Резервування та відновлення

Створення резервної копії конфігурації

Копіювання конфігурації на TFTP сервер

TRB-C-SW01# copy running-config tftp:

Address or name of remote host []? 192.168.20.10

Destination filename [TRB-C-sw01-confg]? TRB-C-sw01-backup-YYYYMMDD.cfg

Локальне збереження конфігурації

TRB-C-SW01# copy running-config startup-config

TRB-C-SW01# write memory

Автоматичне резервне копіювання

Створення архівної конфігурації

TRB-C-SW01(config)# archive

TRB-C-SW01(config-archive)# path tftp://192.168.20.10/TRB-C-sw01-$h-$t

TRB-C-SW01(config-archive)# maximum 10

TRB-C-SW01(config-archive)# time-period 1440

TRB-C-SW01(config-archive)# exit

Відновлення конфігурації

Відновлення з TFTP сервера

TRB-C-SW01# copy tftp: startup-config

Address or name of remote host []? 192.168.20.10

Source filename []? TRB-C-sw01-backup-YYYYMMDD.cfg

Перезавантаження для застосування

TRB-C-SW01# reload

Діагностика та усунення неполадок

Основні команди діагностики

Перевірка статусу портів

TRB-C-SW01# show interface status

TRB-C-SW01# show interface GigabitEthernet1/0/1

Перевірка VLAN

TRB-C-SW01# show vlan brief

TRB-C-SW01# show interface trunk

Перевірка MAC адрес

TRB-C-SW01# show mac address-table

TRB-C-SW01# show mac address-table vlan 30

Перевірка Spanning Tree

TRB-C-SW01# show spanning-tree

TRB-C-SW01# show spanning-tree vlan 30

Перевірка port security

TRB-C-SW01# show port-security

TRB-C-SW01# show port-security interface GigabitEthernet1/0/5

Моніторинг продуктивності

Перевірка використання CPU та пам'яті

TRB-C-SW01# show processes cpu

TRB-C-SW01# show memory

Перевірка температури та живлення

TRB-C-SW01# show environment

TRB-C-SW01# show power

Статистика інтерфейсів

TRB-C-SW01# show interface counters

TRB-C-SW01# show interface counters errors

Логування та події

Перевірка логів

TRB-C-SW01# show logging

TRB-C-SW01# show logging | include ERROR

Перевірка err-disabled портів

TRB-C-SW01# show interface status err-disabled

TRB-C-SW01# show errdisable recovery

Фінальна конфігурація та збереження

Перевірка конфігурації

Перевірка повної конфігурації

TRB-C-SW01# show running-config

Перевірка основних параметрів

TRB-C-SW01# show version

TRB-C-SW01# show ip interface brief

TRB-C-SW01# show vlan brief

TRB-C-SW01# show interface trunk

Збереження та документування

Остаточне збереження конфігурації

TRB-C-SW01# copy running-config startup-config

TRB-C-SW01# write memory

Експорт конфігурації для документації

TRB-C-SW01# show running-config | redirect tftp://192.168.20.10/TRB-C-sw01-final.cfg

Створення документації

Створення схеми підключень

TRB-C-SW01# show cdp neighbors detail

TRB-C-SW01# show lldp neighbors detail

Експорт важливої інформації

TRB-C-SW01# show interface description

TRB-C-SW01# show vlan brief

TRB-C-SW01# show ip route

3.3 Інструкція з використання тестових наборів та тестових програм

Ця інструкція розроблена для забезпечення послідовного та ефективного тестування комп'ютерної мережі мережі супермаркетів "Торба". Її мета — мінімізувати простої, підвищити стабільність роботи касових систем, терміналів оплати та систем обліку, а також гарантувати безперебійний обмін даними між усіма вузлами мережі. Виконання цих процедур дозволить швидко виявляти потенційні проблеми та попереджувати збої, що критично важливо для операційної ефективності "Торби".

Загальні принципи тестування

1. Планування та періодичність

Тестування має проводитись за чітким графіком:

Регулярні планові перевірки: Щотижня або щомісяця, залежно від критичності сегмента мережі.

Після змін: Кожного разу після внесення змін до мережевої інфраструктури (додавання нового обладнання, зміна конфігурації, оновлення ПЗ).

При виникненні проблем: Негайно після виявлення будь-яких аномалій у роботі мережі.

2. Документування

Всі результати тестування, виявлені проблеми та вжиті заходи мають бути ретельно задокументовані. Це створює базу знань для подальшого аналізу та дозволяє відстежувати динаміку стану мережі.

3. Ізоляція та вплив

За можливості, тестування критичних ділянок мережі слід проводити у непікові години або, якщо це можливо, на ізольованих тестових сегментах, щоб мінімізувати вплив на поточні операції супермаркету.

4. Використання стандартизованих наборів

Застосування затверджених тестових наборів та програм забезпечує одноманітність та порівнянність результатів між різними локаціями "Торби".

Необхідні інструменти та програмне забезпечення

А. Фізичні тестові набори (для діагностики на місці)

Кабельний тестер (LAN Cable Tester): Для перевірки цілісності та правильної розкладки мережевих кабелів (UTP/STP), виявлення обривів, коротких замикань та перехрестних пар. Рекомендується мати тестери з можливістю трасування кабелю (тональний генератор та індуктивний щуп) для швидкого пошуку кабелів у стінах або каналах.

Мережевий аналізатор (Handheld Network Analyzer): Портативний пристрій для більш глибокої діагностики: вимірювання швидкості з'єднання, виявлення колізій, аналізу трафіку, визначення активних пристроїв у сегменті.

Тестовий Ethernet-кабель: Завжди мати під рукою кілька перевірених патч-кордів різної довжини для швидкої заміни підозрілих кабелів.

Мультиметр: Для перевірки живлення активного мережевого обладнання та PoE (Power over Ethernet) інжекторів/портів.

Б. Програмне забезпечення для тестування мережі

Ping (Пакетна Інтернет Група): Стандартна утиліта для перевірки доступності мережевих вузлів та вимірювання часу відгуку (latency).

Приклад використання: ping 192.168.1.1 (для перевірки маршрутизатора), ping 8.8.8.8 (для перевірки зовнішнього доступу).

Параметри:

-t (для Windows) / без параметрів (для Linux/macOS) – безперервний пінг.

-n <кількість> (для Windows) / -c <кількість> (для Linux/macOS) – кількість пакетів.

Traceroute / Tracert: Дозволяє відстежити маршрут пакетів до цільового вузла, виявляючи ділянки з високою затримкою або втратами.

Приклад використання: tracert kasovy-server (Windows), traceroute 192.168.1.100 (Linux/macOS).

Nslookup / Dig: Для діагностики DNS-служби, перевірки коректності розпізнавання доменних імен в IP-адреси.

Приклад використання: nslookup google.com, dig local-server.TRB.ua.

Iperf3: Програма для вимірювання пропускної здатності мережі (bandwidth). Дозволяє тестувати швидкість між двома точками в мережі (клієнт-сервер).

Використання: Запустити Iperf3 на одному комп'ютері як сервер (iperf3 -s), на іншому як клієнт (iperf3 -c <IP_сервера>).

Wireshark: Потужний мережевий аналізатор трафіку. Дозволяє перехоплювати та аналізувати пакети даних, виявляти аномалії, неправильні протоколи, проблеми з безпекою. Вимагає певних знань для інтерпретації данх.

Програми для моніторингу мережі (наприклад, Zabbix, PRTG, Nagios): Для постійного моніторингу стану пристроїв, завантаження каналів, температури обладнання та сповіщення про відхилення. Хоча це не тестовий набір, а система моніторингу, її дані є цінним джерелом для ініціювання тестування.

Вбудовані утиліти мережевого обладнання: Веб-інтерфейси

маршрутизаторів, комутаторів, точок доступу часто містять власні діагностичні інструменти (ping, traceroute, журнал подій).

Послідовність виконання тестових процедур

Етап 1: Візуальний огляд та фізична перевірка

Кабельна інфраструктура: Перевірити всі патч-корди на видимі пошкодження. Переконатися у надійній фіксації конекторів у портах (комутатори, роутери, робочі станції).

Активне обладнання: Перевірити індикатори на комутаторах, маршрутизаторах, точках доступу. Зелені індикатори зазвичай свідчать про нормальну роботу.

Живлення: Переконатися, що всі мережеві пристрої отримують стабільне живлення. Перевірити роботу блоків живлення та PoE інжекторів.

температурний режим: Перевірити, чи немає перегріву обладнання (особливо у серверних шафах або комірках). Забезпечити належну вентиляцію.

Етап 2: Базове тестування доступності (за допомогою Ping)

Тест "петлі" (loopback): ping 127.0.0.1 – перевірка працездатності мережевого стека на локальному комп'ютері.

Доступність шлюзу (Gateway): ping <IP_адреса_маршрутизатора> (наприклад, ping 192.168.1.1). Якщо шлюз недоступний, проблема, ймовірно, знаходиться на локальному рівні (кабель, мережева карта, налаштування IP).

Доступність ключових внутрішніх вузлів:

ping <IP_адреса_касового_сервера>

ping <IP_адреса_сервера_обліку>

ping <IP_адреса_центрального_сервера_Торби> (якщо доступний з локальної мережі).

Доступність зовнішніх ресурсів (DNS та Інтернет):

ping google.com або ping 8.8.8.8 (Google DNS). Якщо IP пінг проходить, а доменне ім'я ні, це вказує на проблему з DNS.

Етап 3: Розширена діагностика маршрутизації та DNS

Трасування маршруту (Traceroute/Tracert):

tracert <IP_адреса_віддаленого_сервера> (наприклад, центрального сервера "Торби") – дозволить виявити, на якому мережевому пристрої (маршрутизаторі) виникають затримки або втрати пакетів.

tracert 8.8.8.8 – перевірка маршруту до зовнішнього Інтернету.

Діагностика DNS (Nslookup/Dig):

nslookup <ім'я_внутрішнього_сервера.TRB.ua> – перевірка коректності роботи внутрішнього DNS.

nslookup google.com – перевірка роботи зовнішнього DNS.

Етап 4: Тестування пропускної здатності (Iperf3)

Підготовка: На одному ПК (наприклад, сервері або потужній робочій станції) запустити iperf3 -s (режим сервера).

Запуск тесту: На клієнтській машині (наприклад, касовому терміналі, або ПК поруч з ним) запустити iperf3 -c <IP_адреса_сервера>.

Аналіз результатів: Звіріть отриману пропускну здатність з очікуваною для вашого обладнання (наприклад, 100 Мбіт/с або 1 Гбіт/с). Низькі показники можуть свідчити про проблеми з кабелем, мережевою картою, несправний порт комутатора або перевантаження мережі.

Додатково: Протестуйте у режимі UDP (iperf3 -u -c <IP_сервера> -b 100M) для виявлення втрат пакетів, що важливо для VoIP та відео.

Етап 5: Детальний аналіз трафіку (Wireshark)

Запуск: Встановіть Wireshark на комп'ютер, підключений до проблемного сегмента мережі (або використовуйте SPAN-порт на комутаторі для дзеркалювання трафіку).

Фільтрація: Застосовуйте фільтри для фокусування на конкретних протоколах (наприклад, http, dns, smb) або IP-адресах (ip.addr == 192.168.1.5).

Аналіз: Шукайте:

Помилки протоколів: Перезапити, помилки TCP, UDP-контрольні суми.

Несанкціонований трафік: Невідомі з'єднання, підвищена активність на нестандартних портах.

Проблеми з автентифікацією: Помилки NTLM, Kerberos (якщо актуально).

Високу затримку (latency): У графіках I/O можна побачити піки затримки.

Типові сценарії тестування та їх вирішення

Сценарій 1: "Каса не бачить сервер"

Фізичний огляд: Перевірити кабель від каси до розетки/комутатора. Індикатори на мережевій карті каси та порту комутатора.

Ping:

ping 127.0.0.1 (перевірка ОС каси).

ping <IP_адреса_шлюзу> (перевірка зв'язку до роутера/комутатора).

ping <IP_адреса_касового_сервера> (перевірка зв'язку до сервера).

Nslookup: Перевірити, чи каса правильно розпізнає ім'я касового сервера.

Iperf3: Якщо ping проходить, але повільно, перевірити пропускну здатність між касою та сервером.

Wireshark: Запустити на касі для аналізу, чи йдуть запити до сервера і які відповіді повертаються (наприклад, firewall блокує порт).

Сценарій 2: "Повільна робота системи обліку"

Ping: Перевірити час відгуку до сервера обліку з декількох робочих місць. Висока затримка вказує на перевантаження мережі або проблеми з кабелем/комутатором.

Iperf3: Виміряти пропускну здатність між робочими місцями та сервером обліку.

Traceroute: Виявити вузькі місця на шляху до сервера обліку.

Моніторинг мережі: Перевірити завантаження портів комутаторів, що ведуть до сервера обліку та робочих станцій.

Сценарій 3: "Нестабільний Wi-Fi для терміналів оплати"

Візуальний огляд: Розташування точок доступу, відсутність перешкод.

Ping: З терміналу оплати пінг до точки доступу та до шлюзу.

Wi-Fi аналізатор (на смартфоні/ноутбуці): Перевірити рівень сигналу, наявність інтерференції від сусідніх Wi-Fi мереж.

Налаштування точки доступу: Перевірити канали, потужність сигналу, налаштування QoS.

Ведення документації

Для кожної торгової точки "Торби" необхідно вести:

Карта мережі: Схема підключення всіх мережевих пристроїв, IP-адреси.

Журнал тестування: Дата, час, виконані тести, отримані результати, виявлені проблеми, вжиті заходи, відповідальна особа.

Конфігурації обладнання: Збережені копії конфігурацій комутаторів, маршрутизаторів, точок доступу.

3.4 Інструкція по налаштуванню засобів захисту мережі

Захист комп'ютерної мережі — це не разовий процес, а постійна система дій і заходів, спрямованих на забезпечення цілісності, доступності та конфіденційності інформації. У мережі супермаркету «Торба», де працюють касові термінали, сервери баз даних і корпоративна пошта, питання безпеки є пріоритетом. Нижче наведена інструкція, що описує основні технічні й організаційні засоби захисту, які мають бути впроваджені.

Контроль доступу до мережевих ресурсів

Аутентифікація користувачів

Для кожного користувача створюється персональний обліковий запис з унікальним паролем.

Паролі мають бути складними (мінімум 8 символів, великі/малі літери, цифри, спеціальні символи).

Застосовується обмеження часу сесії: після 10 хвилин бездіяльності сеанс завершується.

Можна використовувати двофакторну аутентифікацію для доступу до критичних вузлів (наприклад, через TOTP або SMS-код).

Розмежування прав доступу

Доступ до файлів, програм, налаштувань надається відповідно до ролі (касир, адміністратор, бухгалтер).

Заборонено використовувати спільні облікові записи.

Встановлюються ACL (Access Control Lists) для управління дозволами.

Захист на рівні мережевої інфраструктури

Фаєрвол (Firewall)

На шлюзі встановлюється апаратний або програмний фаєрвол (наприклад, UFW для Ubuntu).

Блокуються всі порти, крім необхідних (наприклад, 80/443 — для веб, 22 — для SSH з whitelist IP).

Ведеться журнал спроб доступу до заборонених портів.

Сегментація мережі

Внутрішня мережа розділяється на віртуальні мережі VLAN:

- VLAN для касових терміналів;
- VLAN для відеоспостереження;
- VLAN для гостьового Wi-Fi;
- VLAN для адміністративного персоналу.

Між VLAN встановлюються обмеження (наприклад, гостьовий Wi-Fi не має доступу до серверної мережі).

Фільтрація MAC-адрес

На комутаторах і точках доступу активується список дозволених MAC-адрес.

Будь-який пристрій поза списком не отримає доступ до мережі.

Шифрування трафіку та захист переданої інформації

Захищене з’єднання (VPN, SSL/TLS)

Зовнішній доступ до внутрішніх ресурсів дозволений лише через VPN з використанням IPsec або OpenVPN.

Адмінпанелі доступні тільки через HTTPS, із встановленим SSL-сертифікатом (Let's Encrypt або корпоративний).

Веб-додатки повинні мати TLS-шифрування.

Шифрування даних на дисках

Серверні жорсткі диски або розділи з важливими даними зашифровані (наприклад, з використанням LUKS, BitLocker).

У разі фізичного доступу до обладнання дані залишаються недоступними без

ключа.

Захист від шкідливого програмного забезпечення

Антивірусне програмне забезпечення

На всіх Windows-станціях встановлено антивірус (наприклад, Microsoft Defender).

Встановлене централізоване оновлення баз даних і щоденне сканування системи.На сервері Ubuntu застосовуються інструменти перевірки цілісності (chkrootkit, rkhunter) та фільтрації трафіку (ClamAV для поштового сервера).

Заборона встановлення ПЗ сторонніми

Користувачі не мають прав адміністратора, що виключає встановлення небажаних програм.Використовується білий список дозволених додатків.

Резервне копіювання та відновлення

Автоматичне резервне копіювання. Виконується щоденне копіювання даних з серверів на окремий NAS або зовнішній накопичувач. Кожні 7 днів створюється повна резервна копія, а щодня — інкрементальна. Перевірка цілісності бекапів. Раз на тиждень бекапи тестуються на можливість відновлення.

Ведеться журнал резервного копіювання.

Моніторинг та журналювання подій

Системи моніторингу. Встановлюється система моніторингу (Zabbix, Grafana), яка контролює навантаження, температуру, мережеву активність.

У разі підозрілої активності (сплеск трафіку, підозрілий порт) адміністратору надсилається сповіщення.

Журнали подій (логування). Активується ведення системних логів (syslog, auditd, ufw.log). Журнали автоматично архівуються і захищаються від змін.

Аналіз логів дозволяє швидко виявити атаки типу brute-force або внутрішні порушення політик.

Фізична безпека мережевого обладнання

Сервери й комутатори розміщені у закритих приміщеннях із обмеженим доступом. Встановлені камери відеоспостереження в зоні серверної. Використовуються шафи з замком, контроль за відкриттям здійснюється через

реєстраційний журнал.

Захист мережі — це багаторівнева система, де кожен компонент (користувач, кабель, комутатор чи програма) має бути врахований і захищений. Ця інструкція охоплює ключові напрямки безпеки: технічний, програмний, організаційний і фізичний. Її впровадження дозволяє мінімізувати ризики несанкціонованого доступу, втрати даних чи збоїв у роботі мережі супермаркету.

3.5 Інструкція з експлуатації та моніторингу в мережі

Після завершення монтажу, налаштування й тестування комп'ютерної мережі наступає не менш важливий етап — її експлуатація та постійний моніторинг. Мережа не є статичною системою. З часом у ній можуть змінюватися умови навантаження, з'являтися нові пристрої, оновлюватися програмне забезпечення. Саме тому важливо не лише запустити мережу, а й забезпечити її стабільну та безпечну роботу протягом усього періоду функціонування.

Експлуатація як щоденна практика

У повсякденному користуванні мережею головна увага приділяється забезпеченню безперебійного доступу до її ресурсів. Це стосується як звичайних працівників (наприклад, касирів або адміністраторів магазину), так і IT-фахівців, відповідальних за обслуговування. Важливо, щоб усі підключені пристрої функціонували стабільно: касові термінали — передавали дані до серверу, принтери — друкували чеки без затримок, а клієнтські комп'ютери — мали безперервний зв'язок з внутрішніми сервісами.

Періодично проводиться перевірка фізичного стану мережевого обладнання: чи працюють усі порти комутаторів, чи немає обривів кабелю, чи надійно тримаються роз'єми. Також важливо слідкувати за температурними режимами в приміщенні серверної або комутаційних шаф — надмірний перегрів може спричинити збої або повну відмову обладнання.

Оновлення програмного забезпечення також є частиною експлуатації. Сервери, точки доступу, маршрутизатори повинні періодично отримувати

оновлення — як для усунення вразливостей, так і для покращення функціональності. Однак такі оновлення проводяться лише в періоди найменшого навантаження або після попереднього тестування, щоб уникнути непередбачуваних збоїв.

Моніторинг як запорука стабільності

У сучасних мережах дуже важливо мати систему моніторингу, яка постійно відстежує стан інфраструктури. Це не лише допомога у виявленні проблем, а й спосіб завчасно запобігти аваріям.

Для реалізації моніторингу використовуються спеціалізовані програми або сервіси, що збирають інформацію про швидкість з'єднання, навантаження на порти, рівень завантаження процесора на сервері, обсяг вільної пам'яті та інші важливі метрики. Якщо якась з них виходить за межі допустимих значень — адміністратор миттєво отримує повідомлення, зазвичай через електронну пошту, месенджер або мобільний додаток.

Завдяки моніторингу можна своєчасно виявити, наприклад, що один із комутаторів почав втрачати пакети, або що один з касових терміналів підключився не до тієї VLAN. У більшості випадків це дозволяє усунути проблему до того, як вона вплине на роботу персоналу або клієнтів.

Ще одним важливим аспектом моніторингу є аналіз логів. Логи — це текстові записи подій, які відбуваються в системі. Вони зберігають інформацію про з'єднання, помилки, оновлення, спроби входу, зміну конфігурацій тощо. За допомогою логів можна відстежити дії як користувачів, так і можливих зловмисників. Регулярний перегляд журналів дозволяє виявити спроби підбору паролів, використання заборонених портів чи некоректну роботу служб.

Взаємодія з користувачами

У процесі експлуатації мережі завжди виникає певна взаємодія з користувачами. Працівники можуть повідомляти про уповільнення роботи, втрату доступу або інші труднощі. Важливо, щоб адміністратор реагував на такі запити оперативно та ввічливо, адже від ефективності вирішення проблем залежить робота цілого підрозділу або магазину.

Крім цього, персонал періодично має проходити інструктаж щодо правил роботи в мережі: не відкривати підозрілі посилання, не змінювати самостійно налаштування мережі, не підключати сторонні пристрої тощо. Такий підхід значно знижує ризики помилок чи загроз із боку внутрішніх користувачів.

Грамотна експлуатація мережі — це щоденна відповідальна робота, а моніторинг — її "очі", які бачать більше, ніж користувач. Лише завдяки постійному контролю, підтримці й профілактиці можна гарантувати, що мережа працюватиме надійно, безпечно та без збоїв. У випадку супермаркету це означає безперебійну роботу кас, оперативний облік товарів і якісне обслуговування клієнтів — а це, своєю чергою, основа довіри та прибутку.

4 ЕКОНОМІЧНА ЧАСТИНА

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки та реалізації комп'ютерної мережі супермаркетів "Торба" і прийняття рішення про його подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для розрахунку вартості розробки та реалізації сайту необхідно виконати наступні етапи:

- описати технологічний процес розробки із зазначенням трудомісткості кожної операції;
- визначити суму витрат на оплату праці основного і допоміжного персоналу, включаючи відрахування на соціальні заходи;
- визначити суму матеріальних затрат;
- обчислити витрати на електроенергію для науково-виробничих цілей;
- розрахувати транспортні витрати;
- нарахувати суму амортизаційних відрахувань;
- визначити суму накладних витрат;
- скласти кошторис та визначити собівартість розробки;
- розрахувати ціну розробки та реалізації проекту DevOps підтримки гри "Danger Path";
- визначити економічну ефективність та термін окупності продукту.

4.1 Визначення стадій технологічного процесу та загальної тривалості розробки та реалізації проекту комп'ютерної мережі супермаркетів "Торба"

Для визначення загальної тривалості розробки та реалізації веб-сайту, дані витрат часу по окремих операціях зведемо у таблицю 4.1.

Таблиця 4.1 - Середній час розробки та реалізації проекту комп'ютерної мережі супермаркетів "Торба", та стадії (операції) технологічного процесу

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1.	Постановка задачі	Керівник	20
2.	Збір інформації	Інженер	15
3.	Розробка проекту	Інженер	132
4.	Підготовка документації	Керівник	40
5.	Доставка обладнання	Інженер	20
6.	Тестування	Інженер	2 5
7.	Здача в експлуатацію	Інженер	3
Разом			252

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України "Про оплату праці" заробітна плата – це "винагорода, обчислена, як правило, у грошовому виразі, яку власник або уповноважений ним орган виплачує працівникові за виконану ним роботу".

Розмір заробітної плати залежить від складності та умов виконуваної роботи,

професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства. Заробітна плата складається з основної та додаткової оплати праці.

Основна заробітна плата нараховується на виконану роботу за тарифними ставками, відрядними розцінками чи посадовими окладами і не залежить від результатів господарської діяльності підприємства.

Додаткова заробітна плата – це складова заробітної плати працівників, до якої включають витрати на оплату праці, не пов'язані з виплатами за фактично відпрацьований час. Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Виходячи з рекомендованих тарифних ставок встановимо часову тарифну ставку для керівника 470грн./год, інженера 155грн./год.

$$З_{осн.} = 470 \cdot 60 + 155 \cdot 192 = 57960 \text{ (грн)}$$

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

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

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

$$К_{дод.} = 57960 \cdot 0.12 = 6955.20 \text{ (грн)}$$

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

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

$$В_{о.п.} = 57960 + 6955.20 = 64915.20 \text{ (грн.)}$$

Крім того, слід визначити відрахування на соціальні заходи:

– єдиний соціальний внесок – 22%

Отже, сума відрахувань на соціальні заходи буде становити:

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

де ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 64915.20 \cdot 0{,}22 = 14281.34 \text{ (грн.)}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

№ п/п	Категорія працівників	Основна заробітна плата, грн.			Додаткова заробітна плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тарифна ставка, грн.	К-сть від-працьов. год.	Фактично нарах. з/пл., грн.			
А	*Б*	*1*	*2*	*3*	*4*	*5*	*6*
1	Інженер	155	192	29760	3571,2	---	---
2	Керівник	470	60	28200	3384	---	---
Разом				57960	6955,2	14281.34	79196,54

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 qi – кількість витраченого матеріалу і-го виду;

pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{B\,i} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна 1-ці, грн.	Загальна сума витрат, грн.
1.	APC Back-UPS RS 1100VA	шт	2	7262,00	14524,00
2.	Коммутатор Cisco C-1000 24T	шт	4	12000,00	48000,00
4.	EuroLAN UTP кабель 4пари кат. 5e	м	900	3,00	2700,00
6.	EuroLAN UTP комутаційний шнур кат. 5e, 1 м	шт	33	12,00	396,00
7.	EuroLAN UTP комутаційний шнур кат. 5e, 2 м	шт	38	15,00	570,00
7.	Комутаційні розетки	шт	33	23,00	759,00
8.	Роз’єми RJ-45	шт	66	2,00	132,00
9.	Короб 16x16	м	50	4,80	240,00
10.	Короб 25x16	м	121	6,80	822,80
11.	Короб 40x16	м	159	11,00	1749,00
12.	Короб 40x25	м	45	12,80	576,00
13.	Організатор кабелю	шт	4	428,00	1712,00
14.	Патч панель 19", 24 порта	шт	4	603,00	2412,00
15.	Шафа настінна 19", 12U	шт	1	3600,00	3600,00
16.	Шафа 6U	шт	3	1850,00	5550,00
18	D-Link D-Link DIR-2150	шт	1	1210	210,00
Р а з о м					84953.00

Отже, загальна сума матеріальних витрат на дану мережу становить 84953,80 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

Т – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даного сайту використовується один ПК з потужністю W = 0,09 кВт, який працює 60 годин.

$$З_е = 0{,}09 \cdot 60 \cdot 7{,}25 = 37.8 \text{ грн}$$

4.5 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є 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.

Для визначення амортизаційних відрахувань застосовуємо формулу:

$$А = \frac{Б_В \cdot Н_А}{100\%} \quad (4.8)$$

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

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

$Н_А$ – норма амортизації, %.

Для проектування даного сайту використовується один комп’ютер (вартість якого становить 40000 грн.), який працює 60 годин.

Тоді: $A = 40000 \cdot 0{,}04 \cdot 60 / 150 = 640{,}00$ (грн.)

4.6 Обчислення накладних витрат

Накладні витрати пов'язані з обслуговуванням виробництва, утриманням апарату управління підприємства (фірми) та створення необхідних умов праці.

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

$$Н_в = В_{о.п.} \cdot 0{,}2 \ldots 0{,}6\,, \qquad (4.9)$$

де $Н_В$ – накладні витрати.

$$Н_в = 64915.20 \cdot 0{,}4 = 32457{,}60 \text{ грн.}$$

4.7 Складання кошторису витрат та визначення собівартості ндр

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до заг. суми
Витрати на оплату праці (основну і додаткову заробітну плату)	64915.20	32,55
Відрахування на соціальні заходи	14281.34	7,16
Матеріальні витрати	84953,80	42,60
Витрати на електроенергію	37,8	0,05
Амортизаційні відрахування	640,00	1,35
Накладні витрати	32457,60	16,28
Собівартість	197285,74	100

Собівартість ($С_В$) НДР розрахуємо за формулою:

$$С_в = В_{о.п.} + В_{с.з.} + З_е + Т_в + А + Н_в, \quad (4.10)$$

$$С_в = 197285{,}74 \text{ (грн.)}$$

4.8 Розрахунок ціни ндр

Ціну НДР можна визначити за формулою:

$$Ц = \frac{С_в \cdot (1 + Р_{рен}) + К + В_{н.і.}}{К}, \quad (4.11)$$

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

К – кількість замовлень, од.;

$В_{і.н.}$ – вартість носія інформації, грн.;

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

$$Ц = 197285{,}74 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 307765{,}75 \text{ (грн)}$$

4.9 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.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ) і термін окупності ($Т_{ОК}$), який можна визначити за формулою 4.12.

$$ЧТВ = -К_В + \sum_{i=1}^{t} \frac{Г П}{(1+i)^t}, \quad (4.12)$$

де $К_В$ – затрати на проект; $Г_п$ – грошовий потік за t – ий рік; t – відповідний рік проекту; i - величина дисконтної ставки (10…15%).

Якщо ЧТВ ≥ 0, то проект може бути рекомендований до впровадження.

$$ЧТВ = -197285,74 + \frac{143542,01}{(1+0,1)} + \frac{143542,01}{(1+0,1)^2} = 51836,76$$

Термін окупності визначається за формулою 4.13:

$$T_{ОК} = T_{ПВ} + \frac{H_В}{Г_{ПР}}, \quad (4.13)$$

де $T_{ПВ}$ – період до повного відшкодування витрат, років; $H_В$ – невідшкодовані витрати на початок року, грн.; $Г_{ПР}$ – грошовий потік на початок року, грн.

$$T_{ОК} = 1 + \frac{66793,00}{143542,01} = 1,5$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 техніко-економічних показників.

Таблиця 4.5 - Техніко-економічні показники ндр

№п/п	Показник	Значення
1.	Собівартість, грн.	197285,74
2.	Плановий прибуток, грн.	110480,01
3.	Ціна, грн.	307765,75
4.	Економічна ефективність	51836,76
5.	Термін окупності, рік	1,5

Враховуючи основі економічні показники, зведені у таблицю 4.5, можна зробити висновок, що при терміні окупності – 1,5 роки проводити роботи по впровадженню даного проекту мережі є доцільним та економічно вигідним. Як можна побачити із розрахунків, основними є витрати на оплату праці та матеріальні витрати.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Державні нормативні акти про охорону праці

Стаття 27. Документи, що належать до нормативно-правових актів з охорони праці

Нормативно-правові акти з охорони праці - це правила, норми, регламенти, положення, стандарти, інструкції та інші документи, обов'язкові для виконання.

Стаття 28. Опрацювання, прийняття та скасування нормативно-правових актів з охорони праці

Опрацювання та прийняття нових, перегляд і скасування чинних нормативно-правових актів з охорони праці провадяться спеціально уповноваженим центральним органом виконавчої влади з нагляду за охороною праці за участю професійних спілок і Фонду соціального страхування від нещасних випадків та за погодженням з органами державного нагляду за охороною праці.

Санітарні правила та норми затверджуються спеціально уповноваженим центральним органом виконавчої влади у галузі охорони здоров'я.

Нормативно-правові акти з охорони праці переглядаються в міру впровадження досягнень науки і техніки, що сприяють поліпшенню безпеки, гігієни праці та виробничого середовища, але не рідше одного разу на десять років.

Стандарти, технічні умови та інші документи на засоби праці і технологічні процеси повинні включати вимоги щодо охорони праці і погоджуватися з органами державного нагляду за охороною праці.

Стаття 29. Тимчасове припинення чинності нормативно-правових актів з охорони праці

У разі неможливості повного усунення небезпечних і шкідливих для здоров'я умов праці роботодавець зобов'язаний повідомити про це відповідний орган

державного нагляду за охороною праці. Він може звернутися до зазначеного органу з клопотанням про встановлення необхідного строку для виконання заходів щодо приведення умов праці на конкретному виробництві чи робочому місці до нормативних вимог.

Відповідний орган державного нагляду за охороною праці розглядає клопотання роботодавця, проводить у разі потреби експертизу запланованих заходів, визначає їх достатність і за наявності підстав може, як виняток, прийняти рішення про встановлення іншого строку застосування вимог нормативних актів з охорони праці.

Роботодавець зобов'язаний невідкладно повідомити заінтересованих працівників про рішення зазначеного органу державного нагляду за охороною праці.

Стаття 30. Поширення дії нормативно-правових актів з охорони праці на сферу трудового і професійного навчання

Нормативно-правові акти з охорони праці є обов'язковими для виконання у виробничих майстернях, лабораторіях, цехах, на дільницях та в інших місцях трудового і професійного навчання, облаштованих у будь-яких навчальних закладах.

Організація охорони праці на зазначених об'єктах, а також порядок розслідування та обліку нещасних випадків з учнями і студентами під час трудового та професійного навчання у навчальних закладах визначаються центральним органом виконавчої влади в галузі освіти та науки за погодженням з відповідним профспілковим органом.

До учнів і студентів, які проходять трудове і професійне навчання (виробничу практику) на підприємствах під керівництвом їх персоналу, застосовується законодавство про охорону праці у такому ж порядку, що й до працівників підприємства.

5.2 Дії працівників у випадку виникнення пожежі

Як нам вже відомо, фактор часу на пожежі є визначальним. Тому дуже важливо своєчасно виявити пожежу. Виявлення пожежі здійснюється за допомогою технічних засобів (автоматичної пожежної сигналізації) персоналом та охороною об'єкта.

У разі виявлення пожежі або її ознак (запаху диму, полум'я або його відблисків) треба негайно повідомити про це телефоном пожежну охорону. При цьому необхідно назвати точну адресу об'єкта, кількість поверхів будівлі (висоту технологічної установки, споруди), місце виникнення пожежі, наявність людей, а також повідомити своє прізвище.

Після виклику пожежної охорони треба задіяти об'єктову систему оповіщення про пожежу, плани ліквідації аварії та евакуації людей. Одночасно здійснюється збір по сигналу тривоги об'єктової пожежної команди (добровільної пожежної дружини). У разі) необхідності викликаються інші рятувальні та оперативні служби < (газова, медична допомога, аварійна енергонагляду, міліція, прокуратура, служба безпеки тощо).

Посадові особи, які прибувають на місце пожежі згідно плану ліквідації аварій, повинні:

- перевірити, чи викликана пожежна охорона, ще раз зв'язавшись безпосередньо з нею;
- негайно організувати рятування та евакуацію людей;
- видалити за межі небезпечної зони усіх працівників, які не задіяні на гасінні пожежі, забезпечити охорону місця події;
- терміново припинити роботи в будівлі, на виробничому устаткуванні (якщо це не викликає загрози виникнення додаткової аварійної ситуації), припинити подачу електричної енергії, горючих речовин, роботу вентиляційних систем тощо;
- забезпечити дотримання техніки безпеки особами, які беруть участь в гасінні пожежі;

- зустріти підрозділи пожежної охорони, передати їм необхідну інформацію, вказати найкоротший шлях під'їзду до осередку пожежі та місць розташування джерел водопостачання.

Після прибуття першого пожежного підрозділу усе керівництво гасінням пожежі переходить до його начальника. Адміністрація та технічний персонал підприємства зобов'язані консультувати керівника гасіння пожежі про конструктивні та технологічні особливості об'єкта, надавати всебічну допомогу, виконувати його вказівки.

5.3 Засоби захисту людини від шкідливих речовин

Основними засобами захисту людини від впливу шкідливих речовин є: гігієнічне нормування їх вмісту у виробничій зоні і на робочому місці, а також різні методи очищення газових викидів (адсорбція, хімічне перетворення) та стоків (первинне, вторинне та третинне очищення). Потрібно, щоб на належному рівні була забезпечена робота колективних (наприклад, вентиляція) та індивідуальних засобів захисту людей.

Адсорбція – процес поглинання газів поверхнею твердих речовин (наприклад, адсорбція газів активованим вугіллям).

Нейтралізація – це перетворення токсичних речовин у нетоксичні чи малотоксичні речовини за допомогою хімічних реакцій. Наприклад, для нейтралізації сірчаної кислоти застосовують карбонат натрію:

$$H_2SO_4+Na_2CO_3 + Na_2SO_4 +H_2O+CO_2 \qquad (5.1)$$

Для перетворення токсичних сумішей газів у нетоксичні чи малотоксичні застосовується дожиг.

Пилоочистка здійснюється за допомогою спеціальних очисних пристроїв і споруд: фільтрів, пилоосаджувальних камер, пилососів, скруберів, електроприладів тощо.

Найбільш ефективним і дешевим способом зменшення кількості пилу є вологе прибирання у приміщенні та вентиляція приміщень.

Контроль за станом робочої зони при забрудненні повітря здійснюється за допомогою спеціальних приладів: загазованість – газоаналізаторами (ВПХР, УГ-2 та ін.); запиленість – фотометрією, мікроскопією тощо.

До загальних заходів попередження дії шкідливих речовин на працюючих належать:

- заміна шкідливих речовин менш шкідливими;
- удосконалення технологічних процесів та устаткування;
- автоматизація і дистанційне керування технологічним процесом;
- герметизація виробничого устаткування, локалізація шкідливих викидів;
- попередні та періодичні медичні огляди робітників, які працюють у шкідливих умовах, профілактичне харчування;
- використання засобів індивідуального захисту.

ВИСНОВКИ

З розвитком сучасних технологій виникає все більше потреб в створенні корпоративних мереж, типу мереж магазину з розмежованим доступом користувачів. Для реалізації такої мережі задіються такі елементи як: мережеве обладнання, різноманітні середовища передачі даних, мережеве програмне забезпечення, а також моделювання та проекція мережі в середовищі симулювання і головне протоколи зв'язку моделі OSI або TCP/IP. Метою роботи було створення комп'ютерної мережі магазину з розмежуванням доступу користувачів, де розмежування доступу налаштовувалося би за допомогою брандмауера або маршрутизатора. Під час виконання кваліфікаційної роботи автором здійснені основні науково-практичні результати:

1. Здійснений аналіз комп'ютерної мережі з демілітаризованою зоною, розглянуті основні компоненти для створення демілітаризованої зони. Показані умови створення DMZ, наведені конкретні приклади з використанням її в сучасних хмарних технологіях. Також були визначені переваги у використанні демілітаризованої зони в якості елементу для розмежування доступу користувачів в комп'ютерній системі.

2. Здійснений: обґрунтований вибір мережевого обладнання для створення комп'ютерної мережі магазину та проаналізовано середовища передачі даних в системі. Був складений опис вимог до: програмного забезпечення на мережевих пристроях та способів захисту мережевих пристроїв. Складено план розробки комп'ютерної мережі з розмежуванням доступом користувачів.

3. Було визначено список роботи задач, які має виконувати комп'ютерна мережа магазину з демілітаризованою зоною. Згідно розроблених задач була складена імітаційна модель корпоративної віртуальної мережі VLAN. Описано процес створення DMZ-зони та її налаштування в Cisco Packet Tracer, що дало можливість створити робочу модель комп'ютерної мережі магазину з розмежуванням доступом користувачів.

4. Спроектована комп’ютерна мережа магазину з розмежуванням доступу користувачів з централізованим управлінням, за топологією «зірка». В процесі розробки проектування було: розроблено три логічні схеми мережі(мережевого, канального та фізичного рівня), розроблено фізичну топологію мережі для трьох будівель(офісу, магазину та складу) та здійснено розрахунок вартості комп’ютерної мережі магазину з розмежуванням доступу. Отже, плани в реалізації комп’ютерної мережі магазину з розмежуванням доступу – було досягнуто. Реалізація і симуляція мережі відбувалася в середовищі Cisco Packet Tracer. Тестування мережі відбувалося в тому самому середовищі. Можна зробити висновок, що цінність даного дослідження полягає в удосконаленні кваліфікаційного рівня розвитку студента, як інженера комп’ютерних мереж, а також зробити доступнішим спосіб створення бюджетної комп’ютерної мережі магазину, тому що у багатьох компоненти або готові системи мають високу вартість.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров Є. В. Комп’ютерні мережі : підручник / Є. В. Буров – Львів : «Магнолія 2006», 2013. – 264 с.
2. Ткаченко В. А. Комп’ютерні мережі та телекомунікації : навч. посібник / В. А. Ткаченко, О. В. Касілов, В. А. Рябик – Харків : НТУ «ХПІ», 2011. – 224 с.
3. Николайчук Я. М. Проектування спеціалізованих комп’ютерних систем : навч. посібник / Я. М. Николайчук, Н. Я. Возна, І. Р. Пітух – Тернопіль : ТзОВ «Терно-Граф», 2010. – 394 с.
4. Кравчук С. О. Основи комп’ютерної техніки: компоненти, системи, мережі : навч. посібник для студ. ВНЗ / С. О. Кравчук, В. О. Шанін. – К. : «Політехніка», 2005. – 344 с.
5. Олексюк В. Організація комп’ютерної локальної мережі / В. Олексюк, Н. Балик, А. Балик – Тернопіль : Підручники та посібники, 2006. – 80 с
6. Москальова В. М. Основи охорони праці: Інтерактивний комплекс навчально-методичного забезпечення. Рівне.НУВГП , 2009.
5. Осадчук В. С. Волоконно-оптичні системи передачі : навч. посібник / В. С. Осадчук, О. В. Осадчук. – Вінниця : ВНТУ, 2005. – 225 с.
7. Встановлюємо Wordpress [Електронний ресурс] – Режим доступу до ресурсу : https://wordpress.co.ua/stvoryty-blog-na-wordpress/4-install-wordpress
8. Арсенюк І. Р. Комп’ютерні мережі. Ч. 1. : навч. посібник / І. Р. Арсенюк, А. А. Яровий. – Вінниця : ВНТУ, 2009. – 117 с.
9. Комп’ютерні мережі : навч. посібник / [О. Д. Азаров, С. М. Захарченко, О. В. Кадук та ін.]. – Вінниця : ВНТУ, 2013. – 374 с.
10. Месюра В. І. Інформаційно-пошукові системи мережі Інтернет. Ч.1. Принципи організації та функціонування Інтернет : навч. посібник / В. І. Месюра, І. Р. Арсенюк, О. М. Роїк – Вінниця : ВДТУ, 2002. – 86 с.
11. Бородкіна І. Л. Internet – технології: проектування Web–сторінки / І. Л. Бородкіна, О. В. Матвієнко. – К. : Центр навч. літератури, 2004. – 154 с.

ДОДАТОК А

Інструкція з налаштування програмного забезпечення серверів на базі Linux Ubuntu 22.04 для мережі магазинів "Торба"

Оновлення списку пакетів

sudo apt update

Оновлення системи

sudo apt upgrade -y

Встановлення необхідних базових пакетів

sudo apt install -y curl wget git vim htop tree unzip software-properties-common

Налаштування користувачів

Створення системного користувача для додатків

sudo adduser --system --group --shell /bin/bash TRB-app

Створення користувача для адміністрування

sudo adduser TRB-admin

sudo usermod -aG sudo TRB-admin

Налаштування SSH для нового користувача

sudo mkdir -p /home/TRB-admin/.ssh

sudo chmod 700 /home/TRB-admin/.ssh

sudo chown TRB-admin:TRB-admin /home/TRB-admin/.ssh

Налаштування часового поясу

Встановлення часового поясу України

sudo timedatectl set-timezone Europe/Kiev

Синхронізація часу

sudo systemctl enable systemd-timesyncd

sudo systemctl start systemd-timesyncd

Безпека системи

Налаштування SSH

Редагування конфігурації SSH

sudo vim /etc/ssh/sshd_config

Рекомендовані налаштування SSH

Port 2222

Protocol 2

PermitRootLogin no

PasswordAuthentication no

PubkeyAuthentication yes

MaxAuthTries 3

ClientAliveInterval 300

ClientAliveCountMax 2

AllowUsers TRB-admin

Перезапуск SSH сервісу

sudo systemctl restart ssh

Налаштування брандмауера UFW

Включення UFW

sudo ufw --force enable

Базові правила

sudo ufw default deny incoming

sudo ufw default allow outgoing

Дозвіл SSH на новому порту

sudo ufw allow 2222/tcp

Дозвіл HTTP та HTTPS

sudo ufw allow 80/tcp

sudo ufw allow 443/tcp

Перевірка статусу

sudo ufw status verbose

Встановлення Fail2Ban

Встановлення Fail2Ban

sudo apt install -y fail2ban

Створення локальної конфігурації

sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Налаштування jail.local

```
[DEFAULT]
bantime = 3600
findtime = 600
maxretry = 3
ignoreip = 127.0.0.1/8 192.168.0.0/16

[sshd]
enabled = true
port = 2222
logpath = /var/log/auth.log

[nginx-http-auth]
enabled = true
```

Запуск та автозапуск Fail2Ban

```
sudo systemctl enable fail2ban
sudo systemctl start fail2ban
```

Веб-сервер та база даних

Встановлення Nginx

Встановлення Nginx

```
sudo apt install -y nginx
```

Створення конфігурації для мережі Торба

```
sudo vim /etc/nginx/sites-available/TRB-stores
```

Конфігурація Nginx для магазинів

```
server {
    listen 80;
    server_name TRB-store.local *.TRB-store.local;
    root /var/www/TRB;
    index index.php index.html index.htm;
```

Логування

```
access_log /var/log/nginx/TRB-access.log;
error_log /var/log/nginx/TRB-error.log;
```

Безпека

```
server_tokens off;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-XSS-Protection "1; mode=block" always;
add_header X-Content-Type-Options "nosniff" always;
location / {
    try_files $uri $uri/ /index.php?$query_string;
}
location ~ \.php$ {
    fastcgi_pass unix:/var/run/php/php8.1-fpm.sock;
    fastcgi_index index.php;
    fastcgi_param SCRIPT_FILENAME $realpath_root$fastcgi_script_name;
    include fastcgi_params;
}
location ~ /\.ht {
    deny all;
}
}
```

Активація конфігурації

```
sudo ln -s /etc/nginx/sites-available/TRB-stores /etc/nginx/sites-enabled/
sudo nginx -t
sudo systemctl restart nginx
```

Встановлення PHP 8.1

Встановлення PHP та необхідних модулів

```
sudo apt install -y php8.1-fpm php8.1-mysql php8.1-curl php8.1-gd php8.1-mbstring php8.1-xml php8.1-zip php8.1-json php8.1-intl
```

Налаштування PHP-FPM

sudo vim /etc/php/8.1/fpm/pool.d/TRB.conf

Конфігурація PHP-FPM пулу для Торба:

[TRB]

user = TRB-app

group = TRB-app

listen = /var/run/php/php8.1-fpm-TRB.sock

listen.owner = www-data

listen.group = www-data

listen.mode = 0660

pm = dynamic

pm.max_children = 50

pm.start_servers = 5

pm.min_spare_servers = 5

pm.max_spare_servers = 35

pm.process_idle_timeout = 10s

pm.max_requests = 500

php_admin_value[date.timezone] = Europe/Kiev

php_admin_value[upload_max_filesize] = 32M

php_admin_value[post_max_size] = 32M

Встановлення MySQL 8.0

Встановлення MySQL

sudo apt install -y mysql-server

Безпечне налаштування MySQL

sudo mysql_secure_installation

Створення бази даних для мережі магазинів

sudo mysql -u root -p

SQL команди для налаштування бази даних

Створення бази даних

CREATE DATABASE TRB_stores CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;

Створення користувача

```
CREATE USER 'TRB_user'@'localhost' IDENTIFIED BY 'strong_password_here';
GRANT ALL PRIVILEGES ON TRB_stores.* TO 'TRB_user'@'localhost';

-- Створення користувача для резервних копій
CREATE USER 'TRB_backup'@'localhost' IDENTIFIED BY 'backup_password_here';
GRANT SELECT, LOCK TABLES, SHOW VIEW ON TRB_stores.* TO 'TRB_backup'@'localhost';

FLUSH PRIVILEGES;
EXIT;
```

Система резервного копіювання

Створення скриптів резервного копіювання

Створення директорії для скриптів

```
sudo mkdir -p /opt/TRB-backup/scripts
sudo mkdir -p /opt/TRB-backup/data
```

Створення скрипту резервного копіювання бази даних

```
sudo vim /opt/TRB-backup/scripts/backup-database.sh
```

Скрипт резервного копіювання бази даних

```
 !/bin/bash
  Конфігурація
DB_NAME="TRB_stores"
DB_USER="TRB_backup"
DB_PASS="backup_password_here"
BACKUP_DIR="/opt/TRB-backup/data"
DATE=$(date +%Y%m%d_%H%M%S)
RETENTION_DAYS=7
```

Створення резервної копії

mysqldump -u $DB_USER -p$DB_PASS --single-transaction --routines --triggers $DB_NAME > $BACKUP_DIR/TRB_db_$DATE.sql

Архівування

gzip $BACKUP_DIR/TRB_db_$DATE.sql

Очищення старих копій

find $BACKUP_DIR -name "TRB_db_*.sql.gz" -mtime +$RETENTION_DAYS -delete

Логування

echo "$(date): Database backup completed - TRB_db_$DATE.sql.gz" >> /var/log/TRB-backup.log

Надання прав виконання

sudo chmod +x /opt/TRB-backup/scripts/backup-database.sh

Налаштування cron для автоматичного резервного копіювання

Редагування crontab

sudo crontab -e

Додавання завдань

0 2 * * * /opt/TRB-backup/scripts/backup-database.sh

0 3 * * 0 /opt/TRB-backup/scripts/backup-files.sh

Моніторинг та логування

Встановлення системи моніторингу

Встановлення htop та iotop для моніторингу

sudo apt install -y htop iotop nethogs

Встановлення Netdata для веб-моніторингу

bash <(curl -Ss https://my-netdata.io/kickstart.sh) --stable-channel

Налаштування ротації логів

Створення конфігурації для логів Торба

sudo vim /etc/logrotate.d/TRB

Конфігурація ротації логів

/var/log/TRB-*.log {

daily

```
    missingok
    rotate 30
    compress
    delaycompress
    notifempty
    copytruncate
}

/var/log/nginx/TRB-*.log {
    daily
    missingok
    rotate 14
    compress
    delaycompress
    notifempty
    sharedscripts
    postrotate
        systemctl reload nginx
    endscript
}
```

Налаштування моніторингу дискового простору

Створення скрипту моніторингу

sudo vim /opt/TRB-backup/scripts/disk-monitor.sh

Скрипт моніторингу дискового простору

```
 !/bin/bash

THRESHOLD=80
EMAIL="admin@TRB-stores.ua"

df -H | grep -vE '^Filesystem|tmpfs|cdrom' | awk '{ print $5 " " $1 }' | while read
```

```
output;
        do
          usage=$(echo $output | awk '{ print $1}' | sed 's/%//g')
          partition=$(echo $output | awk '{ print $2 }')

          if [ $usage -ge $THRESHOLD ]; then
            echo "Увага: Розділ $partition заповнений на $usage%" | mail -s "Попередження про заповнення диска" $EMAIL
          fi
        done
```

Мережеві налаштування

Налаштування мережевого інтерфейсу

Редагування мережевої конфігурації

```
sudo vim /etc/netplan/01-netcfg.yaml
```

Приклад конфігурації мережі

```
network:
  version: 2
  renderer: networkd
  ethernets:
    ens18:
      dhcp4: false
      addresses:
        - 192.168.1.10/24
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8, 8.8.4.4, 1.1.1.1]
      dhcp6: false
```

Застосування налаштувань

```
sudo netplan apply
```

Налаштування DNS

Створення локального DNS файлу

sudo vim /etc/hosts

Додавання записів для мережі магазинів

127.0.0.1 localhost

192.168.1.10 TRB-server.local

192.168.1.10 admin.TRB-store.local

192.168.1.10 pos.TRB-store.local

Автоматизація та обслуговування

Створення скриптів обслуговування

Створення скрипту щоденного обслуговування

sudo vim /opt/TRB-backup/scripts/daily-maintenance.sh

Скрипт щоденного обслуговування

!/bin/bash

LOG_FILE="/var/log/TRB-maintenance.log"

DATE=$(date '+%Y-%m-%d %H:%M:%S')

echo "[$DATE] Початок щоденного обслуговування" >> $LOG_FILE

Очищення тимчасових файлів

find /tmp -type f -mtime +7 -delete

find /var/tmp -type f -mtime +7 -delete

Очищення логів старше 30 днів

find /var/log -name "*.log" -mtime +30 -delete

Оптимізація бази даних

mysql -u TRB_user -pstrong_password_here -e "OPTIMIZE TABLE TRB_stores.*;"

Перевірка дискового простору

df -h >> $LOG_FILE

echo "[$DATE] Завершення щоденного обслуговування" >> $LOG_FILE

Налаштування автоматичних оновлень безпеки

Встановлення unattended-upgrades

sudo apt install -y unattended-upgrades

Налаштування автоматичних оновлень

sudo dpkg-reconfigure -plow unattended-upgrades

Редагування конфігурації

sudo vim /etc/apt/apt.conf.d/50unattended-upgrades

Налаштування безпечних оновлень:

```
Unattended-Upgrade::Allowed-Origins {
   "${distro_id}:${distro_codename}-security";
   "${distro_id}ESMApps:${distro_codename}-apps-security";
   "${distro_id}ESM:${distro_codename}-infra-security";
};

Unattended-Upgrade::AutoFixInterruptedDpkg "true";
Unattended-Upgrade::MinimalSteps "true";
Unattended-Upgrade::Remove-Unused-Dependencies "true";
Unattended-Upgrade::Automatic-Reboot "false";
```

Фінальна перевірка системи

Перевірка статусу всіх сервісів

sudo systemctl status nginx php8.1-fpm mysql ssh fail2ban

Перевірка портів

sudo netstat -tlnp

Перевірка логів

sudo tail -f /var/log/syslog

Тестування веб-сервера

Завершальні налаштування

Створення документації для команди

1. Збережіть всі паролі в безпечному місці

2. Задокументуйте всі зміни в конфігураційних файлах

3. Створіть інструкції для відновлення з резервних копій

4. Налаштуйте моніторинг та сповіщення

Рекомендації по безпеці

- Регулярно оновлюйте систему
- Перевіряйте логи на предмет підозрілої активності
- Тестуйте резервні копії щомісяця
- Використовуйте сильні паролі та двофакторну автентифікацію
- Регулярно аудитуйте користувачів системи