Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення телекомунікацій та електронних систем

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

бакалавра

(освітній ступінь)

на тему: Розробка проекту комп'ютерної мережі компанії «BST

Виконав: студент VI курсу, групи КІб-602

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

_____ Юрій ГРЕСЬКІВ

(ім'я та прізвище)

Керівник Ігор ГЕНИК

(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 телекомунікацій та електронних систем
Циклова комісія комп'ютерної інженерії
Освітній ступінь бакалавр
Освітньо-професійна програма: Комп'ютерна інженерія
Спеціальність: 123 Комп'ютерна інженерія
Галузь знань: 12 Інформаційні технології

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"06" травня 2025 року

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

Греськіву Юрію Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Розробка проекту комп'ютерної мережі компанії «BST

керівник роботи Геник Ігор Степанович
(прізвище, ім'я, по батькові)

затверджені наказом Відокремленого структурного підрозділу «Тернопільський фаховий коледж Тернопільського національного технічного університетут імені Івана Пулюя» від 05.05.2025 р №4/9-217.

2. Строк подання студентом роботи: 20 червня 2025 року.

3. Вихідні дані до роботи: плани приміщень, завдання на проектування, стандарти побудови СКС, документація на мережеве обладнання і сервери

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

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

- План приміщень
- Логічна топологія
- Фізична топологія
- Таблиця IP-адрес
- Таблиця техніко-економічних показників
- Модель мережі

6. Консультанти розділів роботи

Розділ	Ім'я, прізвище та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Економічний розділ	Оксана РЕДЬКВА заст. директора з НВР		
Безпека життєдіяльності, основи охорони праці	Володимир ШТОКАЛО викладач		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Отримання і аналіз технічного завдання	06.05	
2	Збір і узагальнення інформації	19.05	
3	Написання першого розділу	23.05	
4	Розробка технічного та робочого проекту	28.05	
5	Написання спеціального розділу	3.06	
6	Розрахунок економічної частини	5.06	
7	Написання розділу охорони праці	7.06	
8	Виконання графічної частини	12.06	
9	Оформлення проекту	16.06	
10	Погодження нормоконтролю	18.06	
11	Попередній захист роботи	20.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: 06 травня 2025 року

Студент _____ Юрій ГРЕСЬКІВ
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Греськів Ю.І. Розробка проекту комп’ютерної мережі компанії «BST»: кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 123 Комп’ютерна інженерія. - Тернопіль : ВСП ТФК ТНТУ, 2025. -99с.

У кваліфікаційній бакалаврській роботі висвітлено процес розробки комп’ютерної мережі для компанії «BST» з урахуванням сучасних стандартів і вимог. Проєктом передбачено реалізацію гібридної фізичної топології, впровадження дротового сегменту на основі стандарту IEEE 802.3ab та бездротового – за технологією IEEE 802.11ac. Для забезпечення безпеки бездротового зв’язку застосовано метод шифрування WPA2-PSK із роботою у частотних діапазонах 2.4 ГГц і 5 ГГц. Мережева взаємодія реалізована за моделлю клієнт-сервер, із використанням стеку протоколів TCP/IP. Серверна частина функціонує під керуванням AlmaLinux Stream 9, з використанням iptables як міжмережевого екрану. Для забезпечення доступу до мережі Інтернет використано технологію NAT, а обмін файлами здійснюється через протокол FTP. Зпроєктована мережа відповідає вимогам сучасних IT-компаній до продуктивності, надійності та інформаційної безпеки.

Ключові слова: комп’ютерна мережа, гібридна топологія, TCP/IP, IEEE 802.11ac, AlmaLinux, NAT, iptables, клієнт-сервер.

ANNOTATION

Hreskiv Y.I. Development poject of a Computer Network for the “BST” Company: qualification work for obtaining a bachelor's degree, specialty 123 Computer Engineering. Ternopil Separate Structural Subdivision "Ternopil Professional College of Ivan Puluj National Technical University", 2025. -99p.

The bachelor's thesis presents the process of developing a computer network for the "BST" company in accordance with modern standards and requirements. The project provides for the implementation of a hybrid physical topology, the deployment of a wired segment based on the IEEE 802.3ab standard, and a wireless segment using IEEE 802.11ac technology. To ensure wireless communication security, WPA2-PSK encryption is used, operating in both 2.4 GHz and 5 GHz frequency bands. Network interaction is implemented using the client-server model based on the TCP/IP protocol stack. The server side runs under AlmaLinux Stream 9 and utilizes iptables as a firewall. Internet access is provided via NAT technology, and file exchange is carried out through the FTP protocol. The designed network meets the performance, reliability, and information security requirements of modern IT companies.

Keywords: computer network, hybrid topology, TCP/IP, IEEE 802.11ac, AlmaLinux, NAT, iptables, client-server.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

DHCP (Dynamic Host Configuration Protocol) – протокол динамічного призначення IP-адрес: автоматично надає параметри мережі клієнтам.

DNS (Domain Name System) – система доменних імен: служба, що перетворює доменні імена на IP-адреси.

FTP (File Transfer Protocol) – протокол передавання файлів: стандартний протокол для обміну файлами між комп'ютерами в мережі.

HTTPS (HyperText Transfer Protocol Secure) – захищений протокол передавання гіпертексту: розширення HTTP з шифруванням (SSL/TLS) для безпечного з'єднання.

IP-address (Internet Protocol address) – IP-адреса: унікальний числовий ідентифікатор, що призначається кожному пристрою в мережі для його ідентифікації та адресації.

ISP (Internet Service Provider) – постачальник послуг Інтернету: компанія, що надає користувачам доступ до мережі Internet.

LAN (Local Area Network) – локальна обчислювальна мережа: мережа, що охоплює обмежену територію (офіс, будівля).

MAC (Media Access Control) address – MAC-адреса: апаратний (фізичний) ідентифікатор мережевого інтерфейсу, записаний виробником.

MAT (MAC Address Translation) – трансляція MAC-адрес: технологія заміни MAC-адрес у заголовках Ethernet-пакетів.

NAT (Network Address Translation) – трансляція мережевих адрес: спосіб зміни IP-адрес у заголовках пакетів для маршрутизації між локальною та глобальною мережею.

SSID (Service Set Identifier) – ідентифікатор мережі Wi-Fi: унікальна назва бездротової мережі.

TCP/IP (Transmission Control Protocol / Internet Protocol) – набір мережевих протоколів, який забезпечує з’єднання та обмін даними в мережі Internet.

UDP (User Datagram Protocol) – протокол користувацьких дейтаграм: простий транспортний протокол без встановлення з’єднання, використовується для швидкої передачі даних.

URL (Uniform Resource Locator) – уніфікований локатор ресурсів: стандартна адреса для доступу до ресурсів в Internet (веб-сторінки, файли тощо).

UTP (Unshielded Twisted Pair) – неекранована вита пара: тип кабелю, який широко застосовується у комп’ютерних мережах.

VLAN (Virtual Local Area Network) – віртуальна локальна мережа: логічне об’єднання пристроїв у межах мережі незалежно від їх фізичного розміщення.

VPN (Virtual Private Network) – віртуальна приватна мережа: технологія безпечного з’єднання через загальнодоступні мережі.

WAN (Wide Area Network) – глобальна обчислювальна мережа: мережа, що охоплює великі географічні райони (міста, країни).

Wi-Fi (Wireless Fidelity) – бездротова технологія передачі даних, що забезпечує доступ до мережі без фізичного підключення кабелем.

ВСТУП

У кваліфікаційній роботі було поставлено завдання зі створення комп’ютерної мережі для компанії «BST». Розроблена мережа буде побудована на сучасних стандартах і протоколах з використанням актуального апаратного і програмного забезпечення

Актуальність теми обумовлена стрімким розвитком інформаційних технологій і необхідністю забезпечення стабільної, безпечної та високопродуктивної комунікаційної інфраструктури в сучасних компаніях. Ефективна комп’ютерна мережа є основою для оптимізації бізнес-процесів, обміну інформацією, спільної роботи та зберігання даних. Особливо це важливо для компаній, таких як «BST», які активно впроваджують цифрові технології у свою діяльність.

Практична цінність роботи полягає в розробці реального проєкту комп’ютерної мережі, який може бути впроваджений у діяльність підприємства. Запропоновані технічні рішення дозволяють підвищити рівень продуктивності, забезпечити інформаційну безпеку та забезпечити масштабованість мережі відповідно до потреб компанії. Результати роботи можуть бути використані як типове рішення для впровадження в інших організаціях зі схожими вимогами до мережевої інфраструктури.

ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.5 Найменування та область застосування

Темою кваліфікаційної роботи є проєктування комп’ютерної мережі для підприємства «BST». Метою цього проєкту є створення функціональної, ефективної та масштабованої мережевої інфраструктури, яка забезпечуватиме стабільний доступ користувачів до високошвидкісної системи передачі даних, локальних та глобальних інформаційних ресурсів, а також до необхідних мережевих сервісів і служб.

Запропоноване рішення орієнтоване на використання як в офісному просторі, так і в умовах гнучкої організації праці, включаючи підтримку стаціонарних робочих місць і мобільних користувачів. Розроблена мережа може бути ефективно впроваджена в організаціях, які потребують надійного обміну даними між підрозділами, централізованого доступу до серверів, ресурсів Інтернету, IP-телефонії, хмарних сервісів і систем віддаленого адміністрування [1].

Проєкт має високу практичну цінність і може бути адаптований для компаній малого та середнього бізнесу, навчальних установ, офісних центрів, які потребують безпечної, продуктивної та керованої комп’ютерної мережі.

1.1.2 Призначення розробки

На першому етапі підготовки до проєктування комп’ютерної мережі для підприємства «BST» було узгоджено з замовником перелік основних завдань, що підлягали реалізації в рамках технічного завдання. Зокрема, передбачалося:

- Забезпечити можливість доступу працівників і клієнтів компанії до основних мережевих сервісів.

- Виконати проєктування мережі відповідно до встановлених стандартів і технічних вимог.

- Організувати централізований і безпечний доступ користувачів до глобальної мережі Інтернет.

- Інтегрувати ключові сервіси локальної мережі, необхідні для забезпечення внутрішньої комунікації та обміну даними.

- Реалізувати заходи із захисту внутрішньої мережі від зовнішніх загроз та несанкціонованого доступу з боку Інтернету.

- Забезпечити криптографічний захист бездротового сегмента мережі від підключення сторонніх осіб.

- Розробити систему моніторингу та контролю за функціонуванням мережевої інфраструктури.

- Підготувати повний пакет технічної документації, що супроводжує розроблений мережевий проєкт.

1.1.3 Вимоги до апаратного і програмного забезпечення

Для реалізації поставлених завдань із проєктування комп’ютерної мережі компанії «BST» необхідно здійснити закупівлю та монтаж відповідного мережевого обладнання. До складу необхідних ресурсів входить як активне, так і пасивне обладнання, витратні матеріали, а також спеціалізоване програмне забезпечення.

Серед пасивної частини мережі передбачено використання кабельних каналів (коробів, гофрованих рукавів) та необхідних елементів кріплення. Для прокладання магістральних ліній обрано сертифікований кабель, сумісний із технологією Gigabit Ethernet, а також комплектуючі для його термінування. Передбачено встановлення мережевих розеток типу RJ-45 категорії 6,

монтажних елементів до них, а також патчпанелі на 24 порти. Патчкорди категорії 6 застосовуються для з’єднання патчпанелі з комутаторами та для підключення абонентських пристроїв до мережевих точок. Також до складу інфраструктури входить телекомунікаційна шафа, яка повинна відповідати вимогам з пожежної безпеки та вміщувати все необхідне обладнання. Для забезпечення надійної роботи передбачено блок безперебійного живлення типу line-interactive або on-line з відповідним запасом потужності.

До активного мережевого обладнання входять маршрутизатори з підтримкою безпровідного стандарту IEEE 802.11ac та гігабітних портів Ethernet. Планується встановлення комутаторів, сумісних із Gigabit Ethernet, зокрема одного комутатора з функціями статичної маршрутизації та пристроїв, які підтримують стандарт VLAN IEEE 802.1Q. Серверна частина представлена двома окремими серверами: перший - для реалізації функцій доступу до Інтернету та міжмережевого екранування, оснащений процесором Intel, оперативною пам’яттю обсягом не менше 16 ГБ, RAID-контролером та двома жорсткими дисками по 2 ТБ. Другий сервер виконує роль файлового сховища, має аналогічну конфігурацію, проте з дисковою підсистемою на базі двох накопичувачів по 4 ТБ.

Програмне забезпечення для серверної частини обирається з урахуванням підтримки протоколів TCP/IP, наявності функціоналу для створення міжмережевих екранів, відмовостійкості, відкритого ліцензування та можливості регулярного оновлення.

1.1.4 Вимоги до документації

Для забезпечення належного функціонування, технічної підтримки та своєчасного обслуговування розробленої комп’ютерної мережі компанії «BST» розробник повинен підготувати повний пакет технічної документації. Цей пакет документів є важливою складовою завершеного проєкту та

гарантує можливість подальшої експлуатації мережі без залучення сторонніх фахівців. Документація має включати поетапно сформовану проєктну інформацію, що відображає всі ключові технічні рішення та конфігурації.

До обов'язкових матеріалів належить план приміщень, у якому вказано місця встановлення активного та пасивного мережевого обладнання, розміщення кабельних трас, розеток і шаф. Логічна топологія повинна чітко демонструвати принципи зв'язку між мережевими вузлами, серверними ресурсами, маршрутизаторами, комутаторами та іншими активними пристроями. Фізична топологія, у свою чергу, має відображати фактичне кабельне з'єднання пристроїв і розміщення інфраструктурних елементів відповідно до плану приміщення.

Особливу увагу слід приділити таблиці IP-адресації, яка містить точну відповідність між MAC-адресами, IP-адресами, ролями пристроїв і їхніми фізичними інтерфейсами. Вона необхідна для адміністрування, усунення несправностей і масштабування мережі.

Крім того, розробник зобов'язаний надати інструкції щодо первинного та повторного налаштування мережевих компонентів, зокрема серверів, комутаторів, маршрутизаторів та кінцевих пристроїв користувачів. Окремим пунктом повинні бути методичні рекомендації з тестування працездатності мережі: перевірка пропускної здатності, наявності зв'язку між вузлами, доступності мережевих служб і сервісів, а також засоби локалізації можливих проблем.

Завершує комплект документації опис системи моніторингу, яка дозволить автоматично або вручну відслідковувати технічний стан мережі, навантаження на її вузли, події безпеки, журналювання збоїв і підозрілої активності. Такий підхід до оформлення документації дозволяє забезпечити безперебійну роботу мережі та підвищити її експлуатаційну надійність у довгостроковій перспективі.

1.1.5 Техніко-економічні показники

Проєкт локальної комп'ютерної мережі характеризується сукупністю визначених технічних та економічних параметрів. Основні з них узагальнено та представлено в таблиці 1.1.

Під час підбору мережевого обладнання для реалізації даного проєкту необхідно дотримуватися вказаних показників, оскільки вони впливають на ефективність функціонування системи та відповідність її експлуатаційним вимогам підприємства.

Таблиця 1.1 – Основні технічні та економічні характеристики проєкту локальної мережі

№ п/п	Характеристика	Показник
1	2	3
1	Тип фізичної топології	Комбінована (гібридна)
2	Тип логічної топології	Gigabit Ethernet (стандарт IEEE 802.3ab)
3	Операційна система сервера доступу до Інтернету	AlmaLinux 9 amd64
4	ОС файлового сервера	AlmaLinux 9 amd64
5	Маршрутизатор для безпровідного доступу	Пристрій із підтримкою шифрування WPA2-PSK
6	Основний мережевий комутатор	Пристрій рівня L3
7	Комутатори для робочих груп	Пристрій рівня L2 чи L2+ відповідно до вимог замовника
8	Метод спільного доступу до Інтернет-каналу	Технологія NAT

Продовження таблиці 1.1

1	2	3
9	ПЗ файлового сервера	Proftpd
10	ОС робочих станцій	Windows 11 Pro
11	Засоби міжмережевого захисту	iptables
12	Орієнтовні витрати на матеріали	до 180 тис.грн.
13	Загальна кошторисна вартість проєкту	до 360 тис.грн.

1.1.6 Стадії та етапи розробки

Перед початком проектування локальної мережі для компанії «BST» необхідно ретельно проаналізувати та врахувати всі вимоги, які висуваються до розробки системи. Ці вимоги формуються на основі технічного завдання, яке складається з урахуванням побажань замовника та обов'язково погоджується з ним для уникнення непорозумінь.

Наступним кроком після детального вивчення вимог є ознайомлення з планом приміщень, у межах яких буде реалізовуватися проект мережі. Аналіз просторового розташування дозволяє розробити логічну топологію мережі - схему взаємозв'язків між мережевими вузлами. Потім на основі логічної топології створюється фізична топологія, що відображає фактичне розміщення мережевого обладнання та кабельних трас на плані приміщення.

Найбільш складним і трудомістким етапом є монтаж інфраструктури - прокладання кабельних каналів, укладання мережевих кабелів, встановлення комутаційного обладнання, виконання термінування та проведення тестування наявності фізичних з'єднань.

На заключному етапі здійснюється конфігурування мережевих пристроїв і налаштування їх параметрів, після чого проводиться комплексне

тестування роботи всієї мережі. Це тестування включає перевірку конфігураційних файлів обладнання, контроль відповідності налаштувань вимогам технічного завдання та оцінку функціональності мережевих сервісів. Такий системний підхід забезпечує надійну та ефективну роботу розробленої мережі.

1.1.7 Порядок контролю та прийому

Порядок контролю та прийому в експлуатацію локальної мережі передбачає комплексний підхід, що включає участь уповноважених представників компанії-замовника та кваліфікованих технічних спеціалістів, відповідальних за впровадження проекту.

На першому етапі проводиться перевірка відповідності фактичних технічних характеристик мережі вимогам, визначеним у технічному завданні. Для цього використовуються як апаратні, так і програмні засоби контролю, що дозволяють детально оцінити роботу мережевого обладнання, стабільність з’єднань, пропускну здатність, безпеку, а також інші критичні параметри мережі.

В процесі приймальних випробувань здійснюється тестування всіх компонентів мережі — від фізичної цілісності кабельної системи до функціональності мережевих сервісів та захисних механізмів. Особлива увага приділяється виявленню та усуненню можливих несправностей чи невідповідностей.

Результати проведених перевірок оформлюються у вигляді офіційної документації, яка містить детальний звіт про технічний стан мережі, підтвердження відповідності вимогам, а також рекомендації щодо подальшої експлуатації та обслуговування. Лише після позитивного завершення всіх контрольних процедур мережа офіційно приймається в експлуатацію, що гарантує її надійність та ефективність у подальшому використанні.

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

Тема кваліфікаційної роботи передбачає проєктування мережевої інфраструктури для компанії «BST».

Для виконання поставленого завдання необхідно:

- Визначити та сформулювати основні вимоги до майбутньої локальної мережі.

- Розробити логічну структуру мережі, що відображає взаємозв'язок її компонентів.

- Спроєктувати фізичну топологію, враховуючи розташування обладнання та кабельної інфраструктури.

- Провести монтаж кабельної системи відповідно до технічних стандартів.

- Підібрати необхідне мережеве обладнання згідно з вимогами, викладеними у розділі 1.1.3 «Вимоги до апаратного і програмного забезпечення».

- Налаштувати операційну систему шлюзу для забезпечення мережевого захисту та організації спільного доступу до Інтернету.

- Сконфігурувати безпровідні маршрутизатори для стабільної роботи у провідній та бездротовій мережах.

- Провести тестування кабельної системи на відповідність стандартам Gigabit Ethernet.

- Перевірити конфігураційні файли мережевого обладнання на відсутність помилок та некоректних налаштувань.

- Підготувати повний комплект технічної документації по мережі.

Проєкт розробляється для компанії «BST», яка спеціалізується на створенні програмного забезпечення, розробці вебсайтів та інтернет-магазинів, а також їх впровадженні й технічній підтримці. Наразі

підприємство займає четвертий поверх багатоповерхового офісного будинку, та розташовано у 16 робочих кабінетах. План розташування кабінетів наведено у документі 2025.КРБ.123.602.10.00.00 ПП.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування логічного типу мережі

Логічна структура мережі побудована на основі комбінації дротових сегментів, організованих за принципом «розширеної зірки», та бездротових зон з комірчастою (cellular) структурою. Такий підхід дозволив сформувати гібридну топологію, яка поєднує переваги обох рішень та забезпечує гнучкість для подальшого масштабування або оновлення мережевої інфраструктури.

Для підвищення мобільності користувачів, що дозволяє працювати без жорсткої прив’язки до конкретного робочого місця, а також для впровадження контролю доступу, в архітектурі мережі застосовано механізм віртуальних локальних мереж (VLAN).

Розподіл комп’ютерної мережі на окремі логічно ізольовані сегменти, кожен з яких функціонує у власному діапазоні IP-адрес, здійснюється шляхом впровадження віртуальних локальних мереж (VLAN). Для реалізації цього механізму застосовується стандарт IEEE 802.1Q, який забезпечує маркування Ethernet-кадрів спеціальними тегами VLAN. Завдяки цьому стає можливим передавання трафіку з різних віртуальних сегментів через один фізичний канал зв’язку без втрати логічного розмежування. Протокол 802.1Q є загальноприйнятим і широко підтримується більшістю сучасного мережевого обладнання. Його застосування дозволяє не лише оптимізувати структуру мережі, підвищуючи її керованість, але й суттєво посилити безпеку, обмежуючи небажану міжсегментну взаємодію. Такий підхід особливо ефективний у корпоративному середовищі, де одночасно функціонують різні підрозділи, сервіси та рівні доступу [4].

В додатку Б представлено схему логічного поділу мережі підприємства «BST» на окремі підмережі у вигляді таблиці «Логічна адресація ЛОМ».

Також у цьому ж додатку подано таблицю «Конфігурація VLAN», де зазначено типи портів комутаторів, необхідні для належного налаштування віртуальних мереж.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з'єднань та їх прокладка

Опис структури та зв'язків між усіма мережевими вузлами представлено на демонстраційних схемах «Логічна топологія» та «Фізична топологія». Побудова локальної мережі здійснювалася з використанням неекранованої витої пари шостої категорії, що забезпечує високі швидкості передавання даних і відповідає сучасним вимогам до офісних мереж.

Під час вибору кабелю було враховано такі критерії, як якість провідника, відгуки користувачів, відповідність державним та міжнародним стандартам, а також співвідношення ціни та якості. В результаті було обрано кабель українського виробництва – Одескабель U/UTP Cat.6 4Pr Indoor, який повністю відповідає нормам ДСТУ IEC 61156-5, ДСТУ EN 50288-6-1 та ТУ У 27.3-05758730-097:2018.

Усі кабельні лінії, що ведуть від патчпанелі до кінцевих пристроїв, прокладено у кабельних каналах (коробах), що забезпечує як естетичний вигляд, так і зручність в обслуговуванні. Безпровідні маршрутизатори підключаються до локальної мережі через патчкорди, що з'єднують їх із настінними мережевими розетками, інтегрованими в кабельні канали. Розміщення маршрутизаторів здійснено на стінах у точках з оптимальним рівнем сигналу та в безпосередній близькості до джерел живлення.

Мережеві розетки, підключені до кабелів, заведені до патчпанелі в комутаційній шафі. У ній реалізується логіка підключень за допомогою патчкордів різної довжини, що дозволяє швидко змінювати схему з'єднань за

потреби. На рисунку 2.1 наведено вигляд патчпанелі, що використовується у даному проекті.

Рисунок 2.1 – Вигляд використаної патчпанелі

Відповідно до планувального креслення приміщень, довжина кабельної лінії між мережевими розетками або між розеткою та патчпанеллю не перевищує 90 метрів. Це відповідає встановленим стандартом обмеженням щодо максимально допустимої довжини з'єднання між комп'ютером і комутаційним обладнанням, яка складає 100 метрів. Залишкові 10 метрів передбачені для підключення за допомогою патчкордів – від розетки до робочої станції та від патчпанелі до комутатора [2].

На рисунку 2.2 наведено приклад патчкорду, що використовується в мережі.

Рисунок 2.2 – Взірець патчкорду

2.2.2 Структура мережевих вузлів та обґрунтування їх застосування

Центральним елементом проєктованої локальної мережі є комутатор третього рівня моделі OSI, який забезпечує взаємозв'язок усіх мережевих вузлів. Основний комунікаційний вузол, що фізично розміщується в серверному приміщенні, включає такі компоненти:

- головний комутатор;
- патчпанелі;
- джерело безперебійного живлення (ДБЖ);
- серверне обладнання.

Усе вищезазначене обладнання інсталюється в телекомунікаційній шафі стандарту 24U. Вибір саме такої шафи зумовлений зручністю монтажу елементів, наявністю механічного захисту (замка) та вбудованими електричними розетками для живлення активних пристроїв.

Комутатори, що обслуговують робочі групи, розміщуються на стінах у межах відповідних підрозділів компанії. У такий самий спосіб здійснюється монтаж бездротових маршрутизаторів – з урахуванням забезпечення оптимального радіусів дії та доступу до електроживлення.

2.3 Обґрунтування вибору мережевого обладнання

Для реалізації технічного завдання необхідно підібрати відповідне мережеве обладнання, зокрема сервери, які забезпечуватимуть функціонування шлюза та файлового сховища.

У додатку В, у таблиці «Порівняльна характеристика апаратних конфігурацій серверів», наведено технічні параметри серверного обладнання, що рекомендовано до використання для реалізації зазначених функцій.

На рисунку 2.3 представлено зовнішній вигляд сервера Dell PowerEdge R530 [15]. Даний пристрій обрано як для сервера шлюза, так і для сервера

зберігання даних, оскільки він поєднує в собі високий рівень продуктивності, надійності, а також має позитивну репутацію щодо тривалості безперебійної роботи (Mean Time Between Failures — MTBF). Виробник Dell є відомим гравцем на ринку серверного обладнання, що гарантує якісну технічну підтримку та оновлення програмного забезпечення.

Рисунок 2.3 – Зовнішній вигляд та комплектація серверу Dell PowerEdge R530

У додатку В, у таблиці «Технічні характеристики комутаторів», подано порівняльний аналіз технічних параметрів комутаційного обладнання, що розглядалось для використання як головного вузла комутації локальної мережі.

В результаті аналізу було обрано комутатор Edge-Core ECS4610-26T/L3 [16] для реалізації функцій центрального елемента мережної інфраструктури. Зовнішній вигляд цього пристрою представлено на рисунку 2.4.

Цей комутатор було обрано з огляду на його підтримку маршрутизації третього рівня (L3), необхідну кількість портів Gigabit Ethernet, функціональність VLAN за стандартом IEEE 802.1Q, а також підтримку функцій якості обслуговування (QoS), необхідних для керування трафіком у розгалуженій мережі. Крім того, пристрій забезпечує високу надійність та масштабованість, що є важливими критеріями для побудови ядра мережі з можливістю подальшої модернізації.

Рисунок 2.4 – Головний комутатор Edge-Core ECS4610-26T/L3

Комутатор, який обслуговує окремий відділ, виконує функцію об’єднання персональних комп’ютерів (ПК) у єдиний сегмент локальної мережі. У таблиці «Порівняння технічних характеристик комутаторів робочих груп», що наведена в додатку, представлено аналіз двох моделей комутаторів, які можуть бути використані для побудови сегментів мережі.

На основі аналізу було прийнято рішення використовувати обладнання від виробника Allied Telesyn, зокрема моделі AT-GS950/8 та AT-GS950/16 [13]. Обидва пристрої підтримують роботу на базі технології Gigabit Ethernet, мають функціональні можливості керованої комутації та підтримують протокол IEEE 802.1Q, що дозволяє налаштовувати віртуальні локальні мережі (VLAN).

Обрані моделі застосовуватимуться як основні комутуючі елементи у відповідних відділах або робочих групах, забезпечуючи ефективне з’єднання пристроїв всередині кожного сегмента з можливістю централізованого керування, моніторингу та подальшої інтеграції в загальну мережеву інфраструктуру.

Порівняння технічних параметрів безпровідних маршрутизаторів від різних виробників представлено в таблиці «Порівняльна характеристика безпровідних маршрутизаторів», що міститься в додатку. Ці пристрої

призначені для забезпечення доступу до локальної мережі клієнтів, що підключаються по бездротовому каналу зв’язку (Wi-Fi).

Кожен з аналізованих маршрутизаторів має щонайменше два основних інтерфейси: один – для з’єднання з провідною частиною мережі (через порт Ethernet), інший – для обслуговування безпровідних пристроїв (через радіоінтерфейс Wi-Fi). Така схема дозволяє забезпечити ефективну інтеграцію бездротового сегмента з основною фізичною інфраструктурою мережі.

У якості основного пристрою для організації доступу бездротових клієнтів до мережі було обрано маршрутизатор Linksys WRT-1900AC [19], зображений на рисунку 2.5. Цей маршрутизатор підтримує стандарти IEEE 802.11ac та IEEE 802.11n, має потужні зовнішні антени, що забезпечують широкий радіус покриття, а також високий рівень продуктивності, що робить його оптимальним для використання в офісному середовищі з великою кількістю клієнтських пристроїв.

Рисунок 2.5 – Wi-fi роутер Linksys WRT-1900AC

Для розміщення серверного обладнання та центрального комутатора передбачено використання комутаційної шафи. Вибір шафи здійснено з урахуванням необхідного запасу місця для подальшого розширення, її висота становить 24U [21]. На рисунку 2.6 наведено зображення обраної комутаційної шафи.

Рисунок 2.6 – Шафа серверна підлогова 24U

Для організації комутації з’єднань планується застосування 24-портової патчпанелі категорії 6. Кабельна інфраструктура буде побудована на основі неекранованої витої пари категорії 6. На рисунку 2.7 представлено обраний нами мережевий кабель - вита пара (U/UTP Cat.6).

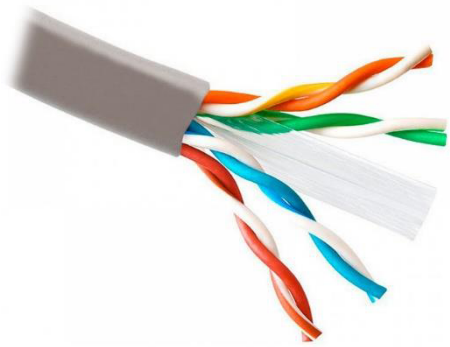


Рисунок 2.7 – Вибраний кабель - вита пара

У таблиці 2.1 представлено список активного та пасивного обладнання, яке передбачено для створення локальної мережі.

Таблиця 2.1 – Перелік активного та пасивного обладнання

№ п/п	Найменування обладнання	Од. вим.	Кіль-кість	Орієнтовна вартість, грн.	Загальна вартість, грн.
1	2	3	4	5	6
1	Кабель типу вита пара U/UTP категорії 6 (305 м)	шт.	2	5500	11000
2	Мережева розетка типу UTP Cat.6	шт.	50	100	5000
3	Патчкорд UTP Cat.6 (1 метр)	шт.	70	17	1190
4	Патчпанель на 24 порти (Cat.6, тип UTP)	шт.	1	1680	1680
5	Кабель-канал (загальна довжина)	м.	130	70	9100
6	Серверна монтажна шафа 24U, 19"	шт.	1	6622	6622
7	Магістральний комутатор Edge-Core ECS4610-26T/L3	шт.	1	22458	22458
8	Комутатор для сегментів – Allied Telesis AT-GS950/8	шт.	5	2900	14500
9	Комутатор Allied Telesyn – AT-GS950/16	шт.	1	3200	3200
10	Сервер для шлюзу – Dell PowerEdge R530	шт.	1	30000	30000
11	Сервер для зберігання даних – Dell PowerEdge R530	шт.	1	34000	34000

Продовження таблиці 2.1

1	2	3	4	5	6
12	Блок безперебійно живлення (ДБЖ) APC серії Smart-UPS 2 кВт	шт.	1	15000	15000
13	Бездротовий маршрутизатор Linksys WRT-1900AC	шт.	2	5200	10400
14	Мережевий фільтр-подовжувач, довжина 5 м, 5 розеток	шт.	2	400	800

Отже, загальна сума матеріальних витрат складає 169 950 грн. Ця сума повністю поміщається в ліміт замовника, що свідчить про раціональний підхід до підбору обладнання з урахуванням технічних вимог і бюджету проєкту.

2.4 Особливості монтажу мережі

Якість виконання монтажних робіт комп'ютерної мережі безпосередньо впливає на її експлуатаційні характеристики, стійкість до завад та загальну надійність функціонування. Тому реалізація мережевої інфраструктури має здійснюватися виключно підготовленими спеціалістами, які володіють практичними навичками та відповідним досвідом у цій сфері. Для забезпечення якісного монтажу необхідне використання професійного інструменту, сертифікованих витратних матеріалів та дотримання відповідних технічних норм.

Процес розгортання локальної мережі умовно поділяється на такі основні етапи:

- попередня підготовка приміщень до інсталяції мережевої інфраструктури;

- прокладання кабельної траси та організація пасивної частини мережі;

- інсталяція та підключення активного мережевого обладнання;

- конфігурування програмного забезпечення та мережевих пристроїв.

Усі перелічені етапи є взаємозалежними, тому кожен з них вимагає належної уваги та ретельного виконання для досягнення гарантованого результату.

Враховуючи, що в рамках даного проєкту для побудови кабельної системи використовується неекранована вита пара категорії 6, під час інсталяції необхідно дотримуватися таких технічних рекомендацій:

- мінімальний радіус вигину кабелю повинен становити не менше одного дюйма (приблизно 2,5 см);

- мінімальна дистанція між кабелем передачі даних та електричними кабелями напругою 220 Вольт має бути не менше чотирьох дюймів (орієнтовно 12 см);

- усі елементи кабельної системи повинні відповідати єдиній категорії, що гарантує узгодженість технічних характеристик і стабільність передачі даних [4].

2.5 Обґрунтування вибору програмного забезпечення

У якості операційної системи для серверного обладнання обрано безкоштовну Open Source ОС AlmaLinux 9 amd64, яка є стабільною та надійною альтернативою комерційному дистрибутиву Red Hat Enterprise Linux (RHEL). AlmaLinux розроблена як повністю сумісний форк RHEL, що забезпечує корпоративний рівень продуктивності та безпеки без витрат на ліцензування. Вона підтримується спільнотою та отримує регулярні оновлення системної безпеки, ядра та прикладного програмного

забезпечення. Завдяки високому рівню стабільності, відкритості коду і довготривалій підтримці, AlmaLinux 9 є оптимальним вибором для розгортання таких сервісів, як шлюзовий сервер для доступу до Інтернету, файловий сервер, а також внутрішні корпоративні служби (наприклад, DNS, DHCP, FTP, Samba, тощо) [14].

Цей вибір також обґрунтований тим, що AlmaLinux відповідає вимогам для розміщення серверних додатків у критично важливих середовищах, включаючи підтримку SELinux, автоматизацію через Ansible, а також сумісність із більшістю систем моніторингу й віртуалізації.

На робочих станціях використовується ліцензійна версія операційної системи Windows 11 Pro, яка належить компанії «BST». Встановлене ПЗ має статус OEM-ліцензії, тобто було придбано разом із апаратною частиною ПК. Windows 11 Pro забезпечує сучасний рівень безпеки, підтримку шифрування, політик групового керування, віддаленого підключення, а також сумісність з більшістю професійного програмного забезпечення, що активно використовується в повсякденній діяльності підприємства.

Таким чином, поєднання відкритої серверної платформи AlmaLinux з комерційною ОС Windows 11 Pro на клієнтських пристроях дозволяє досягти оптимального балансу між надійністю, функціональністю, безпекою та економічною ефективністю всієї мережевої інфраструктури.

2.6 Обґрунтування вибору засобів захисту мережі

Захист локальної мережі базується на використанні програмних файрволів, інтегрованих як у серверні операційні системи, так і в клієнтські. В ОС Linux застосовується вбудований файрвол iptables, який активується за замовчуванням і є потужним інструментом для фільтрації мережевого трафіку.

Iptables зберігає концепцію, закладену в утиліті ipfwadm, де функціонування брандмауера визначається набором правил. Кожне правило складається з умов (стандартів) та дій, які застосовуються до пакетів, що їм відповідають. У порівнянні з ipchains, iptables вводить поняття таблиць — груп незалежних ланцюжків правил, кожна з яких відповідає за певну функцію:

- таблиця filter контролює фільтрацію пакетів;
- таблиця nat обробляє трансляцію мережевих адрес;
- таблиця mangle модифікує заголовки пакетів (наприклад, змінює TTL або TOS).

Важливо, що у iptables змінена логіка проходження пакетів через ланцюжки: вхідні пакети, які призначені для самого хоста, проходять через ланцюжок INPUT, тоді як у ipchains всі вхідні пакети, включно з переданими далі, потрапляли в INPUT. Це розділення дозволяє більш точно контролювати маршрутизацію та фільтрацію трафіку.

Ключова перевага iptables — підтримка фільтрації за станом з’єднання (stateful filtering). Це означає, що брандмауер аналізує не лише окремі пакети за їхніми заголовками (IP-адреса, порт), але й враховує контекст самого з’єднання — чи було воно вже встановлене, нове чи відповідає певним критеріям. Такий підхід дозволяє приймати більш обґрунтовані рішення про дозвіл або блокування трафіку, підвищуючи безпеку мережі.

Для робочих станцій застосовується вбудований у Windows 11 Pro файрвол, який надає базовий захист і керує вхідними та вихідними з’єднаннями відповідно до заданих політик безпеки.

Окрім безпосереднього фільтрування мережевого трафіку, важливим елементом безпеки є розробка й імплементація політик контролю доступу, які регламентують взаємодію користувачів, пристроїв і сервісів у мережі. Вони визначають такі можливості:

Принцип мінімальних привілеїв, за яким кожному користувачу або пристрою надається лише той рівень доступу, який необхідний для виконання їхніх функцій. Це мінімізує ризик несанкціонованого доступу та поширення загроз.

Сегментацію мережі за допомогою VLAN, що дозволяє логічно розділити мережу на окремі сегменти. Це ізолює критичні ділянки мережі та обмежує можливості розповсюдження потенційних атак.

Механізми аутентифікації і авторизації, які гарантують, що доступ до ресурсів отримують лише перевірені користувачі та пристрої.

Фільтрацію мережевого трафіку за IP-адресами, портами, протоколами, що дозволяє детально контролювати, які дані можуть проходити крізь мережу.

Моніторинг, логування та аудит подій безпеки, що допомагають у виявленні та аналізі інцидентів, а також у забезпеченні відповідності внутрішнім та зовнішнім політикам безпеки.

У проектованій локальній мережі зазначені політики реалізуються через комплекс заходів:

- На серверному рівні iptables контролює доступ до мережевих сервісів, враховуючи стан з’єднань і контекст трафіку.

- На робочих станціях використовується Windows Firewall, який захищає локальні системи, керуючи доступом до мережі.

- Мережеві комутатори підтримують функції VLAN, що забезпечують ізоляцію трафіку між різними підрозділами або групами користувачів.

- Безпровідні маршрутизатори конфігуруються із застосуванням сучасних стандартів безпеки, таких як WPA3, та фільтрації за MAC-адресами для додаткового контролю підключень.

Завдяки такому багаторівневому підходу захисту і чітко прописаним політикам доступу, проектована мережа забезпечує надійний рівень безпеки, стабільність функціонування та гнучкість у керуванні доступом до ресурсів.

2.7 Тестування локальної мережі

Процес тестування локальної мережі передбачає проведення комплексної перевірки функціональності та якості з'єднань і здійснюватиметься у два основні етапи [7]:

1. Тестування безпровідної частини мережі

На цьому етапі буде проведено детальний аналіз роботи безпровідних пристроїв у різних точках розміщення. Для оцінки якості радіосигналу використовуватимуться спеціалізовані утиліти, такі як SSIDInsider та NetStumbler. Дані інструменти дозволяють:

- Вимірювати рівень сигналу Wi-Fi в реальному часі;
- Визначати рівень шуму та завади, які впливають на стабільність безпровідного зв'язку;
- Виявляти приховані або непомітні джерела радіоперешкод, які можуть знижувати якість зв'язку;
- Оцінювати покриття безпровідної мережі у різних приміщеннях або зонах офісу.

Результати цього тестування допоможуть оптимізувати розташування точок доступу, налаштувати параметри передавачів і мінімізувати вплив зовнішніх факторів на стабільність та швидкість безпровідної мережі.

2. Тестування провідної частини мережі

На другому етапі тестуватиметься якість кабельної інфраструктури, що є основою для стабільної роботи локальної мережі. Для цього застосовуватимуться професійні кабельні тестери, сертифіковані відповідно до стандарту 1000Base-TX (Gigabit Ethernet). Основні завдання тестування включають:

- Перевірку цілісності та правильності підключення кабелів;
- Визначення довжини кабелю, а також можливих місць ушкоджень або ослаблення сигналу;

- Оцінку відповідності кабельної системи стандартам категорії 6.

- Вимірювання параметру NEXT (Near-End Crosstalk), який характеризує рівень перехресних наводок між парами кабелю і впливає на якість передачі даних;

Цей етап тестування гарантує, що фізична кабельна структура відповідає технічним вимогам, що забезпечує швидку та надійну передачу даних без втрат і затримок.

Такий комплексний підхід до тестування обох складових мережі — безпровідної та провідної — забезпечить високу якість роботи системи, стабільність з’єднань і своєчасне виявлення можливих проблемних ділянок, що дозволить їх оперативно усунути.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з налаштування серверного ПЗ

3.1.1 Інструкції з інсталяції iptables серверу-шлюзу в Інтернет

У більшості офісних мереж, як правило, використовується один загальний канал доступу до Інтернету, який має одночасно обслуговувати всіх користувачів локальної мережі. При цьому важливо забезпечити належний рівень інформаційної безпеки. Для вирішення цього завдання між зовнішнім Інтернет-з'єднанням і внутрішньою мережею впроваджується окремий сервер, що виконує функцію міжмережевого екрана.

Зазвичай для цього використовується сервер на базі операційної системи Linux, обладнаний двома мережевими інтерфейсами: один з них призначений для підключення до локальної мережі, інший — до мережі провайдера. На рисунку 3.1 представлено структурну схему функціонування системи фільтрації трафіку за допомогою засобів iptables [19].

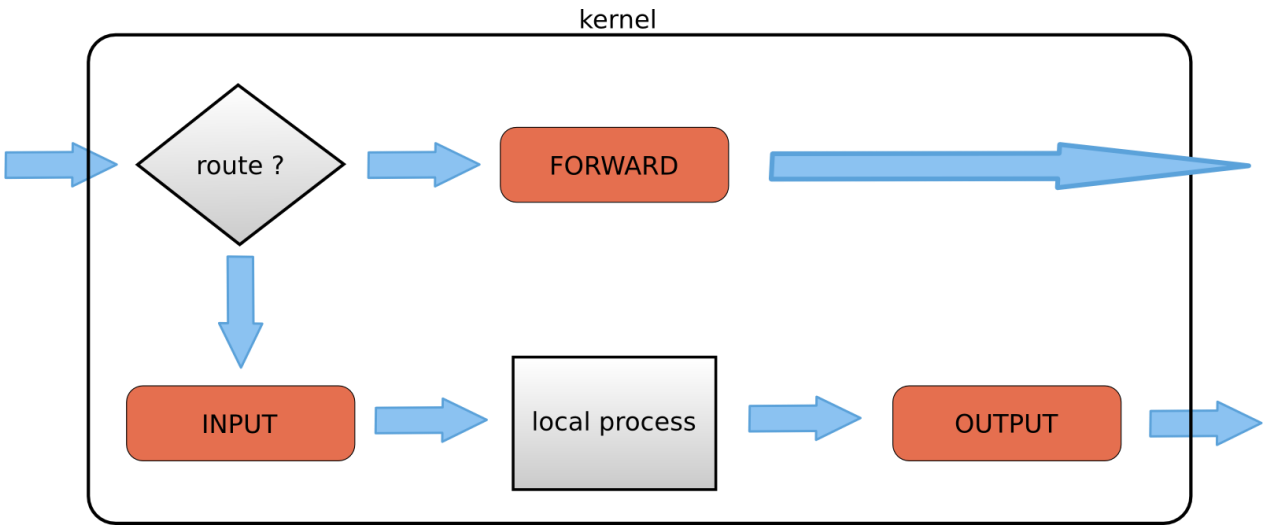


Рисунок 3.1 – Структура обробки пакетів у системі iptables

Приклад налаштування файрвола iptables для забезпечення безпечного доступу локальних користувачів до Інтернету

```
# Задання основних мережевих параметрів
LOCAL_SUBNET="172.99.0.0/16"          # Адресний простір внутрішньої мережі
EXT_IP="212.55.280.121"               # Публічна IP-адреса (надана провайдером)
INTERNAL_IP="172.99.9.2/24"           # IP-адреса інтерфейсу локальної мережі
DEFAULT_GATEWAY="212.55.280.150"      # IP шлюзу провайдера
INT_IFACE="eth0"                      # Інтерфейс внутрішньої мережі
EXT_IFACE="eth1"                      # Інтерфейс, підключений до Інтернету
# Очищення попередніх або тимчасових  правил
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
# Блокування SSH ззовні (крім локальної мережі)
iptables -A INPUT -i $EXT_IFACE -p tcp --dport 22 -j DROP
# Вимкнення доступу до портів служб Microsoft Windows (NetBIOS, SMB)
iptables -A INPUT -p tcp -m multiport --dports 135,139,445 -j DROP
iptables -A INPUT -p udp -m multiport --dports 135,137,138,139 -j DROP
iptables -A FORWARD -p tcp -m multiport --dports 135,137,138,139,445 -j DROP
iptables -A FORWARD -p udp -m multiport --dports 135,137,138,139,445 -j DROP
```

```
# Запобігання підміні адрес — фільтрація локальних IP на зовнішньому інтерфейсі
iptables -A INPUT -i $EXT_IFACE -s $LOCAL_SUBNET -j DROP
# Блокуємо підозрілий трафік з невідомих підмереж на внутрішньому інтерфейсі
iptables -A INPUT -i $INT_IFACE ! -s $LOCAL_SUBNET -j DROP
# Захист від атак типу SYN flood
iptables -A INPUT -p tcp --tcp-flags SYN,ACK SYN,ACK -m state --state NEW -j REJECT --reject-with tcp-reset
iptables -A INPUT -p tcp ! --syn -m state --state NEW -j DROP
iptables -A INPUT -i $EXT_IFACE -p tcp --tcp-flags SYN,ACK,FIN SYN \
    -m state --state NEW -m limit --limit 25/sec --limit-burst 20 -j ACCEPT
iptables -A INPUT -i $EXT_IFACE -p tcp --tcp-flags SYN,ACK,FIN SYN \
    -m state --state NEW -j DROP
# Увімкнення маршрутизації між інтерфейсами
echo 1 > /proc/sys/net/ipv4/ip_forward
# Налаштування NAT для доступу до Інтернету
iptables -t nat -A POSTROUTING -o $EXT_IFACE -s $LOCAL_SUBNET -j SNAT --to-source $EXT_IP
# Додатковий NAT для ICMP
iptables -t nat -A POSTROUTING -o $EXT_IFACE -p icmp -s $LOCAL_SUBNET -j SNAT --to-source $EXT_IP
# Повна блокада IPv6 — якщо не використовується
ip6tables -P INPUT DROP
ip6tables -P OUTPUT DROP
ip6tables -P FORWARD DROP
ip6tables -A INPUT -i $EXT_IFACE -j DROP
ip6tables -A FORWARD -j DROP
```

Цей набір правил забезпечує базовий рівень безпеки, обмежуючи зовнішній доступ до критичних служб, фільтруючи небажаний трафік і захищаючи сервер від типових атак. Подальша конфігурація буде вдосконалюватися під час експлуатації мережі, зокрема шляхом додавання нових правил у ланцюжку FORWARD, що відповідає за транзит трафіку між сегментами мережі.

3.1.2 Налаштування FTP-сервера для локальної мережі

Для обміну файлами всередині локальної мережі доцільно використовувати протокол передачі файлів – FTP. Його особливістю є застосування двох окремих TCP-з'єднань:

1. Керуюче з'єднання - ініціюється клієнтом для передачі команд до сервера. Зазвичай відбувається з'єднання до порту 2121 (альтернатива стандартному 21 порту).

2. З'єднання даних - створюється окремо для кожної сесії передачі файлів.

У якості FTP-сервера рекомендовано використовувати ProFTPD, який вирізняється стабільністю, широкими можливостями конфігурації та підтримкою таких інтеграцій, як MySQL, LDAP тощо. Його встановлення передбачає компіляцію з вихідного коду. Для цього виконуємо:

```
./configure --prefix=/opt/proftpd
make
make install
make distclean
```

При потребі можна додати модулі командою:

```
make --with-modules=mod_tls:mod_sql
```

Запуск демона можливий двома шляхами:

1. Через init-скрипт:

Перейменовуємо /opt/proftpd/etc/rc.d/proftpd.sh.sample у proftpd.sh;

chmod +x /opt/proftpd/etc/rc.d/proftpd.sh

Видаємо дозвіл на виконання:

2. Із запуском через xinetd:

Редагуємо файл /etc/xinetd.d/ftp:

```
service ftp-alt
{
    socket_type = stream
    protocol = tcp
    wait = no
    user = root
    server = /opt/proftpd/sbin/proftpd
    server_args = -n
    disable = no
    port = 2121
}
```

Перезапускаємо службу:

systemctl restart xinetd.

Далі наведемо базову конфігурація ProFTPD

Створимо конфігураційний файл:

cp /opt/proftpd/etc/proftpd.conf.sample /opt/proftpd/etc/proftpd.conf

vi /opt/proftpd/etc/proftpd.conf

Основні параметри налаштування:

```
ServerName          "Локальний FTP"
ServerType          standalone
DefaultServer       on
Port                2121
Umask               027
User                ftpuser
```

```
Group           ftpgroup
MaxInstances    25
UseReverseDNS   off
IdentLookups    off
DisplayLogin    /etc/ftp_welcome.msg
AccessGrantMsg  "Доступ дозволено"
AccessDenyMsg   "Доступ заборонено"
TimeoutIdle     300
TimeoutLogin    120
TimeoutNoTransfer 300
TimeoutStalled  600
```

Для безпеки можна дозволити вхід root-користувачу лише з локальної мережі. У файлі `/etc/ftpusers` дозволяємо логін root:

```
RootLogin on
```

Також налаштовується обмеження доступу за IP:

```
<Limit LOGIN>
  Allow from 192.168.1.0/24
  DenyAll
</Limit>
```

Задамо параметри анонімного доступу:

```
<Anonymous /srv/ftp/public>
  User          ftp
  Group         nogroup
  UserAlias     anonymous ftp
  MaxClients    15 "Забагато підключень"
  <Limit WRITE>
    DenyAll
  </Limit>
```

</Anonymous>

Після цього варто виконати створення системних ресурсів:

touch /var/log/proftpd/proftpd.log

touch /var/log/proftpd/proftpd.errors

mkdir -p /run/proftpd

touch /run/proftpd/proftpd.scoreboard

Також можна змінити повідомлення у привітання:

echo "**Вітаємо** у локальному FTP-сервері компанії **BST**!" > /etc/ftp_welcome.msg

Для ефективного адміністрування FTP-сервера необхідно регулярно контролювати його стан, аналізувати активність користувачів і своєчасно виявляти помилки. Нижче наведено основні команди, що дозволяють виконувати ці завдання.

Команди для перегляду стану активних з'єднань:

ftpwho — виводить перелік поточних користувачів, підключених до FTP-сервера, із зазначенням IP-адрес та дій, які вони виконують.

ftpcount — показує загальну кількість активних підключень, а також окремо анонімні та авторизовані сесії.

ftptop — інтерактивна утиліта, що в режимі реального часу демонструє інформацію про користувачів, які виконують завантаження або вивантаження даних, включаючи обсяг переданих файлів, IP-адресу клієнта та швидкість з'єднання.

Команди для перегляду логів сервера:

tail -f /var/log/proftpd/proftpd.log — дозволяє спостерігати в реальному часі за подіями FTP-сервера: вхід у систему, команди, передача файлів тощо.

tail -f /var/log/proftpd/proftpd.errors — відображає поточні помилки, включаючи невдалі спроби підключення, проблеми з авторизацією або конфігурацією.

Додаткові корисні команди:

netstat -tnp | grep proftpd — дозволяє переглянути всі встановлені TCP-з’єднання, пов’язані з процесом FTP-сервера, включаючи зовнішні IP-адреси та порти.

lsof -i :2121 — перевіряє, чи відкритий порт (наприклад, 2121) та який процес його використовує.

systemctl status proftpd — надає інформацію про поточний стан служби ProFTPD: активність, наявні збої, історію запуску.

Використання цих утиліт значно полегшує обслуговування FTP-сервера, дозволяє швидко реагувати на несправності, контролювати навантаження, а також виявляти потенційні загрози для інформаційної безпеки мережі.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування бездротових маршрутизаторів

Маршрутизатор (router) — це апаратне або програмне рішення, призначене для об'єднання кількох мереж і реалізації процесу передачі даних між ними. Виходячи з наявної інформації про структуру мережі, підключені пристрої та задані правила адміністратором, маршрутизатор визначає оптимальний шлях для пересилання пакетів на відповідний інтерфейс. Пристрій функціонує на третьому (мережевому) рівні еталонної моделі OSI.

Під час налаштування бездротових маршрутизаторів у першу чергу потрібно конфігурувати інтерфейс WAN, через який виконується підключення до внутрішньої (локальної) мережі. Приклад такої схеми зображено на рисунку 3.2. Для запобігання конфліктам під час бездротової передачі кожен маршрутизатор має працювати на окремому радіоканалі, з відступом у п’ять позицій від сусідніх пристроїв. Це дозволяє зменшити рівень взаємних перешкод та уникнути перевантаження ефіру, що може виникати при роботі кількох точок доступу на однакових або близьких частотах.

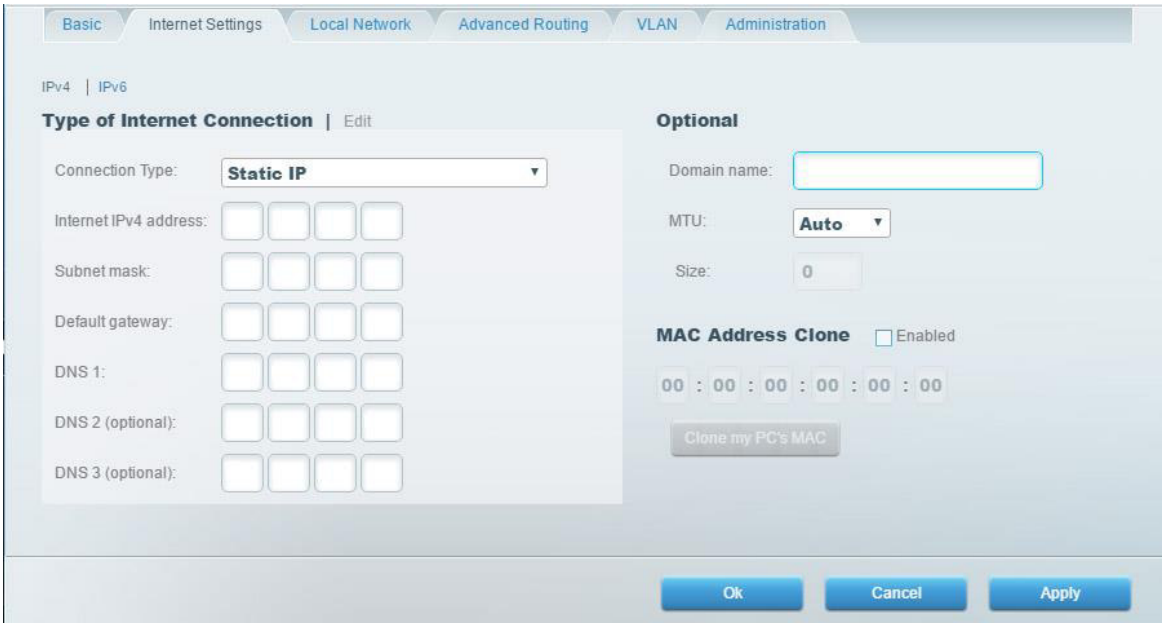


Рисунок 3.2 – Конфігурація WAN-інтерфейсу

Під час налаштування маршрутизатора передбачено автоматичну видачу IP-адрес клієнтським пристроям після підключення до мережі. Для цього використовується вбудований DHCP-сервер. На рисунку 3.3 наведено приклад конфігурації DHCP-функціоналу на маршрутизаторі R1, який забезпечує динамічне призначення мережевих параметрів підключеним користувачам.

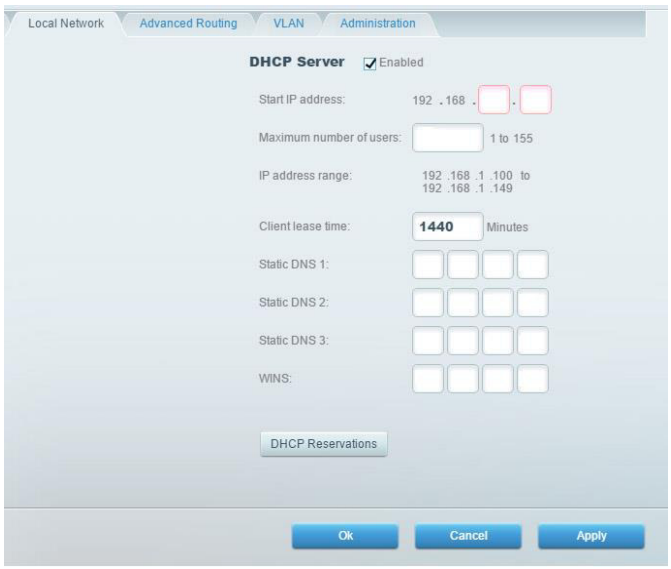


Рисунок 3.3 – Взірець налаштування DHCP-сервера R1

На заключному етапі налаштування слід обрати протокол шифрування для захисту трафіку в радіоканалі та встановити відповідний ключ безпеки, що ілюструється на рисунку 3.4.

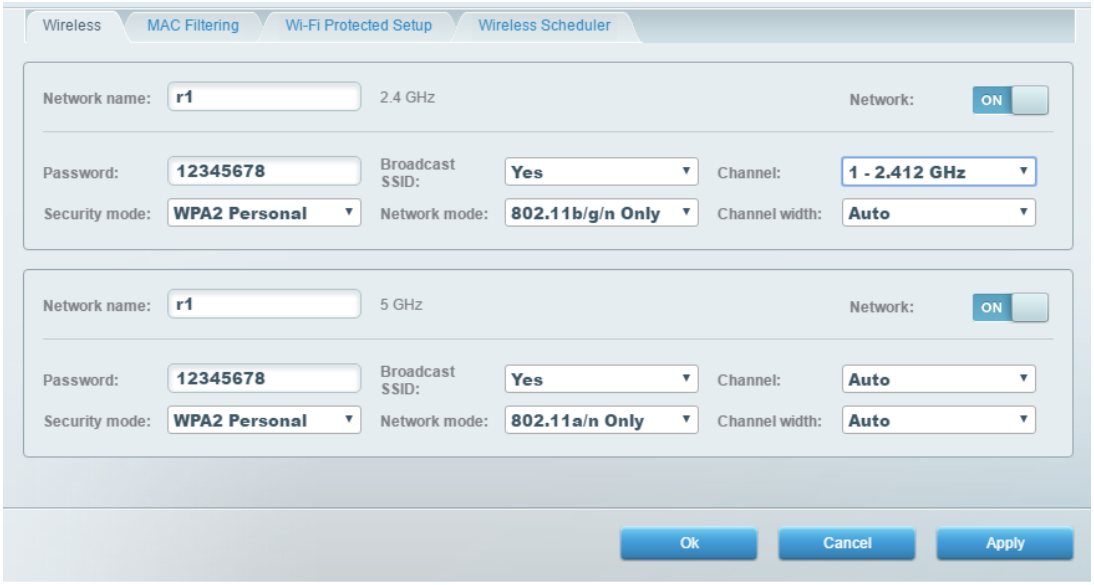


Рисунок 3.4 – Параметри безпеки безпровідного сегменту

Маршрутизатор R2 налаштовується аналогічним чином, з урахуванням індивідуальних особливостей мережевого середовища. Для значного підвищення рівня безпеки передачі даних у бездротовому сегменті локальної мережі рекомендується використовувати MAC-фільтрацію, яка дозволяє обмежити доступ до мережі лише для попередньо визначених пристроїв за їх унікальними MAC-адресами. Впровадження MAC-списків доступу знижує ризик несанкціонованого підключення сторонніх пристроїв та мінімізує можливості атак типу "людина посередині".

Крім того, поряд із MAC-фільтрацією, слід також застосовувати сучасні методи шифрування бездротового трафіку, такі як WPA3, що забезпечує надійний захист інформації від перехоплення та розшифровки. Регулярне оновлення прошивки маршрутизаторів і зміна паролів адміністративного доступу також є важливими кроками для підтримки безпеки мережі на високому рівні.

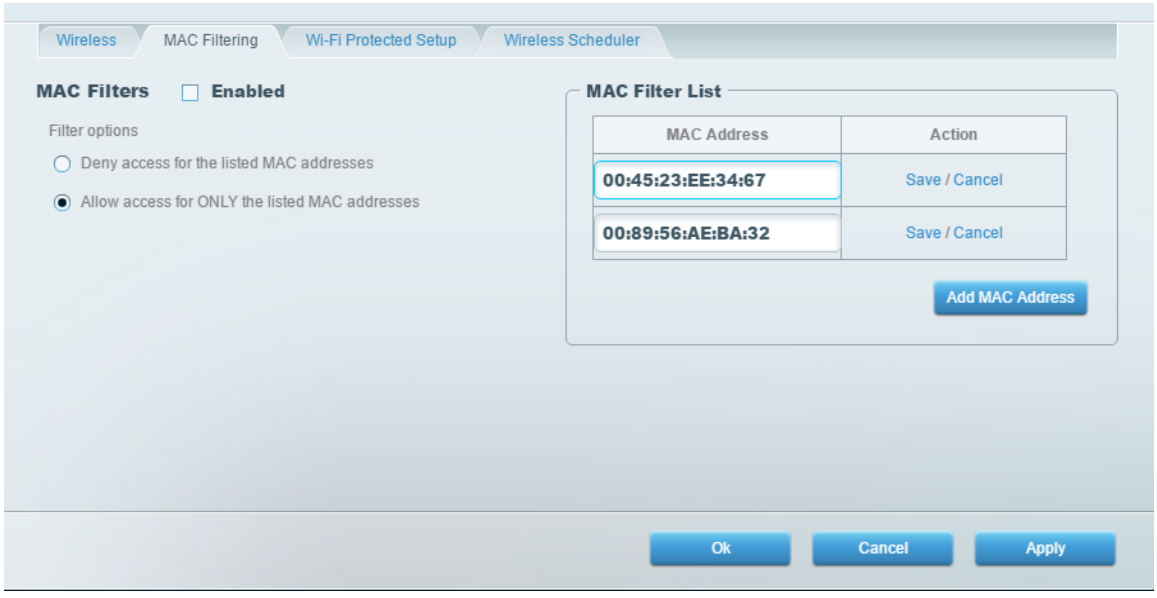


Рисунок 3.5 – Налаштування списків контролю доступу клієнтів до маршрутизатора за MAC-адресами

Приклад налаштування MAC-фільтрації та інших параметрів безпеки наведено на рисунку 3.5. Ця конфігурація є ефективним заходом для запобігання несанкціонованому доступу і підтримки стабільної роботи бездротової мережі.

Також важливо обов’язково замінити стандартний пароль для доступу до веб-інтерфейсу управління маршрутизатором. Це дозволить запобігти несанкціонованому входу зловмисників і забезпечить додатковий рівень захисту пристрою. Використання складного, унікального пароля є однією з базових рекомендацій з безпеки мережевого обладнання.

3.2.2 Інструкції з налаштування центрального комутатора

Отже, здійснимо налаштування віртуальних локальних мереж (VLAN) на комутаторі SW4.

Процедуру конфігурування починаємо з переходу в режим глобального налаштування за допомогою команди:

SW4# configure terminal

SW4(config)#

Далі переходимо до створення необхідних віртуальних сегментів мережі:

SW4(config)# vlan 11

SW4(config-vlan)# name Адміністрація

SW4(config-vlan)# exit

Аналогічні команди використовуються для створення інших VLAN згідно з проєктною таблицею IP-адрес. Після завершення створення VLAN виходимо до глобального режиму:

SW4(config-vlan)# exit

SW4(config)#

Налаштування портів для клієнтів та міжмережевого зв’язку

Порти, що підключені до користувацьких пристроїв (ПК, сервери), мають бути переведені в режим access. Наприклад:

SW4(config)# interface range gigabitEthernet 1/3 - 1/4

SW4(config-if-range)# SWitchport mode access

SW4(config-if-range)# SWitchport access vlan 19

SW4(config-if-range)# exit

У режимі access порт приймає немічені кадри тільки з однієї VLAN — у цьому випадку VLAN 19.

Порти, що з'єднують комутатори між собою, налаштовуються в режим trunk, що дозволяє передавати мічені пакети з різних VLAN

SW4(config)# interface gigabitEthernet 1/1

SW4(config-if)# SWitchport mode trunk

SW4(config-if)# SWitchport trunk allowed vlan 11-24

SW4(config-if)# exit

trunk забезпечує передавання трафіку з усіх VLAN між комутаторами через один фізичний порт.

Призначення IP-адрес VLAN-інтерфейсам (SVI)

Кожній VLAN потрібно призначити відповідний IP-адрес для організації маршрутизації між сегментами. Наприклад:

SW4(config)# interface vlan 11

SW4(config-if)# ip address 172.99.1.100 255.255.255.0

SW4(config-if)# no shutdown

SW4(config-if)# exit

Ці ж дії повторюються для інших VLAN за взірцем :

SW4(config)# interface vlan 12

SW4(config-if)# ip address 172.99.2.100 255.255.255.0

SW4(config-if)# no shutdown

SW4(config-if)# exit

...

SW4(config)# interface vlan 24

SW4(config-if)# ip address 172.99.14.100 255.255.255.0

SW4(config-if)# no shutdown

SW4(config-if)# exit

Додавання маршруту за замовчуванням

Для того, щоб всі підмережі мали вихід в Інтернет через центральний шлюз, налаштовуємо статичний маршрут:

SW4(config)# ip route 0.0.0.0 0.0.0.0 172.99.9.1

Ця команда створює маршрут до всіх невідомих підмереж через шлюз 172.99.9.1.

Збереження конфігурації

Після завершення всіх налаштувань, конфігурацію потрібно зберегти до енергонезалежної пам’яті пристрою:

SW4# copy running-config startup-config

Destination filename [startup-config]?

Press Enter

Це гарантує, що після перезавантаження комутатор завантажиться з актуальними налаштуваннями.

Цей процес є обов’язковим для організації логічного поділу мережі, забезпечення безпеки, пріоритезації трафіку та спрощення адміністрування. Налаштування VLAN також створює передумови для ефективної маршрутизації між сегментами мережі у подальших етапах реалізації інфраструктури.

3.2.3 Інструкції з налаштування комутаторів робочих груп

Комутатори серії Allied Telesyn AT-GS950 підтримують зручний інтерфейс керування через браузер, що дозволяє здійснити налаштування без

використання командного рядка. Для конфігурування віртуальних локальних мереж (VLAN) і IP-параметрів. Доступ до веб-інтерфейсу:

- Під’єднайте комп’ютер до одного з портів комутатора.
- Призначте ПК IP-адресу в підмережі за замовчуванням (наприклад,192.168.1.2, якщо IP пристрою за замовчуванням — 192.168.1.1).
- Відкрийте веб-браузер і введіть IP-адресу комутатора: http://192.168.1.1
- Авторизуйтесь (стандартний логін/пароль: manager / friend, якщо не змінено).

На кожному з комутаторів, встановлених у робочих групах, буде виконане налаштування віртуальних локальних мереж (VLAN) відповідно до інформації, наведеної в таблиці 2.2 «Конфігурація VLAN». Це дозволить логічно розмежувати мережевий трафік між різними структурними підрозділами підприємства та забезпечити відповідний рівень ізоляції та безпеки.

На рисунку 3.6 представлено приклад встановлення типу VLAN на одному з комутаторів робочої групи за допомогою веб-інтерфейсу керування. У даному прикладі вказується тип доступу до VLAN для певних портів комутатора — наприклад, у режимі Untagged для кінцевих пристроїв або Tagged для міжкомутаційного з’єднання (trunk-лінків).

Рисунок 3.6 – Приклад вибору портів

Таке налаштування забезпечує коректну маршрутизацію трафіку у межах визначених віртуальних підмереж та дає змогу головному комутатору ідентифікувати джерело кожного пакету.

Приклад створення VLAN, а також налаштування відповідних параметрів портів комутатора за допомогою веб-інтерфейсу наведено на рисунку 3.7.

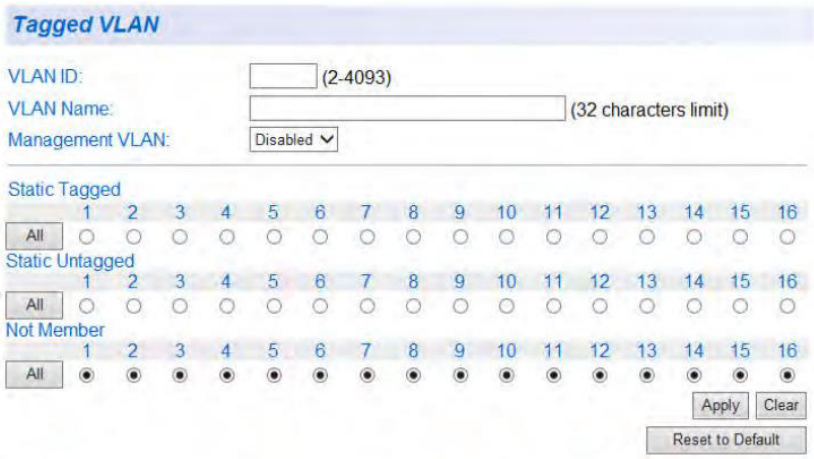


Рисунок 3.7 – Параметри віртуальних мереж

На кожному з комутаторів робочих груп виконується створення необхідних віртуальних локальних мереж (VLAN) відповідно до розробленої схеми IP-адресації.

Після цього для кожного порту встановлюється приналежність до конкретної VLAN та визначається тип порту - Tagged або Untagged, залежно від його функціонального призначення.

Режим Not Member у конфігурації портів означає, що відповідний порт не входить до складу вибраної VLAN і не передає трафік цієї віртуальної мережі.

3.3 Інструкція з використання тестових наборів та тестових програм

У цьому розділі розглянуто процес виявлення та усунення проблем, що можуть виникати під час функціонування комп’ютерної мережі, з використанням вбудованих засобів операційної системи Windows.

Перш за все, діагностика починається з фізичного рівня моделі OSI, який охоплює середовище передавання даних. Оскільки на цьому рівні використовуються кабелі, роз'єми та інші механічні компоненти, більшість збоїв пов'язана саме з ними. Відсутність фізичного з'єднання між вузлами мережі (наприклад, між хостами і комутатором). Така проблема легко виявляється за світлодіодними індикаторами на мережевому обладнанні. Причиною може бути неправильне підключення або пошкодження кабелю. Якщо в інтерфейсі Windows значок мережі має червону позначку, це вказує на відсутність фізичного контакту.

Тестування є завершальним етапом проєктування мережі. Воно охоплює перевірку кабельних сегментів, бездротових з'єднань, конфігурації мережевих пристроїв та серверів. Для оцінки параметрів кабельної системи буде використано тестер-аналізатор Ethernet/Gigabit Ethernet МАКС-ЕМ.

Його основні функції:

- одночасне тестування двох Ethernet/Gigabit Ethernet інтерфейсів; генерація та аналіз трафіку на канальному, мережевому та вищих рівнях;

- збір і відображення статистики по переданому та отриманому трафіку на фізичному, канальному та мережевому рівнях;

- тестування відповідно до рекомендацій RFC-2544;

- вимірювання пропускної здатності, затримки (latency), втрат пакетів при навантаженні, максимальної пропускної здатності (back-to-back);

- перевірка зв’язності каналів і маршрутів на рівні IP;

- організація шлейфів на різних рівнях моделі OSI зі зміною або збереженням полів MAC, IP;

- діагностика мідного кабелю (згасання, довжина до розриву, перехресні перешкоди);

- вимірювання варіацій затримки (PDV);

- аналіз помилкових пакетів (IPER);

- оцінка бітових помилок (BER).

У разі впливу зовнішніх джерел електромагнітного випромінювання сигнал, що надходить до приймача, може бути спотворений або зовсім втрачений. Таку проблему складно діагностувати, оскільки потрібно виявити джерело завад, однак її усунення зазвичай не є складним.

На мережевому рівні OSI здійснюється маршрутизація на основі IP-адрес. Типові проблеми включають:

Неправильна конфігурація TCP/IP-стека. Це може спричинити відсутність доступу до Інтернету або до внутрішніх вузлів мережі. Найчастіше це результат помилок у значеннях IP-адреси, маски підмережі чи шлюзу. Швидка перевірка здійснюється за допомогою команди: ipconfig /all.

Неможливість зв'язку з локальними чи віддаленими вузлами. Використовується утиліта ping, яка надсилає пакети-запити й очікує відповіді. У разі проблеми виводиться повідомлення "Request timed out". Формат команди:

ping [-параметри] ім’я_вузла

Нестабільний зв'язок з певними вузлами в Інтернеті. Для виявлення проблеми застосовується утиліта tracert, яка перевіряє всі проміжні маршрутизатори між відправником і одержувачем. Вона надсилає три пакети на кожен вузол і вимірює час відповіді. Формат команди: tracert [-d] ім’я_вузла

На транспортному рівні функціонують протоколи TCP і UDP. Для діагностики проблем на цьому рівні застосовується команда netstat.

Можливі несправності:

Некоректна робота мережевих протоколів. Для аналізу використовується команда netstat -s -p icmp, netstat -s -p udp, netstat -s -p tcp.

Діяльність шкідливих програм (віруси, трояни), що створюють зайве навантаження на канал. Перевірити всі активні мережеві процеси можна командою: netstat -a -b -o.

3.4 Інструкції по налаштуванню засобів захисту мережі

У середовищі операційної системи Linux функціонування файєрволу забезпечується за допомогою утиліти iptables (для протоколу IPv4) та ip6tables (для протоколу IPv6). У даному розділі буде розглянуто основні типові сценарії застосування iptables для захисту локальної обчислювальної мережі.

Основні типові сценарії використання iptables охоплюють комплексний контроль доступу та фільтрацію мережевого трафіку на різних рівнях. До ключових завдань належать:

1. Фільтрація вхідного та вихідного трафіку — за допомогою правил можна дозволити або заборонити доступ до певних портів, IP-адрес або протоколів, що забезпечує базовий рівень безпеки.

2. Контроль з'єднань за станом (Stateful Firewall) — iptables відстежує стан мережевих з'єднань, що дозволяє пропускати лише пакети, які належать до встановлених чи довірених сесій, що значно підвищує ефективність захисту від атак.

3. NAT (Network Address Translation) — реалізація трансляції мережевих адрес, що дозволяє внутрішнім пристроям мережі виходити в інтернет під спільною зовнішньою IP-адресою, а також перенаправляти порти для доступу до локальних сервісів.

4. Маршрутизація та модифікація пакетів — зміна заголовків пакетів для корекції маршрутизації або застосування спеціальних правил обробки (наприклад, зміна TTL або пріоритетів).

5. Логування мережевого трафіку — збір інформації про проходження пакетів через брандмауер для подальшого аналізу безпекових подій та пошуку аномалій.

На їх основі розроблено конфігураційний скрипт, приклад якого наведено у додатку Г.

Структуру таблиць, що використовуються під час налаштування iptables, наведено на рисунку 3.8.

Рисунок 3.8 – Структура таблиць iptables

3.5 Інструкції щодо експлуатації та моніторингу мережі

Моніторинг у загальному розумінні - це безперервне спостереження за станом і параметрами об’єктів, процесів чи явищ з метою їх оцінки та аналізу. Наприклад, можна спостерігати за погодними умовами протягом певного часу для визначення тенденцій чи прогнозів.

У контексті комп’ютерних мереж моніторинг передбачає систематичний збір та аналіз службових даних, що дозволяють оцінити внутрішні процеси в мережі, виявити потенційні проблеми або визначити продуктивність роботи. Зібрана інформація часто піддається статистичній

обробці, що допомагає прогнозувати подальший розвиток подій і приймати обґрунтовані рішення для підтримки стабільності мережі.

Серед популярних інструментів для мережевого моніторингу є базові утиліти, такі як команди ping та ipconfig, які дозволяють швидко перевірити доступність вузлів та налаштування мережі. Для більш складного контролю застосовуються сервери протоколу SNMP, системи на кшталт Zabbix та інші відкриті рішення. Повноцінним комплексним інструментом є мережевий моніторинг від компанії Cisco - Works NMS, який забезпечує глибокий аналіз і управління мережею.

Вибір конкретних технологій і програмних засобів моніторингу значною мірою визначається вимогами та масштабом мережі, а також специфічними потребами користувачів чи організації.

3.6 Моделювання роботи локальної мережі

Для моделювання роботи локальної мережі було використано програмний продукт Cisco Packet Tracer, який розроблений компанією Cisco Systems. Цей програмний пакет є універсальним інструментом, що поєднує в собі функції навчального симулятора та потужного середовища для проектування та тестування мереж різного масштабу.

Cisco Packet Tracer дає змогу не лише побудувати логічну топологію мережі, але й симулювати її реальну роботу, імітуючи обмін даними між різними мережевими пристроями — комутаторами, маршрутизаторами, серверами та кінцевими користувачами. Це допомагає перевірити правильність налаштувань, протестувати маршрутизацію, взаємодію VLAN, а також відпрацювати сценарії усунення несправностей.

Крім того, платформа підтримує гнучке редагування конфігурацій і зміни параметрів у режимі реального часу, що сприяє глибокому аналізу впливу різних змін на стабільність і продуктивність мережі. Можливість

візуалізації трафіку й показників роботи пристроїв надає інженерам зручний спосіб контролю та оптимізації побудованої мережі.

На рисунку 3.9 представлено логічну топологію, яка відтворює структуру спроектованої локальної мережі, включаючи основні вузли та канали зв’язку між ними.

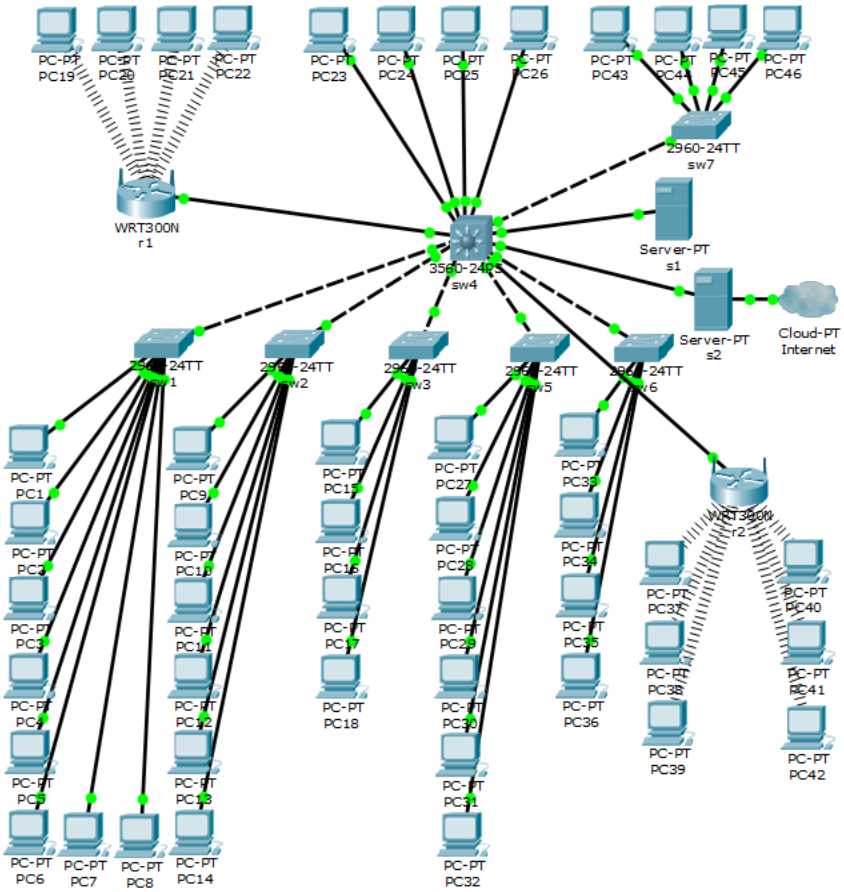


Рисунок 3.9 – Модель мережі компанії BST

Після завершення побудови локальної мережі наступним етапом є налаштування її основних компонентів. Конфігурування мережевих пристроїв виконується на основі даних, наведених у таблиці IP-адрес. Для прикладу наведено результат виконання команди ipconfig /all на робочій станції PC1, що ілюструє поточні параметри мережевого інтерфейсу цієї станції. На рисунку 3.10 показано вивід команди ipconfig /all на робочій станції PC1:

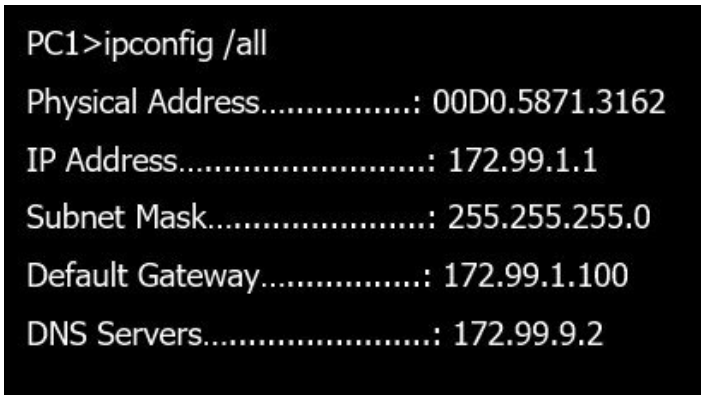


Рисунок 3.10 – Налаштування PC1

Перевіримо проходження пакетів між вузлами PC1 та S1 за допомогою виконання команди:

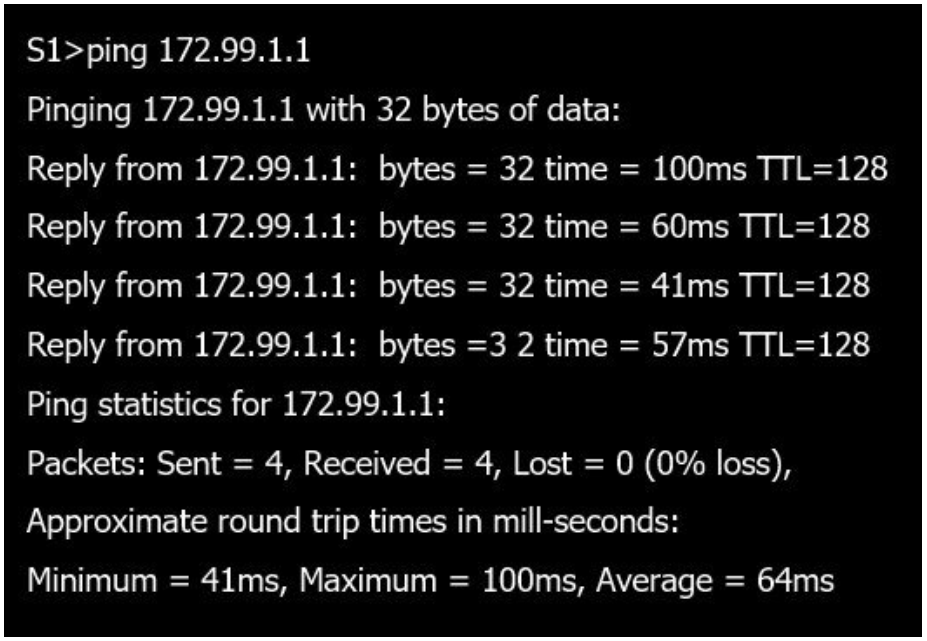


Рисунок 3.11 – Результати «пінгування»

Наведений вище результат виконання команди ping підтверджує коректну роботу протоколу ICMP у процесі перевірки зв’язку між окремими вузлами мережі. Це свідчить про те, що реалізоване моделювання відображає реальні умови функціонування мережі. Отже, зроблені налаштування та прийняті рішення є правильними та ефективними, що гарантує стабільну і

надійну роботу локальної мережі відповідно до вимог, визначених замовником. Таким чином, модель мережі готова до подальшої експлуатації та впровадження в реальному середовищі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для компанії «BST» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР дані витрат часу по окремих операціях технологічного процесу зводяться у таблицю 4.1.

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

№ п/п	Назва стадії	Виконавець	Середній час виконання операції, год.
1	Постановка задачі та збір інформації про об'єкт	Керівник проекту	9
2	Розробка проекту	Інженер	10
3	Затвердження проекту	Керівник проекту	1
4	Монтаж мережі	Технік	30
5	Налагодження мережі та створення технічної документації	Інженер	20
Разом			70

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для компанії «BST» складає 70 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Оплата праці - грошовий вираз вартості і ціни робочої сили, який виступає у формі будь-якого заробітку, виплаченого керівником підприємства найманому працівникові за виконану роботу.

Заробітна плата працівника залежить від кінцевих результатів його роботи, регулюється податками і максимальними розмірами не обмежується.

Основна заробітна плата розраховується за формулою:

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

де $Т_с$ – тарифна ставка, грн.;

$К_г$ – кількість відпрацьованих годин.

Рекомендовані тарифні ставки: керівник проекту – 240 грн./год., інженер – 180 грн./год., технік – 120 грн./год.

Отже, основна заробітна плата для:

1. Керівник проекту - $З_{осн1} = 10 \cdot 240 = 2400$ грн.
2. Інженер - $З_{осн2} = 30 \cdot 180 = 5400$ грн.
3. Технік - $З_{осн3} = 30 \cdot 120 = 3600$ грн.

Сумарна основна заробітна плата становить:

$$З_{осн} = 2400 + 5400 + 3600 = 11400 \ \ грн.$$

Додаткова заробітна плата становить 10 – 15 % від суми основної заробітної плати та обчислюється за формулою 4.2.

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

1. Керівник проекту - $З_{дод1}$= 2400 · 0,12 = 288 грн.
2. Інженер - $З_{дод2}$ = 5400 · 0,12 = 648 грн.
3. Технік - $З_{дод3}$ = 3600 · 0,12 = 432 грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 288+648+432= 1368 \text{ грн.}$$

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

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

$$В_{о.п}=11400 +1368 = 12768 \text{ грн}$$

Необхідно визначити відрахування на соціальні заходи:

1. Фонд страхування на випадок безробіття – 1,6 %;
2. Фонд по тимчасовій втраті працездатності – 1,4 %;
3. Пенсійний фонд – 33,2 %;
4. Внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахувань становить 37,6 %.

Отже, сума відрахувань на соціальні заходи буде становити:

$$В_{с.з.}= ФОП \cdot 0,376, \quad (4.4)$$

де ФОП – фонд оплати праці, грн.

$$В_{с.з.}= 12768 \cdot 0,376 = 4800,77 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія прац.	Основна заробітна плата, грн.			Додатк. зароб. плата, грн.	Нарахув. на ФОП, грн.	Всього витрати на оплату праці, грн.
		Тариф. ставка, грн.	К-сть відпр. год.	Факт. нарах. з/пл., грн.			
1	Керівник проекту	240	10	2400	288	-	-
2	Інженер	180	30	5400	648	-	-
3	Технік	120	30	3600	432	-	-
Разом				11400	1368	4800,77	17568,77

Отже, загальні витрати на оплату праці становлять 17568,77 грн.

4.3 Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни (формула 4.5):

$$M_{Bi} = q_i \cdot p_i \qquad (4.5)$$

де q_i – кількість витраченого матеріалу i-го виду;

p_i – ціна матеріалу i-го виду.

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$З_{м.в.} = \sum M_{Bi} \qquad (4.6)$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Найменування обладнання	Од. вим.	Кількість	Орієнтовна вартість, грн.	Загальна вартість, грн.
1	2	3	4	5	6
1	Кабель типу вита пара U/UTP категорії 6 (305 м)	шт.	2	5500	11000
2	Мережева розетка типу UTP Cat.6	шт.	50	100	5000
3	Патчкорд UTP Cat.6 (1 метр)	шт.	70	17	1190
4	Патчпанель на 24 порти (Cat.6, тип UTP)	шт.	1	1680	1680
5	Кабель-канал (загальна довжина)	м.	130	70	9100
6	Серверна монтажна шафа 24U, 19"	шт.	1	6622	6622
7	Магістральний комутатор Edge-Core ECS4610-26T/L3	шт.	1	22458	22458
8	Комутатор для сегментів – Allied Telesis AT-GS950/8	шт.	5	2900	14500
9	Комутатор Allied Telesyn – AT-GS950/16	шт.	1	3200	3200
10	Сервер для шлюзу – Dell PowerEdge R530	шт.	1	30000	30000
11	Сервер для зберігання даних – Dell PowerEdge R530	шт.	1	34000	34000

Продовження таблиці 4.3

1	2	3	4	5	6
12	Блок безперебійно живлення (ДБЖ) APC серії Smart-UPS 2 кВт	шт.	1	15000	15000
13	Бездротовий маршрутизатор Linksys WRT-1900AC	шт.	2	5200	10400
14	Мережевий фільтр-подовжувач, довжина 5 м, 5 розеток	шт.	2	400	800

Отже, загальна сума матеріальних витрат складає 169 950 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 39 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії – 7 грн.

Тому витрати на електроенергію будуть становити:

$$З_е = 39*0,5*7 = 136,5 \text{ грн.}$$

4.5 Визначення транспортних затрат

Транспортні витрати слід прогнозувати у розмірі 8 – 10 % від загальної суми матеріальних затрат. Транспортні витрати розраховуються за формулою 4.8.

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

де $T_в$ – транспортні витрати.

Отже, транспортні витрати будуть становити:

$$T_в = 169\,950 \cdot 0,08 = 13596\ грн.$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{Б_В \cdot Н_А}{150\,\%} \cdot T, \quad (4.9)$$

де A – амортизаційні відрахування за звітний період, грн.

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

$Н_А$ – норма амортизації, %;

T – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 39 год., балансова вартість ПК – 28000 грн., тому:

$$A = \frac{28000 \cdot 0,05}{150} \cdot 39 = 364\ грн.$$

4.7 Обчислення накладних витрат

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

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 20 – 60 % від суми основної та додаткової заробітної плати працівників, обчислюються за формулою 4.10.

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

де, $H_в$ – накладні витрати.

$$H_в = 17568,77 \cdot 0,3 = 5270,63 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

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

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 - Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці	12768	6,17
Відрахування на соціальні заходи	4800,77	2,32
Матеріальні витрати	169950	82,15
Витрати на електроенергію	136,5	0,07

Продовження таблиці 4.4

1	2	3
Транспортні витрати	13596	6,57
Амортизаційні відрахування	364	0,18
Накладні витрати	5270,63	2,55
Собівартість	**206885,9**	**100,00**

Собівартість (C_B) НДР розрахуємо за формулою 4.11:

$$C_{в} = B_{о.п.} + B_{с.з.} + З_{м.в.} + З_{в} + Т_{в} + А + Н_{в} \quad (4.11)$$

Отже, собівартість дорівнює: $C_{в}$=206885,9 *грн.*

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$Ц = C_{в} \cdot (1+Р_{рен}) \cdot (1+ПДВ), \quad (4.12)$$

де $C_{в}$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності, 25 %

ПДВ – ставка податку на додану вартість, 20 %.

$$Ц = 206885,9 \cdot (1+0,25) \cdot (1+0,2) = 310328,85 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва - категорія, яка характеризує результативність виробництва. Вона свідчить не лише про приріст обсягів виробництва, а й про те, якими витратами ресурсів досягається цей приріст, тобто свідчить про якість економічного зростання.

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 310328,85 – 206885,9 = 103442,95 \text{ грн.}$$

Економічна ефективність ($E_р$) полягає у відношенні результату виробництва до затрачених ресурсів і розраховується за формулою 4.14.

$$E_р = П / С_в, \quad (4.14)$$

де $П$ – прибуток;

$С_в$ – собівартість.

$$E_р = 103442,95 / 206885,9 = 0,5$$

Поряд із економічною ефективністю розраховують (формула 4.15) термін окупності капітальних вкладень ($T_р$):

$$T_р = 1 / E_р \quad (4.15)$$

Допустимим вважається термін окупності до 5 років. В даному випадку $T_р=1/0,5=2$.

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Значення
1.	Собівартість, грн.	206885,9 -грн.
2.	Плановий прибуток, грн.	103442,95 грн.
3.	Ціна, грн.	310328,85 грн.
4.	Економічна ефективність	0,5
5.	Термін окупності, рік	2

Загальна вартість розробленої комп’ютерної мережі для компанії «BST» становить 310328,85 грн.

Зважаючи на високі показники економічної ефективності - 0,5, кошти, вкладені в проведення проектних робіт окупляться за 2 роки.

5. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

Метою даного розділу є забезпечення належного рівня знань щодо організації безпечних умов праці, охорони здоров’я та захисту працівників під час виконання професійної діяльності. У ньому розглядаються основні принципи охорони праці, заходи щодо зниження професійних ризиків, дотримання нормативно-правових вимог та організація безпечного середовища на робочому місці.

Актуальність теми обумовлена необхідністю створення комфортних і безпечних умов для працівників, збереження їх життя, здоров’я та працездатності, що є важливою складовою ефективного функціонування будь-якого підприємства.

5.1 Система організаційно-технічних заходів з пожежної безпеки в компанії “BST”

Система організаційно-технічних заходів з пожежної безпеки в компанії – це комплекс взаємопов'язаних заходів, спрямованих на запобігання пожежам та забезпечення безпеки людей і майна у разі їх виникнення. Вона включає в себе як організаційні, так і технічні заходи, які розробляються та впроваджуються з урахуванням специфіки діяльності компанії та вимог законодавства [10].

Забезпечення пожежної безпеки з організаційно-технічної точки зору має включати розробку інструктивних матеріалів, регламентів і норм виконання технологічних процесів, правил поводження з пожежовибухонебезпечними речовинами й матеріалами і т. ін [10].

Велике значення щодо забезпечення пожежної безпеки має організація навчання, інструктажу й допуску до роботи персоналу, який обслуговує пожежовибухонебезпечні технологічні процеси.

Забезпечення пожежної безпеки неможливе без належного контролю й нагляду за дотриманням норм технологічного режиму, правил і норм техніки безпеки, виробничої санітарії та пожежної безпеки [10].

Кожний об'єкт господарювання, який використовує, переробляє або зберігає вибухонебезпечні речовини й матеріали, повинен розробити заходи щодо організації протиаварійних, газорятувальних робіт та встановити порядок їх виконання в аварійних умовах, а також організувати пожежну охорону при профілактичному та оперативному обслуговуванні дільниць, цехів, підприємств.

Рівень пожежної охорони та порядок профілактичного й оперативного обслуговування об'єктів, необхідність організації підрозділів пожежної охорони та їх чисельність визначається в установленому порядку.

На виробничих об'єктах з метою забезпечення пожежної і вибухової безпеки слід контролювати параметри пожежовибухонебезпеки вихідних речовин, технологічний режим, склад атмосфери виробничих приміщень, технологічне обладнання та електрообладнання [11].

Контролювати необхідно такі пожежовибухонебезпечні параметри, як температура спалаху, межі спалахування, температурні межі спалаху для горючих і легкозаймистих рідин та ін [11].

У виробничих приміщеннях, де можливе накопичення викидів, розливання газоподібних і рідких пожежовибухонебезпечних речовин, необхідно безперервно контролювати їх вміст у повітрі [11].

Компанія «BST», що займається програмуванням та супроводом програмного забезпечення, не належить до сфер, традиційно пов'язаних із високими пожежними ризиками. Проте в сучасному офісному середовищі, обладнаному комп’ютерною технікою, серверними кімнатами та засобами зберігання важливої інформації, дотримання пожежної безпеки є необхідною умовою для непреривної та безпечної роботи підприємства. Далі детальніше опишемо необхідні заходи:

1. Організаційні заходи

1.1. Розробка внутрішніх інструкцій і регламентів. Компанія розробляє та затверджує внутрішню документацію з пожежної безпеки – положення, інструкції, правила евакуації, порядок проведення навчань. У кожному виконавчому документі обов’язково вказуються відповідальні особи (наприклад, адміністратор безпеки, керівник ІТ-відділу) із зазначенням їхніх функцій і повноважень.

1.2. Навчання і інструктаж персоналу. Для кожного співробітника передбачаються регулярні підвищувальні інструктажі з пожежної безпеки, які включають правила поведінки при виявленні пожежі. Працівники навчаються користуванню первинними засобами пожежогасіння та відпрацюванню евакуації, що сприяє зниженню панічних реакцій у разі надзвичайної ситуації.

1.3. Проведення навчань і тренувань. Офіси обладнуються планами евакуації, а персонал проходить щоквартальні тренування з евакуації та практичне використання вогнегасників. Кількість таких заходів зростає за умови розширення штату або зміни офісного планування.

1.4. Захист відповідно до нормативів. Компанія дотримується вимог ДБН і нормативних документів із пожежної безпеки при проектуванні офісних приміщень. Передбачено встановлення первинних засобів пожежогасіння (вогнегасників) у серверних кімнатах і біля пожежних виходів.

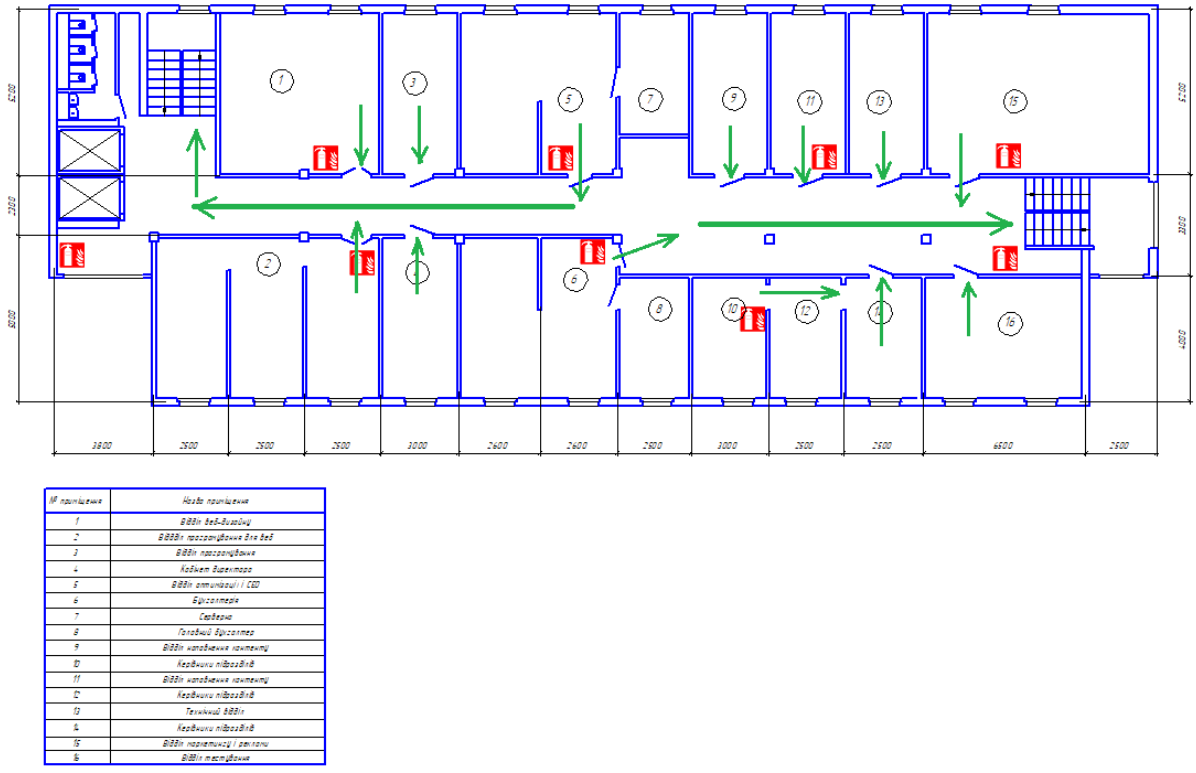
2. Технічні заходи

2.1. Обладнання первинними засобами пожежогасіння. У кожному приміщенні обладнаного електроприладами персоналу (ПК, сервери) передбачаються відповідні кількість вогнегасників – порошкових та CO_2. Вогнегасники розміщуються доступно і відповідають нормам: один на 20–25 м² або поруч із технічними комутаційними стояками.

2.2. Системи оповіщення та безпеки. В офісних приміщеннях встановлюється акустична система оповіщення або сповіщувачі, з'єднані з

мобільними засобами керівництва. Окрім пожежної сигналізації, на входах передбачені світлові сигнальні індикатори.

2.3. Організація шляхів евакуації. Всі кабінети та серверні мають визначені евакуаційні виходи, відповідно до плану. Шляхи мають бути безпечними, з чіткою навігацією та освітленням, що відповідає вимогам безпеки. Розроблений план евакуації з позначеннями вогнегасників наведено на рисунку 5.1



№ приміщення	Назва приміщення
1	ВВІн без-вихідці
2	ВВВІн пасажирські без без
3	ВВІн пасажирські
4	Кабінет директора
5	ВВІн оптимізації і СЕО
6	Бухгалтерія
7	Серверна
8	Головний бухгалтер
9	ВВІн напрямки напрямку
10	Керівники підрозділів
11	ВВІн напрямки напрямку
12	Керівники підрозділів
13	Технічний ВВІн
14	Керівники підрозділів
15	ВВІн паркінгу і ремонту
16	ВВІн тестування

Рисунок 5.1 – План евакуації

2.4. Моніторинг технічного стану. Серверна кімната та основні комутаційні вузли мають системи температурного контролю і датчики чадного газу або перегріву. Це дозволяє своєчасно виявляти теплові загрози до початку займання та своєчасно реагувати на витік тепла.

2.5. Своєчасне обслуговування. Технічний персонал регулярно перевіряє працездатність вогнегасників та пожежних сигналізацій, проводить

періодичні обстеження електропроводки, серверного устаткування, захист від перегріву ЦП та джерел живлення.

5.2 Порядок допуску працівників до робіт з обслуговування електрообладнання

Обслуговування електроустановок у компанії «BST», яка здійснює діяльність у сфері розробки програмного забезпечення, повинно відповідати чинним вимогам електробезпеки. Працівники, які залучаються до робіт з електрообладнанням (серверне обладнання, системи безперебійного живлення, офісна електромережа тощо), мають проходити спеціальну підготовку, інструктажі та отримувати відповідну групу допуску з електробезпеки.

Згідно з Правилами безпечної експлуатації електроустановок споживачів [9], допуск до робіт в електроустановках можливий лише за наявності в працівника кваліфікаційної групи з електробезпеки не нижче III (для робіт у електроустановках до 1000 В). Такий допуск видається за результатами навчання, перевірки знань і медичного огляду. У компанії «BST» це правило поширюється, наприклад, на системного адміністратора, якщо в його обов’язки входить фізичне втручання в електричні мережі або обслуговування техніки у серверній.

Організація допуску включає [8]:

- проведення вступного інструктажу з охорони праці;
- спеціальне навчання (в тому числі з питань електробезпеки);
- перевірку знань (зі складанням протоколу);
- оформлення посвідчення про присвоєння групи допуску;
- ведення журналу допуску до робіт в електроустановках.

Повторна перевірка знань проводиться щороку або після перерви у роботі понад 6 місяців. Додатково працівникам необхідно дотримуватись

Інструкції з охорони праці під час експлуатації електротехнічного обладнання в офісних приміщеннях, яка адаптована до умов діяльності ІТ-компаній.

Варто зазначити, що підвищена увага до безпечної експлуатації електрообладнання в ІТ-компаніях обумовлена високою щільністю розміщення техніки, наявністю обчислювальних комплексів та стабілізаторів напруги, що створюють додаткові ризики у разі порушення правил електробезпеки.

ВИСНОВКИ

В кваліфікаційній роботі розроблено комп’ютерну мережу для компанії «BST». Локальна мережа розроблена з використанням сучасних стандартів та підходів. Для проекту локальної мережі спроектовано логічну та фізичну топологію, вибрано пасивне та активне комутаційне обладнання, сервери та їх програмне забезпечення.

Мережа побудована на гібридній фізичній топології з використанням стандарту IEEE 802.3ab для дротового сегменту та IEEE 802.11ac для бездротового. Для захисту бездротового зв’язку застосовано метод шифрування WPA2-PSK, що забезпечує високий рівень безпеки передачі даних. Мережа функціонує в частотних діапазонах 2,4 ГГц і 5 ГГц. Основу обміну даними становить протокольний стек TCP/IP, а взаємодія між вузлами організована за моделлю клієнт-сервер. Для фільтрації мережевого трафіку використовується міжмережевий екран iptables. Серверна інфраструктура працює під керуванням операційної системи AlmaLinuxLinux Stream 9. Спільний доступ до ресурсів Інтернету реалізовано за допомогою технології NAT, а обмін файлами відбувається на основі протоколу FTP.

Розроблено інструкції з налаштування:

1. Сервера доступу до мережі Інтернет.
2. Міжмережевого екрану iptables.
3. Безпровідних маршрутизаторів.
4. Файлового сервера.
5. Комутатора 3-го рівня моделі OSI.
6. Тестування основних вузлів локально мережі.
7. Інструкції з моніторингу вузлів мережі.
8. Інструкції з налаштування комутаторів робочих груп.

Графічна частина дипломної роботи складається з:

1. План приміщення.

2. Фізична топологія.

3. Логічна топологія.

4. Таблиця техніко-економічних показників.

5. Модель мережі.

В економічній частині проекту зроблено розрахунок повної вартості робіт по проектуванню, встановленню і запуску в експлуатацію мережі.

Останній розділ роботи описує питання охорони праці, та техніки безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Буров, Є.В. Комп’ютерні мережі: навч. посіб. Львів: Магнолія 2006. 2010. 262с.

2. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.

3. Жуков І.А., Дрововозов В.І., Махновський Б.Г. Експлуатація комп’ютерних систем та мереж. Київ: НАУ. 2007. 361с.

4. Комп’ютерні мережі: навч. посіб. / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник/ Львів. Магнолія 2006. 2013. 256 с.

5. Контроль та керування корпоративними комп'ютерними мережами: інструментальні засоби та технології: навч. посіб. / А. М. Гуржій, С. Ф. Коряк, В. В. Самсонов, О. Я. Скляров. Харків: СМІТ. 2014. 544 с

6. Методичні вказівки до виконання кваліфікаційної роботи за спеціальністю №123 «Комп’ютерна інженерія» - Тернопіль.: ВСП ТФК ТНТУ, 2019. -34с.

7. Микитишин А.Г., Митник, П.Д. Стухляк. Телекомунікаційні системи та мережі. Тернопіль: Вид-во ТНТУ імені Івана Пулюя. 2016. 384 с

8. Покропивний С. В., Покропивна Л. А. Охорона праці в галузі ІТ : навч. посіб. — Київ : КНУБА, 2021. — 147 с.

9. Правила безпечної експлуатації електроустановок споживачів : НПАОП 40.1-1.21-98. — Київ : Держбуд України, 2008. — [Чинний документ]. — 110 с.

10. Сокуренко В. В., Горбенко І. В., Пархоменко С. П. Безпека життєдіяльності та охорона праці : навч. посіб. — Харків : ХНУВС, 2021. — 176 с.

11. Третьяков О. В., Бурдейний О. М., Клименко П. В. Основи охорони праці : навч. посіб. — Харків : Планета-Прінт, 2020. — 224 с.

12. Тхір І., Калушка В., Юзьків А. Посібник користувача ПК.3-е видання. – Тернопіль: Підручники і посібники. 2006.-1024с.

13. Allied Telesyn – AT-GS950/8. URL: https://www.інструкціїкористувача.com.ua/allied-telesis/at-gs950-8/%D1%96%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%86%D1%96%D1%8F-%D0%BA%D0%BE%D1%80%D0%B8%D1%81%D1%82%D1%83%D0%B2%D0%B0%D1%87%D0%B0#google_vignette. (дата звернення: 05.06.2025).

14. AlmaLinux9: URL: https://wiki.almalinux.org/#contributions-to-the-wiki /. (дата звернення: 09.06.2025)..

15. Dell Power Edge R530. URL: https://www.dell.com/ua/business/p/poweredge-r530/pd. (дата звернення: 06.06.2025).

16. Edge Core ES4610. URL: http://beta.edge-core.com/ProdDtl.asp?sno=322&ES4610. (дата звернення: 05.06.2025).

17. IPTables настройка. URL: https://1cloud.com/help/linux/nastrojka_linus-firewall_iptables (дата звернення: 10.06.2025).

18. Proftdp URL: http://www.proftpd.org/docs/example-conf.html/. (дата звернення: 05.06.2025).

19. User Guide – WRT1900. URL: https://downloads.linksys.com/downloads/userguide/1224701614608/MAN_WRT1900AC_8820-01897_RevA00_EN_FR-CA_Comprehensive.pdf (дата звернення: 08.06.2025).

20. Налаштування Wi-fi роутерів Linksys. URL: https://my.volia.com/kiev/uk/faq/article/nastroika-wi-fi-routerov-linksys?partner=organic_search&utm_source=google&utm_medium=organic/ (дата звернення: 08.06.2025).

21. Шафа 24u. URL: https://e-server.com.ua/uk/serverni-shafi/pidlogovi-shafi/serverna-shafa-pidlogova-24u-600x800 (дата звернення: 03.06.2025).

ДОДАТКИ

Додаток А. IP-адресація

Таблиця А1 - Таблиця IP-адрес

Назва вузла	Назва кабінету та його номер	Номер VLAN	Адреса вузла/ Маска	Шлюз
1	2	3	4	5
WS_1	Керівники підрозділів	11	172.99.1.1/24	172.99.1.100
WS_2			172.99.1.2/24	
WS_3			172.99.1.3/24	
WS_4	Директор	12	172.99.2.1/24	172.99.2.100
WS_5	Бухгалтерія	13	172.99.3.1/24	172.99.3.100
WS_6			172.99.3.2/24	
WS_7			172.99.3.3/24	
SW_1		1	10.10.10.1/24	-
WS_8	Гол. Бухгалтер	14	172.99.4.1/24	172.99.4.100
WS_9	Відділ програмування під WEB	15	172.99.5.1/24	172.99.5.100
WS_10			172.99.5.2/24	
WS_11			172.99.5.3/24	
WS_12			172.99.5.4/24	
WS_13			172.99.5.5/24	
WS_14			172.99.5.6/24	
SW_2		1	10.10.10.2/24	-
WS_15	Відділ оптимізації і CEO	16	172.99.6.1/24	172.99.6.100
WS_16			172.99.6.2/24	
WS_17			172.99.6.3/24	
WS_18			172.99.6.4/24	
SW_3		1	10.10.10.3/24	-
WS_19	Відділ тестування	17	172.99.7.1/24	172.99.7.100
WS_20			172.99.7.2/24	
WS_21			172.99.7.3/24	
WS_22			172.99.7.4/24	

Продовження таблиці А1

1	2	3	4	5
R_1		17	172.99.7.50/24	172.99.7.100
WS_23	Відділ наповнення контенту	18	172.99.8.1/24	172.99.8.100
WS_24			172.99.8.2/24	
SW_4	Серверна	1	10.10.10.4/24	-
S_1		19	172.99.9.1/24	172.99.9.100
S_2			172.99.9.2/24	
		-	212.55.280.121	212.55.280.150
WS_25	Відділ техпідтримки	20	172.99.10.1/24	172.99.10.100
WS_26			172.99.10.2/24	
WS_27	Відділ веб-дизайну	21	172.99.11.1/24	172.99.11.100
WS_28			172.99.11.2/24	
WS_29			172.99.11.3/24	
WS_30			172.99.11.4/24	
WS_31			172.99.11.5/24	
WS_32			172.99.11.6/24	
SW_5		1	10.10.10.5/24	-
WS_33	Відділ програмування	22	172.99.12.1/24	172.99.12.100
WS_34			172.99.12.2/24	
WS_35			172.99.12.3/24	
WS_36			172.99.12.4/24	
SW_6		1	10.10.10.6/24	-
WS_37	Відділ маркетингу, реклами	23	172.99.13.1/24	172.99.13.100
WS_38			172.99.13.2/24	172.99.13.100
WS_39			172.99.13.3/24	172.99.13.100
WS_40			172.99.13.4/24	172.99.13.100
WS_41			172.99.13.5/24	172.99.13.100
WS_42			172.99.13.6/24	172.99.13.100
WS_43		24	172.99.14.1/24	172.99.14.100
WS_44	Технічний відділ	24	172.99.14.2/24	172.99.14.100
WS_45			172.99.14.3/24	172.99.14.100
WS_46			172.99.14.4/24	172.99.14.100

Додаток Б. Логічна адресація в ЛОМ

Таблиця Б1 – Розподіл логічних адрес

Назва вузла	Робоча група/ Кількість вузлів		Прим.	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
1	2	3	4	5	6	7	8
WS_1	-	3	-	Керівники підрозділів	-	11	172.99.1.0/24
WS_2							
WS_3							
WS_4	-	2	-	Кабінет директора	-	12	172.99.2.0/24
WS_5	-	4	-	Бухгалтерія	-	13	172.99.3.0/24
WS_6							
WS_7							
SW_1						1	10.10.10.0/24
WS_8	-	1	-	Гол. Бухгалтер		14	172.99.4.0/24
WS_9	-	7	-	Відділ програмування для WEB	-	15	172.99.5.0/24
WS_10							
WS_11							
WS_12							
WS_13							
WS_14							
SW_2						1	10.10.10.0/24
WS_15	-	5	-	Відділ оптимізації і CEO	-	16	172.99.6.0/24
WS_16							
WS_17							
WS_18							
SW_3						1	10.10.10.0/24
WS_19	-	5	-	Відділ тестування	-	17	172.99.7.0/24
WS_20							
WS_21							
WS_22							

Продовження таблиці Б1

1	2	3	4	5	6	7	8
R_1						1	10.10.10.0/24
WS_23	-	3	-	Відділ наповнення контенту	-	18	172.99.8.0/24
WS_24							
SW_4	-	3	-	Серверна	-	1	10.10.10.0/24
S_1						19	172.99.9.0/24
S_2							
WS_25	-	2	-	Відділ техпідтримки	-	20	172.99.10.0/24
WS_26							
WS_27	-	7	-	Відділ веб-дизайну	-	21	172.99.11.0/24
WS_28							
WS_29							
WS_30							
WS_31							
WS_32							
SW_5						1	10.10.10.0/24
WS_33	-	5	-	Відділ програмування	-	22	172.99.12.0/24
WS_34							
WS_35							
WS_36							
SW_6						1	10.10.10.0/24
WS_37	-	6	-	Відділ маркетингу і реклами	-	23	172.99.13.0/24
WS_38							
WS_39							
WS_40							
WS_41							
WS_42							
WS_43	-	6	-	Технічний відділ		24	172.99.14.0/24
WS_44							
WS_45							
WS_46							

Таблиця Б2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. Пристар.	Номер порту	Тип порту	Номер VLAN
1	WS_1-WS_2	Eth0	-	SW_1	1-2	Access	11
2	WS_3-WS_4	Eth0	-	SW_1	3-4	Access	12
3	WS_5-WS_7	Eth0	-	SW_1	5-7	Access	13
4	WS_8	Eth0	-	SW_1	8	Access	14
5	WS_9-WS_14	Eth0	-	SW_2	1-6	Access	15
6	WS_15-WS_18	Eth0	-	SW_3	1-4	Access	16
7	WS_19-WS_22	Eth0	-	R_1	WLAN	-	-
8	WS_23-WS_24	Eth0	-	SW_4	1-2	Access	18
9	S_1, S_2	Eth0	-	SW_4	3-4	Access	19
10	WS_25-WS_26	Eth0	-	SW_4	5-6	Access	20
11	WS_27-WS_32	Eth0	-	SW_5	1-6	Access	21
12	WS_33-WS_36	Eth0	-	SW_6	1-6	Access	22
13	WS_37-WS_42	Eth0	-	R_2	WLAN	-	-
14	WS_43-WS_46	Eth0	-	SW_7	1-6	Access	24
15	SW_1	9	Trunk	SW_4	7	Trunk	-
16	SW_2	7	Trunk	SW_4	8	Trunk	-
17	SW_3	5	Trunk	SW_4	9	Trunk	-
18	SW_5	7	Trunk	SW_4	10	Trunk	-
19	SW_6	7	Trunk	SW_4	11	Trunk	-
20	SW_7	7	Trunk	SW_4	12	Trunk	-
21	R_1	WAN	-	SW_4	13	Access	17
22	R_2	WAN	-	SW_4	14	Access	23

Додаток В. Порівняльна характеристика обладнання

Таблиця В1 - Порівняння апаратних конфігурацій серверів

	Dell PowerEdge R530	HP ProLiant DL380 Gen9
Серверний процесор:	Intel Xeon E5-2600V3	Intel Xeon E5-2600V3
Оперативна пам’ять:	16ГБ DDR4	16ГБ DDR4
Дискова підсистема	Контролер PERC H730 1GB Cache, 2 диски 2ТБ HDD	HPE Flexible Smart Array P840ar/2G Controller, 2 диски 2ТБ HDD
Блок живлення	400Вт	400Вт
Мережева карта:	4xGigabit Ethernet	HPE Embedded 1 Gb -4x
Чіпсет	Intel C610	Intel C610
Встановлена ОС	Ні	Ні

Таблиця В2 – Технічні характеристики комутаторів

Параметр/Модель	Edge-Core ES4610	Cisco Catalyst 3750G-24T	Dell N1524
1	2	3	4
К-сть портів (основних)	20	24	24
К-сть слотів для модулів (додаткових)	4 SFP, 2 x 10G	4 SFP	4 SFP
Функції моделі OSI	3, 2	3, 2	3, 2
Швидкість комутаційної шини	128 Гбіт/с	32 Гбіт/с	128 Гбіт/с
Швидкість комутації	95,2 млн. пакетів за сек	38,7 млн. пакетів за сек.	128 млн. пакетів за сек

Продовження таблиці В2

1	2	3	4
Підтримка статичної маршрутизації	Так	Так	Так
Підтримка динамічної маршрутизації	Так	Так	Так
Підтримка ACL	Так	Так	Так
Підтримка IEEE 802.1Q	Так	Так	Так

Таблиця В3 - Порівняння технічних характеристик комутаторів робочих груп

Характеристика	AT-GS950/8	HP 1810-8G	UniFi SWitch US-8
Підтримувані стандарти	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab, IEEE 802.1p, IEEE 802.1Q, IEEE 802.3ad		
Пропускна здатність, Гбіт/с	16	16	16
Швидкість комутації, 88вят. пакетів/с	11,9	11,9	11,9
К-сть портів 10/100/1000	8	8	8
Додаткові слоти SFP	2	-	-
Віддалене керування	Web, Telnet		

Таблиця В4 - Порівняльна характеристика безпровідних маршрутизаторів

Виробник	Linksys	TP-Link	Netis
Марка	WRT-1900AC	AC1750	WF2780
Стандарти	802.11n, 802.11ac, 802.11g, 802.11b,802.3		
Передача на частотах 2,4 та 5 Ггц	+	+	
Кількість портів WAN	1 x Gigabit Ethernet	1 x Gigabit Ethernet	1 x Gigabit Ethernet
Кількість портів LAN	4 x Gigabit Ethernet	4 x Gigabit Ethernet	4 x Gigabit Ethernet
Протоколи безпеки	WPA-Personal, WPA-Enterprice, WPA2-Personal, WPA2-Enterprice		
Віддалене керування	+	+	+
Кількість антен	4	4	4
Статистика переданих/прийнятих пакетів	+	+	+

Додаток Г. Конфігураційний скріпт налаштування фаєрволу iptables

Послідовність команд: показати статус

iptables –L –n –v

Вивід команди для неактивного файрволу:

Chain INPUT (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

Для активного файрволу:

Chain INPUT (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

0 0 DROP all - * * 0.0.0.0/0 0.0.0.0/0 state INVALID

394 43586 ACCEPT all - * * 0.0.0.0/0 0.0.0.0/0 state RELATED, ESTABLISHED

93 17292 ACCEPT all – br0 * 0.0.0.0/0 0.0.0.0/0

1 142 ACCEPT all – lo * 0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy DROP 0 packets, 0 bytes)

pkts bytes target prot opt in out source destination

0 0 ACCEPT all – br0 br0 0.0.0.0/0 0.0.0.0/0

0 0 DROP all - * * 0.0.0.0/0 0.0.0.0/0 state INVALID

0 0 TCPMSS tcp - * * 0.0.0.0/0 0.0.0.0/0 tcp flags: 0x06 / 0x02 TCPMSS clamp to PMTU

0 0 ACCEPT all - * * 0.0.0.0/0 0.0.0.0/0 state RELATED, ESTABLISHED

0 0 wanin all – vlan2 * 0.0.0.0/0 0.0.0.0/0

0 0 wanout all - * vlan2 0.0.0.0/0 0.0.0.0/0

0 0 ACCEPT all – br0 * 0.0.0.0/0 0.0.0.0/0

Chain OUTPUT (policy ACCEPT 425 packets, 113K bytes)

pkts bytes target prot opt in out source destination

Chain wanin (1 references)

pkts bytes target prot opt in out source destination

Chain wanout (1 references)

pkts bytes target prot opt in out source destination

де:

-L: Показати список правил.

-v: Відображати додаткову інформацію. Ця опція показує ім’я інтерфейсу, опції, TOS маски. Також відображає суфікси ‘K’, ‘M’ or ‘G’.

-n: Відображати IP адреса і порт числами (не використовуючи DNS сервера для визначення імен. Це прискорить відображення).

Показати список правил з номерами рядків:

iptables –n –L –v –line-numbers

Приблизний вивід:

Chain INPUT (policy DROP)

num target prot opt source destination

1 DROP all – 0.0.0.0/0 0.0.0.0/0 state INVALID

2 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state RELATED, ESTABLISHED

3 ACCEPT all – 0.0.0.0/0 0.0.0.0/0

4 ACCEPT all – 0.0.0.0/0 0.0.0.0/0

Chain FORWARD (policy DROP)

num target prot opt source destination

1 ACCEPT all – 0.0.0.0/0 0.0.0.0/0

2 DROP all – 0.0.0.0/0 0.0.0.0/0 state INVALID

3 TCPMSS tcp – 0.0.0.0/0 0.0.0.0/0 tcp flags: 0x06 / 0x02 TCPMSS clamp to PMTU

4 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state RELATED, ESTABLISHED

5 wanin all – 0.0.0.0/0 0.0.0.0/0

6 wanout all – 0.0.0.0/0 0.0.0.0/0

7 ACCEPT all – 0.0.0.0/0 0.0.0.0/0

Chain OUTPUT (policy ACCEPT)

num target prot opt source destination

Chain wanin (1 references)

num target prot opt source destination

Chain wanout (1 references)

num target prot opt source destination

Ви можете використовувати номери рядків для того, щоб додавати нові правила.

Показати INPUT або OUTPUT ланцюжки правил:

iptables –L INPUT –n –v

iptables –L OUTPUT –n –v –line-numbers

Зупинити, запустити, перезапустити файрвол;

Силами самої системи:

service ufw stop

service ufw start

Можна також використовувати команди iptables для того, щоб зупинити файрвол і видалити всі правила:

iptables –F

iptables –X

iptables –t nat –F

iptables –t nat –X

iptables –t mangle –F

iptables –t mangle –X

iptables –P INPUT ACCEPT

iptables –P OUTPUT ACCEPT

iptables –P FORWARD ACCEPT

де:

-F: Видалити (flush) всіх правил.

-X: Видалити ланцюжок.

-t table_name: Вибрати таблицю (nat або mangle) і видалити всі правила.

-P: Вибрати дії за замовчуванням (такі, як DROP, REJECT, або ACCEPT).

Видалити правила файрвола. Щоб відобразити номер рядка з існуючими правилами:

iptables –L INPUT –n –line-numbers

iptables –L OUTPUT –n –line-numbers

iptables –L OUTPUT –n –line-numbers | less

iptables –L OUTPUT –n –line-numbers | grep 202.54.1.1

Отримаємо список IP адрес. Просто подивимося на номер зліва і видалимо відповідний рядок. Наприклад для номера 3:

iptables –D INPUT 3

Або знайдемо IP адреса джерела (202.54.1.1) і видалимо з правила:

iptables –D INPUT –s 202.54.1.1 –j DROP

де:

-D: Видалити одне або кілька правил з ланцюжка.

Додати правило в файрвол. Щоб додати одне або кілька правил в ланцюжок, для початку відобразимо список з використанням номерів рядків:

iptables –L INPUT –n –line-numbers

Приблизний висновок:

Chain INPUT (policy DROP)

num target prot opt source destination

1 DROP all – 202.54.1.1 0.0.0.0/0

2 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state NEW, ESTABLISHED

Щоб вставити правило між 1 і 2 рядком:

iptables –I INPUT 2 –s 202.54.1.2 –j DROP

Перевіримо, оновилося чи правило:

iptables –L INPUT –n –line-numbers

Висновок стане таким:

Chain INPUT (policy DROP)

num target prot opt source destination

1 DROP all – 202.54.1.1 0.0.0.0/0

3 DROP all – 202.54.1.2 0.0.0.0/0

3 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state NEW, ESTABLISHED

Зберігаємо правила файрвола. Через iptables-save:

iptables-save > /etc/iptables.rules

Відновлюємо правила. Через iptables-restore:

iptables-restore < /etc/iptables.rules

Встановлюємо політики за замовчуванням. Щоб скидати весь трафік:

iptables –P INPUT DROP

iptables –P OUTPUT DROP

iptables –P FORWARD DROP

iptables –L –v –n

Після перерахованих вище команд жоден пакет не покине даний хост.

ping google.com

Блокувати тільки вхідні з’єднання. Щоб скидати все не ініційовані вами вхідні пакети, але дозволити вихідний трафік:

iptables –P INPUT DROP

iptables –P FORWARD DROP

iptables –P OUTPUT ACCEPT

iptables –A INPUT –m state –state NEW,ESTABLISHED –j ACCEPT

iptables –L –v –n

Пакети вихідні і ті, які були збережені до в рамках встановлених сесій – дозволені.

ping google.com

Скидати адреси ізольованих мереж в публічній мережі:

iptables –A INPUT –i eth1 –s 192.168.0.0/24 –j DROP

iptables –A INPUT –i eth1 –s 10.0.0.0/8 –j DROP

Список IP адрес для ізольованих мереж:

10.0.0.0/8 –j (A)

172.99.0.0/12 (B)

192.168.0.0/16 (C)

224.0.0.0/4 (MULTICAST D)

240.0.0.0/5 (E)

127.0.0.0/8 (LOOPBACK)

Блокування певного IP адреси. Щоб заблокувати адресу зломщика 1.2.3.4:

iptables –A INPUT –s 1.2.3.4 –j DROP

iptables –A INPUT –s 192.168.0.0/24 –j DROP

Заблокувати вхідні запити порту. Щоб заблокувати всі вхідні запити порту 80:

iptables –A INPUT –p tcp –dport 80 –j DROP

iptables –A INPUT –i eth1 –p tcp –dport 80 –j DROP

Щоб заблокувати запит порту 80 з адреси 1.2.3.4:

iptables –A INPUT –p tcp –s 1.2.3.4 –dport 80 –j DROP

iptables –A INPUT –i eth1 –p tcp –s 192.168.1.0/24 –dport 80 –j DROP

Заблокувати запити на вихідний IP адреса.

Щоб заблокувати певний домен, дізнаємося його адресу:

host –ta facebook.com

Висновок: facebook.com has address 69.171.228.40

Знайдемо CIDR для 69.171.228.40:

whois 69.171.228.40 | grep CIDR

Вивід:

CIDR: 69.171.224.0/19

Заблокуємо доступ на 69.171.224.0/19:

iptables –A OUTPUT –p tcp –d 69.171.224.0/19 –j DROP

Також можна використовувати домен для блокування:

iptables –A OUTPUT –p tcp –d www.facebook.com –j DROP

iptables –A OUTPUT –p tcp –d facebook.com –j DROP

Записати подію. Щоб записати в журнал рух пакетів перед скиданням, додамо правило:

iptables –A INPUT –i eth1 –s 10.0.0.0/8 –j LOG –log-prefix «IP_SPOOF A: «

iptables –A INPUT –i eth1 –s 10.0.0.0/8 –j DROP

Перевіримо журнал (за замовчуванням /var/log/messages):

tail –f /var/log/messages

grep –i –color ‘IP SPOOF’ /var/log/messages

Записати подію і скинути (з обмеженням на кількість записів). Щоб не переповнити розділ роздутим журналом, обмежимо кількість записів за допомогою –m. Наприклад, щоб записувати кожні 5 хвилин максимум 7 рядків:

iptables –A INPUT –i eth1 –s 10.0.0.0/8 –m limit –limit 5/m –limit-burst 7 –j LOG –log-prefix «IP_SPOOF A: «

iptables –A INPUT –i eth1 –s 10.0.0.0/8 –j DROP

Скидати або дозволити трафік з певних MAC адрес:

iptables –A INPUT –m mac –mac-source 00:0F:EA:91:04:08 –j DROP

iptables –A INPUT –p tcp –destination-port 22 –m mac –mac-source 00:0F:EA:91:04:07 –j ACCEPT

Дозволити або заборонити ICMP Ping запити. Щоб заборонити ping:

iptables –A INPUT –p icmp –icmp-type echo-request –j DROP

iptables –A INPUT –i eth1 –p icmp –icmp-type echo-request –j DROP

Дозволити для певних мереж/хостів:

iptables –A INPUT –s 192.168.1.0/24 –p icmp –icmp-type echo-request –j ACCEPT

Дозволити лише частину ICMP запитів:

iptables –A INPUT –p icmp –icmp-type echo-reply –j ACCEPT

iptables –A INPUT –p icmp –icmp-type destination-unreachable –j ACCEPT

iptables –A INPUT –p icmp –icmp-type time-exceeded –j ACCEPT

iptables –A INPUT –p icmp –icmp-type echo-request –j ACCEPT

Відкрити діапазон портів:

iptables –A INPUT –m state –state NEW –m tcp –p tcp –dport 7000:7010 –j ACCEPT

Відкрити діапазон адрес:

iptables –A INPUT –p tcp –destination-port 80 –m iprange –src-range 192.168.1.100-192.168.1.200 –j ACCEPT

iptables –t nat –A POSTROUTING –j SNAT –to-source 192.168.1.20-192.168.1.25

Закрити або відкрити стандартні порти. Замінити ACCEPT на DROP, щоб заблокувати порт.

Iptables –A INPUT –m state –state NEW –m tcp –p tcp –dport 22 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 22 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –p udp –m udp –dport 631 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –p tcp –m tcp –dport 631 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p udp –dport 123 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 25 –j ACCEPT

iptables –A INPUT –m state –state NEW –p udp –dport 53 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 53 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 80 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 443 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 110 –j ACCEPT

iptables –A INPUT –m state –state NEW –p tcp –dport 143 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 137 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 138 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 139 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 445 –j ACCEPT

iptables –A INPUT –s 192.168.1.0/24 –m state –state NEW –p tcp –dport 3128 –j ACCEPT

iptables –I INPUT –p tcp –dport 3306 –j ACCEPT

Обмежити кількість паралельних з'єднань до сервера для однієї адреси. Для обмежень використовується connlimit модуль. Щоб дозволити лише 3 ssh з'єднання на одного клієнта:

iptables –A INPUT –p tcp –syn –dport 22 –m connlimit –connlimit-above 3 –j REJECT

Встановити кількість запитів HTTP до 20:

iptables –p tcp –syn –dport 80 –m connlimit –connlimit-above 20 –connlimit-mask 24 –j DROP

де:

--connlimit-above 3: Вказує, що правило діє тільки якщо кількість з'єднань перевищує 3.

--connlimit-mask 24: Вказує маску мережі.

Щоб подивитися допомогу по певним командам і цілям:

iptables –j DROP –h

Перевірка правила iptables.

Перевіряємо відкритість/закритість портів:

netstat –tulpn

Перевіряємо відкритість/закритість певного порту:

netstat –tulpn | grep :80

Перевіримо, що iptables дозволяє з’єднання з 80 портом:

iptables –L INPUT –v –n | grep 80

В іншому випадку відкриємо його для всіх:

iptables –A INPUT –m state –state NEW –p tcp –dport 80 –j ACCEPT

Перевіряємо за допомогою telnet

$ telnet google.com 80