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 ТОВ "КонтрактБуд"**

Виконав: студент VI курсу, групи КІб-602

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

_____ Володимир БІЛОВУС
(ім'я та прізвище)

Керівник Андрій ЮЗЬКІВ
(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

Біловусу Володимиру Андрійовичу
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи **Розробка проекту комп'ютерної мережі ТОВ "КонтрактБуд"**

керівник роботи Юзьків Андрій Васильович
(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, 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 _____ Володимир БІЛОВУС
(підпис) (ім'я та прізвище)

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

АНОТАЦІЯ

Біловус В.А. Розробка проекту комп'ютерної мережі ТОВ «Контракт Буд»: кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 123 Комп'ютерна інженерія. – Тернопіль: ВСП «ТФК ТНТУ», 2025. – 90с.

У кваліфікаційній роботі представлено проєкт локальної комп'ютерної мережі для ТОВ «Контракт Буд». Мережа реалізована за клієнт-серверною архітектурою із серверами доступу до Інтернету й IP-телефонії на базі Asterisk. Враховано параметри пропускної здатності, безпеку передачі даних та стандарти захисту. Використано технологію 1000Base-TX, кабельну систему категорії 6 і безпровідну мережу стандарту Wi-Fi 802.11ac. Проведено розробку фізичної топології, та здійснено моделювання роботи мережі. Реалізовано детальні інструкції для налаштування мережевих пристроїв і серверів.

Ключові слова: комп'ютерна мережа, IP-телефонія, Wi-Fi 802.11ac, Asterisk, клієнт-серверна архітектура.

ANNOTATION

Bilovus V.A. Computer Network Project Development of LLC "Kontrakt Bud" 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. – 90p.

This bachelor's qualification thesis presents the project of a local area network (LAN) for the engineering and construction company LLC "Kontrakt Bud". The network is designed using a client-server architecture, with dedicated servers for Internet access and IP telephony based on the Asterisk platform. The project takes into account bandwidth parameters, data transmission security, and protection standards. The solution employs 1000Base-TX technology, a Category 6 structured cabling system, and a wireless segment based on the Wi-Fi 802.11ac standard. The physical topology of the network was developed, and its operation was simulated. Detailed configuration instructions for network devices and servers were implemented.

Keywords: computer network, IP telephony, Wi-Fi 802.11ac, Asterisk, client-server architecture.

ЗМІСТ

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

ICMP (Internet Control Message Protocol) - протокол керування передачею повідомлень, що використовується для обміну службовою інформацією між пристроями в мережах TCP/IP.

MAT (MAC Address Translation) - трансляція MAC-адрес, що забезпечує перетворення адрес фізичного рівня для маршрутизації трафіку між мережами.

NAT (Network Address Translation) - технологія трансляції мережевих адрес, яка дозволяє кільком пристроям у локальній мережі використовувати одну публічну IP-адресу для доступу до Інтернету.

QoS (Quality of Service) - набір технологій для управління параметрами трафіку з метою забезпечення заданої якості обслуговування у комп’ютерних мережах.

TCP/IP (Transmission Control Protocol / Internet Protocol) - базовий стек протоколів, що забезпечує маршрутизацію, передачу та контроль даних у гетерогенних комп’ютерних мережах, зокрема в Інтернеті.

UDP (User Datagram Protocol) - протокол прикладного рівня без встановлення з’єднання, що забезпечує швидку передачу даних без гарантій доставки.

URL (Uniform Resource Locator) - уніфікований вказівник ресурсу, що використовується для ідентифікації адрес в Інтернеті.

UTP (Unshielded Twisted Pair) - тип мережевого кабелю, що складається з неекранованої витої пари провідників, призначений для передачі даних.

VLAN (Virtual Local Area Network) - віртуальна локальна мережа, що об’єднує вузли за логічним критерієм незалежно від їхнього фізичного розташування.

Брандмауер / Міжмережевий екран - апаратно-програмний засіб контролю доступу між сегментами мережі з метою захисту від несанкціонованого трафіку.

Група - логічне об’єднання комп’ютерів у мережі, призначене для спільного доступу до ресурсів та виконання спільних завдань.

ЛОМ (Локальна обчислювальна мережа) - комп’ютерна мережа, що об’єднує пристрої в межах обмеженої території (офісу, будівлі) з метою спільного доступу до даних та ресурсів.

ОС (Операційна система) - системне програмне забезпечення, яке забезпечує управління апаратними ресурсами та виконання прикладних програм.

Пакет - одиниця передавання даних у комп’ютерній мережі, яка включає службову та корисну інформацію.

ПК (Персональний комп’ютер) - автономний електронний пристрій, призначений для обробки, зберігання та виведення інформації, зазвичай використовується як клієнт мережі.

Протокол - набір правил, що визначають формат та порядок обміну даними між пристроями в комп’ютерній мережі.

Робоча група - об’єднання комп’ютерів у мережі, які спільно використовують локальні ресурси без централізованого адміністрування.

Сеанс - логічне з’єднання між пристроями або користувачами мережі для обміну інформацією протягом певного часу.

СУОП (Система управління охороною праці) - складова загальної системи управління підприємством, що включає сукупність організаційних, технічних, правових, санітарно-гігієнічних та інших заходів, спрямованих на створення безпечних умов праці, запобігання нещасним випадкам та професійним захворюванням.

Фізична топологія - схема фізичних з’єднань між мережевими пристроями, що визначає структуру локальної мережі.

ВСТУП

У сучасних умовах стрімкого розвитку інформаційно-комунікаційних технологій підприємства та організації отримують розширені можливості для підвищення ефективності своєї діяльності за рахунок впровадження інтегрованих телекомунікаційних систем. Основні переваги таких систем [2]:

- забезпечення оперативного обміну даними, включаючи текстові повідомлення, аудіо- та відеоконференції;
- організація безпечного доступу до локальних і глобальних інформаційних ресурсів;
- централізоване зберігання і захист конфіденційної інформації за допомогою серверного обладнання;
- спільне використання мережевих ресурсів, таких як файлові сховища, принтери, сканери тощо;
- централізоване адміністрування, моніторинг і захист вузлів локальної обчислювальної мережі.

В рамках даної кваліфікаційної роботи розроблено оптимальне технічне рішення щодо побудови локальної обчислювальної мережі для інженерно-будівельного підприємства ТОВ «Контракт Буд». Проектована мережа реалізована за клієнт-серверною архітектурою, передбачає високий рівень масштабованості, продуктивності та інформаційної безпеки, відповідає сучасним вимогам до надійності та швидкодії.

У ході розробки здійснено вибір фізичної та логічної топологій, мережевих технологій (1000Base-TX, Wi-Fi 802.11ac), активного та пасивного обладнання, адресного простору, а також серверних рішень, зокрема, сервера IP-телефонії на базі Asterisk. Окрему увагу приділено питанням захисту переданих даних, оптимізації мережевого трафіку та забезпечення безперервної роботи корпоративної мережі.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Назва та галузь застосування розробки

Тема кваліфікаційної роботи охоплює проєктування локальної комп'ютерної мережі для офісного приміщення ТОВ «Контракт Буд». Розроблена мережа відрізняється від типових рішень за рахунок інтеграції як провідних (1000Base-TX), так і безпровідних (Wi-Fi 802.11ac) технологій, що забезпечує її гнучкість, масштабованість і відповідність сучасним вимогам до безпеки та продуктивності.

Проєкт враховує ключові аспекти захисту інформаційного середовища: реалізовано заходи безпеки для дротового та бездротового сегментів мережі, застосовано актуальні методики проектування з урахуванням майбутнього розширення інфраструктури за рахунок надлишкової пропускної здатності.

У межах реалізації проєкту сконфігуровано такі критично важливі мережеві служби:

Шлюзовий сервер для доступу до мережі Інтернет на основі вільної операційної системи FreeBSD.

Сервер IP-телефонії на базі Asterisk.

Розроблена мережева інфраструктура може бути адаптована до інших організацій, у яких є аналогічні функціональні вимоги, відповідно до положень підрозділу 1.1.2 «Призначення розробки».

1.1.2 Призначення розробки

Метою проєкту є розробка локальної комп'ютерної мережі для забезпечення ефективної інформаційної взаємодії та підтримки бізнес-процесів

інженерно-будівельної компанії «Контракт Буд». Реалізація мережевої інфраструктури дозволить вирішити такі технічні та організаційні завдання:

- Інтеграція персональних комп'ютерів компанії в єдину інформаційну систему.

- Забезпечення централізованого управління мережевими потоками даних за допомогою шлюзового сервера.

- Створення умов для мобільного доступу працівників до локальної мережі та ресурсів Інтернету з використанням бездротових технологій.

- Організація спільного використання периферійних пристроїв (принтерів, сканерів) і локальних сервісів.

- Реалізація централізованих механізмів захисту локальної мережі від зовнішніх загроз.

- Забезпечення високого рівня безпеки бездротового сегменту з метою запобігання несанкціонованому доступу.

- Можливість масштабування мережі без необхідності суттєвих змін у фізичній інфраструктурі.

- Ефективне використання ресурсів локальної мережі (мережеві накопичувачі, спільне ПЗ).

- Інтеграція сервісу IP-телефонії для реалізації внутрішніх голосових комунікацій між співробітниками компанії з мінімальними витратами.

Для досягнення поставлених цілей проєкт передбачає наступну послідовність дій:

- Проєктування системи кабельних каналів із використанням коробів відповідних розмірів.

- Прокладання кабельних сегментів відповідно до обраної фізичної топології.

- Вибір та впровадження типу кабелю, що відповідає обраному стандарту (наприклад, категорія 6).

- Розгортання бездротового сегменту із застосуванням відповідного стандарту (Wi-Fi 802.11ac) та мережевого обладнання.

- Налаштування основних мережевих служб та конфігурація обладнання, зокрема сервера IP-телефонії на базі Asterisk для внутрішнього голосового зв’язку.

Запропоноване рішення спрямоване на створення надійної, безпечної та масштабованої мережевої інфраструктури, що відповідає сучасним технічним вимогам і виробничим потребам компанії.

1.1.3 Вимоги до апаратного і програмного забезпечення

Локальна комп’ютерна мережа являє собою інтегровану систему, що складається з апаратної та програмної складових. Ефективне функціонування мережі забезпечується належним підбором кожного з компонентів відповідно до сучасних стандартів, вимог масштабованості, безпеки та надійності.

Програмне забезпечення локальної мережі включає:

- Операційні системи користувацьких робочих станцій, які повинні підтримувати мережевий стек протоколів TCP/IP, оскільки саме на цьому протоколі базується взаємодія в локальному та глобальному мережевому середовищі.

- Серверні операційні системи, що використовуються для побудови функціонального серверного середовища. До основних вимог до серверних ОС належать: висока надійність, стабільність у роботі, підтримка оновлень без переривання сервісів, а також оптимальне співвідношення вартості та функціональності.

Апаратне забезпечення локальної мережі поділяється на активне та пасивне:

- Пасивне мережеве обладнання включає кабельну інфраструктуру (виту пару, патчкорди, патчпанелі тощо). Підбір елементів виконується з урахуванням вимог до пропускної здатності та можливості подальшого розширення мережі.

- Комутатори (мережеві свічі) поділяються на магістральні (центральні) та сегментні. Всі комутатори повинні підтримувати стандарти IEEE: 802.3 (Ethernet), 802.3u (Fast Ethernet), 802.3ab (Gigabit Ethernet), 802.1p (QoS), 802.1Q (VLAN). Центральний комутатор має підтримувати функції статичної маршрутизації для забезпечення ефективного управління трафіком.

- Бездротові точки доступу мають відповідати сучасним стандартам IEEE 802.11b/g/n/ac, а також забезпечувати підтримку актуальних протоколів захисту бездротового з'єднання: WPA-PSK та WPA2-PSK.

- Серверне обладнання обирається з урахуванням перспектив розширення мережі, зростання обсягу оброблюваних даних та збільшення кількості користувачів. Повинна бути забезпечена достатня продуктивність, надійність і резервування.

Такий підхід до вибору апаратного та програмного забезпечення дозволяє сформувати стабільну, масштабовану і захищену мережеву інфраструктуру, готову до розширення та впровадження додаткових сервісів.

1.1.4 Вимоги до документації

У рамках проєкту локальної комп'ютерної мережі передбачено формування повного пакету технічної документації, необхідної для впровадження, експлуатації та обслуговування мережевої інфраструктури. До складу документації входять:

1. Інструкції з конфігурування мережевого обладнання та серверних систем - містять покрокові алгоритми налаштування активного обладнання, мережевих інтерфейсів, служб доступу до мережі та IP-телефонії.

2. Схема логічної топології - відображає логічні зв’язки між вузлами мережі, розподіл на підмережі, реалізацію VLAN, а також маршрутизаційні зв’язки.

3. План розміщення мережевої інфраструктури на плані приміщення - включає розташування мережевих пристроїв, точок доступу, кабельних каналів та комунікаційних розеток.

4. Схема фізичної топології - демонструє фізичне з’єднання мережевих пристроїв, типи використовуваних каналів передачі даних та вузлову структуру.

5. Адресний план (таблиця IP-адресації) - містить повний перелік IP-адрес, призначених мережевим пристроям, з урахуванням статичної та динамічної адресації.

6. Інструкції з моніторингу та обслуговування мережі - описують процеси контролю працездатності мережевих вузлів, методи збору діагностичних даних та перевірки параметрів продуктивності.

Наявність зазначеної документації забезпечує ефективне впровадження, належну підтримку та можливість масштабування мережі відповідно до змін у структурі підприємства або технологічних вимогах.

1.1.5 Техніко-економічні показники

Техніко-економічні показники проєкту визначають ключові параметри, що характеризують функціональні та вартісні аспекти побудови локальної комп’ютерної мережі. Основні з них наведено нижче:

1. Базові мережеві технології – провідна передача даних за стандартом 1000Base-TX та безпровідна передача за стандартом Wi-Fi 802.11ac.

2. Тип фізичної топології – гібридна, що забезпечує гнучкість розгортання та можливість масштабування мережі.

3. Пропускна здатність ядра мережі – 1 Гбіт/с, що гарантує високу швидкість обміну даними між основними вузлами.

4. Максимальна швидкість безпровідного сегменту – до 1000 Мбіт/с (теоретичне значення відповідно до стандарту 802.11ac).

5. Загальна вартість реалізації проєкту – не перевищує 350 тис. грн, включаючи витрати на обладнання, інсталяцію та первинне налаштування.

6. Собівартість проєкту – до 250 тис. грн, що включає прямі витрати на закупівлю апаратного забезпечення та витратні матеріали.

7. Плановий прибуток – не менше 50 тис. грн, з урахуванням рентабельності реалізації послуг зі створення мережі.

Наведені показники демонструють доцільність впровадження даного проєкту з технічної точки зору, а також його економічну ефективність у межах бюджету організації.

1.1.6 Стадії та етапи розробки

Проектування є ключовим етапом створення будь-якої інженерної системи, що забезпечує її функціональність, надійність та довговічність. Належним чином спроєктована комп’ютерна мережа мінімізує ризики помилок під час монтажу та знижує ймовірність подальших доопрацювань, які, у свою чергу, потребують додаткових фінансових витрат. Це твердження в повній мірі стосується і проектування кабельної системи як невід'ємної складової інженерної інфраструктури будівлі.

Проєкт має відповідати чинним нормативним документам і стандартам, враховувати специфіку діяльності організації, перспективу її розвитку, можливе зростання кількості користувачів та зміни у внутрішній структурі підприємства.

Стадії проєктування локальної комп’ютерної мережі традиційно поділяються на три основні етапи:

1. Розроблення технічного завдання – визначення вимог до майбутньої мережі, її функціоналу та характеристик.

2. Формування робочого проєкту – створення детальної технічної документації, схем, специфікацій та планів.

3. Підготовка виконавчої документації – фіксація фактичного виконання робіт, конфігурацій та технічного стану системи.

У межах реалізації проєкту локальної мережі для інженерно-будівельної компанії «Контракт Буд» передбачено такі етапи розробки:

1. Аналіз потреб замовника та ознайомлення з вимогами до інформаційної інфраструктури підприємства.

2. Планування стадій впровадження та формування технічного завдання.

3. Вибір логічної топології мережі відповідно до сценаріїв використання.

4. Визначення фізичної топології з урахуванням особливостей приміщень та маршруту прокладання кабелів.

5. Підбір та підключення активного й пасивного мережевого обладнання.

6. Налаштування мережевих пристроїв відповідно до технічного завдання.

7. Проведення тестування мережі на фізичному рівні (перевірка кабельних з’єднань, портів, обладнання).

8. Перевірка функціональності конфігурації мережі, сервісів і служб.

9. Підготовка пакета технічної документації.

10. Розроблення інструкцій з експлуатації та адміністрування мережі.

Комплексне дотримання вказаних етапів забезпечує ефективне проєктування, впровадження та подальшу підтримку мережевої інфраструктури відповідно до сучасних вимог.

1.1.7 Порядок контролю та прийому

Завершальним етапом впровадження локальної комп’ютерної мережі є контроль якості реалізації проєкту та приймання системи в експлуатацію. Основна мета – перевірка відповідності фактично реалізованої мережі

технічному завданню, проєктній документації та вимогам до експлуатаційних характеристик.

Контроль здійснюється шляхом тестування ключових технічних параметрів мережі, зокрема:

- фізичної цілісності кабельної системи;
- відповідності пропускної здатності заявленим стандартам;
- коректності функціонування активного мережевого обладнання;
- стабільності роботи мережевих служб і сервісів.

Для виконання контрольних заходів використовуються:

- Апаратні засоби тестування – сертифікований кабельний тестер, що відповідає вимогам стандарту 1000Base-TX, та інші діагностичні пристрої;

- Програмні засоби контролю – спеціалізовані утиліти для перевірки пропускної здатності, затримок, втрат пакетів, коректної маршрутизації та роботи мережевих служб (ping, traceroute, iperf, Wireshark та ін.).

У разі виявлення невідповідностей результати тестування фіксуються, і відповідні вузли підлягають корекції або заміні. Прийомка мережі в експлуатацію здійснюється після усунення всіх недоліків, складання виконавчої документації та підписання акту прийому-передачі.

1.2 Опис компанії та характеристика «Контракт Буд»

Компанія «Контракт Буд» спеціалізується на проектуванні, будівництві та технічному обслуговуванні житлових і комерційних об'єктів. Організаційна структура підприємства включає такі основні підрозділи:

1. Відділ проектування будівель і споруд – реалізовує ключові виробничі функції компанії.

2. Відділ транспорту та логістики.

3. Бухгалтерський підрозділ.

4. Адміністративне керівництво (директор).

5. Керівники структурних підрозділів.

6. Виробничий відділ.

7. ІТ-відділ (серверна кімната).

8. Рієлторський підрозділ.

9. Відділ взаємодії з юридичними особами та підрядними організаціями.

10. Рецепція (офіс-менеджер).

Просторове розташування підрозділів представлено на кресленні «План приміщення». Також на даному кресленні наведено приблизне розташування комп'ютеризованих робочих місць. Такі дані необхідні для правильної побудови фізичної топології мережі.

Вихідні дані для проектування локальної обчислювальної мережі:

1. План офісного простору, для якого розробляється мережева інфраструктура.

2. Технічне завдання, сформоване відповідно до вимог замовника та функціональності і характеристик ЛОМ.

3. Необхідність врахування специфіки комунікаційних процесів в компаніях цієї галузі.

4. Пропускна здатність проектованої мережі має бути з резервом, достатнім для подальшого розвитку компанії.

5. Можливість масштабування мережі без радикальної перебудови інфраструктури.

6. Забезпечення надійного захисту критичних вузлів локальної мережі.

7. Гарантована стабільність та безперебійність роботи мережевого обладнання.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічної структури мережі

З огляду на вимоги до високої швидкодії, масштабованості та гнучкості інфраструктури, основа локальної обчислювальної мережі проєктується на базі технології Gigabit Ethernet, яка забезпечує швидкість передачі даних до 1 Гбіт/с та є на сьогодні одним із найпоширеніших стандартів для створення надійних дротових мереж. Цей стандарт відповідає специфікації IEEE 802.3ab для передачі по витій парі (UTP Cat5e/6).

Для реалізації бездротового сегменту обрано технологію Wi-Fi 5 згідно зі стандартом IEEE 802.11ac, яка забезпечує швидкість до 1,3 Гбіт/с (теоретично) та підтримує сучасні методи модуляції, широкий діапазон каналів (5 ГГц) і просторове мультиплексування (MIMO). Бездротовий доступ реалізується з використанням комірчастої топології, що передбачає покриття території мережею з декількох точок доступу (AP), які забезпечують безперервне з'єднання з можливістю роумінгу.

Таким чином, загальна фізична топологія мережі є гібридною, оскільки поєднує в собі провідні елементи (зіркоподібна топологія з використанням комутаторів) та бездротові компоненти (комірчаста структура).

Схема структури гібридної фізичної топології наведена на рисунку 2.1.

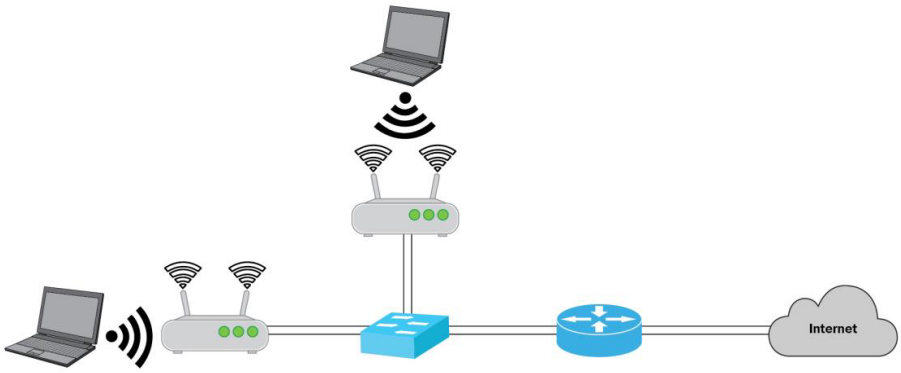


Рисунок 2.1 – Гібридна фізична топологія

Такий підхід дозволяє досягти високої продуктивності, зручності в експлуатації та подальшого розширення мережі без потреби у значних капіталовкладеннях.

Для задоволення функціональних потреб будівельної компанії в межах локальної обчислювальної мережі передбачено впровадження ряду ключових сервісів. Зокрема, планується розгортання таких служб:

Мережевий шлюз, який забезпечуватиме маршрутизацію трафіку між локальною мережею підприємства та глобальною мережею Інтернет, надаючи користувачам доступ до зовнішніх вебресурсів та сервісів.

Сервер IP-телефонії, призначений для обробки голосового трафіку за технологією VoIP (Voice over IP), що дозволить забезпечити внутрішню телефонію без потреби у фізичних телефонних лініях.

З метою підключення мобільних і безпровідних пристроїв до локальної мережі передбачається використання бездротового зв’язку за стандартом IEEE 802.11ac, який забезпечує високошвидкісну передачу даних у діапазоні 5 ГГц. Цей стандарт сумісний з IEEE 802.11n та дозволяє досягати швидкості передачі даних до 6,77 Гбіт/с при використанні технології 8x MU-MIMO, що суттєво перевищує показники попередніх стандартів.

Для кращого розуміння переваг обраного стандарту наведено короткий огляд найбільш поширених версій стандартів IEEE 802.11 [4]:

802.11a – забезпечує передачу даних зі швидкістю до 54 Мбіт/с у діапазоні 5 ГГц.

802.11b – працює в діапазоні 2,4 ГГц, підтримує швидкість до 11 Мбіт/с, широко застосовувався в попередні роки.

802.11g – також працює на частоті 2,4 ГГц, але забезпечує вищу швидкість до 54 Мбіт/с (до 108 Мбіт/с у турборежимі).

802.11n – дозволяє досягти швидкості до 300 Мбіт/с за рахунок використання множинних антен та покращених методів модуляції.

802.11ac – сучасний стандарт, що функціонує на частоті 5 ГГц, забезпечує пропускну здатність від 433 Мбіт/с до 6,77 Гбіт/с, підтримує багатокористувацьку передачу (MU-MIMO), а також відзначається нижчим енергоспоживанням, що сприяє збільшенню автономності мобільних пристроїв.

Таким чином, локальна мережа компанії «Контракт Буд» складатиметься з дротової та бездротової складових, що в сукупності забезпечать високу продуктивність, гнучкість та мобільність користувачів.

Окрім вибору фізичних засобів передачі даних, важливо також реалізувати логічну структуризацію мережі. З цією метою буде застосовано сегментацію на підмережі, яка реалізується за допомогою комутатора третього рівня. Це дозволить зменшити рівень широкомовного трафіку, підвищити безпеку, керованість та ефективність роботи мережі.

У додатку В представлено таблиці, що містять інформацію про:

- логічну адресацію в ЛОМ (локальній обчислювальній мережі), включно з IP-діапазонами для кожного сегмента;

- конфігурацію VLAN, де зазначено відповідність портів комутаторів до логічних сегментів мережі.

2.2 Розробка схеми фізичного розташування кабелів та вузлів

2.2.1 Типи кабельних з’єднань та їх прокладка

У процесі проєктування локальної обчислювальної мережі для підприємства прийнято рішення використовувати гібридну фізичну топологію, яка поєднує елементи провідної та безпровідної інфраструктури. Основу мережі становитиме топологія «Зірка», яка буде реалізована у дротовому сегменті. В межах цієї топології всі кінцеві пристрої підключаються до центрального комутатора, що забезпечує централізоване управління мережею, її масштабованість та надійність.

Для побудови провідного сегмента мережі буде застосовано вита пара категорії 6 (Cat 6). Цей тип кабелю призначений для високошвидкісної передачі даних до 10 Гбіт/с на відстані до 55 метрів та до 1 Гбіт/с на відстані до 100 метрів. Завдяки покращеному захисту від перешкод і меншому рівню внутрішніх наведень, Cat 6 є оптимальним вибором для сучасних офісних приміщень та корпоративних мереж. Кабель має розділювач пар та підвищену щільність ізоляції, що дозволяє знизити рівень перехресних завад (NEXT – Near-End Crosstalk) і забезпечити стабільну передачу трафіку при високому навантаженні.

Прокладка кабелів здійснюватиметься в кабель-каналах уздовж стін або під підвісною стелею відповідно до вимог чинних нормативних документів. У місцях з підвищеним електромагнітним фоном доцільно застосовувати екрановані варіанти кабелю (FTP або STP Cat 6), що додатково захищають мережу від зовнішніх електромагнітних завад.

Безпровідна частина локальної мережі будується за принципом комірчастої топології, яка передбачає використання точок доступу (Access Point) для обслуговування клієнтських пристроїв. Існує два основних підтипи бездротового з’єднання:

З’єднання «точка-точка» – коли пристрої з безпровідними адаптерами з’єднуються між собою безпосередньо, формуючи тимчасову однорангову мережу.

Інфраструктурне з’єднання – коли всі клієнтські пристрої з безпровідними модулями підключаються до точки доступу, яка виступає центральним вузлом для організації бездротового трафіку.

У проєктованій мережі буде реалізовано інфраструктурний тип з’єднання, що дозволяє централізовано керувати трафіком, обмежувати доступ до ресурсів мережі, впроваджувати механізми автентифікації та шифрування, а також забезпечити вищу продуктивність і безпеку порівняно з одноранговими мережами.

Таким чином, поєднання провідного сегмента на основі кабелю Cat 6 із безпровідною інфраструктурою на основі топології комірки забезпечує гнучкість, масштабованість і високу пропускну здатність локальної мережі, що повністю відповідає потребам сучасного будівельного підприємства.

2.2.2 Будова вузлів та необхідність їх застосування

Локальні обчислювальні мережі складаються з кінцевих та проміжних пристроїв, які поєднані між собою кабельною інфраструктурою.

Вузли мережі - це кінцеві та проміжні пристрої, що мають мережеві адреси. До вузлів відносяться комп'ютери з мережевими інтерфейсами, які можуть функціонувати як робочі станції, сервери або поєднувати обидві функції. Також до вузлів належать мережеві периферійні пристрої (принтери, плотери, сканери), телекомунікаційне обладнання (модеми колективного використання), а також маршрутизатори [6].

Як відомо, сегмент мережі - це сукупність вузлів, що використовують спільне середовище передачі даних.

Логічна мережа - це сукупність вузлів, які мають спільну систему адресації третього рівня моделі OSI. Прикладами таких мереж є IPX-мережі та IP-мережі. Кожна з них має власну адресу, що використовується маршрутизаторами для передачі даних між різними мережами. Одна мережа може бути поділена на підмережі, що є лише логічним розмежуванням в межах тієї ж системи адресації. Водночас мережа може складатися з кількох сегментів, і один сегмент може бути частиною декількох мереж.

У серверній кімнаті розміщено головний комутаційний вузол, який реалізовано у вигляді комутаційної шафи [12]. У цій шафі встановлено таке обладнання:

1 Центральний комутатор;

2 Безперебійний блок живлення;

3 Сервери.

4. Патч - панель

Проміжні комутаційні вузли реалізовані у вигляді комутаторів робочих груп, що встановлюються в межах окремих відділів і монтуються на стінах. Крім того, у деяких підрозділах буде розміщено безпровідні маршрутизатори, які також монтуватимуться на стінах біля електричних розеток.

2.3 Обґрунтування вибору комунікаційного обладнання

Для забезпечення належного функціонування локальної мережі компанії особливу увагу приділено вибору активного мережевого обладнання, зокрема комутаторів, серверів та точки доступу. Точка доступу забезпечує роботу безпровідних сегментів мережі.

Безпровідні ділянки мережі проєктуються з використанням точок доступу, що відповідають сучасному стандарту IEEE 802.11ac. У таблиці «Порівняльна характеристика точок доступу» (додаток Г) наведено технічні характеристики декількох моделей точок доступу для порівняння та вибору оптимального варіанту відповідно до вимог проєкту.

Основним призначенням точок доступу в структурі локальної мережі є забезпечення підключення мобільних користувачів та пристроїв до мережевої інфраструктури компанії. В межах даного проєкту для реалізації безпровідного доступу було обрано точку доступу TRENDnet AC1200, яка відповідає вимогам щодо пропускної здатності, стабільності та зони покриття.

Зовнішній вигляд вибраної моделі представлено на рисунку 2.2

Рисунок 2.2 – Точка доступу фірми TredNET моделі AC1200

Центральний комутатор виконує ключову роль у структурі локальної обчислювальної мережі, оскільки саме він забезпечує інтеграцію всіх сегментів мережі в єдину інфраструктуру. Через нього здійснюється передача міжсегментного трафіку, а також маршрутизація даних до та з глобальної мережі Інтернет.

У таблиці «Порівняльна характеристика комутаторів» (додаток Г) наведено аналіз технічних характеристик декількох моделей комутаторів, які можуть бути використані як центральний елемент мережі. Порівняння виконано з урахуванням вимог до пропускної здатності, підтримки віртуальних локальних мереж (VLAN), кількості портів та функцій управління.

За результатами аналізу для реалізації центрального вузла локальної мережі було обрано модель Edge-Core ES4610, яка відповідає технічним та експлуатаційним вимогам проєкту. Зовнішній вигляд вибраного комутатора представлено на рисунку 2.3 [15].

.

Рисунок 2.3 – Комутатор фірми Edge-Core моделі ES4610

Комутатор сегменту мережі виконує функцію об’єднання персональних комп’ютерів певного підрозділу в єдину мережеву групу. Основні вимоги до комутатора для такого сегменту включають:

Підтримку швидкості передачі даних до 1000 Мбіт/с.

Наявність восьми портів для підключення пристроїв.

Відповідність стандартам IEEE 802.3, IEEE 802.3u, IEEE 802.3x та IEEE 802.3ab.

Забезпечення автоматичного узгодження швидкості роботи портів (автоузгодження).

У додатку Г, у таблиці «Порівняння технічних характеристик комутаторів», наведено аналіз різних моделей комутаторів, які можна використовувати для робочих груп. Для цієї мережі обрано чотири пристрої TP-Link TL-SG3210, приклад яких наведено на рисунку 2.4 [11].

Рисунок 2.4 - TP-Link моделі TL-SG3216

Для локальної обчислювальної мережі також планується використання 16-портової версії комутатора TP-Link TL-SG3216.

У додатку Г у таблиці «Порівняння апаратних конфігурацій серверів» наведено порівняльний аналіз серверного обладнання від різних виробників. В якості серверної платформи обрано систему ARTLINE Business R33 v01. Зовнішній вигляд обраного сервера представлено на рисунку 2.5.

Рисунок 2.5 – Сервер ARTLINE Business R33 v01

Переваги сервера ARTLINE Business R33 v01:

1. Висока продуктивність завдяки сучасним процесорам і великому об’єму оперативної пам’яті, що забезпечує швидку обробку великих обсягів даних.

2. Надійність і стабільність роботи в цілодобовому режимі, що є критично важливим для корпоративних мереж.

3. Розширені можливості масштабування - підтримка додаткових модулів пам’яті, накопичувачів та інших компонентів.

4. Ефективна система охолодження, що забезпечує оптимальний тепловий режим і подовжує термін служби обладнання.

5. Підтримка сучасних стандартів безпеки та резервного копіювання для захисту даних.

6. Компактний дизайн, що дозволяє зручно інтегрувати сервер у існуючу інфраструктуру.

В таблиці 2.1 зведено обладнання, яке необхідне для проекту мережі.

Таблиця 2.1 – Пасивне та активне мережеве обладнання та сервери

№ п/п	Назва елементу	Модель	Од. вим.	К-ть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6	7
1	Серверно-комутаторна шафа	ШС-24U	шт	1	11480	11480
2	Патчпанель	24 порти, кат. 6 UTP	шт	1	1750	1750
3	Розетка RJ-45	E-Server сфе 6	шт	43	90	3870
4	Кабель-канали (різного січення)	-	м	90	63	5670
5	Вита пара	UTP кат. 6	м	500	15	7500
6	Патчкорд	UTP кат. 6	шт	80	21	1680
7	Джерело живлення (ДБЖ)	APC Smart-UPS RS 1100	шт	1	17800	17800
8	Швидкомонтажний дюбель	-	шт	200	1,2	240
9	Кріпильні шуруп	-	шт	200	1,3	260
10	Тримачі для кабелів	-	шт	4	240	960
11	Головний комутатор	Edge-Core ES4610	шт	1	12100	12100
12	Комутатор сегменту мережі	TP-Link TL-SG3216	шт	1	3300	3300
13	Комутатор сегменту	TP-Link TL-SG3210	шт	4	2900	11600
14	Серверне обладнання	ARTLINE Business R33 v01	шт	2	31000	62000
15	Точка доступу	TredNET AC1200	шт	1	2300	2300
Всього, грн.						142510

Програмне забезпечення для серверів надається безкоштовно, тому його вартість не включена у матеріальні витрати. Операційні системи для робочих станцій були закуплені разом із комп'ютерним обладнанням.

2.4 Особливості монтажу мережі

Кабельна інфраструктура локальної мережі буде побудована з використанням неекранованої витої пари категорії 6, що забезпечує високу швидкість передачі даних і стабільність роботи мережі. Важливим етапом є ретельне планування схеми розміщення пасивного мережевого обладнання, яке включає патчпанелі, розетки та кабельні канали.

Для ефективного функціонування мережі необхідно визначити оптимальні місця розташування центрального комутаційного вузла, а також проміжних комутаторів у разі потреби сегментації мережі на декілька частин.

Зазначається, що максимальна довжина кабельного з'єднання між комутатором і робочою станцією не повинна перевищувати 100 метрів. В ідеалі рекомендується утримувати довжину кабелю на рівні близько 90 метрів, щоб забезпечити надійне підключення мережевої розетки біля робочого місця.

Якщо відстань між двома мережевими вузлами, з'єднаними витою парою, перевищує 100 метрів, сигнал може деградувати і ставати спотвореним. Це залежить від якості кабелю та відповідності його параметрів стандартам категорії 6.

Тому важливо прокладати кабелі відповідно до встановлених норм і рекомендацій, а також встановлювати комутатори поблизу джерел живлення для зручності монтажу та обслуговування.

Для акуратного та безпечного прокладання кабелів будуть застосовуватись спеціальні кабельні короби і кріплення, які забезпечують захист кабелю від механічних пошкоджень, зручність монтажу та можливість

подальшого розширення мережі. Такий підхід сприяє підтримці високої якості сигналу і довговічності мережевої інфраструктури.

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

Для локальної мережі компанії було обране програмне забезпечення, яке максимально відповідає потребам користувачів і забезпечує стабільну та ефективну роботу всієї інфраструктури.

1. Операційна система для робочих станцій - Windows 10 Professional. Ця версія ОС є популярним і широко використовуваним рішенням у корпоративному секторі завдяки інтуїтивному інтерфейсу, широкій сумісності з різноманітним програмним забезпеченням і розвиненій системі підтримки. Ліцензії на Windows 10 Pro були придбані разом із комп'ютерним обладнанням, що гарантує легальність використання та доступ до офіційних оновлень і технічної підтримки від Microsoft. Вибір саме цієї ОС базується на тому, що більшість прикладних програм, необхідних для щоденної роботи співробітників будівельної компанії, розроблені під платформу Windows. Це забезпечує сумісність і стабільність у роботі, знижуючи ризики збоїв і проблем сумісності.

2. Операційна система для серверів - FreeBSD 13 amd64. FreeBSD - це потужна, надійна і масштабована UNIX-подібна операційна система, яка відома своєю стабільністю та високим рівнем безпеки. Вона підтримує широкий набір мережевих сервісів і має відкритий код, що дозволяє безкоштовно використовувати її без необхідності купувати дорогі ліцензії. Використання FreeBSD на серверній частині мережі обумовлено її здатністю ефективно управляти мережевим трафіком, надавати необхідні сервіси, а також підтримувати складні конфігурації для корпоративного середовища. Завдяки своїй модульній архітектурі та надійним механізмам безпеки, FreeBSD є

оптимальним вибором для забезпечення стабільної роботи серверів, а також їх масштабування в майбутньому.

Загалом, поєднання Windows 10 Professional на робочих станціях і FreeBSD на серверах дозволяє створити збалансовану систему, що поєднує зручність і знайомий інтерфейс для користувачів із надійністю та функціональністю серверної інфраструктури. Це сприяє підвищенню продуктивності роботи співробітників і забезпечує стабільну роботу всієї локальної мережі компанії.

2.6 Обґрунтування вибору засобів захисту мережі

Для забезпечення безпеки локальної обчислювальної мережі (ЛОМ) буде застосовано міжмережевий екран (файрвол) ipfirewall. Цей інструмент дозволяє здійснювати ефективний контроль та фільтрацію мережевого трафіку, а також збирати статистику передачі даних на основі заданих критеріїв.

Основні функціональні можливості ipfirewall включають:

- Фільтрацію трафіку на різних рівнях моделі OSI, зокрема на мережевому, канальному та транспортному рівнях, що дозволяє забезпечити гнучкий контроль доступу та безпеку.

- Підтримку технологій трансляції мережевих адрес (NAT), таких як SNAT (Source NAT) і DNAT (Destination NAT), що забезпечує приховування внутрішніх IP-адрес і перенаправлення трафіку.

- Пріоритизацію мережевого трафіку з використанням алгоритмів керування чергами, таких як Class-Based Queuing (CBQ) та Hierarchical Token Bucket (HTB), що допомагає оптимізувати пропускну здатність мережі і гарантувати якість обслуговування (QoS).

- Маркування пакетів із подальшою маршрутизацією на основі заданих правил, що сприяє більш ефективному управлінню потоками даних та забезпеченню безперебійної роботи мережі.

Застосування ipfirewall у проекті дозволить надійно захистити локальну мережу від несанкціонованого доступу, а також оптимізувати передачу даних відповідно до пріоритетів компанії.

2.7 Тестування та налагодження мережі

Тестування локальної мережі є невід'ємною та ключовою складовою процесу її проектування, впровадження та подальшої експлуатації. Воно дозволяє не лише підтвердити відповідність мережі технічним вимогам і специфікаціям, а й своєчасно виявити та усунути потенційні помилки чи недоліки у налаштуванні мережевого обладнання, що можуть негативно впливати на продуктивність та надійність роботи мережі.

Особлива увага приділяється тестуванню обох сегментів локальної мережі - провідного та безпровідного. Провідна частина перевіряється на цілісність кабельної системи, якість з'єднань, відповідність стандартам передачі даних (наприклад, перевірка швидкості та стабільності сигналу по кабелю категорії 6), а також працездатність комутаторів і маршрутизаторів. Безпровідна частина тестується на стабільність з'єднання, рівень сигналу, пропускну здатність, а також на можливість одночасного обслуговування необхідної кількості користувачів без втрати якості.

Для якісного тестування використовуються спеціалізовані апаратні засоби - тестові набори, які дозволяють імітувати різні типи мережевого навантаження, перевірити роботу мережевих портів та визначити помилки передачі. Крім того, застосовуються програмні засоби - тестові програми, які аналізують трафік, проводять діагностику мережевих протоколів та виявляють проблемні ділянки у мережі.

Детальні інструкції щодо вибору, налаштування та використання таких інструментів викладені у розділі 3.2 «Інструкції з використання тестових наборів та тестових програм», що допоможе фахівцям максимально ефективно

організувати процес тестування та забезпечити високу якість роботи локальної мережі.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з інсталяції і налаштування ПЗ серверів

3.1.1 Інструкції з налаштування сервера S2

У цьому розділі розглядається принцип побудови правил для фільтрації IP-трафіку на сервері, що працює під керуванням операційної системи FreeBSD. Сервер виконує функцію міжмережевого екрану (файрвола) із використанням ipfw - вбудованого інструменту для контролю та фільтрації мережевого трафіку.

Для початку конфігурації необхідно вказати основні параметри у файлі /etc/rc.conf, який відповідає за запуск системних служб під час старту ОС. Тут потрібно активувати маршрутизацію (gateway_enable="yes"), увімкнути файрвол (firewall_enable="yes") та вказати шлях до скрипта з правилами фільтрації (firewall_script="/etc/rc.ipfw"). Також активується ведення логів файрвола (firewall_logging="yes") і запуск демона NAT (natd_enable="yes"), який відповідає за трансляцію мережевих адрес для виходу у зовнішню мережу. Вказуються параметри запуску NAT через /sbin/natd з конфігураційним файлом /etc/natd.conf.

Основний скрипт налаштування файрвола починається з оголошення змінних, які описують внутрішній (int_if) та зовнішній (ext_if) мережеві інтерфейси, IP-адреси інтерфейсів, а також локальну мережу та зовнішню підмережу. Окрім того, визначається діапазон динамічних портів (uports), який використовуватиметься для встановлення з’єднань.

Далі встановлюються правила доступу до мережевих сервісів. Зазначається, які протоколи будуть доступні для користувачів локальної мережі (наприклад, HTTP, HTTPS, POP3, SMTP), а які - для привілейованих користувачів, котрі отримують розширені права (FTP, SSH, ICQ).

Для коректної роботи файрвола вводяться змінні зі списками дозволених сервісів, які автоматично конвертуються у відповідні порти за допомогою стандартного файлу /etc/services.

У початковій частині скрипту описуються базові правила. Зокрема, всі пакети, які проходять через локальний інтерфейс lo0, пропускаються без обмежень, що забезпечує нормальну роботу локальних процесів. Водночас забороняється доступ до адрес локального хоста (127.0.0.0/8) ззовні, що виключає можливість підробки пакетів із цієї мережі.

Для захисту від атак, пов’язаних із підміною IP-адрес (spoofing), додаються правила, які блокують трафік із приватних IP-діапазонів, що надходить на зовнішній інтерфейс. Це дозволяє запобігти проникненню недозволених пакетів у мережу.

Наступні правила визначають дозволений трафік між внутрішньою мережею та зовнішнім світом: зокрема, пропускається весь трафік, що йде із локальної мережі в будь-якому напрямку, а також дозволяється зворотній трафік на локальну мережу.

Для реалізації NAT використовується механізм divert, який спрямовує відповідний трафік до демона natd. Це дозволяє багатьом пристроям локальної мережі одночасно використовувати один зовнішній IP для виходу в Інтернет.

Для активації налаштувань потрібно запустити скрипт командою /bin/sh /etc/rc.ipfw. Цей скрипт містить повний набір правил, які забезпечують захист локальної мережі від несанкціонованого доступу, а також організовують спільний вихід у мережу Інтернет.

3.1.2 Інструкції з налаштування сервера S1

Asterisk - це програмна телефонна станція (АТС), яка забезпечує передачу голосового і відео зв’язку через IP-мережі. Вона є популярним рішенням для організації корпоративної IP-телефонії завдяки своїй гнучкості та широкому

функціоналу. Для початку налаштування системи IP-телефонії на базі Asterisk необхідно виділити окремий сервер і встановити на нього операційну систему FreeBSD, яка забезпечить стабільність і надійність роботи.

Сервер Asterisk може бути інтегрований у різні схеми мережі - як у складі локальної мережі, так і в більш складних конфігураціях з доступом до Інтернету для зовнішніх дзвінків. Це дозволяє масштабувати систему та налаштовувати її під потреби конкретної організації.

Для початку роботи з Asterisk потрібно налаштувати конфігураційні файли, які визначають доступ до системи та функції веб-інтерфейсу. Файл /etc/asterisk/manager.conf містить налаштування для менеджерського інтерфейсу, який дозволяє адмініструвати систему дистанційно. У цьому файлі необхідно активувати підтримку веб-інтерфейсу, встановивши параметри enabled = yes та webenabled = yes. Далі додається користувач із необхідними правами, наприклад, користувач Administrator, для якого задається пароль (secret) та визначаються права читання і запису для різних розділів системи, таких як керування системою, журналами, викликами, користувачами, конфігурацією тощо.

Наступним кроком є налаштування веб-сервера Asterisk у файлі /etc/asterisk/http.conf. Тут визначається, чи буде веб-сервер активований (enabled = yes), чи будуть доступні статичні файли (enablestatic = yes), а також вказується IP-адреса та порт, на яких веб-сервер буде слухати запити. У наведеному прикладі сервер працює локально на інтерфейсі 127.0.0.1.

Після внесення змін необхідно перевірити коректність конфігурації за допомогою утиліти checkconfig, яка аналізує синтаксис та можливі помилки у файлах налаштувань. Для коректної роботи веб-інтерфейсу створюється символічне посилання (ln -s), яке вказує на каталог зі статичними файлами Asterisk. Це дозволяє системі правильно знаходити необхідні ресурси для відображення інтерфейсу.

Також важливо встановити відповідні права на запис у каталог /usr/share/asterisk/static-http/config, щоб забезпечити можливість збереження конфігурацій та змін, зроблених через веб-інтерфейс.

Після завершення налаштувань сервер Asterisk необхідно перезапустити командою /etc/init.d/asterisk restart, щоб застосувати зміни.

Веб-інтерфейс управління Asterisk PBX стає доступним за адресою у браузері за форматом:

http://IP-адреса_сервера:8088/asterisk/static/config/index.html

Тут адміністратор може керувати налаштуваннями АТС, створювати правила маршрутизації дзвінків (DialPlan) та додавати користувачів системи.

Для повноцінної роботи IP-телефонії необхідно створити хоча б один DialPlan - це набір правил, які визначають логіку маршрутизації дзвінків, та зареєструвати кількох користувачів (Users), які зможуть здійснювати та приймати дзвінки.

Таким чином, налаштування Asterisk включає підготовку операційної системи, конфігурацію менеджерського та веб-інтерфейсів, організацію правил маршрутизації дзвінків і створення облікових записів користувачів. Цей підхід забезпечує гнучкість, безпеку та ефективність у роботі корпоративної IP-телефонії.

Розробимо приклад конфігурації Asterisk для сервера з IP 192.168.28.201

1. Налаштування менеджерського інтерфейсу (/etc/asterisk/manager.conf):

```
[general]
enabled = yes              ; Активуємо менеджерський інтерфейс
webenabled = yes           ; Дозволяємо доступ через веб
[Administrator]
secret = YourStrongPassword ; Встановлюємо пароль для адміністратора
read = system,call,log,verbose,command,agent,user,config  ; Права на читання
write = system,call,log,verbose,command,agent,user,config ; Права на запис
```

2. Налаштування HTTP-сервера Asterisk (/etc/asterisk/http.conf):

[general]

enabled = yes ; Вмикаємо HTTP-сервер Asterisk

enablestatic = yes ; Дозволяємо статичні файли

bindaddr = 192.168.28.201 ; Вказуємо IP-адресу сервера

bindport = 8088 ; Порт, на якому працюватиме веб-інтерфейс

3. Створення символічного посилання для статичних файлів:

sudo ln -s /var/lib/asterisk/static-http /usr/share/asterisk

sudo chmod -R u+w /usr/share/asterisk/static-http/config

4. Перезапуск служби Asterisk для застосування налаштувань:

sudo /etc/init.d/asterisk restart

5. Приклад базового DialPlan (/etc/asterisk/extensions.conf):

[general]

static = yes

writeprotect = no

6. Приклад створення користувача SIP (`/etc/asterisk/sip.conf`):

[default]

exten => 1000,1,Answer() ; Відповідаємо на дзвінок на внутрішній номер 1000

exten => 1000,n,Playback(hello-world) ; Відтворюємо вітальне повідомлення

exten => 1000,n,Hangup() ; Завершуємо дзвінок

exten => 2000,1,Dial(SIP/2000,20) ; Дзвінок на користувача SIP з номером 2000 з таймаутом 20 секунд

exten => 2000,n,Voicemail(2000@default,u) ; Якщо не відповідає, перекидаємо на голосову пошту

exten => 2000,n,Hangup()

6. Приклад створення користувача SIP (/etc/asterisk/sip.conf):

[general]

context=default

allowguest=no

srvlookup=yes

udpbindaddr=0.0.0.0

[2000]

type=friend

host=dynamic

secret=User2000Pass

context=default

disallow=all

allow=ulaw

callerid="User 2000" <2000>

Отже цими скриптами:

- Встановлено і активовано веб-інтерфейс Asterisk з IP 192.168.28.201.
- Забезпечено базове управління через менеджерський інтерфейс.
- Налаштований простий DialPlan для тестових дзвінків.
- Створено базового SIP-користувача.

Ця конфігурація є стартовою та легко розширюється для більш складних сценаріїв IP-телефонії.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкція з налаштування Wi-Fi точки доступу

Налаштування точки доступу складається з таких основних кроків:

1. Встановлення параметрів ідентифікації точки доступу.
2. Конфігурування параметрів безпеки точки доступу.
3. Налаштування локального мережевого інтерфейсу.
4. Конфігурація безпровідного мережевого інтерфейсу.
5. Встановлення інших параметрів роботи точки доступу, таких як дата, час тощо.

Перед початком налаштування потрібно увійти в інтерфейс керування точкою доступу, використовуючи рекомендовані в документації параметри. В нашому випадку IP-адреса точки доступу – 192.168.33.200, маска підмережі – 255.255.255.0. Логін за замовчуванням – admin, пароль відсутній.

На першому етапі ідентифікації необхідно вказати параметр Wireless Network Name (SSID). Для кожної безпровідної групи користувачів буде використано окреме ім’я мережі. Цю настройку виконують у розділі Setup → Wireless Network.

Безпека точки доступу включає зміну пароля для входу в панель управління, що робиться у розділі Maintenance, де спочатку вказується старий пароль, а потім новий. Конфігурація протоколу шифрування безпровідного трафіку виконується у розділі Setup → Wireless Network.

Технологія WPA (Wi-Fi Protected Access) - це стандарт шифрування для бездротових мереж, що значно покращує безпеку порівняно з WEP. WPA забезпечує захист доступу до мережі через використання протоколу EAP (Extensible Authentication Protocol), а також надійне шифрування переданих даних. WPA призначена для роботи із сервером автентифікації 802.1X, який видає унікальні ключі кожному користувачу. Водночас вона може працювати у спрощеному режимі «Pre-Shared Key» (PSK), що використовується у домашніх мережах та невеликих офісах, де всі користувачі мають один спільний пароль. Режим WPA-PSK, також відомий як WPA-Personal, дозволяє обмінюватися даними з точкою доступу за допомогою методів шифрування TKIP або AES. Приклад налаштування протоколу WPA-PSK наведено на рисунку 3.1.

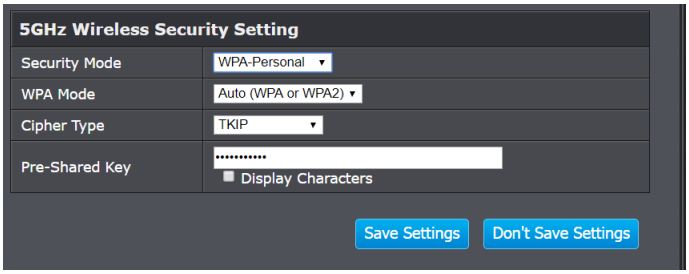


Рисунок 3.1 - Параметри шифрування WPA-PSK

Перейдемо до конфігурування локального мережевого інтерфейсу, яке здійснюється в меню Setup → Lan Setup.

Для інтерфейсів точки доступу застосовуватиметься статична IP-адресація. Інтерфейсу точки доступу буде призначено IP-адресу відповідно до даних, наведених у додатку «Таблиця IP-адресації».

Приклад присвоєння IP-адреси наведено на рисунку 3.2.

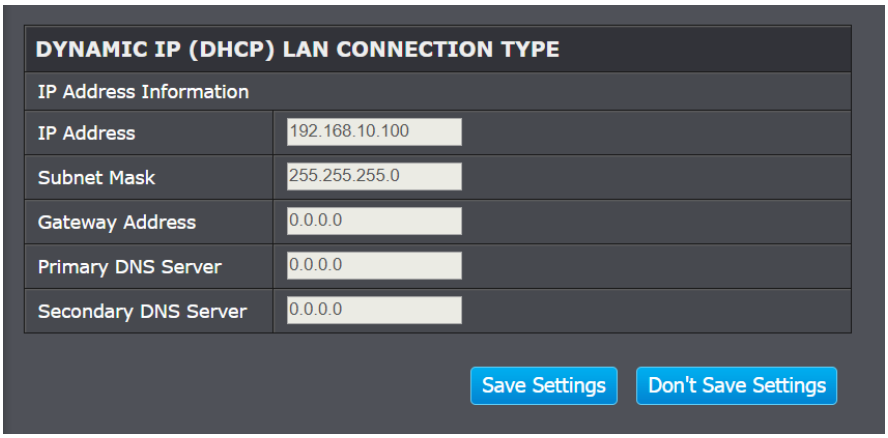


Рисунок 3.2 - Внесення IP-адреси точки

Перейдемо до конфігурування бездротового інтерфейсу точки доступу, яке здійснюється в розділі Setup → Wireless Network Settings, як продемонстровано на рисунку 3.3.

Необхідно також вибрати режим роботи точки доступу - Access Point. У цьому режимі пристрій функціонує як центральна точка бездротової мережі, яка приймає підключення від клієнтських пристроїв (ноутбуків, смартфонів, планшетів тощо) та забезпечує їм доступ до локальної мережі та Інтернету. Точка доступу в режимі Access Point відповідає за передачу даних між бездротовими клієнтами та дротовою мережею, виконує функції управління бездротовим зв'язком і організовує ефективне розподілення радіочастотного спектру. Цей режим є основним для створення бездротових мереж у домашніх, офісних та громадських середовищах.

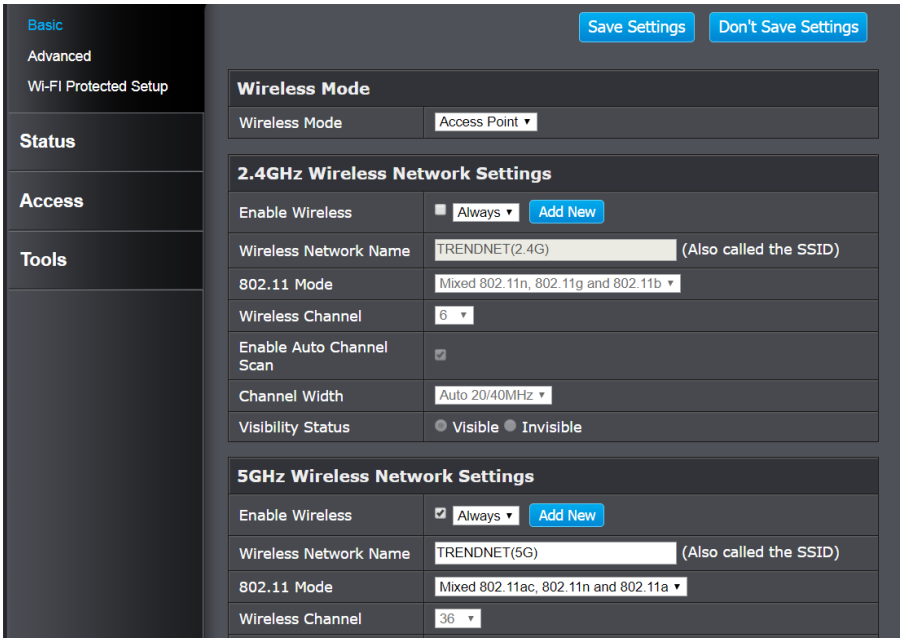


Рисунок 3.3 - Параметри Wireless інтерфейсу

3.2.2 Налаштування центрального комутатора

За допомогою функціоналу операційної системи основного комутатора мережа поділяється на окремі сегменти, кожен з яких міститиме комутатор робочої групи. Дані для конфігурування беруться з таблиці IP-адрес. Такий поділ дозволяє ізолювати трафік кожної робочої групи в межах свого сегменту.

Приклад налаштування сегменту для серверів:

Switch> enable

Switch# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# interface range Gi0/1 - 2

Switch(config-if-range)# switchport access vlan 24

% VLAN 24 створиться автоматично, оскільки вона була відсутня

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# exit

Switch(config)# interface vlan 24

Switch(config-if)# ip address 192.168.24.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Подібним чином налаштовуємо VLAN 25:

Switch(config)# interface Gi0/3

Switch(config-if)# switchport access vlan 25

% VLAN 25 створено автоматично

Switch(config-if)# switchport mode access

Switch(config-if)# exit

Switch(config)# interface vlan 25

Switch(config-if)# ip address 192.168.25.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Далі створюємо VLAN 26:

Switch(config)# interface Gi0/4

Switch(config-if)# switchport access vlan 26

% VLAN 26 створено автоматично

Switch(config-if)# switchport mode access

Switch(config-if)# exit

Switch(config)# interface vlan 26

Switch(config-if)# ip address 192.168.26.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Налаштовуємо VLAN 27:

Switch(config)# interface Gi0/5

Switch(config-if)# switchport access vlan 27

% VLAN 27 створено автоматично

Switch(config-if)# switchport mode access

Switch(config-if)# exit

Switch(config)# interface vlan 27

Switch(config-if)# ip address 192.168.27.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Конфігуруємо VLAN 28 для інтерфейсів Gi0/6 до Gi0/9:

Switch(config)# interface range Gi0/6 - 9

Switch(config-if-range)# switchport access vlan 28

% VLAN 28 створено автоматично

Switch(config-if-range)# switchport mode access

Switch(config-if-range)# exit

Switch(config)# interface vlan 28

Switch(config-if)# ip address 192.168.28.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Аналогічно налаштовуємо VLAN 33:

Switch(config)# interface Gi0/10

Switch(config-if)# switchport access vlan 33

% VLAN 33 створено автоматично

Switch(config-if)# switchport mode access

Switch(config-if)# exit

Switch(config)# interface vlan 33

Switch(config-if)# ip address 192.168.33.254 255.255.255.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Після чого налаштовуємо VLAN 21, 22, 23, 29, 30, 31, 32 за аналогією, призначаючи відповідні IP-адреси.

Далі конфігуруємо транкові порти на інтерфейсах Gi0/11 до Gi0/15:

Switch(config)# interface range Gi0/11 - 15

Switch(config-if-range)# switchport mode trunk

Switch(config-if-range)# exit

Активуємо маршрутизацію між VLAN-інтерфейсами на комутаторі рівня 3:

Switch(config)# ip routing

І насамкінець встановлюємо маршрут за замовчуванням, який вказує шлюз у мережі:

Switch(config)# ip route 0.0.0.0 0.0.0.0 192.168.28.200

3.2.3 Інструкції з налаштування комутаторів робочих груп

Для налаштування VLAN відповідно до стандарту IEEE 802.1Q на комутаторах TP-Link TL-SG3210 та TL-SG3216 застосовується аналогічний підхід. Послідовність дій виглядає наступним чином:

Спершу необхідно створити потрібні VLAN-и на пристрої:

switch(config)# vlan 21

Після створення VLAN слід присвоїти йому зрозуміле ім’я, що полегшує ідентифікацію

switch(config-vlan)# name group1

Порти, які мають належати до певної віртуальної мережі, налаштовуються в режим access та асоціюються з відповідним VLAN:

switch(config)# interface gigabitEthernet 1/0/3

switch(config-if)# switchport mode access

switch(config-if)# switchport access vlan 21

Для з’єднання з іншими комутаторами або обладнанням, що підтримує VLAN, один із портів налаштовується у режим trunk, який дозволяє передавати трафік кількох VLAN:

switch(config)# interface gigabitEthernet 1/0/1

switch(config-if)# switchport mode trunk

Налаштування VLAN на комутаторах TP-Link TL-SG3210 та TL-SG3216 передбачає створення віртуальних мереж, присвоєння їм імен, а також налаштування портів у відповідні режими - access для підключення кінцевих

пристроїв та trunk для передачі трафіку кількох VLAN. Це дозволяє ефективно сегментувати мережу та забезпечити її структурованість і безпеку.

3.3 Інструкції з використання тестових наборів та тестових програм

Для перевірки фізичних характеристик мережі стандарту Gigabit Ethernet використовують спеціалізований прилад Fluke Networks LRPRO-2000, який дозволяє оцінити якість кабельних з’єднань та виявити можливі несправності або перешкоди.

Поряд з апаратними засобами, для тестування мережі широко застосовують стандартні програмні утиліти операційної системи Windows, зокрема ipconfig та ping, які допомагають перевірити конфігурацію мережевого інтерфейсу та встановити зв’язок з іншими вузлами мережі.

Для коректної перевірки підключення Microsoft рекомендує виконувати наступні кроки:

Запуск команди ipconfig для отримання основних параметрів мережевого інтерфейсу: IP-адреси, маски підмережі, шлюзу за замовчуванням і адреси DNS-сервера. Це дозволяє переконатися, що комп’ютер отримав коректні налаштування.

Перевірка роботи мережевого стеку локальної машини за допомогою команди ping 127.0.0.1 (локальний цикл). Якщо цей тест не проходить, це свідчить про проблеми з драйверами або налаштуваннями мережевого адаптера.

Тестування зв’язку з шлюзом за замовчуванням, виконавши ping [IP-шлюзу]. Якщо відгук відсутній, потрібно перевірити правильність IP-адреси шлюзу та його доступність.

При повторній невдачі варто перевірити IP-адресу віддаленого вузла, а також працездатність усіх маршрутизаторів між локальним комп’ютером і віддаленим пристроєм.

Оцінка зв’язку з DNS-сервером через команду ping [IP DNS]. У разі відсутності відповіді необхідно перевірити правильність конфігурації DNS та роботу проміжних вузлів.

Для визначення фактичної пропускної здатності мережі, тобто реальної швидкості передачі та прийому даних між двома точками, застосовується утиліта iperf. Вона є простою у використанні та дає точні результати за умови дотримання певних рекомендацій:

Вимкнути або припинити роботу всіх програм, що активно використовують мережу, щоб уникнути спотворень у вимірах.

Обмежити запуск фонового програмного забезпечення, яке може споживати системні ресурси.

Переконатися, що необхідні мережеві порти відкриті та не блокуються між клієнтом і сервером.

Задокументувати отримані показники для подальшого аналізу.

Запуск iperf у режимі сервера здійснюється командою: iperf -s -p 80,

де -s - означає серверний режим, а -p 80 - порт, що використовується.

Для тестування UDP-трафіку додають параметр

-u: iperf -s -u -p 80.

Клієнтська частина запускається так:

iperf -c 172.16.12.1 -p 80 -t 180,

де -c - режим клієнта, 172.16.12.1 - IP сервера, а -t 180 - тривалість тесту у секундах.

Повний перелік параметрів утиліти iperf наведено у додатку Д.

Для аналізу бездротових мереж використовуються спеціалізовані програми, такі як WifiAnalyzer та inSSIDer. Вони дозволяють визначити рівень сигналу до точки доступу, швидкість бездротового каналу, а також переглянути список активних каналів Wi-Fi. Цей аналіз важливий для виявлення прихованих

або конкурентних точок доступу, які працюють на тих же каналах, що може спричиняти перешкоди і знижувати якість зв’язку.

Крім вищеназваних інструментів, в операційній системі доступний широкий набір команд для діагностики мережі:

PING - перевірка доступності вузлів та перевірка працездатності aspbxyjuj з’єднання.

Telnet - забезпечує можливість віддаленого керування через емуляцію терміналу.

Remote Shell (RSH) - дозволяє запускати команди на віддаленому Unix-хості.

Remote Execution (REXEC) - виконує процеси на віддаленому комп’ютері.

ARP - відображає таблицю відповідностей IP-адрес і MAC-адрес у локальній мережі.

IPCONFIG - показує поточні мережеві налаштування.

NBTSTAT - виводить інформацію про NETBIOS імена і їх відповідність IP.

NETSTAT - надає відомості про поточні мережеві з’єднання.

ROUTE - відображає і дозволяє змінювати таблицю маршрутизації.

HOSTNAME - показує ім’я локального комп’ютера.

У Linux-системах для перегляду апаратної конфігурації широко використовуються такі команди:

lspci - виводить список всіх пристроїв, підключених до PCI-шини.

lshw - надає детальну інформацію про апаратне забезпечення.

lsusb - показує пристрої, підключені через USB.

Для моніторингу системних процесів використовується команда top, яка в режимі реального часу відображає інформацію про активність процесів, завантаження процесора, пам’яті та інші параметри, оновлюючи дані через задані інтервали.

На рисунку 3.4 наведено приклад головного вікна програми top, що ілюструє роботу моніторингу системи.

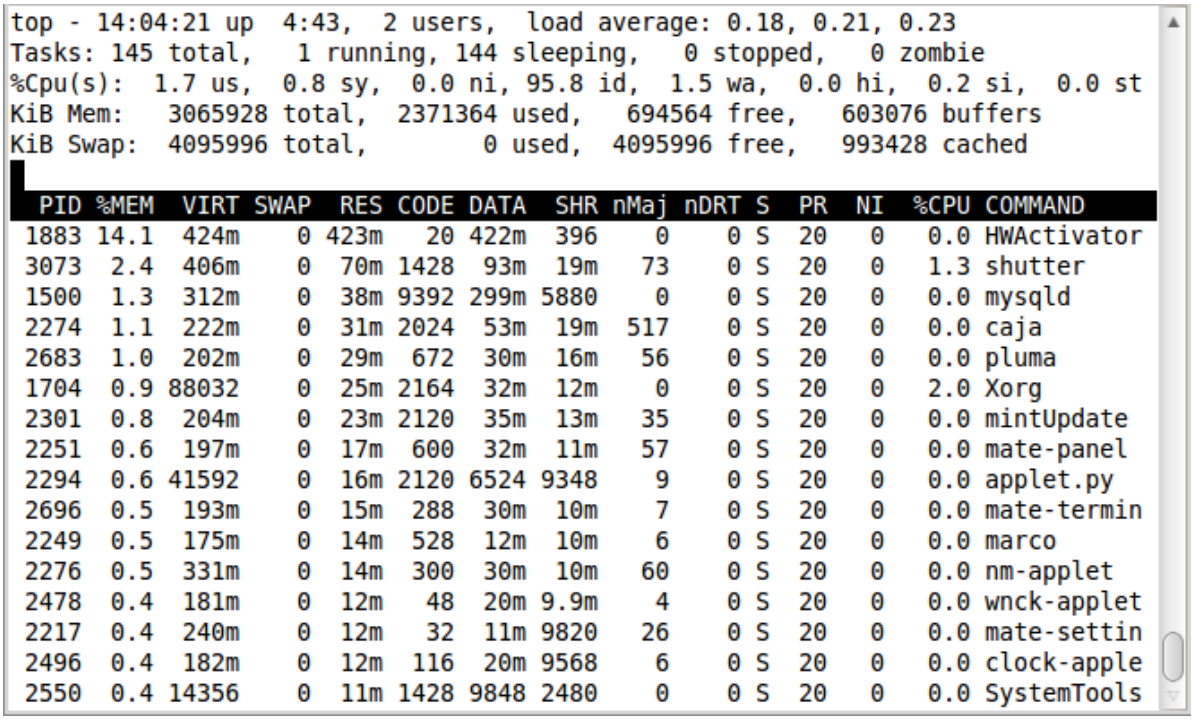


Рисунок 3.4 – Результати роботи команди top в Linux

Для кожного процесу відображаються: PID (ідентифікатор процесу), користувач, під чиїм іменем він запущений, пріоритет, відсоток використання процесора і пам’яті, час виконання, команда (ім’я процесу).

Цей список оновлюється в реальному часі, що дозволяє виявляти найбільш ресурсомісткі процеси.

Таким чином, команда top є незамінним інструментом для адміністраторів і користувачів, які хочуть оперативно оцінити стан системи, виявити проблеми з продуктивністю, а також керувати активними процесами.

Утиліта vmstat використовується для моніторингу активності системи, дає інформацію про стан апаратних ресурсів та роботу операційної системи. Команда vmstat генерує звіт про процеси, пам’ять, swap-простір, поблочне введення/виведення, переривання та навантаження на процесор.

Для отримання статистики використання пам’яті можна виконати команду:

vmstat –m

яка показує обсяг використаної пам’яті по модулях.

Для отримання інформації про активність і неактивність сторінок пам’яті слід використати:

vmstat –a

що дозволяє аналізувати, які сторінки пам’яті активно використовуються, а які ні.

Команда uptime показує, як довго система працює без перезавантаження. Це корисно для оцінки стабільності роботи сервера або комп’ютера.

Команда ps використовується для виводу списку поточних процесів. За замовчуванням вона показує лише процеси користувача, що виконав команду. Для виведення всіх процесів застосовують параметри: ps -a або ps -e

Утиліта iptraf призначена для моніторингу мережевої активності в режимі реального часу. Вона надає детальну статистику про мережевий трафік, що допомагає у виявленні проблем і аналізі мережевих потоків.

Основні можливості iptraf:

- Відображення статистики TCP-з’єднань.
- Моніторинг IP-трафіку по мережевих інтерфейсах.
- Аналіз трафіку за різними мережевими протоколами.
- Відстеження трафіку по портам і розмірам пакетів.
- Статистика трафіку за адресами другого рівня (наприклад, MAC-адреси).

Отже, наведені утиліти забезпечують комплексний підхід до моніторингу та діагностики роботи операційної системи і мережевої інфраструктури. Інструменти, такі як vmstat **і** uptime, дозволяють оцінити стан системних ресурсів і тривалість роботи сервера, що є важливим для підтримки стабільності. Команда ps допомагає контролювати активні процеси, що забезпечує управління навантаженням на систему. Утиліта iptraf дає детальну інформацію про мережевий трафік у реальному часі, що є незамінним для виявлення мережевих

проблем і оптимізації роботи мережі. Використання цих інструментів дозволяє підтримувати ефективну роботу апаратного та програмного забезпечення мережевого середовища.

3.4 Налаштуванню засобів захисту мережі

Розглянемо набір правил для контролю мережевого трафіку.

Дозволимо вихідні з’єднання з операційної системи сервера до необхідних служб:

${ipfw} add allow tcp from $external_ip $user_ports to any $allowed_services out xmit $external_iface

Дозволимо вхідний трафік у внутрішню мережу, але лише для необхідних служб та лише у відповідь на ініційовані з’єднання:

${ipfw} add allow tcp from any $from_lan to $internal_network $user_ports in recv $external_iface established

Варто звернути увагу на параметр established, який пропускає лише ті пакети, що є відповіддю (позначені прапорами TCP ACK або RST).

Аналогічне правило застосуємо для VIP-клієнтів:

${ipfw} add allow tcp from any $vip_source to $vip_network $user_ports in recv $external_iface established

Для ОС сервера встановлюємо правило:

${ipfw} add allow tcp from any $routing_source to $external_ip $user_ports in recv $external_iface established

Для коректної роботи DNS сервісів прописуємо:

${ipfw} add allow udp from $external_ip $user_ports to any domain out xmit $external_iface

${ipfw} add allow udp from any domain to $external_ip $user_ports in recv $external_iface

${ipfw} add allow udp from any domain to $internal_network $user_ports in recv $external_iface

Перше правило відкриває вихідний UDP-трафік на порт 53, а два наступні дозволяють отримувати відповіді DNS для сервера та локальної мережі.

Правила для ICMP-протоколу:

${ipfw} add allow icmp from any to me icmptypes 0,3,4,11,12 in

${ipfw} add allow icmp from any to $internal_network icmptypes 0,3,4,11,12 in recv $external_iface

${ipfw} add allow icmp from me to any icmptypes 3,8,12 out

Пояснення кодів ICMP:

0 - echo reply

3 - destination unreachable

4 - source quench

5 - redirect

8 - echo request

9 - router advertisement

10 - router solicitation

11 - time-to-live exceeded

12 - IP header bad

13 - timestamp request

14 - timestamp reply

15 - information request

16 - information reply

17 - address mask request

18 - address mask reply.

Додаткові універсальні правила для портів із номером більшим за 1024 (у тому числі для FTP і інших сервісів):

${ipfw} add allow tcp from $external_ip $user_ports to any $user_ports out xmit $external_iface

${ipfw} add allow tcp from any $user_ports to $external_ip $user_ports in recv $external_iface established

${ipfw} add allow tcp from any $user_ports to $vip_network $user_ports in recv $external_iface established

Для фіксації спроб встановлення з’єднань, що не відповідають правилам:

${ipfw} add deny log loglimit 700 tcp from any to $external_ip in recv $external_iface setup

Параметр loglimit перевизначає обмеження на кількість логів у Ipfirewall.

І наостанок забороняємо весь інший трафік, що не відповідає вказаним правилам:

${ipfw} add deny all from any to any

У наведених правилах фільтрації трафіку реалізовано комплексний підхід до забезпечення безпеки мережі. Вони дозволяють контролювати вхідний та вихідний трафік, забезпечують доступ лише до необхідних сервісів і обмежують взаємодію з мережевими вузлами, враховуючи стан TCP-з'єднань. Особливу увагу приділено коректній роботі DNS та ICMP, що сприяє стабільності мережевих процесів.

Логування спроб встановлення з’єднань допомагає відслідковувати потенційні загрози, а заборона всього іншого трафіку мінімізує ризики несанкціонованого доступу. Загалом, ці правила сприяють підвищенню захищеності і надійності роботи серверної операційної системи та локальної мережі.

3.5 Інструкції з експлуатації та моніторингу в мережі

Моніторинг роботи вузлів локальної обчислювальної мережі (ЛОМ) та сервісів є надзвичайно важливим для стабільної та ефективної експлуатації мережі. Він базується на централізованому зборі ключових показників, що відображають стан мережі в певні часові проміжки. Такі показники дозволяють відстежувати використання системних ресурсів та робити висновки про їх ефективність на основі аналізу даних за визначені періоди. Для збору метрик із серверів застосовуватимуться інструменти node_exporter та Prometheus, які відповідають за агрегацію та збереження інформації у базі даних. Для

візуалізації та аналізу отриманих даних використовуватиметься платформа Grafana, що дозволяє будувати інформативні графіки.

Окрім збору та аналізу метрик, не менш важливо забезпечити централізований збір і обробку лог-файлів із серверів та мережевого обладнання. Лог-файли містять детальну інформацію про події, помилки та інші критичні ситуації, що виникають у роботі системи, тому їхнє своєчасне опрацювання допомагає оперативно виявляти та усувати несправності, а також проводити аудит безпеки. Для реалізації цього процесу буде використаний комплексний стек інструментів, який складається з ElasticSearch, Fluent-Bit та Kibana.

ElasticSearch виступає у ролі потужної системи зберігання та пошуку даних, що оптимізована для швидкого індексування і аналізу великих обсягів логів у реальному часі. Fluent-Bit служить легким і ефективним агентом для збору логів із різних джерел, їхнього попереднього оброблення та надійної передачі у ElasticSearch. Kibana забезпечує зручний веб-інтерфейс для візуалізації та детального аналізу зібраної інформації, дозволяючи користувачам створювати дашборди, задавати складні запити і відстежувати тенденції та аномалії у роботі мережі. Такий підхід дозволяє не лише своєчасно реагувати на проблеми, а й проводить проактивний аналіз для підвищення стабільності та безпеки інфраструктури.

3.6 Моделювання локальної мережі

Метою моделювання є створення локальної мережі відповідно до заданої логічної топології та проведення тестування її функціональності за допомогою імітації роботи протоколу ICMP. Основне завдання полягає у верифікації правильності побудови мережі, перевірці зв’язності між вузлами, а також оцінці реакції мережевих пристроїв на ICMP-пакети, які використовуються для діагностики доступності та затримок у мережі.

Для цього формується логічна структура мережі, яка відповідає топології, наведеної на рисунку 3.5. В ході моделювання відтворюються ключові елементи мережі: комутатори, маршрутизатори, кінцеві вузли та канали зв'язку між ними. Імітація роботи протоколу ICMP дозволяє виявити можливі проблеми з маршрутизацією, затримками або втратою пакетів, що є критично важливим для забезпечення надійності мережевої інфраструктури. Таким чином, моделювання є важливим етапом у процесі проектування мережі, що допомагає уникнути помилок на стадії впровадження і забезпечує оптимальну роботу локальної мережі.

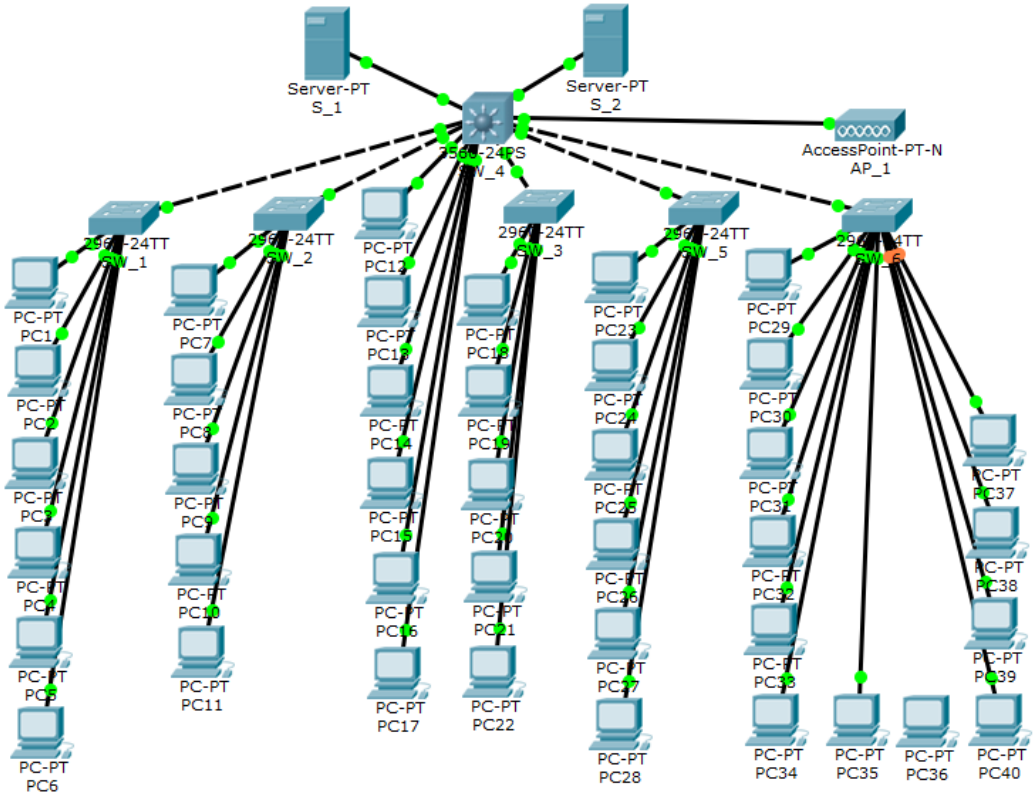


Рисунок 3.5 – Змодельована ЛОМ ТОВ «Контракт Буд»

Здійснимо моделювання роботи протоколу ICMP між вузлами S_1 та PC1. Для цього налаштуємо стек протоколів TCP/IP на вузлі S_1 відповідно до параметрів, наведених на рисунку 3.6. Це дозволить імітувати обмін ICMP-

пакетами між зазначеними пристроями та оцінити якість мережевого з’єднання, а також перевірити коректність маршрутизації й доступність вузлів у мережі

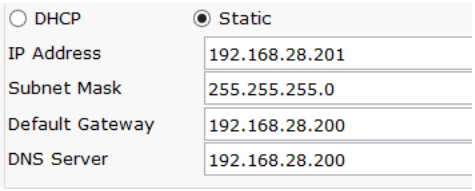


Рисунок 3.6 – Параметри стеку TCP/IP серверу S_1

На рисунку 3.7 наведено приклад налаштування TCP/IP для вузла PC1.

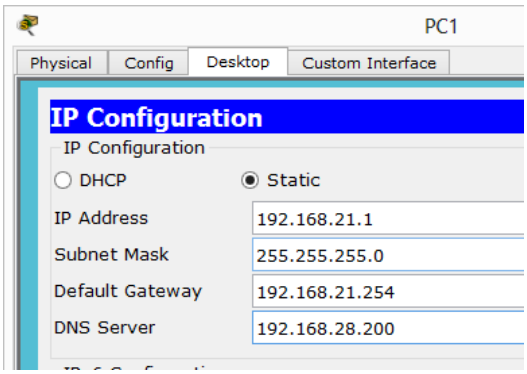


Рисунок 3.7 – Параметри стеку TCP/IP хоста WS_22

На хості PC1 виконаємо команду ping 192.168.28.201.

```
PC1>ping 192.168.28.201
Pinging 192.168.28.201 with 32 bytes of data:
Reply from 192.168.28.201: bytes=32 time=0ms TTL=128
Reply from 192.168.28.201: bytes=32 time=0ms TTL=128
Reply from 192.168.28.201: bytes=32 time=0ms TTL=128
Reply from 192.168.28.201: bytes=32 time=0ms TTL=128
Ping statistics for 192.168.28.201:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
PC1>
```

Рисунок 3.8 – Результати команди Ping на хості PC1

На рисунку 3.8 наведено результати її виконання. Результатом моделювання стало успішне надсилання та отримання пакетів по протоколу ICMP між сервером S_1 і робочою станцією PC1, що підтверджує коректну роботу мережевого з’єднання між цими вузлами.

Моделювання мережі є доцільним кроком для перевірки правильності побудови логічної топології та оцінки взаємодії мережевих компонентів до їх впровадження в реальному середовищі. Результати моделювання підтвердили коректну роботу протоколу ICMP і забезпечення зв’язку між ключовими вузлами, що свідчить про ефективність обраної конфігурації мережі.

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Економічна частина кваліфікаційної роботи використовується для здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки комп'ютерної мережі для ТОВ «КонтрактБуд» і прийняття рішення про її подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Розрахунок вартості науково-дослідної роботи (НДР) здійснюється поетапно та включає такі основні кроки:

1. Формування опису технологічного процесу розробки із деталізацією трудомісткості кожної виконуваної операції.

2. Визначення загальних витрат на оплату праці основного та допоміжного персоналу з урахуванням обов'язкових соціальних внесків.

3. Розрахунок необхідних матеріальних витрат.

4. Обчислення споживання електроенергії, що використовується для виконання науково-виробничих завдань.

5. Оцінка транспортних витрат, пов'язаних із реалізацією НДР.

6. Нарахування амортизаційних відрахувань на основні засоби, що залучені до виконання роботи.

7. Визначення обсягу накладних витрат.

8. Складання кошторису та обчислення повної собівартості науково-дослідної роботи.

9. Розрахунок остаточної ціни НДР.

10. Аналіз економічної ефективності реалізованої мережі та визначення строку її окупності.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

Для визначення загальної тривалості проведення НДР доцільно звести у таблицю 4.1 дані витрат часу по окремих операціях технологічного процесу. Виконавцями стадій технологічного процесу будуть: керівник, інженер, технік. В таблиці 4.1 наводяться стадії технологічного процесу та середній час їх виконання.

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

№ п/п	Назва операції (стадії)	Виконавець	Час викон. операції, год.
1	2	3	4
1	Постановка задачі, формування технічного завдання на проект локальної мережі.	Керівник проекту	5
2	Проектування логічної та фізичної топології локальної мережі. Аналіз інформаційних потоків локальної мережі. Розробка логічної адресації та конфігурації для апаратного та програмного забезпечення.	Інженер	10
3	Монтаж мережі (прокладання кабельних каналів, вертикальних та горизонтальних кабельних каналів). Здійснюється монтаж та підключення пасивного обладнання.	Технік	30

Продовження таблиці 4.1

1	2	3	4
4	Конфігурування мережевого обладнання (налаштування апаратного та програмного забезпечення). Налагодження мережі. Тестування конфігурацій апаратного та програмного забезпечення служб ЛОМ.	Інженер	15
5	Підготовка документації. Написання кабельного журналу, списку мережевого обладнання та його технічних характеристик.	Інженер	5
Разом		-	65

Сумарний час виконання операцій технологічного процесу з проектування мережі для ТОВ «КонтрактБуд» становить 65 год.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Відповідно до Закону України «Про оплату праці» заробітна плата – це винагорода у грошовому виразі, яка виплачується працівникові за виконану ним роботу.

Розмір заробітної плати залежить від складності та умов виконуваної роботи, професійно-ділових якостей працівника, результатів його праці та господарської діяльності підприємства.

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.

Приймемо такі тарифні ставки: керівник проекту – 250 грн./год., інженер – 200 грн./год., технік – 150 грн./год.

Отже, основна заробітна плата для:

- керівника проекту $З_{осн1} = 5 \cdot 250 = 1250$ грн.
- інженера $З_{осн2} = 30 \cdot 200 = 6000$ грн.
- техніка $З_{осн3} = 30 \cdot 150 = 4500$ грн.

Сумарна основна заробітна плата складає:

$$З_{осн} = 1250 + 6000 + 4500 = 11750 \text{ грн}$$

Додаткова заробітна плата становить 10-15 % від суми основної заробітної плати:

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

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

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника проекту $З_{дод1} = 1250 \cdot 0,12 = 150$ грн.
- інженера $З_{дод2} = 6000 \cdot 0,12 = 720$ грн.
- техніка $З_{дод3} = 4500 \cdot 0,12 = 540$ грн.

Загальна додаткова заробітна плата становить:

$$З_{дод} = 150 + 720 + 540 = 870 \text{ грн.}$$

Загальні витрати на оплату праці $В_{о.п.}$ визначаються за формулою:

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

$$В_{о.п} = 11750 + 870 = 12620 \text{ грн.}$$

Крім того, слід визначити відрахування на соціальні заходи:

- фонд страхування на випадок безробіття – 1,6 %;
- фонд по тимчасовій втраті працездатності – 1,4 %;
- пенсійний фонд – 33,2 %;

- внески на страхування від нещасного випадку на виробництві та професійного захворювання - 1,4%.

Загальна сума зазначених відрахування становлять 37,6 %. Отже, сума відрахувань на соціальні заходи буде становити:

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

ФОП – фонд оплати праці, грн.

$$В_{с.з.} = 12620 \cdot 0,376 = 4745,12 \text{ грн.}$$

Проведені розрахунки витрат на оплату праці зведено у таблиці 4.2. Розраховано заробітну плату для керівника проекту, інженера, техніка.

Кожен із вище зазначених робітників виконує свій перелік обов'язків.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія працівників	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	2	3	4	5	6	7	8
1	Керівник проекту	250	5	1250	150	-	-
2	Інженер	200	30	6000	720	-	-
3	Технік	150	30	4500	540	-	-
Разом				11750	870	4745,12	17365,12

Отже, загальні витрати на оплату праці становлять 17365,12 грн.

4.3 Розрахунок матеріальних витрат

Розрахунок матеріальних витрат визначаються як добуток кількості витрачених матеріалів та їх ціни:

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

де q_i – кількість витраченого матеріалу 1-го виду;

p_i – ціна матеріалу 1-го виду.

Звідси, загальні матеріальні витрати можна визначити:

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

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№ п/п	Назва елементу	Модель	Од. вим.	К-ть	Ціна, грн.	Сума, грн.
1	2	3	4	5	6	7
1	Серверно-комутаторна шафа	ШС-24U	шт	1	11230	11230
2	Патчпанель	24 порти, кат. 6 UTP	шт	1	2000	2000
3	Розетка RJ-45	UTP кат. 6	шт	43	90	3870
4	Кабель-канали (різного січення)	-	м	90	63	5670
5	Вита пара	UTP кат. 6	м	500	15	7500

Продовження таблиці 4.3

1	2	3	4	5	6	7
6	Патчкорд	UTP кат. 6	шт	80	21	1680
7	Джерело живлення (ДБЖ)	APC Smart-UPS RS 1100	шт	1	17800	17800
8	Швидкомонтажний дюбель	-	шт	200	1,2	240
9	Кріпильні шуруп	-	шт	200	1,3	260
10	Тримачі для кабелів	-	шт	4	240	960
11	Головний комутатор	Edge-Core ES4610	шт	1	12000	12000
12	Комутатор сегменту мережі	TP-Link TL-SG3216	шт	1	3400	3400
13	Комутатор сегменту	TP-Link TL-SG3210	шт	4	2900	11600
14	Серверне обладнання	ARTLINE Business R33 v01	шт	2	31000	62000
15	Точка доступу	TredNET AC1200	шт	1	2300	2300
Всього, грн.						142510

Отже, загальна сума матеріальних витрат для проектування локальної мережі становить 142510,00 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

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

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання, год;

S – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 16 годин, споживана потужність - 0,5 кВт/год, вартість 1 КВт електроенергії становить – 7 грн.

Отже, вартість витрат на електроенергію становить

$$З_е = 0,5 \cdot 16 \cdot 7 = 56 \text{ грн.}$$

4.5 Визначення транспортних витрат

Транспортні витрати слід прогнозувати у розмірі 1-10 % від загальної суми матеріальних затрат:

$$Т_в = З_{м.в.} \cdot 0,01...0,1, \qquad (4.8)$$

де $Т_в$ – транспортні витрати.

Отже,

$$Т_в = 142510,00 \cdot 0,02 = 2850,20 \text{ грн.}$$

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фондів. Для визначення амортизаційних відрахувань застосовуємо формулу 4.9:

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

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

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

$Н_А$ – норма амортизації, %

Т – час роботи за ПК, год.

Враховуючи, що балансова вартість ПК – 30000 грн., то амортизаційні відрахування становитимуть:

$$A = \frac{30000 \cdot 0{,}05}{150} \cdot 16 = 160{,}00 \; грн.$$

4.7 Обчислення накладних витрат

Накладні витрати охоплюють комплекс витрат, які не належать безпосередньо до основного виробничого процесу, але є необхідними для забезпечення його функціонування. Вони включають витрати на організацію та обслуговування виробництва, утримання адміністративно-управлінського персоналу, бухгалтерії, відділу кадрів, а також витрати на охорону праці, пожежну безпеку, технічне обслуговування обладнання, прибирання приміщень, комунальні послуги (вода, електроенергія, опалення), зв'язок, охорону об'єкта тощо. Також до накладних витрат належать витрати на амортизацію адміністративних приміщень та офісного обладнання, витрати на службові відрядження управлінського персоналу, канцелярські товари, інші господарські потреби, що створюють необхідні умови для організації ефективної праці на підприємстві.

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

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

де $Н_в$ – накладні витрати.

$$Н_в = 12620 \cdot 0,4 = 5048 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблиці 4.4.

Таблиця 4.4 – Загальний кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Витрати на оплату праці	12620	7,51
Відрахування на соціальні заходи	4745,12	2,82
Матеріальні витрати	142510,00	84,83
Витрати на електроенергію	56	0,03
Транспортні витрати	2850,20	1,70
Амортизаційні відрахування	160,00	0,10
Накладні витрати	5048	3,00
Собівартість	**167989,3**	100,00

Собівартість ($С_в$) НДР розрахуємо за формулою:

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

Отже, собівартість виконання науково-дослідної роботи дорівнює:

$С_в$= 167989,3 грн.

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

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

де $С_в$ – собівартість виконання НДР;

$Р_{рен.}$ – рівень рентабельності, 1,24 %

ПДВ – ставка податку на додану вартість, 25 %.

$$Ц = 167989,3 \cdot (1+0,24) \cdot (1+0,25) = 260383,42 \text{ грн.}$$

4.10 Визначення економічної ефективності і терміну окупності капітальних вкладень

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

Прибуток розраховується за формулою:

$$П = Ц - С_в \quad (4.13)$$

$$П = 260383,42 - 167989,3 = 92394,12 \text{ грн.}$$

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

$$Е_р = П / С_в, \quad (4.14)$$

де П – прибуток;

$С_в$ – собівартість.

$$E_р = 92394,12 / 167989,3 = 0,55$$

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

$$T_р = 1 / E_р \quad (4.15)$$

В нашому випадку $T_р$= 1/0,55 = 1,82, що є нормальним, оскільки допустимим вважається термін окупності до 5 років.

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

Таблиця 4.5 - Техніко-економічні показники розробки мережі

№ п/п	Показник	Одиниця виміру	Значення
1.	Собівартість	грн.	167989,3
2.	Плановий прибуток	грн.	92394,12
3.	Ціна	грн.	260383,42
4.	Економічна ефективність	-	0,55
5.	Термін окупності	рік	1,82

Загальна вартість впровадження розробленої комп'ютерної мережі для товариства «КонтрактБуд» становить 260 383,42 грн. Проведені економічні розрахунки свідчать про високу рентабельність проєкту: строк окупності становить лише 1,82 роки, а коефіцієнт економічної ефективності дорівнює 0,55, що перевищує нормативне значення для подібних інвестицій.

Отже, реалізація запропонованого технічного рішення є економічно доцільною. Впровадження комп'ютерної мережі забезпечить підвищення продуктивності праці, оптимізацію внутрішніх бізнес-процесів, покращення якості обробки даних, а також створить передумови для подальшого розвитку цифрової інфраструктури підприємства.

5 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

Охорона праці - це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності [1].

5.1 Дотримання вимог пожежної безпеки в ТОВ "КонтрактБуд"

Протипожежна безпека на підприємстві в Україні – невіддільна частина організації робочого простору і процесів згідно з нормами чинного законодавства [1].

Зокрема, цю сферу регламентують Правила пожежної безпеки в Україні, затверджені наказом Міністерства внутрішніх справ України, зі змінами, які періодично вносяться відповідними наказами [1].

Зафіксовані на законодавчому рівні вимоги пожежної безпеки зобов'язані виконувати – незалежно від приналежності та розміру статутного капіталу, обороту, кількості співробітників, форми власності, кодів ЗЕД, сфери роботи та інших аспектів – будь-які суб'єкти, що ведуть свою господарську діяльність на українській території.

Тому необхідно бути в курсі цих змін і коригувати організаційну роботу в даному секторі на виробництвах і в компаніях.

А для цього слід регулярно проводити моніторинг нормативної бази та проходити відповідне навчання, щоб оновити не лише теоретичну базу, а й практичні навички співробітників.

Пожежна безпека входить в комплекс заходів з охорони праці, і організаційна робота в цій сфері на об'єктах господарювання включає широкий спектр заходів, а саме:

- створення умов для безпечної праці,

- мінімізації ризику виникнення пожеж,

- своєчасне і повноцінне забезпечення технічними засобами для запобігання займання та усунення самих пожеж та їх наслідків,

- контроль дотримання протипожежних вимог і норм законодавства,

- розробка і впровадження регламентів по гасінню пожеж, евакуації та порятунку з місць пожежі й задимлення людей і майна (матеріальних цінностей),

- внутрішнє і зовнішнє навчання співробітників [1].

У разі, якщо підприємство орендує площі в іншої особи, сторони повинні в письмовій формі домовитися про те, хто з них і на яких умовах здійснює ці роботи.

Вимоги до пожежної безпеки на підприємстві неухильно повинен дотримуватися кожен співробітник, а організаційна складова при цьому покладається на посадових осіб за відповідним рішенням керівництва і прописується в посадових інструкціях і положеннях по структурним підрозділам.

Зокрема, вказуються конкретні території, ділянки, зони, об’єкти, цілі будівлі і їх частини, поверхи, на яких відповідального співробітника повинне проводити такі організаційні роботи.

Відповідальні особи зобов’язуються розробити, впровадити та підтримувати в певному інструкцією і положенням на ввірених їм об’єктах протипожежний режим і інструкції відповідно до вимог, викладених в нормативних актах.

Залежно від особливостей виробничого процесу, крім загальних вимог пожежної безпеки, здійснюються спеціальні протипожежні заходи для окремих видів виробництв, технологічних процесів та промислових об'єктів. Для споруд та приміщень, в яких експлуатуються відеотермінали та ЕОМ такі заходи визначені правилами пожежної безпеки в Україні та іншими нормативними документами [2].

Будівлі і ті їх частини, в яких розташовуються ЕОМ, повинні бути не нижче II ступеня вогнестійкості. Над та під приміщеннями, де розташовуються ЕОМ, а також у суміжних з ними приміщеннях не дозволяється розташування

приміщень категорій А і Б за вибухопожежною небезпекою. Приміщення категорії В слід відділяти від приміщень з ЕОМ протипожежними стінами.

Важливою складовою протипожежного режиму на будь-якому об’єкті є розробка і впровадження порядку дій при виникненні пожежі. Неодмінно має бути план евакуації, описано, як повинні відключатися електроустановки, що і в якій послідовності необхідно робити співробітникам.

Відповідно, для кожного об’єкта, кожного приміщення (крім коридорів, санвузлів, басейнів і подібних приміщень), окремих видів робіт складаються інструкції, за якими повинен працювати персонал, залучений на певних ділянках і в виконанні окремих видів робіт. За інструкціями проводиться навчання (інструктаж) персоналу з подальшим контролем знань.

Для ліквідації невеликих осередків пожежі, а також для гасіння пожеж на початковій стадії їх розвитку (до прибуття штатних підрозділів пожежної охорони) призначені первинні засоби пожежогасіння.

Поміж первинних засобів пожежогасіння найважливіша роль відводиться найефективнішим із них - вогнегасникам. Установлено, що з використанням вогнегасників успішно ліквідують загоряння протягом перших чотирьох хвилин від миті їх виникнення, тобто ще до прибуття пожежних підрозділів. Вогнегасники слід установлювати в легкодоступних місцях (у коридорах, біля входів або виходів із приміщень тощо) та на видноті, а також у пожежонебезпечних місцях, де найімовірнішою є поява осередків пожежі. При цьому слід забезпечити їх захист від потрапляння прямих сонячних променів та безпосередньої (без загороджувальних щитків) дії опалювальних і нагрівальних приладів. Переносні вогнегасники мають розміщуватися шляхом навішування їх на вертикальні конструкції на висоті не більше 1,5 м від рівня підлоги до нижнього торця вогнегасника та на відстані од дверей, достатній для їх повного відчинення, або встановлення в пожежних шафах поряд із

пожежними кранами, в спеціальних тумбах або на пожежних щитах (стендах).

Переносні вогнегасники містять у собі обмежену кількість вогнегасної речовини, безперервна подача якої відбувається протягом невеликого проміжку часу, внаслідок чого помилки, допущені під час їх використання, виправити неможливо. Тому слід досконало знати правила роботи з вогнегасниками (див. рис. 5.1). В нашому випадку вибрано вогнегасники ВВК-5, які мають корисну масу діючої речовини 5 кілограм.

Рисунок 5.1 – Правила застосування ВВК-5

Даний тип вогнегасників призначений для гасіння загорянь різних речовин, горіння яких не може відбуватися без доступу повітря, загоряння електроустановок, що знаходяться під напругою не більше 10кВ. Так само даний вогнегасник отримав широке поширення в офісних приміщеннях за наявності оргтехніки, а також в житловому секторі.

У разі виникнення пожежі першочерговим завданням є забезпечення безпечної та швидкої евакуації всіх працівників і відвідувачів приміщення, а також оперативне застосування первинних засобів пожежогасіння для стримування загоряння до прибуття пожежної служби.

В загальнодоступних приміщеннях повинен бути вивішений план евакуації, на якому чітко вказано напрямки евакуації, основний та запасний (аварійний) виходи та розміщення засобів пожежогасіння. Взірець розробленого плану евакуації наведено на рисунку 5.2.

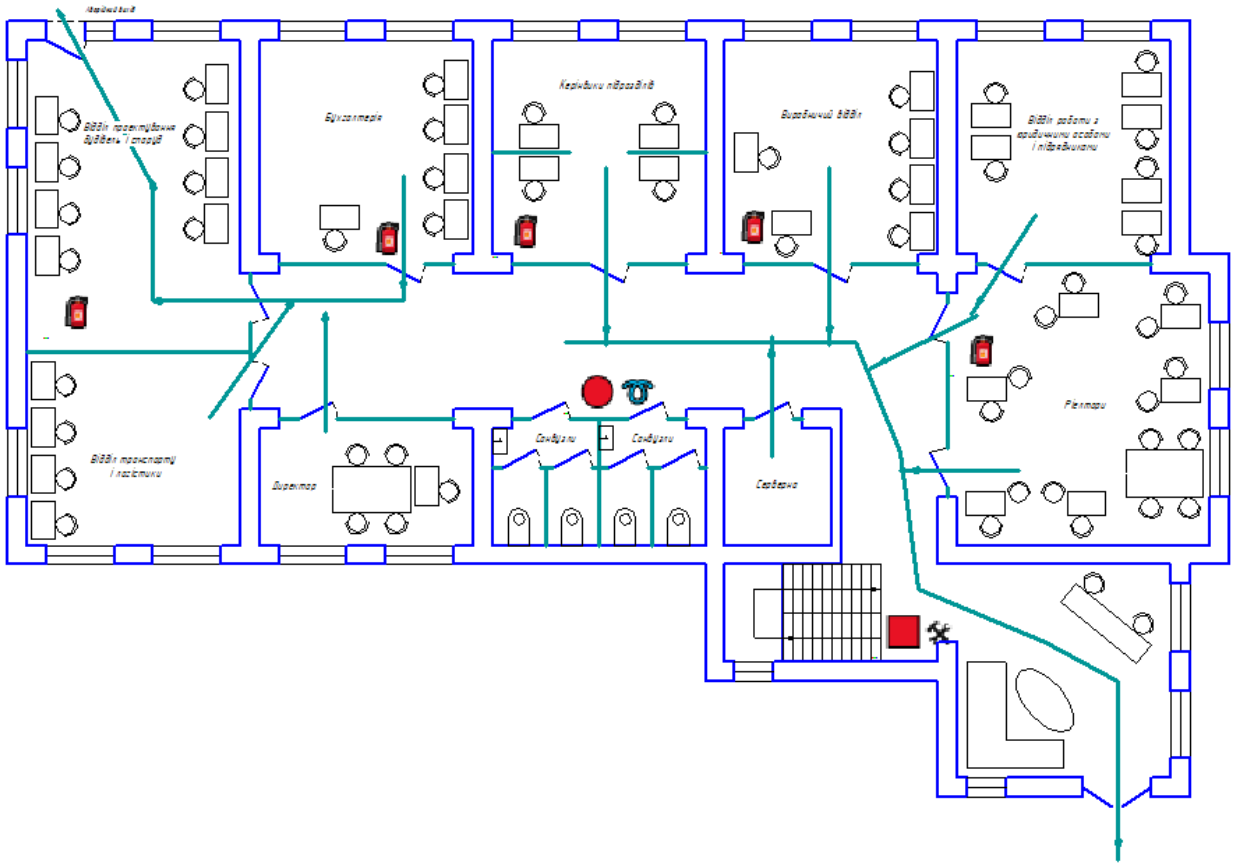
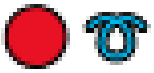


Рисунок 5.2 – План евакуації з ТОВ “КонтрактБуд”

Умовні позначення на плані евакуації :

 Вогнегасник ВВК-5

 Пожежний щит

 Пожежний рукав

5.2 Система управління охороною праці в ТОВ “КонтрактБуд”

Для створення на робочому місці в кожному структурному підрозділі умов праці відповідно до нормативно-правових актів, а також забезпечення додержання вимог законодавства щодо прав працівників у галузі охорони праці роботодавець забезпечує функціонування системи управління охороною праці (СУОП) – частини загальної системи управління організацією, яка сприяє запобіганню нещасним випадкам та професійним захворюванням на виробництві і включає в себе комплекс організаційних, технічних, санітарно-гігієнічних та лікувально-профілактичних заходів для збереження життя, здоров’я та працездатності найманих працівників [8].

СУОП підприємства складається з суб'єкта та об'єкта управління, що інформативно зв'язані між собою, а також правових, організаційних, науково-технічних, санітарно-гігієнічних, соціально-економічних та лікувально-профілактичних заходів і засобів.

Суб'єктом управління є орган управління та виконавчий орган (роботодавець, СОП, керівники структурних підрозділів і допоміжних служб, комісія з питань охорони праці). Об'єкт управління – виробнича діяльність працівників, будівлі та споруди, виробниче обладнання, технологічні процеси, виробниче середовище.

СУОП підприємства повинна забезпечувати [3]:

- планування заходів з охорони праці;

- здійснення попереджувальних і коригувальних дій;

- адекватне та постійне управління;

- адаптацію до обставин, що змінилися;

- вплив громадських об'єднань працівників підприємства (комісій з питань охорони праці, уповноважених найманими працівниками осіб з питань охорони праці, профспілок тощо) на її функціонування;

- контроль виконання поточного та оперативних планів;

- документально оформлене визначення структури, стану та ефективності її роботи;

- інтеграцію в загальну систему управління.

Основні функції СУОП підприємства [10]:

- прогнозування виробничого ризику;

- організація, планування та координація роботи з охорони праці;

- правове, інформаційне, методичне забезпечення охорони праці;

- кадрове і професійне забезпечення охорони праці;

- проектно-конструкторське, метрологічне, технологічне, матеріально-технічне забезпечення охорони праці;

- нормалізація санітарно-гігієнічних умов праці;

- лікувально-профілактичне, медичне й соціальне забезпечення охорони праці;

- мотивація безпечної роботи;

- контроль за станом охорони праці;

- облік, аналіз і оцінка показників стану умов і безпеки праці та функціонування СУОП.

Для забезпечення функціонування СУОП роботодавець [10]:

- створює відповідні служби і призначає посадових осіб, які вирішують конкретні питання охорони праці, контролює виконання покладених на них функцій;

- бере участь у розробці та реалізації комплексних заходів для підвищення рівня охорони праці;

- забезпечує належне утримання та моніторинг технічного стану будівель і споруд, виробничого обладнання та устаткування;

- забезпечує здійснення профілактичних заходів для усунення причин нещасних випадків і професійних захворювань;

- організовує проведення атестації робочих місць за умовами праці, оцінки технічного стану виробничого обладнання та устаткування та вживає заходів щодо усунення небезпечних і шкідливих виробничих чинників;

- затверджує нормативні акти з охорони праці, що діють у межах підприємства;

- контролює додержання працівником вимог з охорони праці;

- організовує пропаганду безпечних методів праці;

- вживає заходів для допомоги потерпілим від нещасних випадків, ліквідації аварій на підприємстві.

Розроблення та впровадження системи управління охороною праці (СУОП) має здійснюватися за активної участі керівництва підприємства, фахівців служби охорони праці, представників профспілкової організації або осіб, уповноважених працівниками.

Запровадження СУОП оформлюється відповідним наказом чи розпорядженням керівника підприємства, де застосовується наймана праця, незалежно від форми власності чи напряму господарської діяльності.

Організацію та координацію роботи системи управління охороною праці на виробництві забезпечує служба охорони праці або посадова особа, яка виконує її функції.

Отже, система управління охороною праці є невід'ємною частиною загальної системи управління підприємством, що забезпечує створення безпечних і здорових умов праці відповідно до чинного законодавства. Її ефективне функціонування можливе лише за умови комплексного підходу, який охоплює організаційні, технічні, санітарно-гігієнічні та профілактичні заходи, а також за активної участі керівництва, служби охорони праці й представників трудового колективу. Реалізація СУОП сприяє зниженню виробничих ризиків, попередженню нещасних випадків, підвищенню рівня безпеки працівників і формуванню культури охорони праці на підприємстві.

ВИСНОВКИ

Для проекту локальної мережі розроблено:

1. Логічну топологію.
2. Фізичну топологію.
3. Таблицю IP-адрес.

Додатково розроблено детальні інструкції з налаштування центрального комутатора, безпровідної точки доступу, сервера-шлюза та сервера IP-телефонії. В дипломній роботі розроблено проект локальної мережі стандарту Gigabit Ethernet та 802.11ac. Розроблена локальна комп'ютерна мережа відповідає сучасним вимогам, що ставляться до локальних мереж середніх за розміром. При розробці враховано можливість керування та моніторингу, побудова структури мережі, підмережі якої відповідають відділам, можливість роботи з ресурсами мережі для стаціонарних та мобільних пристроїв, враховано основні аспекти захисту локальної мережі.

Засобами програми PacketTracer змодельовано роботу локальної мережі, а саме роботу протоколу ICMP.

Кваліфікаційна робота містить повністю завершену логічну і фізичну топології мережі, які подано в графічній частині.

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

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

ПЕРЕЛІК ПОСИЛАНЬ

1. В.І. Кошель, Г.П. Сав'юк, Б.С. Дзундза Основи охорони праці. Навчально-методичний посібник для студентів вищих навчальних закладів педагогічного напрямку / [Укаладачі: В.І. Кошель,Г.П. Сав'юк, Б.С. Дзундза] – Івано-Франківськ: НАІР, 2020. – 182 с.

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. – К.: НАУ , 2007.-361с.

4. Коваленко А. Є. Корпоративні комп'ютерні мережі та телекомунікації. – К. : НУХТ, 2014. – 278 с.

5. Комп'ютерні мережі : Навчальний посібник / В. Г. Хоменко, М. П. Павленко. – Харків: ЛАНДОН-ХХІ, 2014. – 316 с.

6. Микитишин А.Г. Комплексна безпека інформаційних мережевих систем : навч.посібн. / А.Г. Микитишин , М.М. Митник , П.Д. Стухляк. - Тернопіль : ТНТУ імені Івана Пулюя, 2016. - 261 с

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

8. Млавець Ю.Ю. Безпека життєдіяльності (конспект лекцій для студентів математичного факультету і факультету післядипломної освіти та доуніверситетської підготовки). – Ужгород: ДВНЗ "УжНУ", 2015. – 40 с

9. Оліх О. Я. Сучасні комп'ютерні технології. Принципи побудови комп'ютерних мереж : навч. посіб. / О. Я. Оліх. — Київ : ВПЦ «Київ. ун-т», 2015. — 480 с. — ISBN 978-966-439-740-4.

10. Шудренко І. В. Основи охорони праці : навч. посіб. / І. В. Шудренко. – Житомир : Видавець, О. О. Євенок, 2016. – 214 с.

11. TL-SG3210 URL: http://www.tp-link.ua/uk/products/details/cat-39_TL-SG3210.html - (дата звернення: 3.06.2025).

12. Wi-Fi Protected Access. URL: https://uk.wikipedia.org/wiki/Wi-Fi_Protected_Access. (дата звернення: 06.06.2025)

13. Інструкції з налаштування VoIP обладнання Asterisk URL: https://zadarma.com/ua/support/instructions/asterisk/- (дата звернення: 09.06.2025)

14. Класифікація груп основних засобів та інших необоротних активів. Методи нарахування амортизації. URL: http://tc.nusta.com.ua/dkpku/komentar/3_s145/index_2.htm. (дата звернення: 4.06.2025).

15. Коммутатор Edge-Core ES4610. URL: https://www.edge-core.com/productsInfo.php?cls =&cls2=&cls3=64&id=124 (дата звернення: 01.06.2025)

ДОДАТКИ

Додаток А. Конфігураційний файл файрвола ipfw

```
#!/bin/sh
# Manual script for ipfw
echo -n "Starting firewall..."
ipfw="/sbin/ipfw"
uports="1025-65535"
int_if="em0"
ext_if="xl0"
int_ip="192.168.28.200"
ext_ip="213.23.240.23"
int_net="192.168.0.0/16"
ext_net="213.23.240.23/24"
vip_net="192.168.28.0/27"
for_lan="smtp, pop3, domain, http, https"
for_vip="aol, ftp, ssh"
for_rout="ftp, domain, ssh"
Services="smtp, pop3, http, https, domain, aol, ssh, ftp"
${ipfw} add allow all from any to any via lo0
${ipfw} add deny all from any to 127.0.0.0/8
${ipfw} add deny all from 127.0.0.0/8 to any in recv $ext_if
${ipfw} add deny all from 10.0.0.0/8 to any in recv $ext_if
${ipfw} add deny all from 172.16.0.0/16 to any in recv $ext_if
${ipfw} add deny all from 192.168.0.0/16 to any in recv $ext_if
${ipfw} add allow all from $int_net to any in recv $int_if
${ipfw} add allow all from any to $int_net out xmit $int_if
${ipfw} add divert natd all from $int_net to not $int_net out xmit $ext_if
```

```
${ipfw} add divert natd all from any to $ext_ip in recv $ext_if
${ipfw} add allow tcp from $ext_ip $uports to any $Services out xmit $ext_if
${ipfw} add allow tcp from any $for_lan to $int_net $uports in recv $ext_if established
${ipfw} add allow tcp from any $for_vip to $vip_net $uports in recv $ext_if stablished
${ipfw} add allow tcp from any $for_rout to $ext_ip $uports in recv $ext_if established
${ipfw} add allow udp from $ext_ip $uports to any domain out xmit $ext_if
${ipfw} add allow udp from any domain to $ext_ip $uports in recv $ext_if
${ipfw} add allow udp from any domain to $int_net $uports in recv $ext_if
${ipfw} add allow tcp from $ext_ip $uports to any $uports out xmit $ext_if
${ipfw} add allow tcp from any $uports to $ext_ip $uports in recv $ext_if established
${ipfw} add allow tcp from any $uports to $vip_net $uports in recv $ext_if established
${ipfw} add allow icmp from any to me icmptypes 0,3,4,11,12 in
${ipfw} add allow icmp from any to $int_net icmptypes 0,3,4,11,12 in recv $ext_if
${ipfw} add allow icmp from me to any icmptypes 3,8,12 out
${ipfw} add deny log logamount 700 tcp from any to $ext_ip in recv $ext_if setup
${ipfw} add deny all from any to any
echo "DONE"
```

Додаток Б. Таблиця IP адрес

Таблиця Б1 – IP-адресація

№ п/п	Познач. вузла	Назва відділу	Номер VLAN	Адреси вузлів/ Маска	Шлюз
1	WS_1-WS_6	Ріелтори	21	192.168.21.1/24–192.168.21.6/24	192.168.21.254
2	WS_7-WS_9	Юридичний відділ	22	192.168.22.1/24-192.168.22.3/24	192.168.22.254
3	WS_10-WS_11	Відділ роботи з підрядниками	23	192.168.23.1/24-192.168.23.2/24	192.168.23.254
4	WS_12-WS_14	Керівники підрозділів	24	192.168.24.1/24-192.168.24.2/24	192.168.24.254
5	WS_15	Заступник	25	192.168.25.0/24	192.168.25.254
6	WS_16	Офіс-менеджер	26	192.168.26.0/24	192.168.26.254
7	WS_17	Директор	27	192.168.27.0/24	192.168.27.254
9	S_1	Комп’ютерний відділ і	28	192.168.28.201/24	192.168.28.254
10	S_2		28	192.168.28.200/24	213.23.240.254
			-	213.23.240.23	
11	WS_18 - WS_22	Бухгалтерія	29	192.168.29.1/24-192.168.29.5/24	192.168.29.254
12	WS_23 - WS_28	Виробничий відділ	30	192.168.30.1/24-192.168.30.6/24	192.168.30.254
13	WS_29 - WS_36	Відділ проектування будівельних споруд	31	192.168.31.1/24-192.168.31.8/24	192.168.31.254
14	WS_37-WS_40	Відділ транспорту і логістики	32	192.168.32.1/24-192.168.32.4/24	192.168.32.254
15	AP_1	Рецепція	33	192.168.33.1/24	192.168.33.254

Додаток В. Логічна адресація в ЛОМ

Таблиця В1 – Поділ на VLAN

№ п/п	Діапазон позначення вузлів	Група/К-сть вузлів		Прим	Назва кабінету та його номер		Номер VLAN	Адреса підмережі/ Маска
1	WS_1-WS_6, SW_1	-	7	1	Ріелтори	-	21	192.168.21.0/24
2	WS_7-WS_9, SW_2	-	4	1	Юридичний відділ	-	22	192.168.22.0/24
3	WS_10-WS_11	-	2	1	Відділ роботи з підрядниками	-	23	192.168.23.0/24
4	WS_12-WS_14	-	3	1	Керівники підрозділів	-	24	192.168.24.0/24
5	WS_15	-	1	1	Заступник	-	25	192.168.25.0/24
6	WS_16	-	1	1	Офіс менеджер	-	26	192.168.26.0/24
7	WS_17	-	1	1	Директор	-	27	192.168.27.0/24
8	S_1, S_2, SW_4	-	3	1	Комп’ютерний відділ	-	28	192.168.28.0/24
9	WS_18 - WS_22, SW_3	-	6	1	Бухгалтерія	-	29	192.168.29.0/24
10	WS_23 - WS_28, SW_5	-	7	1	Виробничий відділ	-	30	192.168.30.0/24
11	WS_29 - WS_36, SW_6	-	9	1	Відділ проектування споруд	-	31	192.168.31.0/24
12	WS_37 - WS_40	-	4	1	Відділ транспорту і логістики	-	32	192.168.32.0/24
13	AP_1	-	1	1	Рецепція	-	33	192.168.33.0/24

Таблиця В2 - Таблиця конфігурування VLAN

№ п/п	Позначення вузла	Номер порту	Тип порту	Назва мер. пристар.	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	WS_1-WS_6	Eth0	-	SW_1	1-6	Access	21
2	WS_7-WS_9	Eth0	-	SW_2	1-3	Access	22
3	WS_10-WS_11	Eth0	-	SW_2	4-5	Access	23
4	WS_12-WS_1	Eth0	-	SW_4	1-2	Access	24
5	WS_15	Eth0	-	SW_4	3	Access	25
6	WS_16	Eth0	-	SW_4	4	Access	26
7	WS_17	Eth0	-	SW_4	5	Access	27
8	WS_17, S_1, S_2	Eth0	-	SW_4	6-9	Access	28
9	WS_18 - WS_22	Eth0	-	SW_3	1-5	Access	29
10	WS_23 - WS_28	Eth0	-	SW_5	1-6	Access	30
11	WS_29 - WS_36	Eth0	-	SW_6	1-8	Access	31
12	WS_37 - WS_40	Eth0	-	SW_6	9-12	Access	32
13	AP_1	Eth0	-	SW_4	10	Access	33
14	SW_1	7	Trunk	SW_4	11	Trunk	-
15	SW_2	6	Trunk	SW_4	12	Trunk	-
16	SW_3	6	Trunk	SW_4	13	Trunk	-
17	SW_5	7	Trunk	SW_4	14	Trunk	-
18	SW_6	13	Trunk	SW_4	15	Trunk	-

Додаток Г. Порівняльні таблиці обладнання мережі

Таблиця Г1 – Порівняльна характеристика точок доступу

Виробник	TredNET	UBIQUITI	Mikrotik
Модель	AC1200	UAP-AC-LITE	RBOmniTikG-5HacD
Підтримувані стандарти	IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (до 300 Мбіт/с), IEEE 802.11ac (до 1000 Мбіт/с)		
Керування	Веб	Веб	Веб
Частотний діапазон	2.4/5 ГГц		
Протоколи шифрування	WEP, WPA/WPA2-PSK, WPA/WPA2-RADIUS		
Мережева статистика	Так	Так	Так
Режими роботи	Точка доступу, міст, ретранслятор	Точка доступу, міст	Точка доступу, міст, ретранслятор
Підтримка QoS	Так	Так	Так
Підтримка MAC-фільтра	Так	Так	Так

Таблиця Г2 – Порівняльна характеристика комутаторів

Параметр/ Модель	Edge-Core ES4610	AlliedTelesyn AT-9424T	Cisco Catalyst 3750G-24T
1	2	3	4
К-сть портів	20	24	24
К-сть слотів для модулів	4 SFP, 2 x 10G	4 SFP	4 SFP

Продовження таблиці Г2

1	2	3	4
Функції моделі OSI	3, 2	3, 2	3, 2
Швидкість комутаційної шини	128 Гбіт/с	71,4 Гбіт/с	32 Гбіт/с
Швидкість комутації пакетів 64Кбіт	95,2 млн. пакетів за сек.	96 млн. пакетів за сек.	38,7 млн. пакетів за сек.
ACL	Так	Так	Так
Підтримка 802.1q	Так	Так	Так

Таблиця Г3 - Порівняння технічних характеристик комутаторів

Характеристики	HP 1810-8G	TP-Link TL-SG3210
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	20
Моніторинг переданих/прийнятих пакетів	Так	Так
Швидкість комутації,	11,9 млн. пакетів/с	14,9 млн. пакетів/с
К-сть портів 10/100/1000	8	8
Додаткові слоти SFP	-	2
Віддалене керування	Так	Так

Таблиця Г4 - Порівняння апаратних конфігурацій серверів

	ARTLINE Business R33 v01	Supermicro 5019S-C	ProServer DL360p
Процесор	Intel Xeon E-2224G (3.5 - 4.7 ГГц)	Intel Xeon Quad-Core E3-1230 v6 (3.5 - 3.9 ГГц)	Intel Xeon E-2136 (3.3 - 4.5 ГГц)
Об’єм ОЗП	16ГБ	16ГБ	16ГБ
Тип ОЗП	DDR4-2666 МГц (4 слоти, макс. обсяг пам'яті 64 ГБ)	DDR4, Unbuffered, ECC	2666/2400/2133 МГц ECC DDR4 SDRAMф
Дискова підсистема	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ	HDD: 2 x 1 ТБ SSD: 2 x 250 ГБ
Мережева плата	інтегрована	інтегрована	інтегрована
Блок живлення	650 Вт	650Вт	650Вт