Міністерство освіти і науки України

Відокремлений структурний підрозділ «Тернопільський фаховий коледж

Тернопільського національного технічного університету імені Івана Пулюя»

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: Розробка проєкту комп'ютерної мережі ТзОВ "Бучач Друк"

Виконав: студент IV курсу, групи KI-412

Спеціальності <u>123 Комп'ютерна інженерія</u> (шифр і назва спеціальності)

Олег ІЛЬКІВ

(ім'я та прізвище)

Керівник

Андрій ЮЗЬКІВ (ім'я та прізвище)

(им я та прізви

Рецензент

(ім'я та прізвище)

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

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

ЗАТВЕРДЖУЮ

Голова шиклової комісії комп'ютерної інженерії Андрій ЮЗЬКІВ "<u>31</u>" березня 2025 року

ЗАВДАННЯ на кваліфікаційну роботу студенту

<u>Ільківу Олегу Івановичу</u> (прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: Розробка проєкту комп'ютерної мережі ТзОВ "Бучач Друк"

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

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

2. Строк подання студентом роботи: 13 червня 2025 року.

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

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

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

- план приміщень;
- фізична топологія мережі;
- логічна топологія;
- таблиця IP-адрес;
- таблиця техніко-економічних показників.

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

N⁰	Назва етапів кваліфікаційної роботи	Строк виконання	Примітка
3/П		етапів роботи	
1	Отримання і аналіз технічного завдання	01.04	
2	Збір і узагальнення інформації	05.05	
3	Написання першого розділу	16.05	
4	Розробка технічного та робочого проекту	23.05	
5	Написання спеціального розділу	30.05	
6	Розрахунок економічної частини	2.06	
7	Написання розділу охорони праці	4.06	
8	Виконання графічної частини	9.06	
9	Оформлення проєкту	11.06	
10	Погодження нормоконтролю	12.06	
11	Попередній захист роботи	13.06	
12	Захист кваліфікаційної роботи		

7. Дата видачі завдання: <u>01 квітня 2025 року</u>

Студент

(підпис)

<u>Олег ІЛЬКІВ</u> (ім'я та прізвище)

Керівник роботи

(підпис)

Андрій ЮЗЬКІВ (ім'я та прізвище)

АНОТАЦІЯ

Ільків О.І. Розробка проекту комп'ютерної мережі ТзОВ «Бучач Друк»: кваліфікаційна робота на здобуття освітньо-професійного ступеня фахового молодшого бакалавра, за спеціальністю 123 Комп'ютерна інженерія. Тернопіль: ВСП «ТФК ТНТУ», 2025. -88с.

Метою даної роботи є проєктування ефективної, безпечної та надійної мережевої інфраструктури, здатної забезпечити високопродуктивне обслуговування користувачів. У рамках виконання проєкту проведено аналіз вимог до мережі, здійснено підбір необхідного комутаційного обладнання та програмного забезпечення, а також виконано аналіз вимог до засобів забезпечення мережевої безпеки. Розроблено логічну та фізичну топології мережі. Розроблено інструкції щодо інсталяції та налаштування апаратного й програмного забезпечення серверів, мережевого обладнання та клієнських робочих станцій. Окрему увагу приділено економічному обґрунтуванню проєкту, а також дотриманню вимог охорони праці та техніки безпеки

Кваліфікаційна робота містить графічну частину, яка виконана на <u>5</u> аркушах формату A1, та пояснювальну записку яка складається з <u>88</u> аркушів, містить <u>14</u> таблиць та <u>6</u> рисунків.

Ключові слова: ПК, комп'ютерна мережа, комутаційне обладнання, програмне забезпечення, мережевий захист, економічні показники, охорона праці, техніка безпеки.

ANNOTATION

Ilkiv O.I. Design of the Computer Network Project for "Buchach Druk" LLC: qualification work for the attainment of the professional junior bachelor's degree in specialty 123 Computer Engineering. Ternopil: SEI "TCPC of TNTU", 2025... -88 p.

The objective of this thesis is to design an efficient, secure, and reliable network infrastructure capable of delivering high-performance services to end users. The project includes an analysis of network requirements, selection of appropriate switching hardware and software tools, and an assessment of network security mechanisms. Both logical and physical network topologies were developed. The thesis also provides detailed installation and configuration instructions for server hardware and software, network equipment, and client workstations. Particular attention is given to the economic justification of the proposed solution, as well as to compliance with occupational safety and health regulations.

The qualification thesis includes a graphical section presented on five A1 sheets and an explanatory note consisting of 88 pages, containing 14 tables and 6 figures.

Keywords: personal computer, computer network, switching equipment, software, network security

3MICT

Перелік термінів і скорочень	8
Вступ	9
1 Загальний розділ	11
1.1 Технічне завдання	11
1.1.1 Найменування та область застосування	11
1.1.2 Призначення розробки	12
1.1.3 Вимоги до апаратного та програмного забезпечення	13
1.1.4 Вимоги до документації	13
1.1.5 Техніко-економічні показники	14
1.1.6 Стадії та етапи розробки	15
1.1.7 Порядок контролю та прийому	16
1.2 Постановка задачі на розробку проекту. Характеристика підприємства	16
2 Розробка технічного та робочого проекту	19
2.1 Опис та обґрунтування вибору логічного типу мережі	19
2.2 Розробка схеми фізичного розташування кабелів та вузлів	19
2.2.1 Типи кабельних з'єднань та їх прокладка	19
2.2.2 Будова вузлів та необхідність їх застосування	21
2.3 Обгрунтування вибору комунікаційного обладнання	23
2.4 Особливості монтажу локальної мережі	28
2.5 Обтрунтування вибору програмного забезпечення	29
2.6 Тестування та налагодження локальної мережі	30
3 Спеціальний розділ	32
3.1 Інструкції з налаштування програмного забезпечення серверів	32
3.1.1 Інструкції з налаштування служби DHCP	32

					2025.КВР.123.412.04.00.00 ПЗ			
Зм.	Арк.	№ докум.	Підпис	Дата				
Розро	бив	Ільків О.І.			Разаабка апаекти кама'ютернаї	Літ.	Арк.	Аркушів
Перее	зірив	Юзьків А.В.			мережі ТзОВ «Бичач Дрик»		5	88
					ВСЛ ТФК ТНТУ			
Н. Ко	нтр.	Юзьків А.В.			Пояснювальна записка група KI-412			
Затв					м. Тернопіль			

3.1.2 Інструкції з налаштування програмного маршрутизатора	37
3.1.3 Інструкції з налаштування служби спільного зберігання файлів	38
3.2 Інструкції з налаштування активного комутаційного обладнання	42
3.2.1 Інструкції з налаштування головного комутатора	42
3.2.2 Інструкції з налаштування комутаторів робочих груп	46
3.2.3 Інструкції з налаштування маршрутизаторів	47
3.3 Інструкції з використання тестових наборів та програм	49
3.4 Інструкція з експлуатації та моніторингу в мережі	51
3.5 Інструкції з налаштування засобів захисту мережі	52
4. Економічний розділ	56
4.1 Визначення стадій техпроцесу та загальної тривалості проведення НДР	56
4.2 Визначення витрат на оплату праці та відрахувань на соц. заходи	57
4.3 Розрахунок матеріальних витрат	59
4.4 Розрахунок витрат на електроенергію	61
4.5 Визначення транспортних затрат	61
4.6 Розрахунок суми амортизаційних відрахувань	62
4.7 Обчислення накладних витрат	62
4.8 Складання кошторису витрат та визначення собівартості НДР	63
4.9 Розрахунок ціни НДР	64
4.10 Визначення економічної ефективності і терміну окупності капітали	ьних
вкладень	64
5. Охорона праці та безпека життєдіяльності	66
5.1 Законодавча база з питань охорони праці на якій ґрунтується безпека п	раці
в ТзОВ "Бучач Друк"	66
5.2 Вимоги охорони праці до рівнів шуму та вібрації на робочих місцях	70
5.3 Утримання евакуаційних шляхів і виходів з приміщення ТзОВ "Бучач	
Друк"	72
Висновки	77
Перелік посилань	78
	Арк
 ZUZ5.NBP. 123.4 12.04.00.00 113	6

Підпис

Зм.

Арк

№ докум.

Дата

Додаток А.Таблиця IP-адрес	80
Додаток Б. Дані сегментування локальної мережі	82
Додаток В. Мережеве обладнання	84
Додаток Г. Технічні характеристики маршрутизатора Xiaomi Mi 4A	86
Додаток Д. Конфігурацій скрипт IPFW	88

					2025.КВР.123.412.04.00.00 ПЗ
Зм.	Арк	№ докум.	Підпис	Дата	

ПЕРЕЛІК ТЕРМІНІВ І СКОРОЧЕНЬ

АРІ - інтерфейс прикладних програм;

IEEE 802.3ab - стандарт Gigabit Ethernet на витій парі UTP 5e;

IEEE 802.3ab - стандарт Gigabit Ethernet на витій парі UTP 5e;

IEEE 802.3ас - збільшення максимального розміру фрейму до 1522 байт (для підтримки інформації про VLAN стандарту IEEE 802.1Q та пріоритету стандарту IEEE 802.1p);

IEEE 802.3u - стандарт Fast Ethernet 100Мбіт/с;

IEEE 802.3z – стандарт Gigabit Ethernet 1000Мбіт/с;

ISO - Міжнародна Організація по Стандартизації;

ITU – міжнародний союз електрозв'язку;

МІВ - база керуючої інформації;

SNA - архітектура мережевих систем;

SNMP - протокол прикладного рівня для управління мережею;

SOHO – домашній офіс;

ТСР/ІР – протокол управління передачею, Інтернет протокол. Стек протоколів

Інтернет. Використовується для об'єднання гетерогенних мереж;

UTР - неекранована вита пара;

UTP (Unshielded Twisted Pair) - неекранована вита пара;

VLAN (Virtual Local Area Nerwork) - об'єднання ПК за певним критерієм у широкомовний домен;

WDM – мультиплексування з розділенням за довжиною хвилі;

ЛМ – локальна мережа;

ЛОМ – локальна обчислювальна мережа;

МАС адреса – 48 бітна фізична адреса пристрою;

ОС - операційна система;

ПК - персональний комп'ютер.

Зм.	Арк	№ докум.	Підпис	Дата

вступ

Під локальною мережею розуміють спільне підключення певних кількості робочих станцій та мережевих пристроїв до єдиного каналу передачі даних [1].

Впровадження локальних мереж є важливим для компаній з кількох причин:

– Покращення комунікації: Локальна мережа дозволяє компанії спілкуватися та обмінюватися інформацією між різними відділами та працівниками в режимі реального часу. Це підвищує ефективність комунікації та дозволяє швидко реагувати на потреби компанії.

– Збереження часу та ресурсів: Локальна мережа дозволяє компанії обмінюватися інформацією та ресурсами, такими як принтери та сканери. Це дозволяє компанії заощаджувати час та кошти на купівлю та утримання багатої кількості обладнання.

– Підвищення безпеки: Локальна мережа дозволяє компанії забезпечити кращий контроль за доступом до даних та ресурсів. Компанії можуть встановлювати паролі та інші методи автентифікації, щоб забезпечити, що тільки відповідні працівники мають доступ до важливих даних.

– Збільшення продуктивності: Локальна мережа дозволяє компанії забезпечити більш ефективне використання ресурсів та працівників. Наприклад, працівники можуть працювати з одного комп'ютера та мати доступ до однакових даних, що підвищує продуктивність та забезпечує більш ефективну роботу.

Отже, впровадження локальних мереж є важливим для компаній, оскільки дозволяє підвищити ефективність комунікації, зберегти час та ресурси, забезпечити більшу безпеку та збільшити продуктивність.

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

Мета кваліфікаційної роботи - розробка проекту локальної комп'ютерної мережі на основі вимог технічного завдання, складеного між Замовником та Виконавцем.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	10
Зм.	Арк	№ докум.	Підпис	Дата		10

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Проєкт локальної комп'ютерної мережі розробляється на замовлення ТзОВ «Бучач Друк» відповідно до попередньо узгоджених технічних та експлуатаційних параметрів, а також фінансових вкладень. Перед початком проектування були визначені такі ключові вимоги до функціонування мережевої інфраструктури:

1. Забезпечення стабільного з'єднання та обміну даними для всіх активних користувацьких пристроїв.

2. Захист робочих станцій від несанкціонованого доступу та зовнішніх загроз з глобальної мережі.

3. Організація спільного використання мережевих ресурсів між усіма вузлами.

4. Підтримка автоматичного налаштування мережевих параметрів (динамічна конфігурація протоколів).

5. Можливість як дротового, так і бездротового підключення до внутрішньої мережі.

6. Інтеграція єдиного комплексу засобів безпеки для захисту всіх мережевих вузлів (фаєрволи або альтернативні рішення).

7. Надання централізованого доступу до серверних ресурсів.

Хоча цей проєкт створено спеціально для підприємства ТзОВ «Бучач Друк», його структура та окремі технічні рішення можуть бути адаптовані для інших поліграфічних компаній зі схожими масштабами та потребами в комунікації.

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

1.1.2 Призначення розробки

Головною метою даної розробки є побудова локальної мережі компанії, яка забезпечуватиме ефективний та стабільний обмін інформацією між усіма підрозділами підприємства, спільний доступ до каналу Інтернет-провайдера, а також централізоване, надійне зберігання корпоративних даних.

Проєкт локальної мережі для ТзОВ «Бучач Друк» має повністю відповідати технічному завданню замовника і охоплювати такі ключові аспекти:

1. Формування єдиного інформаційного середовища шляхом інтеграції всіх дротових та бездротових клієнтів у спільну мережеву інфраструктуру з доступом до загальних ресурсів.

2. Загальна вартість розробки, монтажу та введення мережі в експлуатацію не повинна перевищувати бюджет, передбачений замовником.

3. Запровадження централізованих заходів кібербезпеки для захисту як стаціонарних, так і мобільних пристроїв від зовнішніх загроз з Інтернету.

4. Організація спільного використання офісного обладнання, такого як принтери, сканери та інші периферійні пристрої.

5. Створення надійної системи збереження даних із централізованим керуванням, що базується на відмовостійкому дисковому сховищі з підвищеним рівнем захисту.

1.1.3 Вимоги до апаратного та програмного забезпечення

Проєкт локальної комп'ютерної мережі для ТзОВ «Бучач Друк», як і будь-який аналогічний мережевий проєкт, передбачає використання як активного, так і пасивного мережевого обладнання, каналів передачі даних та інших технічних засобів.

Зм.	Арк	№ докум.	Підпис	Дата

Активні пристрої в мережі виконують функції маршрутизації та комутації, обробляючи або трансформуючи мережеві сигнали. У межах даного проєкту передбачається впровадження наступного обладнання:

- Керовані комутатори рівня 3 або 2+, що підтримують протоколи spanning tree та забезпечують швидкість передачі даних на портах до 1 Гбіт/с;

- Сервер-шлюз, який забезпечуватиме вихід до Інтернету, а також окремий сервер для централізованого зберігання інформації;

- Бездротові маршрутизатори, сумісні зі стандартом Wi-Fi 802.11ас.

Під час вибору серверного обладнання необхідно враховувати не лише апаратну платформу, але й обрати відповідні серверні операційні системи та необхідне прикладне програмне забезпечення.

Також важливо здійснити аналіз програмної сумісності операційних систем, які планується використовувати на робочих станціях, з урахуванням технічних вимог. Це саме стосується і прикладних програм, що будуть встановлені на клієнтських пристроях.

1.1.4 Вимоги до документації

На всіх стадіях проєктування комп'ютерної мережі необхідно здійснювати ретельне документування - починаючи з формування технічного завдання і завершуючи етапом остаточного тестування системи [2]. У процесі експлуатації важливо фіксувати у відповідній документації всі внесені зміни до мережевої інфраструктури, а також до апаратного або програмного забезпечення клієнтських пристроїв.

Крім того, слід організувати регулярне збирання статистичних показників, здійснювати їх аналіз, а також проводити моніторинг поточного стану мережі. Це дозволяє своєчасно виявляти і вирішувати потенційні проблеми, гарантуючи стабільну роботу системи.

Зм.	Арк	№ докум.	Підпис	Дата

Обов'язковий мінімальний комплект документації має включати такі компоненти:

- Схему логічної структури мережі (логічну топологію).

- План фізичного розміщення обладнання в межах об'єкта (фізична топологія).

- Таблиці призначення IP-адрес для всіх вузлів та клієнтських пристроїв.

- Керівництва з налаштування мережевих вузлів та хостів.

- Акт введення мережі в експлуатацію разом із звітами про проведення тестування.

- Таблиці параметрів конфігурації кожного окремого клієнта мережі.

- Опис апаратного забезпечення та встановленого програмного ПЗ для всіх хостів.

1.1.5 Техніко-економічні показники

Ключові техніко-економічні характеристики проєкту комп'ютерної мережі для ТзОВ «Бучач Друк»:

1. Обрана технологія побудови дротової локальної мережі — 1000Base-ТХ, що забезпечує передачу даних на швидкості до 1 Гбіт/с.

2. Бездротова інфраструктура реалізується на основі стандарту Wi-Fi 802.11ас, що дозволяє досягати високої продуктивності у безпровідному середовищі.

3. Логічна структура мережі є гібридною, поєднуючи елементи різних топологій для оптимального розміщення обладнання і ефективної маршрутизації.

4. Як базова мережева модель використовується стек протоколів TCP/IP, що забезпечує сумісність з сучасним мережевим обладнанням та сервісами.

Зм.	Арк	№ докум.	Підпис	Дата

4. Загальна вартість проєкту, враховуючи монтаж, налаштування та запуск системи, не повинна перевищувати 380 000 грн, згідно з попередніми фінансовими розрахунками, узгодженими із замовником.

1.1.6 Стадії та етапи розробки

№ докум.

Підпис

Дата

Зм

Арк

Епати проектування локальної мережі для ТзОВ «Бучач Друк» для зручності оформлено в таблицю 1.1

Таблиця 1.1 – Узгоджені етапи проектування мережі для ТзОВ «Бучач Друк»

N⁰	Етап	Опис
п.п.		
1	2	3
1	Аналіз вимог	Формування технічного завдання на основі потреб
	замовника	користувача
2	Узгодження і	Оцінка приміщень, визначення кабельних маршрутів,
	планування	розміщення вузлів
3	Вибір обладнання	Формування списку активних і пасивних мережевих
		пристроїв
4	Розробка логічної	Створення структурної схеми мережі з урахуванням
	топології	зв'язків
5	Розміщення	Візуалізація розташування мережевих компонентів у
	обладнання на плані	приміщеннях
6	Монтаж кабельної	Прокладання фізичних з'єднань згідно з планом
	системи	
7	Інсталяція мережевого	Встановлення та початкове налаштування пристроїв
	обладнання	
8	Налаштування служб	Конфігурація служб TCP/IP, DHCP, DNS, безпеки
	мережі	

Продовження таблиці 1.1

1	2	3
9	Тестування мережі	Перевірка функціонування мережі та виправлення
		можливих проблем
10	Оформлення	
	проєктної	Підготовка повного пакету документації для замовника
	документації	

1.1.7 Порядок контролю та прийому

Після завершення впровадження проєкту комп'ютерної мережі необхідно здійснити тестування та оцінку її основних характеристик. До таких показників належать: швидкість з'єднання між мережевими вузлами, обсяг переданих і прийнятих даних на портах, кількість помилкових кадрів, що були надіслані чи отримані, а також навантаження на основні мережеві вузли.

Перевірка цих технічних параметрів здійснюється за допомогою спеціалізованого обладнання (тестерів, аналізаторів) та програмного забезпечення, яке дозволяє вимірювати і записувати ці показники.

Після виконання всіх робіт створюються та затверджуються відповідні акти, які підтверджують факт здачі мережі в експлуатацію замовнику.

1.2 Постановка задачі на розробку проекту. Характеристика підприємства

Об'єктом дослідження і власне кваліфікаційної роботи є проектування комп'ютерної мережі для компанії ТзОВ "Бучач Друк". Для реалізації цієї задачі створюється технічне завдання, яке враховує всі вимоги до мережі, а також здійснюється аналіз будівельного плану на можливість прокладання

Зм.	Арк	№ докум.	Підпис	Дата

кабельних трас і розміщення обладнання. На основі цього визначається оптимальна топологія та технологія побудови структурованої кабельної системи. Далі, враховуючи технічні вимоги та критерії ціна-якість, вибираються активні та пасивні мережеві пристрої. Останнім етапом є монтаж локальної мережі, налаштування активного мережевого обладнання, серверів і служб локальної мережі.

Основними напрямками діяльності ТзОВ «Бучач Друк» є:

1. Видавнича діяльність, яка включає виготовлення друкованої та іншої поліграфічної продукції як дрібно-серійними, так і серійними партіями.

2. Продаж друкованої продукції через магазини-партнери та онлайнплатформи.

3. Надання інформаційно-консультаційних послуг.

4. Організація виставкової та презентаційної діяльності та розробка презентаційних матеріалів і сувенірів.

5. Розробка індивідуальної рекламної та подарункової продукції.

ТзОВ «Бучач Друк» розташоване в двоповерховій будівлі, більшу частину якої займає виробничий цех (друкарня). Висота будівлі складає 6,2 метри (для обох поверхів), проте в друкарському цеху немає перекриттів між поверхами, оскільки тут встановлена велика друкарсько-пакувальна лінія. Інші частини будівлі мають бетонні перекриття між поверхами, на яких розташовані офіси відділів і структурних підрозділів.

Розміщення відділів та структурних підрозділів компанії наведене на кресленні «План приміщень». Основні відділи компанії:

1. Відділ виробництва (друкарський цех).

2. Відділ препрес (додрукової підготовки).

3. Відділи менеджерів і маркетологів.

4. Бухгалтерія.

5. Відділ редакторів і коректорів.

6. Відділ головного інженера та технолога виробництва.

					2025.KBP.123.412.04.00.00 TI3
Зм.	Арк	№ докум.	Підпис	Дата	

- 7. Офіс-менеджер (прийомна).
- 8. Кабінет директора.
- 9. Відділи верстки та дизайну.
- 10. Відокремлена серверна

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	10
Зм.	Арк	№ докум.	Підпис	Дата		10

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Опис та обґрунтування вибору логічного типу мережі

Для створення ефективних локальних мереж важливо застосовувати принцип поділу мережі на віртуальні підмережі [1]. У нашому випадку для маршрутизації між сегментами мережі використовуються комутатори третього рівня.

На першому етапі відбувається сегментація, тобто поділ вузлів локальної мережі на підмережі. При цьому, окрім принципу доцільності, обов'язково слід враховувати аспекти безпеки даних. Подане сегментування можна побачити в таблиці Б1 додатку Б.

У таблиці Б2 додатку Б наведені дані щодо налаштування VLAN на комутаторах, серверах та безпровідних маршрутизаторах.

Таблиці Б1 та Б2 є основними в подальших етапах проєкту та служать основою для конфігурації мережевих пристроїв. Значення, що вказані в цих таблицях, описують характер інформаційних потоків у мережевих сегментах та є важливою частиною технічної документації проєкту мережі.

2.2 Розробка схеми фізичного розташування кабелів та вузлів:

2.2.1 Типи кабельних з'єднань та їх прокладка

План прокладання кабельних сегментів мережі (горизонтальних та вертикальних) був розроблений відповідно до стандартів для структурованих кабельних систем, з урахуванням специфіки планів приміщень і вимог замовника.

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

На кресленнях «Логічна топологія» та «Фізична топологія» представлено всі вузли мережі, а також схеми їх підключення та інтеграції в загальний інформаційний простір.

Фізичне середовище передачі даних у проекті мережі видавництва — це неекранована вита пара категорії 6. Вибір цього типу кабелю обґрунтовано можливістю майбутнього переходу на більш сучасні стандарти, що забезпечить вищу швидкість передачі даних при доступній ціні. Фізична топологія провідної частини мережі реалізована за типом розширеної зірки. Приклад цієї топології зображено на рисунку 2.1.



Рисунок 2.1 – Фізична топологія «Розширена Зірка»

Оскільки в локальній мережі передбачено використання Wi-Fiсегментів, загальна структура мережі набуває гібридного вигляду - поєднання

						A
					2025.КВР.123.412.04.00.00 ПЗ	20
Зм.	Арк	№ докум.	Підпис	Дата		20

розширеної зірки для дротових підключень і комірчастої топології для бездротових зон доступу.

Прокладання кабелів здійснюється від мережевих розеток користувацьких пристроїв через кабельні канали до патч-панелей у комутаційних шафах, де з'єднання виконуються за допомогою патч-кабелів відповідної довжини.

Кабельна інфраструктура є ключовим елементом будь-якої структурованої кабельної системи. Основне її призначення - передача електричних сигналів між пристроями. Існує широкий спектр типів кабелів, які застосовуються залежно від функціонального призначення та умов експлуатації. Якість сигналу прямо залежить від правильності монтажу кабелю, тому дуже важливо дотримуватися технічних вимог виробника під час інсталяції. Лише в цьому випадку система буде функціонувати згідно з проєктними параметрами [4].

З огляду на технічні вимоги, економічну доцільність і можливість подальшої модернізації, для реалізації дротової частини мережі було обрано неекрановану виту пару категорії 6.

Важливим є дотримання нормативного обмеження щодо максимальної довжини кабельного відрізка: вона не повинна перевищувати 90 метрів між мережевими розетками або між розеткою та патч-панеллю. Це правило є обов'язковим і має вирішальне значення для стабільної роботи мережі.

2.2.2 Будова вузлів та необхідність їх застосування

Локальна мережа, розроблена в рамках даного проєкту, складається з таких основних вузлів:

– Пасивні з'єднувальні елементи - мережеві розетки. Їхнє основне призначення полягає у забезпеченні фізичного підключення робочих станцій

Зм.	Арк	№ докум.	Підпис	Дата	

або периферійних пристроїв до мережі. Оптимальне розміщення розеток - біля відповідного обладнання, найчастіше на стіні.

 Комутатори відділів - активні пристрої, які забезпечують з'єднання всіх елементів конкретного сегмента мережі (підгрупи користувачів). Вони виконують функцію комутації мережевих пакетів у межах своїх підмереж.

 Центральний комутатор - є ядром усієї локальної мережі. Саме через нього здійснюється маршрутизація трафіку між окремими сегментами, що забезпечує цілісність інформаційного середовища компанії.

– Сервери локальної мережі - призначені для централізованого зберігання даних на відмовостійких масивах і надання доступу до необхідних сервісів, включно з Інтернетом.

Центральний комутаційний вузол (до якого підключені головний комутатор і сервери) розташований у серверній кімнаті - в спеціалізованій телекомунікаційній шафі висотою 24U. У ній також змонтовано джерело безперебійного живлення (UPS) та патч-панель.

Для даного проекту вибрано шафу Українського виробника моделі ШС-24U, яка зображена на рисунку 2.2.





Проміжні комутаційні вузли представлені комутаторами, розміщеними в окремих відділах. Щоб зменшити загальну вартість проєкту, в цих приміщеннях не передбачено монтажу окремих комутаційних шаф чи патчпанелей. Залежно від побажань замовника, ці комутатори можуть бути встановлені на стіні, розміщені на робочих поверхнях або приховані за фальш-стелею.

2.3 Обґрунтування вибору комунікаційного обладнання

Далі у цьому підпункті розглянемо обґрунтування вибору обладнання, необхідного для побудови локальної обчислювальної мережі ТзОВ «Бучач Друк».

Як уже зазначалося, центральним елементом мережевої інфраструктури є головний комутатор, який забезпечує об'єднання всіх мережевих компонентів. Порівняльний аналіз технічних характеристик різних моделей комутаторів наведено в таблиці В1 додатку В («Технічні характеристики комутаторів»). Враховуючи наявність відповідної моделі у власності підприємства, її функціональну відповідність вимогам проєкту та технічні характеристики, для використання в якості центрального комутатора обрано модель Allied Telesyn AT-х600-24Ts [18].

У структурних підрозділах компанії передбачено встановлення сегментних (відділових) комутаторів. Таке рішення дозволяє локалізувати трафік у межах кожного відділу, зменшуючи навантаження на центральне мережеве обладнання та підвищуючи ефективність маршрутизації.

В більшості випадків комутатори робочих груп монтуються на стіни за допомогою комплектного кріплення.

Порівняння технічних характеристик восьмипортових моделей комутаторів, що розглядалися для використання в підрозділах, представлено в таблиці В2 додатку В.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	22
Зм.	Арк	№ докум.	Підпис	Дата		23

Згідно з результатами аналізу доступних за ціною та придатних за функціональністю рішень, для відділів було обрано модель TP-Link TL-SG3210 [17].

Аналогічну процедуру порівняльного аналізу проведено і для вибору апаратної платформи серверного обладнання. Дані про це наведено в таблиці ВЗ додатку В («Порівняння апаратних реалізацій серверів»).

В результаті аналізу обрано серверну платформу на базі Dell PowerEdge T40 v04, внутрішню будову якого зображено на рисунку 2.3 [14]

Dell PowerEdge T40 v04 — це надійний сервер початкового рівня, який оптимально підходить для невеликих офісів або робочих груп. Його основні переваги:

 Висока надійність - сервер розроблений для безперервної роботи в офісному середовищі, забезпечуючи стабільність та мінімальний ризик простоїв.

– Продуктивність - процесори Intel Xeon забезпечують достатню обчислювальну потужність для базових серверних задач: зберігання даних, спільний доступ, запуск служб локальної мережі.

– Гнучкість конфігурації - підтримує до 127 ГБ оперативної пам'яті DDR4, декілька накопичувачів (HDD/SSD), можливість розширення за допомогою PCIe слотів.

– Компактний форм-фактор - формат Tower дозволяє легко інтегрувати сервер у звичайне офісне середовище.

– Енергоефективність і тиха робота - пристрій оптимізований для офісної експлуатації з низьким рівнем шуму та помірним енергоспоживанням.

– Простота обслуговування - зручний доступ до внутрішніх компонентів спрощує модернізацію, заміну елементів і обслуговування.

Зм.	Арк	№ докум.	Підпис	Дата



Рисунок 2.3 – Внутрішня будова серверу Dell PowerEdge T40

Для забезпечення бездротового підключення мобільних пристроїв, таких як смартфони, ноутбуки та нетбуки, до локальної мережі, необхідно використати маршрутизатор з підтримкою Wi-Fi.

У таблиці В4 додатку В представлено порівняльний аналіз технічних характеристик популярних моделей Wi-Fi маршрутизаторів. З огляду на високу популярність пристроїв виробника Xiaomi, їхню надійність, стабільність роботи та технічні можливості, було прийнято рішення використовувати маршрутизатор саме цієї марки.

У якості базової моделі обрано Хіаоті Мі 4А, який відповідає потребам бездротового сегменту мережі. Технічні характеристики цієї моделі наведено в додатку Г, а її зовнішній вигляд продемонстровано на рисунку 2.4 [22].

Зм.	Арк	№ докум.	Підпис	Дата



Рисунок 2.4 – Wi-Fi роутер Xiaomi Mi 4A

Для забезпечення стабільного електроживлення мережевого обладнання, а також його безперебійної роботи під час короткочасних перебоїв у подачі електроенергії, передбачено використання джерела безперебійного живлення (ДБЖ) APC Smart-UPS 2200VA [13]. Ця модель оснащена акумуляторами підвищеної ємності, що дозволяє підтримувати обладнання живлення критичного впродовж достатнього часу ДЛЯ організованого завершення роботи або перемикання на резервне джерело.

Для тривалого резервного електроживлення (на кілька годин і більше) у розпорядженні видавництва є власна автономна енергосистема на базі дизельного генератора. Це дозволяє забезпечити безперервну роботу локальної мережі навіть у випадку тривалого знеструмлення.

У таблиці 2.1 наведено перелік активного та пасивного мережевого обладнання, використаного у проєкті локальної мережі.

Зм.	Арк	№ докум.	Підпис	Дата	

2025.КВР.123.412.04.00.00 ПЗ

	Таблиця 2.1 – Перелік активного та пасивного обладнання								
N⁰	Назва обладнання	Од.	К-сть	Ціна 1-	Загалы	на			
п/п		вим.		ці, грн.	сума				
					витрат	,			
					грн.				
1	2	3	4	5	6				
1	Комутаційна шафа 24U для	ШТ.	1	10350	1035	0			
	головного комутаційного вузла								
	(серверної)								
2	Патчпанель 24port, cat. 6	ШТ.	1	4120	4120)			
3	Розетка RJ-45 (cat. 6)	ШТ.	33	130	4290)			
4	Кабельні канали	М.	175	50	8750)			
5	Кабель UTP cat.6	М.	610	24	1464	0			
6	Патчкорди cat. 6	ШТ.	50	34	1700)			
7	ДБЖ APC Smart-UPS 2200VA	ШТ.	1	15600	1560	0			
8	Wi-Fi poyrep Xiaomi Mi 4a	ШТ.	2	3200	6400)			
9	Комутатор Allied Telesyn AT-	ШТ.	1	20800	2080	0			
	x600-24Ts								
10	Комутатор TP-Link TL-SG3210	ШТ.	5	3100	1550	0			
11	Сховище даних (файловий	ШТ.	1	46700	4670	0			
	сервер) Dell PowerEdge T40								
12	Шлюз до Інтернету Dell	ШТ.	1	43500	4350	0			
	PowerEdge T40								
				Разом, грн.	192080)			
		2025.k	(BP.123.412.04	4.00.00 ПЗ		Арк 27			
Зм. ,	Арк № докум. Підпис Дата			· · · •		27			

2.4 Особливості монтажу локальної мережі

Правильне прокладання та монтаж неекранованої витої пари (UTP) є критично важливим для забезпечення стабільної роботи Ethernet-мережі та високої якості передачі даних. У проєкті використовується кабель категорії 6, що забезпечує необхідні характеристики швидкості та надійності. Нижче наведено основні вимоги до монтажу [10]:

1. Перевірка типу кабелю. Перед початком інсталяційних робіт необхідно впевнитися, що використовується відповідна категорія кабелю. Для локальної мережі видавництва обрано кабель Cat 6, що підтримує швидкість до 1 Гбіт/с і має хороший запас пропускної здатності для подальшої модернізації.

2. Роз'ємні з'єднання. Для забезпечення якісного електричного контакту між жилами кабелю та мережевими пристроями використовуються стандартні роз'єми RJ-45, сумісні з обраною категорією кабелю. Обтиснення проводиться за допомогою професійного інструменту (кримпера), що гарантує надійне з'єднання.

3. Контроль довжини лінії. Довжина окремого сегменту кабелю не повинна перевищувати 90 метрів - це максимальна допустима довжина для передачі даних без втрати якості сигналу. Надмірно короткі або довгі лінії не рекомендуються, оскільки це може вплинути на стабільність мережі.

4. Монтаж і кріплення. Кабель повинен бути надійно закріплений спеціальними фіксаторами або тримачами для уникнення механічних пошкоджень або натягів. Прокладання здійснюється у кабельних лотках, кабель-каналах або захисних трубах відповідно до внутрішнього планування приміщень.

5. Розгалуження кабельних ліній. У місцях необхідності розгалуження слід застосовувати тільки заводські розгалужувачі або патч-панелі. Категорично забороняється використовувати саморобні з'єднання (скрутки),

						Арі
					2025.КВР.123.412.04.00.00 ПЗ	20
Зм.	Арк	№ докум.	Підпис	Дата		20

оскільки вони погіршують якість сигналу та не відповідають стандартам інсталяції.

6. Відстань від джерел електроживлення. Кабель UTP необхідно прокладати на відстані не менше 50 см від силових кабелів (220 В), щоб уникнути електромагнітних завад. Особливо це важливо для довгих ділянок або місць із високим рівнем електричного навантаженн

2.5 Обгрунтування вибору програмного забезпечення

Усе програмне забезпечення, що використовується для вирішення конкретних завдань у межах локальної мережі, а також для виконання прикладних задач на персональних комп'ютерах користувачів, класифікується на три основні категорії:

- 1. Серверні (спеціалізовані) операційні системи.
- 2. Операційні системи для робочих станцій.
- Прикладне програмне забезпечення, яке може бути локальним або хмарним.

Для серверного обладнання встановлюється таке ПЗ:

1. Функції проксі-сервера, шлюза та DHCP-сервера реалізуються спеціалізованою службою isc-dhcp41-server, яка відповідає за автоматичну видачу IP-адрес. Для забезпечення захисту від зовнішніх загроз використовується міжмережевий екран (фаєрвол) під назвою ipfw. Усі ці компоненти функціонують на операційній системі FreeBSD версії 12.3 [15].

2. Функціонування мережевого файлового сховища забезпечується службами файлового сервера. У цьому випадку використовується програмне забезпечення proftpd, розгорнуте під ОС FreeBSD 12.3.

3. Загалом, при проектуванні мережі видавництва операційні системи для клієнтів не мають критичного значення, тому допустимо використовувати як Windows, так і безкоштовні або альтернативні ОС, які мають повну

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	20
Зм.	Арк	№ докум.	Підпис	Дата		29

підтримку TCP/IP-протоколів. Тим не менше, рекомендується встановлення OC Windows 10 і новіших версій, а також Linux Ubuntu 20 або вище на робочі станції.

Прикладні програми інсталюються відповідно до потреб користувачів і можуть суттєво відрізнятися між собою. Основна вимога — використання безпечного ПЗ без шкідливих модулів або шпигунського функціоналу, який може стати причиною витоку даних.

2.6 Тестування та налагодження локальної мережі

На початковому етапі перевірки комп'ютерної мережі використовують кабельний тестер, який дозволяє визначити справність фізичних з'єднань.

Щоб переконатися в коректності налаштувань мережевого протоколу TCP/IP, доцільно використовувати стандартні команди ping та tracert, які підтримуються більшістю сучасних ОС. Наприклад, операційна система Linux має великий набір утиліт для діагностики локальних мереж.

Нижче наведено деякі з найвживаніших інструментів [20]:

- Ping — базова утиліта, яка широко застосовується для перевірки доступності пристроїв у мережі. Вона надсилає пакети даних на визначену адресу і отримує зворотні відповіді, якщо зв'язок встановлено.

- Traceroute — інструмент, що дозволяє відстежувати маршрут проходження пакетів від одного пристрою до іншого. За допомогою цієї утиліти можна виявити як внутрішні проблеми мережі, так і збої на стороні провайдера.

- Ifconfig — інформативна утиліта, яка надає дані про конфігурацію мережевих інтерфейсів комп'ютера: IP-адреса, MAC-адреса, MTU тощо. Також дозволяє вносити зміни до цих параметрів.

Зм.	Арк	№ докум.	Підпис	Дата

- Netstat — утиліта, що надає статистичну інформацію про активні мережеві з'єднання, відкриті порти та віддалені підключення. Завдяки її звітам можна визначити, які порти задіяні певними службами.

- Tcpdump — ще один засіб аналізу, який дає змогу перехоплювати та досліджувати мережевий трафік, що проходить через локальний комп'ютер.

Отже, вибір відповідного апаратного або програмного інструменту для діагностики залежить від характеру проблеми з мережею, що виникла. Застосування цих засобів дозволяє оперативно виявити та локалізувати джерело збою.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	21
Зм.	Арк	№ докум.	Підпис	Дата		51

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Інструкції з інсталяції і налаштування програмного забезпечення серверів

3.1.1 Інструкція з налаштування служби DHCP

Отже DHCP (протокол автоматичної конфігурації хостів) - це широко використовуваний мережевий протокол, який дозволяє клієнтським пристроям автоматично отримувати налаштування мережі: IP-адресу, маску підмережі, основний шлюз, DNS-сервери та інші параметри мережевого стеку [20].

Принцип його роботи полягає в тому, що комп'ютер-клієнт надсилає запит на отримання параметрів, а DHCP-сервер повертає відповідний пакет із конфігураційними даними. Адміністратор має можливість організовувати адресний простір: створювати підмережі, резервувати певні адреси, а також встановлювати додаткові обмеження. Завдяки DHCP значно скорочується час на налаштування мережі, адже клієнт отримує адресу автоматично, без потреби ручного втручання. Це особливо зручно для великих та бездротових мереж, де ручне налаштування кожного пристрою є неефективним і схильним до помилок.

У рамках проєктованої локальної мережі передбачено використання динамічного призначення IP-адрес для всіх мережевих вузлів. DHCP-сервер буде розгорнутий на операційній системі FreeBSD, яка підключена до центрального комутатора, до якого в свою чергу приєднано декілька підмереж. Це вимагає налаштування окремих пулів адрес для кожної підмережі в конфігураційному файлі DHCP-серверу.

Крім IP-адрес, DHCP повинен автоматично передавати клієнтам наступні дані:

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	22
Зм.	Арк	№ док∨м.	Підпис	Лата		32

DNS-доменне ім'я (наприклад, symfony.local);

IP-адресу DNS-сервера (наприклад, 8.8.8.8);

Шлюз за замовчуванням.

Щоб інсталювати DHCP-сервер, відкрийте термінал з правами адміністратора та виконайте такі команди:

cd /usr/ports/net/isc-dhcpp41-server

make config install clean

У вікні конфігурації буде доступна єдина опція:

[X] DHCP_PARANOIA Enable support for chroot.

Після успішної інсталяції необхідно перейти до налаштування конфігураційного файлу, де задаються інтерфейси, діапазони IP-адрес, шлюзи та інші параметри. Також потрібно переконатися, що служба DHCP додається до автозавантаження системи.

Подальші налатування варто виконати за нижченаведеним взірцем:

```
option domain-name "company.local";
option domain-name-servers 8.8.8.8;
option routers 192.168.101.254;
authorizative;
log-facility locallog7;
subnet 192.168.101.0 netmask 255.255.255.0 {range
192.168.101.1 192.168.101.15;}
host pc1 {hardware ethernet 00:1c:c4:a5:07:ca; fixed-
address 192.168.101.1;}
host pc2 {hardware ethernet d8:d3:85:dc:df:bc; fixed-
address 192.168.101.2;}
host pc3 {hardware ethernet 44:d3:32:dc:45:bc; fixed-
address 192.168.101.3;}
host pc4 {hardware ethernet 12:d1:85:32:df:11; fixed-
address 192.168.101.4;}
```

Слід підкреслити, що наведене вище налаштування стосується лише першої підмережі (VLAN101). Для інших сегментів мережі потрібно створити подібну конфігурацію, орієнтуючись на цей приклад. У конфігураційному файлі вказано такі параметри:

Зм.	Арк	№ докум.	Підпис	Дата

- option domain-name та option domain-name-servers визначають ім'я DNS-домену та список DNS-серверів із зазначенням їх IP-адрес. Ці значення є загальними для всіх підмереж, але в разі необхідності їх можна змінити у відповідному блоці subnet;

- log-facility відповідає за визначення розділу системного журналу, куди потрапляють записи про роботу DHCP-сервера, збої та інші події. Це дає змогу аналізувати поведінку сервера в нестандартних ситуаціях;

- subnet... вказує адресу та маску конкретної підмережі, в межах якої буде здійснюватися розподіл IP-адрес у динамічному режимі;

- host - описує конкретні пристрої, для яких потрібно встановити статичну IP-адресу за допомогою директиви fixed-address.

Щоб служба DHCP запускалась автоматично після старту операційної системи, необхідно внести відповідні записи у файл /etc/rc.conf.

dhcpd_enable="YES"
dhcpd_flags="-q -3"
dhcpd_conf="/usr/local/etc/dhcpd.conf"
dhcpd_ifaces="bge100"
dhcpd_withumask="022"
dhcpd_chuser_enable="YES"
dhcpd_withuser="dhcpd"
dhcpd_withgroup="dhcpd"
dhcpd_chroot_enable="YES"
dhcpd_devfs_enable="YES"
dhcpd_rootdir="/var/db/dhcpd"

Далі подамо стислу інтерпретацію вказаних параметрів.

Зазначені рядки вимикають виведення службових повідомлень (у тому числі діагностичних) на консоль під час старту системи, а також деактивують підтримку протоколу IPv6 з метою оптимізації споживання мережевого трафіку.

Окрім цього, тут задається шлях до конфігураційного файлу DHCP-сервера та визначається мережевий інтерфейс (у прикладі використано ім'я bge100). Це

Зм.	Арк	№ докум.	Підпис	Дата

ім'я потрібно замінити на фактичну назву інтерфейсу, який використовується у вашій системі.

Особливу увагу слід звернути на параметр встановлення маски прав доступу - значення 022, яке блокує можливість запису до створюваних файлів усім, крім власника.

Крім того, конфігурація передбачає запуск служби DHCP в обмеженому середовищі chroot, де кореневий каталог задано як

/var/db/dhcpd,

а процес виконується з правами користувача dhcpd.

Після виконання вищезазначених дій базова конфігурація DHCPсервера вважається завершеною.

Для перевірки працездатності служби виконайте команду

/usr/local/etc/rc.d/isc-dhcpd start

Вона запускає сервер, а також команду

/usr/local/etc/rc.d/isc-dhcpd status

для перегляду поточного стану і параметрів роботи служби.

Якщо у відповідь ви побачите повідомлення: «dhcpd is running as pid», це свідчить про те, що сервер запущено успішно та працює стабільно. Якщо ж буде виведено повідомлення: «dhcpd is not running», це означає, що під час запуску виникла помилка.

У такому випадку потрібно переглянути файл журналу подій, виявити причину збою та внести відповідні зміни до конфігураційних файлів.

В разі успішного старту сервера може з'явитися текстове повідомлення такого змісту:

Зм.	Арк	№ докум.	Підпис	Дата

Starting dhcpd.

Internet Systems Consortium DHCP Server 4.1.2 Copyright 2004-2020 Internet Systems Consortium. Wrote 0 new dynamic host decls to leases file. Wrote 0 leases to leases file.

Listening on BPF/bge1/00:1c:c4:fa:7c:73/192.168.0.0/24 Sending on Socket/fallback/fallback-net

При цьому надання динамічних IP вказаним DHCP-клієнтам також буде супроводжуватися текстовими повідомленнями, які виглядатимуть приблизно наступним чином:

dhcpd: DHCPDISCOVER from 90:21:55:bd:0b:36 via bge1 dhcpd: DHCPOFFER on 192.168.101.1 to 90:21:55:bd:0b:36 (android 81b37c43c8cbaef2) via bge1

dhcpd: DHCPREQUEST for 192.168.101.1 (192.168.101.254) from 90:21:55:bd:0b:36 (android_81b37c43c8cbaef2) via bge1

dhcpd: DHCPACK on 192.168.101.1 to 90:21:55:bd:0b:36 (android 81b37c43c8cbaef2) via bge1

Призначення фіксованих IP-адрес, закріплених за конкретними МАСадресами мережевих інтерфейсів, виконується за наступним принципом:

dhcpd: DHCPDISCOVER from 00:1c:c4:a5:07:ca via bge1

dhcpd: DHCPOFFER on 192.168.101.2 to 00:1c:c4:a5:07:ca via bge1

dhcpd: from the dynamic address pool for 192.168.101.0/24 dhcpd: DHCPREQUEST for 192.168.101.2 (192.168.101.1) from 00:1c:c4:a5:07:ca via bge1

dhcpd: DHCPACK on 192.168.3.2 to 00:1c:c4:a5:07:ca via bge1

Таким чином, наведений спосіб спостереження за роботою DHCPсервера є доступним і зручним у використанні. Водночас для системного

Зм.	Арк	№ докум.	Підпис	Дата	
адміністратора він виступає ефективним і надійним інструментом для контролю за функціональним станом служби.

3.1.2 Інструкції з налаштування програмного маршрутизатора

Програмна маршрутизація у даному проєкті реалізується за допомогою сервісу ірfw, що працює під керуванням операційної системи FreeBSD. Основна функція, яку ми використовуватимемо - це трансляція мережевих адрес (NAT), яка є однією з найбільш популярних можливостей ірfw [25].

Трансляція мережевих адрес (NAT) - це процес, при якому змінюються IP-адреси пакетів даних, коли вони проходять через маршрутизатор або інший мережевий пристрій. Завдяки NAT, приватні мережі можуть використовувати внутрішні (недоступні ззовні) IP-адреси, а доступ до Інтернету здійснюється через одну або кілька публічних адрес. Це дозволяє економити публічні IPадреси, а також покращує безпеку, оскільки внутрішні адреси залишаються прихованими для зовнішніх мереж. NAT часто застосовується в мережах, де потрібно забезпечити Інтернет-доступ для великої кількості пристроїв, одночасно захищаючи їх від потенційних загроз з Інтернету.

Налаштування виконується у кілька етапів:

1. Спочатку необхідно обрати мережевий інтерфейс, через який здійснюватиметься NAT. Якщо, наприклад, використовується інтерфейс з назвою "em0", тоді його слід активувати та присвоїти йому відповідну IPадресу за допомогою наступної команди:

ifconfig em0 inet 192.168.100.1/24 up

2 Далі потрібно задати правила у системі ірfw, які забезпечать маршрутизацію та фільтрацію трафіку між інтерфейсами. Якщо NAT здійснюється через "em0", а підключення до провайдера здійснюється через інтерфейс "em2", слід виконати такі команди

Зм.	Арк	№ докум.	Підпис	Дата

Налаштування правила для NAT, перенаправлення трафіку через інтерфейс em0

ipfw add divert natd ip from any to any via em0

Дозволяємо трафік через інтерфейс em2 (інтерфейс, який з'єднує сервер з провайдером)

ipfw add pass all from any to em2

Увімкнення маршрутизації ІР на сервері, що дозволяє пересилати пакети між мережами

sysctl net.inet.ip.forwarding=1

Запуск служби NAT (natd) для перетворення адрес

/etc/rc.d/natd start3. На завершальному етапі необхідно активувати фаєрвол на NAT-сервері. Щоб обмежити зовнішній доступ до внутрішньої мережі, потрібно вказати відповідні обмеження. Наприклад, щоб заборонити доступ з Інтернету до порту 80, можна застосувати таке правило:

ipfw add deny tcp from any to any 80

Ця послідовність дій дозволяє налаштувати базову маршрутизацію з NAT та забезпечити початковий рівень безпеки внутрішньої мережі. Надалі, залежно від потреб, системний адміністратор зможе розширити чи адаптувати зроблені налаштування системи безпеки.

3.1.3 Інструкції з налаштування служби спільного зберігання файлів

Для організації обміну даними та їх спільного зберігання часто використовується FTP-протокол. Цей протокол відрізняється від інших тим, що для передачі даних за допомогою TCP встановлюються два окремих з'єднання.

Зм.	Арк	№ докум.	Підпис	Дата

Перше з'єднання, яке називається керуючим, служить для обміну командами та відповідями. Воно працює за принципом "клієнт/сервер". Спочатку сервер відкриває порт 21 та чекає на запити від клієнтів. Потім клієнт ініціює з'єднання, відкриваючи порт 21. Це з'єднання залишається активним протягом усього часу, поки триває обмін інформацією між клієнтом та сервером.

Друге з'єднання використовується безпосередньо для передачі даних і залишається активним лише під час фактичного перенесення файлів.

Головною проблемою цього протоколу є те, що дані передаються у відкритому вигляді, без шифрування, що ставить під загрозу конфіденційність. Зокрема, навіть дані для автентифікації передаються у вигляді "простого тексту". Щоб уникнути перехоплення інформації, рекомендується використовувати шифрування, наприклад, SSL.

В цьому проєкті для файлового сервера вибрана операційна система FreeBSD. Це рішення обґрунтоване її підтримкою необхідних протоколів, надійністю, стабільністю, мінімальними вимогами до апаратного забезпечення та безкоштовним доступом. На сервері встановлено ProFTPD з підтримкою TLS, що є криптографічним протоколом для забезпечення безпечної передачі даних між вузлами.

Приклад налаштування ProFtpd + TLS на нашрому сервері наведемо нижче. Отжн почнемо з інсталяці і запуску служби:

cd /user/ports/ftp/proftpd

make config

make install

Далі поступово редагуємо за взірцем запис в proftpd.conf:

ee /usr/local/etc/proftpd.conf

Натупне - створення SSL сертифікату. Він повинен підтримуватися відповідною версією чи реалізацією протоколу TLS. Перевіримо чи сертифікат SSL міститься в каталозі:

						Арн
					2025.КВР.123.412.04.00.00 ПЗ	30
Зм.	Арк	№ докум.	Підпис	Дата		33

/Usr/local/etc/proftpd/ssl.

Можливий варіант, що він відсутній на сервері, тоді створюємо каталог за допомогою команди:

Mkdir /usr/local/etc/proftpd/ssl.

Продедуру ствіорення сертифікату виконано командами:

Генерація нового SSL сертифікату за допомогою OpenSSL.

Параметри:

-new: створення нового запиту на сертифікат

-х509: генерація самопідписаного сертифікату

-days 365: сертифікат дійсний протягом 365 днів

-nodes: без захисту паролем для приватного ключа

-out: шлях для збереження сертифікату

-keyout: шлях для збереження приватного ключа

openssl req -new -x509 -days 365

-nodes -out /usr/local/etc/proftpd/ssl/proftpd.cert.pem

-keyout /usr/local/etc/proftpd/ssl/proftpd/key/pem

На наступному кроці, в разі успішного генерування самого сертифікату необхідно внести відповідні дані. В тому вмпадку робимо активними всі записи щодо TLS в ProFtpd. Щоб активувати TLS на сервері, необхідно просто видалити символи коментарів із відповідних рядків у конфігураційному файлі proftpd.conf за взірцем:

ee /usr/local/etc/proftpd/proftpd.conf

Include /usr/local/etc/proftpd/tls.conf

Конфігураційний файл редагується відповідно до шаблону, наданого в tls.conf:

Редагуємо конфігураційний файл для TLS

Задаємо шлях до логів для TLS

TLS Log /var/log/proftpd/tls.log

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

Вказуємо протокол TLS, який буде використовуватись

TLS Protocol SSLv23

Вимикаємо запит сертифіката від клієнта

TLS Options NoCertRequest

Вказуємо файл сертифіката сервера

TLSA CertificateFile /etc/proftpd/ssl/proftpd.cert.pem

Вказуємо файл ключа сервера

TLSA CertificateKeyFile /etc/proftpd/ssl/proftpd.key.pem

Відключаємо перевірку клієнтського сертифіката

TLS VerifyClient off

Вимикаємо обов'язкове використання TLS для всіх підключень

TLS Required on

Робимо ProFtpd командою:

/usr/local/etc/rc.d/proftpd.sh

Пробуємо підключитися клієнтом, який підтримує SSL-з'єднання. Якщо виникне проблема під час підключення, необхідно перевірити файл журналу для опису помилки.

/var/log/proftpd/tls.conf.

Іноді варто передбачити загальну папку для обміну файлами між клієнтами мережі або для організації черги друку. Спочатку необхідно створити саму папку, наприклад:

/home/public/files

Для налаштування автоматичного запуску ProFTPd при завантаженні системи, в файлі /etc/rc.conf загальної конфігурації операційної системи необхідно додати наступний рядок

proftpd_enable=«yes»

Щоб зміни вступили в силу, потрібно перезавантажити систему за допомогою команди:

						Api
					2025.КВР.123.412.04.00.00 ПЗ	11
Зм.	Арк	№ докум.	Підпис	Дата		41

Shutdown -r now

Основні налаштування FTP-сервера завершено. Під час експлуатації сервера можна вносити зміни до його конфігурації, додаючи необхідні правила для коригування його роботи.

3.2 Інструкції з налаштування активного комутаційного обладнання

3.2.1 Інструкції з налаштування головного комутатора

Комутатори третього рівня використовуються для поділу локальної мережі на окремі сегменти, що дозволяє ефективно використовувати широкий домен мережі та покращує її технічні характеристики. VLAN (віртуальна локальна мережа) є групою хостів, які взаємодіють між собою, якби вони знаходились в одному домені чи робочій групі, незважаючи на своє фізичне розташування.

Це дозволяє об'єднувати кінцеві точки, навіть якщо вони не підключені до одного комутатора. VLAN функціонують подібно до фізичних локальних мереж, але надають гнучкість у їх організації, дозволяючи змінювати структуру мережі через програмну конфігурацію, а не фізичні зміни у підключенні пристроїв.

Однією з ключових переваг використання VLAN є можливість зміни конфігурації мережі без необхідності переміщувати комп'ютери або пристрої фізично. Всі необхідні зміни можна здійснити шляхом перепрограмування параметрів на комутаторі.

Для налаштування центрального комутатора необхідно виконати наступні кроки:

Спочатку створюємо потрібні VLAN, увійшовши в режим конфігурації портів:

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	12
Зм.	Арк	№ докум.	Підпис	Дата		42

Вхід в режим VLAN конфігурації на комутаторі для створення VLAN Sw6(config)# vlan database

Створення VLAN 101 з назвою vlan101 Sw6(config-vlan)# vlan 101 name vlan101 # Створення VLAN 102 з назвою vlan102 Sw6(config-vlan)# vlan 102 name vlan102 # Створення VLAN 103 з назвою vlan103 Sw6(config-vlan)# vlan 103 name vlan103 # Створення VLAN 104 з назвою vlan104 Sw6(config-vlan)# vlan 104 name vlan104 # Створення VLAN 105 з назвою vlan105 Sw6(config-vlan)# vlan 105 name vlan105 # Створення VLAN 106 з назвою vlan106 Sw6(config-vlan)# vlan 106 name vlan106 # Створення VLAN 107 з назвою vlan107 Sw6(config-vlan)# vlan 107 name vlan107 # Створення VLAN 108 з назвою vlan108 Sw6(config-vlan)# vlan 108 name vlan108 # Створення VLAN 109 з назвою vlan109 Sw6(config-vlan)# vlan 109 name vlan109 # Створення VLAN 110 з назвою vlan110 Sw6(config-vlan)# vlan 110 name vlan110 # Створення VLAN 111 з назвою vlan111 Sw6(config-vlan)# vlan 111 name vlan111 # Створення VLAN 112 з назвою vlan112 Sw6(config-vlan)# vlan 112 name vlan112 Робимо доступні додані vlan:

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

vlan 101-112 state enable

Послідовно конфігуруємо кожен порт свяча, до якого підключено відповідний комутатор групи, або сервери чи окремі робочі станції: # Налаштування інтерфейсу port1.0.1 для доступу до VLAN 104 Sw6(config-if)# interface port1.0.1 Sw6(config-if)# switchport access vlan 104 # Налаштування інтерфейсів port1.0.2-5 для доступу до VLAN 105 Sw6(config-if)# interface port1.0.2-5 Sw6(config-if)# switchport access vlan 105 # Налаштування інтерфейсів port1.0.6-11 для доступу до VLAN 106 Sw6(config-if)# interface port1.0.6-11 Sw6(config-if)# switchport access vlan 106 # Налаштування інтерфейсу port1.0.12 для доступу до VLAN 107 Sw6(config-if)# interface port1.0.12 Sw6(config-if)# switchport access vlan 107 # Налаштування інтерфейсів port1.0.13-17 для роботи в режимі trunk Sw6(config-if)# interface port1.0.13-17 Sw6(config-if)# switchport mode trunk Наведемо приклад налаштування IP-адрес для VLAN інтерфейсів на комутаторі. Це дозволяє кожному VLAN мати свою окрему IP-адресу, що необхідно для маршрутизації між VLAN або для управління комутатором: # Налаштування IP-адреси для VLAN 1 (за замовчуванням) Sw6(config)# interface vlan 1 Sw6(config-if)# ip address 192.168.1.1 255.255.255.0 Sw6(config-if)# no shutdown # Налаштування IP-адреси для VLAN 104 Sw6(config)# interface vlan 104 Sw6(config-if)# ip address 192.168.104.1 255.255.255.0

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

Зм.	Дарк № докум. Підпис Дата 2025.КВР.123.412.04.00.00 ПЗ	45
		Арк
	Sw6(config)# interface vlan 11	
	# Налаштування IP-адреси для VLAN 11	
	S3(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.10.1 255.255.255.0	
	Sw6(config)# interface vlan 10	
	# Налаштування IP-адреси для VLAN 10	
	Sw6(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.9.1 255.255.255.0	
	Sw6(config)# interface vlan 9	
	# Налаштування IP-адреси для VLAN 9	
	Sw6(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.8.1 255.255.255.0	
	Sw6(config)# interface vlan 8	
	# Налаштування IP-адреси для VLAN 8	
	Sw6(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.107.1 255.255.255.0	
	Sw6(config)# interface vlan 107	
	# Налаштування IP-адреси для VLAN 107	
	Sw6(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.106.1 255.255.255.0	
	Sw6(config)# interface vlan 106	
	# Налаштування IP-адреси для VLAN 106	
	Sw6(config-if)# no shutdown	
	Sw6(config-if)# ip address 192.168.105.1 255.255.255.0	
	Sw6(config)# interface vlan 105	
	# Налаштування IP-адреси для VLAN 105	
	Sw6(config-if)# no shutdown	

Sw6(config-if)# ip address 192.168.11.1 255.255.255.0 Sw6(config-if)# no shutdown

I на завершення задаємо маршрут «за замовчуванням»: Sw6(config)#ip route 0.0.0.0/0 192.168.105.253

Якщо цей маршрутизатор чи комутатор входить до складу корпоративної мережі та має підключення до Інтернету через шлюз, то вказана команда направляє весь трафік без визначеного маршруту до зазначеного шлюзу, що забезпечує з'єднання з зовнішніми мережами.

3.2.2 Інструкції з налаштування комутаторів робочих груп

Для того, щоб почати налаштування комутатора, спершу необхідно вручну призначити йому відповідну IP-адресу, а також налаштувати логін і пароль для віддаленого доступу. Крім цього, під час роботи комутатора слід передбачити налаштування засобів контролю якості пакетів, що передаються в межах локальної мережі.

Налаштуємо обліковий запис системного адміністратора за наступним прикладом [17]:

Створення облікового запису адміністратора з ім'ям "tplink", рівнем доступу "admin" та паролем "admin"

TL-link(config)#user name tplink privilege admin password 0 admin

Налаштування контролю доступу для користувача з IP-адресою 192.168.101.1, обмежуючи доступ до комутатора з цієї конкретної адреси.

TL-link(config)#user access-control ip-based 192.168.101.1 255.255.255.255

Основні налаштування включають в себе конфігурацію правил для функціонування віртуальних мереж (VLAN) на кожному окремому комутаторі в мережі. Ці налаштування визначають, як комутатори будуть обробляти пакети даних, сегментуючи мережу на окремі логічні мережі, що

Зм.	Арк	№ докум.	Підпис	Дата

дозволяє знизити навантаження та покращити безпеку і ефективність комунікацій між пристроями в межах мережі..

Наведений нижче перелі налаштувань дозволяє налаштувати VLAN та порти для роботи в режимах access і trunk відповідно, що необхідно для коректної роботи сегментованої мережі

1. Створення VLAN та призначення йому імені:

TL-link(config)# vlan2 # Створюємо VLAN з ідентифікатором 2

TL-link(config)# interface vlan2 # Перемикаємося в конфігурацію інтерфейсу VLAN2

TL-link(config-vlan)# name group2 # Призначаємо ім'я VLAN2 як "group2"

2. Налаштування портів для приєднання до конкретного VLAN: TL-link(config)# interface gigabitEthernet 1/0/2-5 # Вибираємо порти 1/0/2 до 1/0/5 для налаштування

TL-link(config-if)# switchport mode access # Переводимо порти в режим доступу (Access)

TL-link(config-if)# switchport access vlan 101 # Призначаємо порти до VLAN 101

3. Налаштування першого порту в режимі trunk:

TL-link(config-if)# switchport mode trunk # Встановлюємо режим trunk для порту

3.2.3 Інструкції з налаштування маршрутизаторів

У цьому підрозділі описується основний процес налаштування точки доступу Wi-Fi. Потрібно визначити SSID для різних частотних діапазонів

Зм.	Арк	№ докум.	Підпис	Дата

(якщо точка доступу працює в двох діапазонах) та встановити пароль для підключення до бездротової мережі.

SSID (Service Set Identifier) - це унікальне ім'я, яке ідентифікує бездротову мережу Wi-Fi. Воно дозволяє пристроям знаходити доступні точки доступу та підключатися до них. SSID може бути відкритим (публічним) або прихованим. Приховані SSID не відображаються у списку доступних мереж, що додає рівень безпеки, хоча не є надійним захистом від зловмисників.

Також для забезпечення безпеки переданих через мережу даних слід вибрати один з варіантів шифрування та налаштувати його відповідно до вимог.

Отже, встановимо параметри шифрування, як показано на рисунку 3.1.

	When the feature is will switch to 5G net	on, 2.4G and 5G networks will sh work If the device is close, and to	a name. The router will ch 4G network if it's far away.	oose the best available signal. For example, it Brief interruptions may occur during the swite
Wi-Fi				
	Switch	* Enable © Disable		
	Xiaomi_09E9	Name		
	Devices won't be	able to see this network		
	Mixed (WPA/WPA2	e-personal) Encryption 🤝		
		Password 👁		
	2.4G options			
	Auto (2)	Wireless channel \checkmark		
	High	Simal draneth su		

Рисунок 3.1 – Параметри шифрування wi-fi сегменту

Для підвищення безпеки мережі необхідно змінити стандартний пароль для входу в систему управління Wi-Fi роутером. Це запобігає несанкціонованому доступу до налаштувань маршрутизатора. Як згадувалося

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	18
Зм.	Арк	№ докум.	Підпис	Дата		40

раніше, всі бездротові пристрої та точка доступу будуть отримувати IP-адреси від DHCP-сервера локальної мережі, тому важливо налаштувати відповідні параметри локального інтерфейсу бездротового маршрутизатора.

Wi-Fi маршрутизатор оснащений корисним набором інструментів для моніторингу та збору статистики, що дозволяє адміністратору відслідковувати рівень завантаження процесора і загальний стан мережі, що полегшує управління та покращує ефективність мережі.

Взірець результатів наведемо на рисунку 3.2 (Закладка «Router info»).

Router info				
Mi Router 4A Giga Version	MiWiFi Release 2.28.132	50:D2:F5:07:09:E9	23319/20040888 IN	
Real-time network status Real-time downstream speed: 0.16KB/S	Real-time upstream speed:	Connected devices ba	ndwidth	Client: 1
0.48KB/S			Enginere1 597.3KB	100.0%
250(0)				
200KBm				
150KEm				
toocbis				
50054		Total download: 635.9K8	/ Total upload: 295.56KB / Dev	ices: 1
Bandwidth: ~ M / Max download spe	ed: 171.56K8/5			
CPU	CPU load:0.70%	Storage		Used:36.00%
100%		100%		
875		80%		

Рисунок 3.2 – Вікно перегляду статусу і статистики

3.3 Інструкція з використання тестових наборів та тестових програм

Тестер кабелю є важливим інструментом для перевірки кабелів типу UTP. Цей простий пристрій дає змогу перевірити, чи правильно підключено провідники в кабелі, виявити пошкодження або обриви провідників. Коли кабель підключено до тестера, на екрані з'являється індикація правильності

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	10
Зм.	Арк	№ докум.	Підпис	Дата		49

підключення провідників. У разі коректного з'єднання на екрані з'являється напис «OK» або «PASS». Якщо виникає проблема з підключенням, тестер відобразить повідомлення про помилку, вказуючи на точне місце обриву чи інший тип пошкодження.

Використання тестера кабелів UTP є важливим кроком для забезпечення якісного з'єднання в мережі, оскільки навіть незначні пошкодження можуть впливати на швидкість передачі даних, що, в свою чергу, знижує ефективність мережі.

Професійні кабельні тестери - це спеціалізовані інструменти, призначені для перевірки та тестування кабельних з'єднань в мережах. Вони використовуються для виявлення проблем з кабелями, таких як неправильне підключення проводів, обриви, коротке замикання, перехрещування або пошкодження. Професійні тестери забезпечують більш точну та детальну діагностику кабелів, що особливо важливо при роботі з великими інфраструктурами або складними мережами.

Для діагностики мережевих з'єднань також використовуються програмні інструменти, наприклад, команда ping. Вона надсилає пакет запиту до вказаного хоста для перевірки доступності мережі. Якщо хост доступний, буде отримано відповідь з вказівкою часу, який потрібен для обміну пакунками. Якщо відповідь не надійшла або була перевищена максимальна тривалість очікування, це може вказувати на проблеми з адресою, перевантаження мережі чи відсутність хоста [21].

Ще одним корисним інструментом є команда tracert, яка дозволяє з'ясувати шлях, яким проходять пакети через мережу, показуючи інформацію про кожен проміжний пристрій на шляху до кінцевого хоста. Це дає змогу краще зрозуміти, як працює мережа і де можуть виникати затримки.

Для моніторингу роботи операційної системи FreeBSD є кілька утиліт. Одна з них - ps, яка виводить список усіх активних процесів і користувачів. Якщо необхідно постійно оновлювати інформацію, можна використовувати

						/
					2025.КВР.123.412.04.00.00 ПЗ	
Зм.	Арк	№ докум.	Підпис	Дата		l ^s

команду top, яка дозволяє отримати актуальні дані про ресурси системи та активні процеси.

3.4 Інструкція з експлуатації та моніторингу в мережі

FreeBSD має набір інструментів для моніторингу системних ресурсів, які дають адміністраторам змогу відстежувати процеси та використовувані ресурси операційної системи. Ось кілька основних утиліт:

top - дозволяє в реальному часі переглядати список активних процесів та їхнє використання ресурсів, таких як процесор, пам'ять і пристрої вводу/виводу. Користувачі можуть сортувати процеси за різними критеріями й налаштовувати розмір екрану.

vmstat - надає узагальнену інформацію про використання системних ресурсів, зокрема ЦП, пам'яті та дисків. Користувачі можуть контролювати обсяг дискових ресурсів і кількість активних процесів.

iostat - орієнтована на моніторинг дискової підсистеми та дає користувачам можливість спостерігати за швидкістю передачі даних і використанням простору на жорстких дисках.

netstat - відображає інформацію про мережеві з'єднання та використання мережевих ресурсів, зокрема пропускну здатність трафіку і кількість переданих пакетів. Адміністратори можуть перевіряти стан підключень і переглядати параметри мережевих інтерфейсів.

systat - дає змогу моніторити використання різних системних ресурсів, таких як ЦП, пам'ять, порти та інтерфейси, а також відображати інформацію про активні процеси та мережеві з'єднання.

Таким чином, утиліта top є потужним інструментом для відстежування використання системних ресурсів у FreeBSD. Вона дозволяє бачити список процесів, їхній взаємозв'язок із системою та використання ресурсів. У процесі роботи утиліта показує інформацію про ідентифікатори процесів, власників,

					202
Зм.	Арк	№ докум.	Підпис	Дата	

команди, використану пам'ять, введення/виведення та стан кожного процесу. Крім того, користувачі можуть сортувати список процесів за різними критеріями, такими як використання пам'яті чи навантаження на диск.

Утиліта також надає можливість переглядати загальні й тривалі статистичні дані про використання системних ресурсів, що робить її корисним інструментом для системних адміністраторів у FreeBSD. Тому її використання є важливим для адміністрування мережі.

3.5 Інструкції з налаштування засобів захисту мережі

Забезпечення безпеки локальної мережі є однією з основних задач у галузі інформаційної безпеки, адже це безпосередньо впливає на захист конфіденційної інформації від несанкціонованого доступу, можливих кібератак та інших загроз. Мережеві інфраструктури, особливо в умовах сучасних технологій та інтернет-загроз, вимагають належної уваги до безпеки на всіх рівнях комунікацій. Важливим елементом захисту є інтеграція власних мережевих пристроїв, таких як маршрутизатори, комутатори та брандмауери, які дозволяють систематично та ефективно контролювати всі аспекти мережевих з'єднань та доступу [21].

Рівні захисту мережі. Одним із основних способів підвищення безпеки є налаштування правил на рівні маршрутизації. За допомогою маршрутизаторів можна визначати маршрути для передавання даних і фільтрувати мережевий трафік, що проходить через мережу, на основі специфічних політик безпеки. Наприклад, використання брандмауерів і маршрутизаторів дозволяє забезпечити фільтрацію вхідного та вихідного трафіку, знижуючи ймовірність атак на мережу.

З іншого боку, налаштування безпеки на рівні комутаторів дає змогу контролювати доступ до мережевих портів. Комутатори забезпечують функцію віртуальних локальних мереж (VLAN), що дозволяє сегментувати

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	52
Зм.	Арк	№ докум.	Підпис	Дата		52

мережу та обмежити доступ до окремих її частин. Це важливий крок у захисті локальної мережі, оскільки дозволяє ізолювати критичні сегменти і зменшити ризик поширення атак.

Засоби контролю доступу та автентифікація. Не менш важливим етапом є налаштування доступу до ресурсів мережі. Базовим елементом захисту є використання надійних паролів, двофакторної автентифікації та організація доступу на основі ролей (RBAC). Це дозволяє обмежити доступ до чутливої інформації і забезпечити розмежування прав доступу для різних користувачів мережі. Однак, для забезпечення найвищого рівня безпеки варто використовувати складні паролі, що ускладнює спроби їх злому за допомогою атак на основі підбору [21].

Для ще більшого підвищення рівня захисту в умовах передачі чутливої інформації, важливим впровадження шифрування кроком £ даних. Використання протоколів безпеки, таких як SSL/TLS, для захищених з'єднань між клієнтами серверами, дозволяє не тільки забезпечити та конфіденційність, але й гарантує цілісність та аутентифікацію передаваних даних. Це критично важливо для захисту від атак "Man-in-the-Middle" (МІТМ), які можуть стати причиною витоку чутливої інформації.

Виявлення та захист від кібератак. Не менш важливим елементом безпеки є використання спеціалізованого програмного забезпечення для виявлення і блокування потенційно шкідливих програм, а також для запобігання кібератакам. Антивірусні системи, фаєрволи та системи виявлення і запобігання вторгнень (IDS/IPS) допомагають захистити мережу від шкідливих програм, атак на основі вразливостей та інших видів загроз. Крім того, такі системи можуть виявляти незвичну активність в мережі, що може свідчити про спробу зламу або порушення політики безпеки.

Також важливим є налаштування засобів моніторингу та логування, які дозволяють своєчасно виявляти аномалії в роботі мережі, проводити аудит доступу і фіксувати всі події, пов'язані з потенційними загрозами. Це дає

						Арк	
					2025.КВР.123.412.04.00.00 ПЗ		
Зм.	Арк	№ докум.	Підпис	Дата		55	

можливість швидко реагувати на інциденти безпеки та вживати заходів для їх усунення.

Оновлення програмного забезпечення та навчання користувачів

Враховуючи динамічність сучасних загроз, забезпечення безпеки локальної мережі потребує постійної актуалізації програмного забезпечення на мережевих пристроях та комп'ютерах, підключених до мережі. Регулярні оновлення операційних систем, додатків і програмних продуктів є критично важливими для захисту від відомих вразливостей, які можуть бути використані кіберзлочинцями для проникнення в мережу.

Нарешті, одним із ключових аспектів безпеки є навчання користувачів мережі щодо основ інформаційної безпеки. Системи захисту можуть бути надзвичайно потужними, однак вони не матимуть ефективності без усвідомлення користувачами загроз, таких як фішинг, соціальна інженерія та інші методи атак. Регулярне проведення тренінгів та інформаційних кампаній щодо безпеки є необхідним кроком для зменшення людського фактора в атаках.

Використання брандмауера ipfw. Одним із найбільш ефективних засобів захисту локальної мережі є налаштування брандмауера ipfw на сервері. Цей брандмауер дозволяє ефективно фільтрувати мережевий трафік на різних рівнях OSI-моделі (канальному, мережевому та транспортному), блокуючи небажаний трафік і дозволяючи лише авторизовані з'єднання. Його висока продуктивність і гнучкість налаштувань дозволяють адаптувати правила фільтрації відповідно до потреб конкретної мережі.

Таким чином, забезпечення безпеки локальної мережі є складним і багатогранним процесом, що вимагає використання різноманітних технічних і організаційних заходів. Ключовими елементами є налаштування надійного доступу, шифрування даних, моніторинг трафіку, своєчасні оновлення та навчання користувачів. Це дозволяє створити надійний захист від зовнішніх і

Зм.	Арк	№ докум.	Підпис	Дата

внутрішніх загроз та забезпечити конфіденційність і цілісність інформації в локальній мережі.

Для запобігання несанкціонованому доступу до мережі, ми можемо налаштувати додаткові правила безпеки, наприклад, заборонити доступ до порту 23 (Telnet), оскільки це небезпечний протокол.

Забороняємо Telnet доступ

ipfw add deny tcp from any to any 23.

						Арн
					2025.КВР.123.412.04.00.00 ПЗ	55
Зм.	Арк	№ докум.	Підпис	Дата		50

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічної частини кваліфікаційної роботи є здійснення економічних розрахунків, спрямованих на обчислення собівартості та повної ціни проекту мережі. Також важливим є визначення економічної ефективності розробки для ТзОВ «Бучач Друк» і прийняття рішення про її подальше впровадження в роботу.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

Таблиця 4.1 - Середній час виконання НДР та стадій технологічного процесу

No			Час викон.
	Назва операції (стадії)	Виконавець	операції,
11/11			год.
1	2	3	4
1	Постановка задачі та збір інформації про	Керівник	5
	об'єкт. Формування технічного завдання.	проекту	5
2	Розробка проекту (Проектування логічної та фізичної топології локальної мережі) Вибирається пасивне та активне мережеве обладнання.	Інженер	15
3	Монтаж мережі. На даному здійснюється монтаж на підключення пасивного мережевого обладнання.	Технік	40
	2025.KBP.12.	3.4 <i>12.04.00.00</i>	ПЗ

Зм

Арк

№ докум.

Підпис

Дата

Продовження таблиці 4.1

1	2	3	4
4	Налагодження мережі. На даному етапі інсталюються ОС серверів та робочих станцій. Конфігуруються мережеві служби та сервіси. Далі виконується тестування роботи.	Інженер	20
5	Підготовка документації. На даному етапі готується технічна документація на локальну мережу. Інструкції з налаштування служб та сервісів.	Інженер	10
	Разом	-	90

Сумарний час виконання операцій технологічного процесу, які будуть виконуватись для проектування локальної мережі для ТзОВ «Бучач Друк» складає 90 годин.

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

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

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

Основна заробітна плата розраховується за формулою:

$$\mathcal{G}_{OCH.} = T_c \cdot \mathcal{K}_{\mathcal{C}}, \qquad (4.1)$$

					2025.КВР.123.412.04.00.00 ПЗ	Арк
						57
3м.	Арк	№ докум.	Підпис	Дата		57

де *T_c* – тарифна ставка, грн.;

К_г – кількість відпрацьованих годин.

Отже, основна заробітна плата для працівників становить:

1. Керівник проекту - $3_{\text{осн1}} = 5 \cdot 120 = 600$ грн.

2. Інженер - $3_{\text{осн2}} = 45 \cdot 90 = 4050$ грн.

3. Технік - $3_{\text{осн3}} = 40 \cdot 60 = 2400$ грн.

Сумарна основна заробітна плата становить:

З_{осн} = 600 + 4050 + 2400 =7050,00 грн.

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

$$3_{\partial o \partial .} = 3_{o c H.} \cdot K_{\partial o n \pi.}$$
, (4.2)

де *К*_{допл.} – коефіцієнт додаткових виплат працівникам: 0,1 – 0,15.

Отже, додаткова заробітна плата по категоріях працівників становить:

- керівника проекту: $3_{дод1} = 600 \cdot 0, 13 = 78$ грн.
- інженера: $3_{\text{дод2}} = 4050 \cdot 0, 13 = 526, 50$ грн.
- техніка: З_{дод3}= 2400 · 0,13 = 312,00 грн.

Зм

Загальна додаткова заробітна плата становить:

Звідси загальні витрати на оплату праці розраховуються за формулою 4.3:

$$B_{o.n.} = 3_{och.} + 3_{dod}$$
, (4.3)

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

$$B_{c.3.} = \Phi O \Pi \cdot 0,22, \tag{4.4}$$

					Арк
				2025.КВР.123.412.04.00.00 ПЗ	58
Арк	№ докум.	Підпис	Дата		50

де ФОП – фонд оплати праці, грн.

 $B_{c.3}$ = 7966,5 · 0,22 = 1752,63 грн.

Проведені розрахунки витрат на оплату праці зведемо у таблицю 4.2.

		Основна	і заробітна	плата, грн.	Лолатк.	Hapax.	Всього
№ п/п	Категорія працівни- ків	Тариф. ставка, грн.	К-сть від- працьов.	Фактично нарах. з/пл., грн.	зароб. плата, грн.	на ФОП, грн.	витрати на оплату праці, грн.
			год.				
1	Керівник	120	5	600,00	78,00	-	-
	проекту						
2	Інженер	90	45	4050,00	526,50	-	-
3	Технік	60	40	2400,00	312,00	-	-
	Р	азом		7050,00	916,50	1752,63	9719,13

T (10	n ·			•
Tabinung 4.7 -	Звелені	DOBDAXVHKI	и витрат на	оппату праш
1 аолицл 1.2	оведени	pospanymin	i biiipui iiu	оплату праці

Отже, загальні витрати на оплату праці становлять 9719,13 грн.

4.3 Розрахунок матеріальних витрат

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

$$M_{Bi} = q_i \cdot p_i \tag{4.5}$$

де *q_i* – кількість витраченого матеріалу *i*-го виду;

p_i – ціна матеріалу *і*-го виду.

Зм

Звідси, загальні матеріальні витрати можна визначити за формулою 4.6:

$$\mathcal{G}_{M.6.} = \sum M_{Bi} \tag{4.6}$$

					Арк
				2025.КВР.123.412.04.00.00 ПЗ	50
Арк	№ докум.	Підпис	Дата		59

Проведені розрахунки занесемо у таблицю 4.3.

JNO	Назва обладнання	Од.	К-	Ціна 1-ці,	Загальна
п/п		вим.	сть	грн.	сума витрат,
					грн.
1	2	3	4	5	6
1	Комутаційна шафа 24U для	ШТ.	1	10350	10350
	головного комутаційного				
	вузла (серверної)				
2	Патчпанель 24port, cat. 6	ШТ.	1	4120	4120
3	Розетка RJ-45 (cat. 6)	шт.	33	130	4290
4	Кабельні канали	М.	175	50	8750
5	Кабель UTP cat.6	М.	610	24	14640
6	Патчкорди cat. 6	ШТ.	50	34	1700
7	ДБЖ APC Smart-UPS	ШТ.	1	15600	15600
	2200VA				
8	Wi-Fi poyrep Xiaomi Mi 4a	ШТ.	2	3200	6400
9	Комутатор Allied Telesyn	ШТ.	1	20800	20800
	<u>AT-x600-24Ts</u>				
10	Комутатор ТР-Link TL-	ШТ.	5	3100	15500
	SG3210				
11	Сховище даних (файловий	ШТ.	1	46700	46700
	сервер) Dell PowerEdge T40				
12	Шлюз до Інтернету Dell	ШТ.	1	43500	43500
	PowerEdge T40				
					102080

Підпис

Зм.

Арк

№ докум.

Дата

Загальна сума матеріальних витрат на розробку мережі становить 192080 грн.

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію одиниці обладнання розраховуються за формулою 4.7:

$$3_e = W \cdot T \cdot S \tag{4.7}$$

де *W* – необхідна потужність, кВт; *T* – кількість годин роботи обладнання; *S* – вартість кіловат-години електроенергії.

Час роботи ПК над даним проектом становить 8 годин, споживана потужність - 0,5 кВт/год, вартість 1 кВт електроенергії для промислових підприємств в робочий час (7-19 год) на момент розрахунку становить – 7,00 грн. Тому витрати на електроенергію будуть становити:

$$3_e = 0,5 \cdot 8 \cdot 7,00 = 28,00$$
 грн.

4.5 Визначення транспортних затрат

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

$$T_{e} = 3_{\text{M.B.}} \cdot 0,08...0,1, \tag{4.8}$$

де Т_в – транспортні витрати.

Отже, транспортні витрати будуть становити:

 $T_{e} = 192080,00 \cdot 0,09 = 17287,20$ грн.

					2025.КВР.123.412.04.00.00 ПЗ
Зм.	Арк	№ докум.	Підпис	Дата	

_{Арк} 61

4.6 Розрахунок суми амортизаційних відрахувань

Комп'ютери та оргтехніка належать до четвертої групи основних фонді. Мінімально допустимі строки їх використання 2 роки [19]. Для визначення амортизаційних відрахувань використовуємо формулу:

$$A = \frac{B_B \cdot H_A}{100\%} \cdot T, \tag{4.9}$$

де A – амортизаційні відрахування за звітний період, грн.; E_B – балансова вартість групи основних фондів на початок звітного періоду, грн.; H_A – норма амортизації, %; T – кількість годин роботи обладнання, год.

Враховуючи, що ПК працює над даним проектом 8 год., балансова вартість ПК – 33000 грн., тому:

$$A = \frac{33000 \cdot 0.04}{150} \cdot 8 = 70.4 \text{грн.}$$

4.7 Обчислення накладних витрат

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

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

$$H_{e} = B_{o.n.} \cdot 0, 2...0, 6, \tag{4.10}$$

де *H*_в – накладні витрати.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	62
Зм.	Арк	№ докум.	Підпис	Дата		02

*H*_e = 7966,67 · 0,4 = 3 186,67 грн.

4.8 Складання кошторису витрат та визначення собівартості НДР

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

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

Зміст витрат	Сума, грн.	В % до загальної
		суми
Витрати на оплату праці	7966,67	3,57
Відрахування на соціальні заходи	1752,63	0,79
Матеріальні витрати	192080,00	86,11
Витрати на електроенергію	28,00	0,01
Транспортні витрати	17287,20	7,75
Амортизаційні відрахування	70,40	0,03
Накладні витрати	3 186,67	1,74
Собівартість	222 371,57	100,00

Таблиця 4.4 - Кошторис витрат на НДР

Собівартість (С_в) НДР розрахуємо за формулою 4.11:

$$C_{6} = B_{o.n.} + B_{c.3.} + 3_{M.6.} + 3_{6} + T_{6} + A + H_{6}$$
(4.11)

Отже, собівартість дорівнює: $C_{e} = 222 \ 371,57 \ грн.$

Зм.	Арк	№ докум.	Підпис	Дата

2025.КВР.123.412.04.00.00 ПЗ

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою 4.12:

$$\mathcal{U} = C_{\theta} \cdot (1 + P_{peh}) \cdot (1 + \Pi \mathcal{A}B), \qquad (4.12)$$

де C_{θ} – собівартість виконання НДР;

*Р*_{рен.} – рівень рентабельності,

ПДВ – ставка податку на додану вартість.

 $U = 222 \ 371,57 \cdot (1+0,3) \cdot (1+0,2) = 346 \ 899,65$ 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.

Для визначення ефективності продукту розраховують чисту теперішню вартість (ЧТВ), можна визначити за формулою 4.13 та термін окупності ($T_{o\kappa}$), який можна визначити за формулою 4.14.

$$\Psi TB = -K_{B} + \sum_{i=1}^{t} \frac{\Gamma_{II}}{(1+i)^{t}},$$
(4.13)

де К_В – затрати на проект;

Г_п – грошовий потік за t – ий рік;

t – відповідний рік проекту;

і - величина дисконтної ставки (10...15%).

Якщо $\text{ЧTB} \ge 0$, то проект може бути рекомендований до впровадження.

Зм.	Арк	№ докум.	Підпис	Дата	

2025.КВР.123.412.04.00.00 ПЗ

_{Арк} 64

$$\Psi TB = -222371,57 + \frac{194538,1}{(1+0,15)} + \frac{194538,1}{(1+0,15)^2} = 93890,75 \,\mathrm{rph}$$

Термін окупності визначається за формулою:

$$T_{OK} = T_{\Pi B} + \frac{H_B}{\Gamma_{\Pi P}}$$
(4.14)

де Т_{ПВ} – період до повного відшкодування витрат, років;

Н_В – невідшкодовані витрати на початок року, грн.;

 $\Gamma_{\Pi P}$ – грошовий потік на початок року, грн.

$$T_{OK} = 1 + \frac{53208,00}{194538,1} = 1,3$$

Всі дані розрахунків внесемо в зведену таблицю 4.5 технікоекономічних показників.

№ п/п	Показник	Значення
1.	Собівартість, грн.	222 371,57
2.	Плановий прибуток, грн.	66 711,47
3.	Ціна, грн.	346 899,65
4.	Чиста теперішня вартість, грн.	93890,75
5.	Термін окупності, рік	1,3

Таблиця 4.5 - Техніко-економічні показники розробки мережі

Загальна вартість розробленої комп'ютерної мережі для ТзОВ «Бучач Друк» становить 346 899,65 грн. Термін окупності становить 1,3 роки.

Отже загальна вартість розробленої мережі поміщується в граничну межу замовника (380 тис. грн.), має хороший рівень рентабельності та термін окупності і рекомендується до впровадження.

					ſ
Зм.	Арк	№ докум.	Підпис	Дата	

5 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ

У сучасних умовах проблемою державної та суспільної значущості стає забезпечення безпеки життєдіяльності населення, збереження головної цінності - її громадян, їх здоров'я та життя. Виходячи з сучасних уявлень, безпека життєдіяльності є багатогранним об'єктом розуміння й сприйняття дійсності, що потребує інтеграції різних стратегій, сфер, аспектів, форм і рівнів пізнання [3].

Дотримання базових засад і положень охорони праці є важливим аспектом організації роботи будь-якого підприємства від малого офісу до промислових гігантів. В даному розділі роботи буде описано питання на яких грунтується безпека праці в ТзОВ "Бучач Друк".

5.1 Законодавча база з питань охорони праці на якій ґрунтується безпека праці в ТзОВ "Бучач Друк"

В Україні встановлено законодавчі норми, що регулюють права й обов'язки громадян, а також визначають структуру органів влади та промисловості. Основним законом держави є Конституція України, яка гарантує рівні права та свободи всім громадянам. Зокрема, вона забезпечує право на вільний вибір роботи з безпечними і здоровими умовами праці, право на відпочинок, соціальний захист у випадку втрати працездатності або в старості, а також інші соціальні гарантії. Усі закони та нормативно-правові акти повинні відповідати положенням Конституції та не суперечити їй.

Рамковим документом у галузі охорони праці є Закон України «Про охорону праці», що був ухвалений Верховною Радою України 14 жовтня 1992 року з наступними змінами та доповненнями до нього.Правове регулювання охорони праці в Україні ґрунтується на низці законодавчих актів, серед яких

Зм.	Арк	№ докум.	Підпис	Дата

основними є Закон України «Про охорону праці» та Кодекс законів про працю (КЗпП) [3].

Далі детальніше зупинимось на Законі України «Про охорону праці», який прийнятий 14 жовтня 1992 року та оновлений 21 листопада 2002 року, визначає правові засади забезпечення безпечних та нешкідливих умов праці. Закон складається з дев'яти розділів, які регламентують основні принципи державної політики у сфері охорони праці, права та обов'язки суб'єктів трудових відносин, а також порядок організації системи управління охороною праці [3].

У першому розділі Закону окреслено базові терміни та принципи, серед яких пріоритет життя і здоров'я працівника над виробничими результатами, повна відповідальність роботодавця за створення безпечних умов праці, соціальний захист працівників, а також норма про перевагу міжнародних договорів над національним законодавством у сфері охорони праці.

Другий розділ гарантує працівникам право на інформування про умови праці, компенсацію за шкідливі умови, соціальне страхування, забезпечення засобами індивідуального захисту та відмову від виконання робіт, що становлять загрозу життю або здоров'ю.

Розділ третій визначає обов'язки роботодавців щодо створення системи управління охороною праці. Закон вимагає створення служби охорони праці на підприємствах із чисельністю понад 50 осіб, а також передбачає обов'язкове проведення навчань, інструктажів і медичних оглядів працівників. Фінансування охорони праці покладається на роботодавця і становить від 0,2% до 0,5% залежно від джерела фінансування.

Четвертий розділ встановлює механізми економічного стимулювання заходів з охорони праці. Визначено, що витрати, пов'язані з аваріями та розслідуванням їх причин, покриває роботодавець.

Зм.	Арк	№ докум.	Підпис	Дата

У п'ятому розділі йдеться про нормативно-правові акти, що регулюють охорону праці, обов'язкові для виконання всіма суб'єктами господарювання. Ці документи мають переглядатися не рідше ніж раз на 10 років.

Розділи шостий і сьомий визначають структуру державного управління та нагляду за охороною праці. Визначено повноваження Кабінету Міністрів України, спеціалізованих центральних органів виконавчої влади, місцевих адміністрацій, а також профспілок, які здійснюють громадський контроль.

Восьмий розділ описує відповідальність за порушення законодавства: дисциплінарну, адміністративну, матеріальну та кримінальну. Максимальний штраф становить 5% від місячного фонду оплати праці.

У заключному, дев'ятому розділі, визначено дату набуття чинності закону та вказано перелік нормативно-правових актів, ухвалених для його реалізації. Серед них – положення про розслідування нещасних випадків, механізми відшкодування шкоди, правила накладення штрафів та інші документи, затверджені Кабінетом Міністрів України.

Далі наведемо основні положення Кодексу законів про працю України (КЗпП). Отже Кодекс законів про працю України (КЗпП) - це основний нормативно-правовий акт, що регулює трудові правовідносини між працівником і роботодавцем [3]. Прийнятий у 1971 році, він неодноразово зазнавав змін відповідно до суспільно-економічних трансформацій, зокрема після здобуття Україною незалежності.

КЗпП складається з преамбули та 18 розділів, які охоплюють усі ключові аспекти трудового права: від укладення трудового договору до умов його припинення, регулювання робочого часу, охорони праці, соціального захисту тощо. Основні аспекти, які регулює Кодекс [5]:

1. Трудовий договір

Кодекс закріплює порядок укладення, зміни та припинення трудового договору (розділ III). Передбачено, що договір може бути безстроковим, строковим або таким, що укладається на час виконання певної роботи.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	69
Зм.	Арк	№ докум.	Підпис	Дата		00

Установлено обов'язок оформлення трудових відносин наказом (розпорядженням) та ведення трудової книжки.

2. Робочий час і час відпочинку

КЗпП регламентує норму тривалості робочого часу (не більше 40 годин на тиждень), скорочену тривалість для окремих категорій працівників, а також порядок надання вихідних, святкових та щорічних відпусток (розділи IV–V).

3. Оплата праці

Визначено принципи нарахування заробітної плати, гарантії мінімального рівня оплати праці, порядок виплат, строки та відповідальність роботодавця за затримку зарплати (розділ VI). Передбачено також захист прав працівників у разі банкрутства підприємства.

4. Гарантії та компенсації

Кодекс містить положення щодо соціальних гарантій працівників, у тому числі під час мобілізації, тимчасової непрацездатності, навчання, переведення на іншу роботу тощо (розділ VII).

5. Охорона праці

У розділі XI викладено основи правового регулювання охорони праці. Роботодавець зобов'язаний забезпечити безпечні й нешкідливі умови праці, організувати навчання з питань безпеки, забезпечити працівників засобами індивідуального захисту, а також здійснювати медичні огляди.

6. Трудова дисципліна

Розділ X встановлює правила внутрішнього трудового розпорядку, механізми заохочення та дисциплінарної відповідальності, порядок накладення стягнень і їх оскарження.

7. Особливості праці окремих категорій працівників

У Кодексі приділено увагу умовам праці жінок, неповнолітніх, осіб з інвалідністю та інших соціально вразливих груп (розділ XIII). Закріплено

					20,
Зм.	Арк	№ докум.	Підпис	Дата	

обмеження на виконання важких та небезпечних робіт, гарантії додаткового захисту та пільг.

8. Захист трудових прав

Кодекс передбачає створення трудових колективів, діяльність профспілок, участь працівників в управлінні підприємствами (розділи XIV– XV), а також механізми вирішення трудових спорів, включно з порядком їх розгляду в комісіях з трудових спорів або в суді (розділ XVI) [5].

Безпосередньо в умовах товариства «Бучач Друк» важливим розділом Кодексу законів про працю є розділ "Охорона праці". В ньому зазначено, що на будь-якому об'єкті, де працюють люди, повинні бути створені здорові й безпечні умови праці, що відповідають вимогам охорони праці. Всі будівлі і обладнання не повинні створювати загрози працюючим, а також негативно впливати на стан їхнього здоров'я та самопочуття.

Роботодавець або уповноважені ним органи повинні:

– дбати про умови праці, їх полегшення, оздоровлення навколишнього середовища, виконання правил безпеки й інструкцій з охорони праці;

– забезпечувати контроль здоров'я для працівників із шкідливими умовами праці, забезпечувати спецодягом та засобами захисту працюючих від шкідливого впливу речовин, що використовуються в процесі праці;

 – слідкувати за дотриманням трудового законодавства на підлеглому об'єкті, створювати умови для здійснення контролю за умовами праці, дбати про відпочинок працюючих.

5.2 Вимоги охорони праці до рівнів шуму та вібрації на робочих місцях

Гранично дозволений рівень шуму закріплений у Державних санітарних нормах допустимих рівнів шуму в приміщеннях житлових та громадських

Зм.	Арк	№ докум.	Підпис	Дата

будинків і на території житлової забудови (наказ Міністерства охорони здоров'я від 22.02.2019 № 463) [5].

Так, допустимі рівні звуку в приміщеннях визначаються за рівнем звукового тиску постійного шуму (дБА) та критеріями шуму (NC).

Зокрема, у житлових приміщеннях допустимий рівень шуму вдень (08:00 - 22:00) - 40 дБА, а вночі (22:00 - 08:00) - 30 дБА. При цьому максимальний рівень вдень - 55 дБА, вночі - 45 дБА. Для загального розуміння: рівень звуку 30 дБА - це шепіт і цокання настінного годинника; 45 дБА - звук звичайної розмови; 65 дБА - звук голосної розмови, який чітко чутно стороннім [3].

Для офісів та приміщень, обладнаних персональними комп'ютерами або технікою для бізнесу допустимий рівень шуму цілодобово - 50 дБА, а максимальний - 65 дБА. Також для приміщень для розташування шумних агрегатів – 75 дБА, а для промислових приміщень - 90 дБА [5]

Крім офісних приміщень в склад друкарні входить власне друкарський цех. Джерелом шуму в нашому друкарському цеху є друкарська машина КВА Compacta 213. Отже у даному виробничому приміщенні рівень шуму становить 80 дБА, що відповідає допустимим санітарно-гігієнічній нормі що дорівнює 90 дБА [3] Відповідно до ДСН 3.36-037-99.

Для зменшення шкідливого рівня шуму використовують в основному організаційно–технічні методи, що включають використання малошумних технологічних процесів, оснащення машини засобами дистанційного керування, удосконалення технології ремонту та обслуговування, використання раціональних режимів праці та відпочинку.

Разом з тим в друкарському офсетному цеху друкарні вібрація по джерелу утворення є технологічна, тобто передається різними шляхами від технологічного обладнання та транспортно-технологічна (передається від стаціонарно встановлених машин). Тому для захисту від вібрації на даному підприємстві використовуються такі методи :

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	71
Зм.	Арк	№ докум.	Підпис	Дата		

- віброізоляція – досягається встановленням машин на спеціальні віброізолятори, застосування гнучких елементів в системах трубопроводів та комунікацій, використовуються еластичні прокладки у трубопроводах і т.д.;

- віброгасіння динамічного виду досягається встановленням друкарської машини на масивному фундаменті. Маса фундаменту має бути підібрана таким чином, щоб амплітуда коливань підошви фундаменту не перевищувала 0,1 – 0,2 мм. Також по місцях проходу повинні бути встановлені вибропоглинаючі килимки.

5.3 Утримання евакуаційних шляхів і виходів з приміщення ТзОВ "Бучач Друк"

Утримання евакуаційних шляхів і виходів в потрібному стані є дуже важливим для своєчасного евакуації людей та матеріальних цінностей. Забороняється зменшувати кількість та розміри евакуаційних виходів з будівель і приміщень, зменшувати класи вогнестійкості несучих та огороджувальних конструкцій, застосовувати будівельні матеріали з вищими показниками пожежної небезпеки, змінювати інженерні та планувальні рішення й умови освітлення згідно з нормованою вимогою.

У розміщення технологічного, експозиційного разі та іншого обладнання у приміщеннях повинні бути забезпечені евакуаційні проходи до сходових кліток та інших шляхів евакуації. Розміщення крісел в актових i конференц-залах, залах зборів і нарад та В інших подібних приміщеннях повинно відповідати вимогам ДБН В.1.1-7:2016 «Пожежна безпека об'єктів будівництва. Загальні вимоги», ДБН В.2.2-9-2009, «Громадські будинки та споруди», ДБН В.2.2-13-2003 «Спортивні та фізкультурно-оздоровчі ДБН B.2.2-28:2010 споруди», «Будинки ДБН В.2.2-16-2005 адміністративного побутового призначення», та «Культурно-видовищні та дозвіллєві заклади» [5].

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	72
Зм.	Арк	№ докум.	Підпис	Дата		12
У приміщенні, яке має один евакуаційний вихід, дозволяється одночасно розміщувати (дозволяється перебування) не більше 50 осіб.

Двері на шляхах евакуації повинні відчинятися в напрямку виходу з будівель (приміщень).

Не нормується напрямок відчинення дверей для [5]:

- квартир у житлових будинках;
- приміщень з одночасним перебуванням не більше ніж 15 осіб,
 крім приміщень категорій А і Б за вибухопожежною та пожежною небезпекою;
- комор і технічних приміщень площею не більше ніж 200 м² і без постійних робочих місць;
- технічних поверхів площею не більше ніж 200 м², у яких розміщується тільки інженерне обладнання та/або прокладаються інженерні мережі будинку, і у яких відсутні постійні робочі місця;
- балконів, лоджій (за винятком дверей, що ведуть до зовнішньої повітряної зони сходових кліток типу Н1);
- виходів на площадки сходів типу СЗ;
- санітарних вузлів. За наявності людей у приміщенні двері евакуаційних виходів можуть зачинятися лише на внутрішні запори, які відчиняються зсередини без ключа.

Килими, килимові доріжки й інше покриття підлоги у приміщеннях з одночасним перебуванням 50 та більше осіб, коридорах, на сходових клітках повинні кріпитися до підлоги і бути помірно небезпечними щодо токсичності продуктів горіння, мати помірну димоутворювальну здатність та відповідати групам поширення полум'я РП1, РП2.

Сходові марші і площадки повинні мати справні огорожі із поручнями, котрі не повинні зменшувати ширину сходових маршів і площадок.

На сходових клітках (за винятком незадимлюваних) дозволяється встановлювати прилади опалення, у тому числі на висоті 2,2 м та вище від

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	73
Зм.	Арк	№ докум.	Підпис	Дата		13

поверхні проступів та сходових площадок, сміттєпроводи, поверхові сумісні електрощити, поштові скриньки та пожежні кран-комплекти за умови, що це обладнання не зменшує нормативної ширини проходу сходовими площадками та маршами.

Сходові клітки, внутрішні відкриті та зовнішні сходи, коридори, проходи та інші шляхи евакуації мають бути забезпечені евакуаційним освітленням. Світильники евакуаційного освітлення повинні вмикатися з настанням сутінків у разі перебування в будинку людей.

Світлові покажчики «Вихід» необхідно постійно утримувати справними. У залах для глядачів, виставкових, актових залах та інших подібних приміщеннях вони мають бути увімкнуті на весь час перебування людей (проведення заходу).

На випадок відключення електроенергії обслуговуючий персонал будинків (крім житлових), де у вечірній та нічний час можливе перебування людей, повинен мати електричні ліхтарі. Кількість ліхтарів визначається адміністрацією, виходячи з особливостей об'єкта, наявності чергового персоналу, кількості людей у будинку (але не менше одного ліхтаря на кожного

працівника, який чергує на об'єкті у вечірній або нічний час). Сміттєзбірні камери та стволи повинні регулярно очищатися від сміття та горючих відходів, які треба збирати на спеціально виділених майданчиках у контейнери або ящики з негорючих матеріалів.

Двері сміттєзбірних камер повинні утримуватися замкненими на замок.

Порядок експлуатації пожежних ліфтів визначається чинним законодавством.

Не допускається [23]:

улаштовувати на шляхах евакуації пороги, виступи, турнікети,
 двері розсувні, підйомні, такі, що обертаються, та інші пристрої,
 які перешкоджають вільній евакуації людей;

					2025.KBP.123.412.04.00.00 ПЗ
Зм.	Арк	№ докум.	Підпис	Дата	

- захаращувати шляхи евакуації меблями, обладнанням, різними матеріалами;
- забивати, заварювати, замикати на замки, болтові з'єднання та інші запори, що важко відчиняються зсередини, двері на шляхах евакуації та евакуаційних виходах;
- розташовувати у тамбурах виходів, за винятком квартир та індивідуальних житлових будинків, гардероби, вішалки для одягу, сушарні, пристосовувати їх для торгівлі, а також зберігання, у тому числі тимчасового, будь-якого інвентарю та матеріалу;
- захаращувати меблями, устаткуванням та іншими предметами двері, люки на балконах і лоджіях, переходи в суміжні секції та виходи на зовнішні евакуаційні драбини, евакуаційні площадки квартир житлових будинків;
- знімати встановлені на балконах (лоджіях) драбини;
- улаштовувати у сходових клітках приміщення будь-якого призначення (кіоски), обладнання;
- улаштовувати у загальних коридорах комори і вбудовані шафи,
 за винятком шаф для інженерних комунікацій, зберігати в шафах (нішах) для інженерних комунікацій горючі матеріали;
- розташовувати в ліфтових холах приміщення різного призначення;
- робити засклення або закладання жалюзі і отворів повітряних зон у незадимлюваних сходових клітках;
- знімати двері вестибюлів, холів, тамбурів і сходових кліток;
- заміняти скло, що не дає скалок при руйнуванні, на звичайне у дверях;
- знімати пристрої для самозачинення дверей сходових кліток, коридорів, холів, тамбурів, а також фіксувати самозакривні двері у відчиненому положенні;

					2
Зм.	Арк	№ докум.	Підпис	Дата	

2025.КВР.123.412.04.00.00 ПЗ

- зменшувати нормативну площу фрамуг у зовнішніх стінах сходових кліток або закладати їх;
- розвішувати у сходових клітках на стінах дзеркала, стенди, панно, інші горючі матеріали.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	76
Зм.	Арк	№ докум.	Підпис	Дата		70

висновки

В кваліфікаційній роботі проведено анлаіз технічного завдань та вимог замовника, зроблено аналітичний огляд літератури та існуючих рішень в даному напрямку. Розроблено логічну та фізичну топологію мережі. Вибрано для мережі пасивне та активне комутаційне обладнання, сервери та їх програмне забезпечення.

Особливу увагу звернуто на конфігурування служби DHCP, та проксісервера для доступу до мережі Інтернет. Для забезпечення інформації безпеки мережі в цілому сконфігуровано міжмережевий екран ірfw.

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

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

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

					ſ
Зм.	Арк	№ докум.	Підпис	Дата	

ПЕРЕЛІК ПОСИЛАНЬ

1. Антонов В. М. Сучасні комп'ютерні мережі: Навч. Посібник. Київ: «МК-Прес». 2015. 480с.

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

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

4. Калита Д. М. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: навч. посіб. для студ. вищих закл. освіти. К. : ВПЦ "Київський ун-т", 2023. 326с.

5. В.І. Кошель, Г.П. Сав'юк, Б.С. Дзундза. Основи охорони праці. навчально-методичний посібник для студентів вищих навчальних закладів педагогічного напрямку. Івано-Франківськ: НАІР, 2020. 182 с.

6. Мельник I. Проектування та дослідження комп'ютерних мереж. К.: Університет «Україна», 2020. 362 с.

7. Методичні вказівки для виконання кваліфікаційної роботи із спеціальності 123 "Компютерна інженерія"/ Тернопіль: ВСП ТФК ТНТУ, 2022.

8. Москальова В.М. Основи охорони праці: Підручник. К.: ВД "Професіонал", 2015. 672с.

9. Николайчук Я.М. Проектування спеціалізованих комп'ютерних систем: Навчальний посібник. Тернопіль: ТзОВ "Терно-граф", 2010. 392с.

10. Погорілий С.Д.. Комп'ютерні мережі. Апаратні засоби та протоколи передачі даних: Підручник К.: ВПЦ "Київський університет, 2018. 138с.

11. Ткаченко В. Комп'ютерні мережі та телекомунікації: навч. посіб. Харків: НТУ "ХПІ", 2011. 224 с.

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	70
Зм.	Арк	№ докум.	Підпис	Дата		/0

12. Царьов Р. Ю. Структуровані кабельні системи : навч. посіб. для студентів вищих навчальних закладів. Одеса: ОНАЗ ім. О.С. Попова, 2013. 260 с

13. APCSmartUPS2000:URL:https://www.apc.com/shop/al/en/products/APC-Smart-UPS-2200VA-Rack-Mount-LCD-230V-with-SmartConnect-Port/P-SMT2200RMI2UC/ (дата звернення:26.05.2025).

14. DellPowerEdgeT40:URL:https://www.dell.com/rs/business/p/poweredge-t40/pd (дата звернення: 26.05.2025).

15. FreeBSD 12.2: URL: https://www.freebsd.org/releases/12.2R/schedule//. (дата доступу: 26.05.2025).

16. IPWF на FreeBSD: URL: https://intellect.icu/fajervol-ipfw-vo-freebsd-nastraivaem-s-nulya-primer-prostogo-konfiga-11170/ (дата зверення: 26.05.2025).

17. TL-SG3210.URL: https://www.tp-link.com/ru-ua/products/details/cat-42_TL-SG3210.html. (дата звернення: 26.05.2025).

18. x600-24Ts: URL: https://www.alliedtelesis.com/products/switches/x600-24ts/. (дата звернення: 26.05.2025).

19. Амортизаціяосновнихзасобів.URL:http://www.visnuk.com.ua/ua/pubs/id/3728/(дата зверненя: 03.06.2025).

20. Базові поняття мережевих технологій URL: http://um.co.ua/8/8-17/8-1748.html. (дата звернення: 16.05.2025).

21. Безпека мережі. URL: https://uk.wikipedia.org/wiki/Безпека_мережі. (Дата зверення: 10.06.2025).

22. Poyrep Xiaomi Mi wi-fi 4A URL: https://www.xiaomi.ua/routerxiaomi-mi-wi-fi-router-4a-global-dvb4230gl/p33565/ (Дата звернення: 26.05.2025).

23. Утримання евакуаційних шляхів та виходів. URL: https://nmc.dsns.gov.ua/upload/1/6/9/7/1/sait-pdf-faili-ldistnavc-pb-tema-13.pdf. (Дата зверення: 22.05.2025).

					2025.KBP.123.412.04.00.00 FI
Зм.	Арк	№ докум.	Підпис	Дата	

ДОДАТОК А. ТАБЛИЦЯ ІР-АДРЕС

Таблиця А1 – Таблиця ІР-адрес

N⁰	Позна	Назва кабінету	VLA	Адреса	Шлюз	
Π/Π	чення	(відділу)	Ν	вузла/Маска		
	вузла					
1	2	3	4	5	6	
1	WS_1	Відділ додрукової	101	192.168.101.1/24	192.168.101.25	4
2	WS_2	підготовки і		192.168.101.2/24	192.168.101.25	4
3	WS_3	кольороподілу		192.168.101.3/24	192.168.101.25	4
4	WS_4	Виробничий відділ	102	192.168.102.1/24	192.168.102.25	4
5	WS_5			192.168.102.2/24	192.168.102.25	4
6	WS_6	Бухгалтерія	103	192.168.103.1/24	192.168.103.25	4
7	WS_7			192.168.103.2/24	192.168.103.25	4
8	WS_8			192.168.103.3/24	192.168.103.25	4
9	WS_9			192.168.103.4/24	192.168.103.25	4
10	WS_10	Директор	104	192.168.104.1/24	192.168.104.25	4
11	WS_11	Сист. адмін		192.168.104.2/24	192.168.104.25	4
12	WS_12	Відділ верстки і	106	192.168.106.1/24	192.168.106.25	4
13	WS_13	дизайну		192.168.106.2/24	192.168.106.25	4
14	WS_14			192.168.106.3/24	192.168.106.25	4
15	WS_15			192.168.106.4/24	192.168.106.25	4
16	WS_16			192.168.106.5/24	192.168.106.25	4
17	WS_17			192.168.106.6/24	192.168.106.25	4
18	WS_18			192.168.106.7/24	192.168.106.25	4
19	WS_19	Менеджери і	107	192.168.107.1/24	192.168.107.25	4
20	WS_20	маркетологи		192.168.107.2/24	192.168.107.25	4
21	WS_21			192.168.107.3/24	192.168.107.25	4
22	WS_22			192.168.107.4/24	192.168.107.25	4
23	WS_23			192.168.107.5/24	192.168.107.25	4
24	WS_24	Магазин-склад		192.168.107.6/24	192.168.107.25	4
25	WS_25	Редактори і	108	192.168.108.1/24	192.168.108.25	4
26	WS 26	коректори		192.168.108.2/24	192.168.108.25	4
27	WS 27			192.168.108.3/24	192.168.108.25	4
28	WS 28			192.168.108.4/24	192.168.108.25	4
29	WS_29	Гол. Інженер	109	192.168.109.1/24	192.168.109.25	4
30	WS_30	Гол. Технолог	109	192.168.109.2/24	192.168.109.25	4
31	WS_31	Прийомна	110	192.168.110.1/24	192.168.110.25	4
32	AP_1	Менеджери	107	192.168.107.50/24	192.168.107.25	4
					<u> </u>	
\square			20	ר וח כרו ממע אין	רח חס	Ľ
1	1		ZU	2.7.10P. 12.3.4 12.04.00	1.00 113	1

	Продон	зження таблиці А1			
1	2	3	4	5	6
33	AP_2	Кімната	111	192.168.111.50/24	192.168.111.254
		відпочинку			
34	S_1	Серверна	105	192.168.105.252/24	192.168.105.254
35	S_2		105	192.168.105.253/24	192.168.105.254
			-	Надається провайде	ООМ
36	SW_1	Відділ додрукової	1	192.168.1.1/24	192.168.1.254
		підготовки і			
		кольороподілу			
37	SW_2	Бухгалтерія	1	192.168.1.2/24	192.168.1.254
38	SW_3	Відділ верстки і	1	192.168.1.3/24	192.168.1.254
		дизайну			
39	SW_4	Менеджери і	1	192.168.1.4/24	192.168.1.254
		маркетологи			
40	SW_5	Редактори і	1	192.168.1.5/24	192.168.1.254
		коректори			
41	SW_6	Серверна	1	192.168.1.6/24	192.168.1.254

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	Q1
Зм.	Арк	№ докум.	Підпис	Дата		01

додаток б. дані сегментування локальної мережі

Таблиця Б1 - Таблиця логічної адресації локальної мережі

N⁰	Позначення	Робоча	l	Назва кабінету та	a	Номер	Адреса
п/п	вузлів	група/]	К-	його номер		VLAN	підмережі/
		сть вуз	лів				Маска
1	2	3	4	5	6	7	8
1	WS_1-WS_3,	-	4	Відділ	-	101	192.168.101.0/24
	SW_1			додрукової			
				підготовки і			
				кольороподілу			
2	WS_4-WS_5	-	2	Виробничий	-	102	192.168.102.0/24
				відділ			
3	WS_6 -	-	5	Бухгалтерія	-	103	192.168.103.0/24
	WS_9, SW_2						
4	WS_10,		2	Директор, сист.		104	192.168.104.0/24
	WS_11			адміністратор			
5	S_1, S_2,	-	4	Серверна	-	105	192.168.105.0/24
	SW_6						
6	WS_12-		6	Відділ верстки і	-	106	192.168.106.0/24
	WS_18,			дизайну			
	SW_3						
7	WS_19-	-	8	Менеджери і	-	107	192.168.107.0/24
	WS_24,			маркетологи			
	SW_4, AP_1						
	1	I	1	1	1	1	1

Зм.	Арк	№ докум.	Підпис	Дата

Продовження таблиці Б1.							
1	2	3	4	5	6	7	8
8	WS_25-	-	5	Редактори і	-	108	192.168.108.0/24
	WS_28,SW_5			коректори			
9	WS_29,	-	1	Гол. Інженер і	-	109	192.168.109.0/24
	WS_30			технолог			
10	WS_31	-	1	Прийомна	-	110	192.168.110.0/24
11	AP_2			Кімната		111	192.168.111.0/24
				відпочинку			

Таблиця Б2 - Таблиця конфігурування VLAN

N⁰	Позначення вузла	Ном.	Тип	Назва	Номер	Тип	Номер
Π/Π		порту	порту	пристрою	порту	порту	VLAN
1	WS_1-WS_3	Eth0	-	SW_1	2-4	Access	101
2	WS_4-WS_5	Eth0	-	SW_1	5-6	Access	102
3	WS_6 - WS_9	Eth0	-	SW_2	2-5	Access	103
4	WS_10-WS_11	Eth0	-	SW_6	1-2	Access	104
5	S_1, S_2	Eth0,	-	SW_6	3-4	Access	105
		Eth0					
6	WS_12-WS_18	Eth0	-	SW_3	2-8	Access	106
7	WS_19-WS_24, AP_1	Eth0	-	SW_4,	2-7, 5	Access	107
				SW_6			
8	WS_25-WS_28,	Eth0	-	SW_5	2-6	Access	108
9	WS_29-WS_31	Eth0	-	SW_6	2-4	Access	109
10	WS_30	Eth0	-	SW_6	5	Access	110
11	SW_1	1	Trunk	SW_6	11	Trunk	-
12	SW_2	1	Trunk	SW_6	12	Trunk	-
13	SW_3	1	Trunk	SW_6	13	Trunk	-
14	SW_4	1	Trunk	SW_6	14	Trunk	-
15	SW_5	1	Trunk	SW_6	15	Trunk	-
16	AP_2	1	Trunk	SW_6	15	Trunk	
							Арк
Зм. А	ок № докум. Підпис Да	ama	202	'5.KBP.123.47	12.04.00.0	10 1 13	83

додаток в. мережеве обладнання

	Allied Telesyn	TP-Link	Mikrotik CRS125-
	AT-x600-24Ts	T2600G-28TS	24G-1S-RM
1	2	3	4
Підтримувані функції	L2, L3		
Комутація кадрів	96	56	50
Гбіт/с			
Кадрів/пакетів в	71,4	41,67	30
секунду			
К-сть портів	24+4	24+4	24+1
10/100/1000 BASE-TX			
Засоби віддаленого	WEB, Telnet, SSH	I	I
керування			
Підтримка технології	Так		
VLAN			

Таблиця В1 – Технічні характеристики комутатора

Таблиця В2 – Порівняльна характеристика 8-ми портових комутаторів

	TP-Link	Planet	HP
1	2	3	4
Модель	TL-SG3210	GSD-1002M	V1810-8G
Пропускна здатність	14,9 млн. пакетів	14,9 млн. пакетів	11,9 млн. пакетів
	за секудну	за секудну	за секудну
Швидкість шини	20 Гбіт/с	20 Гбіт/с	16 Гбіт/с
комутатора			

Зм.	Арк	№ докум.	Підпис	Дата

Продовження	габлиці В2		
1	2	3	4
К-сть портів 10/1000	8 + 2 SFP	8 + 2 SFP	8
Підтримувані	802.3, 802.3u, 802.3	ab, 802.3	
стандарти			
Jumbo пакети	Підтримуються		
VLAN, QoS	Підтримуються		
Підтримка	Так		
технології VLAN			

Таблиця ВЗ – Порівняння апаратних конфігурацій серверів

Сервер	Dell PowerEdge	HP ProLiant ML30	ARTLINE
	T40 v04	Gen10	Business T19
1	2	3	4
Тип виконання	Tower		
Процесор	Intel Xeon E-	Intel Xeon E-2124	Intel Core i7-
	2224G		9700F
Чіпсет	Intel C246	Intel C246	Intel H370
Пам'ять	UDIMM ECC DDR	4-2666 МГц (4 слоти	и, 64 ГБ макс.) –
оперативна	32ГБ		
Рівні RAID	0/1/5/10 - Intel Rapi	d Storage Technology	v(RSTe)
ЖМД	HDD: 2 x 1 ТБ; SSI	D: 2 x 250 ГБ	
ЛОМ	Gigabit Ethernet		

Зм.	Арк	№ докум.	Підпис	Дата

Таблиця В4 – Порівняльна характеристика маршрутизаторів

Виробник	Xiaomi	TP-LINK	Linksys
Марка	Mi 4A R4A	Archer C50	MR8300
Стандарти	802.11ac, 802.11r	1	
Підтримувані частоти	2,4Ггц, 5Ггц		
Протоколи безпеки	WPA-PSK, WPA	2-PSK	
Підтримувані	IPsec, L2TP, PPP	oE, PPTP	
протоколи			
Кількість портів LAN	2	1	4

						Арк
					2025.КВР.123.412.04.00.00 ПЗ	96
Зм.	Арк	№ докум.	Підпис	Дата		80

ДОДАТОК Г. ТЕХНІЧНІ ХАРАКТЕРИСТИКИ ХІАОМІ МІ 4А

Технічні характеристики маршрутизатора Хіаоті Мі 4А:

- Частота роботи Wi-Fi: 2.4 ГГц, 5 ГГц.

- Інтерфейси: 2 порти LAN 10/100 Мбіт/сек, 1 порт WAN 10/100 Мбіт/сек.

- Швидкість LAN портів: 100 Мбіт/с.

- Кількість антен: 4.

- Швидкість Wi-Fi: 1167 Мбіт/с.

- WAN-порт: Ethernet.

- Стандарт зв'язку: 802.11а, 802.11ас, 802.11b, 802.11g, 802.11n.
- Стандарт швидкості Wi-Fi: AC1200.
- Підтримка протоколів: IPsec, L2TP, PPPoE, PPTP.

- Конструкція антен: стаціонарні.

- Функції безпеки: батьківський контроль, захист від DoS-атак, міжмережевий екран SPI.

- Функції VPN: PPTP, L2TP, IPSec.

- Підтримка VPN-тунелів: Так.

- Функції бездротового режиму: увімкнення/вимкнення бездротового мовлення, міст WDS, WMM, статистика бездротового під'єднання.

- Швидкість передавання сигналів: 5 ГГц: до 867 Мбіт/сек, 2.4 ГГц: до 300 Мбіт/сек.

- Тип під'єднання WAN: динамічний ІР/статичний ІР/РРРоЕ/РРТР (Dual Access)/L2TP (Dual Access).

- DHCP: сервер, клієнт, список клієнтів DHCP, резервування адрес.

- Перенаправлення портів: віртуальний сервер, Port Triggering, DMZ.
- Динамічний DNS: DynDns, Comexe, NO-IP.

- Протоколи: підтримка IPv4 і IPv6.

Зм.	Арк	№ докум.	Підпис	Дата

ДОДАТОК Д. КОНФІГУРАЦІЙ СКРИПТ ІРҒW

#!/bin/sh

Налаштування мережевого інтерфейсу ifconfig em0 inet 192.168.1.1/24 up # Налаштування ipfw ipfw -q flush ipfw add divert natd ip from any to any via em0 ipfw add pass all from any to any # Налаштування NAT sysctl net.inet.ip.forwarding=1 sysctl net.inet.ip.fw.enable=1 sysctl net.inet.ip.fw.one_pass=1 sysctl net.inet.ip.fw.dyn_max=4096 sysctl net.inet.ip.fw.dyn_count=0 sysctl net.inet.ip.fw.dyn_ack_lifetime=120 sysctl net.inet.ip.fw.dyn_syn_lifetime=20 sysctl net.inet.ip.fw.dyn_fin_lifetime=1 natd -f /etc/natd.conf # Налаштування firewall (необов'язково) ipfw add deny tcp from any to any 22 # Запуск NAT /etc/rc.d/natd start echo "NAT gateway configured."

Зм.	Арк	№ докум.	Підпис	Дата	