Форма № Н-9.02

Міністерство освіти і науки України

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

(повне найменування вищого навчального закладу)

Відділення інформаційних технологій, менеджменту, туризму та підготовки іноземних громадян

(назва відділення)

Циклова комісія комп'ютерної інженерії

(повна назва циклової комісії)

ПОЯСНЮВАЛЬНА ЗАПИСКА

до кваліфікаційної роботи

фахового молодшого бакалавра

(освітньо-професійного ступеня)

на тему: **Розробка проєкту комп'ютерної мережі компанії "КЕТ"**

Виконав: студент IV курсу, групи КІ-418

Спеціальності 123 Комп'ютерна інженерія

(шифр і назва спеціальності)

Максим БАЛЮК

(ім'я та прізвище)

Керівник Василь ПИЖ

(ім'я та прізвище)

Рецензент _____

(ім'я та прізвище)

Тернопіль – 2025

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

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

ЗАТВЕРДЖУЮ
Голова циклової комісії
комп'ютерної інженерії
_____ Андрій ЮЗЬКІВ
"31" березня 2025 року

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

Балюку Максиму
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: **Розробка проєкту комп'ютерної мережі компанії "КЕТ"**

керівник роботи Пиж Василь Степанович
(прізвище, ім'я, по батькові)

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

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

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

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

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

6. Консультанти розділів роботи

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

КАЛЕНДАРНИЙ ПЛАН

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

7. Дата видачі завдання: 01 квітня 2025 року

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

Керівник роботи _____ Василь ПИЖ
(підпис) (ім'я та прізвище)

АНОТАЦІЯ

Кваліфікаційна робота на тему «Проєктування комп'ютерної мережі для підприємства "КЕТ"» має на меті створення надійної мережі для стабільної роботи інформаційної інфраструктури компанії.

У роботі розглянуто організаційну структуру, обрано топологію та технології, підібрано обладнання й програмне забезпечення, описано налаштування мережевих вузлв. Висвітлено економічне обґрунтування проєкту, а також заходи з охорони праці.

Робота буде корисною для студентів технічних спеціальностей, які вивчають комп'ютерні мережі. Проєкт містить пояснювальну записку на 87 аркушах А4 і креслення на аркушах А1.

The qualification thesis titled "Design of a Computer Network for the KET Company" aims to develop a reliable network to ensure stable operation of the company's information infrastructure.

The project analyzes the organizational structure, selects appropriate technologies and topology, chooses hardware and software, and describes network node configuration. It also includes a cost estimate and occupational safety measures. The work is useful for technical students studying computer network design and maintenance.

The project includes an 87-page A4 explanatory report and A1-format diagrams and schematics.

ЗМІСТ

ВСТУП

У сучасному світі електронно-обчислювальна техніка стала невід'ємною частиною нашого повсякденного життя — як у професійній діяльності, так і під час навчання чи дозвілля. Персональні комп'ютери нині займають у побуті таке ж важливе місце, як телевізори чи телефони. Вони виконують численні функції: є записниками, довідниками, бухгалтерами, перекладачами, віртуальними наставниками, кінотеатрами, засобами зв'язку тощо. За їх допомогою можна замовити квитки, надіслати листа, оформити документи чи здійснити інші повсякденні справи.

Глобальна мережа Інтернет відкрила користувачам доступ до необмежених інформаційних ресурсів. Наприклад, студент має змогу дистанційно користуватись бібліотеками університетів з усього світу або підтримувати зв'язок із близькими, які перебувають за кордоном. Для цього достатньо мати комп'ютер із доступом до Інтернету.

Швидкий розвиток комп'ютерних технологій вимагає впровадження новітніх інженерних рішень. Постійно удосконалюються засоби взаємодії з пристроями. Багато операцій нині виконується за допомогою комп'ютерної миші — від керування програмами до створення креслень, графіки та ілюстрацій.

Підключений до комп'ютера принтер дозволяє швидко й якісно друкувати документи, забезпечуючи зручність і тишу в роботі.

Водночас науковці активно працюють над створенням комп'ютерів, здатних розпізнавати людське мовлення. Сучасні електронні системи вже починають наслідувати принципи роботи людського мозку, що відкриває шлях до створення самонавчальних пристроїв. У найближчому майбутньому спілкування з комп'ютером рідною мовою стане реальністю, зробивши технології ще простішими й доступнішими для кожного.

1 ЗАГАЛЬНИЙ РОЗДІЛ

1.1 Технічне завдання

1.1.1 Найменування та область застосування

Тема кваліфікаційної роботи — розробка проєкту комп’ютерної мережі для підприємства “КЕТ”.

Основна мета проєкту полягає у створенні сучасної локальної мережі, яка повністю відповідатиме потребам компанії та забезпечуватиме її ефективне функціонування.

Запропонована мережа повинна виконувати низку важливих завдань, серед яких:

- інтеграція персональних комп’ютерів, розміщених у різних підрозділах організації, в єдиний інформаційний простір;
- забезпечення спільного високошвидкісного доступу до Інтернету для всіх користувачів;
- створення умов для використання як локальних сервісів, так і ресурсів глобальної мережі Інтернет;
- впровадження зручного та швидкого механізму обміну інформацією між співробітниками;
- централізоване зберігання, обробка та резервне копіювання даних з метою підвищення продуктивності роботи персоналу;
- оптимізація використання програмного та апаратного забезпечення, що дозволяє уникнути зайвого дублювання;
- підвищення рівня інформаційної безпеки шляхом централізованого адміністрування та ефективного контролю доступу до ресурсів мережі.

1.1.2 Призначення розробки

Метою створення комп’ютерної мережі є забезпечення ефективної взаємодії між усіма структурними підрозділами підприємства. Розроблена мережа повинна об’єднати персональні комп’ютери в єдине інформаційне середовище, що дозволить суттєво пришвидшити процес обміну даними.

Мережа має забезпечити спільне використання офісного обладнання, такого як принтери, сканери та інші периферійні пристрої, а також забезпечити колективний доступ до програмного забезпечення та централізованих баз даних. Одним із важливих завдань є організація централізованого зберігання критично важливої інформації з можливістю її резервного копіювання та належного захисту.

Також мережа повинна забезпечити користувачам швидкий і стабільний доступ до мережі Інтернет через спільний канал зв’язку, що сприятиме оптимізації витрат на апаратне та програмне забезпечення. Одним із ключових напрямів її використання є підтримка електронного документообігу, що підвищує загальну ефективність управління підприємством.

1.1.3 Вимоги до апаратного та програмного забезпечення

Апаратне забезпечення проєктованої комп’ютерної мережі має забезпечувати стабільний, швидкий і продуктивний доступ до корпоративних ресурсів підприємства. Розгортання мережі здійснюється з урахуванням планувань приміщень, у яких передбачено розміщення комп’ютерного обладнання.

Окрім цього, важливо передбачити надійні засоби захисту від несанкціонованого доступу, щоб запобігти підключенню сторонніх осіб до внутрішньої мережі.

Слід передбачити можливість подальшого розширення та модернізації мережі шляхом підключення додаткового обладнання або заміни існуючих компонентів. Для побудови мережі необхідно забезпечити наявність таких елементів:Наявність мережевих інтерфейсних карт (мережевих адаптерів) у кожному комп’ютері.

– Комутатор або маршрутизатор для забезпечення зв’язку між пристроями.
– Якісне мережеве кабелювання або обладнання для бездротового з’єднання (Wi-Fi).
– Стабільне джерело електроживлення з можливістю резервного жи- влення (UPS).
– Встановлена операційна система з підтримкою мережевих функцій (наприклад, Windows, Linux).
– Наявність антивірусного програмного забезпечення та брандмауера для захисту мережі.
– Серверне програмне забезпечення (у разі потреби: файловий сервер, сервер баз даних тощо).
– Засоби для резервного копіювання даних та їх відновлення.
– Програмне забезпечення для моніторингу та адміністрування мережі.
– Ліцензійне програмне забезпечення для безпечної та стабільної роботи користувачів.

1.1.4 Стадії та етапи розробки

При організації мережі всі етапи можна розподілити таким чином:

— Збір інформації

— Розробка та затвердження проектів

— Фізичне впровадження мережі

— Експлуатація та моніторинг мережі

— На етапі збору інформації потрібно вирішити кілька важливих питань:

— Ознайомитись з планом організації та визначити можливості її розвитку.

— Визначити, чи існує якась комп'ютерна мережа.

— Урахувати побажання керівництва щодо планованого використання мережі.

— Вибрати програмне забезпечення, яке буде використовуватись у мережі.

— Визначити тип топології, технології, провідників та іншого обладнання першого рівня.

— Розрахувати необхідну кількість повторювачів і концентраторів для робочих груп.

— Оцінити потребу в основних і проміжних комунікаційних вузлах.

— Вибрати відповідні комутатори.

— Визначити, які маршрутизатори будуть використовуватись.

— З'ясувати тип підключення до глобальної мережі.

1.1.5 Вимоги до документації

У результаті виконання проєктних робіт має бути сформовано наступний комплект документації:

– Проєкт структурованої кабельної системи (СКС) — включає зага- льну концепцію побудови мережевої інфраструктури, опис рішень та вибраного обладнання;

– План розміщення СКС — графічне відображення фактичного прокладання кабелів, розташування розеток, комутаційних панелей та іншого мережевого обладнання;
– Логічна топологія мережі — схема, що описує логічні зв’язки між мережевими пристроями, маршрути передачі даних та ієрархію взаємодії;
– Фізична топологія мережі — план, що ілюструє фізичне з'єднання всіх мережевих компонентів, включаючи кабелі, комутатори, маршрутизатори та сервери;
– Зведена таблиця MAC-адрес та IP-адрес — резюме, яке містить відповідність між фізичними (MAC) та логічними (IP) адресами всіх задіяних при- строїв у мережі.

1.1.6 Техніко-економічні показники

Проєктована мережа має відповідати таким основним вимогам:

– бути сучасною та водночас економічно вигідною;
– забезпечувати швидкість передачі даних на рівні 100 або 1000 Мбіт/с;
– передбачати можливість масштабування і подальшого розширення;
– гарантувати всім користувачам доступ до Інтернету;
– підтримувати стабільну роботу навіть при збільшенні кількості підключених пристроїв;
– мати зручну і надійну систему управління для ефективного адміністрування мережі.

1.1.7 Порядок контролю та прийому

Етап приймання мережі є надзвичайно важливим, оскільки саме він визначає якість її функціонування протягом усього терміну експлуатації. Після завершення всіх робіт, передбачених договором, замовнику надсилається пи-

сьмове повідомлення разом із повним комплектом погодженої документації. Отримавши ці матеріали, замовник зобов’язаний провести детальну перевірку мережі та її технічних характеристик, а потім здійснити прийняття мережі в експлуатацію за участю приймальної комісії.

Усі внесені доповнення, зміни або розширення робочих місць оформлюються відповідними актами та додаються до основного Технічного завдання. Робочі місця системи кабельного зв’язку (СКС) мають бути розташовані згідно з планом, що визначений у фізичній топології мережі.

1.2 Опис задачі та характеристика підприємства (організації, установи)

Метою даного проєкту є розробка та впровадження локальної комп’ютерної мережі, яка забезпечить ефективну взаємодію між персональними комп’ютерами підприємства. Передбачається створення стабільної інфраструктури для швидкого, безпечного та безперебійного обміну інформацією між робочими станціями. Крім того, мережа надасть користувачам постійний доступ до локальних ресурсів, спільних баз даних, а також до глобальної мережі Інтернет, що є необхідним для підтримки сучасного бізнес-процесу.

Проєкт реалізується в межах першого поверху адміністративної будівлі, де заплановано розміщення мережевого обладнання та кабельних трас. Висота стель у приміщенні становить 3,3 метра, що дозволяє зручно реалізувати приховане прокладання кабелю. Стіни мають комбіновану будову: частково з гіпсокартону, частково — поштукатурені, що дозволяє застосувати різні способи монтажу кабельної інфраструктури залежно від типу поверхні.

Для досягнення естетичності та безпеки прокладання кабелів буде виконано прихованим способом. У місці встановлення комутаційної шафи передбачено монтаж кабельного каналу з використанням пластикового короба від-

повідного перерізу для організованого підведення всіх мережевих ліній. Комутаційне обладнання буде розміщено в окремому технічному приміщенні, що забезпечить йому захист від стороннього доступу та несприятливих впливів зовнішнього середовища.

Проєкт розробляється для підприємства, яке активно працює на ринку рекламної продукції. Основна діяльність компанії полягає у наданні повного комплексу послуг — від розробки концепції до виробництва та розповсюдження рекламних матеріалів. Надійна комп'ютерна мережа дозволить працівникам ефективно виконувати свої функції, оперативно обробляти графічні та текстові файли, обмінюватися матеріалами з клієнтами й підрядниками, а також зберігати великі обсяги даних на мережевих сховищах.

2 РОЗРОБКА ТЕХНІЧНОГО ТА РОБОЧОГО ПРОЕКТУ

2.1 Розробка та обґрунтування логічної та фізичної схем мережі [10,11]

Під топологією комп’ютерної мережі, яку іноді називають компонуванням, конфігурацією або структурою, розуміють фізичне розміщення мережевих елементів — комп’ютерів та комунікаційного обладнання — а також спосіб їх з’єднання за допомогою засобів передачі даних, таких як кабелі або бездротові канали. Топологія є основоположним аспектом при проєктуванні мережевої інфраструктури, оскільки вона визначає схему зв’язків між складовими і суттєво впливає на функціональність, продуктивність та надійність системи загалом.

Особливо варто підкреслити, що термін «топологія» здебільшого застосовується у контексті локальних обчислювальних мереж (LAN). У таких мережах фізичні з’єднання та структура передачі даних зазвичай чітко визначені, прозорі і легко піддаються аналізу та візуалізації.

Це дає змогу точно визначити, яким чином здійснюється передача даних між окремими пристроями та які маршрути використовуються для їх взаємодії.

Навпаки, у глобальних мережах (WAN) структура з’єднань значно складніша і зазвичай недоступна для безпосереднього перегляду кінцевими користувачами.

В таких мережах маршрути передачі даних часто формуються динамічно, базуючись на алгоритмах маршрутизації та актуальних мережевих умовах.

Кожен новий сеанс зв’язку може проходити різними логічними і фізичними шляхами, що робить статичне уявлення топології менш практичним і менш інформативним для користувача.

Топологія мережі безпосередньо впливає на ряд ключових характеристик мережевої системи, зокрема:

– визначає тип і кількість необхідного мережевого обладнання, включаючи комутатори, концентратори, маршрутизатори та повторювачі;
– встановлює вимоги до середовища передачі даних, тобто до видів та обсягів використовуваних кабелів або бездротових каналів;
– впливає на вибір методів керування доступом до спільного середовища передачі даних, що особливо важливо для топологій із одним фізичним каналом;
– визначає загальний рівень надійності мережі, зокрема її здатність до відновлення у випадку пошкодження окремих ліній зв’язку чи вузлів;
– формує можливості для подальшого розширення мережі — наскільки просто і з мінімальними затратами можна додати нові вузли або змінити конфігурацію в майбутньому.

Отже, вибір топології є одним із ключових рішень при побудові мережевої архітектури, оскільки він визначає як поточну ефективність роботи мережі, так і її здатність адаптуватися до змін.

У сфері комп’ютерних мереж прийнято виділяти три основні типи топологій, які визначають спосіб з’єднання окремих вузлів.

Кожна з них має свої особливості, що впливають на принципи передачі даних, складність реалізації, надійність, вартість створення мережі та її масштабованість.

Основні види топологій включають:

– бути чутливою до збоїв — пошкодження одного сегмента шини здатне призвести до порушення роботи всієї мережі (див. рис. 2.1);
– Топологія «зірка» (star) — вирізняється наявністю центрального вузла, що виконує функції концентратора або комутатора. Усі інші пристрої мережі (тобто периферійні вузли) під’єднуються до цього центрального елемента окремими кабелями, кожен з яких утворює індивідуальне фізичне з’єднання. Така конфігурація значно підвищує надійність ме-

режі: у разі виходу з ладу одного з периферійних пристроїв або його з'єднання робота інших вузлів не порушується. Крім того, ця схема спрощує технічне обслуговування та виявлення несправностей, забезпечує високу швидкість передавання даних і дає змогу без ускладнень розширювати мережу шляхом додавання нових пристроїв. Основним недоліком є залежність усієї системи від центрального елемента: його несправність призводить до повної зупинки мережі (див. рис. 2.2);

– Кільцева топологія (ring) — передбачає таке компонування, за якого кожен вузол (комп'ютер) з'єднаний безпосередньо з двома іншими, утворюючи логічне кільце. Дані передаються по колу в одному напрямку (або в обох — у разі подвійного кільця), а кожен вузол приймає пакет, перевіряє, чи адресований він саме йому, і, якщо ні, пересилає його далі. Така схема забезпечує впорядковану передачу інформації без конфліктів та дозволяє ефективно використовувати пропускну здатність мережі. Однак система є вразливою до збоїв: вихід з ладу будь-якого вузла або відрізка кабелю може повністю порушити процес обміну даними (див. рис. 2.3).

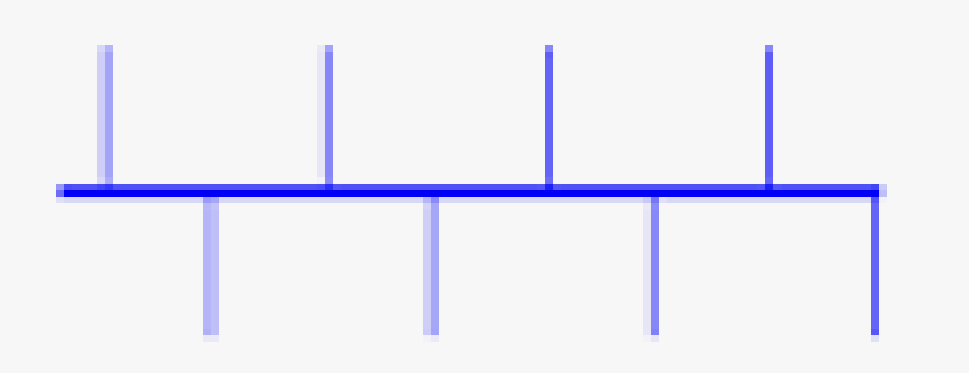


Рисунок 2.1 - Топологія типу "шина"

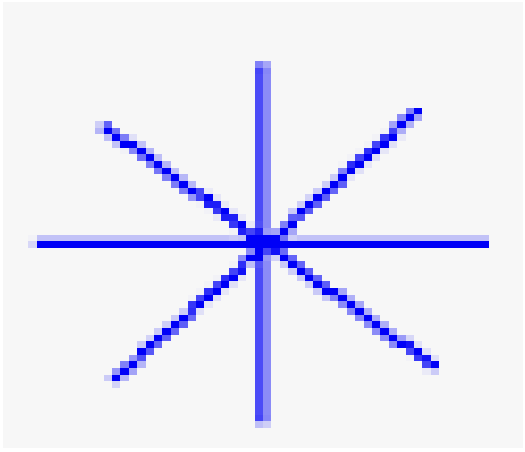


Рисунок 2.2 - Топологія типу “зірка”

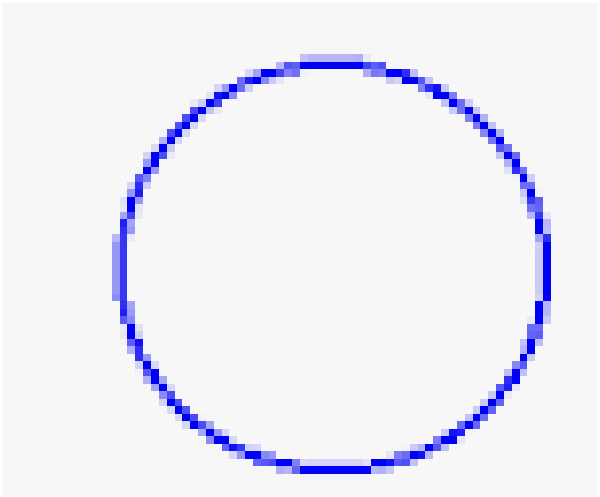


Рисунок 2.3 - Топологія типу “кільце”

На практиці нерідко використовують і комбінації базових топологій, але більшість мереж орієнтовані саме на ці три. Розглянемо тепер коротко особливості перерахованих мережних топологій.

Ethernet 100BASE-T (Fast Ethernet)

Fast Ethernet — це вдосконалена версія класичного Ethernet, яка забезпечує передавання даних зі швидкістю 100 Мбіт/с, що у десять разів перевищує швидкість початкового стандарту 10BASE-T (10 Мбіт/с). Ця технологія була

стандартизована в рамках IEEE під номером 802.3u у 1995 році та стала логічним розвитком технологій локальних мереж.

Позначення 100BASE-T розшифровується наступним чином:

– 100 — максимальна пропускна здатність у мегабітах за секунду;
– BASE — базовий метод передачі (тобто використання одного ка- налу для всієї смуги пропускання без модуляції несучої частоти);
– T — тип середовища передачі, тобто виті пари (Twisted Pair). Основні різновиди 100BASE-T:
– 100BASE-TX:
– Найпоширеніший варіант Fast Ethernet.
– Використовує дві пари провідників (1 пара для передавання, 1 — для прийому).
– Середовище передачі: екранована або неекранована витата пара категорії 5 (Cat 5 або вище).
– Максимальна довжина сегмента — 100 метрів.
– Метод кодування: MLT-3 з 4B/5B кодуванням.
– Топологія: Зіркоподібна (через комутатори або концентратори).
– Тип кабелю: Вита пара (UTP або STP).
– Зворотна сумісність: з 10BASE-T (через автонеготіацію інтерфейсу).

Переваги Fast Ethernet:

– Значно вища швидкість у порівнянні з 10BASE-T.
– Просте впровадження завдяки використанню існуючої інфраструктури (вита пара).
– Сумісність із попередніми поколіннями Ethernet. Недоліки:
– Обмежена дальність (до 100 метрів без підсилювачів або ретранс- ляторів).

– Не забезпечує достатньої швидкості для деяких сучасних застосу- нків (напр., передавання відео 4K, великі обсяги даних).

Для своєї мережі обираю кабель _ Cat 5e (UTP).(див. рис. 2.4.), технологію Ethernet, топологію — комбіновану (зіркова та комірчата)

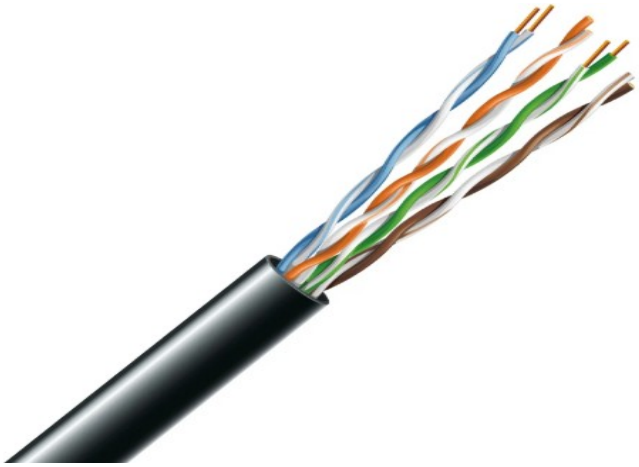


Рисунок 2.4 - Неекранована вита пара категорії 5е

Для побудови мережевої інфраструктури було використано шість некерованих комутаторів, кожен з яких обладнано вісьмома портами. Вони забезпечують підключення кінцевих пристроїв у межах локальних сегментів мережі. Усі ці комутатори з’єднані окремими фізичними лініями з центральним керованим комутатором.

Використання керованого комутатора в якості головного мережевого вузла дає змогу організувати логічне розділення мережі на окремі незалежні сегменти — робочі групи.

Для реалізації цієї мети було створено декілька віртуальних локальних мереж (VLAN), кожна з яких об’єднує пристрої за функціональною ознакою.

Подібна структура забезпечує ізоляцію трафіку між різними VLAN, що підвищує рівень безпеки та ефективності передавання даних.

Для кожної віртуальної мережі передбачено налаштування маршрутизації на вихід .

Крім того, до центрального комутатора підключено точку доступу Wi-Fi, яка також віднесена до окремого VLAN.

Це забезпечує логічне відокремлення бездротового сегмента від дротових підмереж і дозволяє централізовано контролювати доступ до ресурсів мережі.

Усі вищенаведені налаштування та структура мережі докладно від- ображені у таблицях 2.1 та 2.2, де представлені відповідні IP-адреси, VLAN- ідентифікатори та типи підключених пристроїв.

Таблиця 2.1 – Логічна адресація в мережі

Позначення вузлів	Робоча група /Кількість вузлів		і Назва кабінету	Номер VLAN	Адреса підмережі/Маска
1	2		3	4	5
WS_01 – WS_10, PR_A, S_A, S_B	office	13	Відділ дизайну	20	192.168.10.0/24
WS_11	office	1	IT-відділ	20	192.168.20.0/24
WS_12 – WS_15, S_C	buch	5	Адміністрація	5	192.168.5.0/24
Ap_1, Ap_2	wifi		Гостьовий Wi-Fi	8	192.168.5.0/24

Таблиця 2.2 - Таблиця конфігурування VLAN на портах SW_3

№ п/п	Познач вузла	Номер порту	Тип порту	Назва ме- реж. пр-ю	Номер порту	Тип порту	Номер VLAN
1	2	3	4	5	6	7	8
1	SW_3	1	Access	SW_1	16	Access	10
2		2	Access	SW_2	16	Access	10
3		3	Access	A_1	-	Access	10
4		4	Access	SW_4	16	Access	10
5		5	Access	SW_5	16	Access	2
6		6	Access	резерв	-	Access	10
7		7	Access	AP_1	wan	Access	3
8		8	Access	AP_2	wan	Access	3
9		9	Access	S_1	eth1	Access	10
10		10	Trunk	S_2	eth1	Trunk	
11		11	Access	WS_13	eth1	Access	10

2.2 Обґрунтування вибору комунікаційного обладнання

У структурі локальної мережі передбачено застосування комутаторів робочих груп із вісьмома портами. Для реалізації проєкту заплановано придбати чотири одиниці відповідного мережевого обладнання.

З метою вибору оптимального варіанту було проведено порівняльний аналіз трьох моделей комутаторів, який охоплює їх основні технічні характери-

стикита експлуатаційні особливості. Детальні параметри пристроїв подано в таблиці 2.3.

На підставі аналізу даних таблиці 2.3, з урахуванням співвідношення вартості та функціональних можливостей комутаторів, для впровадження в мережу було обрано модель TP-Link TL-SF1008P. Зовнішній вигляд цього мережевого пристрою представлено на рисунку 2.5.

Таблиця 2.3 – Порівняльна характеристика 8-портових комутаторів

Характеристика	D-Link DES-1009MPA1A	Planet GSD-804P-EU	Hikvision DS-3E031 0HP-E
1	2	3	4
Тип керування	Некерований	Некерований	Некерований
кількість портів	8	8	10
Порти доступу (тип/швидкість)	Немає (всі порти однакові	8 x 10/100/1000 Мбіт/с (GE)	8 x 10/100 Мбіт/с (FE)
Uplink порти (тип/швидкість)	1 x 10/100/1000 Мбіт/с (GE)	Немає (всі 8 портів GE)	2 x 10/100/1000 Мбіт/с (GE)
SFP/SFP+ слоти	Немає	Немає	Немає
Підтримка PoE	Так	Так	Так
Стандарти PoE	IEEE 802.3af	IEEE 802.3af/at	IEEE 802.3af/at/bt
Дальність PoE (спец. режим)	До 250 м (в режимі Extend, 10 Mbps)	До 250 м (в режимі Extend, 10Mbps)	До 300 м (в режимі Extend, 10Mbps)

Продовження таблиці 2.3

1	2	3	4
Кома здат- ність	1.6 Гбіт/с	16 Гбіт/с	5.6 Гбіт/с
Швидкість пере-силання пакетів	1.19 Mpps	11.9 Mpps	4.166 Mpps
Розмір таблиці MAC-адрес	2K записів	До 8K записів	16K записів
Форм-фактор	Настільний	Настільний	Настійний
Габарити	171 x 98 x 27 мм	217 x 135 x 43 мм	217.6 x 103.35 x 27.8 мм
Вага	0.4 кг	0.89 кг	0.55 кг
ціна (грн)	2200 грн	3500 грн	6000 грн

Рисунок 2.5 – Зовнішній вигляд комутатора TP-Link TL-SF1008P

У структурі мережі передбачено застосування бездротових точок доступу з метою забезпечення мобільності користувачів та розширення зони дії Wi-Fi-сигналу.

Сучасний ринок телекомунікаційного обладнання пропонує великий вибір точок доступу від різних виробників, які відрізняються функціональністю, технічними характеристиками та ціновим діапазоном.

Враховуючи вимоги до побудови мережевої інфраструктури, було обрано три моделі бездротових точок доступу, які найбільш відповідають поставленим критеріям. Порівняльні характеристики цих пристроїв наведено в таблиці 2.4.Основні відмінності:

Netgear WAC104 — це двохдіапазонна бездротова точка доступу, що підтримує стандарти Wi-Fi 802.11ac/n на частотах 2.4 ГГц і 5 ГГц. Пристрій забезпечує швидкість до 1167 Мбіт/с (300 Мбіт/с на 2.4 ГГц та 867 Мбіт/с на 5 ГГц), підтримує до 4 окремих SSID.

Ubiquiti UniFi U6 Lite - це сучасна точка доступу з підтримкою Wi-Fi 6 (на 5 ГГц) та портом Gigabit Ethernet. Вона частина екосистеми UniFi для централізованого керування, добре підходить для домашнього використання або малого бізнесу.

Таблиця 2.4 – Порівняльна характеристика точок доступу

Характеристика	TP-LINK TL-WA801ND	Ubiquiti UniFi U6 Lite	Netgear WAC104
1	2	3	4
Стандарти Wi-Fi	802.11b/g/n (Wi-Fi 4)	802.11a/b/g/n/ac/ax (Wi-Fi 6)	802.11ac, 802.11n, 802.11g, 802.11b
Діапазони частот	2.4 ГГц (Single-Band)	2.4 ГГц, 5 ГГц (Dual-Band)	Двохдіапазонний: 2.4 ГГц та 5 ГГц

Продовження таблиці 2.4

1	2	3	4
Сукупна швид-кість Wi-Fi	До 300 Мбіт/с	До ~1500 Мбіт/с (Wi-Fi 6 на 5 ГГц)	До 1167 Мбіт/с
Швидкість по діапазонах	2.4 ГГц: до 300 Мбіт/с	2.4 ГГц: до 300 Мбіт/с, 5 ГГц: до 1201 Мбіт/с	2.4 ГГц — до 300 Мбіт/с 5 ГГц — до 867 Мбіт/сс
MIMO конфігурація	2x2	2x2 (на обох діапазонах)	2x2 MIMO
Ethernet порти (кількість/швид кість	1 x 10/100 Міт/с (FE	1 x10/100/1000 Мбіт/с(GE)	(10/100/1000Мбіт/с)
Підтримка PoE	Так (Passive PoE)	Так (802.3af, Passive PoE)	ні
Тип антени	Зовнішні, знімні	Вбудована	2 зовнішні нерозбірні антени
Посилення антени	2 x 4 dBi (орієнт.)	2.4 ГГц: 2.8 dB 5 ГГц: 3 dBi	5 дБі
ціна	1400 грн	5500 грн	1500–2000 грн

На основі аналізу даних, наведених у таблиці 2.4, з урахуванням основних технічних характеристик, рівня продуктивності, енергоефективності та від-

повідності имогам проєктованої мережі, для впровадження було обрано модель бездротової точки доступу Netgear WAC104.

Цей пристрій забезпечує стабільну передачу даних, підтримує сучасні стандарти бездротового зв’язку та характеризується оптимальним співвідношенням ціни й функціональності.

Зовнішній вигляд обраної точки доступу представлено на рисунку 2.6.

Рисунок 2.6 – Вигляд точки доступу Netgear WAC104

У складі проєктованої комп’ютерної мережі заплановано використання трьох персональних комп’ютерів моделі ASUS ExpertCenter D5 (D500MA) , які виконуватимуть функції робочих станцій для користувачів.

ASUS ExpertCenter D5 (D500MA) — це сучасний системний блок, який поєднує в собі високу продуктивність, надійність та ефективність, що робить його оптимальним рішенням для бізнесу та професійного використання.

Ці системні блоки забезпечують стабільну роботу під час виконання багатозадачних процесів, роботи з ресурсоємними програмами, а також обробки великого обсягу даних. З

авдяки продуктивному процесору (доступні варіанти з Intel Core i5/i7 або AMD Ryzen).

Основні технічні параметри та конфігурація цих комп’ютерів узагальнені у таблиці 2.5 а зовнішній вигляд приведено на рисунку 2.7

Таблиця 2.5 – Хатактеристики сервера ASUS ExpertCenter D5 (D500MA)

Характеристика	Значення для ARTLINE Business T61
1	2
Бренд	ASUS
Модель	ExpertCenter D5 (D500MA)
Тип корпусу (форм-фактор)	Малий (SFF)
Процесор	Intel Core i5-12400
Кількість ядер процесора	6 ядер (12 потоків)
Максимальна частота процесора	До 4.4 ГГц
Кількість ЦП у комплекті	1
Максимальна кількість слотів ЦП	1
Тип пам'яті	DDR4
Накопичувачі	256 ГБ / 512 ГБ SSD (M.2 NVMe)

Продовження таблиці 2.5

1	2
Підтримка RAID	Так (RAID 0, 1, 10)
Матринська плата	ASUS Proprietary (Intel B660/H670)
Відеокарта	Intel UHD Graphics 730 (інтегрована)
Мережеві інтерфейс	Gigabit Ethernet (1× RJ-45) Bluetooth 5.
ціна	27000

Один комп’ютер працює як файловий сервер і знаходиться в серверній кімнаті.

Другий використовується як інтернет-шлюз, забезпечуючи захищений вихід у мережу та централізоване управління.

Третій комп’ютер функціонує як сервер бухгалтерського програмногозабезпечення й встановлений безпосередньо в бухгалтерському відділі для забезпечння локального доступу до облікових систем.

Рисунок 2.7 – Зовнішній вигляд ARTLINE Business T61 (T61v04)

У мережі передбачено використання керованого комутатора У таблиці 2.6 приведені порівняльні характеристики комутаторів.

Таблиця 2.6 – Порівняльна характеристика керованих комутаторів

Характеристика	Linksys LGS310 MPC	Cisco CBS250-16T-2G	Netgear GS308
1	2	3	4
Тип керування	Керований (Managed / Smart Plus)	Smart Managed (Налаштовуваний)	(без налаштувань, plug-and-play)
Кількість портів	10	18	8
орти LAN (RJ45)	8 x 10/100/1000 Мбіт/с (GE)	16 10/100/1000 Мбіт/с (GE	8 × 1Gbps (10/10/1000 Мбіт/с)
SP/SFP+ слоти	2 x 1G SFP	2 x 1G SFP	4 x G SFP
Підтима PoE	Так (PoE+)	Ні	Немає
Рівень кеування	L2 L3 Static Routin	L2 / L3 Static Routin	L
Швидкість пересилання пакетів	14.88 Mpps	26.78 Mpps	11.8 Mpps
Розмір таблиці MAC-адрес	8K записів	16K записів	16K записів
ціна	6500 грн	13000 грн	2 516 грн

Виходячи з таблиці 2.6, враховуючи співвідношення ціни до технічних характеристик пристрою для мережі вибрано комутатор Linksys LGS310MPC , зовнішній вигляд якого зображено на рисунку 2.8.

Рисунок 2.8 – Зовнішній вигляд Linksys LGS310MPC

Основні відмінності:

Linksys LGS310MPC: Компактний керований комутатор з 8 портами GE PoE+ та 2 портами 1G SFP. Підтримує статичну маршрутизацію. Пасивне охолодження.

Cisco CBS250-16T-2G: Smart Managed комутатор з 16 портами GE та 2 портами 1G SFP. Не має підтримки PoE. Вища комутаційна здатність порівняно з Linksys та MikroTik.

Netgear GS308 - простий неуправляний комутатор з 8 портами Gigabit Ethernet (10/100/1000 Мбіт/с). Він не має портів SFP, не підтримує PoE і не має функцій керування. Комутаційна здатність становить 16 Гбіт/с, що є стандарт-

ним показником для 8 портів 1G. Пристрій працює за принципом plug-and-play, не потребує налаштувань і має пасивне охолодження.

2.3 Особливості монтажу мережі

Під час прокладання кабелю необхідно чітко дотримуватися технічних вимог, які гарантують надійність і стабільність роботи мережі. Максимальна довжина кабелю не повинна перевищувати 100 метрів для горизонтальної розводки, а в робочих зонах – 10 метрів при використанні патч-кордів у комутаційних шафах. Перевищення цих норм може спричинити втрату сигналу та погіршення якості зв'язку.

При монтажі слід уникати сильного натягу – максимально допустиме зусилля становить 50 ньютонів. Надмірне натягнення може пошкодити провідники та погіршити електромережні характеристики. Якщо кабель було пошкоджено, недостатньо просто послабити натяг – необхідно повністю замінити пошкоджену ділянку.

Важливо дотримуватися правил вигину кабелю: під час монтажу радіус вигину має бути не менше восьми діаметрів кабелю, а під час експлуатації – не менше чотирьох. Порушення цих вимог може призвести до пошкодження ізоляції та внутрішніх провідників, що негативно вплине на передачу даних. Особливо часто такі проблеми виникають біля інформаційних розеток, де зайві ділянки кабелю нерідко згортають у петлі або джгути, що суперечить технічним нормам.

Надлишки кабелю слід акуратно розміщувати у спеціальних коробах або нішах, дотримуючись вимог до вигинів. У комутаційних шафах кабель має бути рівномірно розкладений у лотках або на стійках, без різких згинів.

Монтажні роботи рекомендується проводити за температури не нижче 0 °C. Якщо ж роботи необхідно виконувати в більш суворих умовах, слід вжити додаткових заходів для захисту кабелю.

Якщо роботи проводяться при температурі нижче 0 °С, кабель попередньо потрібно прогріти в приміщенні з температурою не нижче 10 °С. На місце монтажу слід брати лише необхідну кількість кабелю, розраховану на кілька годин роботи.

Після завершення прокладання залишки кабелю необхідно повернути в тепле приміщення, щоб запобігти пошкодженню ізоляції через переохолодження.

Для зберігання кабель намотують на котушки діаметром не менше 25–30 см, оскільки занадто туге намотування може пошкодити зовнішню оболонку. Також важливо уникнути механічних навантажень – наприклад, неправильного підвішування або складання кабелю в мотки. Опорні точки повинні розташовуватися на відстані 120–150 см одна від одної. Категорично заборонено скручувати кабель під час монтажу, оскільки це може призвести до пошкодження оболонки або порушення структури витої пари.

Щоб уникнути впливу електромагнітних перешкод (наприклад, від люмінесцентних ламп або неекранованих силових кабелів), мінімальна відстань між ними та кабелем "вита пара" повинна становити не менше 150 мм.

Монтаж має проводитися згідно з інструкцією виробника, особливо для кабелів категорії 6, де критично важливо дотримуватися технологічних норм (правильне зняття ізоляції, контроль довжини розкручування пар, використання спеціалізованого інструменту). Інформаційні розетки повинні бути підключені за однією схемою (T568A або T568B) – різні стандарти на кінцях кабелю призводять до погіршення сигналу.

2.4 Тестування мережі [14]

Тестування комп’ютерних мереж може включати різноманітні методи, серед яких особливе значення має тестування на проникнення. Цей підхід

передбачає імітацію дій потенційних зловмисників для оцінки рівня захищеності інформаційної системи чи мережевої інфраструктури. Перевірка виконується як зовнішніми тестувальниками, які не мають санкціонованого доступу, так і внутрішніми користувачами з певним рівнем повноважень.

Процес тестування полягає у активному скануванні та аналізі системи з метою виявлення можливих слабких місць. Такі вразливості можуть виникати через некоректні налаштування, програмні чи апаратні помилки, а також недостатність організаційних чи технічних заходів безпеки. Аналіз проводиться з урахуванням типових методів, які можуть застосовувати зловмисники, включаючи можливість експлуатації виявлених недоліків.

Після завершення тестування результати документуються та передаються власнику системи.

Якісний звіт містить не просто перелік знайдених вразливостей, а й оцінку потенційного впливу можливих атак на функціонування організації. Додатково надаються технічні рекомендації щодо усунення ризиків та вдосконалення заходів безпеки.

Тестування комп’ютерних мереж може включати різноманітні методи, серед яких особливе значення має тестування на проникнення. Цей підхід передбачає імітацію дій потенційних зловмисників для оцінки рівня захищеності інформаційної системи чи мережевої інфраструктури.

Перевірка виконується як зовнішніми тестувальниками, які не мають санкціонованого доступу, так і внутрішніми користувачами з певним рівнем повноважень.

Процес тестування полягає у активному скануванні та аналізі системи з метою виявлення можливих слабких місць. Такі вразливості можуть виникати через некоректні налаштування, програмні чи апаратні помилки, а також недостатність організаційних чи технічних заходів безпеки. Аналіз проводиться з

урахуванням типових методів, які можуть застосовувати зловмисники, включаючи можливість експлуатації виявлених недоліків.

2.5 Захист комп'ютерної мережі

Захист комп'ютерних мереж передбачає комплексний підхід, спрямований на запобігання несанкціонованим втручанням, протидію кіберзагрозам та забезпечення стабільної роботи інформаційних систем. Він поєднує технічні рішення з організаційними процедурами для підтримки цілісності, доступності та конфіденційності даних, що передаються та зберігаються в мережі. Головне завдання полягає у нейтралізації потенційних ризиків - від зовнішніх атак до внутрішніх загроз, які можуть виникнути через помилки співробітників, порушення правил безпеки чи навмисні шкідливі дії.

Важливим елементом сучасної мережевої безпеки є системи аналізу трафіку в режимі реального часу, які дозволяють виявляти аномальну активність на ранніх етапах. Такі системи базуються на складних алгоритмах машинного навчання, що постійно вдосконалюють свої правила виявлення на основі аналізу поведінки мережевих пристроїв і користувачів. Паралельно з цим активно розвиваються механізми проактивного захисту, здатні прогнозувати потенційні загрози ще до їх матеріалізації.

Особливу увагу приділяють організації безпечного доступу до мережевих ресурсів, де традиційні парольні системи поступово замінюються більш надійними методами аутентифікації. Багатофакторні системи перевірки, що поєднують біометричні дані, апаратні ключі та одноразові коди, стають стандартом для захисту критично важливих інформаційних активів. При цьому постійно вдосконалюються механізми управління доступом, що дозволяють реалізувати принцип мінімально необхідних привілеїв для кожного користувача.

Не менш важливим аспектом є захист периметру мережі, де сучасні рішення поєднують традиційні технології з новітніми підходами. Віртуалізація мережевих елементів дозволяє створювати динамічні системи захисту, здатні адаптуватися до змін конфігурації мережі в реальному часі. Особливу роль відіграють системи захисту від розподілених атак типу "відмова в обслуговуванні", які стали одними з найпоширеніших загроз для сучасних інформаційних інфраструктур.

Окремо варто відзначити постійне вдосконалення механізмів резервування та відновлення даних, що дозволяє мінімізувати наслідки потенційних інцидентів. Сучасні системи бекапу реалізують складні стратегії збереження інформації, поєднуючи локальні, хмарні та гібридні рішення.При цьому особлива увага приділяється захисту самих резервних копій від несанкціонованого доступу або пошкодження.

3 СПЕЦІАЛЬНИЙ РОЗДІЛ

3.1 Налаштування комутатора Linksys LGS310MPC

Для налаштування комутатора Linksys LGS310MPC спочатку підключіться до його веб-інтерфейсу. Відкрийте будь-який браузер і введіть у адресному рядку стандартну . Після цього з'явиться сторінка авторизації, де необхідно ввести облікові дані для доступу до панелі керування. За замовчуванням логін і пароль зазвичай встановлені як "admin". Після успішного входу відкриється інтерфейс налаштувань, де можна конфігурувати параметри роботи комутатора. (див. рис. 3.1).

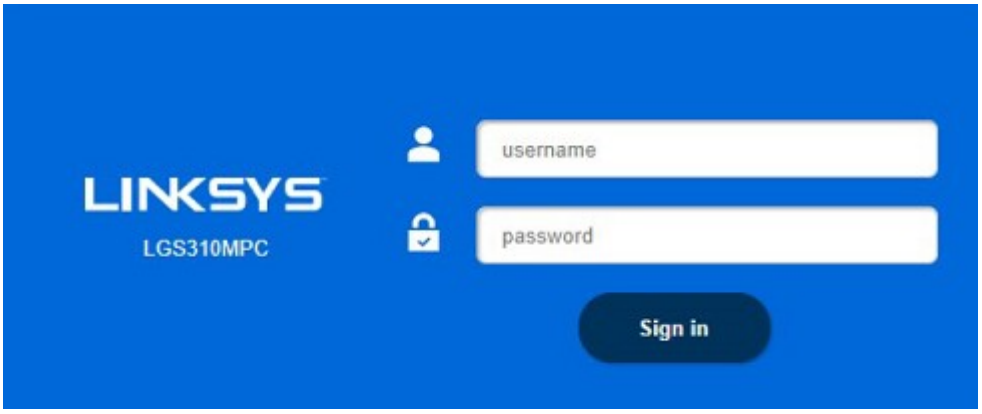


Рисунок 3.1 – Вікно авторизації

Основні налаштування починаються з конфігурації IP. У розділі System Settings - IP Configuration можна змінити адресу на статичну, вказавши нову IP-адресу, маску підмережі та шлюз. Для роботи з VLAN перейдіть у відповідний розділ VLAN Settings, де можна створювати нові віртуальні мережі та призначати порти. (див. рис. 3.2).

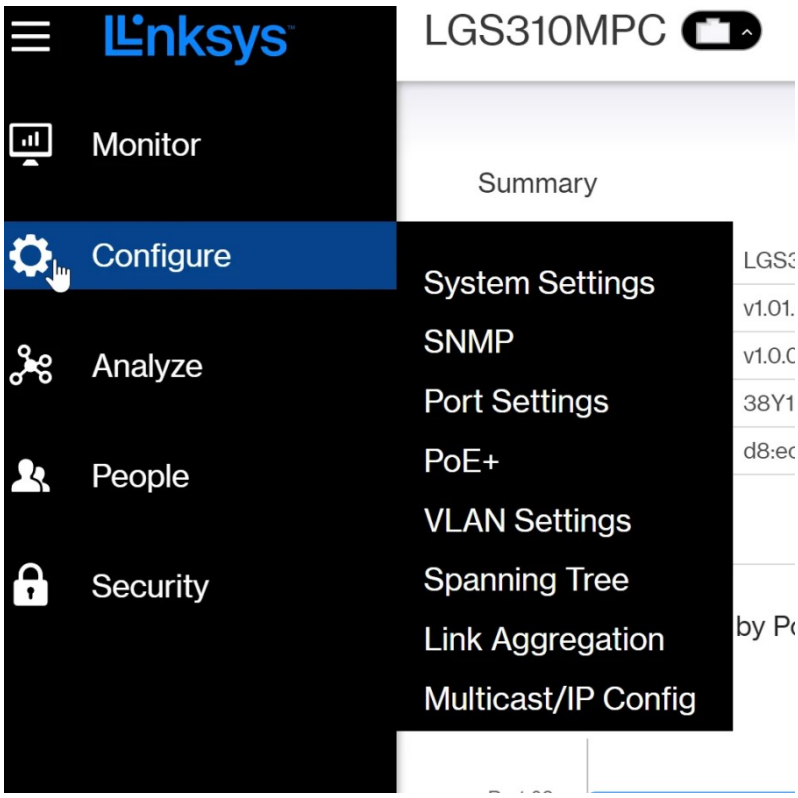


Рисунок 3.2 – Головне вікно інтерфейсу

Веб-інтерфейс налаштування VLAN у комутаторі Linksys LGS310MP має чітку структуру. У верхній частині розташовані три основні вкладки: System

Status для перегляду загального стану системи, Quick Start для швидкого налаштування та Configuration для детальної конфігурації.

У лівій частині екрана знаходиться меню з основними розділами. Розділ System Management включає підпункти System Information, Time, SNMP та Logs. Також доступні розділи Quality of Service, Port Management та VLAN Management.

Основний вміст сторінки присвячений налаштуванню VLAN. У верхній частині відображаються поточні параметри: Current Default VLAN зі значенням 1 та Default VLAN after Reboot, де також вказано значення 1 з можливістю змінити його в діапазоні від 1 до 4094. Для збереження змін є кнопки Apply та Cancel. (див.рис 3.3)

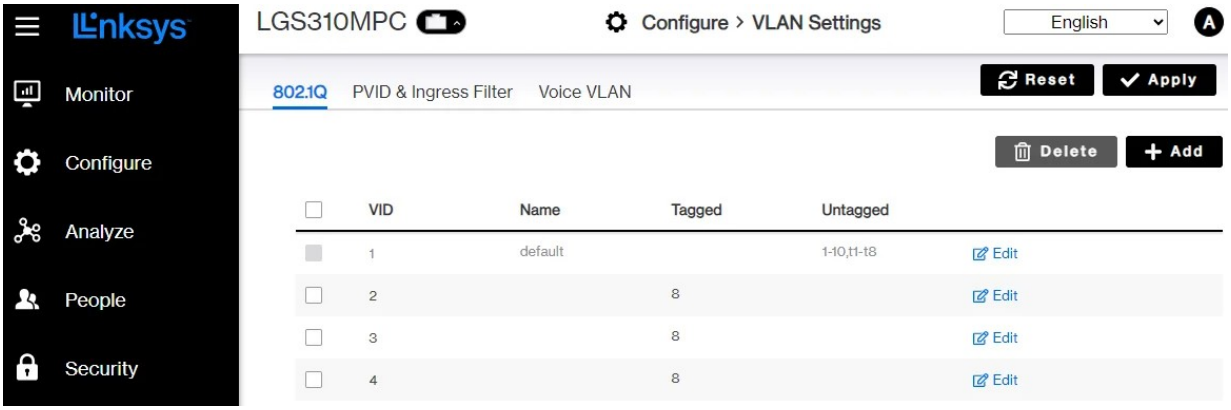


Рисунок 3.3 – Вікно налаштування VLAN у комутаторі Linksys LGS310MP

Розділу налаштування Voice VLAN (голосового VLAN) у веб-інтерфейсі керування (див. рис. 3.4)

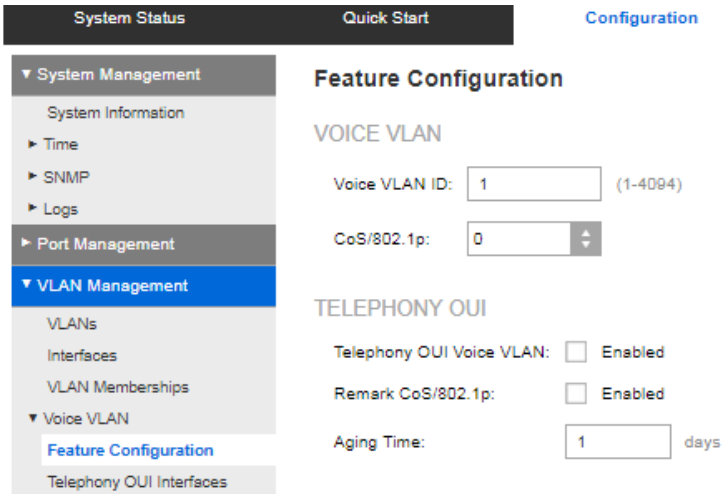


Рисунок 3.4 – Розділу налаштування Voice VLAN

Наступним кроком є визначення, які порти будуть включені до кожної VLAN. Для цього потрібно перейти до вікна “Port to VLAN”.

У цьому розділі виконується призначення портів до певних VLAN, а також визначення режиму кожного порту: Tagged або Untagged.

Tagged-порти використовуються, коли через них проходить трафік декількох VLAN, а Untagged — коли порт належить лише одній VLAN. Ці налаштування повинні відповідати попередньо розробленій схемі мережі, наприклад, згідно таблиці 2.4 (див. рис. 3.5).

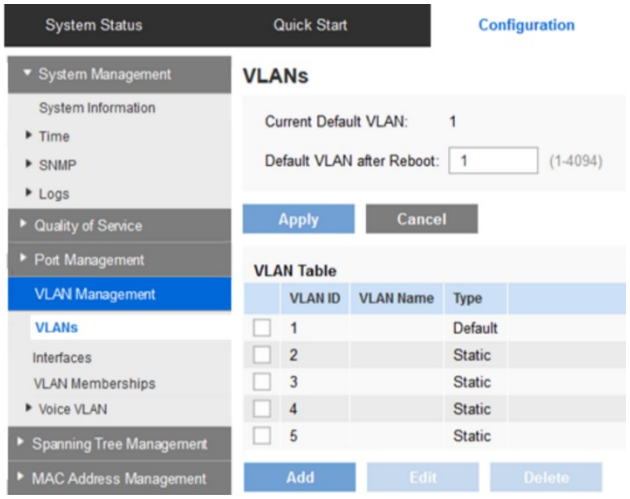


Рисунок 3.5 – Вікно привязки портів

Веб-інтерфейс налаштування VLAN у комутаторі Linksys LGS310MP завершується розділами для контролю та оптимізації віртуальних мереж. У нижній частині екрана завжди присутні кнопки Apply (застосувати) та Cancel (скасувати), які дозволяють зберегти зміни або повернутися до попередніх налаштувань.

Останніми елементами інтерфейсу є налаштування часу оновлення MAC-адрес (Aging Time), яке визначає, як довго комутатор зберігає інформацію про пристрої у таблиці MAC-адрес. Також доступні функції фільтрації трафіку за MAC-адресами виробників VoIP-обладнання (Telephony OUI), що особливо важливо для роботи голосових VLAN.

Для завершення налаштувань рекомендується перевірити всі внесені зміни у таблиці VLAN Table, де відображаються створені VLAN з їх ідентифікаторами, іменами та типами. Після збереження конфігурації комутатор готовий до роботи з налаштованими віртуальними мережами..

3.2 Налаштування точки доступу [12]

Першим кроком у процесі налаштування є фізичне з'єднання всіх необхідних компонентів. Комутатор Linksys LGS310MP має порти, що підтримують живлення через Ethernet (PoE), тому точку доступу можна підключити лише одним кабелем Ethernet — це забезпечить як передачу даних, так і живлення. Для цього кабель підключається до одного з PoE-портів, які на цьому комутаторі зазвичай знаходяться з першого по восьмий порт. (див.рис.3.7)

Комп’ютер, який використовуватиметься для налаштування, підключається до будь-якого іншого порту комутатора, бажано з 9 або 10, які не мають PoE, щоб уникнути можливих конфліктів або пошкоджень. Після цього вмикається живлення комутатора, якщо він ще не був увімкнений. алі потрібно отримати доступ до інтерфейсу керування комутатором через веб-браузер. За замовчуванням комутатор має IP-адресу 192.168.1.1. Це означає, що комп’ютер, з якого виконується налаштування, також повинен мати IP-адресу з тієї ж підмережі. Наприклад, можна вручну призначити комп’ютеру IP-адресу 192.168.1.2 із маскою підмережі 255.255.255.0. Після цього відкривається будь-який сучасний браузер, де в адресному рядку вводиться IP-адреса комутатора. З’явиться сторінка входу до системи, де потрібно ввести ім’я користувача та пароль.

Якщо пристрій новий або налаштовується вперше, то типово логін — admin, пароль — admin. Якщо дані не підходять, можливо, комутатор вже був налаштований, і доведеться скинути його до заводських параметрів.

Після входу до системи адміністрування можна приступати до налаштування логіки обробки трафіку. У багатьох випадках може виникнути потреба у створенні віртуальних локальних мереж (VLAN), щоб розділити трафік точки доступу і решти пристроїв, підвищити безпеку, або налаштувати QoS — пріоритети трафіку. Створення VLAN починається з додавання нового ідентифікатора VLAN, наприклад VLAN ID 10 для Wi-Fi пристроїв. Після цього в налаштуваннях портів комутатора вибирається, який порт буде членом цієї VLAN. Порт, до якого підключена точка доступу, зазвичай додається в режимі "Access", якщо на ньому буде лише одна VLAN. Якщо ж точка доступу підтримує передачу кількох VLAN одночасно (наприклад, для гостьової мережі та внутрішньої), порт налаштовується в режимі "Trunk" (Tagged), і до нього додаються відповідні VLAN ID.

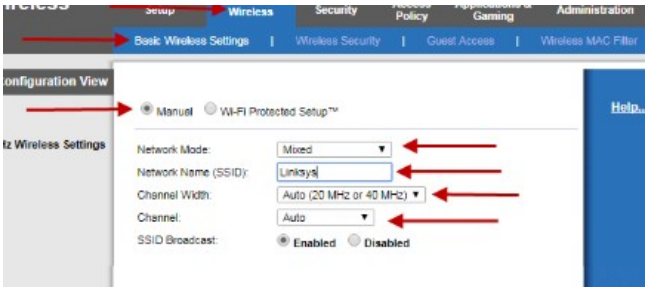


Рисунок 3.7 – налаштування бездротової мережі (Wi-Fi)

Наступним кроком перевіряється, чи точка доступу отримала живлення та IP-адресу. Якщо у мережі є DHCP-сервер (наприклад, на маршрутизаторі), то точка доступу автоматично отримає адресу і буде доступна через браузер. Якщо ж IP-адреса не призначається автоматично, необхідно дізнатися адресу за замовчуванням із документації до точки доступу та вручну підключитися до неї для первинного налаштування. Там задається статична IP-адреса, шлюз, DNS-сервер, і при потребі — ідентифікатор VLAN, у якому вона має працювати.

Після завершення основних налаштувань важливо зберегти всі зміни, зроблені як у комутаторі, так і в точці доступу. У веб-інтерфейсі комутатора зазвичай є окрема кнопка або пункт меню для збереження конфігурації в енергонезалежну пам’ять. Якщо цього не зробити, після перезавантаження комутатора всі налаштування буде втрачено. Після збереження бажано перезапустити як точку доступу, так і сам комутатор, щоб переконатися, що всі пристрої коректно завантажилися, отримали IP-адреси та функціонують відповідно до заданих параметрів.

Таким чином завершується процес налаштування точки доступу через керований комутатор Linksys LGS310MP. Це дозволяє гнучко керувати трафіком, забезпечувати живлення по одному кабелю Ethernet, і масштабувати мережу з урахуванням вимог до безпеки, пріоритетності та ізоляції трафіку.

3.3 Налаштування програмного маршрутизатора PfSense [13,14]

PfSense — це потужний брандмауер і професійна операційна система, розроблена на основі надійної FreeBSD. Вона поєднує в собі високу продуктивність, стабільність і розширені можливості безпеки, що робить її ідеальним вибором як для домашніх користувачів, так і для корпоративних мереж.

Головною перевагою PfSense є її універсальність. Система дозволяє ефективно розділяти мережу на логічні сегменти, налаштовувати складні правила фаєрволу, організовувати VPN-з'єднання та керувати мережевим трафіком. Вона підтримує такі функції, як маршрутизація, балансування навантаження, система виявлення та запобігання вторгненням (IDS/IPS), а також багато інших професійних мережевих сервісів.

Окремо варто відзначити зручний веб-інтерфейс керування, який відрізняється інтуїтивною структурою та детальними поясненнями всіх нала-

штувань. Це значно спрощує процес конфігурації навіть для користувачів, які не мають глибоких знань у адмініструванні мереж.

Ще одна важлива перевага PfSense — її відкритий вихідний код і безкоштовна ліцензія. Завдяки основі на FreeBSD, система забезпечує високий рівень стабільності та безпеки, що підтверджено її широким використанням у різних сферах — від малих офісів до великих корпоративних мереж.

У наступних розділах ми детально розглянемо процес встановлення PfSense на комп'ютер із двома мережевими інтерфейсами, що дозволить створити базову конфігурацію для подальшого налаштування мережевого захисту та управління трафіком.

Операційна система pfSense відома своєю ефективністю та низьким споживанням системних ресурсів, що робить її придатною для використання навіть на апаратному забезпеченні з невисокими характеристиками. Проте рівень завантаження апаратної частини безпосередньо залежить від того, наскільки інтенсивно використовується система. Кількість одночасно активних сервісів, обсяги переданих і оброблених даних, а також встановлені додаткові програмні модулі — все це істотно впливає на завантаження центрального процесора та використання оперативної пам’яті. Таким чином, чим більше навантаження планується, тим потужнішою має бути апаратна платформа, на якій розгортається pfSense.

Особливо важливим фактором стабільної роботи системи є сумісність мережевих інтерфейсів. pfSense базується на FreeBSD, тому підтримка мережевих карток не така широка, як у деяких інших системах. Найбільш рекомендованими до використання є мережеві адаптери виробництва Intel, оскільки вони забезпечують високу стабільність, низьку затримку та повну сумісність з драйверами системи. Водночас можливо використання карток і від інших виробників, проте перед придбанням обладнання слід перевірити його на сумісність, звернувшись до офіційної документації або списку підтримуваних пристроїв на сайті проекту pfSense.

pfSense створена з прицілом на забезпечення комплексної мережевої безпеки. Її можна успішно впроваджувати як у корпоративному середовищі, так і для захисту домашньої мережі. Завдяки надзвичайно широким можливостям конфігурації, яких нараховується понад сотню, pfSense часто використовується як основний маршрутизатор або міжмережевий екран. Вона підтримує функції фаєрволу, NAT, VPN, балансування навантаження, контроль пропускної здатності, моніторинг трафіку тощо. Крім того, через вбудовану систему розширень можна інтегрувати потужні засоби захисту, такі як Snort або Suricata, які дозволяють реалізувати функціональність систем виявлення та запобігання вторгненням (IDS/IPS).

У системі pfSense можна реалізувати додаткові фізичні мережеві інтерфейси, які дозволяють розділяти трафік за окремими напрямками. Наприклад, один із інтерфейсів може бути виділений для створення демілітаризованої зони (DMZ), у якій розміщуються публічно доступні ресурси (веб-сервери, поштові сервери тощо), ізольовані від внутрішньої корпоративної мережі. Також можливо налаштування окремих сегментів для гостьових мереж, служб адміністрування або IoT-пристроїв, що значно підвищує рівень безпеки та контроль над трафіком.

Однією з ключових переваг pfSense є постійна підтримка розробниками, що проявляється у регулярних оновленнях як самої операційної системи, так і її модульних компонентів. Ці оновлення не лише усувають виявлені вразливості, а й додають новий функціонал, забезпечуючи захист від сучасних кіберзагроз. Завдяки цьому pfSense залишається актуальним і надійним рішенням для захисту мережевої інфраструктури.

Безпекова архітектура pfSense ґрунтується на використанні механізму Stateful Packet Inspection (SPI) — станового аналізу мережевих пакетів, який дозволяє відстежувати статус з'єднання і приймати рішення про пропуск або блокування трафіку на основі контексту, а не лише окремих пакетів. Продуктивність SPI залежить від апаратного забезпечення: при використанні сучасних

мережевих інтерфейсів і потужного процесора система може обробляти трафік на швидкості до 10 Гбіт/с. Зручний графічний інтерфейс адміністрування дозволяє створювати так звані «псевдоніми» — об’єднання IP-адрес, портів і протоколів у логічні групи. Це значно спрощує конфігурацію складних правил фільтрації та підвищує гнучкість налаштувань. pfSense оснащена розвиненою системою моніторингу й логування.

Усі події фіксуються в журналах, доступ до яких здійснюється через вебінтерфейс. Це дозволяє адміністраторам у режимі реального часу аналізувати дії користувачів, виявляти підозрілу активність та своєчасно реагувати на загрози.

PfSense підтримує 64-бітні процесори та може бути інстальований практично на будь-яке апаратне забезпечення. Компанія Netgate також пропонує власні пристрої з попередньо встановленою системою PfSense.

Завантаження та встановлення PfSense є безкоштовним і виконується з офіційного вебсайту. На сторінці завантаження необхідно вибрати архітектуру AMD64, тип інсталяційного образу та сервер для завантаження. Після цього завантажений образ слід розпакувати і записати на USB-накопичувач або CD-диск. (див. рис. 3.12).

Рисунок 3.12 - Вікно налаштування PfSense

Після завантаження pfSense відкриється меню налаштувань.

На першому етапі слід виконати початкову конфігурацію мережі та веб-інтерфейсу (див. рис. 3.13).

Інші параметри можна налаштувати вже після завершення основної інсталяції.

Спочатку потрібно вибрати пункт «Set interface(s) IP address», який знаходиться під номером 2 у меню.

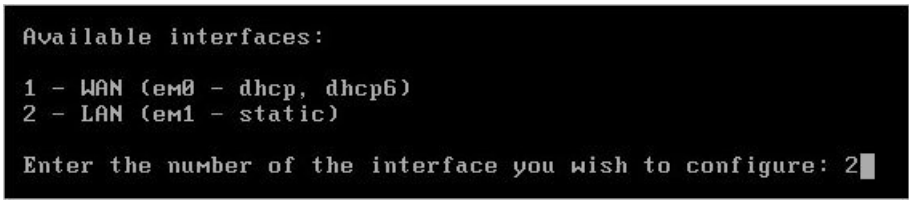


Рисунок 3.13 - Вікно налаштування фізичних інтерфейсів PfSense

Вибираємо інтерфейс для налаштування. Спочатку внутрішній (LAN) (див.рис. 3.14 - 3.16):

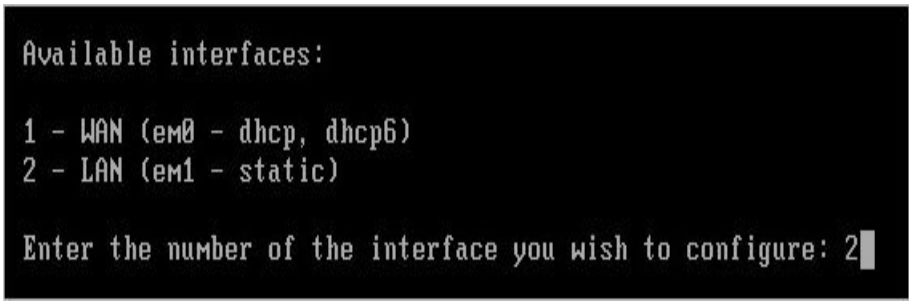


Рисунок 3.14 - Вікно налаштування фізичних інтерфейсів Lan PfSense

Задаємо IP-адресу відповідно до нашої інфраструктури (див.рис. 3.15):

Рисунок 3.15 - Вікно налаштування фізичних інтерфейсів PfSense. Додаємо IP адресу інтерфейсу

Вказуємо маску підмережі (див.рис. 3.16)

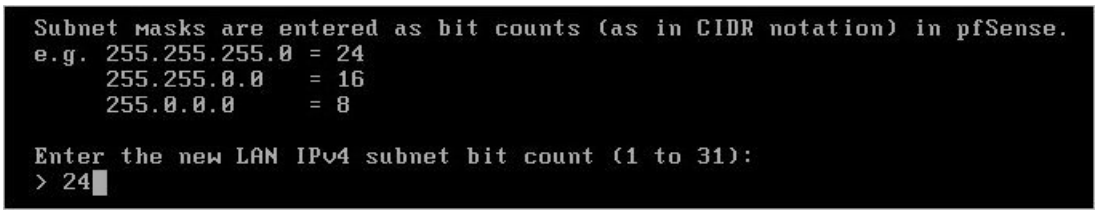


Рисунок 3.16 - Вікно налаштування фізичних інтерфейсів PfSense. Додаємо маску інтерфейсу

За потреби вказується IP-адреса шлюзу, якщо ж вона не потрібна — достатньо натиснути Enter, щоб пропустити цей етап. Далі слід відмовитися від використання HTTP як протоколу для веб-конфігуратора.

Після цього відкриваємо веб-браузер і переходимо за адресою сервера: https://192.168.0.23. У разі появи попередження про потенційну небезпеку підключення, його можна проігнорувати й продовжити завантаження сторінки.

На екрані з’явиться форма авторизації. Для входу використовуються стандартні облікові дані: логін «admin» і пароль «pfsense».

Після успішного входу починається базове налаштування системи. Через інтернет знову використовується ім’я користувача «admin» та пароль «pfsense».

Далі обирається порт для підключення та підтверджується використання сертифіката безпеки.

Система запропонує покрокову інструкцію, яка допоможе завершити первинну конфігурацію. Після цього відкриється доступ до додаткових параметрів, де можна адаптувати інтерфейс згідно з потребами конкретної мережі.

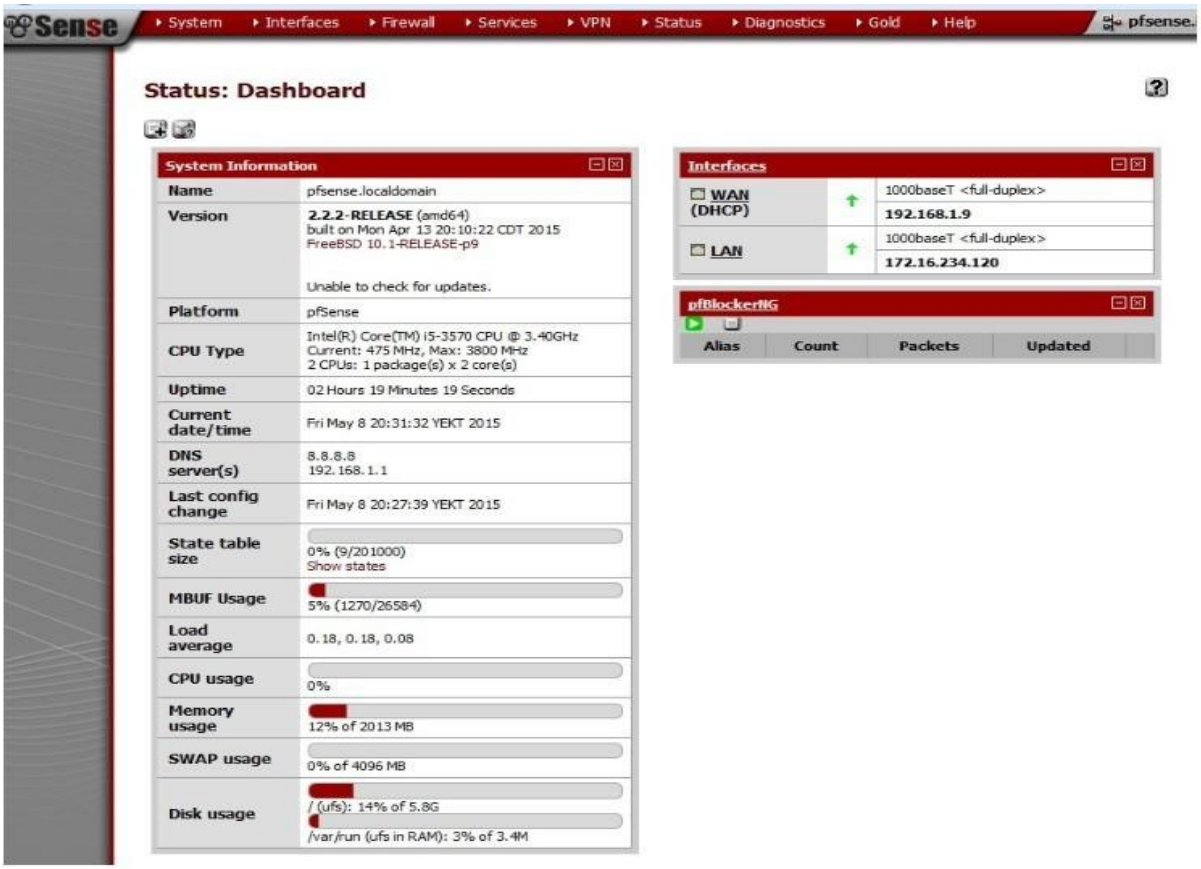


Рисунок 3.17 - Вікно WEB інтерфейсу PfSense

Після налаштування мережевих інтерфейсів відкривається меню з обмеженим набором функцій, серед яких передбачено доступ до командного рядка (shell). Однією з корисних опцій цього меню є можливість відновлення пароля для доступу до веб-інтерфейсу.

Розробники pfSense наполегливо радять виконувати основну конфігурацію системи через графічний веб-інтерфейс, який відзначається зручністю у користуванні та широкими можливостями персоналізації завдяки гнучким налаштуванням віджетів.

У головному розділі веб-інтерфейсу відображається загальна інформація про систему. Інтерфейс легко адаптується під потреби користувача — віджети можна додавати або видаляти залежно від власних вподобань.

– Система PfSense: Тут можна налаштовувати веб-сервер, додавати параметри безпеки, керувати авторизацією користувачів, конфігурувати брандмауер та управляти мережевими параметрами. Також передбачена можливість регулювання продуктивності системи шляхом увімкнення або вимкнення окремих сервісів. У цьому розділі можна створювати центри сертифікації (CA), необхідні для налаштування VPN-серверів.
– Загальні налаштування: Цей розділ дозволяє змінювати ім’я системи, доменне ім’я, параметри сервера та персоналізувати PfSense. Тут також створюються групи користувачів із визначенням індивідуальних прав доступу.
– Інтерфейси PfSense: Містить параметри налаштування WAN та LAN, включно з логічними і фізичними інтерфейсами, а також різними режимами роботи мережі.
– Брандмауер: Тут створюються та редагуються основні правила роботи брандмауера. Важливою функцією є можливість створення псевдонімів для IP-адрес та портів, що полегшує групування адрес для більш ефективного управління правилами. Порядок розташування правил має значення: індивідуальні правила розміщуються зверху, а загальні — унизу, що забезпечує правильний пріоритет їх застосування. У цьому розділі також налаштовують NAT і його компоненти, а та-

кож створюють плаваючі правила для гнучкішого контролю мережевого трафіку.

– Служби та послуги: Однією з ключових служб є DNS-перетворювач, що розширює можливості налаштування правил і обробки DNS-запитів. ключа, алгоритм хешування, термін дії та повне ім’я сертифіката. Цей CA знадобиться для створення OpenVPN-сервера та налаштування LDAP через LDAPS (див. рис. 3.18).

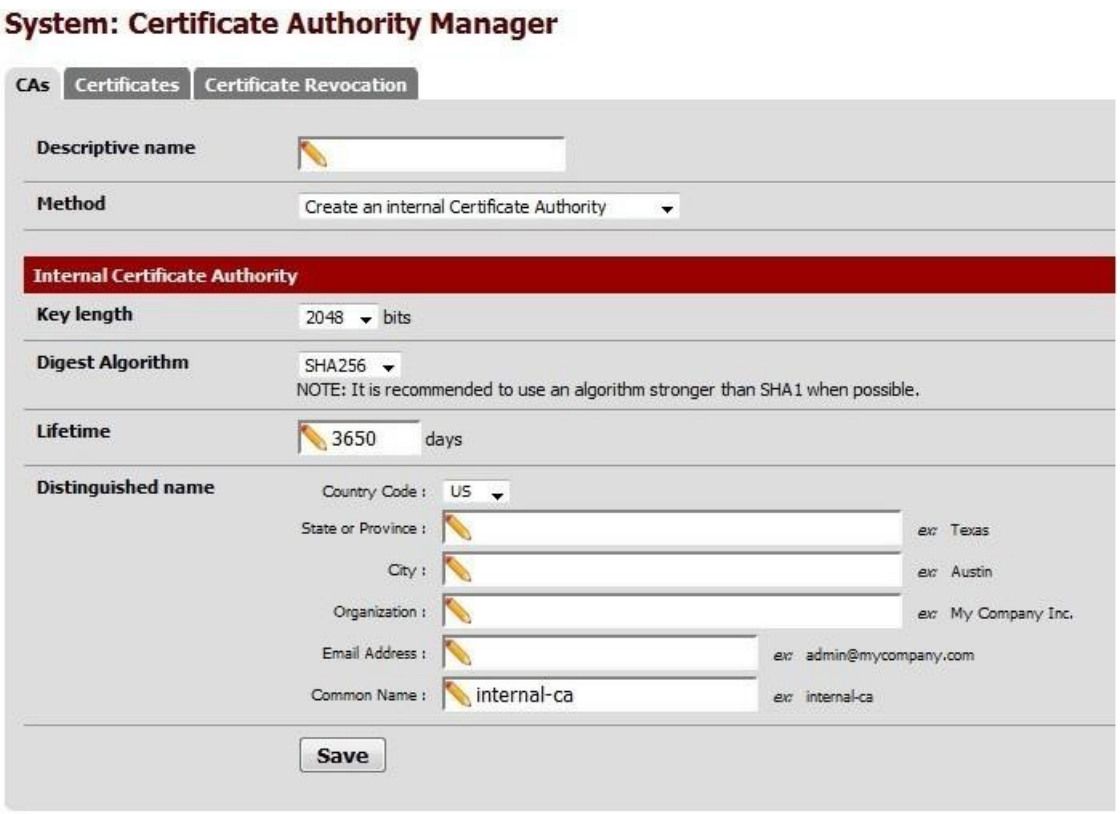


Рисунок 3.18 - Вікно WEB інтерфейсу PfSense для створення ключа авторизації

Перейдемо до налаштування правил фільтрації трафіку (див. рис. 3.19). Для групування адрес, портів чи URL використовуйте вкладку Aliases. Також можна встановлювати часові проміжки для дії правил. За замовчуванням існує

правило «все дозволено» та правило, що забезпечує доступ до веб-інтерфейсу. Процес створення правил досить простий.

Проте є низка додаткових можливостей, наприклад, дозволені ОС, які можна виставити TCP-прапори, графік роботи правила, і навіть інспектор протоколів прикладного рівня.

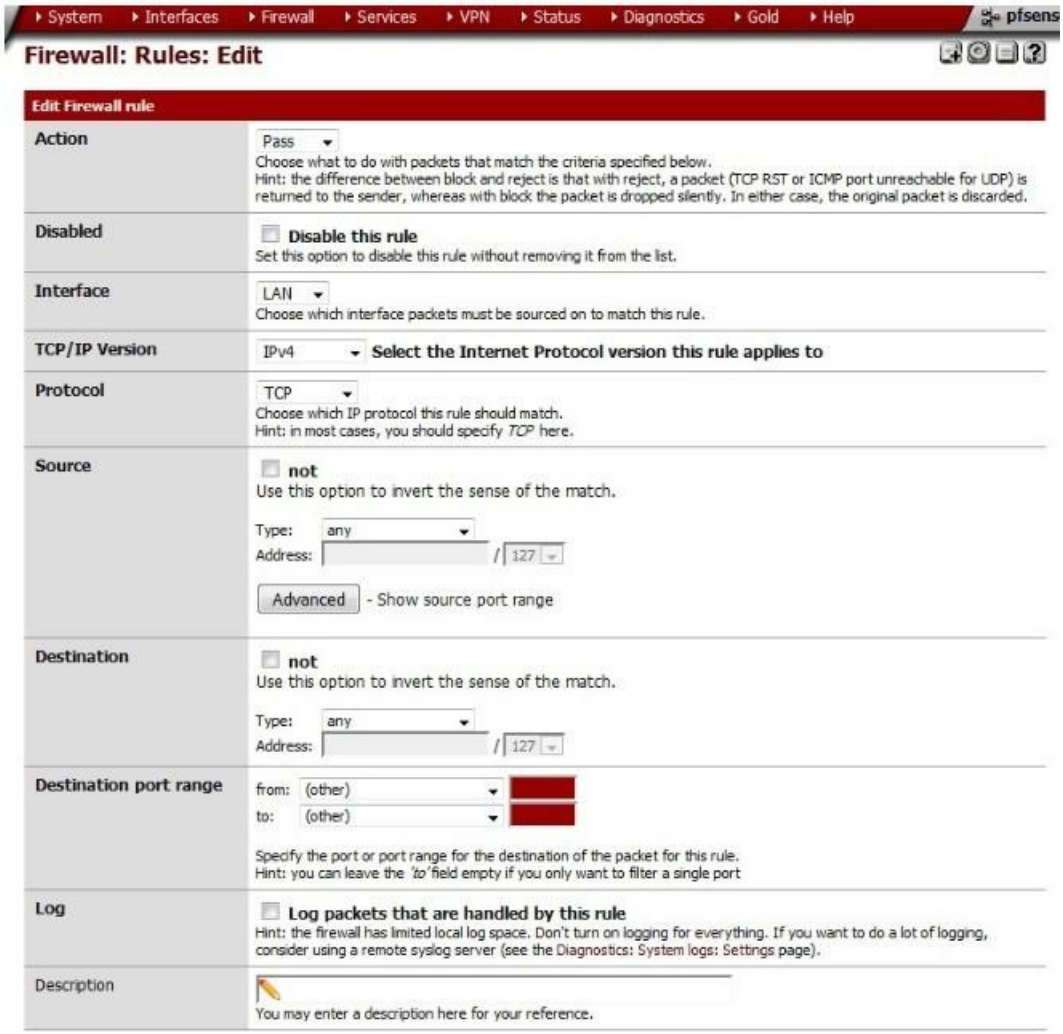


Рисунок 3.19 - Вікно WEB інтерфейсу PfSense для вказування правил фільтрації потоків

Налаштування віддаленого доступу OpenVPN з автентифікацією по паролю та сертифікату можна переглянути тут — www.youtube.com/watch?v=VdAHVSTl1ys.

Для віддаленого доступу доступні протоколи IPSec, L2TP, PPTP та OpenVPN, причому PfSense попереджає, що PPTP є небезпечним і радить обрати інший.

Аутентифікація в локальній базі була вибрана з метою збереження можливості віддаленого підключення у разі несправностей із серверами каталогів.

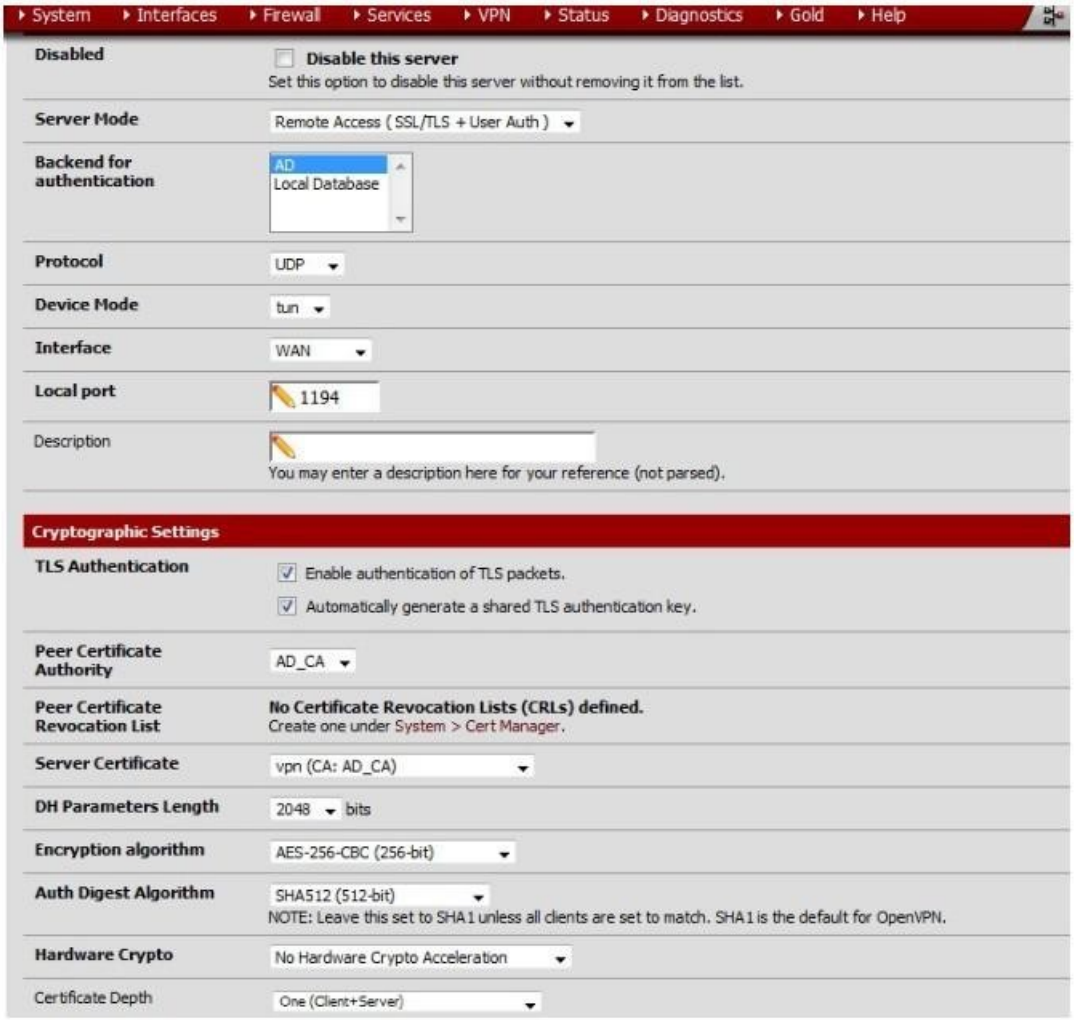


Рисунок 3.20 - Вікно WEB інтерфейсу PfSense для підключення бази АД

Щоб експортувати налаштування OpenVPN для різних платформ, потрібно встановити пакет OpenVPN Client Export Utility з доступного списку пакетів. Після цього у Cert Manager створюємо сертифікати для VPN-сервера та клієнтів, які відрізняються лише типом. Далі налаштовуємо сервер OpenVPN, обравши режим «Remote Access (SSL/TLS + User Auth)» та конфігуруємо аутентифікацію сервера.

Протокол, порт, потрібний сертифікат сервера VPN і виставляємо потрібні параметри шифрування (див.рис. 3.20). Те, що пропонується за умовчанням, — не найкращий вибір.

Далі налаштовуємо VPN-мережу та параметри для клієнтів, наприклад, чи надавати клієнту DNS-сервери або чи направляти весь його трафік через тунель. Після збереження переходимо на вкладку client export, звідки експортуємо потрібні налаштування та сертифікат користувача (див. рис. 3.21).

Рисунок 3.21 - Вікно WEB інтерфейсу PfSense для налаштування авторизації VPN користувача

При налаштуванні сервера можна скористатися майстром (Wizard), який крок за кроком проведе вас через процес налаштування OpenVPN. Проте, якщо

віддаленим доступом користується багато користувачів, робота з видачею та відгуком сертифікатів, експортом налаштувань і додаванням користувачів у локальну базу стає доволі рутинною, але відповідальною задачею. На мою думку, у разі масштабування доцільно використовувати окремий центр сертифікації (CA) з CRL та єдину систему автентифікації, наприклад Active Directory. Якщо ж кількість користувачів невелика, запропонований варіант цілком ефективний.

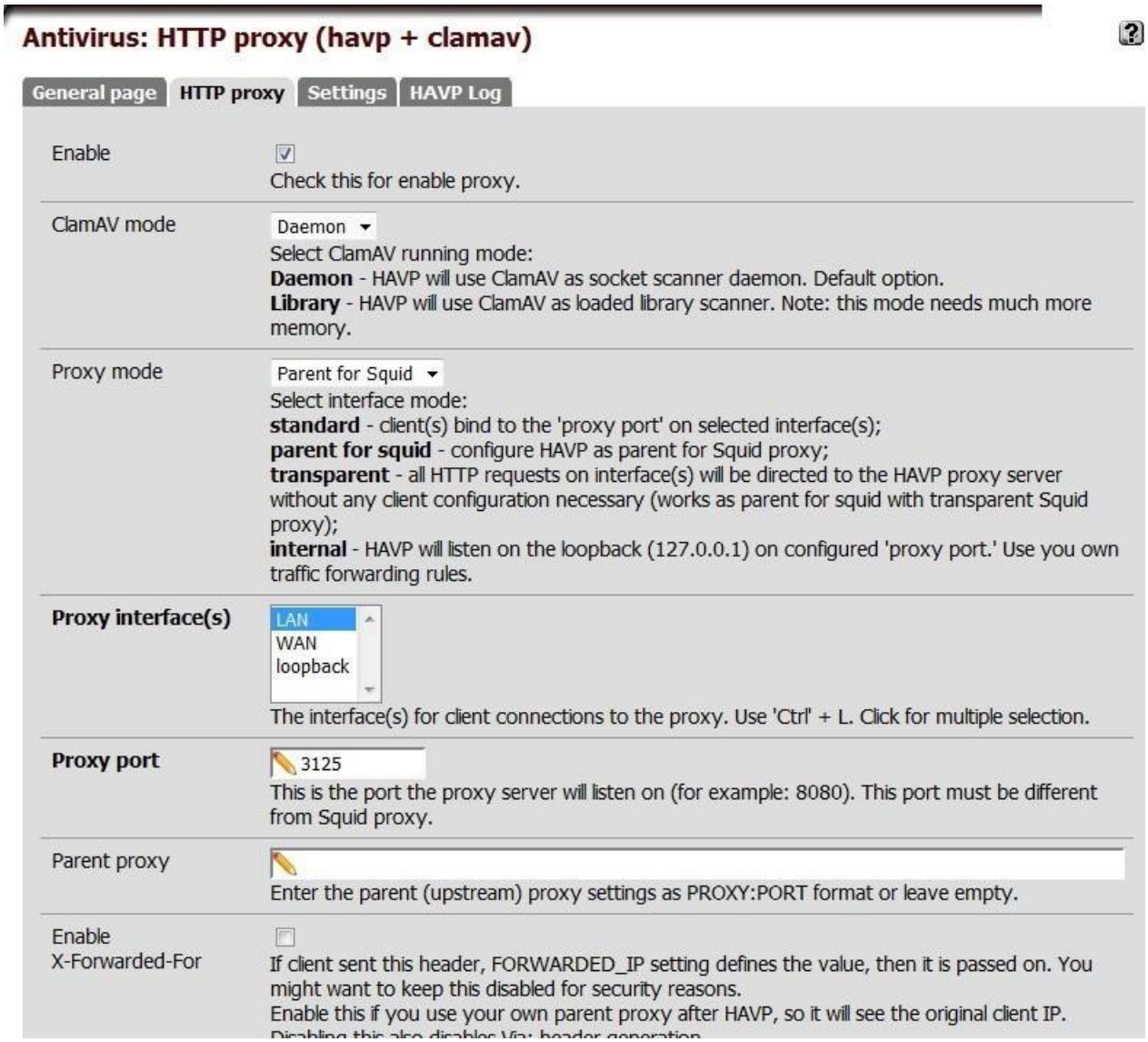


Рисунок 3.22 - Вікно WEB інтерфейсу PfSense для встановлення HAVP-пакету проксі із ClamAV сканером

Залишилося налаштувати проксі, фільтрацію контенту та антивірусну перевірку (див. рис. 3.22). Встановлюємо пакет HAVP — проксі-сервер із сканером ClamAV. Для конфігурації вказуємо режим роботи ClamAV та проксі, порт, інтерфейс і параметри перевірки трафіку. Оскільки використовується Squid, вибираємо режим «Parent for Squid». Окремо налаштовуємо оновлення антивірусних баз та їх дзеркала.

Переходимо до налаштування Squid.

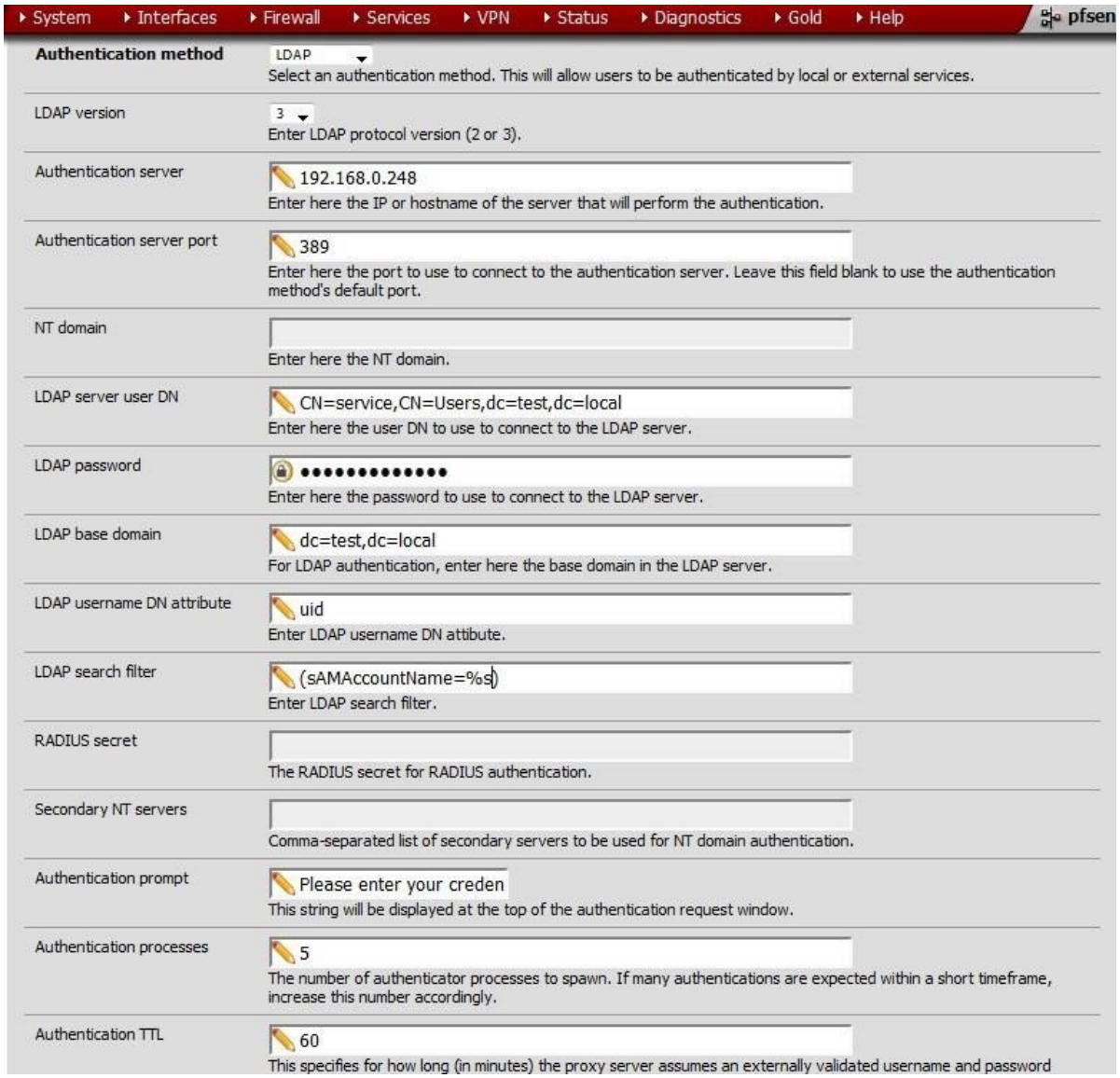


Рисунок 3.23 - Вікно WEB інтерфейсу PfSense для встановлення матоду авторизації Squid та для інтеграції з контролером домену

Після встановлення пакета вибираємо режим роботи проксі та порт, а на вкладці «Auth Settings» вказуємо обраний метод аутентифікації. Оскільки планується використання Active Directory як бази користувачів, застосовуємо протокол LDAP. Налаштування для інтеграції з контролером домену наведено нижче (див. рис. 3.23).

При необхідності налаштовуємо параметри вишого проксі, керування кешем та трафіком, а також ACL.

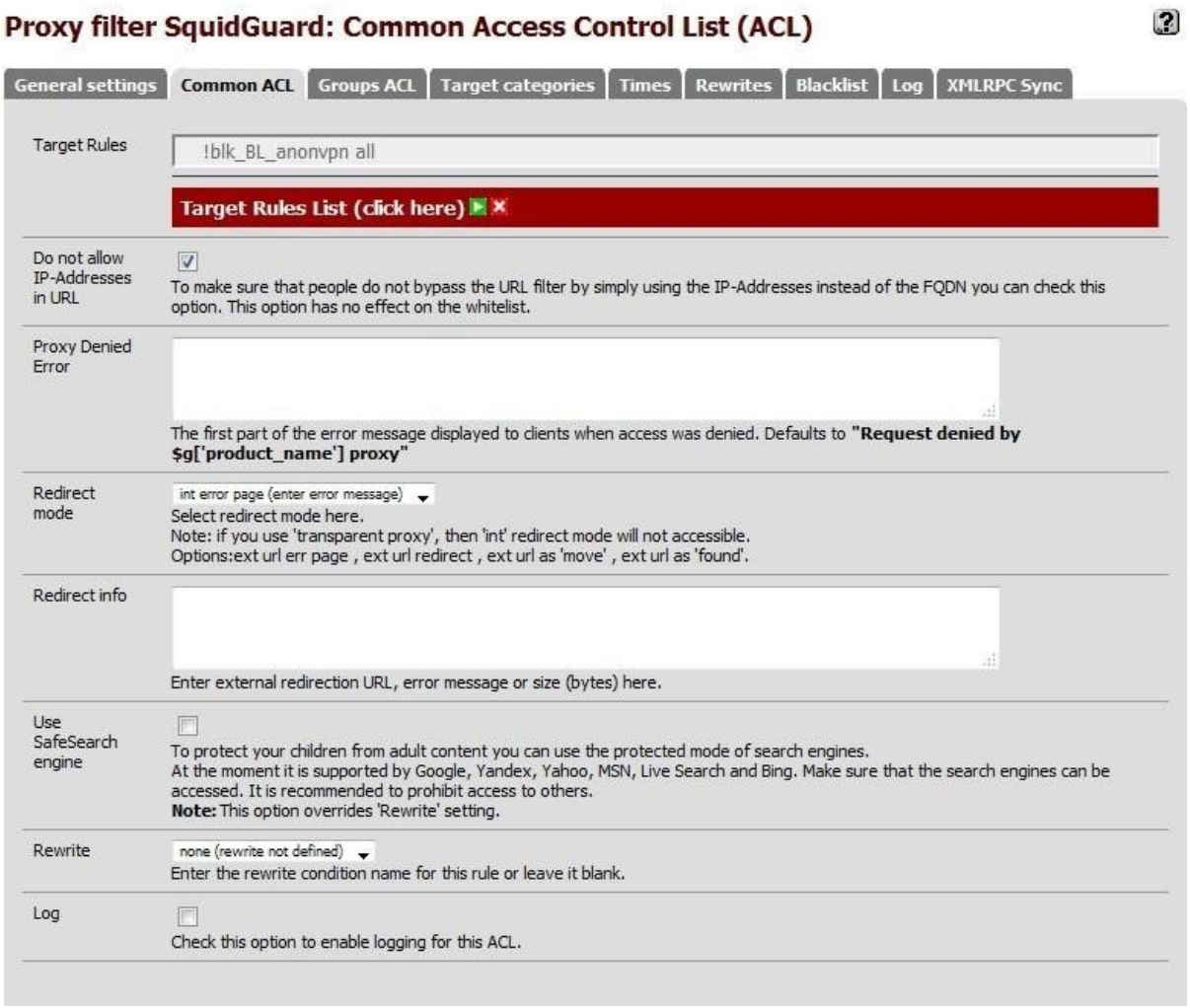


Рисунок 3.24 - Вікно WEB інтерфейсу PfSense для доналаштування Squid. Proxy filter SquidGuard: Common Access Control List (ACL)

Тепер налаштовуємо фільтрацію за допомогою squidGuardian (див. рис. 3.24). Після встановлення через меню "Services" у пункті "Proxy filter" переходимо до конфігурації squidGuardian. На вкладці Blacklist вказуємо джерело завантаження блеклистів у форматі tar або tar.gz, а на вкладці General settings активуємо використання цих блеклистів.

Наступним кроком є налаштування фільтрації за допомогою squidGuardian (див. рис. 3.24). Після встановлення пакета через меню "Services" у розділі "Proxy filter" переходьте до його конфігурації. На вкладці Blacklist потрібно вказати джерела для завантаження блеклистів у форматах tar або tar.gz — це дозволить системі автоматично оновлювати списки заборонених сайтів. На вкладці General settings слід активувати опцію використання блеклистів, щоб фільтрація працювала ефективно. Такий підхід забезпечує контроль доступу до небажаного контенту і підвищує безпеку мережі загалом.

3.4 Інструкція з використання тестових наборів та тестових програм

Для діагностики мережевих з’єднань використовують команди PING та TRACERT. Якщо виникають підозри на відсутність зв’язку з певним мережевим вузлом, першим кроком зазвичай є команда PING (Packet Internet Groper). Ця утиліта дозволяє перевірити коректність налаштувань TCP/IP як на локальному, так і на віддаленому комп’ютері.

Головне призначення команди — визначити наявність фізичного зв’язку між двома мережевими пристроями. Для обміну пакетами з віддаленим вузлом використовується протокол ICMP. Віддалена система відповідає, надсилаючи пакети назад, утворюючи так зване «коло». Результатом виконання команди є інформація про час відповіді та повідомлення про помилки, якщо відповіді немає.

У Windows команда має такий синтаксис:

ping [ключі] адреса (ім’я) вузла

Нижче наведені основні ключі для команди ping:

– -t — надсилає запити безперервно до тих пір, поки не буде зупинено командою Ctrl-C;
– -a — показує імена вузлів замість IP-адрес;
– -n число — задає кількість відправлених ехо-запитів;
– -l довжина — встановлює розмір ехо-запиту;
– -f — забороняє фрагментацію пакету, що допомагає перевірити, чи змінюється розмір пакета на маршруті;
– -i час — визначає час життя пакету (TTL — Time to Live);
– -v тип — задає тип обслуговування (TOS);
– -r число — відображає маршрут для вказаної кількості переприйомів;
– -s число — задає час для певної кількості переприйомів;
– -j список вузлів — маршрутизує пакети через перелічені вузли, які можуть бути розділені шлюзами;
– -k список вузлів — маршрутизує пакети через перелічені вузли без розділення шлюзами.
– w час — задає час очікування відповіді у мілісекундах.

Команда TRACERT також використовує протокол ICMP, але її мета — визначити всі проміжні пристрої, через які проходить пакет на шляху до кінцевого вузла. З її допомогою можна отримати детальну інформацію про роботу мережі. Приклад використання показаний на рисунку 3.25.

Синтаксис команди:tracert [ключі] ім’я_вузла

– -d — використовувати IP-адреси замість імен вузлів;
– -h максимальне_число_переприйомів — задає максимальну кількість спроб для досягнення цілі;

– -j список_вузлів — маршрутизує пакети через перелік зазначених вузлів, причому послідовні вузли можуть бути розділені шлюзами, що дозволяє гнучко обирати шлях серед вказаних систем;

– -w час — встановлює час очікування відповіді в мілісекундах.

Також існує команда IPCONFIG, яка використовується для отримання інформації про налаштування TCP/IP на сервері або робочій станції Windows NT. Вона показує дані про всі мережеві адаптери в системі, а також про з'єднання PPP. Основні відомості, що відображаються:

– IP-адреса;

– маска підмережі;

– шлюз за замовчуванням;

– DNS-сервери;

– домен NT.

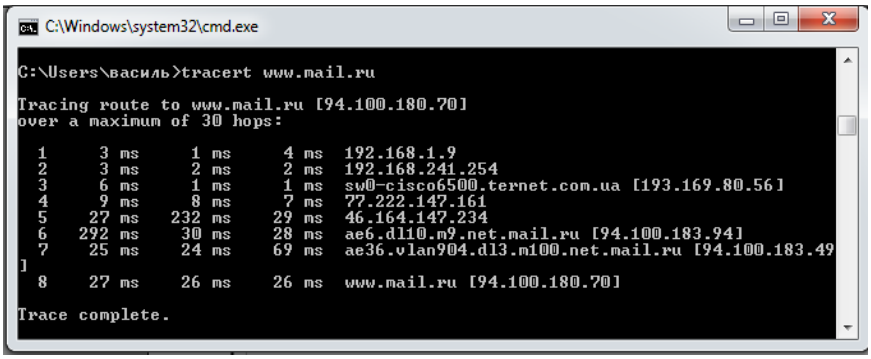


Рисунок 3.25 – Застосування команди TRACERT

4 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу даної кваліфікаційної роботи є проведення економічного обґрунтування доцільності розробки проєкту локальної комп'ютерної мережі для підприємства "КЕТ", а також визначення її економічної ефективності з подальшим прийняттям рішення щодо впровадження або відмови від реалізації проєкту.

Для розрахунку вартості науково-дослідної роботи необхідно пройти низку послідовних етапів:

- описати технологічний процес створення мережі з деталізацією трудомісткості кожного етапу; визначити витрати на оплату праці основного та допоміжного персоналу з урахуванням обов'язкових соціальних внесків;
- обрахувати матеріальні витрати, необхідні для реалізації проєкту;
- здійснити розрахунок споживання електроенергії для забезпечення виробничих процесів; врахувати транспортні витрати, пов'язані з реалізацією проєкту;
- здійснити нарахування амортизаційних відрахувань для обладнання та інфраструктури; визначити рівень накладних витрат;
- скласти загальний кошторис і визначити повну собівартість науково-дослідної роботи; встановити ціну виконання проєкту.

4.1 Визначення стадій технологічного процесу та загальної тривалості проведення НДР

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

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

№ п/п	Назва операції	Виконавець	Середній час виконання, год
1	Підготовка	Інженер	6
2	Проєктування мережі	Інженер	18
3	Прокладання кабелю	Технік	14
4	Монтаж обладнання	Технік	10
5	Налаштування ПЗ	Лаборант	9
6	Перевірка та тестування	Технік	7
Разом		—	64

4.2 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Згідно із Законом України «Про оплату праці», заробітна плата – це грошова винагорода, яку роботодавець або уповноважена особа виплачує працівнику за виконану ним роботу.

Рівень заробітної плати визначається з урахуванням складності та умов праці, професійних навичок і якостей працівника, результатів його діяльності, а також фінансових показників підприємства.

Заробітна плата поділяється на основну та додаткову. Основна частина – це оплата за фактично виконану роботу відповідно до тарифних ставок, окладів або відрядних розцінок, і вона не залежить від економічного стану підприємства.

Нараховують додаткову заробітну плату залежно від досягнутих і запланованих показників, умов виробництва, кваліфікації виконавців. Джерелом додаткової оплати праці є фонд матеріального стимулювання, який створюється за рахунок прибутку.

Основна заробітна плата розраховується за формулою:

$$Зосн.=Тс\times Кг, \quad (4.1)$$

де Тс – тарифна ставка, грн.;

Кг – кількість відпрацьованих годин. Зосн.= 160*32 + 120*25 + 105*20 = 10220грн.

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

$$Здод.= Зосн.\times Кдопл., \quad (4.2)$$

де Кдопл. – коефіцієнт додаткових виплат працівникам. Здод.= 10220 * 0,12 = 1226,40 грн.

Звідси загальні витрати на оплату праці (Во.п.) визначаються за формулою:

$$Во.п.= Зосн.+ Здод., \quad (4.3)$$

Во.п. = 10220 + 1226,40 = 11446,40 грн .

Крім того, слід визначити відрахування на заробітну плату:

1. єдиний соціальний внесок .

Отже, сума відрахувань на соціальні заходи буде становити:

$$Вз.п.=ФОП \times 0,22, \quad (4.4)$$

де ФОП – фонд оплати праці, грн. Во.п. = 11446,40 * 0,22 = 2518,21 грн.

Проведені розрахунки зведемо у наступну таблицю 4.2.

Таблиця 4.2 - Зведені розрахунки витрат на оплату праці

№ п/п	Категорія	заробітна плата, грн.			Дод. заробіт-напла-	Нарах. на ФОП,	Всього ви-трати на опл. пр.,
	праці-	Тарифна	К-сть	Факт.			
	вників	ставка,	від-пра-	нарах.	та, грн.	грн.	грн.
		грн.	цьов.	з/пл.,			6=3+4+5
			год.	грн.			
А	Б	1	2	3	4	5	6
1	Інженер	160	32	5120,00	614,40	—	—
2	Технік	120	25	3000,00	360,00	—	—
3	Лаборант	105	20	2100,00	252,00	—	—
	Разом	—	—	10220,00	1226,40	2518,21	13964,61

4.3 Розрахунок матеріальних витрат

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

$$МВі = qi \times pi , \quad (4.5)$$

де qi – кількість витраченого матеріалу і-го виду; pi – ціна матеріалу і-го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$Зм.в. = \sum МВі \quad (4.6)$$

Зм.в .= 243890,00грн.

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

№	Найменування матеріалу	Од.	Кількість	Ціна, грн	Сума, грн
1	Кабель UTP Cat6	м	700	16,00	11200,00
2	Роз’єми RJ-45	шт	180	15,00	2700,00
3	Розетки RJ-45	шт	50	90,00	4500,00
4	Кабель-канал 40×25×2м	шт	60	52,00	3120,00
5	Дюбель	шт	300	0,55	165,00
6	Комутатори TP-Link TL-SF1008P	шт	4	3900,00	15600,00
7	Керований комутатор MikroTik CRS305	шт	1	12500,00	12500,00
8	Точка доступу TP-Link EAP225	шт	2	4600	9200,00
9	Сервер HP ProLiant DL20 Gen10	шт	3	65000,00	195000,00
	Разом				243890

4.4 Розрахунок витрат на електроенергію

Затрати на електроенергію 1-ці обладнання визначаються за формулою:

$$Зе=W \cdot T \cdot S, \quad (4.7)$$

де W – необхідна потужність, кВт;

T – кількість годин роботи обладнання;

S – вартість кіловат-години електроенергії.

Для розробки проекту даної локальної комп'ютерної мережі використовується один ПК, потужність якого W = 0,5 кВт і який працює 33 годин.

Зе = 0,45 кВт * 32 год * 6,80 грн = 97,92 грн

4.5 Визначення транспортних затрат

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

$$Тв=Зм.в.\times 0,08 \dots 0,1, \quad (4.8)$$

де ТВ – транспортні витрати.

Тв Тв = 243890,00 * 0,09 = 21950,10 грн

4.6 Розрахунок суми амортизаційних відрахувань

Характерною особливістю застосування основних фондів у процесі виробництва є їх відновлення.

Для відновлення засобів праці у натуральному ви- разі необхідне їх відшкодування у вартісній формі, яке здійснюється шляхом амортизації.

Комп'ютери та оргтехніка належать до четвертої групи основних фондів.

Мінімально допустимі строки їх корисного використання 2 роки.

Для визначення амортизаційних відрахувань застосовуємо формулу:

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

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

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

НА – норма амортизації, %.

Для проектування даної комп'ютерної мережі використовується один комп'ютер (вартість якого становить 23000,00 грн.), який працює 33 годин.

Тоді:

А = 24000 грн * 0,05 * 32 / 150 = 256,00 грн

4.7 Обчислення накладних витрат

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

$$Нв = Во.п. \times 0,2 \ldots 0,6, \quad (4.10)$$

де НВ – накладні витрати.

$$Нв = 11446,40 \cdot 0,5 = 5723,20 \text{ грн.}$$

4.8 Складання кошторису витрат та визначення собівартості НДР

Результати проведених вище розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 – Кошторис витрат на НДР

Стаття витрат	Сума, грн	Відсоток від загальної суми, %
Оплата праці	11446,40	5,03
Соціальні відрахування	2518,21	1,11
Матеріальні витрати	243890,00	85,02
Електроенергія	97,92	0,03
Транспортні витрати	21950,10	7,65
Амортизація	256,00	0,09
Накладні витрати (2,5%)	7172,94	2,49
Усього (Собівартість)	287331,57	100,00

Собівартість (СВ) НДР розрахуємо за формулою:

Св= Во.п.+ Вс.з.+ Зм.в.+ Зе + Тв +А+ Нв Св= 287881,83 грн. (4.11)

4.9 Розрахунок ціни НДР

Ціну НДР можна визначити за формулою:

$$Ц = Св \cdot (1+Ррен) \cdot (1+ПДВ), \quad (4.12)$$

де Ррен. – рівень рентабельності; К – кількість замовлень, од.;

Ві.н. – вартість носія інформації, грн.;

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

Ц= 287331,57 + 57466,31 = 345638,28 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) і термін окупності ($T_{ОК}$).

$$ЧТВ = -K_B + \sum_{i=1}^{t} \frac{Г_П}{(1+i)^t} \quad (4.13)$$

де КВ – затрати на проект;

Гп – грошовий потік за t – ий рік;

t – відповідний рік проекту;

i - величина дисконтної ставки (10…15%).

ЧТВ = — 287881,83 +258774,33/(1+0,15)+ 258774,33/ (1+0,15)2=1311910,98 (грн.)

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

Термін окупності визначається за формулою:

$$T_{ОК} = Т_{ПВ} + \frac{H_B}{Г_{ПР}} \quad (4.14)$$

де ТПВ – період до повного відшкодування витрат, років; НВ – невідшкодовані витрати на початок року, грн.;

ГПР – грошовий потік на початок року, грн. ТОК=1+29107,50/258774,33=1,11

Таблиця 4.5 - Економічні показники НДР

№ п/п	Показник	Значення
1.	Собівартість	287881,83
2.	Плановий прибуток (20%)	57576,37
3.	Ціна	345638,20
4.	Чиста теперішня вартість (ЧТВ)	131910,98
5.	Термін окупності	1,11 роки

В результаті аналізу економічних показників, розрахованих та зведених у таблицю 4.5, можна прийти до висновку, що при терміні окупності – 1,1 роки. Проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним.

5 ОХОРОНА ПРАЦІ, ТЕХНІКА БЕЗПЕКИ ТА ЕКОЛОГІЧНІ ВИМОГИ

5.1 Пожежна безпека приміщення комп’ютерної компанії “КЕТ”

Забезпечення пожежної безпеки у приміщеннях комп’ютерної компанії “КЕТ” є важливою складовою безпечної експлуатації офісного простору, особливо враховуючи інтенсивне використання електронного обладнання, зокрема серверів, комп’ютерів, маршрутизаторів, мережевих комутаторів, офісної техніки та великої кількості електрокабелів.

Основними причинами виникнення пожеж у таких приміщеннях можуть бути: коротке замикання, перегрів обладнання, перевантаження електромережі, несправність розеток або людський фактор (залишення ввімкнених приладів, порушення правил користування електрообладнанням тощо).

Компанія “КЕТ” дотримується чинних норм пожежної безпеки згідно з ДБН В.2.5-56:2014, Правилами пожежної безпеки в Україні (НАПБ А.01.001-2014) та внутрішніми розпорядчими документами. Усі приміщення оснащені системою пожежної сигналізації, датчиками диму, ручними сповіщувачами та централізованим оповіщенням. Обов’язковою умовою є наявність сертифікованих вогнегасників (порошкових та вуглекислотних), які проходять щорічне технічне обслуговування.

Кожен працівник компанії ознайомлений із правилами евакуації та вміє користуватись первинними засобами пожежогасіння. Працівники регулярно проходять первинний, повторний, позаплановий та цільовий інструктажі з пожежної безпеки. У компанії проводяться тренування з евакуації, на яких працівники відпрацьовують навички організованого покидання приміщень.

Усі евакуаційні виходи відкриті та позначені згідно зі стандартами — світловими табличками, фотолюмінесцентними стрілками та планами евакуації. Всі дерев'яні елементи оброблені вогнезахисними засобами, а легкозаймисті матеріали зберігаються у спеціально відведених, захищених місцях.

Крім того, у компанії “КЕТ” заборонено користуватись електронагрівальними приладами (чайниками, обігрівачами) без відповідного дозволу адміністрації та технічної перевірки. Перед завершенням робочого дня відповідальні особи здійснюють контроль за вимкненням усіх електроприладів, освітлення, перевіряють стан розеток і проводів.

5.2 Системний підхід у безпеці життєдіяльності

Системний підхід у безпеці життєдіяльності є ключовим інструментом створення надійного, безпечного та здорового середовища для працівників комп’ютерної компанії “КЕТ”. Він передбачає розгляд усіх елементів взаємодії “людина — середовище — техніка — організація”, як єдиної інтегрованої системи, де порушення в одному компоненті впливає на всю систему.

У межах цього підходу безпека життєдіяльності розглядається не як набір окремих заходів, а як безперервний процес управління ризиками, що охоплює виявлення небезпек, їх аналіз, оцінку ризиків, планування та реалізацію заходів, моніторинг результатів, коригування дій та вдосконалення безпекових механізмів.

Компанія “КЕТ” впровадила багаторівневу модель безпеки, яка включає такі ключові напрямки:

1. Аналіз умов праці

Постійно здійснюється оцінка робочих місць на предмет відповідності санітарно-гігієнічним, ергономічним, електробезпековим та психологічним вимогам. Проводиться вимірювання рівня освітлення, шуму, мікроклімату, організовується провітрювання та очищення повітря. Здійснюється аудит кабельних систем, організації робочого простору, техніки безпеки при користуванні ПК, периферійними пристроями, мережевим обладнанням.

2. Навчання та інструктажі

Усі працівники проходять вступний, первинний, повторний, позаплановий та цільовий інструктажі з охорони праці, техніки безпеки, пожежної безпеки та надання першої медичної допомоги. Навчання проводиться як очно, так і дистанційно — через корпоративну платформу з відеоуроками, тестами та інструкціями.

3. Управління психоемоційним станом персоналу

Ураховуючи інтенсивне використання комп'ютерної техніки, ризики зорового перенапруження, розумового вигорання та стресу, компанія забезпечує:

- гнучкий графік роботи;
- перерви для відпочинку очей і тіла;
- доступ до психологічної підтримки;
- неформальні заходи (тимбілдінг, спортивні події);
- можливість часткової або повної віддаленої роботи.

4. Організаційні заходи безпеки

Здійснюється постійне планування, аудит ризиків та контроль за їх мінімізацією. Для цього існує система подання скарг і пропозицій щодо покращення умов праці. Ведеться документація з охорони праці, фіксуються всі події, пов'язані з безпекою — навіть потенційно небезпечні (near-miss).

5. Профілактика професійних захворювань

Робочі місця обладнані з урахуванням ергономічних вимог: регульовані крісла, столи, підставки під ноги, монітори встановлені на оптимальній висоті. Працівники проходять періодичні профілактичні медичні огляди, консультації офтальмолога та терапевта. Рекомендується гімнастика для очей та м'язів, йога або активний рух у перервах.

6. Інтеграція цифрових інструментів у безпеку

Компанія застосовує системи моніторингу температурного режиму серверних, автоматичні оповіщення про технічні несправності, відеоспостереження на об’єкті. Системи електроживлення обладнані стабілізаторами та джерелами безперебійного живлення (UPS).

5.3 Екологічна відповідальність та поводження з електронними відходами

Екологічна відповідальність є невід’ємною частиною сучасної корпоративної політики компанії “КЕТ”. Компанія визнає важливість збереження навколишнього природного середовища не лише як обов’язок перед державними екологічними нормами, а і як етичний обов’язок перед суспільством, майбутніми поколіннями та власними працівниками.

Основний акцент робиться на безпечному поводженні з електронними відходами, які утворюються в результаті діяльності компанії. До них належать: зношені комп’ютери, сервери, монітори, принтери, клавіатури, миші, жорсткі диски, кабелі, акумулятори, картриджі, системні блоки тощо. Усі ці компоненти містять елементи, що можуть бути токсичними або небезпечними у разі потрапляння до навколишнього середовища.

Для безпечної утилізації обладнання укладено договори зі спеціалізованими фірмами, які мають відповідні ліцензії на збирання, транспортування та переробку електронних відходів згідно з вимогами Закону України «Про управління відходами». У компанії призначено відповідальну особу, яка веде облік утворених електронних відходів та контролює правильність їхнього зберігання і передачі на утилізацію.

Крім поводження з технікою, у компанії активно діє система сортування побутових і офісних відходів. Працівники мають доступ до контейнерів для роздільного збору паперу, пластику, металу, скла, батарейок, люмінесцентних

ламп. Усі контейнери мають відповідне маркування, розміщені в зонах загального користування, а персонал регулярно інформується про правила сортування.

З метою зменшення екологічного сліду компанія “КЕТ” вжила такі заходи:

– запроваджено електронний документообіг, що дозволило скоротити використання паперу більш ніж на 70%;
– використовуються енергоощадні LED-лампи, які споживають до 10 разів менше електроенергії;
– установлено таймери і сенсорні вимикачі освітлення, які вимикають світло автоматично в порожніх приміщеннях;
– техніка налаштована на “режим сну”, коли не використовується;
– організовано закупівлю картриджів для принтерів з можливістю повторної заправки або відправки на переробку;
– встановлено політику “зеленої закупівлі” — надається перевага постачальникам, які дотримуються принципів екологічної відповідальності.

Крім внутрішніх заходів, компанія прагне брати участь у зовнішніх екологічних ініціативах. Щороку працівники залучаються до акцій із посадки дерев, прибирання міських територій, екомарафонів та флешмобів. Такі заходи не лише формують корпоративну згуртованість, а й підвищують екологічну свідомість кожного учасника.

Для підвищення рівня екологічної грамотності проводяться внутрішні вебінари, інформаційні кампанії, розповсюджуються буклети про вплив електронного сміття на довкілля та поради щодо ощадливого використання ресурсів.

У майбутньому компанія “КЕТ” планує впровадити систему екологічного менеджменту відповідно до стандарту ISO 14001:2015, що дозволить структуровано і прозоро керувати всіма аспектами впливу на довкілля, а також покращити звітність, облік і стратегічне планування в цьому напрямі.

Завдяки цим крокам компанія не лише виконує законодавчі вимоги, але й відіграє активну роль у формуванні сталої екологічної політики на рівні регіону, створюючи приклад для інших організацій у сфері ІТ.

ВИСНОВКИ

У ході виконання кваліфікаційної роботи для підприємства КЕТ було спроєктовано комп’ютерну мережу. Проведено аналітичний огляд наукової літератури та існуючих рішень, на основі якого розроблено логічну та фізичну топологію мережі. Обґрунтовано вибір пасивного й активного комутаційного обладнання, сервера, точки доступу та програмного забезпечення.

Кваліфікаційна робота містить повний опис логічної та фізичної структури мережі, таблицю IP-адресації, а також техніко-економічні показники, представлені в графічній частині.

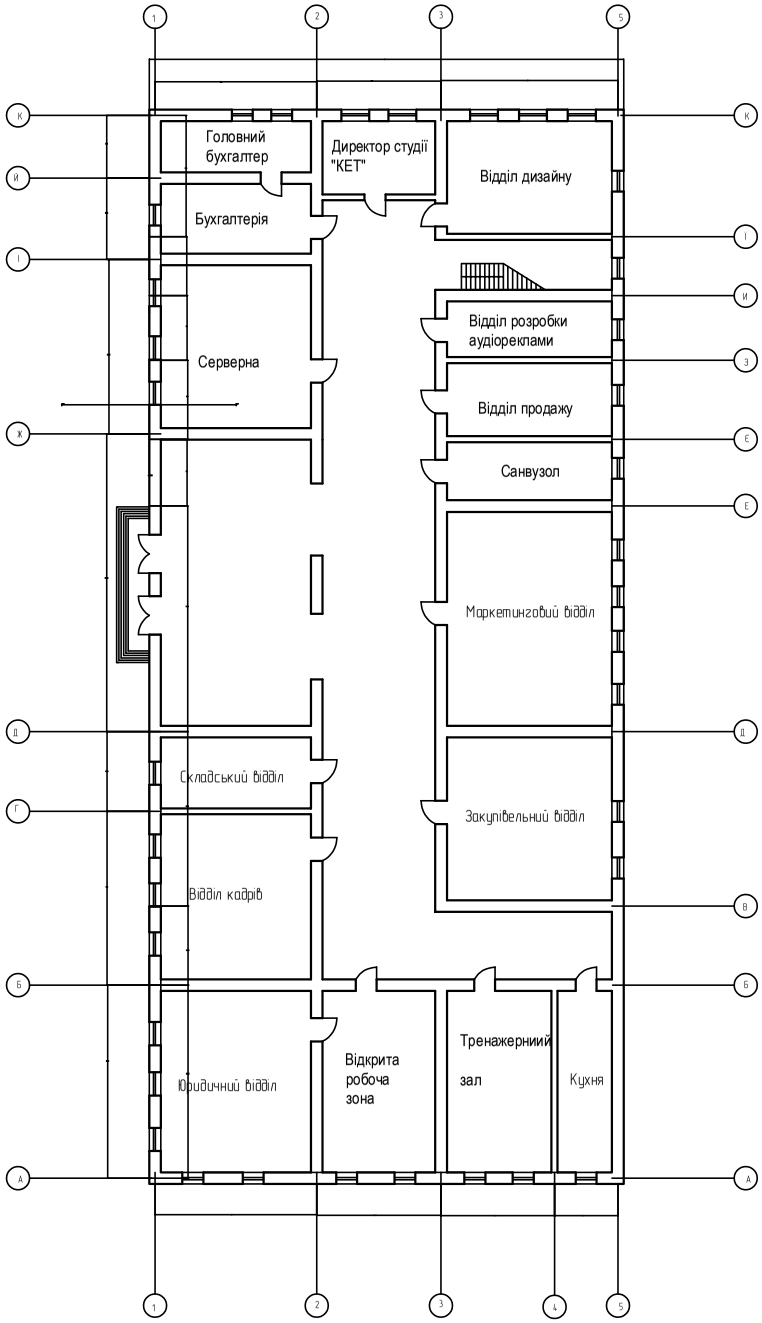
У розділі економічного обґрунтування визначено собівартість створення мережі, її економічну доцільність, термін окупності та інші ключові показники.

Останній розділ присвячено питанням охорони праці та дотримання вимог техніки безпеки при експлуатації мережного обладнання.

ПЕРЕЛІК ПОСИЛАНЬ

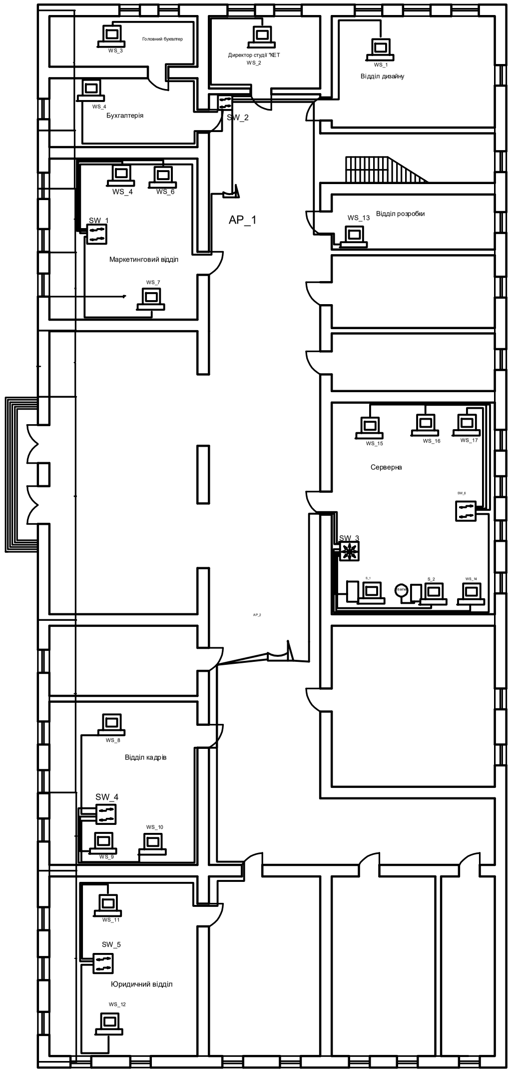
1. Антонов В.М. Сучасні комп'ютерні мережі. Підручник - К.: "МК-Прес", 2005. - 480 с.
2. Буров Є. Комп'ютерні мережі, 2-е видання. - БаК, 2004. - 584 с.: іл.
3. Блозва А.І., Матус Ю.В., Смолій В.В., Гусєв Б.С., Касаткін Д.Ю., Осипова Т.Ю., Савицька Я.А. Комп’ютерні мережі: навчальний посібник. Київ: Компрінт, 2017. 821с.
4. Горбатий І.В., Бондарєв А.В. Телекомунікаційні системи та мережі. Принципи функціонування, технології та протоколи. Львів: Львівська політехніка. 2016. 336с.
5. Додонов О. Г., Ланде Д. В., Путятін В. Г. Інформаційні потоки в глобальних комп’ютерних мережах.- К.: Наук, думка, 2009. - 295 с
6. Іртегов Д.В. Введення в мережні технології, К., 2014.
7. Комп'ютерні мережі. Принципи, технології, протоколи. Ювілейне видання. Оліфер В. Г.Оліфер Н. А.
8. Рамський Ю.С., Олексюк В.П., Балик А.В. Р21 Адміністрування комп’ютерних мереж і систем: Навч. пос. - Тернопіль: Навчальна книга – Богдан, 2010. - 196 с.
9. Шорошев В. В. Теоретичні і практичні аспекти організації і побудови архітектури захищених комп’ютерних систем. Монографія. - К.: ДУПСТ, 2011. - с.257.
10. Встановлення Ubuntu 20.04 URL:https://www.digitalocean.com/comm unity/ tutorials/initial-server-setup-with-ubuntu-20-04. (дата звернення: 13.05.2025).
11. Глобальні компютерні мережі URL:https://pidru4niki.com/74236/informatika/globalni_kompyuterni_merezhi (дата звернення: 18.04.2024).
12. Комутатори . URL:http://hotline.ua/computer/kommutatory/ . (дата звернення: 11.04.2025).

13. Мережеве устаткування компютерних мереж. URL: https://stud.com.ua/53330/informatika/merezheve_ustatkuvannya_programni_komponenti_ upravlinnya_merezheyu (дата звернення: 11.05.2025).
14. Методи тестування та діагностики компютерних мереж. URL: file:///C:/Users/Downloads/metody-testirovaniya-i-diagnostirovaniya-kompyuternyh-setey.pdf (дата звернення: 3.05.2025).
15. Охорона праці – Москальова В.М. URL: http://studentbooks.com.ua/content/view/1327/76/ . (дата звернення: 3.05.2025).
16. Організація компютерних мереж. URL:http://nickshevtsov.blogspot. com/ 2017/10/blog-post.html (дата звернення: 22.04.2025).
17. Пожежна безпека на робочому місці. URL:https://ohoronapraci.kiev.ua/article/news/pozezna-bezpeka-na-robocomu-misci (дата звернення: 23.05.2025).
18. Як налаштувати UniFi AP без контролера https://wfshop.kiev.ua/kak-nastroit-unifi-ap-bez-kontrollera
19. Налаштування програмного VLAN у RouterOS на обладнанні Mikrotik URL: https://lanmarket.ua/ua/stats/bazovye-osnovy-nastroyki-vlan-v-routeros-na-oborudovanii-mikrotik-vlan-dlya-chaynikov-segmentatsiya/. Сайт lanmarket.ua (дата звернення: 19.05.2025).
20. Перевірка та тестування швидкості домашньої мережі. URL: https://www.agsat.com.ua/info/proverka-i-testirovanie-skorosti-domashney-seti/ (дата звернення: 19.05.2025).

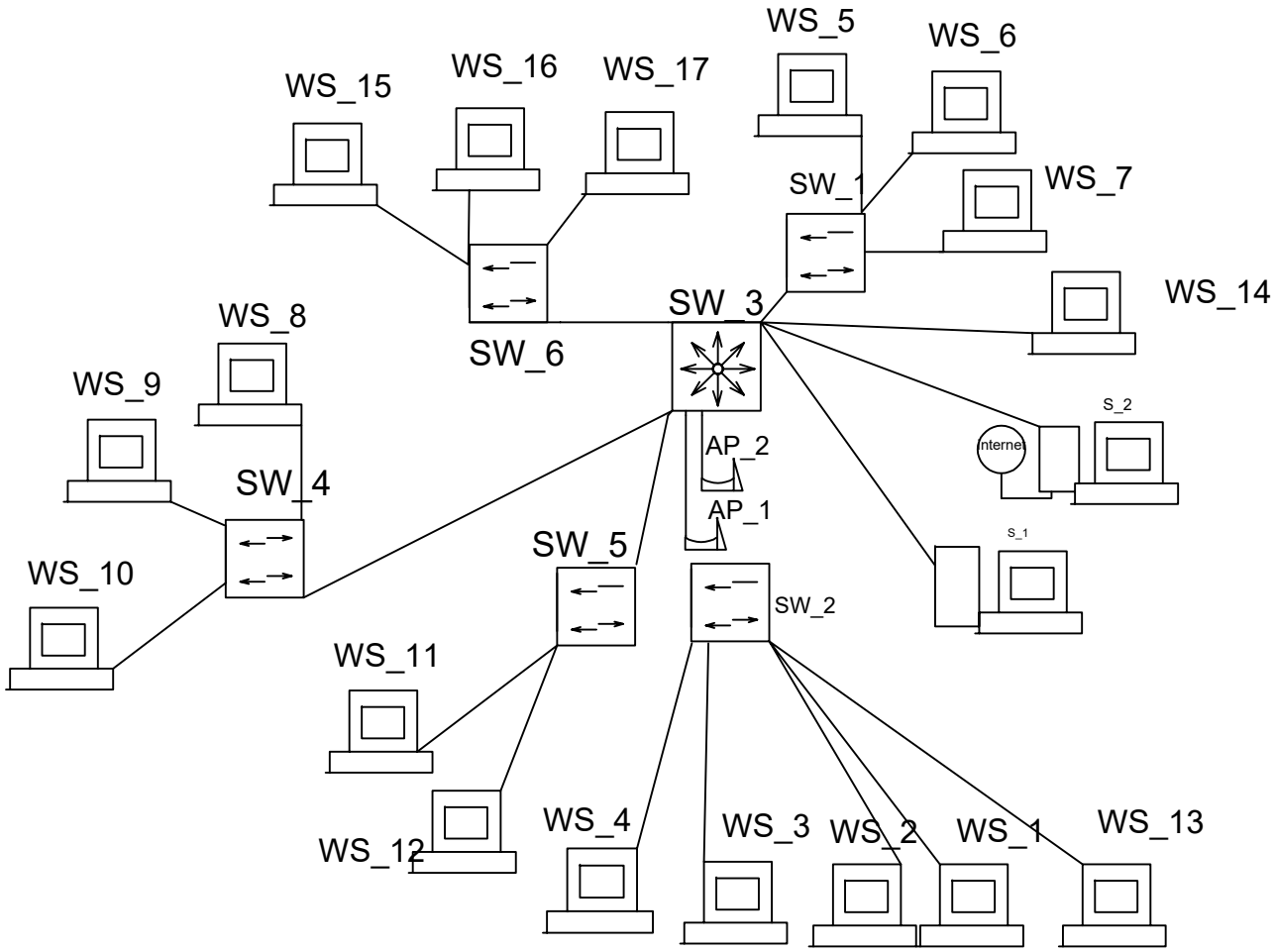


						2025.КВР.123.418.01.00.00 ПП	
Зм.	Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі підприємства "КЕТ" План приміщень	Літ.	Маса	Масшт.
Розроб.		Болюк М. А.						1:100
Керів.		Лук В. С.				Аркуш 1	Аркушів 1	
Н.контр.		Прийма В. А.				ВСП ТФК ТНТУ КІ-418, м.Тернопіль		
Рецензія								
затв.								

2025.КВР.123.418.01.00.00 ФТ



				2025.КВР.123.418.01.00.00 ФТ				
Зм. Арк.	№Докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі підприємства "КЕТ" Фізична топологія	Літ.	Маса	Масшт.	
Розроб.	Балюк М.А.				Н		1:100	
Керів.	Пиж В.С.				Аркуш 1	Аркушів 1		
Н.контр.	Приймак В.А.				ВСП ТФК ТНТУ КІ-418, м.Тернопіль			
Реценз.								
Затв.								



						2025.КВР.123.418.01.00.00 /ІТ	
Зм.	Арк.	№Докум.	Підпис	Дат.			
Розроб.		Балюк М.А.			Розробка проекту комп'ютерної мережі підприємства "Infopulse" /Логічна топологія	Літ.	Маса / Масшт.
Керів.		Пих В.С.					-
Н.контр.		Приймак В.А.				Аркуш 1	Аркушів 1
Рецензія						ВСП ТФК ТНТУ КІ-418, м.Тернопіль	
Затв.							

ТАБЛИЦЯ IP-АДРЕСАЦІЇ В МЕРЕЖІ

№ П.П	НАЗВА	IP-АДРЕСА	МАСКА	РОБОЧА ГРУПА	Vlan
1	WS_1	192.168.10.10	255.255.255.0	office	10
2	WS_2	192.168.10.11	255.255.255.0	office	10
3	WS_3	192.168.10.12	255.255.255.0	office	10
4	WS_4	192.168.10.13	255.255.255.0	office	10
5	WS_5	192.168.10.14	255.255.255.0	office	10
6	WS_6	192.168.10.15	255.255.255.0	office	10
7	WS_7	192.168.10.16	255.255.255.0	office	10
8	WS_8	192.168.10.17	255.255.255.0	office	10
9	WS_9	192.168.10.18	255.255.255.0	office	10
10	WS_10	192.168.10.19	255.255.255.0	office	10
11	WS_11	192.168.10.20	255.255.255.0	office	10
12	WS_12	192.168.10.21	255.255.255.0	office	10
13	WS_13	192.168.10.22	255.255.255.0	office	10
14	WS_14	192.168.2.10	255.255.255.0	buch	2
15	WS_15	192.168.2.11	255.255.255.0	buch	2
16	WS_16	192.168.2.12	255.255.255.0	buch	2
17	PR_1	192.168.10.50	255.255.255.0	office	10
18	S_1	192.168.10.100	255.255.255.0	office	10
19	S_2	192.168.10.101	255.255.255.0	office	10
20	A_1	192.168.10.30	255.255.255.0	office	10
21	S_3	192.168.2.100	255.255.255.0	buch	2
22	SW_3	192.168.10.250	255.255.255.0	office	10
23	AP_1	192.168.10.110	255.255.255.0	WIFI	3
24	AP_2	192.168.10.111	255.255.255.0	WIFI	3

ТАБЛИЦЯ ТЕХНІКО-ЕКОНОМІЧНИХ ПОКАЗНИКІВ

№ п\п	параметр	одиниці вимірювання	значення	№ п\п	параметр	одиниці вимірювання	значення
1	технологія мережі	–	ethernet 100\1000	10	операційна система сервера терміналів	–	windows server 2012R2
2	топологія мережі	–	гібридна	11	операційна система proxyсервера	–	Debian 10
3	середовище передачі	–	Вита пара кат. 5E	12	операційна система сервера терміналів	–	windows server 2012R2
4	кількість серверів	шт	3	13	тип доступу до Internet	–	реальна IP, вита пара
5	кількість вузлів мережі	шт	24	14	термін окупності	рік	1,3
6	марка головного комутатора	–	Cisco CBS250-16T-2G	15	плановий прибуток	грн	167274,33
7	марка 16-ти портового комутатора	–	D-Link DES-1009MP	16	собівартість	грн	298704,16
8	марка точки доступу	–	Ubiquiti UniFi U6 Lite	17	ціна	грн	465978,49
9	марка сервера	–	ARTLINE Business T61 (T61v04)	18			

						2025.КВР.123.418.1.00.02 ТБ	
Зм.	Арк.	№докум.	Підпис	Дат.	Розробка проекту комп'ютерної мережі підприємства "КЕТ" Таблиця техніко-економічних показників	Літ.	Маса	Масшт.
Розроб.		Болюк М. А.						
Керів.		Лук. В. С.					-	
Н.контр.		Приймак В. А.				Аркуш 1	Аркушів 1	
Затв.						ВСП ТФК ТНТУ КІ-418, м.Тернопіль		