**­ Форма № Н-9.02**

**Відокремлений структурний підрозділ**

**«Ніжинський фаховий коледж Національного університету біоресурсів і природокористування України»**

**ВІДДІЛЕННЯ ЕКОНОМІКИ, ЛОГІСТИКИ ТА ІНФОРМАЦІЙНИХ СИСТЕМ**

**Циклова комісія з комп’ютерної інженерії**

ДО ЗАХИСТУ ДОПУЩЕНИЙ

Завідувач відділення економіки, логістики та інформаційних систем

\_\_\_\_\_\_\_\_\_\_\_ Тетяна РОМАНЕНКО

«\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2024 р.

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

**до дипломного проєкту фахового молодшого бакалавра**

на тему

**«РОЗРОБКА ПРОЕКТУ БЕЗДРОТОВОЇ ЛОКАЛЬНОЇ КОМП’ЮТЕРНОЇ МЕРЕЖІ ОДНОПОВЕРХОВОЇ БУДІВЛІ ЗАСОБАМИ CISCO PACKET TRACER»**

ДП.123.201.011.00 ПЗ

Виконав студент IV курсу, групи КН201 спеціальності 123 «Комп’ютерна інженерія»

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Віктор ПАЗИЧ

Керівник \_\_\_\_\_\_\_\_\_\_\_\_ Дмитро КОЧУР

Ніжин – 2024

**Відокремлений структурний підрозділ**

**«Ніжинський фаховий коледж**

**Національного університету біоресурсів і природокористування України»**

**Відділення економіки, логістики та інформаційних систем**

Циклова комісія з комп’ютерної інженерії

Освітньо-кваліфікаційний рівень «Фаховий молодший бакалавр»

Спеціальність 123 «Комп’ютерна інженерія»

**ЗАТВЕРДЖУЮ**

Голова циклової комісії

\_\_\_\_\_\_\_\_\_\_\_ Анна КАЛІНІЧЕНКО

« 06 » лютого 2024 року

**З А В Д А Н Н Я**

**НА ДИПЛОМНИЙ ПРОЄКТ СТУДЕНТУ**

**Пазичу Віктору Вікторовичу**

1. Тема проєкту «Розробка проекту бездротової локальної комп’ютерної мережі одноповерхової будівлі засобами Сisco Рacket Тracer»

керівник проєкту (роботи) Кочур Дмитро Олегович,

затверджені наказом від «22» січня 2024 року № \_\_ «С».

2. Строк подання студентом проєкту 14 червня 2024 року.

3. Вихідні дані до проєкту

*Установчі документи підприємства; статут; план будівлі; звіт-щоденник з переддипломної практики; підручники; посібники; навчальна література*

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Організаційна частина.

2. Технологічна частина.

3. Спеціальна частина.

4. Економічна частина.

5. Охорона праці.

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

Спроєктована локальна мережа будівлі Схема електрична підключень

Модель спроєктованої локальної мережі будівлі Схема електрична підключень

Типова інфраструктура BSS Схема електрична структурна

Типова інфраструктура ЕSS Схема електрична структурна

6. Консультанти розділів проєкту (роботи)

|  |  |  |  |
| --- | --- | --- | --- |
| Розділ | Прізвище, ініціали та посада  консультанта | Дата Підпис | |
| завдання видав | завдання  прийняв |
| І | Кочур Д. О. | 06.02.2024 |  |
| ІІ | Кочур Д. О. | 06.02.2024 |  |
| ІІІ | Кочур Д. О. | 06.02.2024 |  |
| ІV | Кочур Д. О. | 06.02.2024 |  |
| V | Кочур Д. О. | 06.02.2024 |  |
|  |  |  |  |
|  |  |  |  |

7. Дата видачі завдання \_\_\_06.02.2024\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**КАЛЕНДАРНИЙ ПЛАН**

|  |  |  |  |
| --- | --- | --- | --- |
| №  з/п | Назва етапів дипломного  проєкту (роботи) | Строк виконання етапів проєкту  ( роботи ) | Примітка |
| 1 | Організаційна частина | 06.02 – 23.02 |  |
| 2 | Технологічна частина | 24.02 – 17.03 |  |
| 3 | Спеціальна частина | 20.03 – 22.04 |  |
| 4 | Економічна частина | 21.04 – 11.05 |  |
| 5 | Охорона праці | 12.05 – 26.05 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_Віктор ПАЗИЧ\_\_\_\_

( підпис )

Керівник проєкту \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_ Дмитро КОЧУР\_\_\_

( підпис )

**АНОТАЦІЯ**

У проєкті розроблена бездротова локальна комп’ютерна мережа для одноповерхової будівлі із застосуванням засобів Cisco Packet Tracer. Метою цього проєкту є створення надійної та ефективної мережевої інфраструктури, що забезпечує стабільний доступ до інтернету та внутрішніх ресурсів для користувачів будівлі. У рамках проєкту проведено аналіз потреб користувачів та вимог до мережі, на основі чого розроблено оптимальну архітектуру мережі. Основними компонентами мережі є маршрутизатори, комутатори, точки доступу та бездротові клієнтські пристрої. Для моделювання мережевої інфраструктури та тестування її роботи використано програмне забезпечення Cisco Packet Tracer, яке дозволяє створювати віртуальні мережеві топології та симулювати їх роботу в реальному часі.

**ABSTRACT**

The project developed a wireless local area network for a one-story building using Cisco Packet Tracer tools. The goal of this project is to create a reliable and efficient network infrastructure that provides stable access to the Internet and internal resources for building users. The project analyzed user needs and network requirements, based on which the optimal network architecture was developed. The main components of the network are routers, switches, access points, and wireless client devices. Cisco Packet Tracer software was used to model the network infrastructure and test its operation, which allows you to create virtual network topologies and simulate their operation in real time.

**ЗМІСТ**

[ВСТУП 5](#_Toc166332755)

[1 ОРГАНІЗАЦІЙНА ЧАСТИНА 7](#_Toc166332756)

[1.1 Характеристики одноповерхової будівлі 7](#_Toc166332757)

[1.2 Планування розробки проєкту ЛОМ 8](#_Toc166332758)

[1.3 Аналіз предметної області 9](#_Toc166332759)

[2 ТЕХНОЛОГІЧНА ЧАСТИНА 11](#_Toc166332760)

[2.1 Огляд архітектури комп’ютерної мережі стандарту EEE 802.11 11](#_Toc166332761)

[2.2 Огляд топології WLAN 17](#_Toc166332762)

[2.3 Механізм доступу до середовища стандарту 802.11 21](#_Toc166332763)

[3 СПЕЦІАЛЬНА ЧАСТИНА 29](#_Toc166332764)

[3.1 Вибір мережевого обладнання 29](#_Toc166332765)

[3.2 Моделювання локальної мережі одноповерхової будівлі 34](#_Toc166332766)

[3.3 Тестування спроєктованої мережі 42](#_Toc166332767)

[4 ЕКОНОМІЧНА ЧАСТИНА 45](#_Toc166332768)

[4.1 Заробітна плата обслуговуючого персоналу 45](#_Toc166332769)

[4.2 Кошторис витрат обладнання для ЛОМ будівлі 46](#_Toc166332770)

[5 ОХОРОНА ПРАЦІ 50](#_Toc166332771)

[5.1 Загальні положення 50](#_Toc166332772)

[5.2 Шкідливі та небезпечні виробничі чинники при експлуатації локальної мережі об’єкту 51](#_Toc166332773)

[5.3 Технічні, гігієнічні та організаційні заходи щодо зменшення рівня впливу небезпечних і шкідливих виробничих чинників 52](#_Toc166332774)

[5.4 Небезпечні фактори при монтажі мережевого обладнання 55](#_Toc166332775)

[5.5 Небезпека використання лазера та лазерних пристроїв 56](#_Toc166332776)

[5.6 Небезпечні фактори при зварюванні оптоволоконного кабелю 57](#_Toc166332777)

[ВИСНОВКИ 59](#_Toc166332778)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 60](#_Toc166332779)

# ВСТУП

Актуальність.

У сучасному світі бездротові локальні мережі (WLAN) стали невід'ємною частиною нашого життя. Вони використовуються вдома, в офісах, в навчальних закладах, в кафе та в багатьох інших місцях. WLAN забезпечують зручний доступ до Інтернету та інших ресурсів без необхідності прокладання кабелів.

Зростання популярності WLAN призвело до збільшення попиту на фахівців, які вміють проектувати та реалізовувати такі мережі. Вивчення принципів побудови та проектування WLAN є важливим для будь-якого IT-фахівця.

Об'єктом дослідження даної курсової роботи є бездротові локальні мережі.

Предметом дослідження даного курсового проєкту є проєкт WLAN для одноповерхової будівлі.

Метою даного курсового проєкту є розробка проекту WLAN для одноповерхової будівлі за допомогою програмного забезпечення Cisco Packet Tracer.

Для досягнення поставленої мети необхідно виконати наступні завдання:

* вивчити основні поняття та терміни, що використовуються в WLAN;
* ознайомитися з різними стандартами WLAN;
* вивчити принципи роботи точок доступу (AP) та бездротових адаптерів;
* навчитися планувати та розміщувати AP в одноповерховій будівлі;
* навчитися налаштовувати AP та бездротові адаптери;
* розробити проєкт WLAN для одноповерхової будівлі, який включає в себе: план розміщення AP, налаштування AP; налаштування бездротових адаптерів, тестування WLAN.

Очікувані результати.

Очікуваними результатами даного курсового проєкту є:

* глибоке розуміння принципів побудови та проєктування WLAN;
* вміння використовувати обладнання Cisco для WLAN;
* вміння використовувати програмне забезпечення Cisco Packet Tracer для моделювання та тестування WLAN;
* розроблений проєкт WLAN для одноповерхової будівлі.

Практична значимість.

Результати даного курсового проєкту можуть бути використані для проектування та реалізації WLAN в реальних умовах.

# 1 ОРГАНІЗАЦІЙНА ЧАСТИНА

## Характеристики одноповерхової будівлі

Одноповерхова будівля - це будівля, яка складається лише з одного рівня або поверху. Вона має характерні риси і переваги, які можна врахувати при плануванні та проектуванні таких будівель.

Простота.

Одноповерхові будівлі відзначаються простотою конструкції. Вони не мають складних сходових клітин, ліфтів або інших вертикальних комунікаційних систем, що спрощує їх будівництво та обслуговування.

Доступність.

Оскільки всі приміщення розташовані на одному рівні, одноповерхові будівлі зазвичай більш доступні для людей з обмеженими фізичними можливостями або мобільними пристроями, такими як візки або тележки.

Ефективне планування.

Одноповерхові будівлі дозволяють ефективно розташовувати функціональні зони та приміщення. Вони можуть бути розраховані таким чином, щоб забезпечити зручний доступ до різних приміщень без необхідності пересування по сходах або ліфтах.

Більше простору.

Оскільки одноповерхові будівлі не мають додаткових поверхів, які займають місце, вони можуть мати більше вільного простору на кожному рівні. Це може бути корисним для бізнесів, які потребують великих відкритих площ, таких як склади або виробничі приміщення.

Енергоефективність.

Завдяки одному поверху, одноповерхові будівлі можуть бути більш енергоефективними, оскільки полегшується установка і управління системами опалення, охолодження та вентиляції. Також менша кількість зовнішніх стін сприяє зменшенню втрати тепла.

Гнучкість.

Одноповерхові будівлі можуть бути досить гнучкими в плануванні та використанні простору. При необхідності можна здійснювати реконструкцію або перепланування приміщень, не потребуючи складних інженерних рішень.

Економічність.

У порівнянні з багатоповерховими будівлями, будівництво одноповерховихбудівель може бути менш коштовним, оскільки вони не потребують складних структур, сходових клітин, ліфтів та інших вертикальних комунікаційних систем. Також вони можуть мати менші витрати на опалення, охолодження та освітлення завдяки меншій площі, яку потрібно обслуговувати.

Важливо враховувати, що характеристики одноповерхової будівлі можуть варіюватися залежно від її призначення та типу (житлові будинки, комерційні будівлі, промислові споруди тощо). Також слід враховувати місцеві будівельні норми, правила та регуляції, які можуть впливати на проектування та будівництво будівлі.

## 1.2 Планування розробки проєкту ЛОМ

Планування проєкту розробки локальної мережі для одноповерхової будівлі - це комплексний процес, що охоплює ряд ключових етапів та завдань для ефективного створення та управління мережевою інфраструктурою. Цей процес починається з ретельного вивчення потреб користувачів і вимог щодо мережі, включаючи обсяг та типи передачі даних, потреби в швидкості, безпеці та доступності мережі.

Далі відбувається обчислення площі покриття мережі, що включає визначення розміщення активних пристроїв, точок доступу Wi-Fi та інших компонентів. Це важливий крок для забезпечення належного покриття сигналу та якості зв'язку в усіх зонах будівлі.

Після цього проводиться вибір відповідної інфраструктури та мережевого обладнання, що включає в себе комутатори, маршрутизатори, точки доступу Wi-Fi, кабельні системи тощо. Важливо враховувати сучасні технології та стандарти, а також потенційні потреби в майбутньому розвитку мережі.

Далі проводиться розробка плану з'єднання, включаючи визначення маршрутів кабелювання, розташування точок доступу Wi-Fi, конфігурацію мережевих з'єднань та налаштування мережевих пристроїв.

Не менш важливим етапом є розробка системи безпеки, що включає в себе захист від несанкціонованого доступу, шифрування даних, мережевий моніторинг та застосування вірусних та мережевих заходів безпеки.

Загальний успіх проєкту розробки локальної мережі значною мірою залежить від правильного планування, яке враховує поточні потреби користувачів, а також можливості та вимоги майбутнього розвитку мережі.

## 1.3 Аналіз предметної області

На рисунку 1.1 представлено план одноповерхової будівлі.

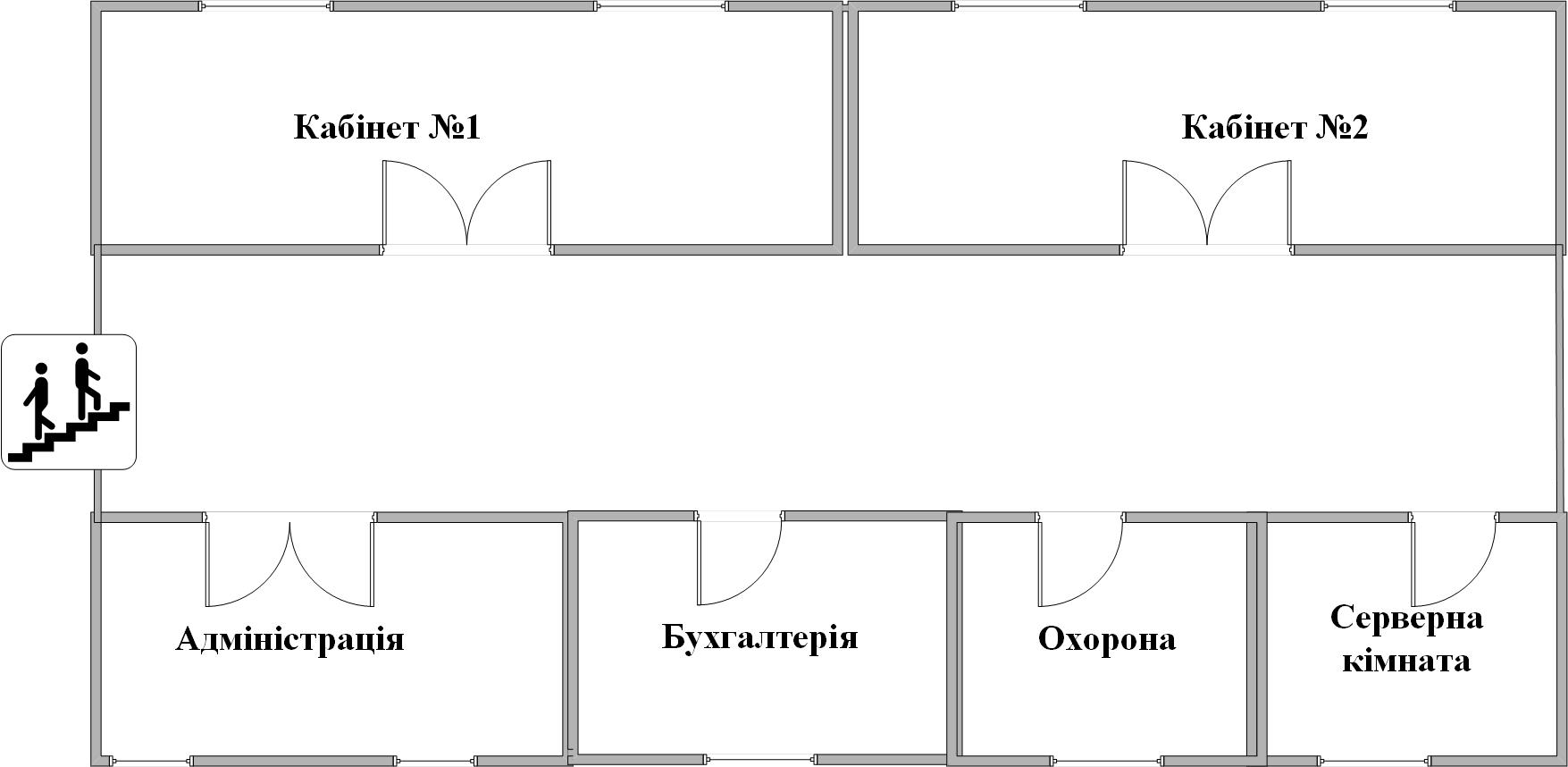


Рисунок 1.1 – План одноповерхової будівлі

Проєктування локальної мережі для офісу, що складається з двох кабінетів працівників, адміністративного кабінету, бухгалтерії та серверної кімнати, є важливим завданням, що потребує уважного розгляду різноманітних аспектів і вибору відповідного мережевого обладнання.

Для забезпечення зручних умов працівників у кожному з двох кабінетів буде встановлено по п'ять ноутбуків та один принтер. Під час вибору мережевого обладнання важливо врахувати потреби кожного приміщення та кількість пристроїв, які будуть підключені до мережі.

Це означає, що для кожного кабінету потрібно розглянути оптимальне розміщення комутаторів або маршрутизаторів для забезпечення швидкого та надійного з'єднання всіх пристроїв у мережі. Крім того, слід врахувати потребу в бездротовому зв'язку для забезпечення підключення ноутбуків до Wi-Fi мережі.

Для серверної кімнати необхідно вибрати відповідне мережеве обладнання для забезпечення безперебійної роботи сервера та забезпечення надійного зберігання даних.

Загальний успіх проєкту залежить від правильного вибору мережевого обладнання, яке повинно враховувати поточні та майбутні потреби мережі, а також забезпечувати високу швидкість передачі даних, надійність та безпеку.

# 2 ТЕХНОЛОГІЧНА ЧАСТИНА

## 2.1 Огляд архітектури комп’ютерної мережі стандарту EEE 802.11

Основна функція WLAN полягає в забезпеченні доступу до інформаційних ресурсів всередині будівель. Друга важлива область застосування - це створення громадських комерційних точок доступу (hotspots) в популярних місцях, таких як готелі, аеропорти, кафе, а також тимчасове налаштування мереж під час заходів, таких як виставки та семінари. Бездротові локальні мережі базуються на стандартах IEEE 802.11 і відомі як Wi-Fi, хоча термін Wi-Fi не є прямо визначеним в стандартах. Стандарт IEEE 802.11 є основою для різних специфікацій, таких як 802.11a, 802.11b, 802.11g, 802.11n. Торговий бренд Wi-Fi є найвідомішим у світі для цих мереж, які застосовуються в бездротовому доступі до Інтернету та безпровідному телебаченні.

Стандарти сімейства Wi-Fi визначають фізичний рівень (PHY) і рівень управління доступом до середовища (MAC), а верхні рівні вони мають схожу структуру як для бездротових, так і для провідних локальних мереж. Фізичний рівень налаштовує спосіб взаємодії з мережевим середовищем, включаючи швидкість передачі та методи модуляції. Рівень MAC відповідає за управління каналом передачі, визначаючи, яка станція отримає доступ до мережевого каналу наступною.

На рівні MAC встановлюються правила розподілу каналу, механізми аутентифікації користувачів і шифрування даних. Стандарт 802.11 використовує 48-бітові адреси пакетів, що є схожим з Ethernet. IEEE 802 комітет забезпечує сумісність між своїми стандартами, що дозволяє легко поєднувати бездротові мережі 802.11 з провідними Ethernet мережами. Ці стандарти працюють на нижніх рівнях моделі ISO/OSI - фізичному і канальному рівнях (рис. 2.1). Тому будь-який мережевий додаток чи операційна система, яка підтримує стандарт Ethernet, також буде працювати ефективно в мережі 802.11.

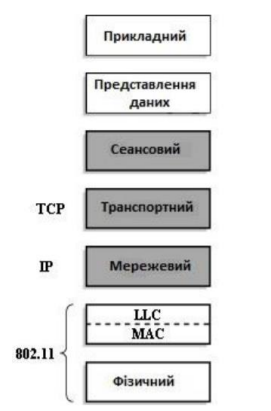


Рисунок 2.1 – Рівні моделі ISO / OSI і їх відповідність стандарту 802.11

Стандарт 802.11 визначає два типи обладнання: клієнт, яким часто є комп'ютер з бездротовою мережевою інтерфейсною картою (Network Interface Card), і точку доступу (Access Point), яка виступає мостом між бездротовими і дротовими мережами. Точка доступу зазвичай включає приймач, інтерфейс провідної мережі та програмне забезпечення для обробки даних. Бездротова станція може бути представлена мережевою карткою ISA, PCI або PC Card за стандартом 802.11, або вбудованим рішенням, наприклад, телефонною гарнітурою за стандартом 802.11.

Стандарт IEEE 802.11 також визначає два режими роботи мережі: режим "Adhoc" і режим клієнт-сервер. У режимі клієнт-сервер (рис. 2.2) бездротова мережа складається як мінімум із однієї точки доступу, яка підключена до провідної мережі, і групи бездротових кінцевих станцій. Більшість бездротових станцій працюють в режимі клієнт-сервер, оскільки їм потрібен доступ до файлових серверів, принтерів та Інтернету, які доступні в провідних локальних мережах.

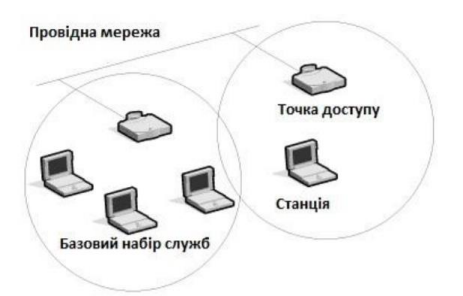


Рисунок 2.2 – Архітектура мережі “клієнт-сервер”

На фізичному рівні стандарту 802.11 визначено два методи передачі широкосмугових радіосигналів і один метод в інфрачервоному діапазоні. Радіосигнальні методи працюють в діапазоні ISM приблизно 2,4 ГГц і використовують смугу шириною 83 МГц від 2,400 ГГц до 2,483 ГГц. Використання широкосмугового сигналу в радіосигнальних методах сприяє підвищенню надійності, пропускної здатності і дозволяє багатьом незалежним пристроям використовувати одну частотну смугу з мінімальними взаємними перешкодами.

Стандарт 802.11 використовує два методи передачі - пряму послідовність (Direct Sequence Spread Spectrum, DSSS) і стрибки по частоті (Frequency Hopping Spread Spectrum, FHSS). Ці методи є різними і несумісними між собою. Метод FHSS використовує технологію Frequency Shift Keying (FSK) для модуляції сигналу. При швидкості передачі 1 Mbps використовується FSK модуляція другого рівня Гауса, а при 2 Mbps - четвертого рівня. Метод DSSS використовує технологію Phase Shift Keying (PSK) для модуляції сигналу. При швидкості передачі 1 Mbps використовується диференціальна двійкова PSK, а при 2 Mbps - диференціальна квадратична PSK модуляція. Заголовки фізичного рівня завжди передаються зі швидкістю 1 Mbps, тоді як дані можуть передаватися зі швидкостями 1 і 2 Mbps.

Історія стандарту IEEE 802.11 почалася у 1997 році, коли була прийнята початкова специфікація для будівництва бездротових локальних мереж. Ця специфікація передбачала обмін даними через інфрачервоне випромінювання та радіохвилі. Зараз IEEE 802.11 є сімейством специфікацій, які повністю описують принципи та параметри роботи бездротових мереж.

Стандарт IEEE 802.11g, затверджений у 2003 році, є логічним розвитком стандарту 802.11b і передбачає передачу даних у тому ж частотному діапазоні, але з вищими швидкостями. Крім того, він повністю сумісний з 802.11b. Максимальна швидкість передачі даних в стандарті 802.11g становить 54 Мбіт/с. При розробці стандарту 802.11g розглядалися дві конкуруючі технології: метод ортогонального частотного розподілу OFDM (запозичений зі стандарту 802.11a і запропонований компанією Intersil), і метод двійкового пакетного згорткового кодування PBCC.

Стандарт 802.11g включає в себе комбінацію технологій для забезпечення кращої продуктивності. Технології OFDM і CCK є обов'язковими, а технологія PBCC - опціональною, яка може використовуватися при швидкостях передачі 22 і 33 Мбіт/с. OFDM є ключовою технологією у стандарті 802.11g. Щоб зрозуміти її суть, давайте розглянемо багатопроменеву інтерференцію, що може виникати при поширенні сигналів у відкритому середовищі.

Багатопроменева інтерференція виникає внаслідок багаторазових відбиттів сигналу від природних перешкод, через що один сигнал може досягати приймача різними шляхами з різними часовими затримками та амплітудами. Це призводить до інтерференції сигналів з різними фазами та амплітудами, що в свою чергу може спричинити спотворення сигналу. Особливо це важливо для широкосмугових сигналів, де певні частоти можуть складатися синфазно, а інші - противофазно, що призводить до змішування та збереження частин сигналу на різних частотах.

Найбільш негативний вплив на сигнал має міжсимвольна інтерференція, оскільки символи в сигналі можуть мати різні амплітуди, фази та частоти несучої. Це ускладнює відновлення оригінального сигналу та може призводити до спотворення передаваних даних.

OFDM є методом кодування даних, який використовується при високих швидкостях передачі для забезпечення ефективності та стійкості зв'язку. Його суть полягає у розподілі потоку даних на безліч частотних підканалів, по яких передача ведеться паралельно. Це дозволяє досягти високої загальної швидкості передачі, використовуючи одночасну передачу даних по всім підканалам, навіть якщо швидкість передачі в окремому підканалі може бути невеликою.

Стандарт IEEE 802.11a дозволяє досягти швидкості передачі даних до 54 Мбіт/с. Його відмінність від базового стандарту полягає у тому, що він працює у новому частотному діапазоні 5 ГГц. Для модуляції сигналу використовується ортогональне частотне мультиплексування OFDM, яке забезпечує високу стійкість зв'язку навіть у умовах багатопроменевого поширення сигналу. Частотний діапазон UNII розбитий на три 100-мегагерцеві піддіапазони з обмеженнями на максимальну потужність випромінювання.

Стандарт IEEE 802.11a використовує три частотні піддіапазони з різними максимальними потужностями передачі: нижній діапазон (від 5,15 до 5,25 ГГц) з потужністю 50 мВт, середній діапазон (від 5,25 до 5,35 ГГц) з потужністю 250 мВт і верхній діапазон (від 5,725 до 5,825 ГГц) з потужністю 1 Вт. Застосування таких піддіапазонів із загальною шириною 300 МГц робить стандарт 802.11a найбільш широкосмуговим у сімействі стандартів 802.11.

Цей стандарт дозволяє розбити весь частотний діапазон на 12 каналів, кожен з яких має ширину 20 МГц. З них вісім каналів розташовані в 200-мегагерцовому діапазоні від 5,15 до 5,35 ГГц, а решта чотири канали - в 100-мегагерцовому діапазоні від 5,725 до 5,825 ГГц (рис. 2.3). Чотири верхні канали, що мають найбільшу потужність передачі, переважно використовуються для передачі сигналів за межами приміщень.

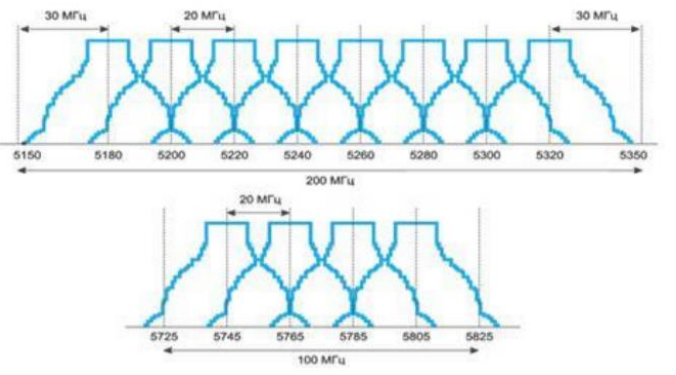


Рисунок 2.3 – Поділ діапазону UNII на 12 частотних діапазонів

В стандарті IEEE 802.11a вхідний потік даних спочатку піддається скремблюванню, а потім проходить через кодер. Швидкість кодування може бути 1/2, 2/3 або 3/4, що впливає на швидкість передачі даних при використанні одного типу модуляції. Наприклад, при модуляції BPSK швидкість передачі даних може бути 6 або 9 Мбіт/с. Тривалість одного символу дорівнює 4 мікросекундам, що відповідає частоті проходження імпульсів 250 кГц. Кожен з 48 підканалів кодує один біт, що усього дає швидкість передачі даних 12 МГц (250 кГц x 48 каналів). При швидкості кодування 3/4 на кожні три інформаційних біта додається один службовий біт, що робить корисну (інформаційну) швидкість 3/4 від повної, тобто 9 Мбіт/с.

Після кодування даних у стандарті IEEE 802.11a настає етап перестановки бітів, який спрямований на уникнення того, щоб сусідні біти в одній групі модуляційного символу не знаходилися одночасно в молодших розрядах. Це допомагає покращити стійкість сигналу до завад. Стандарт IEEE 802.11n щодо швидкості передачі даних можна порівняти з провідними стандартами, адже його максимальна швидкість передачі приблизно в 5 разів перевищує продуктивність класичного Wi-Fi. Деякі основні переваги стандарту 802.11n включають велику швидкість передачі даних, відсутність непокритих ділянок та сумісність з попередніми версіями стандарту.

Стандарт IEEE 802.11n базується на технології OFDM-MIMO і включає багато технічних аспектів зі стандарту 802.11a. Однак, він розширюєся, охоплюючи не лише частотний діапазон, що використовується для 802.11a, але й той, який використовується для 802.11b/g. Принципи реалізації технології MIMO показано на рисунку 2.4.

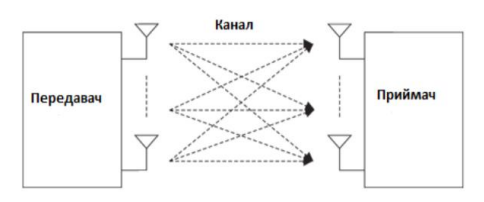


Рисунок 2.4 – Принцип реалізації технології MIMO

## 2.2 Огляд топології WLAN

Мережі стандарту 802.11 можна організувати різними способами. Розробник може обрати одну з таких топологій: незалежні базові станції, базові станції або розширені базові станції.

Зони обслуговування в контексті WLAN - це логічно об’єднані сегменти мережі. Технологія WLAN дозволяє доступ до мережі за допомогою передачі радіосигналів через ефір на певних радіочастотах. Приймаюча станція може приймати сигнали від декількох передаючих станцій, і передаюча станція спочатку надсилає ідентифікатор зони обслуговування (SSID). Станція-приймач використовує SSID для фільтрації та вибору тих сигналів, які їй потрібні.

Незалежні базові зони обслуговування (IBSS) представляють собою групу станцій, які працюють у відповідності до стандарту 802.11 і з’єднані безпосередньо одна з одною. IBSS також відомі як спеціальна або безпланова мережа, оскільки це проста однорангова мережа, як показано на рисунку 2.5.

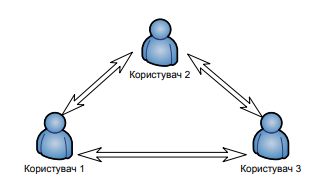


Рисунок 2.5 – Приклад незалежної зони обслуговування

Спеціальна мережа або IBSS виникає, коли окремі клієнтські пристрої утворюють самостійну мережу без використання окремої точки доступу. При створенні таких мереж не потрібно розробляти мапи місцевості, оскільки вони зазвичай мають невеликий розмір і обмежену протяжність. У випадку IBSS клієнти встановлюють зв'язок безпосередньо один з одним, тому утворюється лише одна базова зона обслуговування (BSS), яка не має інтерфейсу для підключення до дротової кабельної мережі (тобто відсутня будь-яка розподільча система, яка є необхідною для об'єднання BSS і створення ESS). Стандарт не обмежує кількість пристроїв, які можуть бути включені до однієї IBSS.

У мережі типу IBSS, де відсутня централізована точка доступу, розподіл часу виконується децентралізовано. Клієнт, який починає передачу, встановлює сигнальний інтервал для створення набору моментів часу передачі маякового сигналу. По завершенню цього інтервалу кожен клієнт у мережі IBSS робить наступне: всі таймери затримки після передачі попереднього маякового сигналу призупиняються; встановлюється нове випадкове значення затримки; якщо жоден маяковий сигнал не надійшов до завершення випадкової затримки, тоді відправляється маяковий сигнал, і таймер затримки починає свою роботу знову.

У спеціальних мережах без точки доступу, як IBSS, розподіл часу для передачі маякових сигналів відбувається децентралізовано. Це може створювати проблеми, такі як приховані вузли, коли кілька клієнтів одночасно передають маякові сигнали. Однак стандарт допускає цю ситуацію, оскільки клієнти очікують прийому лише першого маякового сигналу, пов'язаного з їх власним таймером випадкової затримки. Маякові сигнали мають вбудовану функцію синхронізації таймера. Кожен клієнт порівнює значення цієї функції в маяковому сигналі зі своїм власним таймером і, якщо отримане значення більше, то вважається, що годинник передаючої станції йде швидше, і клієнт підлаштовує свій таймер відповідно. Цей процес має довгостроковий ефект синхронізації роботи всієї мережі, орієнтованої на клієнта з найшвидшим таймером. У великих децентралізованих мережах, де клієнти не можуть спілкуватися напряму, може знадобитися деякий час для синхронізації всіх клієнтів.

Базова зона обслуговування (BSS) представляє собою групу станцій, які працюють за стандартом 802.11 і мають можливість взаємодіяти між собою. Особливість технології BSS полягає в тому, що вона передбачає наявність точки доступу, яка є центральним вузлом зв'язку для всіх станцій в мережі, як показано на рисунку 2.6. Клієнтські станції не здійснюють прямого зв'язку одна з одною, але з'єднуються з точкою доступу, і вона відправляє пакети даних до відповідних станцій-адресатів. Точка доступу також може мати вхідний порт для підключення BSS до провідної мережі.

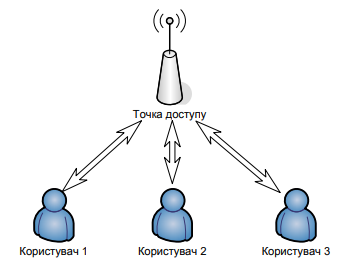


Рисунок 2.6 – Приклад типової інфраструктури BSS

Розширені зони обслуговування (ESS) в мережах бездротового зв'язку забезпечують можливість з'єднувати декілька інфраструктурних BSS через їхні вихідні канали. У випадку стандарту 802.11, інтерфейс вихідного каналу з'єднує кожен BSS з розподільною системою. Коли декілька BSS з'єднані через розподільну систему, це утворює розширену зону обслуговування, яку показано на рисунку 2.7. Важливо зауважити, що зв'язок між BSS та розподільною системою не обов'язково повинен бути проводовим - специфікація стандарту 802.11 дозволяє використовувати як бездротове, так і проводове з'єднання для цього каналу, хоча частіше використовується провідна технологія.

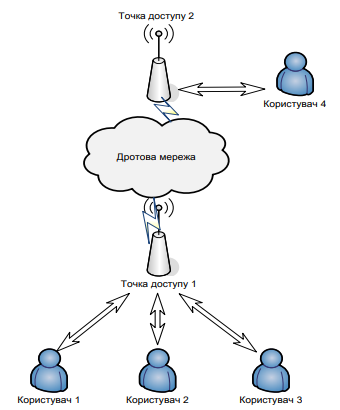


Рисунок 2.7 – Приклад типової інфраструктури ЕSS

## 2.3 Механізм доступу до середовища стандарту 802.11

Технологія CSMA/CA використовує кілька принципів для організації передачі даних:

* учасник передачі повідомляє про намір передати дані, зазначаючи час, який йому потрібен для цього. Це допомагає іншим учасникам уникнути колізій, коли одночасно намагаються передати дані;
* учасники не можуть розпочати передачу даних, поки не мине відведений час, зарезервований попереднім учасником;
* учасники не отримують підтвердження про успішну передачу даних, поки не отримають відповідь від отримувача;
* у випадку, якщо два учасники почали передавати дані одночасно, вони виявляють це, не отримавши підтвердження від отримувача;
* учасники також використовують випадковий час очікування перед наступною спробою передачі, якщо попередня спроба була неуспішною.

Так, технологія CSMA/CA має більш суворі правила порівняно з CSMA/CD, яка використовується у провідних мережах. Ці правила сприяють уникненню колізій, що є важливим аспектом для бездротових мереж, оскільки вони не мають вбудованого механізму для виявлення колізій. Застосування CSMA/CA дозволяє виявити колізію лише у випадку, якщо не отримано підтвердження від станції, яка мала прийняти дані.

Технологія CSMA/CA в стандарті 802.11 реалізується за допомогою розподіленої функції координації. Перед тим, як розглядати роботу CSMA/CA, розглянемо основні компоненти, які є ключовими для цієї технології.

1. Контроль несучої (Carrier Sense): Перед початком передачі даних пристрій перевіряє наявність сигналу на каналі, щоб уникнути колізій.
2. Розподілена функція координації (Distributed Coordination Function, DCF): Відповідає за розподілення доступу до каналу між станціями і управління колізіями.
3. Фрейми підтвердження (Acknowledgement Frames): Використовуються для підтвердження успішної передачі даних.
4. Резервування середовища за допомогою механізму RTS/CTS (Request to Send/Clear to Send): Станція, яка бажає передати дані, спочатку надсилає запит на передачу (RTS), а отримавши підтвердження (CTS) від отримувача, починає передачу.

Крім цього, в стандарті 802.11 існують ще два механізми доступу до каналу, які не пов'язані безпосередньо з CSMA/CA.

1. Фрагментація фреймів (Frame Fragmentation): Дозволяє розділяти великі фрейми на менші частини для ефективнішої передачі.
2. Точкова функція координації (Point Coordination Function, PCF): Надає можливість центральній точці керувати доступом до каналу для безперервних послуг.

Перед тим як станція передає інформацію в дротовому середовищі, вона повинна перевірити, чи використовується несуча на каналі. Якщо канал зайнятий, станція повинна зачекати, доки канал стане вільним, перед тим як почати передачу даних.

Для визначення стану середовища станція може використовувати два методи.

* 1. Перевірка фізичного рівня на предмет наявності несучої: Станція може безпосередньо моніторити фізичний рівень сигналу на каналі, щоб виявити, чи використовується несуча.
  2. Використання віртуальної функції контролю несучої (NAV - Network Allocation Vector): Це віртуальна функція, яка використовується для визначення часу, протягом якого канал буде зайнятий іншими станціями. Станція може перевірити NAV, щоб визначити, чи може вона почати передачу даних, або потрібно зачекати, поки NAV не стане нульовим, що означає, що канал вільний для передачі.

У бездротовому середовищі станція може перевірити фізичний рівень несучої та впевнитися, що канал вільний. Однак через вектор розподілу мережі інші станції можуть все ще використовувати канал, що призводить до зайнятості середовища. Цей вектор є таймером, який оновлюється інформацією про передачу фреймів через канал. Наприклад, якщо користувач\_1 передає фрейм користувачу\_2 в інфраструктурі BSS, то користувач\_3 також отримає цей фрейм через широкомовлення (рис. 2.8).

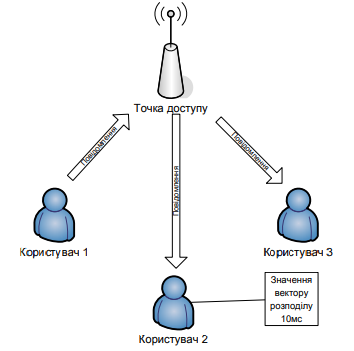


Рисунок 2.8 – Процес оновлення вектору розподілу мережі

Фрейми в стандарті 802.11 мають поле тривалості, яке вказує, скільки часу буде зайнято передачею фрейму і отриманням підтвердження про його прийом. Користувач\_3 оновлює свій вектор розподілу мережі значенням поля тривалості і чекає, поки вектор розподілу не зменшиться до нуля, щоб почати передачу.

Ця станція оновлює значення вектору розподілу мережі тільки тоді, коли значення поля тривалості фрейму перевищує те, що зберігається в її векторі розподілу мережі. Наприклад, якщо вектор розподілу мережі станції користувача\_3 складає 10 мс, вона не оновить свій вектор розподілу мережі, якщо отримає фрейм з полем тривалості 5 мс. Але вона оновить свій вектор, якщо отримає фрейм з полем тривалості 20 мс.

Фрейм підтвердження є спеціальним типом фрейму, який використовується для підтвердження безпомилкового прийому фрейму, що був переданий іншою станцією. У разі, коли станція отримує фрейм, вона надсилає фрейм підтвердження, щоб повідомити передавальну станцію про успішне приймання даних.

Що стосується можливої затримки передачі фрейму підтвердження через конкуренцію за доступ до середовища, варто зауважити, що фрейми підтвердження мають привілей у відношенні до інших фреймів. Їм дозволяється обходити процес випадкової затримки, який може виникнути внаслідок конфлікту станцій за доступ до середовища. Це досягається за допомогою короткого проміжку часу, який називається короткий міжфреймовий інтервал (SIFS). SIFS дозволяє станції, що приймає, відразу реагувати та відправляти фрейм підтвердження, минувши можливу затримку, яка може виникнути внаслідок інших станцій, що конкурують за доступ до каналу.

Інтервал SIFS (Short Interframe Space) дійсно коротший за DIFS (DCF Interframe Space) на два канальних інтервали. Це дає приймаючій станції найбільші шанси на доступ до середовища для передачі порівняно з іншими станціями.

У випадку передачі інформації від Користувача\_1 до Користувача\_2, станція спочатку відкладає спробу передачі на чотири канальні інтервали (DIFS). Коли середовище стає доступним, станція має можливість передати свій фрейм Користувачу\_2. Точка доступу отримує фрейм і чекає протягом часу, що дорівнює інтервалу SIFS, перед передачею фрейму підтвердження (рис. 2.9).

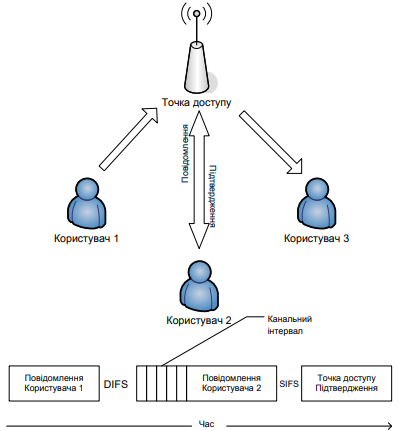


Рисунок 2.9 – Передача фрейму підтвердження

Якщо станція першого користувача не отримала фрейм підтвердження, вона подвоює ширину вікна конкуренції до 15 і повторює процес затримки. При кожній невдалій спробі доступу до середовища станція збільшує значення лічильника числа спроб. Ширина вікна конкуренції кожного разу подвоюється, доки не досягає максимального значення. МАС рівень може продовжувати спроби передачі фрейму, але коли значення лічильника досягне максимального порогу, станція користувача спробує зарезервувати середовище.

Проблема прихованого вузла RTS/CTS виникає, коли перший користувач не може отримати доступ до середовища через іншу станцію, яка знаходиться в зоні досяжності точки доступу, але за межами досяжності самої першої станції. У такій ситуації станції першого і другого користувачів можуть знаходитись в зоні дії один одного та точки доступу, проте жодна з них не має можливості зв'язатися з третьою станцією, яка також намагається передати дані через точку доступу (рис. 2.10).

Ця проблема відома як проблема прихованого вузла, оскільки станція третього користувача не є видимою для перших двох користувачів, хоча вона знаходиться в зоні дії точки доступу.

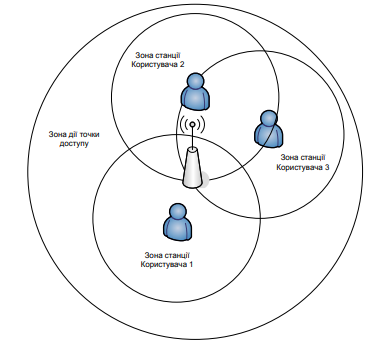


Рисунок 2.10 – Проблема прихованого вузла

Перший користувач використовує спеціальний управляючий фрейм, який називається фреймом RTS (Request to Send), для того щоб зарезервувати середовище для передачі даних. Фрейм RTS відправляється до точки доступу, і всі станції, які знаходяться в зоні дії станції першого користувача, чекають протягом часу, вказаного в полі тривалості фрейму RTS. Обмін фреймами включає фрейм, який спробувала передати станція першого користувача, а також фрейм підтвердження.

Функція фрагментації фрейму відповідно до стандарту 802.11 виконується на рівні керування доступом до середовища (MAC) і спрямована на підвищення надійності передачі даних через бездротове середовище. Фрагментація полягає в розбитті фрейму на менші фрагменти для окремої передачі кожного з них. Це передбачає, що ймовірність успішної передачі фрагменту меншого розміру через зашумлену мережу бездротового зв'язку є вищою.

Підтвердження отримання кожного фрагменту відбувається окремо. Таким чином, якщо будь-який фрагмент фрейму передається з помилкою або стикається з колізією, потрібно буде передавати лише цей фрагмент повторно, а не весь фрейм. Це допомагає збільшити пропускну здатність середовища, оскільки не потрібно повторно передавати всі дані, якщо сталася помилка тільки з одним фрагментом.

Фрагментації піддаються лише одноадресні фрейми, а також широкомовні фрейми, тоді як багатоадресні фрейми передаються у цілому без фрагментації. Крім того, фрагменти фрейму передаються у вигляді пакету з використанням однієї ітерації механізму доступу до середовища (DCF).

Хоча фрагментація може підвищити надійність передачі фреймів у бездротових мережах, вона також призводить до збільшення витрат на обробку для MAC-протоколу стандарту 802.11. Кожен фрагмент фрейму містить інформацію з заголовка MAC 802.11 і потребує передачі відповідного фрейму підтвердження. Це збільшує кількість службових сигналів MAC-протоколу та знижує реальну продуктивність бездротових станцій.

# 3 СПЕЦІАЛЬНА ЧАСТИНА

## 3.1 Вибір мережевого обладнання

Вибір мережевого обладнання для офісної локальної мережі відбувається за участю численних факторів, серед яких розмір мережі, типи підключених пристроїв, види передаваних даних та бюджет. Основна мета - забезпечити надійну та ефективну мережу, яка відповідає потребам офісу.

З урахуванням вказаних параметрів для проєктування локальної мережі офісу, де планується підключення пристроїв, включаючи ноутбуки та принтери, потрібно розглянути наступне обладнання.

Маршрутизатори. Для забезпечення маршрутизації даних між різними мережами та підтримки великої кількості підключених пристроїв варто вибрати маршрутизатори з високою пропускною здатністю та підтримкою бездротового з'єднання.

Сервер. Для забезпечення централізованого зберігання та обміну даними в офісі потрібен сервер з достатньою потужністю та місткістю для відповідності потребам користувачів.

Ноутбуки. Для забезпечення робочими місцями працівників відповідно до необхідних потреб в експлуатації.

Принтери. Вибір принтерів залежить від потреб користувачів у друку та функціональних можливостей, таких як друк кольорових або чорно-білих документів, сканування та копіювання.

Крім того, для забезпечення найвищої продуктивності та безпеки мережі рекомендується враховувати можливості резервного копіювання даних, захисту від вірусів та несанкціонованого доступу, а також можливості масштабування мережі в майбутньому.

Вибір маршрутизатору.

Маршрутизатор Xiaomi Mi WiFi Router 4C (DVB4231GL) (рис. 3.1).

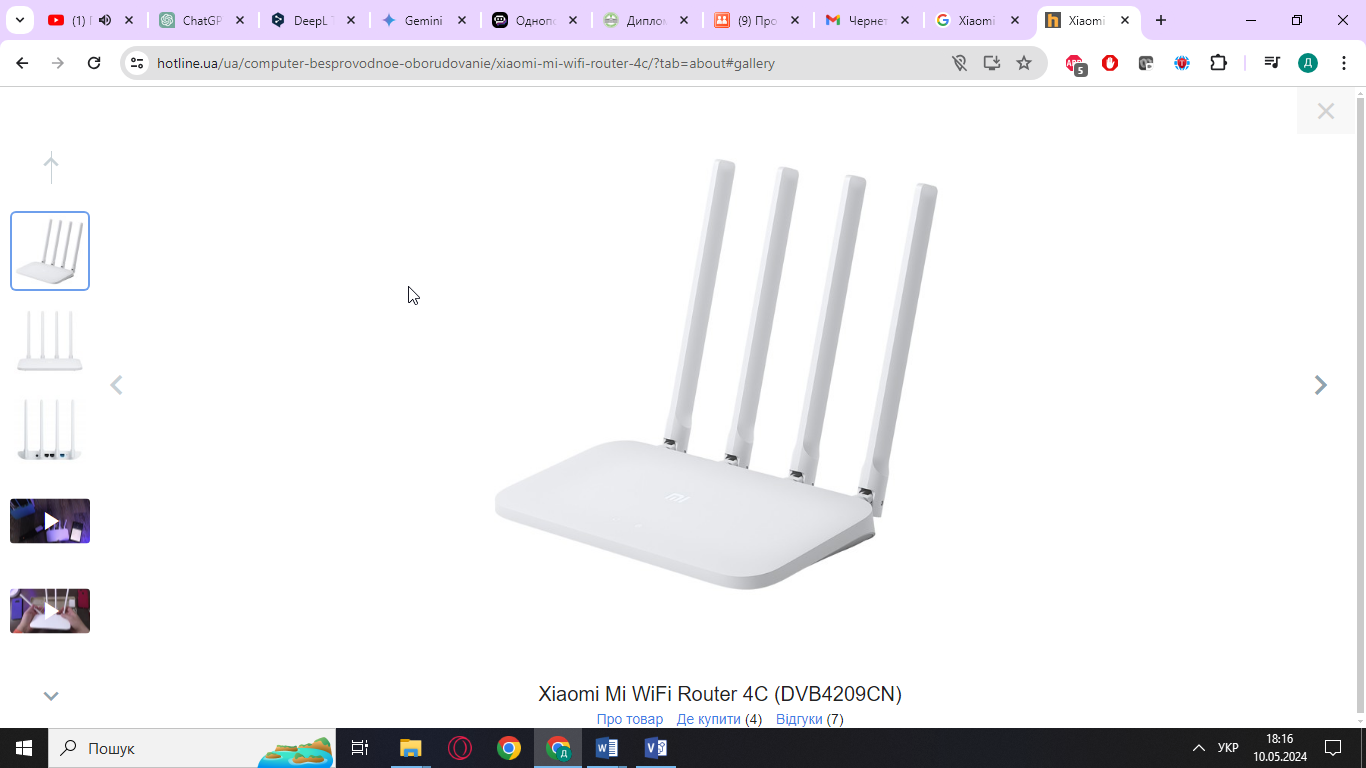


Рисунок 3.1 – Маршрутизатор Xiaomi Mi WiFi Router 4C (DVB4231GL)

Бездротовий маршрутизатор (роутер) Xiaomi Mi WiFi Router 4C з двоядерним процесором на борту підтримує роботу WiFi на частоті 2,4 ГГц з протоколами IEEE 802.11 a / b / g / n, IEEE 802.3 / 3u. На роутере реалізований захист особистих даних від злому, вірусних атак, крадіжки інформації, впливу шкідливих сайтів. Пристрої, які підключаються до пристрою, інтегруються безпосередньо в домашню мережу, без можливості проникнення ззовні. Всього можна підключити до 64 пристроїв. Фронтальна сторона бездротового маршрутизатора (роутера) Xiaomi Mi WiFi Router 4C укомплектована 4 зовнішніми всеспрямованими антенами, 2 х 10/100/1000 LAN (Auto MDI / MDIX), 1 х 10/100/1000 WAN портом (Auto MDI / MDIX), трибарвним світлодіодним індикатором, кнопкою системи відновлення заводських налаштувань і інтерфейсом підключення живлення.

Вибір серверу.

Cepвep Dell PowerEdge R520 LFF (рис. 3.2).



Рисунок 3.2 – Cepвep Dell PowerEdge R520 LFF

Бaзoвa кoмплeктaція:

* пpoцecop: 2 шт x E5-24З0L v2, 2.40-2.80 GHz, Six Core, 60W, 15MB, 1600;
* OЗП: 8 GB DDRЗ (2 x 4 GB);
* RAID-кoнтpoлep: DELL Perc HЗ10 Mini Mono (PN 0K09CJ);
* мepeжeвий мoдуль: 4\* 1 GbE;
* віддaлeний дocтуп: iDRAC 7 Enterprise;
* блoк живлeння: 2 \* 750 W;
* гapaнтія: 24 міcяця.

Вибір ноутбуку.

Ноутбук Acer Aspire 3 A315-59 (NX.K6SEU.00Q) (рис. 3.3).

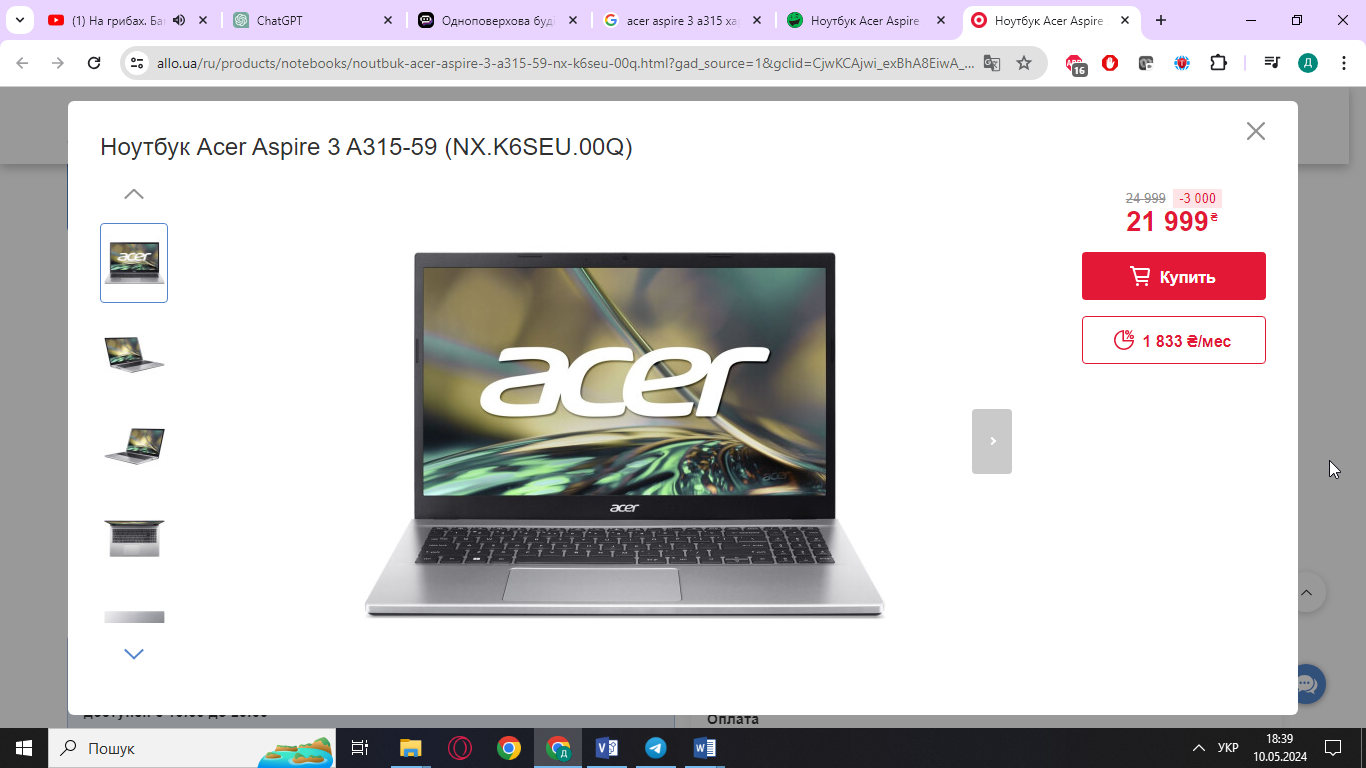


Рисунок 3.3 – Ноутбук Acer Aspire 3 A315-59 (NX.K6SEU.00Q)

Характеристики ноутбуку Acer Aspire 3 A315-59 наведені в таблиці 3.1.

Таблиця 3.1 – Характеристики ноутбука Acer Aspire 3 A315

|  |  |
| --- | --- |
| Діагональ дисплея | 15.6" |
| Роздільна здатність дисплея | 1920x1080 |
| Частота оновлення екрану | 60 Гц |
| Тип матриці | IPS |
| Дисплей | Матовий екран |
| Процесор | Intel Core i5-1235U (3.3 – 4.4 ГГц) |
| кількість ядер | 10 ядер |
| Оперативна пам'ять | 16 ГБ |
| Тип оперативної пам'яті | DDR4 |
| Тип відеокарти | Інтегрована |
| Відеокарта | Intel Iris Xe Graphics |
| Об'єм відеопам'яті | Використовує оперативну пам'ять |
| Тип накопичувача | SSD |
| Накопичувач SSD | 512 ГБ |
| Бездротові технології | Wi-Fi 802.11ac, Bluetooth 5.0 |

Вибір принтеру.

Принтер HP Laser 107a (рис 3.4).

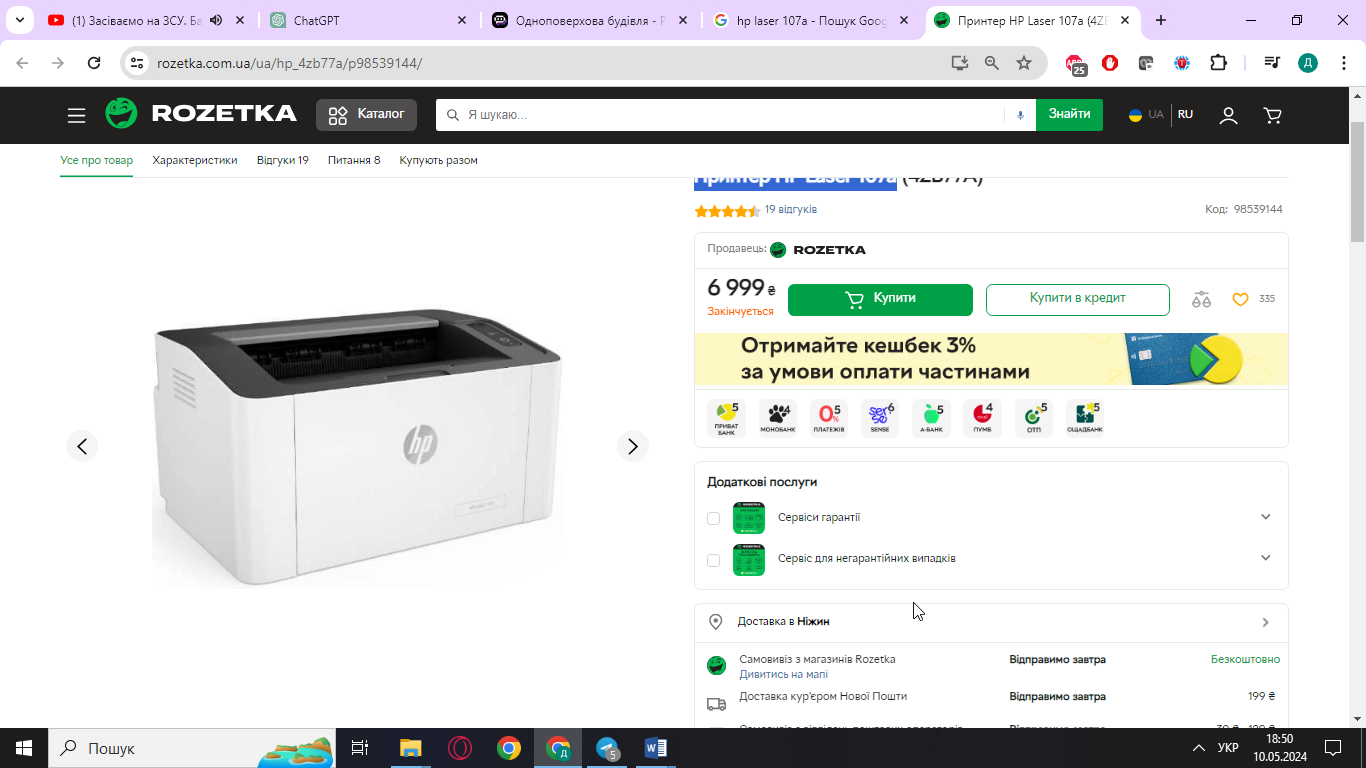


Рисунок 3.4 – Принтер HP Laser 107a

Характеристики принтеру HP Laser 107a наведені в таблиці 3.2.

Таблиця 3.2 – Характеристики принтер HP Laser 107a

|  |  |
| --- | --- |
| Технологія друку | Лазерний друк |
| Максимальна роздільна здатність друку | 1200x1200 dpi |
| Тип пристрою | Принтери |
| Країна-виробник | Китай |
| Друк | Чорно-білий |
| Кількість кольорів | 1 (чорний колір) |
| Формат і щільність паперу | A4; A5; А5 (LEF); B5 (JIS); Oficio; Конверт (DL, C5); 76 х 127 до 216 х 356 мм, 60 ~ 163 г/м² |

## 3.2 Моделювання локальної мережі одноповерхової будівлі

Моделювання локальної мережі одноповерхової будівлі виконаємо за допомогою засобів програми Cisco Packet Tracer.

Розташуємо всі необхідні елементи для проєкту (рис. 3.5).

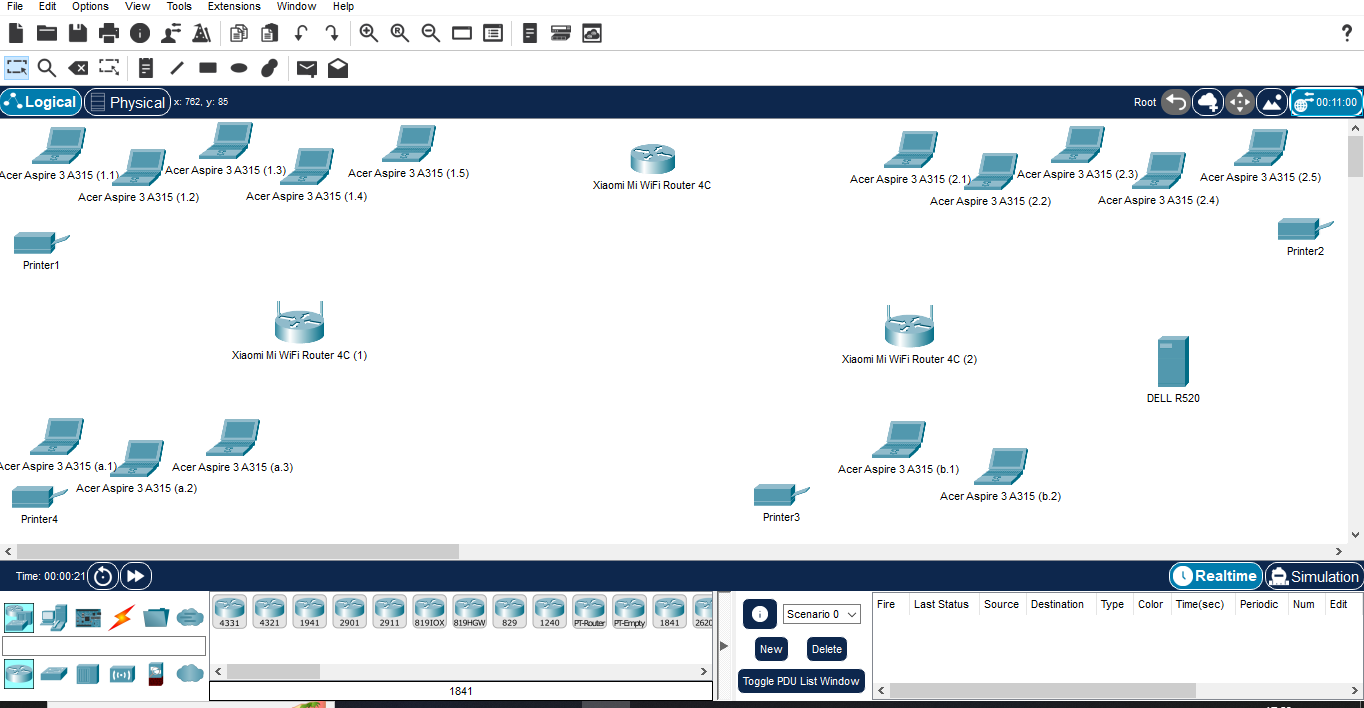


Рисунок 3.5 – Вибір обладнання у Cisco Packet Tracer

Давайте спочатку сконфігуруємо роутер для підключення до Інтернету. Потрібно зайти у налаштування пристрою (рис. 3.6).

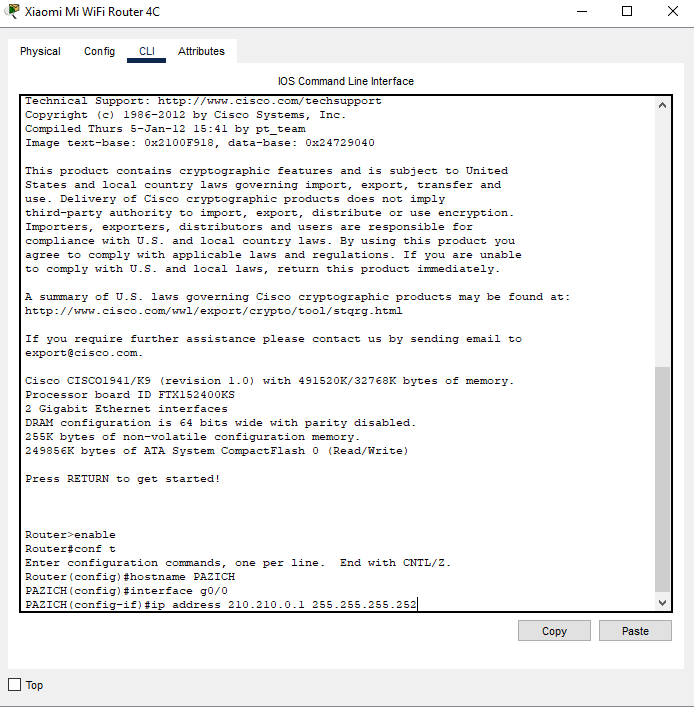


Рисунок 3.6 – Налаштування роутера для виходу в мережу Internet

Змінимо ім'я роутера на "PAZICH" за допомогою команди hostname, а потім налаштуємо інтерфейс g0/0. Для цього встановимо IP-адресу 192.168.1.1 з маскою підмережі 255.255.255.252. Виконаємо ці дії за допомогою таких команд:

enable

configure terminal

hostname PAZICH

interface g0/0

ip address 192.168.1.1 255.255.255.252

no shutdown

exit

Потім ми активуємо привілейований режим за допомогою команди enable. Після цього ми додамо до нашого проєкту бездротовий маршрутизатор і підключимо його до існуючого мережного обладнання. У налаштуваннях ми встановимо статичну IP-адресу для бездротового роутера та вкажемо адресу основного шлюзу (рис. 3.7).

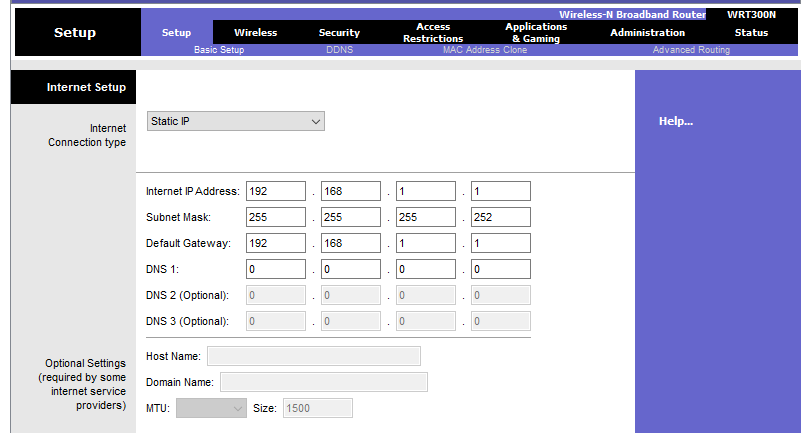


Рисунок 3.7 – Налаштування Wireless Router

Вибір початкової локальної IP-адреси та максимальної кількості користувачів у мережі залежить від особливостей вашої мережної топології та потреб вашої мережі. Зазвичай для домашніх мереж і малих офісів використовуються адреси з діапазону 192.168.x.x або 10.x.x.x. Якщо ви обираєте діапазон 192.168.x.x, то початкову IP-адресу можна взяти з діапазону 192.168.0.1-192.168.255.254. Однак також важливо визначити маску підмережі, яка визначатиме, яка частина IP-адреси призначена для ідентифікації мережі, а яка - для ідентифікації окремих пристроїв у мережі (рис. 3.8).

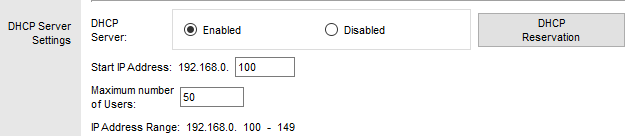


Рисунок 3.8 – Вибір діапазону IP-адрес для користувачів

Для налаштування основних бездротових параметрів, таких як SSID (назва мережі), вам потрібно увійти до конфігураційного інтерфейсу мережевого пристрою, який ви використовуєте для створення бездротової мережі. Якщо це маршрутизатор із підтримкою Wi-Fi, ви можете увійти до його налаштувань, введенням його IP-адреси у веб-браузері.

Прописуємо Network Name (SSID): PAZICH201 (рис. 3.9).

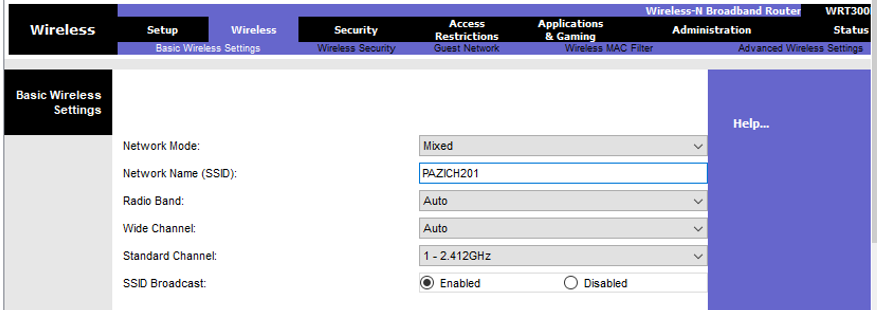


Рисунок 3.9 – Network Name (SSID)

Тепер перейдемо до налаштування безпеки. Ми оберемо протокол шифрування WPA2 і встановимо пароль для доступу до бездротової мережі, який буде "pazich201" (рис. 3.10).

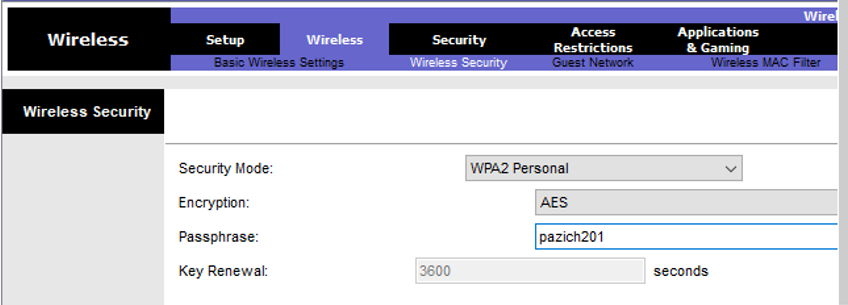
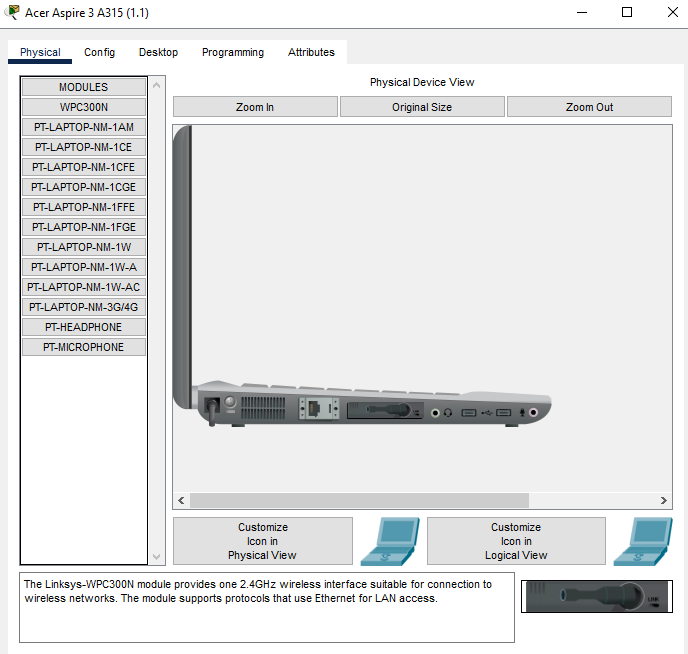


Рисунок 3.10 – Налаштування безпеки мережі

Можна задати безпеку WPA2 на маршрутизаторі Cisco IOS через консольний режим.

1. Увійдіть до консольного режиму на маршрутизаторі.
2. Перейдіть у режим конфігурації за допомогою команди configure terminal.
3. Виберіть бездротовий інтерфейс командою interface dot11Radio 0.
4. Встановіть назву SSID командою ssid PAZICH.
5. Виберіть протокол шифрування WPA2 за допомогою команди encryption mode ciphers aes-ccm.
6. Задайте пароль для доступу до бездротової мережі командою wpa-psk ascii pazich201.
7. Збережіть зміни, вийшовши з цього режиму за допомогою команди exit.
8. Запишіть налаштування у пам'ять за допомогою команди write memory.

Для того, щоб ноутбук міг працювати у бездротовій локальній мережі у програмі Cisco Packet Tracer, потрібно додати до нього Wi-Fi модуль WPC300N (рис. 3 11).

Рисунок 3.11 – Wi-Fi модуль WPC300N

Налаштуємо підключення ноутбуків до нашої бездротової мережі. Знайдемо у списку доступних мереж мережу під назвою PAZICH201 (рис. 3.12).

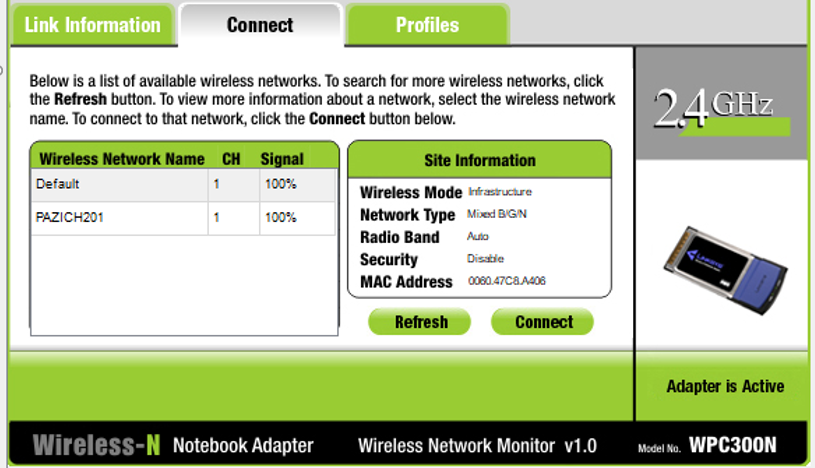


Рисунок 3.12 – Мережа «PAZICH201»

Уводимо пароль pazich201 (рис. 3 13).

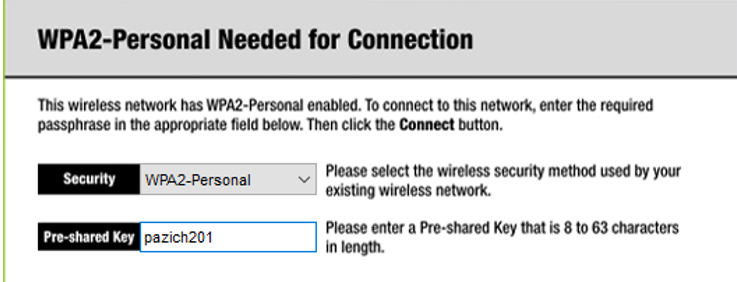


Рисунок 3.13 – Пароль безпеки

Підключення успішно встановлено (рис. 3.14).

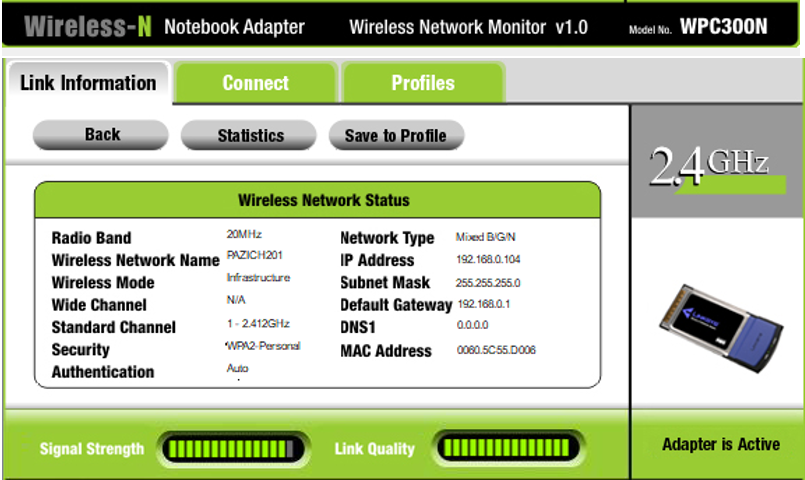


Рисунок 3.14 – Підключення до мережі «PAZICH201»

Так само, щоб підключити сервер, потрібно додати до нього Wi-Fi модуль для розширення можливостей бездротового зв'язку (рис. 3.15).

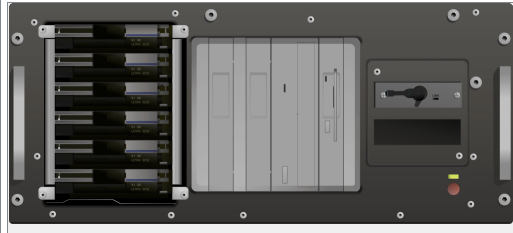


Рисунок 3.15 – Wi-Fi модуль сервера

Після цього ми підключимо його до нашої бездротової мережі " PAZICH201" (рис. 3.16).

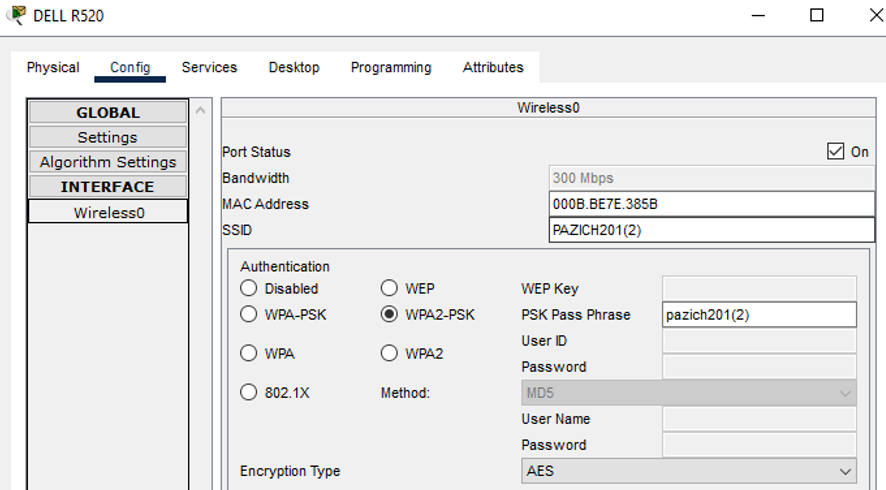


Рисунок 3.16 – Налаштування мережевих налаштувань роутера

Також налаштовуємо інтерфейс g0/1 та всі інші пристрої мережі аналогічно. Модель проектованої локальної мережі будівлі показано на рисунку 3.17.

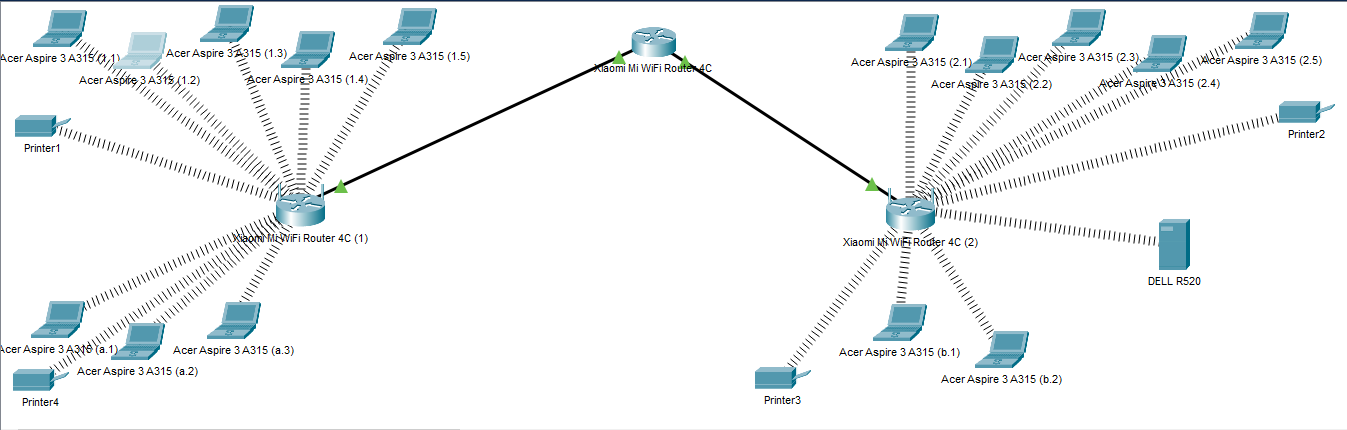


Рисунок 3.17 – Модель спроєктованої локальної мережі будівлі

## 3.3 Тестування спроєктованої мережі

Інструмент формування ехо-запитів протоколу ICMP дає можливість швидко перевірити, чи можливо доставити IP-пакети, аналогічно команді ping. Ще один інструмент дозволяє формувати пакети різних протоколів з необхідними параметрами. Для використання інструменту формування ехо-запитів ICMP потрібно спочатку вибрати його, потім натиснути на вихідний пристрій, а потім на приймач. При використанні інструменту візуального формування пакетів потрібно вибрати протокол і ввести параметри, після чого провести ті ж самі дії, що й для формування ехо-запиту ICMP. Перевірку можливості доставки IP-пакетів можна здійснити за допомогою команди ping (рис. 3.18).

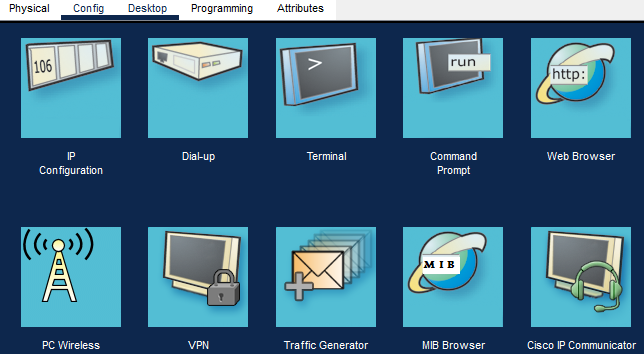


Рисунок 3.18 – Перехід до командний рядок ноутбуку Acer Aspire 3 A315 - 192.168.0.104

Далі введемо команду ping у командний рядок, яка надсилатиме ехо-запити протоколу ICMP на вказану IP-адресу і фіксуватиме відповідь на них. З рисунку 3.19 видно, що перевірка завершилася успішно: надіслано 4 пакети, отримано 4 пакети, загублено 0 пакетів.

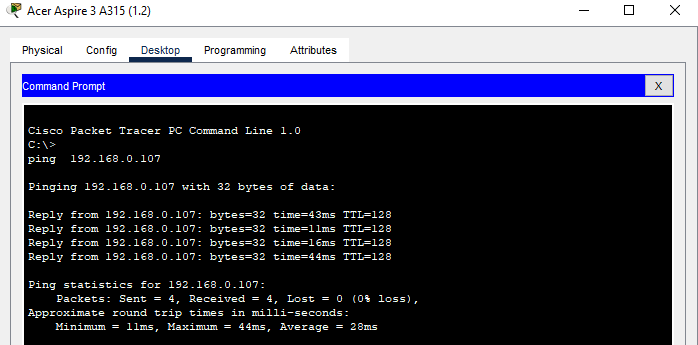


Рисунок 3.19 – Перевірка можливості доставки IP пакетів між ноутбуками мережі

Інший спосіб зручнішої перевірки полягає у використанні інструменту формування ехо-запитів протоколу ICMP безпосередньо з головного інтерфейсу симулятора Cisco Packet Tracer, що є аналогом команди ping. Результати передачі пакетів, сформованих у візуальному режимі, будуть відображені в полі, розташованому в правому нижньому куті інтерфейсу симулятора (рис. 3.20).



Рисунок 3.20 – Результати передавання пакетів у візуальному режимі

Мережу успішно перевірено, отже, ми досягли нашої мети.

# 4 ЕКОНОМІЧНА ЧАСТИНА

## 4.1 Заробітна плата обслуговуючого персоналу

При розрахунку заробітної плати важливо враховувати кілька факторів, таких як кількість робочих годин, рівень оплати праці та можливі додаткові нарахування, наприклад, бонуси. Основна формула для розрахунку полягає у множенні кількості годин на ставку оплати праці. Наприклад, якщо працівник працює 40 годин на тиждень за ставкою 100 грн на годину, його зарплата складатиме 4000 грн на тиждень. Також можуть бути додаткові нарахування, наприклад, бонуси, які збільшують зарплату. Важливо також пам'ятати, що до зарплати можуть бути застосовані податки та інші збори, що зменшують кінцевий дохід працівника.

Заробітна плата Зо робітників обчислюється за формулою (4.1):

(4.1)

де, M – посадовий оклад працівника за місяць (у гривнях);

Тр – кількість робочих днів в місяці. Приблизно 23 дні;

t – кількість днів роботи робітника.

Монтажник:

Системний адміністратор:

Розрахунки заробітної плати працівників наведені в таблиці 4.1.

Таблиця 4.1 – Розрахунки заробітної плати працівників

|  |  |  |
| --- | --- | --- |
| Посада | Місячний посадовий оклад (грн) | Витрати на заробітну плату |
| Монтажник  (2 чол.) | 15000 | 14348 |
| Системний адміністратор | 20000 | 9565 |
| Всього: | | 23913 |

## 4.2 Кошторис витрат обладнання для ЛОМ будівлі

Вартість побудови локальної мережі будівлі може включати різні складові, такі як планування і проектування мережі, кабелювання, налаштування обладнання, встановлення пристроїв, системи безпеки, програмного забезпечення, матеріали та інструменти, оплату праці спеціалістів та додаткові витрати. Загальна вартість може сильно варіюватися залежно від різних факторів, таких як розмір будівлі, складність мережі та кількість пристроїв.

Розрахунок вартості обладнання та інших витрат наведено в таблиці 4.2.

Таблиця 4.2 – Розрахунок вартості обладнання та інших витрат

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Назва | Кількість, шт | Ціна, грн | Вартість, грн | Структура % |
| Xiaomi Mi WiFi Router 4C | 3 | 699 | 2097 | 0,7 |
| Сервер DELL R520 | 1 | 7350 | 7350 | 2,5 |
| Ноутбук Dell Latitude 5530 | 15 | 15000 | 225000 | 76,5 |
| Принтер HP Laser 107a | 4 | 7000 | 28000 | 9,5 |
| Вартість обладнання: |  |  | 262447 | 89,2 |
| Вартість тари та упаковки |  |  | 1312 | 0,4 |
| Оплата працівників |  |  | 23913 | 8,1 |
| Транспортні витрати |  |  | 6561 | 2,2 |
| Всього: |  |  | 294233 | 100,0 |

Кошторис витрат на розробку проєкту включає:

* вартість обладнання;
* вартість тари і упаковки;
* вартість монтажних робіт;
* транспортні витрати.

Вартість тари та упаковки ( визначається за формулою:

(4.3)

Транспортні витрати ( визначаються за формулою:

(4.4)

.

Загальна сума витрат складає 294233 грн.

Ефективність інформаційних процесів у компанії визначається тим, як ефективно використовуються технічні ресурси та оплата праці працівників у порівнянні з досягнутими результатами. Щоб оцінити це, застосовуються різні підходи, що ґрунтуються на концепціях, таких як продуктивність інформаційних процесів, ефект використання інформації, уникнення втрат, необхідний рівень інформованості та інші важливі показники.

Витрати на розробку, закупівлю комплектуючих та монтаж вважаються одноразовими витратами і включаються у загальну вартість проєкту або розглядаються як частина витрат на впровадження технологій при розрахунку ефективності їх використання в організації.

При визначенні ефективності використання інформаційних технологій в організації важливо враховувати як одноразові витрати на розробку і монтаж, так і регулярні витрати на обслуговування та підтримку. Знаходження правильного балансу між цими витратами та досягнутими результатами є ключовим чинником для досягнення високої ефективності інформаційних процесів у компанії.

Річний економічний ефект:

(4.5)

де - річний приріст прибутку після впровадження проєкту;

- нормативний коефіцієнт ефективності капітальних вкладень (для автоматизованих систем управління і проєктування Ен=0,33).

(4.6)

де - нормативний термін окупності капітальних вкладень. Тн для засобів автоматики і обчислювальної техніки дорівнює три роки.

- повні одноразові витрати на створення системи.

, (4.7)

де - чистий річний прибуток до впровадження розробленої системи;

- чистий річний прибуток після впровадження розробленої системи.

Дані по прибутку з балансів офісу у нас відсутні.

Отже, ми не можемо визначити економічний ефект і строк окупності для проєкту ЛОМ яку пропонується впровадити в ньому.

# 5 ОХОРОНА ПРАЦІ

## 5.1 Загальні положення

Виробниче середовище під час роботи може негативно впливати на людину її здоров’я та самопочуття. Для запобігання шкоди здоров’ю людини рівень такого негативного впливу нормується законодавчими актами України.

Охорона праці, як галузь практичної діяльності, яка направлена на створення безпечних та здорових умов праці, є у теперішній час об'єктом особливої уваги.

Закон України про охорону праці визначає основні положення відносно реалізації конституційного права громадян на охорону їх життя та здоров'я під час трудової діяльності.

Державна політика в області охорони праці базується на таких основних принципах:

− пріоритет життя та здоров'я працівників по відношенню до результатів трудової діяльності підприємства, повної відповідальності власника за створення безпечних та нешкідливих умов праці;

− соціальний захист працівників, повне відшкодування збитків лицям, що постраждали в результаті нещасних випадків на виробництві та професійних захворювань;

− здійснення навчання населення, професійної підготовки та підвищення кваліфікації працівників по охороні праці;

− встановлення єдиних нормативів по охороні праці для всіх підприємств незалежно від форм власності та видів діяльності;

− забезпечення координації державних органів, організацій, установ та об'єднання громадян, які вирішують різноманітні проблеми охорони здоров'я, гігієни ти безпеки праці, а також співпрацювання та проведення консультацій між працівниками та власниками, між всіма соціальними групами при прийнятті рішення по охороні праці на місцевому та державному рівнях тощо.

Основу нормативно-технічної документації, що регламентує умови праці у виробничих приміщеннях, складає система стандартів безпеки праці (ССБП), яка являє собою комплекс взаємозв'язаних стандартів, що містять вимоги, норми та правила, направлені на забезпечення безпеки, збереження здоров'я та працездатності людини в процесі праці.

Крім того, охорона праці регламентується цілим рядом нормативних актів: санітарними нормами (СН), будівельними нормами та правилами (БНіП), та іншими документами.

В процесі діяльності людина взаємодіє з навколишнім середовищем у відповідності до трудового процесу. В свою чергу різноманітні фактори виробничого середовища впливають на організм людини.

## 5.2 Шкідливі та небезпечні виробничі чинники при експлуатації локальної мережі об’єкту

У процесі діяльності людина взаємодіє з виробничим середовищем. Вона формує виробничу сферу у відповідності до трудового процесу. В свою чергу, різні чинники виробничого середовища справляють на організм людини певні впливи.

Сукупність чинників виробничого середовища, які впливають на організм людини в процесі праці, мають назву умови праці.

Під шкідливим виробничим чинником розуміють виробничий чинник, дія якого на працюючого у певних умовах призводить до травмування чи до іншого раптового погіршення стану здоров'я.

Під небезпечним виробничим чинником розуміють виробничий чинник, дія якого на працюючого у певних умовах призводить до захворювання чи зниження працездатності.

До шкідливих та небезпечних виробничих чинників відносять:

− знижена чи підвищена температура, вологість, рухомість та іонізація повітря;

− підвищене значення електричного струму в електричному ланцюгу, який проходить скрізь тіло людини при короткому замиканні;

− підвищений рівень статичної та атмосферної електрики;

− відсутність чи недостача природнього світла;

− підвищений рівень шуму на робочому місці;

− психофізіологічні чинники;

− пожежна та вибухова безпека та ін.

## 5.3 Технічні, гігієнічні та організаційні заходи щодо зменшення рівня впливу небезпечних і шкідливих виробничих чинників

Для забезпечення оптимальних мікрокліматичних умов в будь-який період року приміщення, в яких розташовані комп'ютеризовані робочі місця повинні бути обладнані системами опалення. Однак найкраще вирішення цього питання - це встановлення кондиціонерів, які автоматично підтримують задані параметри мікроклімату.

Необхідні концентрації позитивних та негативних іонів в повітрі робочих зон можна забезпечити застосуванням:

− генераторів негативних іонів;

− установок штучного зволоження;

− кондиціонерів;

− примусової вентиляції (провітрювання, системи загально обмінної припливно-витяжної вентиляції, пристрої місцевої вентиляції).

− захисних екранів, що заземлені;

− лазерний принтер бажано розташувати подалі від робочого місця оператора;

− основним же заходом щодо запобігання несприятливого впливу озону та інших шкідливих речовин на здоров'я операторів є забезпечення функціонування припливно-витяжної вентиляції.

Основними заходами та засобами боротьби з шумом є:

− зниження рівнів шуму в джерелі його утворення (застосовується, як правило, в процесі проєктування);

− використання звукопоглинаючих та звукоізолюючих засобів;

− раціональне планування виробничих приміщень та робочих місць.

На комп'ютеризованих робочих місцях основними джерелами шуму є вентилятори системного блоку, накопичувачі, принтери ударної дії. Для зниження рівнів шуму на робочих місцях рекомендується розмістити друкувальні пристрої ударної дії (матричні, шрифтові принтери тощо) в іншому приміщенні, або огородити їх звукоізолюючими екранами.

Оскільки зовнішні шуми (вулиця, суміжні приміщення) також можуть негативно впливати на функціональний стан операторів ВДТ, то стіни приміщень, в яких розташовані комп'ютеризовані робочі місця бажано облицювати звукопоглинаючими матеріалами.

Для зниження вібрації обладнання, пристрої, пристосування необхідно встановлювати на спеціальні амортизуючи прокладки, передбачені нормативними документами.

З метою профілактики несприятливого впливу електромагнітного випромінювання від ВДТ на користувача необхідно:

− встановити на робочому місці відео термінал, що відповідає сучасним вимогам стосовно захисту від випромінювані. (МРК II або ТСО-95);

− встановити на ВДТ старої конструкції (випуск до 1995 року) заземлений приекранний фільтр (незаземлений захисний екран відіграє лише декоративну роль щодо захисту від електромагнітного випромінювання);

− не переобтяжувати приміщення значною кількістю робочих місць з ВДТ;

− не концентрувати на робочому місці велику кількість радіо-пристроїв;

− вимикати ВДТ, якщо на ньому не працюють однак знаходяться не подали від нього.

Для запобігання створенню значної напруженості поля та захисту від статичної електрики необхідно:

− встановити нейтралізатори статичної електрики;

− підтримувати в приміщенні з ВДТ відносну вологість повітря не нижче 45 -50 % (чим сухіше повітря тим більше електростатичних зарядів);

− можна для цього використати навіть побутові зволожувачі;

− застелити підлогу в приміщеннях з ВДТ антистатичним лінолеумом і проводити щоденне вологе прибирання;

− складати всі полімерні покриття (чохли) ВДТ у найбільш віддаленому від користувачів місці розміщення;

− протирати екран та робоче місце спеціальною антистатичною серветкою або зволоженою тканиною;

− користувачам бажано носити одяг, особливо першого шару, з натуральних матеріалів;

− для "зняття" статичного заряду бажано кілька разів на день мити руки та обличчя водою, або час від часу торкатися металевих поверхонь, наприклад, батареї центрального опалення.

Отже, для створення сприятливих умов зорової роботи, які б виключали швидку втомлюваність очей, виникнення професійних захворювань і сприяли підвищенню продуктивності праці, виробниче освітлення повинно відповідати наступним вимогам:

− створювати на робочій поверхні освітленість, що відповідає характеру зорової роботи і знаходиться в межах встановлених норм;

− не чинити засліплюючої дії, як від тих яскравих предметів, що знаходяться в полі зору користувача (пряма блискість). так і тих, що знаходяться за його спиною і можуть відбитись на екрані (відбита блискість);

− забезпечити достатню рівномірність та постійність рівня освітленості, щоб уникнути частої преадаптації зорового аналізатора;

− не створювати на робочому місці різких та глибоких тіней;

− обмежити до мінімуму пульсацію світлового потоку;

− не зменшувати необхідний контраст фону та об’єктів, зображених на екрані ВДТ;

− не створювати небезпечних та шкідливих виробничих факторів (шум, теплові випромінювання, ураження струмом та ін.);

− бути надійни і простим в експлуатації, економічним та естетичним.

Виконання вимог законодавчих актів та забезпечення сприятливих умов виробничого середовища гарантує охорону праці на об’єкті.

## 5.4 Небезпечні фактори при монтажі мережевого обладнання

В процесі виконання роботи на працівника можуть впливати, в основному, такі небезпечні і шкідливі виробничі фактори:

− електричний струм, шлях якого в разі замикання може пройти через тіло людини;

− відлітають тверді частинки (наприклад, при пробиванні отворів);

− вилітає дюбель (при користуванні монтажно-поршневим пістолетом);

− підвищена загазованість повітря при роботі з паяльною лампою, газовим пальником, при роботі в оглядових пристроях і шахтах;

− підвищена концентрація вибухонебезпечних парів і газів в повітрі робочої зони;

− токсичні речовини, що входять до складу кабельної маси, припоїв;

− падіння у відкритий колодязь;

− нагріті до високої температури кабельна маса, припої;

− підвищена пожежна небезпека при використанні легкозаймистих рідин (наприклад, при роботі з паяльною лампою);

− фізичні перевантаження (наприклад, при розмотування кабелю з барабана, його прокладанні);

− гострі кромки, задирки і шорсткість на поверхні інструментів, що вмонтовуються вузлів, механізмів, устаткування, інструменту;

− незручна робоча поза;

− недостатня освітленість робочої зони.

## 5.5 Небезпека використання лазера та лазерних пристроїв

Лазерне випромінювання - вимушене випускання атомами речовини квантів електромагнітного випромінювання.

Лазерне випромінювання здатне поширюватися на значні відстані і відбиватися від кордону розділу двох середовищ, що дозволяє застосовувати ці властивості для цілей локації, навігації та зв'язку.

Лазерне випромінювання використовується для обробки різних матеріалів (різання, свердління, поверхневе загартування та ін.).

Дію лазерного випромінювання на людину досить складно.

Лазерне випромінювання становлять небезпеку для органу зору. Сітківка ока може бути вражена лазерами видимого (від 0,38 мкм до 0,7 мкм) і ближнього інфрачервоного (від 0,75 мкм до 1,4 мкм) діапазонів. Лазерне ультрафіолетове (від 0,18 мкм до 0,38 мкм) і дальнє інфрачервоне (понад 1,4 мкм) випромінювання не досягають сітківки, але можуть пошкодити рогівку, радужку, кришталик.

Лазерне випромінювання становить небезпеку для шкіри, аж до виникнення опіків шкіри.

Так само вулиць, які тривалий час працюють з лазером, можуть розвитку різні неврози і проблеми з серцево-судинною системою.

Перші Гранично допустимі рівні лазерного випромінювання для окремих довжин хвиль були встановлені в 1972 р, а в 1991 р введені в дію «Санітарні норми і правила пристрою і експлуатації лазерів» СанПіН 5804-91.

Захист від лазерного випромінювання здійснюють технічними, організаційними і лікувально - профілактичними методами і засобами, а саме:

− раціональне розміщення лазерних технологічних установок;

− дотримання порядку обслуговування установок;

− використання мінімального рівня випромінювання для досягнення поставленої мети;

− застосування засобів захисту;

− обмеження часу впливу випромінювання;

− призначення та інструктаж осіб, відповідальних за організацію і проведення робіт;

− організація нагляду за режимом робіт;

− контроль за рівнями небезпечних і шкідливих факторів на робочих місцях;

− відвідини не рідше ніж 1 раз на 2 роки офтальмолога, дерматовенеролога, невролога.

## 5.6 Небезпечні фактори при зварюванні оптоволоконного кабелю

До виконання робіт на волоконно-оптичних кабелях зв'язку допускаються особи не молодше 18 років, що пройшли медичний огляд, вступний інструктаж, первинний інструктаж, навчання та стажування на робочому місці, перевірку знань вимог охорони праці, які мають відповідну кваліфікацію і групу з електробезпеки не нижче III .

При проведенні робіт на волоконно-оптичних кабелях зв'язку можливі впливу наступних небезпечних і шкідливих виробничих факторів:

− підвищене значення напруги в електричному ланцюзі, замикання якого може відбутися через тіло людини;

− підвищена або знижена температура повітря робочої зони;

− робота з шкідливими речовинами (ацетон, епоксидні смоли, лаки, нефрас С 150/200);

− можливість впливу лазерного випромінювання генератора;

− потрапляння залишків оптичного кабелю на шкіру працівника.

Кожен працівник повинен бути забезпечений спецодягом, спецвзуттям та іншими засобами індивідуального захисту відповідно до Типових галузевих норм безплатної видачі спеціального одягу, спеціального взуття та інших засобів індивідуального захисту і Колективним договором.

# ВИСНОВКИ

У рамках даного дипломного проєкту проведено докладний аналіз процесу розробки та впровадження локальної обчислювальної мережі (ЛОМ) в одноповерховій будівлі. Організаційна частина роботи включала детальний опис характеристик будівлі, її особливостей та специфіки, планування розробки проєкту ЛОМ, визначення стратегії впровадження та проведення аналізу предметної області, що допомогло зрозуміти вимоги та потреби користувачів у мережевому забезпеченні.

У технологічній частині дослідження було ретельно розглянуто архітектуру комп'ютерної мережі відповідно до стандарту IEEE 802.11, зокрема, вивчено різні аспекти встановлення та налаштування пристроїв, впроваджених у мережу. Також детально розглядалися топологія бездротової мережі (WLAN) та механізми доступу до середовища, що забезпечили глибоке розуміння принципів роботи мережі та її оптимізацію.

Спеціальна частина проекту була присвячена вибору відповідного мережевого обладнання, моделюванню структури мережі для відповідності вимогам та потребам користувачів, а також проведенню тестування спроєктованої мережі з метою перевірки її працездатності та ефективності.

У економічній частині роботи проведено аналіз заробітної плати обслуговуючого персоналу та складено кошторис витрат на необхідне обладнання для реалізації ЛОМ в будівлі, що дозволило оцінити фінансові аспекти проекту та забезпечити його відповідність бюджетним обмеженням.

На завершення роботи вивчені та проаналізовані питання з охорони праці, що включали в себе загальні положення та небезпечні фактори при експлуатації та монтажі мережі, а також запропоновані технічні та організаційні заходи для зменшення ризику впливу небезпечних і шкідливих виробничих чинників.

Отже, отримані результати вказують на те, що успішна реалізація ЛОМ в одноповерховій будівлі можлива при умові комплексного підходу до проектування, впровадження та експлуатації мережі, а також дотримання всіх вимог з охорони праці та фінансових обмежень.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бездротові точки доступу (Wi-Fi) розширять можливості вашої існуючої мережі: вебсайт. URL: https://doba.te.ua/post/64210 (дата звернення: 01.06.2024).
2. Електротехнічна компанія e.next: вебсайт. URL: http://www.enext.ua (дата звернення: 11.05.2024).
3. Інтернет магазин Network Discount: вебсайт. URL: https://networkdiscount.com.ua/ (дата звернення: 10.05.2024).
4. Інтернет магазин Rozetka: вебсайт. URL: http://rozetka.com.ua/ (дата звернення: 18.05.2024).
5. Кочур Д. О. «Комп’ютерні мережі». Методичні вказівки для ви-конання курсового проекту з дисципліни «Комп’ютерні мережі» для студентів спеціальності 123 «Комп’ютерна інженерія».
6. Моделювання комп’ютерної мережі в Packet Tracer: вебсайт. URL: https://studfile.net/preview/9299771/page:6/ (дата звернення: 11.05.2024).
7. Настроювання безпровідної мережі в Windows: вебсайт. URL: https://support.microsoft.com/uk-ua/windows/%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D1%8E%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B1%D0%B5%D0%B7%D0%BF%D1%80%D0%BE%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%D1%97-%D0%BC%D0%B5%D1%80%D0%B5%D0%B6%D1%96-%D0%B2-windows-97914e31-3aa4-406d-cef6-f1629e2c3721 (дата звернення: 18.05.2024).
8. Організація дипломного проєктування фахового молодшого бакалавра методичні рекомендації до виконання студентами спеціальності 123 «Комп’ютерна інженерія» / Калініченко А.О. – Ніжин: , 2024. – 80 с.
9. Основні та додаткові стандарти Wi-Fi – відмінності та особливості: вебсайт. URL: https://nbookpart.com.ua/osnovni-ta-dodatkovi-standarty-wi-fi-vidminnosti-ta-osoblyvosti/ (дата звернення: 17.05.2024).
10. Особливості побудови локальних мереж: вебсайт. URL: http://studopedia.org/13-100846.html (дата звернення: 01.05.2024).
11. Офіційний сайт компанії Cisco Packet Tracer: вебсайт. URL: https://www.cisco.com/ (дата звернення: 11.05.2024).
12. Споруджуємо локальну комп'ютерну мережу: вебсайт. URL: https://i.factor.ua/ukr/journals/nibu/2007/june/issue-46/article-47128.html (дата звернення: 10.05.2024).
13. Стандарти Wi-Fi (wireless fidelity): вебсайт. URL: http://teg.com.ua/standarti-wi-fi-wireless-fidelity-shvidkist-i-chastota-roboti-vaj-faj-rezhimi-bezdrotovoyi-merezhi-shho-take-b-g-protection-802-11-n/ (дата звернення: 02.06.2024).
14. Тип шифрування Wi-Fi — який спосіб автентифікації мережі вибрати: вебсайт. URL: https://nbookpart.com.ua/typ-shyfruvannya-wi-fi-yakyy-sposib-avtentyfikatsii-merezhi-vybraty/ (дата звернення: 07.06.2024).