МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

комп'ютерних систем і мереж

_____ Жуков І.А_____

(підпис) (ПІБ)

"_____"_____2023 р.

КВАЛІФІКАЦІЙНА РОБОТА

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬО-КВАЛІФІКАЦІЙНОГО РІВНЯ

"БАКАЛАВР"

напрям підготовки - 6.050102 "Комп'ютерна інженерія"

Тема: Комп'ютерна мережа підприємства на базі технології *Wi-Fi*

Виконавець: _____ Воронецький А.В

(підпис) **(ПІБ)**

Керівник: _____ Пушкін Ю.О

(підпис) **(ПІБ)**

Нормоконтролер: _____ Журавель С.В

(підпис) **(ПІБ)**

Київ 2023

Факультет_____
Кафедра комп'ютерних систем та мереж
Спеціальність 123 "Комп'ютерна інженерія"

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем та мереж
_____ Жуков І.А
(підпис) (ПІБ)
"_____" _____2023 р.

ЗАВДАННЯ
на виконання дипломного проекту

Воронецькому Артему Віталійовичу
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломного проекту Комп'ютерна мережа підприємства на базі технології Wi-Fi
затверджена наказом ректора від "26"квітня 2023 р., No 591
2. Термін виконання проекту: з "22" травня 2023 р. по "25" червня 2023 р.
3. Вихідні дані до проекту Комп'ютерна мережа підприємства на базі технології *Wi-Fi* і стандарту 802.11ac

4. Зміст пояснювальної записки: Технологія та стандарти *Wi-Fi* мереж; Реалізація комп'ютерної мережі підприємства на базі технології *Wi-Fi* Методи захисту *Wi-Fi* мереж

5. Перелік обов'язкового графічного (ілюстративного) матеріалу:
Презентація Power Point

6.Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1.	Ознайомитись з завданням на виконання дипломного проекту.	22.05.23-25.05.23	
2.	Вивчити спеціальну літературу по темі дипломного проекту.	26.05.23-28.05.23	
3.	Визначити план змісту проекту.	29.05.23-31.05.23	
4.	Зробити опис основних засобів і методів побудови локальної комп'ютерної мереж	01.06.23-05.06.23	
5.	Проаналізувати пристрої для комп'ютерної мережі з *Wi-Fi* технології	06.06.23-08.06.23	
6.	Зробити опис створеної комп'ютерної мережі	09.06.23-12.06.23	
7.	Налаштувати комп'ютерну мережу з технологією *Wi-Fi*	13.06.23-17.06.23	
8.	Оформити пояснювальну записку	18.06.23-20.06.23	
9.	Підготувати презентацію	21.06.23-22.06.23	
10.	Захистити дипломний проект	23.06.23-25.06.23	

7. Дата видачі завдання: "22" травня 2023 р.

Керівник дипломного проекту _____ Пушкін Ю.О

(підпис керівника) (ПІБ.)

Завдання прийняв до виконання _____ Воронецький А.В

(підпис випускника) (ПІБ.)

РЕФЕРАТ

Пояснювальна записка до дипломного проєкту “Комп’ютерна мережа підприємства за технологією Wifi”: 54 с., 25 рис., 2 таблиці, 12 літературних джерел.

WI-FI, БЕЗДРОТОВА МЕРЕЖА, СТАНДАРТ, WPA, VPN, ЗАХИСТ

Об’єкт дослідження – комп'ютерна мережа підприємства на базі технології *Wi-Fi*

Предмет дослідження – локальна комп’ютерна мережа на базі технології *Wi-Fi*

Мета дипломної роботи – створення комп’ютерної мережі для підприємства за технологією *Wi-Fi*

Методи дослідження – проєктування мереж, методи обчислення, методи аналізу комп’ютерних мереж.

Технічні та програмні засоби – середовище проєктування мереж Cisco Packet Tracer – це платформа для візуального моделювання, розроблений компанією Cisco Systems, використовується для створення мережевих топологій та імітування сучасні комп'ютерні мережі

Прогнозні припущення щодо розвитку об’єктів розроблення – модернізація та розширення комп’ютерної мережі.

Результати кваліфікаційної роботи рекомендується використовувати при розробці або модернізації бездротових комп’ютерних мереж.

ЗМІСТ

Кафедра КСМ						
Виконав	Воронецький А.В			Комп'ютерна мережа підприємства на базі технології *Wi-Fi*	Літера	Аркуш 5 / Аркушів 52
Керівник	Пушкін Ю.О					
Консульт.						
Н. контр.	Журавель С.В				КС-431	
Зав. каф.	Жуков І.А.					

ВСТУП

На сьогоднішній день комп’ютерна мережа з технологією *Wi-Fi* є найнеобхіднішою складовою, яка використовується в обчислювальних роботах, щоб користувачі могли підключатися без використання дротової мережі.

Ця технологія з тих пір, як вона була оприлюднена, отримала багато прихильників, дедалі більше замінюючи дротові або *Ethernet*-з’єднання в місцях, які це дозволяють. Прийняття цієї бездротової технології пояснюється її перевагами перед традиційною системою дротової технології та адаптерами *RJ45* та *Ethernet.*

Комп’ютерна мережа дозволяє підвищити продуктивність та ефективність роботи працівників, зменшити витрати та забезпечити гнучкість у роботі. Одним з найбільш поширених технологій бездротового зв'язку є технологія Wi-Fi, яка дозволяє підключати до мережі бездротові пристрої, такі як комп'ютери, смартфони, планшети та інші.

Комп'ютерна мережа на базі технології *Wi-Fi* має безліч переваг, переваги технології *Wi-Fi* полягають в тому, що люди або користувачі технології можуть використовувати мережу в будь-якому місці, що знаходиться в межах діапазону сигналу або передачі. Аналогічно, це дозволяє пристроям: таким як комп’ютери, мобільні телефони та інші, легко підключатися до тієї ж бездротової мережі. Крім цього, *Wi-Fi* дешевше і легше в установці в порівнянні з традиційною дротовою мережею.Правильне налаштування та управління мережею є надзвичайно важливим для забезпечення її надійності та безпеки.

Технологія *Wi-Fi* - безпровідний аналог стандарту *Ethernet*, на основі якого сьогодні побудована велика частина офісних комп'ютерних мереж.

Wi-Fi - означає стандарт бездротового (радіо) зв'язку, який об'єднує декілька протоколів та має офіційне найменування *IEEE* 802.11 (від *Institute of Electrical and Electronic Engineers* - міжнародної організації, що займається розробкою стандартів у галузі електронних технологій). Найбільш відомим та поширеним на сьогоднішній день є протокол *IEEE* 802.11b (зазвичай під скороченням *Wi-Fi* мають на увазі саме цей протокол), що визначає функціонування бездротових мереж.

У даному дипломному проєкті зроблена спроба створити комп'ютерну мережу підприємства за технологією *Wi-Fi* зі стандартом 802.11*ac*.

Створюючи корпоративну *Wi-Fi* мережу зі стандартом 802.11*ac* краще скористатися послугами фахівця, так як для безперебійної, коректної та безпечної роботи безпровідної локальної мережі необхідні проведення створення планів покриття *Wi-Fi* сигналами, правильна установка і головне — професійне налаштування обладнання.

При розміщенні обладнання потрібно точно розрахувати кути відображення сигналу для впевненого прийому його всіма вузлами мережі, вибрати оптимальне розташування точок доступу, маршрутизаторів і при необхідності додаткових комутаторів

Також важливо передбачити можливе розширення мережі, і забезпечити універсальну комутацію пристроїв і передачі даних, тобто можливість підключення різних пристроїв.

Також необхідно захистити дані в мережі при налаштуванні маршрутизаторів, тому в даному проєкті було проаналізована методи захисту особистої інформації. Було розглянуто якість роботи технологій *WPA* та *WPA*2, Ці технології забезпечують стійкий рівень захисту від несанкціонованого доступу до мережі. Для забезпечення високого рівня безпеки в мережах також можна використовувати технологію шифрування *VPN*. Далі було налаштовано безпеку маршрутизатора

Tp-Archer C64.

Необхідним фактором є захист особистих даних в інтернеті, тому при налаштуванні маршрутизатора необхідно використовувати сертифікації *WPA* та *WPA*2 а також шифрування *VPN*.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

Wi-Fi - Wireless Fidelity (бездротова вірність)

РОЗДІЛ 1
ТЕХНОЛОГІЯ ТА СТАНДАРТИ *WI-FI* МЕРЕЖ

1.1. Технологія *Wi-Fi* мереж

Wi-Fi є популярною технологією бездротових мереж. *Wi-Fi* означає «точність бездротового зв'язку». *Wi-Fi* технологію було винайдено *NCR Corporation/AT&T* у Нідерландах у 1991 році. Використовуючи цю технологію, обмін інформацією можливий між двома чи більше пристроями. Технологія *Wi-Fi* створена для мобільних комп'ютерних пристроїв, ноутбуків, для мобільних додатків що потребують *Wi-Fi*, телевізорів, *DVD*-програвачів та цифрових камер. В даному випадку є 2 можливості зв'язку з підключенням *Wi-Fi*: точка доступу - клієнт або підключення клієнт - клієнт.

Wi-Fi - найвідоміша бездротова технологія в світі.

Wi-Fi – це бездротова локальна мережа. За допомогою технології *Wi-Fi* локальні мережі можуть працювати без використання кабелів. Це основний вибір для домашніх і бізнес-мереж. За допомогою бездротового адаптера комп'ютера дані перетворюються в радіосигнал і передають дані в антену для користувачів.

Принцип роботи технології *Wi-Fi*

Wi-Fi технологія - забезпечує високошвидкісне підключення до Інтернету та до мережі без використання кабелів або проводів. Бездротова мережа керує трьома основними елементами: радіосигналами, антеною та маршрутизатором.[1]

Wi-Fi мережі можуть бути створені за допомогою точок доступу (Access Points), які підключаються до провідної мережі та надають доступ до Інтернету для підключених пристроїв. Одна точка доступу може обслуговувати кілька пристроїв одночасно.(див. рис.1.1)

Рис.1.1. Принцип роботи *Wi-Fi*

Фактична трансляція підключається в послідовність, фактично завершується шляхом перегляду стереосистеми, а також вартості проводів з монітором до класифікації.

Для організації мережі необхідно мати спеціальне обладнання, а саме - точка доступу, тобто роутер, підключений до дротової мережі Інтернет та пристрій, який потрібно підключити до бездротової мережі *Wi-Fi*, оснащений радіомодулем(рис.1.2). Роутер обладнаний таким самим радіомодулем, який виконує функції прийому та передачі бездротового сигналу. Ці модулі можуть бути від різних виробників, і відрізнятися між собою конструкцією чіпа, але завдяки єдиному стандарту *Wi-Fi* забезпечується повна їхня сумісність, що означає можливість підключення різних пристроїв до мережі *Wi-Fi*. Інтернету через *Wi-Fi* мережу, недостатньо лише мати модуль *Wi-Fi* у ноутбуці чи смартфоні.

Рис.1.2. Схема роботи *Wi-Fi* маршрутизатора

На сьогоднішній день, приймачі та передавачі, в мережах *Wi-Fi*, нагадують пристрої, які використовують в смартфонах і портативних радіостанціях. Вони

передають і приймають радіохвилі, а також перетворюють цифровий сигнал на радіохвилі і навпаки. Відмінність пристроїв *Wi-Fi* від аналогічних пристроїв полягає в тому, що вони використовують частоти 2,4 ГГц або 5 ГГц, які суттєво вищі, що дозволяє передавати більше інформації.

Wi-Fi дає можливість користувачу отримати доступ до Інтернету в будь-якій території. Тепер можна створити систему на бібліотеках, школах, коледжах, кампусах, особистих інститутах, а також у відкритих публічних місцях, щоб допомогти зробити компанію набагато прибутковішою, а також взаємодіяти з їх клієнтами будь-коли.

Роботу з технологією *Wi-Fi* може мати компанія, використовуючи кабельне телебачення, набагато менше. Радіосигнали передаються з антен і маршрутизаторів, які отримують сигнали приймачами *Wi-Fi*, такими як комп'ютери та стільникові телефони з картами *Wi-Fi*. Кожного разу, коли комп'ютер отримує сигнали в межах 45-90 метрів для маршрутизатора, негайно підключається пристрій.

Від діапазону в приміщенні або на вулиці, навколишнього середовища залежить радіус дії *Wi-Fi*. Карти *Wi-Fi* зчитують сигнали та створюють інтернет-з'єднання між користувачем і мережею. Швидкість пристрою, який використовує з'єднання *Wi-Fi*, збільшується, коли пристрій знаходиться близько ро Wi-Fi роутера, і швидкість зменшується, коли комп'ютер знаходиться на великій відстані від роутера.[1]

Нові ноутбуки та смартфони мають вбудовані карти *Wi-Fi*, що дозволяє користувачам не шукати додаткові карти для доступу до мережі *Wi-Fi*. Якщо доступ до мережі є безкоштовним, то користувачеві буде запропоновано ввести ідентифікатор та пароль. Більшість міст мають гарячі точки, які створюють точки доступу до мережі *Wi-Fi*. Гарячі точки можна знайти в громадських місцях, таких як ресторани, аеропорти, готелі, офіси та університети.

1.2. Стандарти технології *Wi-Fi*

Разом з випуском нової техніки технології передачі даних постійно розвиваються. Щоб знайти найбільш підходящу мережу для своїх потреб, важливо ознайомитися з усіма наявними стандартами *Wi-Fi*, які існують на сьогоднішній

день. *Wi-Fi Alliance* розробила більше двадцяти різних технологій підключення, але чотири з них є найбільш популярними наразі: 802.11b, 802.11a, 802.11g і 802.11n. Найновішим стандартом є 802.11ac, який має значно кращі характеристики, ніж сучасні адаптери.

Стандарт 802.11b є одним зі старших сертифікованих технологій бездротового підключення, що відрізняється високою доступністю. Цей пристрій має чоткі параметри, зокрема:

- швидкість передачі даних - 11 Мбіт/с;
- діапазон частот - 2,4 ГГц;
- радіус дії (без об'ємних перегородок) - до 50 метрів.

Діаграму розвитку стандартів показано на рис.1.3.

Рис.1.3. Діаграма розвитку стандартів *Wi-Fi*

Стандарт 802.11b слабкий і має низьку пропускну здатність. Низька ціна цього *Wi-Fi* підключення, за технічними характеристиками значно відстає від більш сучасних моделей.

Стандарт 802.11a

Ця технологія являє собою поліпшену версію попереднього стандарту. Розробники покращили пропускну здатність пристрою і його тактову частоту. В даній модифікації вплив інших пристроїв на якість сигналу мережі не впливає, завдяки змінам характеристик:

- швидкість передачі інформації – 54 Мбіт / с;
- діапазон частот – 5 ГГц;
- радіус дії – до 30 метрів

Однак всі переваги стандарту 802.11a компенсовані в рівній мірі його недоліками: зменшеним радіусом підключення і високою (у порівнянні з 802.11b) ціною.

Стандарт 802.11g

Оновлена модифікація відповідає найновішим стандартам бездротових мереж, оскільки підтримує технологію 802.11b із значною вищою швидкістю з'єднання в порівнянні з нею:

- швидкість передачі інформації – 54 Мбіт / с;
- діапазон частот – 2,4 ГГц;
- радіус дії – до 50 метрів.

Тактова частота 802.11g знизилася до 2,4 ГГц, але зона покриття мережі повернулася до колишніх показників, характерних для 802.11b як це показано на рис.1.4. Крім того, ціна на адаптер стала більш доступною, що є вагомою перевагою при виборі обладнання.

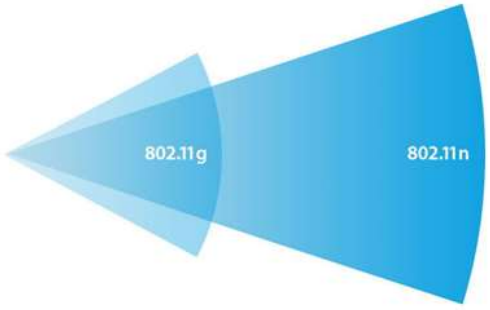


Рис.1.4. Вигляд зони покриття стандартів

Стандарт 802.11n

Стандарт вже давно на ринку і має непогані параметри, виробники досі працюють над покращенням стандарту. Цей стандарт не сумісний з попередніми стандартами, майже не використовується:

- швидкість передачі інформації – теоретично до 480 Мбіт / с, а на практиці виходить наполовину менше;

- діапазон частот – 2,4 або 5 ГГц;

- радіус дії – до 100 метрів

Графік порівняння стандартів 802.11n, 802.11g, 802.11b на рис.1.5.

Рис.1.5. Графік порівняння швидкості передачі даних

У *Wi-Fi Alliance* є стандарти спеціалізованого призначення. Основні модифікації стандартів спеціального призначення:

- 802.11d - забезпечує сумісність пристроїв бездротового зв'язку різних виробників, адаптує їх до особливостей передачі даних на всій території країни;

- 802.11e - визначає якість передачі медіафайлів;

- 802.11i - покращена версія захисту особистої інформації користувачів;

Пристрої, що використовують модифікації 802.11ac, забезпечують користувачам високу якість роботи в Інтернеті. Між переваг цього стандарту можна виділити наступні: Графік максимальної швидкості стандартів(див. рис.1.6)

- висока швидкість. При використанні мережі 802.11ac для передачі даних

Рис.1.6. Графік максимальної швидкості стандартів

- збільшена кількість частот. Модифікація 802.11ac оснащена цілим асортиментом частот 5 ГГц. Новітня технологія володіє сильнішим сигналом. Адаптер з високим діапазоном охоплює смугу частот до 380 МГц;

- зона покриття мережі 802.11ac. Цей стандарт надає більш широкий радіус дії мережі. Крім того, *Wi-Fi* підключення працює навіть через бетонні та гіпсокартонні стіни. Перешкоди, що виникають при роботі побутової техніки та сусідського інтернету, ніяк не впливають на роботу вашого з'єднання;

- оновлені технології. 802.11ac оснащений розширенням *MU-MIMO*, яке забезпечує безперебійну роботу декількох пристроїв в мережі.(див. рис.1.7) Технологія *Beamforming* визначає пристрій клієнта і направляє йому відразу кілька потоків інформації.

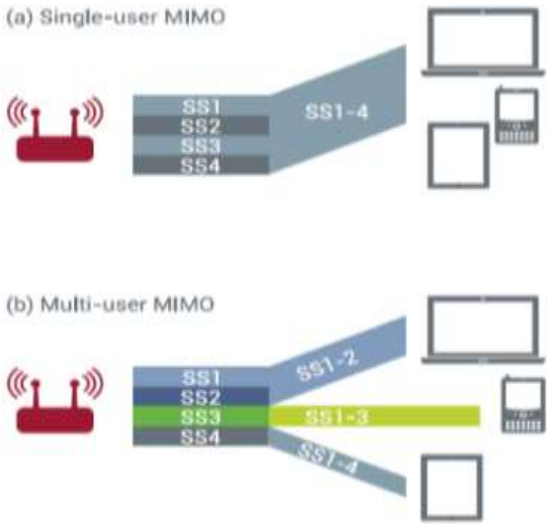


Рис.1.7. Підтримка технології MU-MIMO

Розробляються стандарти *Wi-Fi* 802.11az: позиціонування наступного покоління (*NGP*)[5]

У січні 2015 року була сформована дослідницька група для вирішення потреб «станції щодо визначення її абсолютного та відносного положення щодо іншої станції або станцій, з якими вона пов’язана або не пов’язана». Цілі групи полягають у визначенні модифікацій контролю доступу до медіа та фізичних рівнів, які дозволяють «визначати абсолютну та відносну позицію з кращою точністю по відношенню до протоколу точного вимірювання часу (*MTM*), що виконується на тому самому типі *PHY*, у той час як зменшує використання існуючого бездротового середовища та енергоспоживання, і його можна масштабувати до щільних розгортань».

802.11bf - визначення *WLAN*

Стандарт досліджує використання *WLAN*, яка може сприймати бездротові

сигнали, щоб виявити особливості передбачуваної цілі в певному середовищі, такі як дальність, швидкість, кут, рух, присутність або близькість або жести. Об'єктами можуть бути люди чи тварини, а середовище може бути в кімнаті, будинку, транспортному засобі чи офісі. Початковий проект очікується у вересні 2022 року, а остаточне затвердження очікується в період з липня по вересень 2024 року.

802.11bh – змінні *MAC*-адреси

Стандарт 802.11aq формалізував конфіденційність *MAC* для станцій 802.11, що включає зміну їх MAC-адреси та використання випадкової *MAC*-адреси. Однак це може мати широкий спектр наслідків, які вплинуть не лише на мережі 802.11, а й на багато пов'язаних служб. Цю робочу групу було сформовано для розробки поправки для пом'якшення цих впливів, продовжуючи при цьому захищати переваги конфіденційності користувачів, які надають змінені *MAC*-адреси. Початковий проект цих змін очікується до вересня 2022 року.[5]

802.11bi – покращена конфіденційність даних

Метою цієї поправки є внесення змін до специфікації керування доступом до медіа (*MAC*) 802.11 для створення нових механізмів, які стосуються та покращують конфіденційність користувачів. Користувачі та уряди стурбовані захистом особистої інформації, такої як місцезнаходження, пересування, контакти та діяльність. Сумісність із стандартом 802.11 недостатньо захищає користувачів від атак відстеження та профілювання. Початковий проект пропозиції очікується до березня 2023 року.

Нішеві стандарти *Wi-Fi*

802.11ah : *Wi-Fi HaLow*

802.11ah визначає роботу звільнених від ліцензії мереж у діапазонах частот нижче 1 ГГц (зазвичай діапазон 900 МГц), за винятком діапазонів *TV White Space*. У США це включає 908-928 МГц з різними частотами в інших країнах.

Метою 802.11ah є створення мереж *Wi-Fi* із розширеним радіусом дії, які виходять за рамки типових мереж у діапазоні 2,4 ГГц і 5 ГГц (нижча частота означає більший радіус дії), зі швидкістю передачі даних до 347 Мбіт/с.[5]

на багато пов’язаних служб. Цю робочу групу було сформовано для розробки

802.11bf - визначення *WLAN*

Стандарт досліджує використання *WLAN*, яка може сприймати бездротові

Стандарт досліджує використання *WLAN*, яка може сприймати бездротові сигнали, щоб виявити особливості передбачуваної цілі в певному середовищі, такі як дальність, швидкість, кут, рух, присутність або близькість або жести. Об’єктами можуть бути люди чи тварини, а середовище може бути в кімнаті, будинку, транспортному засобі чи офісі. Початковий проект очікується у вересні 2022 року, а остаточне затвердження очікується в період з липня по вересень 2024 року.

802.11bh – змінні *MAC*-адреси

Стандарт 802.11aq формалізував конфіденційність *MAC* для станцій 802.11, що включає зміну їх *MAC*-адреси та використання випадкової *MAC*-адреси. Однак це може мати широкий спектр наслідків, які вплинуть не лише на мережі 802.11, а й на багато пов’язаних служб. Цю робочу групу було сформовано для розробки поправки для пом’якшення цих впливів, продовжуючи при цьому захищати переваги конфіденційності користувачів, які надають змінені *MAC*-адреси. Початковий проект цих змін очікується до вересня 2022 року.[5]

Метою цієї поправки є внесення змін до специфікації керування доступом до медіа (*MAC*) 802.11 для створення нових механізмів, які стосуються та покращують конфіденційність користувачів. Користувачі та уряди стурбовані захистом особистої інформації, такої як місцезнаходження, пересування, контакти та діяльність. Сумісність із стандартом 802.11 недостатньо захищає користувачів від атак відстеження та профілювання. Початковий проект пропозиції очікується до березня 2023 року.

Нішеві стандарти *Wi-Fi*

802.11ah : *Wi-Fi HaLow*

802.11ah визначає роботу звільнених від ліцензії мереж у діапазонах частот нижче 1 ГГц (зазвичай діапазон 900 МГц), за винятком діапазонів *TV White Space*. У США це включає 908-928 МГц з різними частотами в інших країнах.

Метою 802.11ah є створення мереж *Wi-Fi* із розширеним радіусом дії, які виходять за рамки типових мереж у діапазоні 2,4 ГГц і 5 ГГц (нижча частота

означає більший радіус дії), зі швидкістю передачі даних до 347 Мбіт/с.[5]

Крім того, стандарт спрямований на зниження енергоспоживання, корисне для пристроїв Інтернету речей, щоб спілкуватися на великих відстанях без використання великої кількості енергії. Але він також може конкурувати з технологіями *Bluetooth* у домі через менші потреби в енергії. Протокол був затверджений у вересні 2016 року та опублікований у травні 2017 року.

802.11ay: наступне покоління 60 ГГц

Цей стандарт підтримує максимальну пропускну здатність принаймні 20 Гбіт/с на частоті 60 ГГц (наразі 802.11ad досягає до 7 Гбіт/с), а також збільшує діапазон і надійність. Стандарт був опублікований у липні 2021 року. Порівняння основних стандартів технології *Wi-Fi* (див. табл. 1.1)

Таблиця 1.1

Порівняння стандартів технології *Wi-Fi*

Стандарт *IEEE* 802.11	802.11a	802.11g	802.11n	802.11ac
Макс.швидкість (Мбіт/сек)	До 54	До 54	до 600	До 1300-6000
Покриття(м.)	40/120	40/120	75/250	130/490
Частота (ГГц)	5	2.4	2.4	
Ширина каналу (МГц)	20	20	20/40	20/40/80/160
MIMO	-	-	*SU-MIMO*	*MU-MIMO*
Безпека	*WEP*	*WEP/WPA*	*WEP/WPA/WPA2*	*WEP/WPA/WPA2*

1.3 Переваги та недоліки *Wi-Fi* технології

Переваги бездротової мережі

Доступність: для бездротових мереж не потрібні дроти чи кабелі, тому користувачі можуть спілкуватися, навіть коли вони рухаються. Це дозволяє користувачам переміщатися без відключення. В результаті відбувається підвищення продуктивності.

Легке встановлення: установити бездротову мережу швидше та простіше порівняно з дротовою мережею. Це також зменшує використання кабелів, які

важко встановити, і створює ризик для безпеки, оскільки користувач може зачепитись за дроти. Якщо користувачі хочуть змінити мережу, необхідно оновити бездротову мережу відповідно до нових конфігурацій.

Широке охоплення: бездротові мережі мають ширше охоплення, ніж дротові мережі. Їх можна легко розширити до місць, де дроти та кабелі недоступні.

Гнучкість: налаштування бездротової мережі допомагає користувачеві легко виконувати роботу вдома. Завдяки цій мережі користувачі можуть працювати більш продуктивно, а також мати доступ до даних клієнтів.[3]

Ефективність: бездротові мережі дозволяють покращити передачу даних. Завдяки бездротовій мережі передача інформації між користувачами відбувається набагато швидше.

Рентабельність: бездротові мережі є економічно ефективними, оскільки вони дешевші та легші в установці. Незважаючи на високі початкові інвестиції, з часом загальні витрати зменшуються.

Недоліки бездротової мережі

Безпека: під час використання бездротових мереж безпека є великою проблемою. Якщо бездротова мережа встановлена належним чином або обслуговується належним чином, це може спричинити серйозні загрози безпеці. Підключення фізичних компонентів, таких як дроти, не вимагає бездротової мережі. Їм потрібен лише бездротовий адаптер, який автоматично підвищує ризик злому, оскільки хакери можуть легко отримати доступ до мережі.

Обмежена пропускна здатність: бездротові мережі не можуть підтримувати *VTC* або відеотелеконференції, оскільки вони мають мінімальну пропускну здатність також має обмежені можливості розширення, оскільки немає бездротового спектру для зайняття. Пропускна здатність може бути вкрадена іншими користувачами, якщо мережа не захищена паролем.

Швидкість: швидкість бездротової мережі нижча за швидкість дротових мереж. У бездротовій мережі передача або обмін файлами відбувається набагато повільніше. Швидкість також залежить від розташування користувача відносно мережі. Чим далі користувач від мережі, тим гірше стає зв'язок. Це величезна проблема для великих приміщень або будівель.[3]

Вартість: бездротові мережі зазвичай недорогі, але вартість встановлення дуже висока. Налаштування бездротової мережі є дуже дорогим, а інколи це пов'язано з додатковими витратами. Бездротова мережа може вимагати встановлення спеціального обладнання, яке може бути дорогим. Схильність до перешкод: через зовнішні фактори, як-от пилові бурі або туман у бездротових мережах існує висока ймовірність виникнення перешкод. Бездротові мережі дуже схильні до перешкод; отже, туман, радіація, радіосигнали чи будь-які подібні перешкоди можуть спричинити збій у бездротовій мережі. Якщо в одній зоні занадто багато користувачів, повітряна смуга, за допомогою якої передаються сигнали, може бути перевантажена

Покриття: зона покриття бездротової мережі мінімальна. Типовий бездротовий маршрутизатор дозволяє користувачам користуватися мережею на відстані від 45 до 90 метрів.

Потрібні базові знання комп'ютера: для налаштування бездротової мережі потрібні мінімальні знання комп'ютера. Користувачі, які не мають досвіду роботи з комп'ютером, можуть зіткнутися з проблемами встановлення бездротової мережі. Існує високий ризик безпеки, і хакери можуть легко зламати ці мережі.[3]

1.4. Безпека комп'ютерних мереж технології *Wi-Fi*

Технологія *Wi-Fi* передбачає важливість забезпечення безпеки, оскільки це забезпечує захист персональних даних в мережі. Незахищені бездротові маршрутизатори можуть бути легко доступними для підключення, однак це може стати проблемою, оскільки будь-яка особа, яка підключена до вашого бездротового маршрутизатора, може завдати шкоди та зловмисно здобути дані користувача. Тому, для забезпечення безпеки пристроїв, що працюють на базі бездротових технологій, необхідно приділяти належну увагу заходам безпеки.

Бездротовий маршрутизатор – це один з видів апаратного пристрою, який зазвичай використовується вдома. Це основний пристрій бездротової мережі. Даний маршрутизатор в основному використовується постачальниками послуг Інтернету для підключення кабелю до Інтернету. Іноді його також називають пристроєм *WLAN* (бездротова локальна мережа). Бездротова мережа також називається мережею *Wi-Fi*

Основною функцією цього роутера є об'єднання мережевих функцій роутера і бездротової точки доступу. Подібно до дротової мережі, концентратор є проміжним розташуванням, до якого підключаються всі комп’ютери для забезпечення доступу комп’ютерів до мережі. Зараз наявні бездротові концентратори працюватимуть як маршрутизатори, але це шлюзи.

Найпоширенішим способом підключення до Інтернету без використання кабелю є настільний маршрутизатор *Wi-Fi*. Ці маршрутизатори невеликі за розміром і мають антени. Роутер роздає *Wi-Fi* в будь-якому місці: в офісі або вдома.

Розширювач діапазону *Wi-Fi* розташований у масиві, щоб збільшити або розширити покриття Інтернету.

Мобільна точка доступу/точка доступу *Wi-Fi*

Кожний смартфон має мобільну точку доступу. Після того, як точку доступу в смартфоні ввімкнено, оператор мобільного зв’язку може забезпечити бездротовий доступ до мережевого з’єднання використовуючи інші пристрої, щоб забезпечити доступ до Інтернету. Точка доступу *Wi-Fi* може бути в смартфонах, при наявності мобільного інтернета можна роздавати *Wi-Fi* для інших пристроїв. Це портативний пристрій, який використовує вишки стільникового зв’язку для трансляції сигналів.

Різні пристрої, такі як ноутбуки, плеєри *iPod*, можна підключити бездротовим способом до пристрою, який підключається до Інтернету, в будь якому місці. Подібно до смартфона, місячна вартість мобільної точки доступу залежить від використання вибраного тарифного плану. Цей вид точки доступу є більш послідовним, щоб дозволити доступ до Інтернету шляхом пошуку стаціонарних громадських точок доступу *Wi-Fi*.

Висновки до розділу

У даному розділі проаналізував використання технології *Wi-Fi* , принцип роботи та встановлення даної технології, визначено переваги та недоліки використання бездротових мереж, також проаналізовано можливості існуючих стандартів для подальшого використання в розробці мережі підприємства на базі технології *Wi-Fi* було обрано основний стандарт 802.11ac.

РОЗДІЛ 2
РЕАЛІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА НА БАЗІ ТЕХНОЛОГІЇ *WI-FI*

2.1 Опис підприємства

В даній роботі розглядається можливість створення комп'ютерної мережі підприємства "*Computer Service*".

Підприємство "*Computer Service*" спеціалізується на різних аспектах комп'ютерної діяльності. Приміщення має два поверхи: на першому поверсі розташовані технічний відділ, серверна кімната, відділ роботи з корпоративними клієнтами та кабінет генерального директора.

Технічний відділ займається розробкою та підтримкою технічних аспектів продуктів або послуг компанії. Цей відділ контролює процес розробки нових продуктів, оновлення та вдосконалення існуючих продуктів, вирішення технічних питань, а також даний відділ надає консультації з технічних питань.

Відділ роботи з клієнтами забезпечує зв'язок з клієнтами та вирішення їх проблем. Цей відділ надає інформацію про нові продукти та послуги компанії, відповідає на запитання клієнтів, надає підтримку після продажу та вирішуються питання з обслуговуванням клієнтів.

Також на першому поверсі знаходиться серверна кімната та кабінет генерального директора. Доступ до серверної кімнати має тільки директор та працівники технічного відділу у разі вирішення несправностей.

На другому поверсі даного підприємства знаходяться: фінансовий відділ, відділ управління персоналом та відділ продажу.

У фінансовому відділі контролюються фінансові аспекти діяльності компанії. Цей відділ забезпечує бухгалтерський та фінансовий облік, планування та бюджетування, аналізує фінансові результати та розробляє стратегії.

бюджетування, аналізує фінансові результати та розробляє стратегії фінансового розвитку компанії.

Відділ продажу відповідає за продаж продуктів або послуг компанії. В даному відділі розробляються стратегії продажу, пошук нових клієнтів, проводять переговори та укладаються угоди, а також підтримуються відносини з постійними клієнтами.

Важливим відділом в даній компанії є відділ управління персоналом. Цей відділ забезпечує роботу зі створенням та виконанням політики компанії щодо управління персоналом.

Основні завдання відділу управління персоналом включають:

- підбір та рекрутинг нових співробітників;
- розробка та виконання процесів навчання та розвитку персоналу;
- проведення оцінки роботи працівників та визначення системи мотивації;
- вирішення конфліктних ситуацій та підтримка комунікацій між співробітниками;
- забезпечення дотримання законодавства щодо праці та соціальних питань.

Відділ управління персоналом забезпечує належне управління персоналом, що є ключовим фактором ефективної діяльності компанії. Допомагає співробітникам розвиватись та досягати своїх цілей, та забезпечує гармонійні відносини в колективі. План будівлі 1 та 2 поверху (див. рис.2.1, рис.2.2)

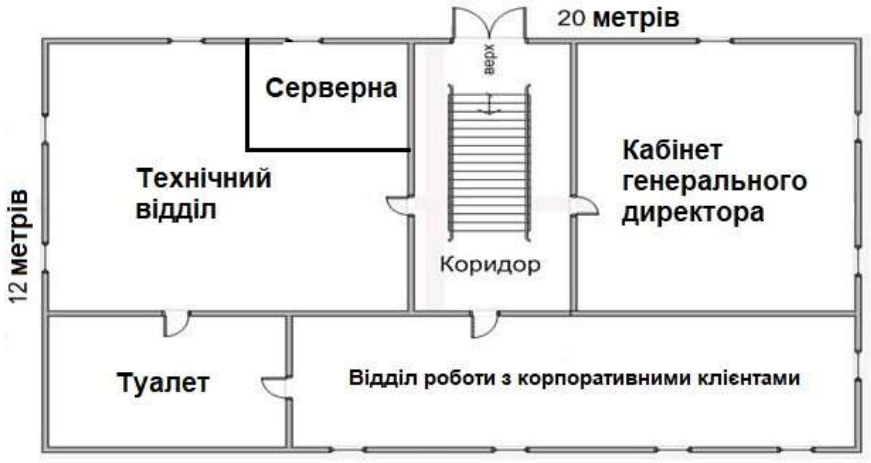


Рис.2.1. План будівлі 1 поверху

Рис.2.2. План будівлі 2 поверху

Підприємство "*Computer Service*" існує мережа 13 комп'ютерів, 2 ноутбуки, 2 маршрутизатора, 2 комутатора, 4 принтера, 2 сканера, 1 сервер, 13 мережевих адаптерів для комп'ютерів.

Для створення структурної схеми бездротової мережі за технологією *Wi-Fi* було використано програму *Cisco Packet Tracer*.Структурна схема проектованої мережі зображена на рис.2.3.

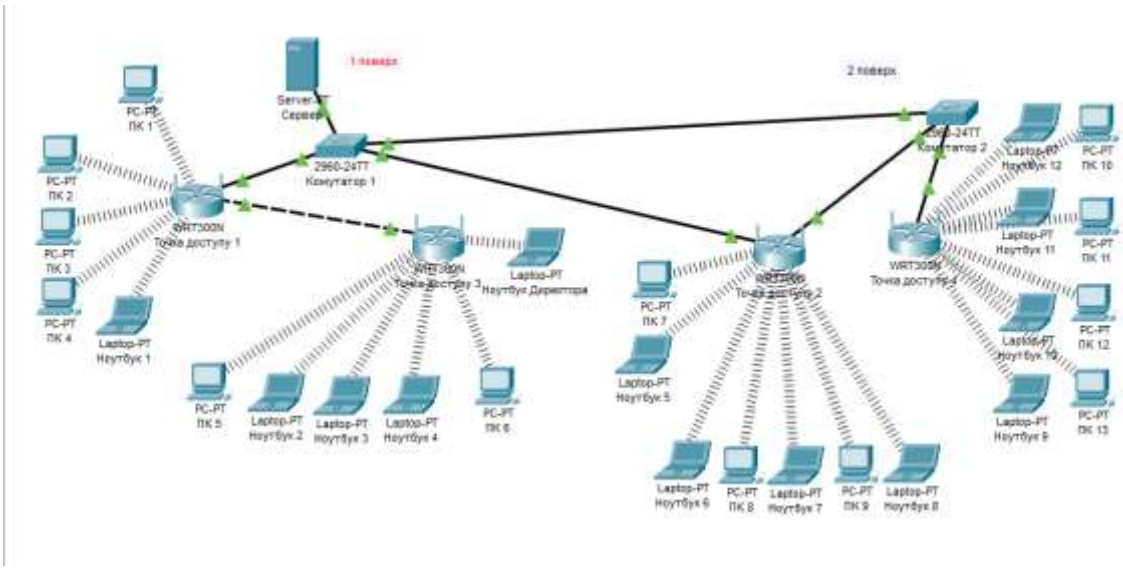


Рис.2.3. Структура проектованої мережі

Cisco Packet Tracer – це крос-платформенний інструмент візуального моделювання, розроблений компанією *Cisco Systems*, що дозволяє користувачам створювати мережеві топології та імітувати сучасні комп'ютерні мережі.

Програмне забезпечення дозволяє користувачам імітувати конфігурацію маршрутизаторів і комутаторів *Cisco* за допомогою імітаційного інтерфейсу командного рядка. *Packet Tracer* використовує користувальницький інтерфейс *drag-and-drop* , що дозволяє користувачам додавати та видаляти модельовані мережеві пристрої, як вони вважають за потрібне. Програма спрямована переважно на сертифікованих студентів *Cisco Network Associate Academy* як навчальний інструмент, який допомагає їм вивчати фундаментальні концепції *CCNA*. Раніше студенти, які навчаються в програмі Академії *CCNA*, могли вільно завантажувати та використовувати інструмент безкоштовно для навчального використання. З серпня 2017 року з версією 7.1 є безкоштовним для всіх.

2.2. Розміщення обладнання в офісі

Зображено план розміщення обладнання на підприємстві(рис.2.4). В технічному відділі знаходиться 4 комп'ютери ,ноутбук та принтер, в серверній кімнаті знаходиться сервер, комутатор та маршрутизатор. Відділ роботи з корпоративними клієнтами має 2 комп'ютери та 3 ноутбуки. В кабінеті генерального директора підприємства розташовано ноутбук та точка доступу, принтер та сканер.

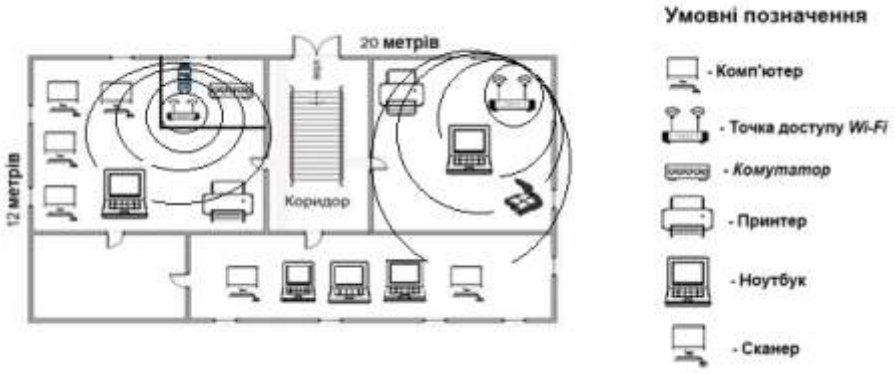


Рис.2.4. Розміщення техніки на 1 поверсі

На 2 поверсі в фінансовому відділі розташовано комп'ютер, ноутбук, принтер для друкування фінансових звітів та маршрутизатор. У відділі продажу є 2 комп'ютери, 3 ноутбуки. У фінансовому відділі знаходиться точка доступу

комп’ютер, ноутбук та принтер. Відділ управління персоналом має 4 комп’ютери,4 ноутбуки,точку доступу,комутатор,принтер та сканер.(див. рис.2.5)

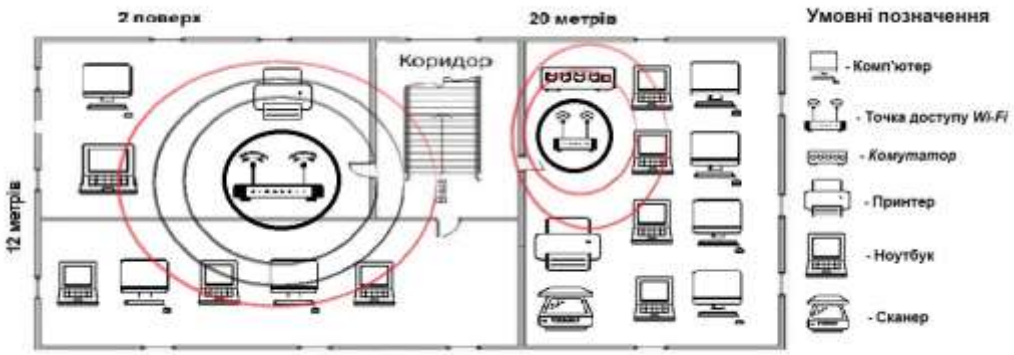


Рис.2.5. Розміщення техніки на 2 поверсі

Обране обладнання розташоване в відповідних місцях для зручності роботи робітників на підприємстві, також точки доступу *Wi-Fi* розташовані таким чином щоб на поверсі у всіх користувачів був якісний доступ до інтернету. Використовуємо по 2 точки доступу на кожний поверх, для того щоб всім працівникам було зручно працювати з інтернетом та не було проблем з інтернетом. Для друкування та сканування документів використовують принтери та сканер.

2.3 Вибір необхідного обладнання для мережі

Рис.2.6. Маршрутизатор *TP-Link ARCHER A64*

До двухдіапазонного маршрутизатора *Archer A64* можна підключити пристрої: при діапазоні 2,4 ГГц можна забезпечити комфортну роботу з електронною поштою, також використання браузерів для перегляду веб-сторінок та простих завдань, тоді як діапазон 5 ГГц використовується для більш важких задач в яких швидкість передачі даних має важливу роль.

Новий рівень безпеки *WPA3* – це найновіший протокол, що підвищує безпеку персональних *Wi-Fi* мереж. Завдяки чотирьом високопродуктивним зовнішнім антенам роутера *Archer A64* сигнал *Wi-Fi* буде у всьому будинку, а технологія *Beamforming* дозволить покращити якість сигналу для пристроїв за рахунок виявлення їх розташування концентрування сигналу в їх напрямі. Взаємодія з кількома пристроями *Wi-Fi* одночасно з швидкістю до 1200 Мбіт/с за стандартом 802.11ac та технологією *MU MIMO* забезпечить швидкий та надійний обмін даними з кількома пристроями одночасно, уникаючи затримок. Крім того, з 10 раз швидшими гігабітними портами *Ethernet* (1 порт *WAN* + 4 порти *LAN*), *Archer A64* забезпечує швидкість до десяти разів вище швидкості стандарту *Fast Ethernet*, забезпечуючи швидке та надійне підключення для комп'ютерів, *Smart TV* та ігрових консолей. Завдяки доступній ціні, *Archer A64* стане чудовим вибором для тих, хто хоче ознайомитися з гігабітною швидкістю підключення.

Потрібно перевести *Archer A64* в режим точки доступу, щоб перетворити наявну дротову мережу на бездротову.

Рис.2.7. Комутатор *TP-LINK TL-SF1024D*

Призначення пристрою

Комутатор *TP-LINK TL-SF1024D* являє собою високопродуктивний, що забезпечує безрозривний зв'язок мережевого пристрою для поновлення старої мережі і збільшення її пропускної здатності до 100 Мбіт/с. Всі 24 порти підтримують технологію авто-*MDI/MDIX*, яка усуває необхідність застосування кабелю з перехресними парами. Більш того, завдяки інноваційній енергозберігаючій технології виріб дозволить зберегти до 75% споживаної електроенергії. Тому даний продукт є екологічно-безпечним рішенням для вашої ділової мережі.(див. рис.2.7)

Енергозберігаюча технологія

Виріб оснащений сучасною енергозберігаючою технологією Green Ethernet, за допомогою якої збільшується пропускна здатність мережі зі меншою затратою енергії.

Робочі характеристики

Металевий корпус *TL-SF1024D* робить комутатор найбільш досконалим, якісним продуктом. Завдяки використанню неблокуючої архітектури пристрій має можливість передавати і фільтрувати пакети на максимальній допустимій для мережі швидкості щоб забезпечити максимальну пропускну здатність.

Використання пристрою

Для пристрою не потрібна додаткове налаштування. Функція автоузгодження, яка присутня на кожному порту, спрощує процес встановлення та автоматично визначає швидкість з'єднання мережевого пристрою (10 або 100 Мбіт/с). Це дозволяє налаштувати сумісність та оптимальний режим роботи без додаткових зусиль.

Сервер *Dell PowerEdge* T620 *Tower* – це ідеальна система для малих і середніх підприємств і центрів обробки даних, яка має ємнісну пам’ять та сховища . Цей пристрій може бути використаний для високопродуктивних обчислень та для загального призначення. Сервер також може повністю сумісний з іншими додатками і інфраструктурами. *Dell* T620 підтримує 24 модуля *DIMM* і 8 відсіків для дисків, тому пристрій може задовольнити потреби користувача у важких задачах. Обчислювальна потужність *Intel Xeon* E5-26xx V1 / V2 робить сервер більш продуктивним та ефективним.(див. рис.2.8)

Рис.2.8. Сервер *DELL* T620 *Tower*

Продуктивність сервера

Ця система може підтримувати до двох процесорів з сімейства E5-2600 або E5-2600 v2 з 12 ядрами в кожному. Для живлення використовується блок живлення *Platinum Plus* з потужністю 495 Вт, 750 Вт або 1100 Вт, що забезпечує високу продуктивність системи.

Обсяг пам’яті

Щодо пам'яті, чіпсет Intel C602 дозволяє використовувати до 24 модулів *DDR*3 *DIMM* в конфігурації з двома процесорами, які можуть бути як реєстрові (*RDIMM*), так і зі зниженою навантаженням (*LRDIMM*). Кожен процесор контролює до 12 модулів пам'яті, які можуть працювати на швидкості до 1866 MT / с. Завдяки цьому, сервер вежі T620 може підтримувати до 768 ГБ пам'яті при використанні завантажених модулів пам'яті об'ємом 32 ГБ на всі канали пам'яті.[4]

Місце зберігання

Корпус *Dell* T620, спереду має можливість монтажу восьми 3,5 дюймових дисків *SAS / SATA* в стійку. Також є опція для 2,5-дюймових твердотільних накопичувачів *PCIe*. З певною конфігурацією сховища і двома встановленими ЦП, система підтримує до 48 ТБ внутрішнього сховища. Всі жорсткі диски розташовані за замикається лицьовою панеллю. Вибір додаткових *RAID*-контролерів *PERC*8 забезпечує продуктивність і додаткові параметри *RAID*.

Можливості розширення

Для збільшення обчислювальної потужності або розгортання інфраструктури віртуальних робочих столів (*VDI*) система забезпечує підтримку до чотирьох додаткових внутрішніх прискорювачів обробки графіки з одинарної або подвійної шириною по 300 Вт.Задня панель має 7 слотів *PCIe* 3.0 які підтримують додаткові контролери зберігання, *LOM* або багатоядерних прискорювачів *GPU* від *Nvidia* і *AMD.*Якщо пристрій має один процесор, підтримуються тільки дві відеокарти.
Є також кілька роз'ємів *USB* і відео роз'єм для підтримки ряду зовнішніх пристроїв.

Wi-Fi адаптер *TP-LINK Archer T4U Plus AC*1300 є зовнішнім *USB*-адаптером для підключення до бездротових мереж на швидкості *AC*1300, що може досягати швидкості до 867 Мбіт/с на частоті 5 ГГц та до 400 Мбіт/с на частоті 2.4 ГГц.(див. рис.2.9)

Рис.2.9. Мережевий адаптер *TP-LINK Archer T4U Plus AC1300*

Адаптер підтримує технологію *MU-MIMO*, ця технологія дозволяє передавати та отримувати дані одночасно на кількох пристроях, що забезпечує більш стабільне та швидке з'єднання.

Адаптер має дві зовнішні антени, які покращують якість з'єднання та забезпечують кращий прийом та передачу сигналу. Також він оснащений роз'ємом USB 3.0, що дозволяє передавати дані з вищою швидкістю, ніж *USB* 2.0.

*TP-LINK Archer T4U Plus AC*1300 підтримує такі види протоколів безпеки, такі як *WEP*, *WPA/WPA2*, та *WPA-PSK/WPA2-PSK*, що забезпечує надійний захист мережі. Встановлення та налаштування адаптера є досить простим завдяки наявності інтуїтивно зрозумілого інтерфейсу драйвера. На підприємстві використовуються комп'ютери *ARTLINE Business* B48v02(див. табл. 2.1)

Таблиця 2.1

Характеристики комп’ютера *ARTLINE Business B48v02*

Характеристики	Опис
Процесор	*Intel Core* i5-10400F
Оперативна пам'ять	8 ГБ *DDR4*
Жорсткий диск	1 ТБ *HDD*
SSD	256 ГБ
Відеокарта	*NVIDIA GeForce GTX* 1650
Операційна система	*Windows 10 Pro*
Роздільна здатність екрану	1920 x 1080 (*Full HD*)
Величина екрану	23.8 дюйма
Мережеві інтерфейси	*Ethernet*, *Wi-Fi*, *Bluetooth* 5.0
Порти введення/виведення	*USB* 3.2 *Type-C*, 2 x *USB* 2.0, 2 x *USB* 3.2 *Gen* 1, *HDMI*, *DisplayPort*, *RJ*-45 *Ethernet*, аудіо вихід/вхід
Додаткові характеристики	клавіатура та миша в комплекті, підтримка двох моніторів

Крім комп’ютерів підприємство має 13 ноутбуків *Lenovo IdeaPad* 115IGL7

Ноутбук *Lenovo IdeaPad* 115IGL7 має компактний та легкий дизайн, що дозволяє зручно переносити його з місця на місце. Ноутбук має достатньо потужний процесор та достатньо оперативної пам'яті для роботи з офісними документами.

Підприємство має 4 принтери *HP LaserJet* M111a (7MD67A)

HP LaserJet M111a - це чорно-білий лазерний принтер, який призначений для друку документів в домашніх умовах або в невеликих офісах.

Підприємство має 2 сканери *Canon CanoScan LiDE* 300

Canon CanoScan LiDE 300 - це плоскодзеркальний сканер, який призначений для сканування фотографій, документів та інших матеріалів.

2.4 Програмне забезпечення

Підприємство “*Computer Service*” має різні відділи які займаються конктретними задачами тому використовують спеціальні програми для виконання завдань:

У фінансовому відділі офісу використовуються різні програмні засоби для ефективної роботи з даними та документами.

Основні програми:

1. *Microsoft Excel* - це програма для створення документів, яка дозволяє проводити розрахунки, аналізувати дані та створювати звіти. Є необхідним інструментом для бухгалтерів та фінансових аналітиків.

2. *QuickBooks* - це програма використовується для обліку фінансів та бухгалтерської звітності. Воно дозволяє стежити за доходами та витратами, формувати рахунки-фактури та звіти про баланс та прибуток.

3. *Google Docs* - це безкоштовний онлайн-сервіс, який включає в себе текстовий редактор, електронну таблицю та презентаційний інструмент. Це дозволяє працювати з документами в реальному часі та забезпечує легкий доступ до них з будь-якого місця.

WinRAR – це програма для створення та розпаковування файлових архівів на ОС *Windows*. Підтримує багато форматів архівів, включаючи *RAR, ZIP, 7Z, TAR*.

ISO та інші. *WinRAR* має високий ступінь стиснення даних, завдяки цьому можна зменшити розмір файлів та скоротити час їх передачі/

Основні програми:

1. *AutoCAD* - це програмний засіб для проектування та креслення в області механіки, електрики та архітектури. Воно дозволяє створювати та редагувати детальні 2D та 3D моделі.

2. *MATLAB* - це програма для виконання математичного моделювання та аналізу даних. Дозволяє створювати та редагувати математичні моделі, проводити аналіз даних та виконувати чисельні обчислення.

Відділ управління персоналом використовує програму *SAP SuccessFactors* для ефективної роботи з даними про працівників та управлінням персоналом.

SAP SuccessFactors - це програмне забезпечення для управління персоналом, яке дозволяє керувати відділом кадрів, займатися плануванням робочих місць, наймом та звільненням співробітників, оцінкою їхньої продуктивності та розвитком кар'єри.

При проектуванні комп’ютерної безпровідної мережі за технологією *Wi-Fi* було використано протокол *DHCP* для автоматичного надання вільних IP – адрес пристроям. Також на першому поверсі було використано захист підключення пристроїв до маршрутизатора (*WPA2 PSK*), на другому поверсі захист підключення використано (*WEP*).

DHCP (*Dynamic Host Configuration Protocol*) - це протокол, ой використовується в комп'ютерних мережах для автоматичного налаштування параметрів мережі на комп'ютерах-клієнтах. *DHCP* дозволяє комп'ютерам отримувати *IP*-адреси, маски мережі, адреси шлюзу мережі та інші параметри автоматично з *DHCP*-сервера в мережі, що значно спрощує налаштування мережі та зменшує можливість помилок. *DHCP*-сервер надає комп'ютеру вільну *IP*-адресу з пулу, а також інші параметри, такі як маска мережі, адреса шлюзу та *DNS*-сервера. *DHCP*-протокол є стандартом, що підтримується різними операційними системами та мережевими пристроями, що робить його універсальним рішенням для автоматичної настройки мережі в різних середовищах.

Висновки до розділу:

В даному розділі було створено план приміщення підприємства, обрано необхідне обладнання для проектованої мережі, розташовано обладнання в приміщенні, реалізовано комп’ютерну мережу підприємства за технологією Wi-Fi у програмі Cisco Packet tracer. Визначено програмні засоби для використання певних задач для кожного відділу підприємства. Налаштовано пристрої для доступу в інтернет та передачі даних між пристроями. Було обрано топологію “зірка” при створенні бездротової комп’ютерної мережі.

РОЗДІЛ 3. МЕТОДИ ЗАХИСТУ *WI-FI* МЕРЕЖ

1.1. Захист інформації

Щоб мінімізувати ризики для вашої бездротової мережі потрібно зробити такі дії:

1. Змінити паролі за замовчуванням. Більшість мережевих пристроїв, включно з бездротовими точками доступу, попередньо налаштовані з паролями адміністратора за замовчуванням для спрощення налаштування. Ці паролі за замовчуванням легко отримати в Інтернеті, тому вони забезпечують лише мінімальний захист. Зміна паролів за замовчуванням ускладнює зловмисникам доступ до пристрою. Використання та періодична зміна складних паролів є першою лінією захисту вашого пристрою.

2. Необхідно обмежити доступ. Доступ до вашої мережі повинні мати лише авторизовані користувачі. Кожен пристрій, підключений до мережі, має адресу керування доступом до медіа (*MAC*-адресу). Потрібно обмежити доступ до вашої мережі, відфільтрувавши ці *MAC*-адреси. Докладні відомості про ввімкнення цих функцій наведено у документації користувача. Також є можливість скористатися гостьовим обліковим записом, який широко використовується у багатьох бездротових маршрутизаторах. Ця функція дозволяє надавати бездротовий доступ гостям на окремому бездротовому каналі з окремим паролем, зберігаючи при цьому конфіденційність ваших основних облікових даних.

Шифрування даних у мережі. Шифрування бездротових даних запобігає їх перегляду будь-ким, хто може отримати доступ до вашої мережі. Існує кілька протоколів шифрування, які забезпечують такий захист. *Wi-Fi Protected Access* (*WPA*), *WPA2* і *WPA3* шифрують інформацію, що передається між бездротовими маршрутизаторами і бездротовими пристроями. *WPA3* наразі є найсильнішим шифруванням. *WPA* і *WPA2* все ще доступні, проте рекомендується

використовувати обладнання, яке спеціально підтримує *WPA3*, оскільки використання інших протоколів може зробити вашу мережу вразливою для зловмисників. [10]

1. Необхідно захистити ідентифікатор набору послуг користувача (SSID). Щоб запобігти легкому доступу сторонніх осіб до приватної мережі, забороняється розповсюджувати свій *SSID*. Усі *Wi-Fi* роутери дозволяють користувачам захищати *SSID* свого пристрою, що ускладнює зловмисникам пошук мережі. Потрібно змінити свій *SSID* на щось унікальне. Якщо залишити його за замовчуванням, потенційний зловмисник зможе визначити тип роутера і, можливо, використати будь-які відомі вразливості.

2. Встановити брандмауер. Встановлення брандмауера на бездротових пристроях (брандмауер на базі хоста), а також у домашній мережі (брандмауер на базі маршрутизатора або модема). Зловмисники, які можуть безпосередньо підключитися до вашої бездротової мережі, можуть обійти мережевий брандмауер - брандмауер на основі хоста додаватиме рівень захисту даних на комп'ютері.

3. Використання антивірусного програмне забезпечення. Встановлення антивірусного програмного забезпечення та регулярне виконання оновлень на комп’ютері для пошуку вірусів. Багато антивірусних програм також мають додаткові функції, які виявляють або захищають від шпигунських та рекламних програм.

4. Використання спільного доступу до файлів. Обмін файлами між пристроями слід вимикати, якщо не потрібен. При необхідності забезпечувати спільний доступ до файлів лише у домашній або робочій мережі, але у загальнодоступних мережах не використовувати. Можливість створення спеціального каталогу для спільного доступу до файлів і обмеження доступу до всіх інших каталогів. Крім того, вам необхідно захистити паролем все, до чого надається спільний доступ.[10]

Постійно оновлювати програмне забезпечення точки доступу. Виробник вашої бездротової точки доступу періодично випускає оновлення та виправлення для програмного забезпечення та мікропрограми пристрою. Обов'язково регулярно

потрібно робити перевірку сайту виробника на наявність оновлень і виправлень для вашого пристрою.

1. Перевірка параметрів безпеки бездротового зв'язку вашого інтернет-провайдера або виробника маршрутизатора. Інтернет-провайдер користувача і виробник маршрутизатора можуть надати інформацію або ресурси, які допоможуть захистити вашу бездротову мережу. Для отримання конкретних пропозиції або інструкції від працівника звертаємось до розділу підтримки клієнтів на сайті.

2. Підключення за допомогою віртуальної приватної мережі (*VPN*). Багато компаній та організацій використовують *VPN*. *VPN* дозволяє працівникам безпечно підключатися до своєї мережі, перебуваючи за межами офісу. *VPN* шифрує з'єднання на стороні відправника та отримувача і не пропускає трафік, який не зашифрований належним чином. [10]

3.2. Технології *WPA* та *WPA2*

WPA, скорочено від *Wi-Fi protected access*, - це стандарт мережевої безпеки, який зараз є обов'язковим для бездротових мереж і захищає їх за допомогою автентифікації та шифрування, замінюючи старішу систему *WEP* (*Wired Equivalent Privacy*).

WPA - це розроблений *Wi-Fi Alliance* стандарт сертифікації безпеки для захисту бездротових комп'ютерних мереж. Стандарт був офіційно прийнятий у 2003 році і був покликаний замінити дротовий еквівалент конфіденційності (*WEP*), який мав багато відомих вразливостей безпеки. Альянс *Wi-Fi* мав намір використовувати WPA як проміжний протокол до розробки більш безпечного Wi-Fi-захищеного доступу 2 (*WPA*2). Згодом *Wi-Fi Alliance* створив кілька версій *WPA*, а саме *WPA*, *WPA*2 і *WPA*3.

WPA вимагає, щоб користувачі вводили пароль для автентифікації, щоб забезпечити захист мереж *Wi-Fi*. Підтримує сервери автентифікації або сервери віддаленого входу з автентифікацією (*RADIUS*). Крім того, шифрує дані краще, ніж *WEP*.*WPA* не вимагає оновлення обладнання бо був створений з урахуванням зворотної сумісності. Користувачі можуть додати *WPA* до апаратного забезпечення через оновлення прошивки. Бездротові комп'ютерні мережі, які

захищає *WPA*, мають попередньо наданий ключ і використовують протокол *TKIP*. *TKIP* використовує шифр *RC*4 для шифрування.

Організації можуть застосовувати стандарт *WPA* в одному з двох режимів, які використовують ці режими у всіх трьох поколіннях *WPA*:

1. *WPA personal*: Має назву *WPA* з попередньо наданим ключем (*WPA-PSK*). Призначений для використання в невеликих або домашніх мережах. Його система легко налаштовується. Однак, якщо пристрій буде скомпрометовано, всі пристрої в мережі повинні змінити свої паролі.[11]

2.*WPA enterprise*: Цей режим призначений для середніх і великих мереж і також відомий як *WPA*-802.1x. Його систему складніше налаштувати. Користувачі повинні використовувати свої особисті дані, щоб приєднатися до мережі через сервер *RADIUS*. Якщо пристрій зламано, адміністратори можуть скасувати доступ до нього незалежно від інших пристроїв. Користувачі *WPA* також можуть зіткнутися з наступними обмеженнями.

Прошивки, випущені до 2003 року, не можуть бути оновлені для підтримки *WPA*. Не працює зі старими операційними системами, такими як *Windows* 95.

WPA Enterprise відносно складніше налаштувати, і звичайним користувачам може знадобитися консультація експерта, що може призвести до додаткових витрат.

Особливості *WPA*

Основні елементи *WPA*:

1. Протокол цілісності тимчасового ключа (*Temporal Key Integrity Protocol, TKIP*)

TKIP - це протокол шифрування, створений *Wi-Fi Alliance* та *IEEE* 802.11i *Task Group* для заміни *WEP* без необхідності заміни застарілого обладнання. Використовує шифр *Rivet Cipher* 4 (*RC*4), як і *WEP*, для шифрування даних і був розроблений для подолання вразливостей *WEP*.

TKIP використовує 128-бітний спільний тимчасовий ключ між бездротовим користувачем і точками доступу (*AP*). Розподіляє нові тимчасові ключі кожні 10 000 пакетів, підвищуючи безпеку мережі. Дає гарантію, що один і той самий

ключ не буде повторно використовуватися для шифрування даних, часто обробляючи зміни в ключах шифрування.

2. Розширений стандарт шифрування (*AES*)

Протокол шифрування *AES* був представлений разом з *WPA*2. *AES* - це стандарт шифрування з симетричним ключем, який використовує три блокові шифри: *AES*-128, *AES*-192 і *AES*-256. У *Wi-Fi* використовується 802.1X або попередньо надані ключі (PSK) для генерації ключів станції для всіх пристроїв.

На відміну від *WEP* і *TKIP*, *AES* сумісний лише з обладнанням, яке реалізує стандарт *AES*. Забезпечує високий рівень безпеки для клієнтів, такий як безпека інтернет-протоколу (*IPSec*). Це найкращий режим шифрування в бездротових мережах, які містять конфіденційні дані.

3. Вбудована автентифікація

Вбудована автентифікація дозволяє користувачам отримувати доступ без необхідності вводити пароль. У цьому режимі комп'ютери автентифікуються за допомогою *RADIUS*. *IP*-адреса і ключі *RADIUS* надаються автоматично. RADIUS IP - це IP-адреса сервера *RADIUS*, а ключ - це *PSK* для сервера *RADIUS*. Це також називається машинною автентифікацією.

Користувачі можуть досягти цього за допомогою розширюваного протоколу автентифікації - безпеки транспортного рівня (*EAP-TLS*). Крім того, певні опції сервера *RADIUS* забезпечують автентифікацію машини за допомогою захищеного розширюваного протоколу автентифікації - *Microsoft Challenge Handshake Authentication Protocol Version* 2 (*PEAP-MSCHAP v*2), включаючи сервер мережевої політики *Windows* (*NPS*).[11]

4. Чотиристороннє рукостискання

Бездротовий клієнт і точка доступу обмінюються повідомленнями під час чотиристороннього рукостискання для створення ключів шифрування. Це безпечний метод автентифікації для мережевої передачі даних. Розроблений таким чином, що точка доступу і бездротовий клієнт можуть індивідуально довести, що кожен з них знає *PSK* або парний головний ключ (*PMK*), не надсилаючи ключ. Він використовує *PMK* для шифрування даних, але *PMK* не передається мережею

5. Перевірка цілісності повідомлення (*MIC*)

Перевірка цілісності повідомлення - це поліпшення безпеки для шифрування *WEP*, яке використовується в бездротових мережах. У *WPA* використовується для запобігання атакам типу "зловмисник посередині". *TKIP* використовується для підтвердження автентичності пакетів у *WPA*. Крім того, у *WPA* використовується лічильник кадрів, щоб уникнути цих атак.

MIC запобігає атакам на зашифровані пакети, відомим як атаки на перестановку бітів. Під час атаки "перекидання бітів" дані перехоплюються, дещо змінюються і повторно передаються. Одержувач приймає повторне повідомлення як справжнє. *MIC* додає кілька байт до кожного пакету, щоб зробити його захищеним від несанкціонованого доступу, і використовує алгоритм хешування, щоб запобігти модифікації даних під час передачі.

Існує три версії технології *WPA* три версії:

- *Wi-Fi Protected Access* (*WPA*)

WPA - це програма сертифікації безпеки першого покоління. Програма заснована на частинах стандарту 802.11i. Стандарт був розроблений як тимчасовий стандарт;

- *Wi-Fi Alliance* для заміни старого *WEP*, який мав багато вразливостей у безпеці. Офіційно прийнятий у 2003 році.*WPA* є зворотньо-сумісним і був розроблений для використання з існуючим застарілим обладнанням, яке використовувало *WEP*;

- *WPA-PSK* використовує 256-розрядні ключі, які значно безпечніші, ніж 64-розрядні та 128-розрядні ключі, що використовуються в *WEP*. Захищає інформацію за допомогою шифрування і вимагає автентифікації від користувача.

Особливості та вдосконалення, впроваджені у *WPA* 1:

- *WPA* використовує *MIC* для захисту заголовка і корисного навантаження, щоб гарантувати, що дані не будуть змінені під час передачі, що підвищує значення. перевірки цілісності (*ICV*);

- гарантує централізовані механізми автентифікації та динамічне управління ключами, змушуючи користувачів входити в систему за допомогою структури 802.1X *EAP*; для запобігання загрозам повторного відтворення.

включено лічильник

Wi-Fi Protected Access 2 (*WPA*2)

*WPA*2 - це програма сертифікації безпеки другого покоління. Заснована на ратифікованому стандарті IEEE 802.11i. Сертифікація *WPA*2 почалася в 2004 році, протокол офіційно був прийнятий в 2006 році на заміну *WPA*.[11]

*WPA*2 може бути корисним для домашніх мереж , але він вразливий для корпоративних мереж . Тому що зловмисники можуть мати доступ до мережі, захищеної *WPA*2. Після доступу до мережі вони можуть отримати доступ до паролів. Атаки за допомогою словника є найбільш вразливою частиною *WPA*2 для паролів. Вигляд підключених пристроїв з використанням *WPA*2 показано на рис.3.1.

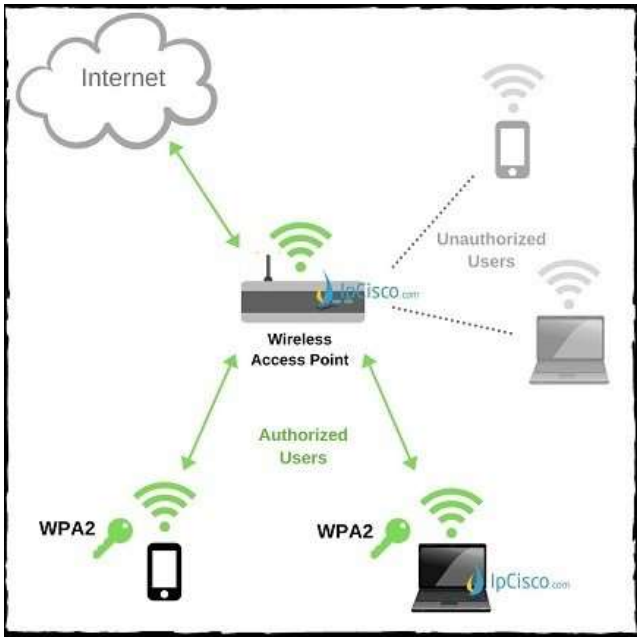


Рис.3.1. Вигляд підключення пристроїв за *WPA*2

*WPA*2 є зворотньо сумісним з бездротовими клієнтами з підтримкою *WPA*. За допомогою *WPA* і *WPA*2 можна підвищити рівень безпеки на маршрутизаторі

*WPA*2 використовує шифрування *AES* і впроваджує механізми шифрування *CCMP* і *TKIP*.

Персональний *WPA* використовує попередньо наданий ключ для перевірки початкових облікових даних користувачів. Мережі *Wi-Fi*-захищеного доступу 2 з попередньо наданим ключем (*WPA-PSK*) мають одну парольну фразу, яка є спільною для всіх користувачів. *Enterprise WPA*2 використовує *IEEE* 802.1X і EAP

як протоколи шифрування. *WPA*2 використовує шифрування *AES* і впроваджує механізми шифрування *CCMP* і *TKIP*.

Персональний *WPA* використовує попередньо наданий ключ для перевірки початкових облікових даних користувачів. Мережі *Wi-Fi*-захищеного доступу 2 з попередньо наданим ключем (*WPA-PSK*) мають одну парольну фразу, яка є спільною для всіх користувачів. *Enterprise WPA*2 використовує *IEEE* 802.1X і *EAP* як протоколи шифрування.

Хоча сертифікація *WPA*2 має менше вразливостей, ніж її попередник, все ж може бути піддана специфічним кіберзагрозам. Щоб мінімізувати вразливості постачальники надають патчі безпеки для *WPA*2.

Користувачі можуть легко підключитися до мережі *Wi-Fi*, натиснувши кнопку або ввівши *PIN*-код, скориставшись функцією захисту *Wi-Fi* (WPS), яка постачається разом з *WPA*2. Бездротовий клієнт автоматично налаштовує ідентифікатор набору послуг (*SSID*) і *PSK*.

Основні функції і покращення, представлені в *WPA*2:

- на відміну від *WEP* і *WPA*, які використовували шифрування *RC*4, *WPA*2 використовує протоколи шифрування *AES-CCMP*;

- *WPA*2 вирішує проблеми з проникненням, які були у його попередника, *WPA*, використовуючи режим лічильника з протоколом шифрування блочного ланцюжка повідомлень з кодом автентифікації (*CCMP*) разом з *TKIP*;

- покращення шифрування автентифікації з більш надійними налаштуваннями за замовчуванням, які сприяють надійності та адаптивності.[11]

Wi-Fi Protected Access 3 (*WPA*3)

*WPA*3 - це третя схема сертифікації мережевої безпеки. Пропонує покращену безпеку в порівнянні зі своїми попередниками. *WPA*3 також використовує *AES*, замінив *CCMP* на протокол Галуа/лічильник (*GCMP*). Довжина ключа для *AES* збільшилася. *WPA3* personal використовує 128- або 192-розрядні ключі, тоді як *WPA*3 enterprise використовує 192-розрядні ключі.

При передачі криптографічних ключів між маршрутизаторами і пристроями використовується механізм автентифікації 384-бітних хешованих повідомлень. Також містить додаткові функції, які підвищують безпеку Wi-Fi,

забезпечують вищу криптографічну стійкість і дозволяють більш сувору автентифікацію.

Основні функції та покращення, представлені в *WPA*3:

- замінює *WPS*, який легко використовується з протоколом забезпечення пристроїв *Wi-Fi* (*DPP*). За допомогою *DPP* користувачі можуть приєднуватися до мережі без введення паролів, використовуючи для автентифікації мітки ближнього зв'язку (*NFC*) або *QR*-коди.

- на відміну від *WPA* і *WPA*2, які використовують протокол шифрування рукостискання, має загрози від офлайн-атак, *WPA*3 використовує одночасну автентифікацію рівних (*SAE*), стійку до офлайн-атак.

- пропонує пряму секретність, яка дає гарантію, що бездротовий трафік не може бути розшифрований згодом, навіть за допомогою *PSK*. У *WPA* і *WPA*2 бездротовий трафік може бути перехоплений і розшифрований пізніше за допомогою *PSK*.

*WPA*3 робить захищені кадри керування (*PMF*) обов'язковими, на відміну від *WPA*2, де вони є необов'язковими. *PMF* захищає багатоадресні керуючі кадри від підробки та одноадресні керуючі кадри від підслуховування та підробки.

Відбувається заміна відкритої автентифікації на опортуністичне бездротове шифрування (*OWE*). *OWE* гарантує, що трафік шифрується між бездротовим клієнтом і точкою доступу за допомогою обміну Діффі-Хеллмана. Кожен бездротовий клієнт використовує різні ключі, таким чином гарантуючи, що інші клієнти не зможуть розшифрувати ваш трафік.[11]

Важливість *WPA*

Найважливішою перевагою *WPA* є високий рівень безпеки, який забезпечує для мереж. Причина важливості використання даної технології:

1. Покращує безпеку бездротової мережі

WPA забезпечує користувачам надійний та покращений захист бездротової мережі. *WPA* вимагає, щоб користувачі проходили автентифікацію перед доступом до бездротових локальних мереж (*WLAN*). Алгоритм *TKIP* в *WPA* виконує *MIC* для корисного навантаження і заголовків повідомлень, щоб гарантувати, що пакети даних є автентичними. На відміну від свого попередника, *WEP*, не використовує

дані, роблячи їх нечитабельними для інших і захищаючи інтернет-активність від порушень конфіденційності.

3.3. Шифрування *VPN*

Оскільки для розшифрування даних, що передаються, потрібен ключ шифрування, зловмисники, які посягають на кібербезпеку, з більшою ймовірністю будуть переслідувати більш легку ціль. Шифрування *VPN* має вирішальне значення для зменшення ризику компрометації ваших даних під час їх передачі через Інтернет завдяки кодуванню пакетів даних. Шифрування ваших конфіденційних даних під час передачі та приховування вашої *IP*-адреси є основним завданням VPN для захисту конфіденційності користувача в Інтернеті.

VPN не шифрує текстові повідомлення *SMS* (стандартна служба обміну повідомленнями). Ці типи повідомлень передаються через стільникову мережу оператора вашого мобільного пристрою, а не через Інтернет. *VPN* шифрує інтернет-трафік в Інтернеті або спілкування через Інтернет.[11]

VPN використовується споживачами та організаціями для забезпечення віддаленого доступу, який захищається шляхом зміни вашої *IP*-адреси та шифрування інтернет-трафіку. Це робить користувача анонімним в Інтернеті і гарантує, що ваша діяльність в Інтернеті є приватною, щоб забезпечити вашу безпеку. Дані на ваш пристрій і з нього проходять через зашифрований *VPN*-тунель до *VPN*-сервера, який слугує шлюзом до загальнодоступного Інтернету. Шифрування та шифри - це ключ до безпеки *VPN*. Протокол *VPN* - це процес, який використовується для створення захищеного зашифрованого шляху між двома комп'ютерами за допомогою зашифрованого *VPN*-з'єднання. Протоколи *VPN* відрізняються у різних постачальників послуг *VPN*, що може впливати на безпеку, швидкість, можливості та вразливості. Нижче наведено найпоширеніші протоколи *VPN*:

OpenVPN - це дуже безпечний протокол *VPN*, який вважається галузевим стандартом, що використовується сьогодні. *OpenVPN* - це технологія з відкритим вихідним кодом, яка легко налаштовується. Використовуються бібліотека *OpenSSL* і протоколи безпеки транспортного рівня (*TLS*), що робить її надійним і

безпечним рішенням

Шифрування *OpenVPN* складається з шифрування каналу даних і шифрування каналу управління. Шифрування каналу даних складається з шифру та хеш-автентифікації для захисту даних. Шифрування каналу управління або *TLS*-шифрування складається з шифру, хеш-автентифікації та шифрування рукостисканням для захисту з'єднання між вашим пристроєм і VPN-сервером.

Алгоритм або шифр кодує дані, безпечний хеш-алгоритм (*SHA*) перевіряє автентичність даних і *SSL*/*TLS*-з'єднання, а шифрування "рукостискання" захищає з'єднання. Включення ключів шифрування *Perfect Forward Secrecy* або ефемерних ключів шифрування шляхом генерації унікальних приватних ключів та їх утилізації після кожного *TLS*-з'єднання слугує додатковим рівнем безпеки. Надійне шифрування на обох каналах разом з *Perfect Forward Secrecy* робить *OpenVPN* операційно дуже безпечним протоколом;

L2TP/*IPSec*

Протокол тунелювання другого рівня (*L2TP*) зазвичай реалізується в парі з *IPSec*, створюючи захищене з'єднання між вашим пристроєм і *VPN*-сервером. *IPSec*, або безпека інтернет-протоколу, - це протокол захисту пакетів на мережевому рівні, який надає методи шифрування частини даних кожного пакета і його заголовка для забезпечення конфіденційності даних. Для роботи *IPSec* в Інтернеті між пристроєм-відправником і пристроєм-одержувачем має бути спільний відкритий ключ. Ключовими моментами, на які слід звернути увагу при використанні цього протоколу, є те, що брандмауери можуть легко заблокувати порт, який використовується *L2TP/IPSec*, а також те, що слід уникати використання попередньо наданих ключів (*PSK*).

SSTP

Secure Socket Tunneling Protocol (*SSTP*) - це *VPN*-протокол, що належить Microsoft і використовується переважно в операційних системах *Windows*. Хоча він надає більшість функцій, які надає *OpenVPN*, він не є технологією з відкритим вихідним кодом. Він також може використовуватися в *Linux*, але не так часто використовується на комп'ютерах Mac. *IKEv2/IPSec*

Internet Key Exchange v2 (IKEv2) також використовується в парі з *IPSec*, як

згадувалося вище, і особливо часто використовується для мобільних пристроїв.

IKEv2/IPSec успішно відновлює з'єднання, коли воно тимчасово втрачено або розірвано, що робить його надійним і безпечним протоколом для мобільних пристроїв.[11]

WireGuard

WireGuard - відносно новий протокол *VPN*, який конкурує з *OpenVPN*. Це технологія з відкритим вихідним кодом, яка фокусується на швидкості та надійному шифруванні і набуває все більшої популярності.

PPTP

Протокол тунелювання "точка-точка" - це метод, який використовується для створення *VPN* через комутоване з'єднання. Ключовим моментом тут є те, що цей протокол не такий безпечний, як інші протоколи, згадані вище, оскільки його легше зламати.

Шифрування використовує математичну функцію, яка бере читабельний відкритий текст і випадковим чином перетворює його на нечитабельний зашифрований текст, який неможливо зрозуміти, якщо його не розшифрувати назад у читабельний відкритий текст. Шифрування захищає дані від читання або компрометації в разі їх втрати або крадіжки. Той, хто отримує зашифровані дані, не може їх прочитати або зробити з ними щось, якщо у нього немає ключа шифрування, щоб розблокувати або розшифрувати їх до читабельної форми. Детальніше про те, чому шифрування необхідне, читайте в нашому блозі. Ключові елементи шифрування включають в себе наступне:

Алгоритм шифрування - математична функція або шифр, який використовується для шифрування та розшифрування даних.

Ключ шифрування - подібно до пароля, ключ необхідний для доступу до зашифрованих даних або їх розшифрування.

Довжина ключа - чим більша довжина ключа, тим він надійніший, оскільки має більше можливих комбінацій, і тим менша ймовірність його зламу під час атаки грубої сили. Наприклад, ключ довжиною 256 біт є стійкішим, ніж 128 біт, і його буде довше зламати. Два найпоширеніші типи шифрування - з приватним ключем, що базується на симетричному алгоритмі шифрування, та з відкритим

ключем, що базується на асиметричному алгоритмі шифрування.

Детальніше про шифрування даних читайте в нашому блозі про шифрування даних.

Симетричне

Симетричний алгоритм шифрування використовує один і той же ключ для шифрування відкритого тексту і розшифрування зашифрованого. Відправник і одержувач повинні мати один і той же ключ, щоб спілкуватися один з одним. Прикладами такого типу алгоритмів або шифрів є *Advanced Encryption Standard* (*AES*) і *Blowfish.* Національний інститут стандартів і технологій (*NIST*) сертифікував *AES*, і він широко використовується як стандарт симетричного шифрування. Найвищий рівень шифрування, який використовують найкращі *VPN*, - 256-бітний *AES*.[11]

Асиметричне

Асиметричний алгоритм шифрування, також відомий як криптографія з відкритим ключем, використовує два ключі - відкритий і закритий. Відкритий ключ може бути у багатьох користувачів, але, як правило, тільки один користувач знає закритий ключ. Ключі працюють як пара по відношенню один до одного таким чином, що відкритий ключ шифрує, а закритий ключ розшифровує дані. RSA є поширеним прикладом асиметричного шифрування.

Користуючись послугами *VPN*, люди можуть уникнути моніторингу їхньої діяльності в Інтернеті та розкриття їхніх особистих даних. *VPN* підтримують безпечні та приватні тунелі зв'язку між пристроєм та інтернетом за допомогою шифрування тунелю та шифрування потоку даних. *VPN* зберігає анонімність вашої IP-адреси і шифрує всі відправлені та отримані дані.

Хоча існує кілька різних протоколів *VPN, OpenVPN* виділяється як галузевий стандарт. Використання стійкого шифрування, такого як *AES*-256, як на каналах передачі даних, так і на каналах управління, в поєднанні з *Perfect Forward Secrecy,* робить *OpenVPN* дуже безпечним і надійним протоколом. Зрештою, безпека методів шифрування, що використовуються з обраним протоколом *VPN*, залежить від збереження секретності ключів.

3.4. Налаштування безпеки маршрутизатора

Необхідно на підключеному до *Archer C64* пристрої використати будь-який браузер, набрати адресу *tplinkwifi.net* або 192.168.0.1 . Після цього потрібно ввести логін та пароль.(рис.3.2)

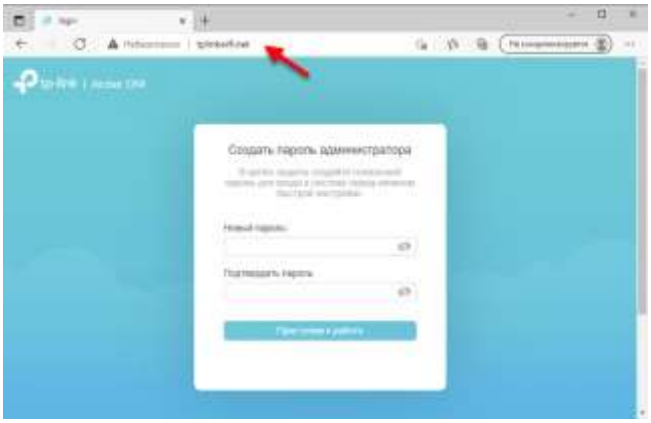
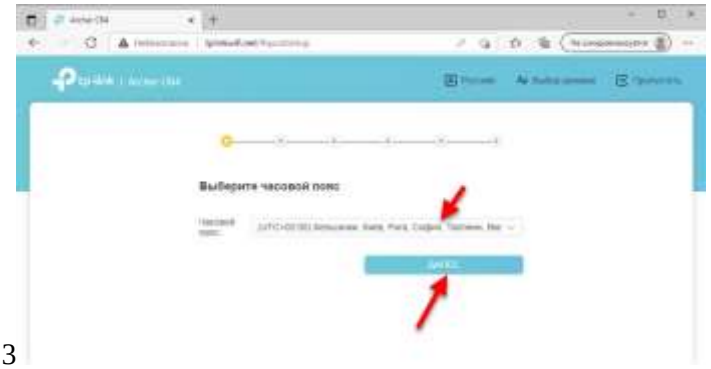


Рис.3.2. Створення нового пароля

Далі потрібно встановити свій часовий пояс.(див. рис.3.3)



3

Рис.3.3. Налаштування часового поясу

Потрібно обрати свого інтернет-провайдера зі списку. Спочатку країну, місто, провайдера і тип підключення до інтернету.(див. рис.3.4)

Рис.3.4. Вибір типу підключення

Вибір провайдера під час налаштування роутера. Якщо вашого провайдера у списку немає – треба обрати галочку "Виберіть тип підключення вручну".

Необхідно обрати тип підключення, який використовує ваш провайдер і натискаємо "Далі". Якщо не знаєте який вибрати - дивіться договір про підключення до інтернету, або телефонуйте в підтримку провайдера.(див. рис.3.5)

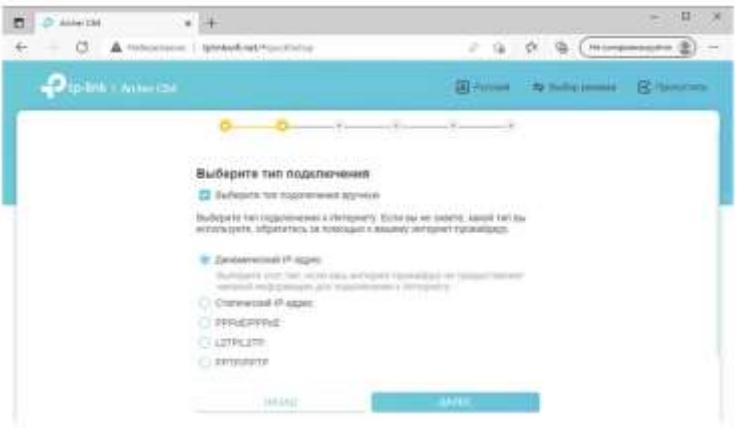


Рис.3.5. Тип підключення

Якщо у вас Динамічний *IP* - просто вибираємо його і натискаємо "Далі", додаткове налаштування не потрібне. Якщо Статичний *IP* - на наступному кроці знадобиться прописати адреси, які видає інтернет-провайдер. Якщо *PPPoE* - потрібно буде вказати ім'я користувача і пароль. Ці дані так само видає провайдер. Якщо ж у вас *L2TP* або *PPTP*, то крім імені користувача (логіна) і пароля, потрібно ще дізнатися і прописати адресу сервера.[12]

У випадку з Динамічною *IP*-адресою роутер запропонує клонувати, або прописати вручну *WAN MAC*-адресу. Це потрібно робити тільки в тому разі, якщо ваш провайдер робить прив'язку за *MAC*-адресою.(див. рис.3.6)

Рис.3.6. Динамічний IP-адрес

Налаштування *Wi-Fi* мережі. Тут потрібно змінити ім'я мережі воно ж *SSID* (це за бажанням) і змінити пароль. Так само за необхідності можна відключити *Wi-Fi* мережу в одному з діапазонів. Наприклад, якщо не потрібна мережа в діапазоні 2.4 ГГц.(див. рис.3.7)

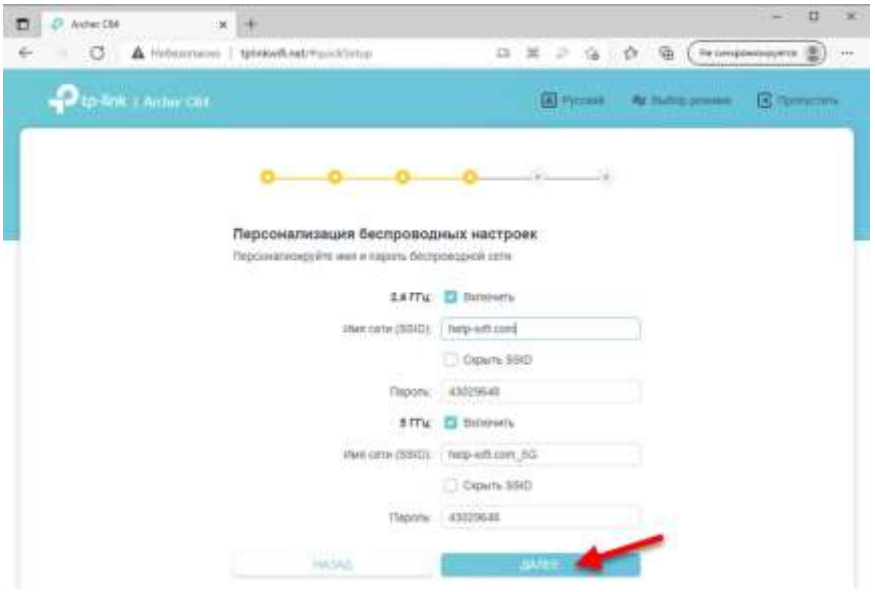


Рис.3.7. Персоналізація безпровідних налаштувань

Роутер збереже налаштування *Wi-Fi* і попросить заново підключитися до бездротової мережі. Уже з новим ім'ям (якщо його змінювали) і паролем. Необхідно підключитись (якщо спочатку були підключені по *Wi-Fi*) і натиснути на кнопку "Далі".(див. рис.3.8)

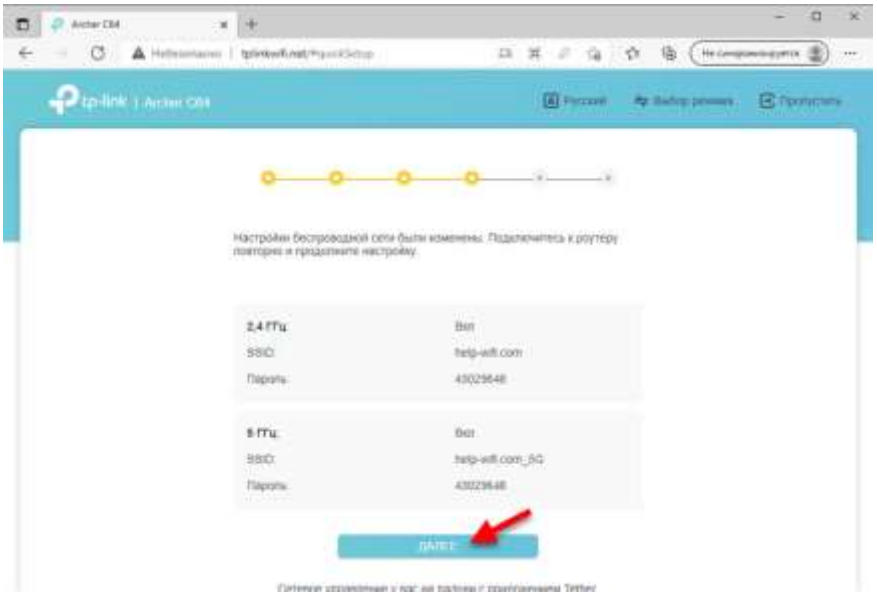


Рис.3.8. Збережені налаштування

Після перевірки інтернет-з'єднання з'явиться вікно з пропозицією увійти, або зареєструватися в сервісі "Хмара TP-Link". Якщо у вас буде обліковий запис, то користувачі зможуть виконати в нього вхід у налаштуваннях роутера і в застосунку TP-Link Tether, після чого керувати роутером віддалено (через інтернет). Це налаштування можна пропустити і пізніше налаштувати все в панелі управління.[12]

Відкриється веб-інтерфейс роутера TP-Link Archer C64, звідки можна виконати налаштування додаткових функцій, подивитися список підключених пристроїв, змінити системні налаштування тощо.(див. рис 3.9)

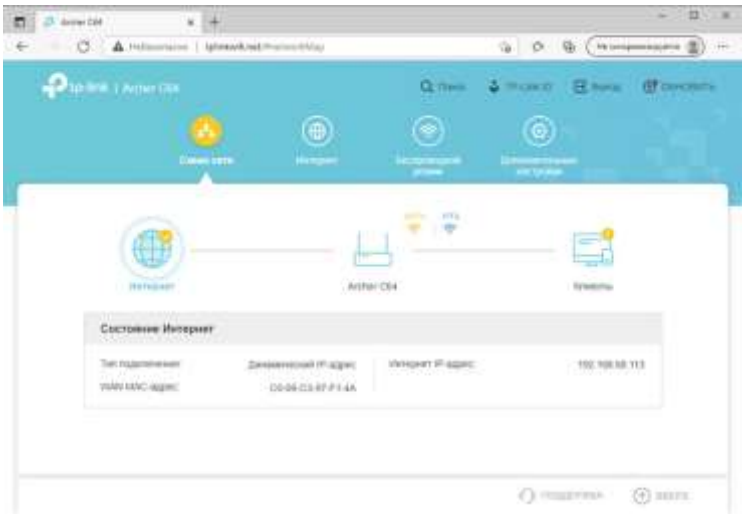


Рис.3.9. Результат налаштування маршрутизатора

Висновки до розділу: У цьому розділі було розглянуто декілька аспектів забезпечення безпеки інформації в мережах. Спочатку було розглянуто загальні питання захисту особистих даних. Важливо мати на увазі, що виявлення потенційних загроз є так само важливим, як і захист від них. Далі було проаналізовано технології *WPA* та *WPA*2, які є стандартами бездротового захисту мережі *Wi-Fi*. Ці технології забезпечують стійкий рівень захисту від несанкціонованого доступу до мережі. Для забезпечення високого рівня безпеки в мережах також можна використовувати технологію шифрування *VPN*. Це дозволяє захистити передачу даних між різними точками мережі, що особливо важливо при використанні відкритих мереж. Нарешті, було розглянуто налаштування безпеки маршрутизатора. Це включає в себе зміну пароля адміністратора, використання технології *WPA*2 для захисту *Wi-Fi* мережі та налаштування фільтрації адрес *MAC*.

ВИСНОВКИ

Для поліпшення наявної мережі на підприємстві було розроблено бездротову мережу *Wi-Fi* зі стандартом 802.11ac, що включає встановлення бездротової точки доступу і бездротових адаптерів на комп'ютерах. Також є можливість використання ноутбуків та персональних комп’ютерів Зменшення кількості кабелів досягається завдяки тому, що співробітники підключаються до мережі без кабелів, принтери використовуються у мережі, і найголовніше, гості матимуть доступ до мережі Інтернет. Бездротова мережа реалізована за стандартом *IEEE* 802.11ac. Основою бездротової мережі є точка доступу (*Access Point*), яка підключається до певної наземної мережевої інфраструктури (каналів Інтернет-провайдера) та забезпечує передачу радіосигналу. Зазвичай точка доступу складається з приймача, передавача, інтерфейсу для підключення до провідної мережі та програмного забезпечення для налаштування.

Була розроблена схема захисту бездротової мережі, яка включає вибір типу шифрування, його версії та методу, а також встановлення пароля для підключення до мережі. Маршрутизатор був налаштований відповідно до вибраної схеми захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1.Веб сторінка: https://www.elprocus.com/how-does-wifi-technology-work/

2. https://tukles.biz.ua/vsi-standarti-wi-fi-merezh/

3.Інформаційний ресурс: https://www.aplustopper.com/wireless-network-advantages-and-disadvantages/

4. https://server-shop.ua/ua/about-computer-networks.html

5.Веб ресурс: https://www.networkworld.com/article/3238664/80211x-wi-fi-standards-and-speeds-explained.html

6.https://moluch.ru/archive/113/29345/

7. https://kovelpost.com/blogs/213

8. https://ua.phhsnews.com/articles/howto/the-difference-between-wep-wpa-and-wpa2-wi-fi-passwords.html

9. https://wifi-help.net/tip-bezopasnosti-i-shifrovaniya-besprovodnoj-seti-kakoj-vybrat

10. https://www.cisa.gov/news-events/news/securing-wireless-networks

11. https://www.spiceworks.com/tech/networking/articles/wpa-wifi-protected-access/

12. https://help-wifi.com/tp-link/wi-fi-router-tp-link-archer-c64-obzor-podklyuchenie-i-nastrojka/