Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: Метод підвищення якості передачі сигналів в бездротових локальних мережах

Виконав(ла): студент(ка) 6 курсу, групи РРм-61
спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

	(підпис)	Бекус Р.В. (прізвище та ініціали)
Керівник	(підпис)	Дунець В.Л. (прізвище та ініціали)
Нормоконтроль	(підпис)	Хвостівська Л.В. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Дунець В.Л. (прізвище та ініціали)
Рецензент	(підпис)	(прізвище та ініціали)

Тернопіль
2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра радіотехнічних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дунець В.Л.
(підпис) (прізвище та ініціали)
«__» _____ 2020 р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

студенту Бекусу Ростиславу Володимировичу
(прізвище, ім'я, по батькові)

1. Тема роботи Метод підвищення якості передачі сигналів в бездротових локальних мережах

Керівник роботи Дунець Василь Любомирович, к.т.н.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «24» листопада 2020 року № 4/7-870

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Об'єкт дослідження: безпровідні локальні мережі на основі стандартів 802.11 ac та 802.11 n; Предмет дослідження: безпровідні технології

4. Зміст роботи (перелік питань, які потрібно розробити)
1. Аналітична частина
2. Основна частина
3. Науково-дослідна частина
4. Охорона праці та безпека в надзвичайних ситуаціях

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

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та	Зелінський І.М., доц. каф. ПВ		
безпека в надзвичайних	Клепчик В.М., стар. викл. каф. ОХ		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання		
2	Аналіз завдання		
3	Виконання розділу 1		
4	Виконання розділу 2		
5	Виконання розділу 3		
6	Виконання розділу 4		
7	Оформлення пояснювальної записки		
8	Оформлення графічного та презентаційного матеріалу		
9	Перевірка роботи на антиплагіат		
10	Попередній захист		
11	Захист		

Студент _____ *Бекус Р.В.*
(підпис) (прізвище та ініціали)

Керівник роботи _____ *Дунець В.Л.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод підвищення якості передачі сигналів в бездротових локальних мережах» // Кваліфікаційна робота // Бекус Ростислав Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, група РРм-61 // Тернопіль, 2020 // с. – 62, рис. – 13, табл. – 6, додат. – 1, бібліогр. – 17.

Ключові слова:

БЕЗДРОТОВІ ТЕХНОЛОГІЇ, АНАЛОГОВИЙ СИГНАЛ, ДОСЛІДЖЕННЯ, ДИСКРЕТНІ ДАНІ, МОДУЛЯЦІЯ, WPAN, WLAN, WMAN, WWAN, WI-FI, IEEE, ТОЧКА ДОСТУПУ, АДАПТЕР, АУТЕНТИФІКАЦІЇ, ШИФРУВАННЯ, WPA2, WARDRIVING, 802.11AC, MU-MIMO

В кваліфікаційній роботі здійснено дослідження проблем і переваг передачі сигналу в мережі WLAN на прикладі стандарту 802.11ac в порівнянні із стандартом 802.11n.

ANNOTATION

Theme of qualification work: "Method of improving the quality of signal transmission in wireless local area networks" // Qualification work // Bekus Rostislav Volodimirovich // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Applied Information Technologies and Electrical Engineering, group PPM-61 // Ternopil, 2020 // with. - 62, fig. - 13, table. - 6, appendix. - 1, bibliogr. - 17.

Keywords: WIRELESS TECHNOLOGY, ANALOG SIGNALS, RESEARCH, DISCRETE DATA, MODULATION, WPAN, WLAN, WMAN, WWAN, WI-FI, IEEE, ACCESS POINTS, ADAPTERS, AUTHENTICATION, ENCRYPTION, WPA2, WARDRIVING, 802.11AC, MU-MIMO

In the qualification work the research of problems and advantages of signal transmission in WLAN network on the example of 802.11ac standard in comparison with 802.11n standard is carried out.

ЗМІСТ

ВСТУП

Актуальність роботи. Актуальність обраної теми випускної роботи бакалавра обумовлена неможливістю існування сучасного інформаційного середовища без використання Wi-Fi технологій. Складно уявити наше життя в сучасних реаліях без бездротових мереж. На поточний момент нам доступно безліч бездротових технологій, таких як Wi-Fi, Bluetooth, WiMAX, ZigBee, GPRS, NFC, LTE і т.д. У даній роботі основна увага буде приділена бездротових локальних мереж зокрема стандарту 802.11 ac.

Бездротові технології містять в собі величезний потенціал розвитку, що впливає на підвищення стабільності та ефективності функціонування всіх системи країни, що в сукупності визначає соціально-технічну базу модернізації. Основне завдання при проектуванні бездротових локально обчислювальних мереж - рішення проблем завадостійкості, а також забезпечення належного рівня швидкості передачі і безпеки даних.

У радіусі роботи і скорості передачі інформації в бездротовій мережі Wi-Fi позначається дуже багато чинників, починаючи від безлічі пристроїв, що створюють випромінювання (наприклад, мобільні телефони, мікрохвильові печі, бездротові гарнітури), до штучних перешкод потрапляють в простір поширення радіохвилі.

Метод який використовується для подавлення цих моментів передбачає експлуатацію все більш потужного обладнання та застосування найсучасніших технологій безпровідного зв'язку.

Метою роботи є дослідження та підвищення якості передачі сигналів у безпровідних мережах. Для досягнення поставленої мети потрібно розв’язати наступні завдання:

1. Провести огляд бездротових мереж та класифікацію бездротових технологій.

2. Проаналізувати механізм передачі сигналів у бездротових локальних мережах.

3. Оцінити якість передачі сигналів стандарту 802.11 ac у подібності з стандартом 802.11 n

4. Виявити проблеми та оцінити способи підвищення якості передачі сигналів у бездротових мережах.

Об’єкт дослідження: бездротові локальні мережі на основі стандартів 802.11 ac та 802.11 n.

Предмет дослідження: бездротові технології.

Методи дослідження: експеримент, метафізичний метод пізнання, порівняльний аналіз, опис, перерахунок, методи статистичних порівнянь.

Наукова новизна одержаних результатів. Здійснено огляд основних стандартів бездротового зв'язку та проведено порівняння продуктивності стандарту 802.11 ac у порівнянні з стандартом 802.11 n. Виявлено перевагу в швидкості передачі інформації і зони покриття при багатоканальної роботі.

Публікації.

Викладені в роботі результати доповідалися та обговорюватися на 3-ій Всеукраїнській науково-практичній конференції молодих учених та студентів «Сучасні інформаційні системи та технології» (м.Херсон, 30 листопада 2020 р.).

РОЗДІЛ 1
АНАЛІТИЧНА ЧАСТИНА

1.1. Основи передачі інформації в безпровідних технологіях

Точкою відліку для історії бездротових технологій прийнято вважати момент трансляції радіосигналу на відстані в кінці 19 століття. Після чого протягом півстоліття з'явилися такі технології як радіо телетрансляція з частотною модуляцією, бездротові телефони, мережі зв’язку. У підсумку в 90-х роках бездротові технології стали невід'ємною частиною нашого життя.

Бездротові технології - по суті, є окремим випадком інформаційних технологій, який використовується коли необхідно передати сигнал між двома і більше об'єктами, при цьому не використовуючи дроти для їх зв'язку. Для такого типу передачі використовується безліч випромінювань, таких як інфрачервоне, оптичне, лазерне, а також радіохвилі. Нас цікавить спосіб за допомогою радіохвиль, далі будуть розглянуті основні поняття характерні для цього методу.

При поданні сигналу у вигляді функції часу, він може бути двох видів: аналоговий та цифровий. Аналоговий сигнал – це фізичний процес, який служить носієм перенесення інформації у просторі та часі в якому не буває пауз і розривів, інакше це сигналу з поступовою зміною своєї інтенсивності в часі. Цифровий сигнал представляється у вигляді послідовності дискретних значень, інакше кажучи це сигнал з постійно підтримуваної інтенсивністю певного рівня протягом періоду часу з подальшою зміною на певну величину. Приклади аналогового та цифрового сигналів можна побачити на рис. 1.1.

Періодичний сигнал, тобто сигнал який повторюється у часі з деяким періодом частиною прийнято вважати найпростішим видом сигналу. Наглядним прикладом для аналогового сигналу є синусоїда а для цифрового - меандр які зображені на рис. 1.2.

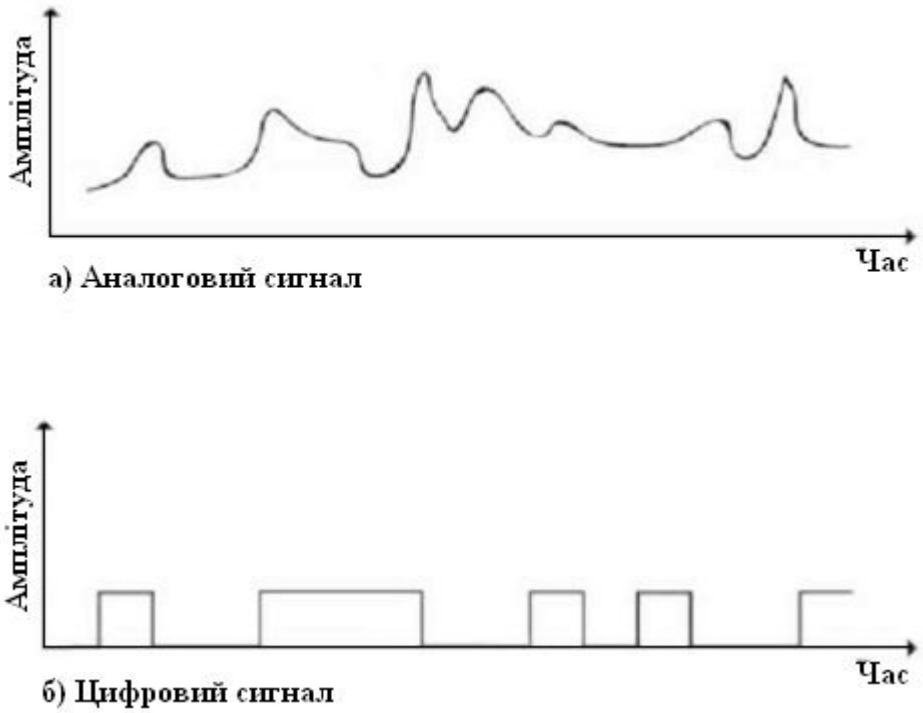


Рисунок 1.1 Схематично зображено сигнали: а) аналоговий, б) цифровий

Математичне визначення: сигнал s (t) є періодично тоді і тільки тоді, коли

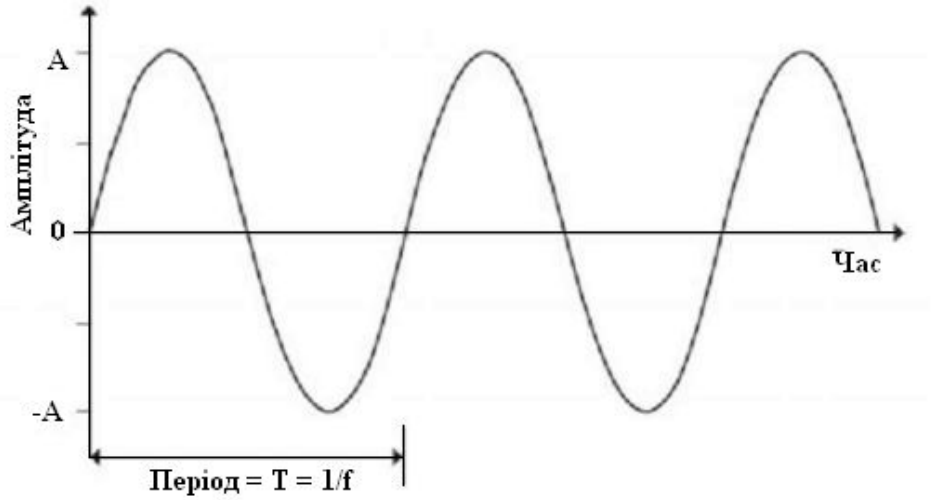
$$s(t+T) = s(t), \text{при} -\infty < t < +\infty$$

де постійна T є період сигналу.

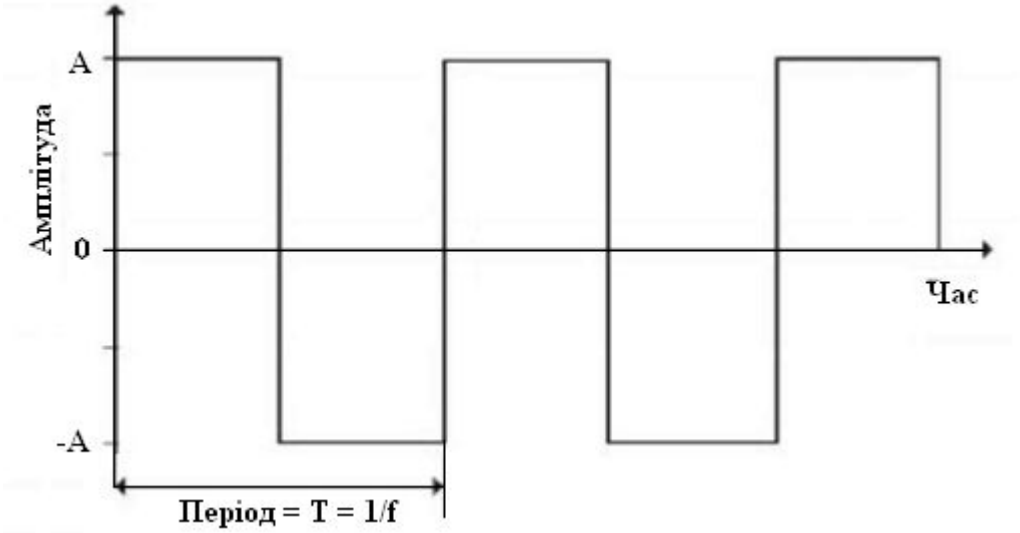
Основоположним аналоговим сигналом вважається синусоїда. Такий сигнал визначається максимальною амплітудою A, фазою φ і частотою f. Максимальна амплітуда вимірюється в вольтах і являє собою інтенсивність сигналу в часі. Темп повторення сигналів є їх частотою і вимірюється в герцах. І нарешті фаза - це міра зсуву за часом в межах T.

Синусоїдальний сигнал представлений в наступному вигляді:

$$s(t) = A\sin(2\pi ft + \varphi).$$



а) Синусоїдальний сигнал



б) Прямокутний сигнал

Рисунок 1.2 Періодичні сигнали

Два синусоїдальних сигнали, один з яких вимірюється в просторі, а другий часу можна співвіднести. Взявши довжину хвилі сигналу λ, припустимо, що швидкість поширення сигналу дорівнює *v*. Тоді період і довжину хвилі можна виразити як: $\lambda = v\ T$, ніж також є співвідношення $\lambda f = v$.

Для отримання електромагнітного сигналу будь-якої форми потрібно застосувати аналіз Фур'є, інакше кажучи поєднати певну кількість синусоїд з відповідними амплітудами, фазами і частотами. Схожим чином будь-який електромагнітний сигнал можна розкласти на періодичні аналогові сигнали.

Область частот, що визначає конкретний сигнал, називається його спектром.

Цифровий сигнал можна представити як:

$$s(t) = \mathrm{A} \times \frac{4}{\pi} \sum_{k=1,3,5\ldots}^{\infty} \frac{\sin(2\pi k f t)}{k}$$

З такого подання, сигнал що містить безкінечне число частотних складових має і безкінечну ширину смуги

Виходячи з вищесказаного, можна вивести наступні міркування. При передачі сигналу через будь-яке середовище він піддається обмеженню переданої ширини смуги від передавальної системи. Більш того вартість передачі збільшується одночасно зі збільшенням переданої смуги. Звідси випливає, що на практиці потрібно апроксимувати інформацію подану у вигляді цифрового сигналу з обмеженням ширини мовлення, однак при такому впливі з'являються спотворення, що викликають перешкоди і труднощі прийому через що з'являються помилок.

В бездротових технологіях використовуються аналогові сигнали (безперервно змінюються електромагнітні хвилі) і цифрові дані (дискретні, текст, числа). Звідси виникає необхідність модуляції, наприклад, для передачі низькочастотного аналогового сигналу (голос) в канал з високочастотної області спектру (телебачення).

В процесі модуляції використовується одна або кілька характеристик сигналу, звідки з'являються три основні технології перетворення цифрового сигналу в аналоговий (рис 1.3)

• Фазова модуляція;

• Амплітудна модуляція;

• Частотна модуляція;

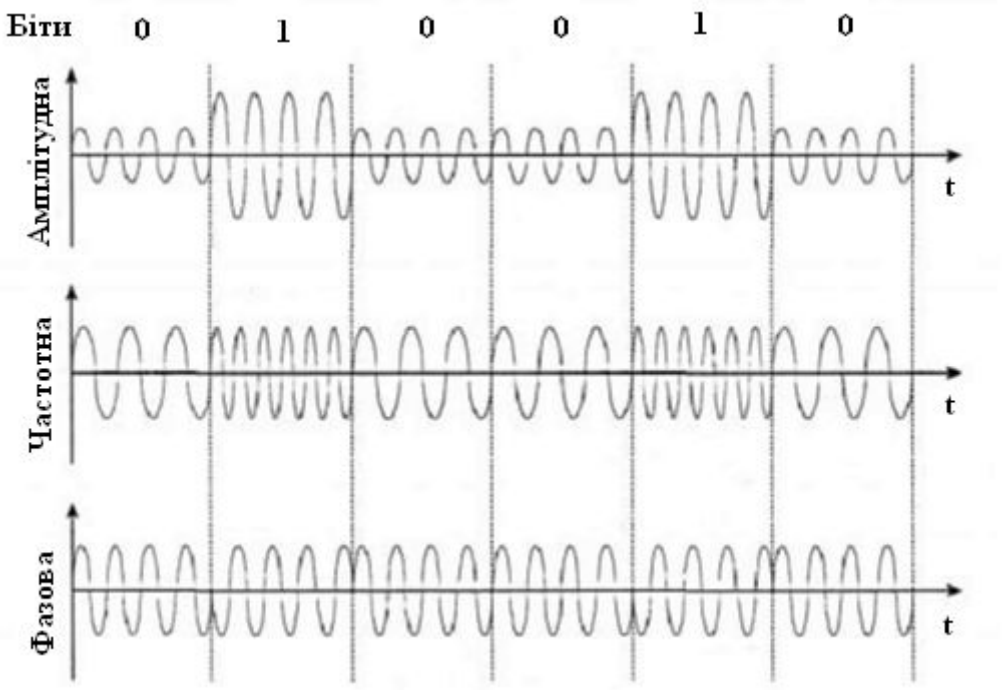


Рисунок 1.3 Види модуляції дискретних даних аналоговими сигналами

Далі перейдемо до розгляду класифікації бездротових технологій.

1.2. Класифікація бездротових технологій

На поточний момент бездротові технології представлені великою різноманітністю, розділеним в основному за сферами застосування. Однак існує багато інших способів їх поділу за класами:

Діяльність зв'язку (рис. 1.4);

• бездротові глобальні мережі топологія (WWAN);

• бездротові мережі масштабу міста (WMAN);

• бездротові персональні мережі (WPAN);

• бездротові локальні мережі (WLAN);

• Операторські;

• Багатоточкові (точка-многоточка);

• Корпоративні;

• Двоточкові (точка-точка);

•. Сфера застосування

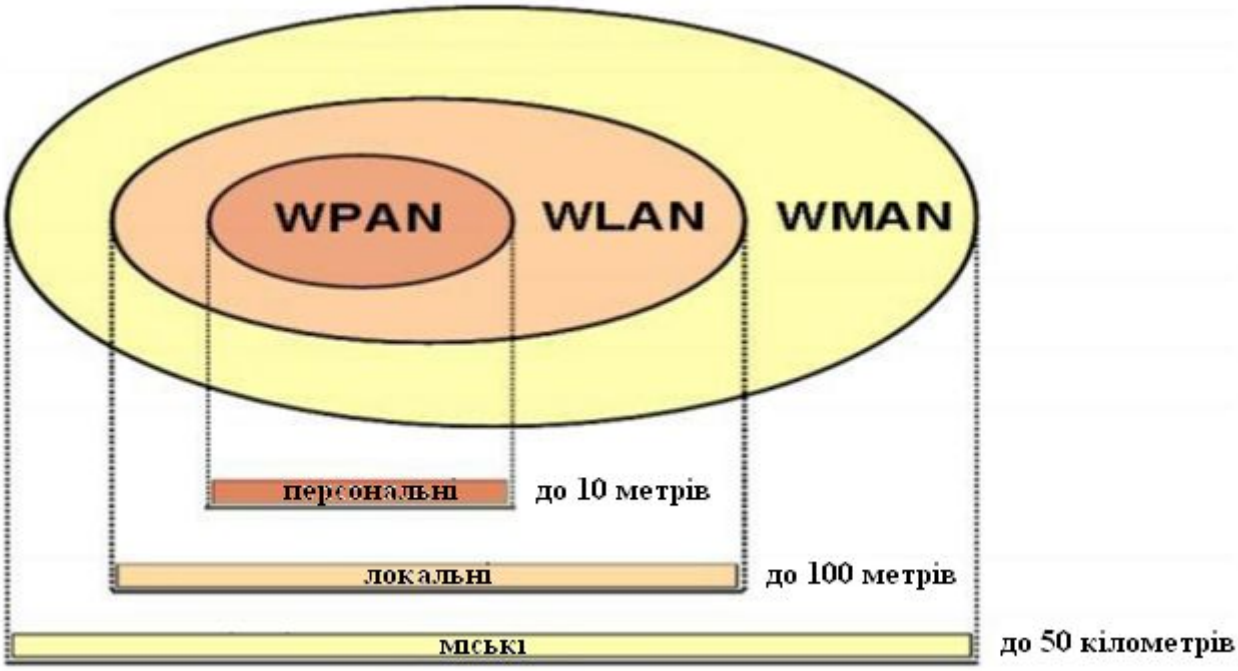


Рисунок 1.4 Радіус дії бездротових мереж

Розглянемо категорії бездротових технологій більш детально на найбільш актуальному прикладі, взявши за критерій дальність зв'язку.

1.2.1 Бездротові персональні мережі.

Для зв'язку різних пристроїв в умовах обмеженого простору застосовуються бездротові персональні мережі. Робочою групою IEEE описаний стандарт 802.15 викладає способи функціонування таких мереж. Як актуального прикладу візьмемо технологію Bluetooth.

Із співвідношення параметрів таких, як: економічність, дальність, швидкість виступає стандарт Bluetooth. Основна ідея його створення це створення дешевого, універсального та надійного радіоінтерфейсу. Така технологія дає змогу забезпечувати сполучення з безлічі обладнанням в режимах передачі сигналів, зокрема даних і мультимедіа.

Принцип дії виходить із взаємодії радіохвиль. Радіозв'язок відбувається в неліцензованому ISM діапазоні 2.4- 2.483 ГГц. Використовується метод розширення спектра FHSS зі стрибкоподібною зміною частоти.

До переваг стандарту можна віднести:

• Низька вартість;

• Захист переданих даних;

• Стандартизація і сумісность;

• Різноманітність та універсальність.

Як недоліки можна згадати щодо високе енергоспоживання і невисоку швидкість обміну даними. Сформована область застосування представлена:

• Телекомунікаційне обладнання і комп'ютерна техніка;

• Системи керування віддаленого доступу і телеметрії;

• Автомобільна електроніка.

1.2.2 Бездротові локальні мережі.

Для зв'язку різних пристроїв в локально-обчислювальну мережу без використання кабельних технологій використовуються бездротові локальні мережі. Робоча група IEEE на прикладі стандарту 802.11 описала норми роботи таких пристроїв, що включають в себе більше 20 сертифікацій. Як приклад розглянемо найбільш актуальну технологію Wi-Fi.

Стандарт 802.11 був спроектований під потреби створення ЛВС з декількох комп'ютерів. Мережі, побудовані за допомогою кабелів, виділяються необхідністю безлічі супровідних робіт пов'язаних з прокладанням проводів всередині робочих територій. Таких недоліків позбавлені бездротові мережі Wi-Fi. Всі пристрої можна підключати з використанням мінімальної кількості ресурсів.

Робочі діапазони і способи модуляції розрізняються залежно від використовуваного стандарту і більш детально будуть розглянуті у другому розділі.

До плюсів технології відносяться:

• Компактність;

• Висока швидкість передачі;

• Високий рівень стандартизації і сумісності даних;

• Різноманітність модулів під різні завдання;

• Висока швидкість передачі даних.

Як недоліки можна виділити порівняно велике енергоспоживання і поганий захист від злому.

Області застосування, продиктовані особливостями стандарту Wi-Fi:

• Комп'ютерна техніка;

• Громадські місця;

• Промисловість;

• Приватні бездротові мережі;

• Системи телеметрії та віддаленого керування.

1.2.3 Бездротові мережі міста.

Бездротові мережі міста це широкосмуговий доступ до мережі з використанням радіоканалу. Робочою групою IEEE був створений стандарт 802.16 в якому описані основні умови взаємодії таких пристроїв. Як приклад візьмемо найбільш актуальну технологію WiMAX.

Перед розробниками завжди стояла проблема «останньої милі» (канал, що з'єднує устаткування користувача з вузлом доступу провайдера). WiMax забезпечує доступ і з'єднує між собою точки Wi-Fi, дозволяє створювати точки віддаленого доступу без прив'язки до географічного положення, забезпечує системами віддаленого моніторингу і т.д.

Способи модуляції і робочих діапазонів сильно варіюються в залежності від стандартів і будуть вказані нижче в порівняльній таблиці.

До переваг стандарту відносяться:

• Легкість підключення;

• Охоплення території;

• Мобільність;

• Якість передачі;

• Високий рівень стандартизації;

• Гнучкість.

Як недоліки потрібно згадати непідготовленість законодавчої бази, дефіцит частот і проблеми застосування технології.

В основному технологія застосовується для надання послуг бізнес-структурам та приватним особам з використанням високошвидкісного доступу в Інтернет.

1.2.4 Бездротові глобальні мережі топологія.

Бездротові глобальні мережі представлено найбільш актуальним стандартом для передачі інформації у бездротовій мережі з великою швидкістю, використовуючи мобільні телефонів та різні пристрої LTE.

Цей стандарт був розроблений консорціумом 3GPP і є закономірним способом модернізації для операторів мереж GSM / UMTS. У дослівному перекладі «довгостроковий розвиток». Використання нового методу цифрової обробки сигналу і модуляції дозволило збільшити швидкість передачі даних в мобільних мережах.

Робоча частота технології знаходиться в проміжку від 800Мгц до 3.5 ГГц. Використовується три види модуляції QPSK, 16QAM, 64QAM.

Переваги стандарту:

• Низьке значення затримки;

• Висока швидкість;

• Підвищена стабільність;

• Доступність.

До недоліків можна віднести можливі розбіжності робочих частот в різних країнах.

Технологія LTE використовується в основному для надання доступу до мережі Internet за допомогою протоколу IP і мобільного зв'язку.

1.3 Порівняльний аналіз стандартів бездротового зв'язку.

Узагальнимо розглянутий матеріал. Для зручності аналізу і сприйняття інформації нижче наведені порівняльні характеристики основних сучасних бездротових технологій (табл. 1.1).

Таблиця 1.1

Стандарти бездротової передачі даних

Технологія	Стандарт	Область застосування	Пропускна здатність, Мбіт / с	Дальність зв'язку	Модуляція, доступ до середовища	Частотний діапазон, ГГц
Bluetooth	802.15.1	WPAN	до 0,7	до 10 м	FHSS	2,4
	V4.0		до 2.3	до 60 м	ГМСК	2,4
	V5.0		до 5	до 100 м	ФГМСК	2.4
Wi-Fi	802. llg	WLAN	до 54	до 140 м	DQPSK	2,4
	802,1 В		до 300	до 250 м	64QAM	2,4 або 5
	802,1 лак		до 1000	до 500 м	256QAM	5-6
WiMAX	802. 16г	WMAN	до 75	до 50 км	OFDM	1,5-11
	802.16е	WWAN	до 40	до 5 км	OFDM	2-13
	802,16м		до 1000	до 100 км	COFDM	2-66
LTE	LTE	WWAN	до 100	до 15 км	OFDM	0,8-3,5
	Розши-рений		до 1000	до 100 км	COFDM	0,8-3,5

Як вже говорилося раніше, з розвитком технологій стандарти удосконалюються і намагаються конкурувати один з одним в одних і тих же практичних застосуваннях і сегментах ринку. У кожного є недоліки та переваги. На поточний момент вибір розглянутих технології обумовлений скоріше не технічними характеристиками, а успіхом проведення маркетингових компаній.

1.4. Висновки до розділу 1

У розділі описано основи передачі інформації в безпровідних технологіях та проведено класифікацію безпровідних технологій, зокрема: WPAN - бездротові персональні мережі, WLAN - бездротова локальна мережа, WMAN - Wire менш Metropolitan Area Networks, WWAN - бездротові широкосмугові мережі. Також в першому розділі проведено порівняльний аналіз найбільш актуальних стандартів безпровідного зв'язку.

РОЗДІЛ 2
ОСНОВНА ЧАСТИНА

2.1. Історія створення локальних мереж WI-FI

Абревіатура «Wi-FI» (від англ.Wireless Fidelity - бездротова точність) сьогодні представляє бренд компанії Wi-Fi Alliance під яким прийнято розуміти відповідність певного пристрою специфікаціям належать до цієї марки. Ця абревіатура вийшла в результаті рекламної компанії для збільшення користувачів як похідне від Hi-Fi.

Початок історії слід шукати в 1985 році за час легімітізації в США використання ISM діапазонів усіма бажаючими. Через 6 років голландська компанія першою в світі представила готовий продукт для бездротової передачі даних. Технологія називалася WL і використовувалася тільки для підвищення якості функціонування касових систем.

Перший єдиний міжнародний стандарт для передачі інформації був затверджений в 1997 році Інститутом Інженерів Електротехніки і Електроніки (IEEE). Його сертифікаційний номер 802.11.

2.2. Основні терміни і елементи мережі.

Для організації мережі Wi-Fi потрібні приймачі та точки доступу. У промисловому секторі також необхідні бездротові комутатори для координації точок доступу.

Приймач Wi-Fi служить для підключення телефону, комп'ютера до бездротової мережі. Сучасні ноутбуки і телефони мають Wi-Fi адаптери. Для отримання доступу до мережі адаптер може з'єднуватися як з точкою доступу, так і з іншими приймачами. У першому випадку вийшла однорангова мережа буде називатися Ad Hoc (від лат. «До нагоди»). У другому назвою режиму буде інфраструктура.

Під точкою доступу на увазі автономний модуль з функцією взаємодії між приймачами і зв'язком з проводовим сегментом мережі. У більшості випадком він складається з мікрокомп'ютера і приймально-передавального пристрою. Серед режимів роботи точок доступу крім основного слід зазначити Wireless Bridge і Repeater.В першому випадку пристрій використовується для об'єднання двох незалежних один від одного дротових мереж. У другому режимі пристрій здійснює ретрансляцію сигналів між точками доступу. Доступ до мережі здійснюється через передачу сигналів по ефірі.

Бездротові комутатори використовуються, коли необхідно централізоване управління і супровід точок доступу. Вони забезпечують величезний спектр функцій включає в себе:

- Управління безпекою;
- Моніторинг користувачів;
- Контроль смуги пропускання;
- Забезпечення сталого прийому даних;
- Балансування навантаження;
- Централізоване опрацювання трафіку.

2.3. Актуальні стандарти бездротових мереж.

Для передачі даних в частотних діапазонах 2,4 - 5 ГГц існує безліч стандартів об'єднаних групою IEEE 802.11. На поточний момент найбільш поширені три види:

- 802.11g;
- 802.1 1n;
- 802.11ac.

Їх специфікації відображені нижче (табл.2.1).

Таблиця 2.1

Порівняльна таблиця актуальних стандартів Wi-FI

Стандарт	802. g	802,1 n	802,1 ac
Дальність зв'язку	до 140 м	до 250 м	до 500 м
Ширина каналу	до 20 МГц	до 40 МГц	до 160 МГц
Частотний діапазон	2,4 ГГц	2,4 ГГц або 5 ГГц	5-6 ГГц
Тип модуляції	DQPSK	64QAM	256QAM
Пропускна здатність	до 54 Мбіт / с	до 300 Мбіт / с	до 1000 Мбіт / с
Сумісність	802,11 б / н	802.11 a / b / g	802.11 a / b / g / n
Рік сертифікації	2003 рік	2009 рік	2013 рік

Вперше метод квадратурної модуляції був застосований в стандарті 802.11n, що позитивно позначилося як на пропускної здатності, так і на дальності зв'язку бездротової мережі. Режим модуляції 256QAM застосовуваний в цифрових передавачах, де необхідна стабільність завадостійкості і широкого радіусу мовлення, використовується в стандарті 802.11ac, що визначає набагато вищий показник швидкості передачі даних.

Слід зазначити, що при ідентичною архітектурі канального рівня, фізична частина бездротових мереж різних стандартів з групи 802.11 відрізняється. Типи модуляції, кодування і відмінності в швидкості з'єднання обумовлені саме фізичної архітектурою.

2.3.1 IEEE 802.11g.

У 2003 році був ратифікований протокол IEEE 802.11g, який використовує частотний діапазон 2,4 ГГц. Описує швидкості передачі аналогічні 802.11a.

У процесі розробки цього стандарту було використано компромісне рішення в області цифрових схем модуляції. Воно виражено в поєднанні двох технологій: OFDM (метод ортогонального частотного поділу) та PBCC (метод двійкового пакетного згорткового кодування). Відповідно основну технологію стандарту представляє - OFDM, а додаткову - PBCC.

Підходячи до проблеми кодування і модуляції сигналів, виникають наступні проблеми.

По-перше, необхідність підтримки низького рівня корисного сигналу обумовленого використанням ISM діапазону. Для цього застомовується технологія розширення спектра, яка по факту зменшує потужність і «розмиває» передачу по діапазону.

По-друге, для конкурентоспроможності швидкість передачі потрібно забезпечувати на найвищому рівні, що в свою чергу визначає збільшення ширини спектра, що неприпустимо через обмеження ISM.

По-третє, надання високої завадостійкості.

Як ми бачимо вищезгадані умови суперечать один одному, внаслідок чого кодування і модуляція - це пошук рівноваги між, так би мовити «золота середина».

2.3.2 IEEE 802.11n.

Протокол використовує частотний діапазон 2,4 ГГц і 5ГГц. Сумісний з 11b / 11a / 11g. Сам стандарт вийшов 11 вересня 2009 року. Описує швидкості передачі до 300 Мбіт / с.

Основне нововведення стандарту полягає у використанні технології MIMO (рис 2.5), поліпшення функції MAC - рівня і збільшення ширини каналу.

Технологія MIMO - множинні входи, множинні виходи. Це радіосистеми з великою кількістю роздільних шляхів передачі і прийому інформації, де мається на увазі присутність в адаптері і точки доступу до 4 антен. За рахунок цієї технології досягається підвищена спектральна ефективність, розширений спектр частот і значно вища швидкість передачі даних. Іншими словами ця технологія робимо можливим вторинне шифрування даних, що також називається просторово - тимчасовим кодуванням STC. У приземлене викладі технологію можна пояснити розпаралелюванням високошвидкісного потоку OFDM на певну суму передач, що залежить від суми антенних каналів.

Залежно від збільшення кількості антен в пристрої, відбувається зростання завадостійкості і якості передачі даних, за фактом обумовленого

зростаючим кількість просторових каналів. З іншого боку підвищується вартість кінцевого обладнання через збільшення складності обробки сигналів.

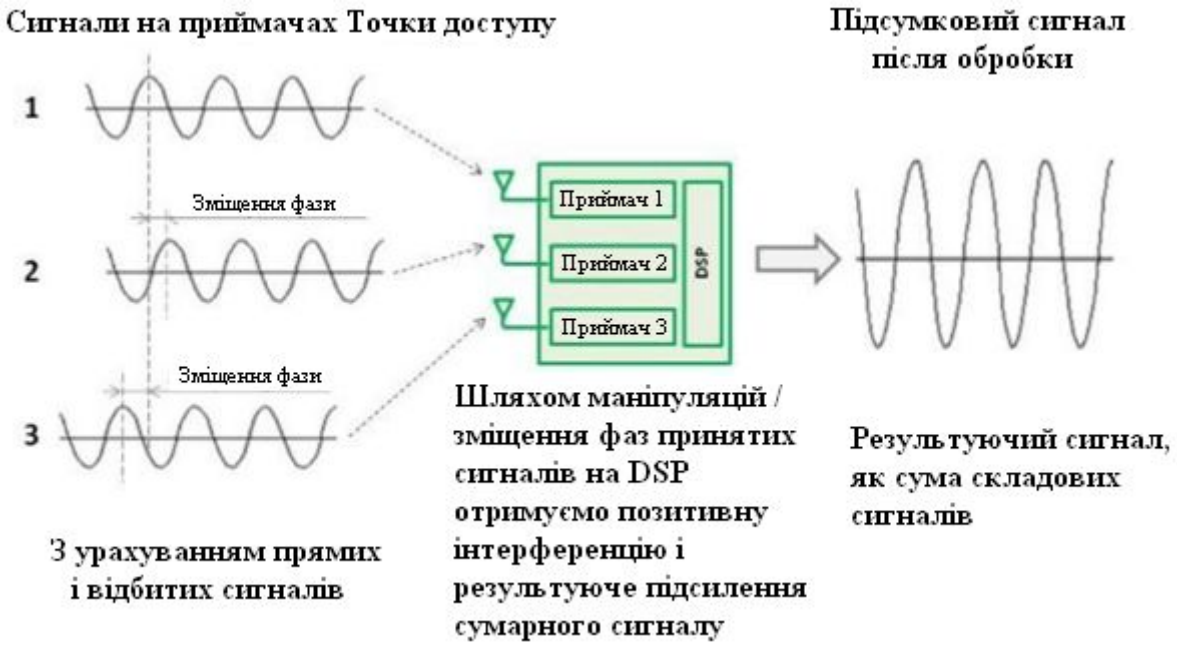


Рисунок 2.1 MIMO. MRC - поліпшення сигналу від клієнта до пункту доступу.

2.3.3 IEEE 802.11ac.

Даний стандарт працює в частотному спектрі 5 - 6 ГГц. Підтримується сумісність з 11b / 11a / 11g / 11n передбачена фізичної архітектурою. Протокол сертифікований 12 жовтня 2013 року. Надає швидкості передачі в теорії при 8 * MU-MIMO до 1 Гбіт / с.

Основний вплив на поліпшення характеристики зв'язку вплинуло використання двох нових технологій. Beamforming (рис. 2.2) - (дослівно «формування променя») спосіб активного зміни спрямованості несучого сигналу. Обов'язкова для стандарту функція забезпечує максимальну ефективність мовлення, враховуючи локацію користувачів. Так само представлено поліпшення MIMO, а саме MU-MIMO. Давайте розберемося, що ж це таке.

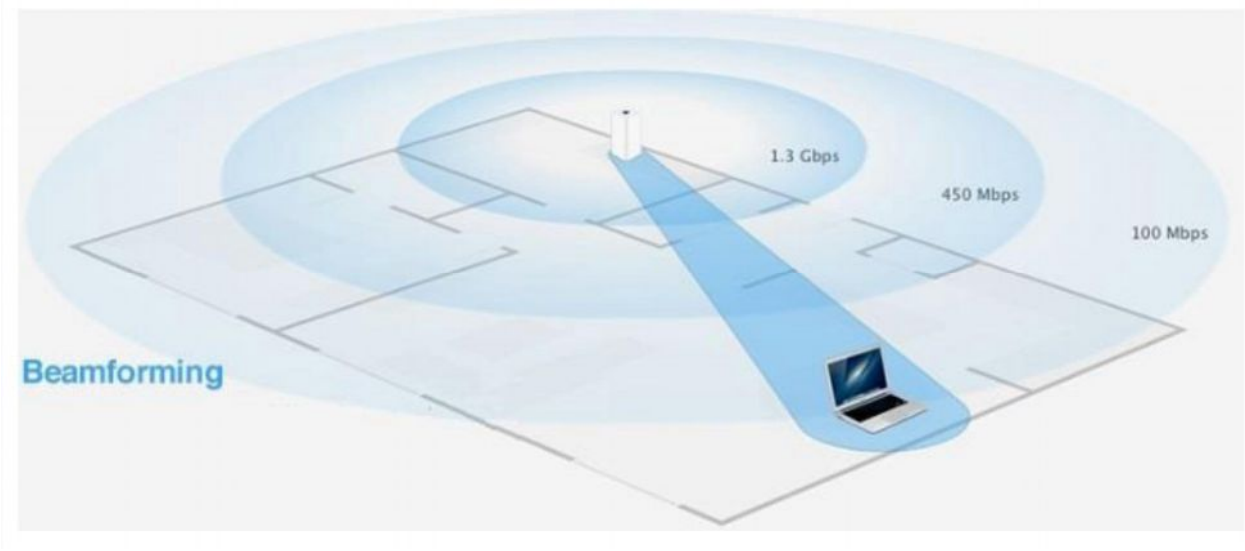


Рис. 2.2 Приклад функціонування технології Beamforming.

MU-MIMO (рис. 2.3). У минулому стандарті призначені для користувача пристрої виявлялися послідовно, що обмежувало кількість фактично використовуваної ємності мережі. Технологія MU-MIMO нівелює цю проблему, дозволяючи робити набагато більше, використовуючи аналогічний доступний спектр.

Рис. 2.3 Приклад функціонування технології MU-MIMO.

Використовується динамічне групування клієнтів, в якому задіяна функція управління діаграмної спрямованості для можливості паралельної передачі просторово рознесених променів до кожному користувачеві. Для забезпечення роботи технології, функціонал повинен бути доступний на вході і виході з'єднання. Реалізація можлива в двох варіантах: SDMA і Downlink MIMO. У першому випадку використовуються відрізняються просторові потоки для передачі даних відповідним користувачам, у другому ж відбувається процес поділу OFDM даних на безлічі, необхідні для оперативного надання користувачам потрібної кількості піднесуть. Таким чином 802.11ac надає якісну можливість повної реалізації стелі швидкостей для інфраструктур з високим показником кінцевих користувачів.

2.4 Забезпечення безпеки технологій Wi-Fi

2.4.1 Історія розвитку.

Група 802.11 дуже швидко набрала широку аудиторію користувачів, за рахунок високої якості і зручності технологій. Тим самим викликавши підвищений інтерес в середовищі кіберзлочинів, таких як крадіжка даних і неузгоджені підключення.

Спочатку спосіб збереження інформації в таких мережах отримав назву WEP, іншими словами «Конфіденційність, аналогічна кабельному з'єднанню». Вже з визначення малося на увазі, що буде говоритися не про дійсно хорошому рівні безпеки, а приблизно про таке ж рівні захисту, що забезпечує кабельний Ethernet. Де вся інформація транслюється у відкритому вигляді, але для доступу до них сторонніх осіб потрібні різні навички поводження з пристроями і протоколами. І також, як умільці легко отримують доступ до Ethernet для шпигунства, так і фахівці в короткі терміни зламали WEP в 2001 році. Криптоаналітики показали, що зловмисники, які мають малими ресурсами, здатні отримати доступ в мережу за одну-дві години. Отже, WEP надавала захист лише від випадково підключається до мережі сторонніх, а серйозним атакуючим групам не було ніякого діла до факту активації шифрування.

Пізніше IEEE формує групу 802.11i і ставить перед нею план: замінити WEP на щось більш суттєве і сумісний з уже існуючими пристроями. У підсумку ця група розробила два окремих способи: одне, так би мовити, з оглядкою назад, а інше - спрямоване в майбутнє. З огляду на продані пристрої, члени 802.11i домоглися того, щоб все вже вироблені на фабриках Wi - Fi - пристрої були сумісні з новою системою захисту TKIP.

TKIP була сумісна зі старими Wi - Fi картами - через установку оновлення прошивки. Ясно це зробили в найпершу чергу, і в 2003 році TKIP був частиною нового методу Wi - Fi - захисту, який отримав назву WPA. Більш того група 802.11i винайшла WPA2 - можний спосіб для наступних версій Wi-Fi, - погодивши в комплекті алгоритм на основі AES з довгим ключем і новим режимом роботи. Цей режим по іншому називається CCMP.

Коли завершилися роботи над винаходом, Wi-FiAlliance опублікувало нову версію стандарту - WPA2. Так WPA мав на увазі лише шифрування TKIP, а WPA2 необхідне узгодження обох алгоритмів, TKIP і AES. З березня 2006 року Wi-Fi Alliance зробив підтримку WPA2 обов'язкової для всіх сертифікованих Wi-Fi-пристроїв.

Проте, певне безліч вразливостей, загальних у WPA і WPA2, залишають лазівки для зломщиків. Наприклад PSK.

Приземлений режим використання ключів PSK приватників і невеликих організацій, де незручно і не прийнято управляти безліччю ключів з використанням серверів аутентифікації 802.1x. При PSK все Wi-Fi- пристрою шифрує мережевий трафік за допомогою 256-бітного ключа. цей ключ можна представляти у вигляді з 64 шістнадцяткових цифр, або як фразу з символів ASCII довжиною від 8 до 63 знаків. Якщо використовується код ASCII, то 256 біт ключа дістаються з пароля з використанням тривіальної криптографічного функції PBKDF2, яка застосовує до шифру ідентифікатор мережі SSID і проводить 4096 бітових «кеш-перетворень». На жаль, навіть при таких способах режим PSK часто виявляється недостатнім для словникових атак перебором паролів 24 - якщо, звичайно, користувач застосовує слабку парольний фразу. Слабкість ключа на основі фіксованого пароля очевидна для

будь-якої криптосистеми і виправляється за допомогою вибору довгих і менш передбачуваних фраз.

Менш помітною і тому більш вразливою виглядає наступна вроджена вразливість WPA2. А саме: зробивши криптоалгоритм TKIP в складі WPA і WPA2 сумісним з приймачами, супроводжуються давно зламаний WEP, Альянс Wi - Fi таким чином допустив, діру, яку з часом вдається збільшити для проведення серйозних нападів. Знайдена в TKIP слабкість укладена в роботі контрольних сум.

У мережі Wi-Fi, де при транслюванні високий випадок втрати біта, для виявлення помилок застосовують контрольні суми. Якщо склад пакета змінився, а сама контрольна сума не змінилася, то пакет підроблено. Хакери винайшли спосіб, який дає змогу змінювати дані в пакетах та знаходити нову контрольну суму для них, таким чином підроблений пакет видаюче за справжній. У своїх працях Тьюз та Бек застосували один з таких інструментів, так званий, Chopchop. Ця програма і стала відправною точкою для розширення атаки на WPA.

Тепер, щоб запобігти тривіальну атаку Chopchop, клієнт реагує відразу ж, як тільки отримує дві невірні контрольні суми MIC в інтервалі 60 секунд. У відповідь на це підозріле подія клієнт відключається на одну хвилину, а потім вимагає повторення обміну ключами з точкою доступу. Точка доступу при виявленні аналогічній ситуації теж відключається на 60 секунд, а потім генерує нові ключі для кожного зі своїх клієнтів. (В стандарті 802.11i допускається, щоб нові майстер-ключі створювалися за запитом без зміни початкової парольної фрази або мережевого ключа.)

Ще один можливий спосіб: «отруєння ARP» дозволяє аналізувати весь трафік внутрішньої мережі компанії і знаходити будь-яку інформацію, в тому числі логіни-паролі (проте в такому випадку потрібен інсайдер з монітором трафіку).

Протокол WPA2 з кодуванням на основі криптоалгоритму AES є обов'язковим у всіх Wi-Fi-пристроях, починаючи з 2006 року і на сьогоднішній день, не показав нічого схожого на подібні уразливості. Тому для забезпечення

належного рівня захисту рекомендується виставляти такі настройки безпеки мережі:

• Назва SSID має бути унікальним для виключення злому способом словникового перебору;

• В якості методу аутентифікації вибирати режим WPA2-PSK;

• Методом шифрування вказувати AES;

Перераховані критерії забезпечують найбільш високий рівень безпеки від злому.

2.4.2 Механізм аутентифікації WPA2.

WPA2 - це програма сертифікації бездротового зв'язку. Перевагами WPA є підвищений захист даних та контроль бездротових мереж. Суттєвою особливістю є сумісність безлічі бездротових пристроїв на апаратному та на програмному рівнях. Низький рівень безпеки, безсумнівно, довго залишався головних недоліком мережі W-Fi.

перші БЛВС, реалізовані на технології VPN, надавали безпеку даних на рівні 3, що залишало слабкість мережі IP для погроз. Здійснений на рівні 2 протокол WPA2 оберігає бездротову мережу набагато краще. Однак лише він один не здатний надати потрібний рівень безпеки корпоративної мережі. Управління ж доступом за цим протоколом в поєднанні з реалізованим протоколом аутентифікації IEEE 802.1X на портах, дає змогу зменшити безліч проблем захисту.

Протокол WEP був уразливим для атак і погано реалізовувався виробниками. У зв'язку з цим він так і не знайшов масового використання в корпоративних мережах. Слабкі місця WEP і те, що їх досить просто реалізувати в незаконних цілях, сприяли розробці стандарту 802.11i, який був сертифікований в 2004 р. Організація Wi-Fi Alliance розробила протокол WPA, в рамках проекту стандарту 802.11i, що забезпечує набагато вищий рівень безпеки, а ніж попередня версія WPA. Наявність множинних ротацій ключів і лічильника пакетів прибирають можливість атаки з відтворенням пакетів або їх повторним введенням. контроль цілісності даних, забезпечує протокол WPA,

використовуючи метод 29. Даний метод зазнає атак «Brute-Force», але при цьому передача трафіку за хвилину автоматично регенерується і, якщо точка доступу заснована на WPA знаходить протягом 60с. більше однієї помилки MIC то сеансові ключі переставляються, зменшуючи, ризик атак до мінімуму. Тим часом протокол WPA2 задіє новий метод кодування, заснований на більш сильному, алгоритмі шифрування AES, ніж RC4. WPA і WPA2 мають 2 режими аутентифікації:

- корпоративному (Enterprise);
- персональному (Personal).

У персональному режимі WPA2 із парольної фрази введеної відкритим текстом, генерується 256-розрядний ключ., Ідентифікатор SSID та ключ PSK і довжина останнього разом визначають математичний базис для створення головного парного ключа PMK, який потрібен для ініціалізації чотиристороннього квантування зв'язку та генерації сеансового ключа PTK, для взаємодії клієнтського пристрою з точкою доступу. Протоколу WPA2-Personal має проблеми підтримки ключів і розподілу, тому його використовують в невеликих офісах, ніж у промисловості. Можливі параметри безпеки приведені в таблиці 2.2.

Таблиця 2.2

Таблиця можливих параметрів безпеки

Властивості	Статичний WEP	Динамічний WEP	WPA	WPA2 (для підприємств)
Авторизація	Общий ключ	EAP	EAP , загальний ключ	EAP , загальний ключ
Шифрування	Стат-ий ключ	Сесс-ый ключ	ТКП>	CCMP (AES)
Алгоритм	RC4	RC4	RC4	AES
Розподіл ключів	Одноразове,вручну	PMK	Виробниче від PMK	Виробниче від PMK
Вектор ініціалізації	Текст, 24 біта	Текст, 24 біта	Розширений вектор, 65 біт	48 біт номер пакета (PN)
Довжина ключа	64/128	64/128	128	256
Інфраструктура	немає	Радіус	Радіус	Радіус
Цілісність	32-розрядна ICV	32-розрядна ICV	64-розрядна MIC	ЕПТ / CBC

Протокол WPA2-Enterprise добре усуває проблеми з розподілом статичних ключів та адміністрування цих ключів. Інтеграція даного протоколу з багатьма корпоративними сервісами аутентифікації дає змогу здійснювати контроль доступу на базі облікових записів.

Аутентифікація відбувається між робочою станцією і центральним сервером аутентифікації. Точка доступу або бездротового контролер здійснюють моніторинг з'єднання. Стандарт 802.1X служить базою для режиму WPA2-Enterprise. До основних компонентів аутентифікації 802.1X відносяться клієнтський запит, аутентифікатор і сервер аутентифікації. Згідно зі специфікацією 802.1X, призначений для користувача запит вважається пристрій, що вимагає доступ до мережі. Зазвичай під запитом мається на увазі ноутбук або будь-яке інше мобільний пристрій. На перевірку клієнтським запитом в кінцевому рахунку виявляється встановлене на цьому пристрої ПО, ініціалізує і відповідає на команди 802.1X (рисунок 2.4).

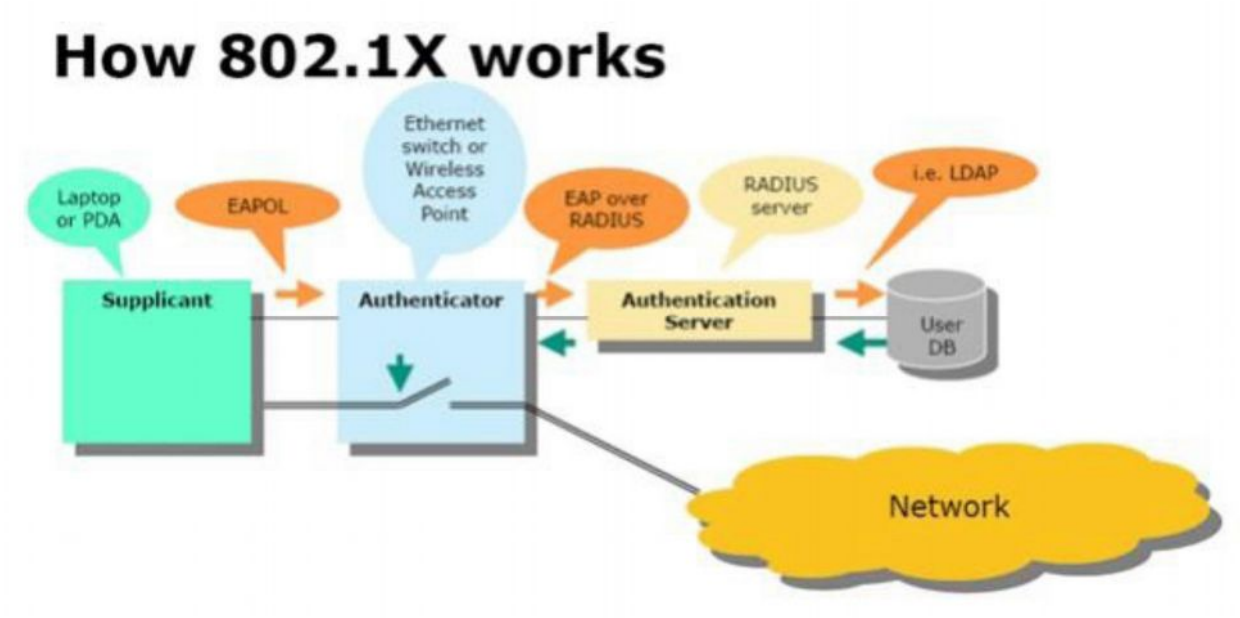


Рис. 2.4 Схема роботи 802.1x

Аутентифікатор (часто це точка доступу, але в централізованій архітектурі доступу він може розташовуватися на комутаторі / контролері) аутентифікує клієнт для доступу до мережі. Це пристрій визначає запити від клієнтського запиту, залишаючи мережевий інтерфейс закритим до тих пір,

поки не отримає від сервера аутентифікації наказ на його відкриття. В свою чергу, останній приймає та обробляє запит на аутентифікацію. Хоча зазвичай в якості сервера аутентифікації використовується сервер RADIUS, в даній ситуації можна використовувати не всякий такий сервер, а лише той, що сумісний з методами аутентифікації. Клієнт і точка доступу змінюються трафіком EAP по протоколу рівня 2 EAPoL. Клієнтський запит не може спілкуватися з сервером RADIUS за допомогою протоколу рівня 3: коли точка доступу отримує трафік EAP від клієнта, вона переформовувалися його в відповідний запит RADIUS і передає серверу RADIUS на виконання (рисунок 2.5).

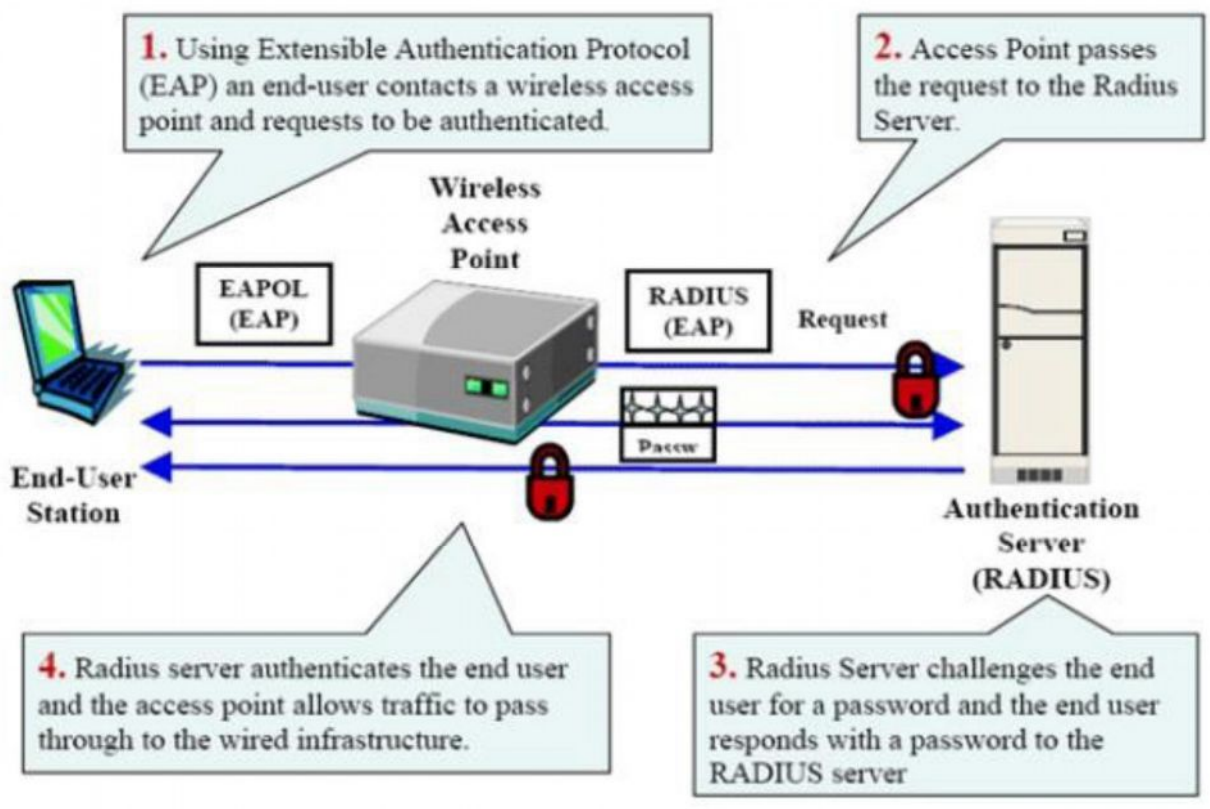


Рис. 2.5 Процедура аутентифікації

Протокол EAP є контейнерним, отже, фактично механізм авторизації виповнюється внутрішніми протоколами. Сьогодні найбільшу кількість застосувань налічують наступні:

• EAP-FAST - дозволяє проводити аутентифікацію за логіном-паролем, трансльованого всередині TLS тунелю між отправщіком і RADIUS- сервером;

• EAP-FAST EAP-TLS - використовує інфраструктуру відкритих ключів (PKI) для аутентифікації користувача і сервера (отправщіка і RADIUS-сервера) через сертифікати, видані довіреним підтверджуючий центр (CA). Вимагає видачі та 32 установки клієнтських сертифікатів на кожен пристрій, тому підходить тільки для керованої корпоративного середовища;

• EAP-TTLS - схожий з EAP-TLS, але при налагодженні тунелю не потрібен клієнтський сертифікат. В такому тунелі, аналогічному SSL-з'єднання браузера, відбувається повторна авторизація;

• PEAP-MSCHAPv2 - схожий на EAP-TTLS в питанні первинного налагодження шифрованого TLS тунелю між користувачем і сервером, що вимагає серверного сертифіката. Далі в такому тунелі здійснюється аутентифікація по протоколу MSCHAPv2;

Архітектура EAP-кадру представлена нижче (рис 2.6).

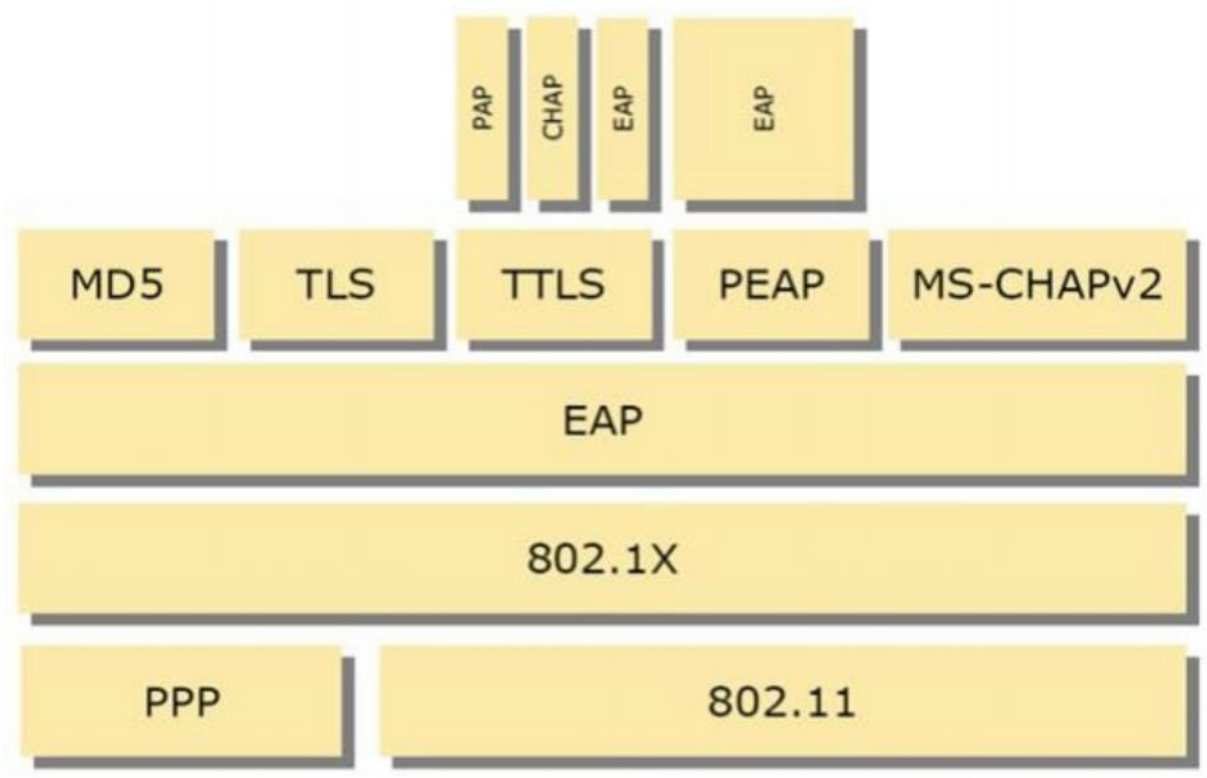


Рис. 2.6 Архітектура EAP кадру.

Виконавши процедуру аутентифікації 802.1X, користувач отримує від сервера аутентифікації головний ключ, який «приєднується» до поточного

сеансу аутентифікації. На основі цього ключа на клієнті і на сервері аутентифікації створюється один і той же парний головний ключ PMK. Аутентифікатор отримує ключ PMK від сервера аутентифікації через попередньо визначеного атрибута 33 RADIUS. Володіючи ключем PMK, клієнт і точка доступу відтворюють парний тимчасовий ключ PTK, практично не обмінюючись ім. Така процедура генерації ключів здійсненна через використання чотиристороннього квантування зв'язку, що запобігає вчинення атак, спрямованих на перехоплення службової інформації.

WPA2 має 3 типи ключів PTK:

- ключ підтвердження ключа KCK, що застосовується для перевірки цілісності кадру EAPOL-Key;

- ключ шифрування ключа KEK, потрібний для шифрування групового тимчасового ключа GTK;

- тимчасові ключі TK - для шифрування трафіку.

Всі «приєднані» до точки доступу бездротові пристрої повинні «вміти» розшифровувати широкомовний і багатоадресний трафік. Вони роблять це за допомогою одного і того ж тимчасового групового ключа GTK. Якщо точка доступу змінює ключ GTK - то вона виробляє новий ключ, використовуючи просте двостороннє квантування зв'язку і ключ KEK для шифрування ключа GTK.

При здійсненні клієнтським пристроєм роумінгу між двома точками доступу повний процес його аутентифікації сервером RADIUS може займати сотні мілісекунд (а то і кілька секунд), що є неприйнятним для телефонів Wi-Fi або потокових додатків ноутбуків. Тому безліч корпоративних бездротових пристроїв оснащуються такими передбаченими специфікацією 802.11i функціями, як попередня аутентифікація і кешування ключа PMK, що дозволяють мінімізувати пов'язану з роумінгом затримку. Попередня аутентифікація дозволяє мобільному клієнту аутентифицироваться на інший, розташованої поблизу точки доступу, перебуваючи «прив'язаним» до своєї первинної точки доступу. При використанні кешування PMK користувачеві,

возвратившемуся з обслуговується роумінгом території - назад, не обов'язково повторне проходження авторизації 802.1X.

2.4.3 Механізм шифрування WPA2

Протокол WPA2 здійснюється на базі шифрування AES. Потребує апаратної підтримки та характеризується необхідністю величезного обсягу обчислень, які іноді відсутній в старому обладнанні. Для авторизації і підтримки цілісності даних WPA2 застосовує протокол CBC-MAC, а для шифрування даних - режим лічильника CTR.

Повідомлення (MIC) коду цілісності протоколу WPA2 є контрольною сумою і на відміну від WEP і WPA надає цілісність даних для заголовка 802.11. Це дозволяє усунути нападу типу «Packet replay» з метою розшифровки пакетів або компрометації криптографічного інформації. Для розрахунку MIC використовується 128-розрядний вектор ініціалізації IV, для шифрування IV - метод AES і часовий ключ, а на виході маємо 128 розрядний підсумок.

Після над цим підсумком і наступними 128 бітами даних проводиться операція «виключне АБО». За допомогою AES і TK шифрується її результат, а потім над останнім результатом і наступними 128 бітами даних знову виконується операція - виключає АБО. Процедура повторюється до вичерпання всій корисного навантаження. Створені на самому останньому кроці результату, перші 64 розряду, потрібні для знаходження значення MIC.

Для шифрування MIC та даних використовується алгоритм який базуються на режимі лічильника. Як і при шифруванні вектора ініціалізації MIC, виконання такого алгоритму бере початок з завантаження 128-розрядного лічильника, де замість значення відповідного довжині даних береться значення лічильника, в поле лічильника рівного одиниці. Слідчо, для кодування кожного пакета використовується свій лічильник.

Використовуючи AES і TK шифруються перші 128 біт даних, а тоді понад 128-біт, де результатом шифрування виступає операція - включення АБО. Перші 128 біт даних дають перший 128-розрядний зашифрований блок. Процедура повторюється до повного шифрування всього 128-розрядного блоку

даних. Після цього остаточне значення в полі лічильника скидається в нуль. Результат останньої операції приєднується до зашифрованого кадру. Після підрахунку MIC з використанням протоколу CBC-MAC проводиться шифрування даних і MIC. Після до цієї інформації спочатку приєднується заголовок 802.11 і поле нумера пакета CCMP, пристиковується «кінцевик» 802.11 і все це разом відправляється за адресою призначення. Розшифровка даних виконується в зворотному шифрування порядку. Для вилучення лічильника задіюється той же алгоритм, що і при його шифруванні. Для дешифрування лічильника і зашифрованою частини корисного навантаження використовується базуються на режимі лічильника алгоритм декодування і ключ TK. Результатом цього процесу є розшифровані дані і контрольна сума MIC. Нарешті, за допомогою алгоритму CBC-MAC, провадиться перерахунок MIC для розшифрованих даних. Якщо значення MIC не збігаються, то пакет скидається. При проходженні процедур порівняння зазначених значень, розшифровані дані йдуть в мережевий стек, а потім користувачеві.

2.4.4 Wardriving

«Wardriving» - це процедура пошуку і злому уразливих точок доступу бездротових мереж Wi-Fi індивідом або групою людей, забезпечених ноутбуком з Wi-Fi-адаптером і мають певний набір програмного забезпечення. Завдання «Wardriving» - під'єднатися до бездротової мережі з різними цілями, починаючи від безкоштовного користування інтернет з'єднанням - до корпоративного шпигунства. Потрібно згадати те - що такий злом може здійснюватися на дуже великій відстані і людина, що здійснює даний злом - може сховатися. Пошук точок доступу відбувається наступним чином: злочинець встановлює на свій ноутбук будь-який мережевий аналізатор - наприклад, InSSIDer - заходить в будь-якої транспорт і їздить по місту, в свою чергу InSSIDer пов'язаний з GPS модулем. Як результат - хакер отримує точки доступу з їх зразковим розташуванням, далі - вже йдучи на поводу особистих інтересів, локалізує потрібну точку доступу для атаки.

Для перехоплення пакетів існує спеціальний режим моніторингу (Monitor Mode). Іноді, для переведення пристрою в такий режим, необхідно встановити в систему спеціальні драйвери, які пишуться під чіп конкретного виробника.

Режим пасивного сканування також не є ліками, так наприклад програма Wellenreter здатна проводити пасивне сканування після впізнання бездротової картки ESSID підміняє наступним: «Thiisuseduntwellenreter», а MAC-адресу змінює на будь-який. На цьому етапі, зловмисникові потрібно роздобути певну кількість пакетів, що транслюються в цій мережі, а коли це буде виконано - вже в спокійній обстановці - за допомогою програми-зломщика отримати потрібний ключ. Для цих цілей найчастіше використовується «Aircrack-ng».

«Aircrack-ng» - це набір програм для виявлення бездротових мереж, та перехоплення даних через бездротові мережі WEP і WPA / WPA2-PSK.

2.4.5 Додаток InSSIDer.

«InSSIDer» - безкоштовний додаток, здатне здійснювати діагностику Wi-Fi-мереж і моніторинг завантаженості бездротових каналів.

За допомогою цієї утиліти ви можете подивитися список всіх знайдених мобільних мереж і дізнатися потужність сигналу, MAC-адресу точки доступу, виробника пристрої, що використовуються канали, ідентифікатор SSID, силу сигналу, ступінь захищеності, швидкість і завантаженість мережі і багато іншого. Потужність сигналу можна побачити за допомогою наочних графіків в режимі реального часу. При використанні програми ви зможете заміряти рівень сигналу в різних приміщеннях у себе вдома або в офісі. Після цього можна вибрати найбільш вільний канал з максимальною швидкістю і мінімальними перешкодами.

В утиліті добре реалізовані можливості по сортуванню результатів сканування мереж.

Інтерфейс утиліти InSSIDer відображений на рисунку 2.7

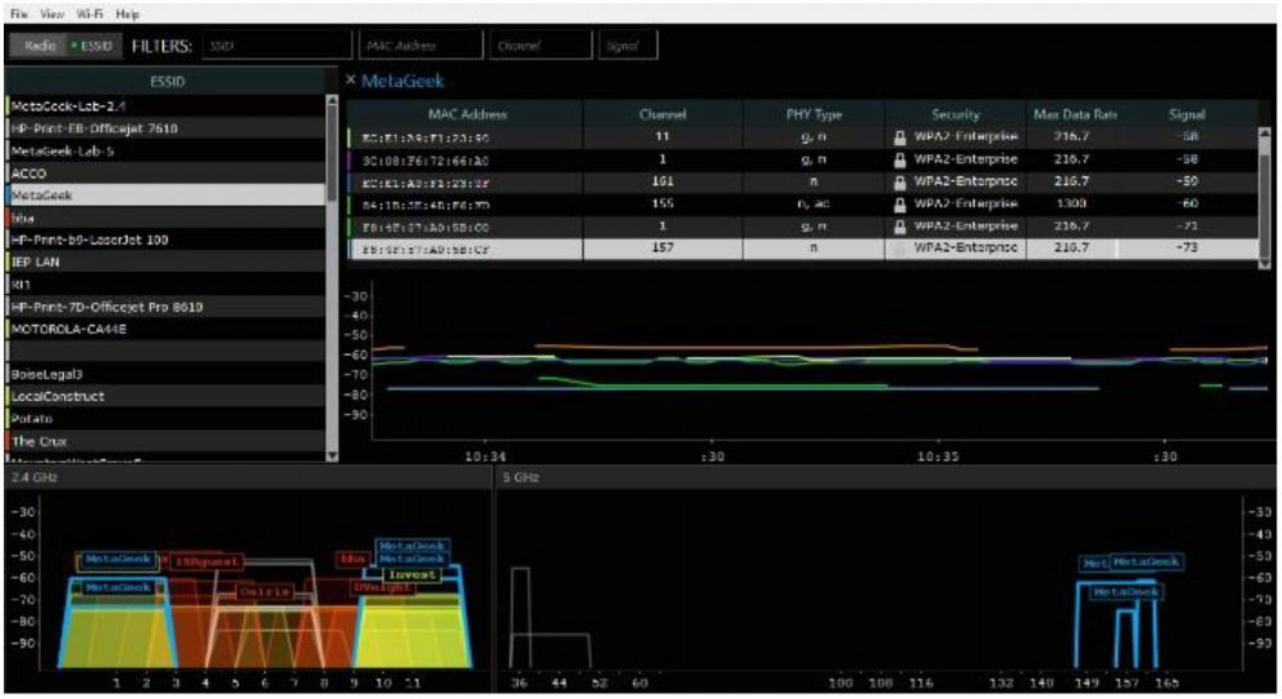


Рис.2.7 Інтерфейс програми InSSIDer

2.5 Технології Wi-Fi які пливають на здоров'я людини.

На сьогоднішній день нас оточує безліч бездротових мереж, через що виникає закономірне питання, чи шкідливий Wi-Fi?

У США є ціле поселення Грін Бенк, де на площі в 33 тисячі квадратних кілометрів заборонено використання не те що бездротових мереж, а будь-якої електроніки. Окремі особистості споруджують собі шапочки, плащі з фольги захищаючи себе таким чином від випромінювання. Деякі підприємці почали випускати шпалери, які блокують випромінювання за ціною 400 доларів за рулон. Ефективні вони нібито за рахунок напилення срібла на поверхню. Що для одних - страх і жах, для інших - непоганий прибуток.

У 2012 році Міжнародне Агентство з Досліджень в області Рака визначило радіовипромінювання як «можливо канцерогенна для людей». Класифікація IARC радіовипромінювання відображає факт, що деякі обмежені докази існують, що випромінювання радіохвиль можливо може бути фактором ризику для раку.

Щоб розібратися в цьому питанні, нам потрібно звернути увагу на те, що наукових підтверджень цих гіпотез немає. На даний момент це не більше ніж домисли.

Однак не можна говорити про абсолютну нешкідливість. Це питання потребує більш якісному аналізі, який в найближчому майбутньому буде проведено Всесвітньою організацією охорони здоров'я (WHO).

Розглянемо актуальну інформацію від цієї організації:

• Health Canada в вересні 2012 виклала на огляд дослідження, з якого можна дізнатися, що Wi-Fi найбільш поширена бездротова технологія (після стільникового зв'язку), широко застосовувана в кафе, школах, офісах, житлових приміщеннях і т.д. За результатами тестів Health Canada пише про те, що вплив радіохвиль мінімально і не несе загрози для людини.

• Health Protection Agency UK заявило, що емісія WLAN значно нижче норм ТО. Агентство провело заміри в офісах, виміряти щільність впливу і за отриманими показниками виявило відсутність шкоди для здоров'я.

• Університет Пенсільванії провів 336 вимірювань в 45 місцях, в чотирьох країнах, в яких виміри сигналів від Wi-Fi перевищують допустимий рівень впливу сигналу.

З проведених досліджень отримано висновок, що при роботі мережі WLAN в звичайному режимі, радіочастотні поля на значно нижчих рівнях, ніж граничні значення. У всіх замірах, рівні сигналу від Wi-Fi були нижчі від міжнародних норм, таких як IEEE C95.1-2005 і ICNIRP і майже у всіх випадках набагато нижче інших радіосигналів в тій же навколишньому середовищу Проведені наукові дослідження показують, що радіохвилі Wi-Fi не потребують в збільшенні заходів безпеки і обмеження у використанні.

Іншими слова немає причин для утримання від використання переваг, наданих технологією. Випромінювання сигналу від обладнання Wi-Fi у всіх місцях, доступних для широкої публіки, має бути не вище рівня, встановленого офіційними медичними інструкціями з техніки безпеки.

Межі, певні в нормативних інструкціях, набагато нижче «порогу шкідливості» і засновані на даних тисяч виданих наукових досліджень по впливу випромінювання радіохвиль.

2.6. Висновки до розділу 2

У розділі розглянуто основні терміни і елементи мережі, актуальні стандарти бездротових мереж, їх аутенфікацію та механізми шифрування. Також, розглянуто технології Wi-Fi які пливають на здоров'я людини.

РОЗДІ 3
НАУКОВО-ДОСЛІДНА ЧАСТИНА

3.1. Порівняння продуктивності 802.11n і 802.11ac

У процесі дослідження двох стандартів була зібрана тестовий майданчик (рис 3.1), що складається з однієї точки доступу і двох Wi-Fi адаптерів:

• Точка доступу D-Link DAP2690 (802.1 1a / b / g / n / ac, 3x3MIMO, 80 MHz);

• Wi-Fi приймач Asus PCE-AC68 (802.1 1ac, 3x3MIMO, 80MHz);

• Wi-Fi приймач Asus N14 (802.1 1n, 3x3MIMO, 40MHz).

Суть експерименту в послідовному зборі вимірів даних для кожного адаптера, поступово збільшуючи кількість інформаційних потоків. В процесі тестування точка доступу конфігурувати залежно від стандарту використовуваного адаптера.

Рисунок 3.1 Схематичне відображення тестового майданчика

Підсумки дослідження функціонування Wi-Fi приймачів в залежності від кількості потоків даних можна побачити в таблиці 3.1.

Таблиця 3.1

Порівняння продуктивності 802.11n та 802.11ac

Адаптер \ кількість потоків	1	2	3	4	5	6	7	8
802.11ac	168.74	293.63	351.44	385.32	414.84	425.65	440.32	442.60
802.11n	110.27	143.88	161.682	162.91	160.27			

При трансляції одного потоку інформації перевагу технології 802.11ac неочевидно: 802.11n демонструє 110Mbps при 40MHz, а 802.11ac 169Mbps при 80MHz.

Далі ж при зростанні кількості потоків Wi-Fi приймач 802.11n зупиняє ріст швидкості приймача вже на трьох потоках (162 Mbps). Одночасно інший адаптер не знижує тенденцію збільшення швидкості аж до семи потоків. Очевидно, що значення питомої швидкості на потік знижується, однак продовжує бути більш ефективним.

Нижче продемонстровано переваги технології 802.11ac (рис 3.2).

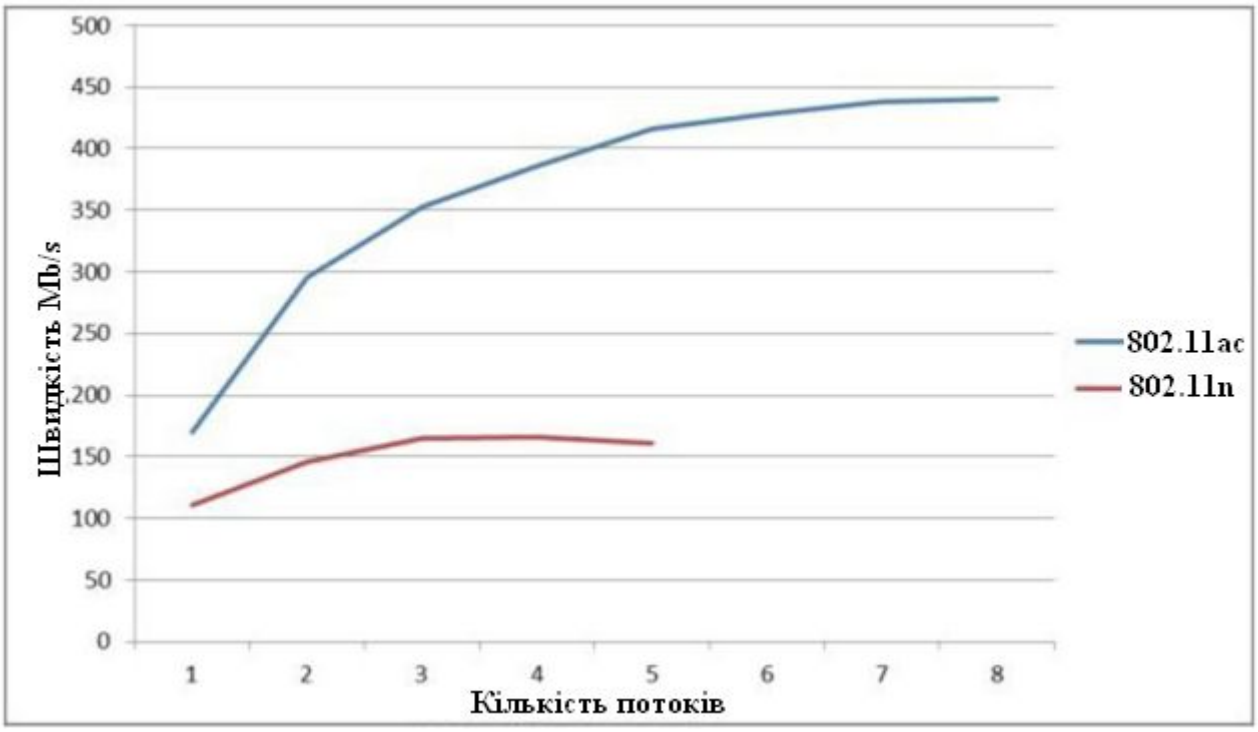


Рисунок 3.2 Графіки продуктивності 802.11ac і 802.11n 3.1.

Розрахунок зони покриття Для того щоб знайти зону покриття каналу зв'язку необхідно прояснити такі поняття як:

• відстань між об'єктами – D;

• центральна частота каналу - F;

• втрати у вільному просторі - FSL (free space loss).

Вираз для розрахунку відстані зв'язку потрібно взяти з формули за якою розраховуються втрати у вільному просторі:

$$FSL = 33 + 20(lgF + lgD)$$

За виразом обчислюється FSL:

$$FSL = Y_{\text{дБ}} - SOM$$

де SOM це запас в енергетиці радіозв'язку прийнятий брати рівним 10 дБ достатнього для інженерного розрахунку, а сумарне підсилення системи виражається таким чином:

$$Y_{\text{дБ}} = P_{t,\text{дБмВт}} + G_{t,\text{дБ}u} + G_{r,\text{дБ}u} - P_{min,\text{дБмВт}} - L_{t,\text{дБ}} - L_{r,\text{дБ}}$$

Де $L_{r,\text{дБ}}$ - втрати сигналу в кабелі приймає тракту, $L_{t,\text{дБ}}$ - втрати сигналу в кабелі передавального тракту, $P_{min,\text{дБмВт}}$ - чутливість приймача на даній швидкості, $G_{r,\text{дБ}u}$ - коефіцієнт посилення приймаючої антени, $G_{t,\text{дБ}u}$ - коефіцієнт посилення передавальний антени, $P_{t,\text{дБмВт}}$ - потужність передавача.

В результаті отримуємо формулу для дальності зв'язку:

$$D = 10^{\left(\frac{FSL}{20} - \frac{33}{20} - lgF\right)}$$

Знайдемо відстань на якому буде стабільно працювати зв'язок при схемі кодування MSC7 для точки доступу D-Link DAP2690 і бездротового адаптера Asus PCE-AC68. Їх паспортні характеристики при MSC7:

• Потужність передавача D-Link DAP2690: 14 дБмВт;

• Потужність передавача Asus PCE-AC68: 14 дБмВт;

• Чутливість D-Link DAP2690: -68 дБмВт;

• Чутливість Asus PCE-AC68: -68 дБмВт;

• Коефіцієнт посилення антени D-Link DAP2690: 6 дБи;

• Коефіцієнт посилення антени Asus PCE-AC68: 6 дБи.

Втрати в антенно-фидерном тракті опускаємо.

Рішення:

Знайдемо відстань при схемі MSC7.

Параметр FSL дорівнює

$$FSL = 14 + 6 * 3 - (-68) - 10 = 90\text{дБ}$$

Знайдемо дальність зв'язку (як приклад візьмемо сотий канал):

$$D_{MSC7} = 10^{\left(\frac{90}{20} - \frac{33}{20} - lg5500\right)} = 0{,}128 \text{ км} \approx 130 \text{ м}$$

3.4. Висновки до розділу 3

В розділі проведений огляд і порівняльний аналіз найбільш актуальних технологій бездротового зв'язку, зокрема 802.11n і 802.11ac. поставлено експеримент та проведено дослідження роботи сучасного стандарту WI-Fi 802.11ac.

РОЗДІЛ 4.
СПЕЦІАЛЬНА ЧАСТИНА

4.1. Область застосування програмного забезпечення Microsoft Office Visio.

Програмні продукти Visio Corporation, об'єднані під загальною назвою Visio, останнім часом активно завойовують світ, виступаючи вже не в якості одного із зразків, а як еталон ділової графіки.

Коли необхідно що-небудь пояснити співрозмовникові, простіше за все взяти олівець і намалювати. Це може бути схема з декількох прямокутників, розташування якихось предметів, зв'язки між об'єктами. Практично в будь–якому звіті, нотатках, поясненнях, статтях є місце для графічного матеріалу. Десь він допомагає розібратися у суті понять і зв'язків, а десь просто робить документ більш привабливим. Усі ці застосування відносяться до ділової графіки.

Власне, для малювання на комп'ютері існують десятки різних засобів. Це і прості графічні редактори типу Paint, і системи растрової графіки типу PhotoFinish, і векторні системи типу Corel Draw. У конструюванні використовуються так звані CAD–системи (системи комп'ютерного проектування – computer – aided design).

Visio не замінює усіх існуючих, особливо сильно розвинутих професійних систем, але усе більш тіснить їх. Особливо це помітно у середовищі професіоналів. Відомо, що професіонала, що звик до одного продукту, практично неможливо схилити до переходу на інший. Але з'являється багато прикладів, коли інженер, що використовує, наприклад, AutoCAD, починає все частіше і частіше застосовувати ще й Visio. Адже існують області, для яких немає спеціалізованих продуктів окрім Visio. Не існує іншого спеціального графічного редактора для малювання хімічних структурних діаграм, ніхто швидше Visio не впорається з малюванням блок– схем

алгоритмів, структурних схем, презентаційною графікою і багатьох інших типів малюнків.

Таким чином Visio відноситься до тих продуктів, які повинні бути на кожному комп'ютері, так само як практично на кожному комп'ютері є текстовий редактор. І незалежно від того, хто за ним працює – студент або академік, початківець або професіонал – Visio надасть йому неоціниму допомогу.

4.2. Загальні принципи програми Microsoft Office Visio.

В основі механізму малювання Microsoft Office Visio лежить векторний редактор. Тобто в простому випадку, не використовуючи жодних досконаліших засобів, ви маєте декілька графічних примітивів (лінія, крива, прямокутник, еліпс тощо), за допомогою яких можна намалювати потрібне зображення, зафарбувати його фрагменти.

Для двовимірних фігур можна використовувати не лише колір, але і зразки зафарбовування. Існують команди для роботи з текстовими блоками, що використовують шрифти, встановлені у Windows, що дозволяють форматувати слова, абзаци та інші фрагменти тексту.

Одиницею малюнка у Visio є шейп (shape – форма, графічний образ). Малюнок набирається з шейпів, як з елементів конструктора, причому при роботі потрібні набори шейпів розташовуються під рукою поряд з вікном малюнка, як палітра у художника. Процес створення малюнка зводиться до перетаскування шейпів з палітри (трафарету) у вікно малюнка і додаванні з'єднувальних елементів.

Набори шейпів адаптують Visio до тієї або іншої області використання і багато в чому визначають ту або іншу версію продукту. Наприклад, версія Visio Professional містить близько 1000 мережевих і телекомунікаційних шейпів, а версія Visio Enterprise – містить велику кількість шейпів для побудови мереж LAN і WAN. Шейпів розроблена велика кількість, вони продовжують розроблятись і можуть розроблятися самим користувачем для певної

специфічної області використання.

Але це не є найголовнішою відмінністю Visio. Виявляється шейпи мають інтелект. Тобто вони знають, як поводитися при тих або інших змінах малюнка. Наприклад, може існувати шейп стіни з віконним отвором, в якому при зміні розмірів стіни збільшуються, а розміри віконного отвору залишаються незмінними, причому ці розміри автоматично відслідковуються.

І, мабуть, останній штрих – існування коннекторів – шейпів, подібних до звичайної лінії, але за рахунок своєї інтелектуальності мають здатність приклеюватися до певних точок інших шейпів, зв'язуючи їх і зберігаючи цей зв'язок при переміщенні шейпів. Тобто, ви можете пересунути декілька мікросхем на схемі двома рухами миші, і при цьому усі електричні зв'язки залишаться незмінними. Найрозумніші коннектори ще й відшукують оптимальний шлях на малюнку, щоб по можливості не перекривати інші шейпи.

4.2.1. Шаблони і трафарети.

Найважливіші елементи Visio – шаблони і трафарети – служать для адаптації програми до потрібної прикладної області і надання процессу малювання властивій Visio легкості і зручності.

Шаблон (Template) – термін, що міцно увійшов останнім часом до практики офісних додатків Windows. У загальному випадку – це спеціальний файл, в якому зберігається інтерфейс додатку, а часто і прообраз малюнка або документу. До складу основних елементів, що зберігаються, входять властивості сторінки малюнка (такі як розмір сторінки, масштаб зображення, одиниця виміру тощо), набір і параметри стилів ліній, тексту і зафарбовування, набір трафаретів, що використовуються.

Подальший розвиток шаблону – візарди (Wizards – помічники, чарівники) – програмні елементи, як при створенні нового файлу малюнка окрім відкриття шаблону і потрібних трафаретів ведуть діалог з користувачем, щоб прийняти значення деяких змінних, і налагоджують малюнок у відповідності до їх значення.

Трафарет (Stencil) – файл з набором майстер–шейпів, зазвичай об'єднаних

якою–небудь загальною ідеєю або орієнтованих на певну прикладну область.

4.2.2. Організація робочого простору Visio. Типи файлів.

Робочий простір Visio містить вікна, меню та інструменти, що використовують для малювання. Його можна налагоджувати, пристосовуючи до області діяльності або просто до своїх звичок.

Користувач може змінювати наступні елементи:

- розмір і положення вікон Visio;
- розмір і розміщення трафаретів Visio;
- спосіб відображення майстер–шейпів в новому в трафареті;
- зображення сторінки;
- лінійки, лінії сітки, точки зв'язку, направляючі лінії;
- зовнішній вигляд панелі інструментів і рядка стану.

Частіше програму Visio запускають або для того, щоб намалювати новий малюнок, або для того, щоб відредагувати існуючий.

Створення нового малюнка зазвичай починають, відкриваючи файл шаблону, який у свою чергу завантажує Visio, відкриває трафарет і сторінку малюнка.

Вже наявний файл відкривається по–різному в залежності від майбутньої роботи. Користувач може відкрити:

- початковий файл, щоб редагувати його;
- копію файла, щоб змінити файл, не впливаючи на оригінал;
- версію тільки для читання, щоб проглянути файл, не змінюючи його.

Visio використовує чотири типи файлів: шаблони, трафарети, малюнки, і робочі простори. Ви можете ідентифікувати тип файлу по em розширенню. Шаблон має розширення .VST, трафарет – .VSS, малюнок – .VSD, робочий простір – .VSW.

Після внесення істотних змін до малюнка, необхідно зберегти файл малюнка. При зміні трафарету або шаблону може виникнути потреба знадобитися зберегти їх.

За замовчуванням Visio зберігає існуючі файли в тому форматі, в якому

вони були створені. Користувач може зберігати файли Visio у додаткових форматах, враховуючи більш ранні версії Visio, використовуючи команду Save As.

Для побудови діаграми, архітектура серед інших фігур у цій роботі виконувалось різних процедур такі як:

Відкрилось програму та вибралось тип фігури або архітектури, які ми хочемо зробити (рис.4.1);

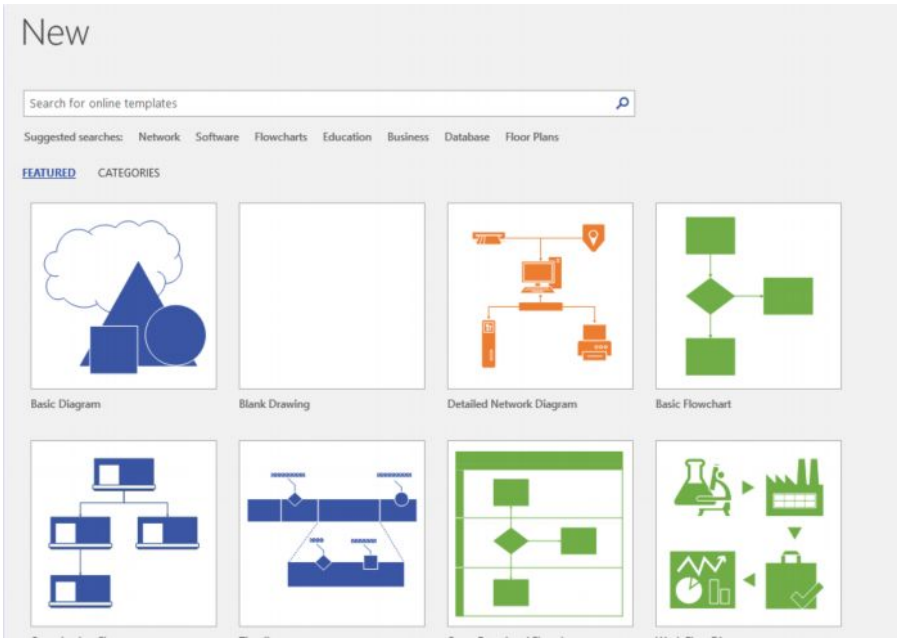


Рисунок 4.1 Панель діаграм у програмного забезпечення VISIO

Для дипломної роботи, мова йде про супутникові системи та телекомунікації, тоді було обрано два варіанти: *Детальний сегментний діаграми* та *бланкова діаграма* (рис.4.1);

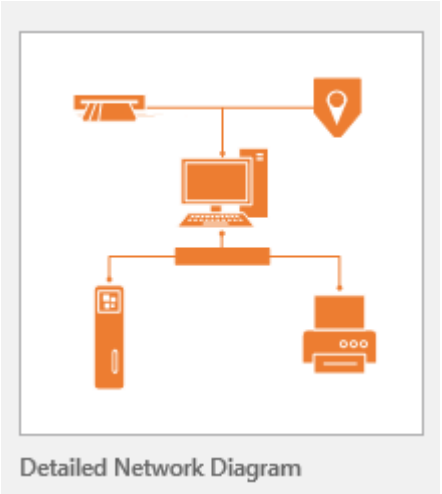


Рисунок 4.2 Детальна модель побудови мережевого діаграм

Детальна модель бо вона приносить з собою деякі мережеві пристрої. Моє завдання було тільки додати до неї кілька елементів для побудови бажаної архітектуру в цьому випадку принципову архітектуру.

Для додавання потрібних цифр та надписів потрібно як показано на (рис.4.3) вибирати TEXT BOX як показано у жовтому кольорі. Можна змінювати кольори, збільшити розмір фігури серед інших варіантів.

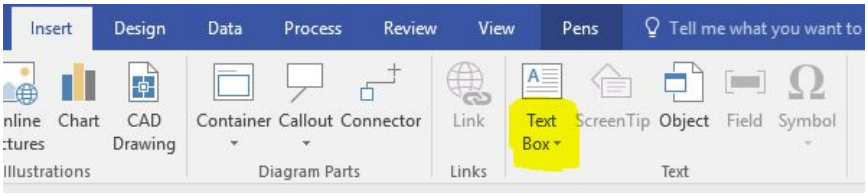


Рисунок 4.3 Вікно для додавання цифр або текст

4.3 Висновок до розділу 5

У цьому розділі описано кроки, які використовувались для побудови структурних схем та архітектури цієї магістерської роботи. За допомогою програмного забезпечення Microsoft Office Visio можна проектувати та використовувати в різних областях навчання від бухгалтерського обліку до механіки. У нього типові та унікальні функції, які багато допомагають і дуже прості у використанні.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1. Охорона праці

В процесі проведення НДР із застосування системи виявлення сигналів, яка підключена до електромережі 220 В, може виникнути електротравматизм як факторів негативного впливу на умови праці обслуговуючого персоналу при роботі із системою. Тому розробка рекомендацій по питанням охорони праці щодо мінімізації негативного впливу електричного струму на обслуговуючий персонал при роботі із системою виявлення сигналів із застуванням стандартів ГОСТ 12.1.009-76. «ССБТ. Електробезпека. Терміни і визначення» та ГОСТ 12.1.038-88 «Электробезопасность. Предельно допустимые значения напряжений прикосновения и токов» є актуальною задачею.

Струм, який проходить крізь людину, є головним ушкоджуючим фактором при електротравмі. Згідно з ГОСТ 12.1.009-76 розрізняють три ступені впливу струму при проходженні через організм людини (змінний струм) [22]:

- відчутний струм – початок болісних відчуттів (до 0-1,5 мА);
- невідпускний струм – судоми і біль, важке дихання (10-15 мА);
- фібриляційний струм – фібриляція серця при тривалості діє струму 2-3с, параліч дихання (90-100 мА).

Основні причини нещасних випадків від дії електричного струму під експлуатації системи:

• випадковий дотик до струмопровідних частин пристрою, що перебувають під напругою;

• поява напруги дотику на металевих конструктивних частинах пристрою (корпусах) у результаті пошкодження ізоляції або з інших причин;

Гранично допустимі значення напруги доторкання та сили струму для нормального (безаварійного) та аварійного (пристрій має певні пошкодження)

режимів пристрою при проходженні струму через тіло людини по шляху „рука - рука” чи „рука - ноги” регламентуються ГОСТ 12.1.038-88 (таблиці 5.1 та 5.2).

Таблиця 5.1

Граничнодопустимі значення напруги та сили струму, що проходить через тіло людини при нормальному режимі пристрою

Вид струму	U*доп*, В (не більше)	I*л*, мА (не більше)
Змінний, 50 Гц	2	0,3
Постійний	8	1

При виконанні роботи в умовах високої температури (більше 25 °С) і відносної вологості повітря (більше 75 %) значення таблиці 5.1 необхідно зменшити у три рази.

Таблиця 5.2

Граничнодопустимі значення струму, що проходять через тіло людини при аварійному режимі пристрою

Вид струму	Нормоване значення	Тривалість дії струму t, с
Змінний, 50 Гц, *Uдот*, В (не більше) *Ил*, мА (не більше)	0,1 500 500	0,2; 0,5; 0,7; 1,0; Більше 1,0 250; 100; 70; 50; 36 250; 100; 70; 50; 6
Постійний *Uдот*, В (не більше) *Ил*, мА (не більше)	 500 500	 400; 250; 230; 200; 40 400; 250; 230; 200; 15

Електробезпека згідно ГОСТ 12.1.009-76 та ГОСТ 12.1.038-88 – це система організаційних і мехнічних заходів і засобів, які забезпечують захист людей від шкідливої і небезпечної дії електричного струму.

Основними заходами захисту від ураження електричним струмом при експлуатації системи:

• забезпечення недоступності струмопровідних частин, що перебувають

під напругою, для випадкового дотику;

• усунення небезпеки ураження з появою напруги на корпусі сиситеми, що досягається захисним заземленням або захисним відключенням;

• захист від випадкового дотику до струмопровідних частин системи застосуванням кожухів або подвійної ізоляції;

• контроль і профілактика пошкоджень ізоляції системи;

• компенсація ємнісної складової струму замикання на землю;

• організація безпечної експлуатації системи.

Профілактика пошкоджень ізоляції системи спрямована на забезпечення її надійної роботи. Насамперед необхідно виключити механічні пошкодження, зволоження, хімічний вплив, запилення, перегріви. Але навіть у нормальних умовах ізоляція поступово втрачає свої початкові властивості, "старіє". З часом розвиваються місцеві дефекти. Опір ізоляції починає різко зменшуватися, а струм витоку - непропорційно зростати. У місці дефекту з'являються часткові розряди струму, ізоляція вигорає. Відбувається так званий пробій ізоляції, внаслідок чого виникає коротке замикання, що, у свою чергу, може спричинити пожежу чи ураження людей струмом. Щоб підтримувати діелектричні властивості ізоляції пристрою, необхідно систематично виконувати профілактичні випробування, огляди, видаляти непридатну ізоляцію і заміняти її.

Таким чином, врахувавши вище сформульовані рекомендації по питанням охорони праці при експлуатації системи реєстрації пульсового сигналу, буде забезпечено небезпечні умови праці обслуговуючого персоналу.

5.2 Безпека в надзвичайних ситуаціях

Створення оптимальних комфортних умов у виробничих приміщеннях по виготовленню системи виявлення сигналів та окремих його деталей є складною задачею, вирішити яку можна наступними заходами та засобами:

– Удосконалення технологічних процесів та устаткування.

– Впровадження нових технологій та обладнання, які не пов'язані з

необхідністю проведення робіт в умовах інтенсивного нагріву дасть можливість зменшити виділення тепла у виробничі приміщення. Наприклад, заміна гарячого способу обробки металу — холодним, нагрів полум'ям – індуктивним, горнових печей – тунельними.

– Раціональне розміщення технологічного устаткування. Основні джерела теплоти бажано розміщувати безпосередньо під аераційним ліхтарем, біля зовнішніх стін будівлі і в один ряд на такій відстані один від одного, щоб теплові потоки від них не перехрещувались на робочих місцях. Для охолодження гарячих виробів необхідно передбачити окремі приміщення. Найкращим рішенням є розміщення тепловипромінюючого обладнання в ізольованих приміщеннях або на відкритих ділянках.

– Автоматизація та дистанційне управління технологічними процесами. Цей захід дозволяє в багатьох випадках вивести людину із виробничих зон, де діють несприятливі фактори (наприклад автоматизоване завантаження печей в металургії, управління розливом сталі).

– Раціональна вентиляція, опалення та кондиціювання повітря. Вони є найбільш розповсюдженими способами нормалізації мікроклімату у виробничих приміщеннях. Так зване повітряне та водоповітряне душування широко використовується у боротьбі з перегріванням робітників в гарячих цехах.

Забезпечити нормальні теплові умови в холодний період року в надтогабаритних та полегшених промислових будівлях дуже важко і економічно недоцільно. Найбільш раціональним варіантом в цьому випадку є застосування променистого нагрівання постійних робочих місць та окремих дільниць. Захист від протягів досягається шляхом щільного закривання вікон, дверей та інших отворів, а також влаштуванням повітряних і повітряно-теплових завіс на дверях і воротах.

Раціоналізація режимів праці та відпочинку досягається скороченням тривалості робочої зміни, введенням додаткових перерв, створенням умов для ефективного відпочинку в приміщеннях з нормальними метеорологічними умовами. Якщо організувати окреме приміщення важко, то в гарячих цехах

створюють зони відпочинку – охолоджувальні альтанки, де засобами вентиляції забезпечують нормальні температурні умови.

Для робітників, що працюють на відкритому повітрі зимою, обладнують приміщення для зігрівання, в яких температуру підтримують дещо вищою за комфортну. Застосування теплоізоляції устаткування та захисних екранів В якості теплоізоляційних матеріалів широко використовуються: азбест, азбоцемент, мінеральна вата, склотканина, керамзит, пінопласт.

На виробництві застосовують також захисні екрани для відгородження джерел теплового випромінювання від робочих місць. За принципом захисту щодо дії тепла екрани бувають відбиваючі, поглинаючі. відвідні та комбіновані. Хороший захист від теплового випромінювання здійснюють водяні завіси, що широко використовуються в металургії.

Використання засобів індивідуального захисту. Важливе значення для профілактики перегрівання мають індивідуальні засоби захисту. Спецодяг повинен бути повітро- та вологопроникним (бавовняним, з льону, грубововняного сукна), мати зручний покрій. Для роботи в екстремальних умовах застосовуються спеціальні костюми з підвищеною теплосвітловіддачею. Для захисту голови від випромінювання застосовують дюралеві, фіброві каски, повстяні капелюхи; для захисту очей – окуляри – темні або з прозорим шаром металу, маски з відкидним екраном. Захист від дії зниженої температури досягається використанням теплого спецодягу, а під час опадів – плащів та гумових чобіт.

5.3 Висновки до розділу 5

У підрозділі з охорони праці сформульовані рекомендації по охорони праці з питань електробезпеки обслуговуючого персоналу при експлуатації системи виявлення сигналів, буде забезпечено безпечні умови праці при експлуатації системи і тим самим мінімізовано ризик ушкодження персоналу електричним струмом. У підрозділі з безпеки в надзвичайних ситуаціях проаналізовано оптимальні комфортні умови у виробничих приміщеннях по

виготовленню системи виявлення сигналів.

ЗАГАЛЬНІ ВИСНОВКИ

У даній роботі був проведений огляд і порівняльний аналіз найбільш актуальних технологій бездротового зв'язку. Розкрито поняття основ передачі інформації в бездротової середовищі. Проведено дослідження роботи сучасного стандарту WI-Fi 802.11ac

Встановлено, що найактуальнішою проблемою локальний бездротових мереж на сьогоднішній день, є захист переданих даних. Тому розглянуті основні схеми шифрування і модуляції сигналу, показані уразливості і способи їх утилізації.

Досліджено основні стандарти бездротового зв'язку 802.11. Була розглянута гіпотеза про шкоду здоров'ю від використання Wi-Fi.

В експериментальній частині роботи було проведено порівняння продуктивності актуального стандарту в порівнянні з попереднім. Виявлено перевагу в швидкості передачі інформації і зони покриття при багатоканальної роботі.

ПЕРЕЛІК ПОСИЛАНЬ

1. Сергиенко, А.Б. Цифровая обработка сигналов: Учеб. пособие / А.Б. Сергиенко. - СПб.: Питер, 2003 - 604 с.: ил

2. Прокис Дж. Цифровая связь: Пер. с англ. / Под ред. Д. Д. Кловского.— М.: Радио и связь, 2000.— 800 с.

3. Рабинер Л. Теория и применение цифровой обработки сигналов / Л. Рабинер, Б. Гоулд. - М. : Мир, 1978. - 847 с.

4. Уидроу, Б. Адаптивная обработка сигналов. / Уидроу Б. Стирнз С.Д.; Пер. с англ. под ред. Шахгильдяна В.В. - М.: Радио и связь, 1989. - 440 с.

5. Лайонс, Р. Цифровая обработка сигналов: Второе издание. Пер. с англ. / Под ред. А.А.Бритова. - М.: ООО «Бином-Пресс», 2006 г. - 656 с.: ил

6. Пролетарский, А.В. Беспроводные сети Wi-Fi / Пролетарский А.В., Чирков Д.Н – М.: Национальный Открытый Университет «ИНТУИТ», (Основы информационных технологий) 2016.

7. Семенов, Ю.А. Алгоритмы и протоколы каналов и сетей передачи данных. Учебное пособие / Семенов Ю.А. – М.: Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2007. -634с.

8. Челухин, В.А. Комплексное обеспечение информационной безопасности автоматизированных систем: учебное пособие / Челухин В.А. – Комсомольск- на-Амуре: ФГБОУ ВПО «КнАГТУ», 2014.- 207с.

9. Гейер, Джим. Беспроводные сети. Первый шаг: Пер с англ. – М.:Издательский дом «Вильяме», 2005.- 192с.

10. Официальный сайт компании D-Link [электронный ресурс] – Режим доступа: www.dlink.ru

11. Википедия, русский проект свободной многоязычной энциклопедии [электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/

12. Стандарты Wi-Fi [электронный ресурс] – Режим доступа: http://viconnect.ru/

13. WPA2-Enterprise, или правильный подход к безопасности Wi-Fi сети [электронный ресурс] – Режим доступа: http://habrahabr.ru/post/150179

14. Модуляция радиосигнала [электронный ресурс] – Режим доступа: https://habrahabr.ru/company/yota/blog/119047/

15. Кратко о MIMO [электронный ресурс] – Режим доступа: http://wi-life.ru/wifi-academy-rus/80211n-mimo-2

16. Технология сетей. Все для построения сетей [электронный ресурс] – Режим доступа: https://nettech.ua/

17. В поисках Wi-Fi [электронный ресурс] – Режим доступа: https://xakep.ru/2016/05/26/www-3wifi/

18.

ДОДАТОК А

Копія тези конференції

ЗМІСТ

УДК 621:396

Дунець В.Л., к.т.н., завідувач кафедри радіотехнічних систем
Бекус Р.В., студент 6 курсу спеціальності «Телекомунікації та радіотехніка»

ДОСЛІДЖЕННЯ ПОКАЗНИКІВ ЯКОСТІ ПЕРЕДАЧІ СИГНАЛІВ В БЕЗДРОТОВИХ ЛОКАЛЬНИХ МЕРЕЖАХ

Тернопільський національний технічний університет імені Івана Пулюя

Мобільні телефони, планшети та ноутбуки є невід'ємною частиною сучасної комунікативної людини, а бездротові локальні мережі дають змогу обмінюватися даними. Основне завдання при проектуванні бездротових локально обчислювальних мереж - це вирішення проблем завадостійкості, а також забезпечення належного рівня швидкості передачі і безпеки даних.

З метою забезпечення належного рівня швидкості передачі даних проведений порівняльний аналіз найбільш актуальних технологій бездротового зв'язку: 802.11ac, 802.11n. В процесі дослідження двох стандартів зібраний тестовий макет, що складається з однієї точки доступу і двох Wi-Fi адаптерів:

- Точка доступу D-Link DAP2690 (802.11a/b/g/n/ac, 3x3MIMO, 80 MHz);
- Wi-Fi приймач Asus PCE-AC68 (802.11ac, 3x3MIMO, 80MHz);
- Wi-Fi приймач Asus N14 (802.11n, 3x3MIMO, 40MHz).

Суть експерименту в послідовному зборі вимірів даних при поступово збільшувані кількість інформаційних потоків для кожного адаптера. В процесі тестування точка доступу конфігурувалась в залежності від стандарту використовуваного адаптера. Результати дослідження функціонування Wi-Fi приймачів в залежності від кількості потоків даних подано в таблицю.

Таблиця 1

Порівняння 802.11ac і 802.11n

Адаптер\ кількість потоків	1	2	3	4	5	6	7	8
802.11ac	168.74	293.63	351.44	385.32	414.84	425.65	440.32	442.60
802.11n	110.27	143.88	161.682	162.91	160.27			

З таблиці видно, що при трансляції одного потоку інформації, перевага буде у технології 802.11ac: 802.11n демонструє 110Mbps при 40MHz, а 802.11ac 169Mbps при 80MHz. Далі ж при зростанні кількості потоків Wi-Fi приймач 802.11n зупиняє ріст швидкості прийому вже на трьох потоках (162 Mbps). Одночасно інший адаптер не знижує тенденцію збільшення швидкості аж до семи потоків. Очевидно, що значення питомої швидкості на потік знижується, однак продовжує бути більш ефективним.

Отже, в процесі дослідження, було проведено порівняння продуктивності стандарту 802.11ac в порівнянні з 802.11n, та виявлено перевагу в швидкості передачі інформації і зони покриття при багатоканальної роботі стандарту 802.11ac.

Перелік джерел посилання.

1. Технологія мереж. Все для побудови мереж [електронний ресурс] - Режим доступу https://nettech.ua/

2. Гейер, Джим. Беспроводные сети. Первый шаг: Пер с англ. – М.: Издательский дом «Вильяме», 2005.- 192с.