МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Роман ОДАРЧЕНКО
“_____” _____2022 р.

КВАЛІФІКАЦІЙНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ МАГІСТР

Тема: «Комплекс автоматизованого технічного обслуговування базової станції стільникової системи»

Виконавець: _____ Богдан ЧУМАЧЕНКО
(підпис)

Керівник: _____ Анатолій ТАРАНЕНКО
(підпис)

Консультанти з окремих розділів пояснювальної записки:

Консультант розділу «Охорона праці» _____ Батир ХАЛМУРАДОВ
(підпис)

Консультант розділу «Охорона навколишнього середовища»
_____ Євгеній БОВСУНОВСЬКИЙ
(підпис)

Нормоконтролер: _____ Денис БАХТІЯРОВ
(підпис)

Київ 2022

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

Роман ОДАРЧЕНКО
“_____”_____2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

Чумаченка Богдана Сергійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема кваліфікаційної роботи: «Комплекс автоматизованого технічного обслуговування базової станції стільникової системи»
затверджена наказом ректора від «07» вересня 2022 р. №1321/ст
2. Термін виконання роботи: з 05.09.2022 р. по 30.11.2022 р.
3. Вихідні дані до роботи:. аналіз структури стільникової системи та особливостей базової станції третього та четвертого поколінь, безпека локальних мереж, розробка методу бездротового технічного обслуговування БС, електромагнітна сумісність
4. Зміст пояснювальної записки: принцип побудови системи стільникового зв’язку третього та четвертого поколінь; регламентні роботи з технічного обслуговування РЛС; розробка способу дистанційного радіоуправління; обчислення параметрів радіовипромінювання
5. Перелік обов'язкового графічного (ілюстративного) матеріалу:. слайди презентації в програмному пакеті Microsoft PowerPoint

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів кваліфікаційної роботи	05.09.2022-06.09.2022	Виконано
2	Вступ	07.09.2022-10.09.2022	Виконано
3	Принцип побудови системи стільникового зв'язку третього та четвертого поколінь	12.09.2022-05.10.2022	Виконано
4	Регламентні роботи з технічного обслуговування РЛС	06.10.2022-15.10.2022	Виконано
5	Розробка способу дистанційного радіоуправління	17.10.2022-05.11.2022	Виконано
6	Обчислення параметрів радіовипромінювання	07.11.2022-12.11.2022	Виконано
7	Охорона праці	07.11.2022-12.11.2022	Виконано
8	Охорона навколишнього середовища	14.11.2022-19.11.2022	Виконано
9	Усунення недоліків та захист кваліфікаційної роботи	21.11.2022-30.11.2022	Виконано

7. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона праці	к.м.н., проф. Батир ХАЛМУРАДОВ		
Охорона навколишнього середовища	к.т.н., доц. Євгеній БОВСУНОВСЬКИЙ		

8. Дата видачі завдання: “22" серпня 2022 р.

Керівник кваліфікаційної роботи _____ Анатолій ТАРАНЕНКО
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Богдан ЧУМАЧЕНКО
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Кваліфікаційна робота «Комплекс автоматизованого технічного обслуговування базової станції стільникової системи» містить 134 сторінки, 60 рисунків, 7 таблиць, 46 використаних джерел.

АРХІТЕКТУРА МЕРЕЖІ, ЛОКАЛЬНА МЕРЕЖА, ТРАНСПОРТНА МЕРЕЖА, СТІЛЬНИКОВИЙ ЗВ'ЯЗОК, 4G, ЕФЕКТИВНІСТЬ, ЕМС, ЗОНА ПОКРИТТЯ.

Об'єкт дослідження – базова станція стільникового зв'язку "Flexi Multiradio BTS", яка працює у мережах 2G, 3G та 4G.

Предмет дослідження – методи підвищення ефективності використання бездротових мереж для регламентно-діагностичних робіт з обслуговування БС.

Мета дипломної роботи – є розробка методу дистанційного радіоуправління базовою станцією в процесі її технічного обслуговування за допомогою бездротового підключення.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1) аналіз структури стільникової системи та особливостей базової станції;

2) розгляд регламенту технічного обслуговування БС;

3) розробка методу дистанційного радіоуправління;

4) розрахунок зони покриття Wi-Fi-діапазону;

5) врахування електромагнітної сумісності/

Метод дослідження – методи теорії інформації та передавання сигналів для аналізу методів передавання інформації у широкосмугових радіосистемах стільникових мереж нового покоління; методи прямого синтезу для розробки структурної схеми мережі; методи проектного аналізу для вибору кращого проектного рішення; метод аналізу ієрархій, комп'ютерне моделювання для визначення основних характеристик спроектованої мережі.

Матеріали дипломної роботи рекомендується використовувати при проведені наукових досліджень, у навчальному процесі та в практичній діяльності фахівців, які займаються експлуатацією стільникових мереж зв'язку.

Прогнозні припущення щодо розвитку об'єкта дослідження – підвищення продуктивності та ефективності регламентних робіт з технічного обслуговування стільникових мереж зв'язку.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АТ	Абонентський термінал.	(Subscriber Terminal)
БС	Базова станція	(Base Station)
МС	Мобільна станція	(Mobile Station)
ЦК	Центр комутації	(Switching Center)
ЛОМ	Локальна обчислювальна мережа	(Local computer network)

Англомовні позначення:

UE	User Equipment	(Обладнання користувача)
UMTS	UMTS Subscriber Identity Module	(Модуль ідентифікації абонента UMTS)
ME	Mobile Equipment	(Мобільне обладнання)
CN	Core Network	(Базова мережа)
UTRAN	Universal Terrestrial Radio Access Network	(Універсальна наземна мережа радіодоступу)
RNS	Radio Network Subsystem	(Підсистема радіомережі)
NB	Node B	(Вузол В (базова станція))
RNC	Radio Network Controller	(Контролер радіомережі)
GERAN	GSM/EDGE Radio Access Network	(Мережа радіодоступу GSM/EDGE)
BTS	Base Transceiver Station	(Базова приймально-передавальна станція)
BSC	Base Station Controller	(Контролер базових станцій).
BSS	Base Station Subsystem	(Підсистема базових станцій).
SIM	Subscriber Identification Module.	(Модуль ідентифікації абонента)
LA	Location Area	(Район розташування)
MAP	Mobile Application Part	(Частина мобільних додатків)
ARQ	Automatic Retransmission Query	(Запит на автоматичну повторну передачу)
RRH	Remote Radio Head	(Дистанційна радіоголовка)
LAN	Local Area Network	(Локальна мережа)

NIC (Network Interface Controller) (Контролер мережевого інтерфейсу)

WLAN (Wireless LAN) (Бездротова локальна мережа)

PHY (Physical Layer) (Фізичний рівень)

DLL (Data Link Layer) (Канальний рівень даних)

CSMA (Carrier Sense Multiple Access) (Множинний доступ із визначенням несучої)

TDMA (Time Division Multiple Access) (Множинний доступ із розділенням часу)

MAC (Media Access Control) (Контроль доступу до медіа)

GSM Global System for Mobile Communication (Глобальна система мобільного зв'язку).

MS Mobile Station (Мобільна станція).

MSC Mobile services Switching Center (Центр комутації).

ВСТУП

Актуальність теми. Все ж таки, теперішній час й майбутнє зі стільниковим зв'язком, будуть дуже відрізнятися один від одного. Маючи такий шалений попит на стільниковий широкосмуговий доступ, як зараз, він буде продовжувати рости й рости, що в свою чергу закликає людство, весь час розвивати наші технології, щоб впоратися зі зростаючою смартизацією Інтернет технологій.

Через що зростає кількість нових локальних мереж, розширюються існуючі мережі, збільшується кількість користувачів цих мереж, підвищуються вимоги до якості розробки та розгортання мереж, і в той же час, проектування безпеки корпоративної мережі є одним із основних факторів при її створенні.

Будь-яке державне чи комерційне підприємство в нашій країні має об'єктивні процеси, які створюють важливість проблеми захисту інформації - під безпекою інформації підприємства зазвичай розуміють захист цієї інформації та захищеної мережі всієї команди від навмисних, випадкових дій або недосвідченості співробітників. і недбалість.

Дотримання вимог безпеки – єдиний спосіб захистити себе. Що стосується питання «Яка інформація потребує захисту та привертає увагу зловмисника?» Це, як правило, важливі терміни, список клієнтів, база облікових програм, паролі та ключі системи «клієнт-сервер», канали зв'язку з підрозділами тощо. Є два способи адекватної оцінки безпеки: перший заснований на близькості значення, заснованому на ідеї, що зловмисник отримає більше, якщо він витратить багато, щоб отримати доступ до інформації, а другий заснований на часовій близькості, заснованій на знищенні інформації докази справи. Проте витоки інформації та кількість завданих ними збитків постійно зростають. Причиною цього є недостатня безпека колективної мережі всередині підприємства та неналежне впровадження захищеного документообігу, що може призвести до навмисної крадіжки інформації, випадкової втрати та випадкового витоку.

У цьому випадку використання традиційних засобів захисту не дасть істотних результатів. Моніторинг удосконалення системи проектування мережі колективної безпеки компанії дозволяє аналізувати та вживати заходів щодо усунення та зменшення загроз.

Організація захисту безпеки підприємства повинна повністю відповідати чинному законодавству та нормативним актам з інформаційної безпеки. Більшість сучасних підприємств, незалежно від форми власності та виду діяльності, не можуть успішно здійснювати свою діяльність без забезпечення системи захисту інформації, включаючи організаційні, нормативні та технічні засоби захисту інформації під час обробки, зберігання та обміну в автоматизованих системах [1-30].

Об'єктом дослідження буде базова станція стільникового зв'язку, її планова діагностика за допомогою безпровідного з’єднання. Також буде розглянуто структуру системи UMTS, проведено аналіз конфігурацій мережі та конфігурації модулів обладнання базової станції, робота з застосунком для підключення до налаштувань базової та радіорелейної станцій, встановлення з’єднання з BSS через віддалений доступ, наведення та пояснення основних концепцій мережі та їх прикладів.

Однією з передумов для мобільного телефонного зв'язку є високочастотні електромагнітні радіохвилі. У деякому сенсі вони служать пристроєм передавання, який передає інформацію зі швидкістю світла. Сигнали виклику або даних оцифровуються і перетворюються в високочастотні електромагнітні поля.

Електромагнітні поля можна знайти всюди в нашому середовищі. Деякі з них мають природне походження; наприклад, поля, що виникають під час грози, а також сонячне світло. Електромагнітні поля, що генеруються технічними засобами, виникають там, де протікає електричний струм. Їх можуть генерувати, наприклад, радіо пристрої, телевізори, а також фени, мікрохвильові печі, стільникові телефони та багато інших електричних пристроїв.

Електромагнітні поля розрізняються по довжині хвилі: чим коротше довжина хвилі, тим буде вищою частота, та навпаки: чим вище частота, тим коротше діапазон сигналів. З цієї причини для широкого покриття стільникового зв'язку підходять тільки «нижні» діапазони частотного спектра, тобто частоти приблизно від 1 до 3800 МГц.

Якщо мобільний телефон рухається, наприклад, в рухомому автомобілі або поїзді, відбувається перемикання між сотами, так зване «Хендовер». І якщо сигнал прийому поточної станції стане слабкішим, а сигнал сусідньої станції стане сильнішим, то стільниковий пристрій узгоджено з базовими станціями– перемикається на ту соту, у якої кращі умови надання зв’язку.

У відповідності з усіма стандартами мобільного радіозв'язку стільникові телефони і базові станції мають пристрій управління для автоматичного регулювання потужності. Таким чином, потужність передачі знижується до мінімуму, необхідного для передачі стабільної передачі. Це зроблено для запобігання взаємних перешкод між передавачами і - особливо в разі мобільних телефонів - для зниження споживань енергії. У той же час більш низька потужність передачі, також призводить до зменшення випромінювання електромагнітної енергії. Мобільні телефони сконструйовані таким чином, що вони не тільки відповідають зазначеним граничним значенням, але і значно нижче їх.

На практиці структура стільникового зв'язку визначається численними індивідуальними вимогами, які пред'являються до сучасної мережі. Це, наприклад, достатня пропускна здатність, висока якість передачі голосу і даних з низьким рівнем помилок та зручність використання в масштабах усієї області, що також включає постачання зв’язку всередині будівель. Кожна сота може обслуговувати тільки обмежену кількість користувачів. Постійно зростаючий попит на пропускну здатність означає, що операторам потрібно збільшувати кількість мобільних радіопередавачів і, отже, саму кількість осередків радіозв'язку. Це дозволяє частіше повторювати використання однакових частот або кодів, доступних у відповідних мережах. Однак радіокомірок, в яких використовуються одні й ті ж частоти або коди, повинні перебувати досить далеко одна від одної, щоб не було взаємних перешкод.

На практиці в основному використовуються так звані секторні антени. Вони залишають поза передачею сигнал у всіх просторових напрямах, але в більшості випадків мають горизонтальний кут відкриття приблизний 120 °. Така «секторизація» в основному дозволяє встановлювати кілька антен на одному антенному місці. Із-за чого, різні сектори забезпечують різні підобласті - таким чином антенне місце може генерувати кілька окремих радіокомірок одночасно. Перевагами цього є збільшена ємність та зручне розташування.

Таким чином, актуальною є задача автоматизації обслуговування та діагностики базових станцій мобільного оператора. Метою дипломної роботи є розробка способу дистанційного радіоуправління базовою станцією в процесі її технічного обслуговування.

Мета – є розробка методу дистанційного радіоуправління базовою станцією в процесі її технічного обслуговування за допомогою бездротового підключення.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1) аналіз структури стільникової системи та особливостей базової станції;

2) розгляд регламенту технічного обслуговування БС;

3) розробка методу дистанційного радіоуправління;

4) розрахунок зони покриття Wi-Fi-діапазону;

5) врахування електромагнітної сумісності/

Об'єктом дослідження *є* – базова станція стільникового зв'язку "Flexi Multiradio BTS", яка працює у мережах 2G, 3G та 4G..

Предметом дослідження – спосіб апаратно-програмного дистанційного управління базової станції.

Науковою новизною є – проведення наукових досліджень, у навчальному процесі та в практичній діяльності фахівців, які займаються експлуатацією стільникових мереж зв'язку.

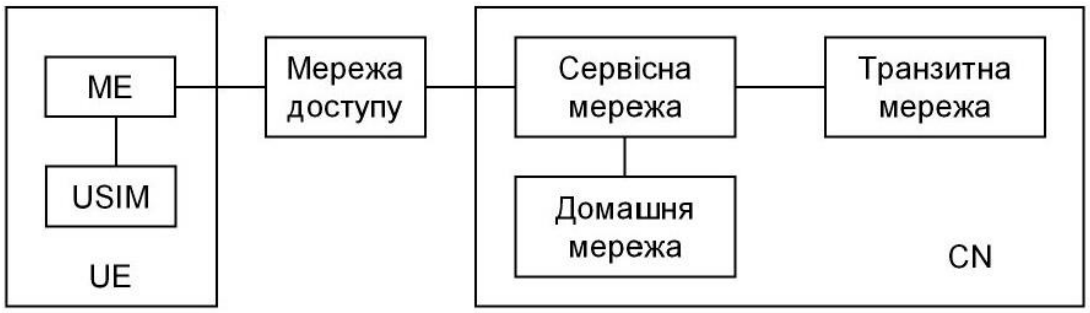
Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
ПРИНЦИП ПОБУДОВИ СИСТЕМИ СТІЛЬНИКОВОГО ЗВ'ЯЗКУ ТРЕТЬОГО ТА ЧЕТВЕРТОГО ПОКОЛІНЬ

1.1 Структура системи *UMTS*

На рис.1.1. наведена загальна структура системи.



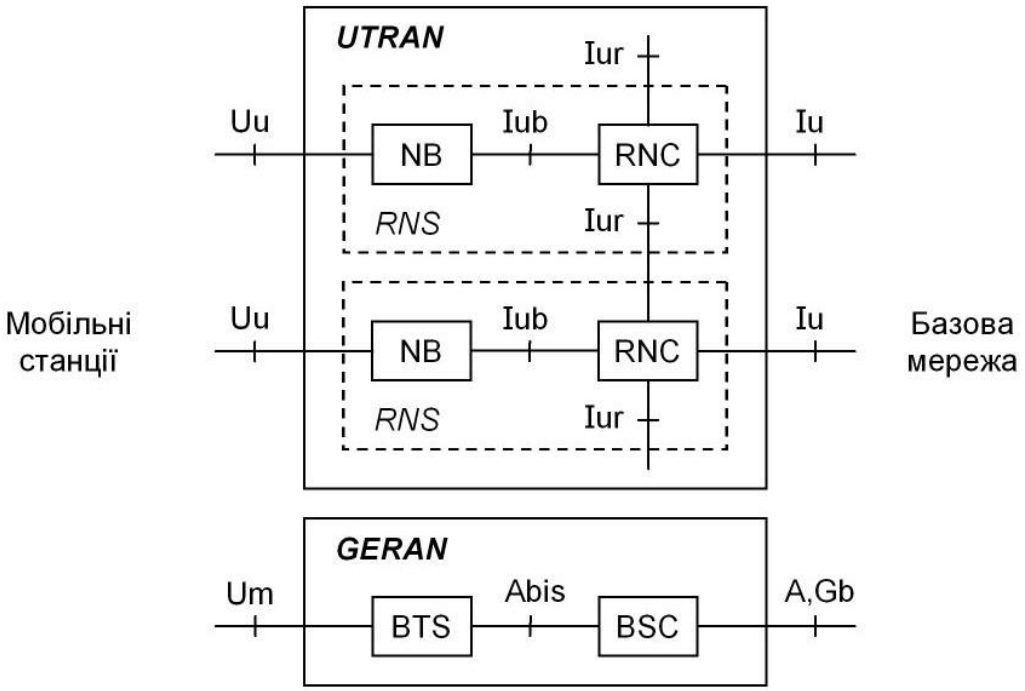
UE	User Equipment	Обладнання користувача (в GSM "Mobile Station")
USIM	UMTS Subscriber Identity Module	Модуль ідентифікації абонента UMTS
ME	Mobile Equipment	Мобільне обладнання (в GSM "Mobile Terminal")
CN	Core Network	Базова мережа (мережеве "ядро")

Рис.1.1. Структура системи UMTS

Модуль *USIM* містить мережні номери абонента, а також алгоритми і параметри мережної безпеки. Мережа доступу підтримує зв'язок між базовою мережею і мобільними станціями. Сервісна мережа передає інформацію від джерела до адресата і виконує фінансові розрахунки. Домашня мережа контролює умови підписки на послуги, а також забезпечує мережну безпеку. Транзитна мережа підтримує зв'язок абонента з зовнішніми мережами.

На рис.1.2. наведена структура мережі доступу.

Особливість *UTRAN* – це взаємодія між контролерами *RNC*, які виконують частину керуючих функцій базової мережі. Це зменшує час установлення з'єднання і пришвидшує виконання хендоверу.



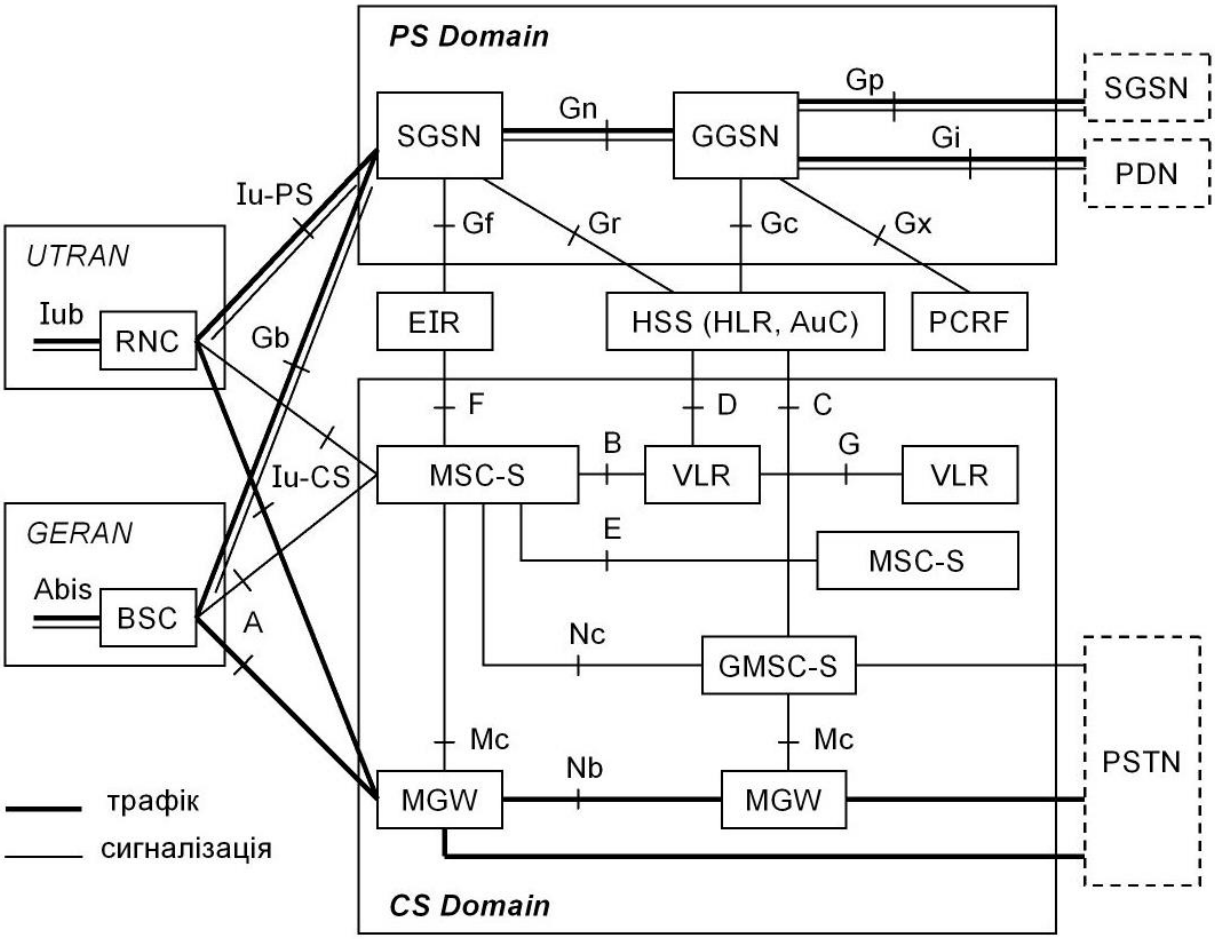
UTRAN	Universal Terrestrial Radio Access Network	Універсальна наземна мережа радіодоступу
RNS	Radio Network Subsystem	Підсистема радіомережі
NB	Node B	Вузол В (базова станція)
RNC	Radio Network Controller	Контролер радіомережі
GERAN	GSM/EDGE Radio Access Network	Мережа радіодоступу GSM/EDGE
BTS	Base Transceiver Station	Базова приймально-передавальна станція
BSC	Base Stations Controller	Контролер базових станцій

Рис.1.2. Мережа доступу

На рис.1.3. наведена структура базової мережі.

PS-домен з комутацією пакетів забезпечує передачу пакетного трафіку. Канальний ресурс в радіо-інтерфейсі не резервують і призначають в динамічному режимі. Ця комутація необхідна для зв'язку мобільної станції з пакетними мережами, зокрема з інтернетом.

CS-домен з комутацією каналів забезпечує передачу мови через виділений канал, який надають абоненту на весь час з'єднання. Це необхідно для зв'язку мобільної станції з телефонною мережею.



PS Domain	Packet-Switched Domain	Домен з комутацією пакетів
SGSN	Serving GPRS Support Node	Вузол підтримки GPRS з функцією сервера
GGSN	Gateway GPRS Support Node	Вузол підтримки GPRS з функцією шлюзу
CS Domain	Circuit-Switched Domain	Домен з комутацією каналів
MSC-S	Mobile Switching Center Server	Сервер центру комутації мобільних послуг
VLR	Visitor Location Register	Візитний регістр місцезнаходження
GMSC-S	Gateway MSC Server	Сервер шлюзу центру комутації
MGW	Media GateWay	Медіашлюз
EIR	Equipment Identity Register	Регістр ідентифікації обладнання
HSS	Home Subscriber Server	Домашній абонентський сервер
HLR	Home Location Register	Домашній регістр місцезнаходження
AuC	Authentication Center	Центр аутентифікації
PCRF	Policy and Charging Rules Function	Функція правил підписки та сплати
PDN	Packet Data Network	Мережа передачі пакетних даних (інтернет)
PSTN	Public Switched Telephone Network	Телефонна мережа загального користування

Рис.1.3. Базова мережа

Медіа-шлюз (*MGW*)

Типова структура зв'язків між центрами комутації і контролерами має вигляд:

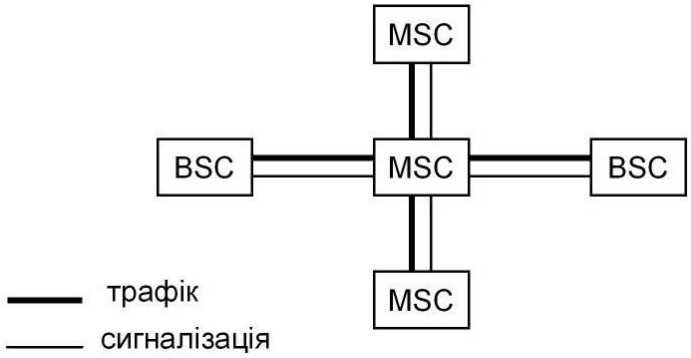


Рис.1.4.

Альтернативна структура, яка відповідає рис.1.3:

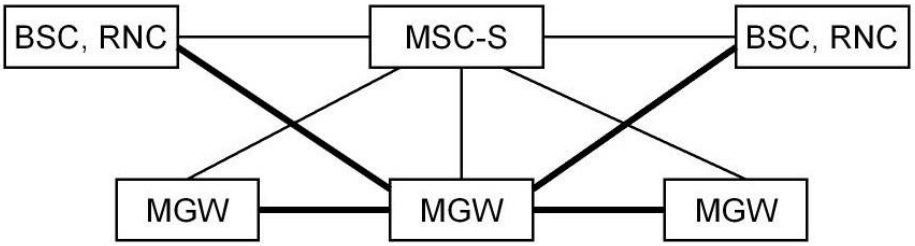


Рис.1.5.

Сервер *MSC-S* виконує управління з'єднаннями, обробку сигналізації, підготовку фінансових розрахунків, підтримує зв'язок з іншими мережами.

Шлюз *MGW* виконує комутацію каналів трафіку.

В системі з альтернативною структурою для збільшення абонентської ємності (це кількість абонентів, яких обслуговують одночасно), достатньо додати шлюз і модернізувати програмне забезпечення сервера. В типовій системі для цього потрібна заміна *MSC*. Проте, вартість *MSC* зазвичай перевищує вартість *MGW*, тому оператори застосовують альтернативний варіант в обох мережах радіодоступу, *GERAN* і *UTRAN*.

Передача мови

Розглянемо особливості мовного зв'язку з набором телефонного номеру. В цьому випадку комутацію каналу трафіку забезпечує домен *CS* (рис.1.3).

Мережа *GERAN*

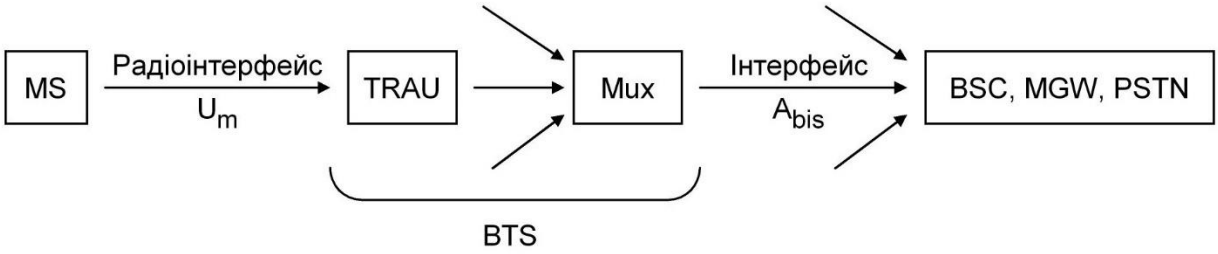


Рис.1.6. Передача мови

MS (*Mobile Station*) містить аналого-цифровий перетворювач, який виконує:

- дискретизацію аналогового мовного сигналу з інтервалом $\Delta t_д$=125 мкс;

- формування цифрового сигналу зі швидкістю передачі (13 бітів)/$\Delta t_д$=13/(125∗10^{-6})=104 кбіт/с.

Швидкість мовного кодера *RPE-LTP* дорівнює (260 бітів)/(20 мс)=13 кбіт/с.

У радіо-інтерфейсі мобільна станція займає один слот з 8 слотів у фреймі (метод доступу *TDMA*).

TRAU (*Transcoding and Rate Adaptation Unit*) декодує сигнал *RPE-LTP* і кодує дискретні відлікі мови за методом *PCM*, *Pulse Code Modulation*, який застосований в телефонній мережі *PSTN*.

Швидкість передачі сигналу *PCM* дорівнює

(8 бітів у слоті)/$\Delta t_д$=8/(125∗10^{-6})=64 кбіт/с – це так званий потік *E*0.

Mux – це мультиплексор, який реалізує метод *TDM* (*Time Division Multiplexing*) і об'єднує потоки *E*0 в потік *E*1:

Рис.1.7. Time Division Multiplexing

Слот 0 містить синхросигнал, слот 16 – повідомлення сигналізації. Мобільна станція займає один слот з 30-ти. Швидкість потоку *E*1 дорівнює (32 слоти)*(8 бітів у слоті)/Δtд=32*64 кбіт/с=2048 кбіт/с.

Тривалість біта за визначенням Tб=$\Delta t/n$=1/($n/\Delta t$), де у другому знаменнику записана швидкість передачі, тобто кількість бітів n, що передають в інтервалі Δt. Тому тривалість бітів 1/(13 кбіт/с) на виході *MS* > 1/(64 кбіт/с) на виході *TRAU* > 1/(2048 кбіт/с) на виході *Mux*.

Цей метод передачі має назву "часове ущільнення" цифрового сигналу.

Базова станція формує (1...4) паралельних потоків $E1$ в залежності від інтенсивності трафіку.

В напрямку передачі від контролера до мобільної станції здійснюють зворотні перетворення.

Швидкість 13 кбіт/с і параметри канального кодера вибрані для деяких типових умов розповсюдження радіохвиль. Ці умови змінюються під час руху абонента. Якщо на вході приймача відношення (сигнал+шум)/(шум) зменшується, то відсоток невиправлених помилок збільшується. Для зниження цього відсотку необхідно застосувати більш потужний канальний код і збільшити кількість надлишкових бітів. При цьому зменшується кількість бітів трафіку в цифровому потоці, який передається з певною заданою швидкістю. В цьому випадку потрібно знижувати кількість бітів мовного кодера в одиницю часу, тобто швидкість мовного кодування.

Таким чином, недолік мережі GERAN – це мовне кодування зі сталою швидкістю і канальне кодування з незмінними параметрами.

1.2 Мережа *UTRAN*

В радіо-інтерфейсі застосований метод множинного доступу з кодовим розділенням сигналів мобільних станцій, тобто метод *CDMA*.

Кодування мови виконують зі змінною швидкістю (принцип *AMR, Adaptive Multi Rate*).

Метод кодування має назву *ACELP, Algebraic Code Exited Linear Prediction*.

Швидкість кодера має 9 значень в діапазоні (6,60...23,85) кбіт/с, і може змінюватися в кожному фреймі. Чим менше відношення (сигнал+шум)/(шум) в радіоканалі, тим більше кількість надлишкових бітів канального кодера, і тим менше швидкість передачі цифрової мови.

В системі *GSM*, за підтримки *AMR* в мобільній станції, швидкість дорівнює (4,75...12,20) кбіт/с.

На рис.3 інтерфейс I_{ub} з'єднує базову станцію *NB* і контролер *RNC*. В цьому інтерфейсі на першому етапі розвитку системи застосована мережна технологія *ATM, Asynchronous Transfer Mode* – режим асинхронної передачі.

Принцип *ATM* полягає у тому, що після установлення з'єднання між передавачем і приймачем, цифровий потік розділяють на короткі пакети. Кожен з них містить заголовок 5 байтів і дані 48 байтів. Пакети передають через віртуальний канал, номер якого вказаний в заголовку. Такий канал існує протягом всього часу з'єднання. Технологія *ATM* забезпечує передачу мовного сигналу, даних і відеоінформації зі сталою і змінною швидкістю, а також з різними параметрами *QoS* (це відсоток втрати пакетів, затримка пакетів, тощо) для різних пакетних застосунків.

У процесі модернізації системи *UMTS* передача пакетних даних за технологією *ATM* була замінена на передачу даних на основі протоколу *IP*. Для передачі потоків даних *E*1/*TDM* мережі *GERAN* через мережу *ATM* (*IP*) застосовують конвертори інтерфейсів.

Види каналів

У мережі *GERAN* існують логічні, часові і частотні канали.

Логічний канал – це інформація певного змісту. Часовий канал – це слот у фреймі. Частотний канал – це смуга частот, в якій розташований спектр радіосигналу.

Кожен часовий і частотний канал використовує одна мобільна станція, яка передає або приймає радіосигнал.

У мережі *UTRAN* існують логічні, транспортні, фізичні, кодові і частотні канали. Канали перших трьох видів наведені на рис.1.4 і рис.1.5

Загальний канал (*Common*) використовує будь-яка мобільна станція. Виділений канал (*Dedicated*) мобільна станція використовує індивідуально.

На відміну від мережі *GERAN*, слоти (інтервали часу) і частотні канали – це загальний ресурс, який одночасно використовують всі мобільні станції в секторі.

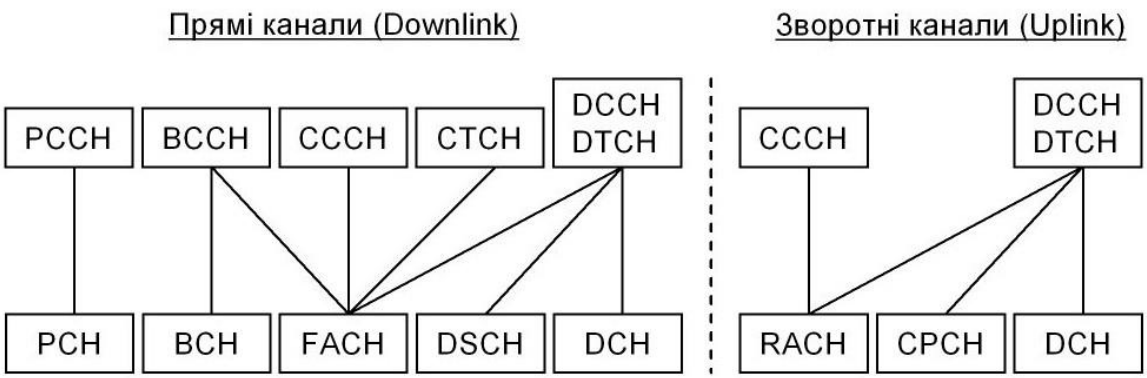
Логічний канал характеризують:

- інформаційний зміст даних;
- структура даних, тобто кількість і об'єм бітових блоків повідомлення.

Транспортний канал характеризують:

- параметри завадостійкого кодування;
- спосіб групування даних для їх подальшої передачі на рівень фізичних каналів.

Фізичний канал характеризує структура блоку даних, яка залежить від заданої швидкості передачі в радіоканалі.



Логічні канали управління

PCCH, Paging Control Channel – пошуковий канал управління
BCCH, Broadcast Control Channel – широкомовний канал управління
CCCH, Common Control Channel – загальний канал управління
DCCH, Dedicated Control Channel – виділений канал управління

Логічні канали трафіку

CTCH, Common Traffic Channel – загальний канал трафіку
DTCH, Dedicated Traffic Channel – виділений канал трафіку

Загальні транспортні канали

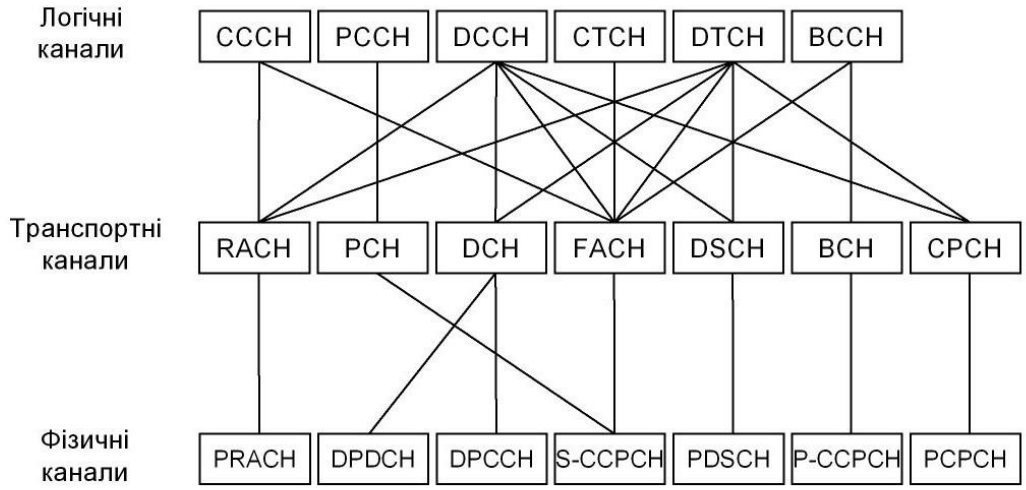
PCH, Paging Channel – канал виклику
BCH, Broadcast Channel – широкомовний канал
FACH, Forward Access Channel – канал прямого доступу
DSCH, Downlink Shared Channel – прямий канал загального користування

RACH, Random Access Channel – канал випадкового доступу
CPCH, Common Packet Channel – загальний канал передачі пакетних даних

Виділений транспортний канал

DCH, Dedicated Channel – виділений канал

Рис.1.8. Логічні і транспортні канали



PRACH / PDSCH / PCPCH = Physical RACH / DSCH / CPCH

DPDCH, Dedicated Physical Data Channel – виділений фізичний канал даних

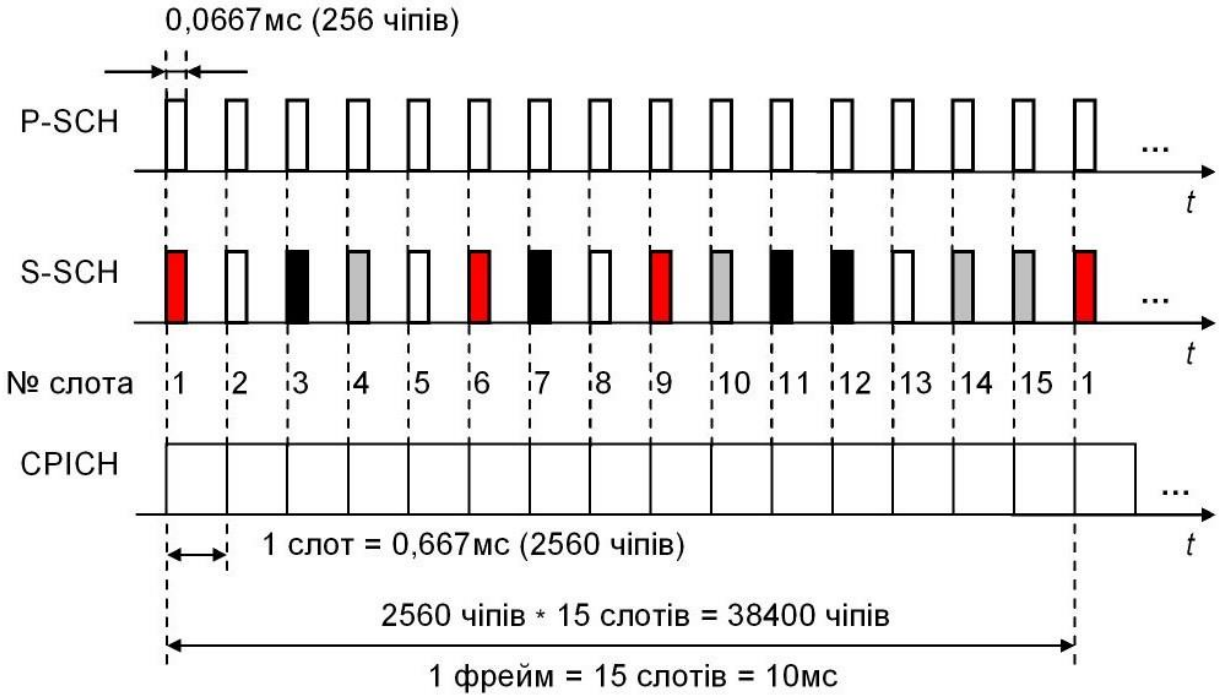
DPCCH, Dedicated Physical Control Channel – виділений фізичний канал управління

P(S)-CCPCH, Primary (Secondary) Common Control Physical Channel – первинний (вторинний) загальний фізичний канал управління

Рис.1.9. Логічні, транспортні і фізичні канали

1.3 Вибір стільника

Базова станція безперервно передає три фізичних канали, які наведено на рис.10



SCH, Synchronization Channel – канал синхронізації
P-SCH, Primary SCH – первинний канал синхронізації
S-SCH, Secondary SCH – вторинний канал синхронізації
CPICH, Common Pilot Channel – загальний пілотний канал

Рис.1.10. Канали синхронізації і пілотний канал

Операцію вибору стільника поділяють на
три етапи. Етап 1

Після увімкнення живлення мобільна станція виконує пошук каналів *P-SCH*. Такий канал містить

код C_p довжиною 256 чіпів. Цей код однаковий для всіх базових станцій і розташований на початку кожного слоту. У мобільній станції кореляційний приймач з опорним кодом C_p працює в режимі сканування і формує пікові відліки.

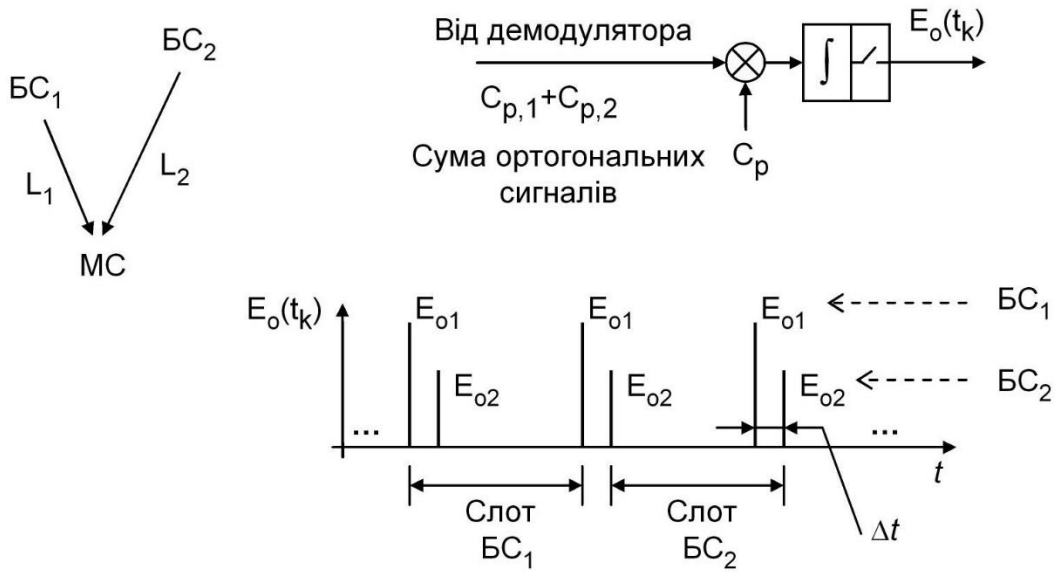


Рис.1.11. Мобільна станція

Мобільна станція вибирає відліки з максимальною амплітудою ($E_{o1}>E_{o2}$), або відліки, які формуються раніше (це E_{o1}, якщо $E_{o1}=E_{o2}$). Результатом обробки цих піків є слотова синхронізація мобільної станції і базової станції, при цьому автоматично враховується затримка сигналу в радіоканалі ($t_З=L/c$). Кожна базова станція формує свою шкалу часу у вигляді послідовності слотів, це спрощує мережу доступу *UTRAN*.

Примітка У системах 3*GPP*2, зокрема *Cdma*2000, базові станції працюють синхронно, для цього використовують сигнали системи супутникової навігації *GPS*. У системі *UMTS* базові станції працюють асинхронно, тому $\Delta t \neq 0$ навіть за умови однакових затримок $t_З$, коли $L1=L2$.

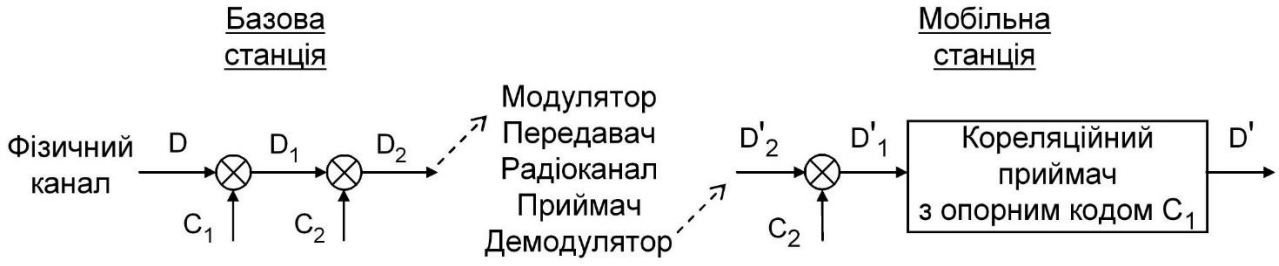


Рис.1.12. Cdma 2000

Сигнали D'_1 і D_1 однакові за двох умов:

- завади і шуми в радіоканалі не впливають на якість приймання, тому $D'_2=D_2$;
- в базовій станції і в мобільній станції використовують однаковий код C_2.

Мета 2-го і 3-го етапів – це формування в мобільній станції опорного коду, який ідентичний коду C_2 базової станції і забезпечує дескремблювання даних.

На 2-му етапі застосовують наступний метод.

У мережі доступу *UTRAN* використовують 512 первинних кодів C_2.
Ці коди поділені на 64 групи, кожна з них містить 512/64=8 кодів.

У каналі *S-SCH* базова станція передає 15 послідовних кодів, кожен код розташований в окремому слоті фрейму (рис.1.13). Кодове слово, яке містить ці 15 кодів, є ідентифікатором (номером) групи кодів C_2:

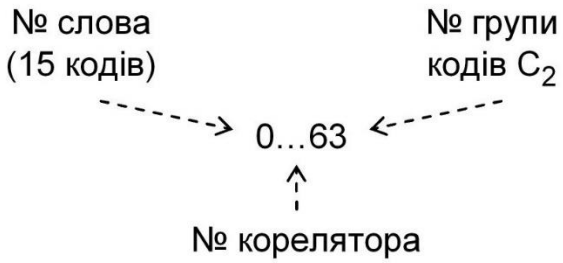


Рис.1.13.

Мобільна станція має 64 корелятори, які працюють паралельно. Опорний сигнал в такому кореляторі – це одне кодове слово з набору 64-х кодових слів. Пікові відліки $E_O(t_K)$ з'являються у тому кореляторі, в якому прийняті 15 кодів однакові з опорним сигналом.

Після цього мобільна станція:

- фіксує межі фрейму і нумерує слоти (рис.1.13);
- визначає номер групи кодів C_2, який дорівнює номеру корелятора;
- обчислює 8 кодів, які містить ця група.

Етап 3

Базова станція передає код C_2 у пілотному каналі *CPICH*. Цей код містить 38400 чіпів і повторюється в кожному фреймі (рис.1.13). У схемі перетворень, яка наведена вище (етап 2):

- D=111... – біти фізичного каналу;

- $C_1=C_{256,0}$=111... – чіпи;

- $D_1=D*C_1$=111... – чіпи;

- $D_2=D_1*C_2=C_2$ – чіпи на модулятор.

Мобільна станція має 8 кореляторів, які працюють паралельно. Опорні коди для цих кореляторів

обчислені на 2-му етапі. Пікові відліки $E_O(t_K)$ формує той корелятор, в якому опорний сигнал збігається з кодом C_2 базової станції. Цей опорний код фіксується, після цього мобільна станція дескремблює фізичні канали базової станції.

Перший такий канал – це *P-CCPCH*, який передається в кодовому каналі $C_{256,1}$ і містить інформацію широкомовного каналу *BCH*.

1.4 Регулювання потужності

Потужність передавача мобільної станції регулюють в двох контурах.

Розімкнутий контур використовують у процесі доступу до мережі

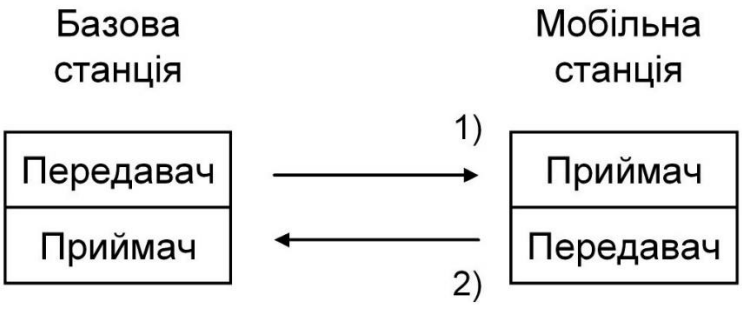


Рис.1.14.

Мобільна станція:

1) вимірює потужність прийнятого сигналу *BCH*,

2) регулює потужність свого передавача для передачі преамбули.

Чим більше затухання радіосигналу у прямому каналі, тим менше потужність сигналу *BCH*, тим більше початкова потужність передавача, і навпаки. Далі, якщо протягом певного часу немає відповіді базової станції в каналі *AICH*, то мобільна станція збільшує потужність передавача з кроком 9 дБ (тобто 8 разів), повторює передачу преамбули, чекає відповідь *AICH*, і т.д.

Замкнутий контур використовують під час реєстрації, а також у процесі передачі трафіку.

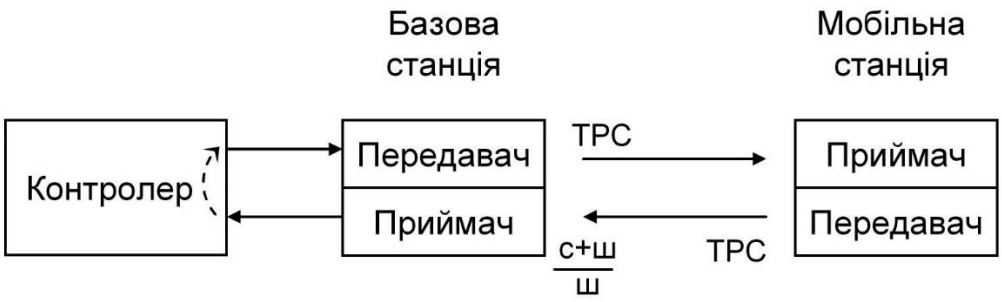


Рис.1.15.

Базова станція вимірює відношення (сигнал+шум)/шум на вході свого приймача.

Контролер отримує результат вимірювання, порівнює його з потрібним значенням, і дає команду мобільній станції змінити потужність передавача.

Ця команда (*TPC*) передається в слоті фізичного каналу. Крок регулювання в замкнутому контурі дорівнює ±1 дБ (тобто 1,26 разів).

Частота регулювання дорівнює (1 рег)/$T_{СЛ}$=(1 рег)/(0,667 мс)=1500 рег/с.

У зворотному каналі мобільна станція передає своє повідомлення *TPC*.

Ця інформація є не командою, а рекомендацією для регулювання потужності передавача базової станції. Контролер враховує ці повідомлення при розподілі потужності базової станції між мобільними станціями. Для цього в кожному кодовому каналі передбачено множення на коефіцієнти G_i.

Інтерференція

У стільникових системах з *OFDM* існують два ефекти, які погіршують якість радіоприймання і збільшують відсоток невиправлених помилок після декодування.

1-й ефект – це інтерференція радіосигналів, які передають у сусідніх смугах частот.

Для компенсації цього ефекту, потоками даних модулюють $N_м<N$ піднесучих у смузі частот $B_м<B$, де N і B – це розмірність перетворень Фур'є і смуга частот радіоканалу. Інші піднесучі в кількості $(N – N_м)$ помножують на 0 у процесі ОШПФ, тому вони відсутні в бічних захисних смугах (ЗС).

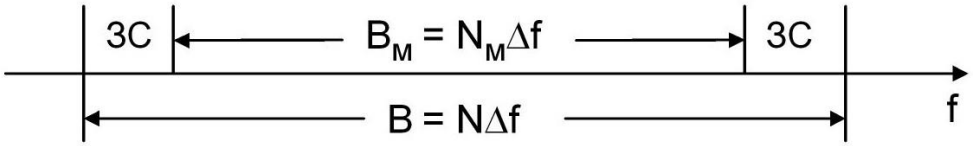


Рис.1.16.

2-й ефект – це інтерференція радіосигналів на межі стільників, якщо сусідні базові станції працюють в однакових смугах частот. Для компенсації цього ефекту застосовують два способи.

1) Просторове рознесення ділянок сусідніх стільників, в яких частоти піднесучих однакові

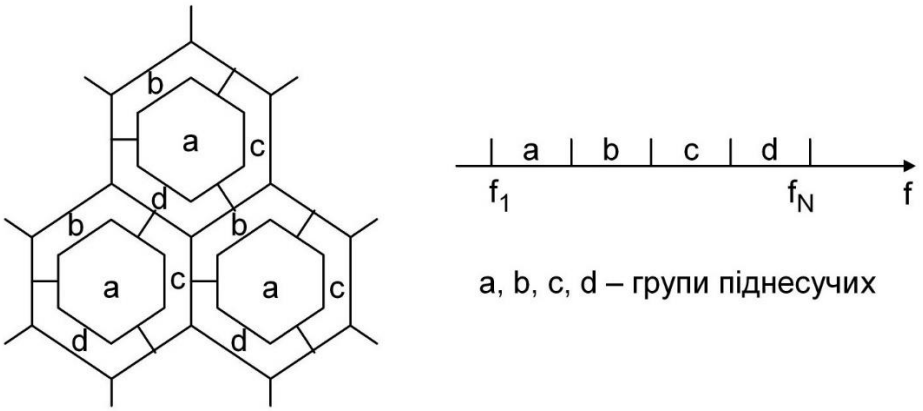


Рис.1.17.

2) Комбінування методів *OFDM* і *DSSS* у передавачі.

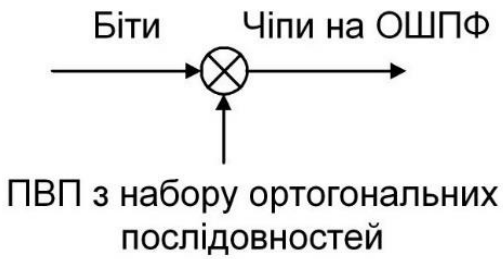


Рис.1.18.

У приймачі здійснюють ШПФ, кореляційне приймання чіпових сигналів і формування бітів.

ВИСНОВОК ДО РОЗДІЛУ 1

У цьому розділі були розглянуті системи UMTS, детально наведена структура базової станції 3G-4G, був зроблений загальний опис роботи основних елементів БС, а також було проведено аналіз роботи системи стільникового зв’язку. Була піднята проблематика зон обслуговування системи стільникового зв’язку, складено плани мережі, що спрощують налаштування, а також наведена логічна топологія. Було описано і показано всі процеси, які зазвичай проходять від абонента до базової станції та навпаки.

РОЗДІЛ 2
РЕГЛАМЕНТНІ РОБОТИ З ТЕХНІЧНОГО ОБСЛУГОВУВАННЯ РЛС

2.1. Види технічного обслуговування

Мережа GSM або UMTS Radio Reporting складається з певної кількості базових станцій. Основні станції (BS) контролюють контролер BSC/RNC або декілька контролерів. Інформація за трафік користувачів й сигналізація від BS та контролерів доставляється в основну мережу, яка складається з медіашлюзів, комутатора, транскодера, одиниць доступу до мережі пакетів та й іншого.

Рис.2.1. Вишка стільникового зв’язку

Отже, радіосистема включає основні станції та їхні контролери, обслуговуванням яких зазвичай займаються певні інженери при виконанні технічних регламентних робіт. Точка розміщення BS називається апаратною або майданчиком. Час

від часу на певних апаратних працюють над технічним обслуговуванням BS, обладнання транспортної мережі, систем живлення, безпеки та пожежної сигналізації, автоматичних систем пожежогасіння, антенно-щоглових конструкцій та трактів живлення.

На Рис.2.2 показано одну із складових системи живлення, яка складається із вступного щита.

Рис.2.2. Трифазне джерело живлення зі змогою резервного з'єднання від генератора

Рис.2.3. Адаптер з підключенням кабелю від генератора

В цьому щиті є: обмежувачі надмірної напруги , вимірювач електроенергії, додаткові адаптери живлення та й автомати певних номіналів для споживачів електроенергії, серед яких: безперебійне джерело живлення (БДЖ), кондиціонери, пожежна сигналізація, витяжна вентиляція, нагрівач й аварійні та робочі світильники.

Найпотрібніші елементи радіодоступу живляться від подачі постійного струму з напругою -48(В), в той же час, вітчизняне обладнання з попередньої епохи, було розроблено під напругу -60(В). У випадку вимкнення енергетичними організаціями електроенергії, з різних надзвичайних причин, існує можливість автоматичного підключення живлення до базової станції від блоку акумуляторних батарей. Даний блок зображено на (Рис.2.4).

Рис.2.4. Вигляд мережі постійного струму

У цьому джерелі знаходиться блок 3х4 акумуляторів, кожен із яких має ємність близьку 150 ампер-годин. До речі, нумерація акумуляторів на фотографії зроблена правильно, від позитивної клеми до негативної. При регламентних роботах проводять тестування блоку акумуляторів й тривалості автономного живлення базової станції, використовуючи навантажувальні резистори. Таким чином, відповідно до результатів цього тестування, можна зробити висновок, чи потрібен новий блок акумуляторів, чи ні.

Також, при затягуванні болтів акумуляторів, виявилося наступне. Потрібно завчасно перевіряти якість обладнання.

Рис.2.5. Приклад неякісної продукції

Акумуляторне джерело безперебійного живлення керує перетворенням змінного струму в постійний. Саме у цьому джерелі, встановлено 4 одиниці стабілізації імпульсу. Вони потрібні для стабілізації напруги при підключенні блоку акумуляторів до навантаження, так як, стабілізована напруга подається через стабілізатор на навантаження не безперервно, а лише протягом деякого інтервалу часу всередині періоду T (періодично, то підключається до навантаження, то відключається від нього).

За формулою наведеною нижче, можна побачити наступне:

$$U_{\text{н ср}} = \frac{1}{T}\int_0^T u_{\text{н}}(t)dt.$$

1) uн - інтервал часу, протягом якого навантаження підключено до джерела напруги, що стабілізується;

2) (T – uн) - тимчасовий інтервал, на якому навантаження відключено від джерела.

Рис.2.6 Прилад зняття напруги

З індикатора ДБЖ ми можемо спостерігати постійну напругу з номіналом 54.1 (В), а також, струм навантаження 32 (А), струм заряду АКБ 0 (А) та температуру на стійці з акумуляторами +18 (°С). Термодатчик потрібен для теплової компенсації напруги акумулятора за температурою навколишнього середовища).

Рис.2.7. Автомати різних номіналів

Відкривши кришку ДБЖ знаходиться ряд електричних автоматів, від яких йдуть кабелі до базової та радіорелейної станції, блоку АКБ та інших споживачів постійного струму. Також на (Рис.2.7), зліва в центрі, видно плату з контактами під виведення зовнішньої аварійної сигналізації та сигналізації про відключення електроенергії чи розряд АКБ.

У даному випадку в апаратній була БС стандарту GSM-900 й виробництва компанії Alcatel.

В середині шафи розташовується основне обладнання: десять передавачів TRAGE, з яких: три комбайнери AGC9E та одна плата керування SUMA. Характеристики цієї базової станції- описується як 4-3-3, що означає: на першому секторі працюють чотири передавачі, на другому та третьому по три. Кожен передавач з'єднаний з комбайнером призначеного сектора. Від комбайнера йдуть два фідери (англ. Jumper) до грозозахисту (англ. Lightning Protection) і далі нагору до антени обраного сектору.

У верхньому кутку шафи розташовані зліва направо 2 плінти під зовнішні аварії, плінт підключення до транспортної мережі за інтерфейсом A-bis (потоки E1), контакти живлення (чорний та синій дроти) та вимикачі, кожен для окремої полиці шафи.

Над шафою базової станції, виходять шість джамперів (відповідно для трьохсекторної збірки), які за допомогою грозозахисту, приєднані до зовнішнього тракту фідера (діаметр фідера 7/8 дюйма).

Рис.2.8. Вигляд грозозахисту

На рисунку нижче, зображено кабельне виведення, яке герметично ізольоване від попадання вологи у середину шкафу.

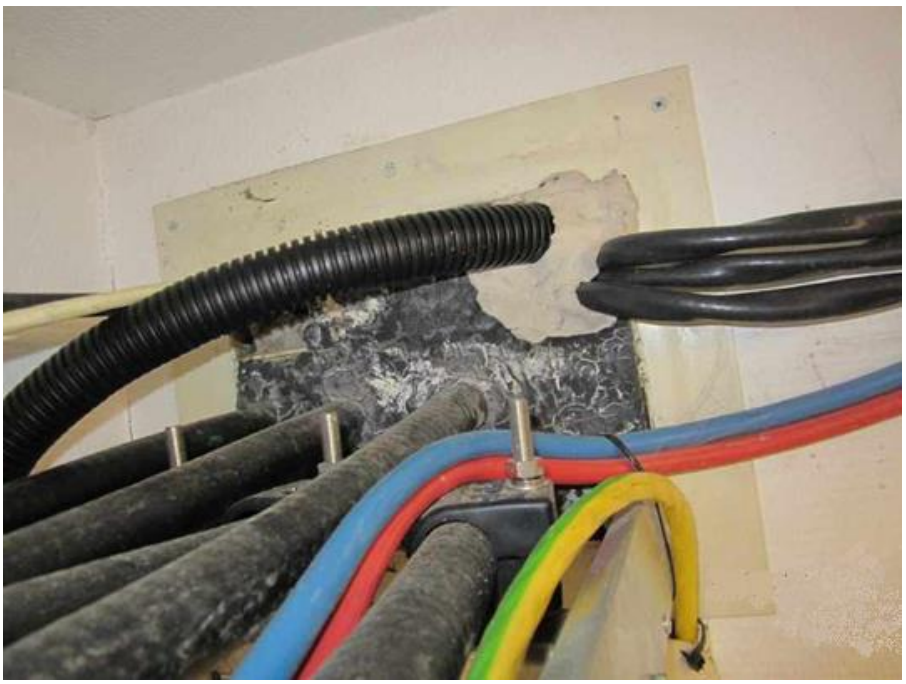


Рис.2.9. Герметична ізоляція від вологи

Також, є "19" стійка. Вона містить у собі: внутрішні блоки РРС і базової станції стандарту UMTS, крос.

Радіорелейка MDP-34MB-25C здатна пропускати 34 Мбіти/с інформаційного трафіку, що в наш час, вважається доволі небагато. Внутрішній блок, з'єднується за допомогою оптичного кабелю до зовнішніх передавачів.

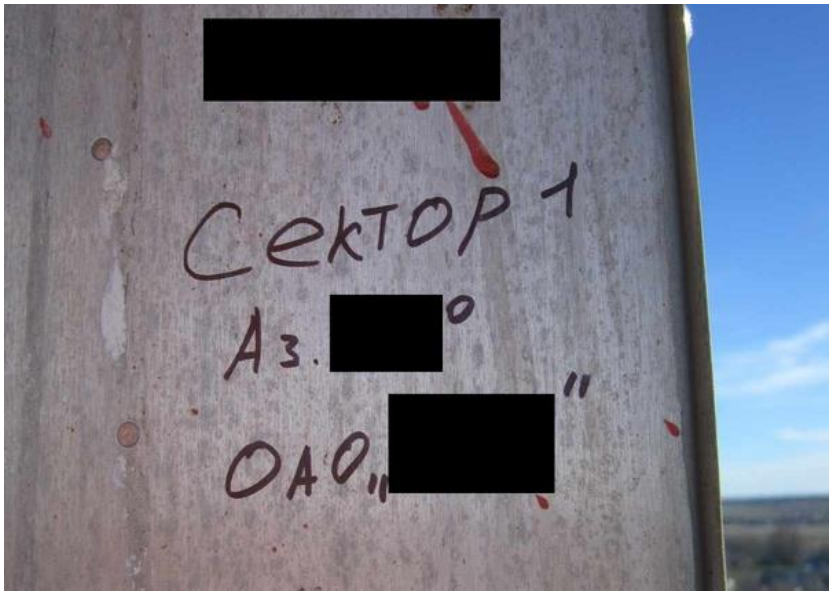


Рис.2.10. Секторна антена

На майбутнє, виконується маркування сектора, яке потрібне для простоти орієнтування при модернізації обладнання чи усунення несподіваних аварій.

Рис.2.11. Юстування РРС прольоту

При юстуванні (налаштуванні) РРЛ прольоту, використовують лівий адаптер, який потрібен для підключення вольтметра. На цьому роз'ємі, напруга є пропорційною рівню прийнятого сигналу від отриманого радіорелейкою. Подальший адаптер потрібен для з'єднання ODU та IDU (outdoor unit & indoor unit) РРС коаксіальним кабелем проміжної частоти. Адаптер потрібно загерметизувати від попадання шкідливої вологи до кабелю. Правий роз’єм використовують для заземлення блоку [9].

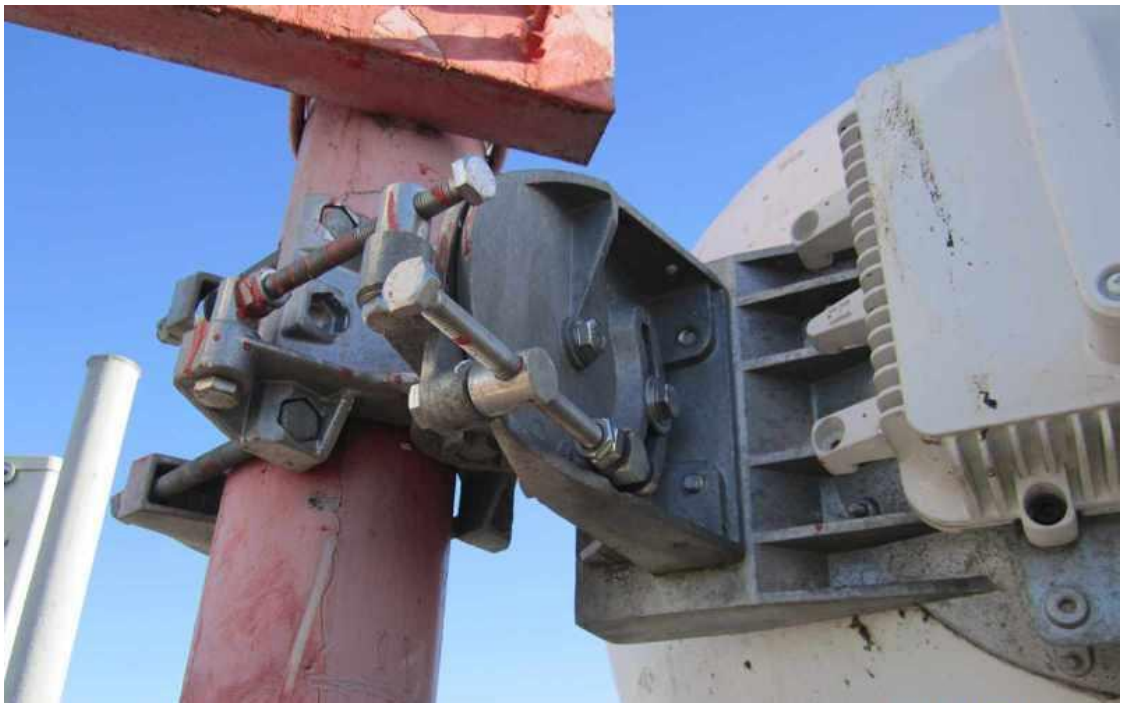


Рис.2.12. Варіант зручного кріплення РРС-антени

Цей процес проходить за допомогою двох довгих гвинтів, які можна обертати в тому чи іншому напрямку для тонкого юстування прольоту між РРЛ.

Також є наступна важлива одиниця базової станції, яка називається RRU – (Remote Radio Unit) за стандартом UMTS.

Рис.2.13. Модуль RRU

Використовують наступний спосіб підключення: зліва тонкий оптичний кабель, який заходить із гофри у передавач. Цей передавач складається із звичайного модуля SFP. Наступним заводиться кабель живлення (теж -48 В, постійний струм), Роз'єм правіше, це- тонкий кабель для підключення до RET (Remote Electrical Tilt) - пристрою, що управляє електричним кутом нахилу секторної антени. Після чого, стоять два джампери до антени та жовто-зелений кабель заземлення.

Фактично, у корпусі міститься дві антени з різною поляризацією (переважно, кути +45 й -45), через те й підключаються два фідери від передавачів. У такий спосіб здійснюється поляризаційне рознесення сигналу, який приймається від абонента [9].

ВИСНОВОК ДО РОЗДІЛУ 2

У даному розділі було розглянуто регламентно-планові технічні роботи з обслуговування базової й радіорелейної станцій. Даний процес розписаний покроково з рекомендацій до обслуговування й діагностики майбутніх проблем. Була наведена залежність та важність цих дій від надійності подальшого використання. А також, більш детально описано принцип роботи кожного з модулів та елементів БС.

РОЗДІЛ 3
Розробка способу дистанційного радіоуправління

3.1. Структура каналу радіозв’язку

У період розвитку радіотехніки термін «бездротовий зв'язок» (Wireless) використовувався для опису поняття радіозв'язку загалом, тобто у всіх випадках бездротової передачі. Згодом цей термін вийшов із вживання, і термін «бездротовий зв'язок» став використовуватися на рівнозначному рівні термінами «радіо» (Radio) або «радіочастота» (RF — радіочастота). Тепер ці два поняття визначені у діапазоні частот від 3 кГц до 300 ГГц. Термін «радіо» часто використовується для опису старіших технологій (радіолокація, радіомовлення, радіотелефонний зв'язок, супутниковий зв'язок та ін.). А термін «бездротовий зв'язок» тепер відноситься до нових технологій радіозв'язку, наприклад, до абонентського доступу, мікростільникової й мобільної телефонії, пейджингового зв'язку тощо.

Різниця між трьома типами бездротових мереж (рис. 3.1): WWAN (бездротова глобальна мережа), WLAN (бездротова локальна мережа) та WPAN (бездротова персональна мережа).

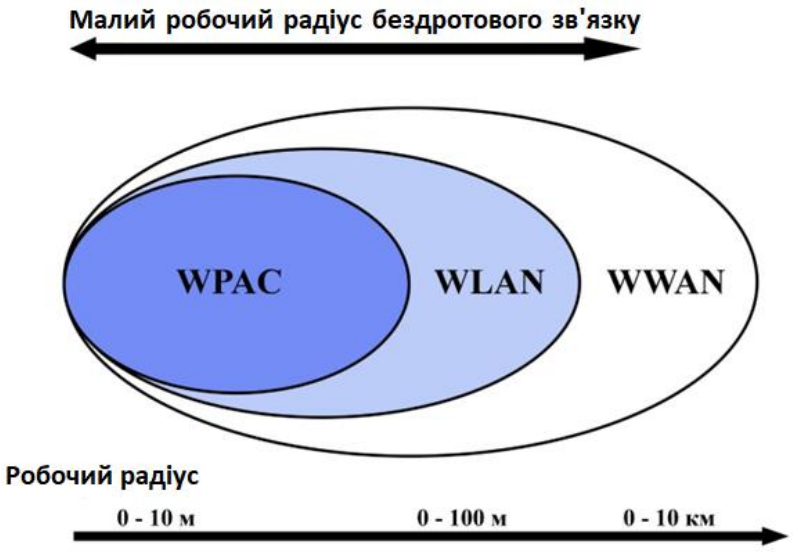


Рис.3.1. Типи бездротових мереж

Аналогічні технології використовуються під час створення зв'язку WLAN і WPAN, і навіть під час створення системи широкосмугового бездротового доступу (BWA - Broadband Wireless Access). Відмінність бездротового зв'язку (рис. 3.2) полягає в дальності дії та характеристиці радіоінтерфейсу. Зв'язок WLAN та WPAN працює в безліцензійних діапазонах частот, а саме, 2,4 (ГГц) та 5 (ГГц), а це означає, що створення цих технологій не потребує узгодження та планування з іншими радіокомунікаціями, що працюють у тому самому діапазоні.

З'єднання BWA (бездротовий широкосмуговий доступ) використовують як ліцензовані, і неліцензовані діапазони (від 2 до 66 ГГц).

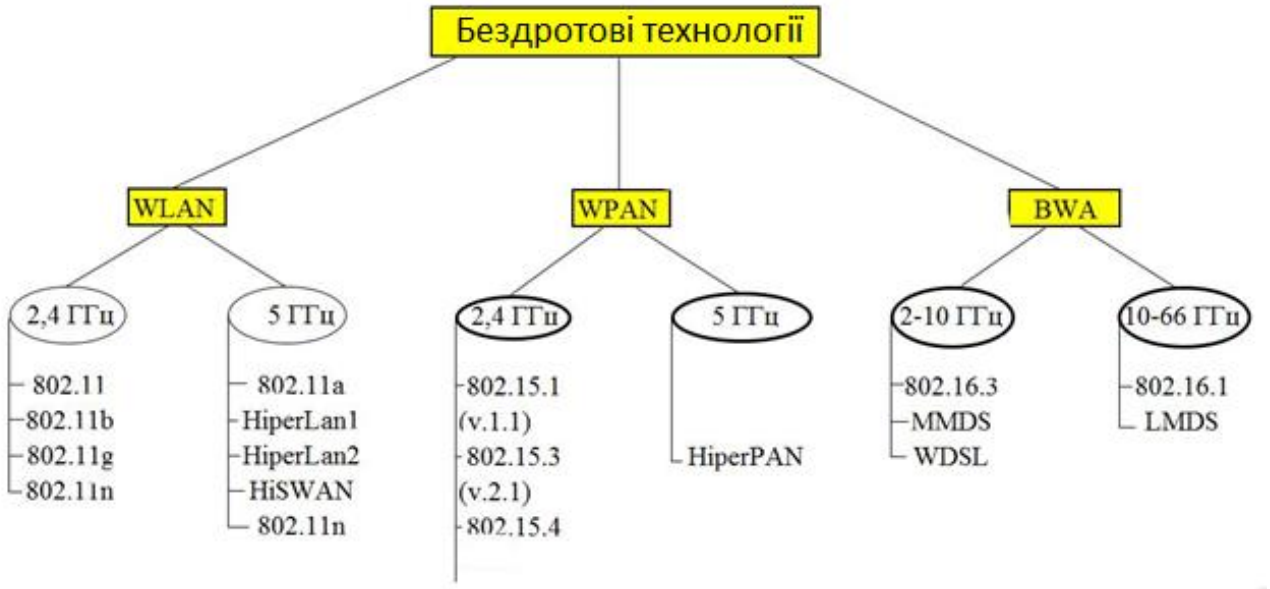


Рис. 3.2. Класифікація бездротових технологій

Основним напрямом локального бездротового зв'язку (WLAN) є організація можливості використання інформаційних ресурсів усередині будівлі.

Другим за важливістю напрямком є організація загальнодоступних комерційних точок підключення (хот-спотів) у місцях великого скупчення людей, таких як кафе, аеропорти, готелі, а також організація тимчасового сполучення у місцях проведення заходів (виставок, семінарів).

Бездротові локальні мережі базуються на сімействі стандартів IEEE 802.11. Ці з'єднання відомі нам під назвою Wi-Fi (Wireless Fidelity), в основному ці стандарти не називаються Wi-Fi, хоча зараз бренд Wi-Fi широко поширений по всьому світу.

LAN-мережі

Мережі LAN, згідно з початковим призначенням, були одними з найпростіших комп'ютерних мереж. Представленими різними типами комп'ютерних мереж, вони мали такі властивості, як: обмежена кількість вузлів між взаємопов'язаними комп'ютерами, (підлога, будівельна зона, офіс), автономні лінії зв'язку між мережевими вузлами (як правило, кабелі, дроти). Початкова топологія локальної мережі була найпростішою й полягала у підключенні мережевих вузлів (ноутбуків та комп'ютерів) до загальної мережевої лінії, яку ще називають шиною (відповідне зображення "шини", показане на рис. 3.3а). Список конкретних об'єктів локальної мережі складався з обмеженої кількості абонентів мережі, які перебувають в певній площині (кімната, дім, кампус), а також, де була наявність телекомунікаційної лінії зв'язку між клієнтами (вузлами). У новітніх місцевих мережах зміни основних функцій вплинули на три аспекти:

1) модифікація топології телекомунікаційних ліній зв'язку (у порівнянні з топологією типу "шина");

2) заміна вигляду вузлів мережі (де, вузлами мережі можуть виступати пристрої з різними типами цифрового контенту: телефонія, відео, аудіо, графіка та інше);

3) впровадження взаємозв'язку між мережею LAN (включно з усіма її компонентами) та магістральною мережею, в якому остання, застосовується для підключення мереж різного призначення (а саме, інших мереж LAN).

Фінальний з цих аспектів сполучений з придбанням сучасними ЛОМ якіснонових характеристик в порівнянні з їх початковими функціями, іншими словами, завдяки з'єднанню з магістральною мережею, ЛОМ отримує можливість виконувати функції мережі доступу до магістральної мережі, проілюстровано у рисунку 3.3 б).

Функціонал інтерфейсу між локальною мережею і магістральною мережею виконуються одним з певних вузлів мережі (LAN), до якого належить мережевий контролер NIC (Network Interface Controller).

У бездротовій локальній мережі (WLAN - Wireless LAN) з'єднання між вузлами мережі здійснюється за допомогою радіосигналів, на відміну від провідної локальної мережі. Вузли містять в собі приймальні й передавальні пристрої. Сфера, в якій розташовані деякі вузли, являється середовищем для поширення радіосигналів. Значить, використання дротових ліній зв’язку не є великою необхідністю. Призначення концентратора провідної локальної мережі виконується за допомогою WLAN AP (Access Point). На наступному рисунку 3.3. в), концентратор з’єднаний з магістральною мережею, а середовище бездротової передачі відмічене пунктирними лініями.

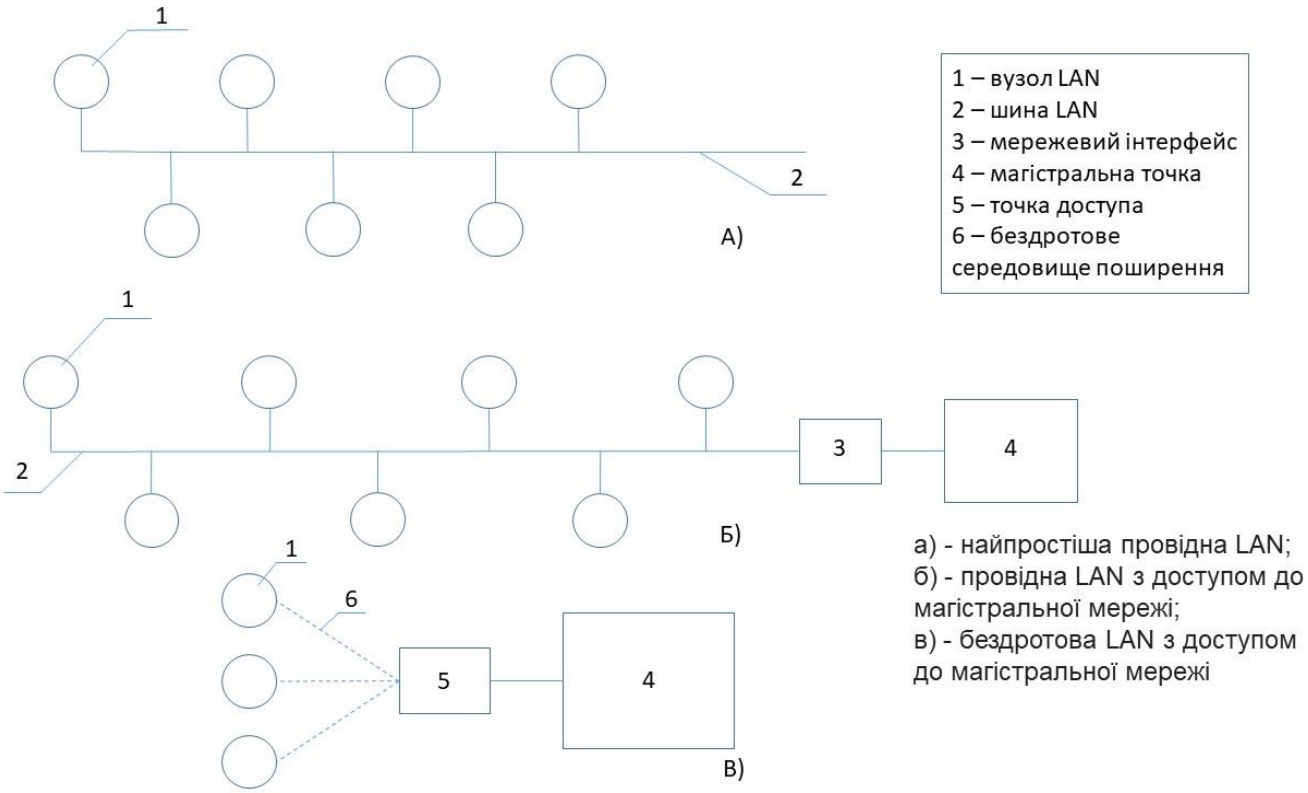


Рис. 3.3. Різновиди LAN

Доцільність й необхідність використання бездротової локальної мережі в порівнянні з дротовими обумовлена перевагами, які можливо отримати за відсутності провідного з'єднання. Ці переваги можна побачити при наступних обставинах:

1)за необхідністю створення локальної мережі між вузлами, які відокремлені природними й штучними бар'єрами (для прикладу, стіни будинків, водні перешкоди, підлогові покриття);

2) при необхідності забезпечення мобільності вузлів, підключених до локальної мережі;

3) коли потрібне отримання доступу до магістральної мережі при доступі до мережі Internet у громадських місцях при тимчасовому перебуванні (вокзали, готелі, читальні зали бібліотек та інше).

Гігантський попит на бездротовий локальний зв'язок (з загального погляду) визначає місце WLAN у новітніх бездротових телекомунікаціях. Найбільш потрібною споживчою характеристикою WLAN є надання доступу клієнтам до магістральної мережі зі зручністю її розгортання й забезпечення взаємного зв'язку клієнтів. Останнє, зокрема, пояснює використання англомовного терміну "hotspot" для громадських місць розгортання WLAN з доступом до мережі Internet.

Під час розробки бездротової технології WLAN постало питання сумісності обладнання, а саме, коли три передових країни світу по розробці бездротових LAN, зіткнулися із проблемою сумісності різних девайсів, виробленими різними виробниками. Європа, США та Японія були серед них передовими. Та й для вирішення даної проблеми була розроблена домовленість, за якою, обладнання різних виробників, змогло працювати і розуміти не тільки свої пристрої, а й інших компаній.

Сполучною властивістю використання обох середовищ є те, що вони є середовищами загального / множинного доступу (MA – Multiple Access), яке зображено на рисунку 3.4, а). Сигнали від різних користувачів в умовах їх незалежної роботи можуть передаватися в один час, що може призвести до накладення сигналів в навколишньому середовищі. Саме ця суперпозиція призводить до різниці в загальному сигналі від кожного з переданих сигналів й це значно ускладнює можливість їх правильного прийому. У середовищах загального доступу, незалежно від її фізичних властивостей, можуть створюватися колізії сигналів. Для запобігання зіткнень передбачається скоординоване використання навколишнього середовища, де обов'язковим компонентом являється моніторинг площі використання. Доступ до середовища, який заснований на моніторингу його зайнятості, називають методом множинного доступу з

контролем несучої CSMA (Career Sense Multiple Access). Локальні мережі різних різновидів (бездротових та дротових) використовують кілька похідних варіантів цього методу доступу.

Доступ вузлів до середовища обох різновидів здійснюється за допомогою мережевих адаптерів WNIC, NIC (Wireless NIC, Network Interface Card), які виконують функції двох нижніх рівнів базової еталонної моделі взаємодії відкритих систем OSI / ISO (The Open Systems Interconnection), а саме:

- підрівня управлінням доступу до середовища MAC (Media Access Control) канального рівня DLL (Data Link Layer).

- фізичного рівня PHY (Physical Layer);

Мережеві девайси (бездротові й дротові) можуть забезпечувати постійний доступ до різних вузлів, моніторинг навколишнього середовища, , формування, передачу й прийом сигналів [11].

У проводному середовищі, яке є двопровідною довгою лінією, наприклад, кабелем, який можна побачити на малюнку 3.4, b); передача сигналу між вузлами можлива при відносно слабкому ослабленні під час їх розподілу. Зіткнення сигналів двох (або більше) вузлів призводить до значної зміни характеристик загального сигналу (в основному енергетичного рівня) порівняно з окремими сигналами. Як результат, кожен вузол може використовувати мережеву карту для виявлення фактів колізій сигналів під час їх передачі й забезпечити всі необхідні заходи щодо використання пріоритету доступу до середовища різних вузлів, якщо це буде необхідно. Спосіб упорядкованого множинного доступу, що зменшує рівень колізій у провідному середовищі, називають множинним доступом з керуванням несучої і пошуком колізій CSMA / CD (CSMAI Collision Detection). Можливість знаходити колізії є суміжною характеристикою провідних носіїв.

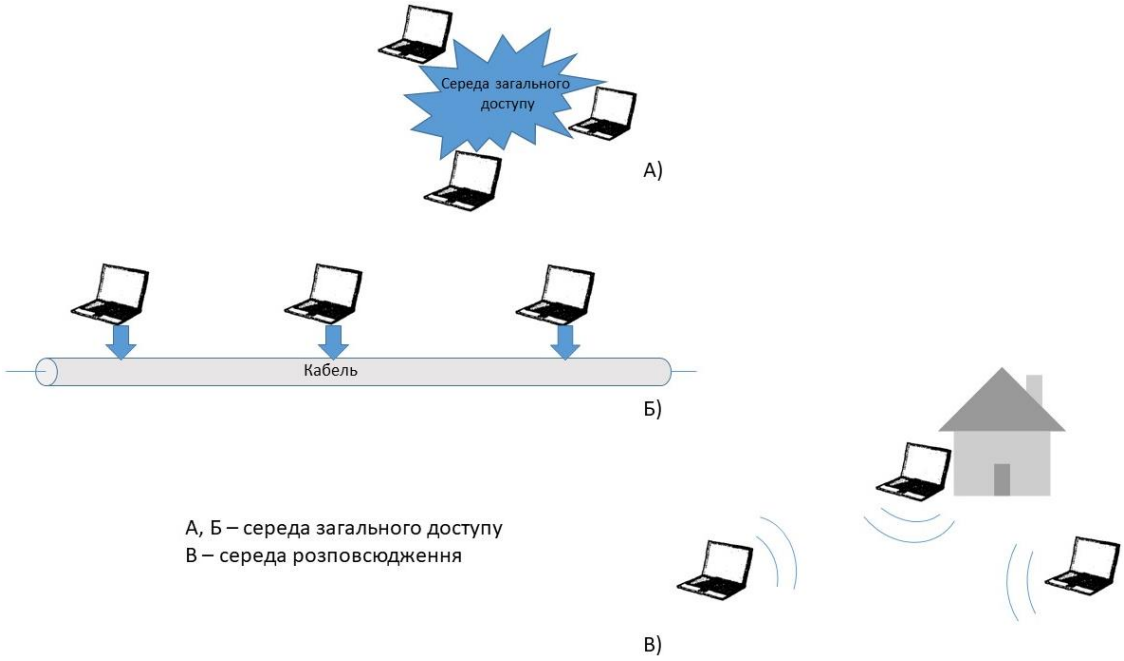


Рис. 3.4. Методи передачі інформації

Цифрові локальні мережі великих організацій переважно являють собою комбінацію дротових та бездротових сегментів. Як правило, мережева архітектура локальної мережі (LAN) має передбачати систему розподілу, яка буде виконувати наступні завдання:

- покриття з'єднанням між різними сегментами локальної мережі (включаючи дротові й бездротові сегменти));

- можливість доступу всіх сегментів локальної мережі до магістрального Internet-середовища.

Доступ до магістральної мережі зазвичай забезпечується за допомогою Web-серверів (серверів обслуговування), які мають відповідні характеристики інтерфейсу, які показані на рисунку 3.5.

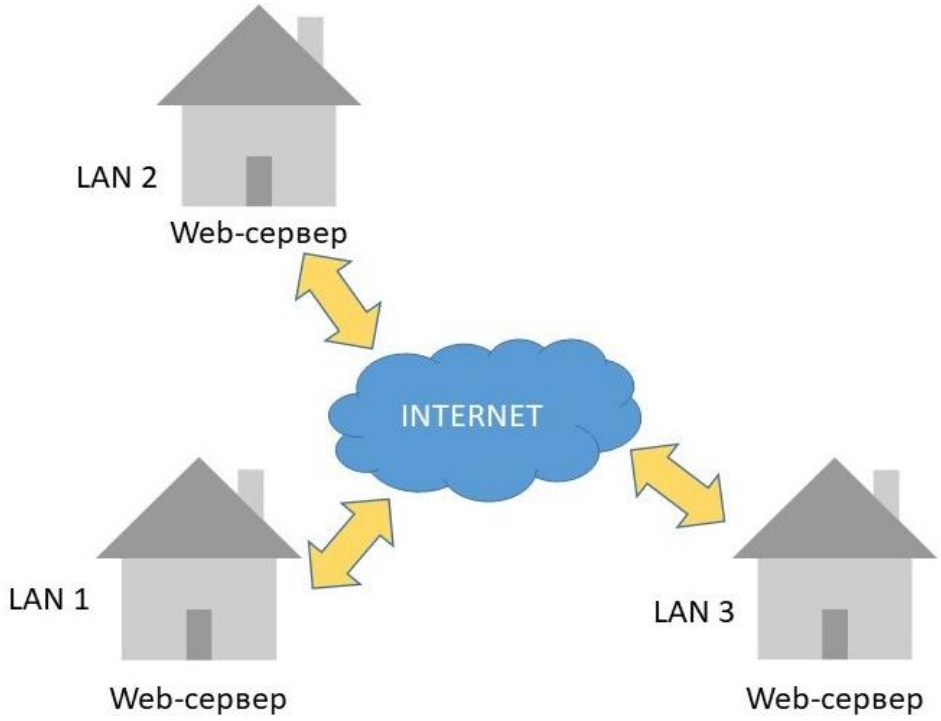


Рис. 3.5. Ілюстрація підключення абонентів різних LAN до магістральної мережі

Безпровідне середовище передачі повідомлень WLAN може оцінюватися за трьома наступними параметрами:

1) площина, яку охоплює WLAN; при розрахунку на одну BSS (Basic Service Set) ця територія являє базову площину обслуговування BSA (Basic Service Area);

2) частотний WLAN-ресурс; для однієї BSS цей ресурс має приблизну ширину 22 МГц в діапазоні 2401-2473 МГц;

3) тимчасовий WLAN-ресурс; в межах кожної BSS цей ресурс є не обмежений.

Контроль доступу до WM (Wireless Medium) призначений для координації роботи станцій, розташованих у BSA, так щоб, частота та часові ресурси всього набору STA BSS не використовувались. Відповідно до стандарту IEEE 802.11, частота, необхідна для передачі сигналів кожного STA, усуне всі частотні ресурси цього BSS (22 МГц). Як правило, станції EMS отримують шляхом координації використання тимчасового ресурсу: коли ознаки однієї з STA випромінюються, іншій не дозволяється випромінювати.

IEEE 802.11 надає два координовані методи, що відповідають двом типам координаційної функції WM:

- Координація PCF (точкова координація);

- Координація DCF (розподілена функція координації).

Обидві функції координації реалізуються службами MAC-підрівня, причому DCF є основою для реалізації PCF. DCF є основним типом координаційних функцій; він реалізується в інфраструктурних мережах BSS і незалежних IBSS (Independent Basic Service Set). PCF реалізується тільки в інфраструктурних мережах.

PCF-координація полягає в тому, що доступ STA до WM контролюється точкою доступу (AP) BSS, а координація зводиться до надання кожному з STA BSS певного періоду часу для випромінювання сигналів. Сегменти слідують один за одним, що означає реалізацію множинного доступу з тимчасовим поділом за часом TDMA (Time Division Multiple Access).

DCF-ккоординація полягає в тому, що можливість доступу до бездротового середовища визначається станціями незалежно, на основі спостереження за випромінюванням інших станцій і виконання передбачених правил доступу. У кожному BSS застосовується технологія доступу WM на основі суперечок (contention), звана доступом з контролем несучої і попередженням колізій CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance).

3.2. Режим роботи станції MIMO

Режим наступності. Режим обміну між двома станціями з тією самою антеною. Передача інформації здійснюється за протоколом 802.11a. Якщо передавальна станція MIMO, а друга, що приймає- звичайна, то в передавальної системі працює тільки одна антена і процес обміну інформацією відбувається, як у перших стандартах Wi-Fi.

Якщо інформація йде від звичайної станції до багатоканальної, то MIMO-станція використовує кілька прийомних антен, але в цьому випадку швидкість передачі не максимальна. Структура преамбули цього режиму аналогічна структурі 802.11a.

Змішаний режим. Обмін у цьому режимі аналогічний обміну між системами MIMO та звичайними станціями. Завдяки цим системам MIMO генерує два різні пакети в залежності від типу приймача. Робота зі звичайними станціями йде повільно, тому що вони не працюють на високій швидкості, а між MIMO — відносно швидше, але все ж таки нижче швидкості в режимі зеленого поля. Преамбула пакета звичайної станції аналогічна стандарту 802.11a, тоді як пакет MIMO дещо змінено.

Якщо працює, як передавач при використані системи MIMO, кожна антена передає лише циклічні зрушення, а не всю преамбулу. З цієї причини енергоспоживання станції знижується, а коефіцієнт посилення каналу вищий. Але не всі старі станції працюють у цьому режимі. Тому що навіть якщо алгоритм синхронізації пристрою заснований на когерентної кореляції.

Режим зеленого поля. У цьому режимі використовуються всі переваги системи MIMO. Мовлення можливе лише між станціями з декількома антенами за наявності застарілих приймачів. При обміні з системою MIMO звичайні станції чекають на звільнення каналу, щоб уникнути колізій. У режимі «з нуля» перші два канали отримуватимуть сигнали тривоги, але не транслюватимуть їх. Причина цього не в тому, щоб залучати до обміну нормальні станції і, як наслідок, збільшувати швидкість роботи. Пакети супроводжуються преамбулами, що підтримуються лише станціями MIMO. Всі ці дії мають максимально використовувати всі можливості системи MIMO-OFDM.

У всіх цих режимах роботи має бути передбачено захист від спотворення сигналів тривоги через роботу сусідніх станцій. Фізично моделі OSI (Open Systems Interconnection) у структурі преамбули використовуються спеціальні поля. Поля сповіщають станцію про те, що відбувається інший обмін інформацією, і слід почекати деякий час. Деякі параметри захисту, як і раніше, доступні на рівні каналу. Режими роботи класифікуються відповідно до смуги пропускання, що використовується:

1. Застарілий режим. Цей режим сумісний із першими версіями Wi-Fi. Для нього характерний пристрій зі смугою пропускання 20 МГц, так само цей режим дуже схожий на стандарт 802.11a/g.

2. Режим подвійної послідовності. Пристрій використовує діапазон 40 МГц, також та сама інформація і дані передаються по верхньому і нижньому (кожний шириною 20 МГц) каналам, але зі зміщенням на 90°. Основний напрямок структури, її приймач – звичайна станція. Подвоєння ширини смуги пропускання гарантує, що вона не спотворюється та досягає високої швидкості.

3. Режим верхньої смуги пропускання. Девайси мають два діапазони частот і, відповідно, підтримують 20 та 40 МГц. У цьому режимі станції обмінюються лише пакетами MIMO. Швидкість мережі максимальна.

4. Режим верхнього каналу. У цьому режимі використовується лише верхня смуга пропускання 40 МГц. Станції можуть обмінюватись будь-якими пакетами.

Бар'єри, що впливають на продуктивність бездротових мереж Wi-Fi та їх причини

1) Робота у своєму робочому радіусі, інших пристроїв Wi-Fi (точки доступу, бездротові камери та інше). Це пов'язано з тим, що Wi-Fi впливає на пристрої навіть якщо існує невеликий бар'єр пристроїв, що працюють на тій же частоті. Бездротові мережі використовують два частотні діапазони 2,4 (ГГц) та 5 (ГГц). Бездротові мережі 802.11b/g працюють у діапазоні 2,4 (ГГц), 802.11a – у діапазоні 5 (ГГц) та 802.11n – у діапазонах 2,4 (ГГц) та 5 (ГГц). Смуга частот 2,4 (ГГц) має 13 каналів для бездротових мереж завширшки 20 (МГц) (802.11b/g/n) або 40 (МГц) з інтервалами 5 (МГц) (IEEE 802.11n). Якщо бездротовий пристрій, який використовує Wi-Fi, використовує один із 13 частотних каналів, він заважатиме сусіднім каналам. Наприклад, якщо точка доступу використовує канал 6, сильні перешкоди торкнуться каналів 5 і 7, а слабкі перешкоди поширяться на канали 4 і 8 і так далі.

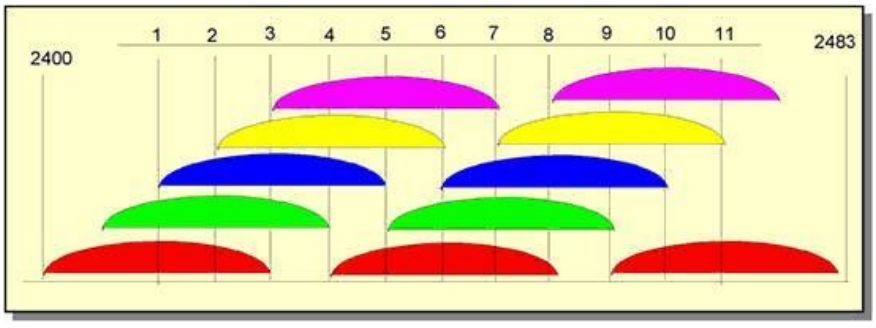


Рис.3.6. Спектр каналу 2.4 ГГц

Колірне кодування вказує на канали, що не перетинаються - [1,6,11], [2,7], [3,8], [4,9], [5,10]. Різні бездротові мережі, розташовані в одній місцевості, повинні будуватися на каналах, що не перетинаються.

2) Робота в зоні, де працює ваш Wi-Fi пристрій Bluetooth-пристрої.

Bluetooth-пристрій також працює в діапазоні - 2,4 (ГГц). Відповідно, може бути порушено роботу Wi-Fi пристроїв.

3) Велика відстань між пристроями Wi-Fi. Бездротові пристрої Wi-Fi мають обмежений радіус дії. Наприклад:

Радіус дії точки доступу Wi-Fi стандарту 802.11b/g становить 60 (м) у приміщенні та до 400 (м) на вулиці. Дальність дії в закритому приміщенні може скоротитися на кілька метрів через розташування приміщення, наявність стін та інших перешкод.

4) Бездротові перешкоди

Певні перешкоди (меблі, стіни, металеві двері тощо), які знаходяться між пристроями Wi-Fi, можуть викликати або не викликати перешкод, закусувати або поглинати радіосигнали, викликаючи часткову або повну втрату сигналу тривоги.

У висотних будинках головна перешкода – це самі будинки.

Наявність складних стін (бетон + арматура), листового металу, штукатурки на стіні, дротових фундаментів тощо, погано позначиться на роботі Wi-Fi-пристроїв і зменшить якість радіопокриття.

У приміщенні причиною перешкод можуть бути дзеркала та тоноване скло.

У таблиці нижче показано залежність негативного впливу середовища на якість Wi-Fi-покриття.

Таблиця 3.1

Список середовищ та їх впливу

Середовище	Додаткові втрати (дБ)	Відсоток повної дистанції
Відкрита площина	0	100%
Чисте вікно (без металу)	3	70%
Тоноване вікно	5-8	50%
Дерев’яна стіна	10	30%
Перегородка	15-20	15%
Підпірна стінка	20-25	10%
Бетонна стеля	15-25	10-15%
Монолітне залізне покриття	20-25	10%

Ефективна відстань відноситься до того, наскільки зміниться радіус розповсюдження після проходження цієї перешкоди порівняно з відкритою місцевістю. Наприклад, якщо радіус розповсюдження Wi-Fi на відкритому майданчику становить 400 (метрів), то після закриття перегородки він зменшиться до 400 м*15% = 60 (метрів). Після другої стіни знову 60 м*15% = 9 (м). Після третьої 9 м*15% = 1,35 (метра). Тому складно налагодити приймання сигналу через три стіни.

Зовнішня передача обумовлена перешкодами у зоні дії сигналу тривоги (наприклад, деревами, лісами, передгір'ями).

Атмосферні перепони (дощ, мокрий сніг) також заважають бездротовій сигналізації.

3.3. Вплив побутових приладів у зоні дії Wi-Fi-пристрою

Список побутових приладів, що впливають на якість Wi-Fi-з'єднання:

- Мікрохвильові печі. Вони можуть послабити сигнал Wi-Fi, і також працюють у діапазоні 2,4 (ГГц).

- рація, якими грають діти. Ці пристрої працюють у діапазоні 2,4 (ГГц).

Працюють та можуть вплинути на роботу Wi-Fi.

- Монітори, електродвигуни, бездротові телефони та ін.

- Бездротові пристрої.

Wi-Fi-з'єднання при використанні стандарту IEEE 802.11n методи збільшення швидкості, пропускної здатності та підтримання стабільності бездротового зв'язку.

При використанні бездротових пристроїв IEEE 802.11n швидкості нижче за очікувані, а пропускна здатність відповідає можливостям 802.11g.

Причини цього:

1) Більшість користувачів використовують вкладку “Стан мережі” на своїх ком-п'ютерах, після чого, помилково бачать швидкість з'єднання в мегабітах за секунду.

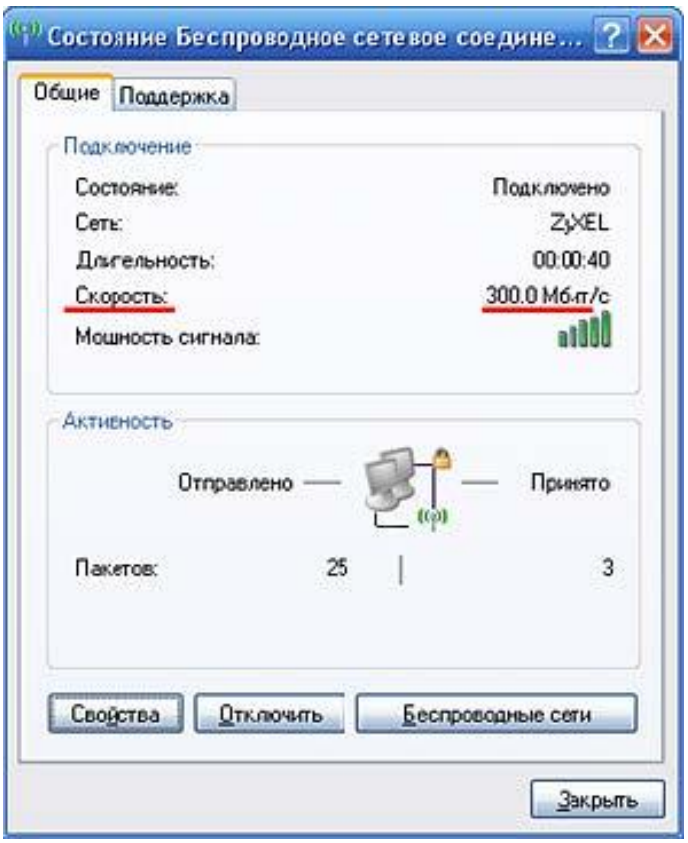


Рис. 3.7. Статус бездротового з'єднання

Помилково припускати, що наведені значення насправді представляють пропускну здатність. Це число відображається драйвером і вказує на фізичну швидкість, на

якій працює вибраний стандарт. Але основні смуги пропускання передачі можуть варіюватися від 50 до 140 Мбіт/с. Це може вплинути на створення точки доступу, що підтримує 802.11n, та підключених до неї бездротових адаптерів.

Якщо ми хочемо отримати справжнє значення швидкості передачі даних бездротового зв'язку, ми можемо використовувати такі комп'ютерні програми, як LAN Speed, Test, NetStress або NetMeter. Це програми для визначення швидкості та пропускної спроможності.

2) Деякі клієнти до точки доступу стандарту 802.11n

Здається, що їхню роботу покращить і примножить підключення до адаптерам стандарту 802.11b/g. Але це теж помилка, тому що у стандарті 802.11n використовуються інші технології, зокрема технологія MIMO. І вони ефективні лише з адаптерами стандарту 802.11n.

3) Старі стандарти із пристроями 802.11n

Також помилково думати, що всі швидкості зв'язку працюватимуть на рівні слабкого пристрою. 802.11n. Точка доступу 802.11n працює зі старими пристроями 802.11g та 802.11b, а також адаптерами 802.11n. Стандарт 802.11n забезпечує механізм сумісності з іншими пристроями. Якщо пристрій старого стандарту лише передає чи приймає інформацію, швидкість роботи знизиться на 50-80%. А якщо ви хочете працювати на максимальній швидкості, потрібно використовувати тільки пристрої стандарту 802.11n.

4) Пропускна здатність більшості пристроїв стандарту 802.11n. може знизитись до 80%. Це пов'язано з використанням методів безпеки WEP або WPA/TKIP. Стандарт 802.11n не працює на високих швидкостях, навіть якщо в ньому використовуються вищезазначені методи захисту. Якщо ви не бажаєте знижувати швидкість, вам необхідно використовувати метод безпеки WPA2/AES для бездротового зв'язку. Або слід використовувати незахищену мережу, але використовувати її небезпечно.

5) WMM (Wi-Fi)

Нам потрібно увімкнути мультимедійний режим. Режим WMM повинен бути увімкнений на всіх пристроях Wi-Fi (точках доступу, бездротових маршрутизаторах та адаптерах).

6). 40 (МГц) збільшення пропускної спроможності в стандарті 802.11n передбачено використання широкосмугових каналів. Зміна ширини каналу з 20 (МГц) на 40 (МГц) може зменшити швидкість, не збільшуючи її. Використання каналу шириною 40 (МГц) дає збільшення пропускної спроможності з 10 до 20 (Мбіт/с), але при дуже сильному шумі. А якщо сигналізація слабка, використання каналу 40 (МГц) буде малоефективним і не збільшить пропускну здатність. При слабкій тривозі показник знижується до 80% і не дає потрібного результату. Якщо ви помітили зниження швидкості при використанні каналу 40 (МГц), можна збільшити швидкість, переключившись на 20 (МГц).

7) Якщо відстань між точкою підключення та адаптером близька, у тому числі якщо з'єднання не встановлено, слід зменшити потужність точки підключення.

Якщо ми не можемо його зменшити, необхідно відсунути пристрої один від одного, усунути антену точки підключення або використовувати антену з малим коефіцієнтом посилення сигналу.

Варіанти бездротових девайсів

Точки підключення можуть бути внутрішніми (у будівлях) та всепогодними (на вулиці).

Опція стану приміщення використовується встановленням зв'язку всередині приміщення. Часто він недорогий, і його тип зазвичай відомий своїм чудовим естетичним зовнішнім виглядом. Створюють точки підключення, розраховані на одну чи дві кімнати та працюють у цій зоні. На відкритій місцевості (прямий огляд) під час використання стандартної все спрямованої антени, дальність передачі сягає 300 (метрів).

Погодні точки доступу призначені для підключення будівель. Залежно від типу антени, такі пристрої можуть створювати мережі каналів на відстані 3-5 (км). Під час використання підсилювачів, з'єднання бездротового каналу- збільшується до максимальної відстані, наскільки може бачити око. У цьому довжина радіоканалу сягає 8-10 (км).

Комбіновані пристрої

Великим інтересом користуються точки бездротового доступу, які включають функції інших пристроїв. Наприклад, високошвидкісний широкосмуговий маршрутизатор із підключеним комутатором Fast Ethernet. Маршрутизатори дозволяють швидко та легко встановити дротове або бездротове підключення до Інтернету чи організувати спільне використання широкосмугового з’єднання та домашнього чи офісного кабельного/DSL-модему.

Рис.3.8. Внутрішня точка доступу

Рис.3.9. Зовнішня точка доступу

3.4. Основні правила інформаційної безпеки

Кожна IT-послуга чи об'єкт у загальній інфраструктурі підприємства має певний фактор ризику, тому розробка концепції безпеки будь-якої установи повинна починатися з їх комплексного аналізу.

Ще одним важливим фактором при плануванні концепції безпеки є облік різних загроз для кожної IT-інфраструктури. Ці аспекти безпосередньо пов'язані з факторами оцінки об'єктів та дають інформацію про подальші дії щодо захисних заходів. Важливим правилом ефективності дій є те, що захист не повинен бути надмірним.

Результати комплексного аналізу видів загроз та оцінки кожного об'єкта IT-інфраструктури є основою для розробки та реалізації політики безпеки. Це коригування та оновлення політики управління, систем моніторингу й аудиту, а також інших системних політик та процедур, які включають профілактичні міри.

Необхідною умовою є наявність випробувальної лабораторії, схожої на типове IT-середовище підприємства. Накопичені знання та досвід аналізу загроз та вразливостей систем є, по суті, унікальною базою знань та є основою для створення надійної та безпечної інфраструктури для подальшого навчання співробітників. Однак, слід зазначити, що при зміні (модернізації) інфраструктури, додаванні нових об'єктів- необхідно проводити переоцінку, аналіз та подальшу зміну політики безпеки.

На цьому етапі можуть виникнути такі небезпеки.

Підвищення привілеїв – це отримання системних привілеїв через переповнення буфера, незаконних атак на адміністративні права.

Фальсифікація – зміна даних, що передаються мережею, зміна файлів.

Моделювання — підробка електронних повідомлень, створення пакетів у відповідь при аутентифікації.

Розкриття – це несанкціонований доступ або незаконне розголошення конфіденційної інформації.

Відхилити – означає видалити важливий файл або покупку, а потім відмовитись підтверджувати свої дії.

Відмова в обслуговуванні – це навантаження мережевих ресурсів великою кількістю шахрайських пакетів.

Методи захисту на всіх рівнях.

Щоб знизити ймовірність успішного вторгнення до IT-середовища підприємства, заходи безпеки мають бути реалізовані на всіх рівнях. Ця концепція інформаційної безпеки означає, що порушення рівня захисту не ставить під загрозу всю систему.

Дизайн та конструкція кожного рівня безпеки повинні виходити з того, що зловмисник може зламати будь-який рівень. Крім того, кожен із рівнів має свої унікальні та ефективні методи захисту. З переліку технологій, що виробляються і доступні багатьма відомими вендорами, можна вибрати найбільш підходящий за технічними та економічними факторами варіант.

Наприклад:

- Захист даних – списки контролю доступу, шифрування.
- Програми - захищені антивірусними системами.
- Комп'ютери - захист операційної системи, керування оновленнями, автентифікація, система виявлення вторгнень лише на рівні хоста.
- Внутрішня мережа – сегментація мережі, IP-безпека, системи виявлення мережевих вторгнень.
- Периметр — програмний та програмно-апаратний міжмережевий екран, створення приватних віртуальних мереж з функціями карантину.
- Фізичний захист - засоби безпеки, контролю доступу та моніторингу.
- Політики та процедури - навчання користувачів та технічного персоналу.

Таким чином, внаслідок комплексних заходів захисту на всіх рівнях спрощується процес виявлення вторгнень та знижуються шанси зловмисника на успіх.

Людський фактор

Більшість рівнів захисту базуються на апаратному та програмному забезпеченні, проте вплив «людського фактору» суттєво змінює загальну картину.

Рівень фізичного захисту

Вимоги до фізичного захисту є базовими та основними.

Отримавши фізичний доступ до обладнання, зловмисник може легко оминути наступні рівні захисту. Ви можете використовувати телефони компанії або

телефонні пристрої для доступу. Витоку конфіденційної інформації включають, зокрема, ноутбуки, які можуть бути за межами корпорації.

У ряді випадків фактор доступу спрямований на заподіяння шкоди. Однак за наявності фізичного доступу можна встановити програмні засоби для моніторингу та контролю важливої корпоративної інформації, яку можуть накопичувати довгий час.

Ви можете використовувати будь-які засоби, які дозволяють кошти підприємства задля забезпечення рівня безпеки фізичного захисту. Можливості безпеки повинні охоплювати всі компоненти IT-інфраструктури. Наприклад, сервісний інженер замінив масив RAID-1, що вийшов з ладу і містить важливі дані корпоративних користувачів. Після цього ви можете відправити накопичувач у сервісний центр, де його можна буде відновити та отримати доступ до даних. І тут вважатимуться, що порушено рівень фізичного захисту підприємства.

Першим кроком у забезпеченні надійного рівня захисту є фізичний поділ інфраструктури сервера та користувача. У той же час обов'язкова наявність окремого захищеного корпусу із суворим контролем доступу та процедурами спостереження. Наявність особистого доступу на основі магнітних карток або біометричних пристроїв значно знижує шанси зловмисника. Серверна має бути обладнана автоматичними системами пожежогасіння та клімат-контролю.

Доступ можна додатково контролювати за допомогою системи відеоспостереження із записом подій.

Віддалений доступ до консолей серверів також суворо контролюється.

Адміністративну групу має сенс розділити на окремий фізичний сегмент із постійним доступом до керованих комутаторів та хостів, як на мережному рівні, так і на логічному рівні індивідуальної ідентифікації.

Наступні заходи щодо забезпечення повного комплексу фізичного захисту, повинні бути зосереджені на видаленні пристроїв введення (дискет та компакт-дисків) з комп'ютерів, де вони більше не потрібні. Якщо це неможливо, необхідно використовувати програмне забезпечення для блокування доступу до носія. Зреш-

тою, має бути забезпечена гарантія фізичного захисту активного мережевого обладнання (комутаторів, маршрутизаторів) у спеціальних шафах з доступом. Крім того, необхідно стежити за тим, щоб комутувалися лише необхідні пристрої та джерела живлення.

Периметр інформаційної системи - це частина мережної інфраструктури, найбільш відкрита для зовнішніх атак.

До периметру входять: Інтернет, філії, партнерські мережі, мобільні користувачі, бездротові мережі.

Інтернет-програми.

Важливо враховувати безпеку цього рівня загалом, а не лише для конкретного маршруту. Можливі напрямки атаки по периметру:

• у мережу організації

• для мобільних користувачів

• від партнерів

Як завжди, напрямок Інтернету є найбільш вразливим, але загроза в іншому напрямку не є незначною. Безпека всіх пристроїв, що входять і виходять із вашої мережі, є дуже важливою. Може бути невизначеність щодо заходів безпеки в мережевій інфраструктурі ділових партнерів або афілійованих осіб, тому слід приділити увагу і цій галузі.

Безпека периметра насамперед забезпечується за рахунок використання брандмауера. Їхня конфігурація зазвичай технічно дуже складна і вимагає висококваліфікованого персоналу, а також ретельного документування налаштувань. Сучасні операційні системи дозволяють легко ізолювати порти, що не використовуються, щоб знизити ймовірність атаки.

Перетворення мережевих адрес (NAT) дозволяє організації блокувати внутрішні порти. При передачі інформації небезпечними каналами необхідно використовувати методи створення віртуальних приватних мереж (VPN) на основі шифрування та тунелів.

Загрози та захист локальної мережі

Атаки можуть бути зроблені лише із зовнішніх джерел. За статистикою дуже великий відсоток успішних атак відноситься до атак у мережевому оточенні. Створення внутрішньої мережевої безпеки має вирішальне значення для запобігання шкідливих та випадкових загроз. Неконтрольована внутрішня мережна інфраструктура дозволяє зловмиснику отримати доступ до важливої корпоративної інформації та контролювати мережевий трафік. Цілком керовані мережі дозволяють зловмиснику отримати доступ до будь-яких ресурсів у будь-якому сегменті мережі. Мережеві операційні системи мають безліч вбудованих мережевих служб, кожна з яких може стати об'єктом атаки.

Для захисту внутрішнього середовища мережі необхідно забезпечити надійні механізми автентифікації користувачів у глобальній службі каталогів (єдиний центр доступу). Взаємна автентифікація на рівні сервера та мережної робочої станції, значно підвищує якість мережної безпеки. Поточні вимоги відносяться до керованого комутованого середовища та логічної сегментації (VLAN). Для керування віддаленими пристроями завжди слід використовувати безпечне протокольне з'єднання (наприклад, SSH). Трафік Telnet можна легко перехопити, а імена користувачів та паролі надаються у відкритому вигляді. Приділяючи пильну увагу захисту резервних копій конфігурації мережевих пристроїв, вони можуть розповісти зловмиснику про топологію мережі.

Рис.3.10. Загрози локальної мережі

Навіть після мережного сегмента мережевий трафік має бути захищеним. Як дротові, так і бездротові з'єднання шифруються та аутентифікуються, ви можете використовувати протокол 802.1X для надання доступу. Це рішення може використовувати облікові записи та паролі у глобальній службі каталогів (Microsoft Active Directory, Novell e-Directory тощо) або цифрові сертифікати. Технологія цифрових сертифікатів забезпечує дуже високий рівень захисту мережевого транспорту, але потребує розгортання інфраструктури відкритих ключів у вигляді сервера та сховища сертифікатів.

Впровадження технологій шифрування та цифрових підписів, таких як підпис IPSec або Server Message Block (SMB), запобігає перехопленню та аналізу мережевого трафіку, а саме:

-Захист локальної мережі

-Взаємна автентифікація користувачів та мережевих ресурсів

-Сегментація LAN

-Шифрування мережевого трафіку

-Блокування порті, що не використовуються.

-Контроль доступу до мережевих пристроїв

-Цифровий метод підписування мережевих пакетів

-Компрометація та захист вашого комп'ютера

Комп'ютерні системи у мережному середовищі виконують кілька завдань, що визначають вимоги безпеки. Мережеві хости можуть бути атаковані, тому що вони доступні багатьом. Зловмисники можуть розповсюджувати шкідливий код (віруси) для атаки. Програмне забезпечення, яке встановлюється на робочі станції та сервери, може містити вразливості в програмному коді, тому своєчасне встановлення оновлень є одним із найважливіших кроків у спільній концепції захисту.

Параметри політики безпеки на рівні комп'ютера повинні контролюватись централізовано, наприклад, за допомогою групової політики.

Захист серверних систем на цьому рівні включає налаштування атрибутів безпеки для файлових систем, політик аудиту, фільтрації портів та інших заходів, залежно від ролі та призначення сервера.

Наявність всіх доступних оновлень операційної системи та програмного забезпечення значно підвищить загальний рівень безпеки. Ви можете використовувати будь-які засоби автоматичної установки та моніторингу оновлень, від найпростіших – Windows Update, Software Update Service (SUS), Windows Update Service (WUS) до найскладніших та найпотужніших – Systems Management Server (SMS).

Використовуючи антивірусний пакет із поточними оновленнями, персональний брандмауер із фільтрацією портів знижує можливість атаки.

Щоб захистити свій комп'ютер, потрібно виконувати наступні рекомендації:

-Взаємна автентифікація користувачів, серверів та робітників станцій

-Захист ОС

-Встановлювання оновлення безпеки

-Перевіряти успіхи та невдачі

-Вимкнути служби, що не використовуються

-Встановлювати та оновлювати антивірусні системи

Мережеві програми дозволяють користувачам отримувати доступ до даних та керувати ними. Програма мережі — це точка доступу до сервера, на якому працює програма. У цьому випадку програма забезпечує певний рівень мережевого обслуговування, яке має бути стійким до атак зловмисників. Як наші власні розробки, так і комерційні продукти, що використовуються для виявлення вразливостей, мають бути ретельно досліджені. Метою атаки може бути знищення коду програми (що призводить до недоступності) та виконання шкідливого коду. Зловмисник також може використовувати тактику розподіленої атаки, спрямовану перевантаження програми. В результаті обслуговування може бути відмовлено (відмова в обслуговуванні).

Програму можна використовувати для непередбачених завдань, таких як пересилання поштових повідомлень (ретрансляція відкритої пошти). Для цього, потрібно лише встановити та налаштувати з необхідною функціональністю та рівнем обслуговування, а програмним кодом можна керувати за допомогою систем моніторингу та антивірусних пакетів. Щоб мінімізувати ризики, виконання додатків повинно бути обмежене мінімальними привілеями мережі.

3.5 Види атак

Захист з використанням MAC-адреси

Один з найбільш поширених способів захисту, це звичайно ж прив'язка MAC-адресою пристрою. Даний спосіб може як дозволяти, так і забороняти підключення до бездротової мережі будь-якого пристрою, достатньо лише вказати його адресу MAC. Після цього вибрати Black list або White list. Само собою, Black list це обмеження підключення до точки доступу, а White list – його протилежність.

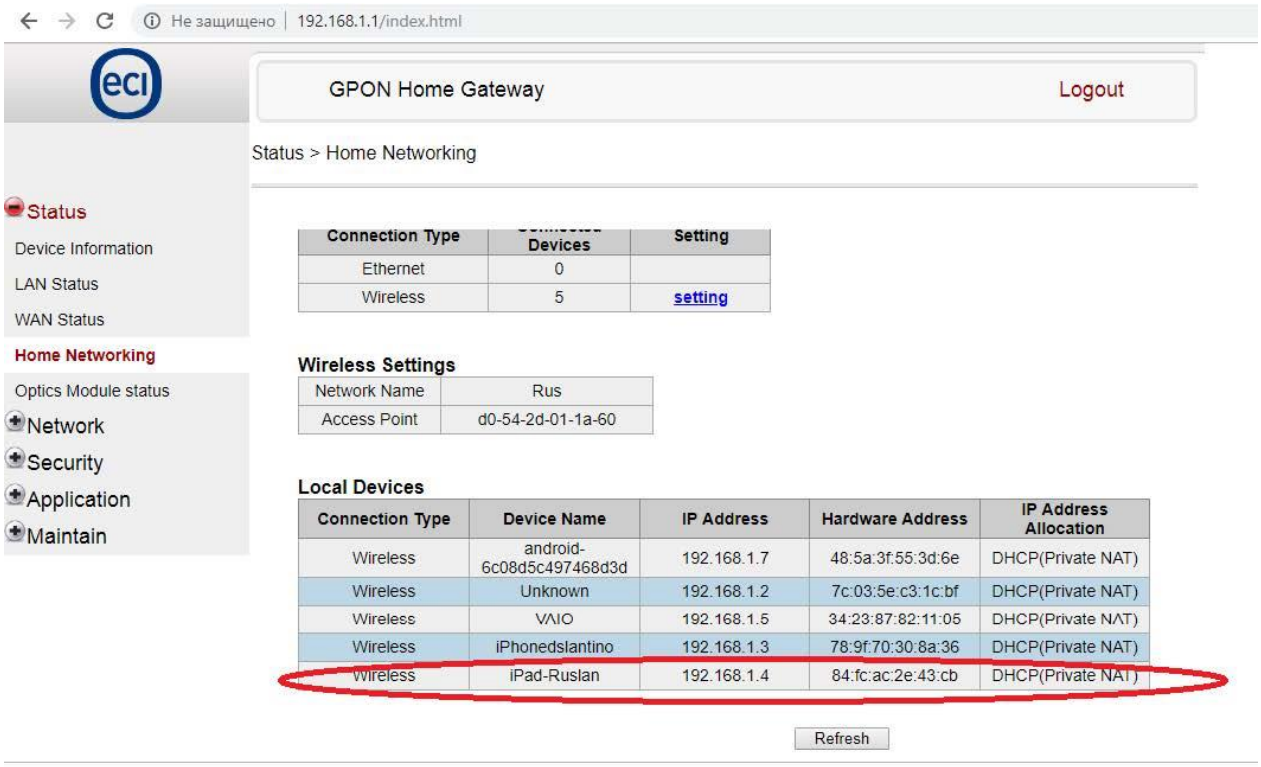


Рис.3.11. Вибір потрібної MAC-адреси із доступного списку

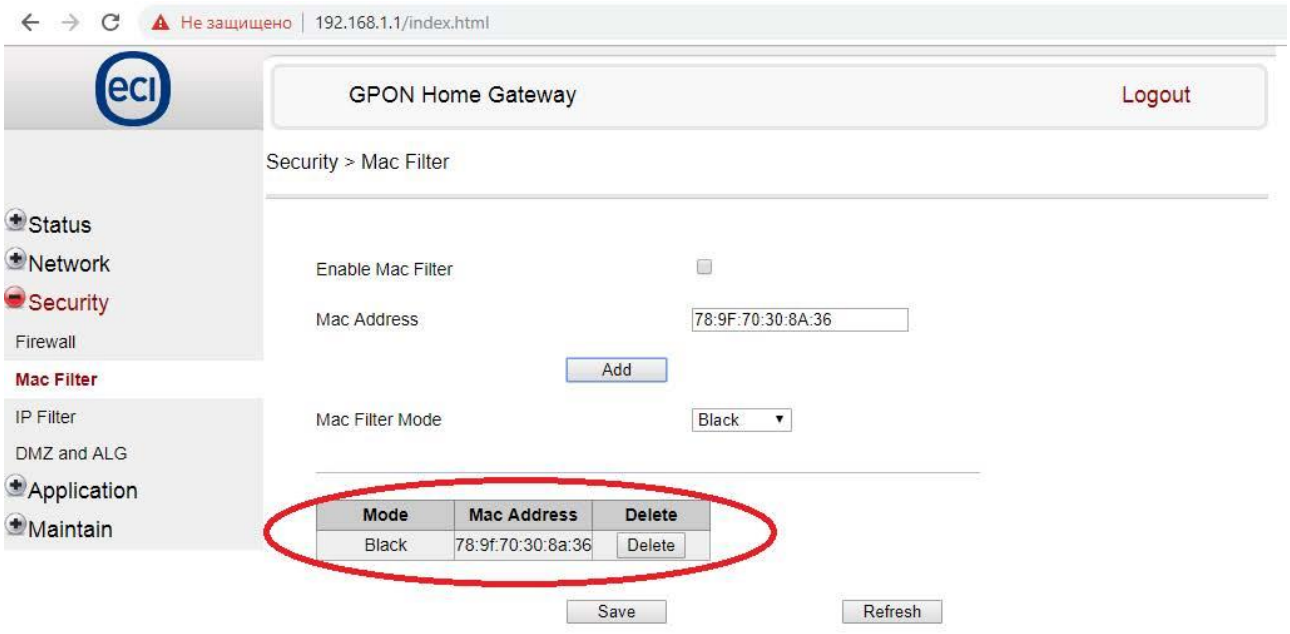


Рис.3.12. Дія над вибраною MAC-адресою

Після чого пристрій відключається від бездротової мережі, і не може до нього підключитися, оскільки стоїть обмеження за адресою MAC, даного пристрою.

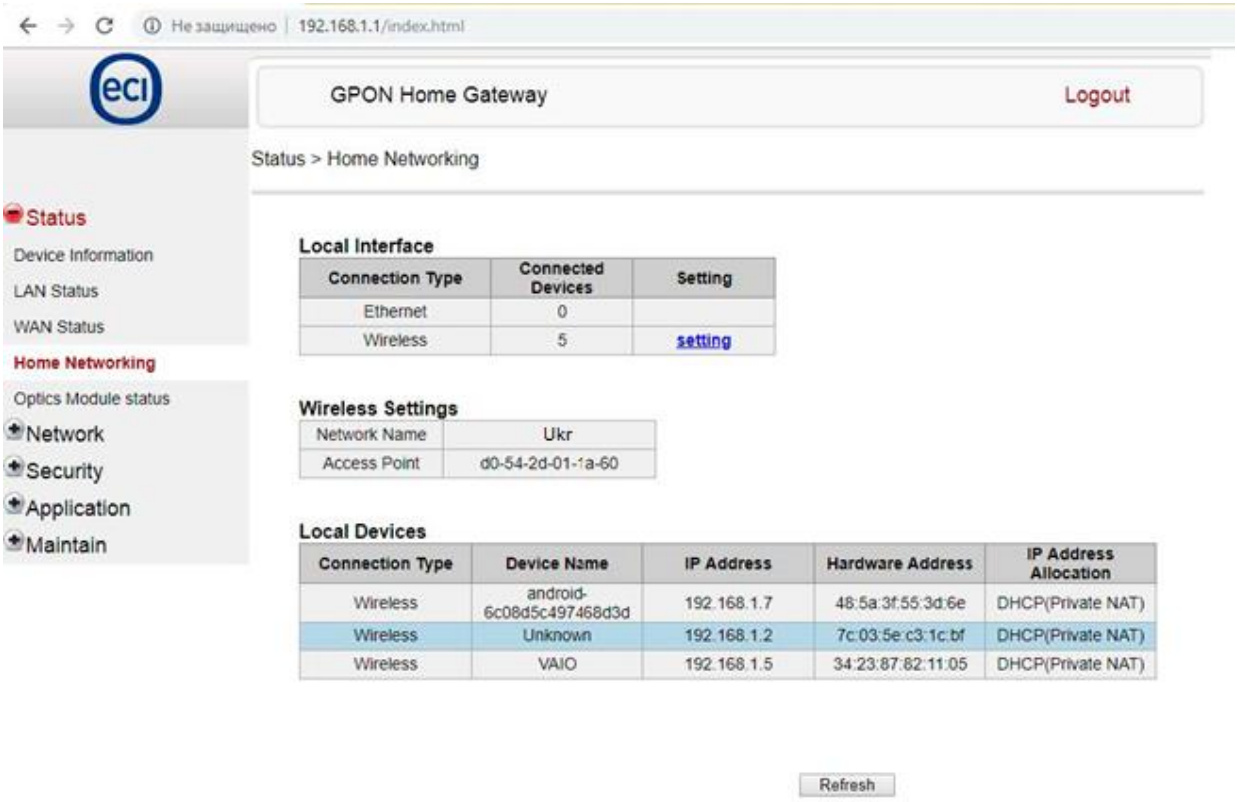


Рис.3.13 Відсутність у списку підключених пристроїв, щойно заблокованого

Використання складного пароля

Звичайно не мало важливою складовою є складність обраного пароля, для бездротової мережі, чим довше і складніше він буде, тим менше шансів, що вашу мережу зможуть зламати, пріоритетно мати в паролі літери різних регістрів, цифри та різні спецсимволи, що досить сильно ускладнить отримання несанкціонованого доступу. мережі.

Приховування точки доступу

Наступним способом захисту є приховування точки доступу, тобто відключення транслювання імені бездротової мережі. Для отримання доступу до такої мережі крім пароля, так само потрібно знати назву точки доступу та спосіб шифрування для проходження аутентифікації. Цей спосіб дозволить приховати бездротову мережу від небажаних підключень.

Для цього потрібно вимкнути SSID broadcast у налаштуваннях роутера.

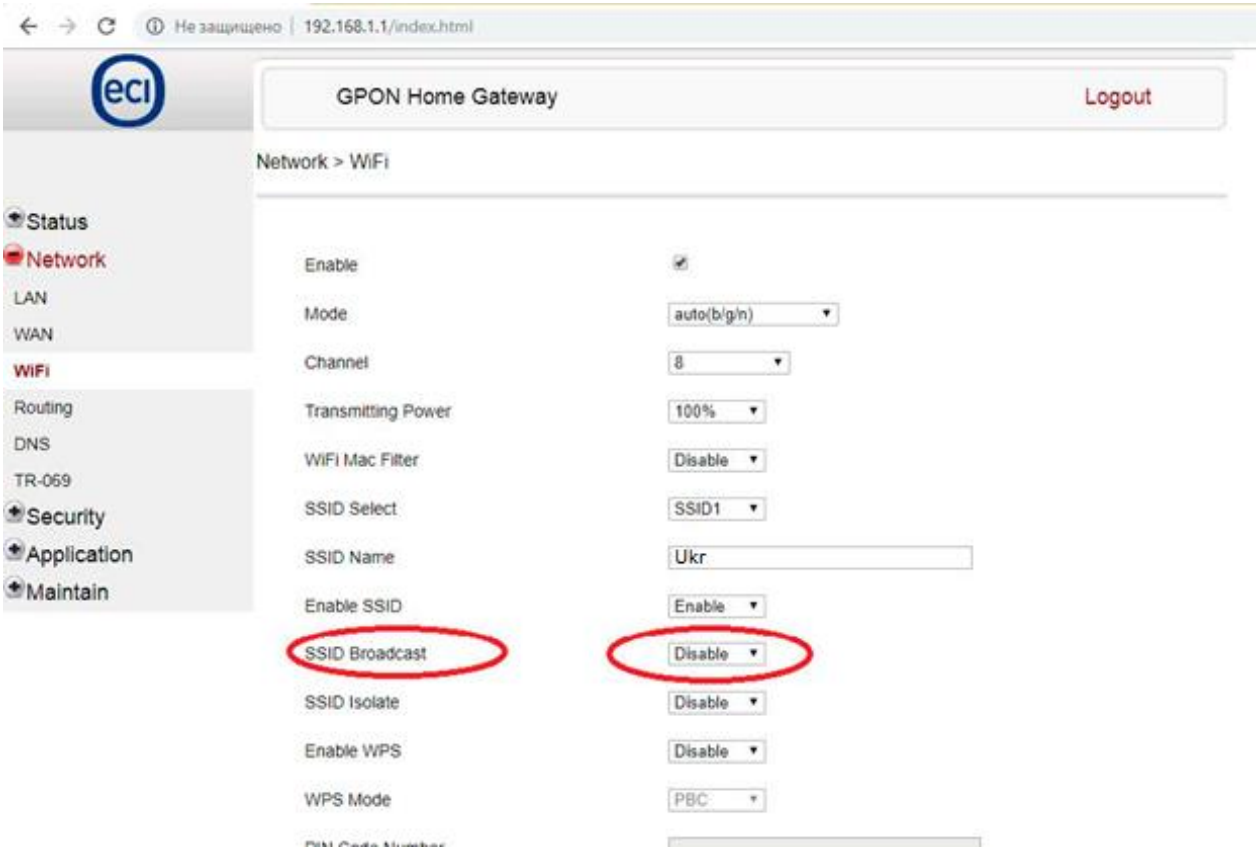


Рис.3.14. Відключення SSID broadcast

Після цього бездротова мережа зникне зі списку доступних мереж, оскільки не відображатиметься її SSID (назва).

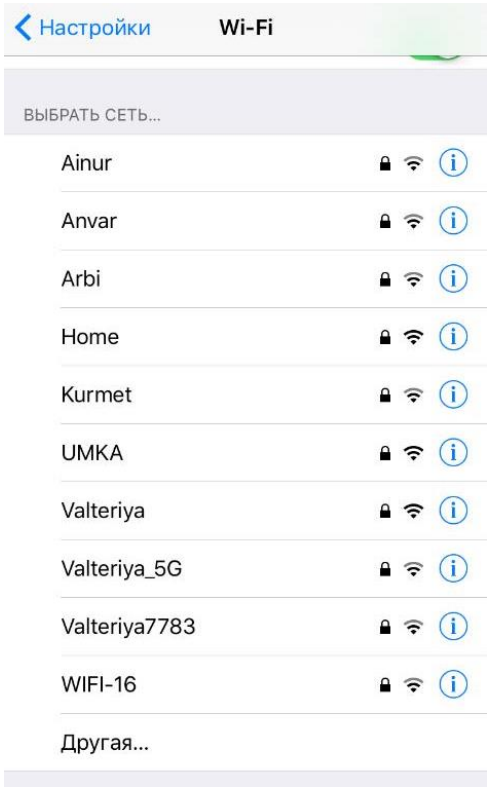


Рис.3.15. Відсутність потрібної бездротової мережі

Далі для підключення до такої мережі потрібно буде вказати назву мережі (SSID), пароль та спосіб шифрування.

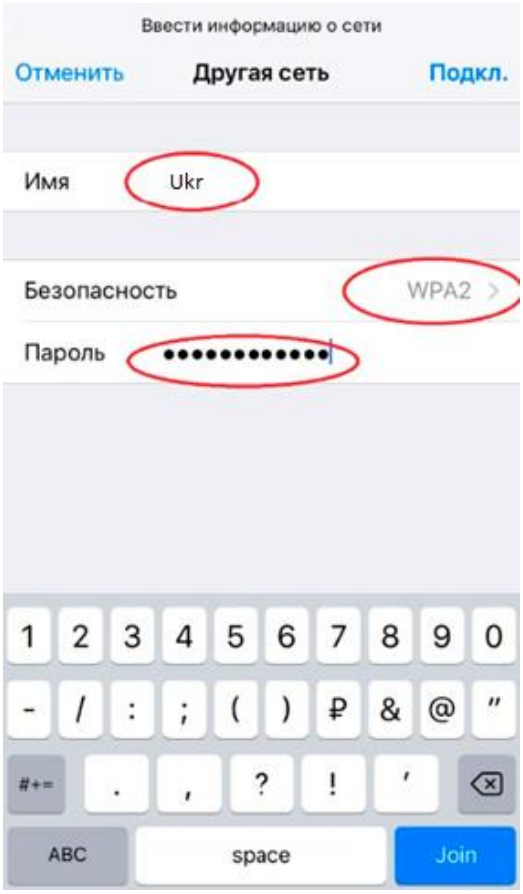


Рис.3.16. Підключення до прихованої бездротової мережі

WPA-3

У червні 2018 року, альянс розробників Wi-Fi оголосив про закінчення розробки нового стандарту безпеки – WPA-3. Це одночасно новий протокол безпеки, і назва відповідної програми сертифікації.

Перш ніж на тому чи іншому обладнанні з'явиться лейбл WPA-3, йому необхідно буде пройти величезну кількість тестів - це гарантує коректну роботу з іншими пристроями, що отримали ту ж мітку. З точки зору користувача стандарт WPA3 можна назвати протоколом безпеки, але мається на увазі під цим не апаратна реалізація, а відповідність нормативам.

Відмінності WPA-3 від WPA-2 Творці WPA3 спробували усунути концептуальні недоробки, що випливли з появою KRACK. Новий стандарт, як і в усіх попередніх випадках, ґрунтується на технологіях його попередника. В анонсі WPA-3 представники альянсу з розробки Wi-Fi говорили про застосування чотирьох нових

технологій, які мають стати на захист бездротового з'єднання. Але лише одна з них стала обов'язковою для реалізації виробниками.

Оскільки ключова вразливість ховалася в чотиристоронньому рукостисканні, WPA-3 додалася обов'язкова підтримка більш надійного методу з'єднання – SEA, також відомого як Dragonfly. Технологія SEA (Simultaneous Authentication of Equals) вже застосовувалася в mesh-мережах та описана у стандарті IEEE 802.11s. Вона заснована на протоколі обміну ключами Діффі – Хеллмана з використанням кінцевих циклічних груп.

SEA відноситься до протоколів типу PAKE та надає інтерактивний метод, відповідно до якого дві і більше сторони встановлюють криптографічні ключі, що базуються на знанні пароля однією або декількома сторонами. Результуючий ключ сесії, який одержує кожна зі сторін для автентифікації з'єднання, вибирається на основі інформації з пароля, ключів та MAC-адрес обох сторін. Якщо ключ однієї зі сторін виявиться скомпрометований, це не спричинить компрометацію ключа сесії. І навіть дізнавшись пароль, атакуючий не зможе розшифрувати пакети.

Ще одним нововведенням WPA-3 буде підтримка PMF (Protected Management Frames) для контролю за цілісністю трафіку. Але в майбутньому підтримка PMF стане обов'язковою для WPA-2.

Не потрапили до сертифікації WPA-3 програми Wi-Fi Easy Connect та Wi-Fi Enhanced Open. Wi-Fi Easy Connect - дозволяє реалізувати спрощене налаштування пристроїв без екрана. Для цього можна використовувати інший, більш сучасний пристрій, вже підключений до бездротової мережі. Наприклад, параметри мережі для датчиків та розумного домашнього начиння можна буде задавати зі смартфона, сфотографувавши QR-код на корпусі девайсу.

Easy Connect заснований на застосуванні аутентифікації за відкритими ключами (у QR-коді передається відкритий ключ) і може використовуватися в мережах з WPA-2 та WPA-3. Ще одна приємна особливість Wi-Fi Easy Connect – можливість заміни точки доступу без необхідності переналаштовувати всі пристрої.

Wi-Fi Enhanced Open має на увазі шифрування всіх потоків даних між клієнтом та точкою доступу. Ця технологія дозволить захистити приватність користувача в публічних мережах, де не потрібна автентифікація. Для генерації ключів у таких мережах застосовуватиметься процес узгодження з'єднання, що реалізується розширенням Opportunistic Wireless Encryption.

Підтримка обох технологій не обов'язкова для сертифікації WPA-3, але виробник може за бажання сам включити їх підтримку в продукт.

Як і в WPA-2, в WPA-3 передбачено два режими роботи: WPA-3-Personal та WPA-3-Enterprise.

WPA-3-Personal забезпечить надійний захист, особливо якщо користувач поставив стійкий пароль, який не можна отримати словниковим перебором. Але якщо пароль не зовсім тривіальний, то має допомогти нове обмеження на кількість спроб автентифікації в рамках одного рукостискання. Також обмеження не дозволить підбирати пароль у офлайновому режимі. Замість ключа PSK у WPA-3 реалізована технологія SEA.

WPA-3-Enterprise передбачає шифрування на основі щонайменше 192-розрядних ключів, що відповідають вимогам CNSA (вони вироблені комітетом NSS для захисту урядових, військових та промислових мереж). Для автентифікованого шифрування рекомендовано застосування 256-розрядних ключів GCMP-256, для передачі та підтвердження ключів використовується HMAC з хешами SHA-384, для узгодження ключів та аутентифікації - ECDH та ECDSA з 384-розрядними еліптичними кривими, для захисту цілісності кадрів - протокол BIPGMAC-256.

3.6. Налаштування адаптера та доступу до БС та РРС

Для налаштувань й планово-діагностичних робіт базової та радіорелейної станцій, потрібне дротове підключення з роз’ємом RS-232, що в свою чергу ускладнює ланцюг підключень. У даній роботі, було запропоновано, використати зі сторони станцій, один адаптер-перетворювач (ADA-14110) з RS-232 до Wi-Fi, а потім, шляхом безпровідного Wi-Fi підключення між ноутбуком та RS-адаптером, з’єднати

дані девайси. Після чого, зона бездротового підключення буде обмежуватися довжиною Wi-Fi-покриття.

Почнемо з процедури підключення до базової та радіорелейної станцій, з можливістю з’єднання з ними через LAN-інтерфейс або роз’єм RS-232, а також проведемо потрібні налаштування.

При вірному налаштуванні й узгодженні з пристроями мережі, ми отримуємо гарантовану надійність і працездатність всієї системи.

Для підключення пристроїв між собою, необхідно мати кабель стандарту RS-232 (рис 3.5).

Рис 3.5. Вигляд кабелю RS-232

Підключившись шляхом цього кабелю до нашого пристрою, виникло сповіщення, стосовно з’єднання з мережею (рис 3.6).

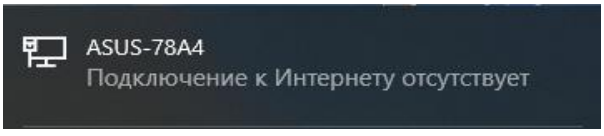


Рис 3.6. Індикація підключення

Внаслідок з’єднання наших пристроїв, необхідно перейти до налаштувань адаптера й прописати певну IP-адресу, шлюз та маску мережі. Відрегулювавши правильне узгодження мережі, необхідно перевірити доступність параметрів з’єднання.

Увійшовши у команди CMD, треба прописати команду “ipconfig”, яка надасть IP-адресу нашого пристрою, маску мережі, а також, вже налаштований нами шлюз (рис 3.7).

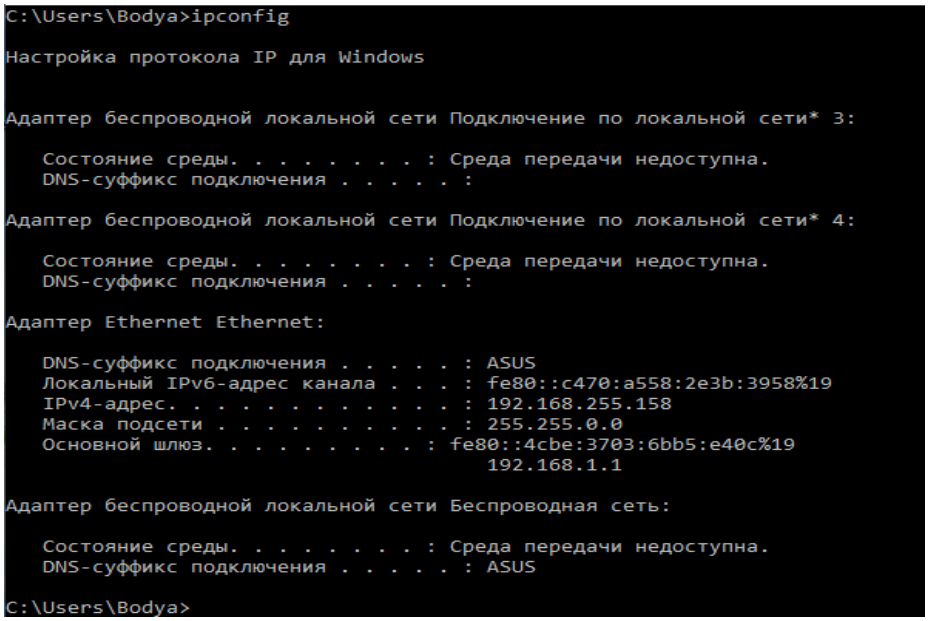


Рис 3.7. Команда “ipconfig”

Потім необхідно ввести команду “ping (+ IP-адресу базової станції)”, у даному випадку БС має саме цю IP-адресу: 192.168.255.131, через що, прописуємо до команд CMD, команду “ping 192.168.255.131”, (рис 3.8).

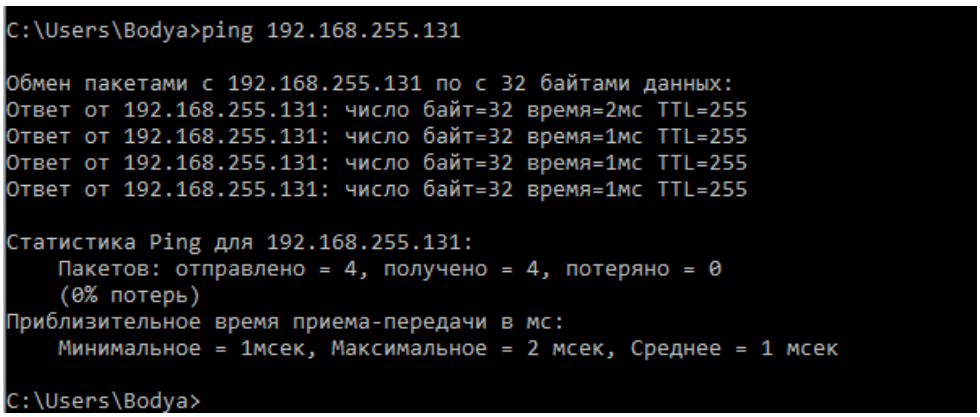


Рис 3.8 Команда “ping”

З чого ми бачимо, що з’єднання стабільне, IP-адреса пінгується, а час затримки 1-2 (мс), що є відмінним показником для цієї мережі.

Для переходу до налаштувань БС, спочатку потрібно відкрити менеджер 2G Flexi BTS, який проведе з'єднання на рівні програми (рис 3.9).

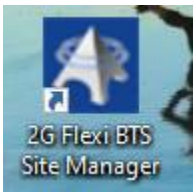


Рис 3.9 Ярлик застосунку

При запуску цього додатку, необхідно прописати IP-адресу нашої базової станції й відповідно до цього- конфіденційний пароль, який може знати тільки довірена особа, яка обслуговує цей комплекс (рис 3.10).

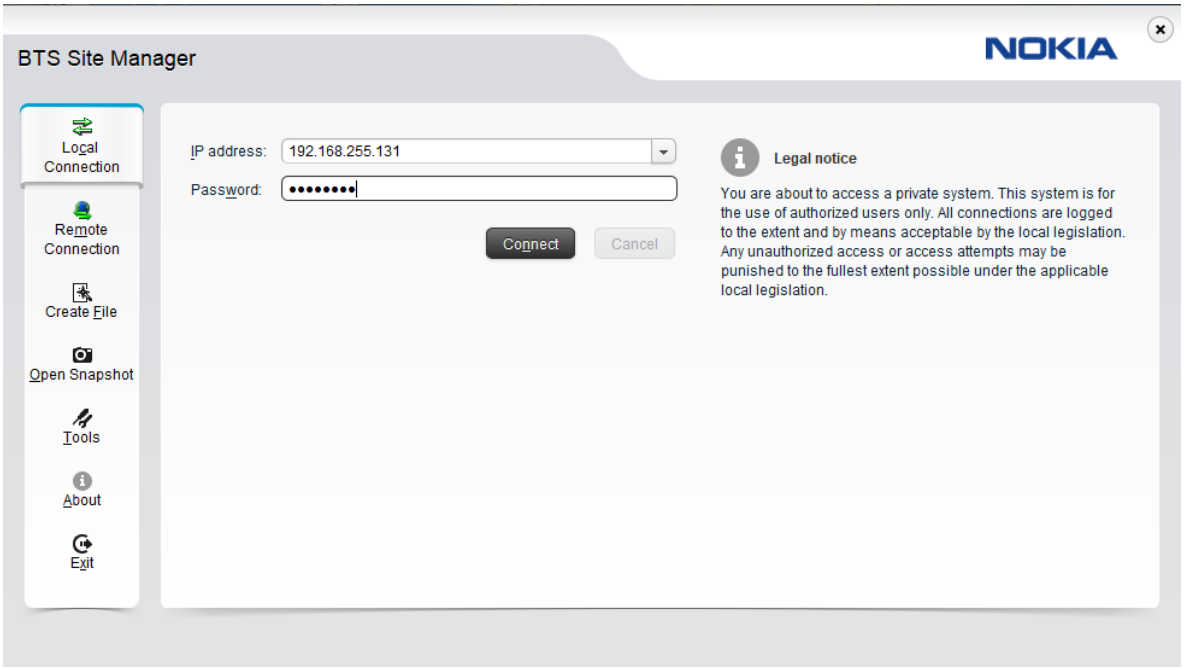


Рис 3.10 Внесення певних даних для входу

Натискаємо "connect", чекаємо повну перевірку сумісності версій ПЗ та наших конфіденційних даних (рис 3.11).

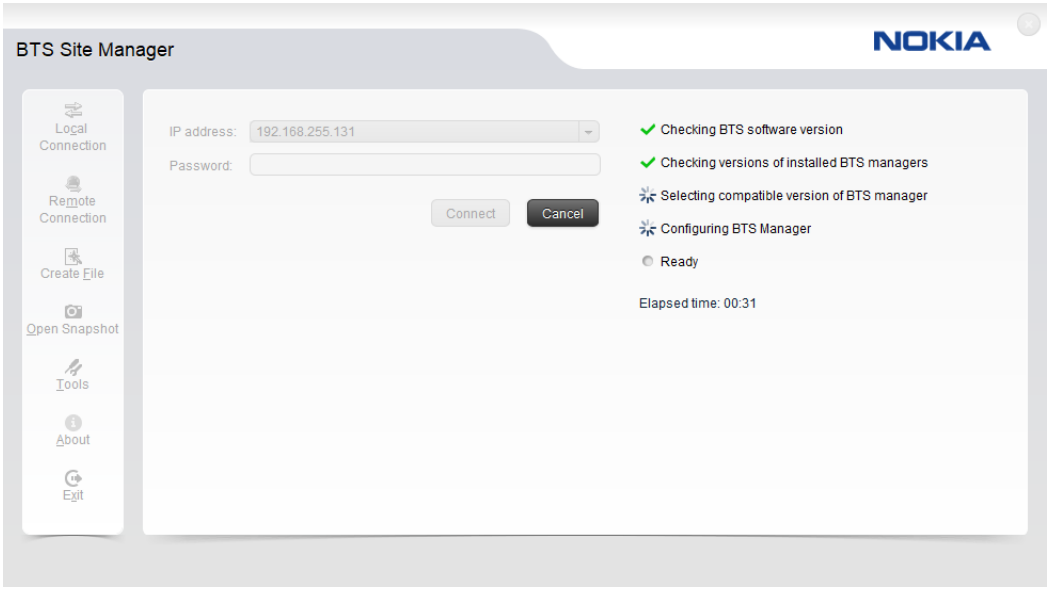


Рис 3.11 Перевірка сумісності

У вікні, що відкрилося, ми бачимо загальне середовище, у якому ми маємо змогу налаштовувати всі важливі функції, що є вкрай необхідним для функціонування комплексу базової станції (рис 3.12) [18].

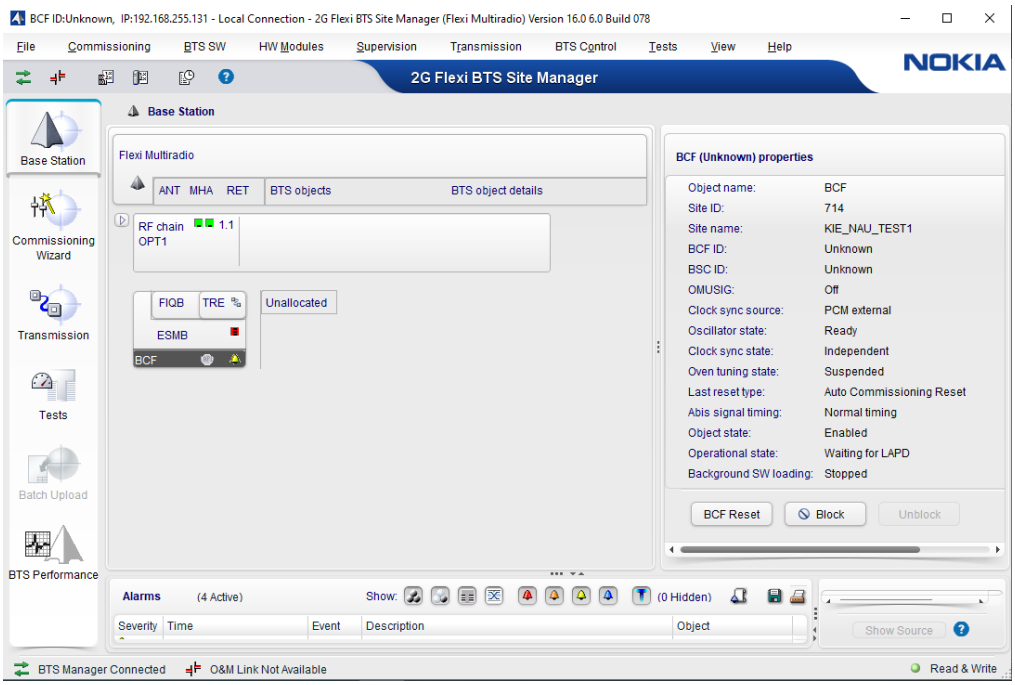


Рис 3.12 Успішне підключення

Але, основними мінусами цього ланцюжка підключень є- його мобільність та випромінювання від джерела до інженера. А, якщо, встановити безпровідний Wi-Fi-

зв’язок, то ми зможемо з’єднуватися від ноутбука до базової станції у мобільний спосіб, із чого слідує наступне, тоді можна буде проводити діагностику й налаштування базової станції на значній відстані, подалі від джерела випромінювання та у комфортному, нешкідливому місці для працівників обслуговування, наприклад, взимку у машині, знаходячись на значній відстані від БС та радіорелейної станції.

Бездротовий канал зв’язку від базової станції до ноутбука, можливо зробити за допомогою, Wi-Fi-адаптера (RS-232 to Wi-Fi).

Відповідно, потрібно підключити базову та радіорелейну станції до модуля Wi-Fi, вже знайомою нами витою парою, яку було показано на рисунку 3.13, а також, провести налаштування адаптера.

Даний адаптер буде зображено на рисунку нижче:

Рис.3.13 Вигляд модулю бездротового підключення

Бездротовий послідовний сервер ADA-14110 передає дані між пристроями, оснащеними інтерфейсом RS-232, через бездротову мережу WLAN. Передача даних здійснюється без втручання у формат даних, що передаються. Робота в бездротовій мережі Wi-Fi WLAN може здійснюватись у режимі віртуального послідовного порту (сервера портів), шлюзу даних MODBUS, послідовного мосту TCP та UDP, TCP та UDP сокету.

Шлюз даних MODBUS перетворює протоколи MODBUS-RTU master/slave та MODBUS-ASCII master/slave у протокол MODBUS-TCP і навпаки. Це дозволяє інтегрувати пристрої MODBUS-RTU/ASCII із пристроями MODBUS-TCP в одну мережу.

ADA-14110 підтримує такі протоколи, як: TCP, UDP, DHCP, SNMP, SSL/TLS, Telnet, Rlogin, LPD, HTTP/HTTPS, SMTP, ICMP, IGMP, ARP. Сервер має WWW-сервер для віддаленого налаштування та керування за допомогою інтернет-браузера і має швидкість передачі даних до 230 кбіт/с.

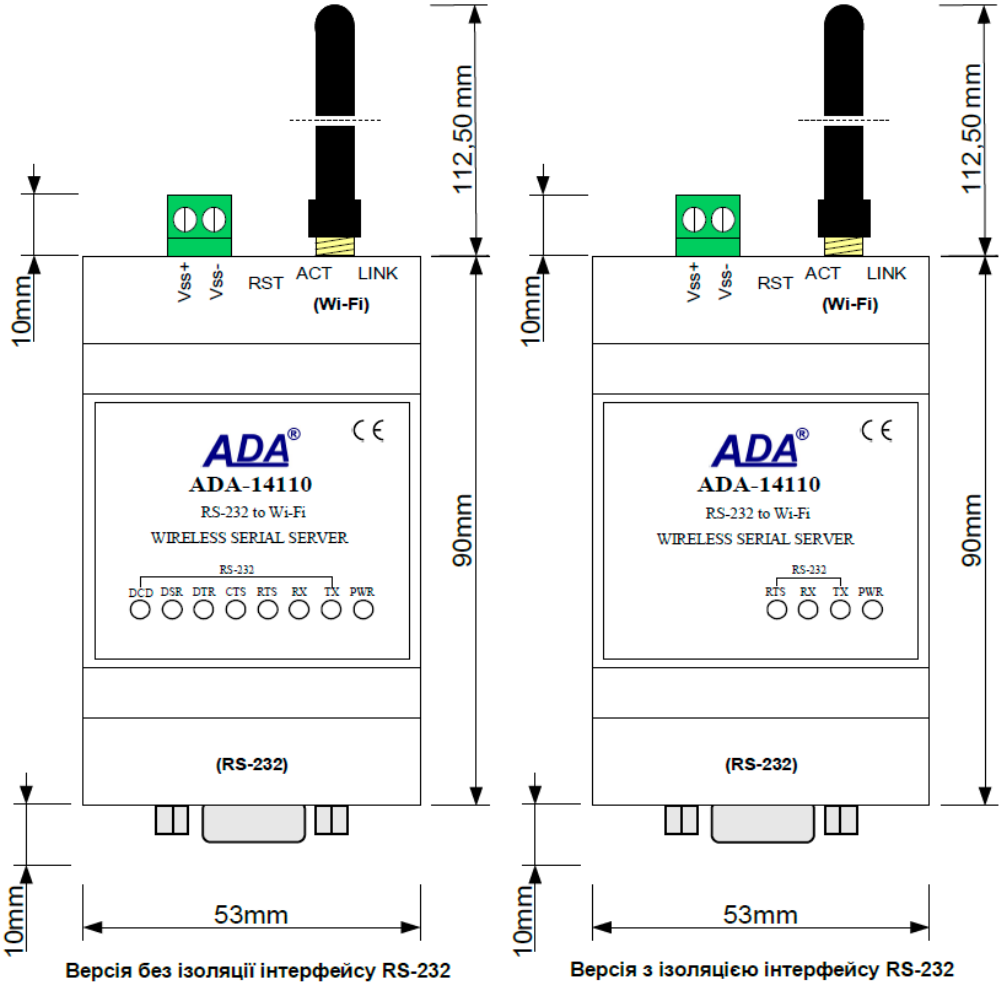


Рис.3.14. Вигляд модулю ADA-14110

Пристрій має стандартний роз'єм DB-9M (вилка) для інтерфейсу RS-232, гвинтову колодку для підключення живлення і SMA для антеної мережі Wi-Fi. Даний девайс пристосований для живлення зовнішнього джерела напруги в діапазоні від

10 до 30 (В) та потужністю до 4 (Вт). Сервер має захист від зворотного включення живлення та захист від КЗ напруги до 15 (кВ) та перенапруги на лініях інтерфейсу RS-232.

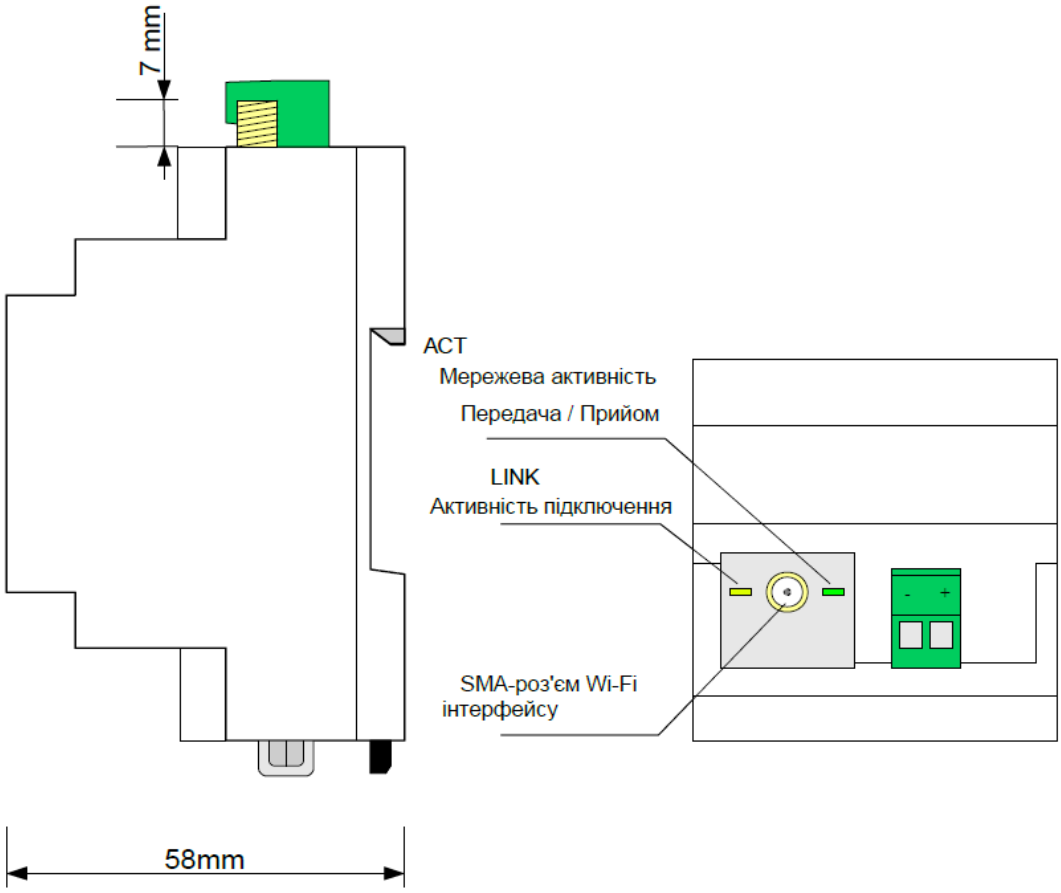


Рис.3.15. Вигляд роз’ємів Wi-Fi та живлення

Дальність передачі у бездротовій мережі Wi-Fi (IEEE 802.11b) є наступною:

- у будинках від 30 (м) до 150 (м),

- на відкритій місцевості до 300 (м),

-на відкритій місцевості при використанні додатково спрямованих антен, відстань покриття до 8 (км), де антени повинні бачити одна одну.

Дальність передачі може бути збільшена за рахунок застосування додатково направлених антен.

ADA-14110 продається з драйверами, які після встановлення створюють в операційній системі додатковий COM-порт, який ще називають - віртуальний. Його

можна використовувати, як стандартний COM-порт, але це не апаратний порт, а віртуальний, створений у системі Windows. Інколи це є причиною, чому деякі програми, що працюють у DOS і використовують цей порт, можуть працювати ненależним чином.

Налаштування Wi-Fi-адаптеру

Для початку перейдемо за адресою http://192.168.0.1, до сторінки налаштувань. Де потрібно вибрати протокол призначень DHCP, який в автоматичному режимі призначує пристроям цієї мережі різну IP-адресу, та знаючи адресу базової станції, потрібно вибрати пул IP-адрес, таким чином, щоб адреса БС попала в цей проміжок. Тому, ми обрали пул адрес від 192.168.255.100 до 192.168.255.200 з маскою мережі 255.255.255.0 [22].

Далі потрібно перевірити IP-адресу ноутбука у цій мережі, щоб DHCP не призначив адресу X.X.X.131, яка вже є зайнятою для БС. Але, також є можливість прописати вручну до роутера IP-адресу БС і призначити її, щоб уникнути проблем з автоматичним присвоєнням. Для цього потрібно додати пристрій, у нашому випадку базову станцію, до таблиці арендованих адрес і там, присвоїти адресу 192.168.255.131 до БС (рис 3.14).

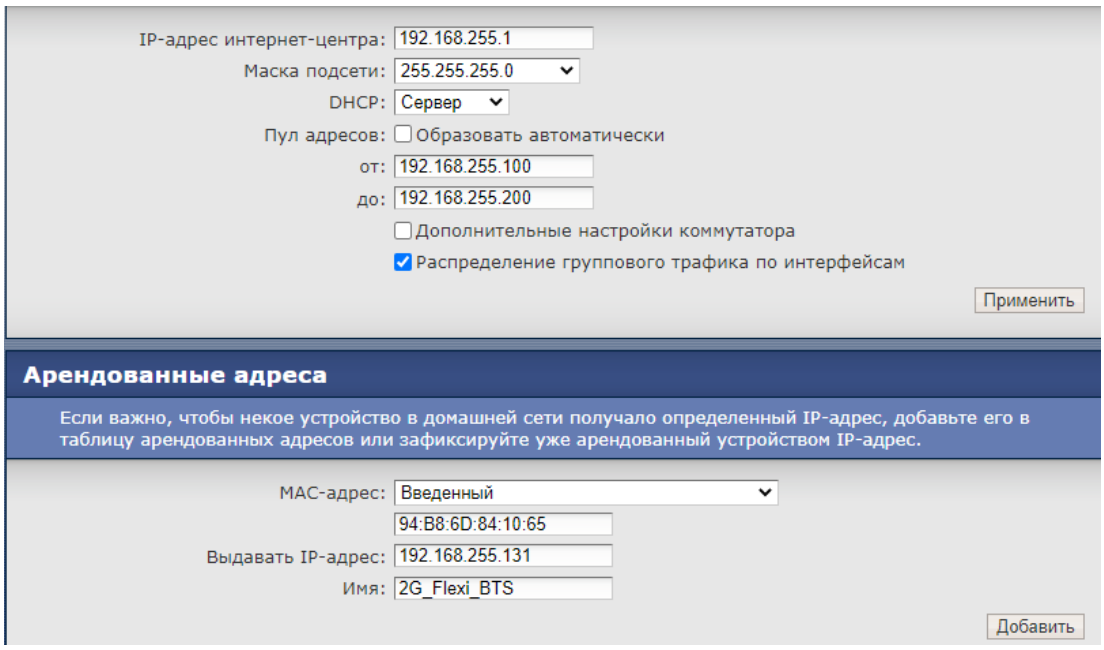


Рис 3.16 Налаштування Wi-Fi-модуля

Після всіх цих дій, можна перевірити доступність базової станції в даній мережі. Для цього потрібно пропінгувати IP-адресу БС (рис 3.17).

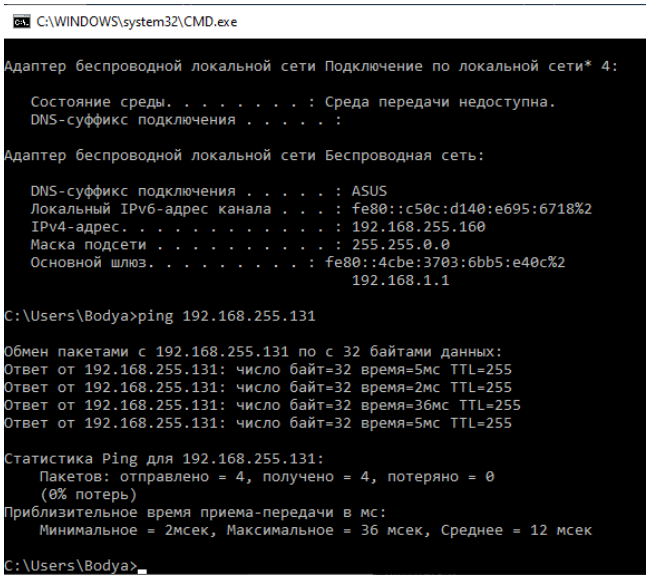


Рис 3.17 Перевірка доступності

Із рисунка 3.17 видно, що з’єднання є, й воно стабільне, але час затримки 2-36 (мс) трохи більший, ніж коли передача була безпосередньо через кабель. Знаючи, що ми тепер маємо стабільний бездротовий доступ до базової станції, ми можемо спробувати зайти через менеджер до налаштувань БС (рис 3.18).

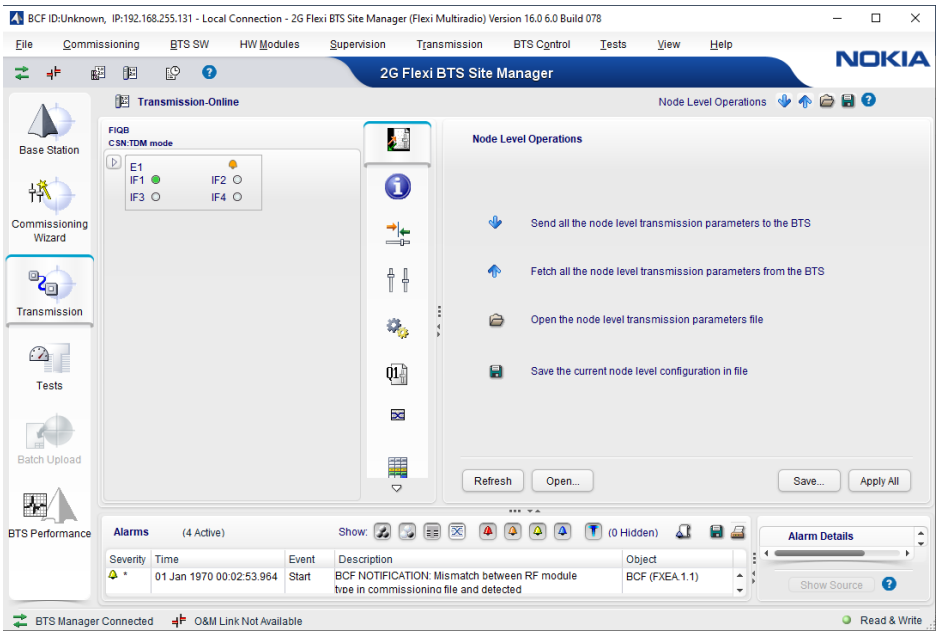


Рис 3.18 Успішне підключення за допомогою радіоканалу

З попереднього рисунку видно, що наш бездротовий канал зв’язку працює, а також ми маємо змогу проводити налаштування цієї базової станції на значній відстані від неї, та знаходитися в комфортних місцях, наприклад, взимку у теплій машині.

У наступному варіанті спробуємо підключитися до радіорелейної станції.

Рис. 3.19. Вікно налаштувань РРС

Майстер введення в експлуатацію визначає мінімальну кількість налаштувань, необхідних для мережного елемента.

Введення в експлуатацію – це процес введення в експлуатацію нововстановленого мережного елемента.

Він налаштовує систему для оперативного використання та визначає всі системні параметри, необхідні для основних функцій. При необхідності процес введення в експлуатацію може бути виконаний і раніше введеному в експлуатацію мережному елементі.

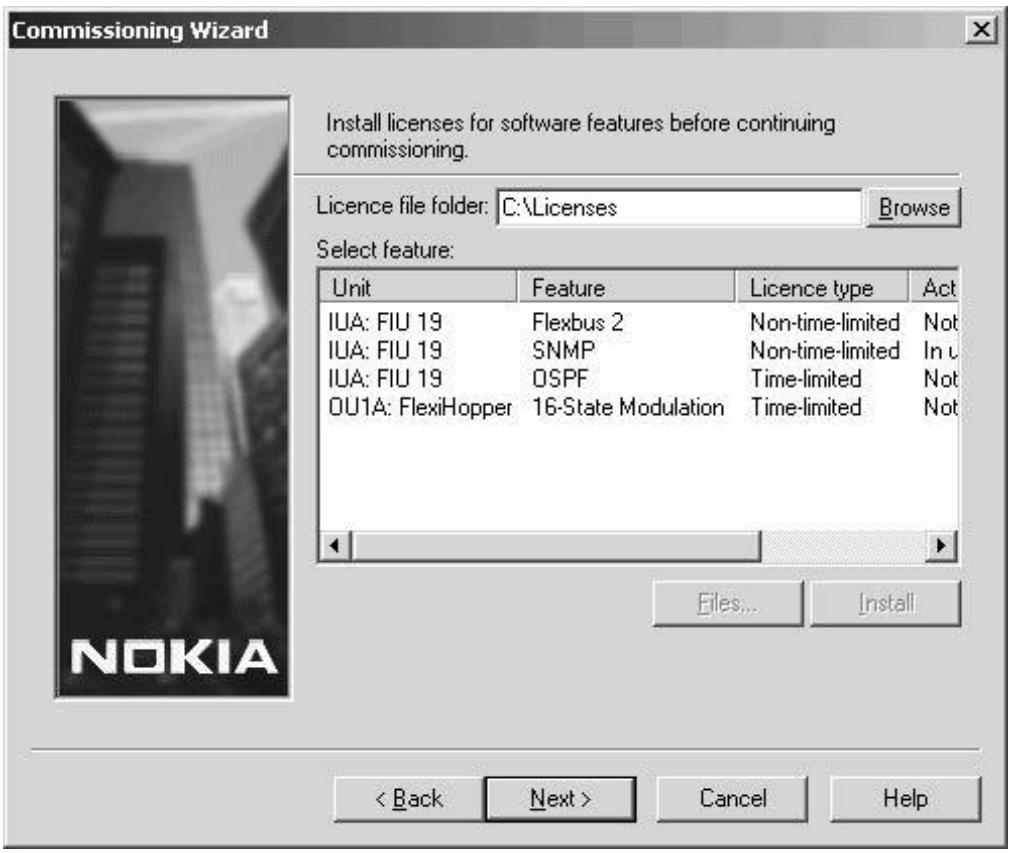


Рис. 3.20. Процес активування ліцензії

Ліцензія – це обмежене за часом право на використання програми, що надається вам на основні Ліцензійної угоди.

Ліцензія надає вам право на отримання описаних нижче видів послуг:

- Використання програми на одному або кількох пристроях. Кількість пристроїв, на яких ви можете використовувати програму, визначається згідно з умовами Ліцензійної угоди.
- Щоб працювати із програмою, ви маєте придбати ліцензію на її використання.
- Ліцензія має обмежений термін дії [24].

Наступною дією налаштуємо характеристики частоти, потужності і інших властивостей РРС:

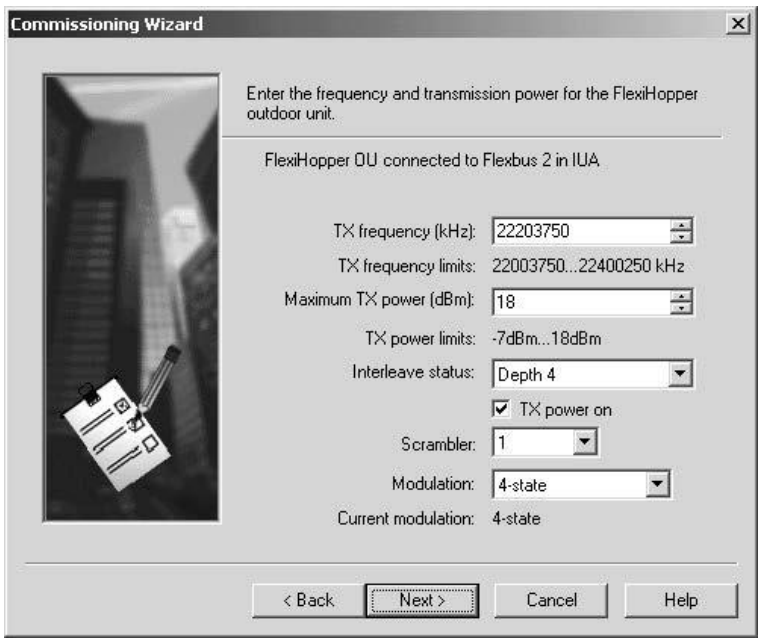


Рис.3.21. Налаштування зовнішніх блоків

Вибираємо значення із рекомендованих значень у технічній документації цього продукту “Product Description for Nokia FlexiHopper”.

Вибираємо тричі “Далі” (“Next”), після чого вводимо останні параметри мережі: IP-адресу, маску мережі та шлюз.

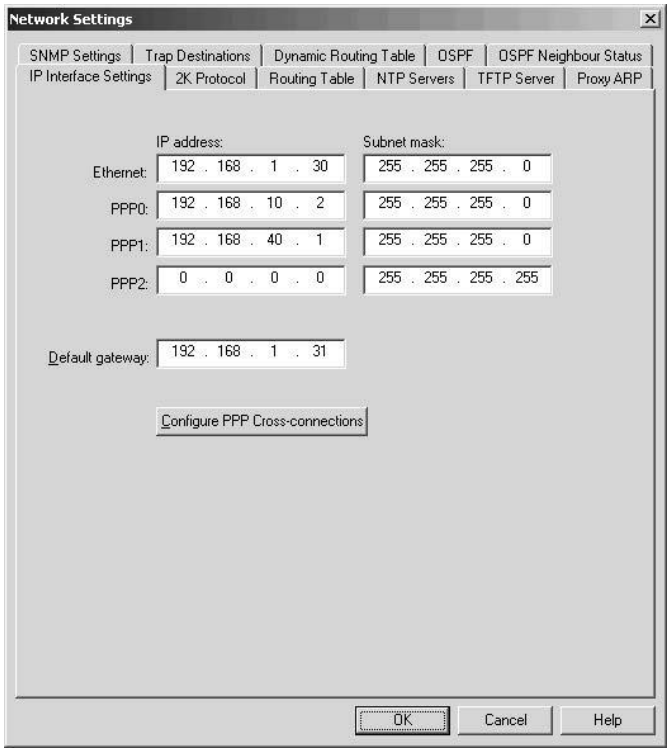


Рис 3.22 Мережеві налаштування БС

Після чого, наше налаштування радіорелейної станції- завершено. Тобто, наш пристрій працює вірно, без нарікань. Із чого можна зробити висновок, цілий ланцюг з підключень від ноутбука до БС та РРС- теж стабільний. Залишилось розрахувати дальність мережевого покриття Wi-Fi, а також, зробити дослідження щодо електромагнітної сумісності між станціями та адаптером Wi-Fi. Ці дії будуть проведені у наступному розділі 4.

ВИСНОВКИ ДО РОЗДІЛУ 3

У даному розділі була повністю вивчена бездротова мережа Wi-Fi та всі протоколи, що сприяють захисту. У результаті були проведені різні види атак, для отримання несанкціонованого доступу до мережі та подальшого впливу на мережу, також були вивчені способи забезпечення безпеки мережі. Але в під час аналізу нашої мережі, було вивчено те, що в цілому будь-яка бездротова мережа не може гарантувати 100% захищеність, тому що існуючі способи захисту вже застаріли, і для їхнього обходу не потрібні великі старання, а якщо брати сучасний новий протокол захисту, то він ще не доопрацьований, оскільки теж є вразливим до різних атак, тому є висновок, що бездротові мережі ще програють проводовим у захисті інформації. Завдяки цій роботі можна зрозуміти всі плюси та мінуси бездротових мереж, а також розібрати способи їх захисту, використовуючи стандартні інструменти, що є в будь-якому роутері. Головною перевагою цієї роботи є практичне виконання атаки при використанні пакету PMKID, так як ця атака була тільки теорією, в цій же роботі є практичне застосування цієї атаки, з використанням спеціальних параметрів для вже відомих інструментів, тим самим отримавши результат. У результаті була реалізована одна з найнебезпечніших атак на сьогоднішній день, вона актуальна як для старого WPA2, так і для нового нещодавно створеного WPA3, тим самим наражаючи на всі бездротові мережі небезпеки, оскільки для цієї атаки навіть не потрібні підключені клієнти, це багато в чому полегшує її реалізацію.

Також було проведено налаштування модуля-Wi-Fi, який служив транзитним пристроєм між базовою та радіорелейною станціями з ноутбуком. Відбулося тестування нашої мережі на всі варіанти атак та захисту від них. Результат підключення є вдалим, тобто, дистанційна діагностика БС пройшла успішно.

РОЗДІЛ 4
ОБЧИСЛЕННЯ ПАРАМЕТРІВ РАДІОВИПРОМІНЮВАННЯ

4.1. Розрахунок зони покриття Wi-Fi

Зона покриття - це радіус зони поширення точки підключення (Wi-Fi-модем). Тобто ми можемо підключитися до точки розподілу в тих зонах за допомогою пристроїв Wi-Fi.

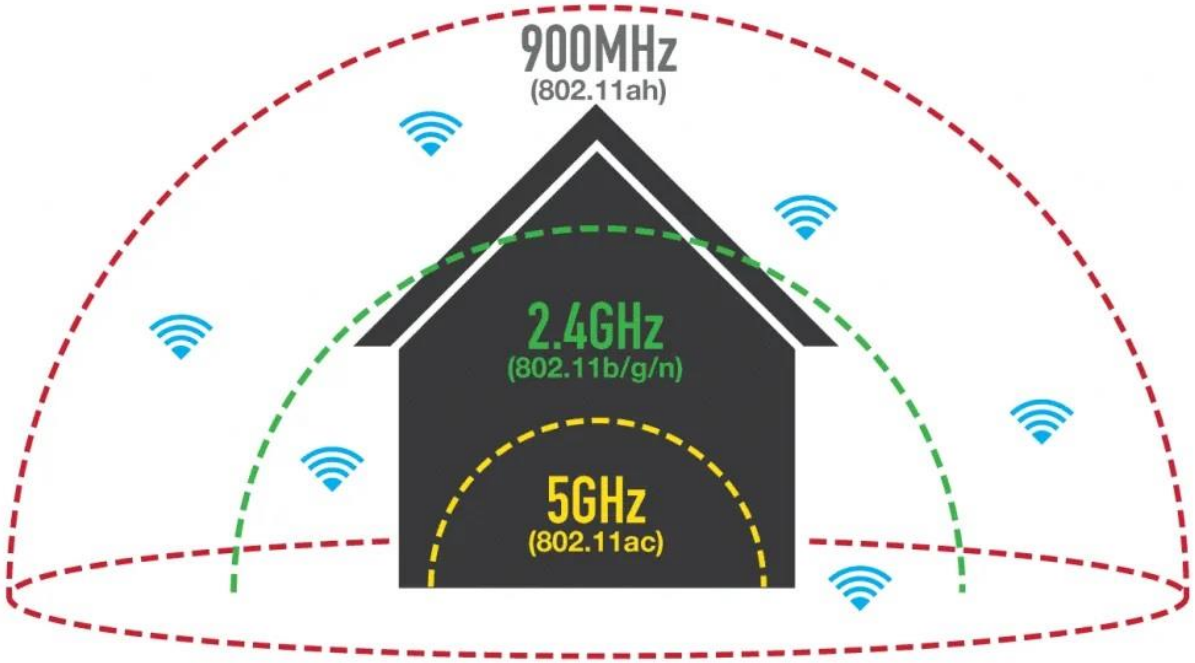


Рис. 4.1. Зони Wi-Fi-інтерфейсу

Як правило, виробник Wi-Fi пристроїв вказує зону постійної роботи Wi-Fi-радіостанції. Отже, передавач з потужністю 16-18 (дБ) має постійну зону роботи Wi-Fi пристроїв 200 (м), враховуючи це й враховуючи, що потужність сигналу пропорційна квадрату відстані, то ми можемо визначити потужність додаткового сигналу, який ми передаємо для кожної відстані:

$$\Delta P = 20(\mathrm{Log}_{10}L - 2{,}3)$$

де:

ΔP- це додаткова потужність, необхідна системі;

L - відстань між

$$\Delta P = 20(\mathrm{Log}1010 - 2{,}3) = 20\cdot(1\text{-}2{,}3) = \text{-}26 \text{ дБ}$$

Необхідну додаткову потужність ΔP можна отримати за допомогою антенного методу. У наявних у продажу антенах, як правило, позначення дається у вигляді dBi (коефіцієнт посилення відносно ізотропної антени), а нам потрібно змінити його на dBd (коефіцієнт посилення відносно дипольної антени).

$$dBd = dBi - 2{,}2$$

При використанні загальної антени, на посилення системи впливають такі фактори:

- Втрати в фідері;
- Коефіцієнт посилення передавальної антени;
- Коефіцієнт посилення приймальної антени;

Втрати всередині фідера (в структурі кабелю) можна визначити за такими характеристиками:

- Втрата в пікселі - 2dBm/m;
- Втрати в кабелі RJ-8U – 0,3 (дБм/в);
- Втрати в роз'ємі 1-2 (дБм/м).

Відповідно до міжнародних правил, неліцензійне використання Wi-Fi- може використовуватися лише на нижчих рівнях потужності, ніж ліцензований користувач.

Радіостанції Wi-Fi 802.11 мають потужність передачі 30-100 (мВт), тому ми використовуємо їх без ліцензії. Дозволена пікова потужність 1 (Вт) (30 дБм), антена оснащена коефіцієнтом посилення 6 (дБі). Тобто, якщо радіостанція не бере участі

в мостовому зв'язку, то її EIRP (ефективність відбиття ізотропної потужності) не повинна перевищувати 36 (дБі).

А для компонентів мосту є окреме правило, на кожні 3 (дБ) посилення антени вище 6 (дБі), потужність передавача повинна зменшуватися на 1 дБ.

Враховуючи вищезазначене, максимальний корисний радіус, коли він не працює як міст, можна знайти:

$$Lmax \approx 1230 \text{ (м)}$$

На радіус зони покриття Wi-Fi можуть впливати об’єкти в зоні передачі.

Ці предмети можуть відбивати або поглинати інфрачервоні хвилі (тканина, папір).

Розрахунок ефективності ізотропної потужності відбиття

Ефективність відбиття ізотропної потужності - це відношення потужності радіочастотного сигналу, спрямованого на антену, до абсолютного значення коефіцієнта посилення антени. Інтегральна характеристика «енергетики» радіостанції (радіопередавача, фідерного тракту, з’єднаного з антеною), повинна дорівнювати значенню потужності ізотропного тертя. Виходячи з того, що дані радіостанції створюють максимум, спрямований на антену діаграми, густина струму радіовипромінювання повинна дорівнювати густині струму потужності радіовипромінювання на однаковій відстані. Одиниця розрахункової потужності (Вт, дБВт, дБм).

ITS використовується як параметр у розрахунках радіомережі та електромагнітної сумісності (здебільшого використовується в супутниковому радіозв’язку та радіомовленні).

Визначаємо ефективність відбиття ізотропної потужності за формулою:

$$EIRP = РПРД - WАФТпрд + GПРД$$

де:

РПРД – вихідна потужність передавача, дБм;

WAФТпрд – втрати сигналу в розподілі AFT, дБ;

GПРД - посилення антени передавача, дБі.

Якщо звернути увагу на цю формулу, то згідно з формулою радіопередавач, оснащений спрямованою антеною малої потужності, може виконувати ту ж функцію, що і потужний радіопередавач, оснащений антеною слабкого направлення.

Таблиця 4.1

Параметри значень

Позначення	Визначення	Одиниці вимірювань	Значення
РПРД	вихідна потужність передавача	дБм	17
GПРД	посилення антени	дБи	12
WAФТпрд	сигнал передавача вимикається	дБ	7

Значення пристрою, необхідні для розрахунку, були взяті з веб-сайту пристрою.

Значення ККД ізотропної потужності відбиття знайдемо за формулою:

$$EIRP = 17 – 7 + 12 = 22 \text{ (дБм)}$$

Розрахунок зони дії сигналу

Цей метод дає можливість визначити теоретичну робочу відстань каналу бездротової мережі на базі пристрою Zyxel. Відстань між антенами, отримана за формулою, є максимальним отриманим теоретичним значенням. Враховуючи бар’єри, які впливають на бездротові мережі, неможливо отримати теоретичну відстань у межах міста.

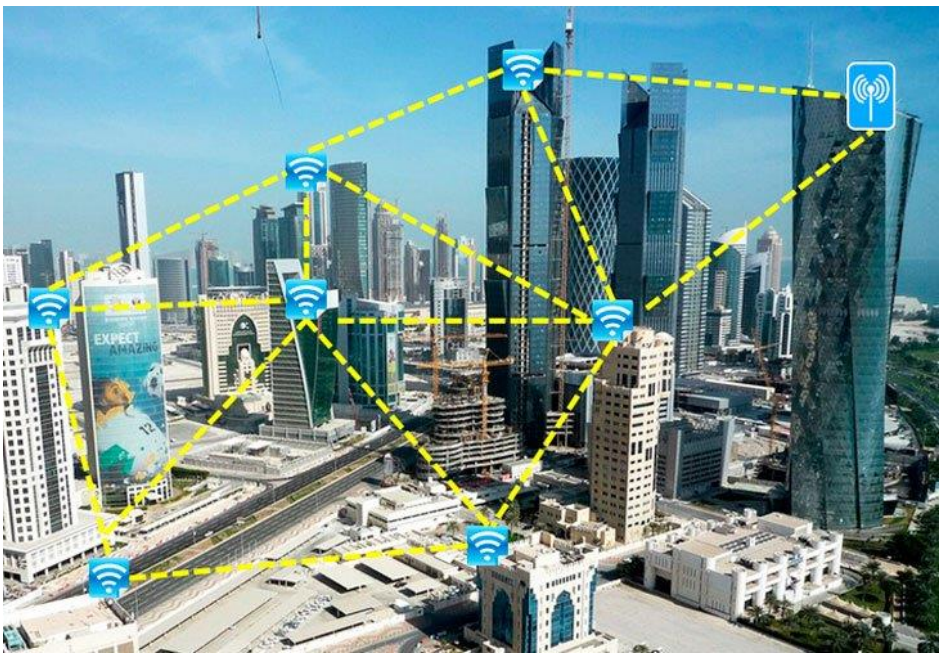


Рис. 4.2. Теоретичне Wi-Fi-покриття

Наведемо формулу для обчислення відстані. Ми отримуємо це з інженерної формули для розрахунку поглинання у вільному просторі:

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

де: FSL (free space loss) - гасіння на відкритій місцевості (дБ);

F - центральний частотний канал, в якому працює система мережі (МГц);

D — відстань між двома точками (км).

FSL визначається набором підсилення мережі. Він розраховується таким чином:

$$YдБ = Pt, дБмВт + Gt, дБи + Gr, дБи – Pmin, дБмВт – Lt, дБ – Lr, дБ,$$

де:

Pt, дБмВт - потужність передавача;

Gt, дБи – коефіцієнт підсилення передавальної антени;

Gr, дБи - коефіцієнт підсилення приймальної антени;

Pmin, дБмВт - чутливість приймача на даній швидкості;

Lt, дБ - втрати сигналу в коаксіальному кабелі, тракт передачі;

Lr, дБ - втрати сигналу в коаксіальному кабелі, тракт приймача.

Таблиця 4.2

Залежність чутливості приймача від швидкості

Ім'я	Точка підключення	Адаптер
Відповідний стандарт	IEEE 802.11a/b/g/n	IEEE 802.11a/b/g/n
Швидкість розповсюдження	300 Мбіт/с	300 Мбіт/с
Діапазон частот	2,4 – 2,4835 ГГц	2,4 – 2,4835 ГГц
Чутливість приймача	-82 дБ: MCS0/8 -79 дБ: MCS1/9 -77 дБ: MCS2/10 -74 дБ: MCS3/11 -71 дБ: MCS4/12 -66 дБ: MCS5/13 -65 дБ: MCS6/14 -63 дБ: MCS7/15	–79 дБ: MCS0/8 –76 дБ: MCS1/9 –74 дБ: MCS2/10 –71 дБ: MCS3/11 –67 дБ: MCS4/12 –63 дБ: MCS5/13 –62 дБ: MCS6/14 –61 дБ: MCS7/15
Потужність передавача	802.11n: 17 дБ	802.11n: 17 дБ

Для кожної швидкості приймач має певну чутливість. Для низьких швидкостей (наприклад, 1-2 мегабіт) чутливість: від -90 (дБмВт) до -94 (дБмВт). При великих значеннях швидкостей чутливість менше.

Залежно від марки радіомодуля максимальна чутливість може дещо відрізнятися. Відповідно, максимальна відстань різна для різних швидкостей.

FSL визначається за такою формулою:

$$FSL = Y_{дБ} – SOM,$$

де:

-SOM (System Operating Margin) - фонд енергії радіозв'язку (дБ).

Він враховує фактори, які негативно впливають на відстань підключення, наприклад:

- температурний дрейф чутливості приймача та вихідної потужності передавача;

- погодні ефекти: туман, сніг, дощ;

- неможливість узгодження антени, приймача, передавача з антенно-фідерним трактом;

Параметр SOM приймається рівним 10 (дБ). Запас посилення 10 (дБ) вважається достатнім для інженерних розрахунків.

Канал середньої частоти береться з таблиці 4.2

Таблиця 4.3

Визначення центральної частоти

Канал	Центральна частота (МГц)
1	2412
2	2417
3	2422
4	2427
5	2432
6	2437
7	2424
8	2447
9	2452
10	2457
11	2462
12	2467
13	2472
14	2484

На закінчення отримуємо формулу контактної відстані:

$$D = 10(FSL/20 – 33/20 – lgF)$$

Апаратне забезпечення Zyxel, що працює в спроектованій мережі, має теоретичну максимальну швидкість 300 (Мбіт/с), але швидкість змінюватиметься в залежності від середовища розробки, де є кілька підключених комп'ютерів. На певних швидкостях (MCS7/15 і MCS0/8) ми визначаємо відстань, між якою з'єднання є стабільним для точки з'єднання та адаптера.

Маємо наступні данні:

1 – Потужність передавача: 17 (дБмВт);

2 – Чутливість точки підключення на MCS7/15: -63 (дБмВт);

3 – Чутливість за точкою MCS0/8: -82 (дБмВт);

4 – Чутливість адаптера на MCS7/15: -61 (дБмВт);

5 – Чутливість адаптера на MCS0/8: -79 (дБмВт);

6 - Посилення антени точки доступу: 2 (дБі)

7 – Коефіцієнт посилення антени адаптера: 0 (дБі)

8 – Антена – немає втрат у фідерному тракті, тобто між бездротовою точкою та антенами.

Рішення задачі:

Визначаємо відстань на швидкості MCS 7/15. Параметр FSL дорівнює:

$$FSL = 17 + 2 + 0 – (-62) – 10 = 71 \text{ (дБ)};$$

Робочу відстань визначаємо за формулою:

$$D = 10(71/20 – 33/20 – lg2457) = 0.032 \text{ (км)}.$$

Визначаємо відстань при швидкості MCS 0/8. Параметр FSL дорівнює:

$$FSL = 17 + 2 + 0 – (-81) – 10 = 90 \text{ (дБ)};$$

Робочу відстань визначаємо за формулою:

$$D = 10(90/20 – 33/20 – lg2457) = 0.288 \text{ (км)}.$$

Ефективна площа антени

Основне призначення антени всередині приймального пристрою полягає в тому, щоб уловлювати частину потужності випромінювання, яка надходить у цю антену. Якщо форма антени більше довжини хвилі, то ефективна площа антени дорівнює її геометричній площі. Потужність, що подається від передавача на вхід приймача, дорівнює щільності енергії, що випромінюється на ефективну площу антени. Конструктивні особливості антени визначають значення коефіцієнта корисної дії та геометричної інтерференції.

Ефективна площа антени залежить від параметрів попереду та залежить від розмірів і об'єму антени. Ми можемо записати співвідношення між спрямованим рухом антени та її ефективною площею наступним чином:

$$G = 4 \cdot \pi \cdot Ae/\lambda 2 = 4 \cdot \pi \cdot f \cdot Ae/c2$$

де:

G - коефіцієнт спрямованого переміщення антени;

A_e – ефективна площа;

f - несуча частота;

c – швидкість світла (3*10^8 м/с);

λ – довжина хвилі несучої.

У таблиці 4.4 наведені значення посилення антени та ефективної площі для деяких популярних типів антен.

Таблиця 4.4

Коефіцієнт посилення і ефективна площа деяких типів антен

Тип антени	Ефективна подача A_e, м^2	Посилення потужності (відносно ізотропної антени)
Ізотропний	$\lambda^2 / 4\pi$	1
Нескінченно малий диполь	$1{,}5 \cdot \lambda^2 / 4\pi$	1,5
Напівхвильовий диполь	$1{,}64 \cdot \lambda^2 / 4\pi$	1,64
Рупорна антена,	$0{,}81 A_e$	$10\, A_e / \lambda^2$
Парабола зовнішньої A_e	$0{,}56 A_e$	$7\, A_e / \lambda^2$

У нашому випадку антена ізотропна, ефективна площа дорівнює $\lambda^2 /4\pi$, а коефіцієнт посилення по потужності дорівнює 1. Діапазон частот Wi-Fi пристроїв становить від 2400 до 2473 (МГц), відповідно, значення довжин хвиль знаходиться в межах від 12,12 до 12,49 (см).

$A = \lambda 2/4\pi = 0.1232/4 \cdot 3{,}14 = 0.0012$ м2

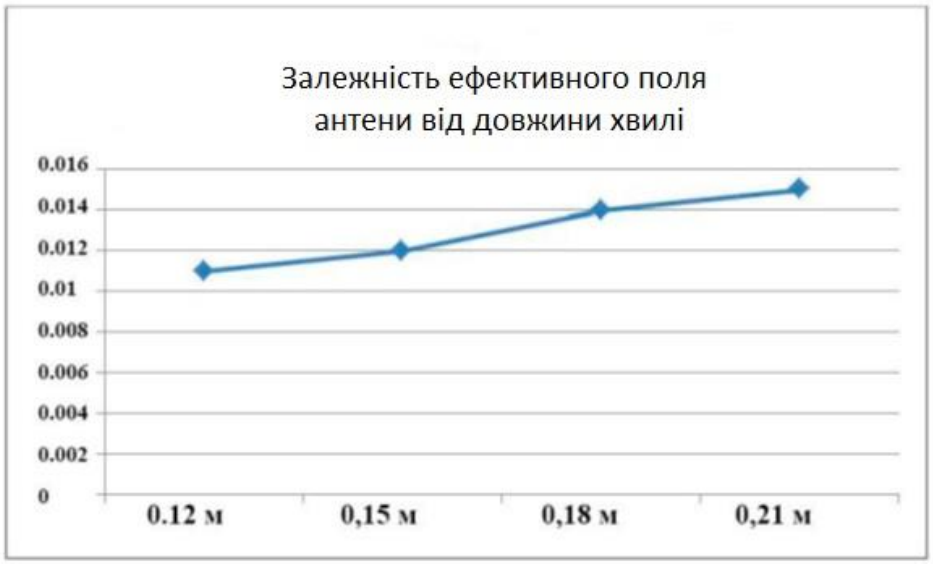


Рис. 4.3. Графік залежності ефективного поля антени від довжини хвилі

4.2. Дослідження електромагнітної сумісності

Задача цього дослідження- це виявити умови забезпечення електромагнітної сумісності (ЕМС) одночасно працюючих окремого джерела ненавмисної радіозавади зі звісною вихідною потужністю ***P*** та будь-якого радіоприймача зі звісним для нього захисним відношенням ***Q***.

Радіопередавальний пристрій (РПД) будемо розглядати як джерело непередбачених радіозавад, тоді радіоприймальний пристрій (РПП) – реципієнт завад, що характеризуються певними особливостями.

Занесемо загальну інформацію щодо приймачів у таблицю Ecxel:

а) Для станції, що заважає (передавальна станція):

- висота підняття антени над рівнем земної поверхні – 15 (м);
- коефіцієнт підсилення антени – 5 (дБ);
- тип поляризації антени – вертикальна;
- втрати у фідері антени – 2 (дБ);

б) Для станції, що піддана заваді (приймальна станція):

- чутливість – -125 (дБм);
- відношення сигнал/завада – 8 (дБ);
- висота підняття антени над рівнем земної поверхні – 15 (м);
- тип поляризації антени – вертикальна;
- коефіцієнт підсилення антени – 2 (дБ);
- втрати у фідері антени – 1 (дБ).

Всі інші поля залишаємо незмінними.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1		0	0,018	0,036	0,054	0,072	0,09	0,108	0,126	0,144	0,162	0,18	0,198	0,216	0,234	0,252	0,27	0,288
2	0 дБ 1	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99
3	-5 дБ 1	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99
4	-10 дБ 1	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99
5	-15 дБ 1	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99	99,99
6	-20 дБ 1	86,43136	86,43136	86,43136	86,42136	86,41136	86,38136	86,33137	86,26137	86,16138	86,0314	85,87141	85,68143	85,45145	85,21148	84,94151	84,65153	84,35156
7	-25 дБ 1	70,16298	70,16298	70,16298	70,15298	70,14299	70,12299	70,08299	70,023	69,93301	69,82302	69,68303	69,52305	69,33307	69,12309	68,89311	68,64314	68,39316
8	-30 дБ 1	56,33437	56,32437	56,32437	56,32437	56,31437	56,29437	56,25437	56,20438	56,13439	56,0444	55,92441	55,78442	55,62444	55,44446	55,25447	55,0445	54,82452
9	-35 дБ 1	44,67553	44,66553	44,66553	44,66553	44,65553	44,63554	44,61554	44,56554	44,50555	44,42556	44,32557	44,21558	44,07559	43,92561	43,76562	43,59564	43,41566
10	-40 дБ 1	34,94651	34,93651	34,93651	34,93651	34,92651	34,91651	34,89651	34,85651	34,80652	34,73653	34,65653	34,56654	34,45655	34,32657	34,19658	34,0466	33,89661
11	-45 дБ 1	26,91731	26,91731	26,91731	26,91731	26,90731	26,89731	26,87731	26,84732	26,80732	26,75732	26,68733	26,60734	26,51735	26,41736	26,30737	26,18738	26,06739
12																		
13																		
14																		
15																		
16																		
17																		
18																		
19																		
20																		
21																		
22																		
23																		

Рис.4.4 Параметри передавачів внесені до таблиці Excel

З отриманих результатів, будуємо графік частотно-територіального рознесення:

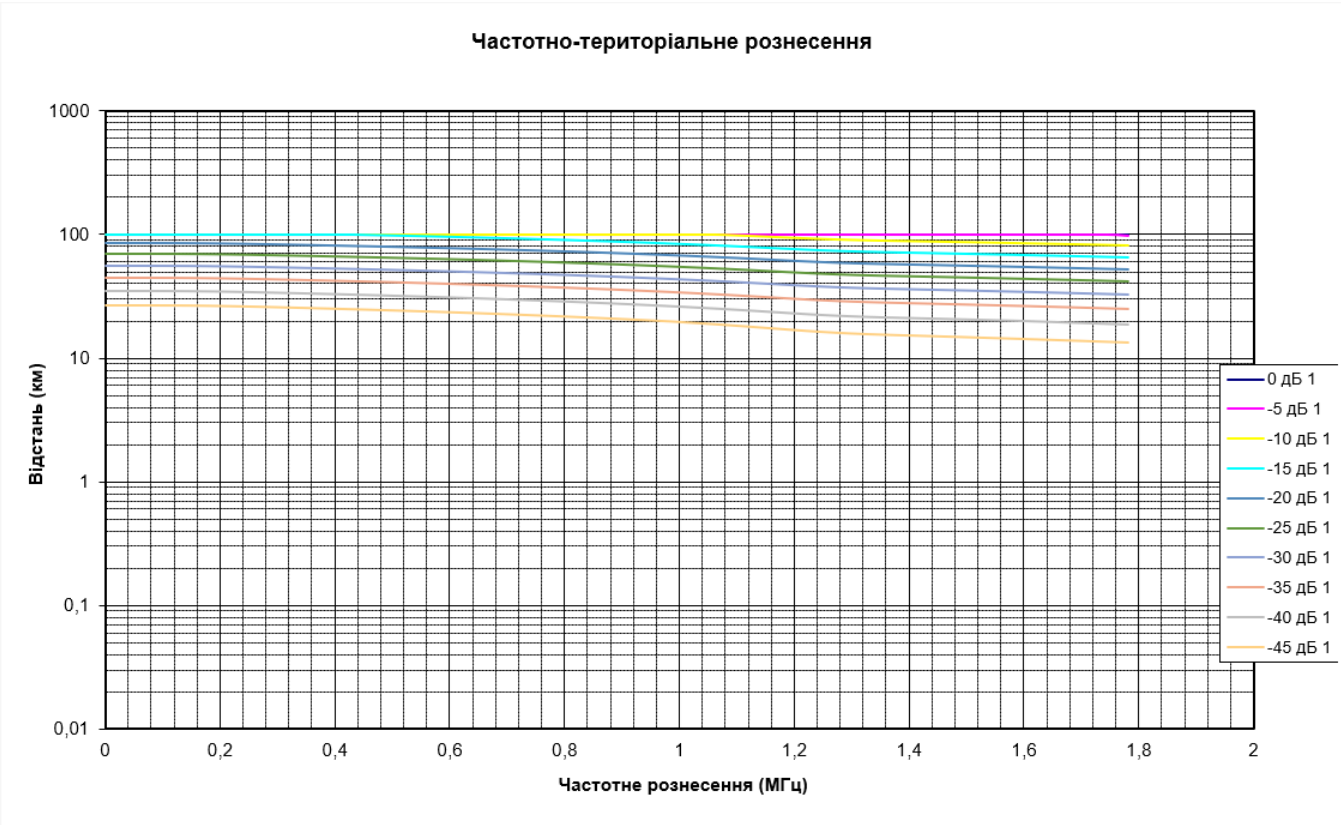


Рис.4.5. Розрахунок частотно-територіального рознесення

У діапазоні частот, які перевищують 30 МГц , або при довжинах хвиль $\lambda \leq 10$ (м) два незалежних радіоелектронних засобі (РЕЗ) можна вважати безумовно сумісними,

якщо відстань r_{ij} між антенами радіоприймального пристрою (РПП) *i*-ї радіоелектронної системи (РЕС) та радіопередавального пристрою (РПД) *j*-ї РЕС перевищує відстань прямої видимості (дальність радіогоризонту) R_{ij}, яка при нормальної тропосферної рефракції визначається звісним співвідношенням:

$$R_{ij} = 4{,}12\left(\sqrt{h_i} + \sqrt{h_j}\right), \text{ (км)},$$

де:

h – висоти підвісу антен відповідних РПП та РПД, (м).

Якщо $r_{ij} \le R_{ij}$, то електромагнітну сумісність (ЕМС) двох незалежних РЕЗ можна забезпечити на основі їх частотного або просторового рознесення, добиранням характеристик антен і потужностей РПД при наданих захисних відношеннях *Q* радіоприймачів, котрі належать відповідним РЕС. При розміщенні на обмеженій території $J \ge 2$ РЕС, кожен *i*-ї РПП опиняється під впливом випромінювань з боку $J - 1$ джерел ненавмисних радіозавад і проблема забезпечення ЕМС кожної *j*-ї РЕС в їх новому територіальному групуванні усугубляється. Тому є потреба у виявленні обмежень, які повинні накладатися на допустимі значення вихідних потужностей радіопередавачів деякої сукупності РЕС, розташованих на обмеженій території, з урахуванням значень об'єктивних незалежних факторів (природних та технічних). Ці фактори можуть впливати на якість електромагнітної обстановки (ЕМО) у точці нагляду.

Залишається перевірити передавач та приймач на парну сумісність.

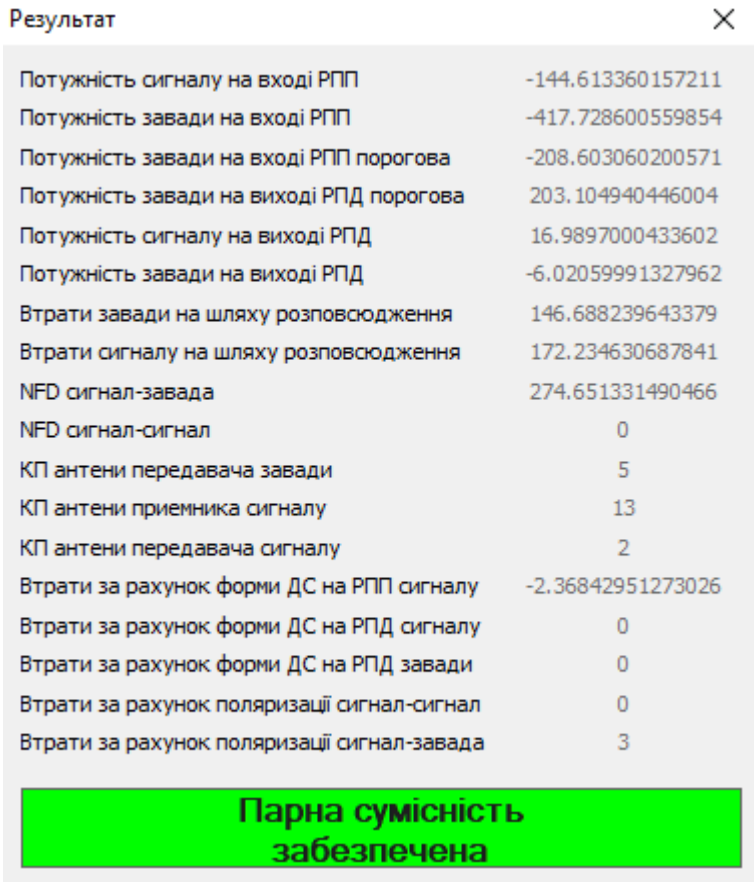


Рис.4.6. Результат сумісності передавачів

Як бачимо, з отриманих результатів, випливає наступне, парна електромагнітна сумісність забезпечена, тому Wi-Fi-модуль та радіорелейна станція можуть працювати й не заважати один одному.

ВИСНОВОК ДО РОЗДІЛУ 4

У цьому розділі дипломної роботи, було розраховано зону Wi-Fi-покриття, було записано декілька рівнів сигналів від відстані двох Wi-Fi-девайсів за допомогою яких, можна вирахувати загальну характеристику сигналів цього діапазону. Також, була розрахована й побудована залежність ефективного поля антени від її довжини. І під фінал роботи, було проаналізовано електромагнітну сумісність, побудовано графік частотно-територіального рознесення наших пристроїв, а також розраховано ЕМС модулю Wi-Fi й базової станції, сумісність була забезпечена на відмінно, без шкоди між пристроями.

РОЗДІЛ 5
ОХОРОНА ПРАЦІ

Питання охорони праці людини необхідно вирішувати на всіх стадіях трудового процесу незалежно від виду професійної діяльності.

Забезпечення безпечних і здорових умов праці в значній мірі залежить від правильної оцінки небезпечних, шкідливих виробничих факторів. Однакові по складності зміни в організмі людини можуть бути викликані різними причинами. Це можуть бути фактори виробничого середовища, надмірне фізичне і розумове навантаження, нервово-емоційна напруга, а також різне сполучення цих причин.

Саме тому суб'єктом охорони праці виступає програміст ІТ відділу авіапідприємства на стадії розробки ним програмного комплексу, призначеного для контролю мережевого ПЗ на наявність дефектів та збоїв, діагностики й ідентифікації дефектів працюючого мережевого устаткування за допомогою дослідження їхніх спектральних графіків сигналу.

Відділ інформаційних технологій, у якому працює програміст знаходиться в центральному корпусі авіакомпанії.

5.1. Аналіз небезпечних і шкідливих факторів, що впливають на програміста

Організація робочого місця програміста. Приміщення, в якому працює програміст, завдовжки 8 м та завширшки 5 м і має загальну площу 40 м^2, висоту стелі 3.5 м. У приміщенні знаходиться 6 робочих місця з ПК. Кожне робоче місце обладнане робочим столом площею 1.44 м^2, стільцем та персональним комп'ютером, що складається з монітора, системного блоку, клавіатури та миші. Згідно з [31] площа на одне робоче місце має становити не менше ніж 6,0 кв. м, а об'єм не менше ніж 20,0 куб. м., тобто площі та об'єму даного приміщення вистачає для розташування 6 робочих місць операторів ПК.

Чинники, які призводять до негайного погіршення здоров'я працівника, називаються небезпечними. Шкідливими чинниками виробничого середовища називаються такі

чинники, які безпосередньо або побічно призводять до порушення працездатності або здоров'я працюючих.

На програміста діють наступні шкідливі та небезпечні чинники, відповідно до [32]: мікроклімат, недостатнє освітлення робочого місця, статична електрика.

Мікроклімат робочої зони програміста. Робота програміста відноситься до категорії Іа, Іб - легких робіт, тому повинні дотримуватися наступні вимоги згідно [33]:

Таблиця 5.1

Оптимальні величини температури, відносної вологості та швидкості руху повітря в робочій зоні виробничих приміщень

Період Року	**Категорія Робіт**	**Температура повітря**	**Відносна вологість**	**Швидкість руху, м/сек.**
Холодний період року	Легка Іа	22 - 24	60 - 40	0,1
	Легка Іб	21 - 23	60 – 40	0,1
Теплий період року	Легка Іа	23 - 25	60 - 40	0,1
	Легка Іб	22 - 24	60 - 40	0,2

Виміряні за допомогою приладів (психрометр Августа) температура та вологість у ІТ відділі відповідають вказаним у таблиці для теплого періоду року. Розташовані у приміщенні 6 ПК являються джерелами тепловиділень, крім того для підтримання у приміщенні в холодний період року оптимальних параметрів мікроклімату використовуються нагріті поверхні опалювальної системи. Нормованим показником ІЧВ являється гранично допустима густина потоку енергії $I_{г.д}$, Вт/м^2, яка встановлюється в залежності від площі опромінюваної поверхні тіла людини ($S_{опр}$). Нормовані рівні складають: $I_{г.д}$ =35 Вт/м^2 при $S_{опр}$ > 50%; $I_{г.д}$=70 Вт/м^2 при $S_{опр}$ ~ 25-50%; $I_{г.д}$=100 Вт/м^2 при $S_{опр}$ < 25%

Природне та штучне освітлення. Нормованим параметром природного освітлення згідно [34] являється коефіцієнт природного освітлення (КПО). КПО

встановлюється в залежності від розряду виконуваних зорових робіт. Робота програміста відноситься до робіт середньої точності (IV розряд зорових робіт, мінімальний розмір об'єкту розрізнення складає 0,5-1,0 мм), для яких при використанні бокового освітлення КПО=1,5%. Для штучного освітлення нормованим параметром виступає $E_{мін}$ – мінімальний рівень освітленості, та $K_п$ – коефіцієнт пульсації світлового потоку, який не повинний бути більшим ніж 20%. Мінімальна освітленість встановлюється в залежності від розряду виконуваних зорових робіт. Для IV розряду зорових робіт вона складає 300-500 лк.

Виробничі випромінювання. Допустимі значення параметрів неіонізуючих електромагнітних випромінювань від монітору комп'ютера представлені в таблиці 5.2. Нормованим параметром невикористаного рентгенівського випромінювання виступає потужність експозиційної дози. На відстані 5 см від поверхні екрану монітору її рівень не повинен перевищувати 100 мкР/год. Максимальний рівень рентгенівського випромінювання на робочому місці програміста зазвичай не перевищує 20 мкР/год.

Таблиця 5.2

Допустимі значення параметрів неіонізуючих електромагнітних випромінювань

Найменування параметра	**Допустимі значення**
Напруженість електричної складової електромагнітного поля на відстані 50 см від поверхні монітора ПК	10 Вт/м
Напруженість магнітної складової електромагнітного поля на відстані 50 см від поверхні монітора ПК	0.3 А/м
Напруженість для операторів ПК не повинна перевищувати	20 кВ/м

На відстані 5-10 см від екрана і корпуса монітора рівні напруженості можуть досягати 6 В/м по електричній складовій, що не перевищує допустимі значення.

Електробезпека. Статична електрика. Приміщення ІТ відділу за небезпекою ураження електричним струмом можна віднести до 1 класу, тобто це приміщення без підвищеної небезпеки (сухе, без пилу, з нормальною температурою повітря, ізольованими підлогами і малим числом заземлених приладів).

На робочому місці програміста з всього устаткування металевим є лише корпус системного блоку комп'ютера, що відповідає стандарту фірми IBM. Згідно з [35]: пункт 5 «Заходи по захисту від статичної електрики», на системному блоці повинно встановлене заземлення для знешкодження статичної електрики. Після проведення огляду системного блоку було встановлено, що на ньому відсутнє заземлення, тобто не відповідає вищевказаним нормам.

Основні причини ураження людини електричним струмом на робочому місці:

– дотик до металевих неструмоведучих частин (корпусу комп'ютера), що можуть виявитися під напругою в результаті ушкодження ізоляції;

– нерегламентоване використання електричних приладів;

– відсутність інструктажу співробітників з правил електробезпеки.

5.2. Організаційні та конструктивно-технологічні заходи для зниження впливу шкідливих виробничих факторів.

Нормалізація повітря робочої зони. Для створення й автоматичної підтримки в ІТ відділі незалежно від зовнішніх умов оптимальних значень температури, вологості, чистоти і швидкості руху повітря, у холодний час року використовується водяне опалення, у теплий час року застосовується кондиціонування повітря [36].

Виробниче освітлення. Під час аналізу освітлення на робочому місті програміста було встановлено, що воно не відповідає встановленим нормам, тому для покращення умов праці рекомендуємо збільшити рівень загальної освітленості приміщення шляхом встановлення 5 додаткових світильників, щоб загальна кількість лам відповідала розрахованому вище значенню, а саме 36 світлодіодних ламп. Також для підтримки запроектованого освітлення у чистому виді необхідно скласти графік, де передбачити очищення віконних блоків і світильників не менше 2 разів на рік [34].

Електробезпека. Електробезпечність у приміщенні ІТ відділу пропоную забезпечити наступними технічними способами і засобами захисту:

– для зменшення накопичення статичної електрики застосовувати зволожувачі і нейтралізатори, антистатичне покриття підлоги;

– забезпечити приєднання металевих корпусів устаткування до жили, що заземлює. Заземлення корпуса ПК забезпечити підведенням жили, що заземлює, до розеток. Опір заземлення 4 Ом, згідно (ПУЭ) для електроустановок з напругою до 1000 В. А також організаційними заходами:

– своєчасне проведення інструктажів з техніки безпеки [37].

Ергономіка та організація робочого місця. Після проведення аналізу робочого місця програміста в ІТ Відділі було з'ясовано, що воно відповідає встановленим вимогам.

Виходячи з результатів аналізу важкості та напруженості праці пропоную скоротити час роботи за комп'ютером, робити перерви сумарний час яких повинен складати 50 хвилин при 8-ми годинному робочому дні [38].

5.2.1. Розрахунок освітленості робочого місця програміста ІТ відділу авіапідприємства на відповідність розряду зорової роботи

За даними вимірювань (люксметр Ю-116) рівень природної освітленості поверхні, де розташований ПК програміста, складає 200 лк при освітленості тієї же поверхні відкритим небосхилом в 20000 лк, тобто КПО = 1%, що не відповідає нормативному КПО.

Для штучного освітлення у приміщенні використовуються світлодіодні лампи Т8 G13, які в порівнянні з люмінесцентними та лампами розжарювання мають ряд істотних переваг: за спектральним складом світла вони близькі до природного світла; мають підвищену світлову віддачу (у 2-5 разів вищу, ніж у ламп розжарювання); мають триваліший термін служби (до 10 тис. годин) [34].

Розрахунок штучного освітлення проведемо для кімнати площею 40 м^2, ширина якої складає 5 м, довжина – 8 м, висота – 3.5 м за методом коефіцієнта використання світлового потоку.

Для визначення потрібної кількості світильників, які повинні забезпечити нормований рівень освітленості, визначимо світловий потік, що падає на робочу поверхню за формулою:

$$F=E*S*K*Z/n \quad (5.1)$$

(де **F** – світловий потік, що розраховується, Лм; **E** – нормована мінімальна освітленість, Лк; Е = 300 Лк; **S** – площа освітлюваного приміщення (у нашому випадку S=40 м^2); **Z** – відношення середньої освітленості до мінімальної (зазвичай приймається рівним 1,1...1,2, в нашому випадку Z=1,1); **K** – коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників в процесі експлуатації (його значення залежить від типу приміщення і характеру робіт, що проводяться в ньому, в нашому випадку К=1,5); **n** – коефіцієнт використання світлового потоку, (виражається відношенням світлового потоку, що падає на розрахункову поверхню, до сумарного потоку всіх ламп, і обчислюється в долях одиниці;) залежить від характеристик світильника, розмірів приміщення, забарвлення стін і стелі, що характеризуються коефіцієнтами відбиття від стін ($\rho_{ст.}$) і стелі ($\rho_{стелі}$), значення коефіцієнтів дорівнюють $\rho_{ст}$ = 40% і $\rho_{стелі}$=60%.

Обчислимо індекс приміщення за формулою:

$$i=S/h(A+B) \quad (5.2)$$

(де **S** – площа приміщення, S=40 м^2; **h** – розрахункова висота підвісу, h = 3.3 м; **A** – ширина приміщення, А = 5 м; **B** – довжина приміщення, В = 8 м.)

Підставивши значення отримаємо: **i=40/3.3(5+8)=0.93**. Знаючи індекс приміщення, знаходимо **n=0.22**. Підставимо всі значення у формулу для визначення світлового потоку **F**:

F=(300*1.5*40*1.1)/0.22=90000 Лм.

Для освітлення використані світлодіодні лампи з матовим покриттям типу LRC-T8-S1500G13-220-22,0W, світловий потік яких **$F_л$ = 2500** Лм.

$$N=F/F_л \quad (6.3)$$

(де **N** – визначуване число ламп; **F** – світловий потік, **F=90000 Лм**; **Fл** – світловий потік однієї лампи, **$F_л$ = 2500 Лм**.)

N=90000/2500=36

В приміщенні використовуються світильники типу ЛПО. Кожен світильник комплектується чотирма лампами. Тобто необхідно використовувати 9 світильників із 36 працюючими лампами в них.

У ІТ відділі авіапідприємства, де аналізувалось робоче місце програміста працює 5 світильників з 20 лампами в них, тому рівень штучного освітлення не задовольняє санітарним нормам.

5.3. Пожежна безпека

Приміщення ІТ відділу центрального офісу авіапідприємства по категорії вибухопожежної і пожежної небезпеки, згідно з [39] відноситься до категорії **Д** «Негорючі речовини та матеріали в холодному стані. Приміщення, в яких знаходяться ГР в системах машин, охолодження та гідроприводу устаткування, в яких не більше 60 кг в одиниці устаткування при тиску не більше 0.2 мПа, кабелі електропроводки до устаткування, окремі предмети меблів на місцях.»

Центральний офіс, у якому знаходиться ІТ відділ по пожежній небезпеці будівельних конструкцій відноситься до категорії **К1** (малопожежонебезпечні), оскільки тут присутні займисті (книги, документи, меблі, оргтехніка і т.д.) і важкогорючі речовини (сейфи, різне устаткування і т.д.), що при взаємодії з вогнем можуть горіти без вибуху.

По конструктивних характеристиках будинок можна віднести до будинків з несучими і огороджуючими конструкціями із природних або штучних кам'яних матеріалів, бетону або залізобетону, де для перекриттів допускається використання дерев'яних конструкцій, захищених штукатуркою або важкогорючими листовими, а також плитними матеріалами.

Отже, ступінь вогнестійкості будинку Центрального офісу можна визначити як третю (III).

Приміщення ІТ відділу авіапідприємства по функціональній пожежній небезпеці відноситься до класу **Ф 4.2**.

Причини виникнення пожежі. Пожежа в ІТ відділі, може привести до дуже несприятливих наслідків (загибель людей, втрата цінної інформації, псування майна і т.д.), тому необхідно: виявити й усунути всі причини виникнення пожежі; розробити план заходів для ліквідації пожежі в будинку; план евакуації людей з будинку.

Причинами виникнення пожежі можуть бути:

– несправності електропроводки, розеток і вимикачів які можуть привести до короткого замикання або пробою ізоляції;

– використання ушкоджених (несправних) електроприладів;

– використання в приміщенні електронагрівальних приладів з відкритими нагрівальними елементами;

– виникнення пожежі внаслідок влучення блискавки в будинок;

– загоряння будинку внаслідок зовнішніх впливів;

– неакуратне поводження з вогнем і недотримання мір пожежної безпеки.

Засоби пожежогасіння та пожежно-охоронної сигналізації. Відповідно до [39]: «3.3. На кожному підприємстві з урахуванням його пожежної небезпеки наказом (інструкцією) повинен бути встановлений відповідний протипожежний режим, у тому числі визначені: ... порядок організації експлуатації і обслуговування наявних технічних засобів протипожежного захисту (протипожежного водопроводу, насосних станцій, установок пожежної сигналізації, автоматичного пожежогасіння, димовидалення, вогнегасників тощо); ...». В приміщенні встановлено 1 переносний вуглекислотний вогнегасник типу ВВК-5, якого вистачить для приміщення даного типу та площі. Також на стелі встановлено 2 бездротових ІЧ датчики диму Страж М-501, які розраховані на площу 40 м^2.

У випадку виникнення пожежі спрацює протипожежна сигналізація, також необхідно відключити електроживлення, викликати за номером 101 пожежну команду, евакуювати людей із приміщення відповідно до плану евакуації, приведеному на Рисунку 5.1 і приступити до ліквідації пожежі вогнегасниками. При наявності невеликого вогнища полум'я, можна скористатися підручними засобами з метою припинення доступу повітря

до об'єкта загоряння.

Рис. 5.1 План евакуації з приміщення ІТ відділу компанії

5.4. Інструкція з охорони праці при роботі з персональним комп'ютером

Загальні вимоги до обладнання робочого місця з ПК.

- Робоче місце для працюючих з відео терміналами необхідно необхідно розташувати таким чином, щоб до поля зору працюючого не потрапляли вікна, освітлювальні прилади, поверхні які мають властивість віддзеркалювання. Поверхня робочого столу не повинна бути полірованою. Для попередження відблисків на екрані відео моніторів, особливо влітку та у сонячні дні, екран відео монітора слід розміщувати так, щоб світло від вікна падало збоку, бажано зліва.
- Екран відео монітору ПК повинен знаходитись від очей користувача (надалі оператора) на відстані не менше 500 – 700 мм. Кут зору в межах 10-40 градусів. Найбільш раціональним є розташування екрану перпендикулярно до лінії зору оператора.
- ПК повинен розташовуватися на відстані не ближче 1 метра від джерела тепла.

- Клавіатура повинна розміщуватися на поверхні столу або спеціальній підставці на відстані 100-300 мм від краю, повернутого до користувача. Кут нахилу панелі клавіатури до горизонтальної поверхні повинен бути в межах від 5 до 15 градусів.
- Висота робочої поверхні стола повинна бути в межах 680-800 мм.
- Крісло повинно забезпечувати операторові зручні умови праці та фізіологічну раціональну робочу позу в процесі праці. Крісло повинно забезпечувати можливість регулювання висоти поверхні сидіння, кут нахилу спинки та висоту спинки.
- Для захисту від прямих сонячних променів, які створюють відблиски на екрані відео монітора на вікнах повинні бути встановлені сонцезахисні пристрої. Екран відео монітора повинен розміщуватись так, щоб світло від вікна падало на робоче місце збоку, бажано зліва.
- Як джерело штучного освітлення в приміщеннях, де встановлено ПК, бажано використовувати люмінесцентні лампи. Можливе застосування ламп розжарювання в світильниках місцевого освітлення. Освітленість робочого місця у горизонтальній площині на висоті 0,8 м від рівня підлоги повинна бути не менш 400 лк. Вертикальна освітленість у площині екрану не більше 200 лк. Для зменшення напруженості зору необхідно забезпечити достатньо рівномірне розподілення яскравості робочої поверхні відео монітора та навколишнього простору.
- У приміщеннях для роботи ПК необхідно проводити щоденне вологе прибирання та регулярне провітрювання протягом робочого дня. Видалення пилу з екрану необхідно проводити не рідше 1 разу на день.
- Для захисту оператора від електромагнітних випромінювань і електростатичних полів, які створює відео монітор необхідно використовувати захисні екрани.
- Користувачам ПК слід носити одежу з природніх матеріалів або комбінованих природних і штучних волокон.

Вимоги безпеки перед початком роботи.

- Перед початком роботи працівник повинен зовнішнім оглядом перевірити цілісність корпусів системного блоку, відео монітора, принтера, клавіатури.

- Перевірити цілісність кабелів живлення, місць їх підключення (розеток електромережі, продовжувачів електромережі, розгалужувальних коробок, штепсельних вилок).
- Підготувати своє робоче місце, прибравши речі, які можуть заважати при виконанні роботи.
- Ввімкнути живлення ПК.
- У випадку, якщо після ввімкнення ПК не проходить загрузка або комп'ютер не виходить на робочий режим, працівник повинен повідомити керівника чи спеціаліста відділу інформаційних технологій.
- При виявленні ушкодження або яких-небудь інших недоліків повідомити безпосереднього керівника. Не приступати до роботи без його вказівки.

Вимоги безпеки під час роботи

- Необхідно стійко розташувати всі складові пристрої на столі, в тому числі і клавіатуру. Разом з тим повинна бути передбачена можливість переміщення клавіатури. ЇЇ розташування і кут нахилу повинні відповідати побажанням користувача ПК. Якщо в конструкції клавіатури не передбачений простір для опору долонь, то її слід розташовувати на відстані не менше 100 мм від краю столу в оптимальній зоні моніторного поля. При роботі на клавіатурі слід сидіти прямо, не напружуватись.
- Для зменшення несприятливого впливу на користувача пристроїв типу "миша" (вимушена поза, необхідність постійного контролю за якістю дій) слід забезпечити вільною більшу площу поверхні столу для переміщення "миші" і зручного упору ліктьового суглоба.
- Не припустимі сторонні розмови, роздратовуючи шуми тощо.
- Періодично при вимкнутому ПК слід видаляти злегка зволоженою мильним розчином хлопко-паперовою салфеткою пил з поверхонь апаратури. Екран і захисний екран протирають ватою, зволоженою спиртом.
- Не дозволяється використовувати рідинні або аерозольні засоби чистки поверхонь ПК.

Забороняється:

- самостійно ремонтувати апаратуру, в яких кінескоп та інші елементи можуть знаходитись під високою напругою (до 25 кВ0.)
- класти будь-які речі на апаратуру ПК, бутерброди та напої на клавіатуру або поруч з нею. Це може вивести її з ладу;
- затуляти вентиляційні отвори в апаратурі, це може призвести до її перегріву і виходу з ладу.

- Для зменшення негативного впливу на стан здоров'я працівників різних факторів ризику, пов'язаних з роботою на ПК, передбачаються додаткові регламентовані перерви для відпочинку користувачів ПК:
  - через кожний час безперервної роботи – 10 хвилин;
  - через кожні 2 години – 15 хвилин.
- При можливості слід чергувати зміну діяльності з іншою, не пов'язаною з роботою на ПК.
- З метою зменшення негативного впливу монотонності доцільно застосовувати чергування операцій введення тексту і введення даних (зміна змісту і темпу роботи) і т.п.
- При роботі на лазерних принтерах:
- Розташовувати принтер необхідно поряд з системним блоком так, щоб з'єднувальні шнури не були натягнуті. Забороняється ставити принтер на системний блок.
- Перш, ніж програмувати роботу принтера, впевніться, що він знаходиться в режимі зв'язку з системним блоком.
- Для досягнення високоякісного, чистого, з високою роздільною здатністю зображення щоб не зіпсувати апарат, потрібно використовувати папір, марка якого вказана в інструкції до принтера (найчастіше папір вагою 60-135 г/м^2, типу Canon або Xerox 4024).
- Обрізання країв паперу повинно бути виконаним гострим лезом ножа, без зазусенців – це зменшить вірогідність загинання паперу.
- При виконанні роботи (більше 20 хвилин), коли втручання користувача в роботу програми не потрібне, бажано вимикати живлення відео монітора.

- Для підтримки загального тонусу м’язів, профілактики кістково-м’язових порушень, зорового дискомфорту та інших несприятливих суб’єктивних почуттів під час регламентованих перерв необхідно виконувати комплекси рекомендованих вправ для очей, для хребта, для рук.
- Кількість мікро пауз до 1-2 хвилин слід визначити індивідуально. Форма та зміст перерв можуть бути різними виконання допоміжних робіт, не пов’язаних з роботою ПК , приймання їжі, виконання рекомендованих вправ.
- Виконання фізичних вправ протягом дня рекомендується індивідуально, залежно від почуття втоми. Гімнастика повинна біти на корекцію вимушеної пози покращення кровообігу, часткову компенсацію, дефіциту рухової активності.
- Про виявлені несправності (іскріння, пробоїв, запаху гару, ознак горіння тощо) негайно припинити роботу, відключити все обладнання від електромережі і терміново повідомити безпосереднього керівника або спеціаліста по ремонту ПК.

Вимоги безпеки при закінчення роботи на ПК.

- Закінчити і зберегти в пам’яті ПК файли, які знаходились у роботі. Виконати всі дії для коректного завершення роботи в оперативній системі.
- Вимкнути принтер та інші периферійні пристрої, вимкнути системний блок. При наявності пристрою безперебійного живлення (ПБЖ) вимкнути його живлення.
- Вимкнути ПК кнопкою «POWER” (ЖИВЛЕННЯ) та вийняти штепсельну вилку кабелю живлення з розетки
- Накрити клавіатуру кришкою для попередження попадання в неї пилу.
- Навести порядок на робочому місці.

Вимоги безпеки в аварійних ситуаціях.

- Якщо після ввімкнення ПК відчувається запах горілого або при доторканні до металевих частин ПК відчувається дія електричного струму, потрібно негайно відключити ПК від електромережі та повідомити про це своєму керівникові.

- У випадку виникнення пожежі негайно розпочати гасіння наявними засобами пожежогасіння і повідомити за телефоном 101 (міська пожежна охорона) та начальнику ДПД підприємства. Пам`ятайте, що загашувати електроустановки слід вуглекислотними вогнегасниками, сухим піском, щоб уникнути ураження електричним струмом.
- При отриманні травми припинити роботу, надати першу медичну допомогу, викликати швидку медичну допомогу за телефоном 103, при необхідності доставити в лікарняний заклад.
- Послідовність надання першої допомоги:
- Усунути вплив на організм небезпечних та шкідливих чинників, які погрожують здоров'ю та життю постраждалого (звільнити від впливу електричного струму, винести із зараженої атмосфери, погасити одяг, що горить, тощо);
- Визначити характер та тяжкість травми, найбільшу загрозу для життя постраждалого та заходів щодо його врятування;
- Виконати необхідні заходи щодо врятування постраждалого за порядком терміновості (відновити прохідність дихальних шляхів, провести штучне дихання, зовнішній масаж серця, зупинити кровотечу, іммобілізувати місце перелому, накласти пов»язку тощо);
- Підтримувати основні життєві функції постраждалого до прибуття медичного працівника;
- викликати швидку медичну допомогу або лікаря, або прийняти заходи для транспортування постраждалого у найближий лікарський заклад.
- Допомога постраждалому, яка надається не медичними працівниками, не повинна замінювати допомогу з боку медичного персоналу та повинна надаватися лише до прибуття лікаря.
- Конкретні дії щодо надання першої допомоги постраждалому при різних ураженнях описані в інструкції № 03-ОП «Про надання першої (долікарської) медичної допомоги при нещасних випадках», яка вивчається робітниками підприємства при проходженні первинного та послідуючих інструктажів з питань охорони праці.

- У разі виникнення інших аварійних ситуацій слід припинити роботу і повідомити про це керівника робіт.

У даному розділі розглянуті заходи, що виключають або що обмежують вплив на технічний персонал ІТ відділу небезпечних і шкідливих виробничих чинників. Зроблений розрахунок освітленості в робочій зоні. Ми отримали 9 світильників з 36 світлодіодними лампами, що є найкращим варіантом освітленості робочої зони та не порушує встановлених норм освітленості 300-500 лк. Було представлено інструкцію з охорони праці при роботі за персональним комп'ютером та рекомендації стосовно пожежної безпеки в ІТ відділі.

РОЗДІЛ 6
ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

6.1. Аналіз впливу техногенних чинників на навколишнє природне середовище

У результаті активної діяльності людини в середовищі існування воно поволі змінювало свій вигляд, що призвело до порушення біосфери і появи штучного середовища, яке називають техногенним (техносферою). За науковими даними, на сьогоднішній день майже все середовище, в якому перебуває людина, є техногенним. Штучно створена людиною техносфера охоплює практично всю планету і навіть вийшла за її межі у космос.

Техногенне середовище (техносфера) як складова навколишнього середовища є похідною діяльності людини, яка виникла як наслідок впливу антропогенних чинників.

Діючи у техногенному середовищі, людина безперервно виконує, як мінімум, два основних завдання:

- забезпечує своє комфортне перебування у середовищі проживання;
- створює та використовує системи захисту від впливу його негативних чинників.

Розрізняють прямий і непрямий вплив на навколишнє середовище та організм людини негативних чинників техносфери [41].

6.2. Принцип роботи базових станцій і стільникових пристроїв та їх негативний вплив на довкілля

У зв'язку зі стрімким зростанням числа технологій і приладів уникнути впливу ЕМП в сучасному світі практично неможливо.

Телефонні трубки і базові станції супроводу стільникового зв'язку є джерелами ЕМП в стільниковому зв'язку. Принцип дії цих джерел ЕМП на людину різний. Відмінною особливістю стільникового телефону, як джерела ЕМП є його максимальне наближення до голови користувача на відстань два-п'ять см в неконтрольованих умовах. Впливу ЕМП піддаються головний мозок, периферичні рецепторні зони вестибулярного, слухового аналізаторів, сітківка очей. Негативні дії випромінювання стільникового телефону піддаються також і оточуючі споживача люди, коли він розмовляє по телефону.

Електромагнітні поля базових станцій генеруються імпульсивно. Все залежить від часу доби, насиченості покриття базових станцій, кількості базових станцій в зоні. Саме базові станції покривають всю зону дії стільникового зв'язку техногенним електромагнітним полем. Так як базові станції розташовуються в місцях постійного перебування людини, то відбувається цілодобовий вплив на людину низькоінтенсивного електромагнітного поля радіочастотного діапазону.

За даними екологів і лікарів-гігієністів відомо, що всі діапазони електромагнітного випромінювання впливають на здоров'я і працездатність людей і мають серйозні наслідки. Вплив електромагнітних полів на людину в силу їх великої поширеності більш небезпечний, ніж радіація. Електричні поля промислової частоти оточують людину цілодобово, завдяки випромінюванню від електропроводки, освітлювальних засобів, побутових електроприладів, ліній електропередач тощо.

Енергетичне навантаження від електромагнітних випромінювань в промисловості і в побуті зростає постійно у зв'язку зі стрімким розширенням мережі джерел фізичних полів електромагнітної природи, а також із збільшенням їх потужностей. Людина не здатна фізично відчувати електромагнітне поле, проте воно викликає зменшення його адаптивних резервів, зниження імунітету, працездатності, під його впливом у людини розвивається синдром хронічної втоми, збільшується ризик захворювань. Особливо небезпечно дію електромагнітних випромінювань на дітей, підлітків, вагітних жінок та осіб з ослабленим здоров'ям.

Вплив електромагнітного поля на клітину. Електромагнітне поле впливає на заряджені частинки і струми, внаслідок чого енергія поля на рівні клітини перетворюється в інші види енергії.

Цитогенетичні дослідження (вихід хромосомних аберації) показали достовірне збільшення клітин з порушеннями в експериментальній групі в порівнянні з контролем. Збільшення хромосомних аберації було також виявлено при опроміненні ЕМП повітряно-сухого насіння і проростків салату. Цитогенетичний аналіз клітин крові корів з ферми показав підвищену кількість генетичних ушкоджень і випадків аномального гематопоезу [42].

Вплив електромагнітного поля на тканини. Слабкі електромагнітні поля при інтенсивності менше порогу теплового ефекту також впливають на зміни в живій тканині. Були проведені дослідження по біологічному впливу стільникового телефону, комп'ютерного блоку та інших електронних засобів. В ході цих досліджень було з'ясовано, що вплив цих джерел проявляється в погіршенні регенерації тканин.

Атоми і молекули в електричному полі поляризуються, полярні молекули орієнтуються у напрямку розповсюдження магнітного поля. Змінне електричне поле викликає нагрівання тканин живих організмів як за рахунок змінної поляризації діелектрика (сухожиль, хрящів, кісток), так і за рахунок появи струмів провідності.

Вплив електромагнітного поля на нервову систему. Перші експериментальні дослідження по впливу електромагнітного поля на нервову систему були проведені в СРСР. Було встановлено наявність прямої дії електромагнітного поля на мозок, мембрани нейронів, пам’ять, умовно-рефлекторну діяльність. У модельних експериментах показано можливість впливу слабких електромагнітних полів на процеси синтезу в нервових клітинах. Отримано виразні зміни імпульсації коркових нейронів, що призводять до порушення переданої інформації в більш складні структури мозку. Виявлено, що при дії електромагнітного поля у надвисокочастотному діапазоні може розвинутися порушення короткочасної пам’яті.

Вплив електромагнітного випромінювання на імунну систему. В даний час накопичено достатньо даних, що вказують на те, що при дії електромагнітного поля порушуються процеси імуногенезу. Встановлено, що під впливом електромагнітного

поля змінюється характер інфекційного процесу, виникають порушення білкового обміну, спостерігається зниження вмісту альбумінів і підвищення гамма-глобулінів в крові. Крім того, електромагнітне поле може виступати в якості алергену або пускового фактора, викликаючи важкі реакції у хворих алергіків при контакті з електромагнітним полем.

Вплив електромагнітного поля на статеву систему. Під впливом електромагнітного випромінювання знижується функція сперматогенезу, змінюється менструальний цикл, уповільнюється ембріональний розвиток, виникають вроджені каліцтва у новонароджених дітей і зменшення лактації у годуючих матерів.

Вплив електромагнітного поля на рослини. В результаті численних досліджень з'ясовано, що електромагнітні хвилі істотно впливають на біологічні об'єкти, які проявляються в різноманітті індукованих ефектів. Як слабкі, так і сильні ЕМП надають досить виражений вплив на морфологічні, фізіологічні, біохімічні та біофізичні характеристики багатьох рослин. Впливають на зростання, розвиток і розмноження рослинних об'єктів.

Теоретично рівні електричного поля, котрі реєструють поблизу повітряних ліній (ПЛ) достатні для пошкодження листя рослин. Проведені спостереження та експерименти по впливу ЕМП ліній електропередачі на рослини показали, що спостерігається зменшення сухої ваги надземної маси рослин вівса, соняшника зростаючих під ПЛ, в порівнянні з контролем. Відзначено негативний вплив ЕМП на величину потенційної нітрогенезної активності грунтової різосферної популяції, довжину проростків рослин.

Вплив слабких електромагнітних полів на живі організми. Слабкі електромагнітні поля при інтенсивності менше порога теплового ефекту також впливають на зміни у живій тканині. Дослідження біологічного впливу стільникового телефону, комп’ютерного блоку та інших електронних засобів проведені в ряді наукових центрів. При цьому шкідливість електронних засобів перевірялась як у робочому, так і у вимкненому стані, в тому числі і без засобів живлення [43].

Результати проведених досліджень з оцінки впливу стільникового телефону, комп’ютера та інших сучасних радіоелектронних засобів на різні організми як у робочому, так і у вимкненому стані виявилися невтішними і показали вкрай негативний їх вплив на стан біологічних об’єктів, яке проявлялось:

- у зниженні рухової активності і виживання мікроорганізмів;
- у збільшенні смертності мікроорганізмів;
- в погіршенні регенерації тканин;
- в порушенні ембріонального і личинкового розвитку;
- у зниженні біохімічних реакцій, порушення метаболізму;
- у зниженні енергетичного потенціалу у всіх життєво важливих системах організму.

6.3. Методи та засоби захисту навколишнього середовища від впливу техногенних чинників

Захист від електромагнітних випромінювань. Для зменшення впливу ЕМВ на персонал та населення, яке знаходиться у зоні дії радіоелектронних засобів, потрібно вжити ряд захисних заходів. До їх числа можуть входити організаційні, інженерно-технічні та лікарсько-профілактичні заходи.

Здійснення організаційних та інженерно-технічних заходів покладено передусім на органи санітарного нагляду. Разом з санітарними лабораторіями підприємств та установ, які використовують джерела електромагнітного випромінювання, вони повинні вживати заходи з гігієнічної оцінки нового будівництва та реконструкції об'єктів, котрі виробляють та використовують радіозасоби, а також нових технологічних процесів та обладнання з використанням ЕМП, проводити поточний санітарний нагляд за об'єктами, які використовують джерела випромінювання, здійснювати організаційно-методичні роботі з підготовки спеціалістів та інженерно-технічний нагляд [44].

Ще на стадії проектування повинно бути забезпечено таке взаємне розташування опромінюючих та опромінюваних об'єктів, яке б зводило до мінімуму інтенсивність опромінення. Оскільки повністю уникнути опромінення неможливо, потрібно зменшити ймовірність проникнення людей у зони з високою інтенсивністю ЕМП, скоротити час перебуванні під опроміненням.

Виключно важливе значення мають інженерно-технічні методи та засоби захисту: колективний (група будинків, район, населений пункт), локальний (окремі будівлі, приміщення) та індивідуальний. Колективний захист спирається на розрахунок поширення радіохвиль в умовах конкретного рельєфу місцевості. Економічно найдоцільніше використовувати природні екрани — складки місцевості, лісонасадження, нежитлові будівлі.

Встановивши антену на горі, можна зменшити інтенсивність поля, яке опромінює населений пункт у кілька разів. Аналогічний результат дає відповідна орієнтація діаграми спрямованості, особливо високоспрямованих антен, наприклад, шляхом збільшення висоти антени. Але висока антена складніша, дорожча, менш стійка. Крім того, ефективність такого захисту зменшується з відстанню.

При захисті від випромінювання екрана повинно враховуватись затухання хвилі при проходженні через екран (наприклад, через лісову смугу). Для екранування можна використовувати рослинність. Спеціальні екрани у вигляді відбивальних і радіо-поглинальних щитів дорогі, малоефективні й використовуються дуже рідко.

Локальний захист дуже ефективний і використовується часто. Він базується на використанні радіозахисних матеріалів, які забезпечують високе поглинання енергії випромінювання у матеріалі та віддзеркалення від його поверхні. Для екранування шляхом віддзеркалення використовують металеві листи та сітки з доброю провідністю. Захист приміщень від зовнішніх випромінювань можна здійснити завдяки обклеюванню стін металізованими шпалерами, захисту віком сітками, металізованими шторами [44].

Опромінення у такому приміщенні зводиться до мінімуму, але віддзеркалене від екранів випромінювання перепоширюється у просторі та потрапляє на інші об’єкти.

Для персоналу, яке обслуговує радіозасоби та перебуває на невеликій відстані потрібно забезпечити надійний захист шляхом екранування апаратури.

Поряд із віддзеркалюючими широко розповсюджені екрани з матеріалів, що поглинають випромінювання. Існує велика кількість радіопоглинальних матеріалів як однорідного складу, так і композиційних, які складаються з різнорідних діелектричних та магнітних речовин. З метою підвищення ефективності поглинаюча поверхня екрана виготовляється шорсткою, ребристою або у вигляді шипів. Радіопоглинаючі матеріали можуть використовуватися для захисту навколишнього середовища від ЕМП, яке генерується джерелом, що знаходиться в екранованому об'єкті.

Засоби індивідуального захисту використовують лише у тих випадках, коли інші захисні заходи неможливо застосувати або вони недостатньо ефективні: при переході через зони збільшеної інтенсивності випромінювання, при ремонтних та налагоджувальних роботах у аварійних ситуаціях, під час короткочасного контролю та при зміні інтенсивності опромінення. Такі засоби незручні в експлуатації, обмежують можливість виконання робочих операцій, погіршують гігієнічні умови.

Для захисту тіла використовується одяг із металізованих тканин та радіопоглинаючих матеріалів. Металізована тканина складається з бавовняних чи капронових ниток, спіральне обвитих металевим дротом, таким чином, ця тканина, мов металева сітка послаблює випромінювання не менш, як на 20-30 дБ. При зшиванні деталей захисного одягу потрібно забезпечити контакти ізольованих провідників. Тому електрогерметизація швів проводиться електропровідними розчинами чи клеями, які забезпечують гальванічний контакт або збільшують ємнісний зв'язок проводів, котрі не контактують.

Очі захищають спеціальними окулярами зі скла з нанесеною на внутрішній бік провідною плівкою двоокису олова. Гумова оправа окулярів має запресовану металеву сітку або обклеєна металізованою тканиною; цими окулярами випромінювання НВЧ послаблюється на 20-30 дБ.

Раніше використовували рукавички та бахіли, проте зараз вважають непотрібними, оскільки допустима величина щільності потоку енергії для рук та ніг у багато разів вища, ніж для тіла.

Колективні та індивідуальні засоби захисту можуть забезпечити тривалу безпечну роботу персоналу на радіооб'єктах [44].

Колективний та індивідуальний захист від шуму. Боротьба з шумом в джерелі його виникнення. Це найбільш дієвий спосіб боротьби з шумом. Створюються малошумні механічні передачі, розроблено способи зниження шуму в підшипникових вузлах, вентиляторах.

Зниження шуму звукопоглинанням. Об'єкт, котрий випромінює шум, розташовують у кожусі, внутрішні стінки якого покриваються звукопоглинальним матеріалом. Кожух повинен мати достатню звукопоглинальну здатність, не заважати обслуговуванню обладнання під час роботи, не псувати інтер'єр цеху. Різновидом цього методу є кабіна, в котрій розташовується найбільш шумний об'єкт і в котрій працює робітник. Кабіна зсередини вкрита звукопоглинальним матеріалом, щоб зменшити рівень шуму всередині кабіни, а не лише ізолювати джерело шуму від решти виробничого приміщення.

Зниження шуму звукоізоляцією. Суть цього методу полягає в тому, що шумовипромінювальний об'єкт або декілька найбільш шумних об'єктів розташовуються окремо, ізольовано від основного, менш шумного приміщення звукоізолювальною стіною або перегородкою. Звукоізоляція також досягається шляхом розташування найбільш шумного об'єкта в окремій кабіні. При цьому в ізольованому приміщенні і в кабіні рівень шуму не зменшиться, але шум впливатиме на менше число людей. Звукоізоляція досягається також шляхом розташування оператора в спеціальній кабіні, звідки він спостерігає та керує технологічним процесом. Звукоізоляційний ефект забезпечується також встановленням екранів та ковпаків. Вони захищають робоче місце і людину від безпосереднього впливу прямого звуку, однак не знижують шум в приміщенні.

Зниження шуму акустичною обробкою приміщення. Акустична обробка приміщення передбачає вкривання стелі та верхньої частини стін звукопоглинальним матеріалом. Внаслідок цього знижується інтенсивність відбитих звукових хвиль. Додатково до стелі можуть підвішуватись звукопоглинальні щити, конуси, куби, встанов-

люватись резонаторні екрани, тобто штучні поглиначі. Ефективність акустичної обробки приміщень залежить від звукопоглинальних властивостей застосовуваних матеріалів та конструкцій, особливостей їх розташування, об'єму приміщення, його геометрії, місць розташування джерел шуму. Ефект акустичної обробки більший в низьких приміщеннях (де висота стелі не перевищує 6 м) витягненої форми. Акустична обробка дозволяє знизити шум на 8 дБА [45].

Заходи щодо зниження шуму слід передбачати на стадії проектуванні промислових об'єктів та обладнання. Особливу увагу слід звертати винесенню шумного обладнання в окреме приміщення, що дозволить зменшити число працівників в умовах підвищеного рівня шуму та здійснити заходи щодо зниження шуму з мінімальними витратами коштів, обладнання та матеріалів. Зниження шуму можна досягти лише шляхом знешумлення всього обладнання з високим рівнем шуму.

Роботу щодо знешумлення діючого виробничого обладнану в приміщенні розпочинають зі складання шумових карт та спектрів шуму обладнання і виробничих приміщень, на підставі котрих виноситься рішення щодо напрямку роботи.

ВИСНОВОК ДО РОЗДІЛУ 6

Інтенсивний розвиток електроніки та радіотехніки викликав забруднення природного середовища електромагнітними випромінюваннями (полями). Головними їхніми джерелами є радіо-, телевізійні і радіолокаційні станції. Поблизу кожного обласного центру, багатьох районних центрів, великих міст розташовані телевізійні центри або ретранслятори, радіоцентри, засоби радіозв´язку різного призначення.

Для зменшення впливу електромагнітних полів на персонал, який знаходиться у зоні дії деяких радіоелектронних засобів необхідним є ряд захисних заходів: організаційні, інженерно-технічні та лікувально-профілактичні.

Існують розроблені на основі медико-біологічних досліджень санітарні норми та правила щодо радіотехнічних і електротехнічних об´єктів. Вони регламентують умови їхньої експлуатації з метою охорони населення від шкідливого впливу електромагнітних випромінювань.

Отже, на етапі проектування взаємне розміщення об’єктів має бути забезпечено таким чином, щоб інтенсивність опромінення була мінімальною. Також треба заздалегідь попіклуватися про зменшення часу перебування персоналу у зоні опромінення. Потужність джерел випромінювання повинна бути найменшою з можливих. Крім того треба вимагати від керуючих органів дотримування державних стандартів України та не порушувати їх норм.

ВИСНОВКИ

Інтернет-мережі повинні розвиватися, щоб стати персоналізованими, під чим мається на увазі, задовольнити різноманітні потреби кожного користувача, будь то людина або розумна річ. Майбутні мережі будуть виглядати, як програмовані платформи, які пропонують не тільки передачу голосу і даних, але й підтримують різні цілі використання, послуг і додатків. Другими словами, одна і та ж фізична інфраструктура буде використовуватися одночасно для різних мережевих сценаріїв.

У першому розділі були розглянуті системи UMTS, детально наведена структура базової станції 3G-4G, був зроблений загальний опис роботи основних елементів БС, а також було проведено аналіз роботи системи стільникового зв'язку. Була піднята проблематика зон обслуговування системи стільникового зв'язку, складено плани мережі, що спрощують налаштування, а також наведена логічна топологія. Було описано і показано всі процеси, які зазвичай проходять від абонента до базової станції та навпаки.

У другому розділі було розглянуто регламентно-планові технічні роботи з обслуговування базової й радіорелейної станцій. Даний процес розписаний покроково з рекомендацій до обслуговування й діагностики майбутніх проблем. Була наведена залежність та важність цих дій від надійності подальшого використання. А також, більш детально описано принцип роботи кожного з модулів та елементів БС.

У третьому розділі була повністю вивчена бездротова мережа Wi-Fi та всі протоколи, що сприяють захисту. У результаті були проведені різні види атак, для отримання несанкціонованого доступу до мережі та подальшого впливу на мережу, також були вивчені способи забезпечення безпеки мережі. Але в під час аналізу нашої мережі, було вивчено те, що в цілому будь-яка бездротова мережа не може гарантувати 100% захищеність, тому що існуючі способи захисту вже застаріли, і для їхнього обходу не потрібні великі старання, а якщо брати сучасний новий протокол захисту, то він ще не доопрацьований, оскільки теж є вразливим до різних атак, тому є висновок, що бездротові мережі ще програють проводовим у захисті інформації. Завдяки цій роботі можна зрозуміти всі плюси та мінуси бездротових

мереж, а також розібрати способи їх захисту, використовуючи стандартні інструменти, що є в будь-якому роутері. Головною перевагою цієї роботи є практичне виконання атаки при використанні пакету PMKID, так як ця атака була тільки теорією, в цій же роботі є практичне застосування цієї атаки, з використанням спеціальних параметрів для вже відомих інструментів, тим самим отримавши результат. У результаті була реалізована одна з найнебезпечніших атак на сьогоднішній день, вона актуальна як для старого WPA2, так і для нового нещодавно створеного WPA3, тим самим наражаючи на всі бездротові мережі небезпеки, оскільки для цієї атаки навіть не потрібні підключені клієнти, це багато в чому полегшує її реалізацію.

Також було проведено налаштування модуля-Wi-Fi, який служив транзитним пристроєм між базовою та радіорелейною станціями з ноутбуком. Відбулося тестування нашої мережі на всі варіанти атак та захисту від них. Результат підключення є вдалим, тобто, дистанційна діагностика БС пройшла успішно.

У четвертому розділі дипломної роботи, було розраховано зону Wi-Fi-покриття, було записано декілька рівнів сигналів від відстані двох Wi-Fi-девайсів за допомогою яких, можна вирахувати загальну характеристику сигналів цього діапазону. Також, була розрахована й побудована залежність ефективного поля антени від її довжини. І під фінал роботи, було проаналізовано електромагнітну сумісність, побудовано графік частотно-територіального рознесення наших пристроїв, а також розраховано ЕМС модулю Wi-Fi й базової станції, сумісність була забезпечена на відмінно, без шкоди між пристроями.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. B. Volochiy, L. Ozirkovskyy and I Kulyk, Designing effective strategies of maintenance. Mathematical models algorithms and techniques, Germany:LAP LAMBERT Academic Publishing, pp. 160, 2015.
2. D.J. Smith, Reliability Maintainability and Risk: Practical Methods for Engineers, Butterworth-Heinemann, pp. 515, 2021.
3. E.C. Ubani and I.C. Nwakanma, "Effectiveness of Maintenance Policies for Cellular System Infrastructure Project", International Journal of Scientific Engineering and Technology, no. 2, pp. 953-960.
4. V.A. Kashtanov and A.I. Medvedev, "Reliability theory of complex systems (Theory and Practice)", Moscow: “European Center for Quality, pp. 470, 2002.
5. E Markova, Y Satin, I Kochetkova, A Zeifman and A. Sinitcina, "Queuing System with Unreliable Servers and Inhomogeneous Intensities for Analyzing the Impact of Non-Stationarity to Performance Measures of Wireless Network under Licensed Shared Access", Mathematics, vol. 8, no. 5, pp. 800, 2020.
6. Amit Kumar and Mangey Ram, The Handbook of Reliability Maintenance and System Safety through Mathematical Modeling, Academic Press, pp. 520, 2021.
7. B. Volochiy, L. Ozirkovskyy, O. Mulyak and S. Volochiy, "Safety estimation of critical NPP I&C systems via state space method", Proceedings of 2nd International Symposium on Stochastic Models in Reliability Engineering Life Science and Operations Management SMRLO 2016, pp. 347-356, 2016.
8. N. Bartolini, "Handoff and Optimal Channel Assignment in Wireless Networks", Mobile Networks and Applications, vol. 6, no. 6, pp. 511-524, 2001.
9. Xie Lang and E Poul, "Heegaard Yuming Jiang Survivability Analysis of Infrastructure-based Wireless Networks", Computer Networks, vol. 128, pp. 28-40, 2017.
10. Yu. Bobalo, B. Volochiy, O. Lozinsky, B. Mandziy, L. Ozirkovskyy, D. Fedasyuk, et al., "Mathematical Models and Methods for Reliability Analysis of Radio Electronic and Software Systems", Lviv Polytechnic National University, pp. 300, 2013.

11. B. Volochiy, B. Mandziy and L. Ozirkovskyy, "Extending The Features of Software For Reliability Analysis of Fault-tolerant Systems", Computational Problems of Electrical Engineering Lviv Politechnic National University, vol. 2, no. 1, pp. 113-121, 2012.

12. S. Volochiy, D. Fedasyuk and R. Chopey, "Formalized development of the state transition graphs using the Erlang phase method", Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications IDAACS 2017, vol. 2, pp. 1098-1101, 2017.

13. D. Fedasyuk and S. Volochiy, "Method of developing the behavior models in form of states diagram for complex information systems", Proceedings of the International Conference on Computer Sciences and Information Technologies CSIT 2015, pp. 5-8, 2015.

14. K. Heimer and E. Brewer, "The Village Base Station", ACM Workshop on Networked Systems for Developing Regions (NSDR), 2010.

15. "Alternative and Sustainable Power for Nigerian GSM/Mobile Base Stations", Infinite Focus Group, 2010.

16. M. H. Alsharif and R. Nordin, "Evolution towards Fifth Generation (5G) Wireless Networks: Current Trends and Challenges in the Deployment of Millimetre Wave Massive MIMO and Small cells", Telecommun. Syst., vol. 64, pp. 617-637, 2016.

17. "Korea Communication Market Data", Netmanias Report, 2015.

18. "LTE Success Story in Korea", Netmanias Report, 2016.

19. Z. Hasan, H. Boostanimehr and V. K. Bhargava, "Green Cellular Networks: A Survey Some Research Issues and Challenges", IEEE Commun. Surv. Tutor., vol. 13, pp. 524-540, 2011.

20. J. Wu, Y. Zhang, M. Zukerman and E. Yung, "Energy-Efficient Base Stations Sleep Mode Techniques in Green Cellular Networks: A Survey", IEEE Commun. Surv. Tutor., vol. 17, pp. 803-826, 2015.

21. D. Feng, C. Jiang, G. Lim, L. J. Cimini, G. Feng and G. Y. Li, "A survey of energy-efficient wireless communications", IEEE Commun. Surv. Tutor, vol. 15, pp. 167-178, 2013.

22. E. Oh, B. Krishnamachari, X. Liu and Z. Niu, "Toward dynamic energy-efficient operation of cellular network infrastructure", IEEE Commun. Mag., vol. 49, pp. 56-61, 2011.

23. "Energy Sources: Solar", Department of Energy, April 2011. Aoaba, A. Amoo and A. Yusuf, "Power management scheme for wireless telephony service providers", Continental Engineering Sciences, vol. 3, pp. 72-79, 2008.

24. Beibei Wang et al., "Green Wireless Communication: A Time – Reversal Paradigm", IEEE journal on Selected Areas in Communications, vol. 29, no. 8, pp. 1698-1709, September 2011.

25. Mohammed H. Alsharif et al., "Survey of Green Radio Communication Networks: Techniques and Recent Advances", Journal of Computer Networks and Communications, December 2013.

26. Julien De Rosny, Geoffroy Lerosey and Mathias Fink, "Theory of Electromagnetic Time-Reversal Mirrors", IEEE TransactionsonAntennas and Propogation, vol. 58, no. 10, pp. 3139-3149, October 2010.

27. George C. Alexandropoulos et al., "Indoor Time Reversal Wireless Communication:Experimental Results for Localization and Signal Coverage", International Conference on Acoustics Speech and Signal Processing (ICASSP), pp. 7844-7848, April 2019.

28. C. Prada et al., "The iterative Time Reversal Mirror:A Solution to self Focusing in the Pulse Echo Mode", The Journal of the Acoustical Society of America, vol. 99, pp. 1119-11129, 1991.

29. D. Rouseff et al., "Underwater Acoustic Communication by Passive –Phase Conugation: Theory and Experimental results", ÏEEE Journal of Ocean Engg., vol. 26, pp. 821-831, 2001.

30. B.E. Henty and D.D. Stancil, "Multipath-Enabled Super Resolution for RF and Microwave Communication using Phase-Conjugate Arrays", Physical Review Letters, vol. 93, pp. 243904-1-243904-4, Dec. 2004.

31. НПАОП 0.00-1.28-10 Правила охорони праці під час експлуатації електронно-обчислювальних машин.

32. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

33. Державні санітарні норми та правила «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу».

34. «ДСН 3.3.6.042-99 Санітарних норми мікроклімату виробничих приміщень».

35. ДБН 13.2.5-28-2006 «Природне і штучне освітлення».

36. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку».

37. ДСТУ 12.1.005-88 «ССБП. Загальні санітарно-гігієнічні вимоги до повітря робочої зони».

38. ДБН В.2.5-28-2006 «Інженерне обладнання будинків і споруд. Природне і штучне освітлення».

39. ДСТУ Б В.2.5-82:2016 «Електробезпека в будівлях і спорудах. Вимоги до захисних заходів від ураження електричним струмом».

40. ДСТУ 8604:2015 «Дизайн і ергономіка. Робоче місце для виконання робіт у положенні сидячи. Загальні ергономічні вимоги».

41. НАПБ Б.03.002-2007 «Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою».

42. Прогнозування екологічних ризиків з використанням аналізу ієрархів та теорії нечітких множин: міжнародна науково-практична конференція «І-й всеукраїнський з'їзд екологів»: Тези доповідей. Україна, м. Вінниця, 4-7 жовтня 2016. – 2016. – С.25.

43. Клап Я. А., Яремкевич О. С., Червецова В. Г., Заярнюк Н. Л., Новіков В. П., Дослідження впливу електромагнітних, постійних магнітних та акустичних полів на організм людини // Вісник Нац. ун-ту "Львівська політехніка". – 2016 – № 812. – С. 365–372.

44. Сучасний стан досліджень впливу електромагнітних випромінювань на організм людини [Електронний ресурс]/[А. П. Чорний, В. В. Никифоров, Д. І. Родькін,

В. Ю. Ноженко] // Інженерні та освітні технології в електротехнічних та комп'ютерних системах: щоквартальний науково-практичний журнал. – Кременчук: КрНУ, 2013.

45. Екологія та охорона навколишнього природного середовища: навч. посібник для вузів / В. С. Джигирей. - 6-те вид., випр. і доп. - К. : Знання, 2017. - 422 с.

46. Боротьба з шумом на виробництві: Довідник / Під ред. О. Я. Юдіна. – М: Машинобудування, 2015. – 297 с.