Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _Інформаційних радіотехнологій і технічного захисту інформації_____
(повна назва)

Кафедра _____Радіотехнологій інформаційно-комунікаційних систем_____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____ГЮІК.ХХХХХХ.001ПЗ_____
(позначення документа)

ДОСЛІДЖЕННЯ ПРОДУКТИВНОСТІ БЕЗПРОВОДОВИХ СИСТЕМ ЗВ'ЯЗКУ
(тема)

Виконав:
студент _II_ курсу, групи РПСКм-20-2_____
_____Карабут А.О._____
(прізвище, ініціали)

Спеціальність 172 Телекомунікації та_____
радіотехніка_____
(код і повна назва спеціальності)

Освітня програма Радіоелектронні пристрої,_
системи та комплекси _____
(повна назва освітньої програми)

Керівник _____доц. Зарудний О.А._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ___Цопа О.І._____
(підпис) (прізвище, ініціали)

2021 р.

Не містить відомостей заборонених до відкритого публікування.

Студент Карабут А.О.

Керівник Зарудний О.А.

Харківський національний університет радіоелектроніки

Факультет Інформаційних радіо технологій і технічного захисту інформації
Кафедра Радіотехнологій інформаційно-комунікаційних систем
Рівень вищої освіти другий (магістерський)
Спеціальність 172 Телекомунікації та радіотехніка
(код і повна назва)

Освітня програма Радіоелектроні пристрої,системи та комплекси
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)
«____»_____ 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Карабут Антон Олександрович
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження продуктивності бездротових систем зв'язку
_____
затверджена наказом університету від 05 листопад 2021 р. № 1647Ст
2. Термін подання студентом роботи до екзаменаційної комісії ____ грудень 2021 р. ___
3. Вихідні дані до роботи провести дослідження продуктивності системи зв'язку стандарту IEEE 802.11ad
_____
4. Перелік питань, що потрібно опрацювати в роботі провести огляд бездротових систем зв'язку, провести огляд стандарту IEEE 802.11ad, особливості побудови системи зв'язку, захищеність сучасних систем зв'язку, оцінка продуктивності системи зв'язку, коефіцієнт підсилення антени в діапазоні 60ГГц.
_____
_____
_____
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) _____
_____
_____
_____
_____
_____
_____
_____
_____
_____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Основна частина	доц. Зарудний О.А.		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Ознайомлення зі завданням. Уточнення ТЗ	01.09.2021	вик.
2	Підбір літератури за темою роботи	12.09.2021-20.09.2021	вик.
3	Перший та другий розділ	21.09.2021-9.10.2021	вик.
4	Третій та четвертий розділ	10.10.2021-24.10.2021	вик.
5	Оформлення презентаційного матеріалу, підготовка	25.10.2021-1.12.2021	вик.
	до захисту у ЕК		

Дата видачі завдання __1__ ___вересня__2021 р.

Студент ________ _____Карабут А.О._____
(підпис) (прізвище, ініціали)

Керівник роботи _____ _____доц. Зарудний О.А._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 81 с., 27 рис., 6 табл., 23 посилань.

Ключові слова: БЕЗПРОВІДНА МЕРЕЖА, ПРОДУКТИВНІСТЬ, 60ГГц, WLAN, HD ДАНІ, IEEE 802.11ad, QPSK, BPSK, OFDM.

Об’єкт дослідження – бездротові системи зв'язку.

Предмет дослідження – бездротові системи зв'язку.

Мета проектування – дослідити продуктивність бездротової системи зв’язку стандарту IEEE 802.11ad.

Результати та їх новизна – в кваліфікаційній роботі проведено дослідження продуктивності бездротової системи зв’язку.

ABSTRAKT

Explanatory note: 81 p., 27 Fig., 6 Tab., 23 Sources.

Keywords: WIRELESS NETWORKS, PERFORMANCE, 60GHz, WLAN, HD, IEEE 802.11ad, QPSK, BPSK, OFDM.

Object of research - wireless communication systems.

Subject of research - wireless communication systems.

The purpose of designing - explore wireless communication systems of the IEEE 802.11ad standard.

Results and novelty - in the qualifying work the performance research carried out of a wireless communication system

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

Tx – Передавач
Rx – Приймач
OFDM – Orthogonal frequency-division multiplexing
WiGig – Wireless Gigabit Alliance
ISO – International Organization for Standardization
OSI – Open Systems Interconnection
FHSS – Frequency Hopping Spread Spectrum
IEEE – Institute of Electrical and Electronics Engineers
MAC – Media Access Control
WWAN – Wireless Wide Area Network
WMAN – Wireless Metropolitan Area Networks
WLAN – Wireless Local Area Network
WPAN – Wireless Personal Area Network
LLC – Logical Link Control
EAP – Extensible Authentication Protocol
RSA – Rivest, Shamir и Adleman
LDPC – Low-density parity-check
BTC – Block Truncation Coding
WEP – Wired Equivalent Privacy
WPA, WPA2 – Wi-Fi Protected Access
ACL – Access Control List
AES – Advanced Encryption Standard
QPSK – Quadrature Phase Shift Keying
BPSK – Binary Phase Shift Keying
QAM – Quadrature Amplitude Modulation
HD – High Definition
HDV – High Definition Video
RSNA – Robust Security Network Association
TKIP – Temporal Key Integrity Protocol
CCMP – Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
GCMP – Galois/Counter Mode Protocol
BIP – Broadcast Integrity Protocol

STA – Station
PBSS – Personal Basic Service set
PCP – PBSS central point
ESS – Extended Service Set

ВСТУП

Бездротові технології навколо нашого життя. Розвиваючись з великою швидкістю створюються нові пристрої та послуги на базі бездротового доступу.

З’явилась велика кількість нових бездротових технологій таких як (Code Division Multiple Access, технологія з кодовим розділенням каналів), GSM (Global for Mobile Communications, глобальна система для мобільних комунікацій), TDMA (Time Division Multiple Access, множинний доступ з розділенням за часом), WAP (Wireless Application Protocol, протокол бездротових технологій), GPRS (General Packet Radio Service, послуга пакетної передачі данних), EDGE (Enhanced Data Rates for GSM Evolution, збільшена передача даних для GSM) та інші, що каже про швидкий розвиток в даному напрямку[1].

Дуже бурно проходіть розвиток локальних мереж (WLAN), Bluetooth (мережа середніх та коротких відстаней). Бездротові мережі в наш час навколо нас у повсякденні: вдома, університетах, школах, аеропортах, ресторанах, підприємства та в інших місцях.

Бездротові мережеві технології як правило розділяють на три типа, що розрізняються за масштабом дії радіосистем, та всі вони успішно застосовуються в бізнесі.

Персональні мережі (PAN) короткодіючі, радіус дії до 10м які зв’язуються з персональним комп’ютером та з іншими пристроями як мобільні телефони планшети та інше. Завдяки таких мереж реалізується просто синхронізація даних, реалізується простий обмін інформації а невеликих робочих групах. Найбільш перспективний стандарт для персональних мереж це Bluetooth[5].

Бездротові локальні мережі (WLAN) радіус дії до 100м. Завдяки цьому реалізується бездротовий доступ до групових ресурсів в будівлі, та в інших місцях. Часто такі мережі використовують для продовження провідних корпоративних локальних мереж. При невеликому навантажені на мережу в деяких випадках бездротова локальна мережа може повністю замінити провідні з’єднання.

Бездротові мережі широкої дії WWAN. Бездротова мережа, що забезпечує мобільним користувачам доступ до їх корпоративним мережам та Інтернету.

Мета роботи: дослідити продуктивність бездротової системи зв’язку стандарту IEEE 802.11ad.

Задачі: провести огляд на сучасні технології WWAN, WMAN, WLAN та WPAN, розглянути стандарт IEEE 802.11.ad, оглянути особливості розповсюдженні радіохвиль в діапазоні 60ГГц, дослідити стандарт IEEE 802.11.ad на завадостійкість, дослідити продуктивності бездротової системи стандарту IEEE 802.11ad, та встановлено межі пропускної здатності.

В даний час технологія бездротової мережі Wi-Fi найбільш розповсюдженою зручною в умовах сучасних вимог мобільності, простоти встановлення та використання, тема кваліфікаційної роботи є актуальною, оскільки проводиться дослідження продуктивності найбільш розповсюдженої бездротової технології.

1 ОГЛЯД ТА АНАЛІЗ БЕЗДРОТОВИХ МЕРЕЖ ЗВЯЗКУ

1.1 Сучасні технології WWAN, WMAN, WLAN та WPAN

Радіомережі (бездротові мережі) забезпечують обмін даними між локальними комп'ютерними мережами, коли використання традиційних кабельних технологій утруднено або недоцільно (дорого). Прикладом ефективного використання бездротової технології радіодоступу є забезпечення зв'язку між сегментами локальних мереж при нестачі фінансових коштів, відсутність дозволу на проведення кабельних робіт або відмова телефонної станції в оренді виділеного каналу. У закритих приміщеннях прокладка кабелю може бути неможливою через нерозбірну підлогу або заборону монтажних робіт.

Основою будь-якої бездротової мережі є її протокол. Як правило, протокол регламентує топологію мережі, маршрутизацію, адресацію, порядок доступу вузлів мережі до каналу передачі даних, формат пакетів, що передаються, набір керуючих команд для вузлів мережі та систему захисту інформації.

Все різноманіття протоколів бездротової передачі даних можна класифікувати кількома різними шляхами, вибравши в якості основного один із параметрів, наприклад топологію мережі, швидкість роботи або алгоритми безпеки. Найбільш поширений метод класифікації в технічній літературі виходить із максимального радіусу дії бездротової мережі. Нижче (рис. 1.1) наведено класифікацію аналізованих протоколів щодо порядку зменшення радіуса.

WWAN (Wireless Wide area network) – в основному це мережі стільникового зв'язку, їхній радіус дії становить десятки кілометрів. До цих мереж належать такі протоколи: GSM, CDMAone, iDEN, PDC, GPRS та UMTS.

WMAN (Wireless Metropolitan Area Networks) – це бездротові мережі масштабу міста. Радіус дії таких мереж кілька кілометрів. Прикладом протоколу цієї мережі є WiMAX.

Wireless LAN (Wireless Local Area Network; WLAN) – це бездротова локальна обчислювальна мережа. Радіус дії цього класу мереж — кілька сотень метрів. До них належать такі протоколи: UWB, ZigBee, Wi-Fi.

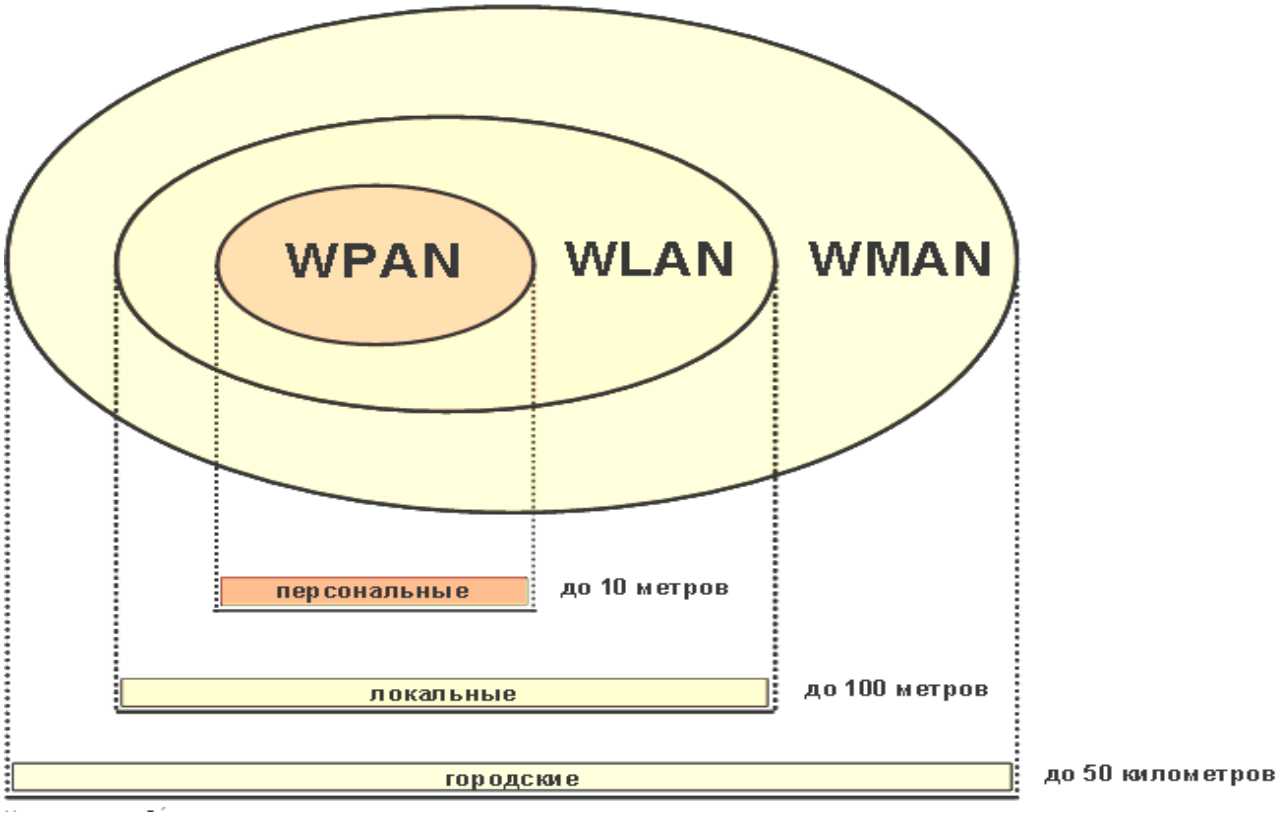

Рисунок 1.1 – Класифікація бездротових технологій за дальністю

WPAN застосовуються для зв'язку різних пристроїв, включаючи комп'ютери, побутові прилади та оргтехніку, засоби зв'язку тощо. WPAN використовується як для об'єднання окремих пристроїв між собою, так і для зв'язку з мережами вищого рівня. Прикладом таких мереж можуть бути протоколи RuBee, X10, Insteon, Bluetooth, Z-Wave, ANT, RFID.

Нижче коротко описується кожен із протоколів, що розглядаються. Ці протоколи обрані для аналізу внаслідок їх поширення в сучасних бездротових мережах зв'язку. Такий вибір дозволяє дати огляд поточного стану інформаційної безпеки у мережах бездротового зв'язку незалежно від розв'язуваних бездротовими мережами задач.[2]

1.2 Сучасні протоколи, технології та стандарти бездротових мереж

Крім радіусу дії мереж роль протоколів важлива щодо рівнів моделі OSI. Еталонна модель OSI, іноді звана стеком OSI, передбачає 7-рівневу мережеву ієрархію, розроблену Міжнародною організацією зі стандартів (International Standardization Organization - ISO) табл. 1.1.

Різних специфікацій стандартів бездротових мереж сімейства 802.1x існує безліч (для позначення одних лише різновидів стандарту 802.11 використовуються практично всі літери англійського алфавіту). В основному всі технології різняться, тільки на трьох перших рівнях OSI (фізичному, канальному та мережевому).

Основою будь-якої бездротової мережі є її протокол. Як правило, протокол регламентує топологію мережі, маршрутизацію, адресацію, порядок доступу вузлів мережі до каналу передачі даних, формат пакетів, що передаються, набір керуючих команд для вузлів мережі та систему захисту інформації.

Слід зазначити, що багато з розглянутих нижче протоколів було розроблено IEEE. Група протоколів IEEE 802.X містить опис мережних специфікацій та надає стандарти, рекомендації та інформаційні документи для мереж та телекомунікацій.

Рекомендації IEEE пов'язані головним чином із двома нижніми рівнями моделі OSI – фізичним та канальним. Ці рекомендації ділять канальний рівень на два підрівні: нижній - MAC (управління доступом до середовища) та верхній - LLC (управління логічним каналом).

Рекомендации IEEE связаны главным образом с двумя нижними уровнями модели OSI — физическим и канальным. Эти рекомендации делят канальный уровень на два подуровня: нижний — MAC (управление доступом к среде) и верхний — LLC (управление логическим каналом).

Таблиця 1.1 – Розділення рівнів моделі OSI

№	Рівень	Англійська	Основні задачі	Приклади

рівня		назва рівня		протоколів
7	Прикладний	A-Application	Форми взаємодії прикладних процесів	TP? TELNET
6	Відображення	P-Presentation	Перетворення даних	
5	Сеансовий	S-Session	Організація та проведення діалогу	SMTP
4	Транспортний	T-Transport	Налагодження наскрізних сполучень	TCP
3	Мережевий	N-Network	Прокладання сполучень між системами	IP
2	Канальний	DL-Data Link	Передавання між суміжними системами	
1	Фізичний	PL-Physical Link	Спряження з фізичними середовищами передавання	Ethernet, Token Ring

Протокол передачі інформації по бездротовому каналу Bluetooth був розроблений групою компаній Ericsson, IBM, Intel, Toshiba та Nokia. Групу розробки було створено на початку 1998 року. 20 травня 1998 року відбулося офіційне представлення спеціальної робочої групи (SIG - Special Interest Group), покликаної забезпечити безперешкодне впровадження технології, що отримала назву Bluetooth.

Bluetooth забезпечує обмін інформацією між такими пристроями, як кишенькові та звичайні персональні комп'ютери, мобільні телефони, ноутбуки, принтери, цифрові фотоапарати, мишки, клавіатури, джойстики, навушники, гарнітури на надійній, недорогій, повсюдно доступній радіочастоті для ближнього зв'язку. Зв'язок цих пристроїв може здійснюватися у радіусі від 10 до 100 метрів друг від друга навіть у різних помещениях.[11]

Протокол UWB був розроблений альянсом компаній WiMedia, а в 2007 році цей протокол був затверджений як міжнародний стандарт ISO/IEC 26907.

WiMedia UWB є стандартом широкосмугового бездротового зв'язку на коротких відстанях. Протокол торкається аспектів взаємодії між пристроями на фізичному рівні (PHY) та підрівні доступу до середовища (MAC). Максимальна

швидкість передачі даних між пристроями WiMedia UWB становить 480 Мбіт/с (як і у дротового USB), пристрої працюють у діапазоні частот від 31 до 106 ГГц. Протокол UWB конкурує із протоколом Bluetooth.

Протокол UWB был разработан альянсом компаний WiMedia, а в 2007 году этот протокол был утвержден в качестве международного стандарта ISO/IEC 26907.

Протокол ZigBee – це стандарт для недорогих, малопотужних бездротових мереж із пористою топологією. Низька вартість дозволяє широко застосовувати цю технологію для бездротового контролю та спостереження, а завдяки малій потужності сенсори мережі здатні працювати довгий час, використовуючи автономні джерела живлення.

Протокол було розроблено альянсом компаній ZigBee. Цей альянс служить органом, який визначає ZigBee стандарти високих рівнів; він також публікує профілі програм, що дозволяє виробникам вихідних комплектуючих випускати сумісні продукти.

Нижні рівні для цього стандарту розроблені IEEE та визначаються стандартами IEEE 802.15.4-2006

Протокол INSTEON розроблений для керування бездротовими пристроями, призначеними для «розумного дому». У протоколі передбачена зворотна сумісність із старішим протоколом X10. Швидкість передачі сигналу управління за новим стандартом набагато вище, передбачаються вбудовані засоби виявлення помилок і повторної передачі сигналу, а передачі використовується гібридний канал — радіозв'язок і мережу електроживлення. Однак на відміну від X10 специфікації INSTEON захищені патентами та використовуються лише його розробниками – компанією Smarthome Technology.

Мережа Z-Wave з функціями самоорганізації та самовідновлення в поєднанні з гнучкими інсталяційними процедурами є просте у використанні мережне рішення. Протокол Z-Wave та чіп високого ступеня інтеграції забезпечує невисоку вартість без компромісу щодо надійності чи універсальності. Реалізується сумісність програм та пристроїв Z-Wave, випущених різними виробниками.

Z-Wave підтримує повний спектр пристроїв, включаючи пристрої, що живляться від мережі змінного струму, від батарей, пристрої з фіксованим розташуванням і пристрої, що переміщуються, а також пристрої, що виконують роль мостів з іншими протоколами.

У технології Z-Wave вузли поділяються на три типи: контролери (Controllers), виконавчі механізми, що маршрутизують (Routing Slaves) і виконавчі механізми (Slaves). У реальній мережі всі типи пристроїв можуть працювати у будь-якій комбінації.

Протокол передачі ANT був розроблений компанією Dynastream Innovations.

Цей протокол насамперед розрахований на компактні пристрої з автономним живленням (трансівери, які використовують цей протокол, відрізняються виключно малим струмом споживання) для передачі відносно коротких пакетів даних. Протокол передбачає організацію відкритих та приватних бездротових мереж, зокрема складного типу з динамічною конфігурацією. Він створений на основі технології PAN (Personal Area Network) та підтримує шари 1-4 стека OSI (Open Systems Interconnection network model). Типове застосування такого протоколу – бездротові датчики.

Несуча частота за протоколом ANT - 2,4 ГГц, кількість частотних каналів при цьому дорівнює 125 (крок 1 МГц в діапазоні 2400... 2524 МГц). Швидкість передачі по радіоканалу (включаючи протокол) може становити до 1 Мбіт/с.

RuBee (IEEE P1902.1) — протокол двостороннього бездротового зв'язку в місцевій регіональній мережі з використанням довгохвильового діапазону (LW) та пакетів даних не більше 128 байт. Протокол RUBee подібний до протоколів серії IEEE 802, також відомих як Wi-Fi (IEEE 802.11), WPAN (IEEE 802.15.4) та Bluetooth (IEEE 802.15.1). RuBee networked, працює за принципом точка-точка та є розвитком стандартів RFID. RuBee передбачає роботу на низькочастотній несучій (131 кГц), дозволяючи використовувати вузли мережі з малим споживанням енергії.

RFID Radio Frequency IDentification. Радіочастотна ідентифікація з'явилася понад тридцять років тому. У 1973 році Маріо Кардулло та його співавтори опублікували патент US 3713148, який описує перший пасивний транспондер RFID

(радіометку). Розвиток та широке впровадження радіочастотної ідентифікації довго стримувалося відсутністю стандартизації. Але в 90-х роках минулого століття Міжнародна Організація Стандартизації (ISO) ухвалила низку стандартів у галузі RFID (серія стандартів ISO 18000-6).

X10 - це міжнародний відкритий індустріальний стандарт, який використовується для зв'язку електронних пристроїв у системах домашньої автоматизації. Стандарт X10 визначає методи та протокол передачі сигналів керування електронними модулями, до яких підключені побутові прилади, з використанням звичайної електропроводки або безпроводових каналів.

Стандарт X10 розроблений у 1975 році компанією Pico Electronics (Шотландія) для керування домашніми електроприладами. Вважається, що це перший стандарт домашньої автоматизації.

Wi-Fi створено в 1991 році NCR Corporation/AT&T (згодом - Lucent Technologies і Agere Systems) в Нідерландах. Wireless Fidelity — бездротова точність — торгова марка Wi-Fi Alliance для бездротових мереж на базі стандарту IEEE 802.11.

Зазвичай схема Wi-Fi мережі містить щонайменше одну точку доступу (так званий режим infrastructure) і щонайменше одного клієнта. Також можливе підключення двох клієнтів у режимі точка-точка, коли точка доступу не використовується, а клієнти з'єднуються за допомогою мережних адаптерів безпосередньо. Точка доступу передає ідентифікатор мережі (SSID) за допомогою спеціальних сигнальних пакетів на швидкості 0.1 Мбіт/с кожні 100 мс. Тому 0.1 Мбіт/с — це найменша швидкість передачі для Wi-Fi. Знаючи SSID-мережі, клієнт може з'ясувати, чи можливе підключення до цієї точки доступу. При попаданні в зону дії двох точок доступу з ідентичними SSID приймач може вибирати між ними на підставі даних рівня сигналу.[3]

PDC (Personal Digital Cellular) – стандарт стільникового зв'язку покоління 2G. Розроблено асоціацією ARIB (Association of Radio Industries and Business) у квітні 2001 року. Використовується виключно на території Японії. В даний час кількість абонентів стільникового зв'язку, які працюють на даному стандарті, скоротилася до

10 мільйонів людей. При тому, що в період максимальної поширеності цього стандарту кількість абонентів сягала 80 мільйонів осіб. PDC використовує частотні канали по 25 кГц з модуляцією pi/4-DQPSK з трьома тимчасовими слотами, що забезпечують передачу зі швидкістю 11.2 кбіт/с або 6 тимчасовими слотами зі швидкістю передачі 5.6 кбіт/с.

PDC використовує два діапазони частот - 800 МГц та 1,5 ГГц.

IDEN (Integrated Digital Enhanced Networks) – технологія для мереж транкінгового та стільникового зв'язку, розроблена компанією MOTOROLA у 1994 році. В основі технології iDEN архітектура GSM при передачі використовують частотні канали по 25 кГц, при цьому для передачі даних використовується частина каналу шириною 20 кГц, решта призначена для захисту каналу. Протокол набув широкого поширення в усьому світі. Діапазон частот - 821-825 МГц.

Стандарт CDMAOne розроблено у 1995 році як технологічний стандарт групи ANSI. CDMAOne заснований на використанні CDMA (множинного доступу з кодовим поділом).

Система CDMA IS-95 фірми Qualcomm розрахована працювати в діапазоні частот 800 МГц, виділеному для стільникових систем стандартів AMPS, N-AMPS і D-AMPS. (Стандарти TIA IS-19, IS-20; IS-54; IS-55, IS-56, IS-88, IS-89, IS-90, (S-553).

Подальший розвиток технології CDMA відбувається у рамках технології CDMA2000. При побудові системи мобільного зв'язку на основі технології CDMA2000 1X перша фаза забезпечує передачу даних зі швидкістю до 153 кбіт/с, що дозволяє надавати послуги голосового зв'язку, коротких повідомлень, роботу з електронною поштою, Інтернетом, базами даних, передачу даних і нерухомих зображень.

WiMAX (Worldwide Interoperability for Microwave Access) – телекомунікаційна технологія, розроблена з метою надання універсального бездротового зв'язку на великих відстанях для широкого спектру пристроїв (від робочих станцій та портативних комп'ютерів до мобільних телефонів). Заснована на стандарті IEEE 802.16, який також називають Wireless MAN.

Назва "WiMAX" була запропонована WiMAX Forum - організацією, заснованою в червні 2001 року для просування та розвитку технології WiMAX. Форум описує WiMAX як "засновану на стандарті технологію, що надає високошвидкісний бездротовий доступ до мережі, альтернативний виділеним лініям та DSL" Максимальна швидкість - до 1 Гбіт/с.

GSM (від назви групи Groupe Special Mobile, пізніше перейменований на Global System for Mobile Communications) (російськ. СПС-900) - глобальний цифровий стандарт для мобільного стільникового зв'язку з поділом частотного каналу за принципом TDMA та середнім ступенем безпеки. Розроблено під егідою Європейського інституту стандартизації електрозв'язку (ETSI) наприкінці 1980-х років.

Комерційне використання стандарту почалося в середині 1991 р., а до 1993 р. було організовано 36 мереж GSM у 22 країнах. На додаток до європейських держав стандарт GSM обрали багато країн Південної Африки, Близького та Далекого Сходу, а також Австралія. На початку 1994 р. число абонентів GSM досягло 1.3 мільйона. Термін GSM є скороченням від Global System for Mobile telecommunications – глобальна система мобільних телекомунікацій.

GSM відноситься до мереж другого покоління (2 Generation), хоча на 2010 рік умовно знаходиться у фазі 2,75G завдяки численним розширенням (1G - аналоговий стільниковий зв'язок, 2G - цифровий стільниковий зв'язок, 3G - широкосмуговий цифровий стільниковий зв'язок, що комутується багатоцільовими комп'ютерними мережами, включаючи Інтернет).

Мобільні телефони випускаються для 4 діапазонів частот: 850 МГц, 900 МГц, 1800 МГц, 1900 МГц.

GPRS (General Packet Radio Service – пакетний радіозв'язок загального користування) – надбудова над технологією мобільного зв'язку GSM, що здійснює пакетну передачу даних. GPRS дозволяє користувачеві мережі стільникового зв'язку здійснювати обмін даними з іншими пристроями в мережі GSM та із зовнішніми мережами, включаючи Інтернет.

Передача даних поділяється за напрямками "вниз" (downlink, DL) - від мережі до абонента і "вгору" (uplink, UL) - від абонента до мережі. Мобільні термінали поділяються на класи за кількістю таймслотів, що одночасно використовуються, для передачі і прийому даних. За даними за червень 2006 р., телефони підтримують до 4-х таймслотів одночасно для прийому по лінії «вниз» (тобто можуть приймати 85 кбіт/с за кодовою схемою CS-4) та до 2-х – для передачі по лінії « вгору» (class 10 або 4+2).

UMTS (Universal Mobile Telecommunications System – Універсальна Мобільна Телекомунікаційна Система) – технологія стільникового зв'язку розроблена Європейським Інститутом Стандартів Телекомунікацій (ETSI) для впровадження 3G у Європі. Як спосіб передачі даних через повітряний простір використовується технологія WCDMA, стандартизована відповідно до проекту 3GPP як відповідь європейських вчених та виробників на вимогу IMT-2000, опублікована Міжнародним союзом електрозв'язку як набір мінімальних критеріїв для мережі стільникового зв'язку третього покоління.

Згідно зі специфікаціями стандарту, UMTS використовує спектри частот: 1885-2025 МГ для передачі даних в режимі від мобільного терміналу до базової станції і 2110-2200 МГц для передачі даних в режимі від станції до терміналу. У США через зайнятість спектра частот у діапазоні 1900 МГц мережами GSM виділено діапазони 1710–1755 МГц та 2110–2155 МГц відповідно. Крім того, оператори деяких країн (наприклад, американський AT&T Mobility) додатково експлуатують смуги частот 850 та 1900 МГц. Уряд Фінляндії на законодавчому рівні підтримує розвиток мережі стандарту UMTS900, що покриває важкодоступні райони країни та використовує діапазон 900 МГц (в цьому проекті беруть участь такі компанії, як Nokia та Elisa).

1.3 Огляд стандарту IEEE 802.11.ad та його переваги

Спостерігається збільшення попиту на більш високу швидкість обміну даними у зв'язку з перспективним розвитком HD технологій. І у світлі нових прогресів

інформаційних технологій, ні Bluetooth, ні інші технології персонального доступу не є передовими стандартом персональних бездротових систем, що не можна сказати про новий IEEE 802.11.ad (60 Ггц).

Спочатку SiBEAM inc. (Придбані корпорацією Silicon Image) створили подібну технологію на використанні міліметрових хвиль (mmWave) смугу частот іменували як Wireless HD. Після того, як перевірили сумісність цієї технології з передачею стиснених форматів відео-файлів (HD), почалася розробка двох стандартів IEEE, з дуже високою пропускною здатністю, якими згодом з'явилися: IEEE 802.15.3c та IEEE 802.11.ad. На сьогоднішній день, IEEE 802.15.3c та IEEE 802.11ad повністю стандартизовані та доступна їх специфікація.

Бездротовий зв'язок, який є актуальним на даний час, включаючи новітні версії Bluetooth, використовує частоти 2.4 і 5 (ГГц), а швидкість передачі даних досягає максимум 100 Мбіт/с. Система, що працює в смузі частот 60 ГГц була представлена, щоб забезпечити більш швидку передачу інформації. [12] Розроблено всього п'ять стандартів, що використовують таку смугу частот: IEEE 802.15.3c, ECMA-387, Wireless HD, IEEE 802.11ad, і WiGig.[7]

Кожен із них має різні специфікації, максимальні пропускні здібності, підтримки від спонсорів, свої недоліки та переваги. Проте їхня головна мета полягає у передачі одного гігабіту в секунду та забезпеченні високої якості зв'язку на відстанях до 10 метрів. Бездротові системи, що функціонують на міліметровому діапазоні хвиль, обіцяють надати швидкість від 1 Гбіт/с до 7 Гбіт/с, яка в 10 разів швидше, ніж існує зараз. Насичений спектр сигналу надає можливість підтримки високої швидкості передачі. Це одна з найбільших неліцензованих смуг пропускання.

Схема бездротової відео мережі представлена на рис. 1.3. І складається з трьох типів пристроїв: відео програвач (HD дисплей), відео джерела (смартфон, планшет) та пристрій, який може виконувати обидві завдання (ноутбук).

Також систему можна у вигляді блокової діаграми (рис 1.2) каналу з Гауссовским шумом. За цією моделлю каналу проводилися вимірювання ймовірності бітової помилки, про які буде згадано нижче.

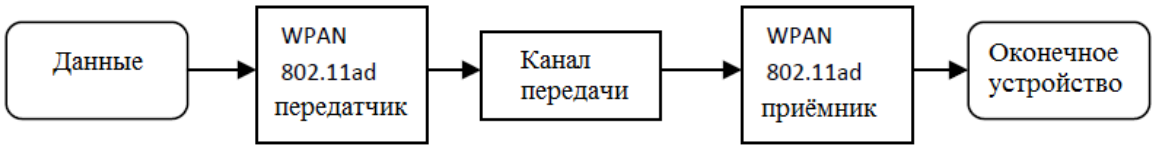

Рисунок 1.2 – Блочна диаграмма канала 802.11ad

Рисунок 1.3 - Приклад бездротової відео мережі

1.4 Безпека бездротових мереж

Як і будь-яка комп'ютерна мережа, Wi-Fi є джерелом підвищеного ризику несанкціонованого доступу. Крім того, проникнути в бездротову мережу значно простіше, ніж у звичайну, не потрібно підключатися до проводів, достатньо опинитися в зоні прийому сигналу.

Бездротові мережі відрізняються від кабельних тільки на перших двох - фізичному (Phy) і частково канальному (MAC) - рівнях семирівневої моделі взаємодії відкритих систем. Вищі рівні реалізуються як у провідних мережах, а реальна безпека мереж забезпечується саме цих рівнях. Тому різниця у безпеці тих та інших мереж зводиться до різниці у безпеці фізичного та MAC-рівнів.

Хоча сьогодні в захисті Wi-Fi-мереж застосовуються складні алгоритмічні математичні моделі аутентифікації, шифрування даних та контролю цілісності їх передачі, проте ймовірність доступу до інформації сторонніх осіб є дуже суттєвою. І якщо налаштування мережі не приділити належної уваги зловмисник може:

- отримати доступ до ресурсів та дисків користувачів Wi-Fi-мережі, а через неї і до ресурсів LAN;
- підслуховувати трафік, витягувати з нього конфіденційну інформацію;
- спотворювати інформацію, що проходить в мережі;
- Впроваджувати підроблені точки доступу;
- розсилати спам, та здійснювати інші протиправні дії від імені вашої мережі.

Але перш ніж приступати до захисту бездротової мережі необхідно зрозуміти основні принципи її організації. Як правило, бездротові мережі складаються з вузлів доступу та клієнтів із бездротовими адаптерами. Вузли доступу та бездротові адаптери оснащуються приймачами для обміну даними один з одним. Кожному AP та бездротовому адаптеру призначається 48-розрядна адреса MAC, яка функціонально еквівалентна адресі Ethernet. Вузли доступу пов'язують бездротові та дротові мережі, забезпечуючи бездротовим клієнтам доступ до дротових мереж. Зв'язок між бездротовими клієнтами в однорангових мережах можливий без AP, але цей метод рідко застосовується в установах. Кожна бездротова мережа ідентифікується адміністратором, що призначається, ідентифікатором SSID (Service Set Identifier). Зв'язок бездротових клієнтів з AP можливий, якщо вони розпізнають SSID вузла доступу. Якщо в бездротовій мережі є кілька вузлів доступу з одним SSID (і однаковими параметрами автентифікації та шифрування), то можливе перемикання між ними бездротових мобільних клієнтів.

Найбільш поширені бездротові стандарти - 802.11 та його вдосконалені варіанти. У специфікації 802.11 визначено характеристики мережі, що працює зі швидкостями до 2 Мбіт/с. У вдосконалених випадках передбачені вищі швидкості. Перший, 802.11b, поширений найбільш широко, але швидко замінюється стандартом 802.11g. Бездротові мережі 802.11b працюють у 2,4-ГГц діапазоні та забезпечують швидкість передачі даних до 11 Мбіт/с. Удосконалений варіант

802.11a був ратифікований раніше, ніж 802.11b, але з'явився на ринку пізніше. Пристрої цього стандарту працюють у діапазоні 5,8 ГГц із типовою швидкістю 54 Мбіт/с, але деякі постачальники пропонують вищі швидкості, до 108 Мбіт/с, у турборежимі. Третій, удосконалений варіант, 802.11g, працює в діапазоні 2,4 ГГц, як і 802.11b, зі стандартною швидкістю 54 Мбіт/с та з більш високою (до 108 Мбіт/с) у турборежимі. Більшість бездротових мереж 802.11g здатні працювати з клієнтами 802.11b завдяки зворотній сумісності, закладеній у стандарті 802.11g, але практична сумісність залежить від конкретної реалізації постачальника. Основна частина сучасного бездротового обладнання підтримує два або більше варіантів 802.11. Новий бездротовий стандарт, 802.16, що називається WiMAX, проектується з метою забезпечити бездротовий доступ для підприємств і житлових будинків через станції, аналогічні станціям стільникового зв'язку. Ця технологія у цій статті не розглядається.

Реальна дальність зв'язку AP залежить від багатьох факторів, у тому числі варіанта 802.11 та робочої частоти обладнання, виробника, потужності, антени, зовнішніх та внутрішніх стін та особливостей топології мережі. Однак бездротовий адаптер з вузькоспрямованою антеною з великим коефіцієнтом посилення може забезпечити зв'язок з AP і бездротовою мережею на значній відстані приблизно до півтора кілометра в залежності від умов.

Через загальнодоступний характер радіоспектру виникають унікальні проблеми з безпекою, які відсутні у провідних мережах. Наприклад, щоб підслуховувати повідомлення в проводовій мережі, необхідний фізичний доступ до такого мережного компонента, як точка підключення пристрою до локальної мережі, комутатор, маршрутизатор, брандмауер або комп'ютер. Для бездротової мережі потрібен лише приймач, такий як звичайний частотний сканер. Через відкритість бездротових мереж розробники стандарту підготували специфікацію Wired Equivalent Privacy (WEP), але зробили її необов'язковим. У WEP застосовується спільний ключ, відомий бездротовим клієнтам та вузлам доступу, з якими обмінюються інформацією. Ключ можна використовувати як для автентифікації, так і для шифрування. У WEP застосовується алгоритм шифрування

RC4. 64-розрядний ключ складається з 40 розрядів, що визначаються користувачем, та 24-розрядного вектора ініціалізації. Намагаючись підвищити безпеку бездротових мереж, деякі виробники обладнання розробили розширені алгоритми зі 128-розрядними та довшими ключами WEP, що складаються зі 104-розрядної та довшої користувальницької частини та вектора ініціалізації. WEP застосовується з 802.11a, 802.11b- та 802.11g-сумісним обладнанням. Однак, незважаючи на збільшену довжину ключа, вади WEP (зокрема слабкі механізми аутентифікації та ключі шифрування, які можна розкрити методами криптоаналізу) добре документовані, і сьогодні WEP не вважається надійним алгоритмом.

У відповідь на недоліки WEP галузева асоціація Wi-Fi Alliance вирішила розробити стандарт Wi-Fi Protected Access (WPA). WPA перевершує WEP завдяки доданню протоколу TKIP (Temporal Key Integrity Protocol) та надійному механізму автентифікації на базі 802.1x та протоколу EAP (Extensible Authentication Protocol). Передбачалося, що WPA стане робочим стандартом, який можна буде подати для схвалення комітету IEEE як розширення для стандартів 802.11. Розширення, 802.11i, було ратифіковано в 2004 р., а WPA оновлено до WPA2 з метою сумісності з Advanced Encryption Standard (AES) замість WEP та TKIP. WPA2 сумісний назад і може застосовуватися спільно з WPA. WPA був призначений для мереж підприємств з інфраструктурою аутентифікації RADIUS (Remote Authentication Dial-In User Service — служба дистанційної аутентифікації користувачів по лініях, що комутуються), але версія WPA, іменована WPA Pre-Shared Key (WPAPSK), отримала підтримку деяких виробників і готується до застосування на невеликих підприємствах. Як і WEP, WPAPSK працює із загальним ключем, але WPAPSK надійніше WEP.[2]

В даному розділі проведено огляд на сучасні технології WWAN, WMAN, WLAN та WPAN які відрізняються між собою за відстанню дії, використанню протоколів для обміну даних. Розглянуто стандарт IEEE 802.11.ad який є одним з найпоширенішим в наш час.

2 ОСОБЛИВОСТІ ПОБУДОВИ СИСТЕМ НА БАЗІ СТАНДАРТУ IEEE 802.11ad

2.1 Особливості поширення електромагнітних хвиль у діапазоні 60 ГГц.

Особливості використання систем бездротового доступу стандарту IEEE 802.11ad, використовують діапазон частот 60 ГГц (довжина хвилі – 5 мм). Цей діапазон довго привертав увагу розробників телекомунікаційних систем. Тому є низка причин. По-перше, у смузі приблизно 57–64 ГГц дуже сильне згасання радіохвиль на атмосферному кисні – до 16 дБ/км (рис.2.1). Ще сильніше загасання при дощі (рис.2.2).

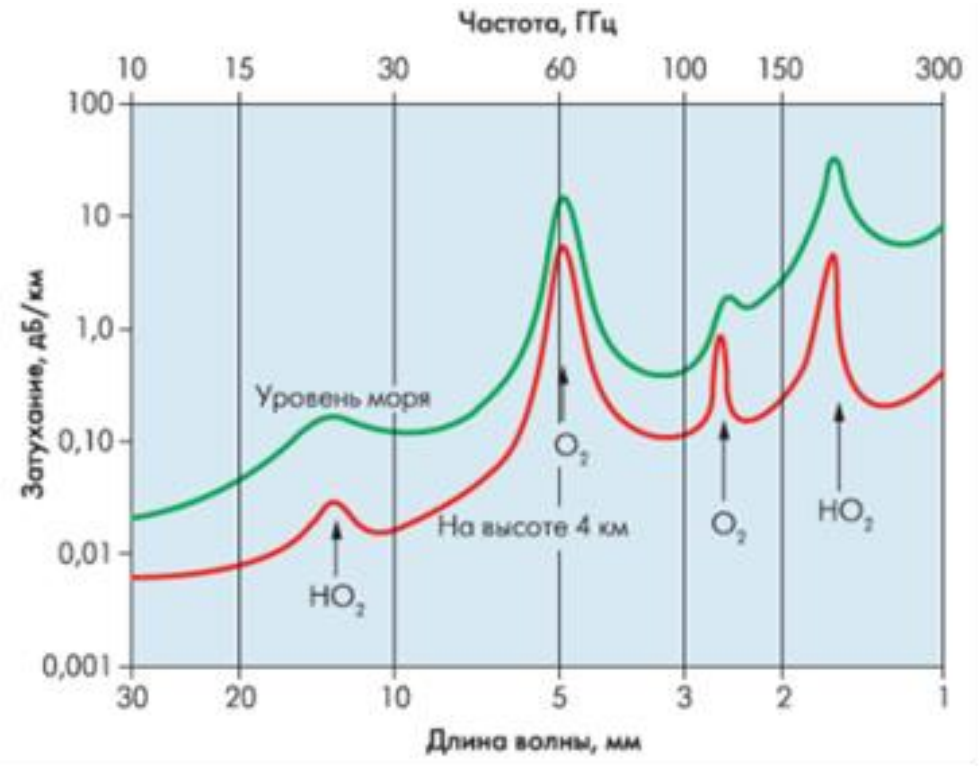

Рисунок 2.1 – Ослаблення сигналу в повітрі за рахунок атмосферного кисню та вологи

Недолік діапазону 60 ГГц загасання радіо хвиль, але цей недолік стає гідністю, якщо задуматися про такі параметри, як скритність, можливість повторного

використання частот, взаємного впливу приймачів і т.п. Для передачі на далекі відстані в одиниці кілометрів діапазон 60 ГГц далеко не оптимальний, але якщо говорити про відстані в сотні та десятки метрів (локальні та персональні мережі, відповідно), картина радикально змінюється.

Насправді, відповідно до закону про розповсюдження електромагнітних хвиль у вільному просторі потужність прийнятого сигналу:

$$Pr = Pt*Gt*Gr*\lambda^2 / (4\pi R)^2, \qquad (2.1)$$

де, Pt – потужність передатчика;

Gt та Gr – підсилення передавальної та приймальної антени;

λ – довжина хвилі випромінювання;

R – відстань між приймачем та передавачем.

Відповідно, для довжини хвилі 5 мм і дальності 100 м відношення Pr/Pt, без урахування посилення антен, складе приблизно -108 дБ. При цьому поглинання на атмосферному кисні (приблизно 1,5 дБ на 100 м) не вплине.

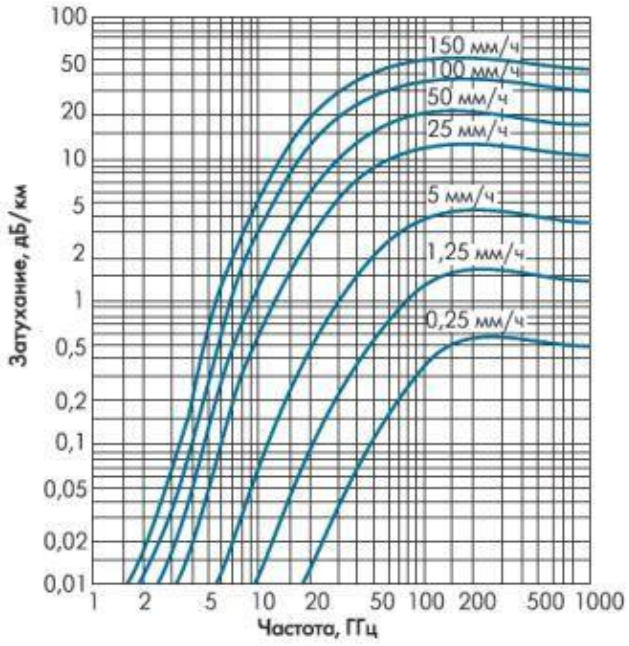

Рисунок 2.2 – Рівень загасання сигналу при опадах

Таким чином, на відносно малих дистанціях у 60-ГГц діапазоні при прямій видимості основний фактор – "природне" послаблення сигналу. Звичайно, воно велике, і це є недоліком. Але його можуть з лишком компенсувати інші переваги. Насамперед, через сильне ослаблення, пов'язане з поглинанням на атмосферному кисні, усувається проблема інтерференції між різними джерелами сигналу, що належать різним мережам. Це дозволяє автоматично вирішити проблему повторного використання частот – зникає завдання частотного розподілу. Саме тому діапазон 60 ГГц у багатьох провідних країнах світу визнано без ліцензійним (рис. 2.3). Одночасно досягаються такі показники, як скритність зв'язку (прихованість), цілісність (стійкість до прицільних перешкод) та стійкість до несанкціонованого підключення (неможливість фальсифікувати мобільну станцію або точку доступу).

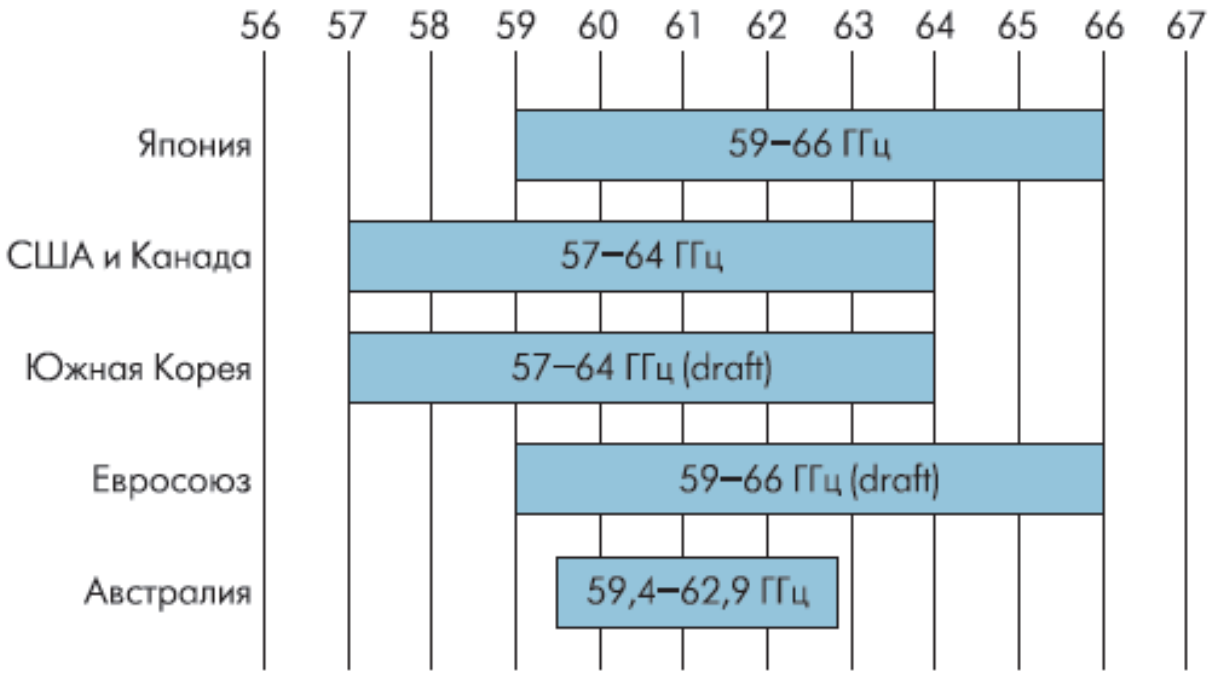

Рисунок 2.3 – Вільні ділянки спектру в діапазоні 60 ГГц в різних державах

Не менш важлива перевага – ширина доступної смуги до 7 ГГц. Це робить 60-ГГц діапазон якщо не безальтернативним, то надзвичайно привабливим для високошвидкісної надширокосмугової передачі (за визначенням FCC США, понад широка смуга – все, що перевищує 500 МГц). Це дозволяє передавати

високошвидкісні потоки інформації, включаючи трансляцію відеопотоків з декількох відеокамер, передачі відеосигналу високої роздільної здатності, про формати якого буде описано нижче. Організацію транспортних потоків у стільникових мережах тощо. Крім того, широка смуга допускає застосування найрізноманітніших схем скремблювання, завадостійкого кодування, вибір оптимальних передачі даних методів модуляції і множинного доступу, що забезпечує можливість передачі даних з необхідною швидкістю при дуже низькому співвідношенні сигнал/шум.

Інший найважливіший фактор – довжини хвиль у міліметровому діапазоні суттєво знижують габарити антенних систем. Для досягнення вузької діаграми спрямованості (тобто для більшого посилення антени) потрібні менші розміри самих антен. Справді, посилення антени можна оцінити як:

$$G = 4\pi S / \lambda^2, \qquad (2.2)$$

де S – апертура антени (тобто її ефективна площа).

Тоді формула розповсюдження електромагнітних. хвиль перетворюється на вигляд:

$$Pr = Pt*St*Sr / (\lambda R)^2, \qquad (2.3)$$

Тобто з урахуванням фактора антени втрати потужності в каналі Pr/Pt виявляються обернено пропорційними квадрату частоти. При ефективній площі 10 $см^2$ посилення антени складе 35 дБ, при S = 1 $см^2$ - 17 дБ (якщо не використовуються антени з фазованими решітками або іншими способами формування вузької ДН).

Для зв'язку в діапазоні 60 ГГц можна створювати мініатюрні антенні системи, аж до інтегрованих в чіп фазованих решіток антенних або спрямованих антен іншої конструкції. Це відкриває блискучі перспективи в плані виробництва монолітних або квазімонолітних інтегрованих приймальних пристроїв, що дозволяють застосовувати їх за принципом "включив - працює". Вся тонкість і складність

конструювання та налаштування радіосистем мм-діапазону прихована від того, хто застосовує такі модулі як готові компоненти. Причому такі інтегровані антенно-трансіверні модулі дозволяють створювати системи з багатопроменевими діаграмами спрямованості, що перебудовуються (smart-антени). У цьому можливі два підходи – антенна система з перемиканням променів (масив спрямованих антен) і антенна система із синтезом діаграми спрямованості (адаптивні).[21]

Все це дозволяє говорити про швидку появу нового класу елементної бази електроніки, відповідно – про принципово нові споживчі пристрої та системи.

Нарешті, відзначимо, що електромагнітне випромінювання в діапазоні 60 ГГц відносно нешкідливе, оскільки не проникає глибше за зовнішні шкірні покриви (поглинається водою). Тим не менш, існуючі норми FCC (Rule 1.1310) обмежують поверхневу щільність потужності випромінювання на рівні 1 мВт/см2 при середній експозиції понад 30 хвилин та 5 мВт/см2 при середній експозиції понад 6 хвилин.

2.2 Формування відеосигналів високої чіткості

Персональна мережа формату IEEE 802.11ad позиціонується на прийомі передачі відеосигналів високої чіткості.

Формат HD – це формат високої чіткості, з'явився порівняно недавно. Цей формат дає вищу якість зображення рахунок збільшення роздільної здатності, тобто. кількість пікселів екрану. Можна виділити два напрями цього формату:

Формат HDV – використовується для відтворення відео з різних носіїв: дисків, касет, флешок, жорсткого диска та ін.

Формат HDTV - телевізійне мовлення різними каналами (ефірне, кабельне, супутникове), інша назва - телебачення високої чіткості (ТВЧ).

Для того, щоб оцінити всі переваги відео високої чіткості, потрібний екран із великою діагоналлю. Електронно-променеві дисплеї великого розміру були занадто дорогими, тому досить довго відео високої роздільної здатності не застосовувалося на практиці. В наш час з'явилися рідкокристалічні та плазмові екрани з великою діагоналлю, а отже, почалося масове поширення відео високої чіткості. Для

перегляду ТВЧ розроблені спеціальні приймачі, дисплеї з великою роздільною здатністю, цифрові інтерфейси HDMI та DVI-D, носії інформації HD DVD та Blu-Ray. У Європі, США, Японії ведеться телевізійне мовлення стандарту ТВЧ супутниковими і кабельними каналами. [20]

Форматом відео стандартної чіткості SD (Standard Definition – стандартна роздільна здатність) є DVD з його роздільною здатністю 720x576 (PAL) або 720x480 (NTSC). На сьогоднішній день поширені два основні роздільні здатності відео високої чіткості (рис. 2.4): HD1080 (1920x1080) та HD720 (1280x720). В обох пропорції екрану становлять 16:9. Позначення, що застосовуються:

- 720p - 1280x720 пікселів, прогресивна розгортка;
- 1080i - 1920x1080 пікселів, черезрядкова розгортка;
- 1080p - 1920x1080 пікселів, прогресивна розгортка.

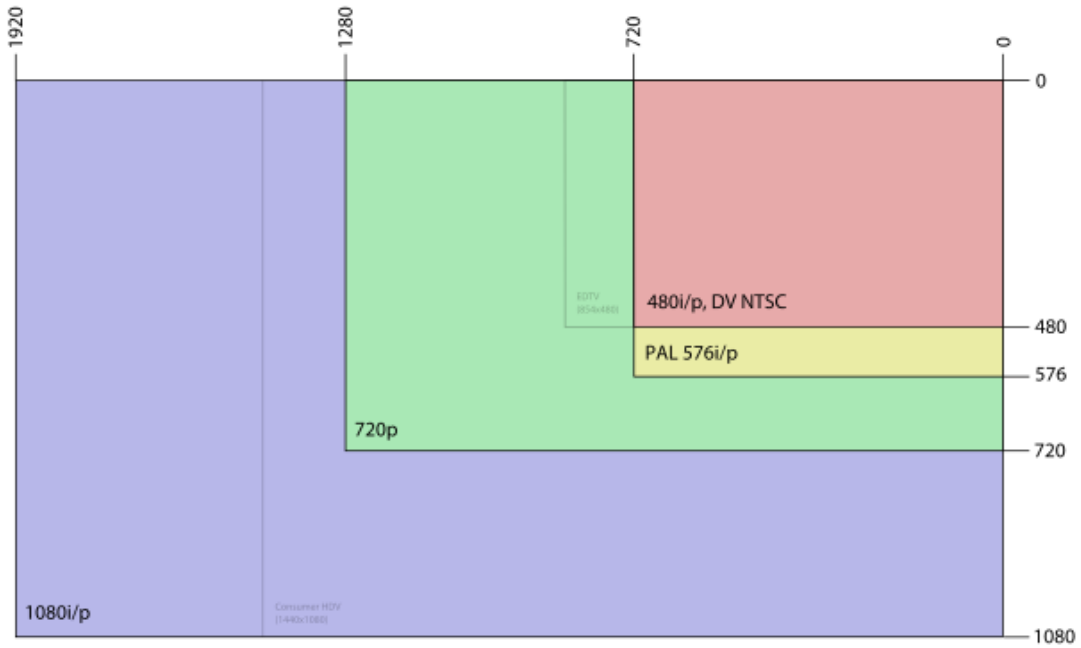

Рисунок 2.4 – Роздільна здатність HD відео

Частота кадрів (frame rate) являє собою число повних зображень, що записуються або передаються, в секунду. В принципі, одне зображення може передаватися як повний кадр (p) або як два послідовні поля (i). Характер зображення та відповідні процеси будуть у цих двох випадках різними.

Позначення Full-HD означає, що телевізор (панель, проектор) підтримує повну роздільну здатність 1920x1080. Позначення HD-Ready показує, що роздільна здатність телевізора менше 1920x1080, наприклад 1024x768 пікселів. Отже, вхідний HD-сигнал буде перетворено (стиснутий) до розмірів 1024x768, що зменшить чіткість картинки.

Одним із найпоширеніших форматів кодування є MPEG-2 HD. Він створений групою Moving Picture Expert Group і є розвитком «звичайного» MPEG-2, який використовується у DVD-Video. MPEG-2 HD забезпечує високу якість відеоряду, проте сам алгоритм компресії не надто ефективний, через що один повнометражний фільм може займати 50 гігабайт і більше.

2.3 Особливості модуляції стандарту IEEE 802.11ad

Вибір схеми модуляції для системи використовує діапазон 60 ГГц дуже залежить від: каналу поширення, використання вузьконаправлених антен/антенних решіток, а також обмежень накладених радіочастотним міністерством. Наприклад, якщо затримка поширення каналу дуже висока, тоді очевидним у схемі модуляції для цього випадку буде використання мультиплексування з ортогональним поділом каналів (OFDM). Така схема спрощує рівномірний розподіл швидкості системи бездротового мультигігабітного доступу. З іншого боку, високий коефіцієнт посилення або кругова поляризація антени можуть служити для зменшення траєкторії руху хвиль, і отже, проста схема модуляції з однією несучою може використовуватися для збереження потужності споживання і зменшення вартості. Як правило, у реалізації схеми CMOS(60-ГГц), підсилювач потужності вимагає меншої потужності та більш високої лінійності роботи. Це означає, що використання простих схем модуляції вигідніше, ніж система OFDM, яка страждає від великого відношення пікової та середньої потужностей (PAPR) і може значно знизити ефективність роботи підсилювача потужності. Крім того, погана характеристика фазових шумів у схемі також обмежує використання модуляції вищого порядку, до квадратурної амплітудної модуляції (QAM), фазової маніпуляції

(PSK) і частотної маніпуляції (FSK). Використання такого низького порядку модуляції також мотивовано величезною не ліцензованою смугою при 60 ГГц. Отже, вибір модуляції є вирішенням низки питань, таких як: оптимальна спектральна ефективність, лінійність підсилювача потужності (PA), рівень фазових шумів, масштабованість, та інше.[18]

На даний момент модуляційними схемами стандарту 802.11ad є:

- π /2 BPSK, π /2 QPSK, π /2 16-QAM для однієї несучої;
- SQPSK, QPSK, 16-64 QAM для OFDM модуляції.

BPSK – найпростіша форма фазової маніпуляції. Робота схеми двійкової ФМн полягає у зміщенні фази коливання, що несе, на одне з двох значень, нуль або (180°) в даному випадку π /2 або 3π /2.

QPSK квадратурна фазова маніпуляція або 4-PSK - використовується сузір'я з чотирьох точок, що розміщені на рівних відстанях на колі, і зсунуті проти годинникової стрілки на π /2. Використовуючи 4 фази, QPSK на символ припадає два біти, як показано на рис. 2.5. Аналіз показує, що швидкість може бути збільшена вдвічі щодо BPSK при тій же смузі сигналу, або залишити швидкість колишньої, але зменшити смугу вдвічі.

Фазоманіпульований сигнал має такий вигляд:

$$s_m(t) = g(t)\cos[2\pi f_c t + \varphi_m(t)], \tag{2.4}$$

де $g(t)$ – визначає огинаючу сигналу;

$\varphi_m(t)$ – є модулюючим сигналом;

$\varphi_m(t)$ – може приймати M дискретних значень;

f_c – частота несучої;

t – час.

Якщо $M = 2$, тоді фазовая маніпуляція називається BPSK, якщо $M = 4$ – QPSK при $M = 8$ 8-PSK і т. д.

Фазоманіпульований сигнал $s_i(t)$ можна розглядати як лінійну комбінацію двох ортонормованих сигналів y_1 та y_2 :

$$S_m(t) = S_1 Y_1 + S_2 Y_2, \tag{2.5}$$

де,

$$Y_1(t) = \sqrt{\frac{2}{E_g}} g(t) \cos[2\pi f_c t + \varphi_m(t)], \tag{2.6}$$

$$Y_2(t) = -\sqrt{\frac{2}{E_g}} g(t) \sin[2\pi f_c t + \varphi_m(t)]. \tag{2.7}$$

Таким чином, сигнал $S_m(t)$ вважатимуться двомірним вектором $[S_1(m,\ M);\ \ S_2(m,\ M)]$. Якщо значення $S_1(m,\ M)$ відкласти по горизонтальній осі, а значення $S_2(m,\ M)$ по вертикальній, то точки з координатами і утворюватимуть просторові діаграми, показані на рис. 2.5.

QAM – називається маніпуляція, коли він змінюється як фаза, і амплітуда сигналу, що дозволяє збільшити кількість інформації, що передається одним станом (відліком) сигналу. Схеми 16-QAM та 64-QAM представлені на рис.2.5 та рис. 2.6 відповідно.

Схеми модуляції для режиму OFDM залишаються аналогічними, але без початкових зрушень, і до вже раніше розібраних варіантів додається метод 64-QAM для передачі даних високої якості.

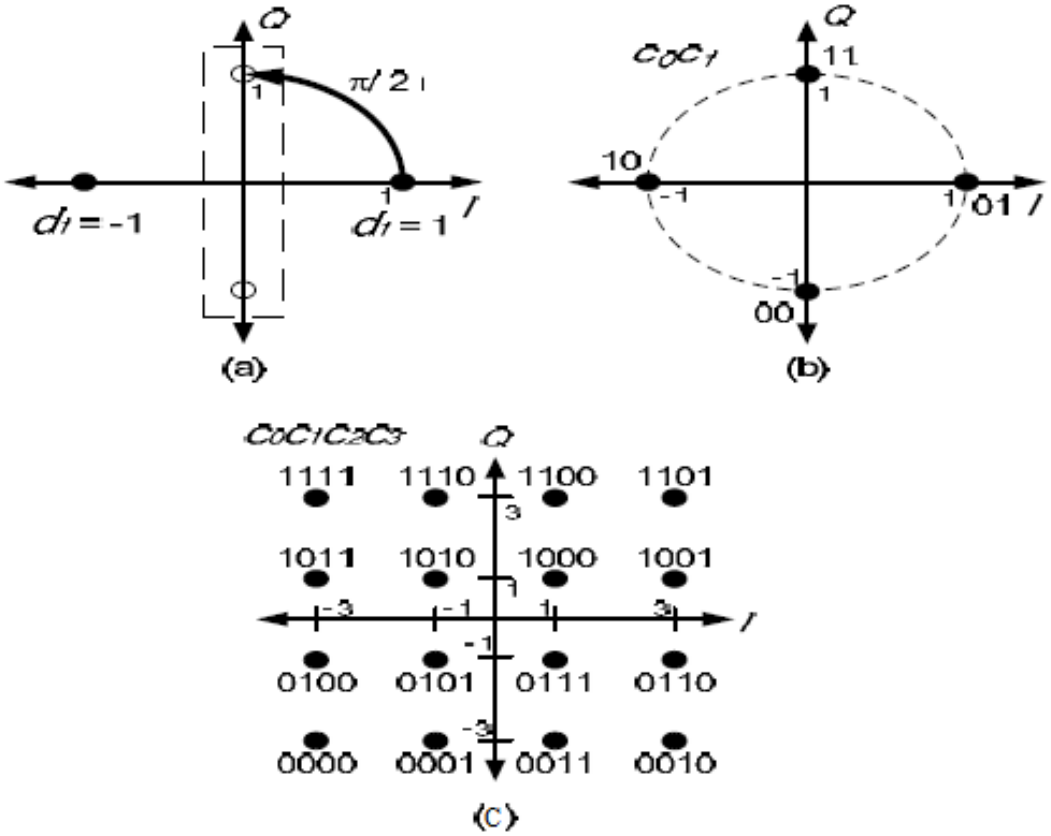

Рисунок 2.5 – модуляційні схеми для однієї несучої

(a)π /2 BPSK, (b) π /2 QPSK, (c) π /2 16-QAM

Ймовірність помилки на біт (BER) при фазових маніпуляціях у каналі з адитивним білим гаусівським шумом (АБГШ) може бути обчислена за формулою та представлена на рис. 2.8:

$$P_b = Q\left(\sqrt{\frac{2E_b}{N_0}}\right), \tag{2.8}$$

де,

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{t^2}{2}}\, dt. \tag{2.9}$$

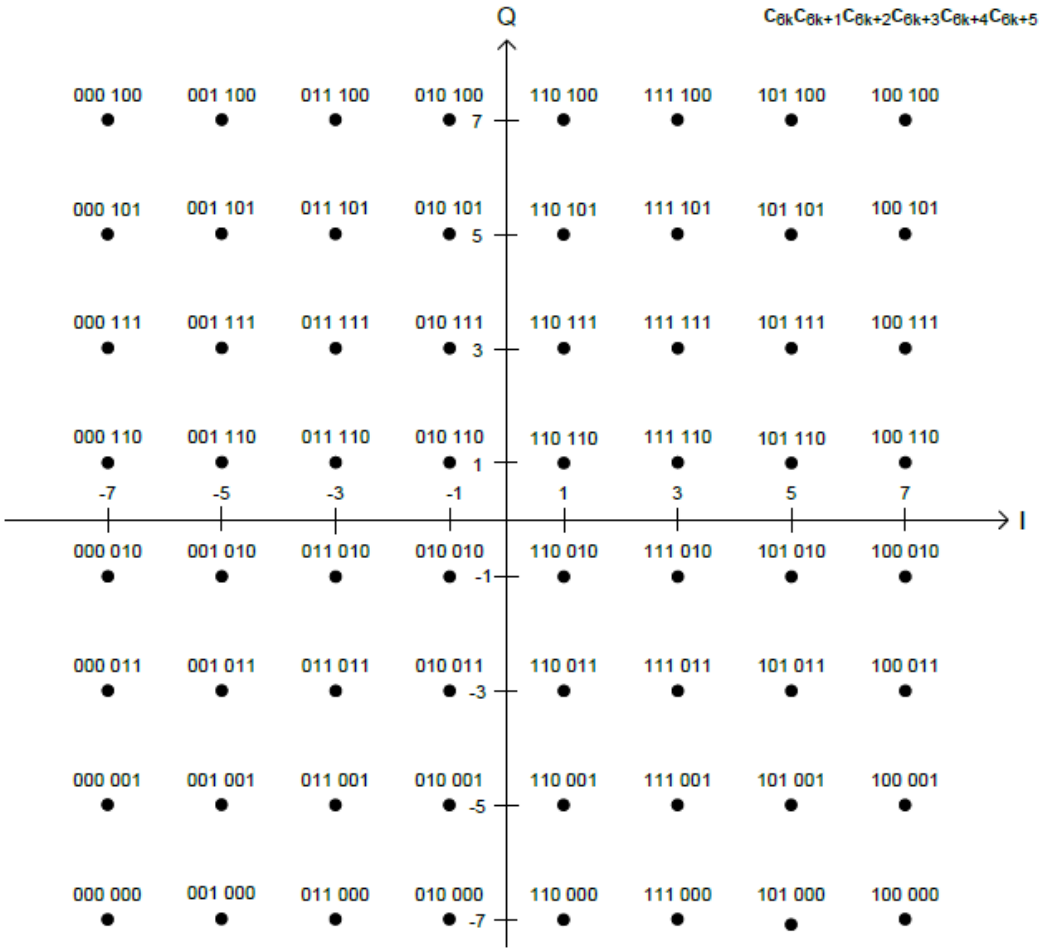

Рисунок 2.6 – Модуляція 64-QAM

Однак не все залежить від модуляції, розглянемо нижче (табл.2.1) збільшення швидкості передачі при різній швидкості порівняльного коду LDPC, для режиму з однією несучою та OFDM табл. 2.2

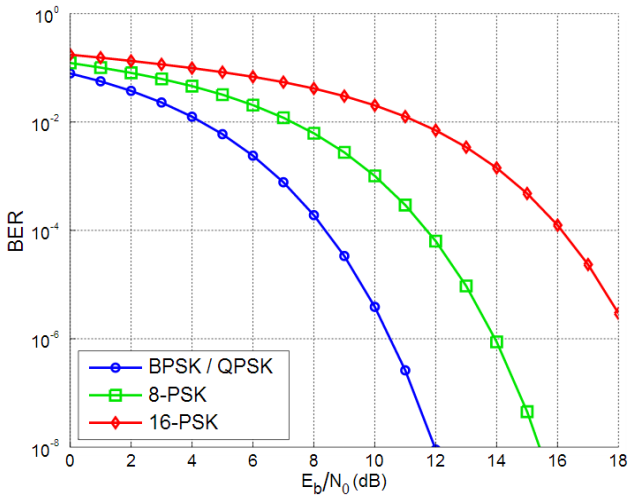

Рисунок 2.7 – Залежність BER від сигнал/шум при фазових маніпуляціях

Таблиця 2.1 – Схеми модуляції та кодування для однієї несучої

№	Модуляція	Кількість кодованих біт на символ	Повторення	Швидкість коду (LDPC)	Швидкість передачі (Mbps)
1	π/2-BPSK	1	2	1/2	385
2	π/2-BPSK	1	1	1/2	770
3	π/2-BPSK	1	1	5/8	962.5
4	π/2-BPSK	1	1	3/4	1155
5	π/2-BPSK	1	1	13/16	1251.25
6	π/2-QPSK	2	1	1/2	1540
7	π/2-QPSK	2	1	5/8	1925
8	π/2-QPSK	2	1	3/4	2310
9	π/2-QPSK	2	1	13/16	2502.5
10	π/2-16QAM	4	1	1/2	3080
11	π/2-16QAM	4	1	5/8	3850
12	π/2-16QAM	4	1	3/4	4620

З даних таблиць можна зробити висновок, що збільшити швидкість передачі в обох випадках можливо і при збільшенні швидкості коду згортки (LDPC). Збільшення швидкості двох режимів становить приблизно 1.5 разу. № 17 та нижче для табл. 2.3 є обов'язковими для всіх приймальних та передавальних пристроїв, які підтримують OFDM, для табл. 2.2 №4 і нижче є так само обов'язковими схемами для всіх приймально-передаючих пристроїв, що працюють в режимі однієї несучої, а 5 і 12 опціональними.[10]

Таблиця 2.2 – Схеми модуляції та кодування для OFDM

№	Модуляція	Швидкість коду (LDPC)	N кбнон	N кбнс	N ібнс	Швидкість передачі (Mbps)
13	SQPSK	1/2	1	336	168	693
14	SQPSK	5/8	1	336	210	866
15	QPSK	1/2	2	672	336	1386
16	QPSK	5/8	2	672	420	1732
17	QPSK	3/4	2	672	504	2079
18	16-QAM	1/2	4	1344	672	2772
19	16-QAM	5/8	4	1344	840	3465
20	16-QAM	3/4	4	1344	1008	4158
21	16-QAM	13/16	4	1344	1092	4504
22	64-QAM	5/8	6	2016	1260	5197
23	64-QAM	3/4	6	2016	1512	6237
24	64-QAM	13/16	6	2016	1638	6756

де, N кбнс – число кодованих біт на символ;

N кбнон – число кодованих біт одну несучу;

N ібнс - кількість інформаційних біт на симлів.

2.4 Особливості захисту інформації на канальному рівні стандарту IEEE 802.11Ad

Крім методів кодування та схем модуляції, фізично, дуже важливо розглянути, як реалізується система захисту інформації на канальному рівні (Framework).

Для канального рівня, стандарту 802.11ad, розроблено алгоритм RSNA, який у свою чергу включає кілька протоколів, описаних нижче:

1. TKIP, протокол цілісності тимчасового ключа

2. CCMP, протокол блокового шифрування з кодом.

3. GCMP, режим протоколу GCM та GMAC [16]. Був розроблений, щоб ефективно забезпечувати аутентифікацію та шифрування зі швидкістю 10 гігабіт в секунду, використовує ½ частку операцій AES на відміну від CCMP, розмір MIC становить 16 окетів проти 8 окетів CCMP.

4. BIP, широкомовний протокол цілісності

Використання CCMP обробки розширює оригінальний розмір пакета на 16 октетів, у тому числі 8 октетів розташовуються у заголовку пакета MPDU і 8 октетів — в MIC-області. Заголовок CCMP складається з наступних частин: PN, ExtIV та ідентифікатора ключа. PN - 48-розрядний номер пакета, що є масивом з 6 октетів рис 2.9.

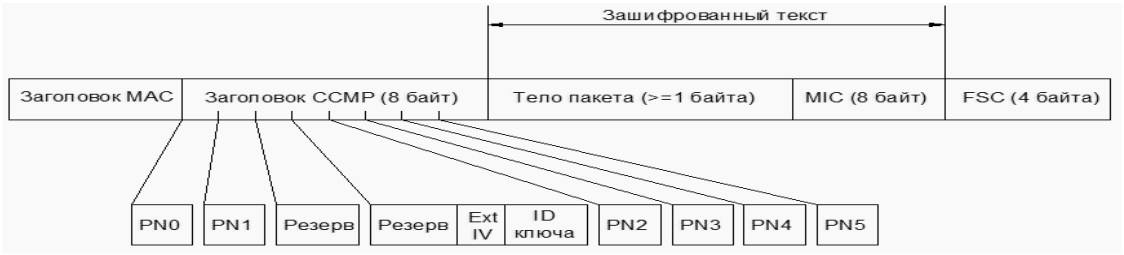

Рисунок 2.9 – Формат пакета CCMP

CCMP перетворює незашифрований текст пакету та інкапсулює їх у пакет даних, використовуючи наступний алгоритм рис. 2.10

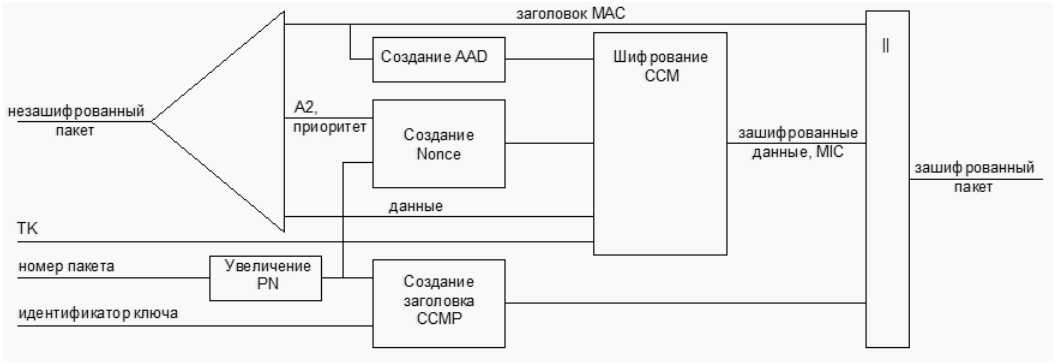

Рисунок 2.10 – Алгоритм роботи CCMP

Збільшується на деякий позитивний номер пакета PN для того, щоб отримувати свій номер для кожного пакета даних так, що номер пакета ніколи не повторюється двічі при використанні одного тимчасового ключа. Варто зазначити, що повторні пакети даних не змінюються під час їх ретрансляції.

Використовуючи поля у заголовку пакета, CCMP створює додаткові автентифікаційні дані (AAD) для CCM. Алгоритм CCM забезпечує шифрування для полів, включених до AAD. Поля заголовка пакета, які можуть бути змінені при його ретрансляції не повинні враховуватися при створенні додаткових автентифікаційних даних і тому вважаються нульовими при створенні AAD.

Складається поле Nonce із номера пакета, адреси A2 та поля пріоритету, яке в існуючій реалізації є зарезервованим, так що його значення має бути рівним нулю.

Новий номер пакета NP та ідентифікатор ключа key ID розміщуються у заголовку пакета MPDU.

Додаткові автентифікаційні дані, поле Nonce безпосередньо дані пакета з використанням тимчасового ключа TK шифруються алгоритмом CCM Цей крок називають CCM originator processing.

Реалізація алгоритму RSNA в системах бездротового доступу стандарту IEEE 802.11ad відбувається одним з чотирьох способів:

1. При використанні IEEE 802.1X в ESS/PBSS, STA забезпечує сумісність алгоритму RSNA з AP/PCP наступним чином (рис. 2.11 а.):

– Система визначає AP / PCP, як сумісні з алгоритмом RSNA від точки доступу AP, пробного відгуку AP, або від PCP точки доступу, пробного відгуку, відповідної кадрової інформації.

– Далі сигнал звертається до відкритої автентифікації у системі ESS.

– STA не викликають відкритих систем автентифікації в PBSS.

– Якщо система вибирає взаємодію з AP або PCP, вона підбирає код під час процесу адаптації і робить вибір.

– Далі система використовує 802.1X IEEE Std-2004 для автентифікації в ESS/PBSS.

– Система задає тимчасової ключів, з допомогою алгоритму генерації ключів, керуючись, протоколом визначальним ключі та його розподіл (TKIP).

– Після пункту 5 система безпеки запам'ятовує узгоджені тимчасові ключі та шифри в MAC і підключає протоколи ЗІ (CCMP, GCMP).

– Якщо вдалося реалізувати керування кадровим захистом, система програмує попарно, тимчасовий ключ і шифр MAC, для захисту від одноразової спрямованої атаки управління кадрами. Також встановлює IGTK та IPN для захисту від групи спрямованих атак управління кадрами.

2. При використанні IEEE 802.1X в IBSS/PBSS для підключення рівної STA необхідно виконати наступну послідовність процедур рис. 2.11 Б:

– У PBSS, якщо система вибирає не синхронізуватися, вона використовує 802.1X IEEE Std-2004 щоб автентифікуватися як рівної STA. У IBSS кожен STA використовує 802.1X IEEE Std-2004 для перевірки автентичності на автентифікацію, з іншими STA. Ось чому в IBSS дві автентифікації відбуваються в один і той же час.

– У IBSS кожен STA встановлює тимчасовий ключ, виконавши алгоритм генерації ключів, використовуючи протокол TKIP. Тому можливо, що два таких алгоритми генерації ключів управління проходять паралельно між будь-якими двома підтримуваними STA.

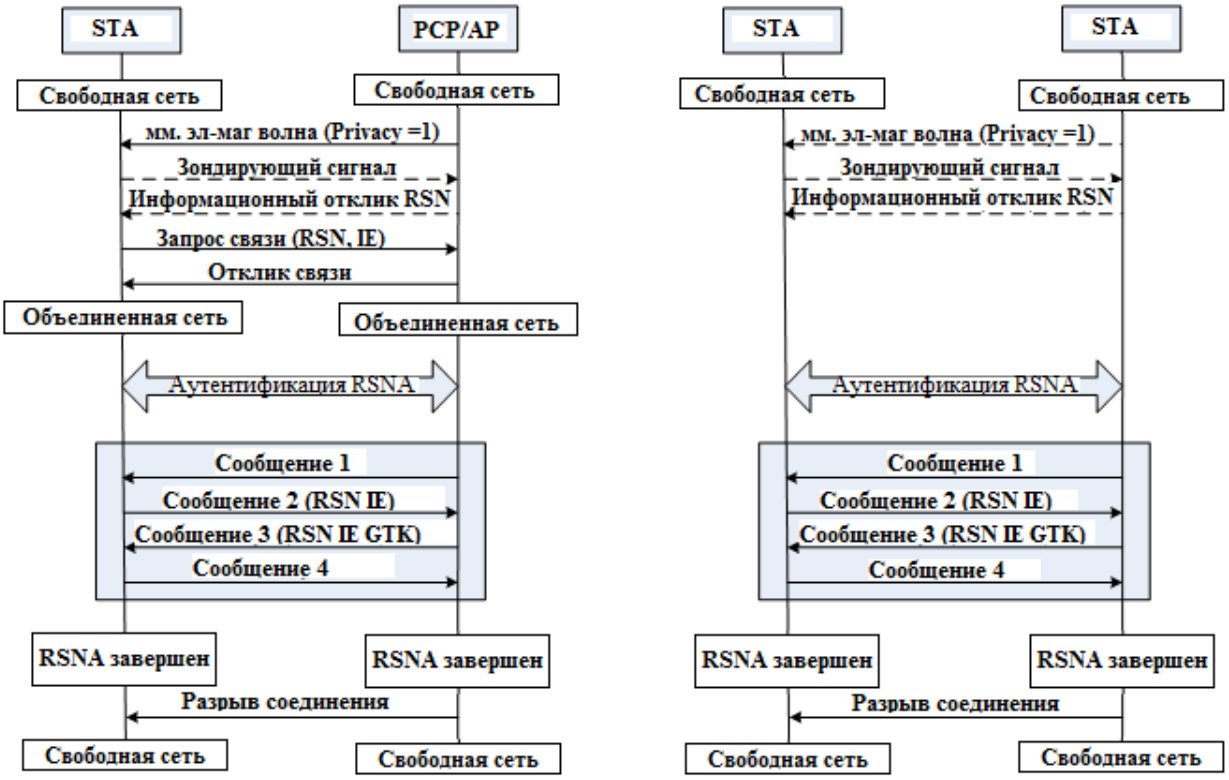

Рисунок 2.11 – Схема реалізації алгоритму RSNA для PBSS

– У PBSS система використовує узгоджені тимчасовий ключ і парний шифр для захисту лінії зв'язку. У IBSS обидва STA, використовують узгоджені часові ключі та парні шифри, для захисту лінії зв'язку.

– Якщо RSNA заснована на PSK в ESS/PBSS, тоді STA встановлює сумісність RSNA з AP/PCP.

– Система встановлює тимчасовий ключ, виконуючи алгоритм управління ключами, і використовуючи протокол, що базується на ключах та їх розподілі (PSK, PMK).

– Він захищає лінію передачі даних, шляхом генерації узгоджених шифрів та встановлених часових ключів у MAC з подальшим викликом захисту.

– Якщо STA реалізувала управління кадровим захистом, система генерує узгоджений попарно шифр і реалізує TK, IGTK та IE.

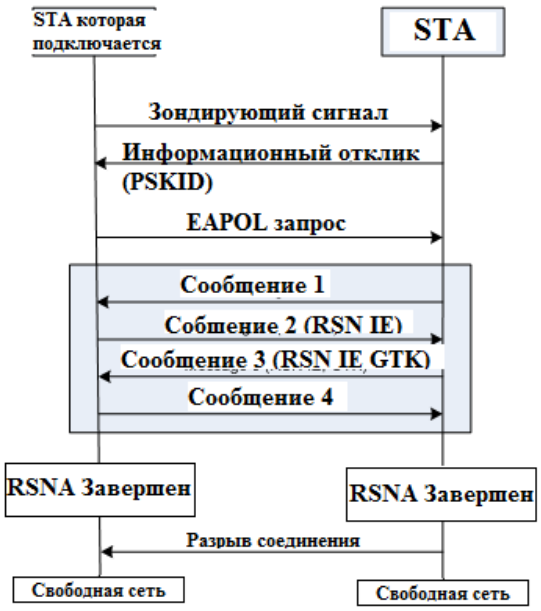

Рисунок 2.12 – Схема роботи алгоритму RSNA для PSK автентифікації в PBSS

3. Якщо RSNA заснована на PSK в IBSS/PBSS, то STA виконує такі послідовність процедур, щоб забезпечити алгоритм RSNA сумісним з STA (рис.2.12):

– STA може реагувати на дані будь-яких приймально-передаючих пристроїв, надіславши зондувальний сигнал або запит кадрової інформації, щоб з'ясувати, чи сумісний пристрій з RSNA.

– Далі сигнал звертається до відкритої автентифікації в системі IBSS.

– У PBSS, система вибирає не синхронізуватися, вона користується процедурами, генерації та розподілу ключів, щоб встановити динамічні ключі та вести передачу шифрів. У IBSS кожна STA використовує процедури, генерації та розподілу ключів, щоб встановити тимчасові ключі та вести передачу шифрів. Важливо звернути увагу, що два рівні STA, можуть слідувати цій процедурі одночасно в IBSS.

– Далі система захищає лінії передачі, програмує узгоджені шифри, встановлює тимчасові ключі і потім, звертається до протоколів захисту.

В данному розділі оглянуто особливості розповсюдженні радіохвиль в діапазоні 60ГГц. В смузі 57–64 ГГц дуже сильне загасання радіохвиль в атмосфері,

особливо при наявності метеорологічних опадів. Проведено огляд на формування відеосигналу високої чіткості та розглянуто формати відео, одним з найпоширеніших форматів кодування є MPEG-2 HD. Модуляція в системі зв’язку IEEE 802.11ad використовується BPSK, QPSK та QAM.

3 ДОСЛІДЖЕННЯ СТАНДАРТУ IEEE 802.11ad

3.1 Критерії оцінки системи зв’язку стандарту IEEE 802.11adc

Для більшості систем зв'язку, ймовірність бітової помилки P_b (BER) використовується, щоб представити надійність системи щодо прийому сигналу та декодування інформації. Наприклад, якщо BER системи $P_b = 10^{-5}$, можна зробити висновок, що це надійна система передачі інформації (звичайно, в залежності від використовуваного стандарту і виду інформації, що передається), а з іншого боку, якщо $P_b = 0{,}5$, то система є явно непрацездатною, так як при прийомі і декодуванні кожного біта інформації ми матимемо 50% ймовірність того, що призводить до некоректної роботи системи. Ця загальноприйнята міра надійності та якості системи зв'язку може привести нас до нового визначення надійності та продуктивності системи зв’язку. Тобто захищеність системи від завад впливає на продуктивність системи в цілому. Оскільки захищеність та продуктивність системи зв’язку тісно зв’язані між собою проаналізуємо захищеність системи.

Оскільки в подальшому як критерій оцінки системи зв’язку ми обрали оцінку захищеності системи в подальшому застосуємо систему відвідного каналу рис. 3.1.

Одним з найважливіших критеріїв якості мультимедійних цифрових систем зв'язку є залежність $P_b = f(E_b / N_O)$ ймовірності появи помилкового біта від відношення енергії сигналу, що припадає на один біт E_b, до спектральної щільності потужності адитивного білого Гаусовского шуму N_0. У цьому випадку передбачається, що єдиним джерелом спотворень сигналу каналу зв'язку є тепловий шум (AWGN). Зручність використання відношення замість відношення потужності сигналу до потужності шуму S/N (SNR), як в аналогових системах зв'язку, полягає в тому, що при такому підході зручніше порівнювати продуктивність цифрових систем на бітовому рівні. Це важливо для цифрових систем, оскільки сигнал може мати довільне n- бітове значення (один символ може кодувати n- біт).

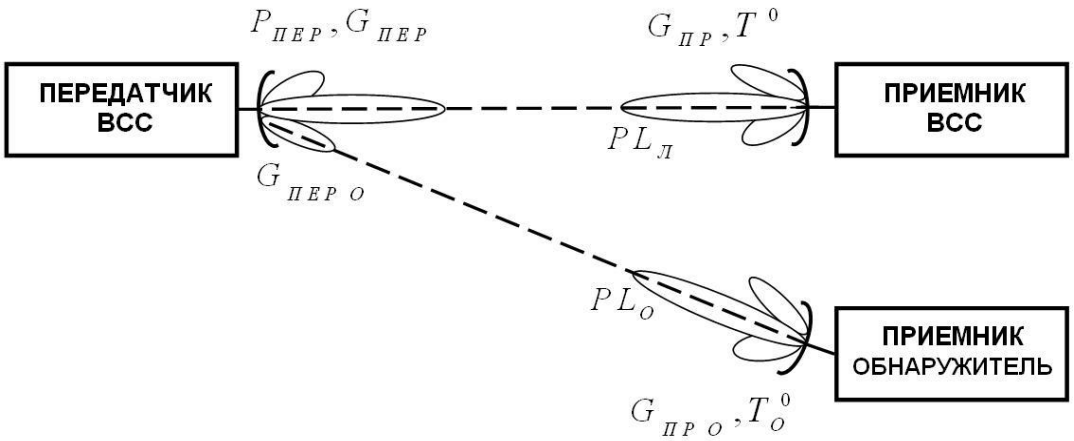

Рисунок 3.1 – Структурна схема відвідного каналу

Тому параметр характеризує відношення сигнал-шум, що припадає на один біт і пов'язаний з наступним співвідношенням:

$$\frac{E_b}{N_0} = \frac{S \cdot T_b}{N/W} = \frac{S/R}{N/W} = \frac{S}{N} \cdot \frac{W}{R}, \tag{3.1}$$

де, T_b – час передачі біта;

N – потужність шуму;

R – швидкість передачі бітів;

W – ширина полоси пропускання

R/W – показує, наскільки ефективно система використовує смугу частот, є спектральною ефективністю системи та виявляється у біт/с/Гц .

Узагальнений вираз ймовірності помилки P_b при когерентному прийомі на фоні перешкод типу AWGN с використанням методу перешкодостійкого кодування М-ічними ортогональними сигналами визначається виразом

$$P_b = \frac{M}{2(M-1)} \cdot \left(1 - \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-x^2/2} \left[Q\left(x + \sqrt{\frac{2E_M}{N_0}} \right) \right]^{M-1} dx \right), \quad (4.2)$$

де, $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-y^2/2} dy$ – гаусовскій інтеграл похибок;

E_M – енергія М-ічного кодового слова.

В окремому випадку, коли М=2 з виразу (3.2) слід відомий вираз бітової помилки для бінарних систем

$$P_b = Q\left(\sqrt{\frac{E_b}{N_o}} \right). \quad (3.3)$$

В табл. 3.1 приведено вирази для ймовірності бітової помилки (для бінарних модуляцій та модуляції QPSK) і ймовірності символьної помилки (для М- арних видів модуляцій).

Для великих відносин E_b / N_0 енергія, що припадає на один символ E_S визначається виразом

$$E_S = E_b \cdot \log_2 M, \quad (3.4)$$

де, $M = 2^k$ – кількість рівноймовірних символів.

Співвідношення між ймовірністю бітової помилки P_b і ймовірністю символьної помилки P_s для ортогональних М-арних сигналів визначається виразом:

$$\frac{P_b}{P_S} = \frac{2^{k-1}}{2^k - 1} = \frac{M/2}{M-1}. \quad (3.5)$$

Для багато фазних сигналів MPSK при використанні коду Грея:

$$P_b \approx \frac{P_S}{\log_2 M}, \ (для \ P_S \ll 1). \tag{3.6}$$

В табл. 1 біноміальний коефіцієнт C_j^M визначається:

$$C_j^M = \frac{M!}{j!(M-j)!}, \tag{3.7}$$

де, $M = 2^k$ – кількість рівноймовірних символів.

Приведені в таблиці 3.1 вирази дозволяють оцінити ймовірності бітової помилки в каналі зв'язку $(P_b)_Л$ відношення сигнал/шум для різних методів передачі інформації в каналі зв'язку, при цьому для забезпечення якості передачі інформації це значення має бути нижчим за певний поріг , який задається вимогами до передачі певного виду інформації (дані, мова, відео тощо), тобто.

$$(P_b)_Л \le (P_b)_{\max}. \tag{3.8}$$

В той же час для забезпечення захищеності каналу зв'язку ймовірність бітової помилки у відвідному каналі $(P_b)_O$ від відношення сигнал/шум повинна бути більшою за певний поріг $(P_b)_{\min}$ (близького до 0,5), тобто.

$$(P_b)_O \ge (P_b)_{\min}. \tag{3.9}$$

Таблиця 3.1 – Вирази для ймовірності бітової P_b та символьної помилки P_S для різних видів модуляції

Вид модуляції	Ймовірність помилки на біт P_b або на символ P_S	Примітка
BASK	$P_b = Q\left(\sqrt{\frac{E_b}{N_o}}\right)$	Для ортогональних сигналів
BPSK	$P_b = Q\left(\sqrt{\frac{2E_b}{N_o}}\right)$	Для антиподних сигналів
QPSK	$P_b = Q\left(\sqrt{\frac{2E_b}{N_o}}\right)$	
BFSK	$P_b = Q\left(\sqrt{\frac{E_b}{N_o}}\right)$	Когерентне виявлення
BFSK	$P_b = \frac{1}{2}\exp\left(-\frac{E_b}{2\cdot N_o}\right)$	Не когерентне виявлення
DPSK	$P_b = 2Q\left(\sqrt{\frac{2E_b}{N_o}}\right)\left[1-Q\left(\sqrt{\frac{2E_b}{N_o}}\right)\right]$	Когерентне виявлення
DPSK	$P_b = \frac{1}{2}\exp\left(-\frac{E_b}{N_o}\right)$	Не когерентне виявлення
MPSK	$P_S(M) \approx 2Q\left(\sqrt{\frac{2E_S}{N_o}}\sin\frac{\pi}{M}\right), M \geq 2$	
DMPSK	$P_S(M) \approx 2Q\left(\sqrt{\frac{2E_S}{N_o}}\sin\frac{\pi}{\sqrt{2}M}\right), M \geq 2$	Не когерентне виявлення
MFSK	$P_S(M) \leq (M-1)\cdot Q\left(\sqrt{\frac{E_S}{N_o}}\right)$	Когерентне виявлення
MFSK	$P_S = \frac{1}{M}\cdot\exp\left(-\frac{E_S}{N_o}\right)\sum_j^M (-1)^j \cdot C_j^M \cdot \exp\left(\frac{E_S}{j\cdot N_o}\right)$	Когерентне виявлення
M-PAM	$P_b = \frac{2(M-1)}{M}\cdot Q\left(\sqrt{\frac{3}{(M^2-1)}\cdot\frac{E_b}{N_o}}\right)$	M – кількість рівнів амплітуди
QAM	$P_b = \frac{2(1-L^{-1})}{\log_2 L}\cdot Q\left(\sqrt{\frac{3\cdot\log_2 L}{(L^2-1)}\cdot\frac{E_b}{N_o}}\right)$	L – кількість рівнів амплітуди в одному вимірі

Виконання рівняння (3.8) та (3.9) забезпечується відповідним енергетичними співвідношеннями (E_b / N_o) в легітимному та нелегітимному каналах, а різниця цих

значень є енергетичним критерієм уразливості системи зв'язку S_Y, який визначається виходячи з наступних співвідношень

$$\begin{cases} (P_b)_{Л} = f\left[\left(\dfrac{E_b}{N_O}\right)_{Л}\right], \\ (P_b)_{O} = f\left[\left(\dfrac{E_b}{N_O}\right)_{O}\right], \\ S_Y = \left(\dfrac{E_b}{N_O}\right)_{Л} - \left(\dfrac{E_b}{N_O}\right)_{O}. \end{cases} \tag{3.10}$$

Розглянемо для прикладу якісну характеристику залежності $P_b = f(E_b / N_0)$, що наведена на рис.3.2

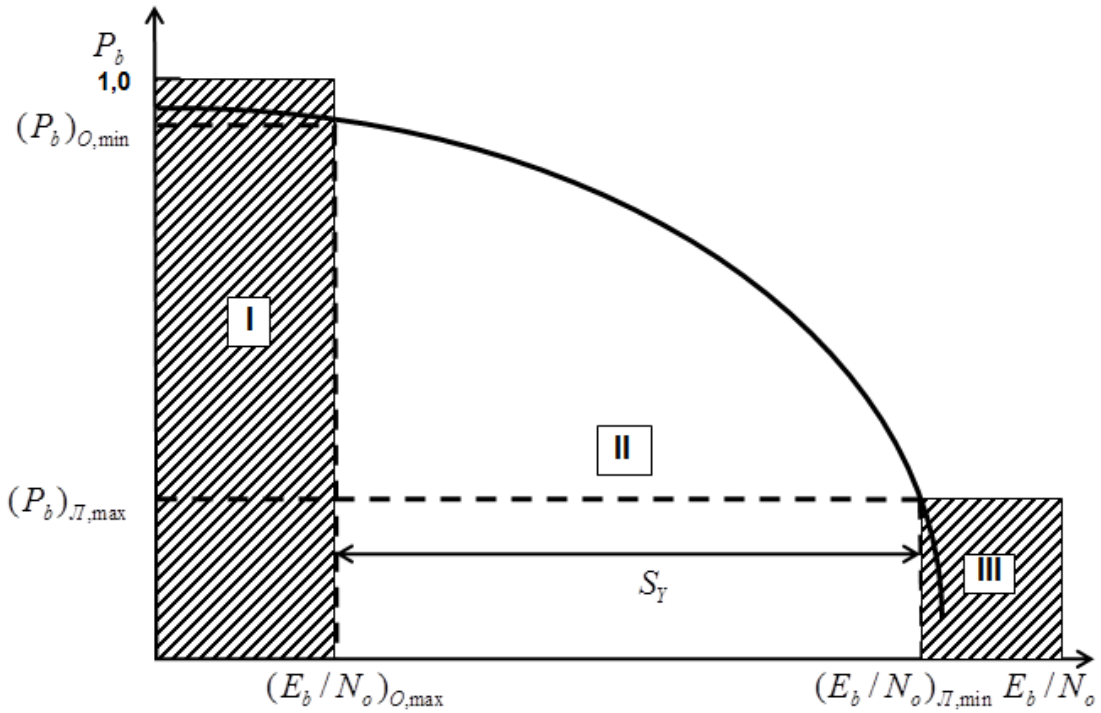

Рисунок 3.2 – Якісна характеристика залежності $P_b = f(E_b / N_0)$

На рис. 3.2 можна виділити три характерні ділянки, які визначають захищеність системи зв'язку. На ділянці I забезпечується повна захищеність каналу

зв'язку від перехоплення повідомлень, на ділянці II захищеність каналу зв'язку може бути забезпечена певними заходами захисту на фізичному рівні, а на ділянці III захист інформації може бути досягнутий в основному тільки методами шифрування інформації. З рис. 3.2 бачимо, що крутіше схил характеристики $P_b = f(E_b / N_0)$, тим менше зона вразливості системи зв'язку, яка оцінюється енергетичним критерієм уразливості системи зв'язку S_Y. Розв'язання задачі мінімізації $[S_Y]_{\min}$, якраз і пов'язане з вирішенням задачі захисту інформації на енергетичному рівні. Використовуючи критерій S_Y можна оцінити вплив тих чи інших характеристик системи зв'язку, параметрів поширення сигналу і методів обробки сигналів фізично на захищеність системи зв'язку. Розглянемо, наприклад, вплив кодування на захищеність системи зв'язку. На рис. 3.3 якісна характеристика залежності $P_b = f(E_b / N_0)$ в залежності від кодування сигналу.

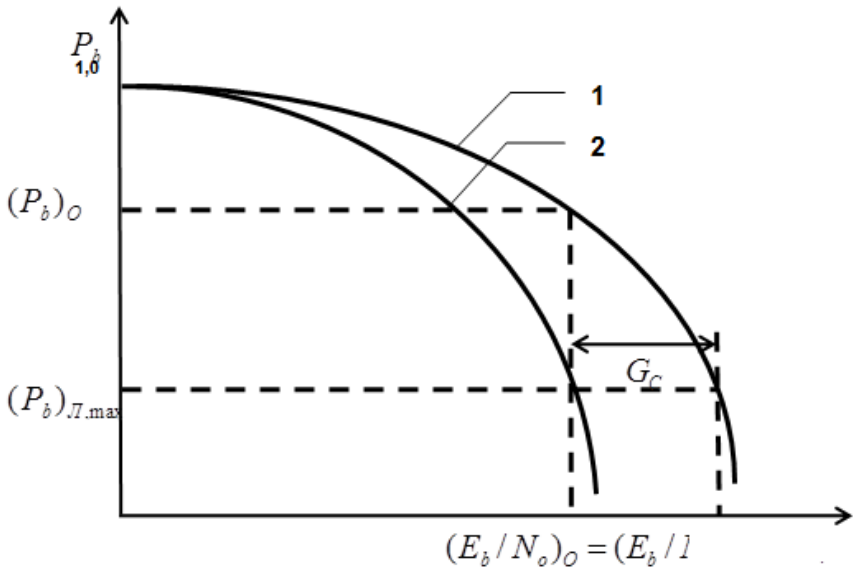

Рисунок 3.3 – Якісна характеристика залежності $P_b = f(E_b / N_0)$ від залежності кодування сигналу

На рис. 3.3 крива 1 відповідає не кодованої передачі сигналів, а крива 2 кодованої. З рис. 3.3 бачимо, що навіть якщо у відвідному і легітимному каналі співвідношення сигнал/шум рівні $(E_b / N_o)_O = (E_b / N_o)_Л$, відсутність параметри про

кодування (крива 1) призводить до значної величини бітової помилки у відвідному каналі в порівнянні з легітимним каналом (Крива 2). Ця величина тим більше чим більше ефективність кодування, визначається величиною коефіцієнта кодування G_C.

В розглянутих вище випадках рівень бітових помилок у каналі зв'язку розглядався як функція перешкод типу теплового шуму. При впливі на канал зв'язку системи зв’язку навмисних перешкод рівень помилок буде функцією суми перешкод теплового шуму і шуму, створюваної постановником перешкод.

$$P_b = f(\frac{E_b}{N_O + J_O}), \tag{3.11}$$

де, J_O – спектральна платність навмисних завад.

В загальному випадку потужність станції навмисних перешкод значно більша за потужність теплового шуму (J_o +N_o). Тоді величина відношення сигнал/перешкода може бути виражена ставленням (E_b / J_o), а відношення енергії біта до спектральної щільності перешкоди, необхідне підтримки заданого рівня помилки в каналі зв'язку $(E_b / J_o)_{TP}$.

Для прикладу розглянемо якісну характеристику залежності $P_b = f(E_b / J_O)$, наведену на рис. 3.4.

Енергетичний запас системи зв'язку проти впливу навмисних перешкод визначається порогом перешкодозахищеності S_{AJ}, який характеризує стійкість системи до спроб її придушення:

$$S_{AJ} = \left(\frac{E_b}{J_O}\right)_{ПР} - \left(\frac{E_b}{J_O}\right)_{TP} \ [дБ], \tag{3.12}$$

де, $\left(E_b / J_O\right)_{ПР}$ – фактичне значення сигнал/шум на вході

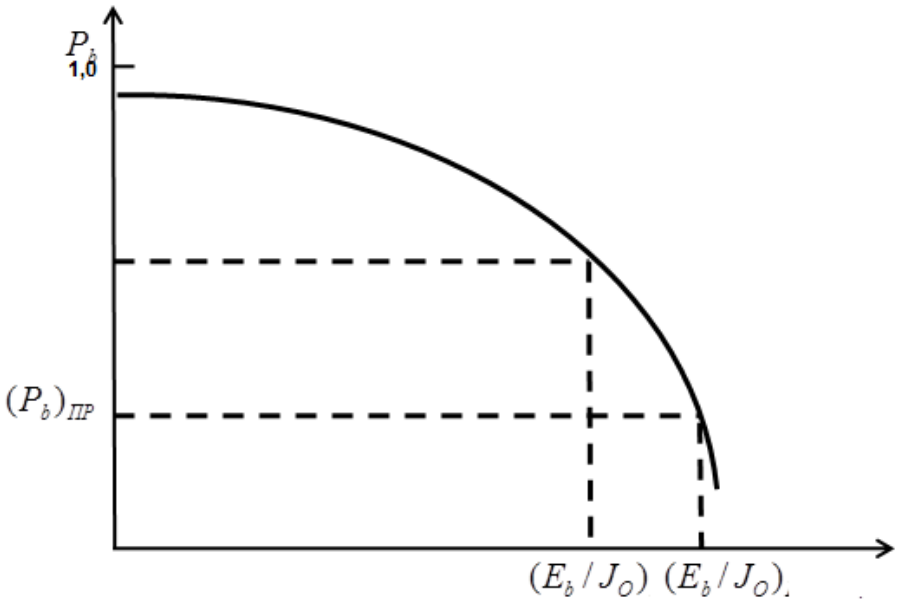

Рисунок 3.4 – Якісна характеристика залежності $P_b = f(E_b / J_O)$

В розглянутих вище випадках показано, що залежність бітової помилки від відношення сигнал/шум $P_b = f(E_b / N_O)$ може бути не тільки мірою оцінки якості легітимного каналу зв'язку при передачі мультимедійної інформації, але мірою оцінки можливостей порушника, що використовує канал відведення для перехоплення інформації і постановки навмисних перешкод.

Даний критерій є найбільш універсальним критерієм оцінки захищеності мультимедійних цифрових систем передачі інформації за наявності відвідних каналів, оскільки дозволяє визначити основні показники захищеності системи зв'язку: скритність та перешкодозахисність.

Враховуючи те, що створювані системи зв’язку орієнтовані на передачу мультимедійної інформації в каналах зв'язку з використанням пакетних протоколів передачі інформації, доцільно використовувати для оцінки показників якості та захищеності систем зв’язку ймовірність пакетної помилки PER (Packet Error Rate), яка пов'язана з параметром бітової помилки BER наступним співвідношенням :

$$PER = 1 - (1 - BER)^L , \qquad (3.13)$$

де, L – довжина інформаційного пакету.

Можна отримати більш простий вираз для пакетної помилки $PER \approx BER^L \approx L \cdot BER$.

В табл. 3.2 наведено деякі дані про стандарти стиснення відеоінформації, що використовуються для реалізації різних відеосервісів у системах зв'язку, та вимоги до показників якості каналів зв'язку, які будуть застосовані для оцінки захищеності як провідних, так і бездротових цифрових систем передачі інформації.

Таблиця 3.2 – Стандарти стиснення відеоінформації та вимоги до пропускної здатності каналу

Стандарт	Розробник стандарту	Пропускна здатність каналу зв'язку *Мбіт/с*	Допустима ймовірність пакетної помилки в каналі зв'язку *PER*
H.261, H.263, H.263+, H.263++	*ITU-T*	*0,064-2,048*	0,01-0,1
MPEG-1	*ISO/IEC JTC1*	*5-10*	-
MPEG-2	*ISO/IEC JTC1*	*3-3,5*	10^{-3}
MPEG-4 ASP	*ISO/IEC JTC1*	*1-2*	-
MPEG-4 AVS, H.264	*ITU-T ISO/IEC JTC1*	*1*	10^{-2}

3.2 Оцінка системи персонального доступу IEEE 802.11ad

Як показано в п. 3.1 критеріями цифрової системи передачі інформації є ймовірності перешкодо захищеності, тобто. ймовірності *BER* або *PER*. Ці величини можуть бути визначені на вході приймача легітимного каналу при впливі генератора перешкод, що знаходиться в нелегітимному відвідному каналі, або на вході приймача виявника, розміщеного у відвідному каналі.

Таким чином, для визначення характеристик перешкодозахищеності та скритності за формулами (3.12, 3.13) необхідно знати енергетичні характеристики сигналу та шуму (або спектральної ефективності) у легітимному та відвідному каналах.

Моделі виміряної ймовірності бітових помилок для випадків різних модуляцій, що несуть сигналу і швидкостей кодування застосовуваного в стандарті бездротового зв'язку IEEE 802.11ad. Спираючись на формули, наведені в табл. 3.1 побудовані графіки залежності BER від SNR (рис. 3.5, 3.6, 3.7, 3.8) для випадків:

- Декілька модуляцій, що використовуються в IEEE 802.11ad:
  - Одна несуча;
  - Канал з OFDM ущільненням.
- Кілька швидкостей кодування (LDPC) стандарту IEEE 802.11ad:
  - Модуляція 16-QAM та одна несуча;
  - Модуляція QPSK та канал з OFDM ущільненням

З приведених нижче графіків бачимо одночасно якість передачі мультимедійної інформації та міру захищеності каналу зв'язку.

Модуляція π/2 BPSK забезпечує найменшу ймовірність бітової помилки при найнижчому співвідношенні сигнал/шум. Тобто забезпечується повна захищеність з одного боку, але в силу простоти модуляції швидкість передачі є мінімальною.

Модуляція π/2 QPSK передбачає підвищення швидкості передачі інформації. Однак забезпечує найменшу BER при середньому із трьох видів модуляцій, співвідношенні сигнал/шум. З цього можна зробити висновок про найкраще забезпечення якості зв'язку та зменшення захищеності каналу, за рахунок більш високих значень SNR за постійної BER.

Модуляція π/2 16-QAM має найбільшу швидкість передачі даних, але водночас має найнижчу захищеність, з точки зору критеріїв, що було наведено вище. Результати BER, при постійному співвідношенні сигнал/шум, виявилися найвищими, що для бездротового каналу зв'язку є недоліком з боку скритності роботи системи.

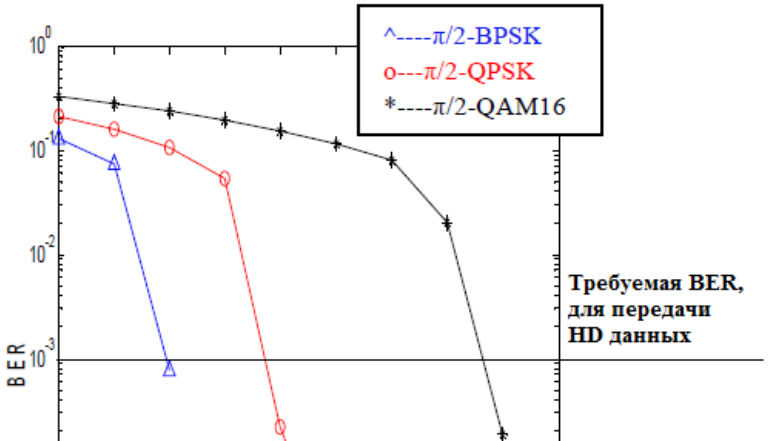

Рисунок 3.5 – Ймовірність бітової похибки для однієї несучої

Розглянемо результати дослідження BER у режимі передачі з кількома несучими (OFDM). В даному випадку використовується модуляція високих порядків.

Модуляція QPSK в даній системі передачі інформації, забезпечує найкращу скритність роботи каналу за рахунок мінімального значення S_y при цьому зменшилась за критерієм стійкості до подавлення тільки модуляції 64-QAM, яка визначає найвищу швидкість передачі та добру стійкість до подавлнення за рахунок високого порога похибки S_{AJ}. Але, якість зв'язку при низькій чутливості приймача та скритність роботи набагато нижча ніж у інших модуляцій, наведених на (рис. 3.6).

Модуляція 16-QAM на даному графіку переважає модуляцію 64-QAM за критерієм надійності передачі даних. Модуляція 16-QAM має середнє значення зони вразливості S_y та найменше значення S_{AJ} у порівняні з модуляцією QPSK та 64-QAM.

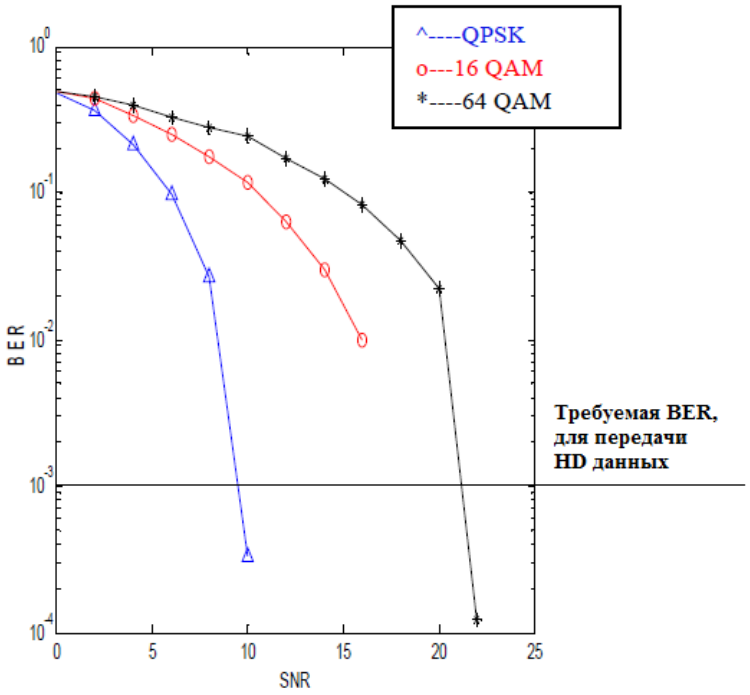

Рисунок 3.6 – Ймовірність бітової похибки для OFDM системи

З метою підвищення порога перешкодозахищеності також були проведені дослідження кодування інформації в стандарті IEEE 802.11ad та отримані результати залежності BER від SNR для різних швидкостей згорткового коду для вище описаних випадків.

На графіку (рис. 3.7) бачимо, що всі три види кодування поводяться однаково по відношенню до значень SNR, це триває до порогу значення SNR=8.5. Після чого всі три криві практично синхронно відносно осі BER зменшуються. Можна зробити висновок, що з даної схеми модуляції оптимальною швидкістю кодування буде становити ½ - LDPC, оскільки саме дана крива забезпечує мінімальну BER за мінімального SNR.

Було проведено вимірювання BER для випадку з OFDM ущільненням та модуляцією QPSK. Отримані результати приведено на (рис. 3.8). З графіків бачимо, що з точки зору захищеності інформації поріг завадозахищеності S_{AJ} та зона вразливість S_y з трьох отриманих результатів найоптимальнішими виявилися у ½-LDPC.

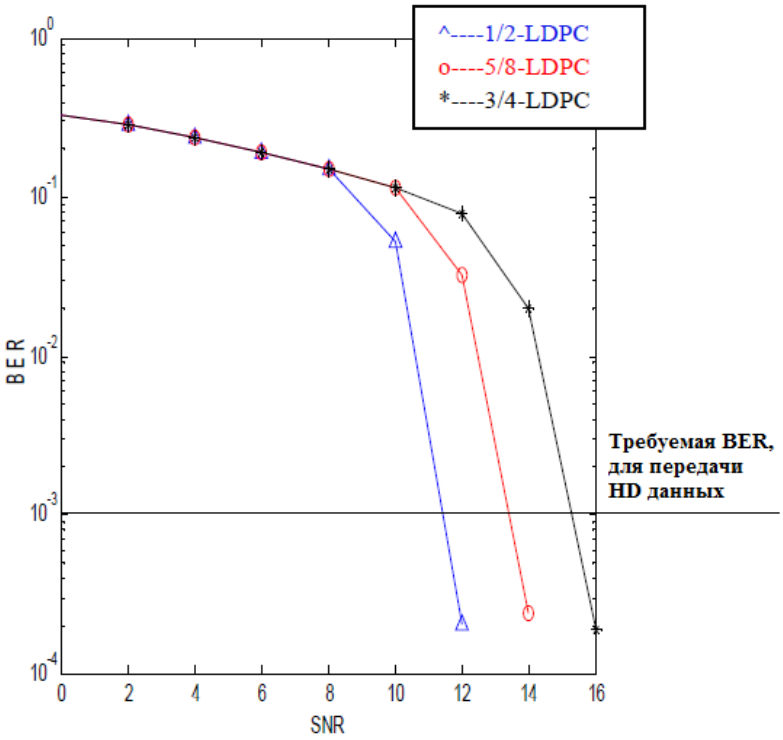

Рисунок 3.7 – Ймовірність бітової похибки для різної швидкості LDPC кодування

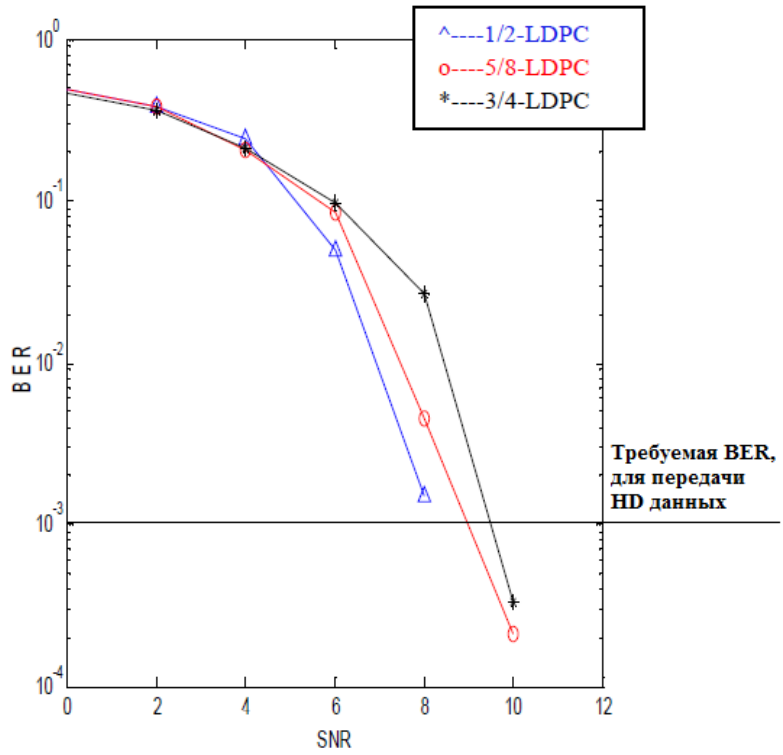

Рисунок 3.8 – Ймовірність бітової похибки для різної швидкості LDPC кодування

У даному розділі була розглянута теорія відвідного каналу, а також проведено дослідження ймовірності бітової помилки залежно від відношення сигнал/шум.

Результати досліджень показали, що при однаковому кодуванні та різних методах модуляції, з однією несучою та декількома несучими, π/2-BPSK забезпечує максимальну продуктивність та мінімальну зону вразливості у першому випадку, а QPSK у другому. Однак найвищий поріг перешкоди опинився у π/2-QPSK у першому випадку і 16-QAM у другому.

Подальші дослідження визначили, що при постійній модуляції та різного кодування для однієї несучої та декількох несучих, 1/2-LDPC забезпечив максимальну продуктивність та стійкість до придушення в обох випадках.

В даному розділі була розглянута теорія відвідного каналу, та поведені дослідження ймовірності бітової похибки в залежності від співвідношення сигнал/шум. За отриманими результатами можна зробити висновок, що при однаковому кодуванні та при різних методів модуляції, з однієї несучої та декількох, модуляція BPSK у порівняні з QPSK, забезпечує максимальну продуктивність та мінімальну зону вразливості. Найбільший поріг завадостійкості має QPSK у порівняні з 16-QAM. При постійній модуляції та використання різного кодування для однієї несучої або декількох, 1/2-LDPC забезпечує максимальну продуктивність та стійкість до завад.

4 ДОСЛІДЖЕННЯ МОДЕЛІВ КАНАЛУ ДЛЯ СИСТЕМИ ЗВ'ЯЗКУ СТАНДАРТУ IEEE 802.11ad

4.1 Модель оцінки продуктивності системи зв’язку стандарту 802. 11ad

Оцінка продуктивності технології реальних умовах представлена на рис. 2.11. Було проведено дослідження технології та побудовано залежність швидкості передачі даних від дистанції передачі. Тому ми використовуємо добре всім відому формулу Шеннона (1), підставивши у ній вираз (2) – ставлення сигнал/шум :

$$C = B \log_2(SNR + 1) \quad (4.1)$$

$$SNR = P_T + G_{\text{пр}} + G_{\text{пер}} - PL_0 - PL(d) - I_L - (KT + 10\log_{10} B - NF) \quad (4.2)$$

де, B – смуга пропускання;

SNR – відношення сигнал/шум;

$G_{\text{пр}}$ та $G_{\text{пер}}$ – коефіцієнт підсилення приймальної та передавальної антени відповідно;

P_T – потужність передатчика;

PL_0 – рівень загаснення за 1 м;

PL(d) – рівень загасання на заданій відстані;

I_L – втрати на апаратурну реалізацію;

NF – рівень шуму;

KT – рівень теплового шуму.

На рис. 4.1 відображено межі швидкості передачі даних в залежності від відстані. За допомогою рис.4.1 можна зробити висновок, що в умовах втрат швидкість 5 Гбіт/с неможливо досягти за будь-якою відстанню. В ситуації ідеальних умов без втрат 5 Гбіт/с, існує в межах трьох метрів, хоча швидкість зменшується набагато швидше, ніж функція часу [7].

Таблиця 4.1 – Параметри системи

P_T – потужність передатчика	10 дБм
Основна частота, fc	60 ГГц
NF– рівень шуму	6 дБ
I_L – втрати на апаратурну реалізацію	6 дБ
N – Термальні втрати	174 дБм/Мгц
B – смуга пропускання	1,5 ГГц
d – відстань	20 м
PL_0– рівень загаснення на 1м.	57,5 дБ

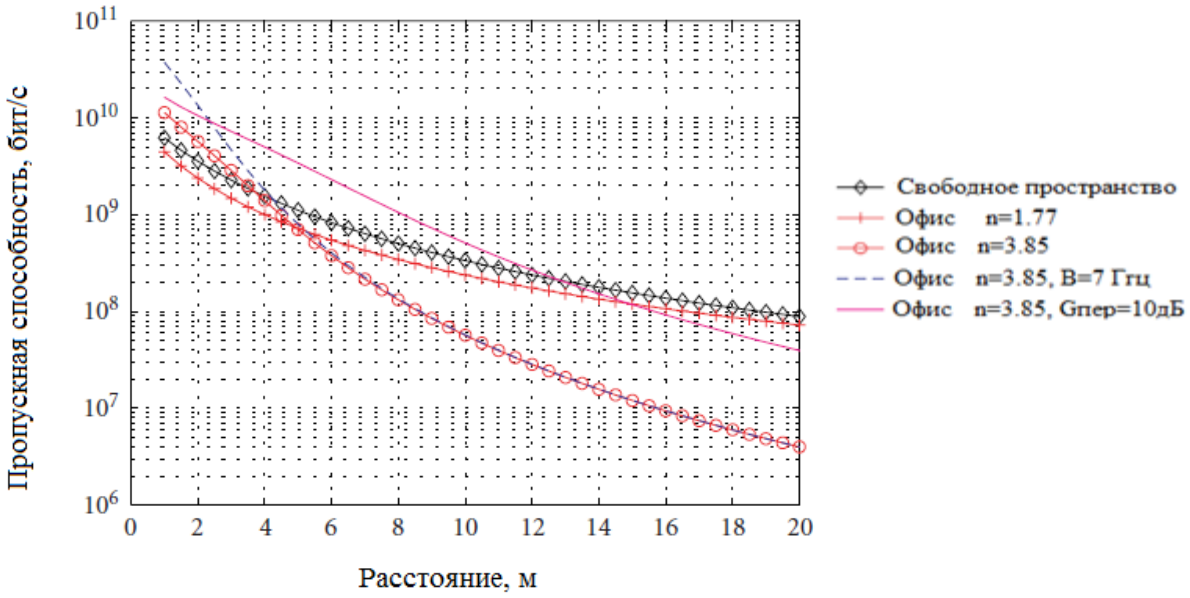

Рисунок 4.1 – Межі Шеннона, у випадку використання IEEE 802.11.ad в приміщені

Щоб покращити пропускну здатність для даних відстаней, необхідно або розширювати смугу пропускання, або вигравати щодо сигнал/шум, або збільшувати обидва параметри. Ці перетворення можна спостерігати на графіку. Зазначимо, що розширення смуги вчетверо дало помітне зростання функції пропускної спроможності для дистанції до п’яти метрів. Також збільшення коефіцієнта посилення ізотропної антени показує важливість використання вузькоспрямованих

антен, оскільки підтримку дуже високої швидкості передачі даних за технологією IEEE 802.11.ad неможливо здійснити при використанні ізотропної антенної конфігурації. [7]

4.2 Модель дослідження необхідного коефіцієнта підсилення антен в діапазоні 60 ГГЦ

На рис. 4.2 відображено графік залежності пропускної здатності від приймальної та передавальної антени [7].

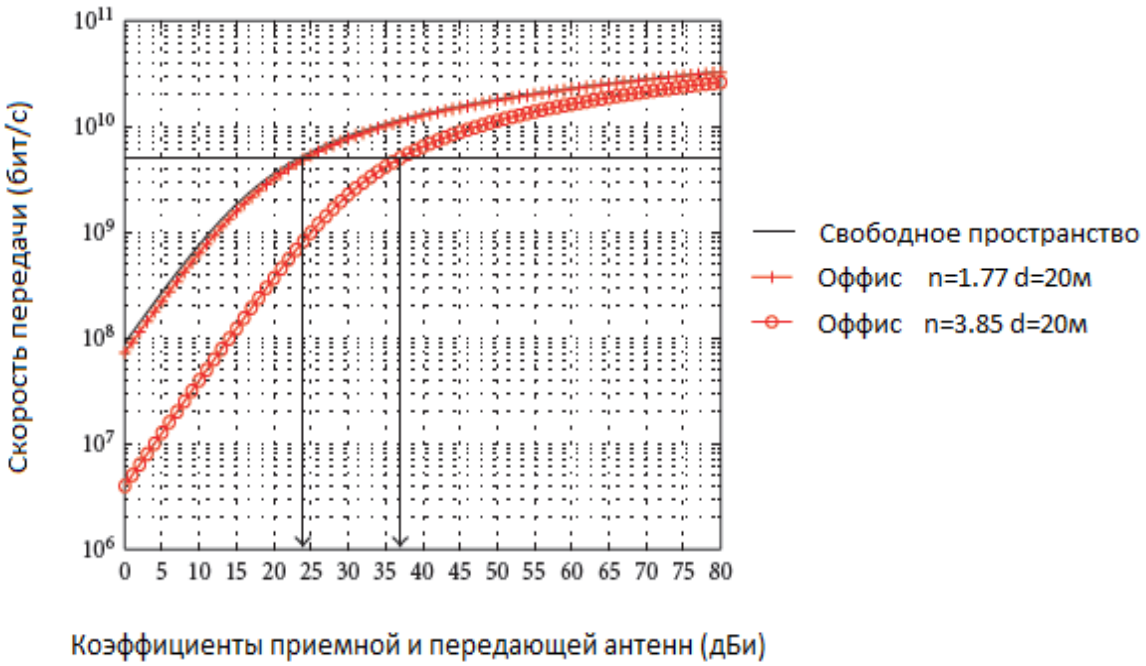

Рисунок 4.2 – Коефіцієнти посилення приймальної та передавальної антен, для досягнення пропускної здатності 5 Гбіт/с

Отже, швидкість передачі 5 Гбіт/с на відстані трансляції 20 метрів досягається при наступних комбінованих коефіцієнтах посилення: 25 (дБі) і 37 (дБі) для випадків без втрат і з втратами відповідно. Вони здадуться реальними значеннями практично. Однак, для досягнення тих же значень пропускної спроможності при

багатопроменевій моделі, необхідно замінювати коефіцієнти на більш високі, для подолання згасання сигналу.

Розрахуємо додаткове підсилення, яке потрібно більш реалістичної моделі поширення хвиль, де канал передачі спотворений багатопроменевим загасанням на відміну від каналу з білим шумом. Щоб полегшити аналіз, використовуємо результати ймовірності бітової помилки при некогерентній (BFSK) модуляції вираз:

$$P_b = \frac{1+K}{2+2k+\overline{\gamma_b}} exp\left(-\frac{K\overline{\gamma_b}}{2+2K+\overline{\gamma_b}}\right) \quad (4.3)$$

де, K та $\overline{\gamma_b}$ є Райсовським, K-фактором і середнім числом відношення енергії переданої за біт до коефіцієнта шуму відповідно.

Вираз (4.3) може бути спрощений у разі Релеєвського завмирання, коли K=0 і одночасно наближено до білого шуму, у разі K→∞.

Якщо, побудувати графік залежності ймовірності бітової помилки від співвідношення сигнал/шум (рис 4.3), для кількох моделей поширення хвиль, стає ясно, що для незакодованих систем, необхідне значення комбінованого коефіцієнта посилення приймальної і передавальної антен, стає недосяжним при заданій ймовірності бітової помилки 10^{-12}. [21]

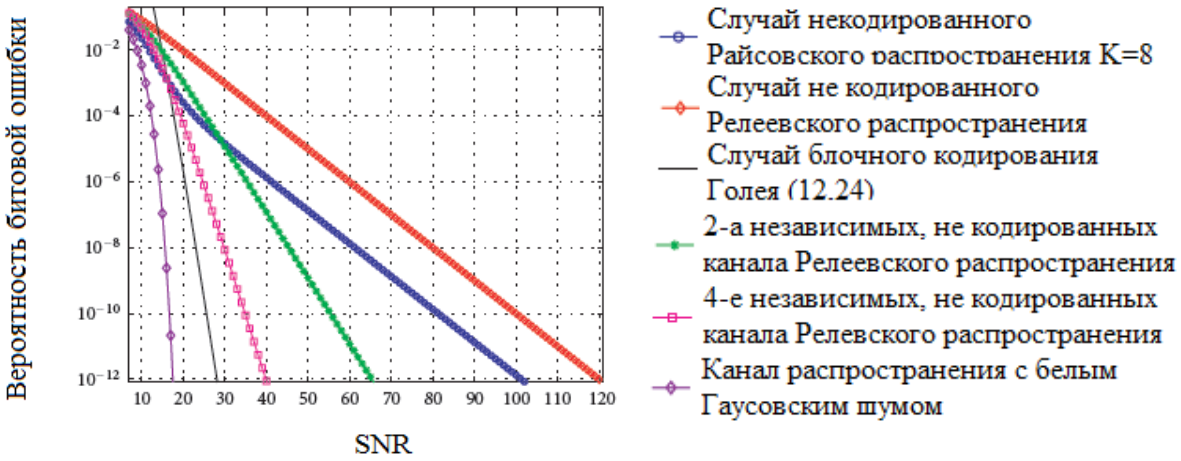

Рисунок 4.3 – Залежність бітової помилки від співвідношення сигнал/шум

Таким чином, кодовані системи, антенні системи високого посилення, повинні бути використані для того, щоб зменшити згасання сигналу, пов'язане з поширенням багатопроменевих хвиль.

Як показано на рис. 4.3 використання рознесеного прийому для випадку двох і чотирьох каналів забезпечує рознесення посилення близько 65 дБ, 80 дБ в порівнянні з одним каналом при BEP 10^{-12}. Однак на практиці ці посилення будуть набагато нижчими, оскільки канал не є незалежним і ідеальним з урахуванням кореляції згасання. Аналогічно, використання канального кодування може поліпшити ймовірність бітової помилки, порівняно з не кодованими випадками. У даній моделі приклад використання коду Голея (24,12) (з відстані Хеммінга Dmin = 8) показує, що ефективність кодування близько 92 дБ в порівнянні з випадком одноканального Релеєвського поширення. Для випадків, що обговорюється вище, можна обчислити запас потужності, у випадку Релеєвського поширення і за умови, що пропускна здатність дорівнює швидкості передачі даних, потужність сигналу обчислюємо як різницю між отриманими Eb/N0 і Eb/N0, що вимагається, при BEP 10^{-12}. Запас потужності для кодованого та рознесеного каналу Релея, а також для каналу з білим шумом представлений нижче:

$$\begin{aligned} M\text{Ray Coded} &= GT + GR - 61, \\ M\text{Ray Div} &= GT + GR - 73, \\ M\text{AWGN} &= GT + GR - 37. \end{aligned} \tag{4.4}$$

Для відеозв'язку високої якості передачі при 60 ГГц, необхідний великий запас лінії зв'язку із-за високого значення затінення та усунення людського ефекту блокування. Експерименти показують, що ефект затінення має логарифмічно нормальний розподіл із нульовим середньоквадратичним відхиленням і досягає 7-10 дБ [17,18]. З іншого боку, ефект блокування людини варіюється від 18-36 дБ [19,20]. Якщо припустити, що необхідний сигнал 10 дБ, то необхідні поєднання Tx-Rx посилення для трьох випадків, наведених вище 71 дБ, 83 дБ і 47 дБ відповідно. Далі ми бачимо, що максимальний коефіцієнт посилення передавальної антени, для якої

дозволена Tx потужність 10 дБм дорівнюватиме 33 дБі. Що змушує посилення приймальної Rx антени бути дуже високим, а саме, 38 дБі, 50 дБі та 14 дБі, відповідно, для трьох розглянутих вище випадків.

4.3 Модель дослідження фазованих антенних решіток

Для одного антенного елемента з коефіцієнтом посилення більше 30 дБі, складно створити надійний канал зв'язку навіть за умов без втрат у діапазоні 60 ГГц. Це пов'язано з людським ефектом блокування, який може легко блокувати та послаблювати вузькоспрямовані сигнали. Щоб подолати цю проблему, необхідно використовувати фазовані решітки або адаптивні решітки, які будуть підбирати і формувати промені по вільних траєкторіях, проходження сигналу. Необхідно встановити скільки ж антенних елементів, потрібно досягнення передбачуваного посилення. Дане посилення відрізняється від посилення решітки, яка підвищує продуктивність з точки зору відношення С/Ш по одній антені. З іншого боку, коефіцієнт посилення антенної решітки можна представити як продукт спрямованості масиву з ефективними антенними решітками. Спрямованість лінійного масиву визначається формулою [27]

$$D = \frac{4\pi}{\iint \left|F_n(\phi,\theta)\right|^2 \sin\theta\, d\theta}, \tag{4.5}$$

де, F_n (φ, θ) є нормованою діаграмою спрямованості одного елемента решітки, змінні φ та θ позначають азимут і кут спрямованості відповідно.

Для лінійної антенної решітки (ЛАР), нормованої діаграмою спрямованості буде вираз (4.6)

$$f_n(\phi,\theta) = \frac{\sin\left((N/2)(kd\cos\theta+\beta)\right)}{N\sin\left((1/2)(kd\cos\theta+\beta)\right)}, \tag{4.6}$$

де, N, d, та β є число елементів антени, антену відстань між двома сусідніми елементами, і фазовий зсув, відповідно.

Ізотропна антенна решітка, з числом елементів до 100-а, здатна домогтися коефіцієнта посилення лише до 23 дБі, що далеко від необхідної цифри раніше розрахованої. Отже необхідні спрямовані елементи поліпшення загального посилення решітки. Як показано на (рис. 4.4), для досягнення посилення 40 дБ, потрібне розташування 10 елементів антенної решітки з коефіцієнтом посилення в 16 дБ на відстані λ / 2.

Багато видів антенних структур вважаються такими, що не підходять для каналу 60 ГГц WPAN / WLAN у зв'язку з деякими вимогами; низька вартість, малі розміри, легка вага, і високий коефіцієнт посилення. Крім того, такі антени повинні забезпечувати роботу з приблизно постійним посиленням та високою ефективністю у широкому діапазоні частот (57-66 ГГц). Важливість формування діаграми спрямованості за 60 ГГц описана вище. Вона може бути досягнута або за допомогою решітки з променями, що перемикаються, або за допомогою фазованих решітки.

У першому випадку система має фіксований набір променів, які можуть бути обрані покриття певної зони обслуговування. Така система може бути реалізована набагато простіше, порівняно з фазованими решітками, для яких потрібна можливість безперервної зміни фазового зсуву між елементами.

Складність полягає в обмеженій кількості елементів. У роботі [21] розроблена 2x2 променева антена з круговою поляризацією на частоті 61 ГГц. Приріст становить близько 14 дБі. Розроблено 4-елементні плоскі грати [22] із середніми втратами перетворення менше 10,6 дБ для чотирьох каналів. Реалізація більшої фазової решітки представляє деякі технічні складності, такі як: більш високе споживання живлення, більш складне управління фазою, сильніший зв'язок між антенами, і так далі. Ці проблеми роблять проектування та виготовлення великих фазованих решіток все більш складним і дорогим.

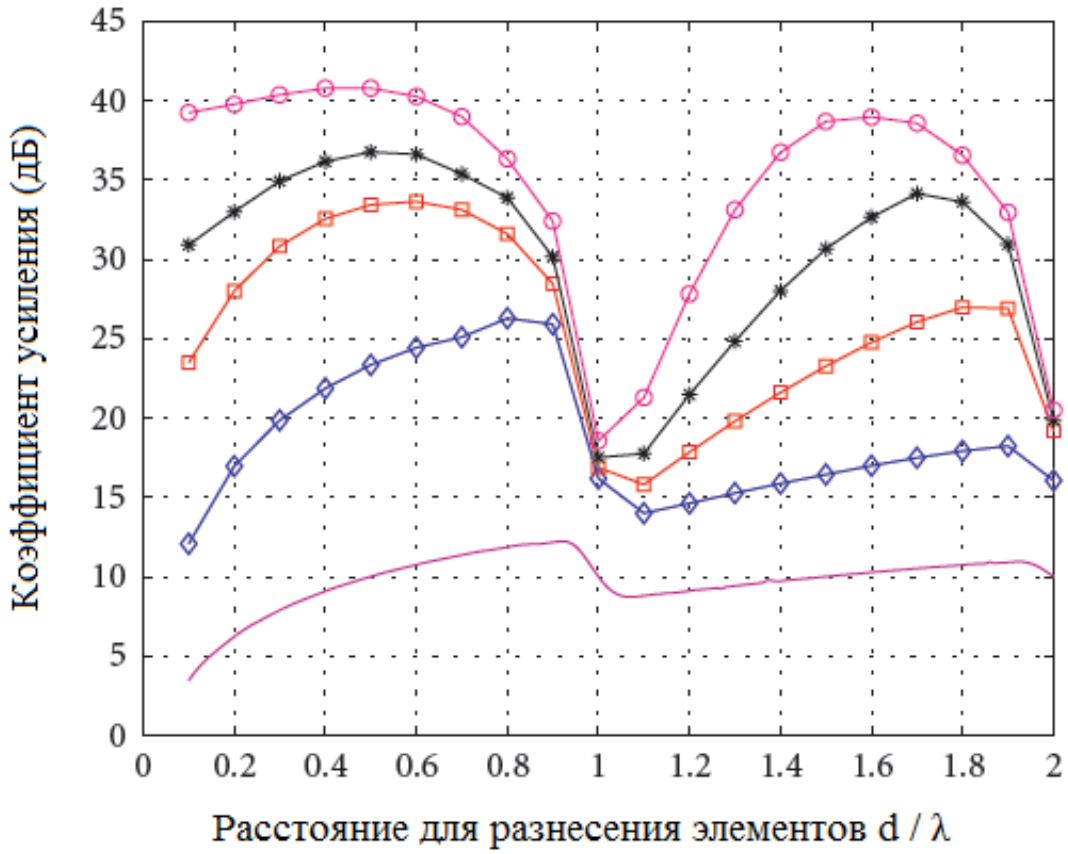

Рисунок 4.4 – Залежність підсилення від антенної відстані

Отже, необхідні додаткові дослідження для розробки решіток меншої вартості, малого розміру, легшої ваги, вищого коефіцієнта посилення та чіткого управління антеною решіткою, які можуть бути інтегровані в електроніку.

Було проведено дослідження моделей продуктивності системи стандарту IEEE 802.11ad, так само було встановлено межі пропускної спроможності 5 Гбіт/с за умов втрат.

Крім цього визначено коефіцієнт посилення антен для якісної передачі інформації, який у свою чергу становив Tx - 33дБі, Rx - 38 дБі в умовах Релеєвського поширення при кодованому каналі зв'язку.

Розрахована модель взаємодії елементів у фазованих антенних решітках. Визначено, що для досягнення необхідного посилення та формування спрямованої ДН антеною системою, потрібно мінімум 10 елементів, розташованих на відстані λ / 2.

В даному розділі було проведено дослідження моделей продуктивності бездротової системи стандарту IEEE 802.11ad, та встановлено межі пропускної здатності 5Гбіт/с в умовах втрат. Встановлено коефіцієнт підсилення антени для якісної передачі даних, що складають Tx – 33дБі, Rx – 38 дБі в умовах Релеєвського розповсюдження при кодуванні каналу. Розрахована модель взаємодії елементів в фазованих антенних решіток, та визначено, що для досягнення необхідних умов та формування діаграми направленості антенної системи необхідно мінімум 10 елементів, що розташовані на відстані полу хвилі λ/2.

ВИСНОВКИ

В першому розділі проведено огляд на сучасні технології WWAN, WMAN, WLAN та WPAN які відрізняються між собою за відстанню дії, використанню протоколів для обміну даних. Розглянуто стандарт IEEE 802.11.ad який є одним з найпоширенішим в наш час.

В другому розділі оглянуто особливості розповсюдженні радіохвиль в діапазоні 60ГГц. В смузі 57–64 ГГц дуже сильне загасання радіохвиль в атмосфері, особливо при наявності метеорологічних опадів. Проведено огляд на формування відеосигналу високої чіткості та розглянуто формати відео, одним з найпоширеніших форматів кодування є MPEG-2 HD. Модуляція в системі зв'язку IEEE 802.11ad використовується BPSK, QPSK та QAM.

В третьому розділі була розглянута теорія відвідного каналу, та поведені дослідження ймовірності бітової похибки в залежності від співвідношення сигнал/шум. За отриманими результатами можна зробити висновок, що при однаковому кодуванні та при різних методів модуляції, з однієї несучої та декількох, модуляція BPSK у порівняні з QPSK, забезпечує максимальну продуктивність та мінімальну зону вразливості. Найбільший поріг завадостійкості має QPSK у порівняні з 16-QAM. При постійній модуляції та використання різного кодування для однієї несучої або декількох, 1/2-LDPC забезпечує максимальну продуктивність та стійкість до завад.

В четвертому розділі було проведено дослідження моделей продуктивності бездротової системи стандарту IEEE 802.11ad, та встановлено межі пропускної здатності 5Гбіт/с в умовах втрат. Встановлено коефіцієнт підсилення антени для якісної передачі даних, що складають Tx – 33дБі, Rx – 38 дБі в умовах Релеєвського розповсюдження при кодуванні каналу. Розрахована модель взаємодії елементів в фазованих антенних решіток, та визначено, що для досягнення необхідних умов та формування діаграми направленості антенної системи необхідно мінімум 10 елементів, що розташовані на відстані полу хвилі $\lambda/2$.

Було проведено дослідження продуктивність бездротової системи зв'язку стандарту IEEE 802.11ad та встановлена пропускна здатність, що складає 5Гбіт/с.

Також встановлено, що при однаковому кодуванні та при різних методів модуляції, з однієї несучої та декількох, модуляція BPSK у порівняні з QPSK, забезпечує максимальну продуктивність. При постійній модуляції та використання різного кодування для однієї несучої або декількох, 1/2-LDPC забезпечує максимальну продуктивність

Завдання на кваліфікаційну роботу виконано в повному обсязі.

ПРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Вишневский, В. М. Беспроводные сети широкополосного доступа к ресурсам Интернета [Текст]/ В. М. Вишневский, 2000. № 10. С. 9 13

2. Шахнович, И. Современные технологии беспроводной связи. [Текст]/ И. Шахнович. - М.: Техносфера, 2004. 288с

3. Wireless II: Ready or Not, Here it Comes [Text]/ Saunders S., Heywood P., Doman A., Bruno L., Allen L; Data Communications. 1999. №. 9. P. 42 68.

4. Рашич, А. В. Сети беспроводного доступа WiMAX: учеб. пособие [Текст]/ Рашич А.В.— СПб.: Изд-во Политехн. ун-та, 2011. — 179 с.

5. Пахомов, С. Анатомия беспроводных сетей [Текст] //КомпьютерПресс.- 2002. №7.175 с.

6. ISO/IEC 26907 Information technology — Telecommunications and information exchange between systems — High-rate ultra-wideband PHY and MAC standard.

7. Nan Guo, Robert C. Qiu, Shaomin S.Mo and Kazuaki Takahashi, '60-GHz Millimeter-Wave Radio: Principle, Technology, and New Results', EURASIP Journal on Wireless Communications and Networking, 2007, Article ID 68253, DOI:10.1155/2007/68253.

8. Buttyґan, L. Securing coding based distributed storage in wireless sensor networks [Text]/ / Buttyґan L. Czap L. Vajda I; Proceedings of the IEEE Workshop on Wireless and Sensor Network Security (WSNS), Atlanta, USA, 2008.

9. Колыбельников, А. ТРУДЫ МФТИ. [Текст] / — 2012. — Том 4, № 2

10. Панюшкин, М. WiMAX – WiRELESS по максимуму. – Мобильные новости, №9 (52), сентябрь 2007, с. 12 – 13.

11. BLUETOOTH SPECIFICATION Version 2.0 + EDR.

12. Hindawi Publishing Corporation [Text]// EURASIP Journal onWireless Communications and Networking. – vol. 2007. - Article ID 78907 10 pages

13. Шахнович, И. Сверхширокополосная связь. Второе рождение?/ И.

Шахнович; ЭЛЕКТРОНИКА: НТБ, 2001, №4, с.8–15.

14. Вишневский, В. Миллиметровый диапазон как промышленная реальность./ В. Вишневский; ЭЛЕКТРОНИКА: Наука, Технология, Бизнес 3/2010, с. 70-72.

15. David, A. The Security and Performance of the Galois [Text]//Counter Mode (GCM) of Operation, INDOCRYPT 2004, Springer-Verlag, 343-355

16. Fiacoo, M. Final report for OFCOM – indoor propagation factors at 17 GHz and 60 GHz [Text]/ August 1998.

17. Anderson, C. In-building wideband partition loss measurements at 2.5 and 60 GHz, [Text]/ IEEE Transactions on Wireless Communications, vol. 3, no. 3, pp. 922–928, 2004.

18. Collonge, S. Influence of the human activity on wide-band characteristics of the 60 GHz indoor radio channel, [Text]/ IEEE Transactions on Wireless Communications, vol. 3, no. 6, pp. 2396–2406, 2004.

19. Smulders, P. Broadband wireless LANs: a feasibility study, Ph.D. thesis, [Text]/ Eindhoven University of Technology, Eindhoven, The Netherlands, 1995.

20. Huang, K-C Millimeter-wave circular polarized beam-steering antenna array for gigabit wireless communications [Text]// Huang K-C , Wang Z.: IEEE Transactions on Antennas and Propagation, vol. 54, no. 2, part 2, pp. 743–746, 2006.

21. A 60 GHz integrated antenna array for high-speed digital beamforming applications, [Text]// in Proceedings of IEEE MTT-S InternationalMicrowave Symposium Digest, vol. 3, pp. 1677–1680, Philadelphia, Pa, USA, June 2003.

22. Определение характеристик готовности и пропускной способности канала связи миллиметрового диапазона волн / А.А. Мерзликин, Д.С. Сальников, А.Н. Битченко, Н.В. Руженцев, А.И. Цопа // Всеукр. межвед. науч.-техн. сб. 2019. Вып. ___. С. 00-00.

23. Оцінка впливу діаграм спрямованості антен на пропускну здатність каналу зв'язку в діапазоні 60 ГГц // А.О. Мерзликин, Д.С. Сальніков, О.І. Цопа // Всеукр. міжвід. наук.-техн. зб. 2019. Вип. ___. С. 00-00.