Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів

Міністерство освіти і науки України
Київський університет імені Борис Грінченка

Бурячок В. Л., Соколов В. Ю.

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ І ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БЕЗПРОВОДОВОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ АПАРАТНОГО РОЗДІЛЕННЯ АБОНЕНТІВ

Монографія

Київ — 2019

УДК 004.056
ББК 32.988-5
Б919

Рекомендовано до видання Вченою радою
Київського університету імені Бориса Грінченка
(протокол від 30.05.2019)

Автори: докт. техн. наук., проф. Бурячок В. Л.
асп. Соколов В. Ю.

Рецензенти: докт. техн. наук., проф. Агеєв Д. В.
докт. техн. наук., проф. Корченко О. Г.
докт. техн. наук., проф. Толюпа С. В.

Б919 Бурячок В. Л., Соколов В. Ю. Методи забезпечення гарантоздатності і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів : Монографія. Київ : КУБГ, 2019. 164 с.

В монографії проведено порівняння науково-методичних підходів щодо забезпечення безпеки в сфері безпроводових технологій (загроз, атак, моделей, шляхів захисту); розроблені технології підвищення рівня захищеності безпроводових мереж в умовах стороннього кібернетичного впливу (методи модуляції сигналів і адаптивного підбору вільних каналів передавання даних, метод підвищення цілісності та доступності з використанням прискорюючих лінз, метод оцінки стану систем захисту безпроводових мереж); розглянуто технічні аспекти забезпечення функціональної безпеки та живучості безпроводових мереж і запропоновано шляхи практичної реалізації заходів із забезпечення безпеки безпроводових технологій.

УДК 004.056
ББК 32.988-5

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ADC – Analog-to-Digital Converter ‘аналого-цифровий перетворювач’
API – Application Programming Interface ‘програмний інтерфейс додатка’
ARM – Advanced RISC Machine ‘поліпшена RISC-машина’
ARP – Address Resolution Protocol ‘протокол визначення адрес’
ASCII – American Standard Code for Information Interchange ‘Американський стандартний код для інформаційного обміну’
AT – від attention ‘увага’
BLE – Bluetooth Low Energy ‘Bluetooth з низьким енергоспоживанням’
BPSK – Binary Phase-Shift Keying ‘двохпозиційна фазова модуляція’
BSD – Berkeley Software Distribution ‘дистрибутив програм Берклі’
CCK – Complementary Code Keying ‘додатковий кодовий ключ’
CDMA – Code Division Multiple Access ‘множинний доступ з кодовим розділенням каналів’
CDP – Cisco Discovery Protocol ‘протокол виявлення Cisco’
CERT – Computer Emergency Response Team ‘команда реагування на комп’ютерні надзвичайні події’
CMS – Content Management System ‘система керування вмістом’
CPU – Central Processing Unit ‘центральний процесор’
CRC – Cyclic Redundancy Check ‘циклічний надлишковий код’
CRM – Customer Relationship Management ‘управління відносинами клієнтів’
CSS – Cascading Style Sheets ‘каскадні таблиці стилів’
DDoS – Distributed Denial-of-Service ‘розподілена атака на відмову в обслуговуванні’
DHCP – Dynamic Host Configuration Protocol ‘протокол динамічної конфігурації вузла’
DNS – Domain Name System ‘доменна система імен’
DoS – Denial-of-Service ‘атака на відмову в обслуговуванні’
DSP – Digital Signal Processor ‘цифровий сигнальний процесор’
EAP – Extensible Authentication Protocol ‘протокол розширеної аутентифікації’
EBCDIC – Extended Binary Coded Decimal Interchange Code ‘розширений двійково-десятковий код обміну інформацією’
EDR – Enhanced Data Rate ‘покращена швидкість передачі даних’
ERP – Enterprise Resource Planning ‘планування ресурсів підприємства’
FCS – Frame Check Sequence ‘послідовність перевірки кадру’
FFT – Fast Fourier Transform ‘швидке перетворення Фур’є’
FHSS – Frequency-Hopping Spread Spectrum ‘стрибкоподібна перебудова робочої частоти’
FPGA – Field-Programmable Gate Array ‘програмована користувачем вентильна матриця’

FTP – File Transfer Protocol ‘протокол передачі файлів’
GCC – GNU Compiler Collection ‘набір компіляторів GNU’
GNU – рекурсивне скор. від “GNU’s not Unix”
GPIO – General-Purpose Input/Output ‘інтерфейс введення/виведення загального призначення’
GPP – General Purpose Processor ‘процесори загального призначення’
HR – Human Resources ‘людські ресурси’
HTML – Hyper Text Markup Language ‘мова розмітки гіпертекстових документів’
HTTP – Hyper Text Transfer Protocol ‘протокол передачі гіпертекстових документів’
I^2C – Inter-Integrated Circuit ‘міжінтеграційна шина’
IaaS – Infrastructure-as-a-Service ‘інфраструктура як сервіс’
IAB – Individual Address Block ‘індивідуальний блок адрес’
ICMP – Internet Control Message Protocol ‘міжмережевий протокол керуючих повідомлень’
IEEE – Institute of Electrical and Electronics Engineers ‘Інститут інженерів з електротехніки та електроніки’
IoT – Internet of Things ‘інтернет речей’
IP – Internet Protocol ‘міжмережевий протокол’
IPsec – IP Security ‘безпека міжмережевого протоколу’
ISM – Industrial, Scientific, and Medical ‘промисловий, науковий та медичний [радіочастотний спектр]’
JSON – JavaScript Object Notation ‘запис об'єктів JavaScript’
LDAP – Lightweight Directory Access Protocol ‘полегшений протокол доступу до каталогів’
LEAP – Lightweight Extensible Authentication Protocol ‘полегшений протокол розширеної аутентифікації’
LPT – Line Print Terminal ‘паралельний порт’
LTE – Long Term Evolution ‘довготерміновий розвиток’
MAC – Media Access Control ‘управління доступом до носія’
MIMO – Multiple Input Multiple Output ‘[система зв’язку] з рознесеними передавальними і приймальними антенами’
NTP – Network Time Protocol ‘мережевий протокол часу’
OFDM – Orthogonal Frequency-Division Multiplexing ‘мультиплексування з ортогональним частотним розділенням каналів’
OLED – Organic Light-Emitting Diode ‘органічний світлодіод’
OSI – Open Systems Interconnection ‘взаємозв’язок відкритих систем’
OUI – Organizationally Unique Identifier ‘унікальний ідентифікатор організацій’
OWASP – Open Web Application Security Project ‘відкритий проект з безпеки веб-додатків’
PaaS – Platform-as-a-Service ‘платформа як сервіс’
PAP – Password Authentication Protocol ‘протокол парольної автентифікації’
PDU – Protocol Data Unit ‘блок даних протоколу’

PEAP – Protected Extensible Authentication Protocol ‘захищений протокол розширеної аутентифікації’
PoE – Power over Ethernet ‘передача електроенергії звитої парою’
POP – Post Office Protocol ‘поштовий офісний протокол’
PSK – Pre-Shared Key ‘попередньо розділений ключ’
PWM – Pulse-Width Modulation ‘широтно-імпульсна модуляція’
QAM – Quadrature Amplitude Modulation ‘квадратурно-амплітудна модуляція’
QPSK – Quadrature Phase-Shift Keying ‘четирьохпозиційна фазова модуляція’
RADIUS – Remote Authentication in Dial-In User Service ‘протокол для реалізації аутентифікації’
RIP – Routing Information Protocol ‘протокол маршрутної інформації’
RPC – Remote Procedure Call ‘виклик віддалених процедур’
RSSI – Received Signal Strength Indication ‘показник рівня отриманого сигналу’
SaaS – Software-as-a-Service ‘програмне забезпечення як сервіс’
SDCC – Small Device C Compiler ‘компактний С крос-компілятор’
SDK – Software Development Kit ‘набір засобів розробки’
SDR – Software-Defined Radio ‘радіо з програмним керуванням’
SER – Symbol Error Rate ‘коефіцієнт символьних помилок’
SMTP – Simple Mail Transfer Protocol ‘простий протокол пересилання пошти’
SNMP – Simple Network Management Protocol ‘простий протокол управління мережею’
SNNR – Signal-and-Noise-to-Noise Ratio ‘відношення суми сигналу і шуму до шуму’
SNR – Signal-to-Noise Ratio ‘співвідношення сигналу до шуму’
SoC – System-on-a-Chip ‘система на кристалі’
SOHO – Small Office / Home Office ‘малий офіс / домашній офіс’
SPI – Serial Peripheral Interface ‘послідовний периферійний інтерфейс’
SQL – Structured Query Language ‘мова структурованих запитів’
SSH – Secure Shell ‘безпечна оболонка’
SSID – Service Set Identifier ‘унікальне найменування безпроводової мережі’
SSL – Secure Sockets Layer ‘рівень захищених сокетів’
STP – Spanning Tree Protocol ‘протокол кістякового дерева’
TCP – Transmission Control Protocol ‘протокол управління передачею’
TI – від “Texas Instruments”
TKIP – Temporal Key Integrity Protocol ‘протокол цілісності тимчасового ключа’
TLS – Transport Layer Security ‘захист на транспортному рівні’
UART – Universal Asynchronous Receiver/Transmitter ‘універсальний асинхронний приймач/передавач’
UDP – User Datagram Protocol ‘протокол датаграм користувача’
USB – Universal Serial Bus ‘універсальна послідовна шина’
UUID – Universally Unique Identifier ‘універсальний унікальний ідентифікатор’
VoIP – Voice over IP ‘голос через IP’

VTP – VLAN Trunking Protocol ‘протокол магістральних віртуальних локальних комп'ютерних мереж’
WASC – Web Application Security Consortium ‘Консорціум безпеки веб-додатків’
WDS – Wireless Distribution System ‘безпроводова розподілена система’
WEP – Wired Equivalent Privacy ‘еквівалент проводової конфіденційності’
Wi-Fi – Wireless Fidelity ‘безпроводова точність’
WiMAX – Worldwide Interoperability for Microwave Access ‘всесвітня сумісність для мікрохвильового доступу’
WLAN – Wireless Local Area Network ‘безпроводова локальна мережа’
WPA – Wi-Fi Protected Access ‘захищений доступ до Wi-Fi’
WPAN – Wireless Personal Area Network ‘безпроводова персональна мережа’
WMAN – Wireless Metropolitan Area Network ‘безпроводова мережа міста’
XSS – Cross-Site Scripting ‘міжсайтове виконання сценаріїв’

ДС – діаграма спрямованості
ЕМЗ – електромагнітна завада
ЗВО – заклади вищої освіти
ІБ – інформаційна безпека
ІТ – інформаційна технологія
ККД – коефіцієнт корисної дії
КП – коефіцієнт підсилення
НВЧ – надвисока частота
НСД – несанкціонований доступ
ОІД – об’єкт інформаційної діяльності
ОЗП – операційний запам’ятовуючий пристрій
ОС – операційна система
ПАРЄ – Парламентська асамблея Ради Європи
ПЗ – програмне забезпечення
ПЛ – прискорююча лінза
САПР – система автоматичного проектування
СУБД – система управління базою даних
СУІБ – система управління інформаційною безпекою
ТБД – точка безпроводового доступу
УКХ – ультракороткі хвилі
ФР – фазовий розподіл

ПЕРЕДМОВА

Події кінця XX – початку XXI сторіччя проходять на фоні трансформації суспільства від постіндустріального до інформаційного. Відбувається бурхливий розвиток та формування глобальної інфраструктури інформаційних технологій (ІТ), що супроводжується інтенсифікацією інформаційних процесів та їх проникненням у всі сфери діяльності людини: соціальну, економічну, політичну тощо, збільшенням залежності приватних осіб, організацій та переважної більшості країн світу від інформаційних систем і мереж, а також підвищенням ступеня їх уразливості від стороннього кібернетичного впливу. Завдяки революції в області інформатизації і комунікацій відбуваються значні зміни у військовій справі. З'являються нові види озброєння, засновані на застосуванні інформаційних та інтернет-технологіях. Такі зміни ведуть до того, що світ стає надто уразливим від появи нових деструктивних впливів – викликів, загроз та фактично неприхованих кібернетичних злочинів в ІТ сфері, які зумовлюють, як результат, збільшення частоти нападів та збитків від витоку інформації.

В світ існує багато технологій і способів передачі інформації між її користувачами. Останнім часом для цього все частіше застосовуються безпроводові мережі, які розгортаються в аеропортах, університетах, готелях, ресторанах, на підприємствах та слугують для підключення користувачів до мережі; об'єднання просторово рознесених підмереж в одну загальну мережу там, де кабельне з'єднання підмереж неможливо або небажано; підключення до мереж провайдерів інтернет-послуг замість використання виділених проводових ліній або звичайного модемного з'єднання тощо.

Разом з цим, поява і активне поширення послуг безпроводового зв'язку на вивели перший план питання забезпечення захисту безпроводових мереж та способи захисту даних в них від проявів стороннього кібернетичного впливу, оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір легкодоступні для перехоплення. Зважаючи, що основи такої діяльності на даний час формалізовані недостатньо, питання щодо забезпечення доступності і цілісності безпроводових мереж (з одночасним підвищенням їх ефективності при передаванні інформації) є надзвичайно актуальними. З цією метою в монографії, по-перше, проведено порівняння науково-методичних підходів щодо забезпечення безпеки в сфері безпроводових технологій, а саме існуючих загроз, атак і моделей побудови безпроводових мереж, а також шляхів реалізації їх захисту. По-друге, розроблені те-

хнології підвищення рівня захищеності безпроводових мереж в умовах стороннього кібернетичного впливу. Потенційним читачам запропоновано модифікований метод оцінки стану систем захисту безпроводових мереж від впливу техногенних та антропогенних загроз, модифіковані методи модуляції сигналів і адаптивного підбору вільних каналів передавання даних в безпроводових мережах, а також метод підвищення цілісності та доступності інформації у безпроводових системах з використанням прискорюючих лінз. По-третє, розглянуто технічні аспекти забезпечення функціональної безпеки та живучості безпроводових мереж й, по-четверте, запропоновано шляхи практичної реалізації заходів із забезпечення безпеки безпроводових технологій.

Монографія відповідає вимогам міжнародної дослідницько-навчальної програми № BTH-90520 «Computer Science: Master Programs for the Swedish Institute Study Scholarships», яка була реалізована в України за фінансованої підтримки Технологічного інституту Блекінґе (Швеція).

Автори висловлюють щиру подяку професорам В. М. Богушу (Національна академія Служби безпеки України), Д. В. Агеєву (Харківський національний університет радіоелектроніки), О. Г. Корченку (Національний авіаційний університет), С. В. Толюпі (Київський національний університет імені Тараса Шевченка) і А. Карлсону (Технологічний інститут Блекінґе), зауваження і поради яких дали можливість суттєво покращити роботу та уникнути ряду помилок.

Розділ 1
НАУКОВО-МЕТОДИЧНІ ПІДХОДИ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В СФЕРІ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ

Кількість точок безпроводового доступу (ТБД) в світі росте з кожним днем, обіцяючи в недалекому майбутньому широкосмуговий вхід в глобальну мережу з будь-якої точки світу. Разом з тим, з розширенням використання безпроводових технологій виникає проблема системного підходу до захисту всієї безпроводової інфраструктури, а не лише окремих ТБД. Проблема ускладнюється легкістю доступу до середовища передавання даних: зловмиснику достатньо бути в зоні покриття, а використання спрямованих антен розширює радіус небезпечної зони до декількох кілометрів. Для системного підходу потрібний універсальний інструментарій, який може легко розширюватися і змінювати свою структуру.

1.1. Аналіз існуючих загроз і атак на безпроводові технології

Дослідженню загроз безпроводовим технологіям та атак, з використанням яких зловмисники отримують до них доступ, присвячено багато публікацій. Так, наприклад, в [1] приведені основні методи побудови і роботи з деревами атак, які дозволяють застосовувати дерева не лише для проводових мереж, а також для безпроводових і змішаних. Автори в [2] і [3] приводять детальний аналіз можливих атак. А в [4] дається спроба систематизації атак на безпроводові мережі, в [5] і [6] надаються перші рекомендації по захисту від несанкціонованого доступу. В [7] приведено статистику використання безпроводових технологій, за якою можна спостерігати динаміку розвитку сучасних безпроводових мереж.

Для систематизації можливих атак на безпроводові мережі і окремі ТБД, як на наш погляд, доцільно використати методику побудови дерева атак. Такий підхід дозволить отримати результати, за допомогою яких можливо побудувати автоматичну систему виявлення атак і потенційних загроз, а також отримати наочний інструментарій спеціалісту з інформаційної безпеки (ІБ) для аналізу і додавання нових видів атак в існуюче дерево. Для побудови дерева атак потрібно систематизувати відомі атаки. Систематизація атак може бути проведена за різними критеріями. Один з них може ґрунтуватися на дослідженні верхнього рівня дерева атак за такими трьома групами: атаки на передавач, приймач та середовище.

1.1.1. Атаки на передавач, приймач і середовище передавання інформації

Головним способом впливу на передавач можуть бути:

атаки типу «відмова в обслуговуванні» в адресу станції (DDoS-атака);

повна імперсоналізація від імені легітимної станції;

приглушення базової станції;

фальсифікація IP-пакетів від імені легітимної станції;

атака підміни ARP-записів.

Атака «відмова в обслуговуванні» в адресу станції полягає у створенні завади при доступі користувача до мережевих ресурсів. Стандартні методи ініціювання DDoS-атаки полягають в передаванні величезної кількості фіктивних пакетів, що заповнюють легальний трафік і призводять до зависання систем.

DDoS-атака може проводитися як на фізичному, так і на канальному рівні. Напад на фізичний рівень у безпроводовій мережі набагато простіший, ніж на фізичний рівень в проводовій мережі, тому що фізичний рівень в безпроводовій мережі – це абстрактне місце навколо точки безпроводового доступу (ТБД). Факт проведення DDoS-атаки на фізичному рівні в безпроводової мережі довести досить важко. Підтвердженням цього може служити, наприклад, створений зловмисником пристрій, що заповнює весь спектр на частоті 2,4 ГГц ЕМЗ (наприклад, за допомогою магнетрона від НВЧ-печі) і нелегальним трафіком (наприклад, використовуючи декілька безпроводових інтерфейсів, які постійно обмінюються даними між собою). На канальному рівні стека OSI атака реалізується менш «грубими» способами (наприклад, імітація чужої MAC-адреси) [8].

Абсолютного захисту від атак не існує, але деякі заходи дозволяють зменшити наслідки їх деструктивного впливу. Серед них – налаштування міжмережевого екрану для відстеження підозрілих пакетів і активності; відстеження топології мережі і блокування «аномальних» даних за маскою, тощо [9].

Повну імперсоналізацію від імені легітимної станції у безпроводовій мережі визначити складніше, ніж в проводовій. SSID (service set identifier) і MAC-адреси ТБД передаються в середовищі у відкритому вигляді. Враховуючи таке, їх досить легко підробити і, як результат, зменшити пропускну здатності мережі, вставляти неправильні фрейми і атакувати алгоритми шифрування, влаштовувати атаки на структуру мережі (наприклад, ARP poisoning для TKIP). Імперсоналізація користувача можлива не тільки у випадку MAC-аутентифікації або застосування статичних ключів, але і при використанні схеми на основі LEAP (lightweight extensible

authentication protocol), EAP-TLS (EAP-transport layer security) або PEAP (protected extensible authentication protocol) [10].

Приглушення базової станції або ТБД надає можливість підмінити її атакуючою станцією. Для тимчасового відключення ТБД часто використовують DDoS-атаку, після чого проводиться підміна на ТБД зловмисника. Абсолютного захисту від подібних атак не існує, але можна зменшити їх ймовірність вибором місця встановлення ТБД [11].

Фальсифікація IP-пакетів від імені легітимної станції (або IP-spoofing) полягає у використанні IP-адреса з викраденої DNS-зони для генерації IP-пакетів, що імітують пакети від вузлів мережі (насправді ж ці пакети можуть використовуватися для крадіжки інформації або злому ресурсів). Існує кілька варіацій атаки: підміна не всліпу (non-blind spoofing) і підміна всліпу (blind spoofing), які відрізняються лише способом отримання доступу до заголовків пакетів [12,13].

Атака підміни ARP-записів (address resolution protocol) побудована на використанні недоліку швидкого з'єднання з легітимною станцією за одним записом IP-адрес без додаткової перевірки MAC-адреси. При підробці пакетів з IP-адресою (в яких буде стверджуватися, що IP належить до MAC-адреси іншого комп'ютера) всі дані, які передаються з використанням скороченого методу визначення комбінацій MAC/IP-адрес, будуть приходити на комп'ютер зловмисника. Таким чином зловмисник може отримати пакети, просто замінюючи в даному локальному кеші комбінації MAC/IP-адрес для будь-яких двох хостів, пов'язаних з фізичною мережею, в якій запущена ТБД [8].

Атаки на приймач поділяються на три підгрупи:

атака «відмова в обслуговуванні» в адресу ТБД;

повна імперсоналізація від імені ТБД;

приглушення клієнтської станції.

Атака «відмова в обслуговуванні» в адресу ТБД та повна імперсоналізація від імені ТБД за принципом дії співпадають з описаними вище для передавача. Різниця полягає лише в напрямку атаки.

Приглушення клієнтської станції дає зловмиснику можливість заміняти клієнта нелегітимною станцією. Також глушіння може використовуватися для відмови в обслуговуванні клієнта або для підміни частини даних [11].

Найбільшу групу атак на середовище можна поділити на дві підгрупи: заповнення ефіру та прослуховування.

Заповнення ефіру проводиться генеруванням навмисних електромагнітних завад (ЕМЗ), які погіршують якість функціонування інформаційної системи. ЕМЗ відрізняються за походженням, структурою і природою. Радіотехнічні, електротехнічні й електронні засоби, що створюють у процесі роботи ЕМЗ, називають джерелами завад (ДЗ).

Відносно класифікації ДЗ ЕМЗ можна розділити на стаціонарні, індустріальні, природні і контактні. Індустріальні ЕМЗ створюються електротехнічними, електронними або радіоелектронними пристроями (крім випромінювання передавача через високочастотний тракт). Як правило, індустріальна завада має імпульсний характер, характеристики якого залежать від типу конкретного пристрою. Контактні ЕМЗ створюються в результаті впливу електромагнітного поля радіопередавача на механічний контакт з перемінним опором, що перевипромінює електромагнітне поле.

За проявом в часі ЕМЗ бувають:

безупинні (рівень не зменшується нижче визначеного граничного рівня довше 1 с);

нетривалі (час дії менше 1 с);

короткочасні (час дії менше 0,2 с);

регулярні (з'являються і зникають через однакові проміжки часу);

нерегулярні;

випадкові стаціонарні (поточний процес має випадкову природу, відбувається без істотних змін математичного очікування завад в часі);

випадкові нестаціонарні (поточний процес має випадкову природу).

По відношенню до ДЗ ЕМЗ бувають:

вузькосмугові;

широкосмугові;

зовнішні (джерело знаходиться поза ДЗ);

внутрішні (джерело знаходиться всередині ДЗ);

міжсистемні (джерело знаходиться в системі, що не відноситься до ДЗ);

внутрісистемні (джерело знаходиться усередині аналізованої системи, але поза ДЗ);

мультиплікаційні (дія на ДЗ змінює комплексну структуру корисного сигналу за рахунок накладення її на комплексну огинаючу деякого випадкового процесу);

симетричні (дія на ДЗ виявляється між двома затискачами джерела індустріальних завад або між фазовими проводами мережі живлення ДЗ);

несиметричні (дія на ДЗ виявляється між виходом джерела індустріальних завад і землі) [3].

Прослуховування, як один із способів атаки на середовище, здійснюється після виявлення безпроводової мережі за рахунок концентрації уваги на потрібному каналі і зборі всіх доступних пакетів окремої мережі. Як і у випадку з несанкціонованим підключенням, зловмисник має можливість аналізувати безпроводові пакети, перебуваючи на значній відстані від ТБД і використовуючи для цього такі програми, як AirMagnet Laptop, Wildpackets Aeropeak, CommView (для ОС Windows) і Ethereal, Kismet, airmon (для ОС Linux), а також додаткові драйвери [4]. Прослуховування поділяється на активне і пасивне.

Одним із методів його реалізації є атака «людина посередині» (man-in-the-middle attack), Вона, як і DDoS-атака, виконується у безпроводових мережах набагато простіше, ніж у проводових. Зазвичай атаки «людина посередині» мають два різновиди: прослуховування і маніпуляція. При прослуховуванні, зловмисник просто прослуховує набір передач між різними хостами, при цьому комп'ютер зловмисника не повинен бути однією зі сторін в з'єднанні. Атаки маніпуляції використовують можливість прослуховування і нелегального захоплення потоку даних з метою зміни його вмісту. Для запобігання атак прослуховування, необхідно проводити шифрування даних на різних рівнях, бажано використовуючи SSH, SSL або IPSEC [8].

Крім того, в застарілих стандартах безпроводових мереж (наприклад, WEP) можуть використовуватися так звані KoreK-атаки, що дозволяють атакуючому отримати ключ після перехоплення набагато меншого обсягу даних, ніж в оригінальному варіанті [14], або «стрибаючі» DoS-атаки (jamming attack), коли зловмисник спочатку аналізує спектр мережі, а потім передає потужний сигнал, щоб створити заваду [15].

1.1.2. Дерево атак на безпроводові мережі та їх характеристики

Для систематизації атак зручно об'єднати відомі атаки в єдину схему – дерево атак, зображену на рис. 1.1.

При цьому головну увагу зосередимо на атаках, спрямованих на середовище – безпроводову мережу. Несанкціоноване прослуховування мережі і внесення змін в її роботу можна змоделювати за допомогою мережі Петрі-Маркова (рис. 1.2), де s_1 – готові до роботи ТБД і клієнт; s_2 – зловмисник, готовий для атаки; t_1 – передача даних між ТБД і клієнтом, перехоплення даних; s_3 – дані отримані і вибраний вид атаки; t_2 – проведення атаки; s_4 – успішна атака.

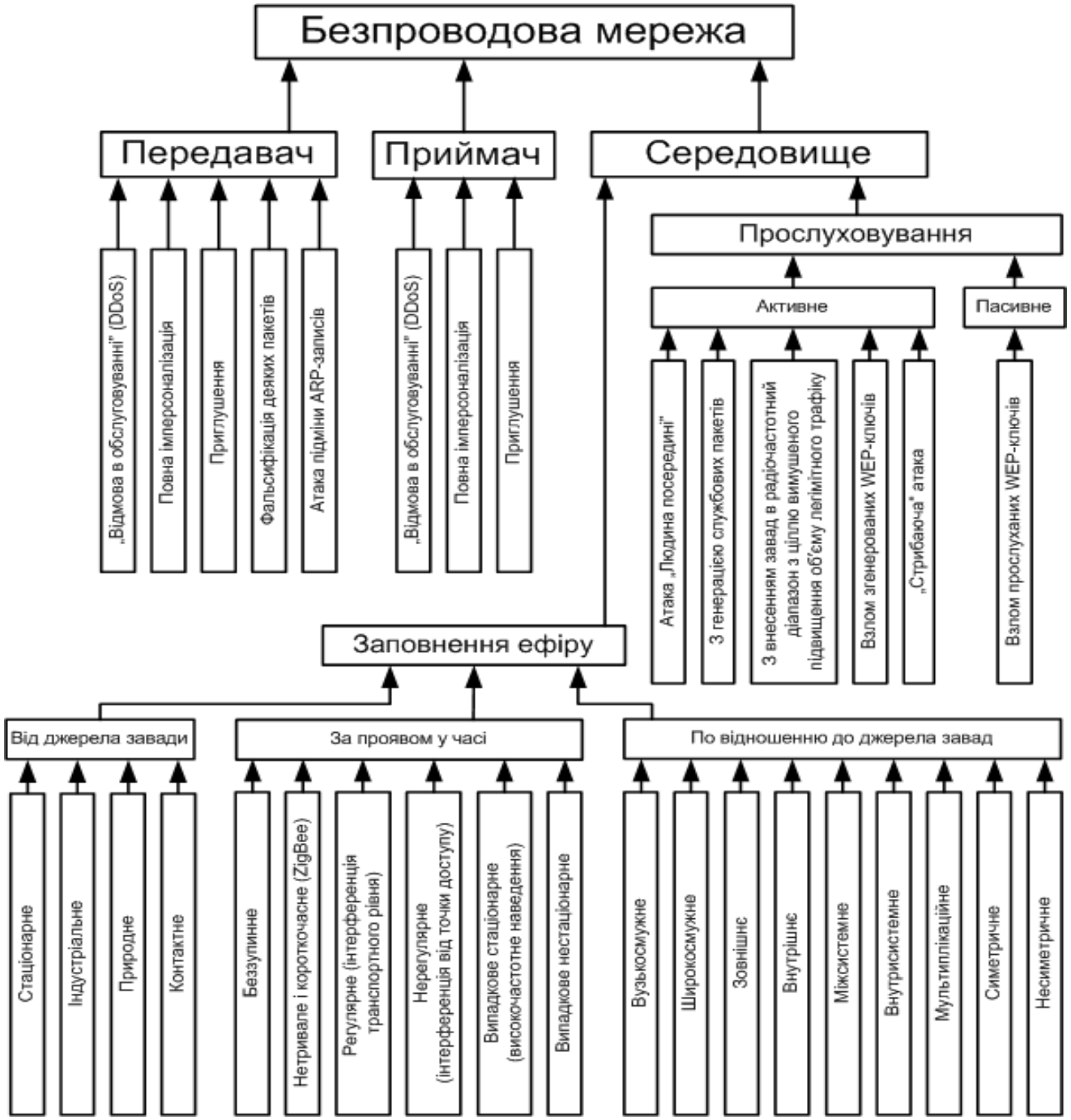


Рис. 1.1. Дерево атак на безпроводову мережу

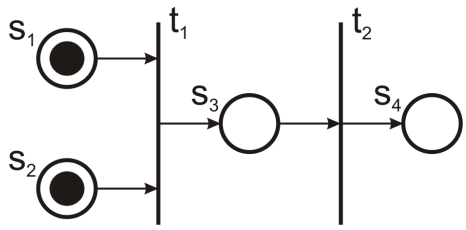


Рис. 1.2. Схема атаки на безпроводову мережу

Елементи матриці, що визначають логічні функції реагування мережі від початку передавання даних до проведення атаки, мають вигляд:

$$v_{S_1 t_2} = \begin{array}{c|cc} & t_1 & t_2 \\ S_1 & 1 & 0 \\ S_2 & 1 & 0 \\ S_3 & S_1 t_1 | S_2 t_1 & 1 \\ S_4 & 0 & 1 \end{array} \quad (1.1)$$

Застосовуючи пуассонівське наближення [16], отримаємо середній час t переміщення по мережі Петрі-Маркова із початкової позиції до кінцевого переходу та ймовірність цього переміщення:

$$P_{\text{a}}(t) = 1 - e^{-t_{\text{a}}/\tau}, \quad (1.2)$$

де t – середній час переміщення по всій мережі.

Залежність ймовірності реалізації атаки від часу для безпроводової мережі показана на рис. 1.3.

За час атаки передані дані будуть втрачені або будуть визнані сумнівними. В табл. 1.1 показана мінімальна кількість даних, яка буде втрачена під час атаки, за умови, що передаються тільки службові дані (кількість службових даних отримана, виходячи з частоти передавання службових пакетів 10 Гц, довжини пакета 110 біт для 802.g11 і 228 біт для 802.11n, а також середнього часу атаки).

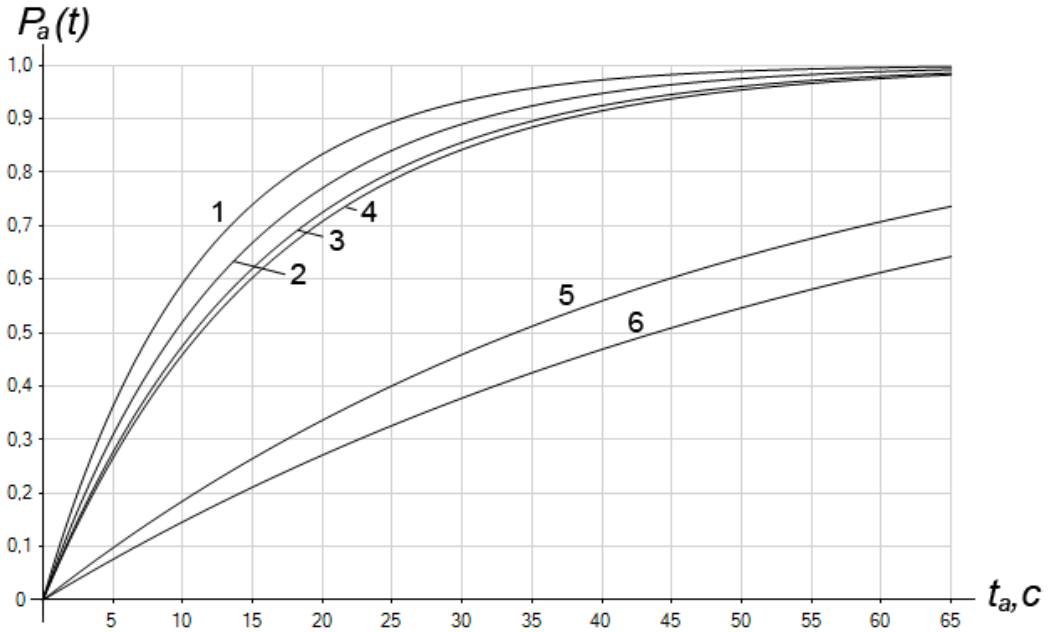


Рис. 1.3. Залежність ймовірності реалізації атаки від часу:
1 – DDoS-атака; 2 – фальсифікація деяких пакетів; 3 – підміна ARP-записів; 4 – повна імперсоналізація; 5 – сканування мережі і приглушення; 6 – злом ключів

Таблиця 1.1

Мінімальні втрати даних при різних атаках

Атака	Середній час переміщення, с	Кількість службових даних за час атаки, кБ	
		802.11g	802.11n
DDoS-атака	11,15	1,5	3,1
Повна імперсоналізація	16,25	2,2	4,5
Сканування мережі і приглушення	48,80	6,6	13,6
Фальсифікація деяких пакетів	13,60	1,8	3,8
Підміна ARP-записів	15,50	2,1	4,3
Злом WEP-ключів	63,25	8,5	17,6

Якщо передаються пакети з даними, то кількість втрачених даних може відрізнятися на кілька десятків або десятків тисяч порядків.

Якщо в комерційній безпроводовій мережі присутня система моніторингу і системний адміністратор відслідковує стан мережі в реальному часі, то можна визначити відношення ймовірностей атаки $P_{\text{а}}$ і захисту $P_{\text{з}}$:

$$P_{\text{а}} + P_{\text{з}} = 1. \tag{1.3}$$

В [16] ймовірність визначається вартістю атаки і засобів захисту:

$$P_{\text{з}} = \frac{q_{\text{з}} \cdot C_{\text{з}}}{q_{\text{з}} \cdot C_{\text{з}} + q_{\text{а}} \cdot C_{\text{а}}}, \tag{1.4}$$

де $C_{\text{з}}$ і $C_{\text{а}}$ – вартість засобів захисту і атаки; $q_{\text{з}}$ і $q_{\text{а}}$ – вагові коефіцієнти, які визначаються через час реакції на атаку $t_{\text{реак}}$; t – середній час переміщення дій зловмисника у мережі:

$$q_{\text{з}} = q_{\text{а}} \frac{\tau}{t_{\text{реак}}}. \tag{1.5}$$

За відношенням часу реакції до часу атаки побудовані криві (рис. 1.4). Виходячи з (1.3) і (1.4), при близькій вартості засобів захисту і атаки маємо:

$$P_{\text{з}} = \frac{\tau \cdot C_{\text{з}}}{\tau \cdot C_{\text{з}} + t_{\text{реак}} \cdot C_{\text{а}}} = \left. \frac{\tau}{\tau + t_{\text{реак}}} \right|_{C_{\text{з}} \approx C_{\text{а}}}. \tag{1.6}$$

З (1.2), (1.3) і (1.6) маємо:

$$t_{\text{реак}} < \tau \left(e^{t_{\text{а}}/\tau} - 1 \right). \tag{1.7}$$

З кривих видно, що при автоматичному виявлені атаки відношення має майже лінійну характеристику (час реакції не перевищує 5 с). Після розкладення (1.7) в ряд Тейлора $t_{\text{реак}} \le \sum_0^{\infty} \frac{t_{\text{а}}^{i+1}}{i! \tau^i}$ і виборі першого члену ряду $t_{\text{реак}} \le t_{\text{а}}$ отримуємо лінійне співвідношення.

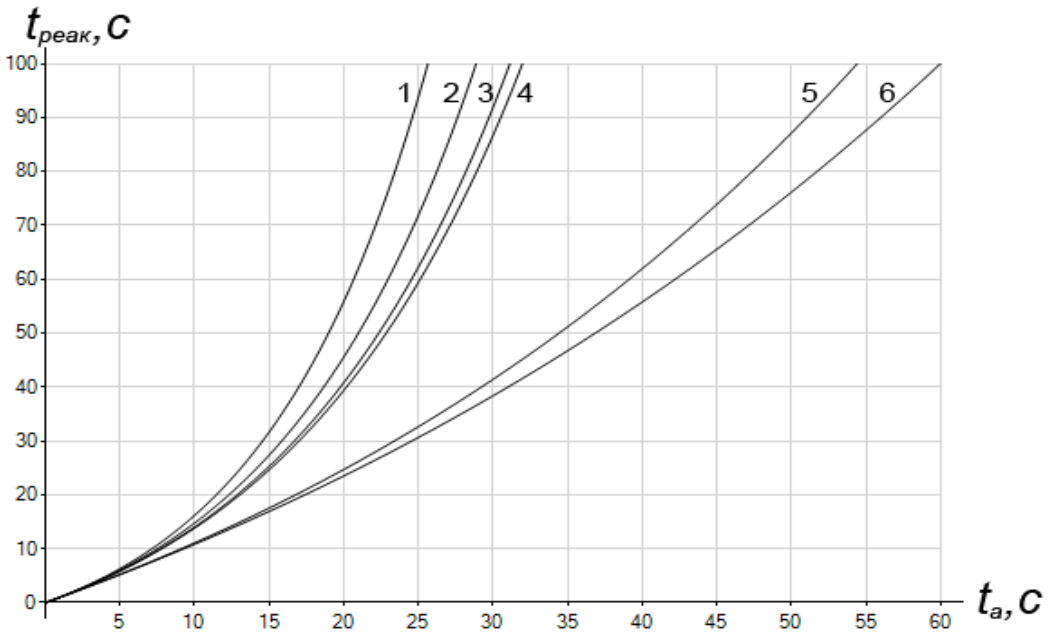


Рис. 1.4. Залежність ймовірності реалізації атаки від часу:
1 – DDoS-атака; 2 – фальсифікація деяких пакетів; 3 – підміна ARP-записів;
4 – повна імперсоналізація; 5 – сканування мережі і приглушення; 6 – злом ключів

Враховуючи, що час реакції при виявленні атаки адміністратором становить близько хвилини (похибка наближення не перевищує 5%, як показано на рис. 1.5), отримуємо ступеневу функцію [17]:

$$t_{\text{реак}} \le \frac{1}{24\tau^3} t_{\text{а}}^4 + \frac{1}{6\tau^3} t_{\text{а}}^3 + \frac{1}{2\tau} t_{\text{а}}^2 + t_{\text{а}}. \qquad (1.8)$$

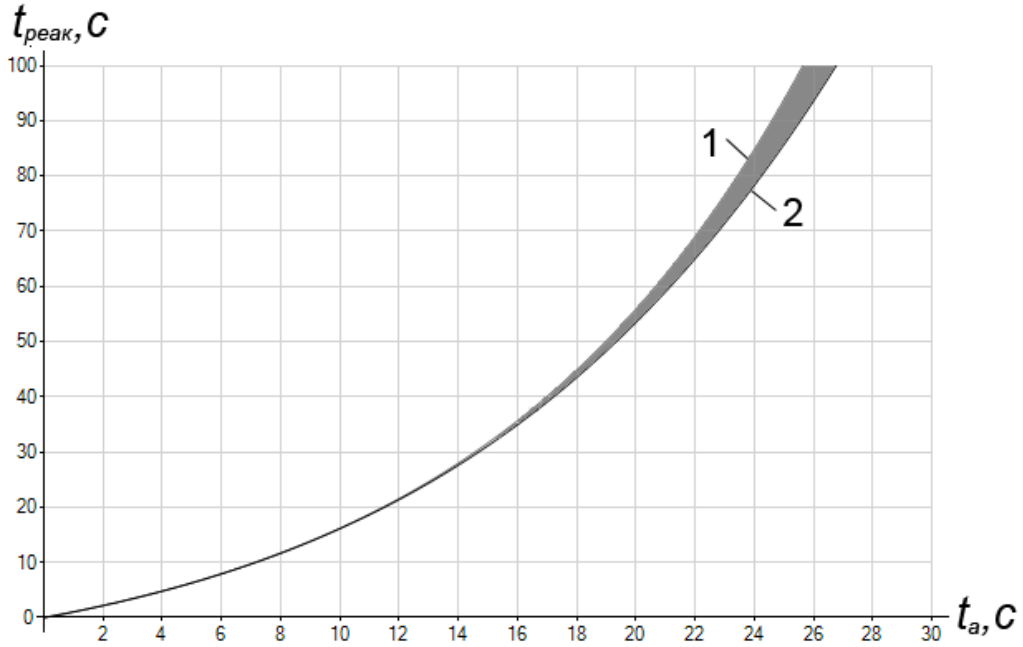


Рис. 1.5. Залежність ймовірності реалізації атаки від часу:
1 – показникова крива; 2 – наближена ступенева крива

1.1.3. Моделі та критерії загроз у безпроводових технологіях

На системи безпроводового зв'язку постійно діє низка загроз: природні, техногенні, людські навмисні і людські ненавмисні. Природні (космічне випромінювання, іонізація іоносфери) і техногенні (випромінювання радіоапаратури) за результатом дуже схожі: вони викликають завади у каналах зв'язку. Навмисні загрози набувають все більшого розповсюдження і проявляються, у вигляді порушень безпеки: введення в систему шкідливих кодів (комп'ютерних вірусів). Людські ненавмисні загрози можна розглядати як форс-мажорні, тому вони дуже важко піддаються узагальненому опису [18,19].

З першого погляду здається, що проблему захисту від порушень безпеки можна вирішити, захищаючи саму інформацію, що передається мережею. Але така загроза зумовлена використанням обчислювальної техніки в апаратурі ліній зв'язку, яка безпосередньо задіяна в передачі даних, наприклад, мультиплексорів і демультиплексорів, комутаторів, маршрутизаторів, підсилювачів, регенераторів, пристроїв керування тощо. Таким чином, мова йде не тільки про цілісність інформації, а і про працеспроможність системи безпроводового зв'язку в цілому [18].

Це вимагає побудови раціональної моделі загроз. Наведемо декілька підходів до їх формування.

Модель «зомбування». Порушення безпеки за такою *моделлю «зомбування»* мають чітко відокремленні стадії, як показано на рис. 1.6: поверхневе вивчення (рекогносцирування), глибоке вивчення (сканування каналів зв'язку), доскональне вивчення (складання карти), отримання доступу до операційної системи (ОС), розширення повноважень, «зомбування» ОС, маніпуляції з інформацією і видалення слідів злочину.

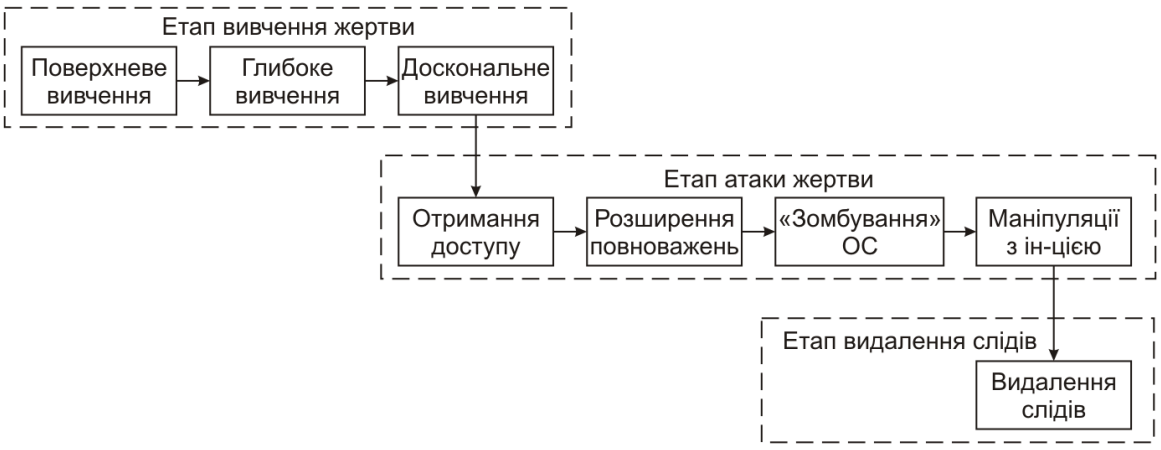


Рис. 1.6. Етапи моделі «зомбування»

«Зомбування» системи проходить за допомогою шкідливого коду, який вводиться в ОС для віддаленого доступу. Після цього з «зомбованої» ОС проводиться наступна атака і додавання нових робочих станцій до «зомбі»-мережі (так звана, ботнет, від англ. *botnet* від robot і network). Після закінчення атаки видаляються сліди перебування зловмисника в системі.

Для моделі «зомбування» ефективність E [$с^{-1} \cdot грн.^{-1}$] є:

$$E = \frac{n \cdot s}{t \cdot C}, \tag{1.9}$$

де n – кількість потенційних серверів, на яких реалізована атака; s – кількість комп'ютерів, які безпосередньо працюють з одним сервером; t – час прибування системи в «зазомбованому» стані; C – вартість атаки: вартість написання ботнету, додаткові витрати на введення і розповсюдження програного коду, додаткові витрати [19].

Модель «чорної скриньки». Якщо розглядати порушення безпеки C_n у вигляді множини підмножин, які характеризують об'єкт:

$$C_n = \{X_n, Y_n, D_n, W_n\}, \tag{1.10}$$

де X_n – підмножина зловмисників, Y_n – підмножина об'єктів, D_n – підмножина втрат, W_n – підмножина зовнішніх дій.

Модель атаки буде у вигляді «чорної скриньки» (див. рис. 1.7): на вхід об'єкта Y_n приходить зовнішні данні і команди W_n, а також дії зловмисника X_n, після чого виникає в результаті відповідь D_n (з втратою або без – в залежності від успішності атаки [20].

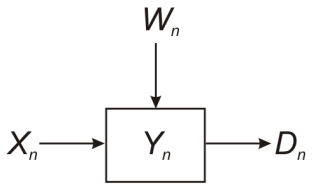


Рис. 1.7. Схема моделі «чорної скриньки»

1.1.4. Методи оцінки загроз у безпроводових мережах

Основними методами оцінки загроз у безпроводових мережах, як правило, є:

1. Метод оцінки ймовірності відмови в обслуговуванні.
2. Метод оцінки очікуваного збитку від загрози.
3. Метод оцінки стану систем захисту телекомунікаційних мереж від впливу техногенних та антропогенних загроз.

Метод оцінки *ймовірності відмови в обслуговуванні* (в результаті стихійного лиха, форс-мажору, повній або частковій втраті даних, несанкціонованого доступу тощо). Він дозволяє отримувати результати у вигляді шкали оцінок потенційних загроз і їх наслідків і оперує з набором показників і для кожного окремого випадку відповідний показник буде різним.

Значення показників виходять приблизні, основані на наявній статистиці або експертних оцінках, що унеможливлює аналіз при малій кількості накопичених статистичних даних [21].

Метод оцінки *очікуваного збитку від і-ї загрози* був вперше запропонований спеціалістами американської фірми IBM:

$$R_i = 10^{S_i+V_i-4}, \tag{1.11}$$

де S_i і V_i – коефіцієнти, що характеризують можливу частоту виникнення загрози і значення можливого збитку при її виникненні (значення обох коефіцієнтів – цілі числа в проміжку $[0, 7]$; для S_i відповідно: 0 – майже ніколи, 7 – більше 1000 разів/рік; V_i відповідно \$1–1 000 000) [20–23].

Дану методику можна описати системою рівнянь, приводячи параметри на інтервалах:

$$\begin{cases} R_i = 10^{S_i+V_i-4} \\ S_i = 7 \cdot 10^{-3} \cdot s_i, 0 \le s_i \le 10^3 \\ S_i = 7, s_i > 10^3 \\ V_i = 7 \cdot 10^{-7} \cdot (v_i - 1), 1 \le v_i \le 10^7 \\ V_i = 7, v_i > 10^7 \end{cases} \tag{1.12}$$

де s_i – прогнозована або реальна кількість атак на рік, v_i – сума прогнозованого або реального збитку в грошових одиницях.

Але в даному випадку не враховано зростання на другому інтервалі, ми пропонуємо виправити формулу, враховуючи зростання на всій області визначення характеристик. В новій формулі пропонується використовувати гіперболічний тангенс (точніше тільки його додатну частину у першому квадранті). Виходячи з характеристик функції гіперболічного тангенсу, введено додаткові коефіцієнти:

$$f(x) = k_{\max} \cdot th\frac{2x}{b_{\max}}, \tag{1.13}$$

де $k_{\max}$ відповідає максимуму шкали, тобто «7», а $b_{\max}$ – максимальному значенню прогнозованої або реальної величини, коефіцієнт «2» введено для кращого масштабування по абсцисі. Тоді систему можна записати таким чином:

$$\begin{cases} R_i = 10^{S_i+V_i-4} \\ S_i = 7 \cdot th\frac{s_i}{500},\ 0 \le s_i \\ V_i = 7 \cdot th\frac{v_i-1}{5\cdot 10^5},\ 1 \le v_i \end{cases} \quad (1.14)$$

Формулу очікуваного збитку від *i*-ї загрози можна записати у вигляді:

$$R_i = 10^{7\cdot th\frac{s_i}{500}+7\cdot th\frac{v_i-1}{5\cdot 10^5}-4}, 0 \le s_i, 1 \le v_i. \quad (1.15)$$

Метод оцінки стану *систем захисту телекомунікаційних мереж від впливу техногенних та антропогенних загроз* оперує з суб'єктивними коефіцієнтами вагомості *i*-ї характеристики W_i і бальними значеннями кожної характеристики G_i, що визначаються за експертними оцінками та дозволяє отримати лише приблизну оцінку ефективності системи захисту проводових і безпроводових мереж. Формула ступеню забезпечення безпеки має вигляд:

$$S = \frac{1}{N}\sum_{i=1}^{N} W_i \cdot G_i, \quad (1.16)$$

де N – кількість характеристик.

Метод має два недоліки: неможливо порівняти системи з різним набором характеристик і не враховується залежність коефіцієнта вагомості і значення характеристики від самої характеристики [21,22].

Разом з цим даний метод нівелює основні недоліки двох інших методів і за результатами оцінки статистичних даних є найбільш адекватним (раціональним) при вирішенні задач оцінки стану безпеки безпроводової мережі.

1.2. Порівняння моделей побудови безпроводових мереж та їх реалізація

Багаторічний досвід розвинутих країн світу свідчить, що проблемам створення безпроводових технологій передачі інформації завжди приділялась значна увага. У 20-х роках минулого століття з'явились перші радіоприймачі з амплітудною модуляцією. У 30-х – радіо з частотною модуляцією та телебачення, а у 70-х – перші телефонні безпроводові системи. У цей час, коли інтернет став безмежним по своїй насиченості джерелом знань і різних даних, які можна передавати як по провідним, так і широкосмуговим безпровідним лініям телекомунікацій – значення останніх зростає майже в геометричній прогресії.

1.2.1. Аналіз спектру сигналів в безпроводових мережах

Як відомо, у проводовій мережі пакети даних передаються у фізичному середовищі, такому як мідний кабель або волоконна оптика. У безпроводовій системі дані передаються буквально по повітрю – через радіоефір. Зважаючи на те, що саме це робить їх доволі доступними для зловмисників, захист як самих безпровідних мереж, так і даних, що ними передаються робить означену проблему надзвичайно актуальною.

Щоб створити безпечний безпроводовий додаток, треба виявити всі можливі напрямки, за якими йтимуть безпроводові «атаки», що були описані в розділі 1.1 (табл. 1.2) та визначитись з тим, яким чином спектр сигналів (сукупність значень, що характеризує процес) в системах безпроводового зв'язку може бути перехоплений зловмисником [23].

Таблиця 1.2

Приклади та цілі атак на відмову в обслуговуванні згідно рівням OSI

Рівень OSI	Завдання рівня	Протоколи	Приклади технологій DoS	Наслідки DoS атак
7	Початок створення пакетів даних. Приєднання і доступ до даних. Призначені для користувача протоколи, такі як FTP, SMTP, Telnet	FTP, HTTP, POP3, SMTP	HTTP GET і HTTP POST запити (форми веб-сайтів: логін, завантаження фото / відео, підтвердження зворотного зв'язку)	Брак ресурсів. Надмірне споживання системних ресурсів службами на сервері, що атакується.
6	Трансляція даних від відправника одержувачу	Протоколи стиснення, кодування даних (ASCII, EBCDIC)	Підробні SSL запити: перевірка шифрованих SSL пакетів потребує багато ресурсів, хакери використовують SSL для HTTP-атак на сервер жертви	Системи, що атакуються, можуть перестати приймати SSL з'єднання або автоматично перезавантажуватися
5	Управління встановленням та завершенням з'єднання, синхронізацією сеансів зв'язку в рамках операційної системи через мережу	Протоколи входу/виходу (RPC, PAP)	Атака на протокол Telnet використовує слабкі місця прог рамного забезпечення Telnet-сервера на комутаторі, щоб зробити сервер недоступним	Унеможливлює для адміністратора управління комутатором
4	Забезпечення передачі інформації між вузлами без помилок, управління передачею повідомлень на 1, 2 та 3 рівнях	TCP, UDP	SYN-flood, атака ICMP-запитами зі зміненими адресами	Досягнення межі по ширині каналу або по кількості допустимих підключень, порушення роботи мережевого обладнання
3	Маршрутизація і передача інформації між різними мережами	IP, ICMP, ARP, RIP	ICMP-flood	Зниження пропускної здатності атакується мережі і можлива перевантаженість брандмауера
2	Установка та супровід передачі повідомлень на фізичному рівні	802.3, 802.5	MAC-flood – переповнення пакетами даних мережевих комутаторів	Потоки даних від відправника одержувачу блокують роботу всіх портів
1	Передача даних у фізичному середовищі	100BaseT, 1000 Base-X, 802.3, 802.5	Глушіння	Неможливість передачі будь-яких повідомлень

Для одержання спектрів сигналів у безпроводових мережах використовують аналізатори спектру, в основі дії яких лежить одне з явищ: інтерференція; залам при наявності дисперсії фазової швидкості; резонанс. Аналізатори спектру дозволяють визначати амплітуду й частоту спектральних компонент, що входять до складу аналізованого процесу. Їх найважливішою характеристикою є роздільність (роздільна спроможність) – найменший інтервал частот між двома спектральними лініями, які ще розділяються аналізатором.

Більш детально розглянемо аналізатори спектру в діапазоні (2,4000÷2.4835) ГГц.

В табл. 1.3 зведені дані про шість найбільш вдалих трансиверів даного класу від виробників Nordic, Texas Instruments і Cypress [24].

Таблиця 1.3

Основні характеристики трансиверів

Мікросхема	Частотний діапазон, МГц	Роздільна здатність, кГц	Діапазон потужності, дБмВт	Роздільна здатність, дБмВт
Nordic nRF24L01	2400–2525	977	–(85÷42)	1,0
TI Chipcon CC2500	2400–2483,5	58–812	–(104÷13)	0,8
TI Chipcon CC2511-F32	2400–2483,5	58–812	–(110÷6,5)	0,5
Cypress CYRF6934	2400–2483	1000	–(90÷40)	~4,1
Cypress CYRF6935	2400–2483	1000	–(95÷40)	~3,1
Cypress CYRF6936	2400–2497	1000	–(97÷47)	~1,3

Їх умовно можна поділити на такі класи:

програмні за допомогою сканування каналів ТБД або клієнтським обладнанням: 14 точок;

програмні за допомогою сканування каналів Bluetooth-пристроями: 79 точок;

низької вартісні (low cost) за $80–200: (170÷180) точок;

саморобні на мікросхемах типу CC25xx до $100: (170÷2100) точок;

середньої вартості за $3–10 тис.: 280 тис. точок;

високої точності і широкого діапазону за $50–100 тис.: до 83,5 млн точок.

Першим на ринку з’явився аналізатор спектру Metageek Wi-Spy 2.4i (Gen 1) на базі мікроконтролера Cypress CYRF6934 (рис. 1.8а).

На мікросборці CYWUSB6935, побудованої на наступній версії мікроконтролера Cypress CYRF6935, через SPI можливо зробити перехідник і підключатися до аналізатору через LPT-порт (рис. 1.8б). На наступній версії мікроконтролера Cypress CYRF6936 зібраний Wi-detector, який доступний в апаратних версіях 2 і 3 (рис. 1.8в). Решта аналізатори зібрані або на роздільної збірці мікроконтролера і радиомодуля Chipcon CC2500 (TI eZ430-RF2500, див. рис. 1.8г) або на інтегрова-

ному в одному чіпі Chipcon CC2511-F32 (Ubiquiti AirView2, див. рис. 1.8д; Metageek Wi-Spy 2.4x, див. рис. 1.8е; Pololu Wixel, див. рис. 1.8ж). Більшість серед наведених аналізаторів спектру не дозволяють змінювати настройки сканування (Metageek Wi-Spy 2.4i, Wi-detector, CYWUSB6935, Ubiquiti AirView2), й лише деякі з них надають таку можливість. Так, наприклад, TI eZ430-RF2500 і Pololu Wixel дозволяють змінювати налаштування один раз при прошивці, а Metageek Wi-Spy 2.4x – з пропрієтарним програмним забезпеченням (ПЗ).

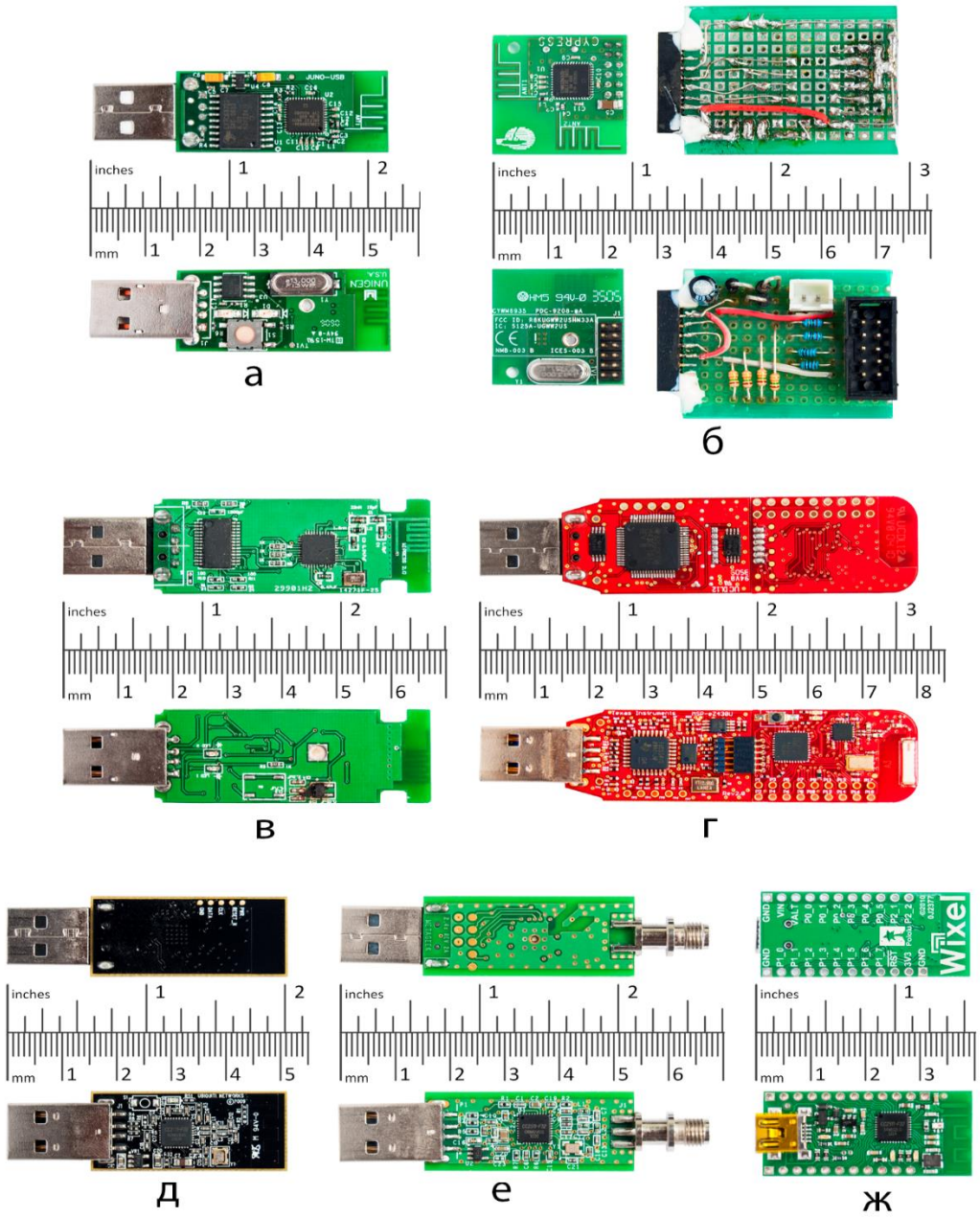


Рис. 1.8. Загальний вигляд плат аналізаторів спектра:
а – Metageek Wi-Spy 2.4i; *б* – CYWUSB6935 (LPT); *в* – Wi-detector;
г – TI eZ430-RF2500; *д* – Ubiquiti AirView2;
е – Metageek Wi-Spy 2.4x і *ж* – Pololu Wixel

Серед усіх аналізаторів найбільш зручним виявився Pololu Wixel. Він має добре продуману архітектуру та забезпечує доступ до зміни прошивки і SDK (на мові програмування С) з повною документацією. Доступна ціна цього пристрою дозволяє одночасно запускати декілька датчиків, збирати і паралельно аналізувати отримані з них дані. Разом з тим практично кожному із протестованих аналізаторів спектру виявилась притаманною помилка у розрахунку амплітуди, яка виникає через дискретизацію точок вимірювання (рис. 1.9).

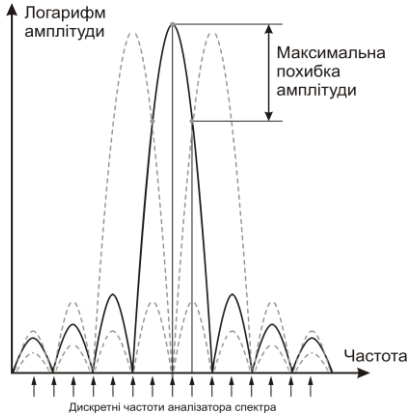


Рис. 1.9. Виникнення максимальної похибки при вимірюванні

У випадку сумірних ширини підканалу (в нашому випадку – 312,5 кГц) і частоти дискретизації аналізатора спектра (500 кГц) ці точки можуть не співпадати з як показано на рис. 1.10. З’являється похибка амплітуди, яку можна виміряти порівнявши точки співпадіння (аналогічно до ефекту биття при накладені двох коливань близької частоти) максимальних і мінімальних частот. На рис. 1.10 показані точки співпадіння: максимального сигналу догори і мінімального – вниз. З графіка видно, що максимальне значення становить мінус 46 дБмВт, а мінімальне – мінус 52 дБмВт. Тобто абсолютна похибка вимірювання складає 6 дБмВт, а відносна – 11,5% [25].

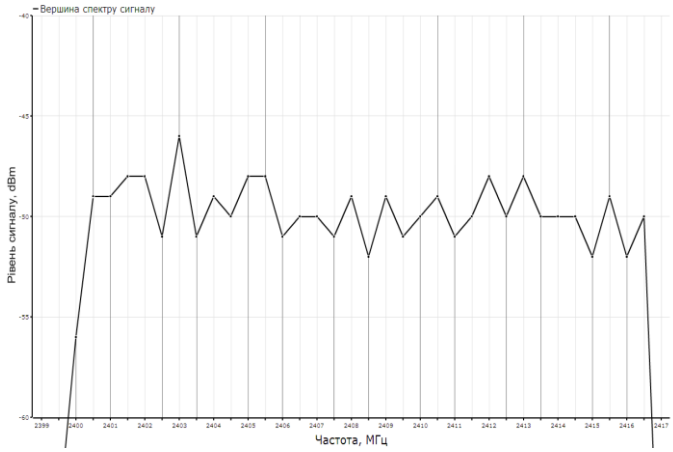


Рис. 1.10. Максимуми і мінімуми, які співпадають з точками аналізатора спектра

1.2.2. Дослідження технологій побудови безпроводових мереж

Сучасні безпроводові телекомунікаційні технології умовно можна поділити на декілька типів (рис. 1.11).

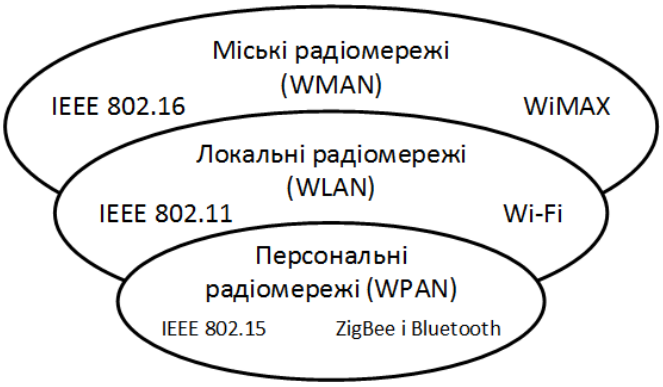


Рис. 1.11. Масштаби організації безпроводових мереж

Ті, що призначені для зв'язку встаткування в межах робочого місця, наприклад, стільникового телефону і ноутбука або комп'ютера і принтера, відносять до класу персональних безпроводових мереж (wireless personal area network, WPAN). Найпоширеніша технологія із цієї категорії – Bluetooth, що має типовий радіус дії до 10 м. Наступним типом безпроводових комунікацій є безпроводові локальні мережі WLAN (wireless local area network). Їх основне призначення полягає у побудові локальних розподілених безпроводових операторських Wi-Fi мереж масштабу окремих приміщень які, як правило, використовуються для продовження провідних корпоративних мереж та створення так званих гарячих точок високошвидкісного доступу в інтернет. У перспективі варто очікувати глобального впровадження єдиної широко смугової безпроводової мережі масштабу міста – WMAN (wireless metropolitan area network).

Нині розвиток мереж безпровідного доступу ґрунтується на нових, взаємодоповнюючих технологіях, кожна з яких має власні можливості й які досить повно описані в сучасній науково-популярній літературі. Найбільш застосовуваними серед них представлені в табл. 1.4 [26].

Серед WLAN технологій найбільш інтенсивно розвиваються технології побудови безпроводових мереж з ортогональним частотним розподіленням каналів. З метою дослідження принципів їх роботи побудуємо їх моделі.

Таблиця 1.4

Порівняння технологій широкосмугового безпроводового доступу

	CDMA 2000	Wi-Fi	WiMAX
Тип технології	Стільникова 3G	WLAN	WMAN
Стандарт	3G	IEEE 802.11	IEEE 802.16
Середня швидкість, Мб/с	0,4–0,7	1–5	1
Переваги	Великий радіус дії, мобільність, висока швидкість передачі	Широкий спектр впровадження, високий ступінь стандартизації, невисока вартість, підвищена працездатність у перспективі	Для мобільної версії – висока швидкість передачі
Недоліки	Регіональні відмінності у технологіях – один і той же пристрій не буде гарантовано працювати скрізь	Обмежений радіус дії, обмежена мобільність, недостатньо висока якість для телефонії та відеододатків, остаточно не вирішені питання сумісності, існують деякі проблеми пов'язані з безпекою	Висока вартість абонентського обладнання. Використання різних частот у різних країнах

1.2.3. Моделювання безпроводових мереж з ортогональним частотним розділенням каналів

Моделювання проводилося двома методами:

за допомогою *структурованої схеми* (САПР LabVIEW);

за допомогою *математичного опису сигналів* (САПР OCG/Signals Analyzer і MatLAB).

Моделі передавача (рис. 1.12) і приймача (рис. 1.13) у різних моделюючих САПР будуть виглядати майже однаково. У модель OFDM-передавача в якості даних можна використовувати генератор випадкових даних (наприклад, генерувати цілі числа в заданому діапазоні з наступним представленням у двійковій формі). Формування і модулювання каналів проводиться окремо для кожного слова. В залежності від типу модуляції використовуються формувачі векторів з різною логікою, а кількість модуляторів каналів з даними завжди дорівнює 48, крім яких формуються чотири службові підканали.

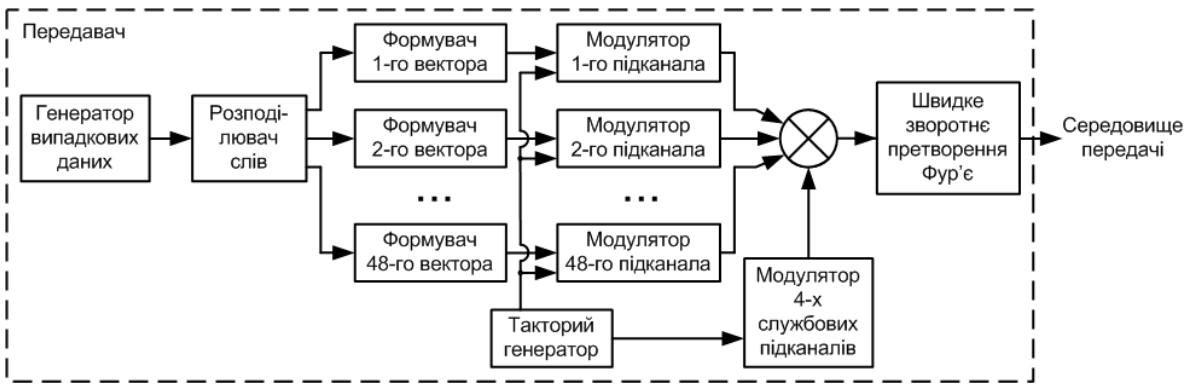


Рис. 1.12. Блок-схема моделі OFDM-передавача

Дана модель не включає згортальне кодування, так як воно застосовується до розподілювача слів, і в даному випадку входить до генератора випадкових даних.

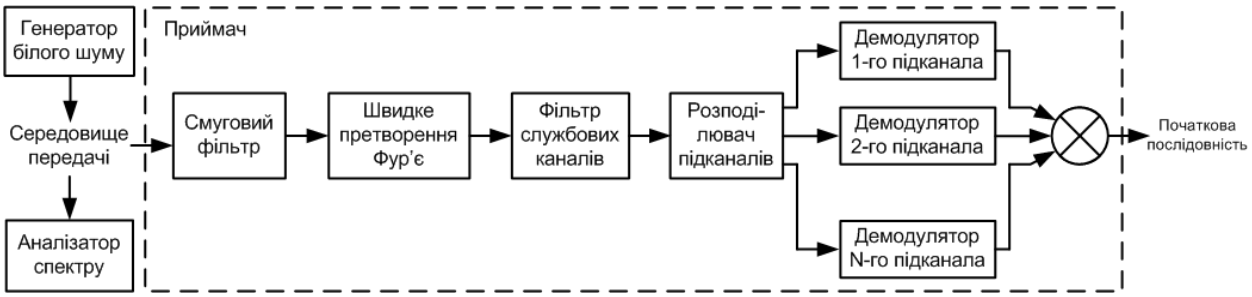


Рис. 1.13. Блок-схема моделі OFDM-приймача

Моделювання розподілення каналів у часі проводилося за допомогою OCG (версія 1209) і Signals Analyzer (версія free), як показано на рис. 1.14, для прикладу вище показана спектрограма сигналу в тому самому діапазоні [27]. Хоча в програмі і не присутні n-QAM модуляції, але програму можна використовувати для наочного отримання спектральної завантаженості каналів у часі, використовуючи PSK-модуляцію сигналу. Діаграма виконана у відтінках сірого: чим ближче до чорного кольору, тим більша амплітуда сигналу. З обох боків спектру видно різке зменшення амплітуди, яке відповідає неосновним коливанням крайніх каналів.

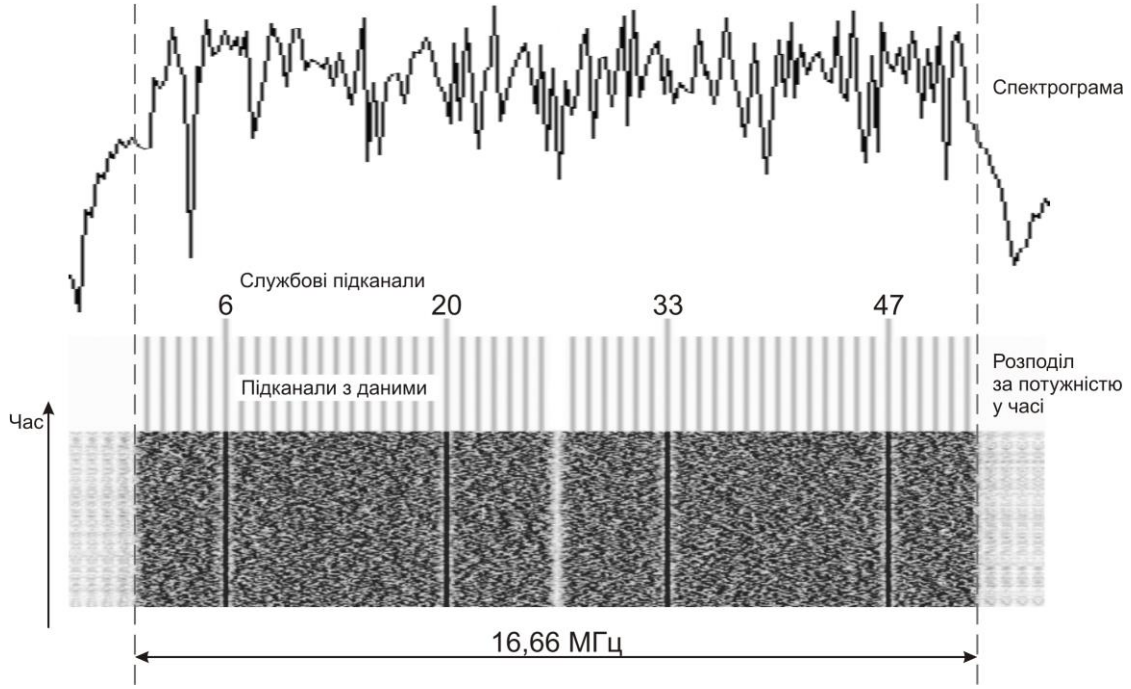


Рис. 1.14. Моделювання завантаженості каналів

Моделювання проводилося за допомогою Modulation Toolkit OFDM із пакета прикладних програм LabVIEW Professional Development System (версія 10.0) [28].

Для перевірки результатів моделювання використовувався зазначений вище аналізатор спектру і у схему, показаній на рис. 1.15. Відстань між ТБД і клієнтом становить 2 м, а посередині розташований аналізатор спектру.

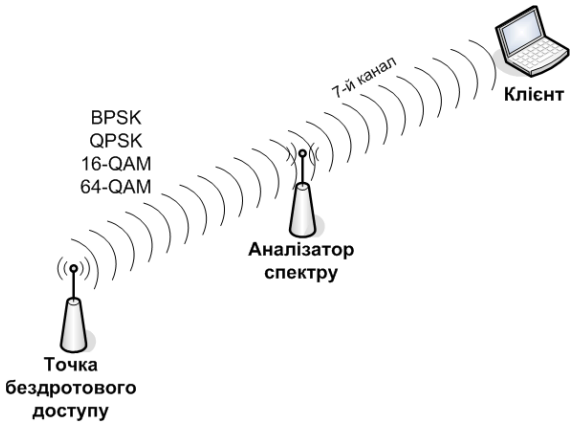


Рис. 1.15. Схема експерименту для визначення відповідності моделей

Для експерименту був вибраний 7-й канал з серединою на частоті 2,442 ГГц, так як він знаходиться саме в середині діапазону і можна отримати чіткий вид затухання спектра.

Для різних швидкостей передачі у стандарті 802.11g (точніше 802.11a) використовуються різні типи модуляції: для 6 і 9 Мбіт/с – двохпозиційна фазова модуляція (BPSK); для 12 і 18 Мбіт/с – четирьохпозиційна фазова модуляція або (QPSK або 4-PSK); для 24 і 36 Мбіт/с – шістнадцятирівнева квадратурна амплітудна модуляція (16-QAM або QASK); для 48 і 54 Мбіт/с – шестидесятичотирьохрівнева квадратурна амплітудна модуляція (64-QAM). При погіршені умов прийому ТБД може перемикатися на нижчу швидкість, так як при зменшені типу модуляції збільшується стабільність роботи через меншу кількість бітів інформації, які приходяться на один підканал (BPSK – 1 біт/такт, QPSK – 2 біт/такт, 16-QAM – 4 біт/такт і 64-QAM – 6 біт/такт).

На рис. 1.16 показані різні типи модуляції: ліворуч LabVIEW-модель і праворуч сигнал знятий з аналізатора спектра. Швидкість передачі залежить від швидкості згортального кодування. Треба зауважити, що обов’язковими для стандарту 802.11a є тільки швидкості передавання 6, 12 і 24 Мбіт/с, які відповідають швидкості згортального кодування ½. З розглянутого видно, що швидкість згортального кодування важлива тільки для точності отримання повідомлень і ніяким чином не впливає на вид спектру. В стандартній моделі при погіршені умов прийому здійснюється автоматичний перехід на меншу швидкість згортального кодування,

а також вид модуляції з меншою кількістю векторі сигналів (тобто з більшою похибкою при демодуляції).

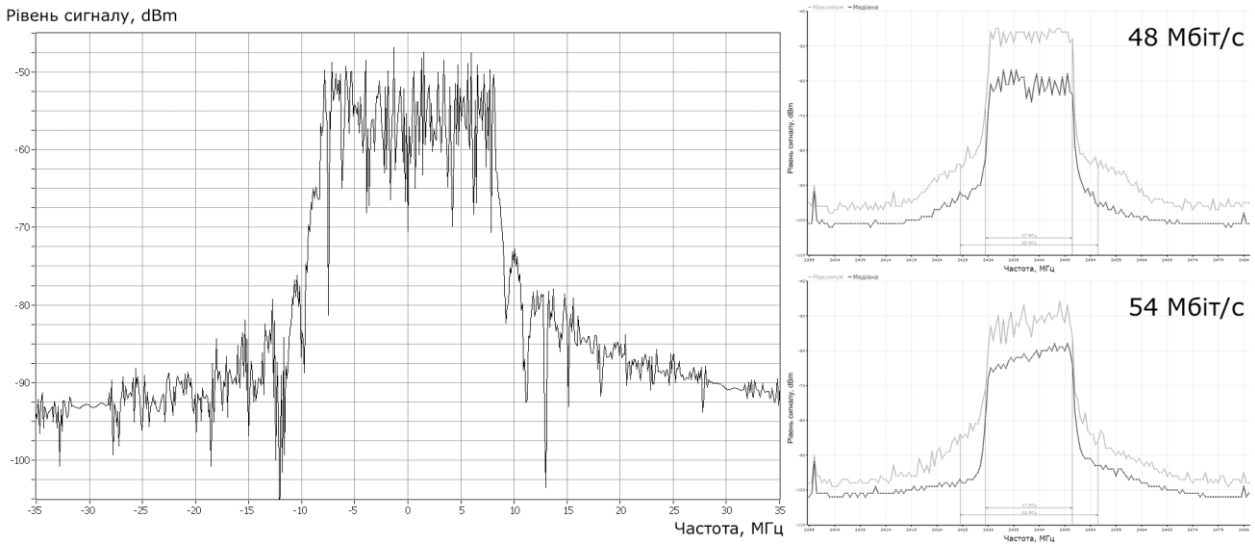


Рис. 1.16. Результат моделювання для 64-QAM

В усіх випадках передавалося одна й та сама кількість інформації (5,2 кБ з урахуванням службових каналів). Всі 52 канали: з них 48 з даними (data tones) і 4 службових (pilot tones) – були завантажені рівномірно.

Піки з обох кінців спектрального діапазону виникають через розрив при передаванні двох послідовних OFDM-символів.

З іншого боку можна моделювати сигнали за допомогою математичного представлення сигналів у програмному комплексі MatLAB 7.8/Simulink 7.3 [29]. У скрипті задаються параметри: кількість підканалів, симетричність сигналу відносно середнього підканалу, розмір пакета даних (рівний 5,2 кБ, як у попередньому моделюванні), ширина каналу передачі, точність (кількість точок вимірювання), після чого генеруються послідовності для кожного типу модуляції. Сгенерована послідовність розподіляється за підканалами і подається на вхід функції Уолша pwelch(), після чого проводиться швидке перетворення Фур'є для сигналів з нульовим середнім каналом fftshift(). Спектр змодельованого сигналу показаний на рис. 1.17. Крім основних підканалів були розраховані спади рівня сигналу на кінцях спектрів за допомогою 16-крайніх підканалів.

У моделі не врахована нерівномірна інтенсивність завантаження службових каналів по відношенню до каналів з даними, тому спектр наближується до ідеального вигляду. Для різних видів модуляції спектр дещо відрізняється потужністю и швидкістю затухання на кінцях, але формою всі спектри майже не відрізняються.

Окремо треба зазначити, що 14-й канал дозволений для використання лише у Японії і тільки для 802.11b, тобто з OFDM він не використовується [30]. До того ж з [31] широкосмуговий радіодоступ для 802.11 обмежується частотою 2,4835 ГГц, а середина 14-го каналу проходиться на частоту 2,484 ГГц, тобто більша частина спектру каналу знаходиться за межею діапазону.

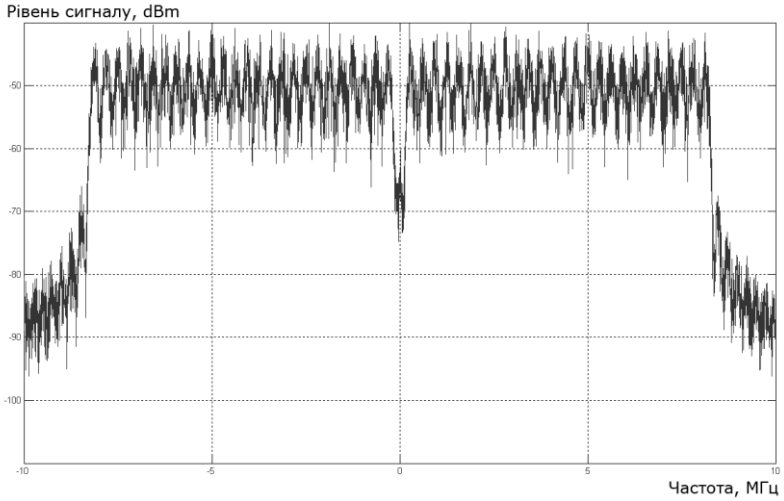


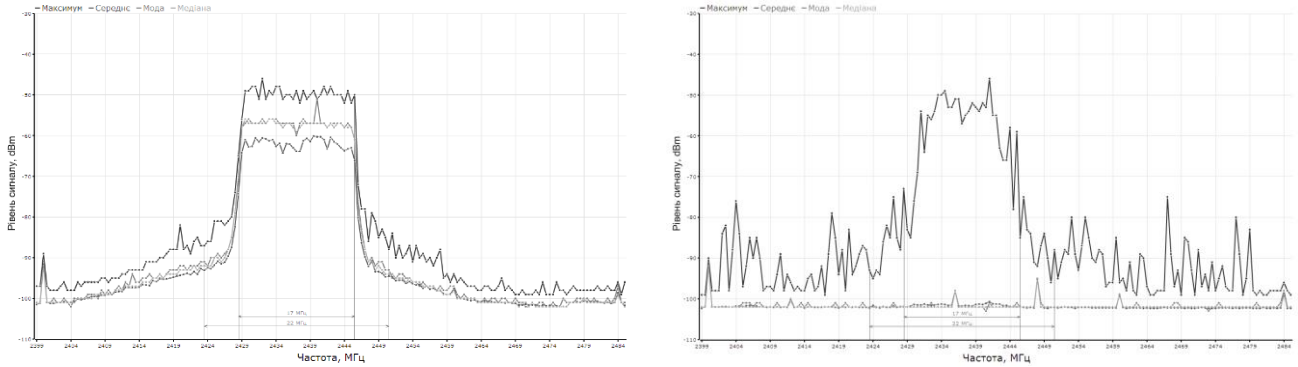
Рис. 1.17. Результат математичного моделювання для 64-QAM

Результати проведеного моделювання із застосуванням структурної моделі для OFDM подано в [32]. Разом з тим, поза на увагою залишилося відношення до реальних об’єктів. У [33] нами було розглянуто моделювання для розширення спектру пристроїв 802.11b стандарту. В [34] зроблено спробу моделювати заваду для пристроїв за стандартом 802.11 від 802.15 пристроїв. З розглянутого видно, що моделювання і реальні об’єкти не співставляються або співствляються не адекватно.

При дослідженні використовувався 6-й канал з переліку рекомендованих (1-й, 6-й і 11-й) з серединою на частоті 2,437 ГГц. Для отримання даних використовувався аналізатор спектру Ubiquiti AirView2 на мікро контролері Chipcon CC2511-F32 з частотою дискретизації 500 кГц з ПЗ Sun Java 6 JRE (32-біта) на ОС Linux Ubuntu 10.04 [35]. Для візуалізації результатів застосований PHP-скрипт (версія інтерпретатора 5.3.3) і бібліотека Open Flash Chart (версія 2) [36].

При аналізі спектру сигналу каналу з максимальним заповненням видно, що форма сигналу добре повторюється для середнього арифметичного значення, а також моди і медіани (рис. 1.18а) [37]. Найкраще форму спектру передають максимальне значення і медіана (так як сума модулів відхилень значень від медіани мінімальна). Але при зменшенні кількості інформації, що передається в каналі (менше 50% заповнення каналу), різко погіршується форма спектру, отриманого з максимальних значень, а середнє, мода і медіана не перевищують рівня шуму

(рис. 1.18б). Таким чином, можна визначити, що присутній сигнал з OFDM-кодування, але важко проводити аналіз інших характеристик сигналу.



а б

Рис. 1.18. Розподілення частот для швидкості передачі 12 Мбіт/с:
а – для потужного сигналу; б – для слабкого

При малому рівні сигналів за спектром важко визначити тип модуляції: так на рис. 1.18б другий канал працює з OFDM (802.11g), а одинадцятий з CCK (802.11b). Перекривання спектрів цих двох каналів відсутнє. На рис. 1.19 добре видно короткий імпульс завади з шириною спектру (2,0÷2,5) МГц, який відповідає заваді від верхньої гармоніки стільникового телефону, ZigBee (IEEE 802.15.4) або BLE-пристрою (IEEE 802.15.1) [38].

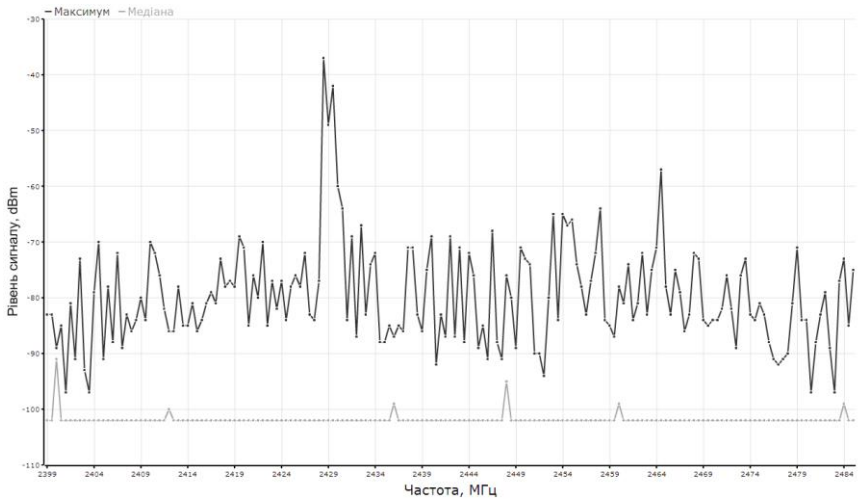


Рис. 1.19. Розподілення частот для двох каналів зі слабкими сигналами

Прикладом застосування ортогонального частотного розділення каналів можуть бути безпроводові мережі з ієрархічною топологією або з роумінгом покриття за протоколом WDS (wireless distribution system).

При побудові мереж з роумінгом виникає проблема найбільш ефективного розташування базових станцій (ТБД), яке у діапазоні дециметрових хвиль (серед-

ня довжина хвилі становить 12,5 см) сильно залежить від розташування перешкод: залізобетонних конструкцій, будівель, дерев, автотранспорту тощо. Крім того, якість передавання залежить від діаграми спрямованості (ДС) антени і її спотворення через вплив землі (тобто якість зв'язку змінюється в залежності від висоти розташування антени) [39].

Працездатність системи напряму пов'язана із цілісністю передавання даних, тому головна задача системи роумінгу – забезпечення мінімального рівня сигналу в усіх точках області покриття. Але вимірювання рівня сигналу в кожній точці при тестуванні системи не є оптимальним.

Розглянемо спрощену систему базових станцій з ізотропними антенами в двомірному просторі. Нанесемо всі базові станції і рівні їх сигналів. Побудуємо діаграму Вороного для виважених зон близькості, як показано на рис. 1.20 [40]. З діаграми видно, що чим потужніша базова станція, тим більша зона покриття.

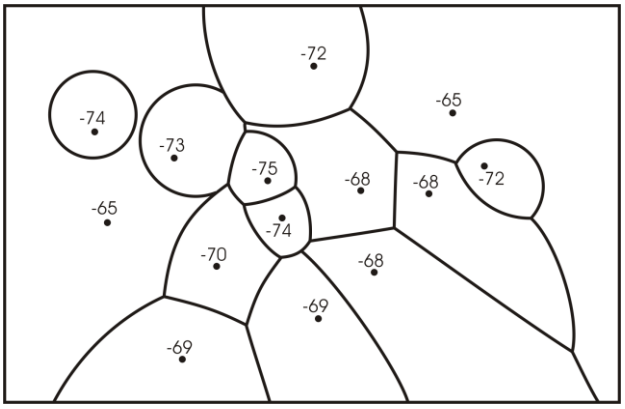


Рис. 1.20. Приклад покриття (рівень сигналу зазначений у дБмВт)

Для перевірки працездатності достатньо перевірити якість покриття (виміряти рівень сигналу за допомогою аналізатора спектра) на межах зон. При виявлені рівня сигналу на одній або декількох кривих меншого за мінімально встановлений додаємо нову базову станцію з більшим рівнем сигналу (так на рис. 1.21 приведено збільшений фрагмент покриття з рис. 1.20) або збільшуємо рівень сигналу найближчих існуючих станцій. Процес побудови діаграми Вороного повторюється; для нового розмежування проводиться повторний аналіз рівня сигналів на межах.

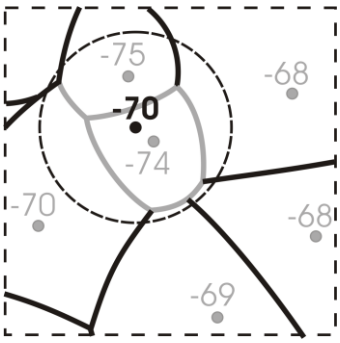


Рис. 1.21. Додавання нової базової станції (рівень сигналу зазначений у дБмВт)

При плановому або аварійному вимкнені існуючих базових станцій діаграма теж буде змінюватися. При побудові системи стійкої до аварійного вимкнення будь-якої базової станції потрібно проводити моделювання, послідовно виключаючи кожну базову станцію з системи, будувати діаграму і досліджувати рівні сигналів на межах.

Приведений метод виявлення потребує дослідження лише меж зон, а не всієї області покриття. При побудові реальних систем потрібно враховувати всі перешкоди і екрани. Метод не вирішує проблем, пов’язаних з інтерференційними процесами при повторному відбитті хвилі від перешкод, з впливом електромагнітних завад у вибраному діапазоні і опадів, тому на практиці краще збільшити мінімальний рівень сигналу на 20–30%.

Використання діаграм Вороного для моделювання безпроводових мереж з ортогональним частотним розділенням каналів дозволить вирішити завдання забезпечення цілісності і доступності для абонентів безпроводових мереж [41].

1.3. Шляхи захисту безпроводових мереж

У міру того, як безпроводові мережі набирають популярність, а технології, націлені на викрадення конфіденційних даних та/або порушення нормальної роботи різноманітних сервісів розвиваються фактично в геометричній прогресії, питання щодо забезпечення їх безпеки і надійності стає завданням критичної важливості. Перехід від одиночних атак на відмову в обслуговуванні до розподілених є цьому відмінним доказом: хакери захоплюють чужі пристрої і використовують їх у своїх цілях без згоди власників.

Саме тому питання щодо забезпечення захисту ТБД від проявів деструктивного кібернетичного впливу стають останнім часом одними із найбільш актуальних. З огляду на це можна сформулювати наступну гіпотезу, що стала останнім часом, на жаль, гнітючою реальністю: чим більше ІТ розвиваються і інтегруються

в наше повсякденне життя, тим більш важливими і затребуваними в будь-яких сферах людської діяльності стають технології ІБ. Підтвердженням цьому можуть служити статистичні дані, оприлюднені корпорацією Web Application Security Consortium (WASC), згідно з якими уразливими до хакерських атак стають більш 96,85% веб-сайтів, близько 74% прикладного та системного ПЗ, приблизно 68% серверних додатків [42]. При цьому не тільки в прикладному і системному ПЗ, але і в серверних додатках домінують ті ж уразливості: відмова в обслуговуванні, компрометація системи і підвищення привілеїв.

З цим погоджуються і фахівці з міжнародної організації Computer Emergency Response Team (CERT). Разом з тим вони стверджують [43], що кількість виявлених вразливостей щорічно стрімко збільшується.

Для запобігання впливу таких і подібних до них вразливостей на власну інфраструктуру, а також її захисту від ряду зовнішніх і внутрішніх загроз, більшість країн світу виділяє нині колосальні фінансові кошти [44]. Але, на жаль, досить часто буває так, що дороге антивірусне ПЗ і дорогі апаратні брандмауери не потрібні більшості замовників, крім для теоретичних доказів того, що вкладені кошти роблять їх мережі від хакерських атак більш захищеними.

1.3.1. Технології забезпечення об’єктивного контролю захищеності безпроводових мереж

Щоб вберегтися від зайвих втрат значна кількість державних і комерційних структур нині застосовують доволі популярну в усьому світі послугу в галузі ІБ тестування на проникнення (penetration test, скор. pentest), й означає санкціонована спробу обійти існуючий комплекс засобів захисту власних ІТ систем і мереж з метою виявити в них слабкі місця (за рахунок ідентифікації максимально можливої кількості уразливостей за обмежений час при заданих умовах й поточному стані) та впевнитись в їх ефективності. Для цього, як правило, досліджуються внутрішній і зовнішній периметри мережі, веб-сайти, бази даних, спеціалізовані додатки, безпроводові мережі тощо, а також проводиться аналіз конфігурацій мережевих пристроїв, додатків і серверів на відповідність стандартам безпеки, тестування співробітників на стійкість до методів соціальної інженерії, фізичне проникнення на територію об’єкта інформаційної діяльності (ОІД), аналіз коду вебсайтів та додатків.

В ході тестування на проникнення роль зловмисника відіграє фахівець, який повинен здійснити атаку на веб-сервер, сервер застосувань або баз даних, персонал або мережа, визначити рівень захищеності, виявити уразливості, ідентифікувати найбільш вірогідні шляхи злому і визначити наскільки добре працюють засоби виявлення і захисту ІС від атак на підприємстві.

Тестування на проникнення може проводитись як у складі аудиту ІБ на відповідність зазначеним вище стандартам, аналізу уразливостей або атестації інформаційної (автоматизованої) системи, так і у вигляді самостійної роботи.

Тестування на проникнення є складовою частиною етичного хакінгу – процесу пошуку та виявлення уразливостей ІБ, а також проведення контрольованих атак, спрямованих, наприклад, як на окремі ІТ системи – CMS, CRM, ERP та інтернет клієнт-банк, так і на інфраструктуру ОІД в цілому.

Проведення тестування на проникнення є трудомістким завданням. Для його реалізації тестувальник повинен володіти навичками використання величезної кількості технік, розуміти всі нюанси технічної та організаційної складової ІБ, володіти навичками соціальної інженерії та дотримуватись певних стандартів, на кшталт:

Penetration Testing Model (BSI);

Payment Card Industry Data Security Standard (PCI DSS);

Information System Security Assessment Framework (ISSAF);

Penetration Testing Execution Standard (PTES);

Open Source Security Testing Methodology Manual (OSSTMM);

Open Web Application Security Project Testing Guide (OWASP);

NIST Special Publication 800-115: Technical Guide to Information Security Testing and Assessment (NIST SP 800-115).

Окрім технік, рекомендованих даними стандартами (найефективнішим серед них є стандарт OWASP, заснований на восьми базах даних від семи компаній, що включає чотири консалтингові фірми і трьох виробників SaaS та містить понад 500 тис. уразливостей) в ході тестування можуть бути змодельовані й перевірені й інші вектори атак, спрямовані на користувачів корпоративних систем (табл. 1.5), зовнішній периметр мережі (периметр IP-адрес і веб-сайтів), безпровідні мережі IEEE 802.11 (Wi-Fi), 802.15 (Bluetooth і ZigBee) і 802.16 (WiMAX), а також переносимі комп’ютери та мобільні пристрої.

Таблиця 1.5

Вектори атаки на корпоративні системи

Вектор атаки	Опис
Фізичний	Атаки з використанням безпосереднього фізичного доступу в середину периметра корпоративної мережі (якщо такий є), що захищається.
Мережевий	Дистанційні атаки на мережеві ресурси і протоколи.
Електронна пошта	Атаки з використанням електронної пошти (в тому числі з елементами соціальної інженерії).
Додатки	Атаки з використанням специфічних додатків використовуваних Замовником (наприклад, веб-портал).
Безпроводові мережі	Атаки спрямовані на безпроводові протоколи передачі даних 802.11 (Wi-Fi), 802.15 (Bluetooth і ZigBee), 802.16 (WiMAX).
Клієнтські додатки	Атаки на клієнтське ПЗ.
Мобільні пристрої	Атаки на мобільні пристрої (мобільні і переносні комп'ютери, смартфони і т. ін.).
Соціальна інженерія	Атаки на користувачів з використанням методів соціальної інженерії.

Тестування на проникнення може проводитись як у складі аудиту ІБ на відповідність зазначеним вище стандартам, аналізу уразливостей або атестації інформаційної (автоматизованої) системи, так і у вигляді самостійної роботи.

Власне аудит ІБ починається з аналізу ризиків і загроз. Він призначений для виявлення найбільш небезпечних загроз з точки зору системи захисту. Елементи тестування на проникнення при цьому можуть (у відповідності зі стандартом ISO 17799) використовуватися для оцінки ефективності реалізації таких захисних механізмів, як «захист від злоякісного коду», «забезпечення мережевої безпеки» та ін. В ході тестування аудитор грає роль зловмисника, мотивованого на порушення безпеки ІТ-систем (мереж) замовника (державної або комерційної структури). Його завдання полягає в тому, щоб знайти відповіді на такі питання: «Як простіше потрапити всередину системи, порушити її працездатність або що-небудь отримати?» та «Якою може бути мінімальна ціна злому?». Інтенсивним перевіркам при цьому піддаються, перш за все, програмні і технічні засоби захисту ІТ систем та мереж з метою визначення в них потенційних проломів: незакритих вразливостей ПЗ, відкритих портів тощо (табл. 1.6). Для цього аудитор застосовує, як правило, ряд стандартних інструментів, які мають різну чутливість до різного роду загроз [45].

При аналізі уразливостей елементи тестування на проникнення можуть використовуватися для оцінки використовуваного в ІТ-системах (мережах) програмного і апаратного забезпечення на предмет спроби їх експлуатації для проникнення в систему. В ході атестації об'єктів інформатизації елементи тестування на проникнення можуть використовуватися для демонстрації на практиці того, що невідповідність вимогам стандартів або іншим нормативно-правовим документам з безпеки інформації може привести до успішної компрометації системи. В ході са-

мостійної роботи елементи тестування на проникнення можуть використовуватися для обґрунтування необхідності проведення робіт з підвищення захищеності або отримання незалежної оцінки рівня безпеки системи.

Таблиця 1.6

Стандартні інструменти для тестування на проникнення

Прилад	Опис
Pwn Pad 	Пристрій оснащений потужним чотирьох ядерним процесором (Qualcomm Snapdragon S4 Pro, 1,5 ГГц), 7-дюймовим екраном з дозволом 1900×1200 і потужною батареєю, що забезпечує до дев'яти годин активної роботи (3950 мА/год.), 2 ГБ ОЗП і 32 ГБ внутрішньої пам'яті. У комплекті йдуть три адаптери: дві потужні зовнішні антени для тестування на проникнення 802.11b/g/n безпроводових мереж і Bluetooth, а також перехідник USB-Ethernet, що дозволяє перевіряти на міцність провідні мережі. Його головною складовою є програмна компонента: Metasploit, SET, Kismet, Aircrack-NG, SSLstrip, Ettercap-NG, Bluelog, Wifite, Reaver, MDK3, FreeRADIUS-WPE, Evil AP, Strings Watch, Full-Packet Capture, Bluetooth Scan і SSL Strip.
CreepyDOL 	Спеціальне ПЗ й пристрій на базі Raspberry Pi за допомогою яких можна створити мережу, що буде перехоплювати Wi-Fi-трафік і збирати конфіденційну інформацію про користувачів. Як результат, пристрій дозволяє позиціонувати власника пристрою. Вся інформація обробляється на центральному сервері, там же можна в реальному часі відслідковувати пересування власника телефону і його перехоплені дані.
Demyo Power Strip 	Призначений для перевірки на міцність Ethernet, Wi-Fi і Bluetooth-мереж. Побудований на базі популярного одноплатного комп'ютера Raspberry Pi і оснащений ARM-процесором 700 МГц, який можна розігнати до 1 ГГц. Також на борті є 512 МБ оперативної пам'яті, SD-карта на 32 ГБ. У якості ОС використовується Debian Linux з набором попередньо встановленого ПЗ: Nmap, OpenVPN, w3af, aircrack-ng, btscanner, ophcrack, John the Ripper та інші.

За місцем розташування аудитора відносно до мережевого периметру корпоративної системи, тестування на проникнення може бути внутрішнім, зовнішнім або комплексним. Зовнішнє тестування на проникнення передбачає тестування зовнішнього периметру мережі, тестування веб-сайтів та спец додатків тощо. Внутрішнє орієнтоване головним чином на внутрішні ресурси (табл. 1.7).

Таблиця 1.7

Типи тестування на проникнення

Тип тестування	Опис
Зовнішнього периметру мережі	Аналіз включає тільки зовнішні IP-адреси компаній, доступні в інтернеті.
Веб-сайтів	Аналіз включає в себе тільки веб-сайти і сервіси компанії, доступні необмеженому колу зовнішніх користувачів.
Спеціалізованих додатків	Аналіз включає різні додатки, доступні зовнішнім користувачам, що взаємодіють з серверами компанії.
Співробітників на стійкість до соціальної інженерії	Спроба отримання доступу до системи компанії з використанням методів соціальної інженерії. Оцінка рівня обізнаності співробітників у питаннях ІБ.
Імітація «втраченого» корпоративного пристрою	Аналіз можливостей потенційного зловмисника, який заволодів корпоративним мобільним пристроєм.
Внутрішнього периметру	Оцінка можливостей зловмисника, який має санкціонований обмежений доступ до корпоративної мережі, аналогічний рівню доступу рядового співробітника або гостя, який має доступ тільки в гостьовий сегмент, або ж має доступ тільки до мережевої розетки.
Окремого компоненту	Веб-додатки, ERP, СУБД.

За обсягом інформації, яка надається аудитору протестовану систему тестування на проникнення може проводитись за методами чорної (black box) або білої (white box) скриньок, а за рівнем інформованості замовника про випробування він може здійснюватися в режимах *black hat* або *white hat*.

В чорній скриньці виконавець імітує групу хакерів, які мають лише назву компанії й практично нульові відомості про систему, що є метою дослідження. Для реалізації поставленого завдання йому необхідні лише діапазон зовнішніх IP-адрес і, можливо, адреси електронних скриньок внутрішніх користувачів системи. В білій – виконавець має доступ до систем і повну інформацію про них. Така модель тестування використовується як частина організаційно-технічного аудиту організації IT і передбачає аналіз процесів і процедур.

У режимі black hat про проведення робіт знають тільки керівники служби ІБ. При цьому завдання групи тестувальників – повністю імітувати дії зловмисника, діючи максимально непомітно і не залишаючи слідів. У такому випадку вдається перевірити рівень оперативної готовності до атак мережевих адміністраторів і адміністраторів ІБ. У режимі white hat будь-яких заходів приховування атакуючих дій не застосовується, а виконавці тестів працюють у постійному контакті з ІБ-службою замовника. Їх основне завдання зводиться до виявлення можливих вразливостей і оцінки ризику проникнення в систему.

За ступенем усвідомленості персоналу досліджуваної IT-системи тестування на проникнення може проводитись:

з повідомленням адміністраторів об’єкта;

без повідомлення адміністраторів;

без повідомлення адміністраторів і фахівців з безпеки.

Типова схема тестування на проникнення приведена на рис. 1.22.

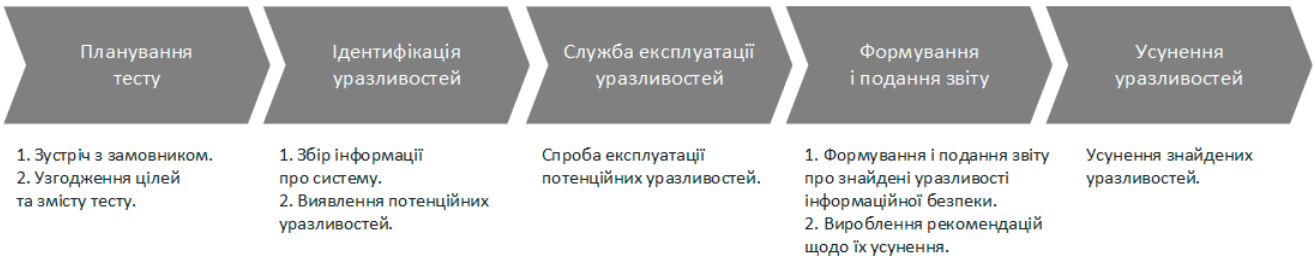


Рис. 1.22. Типовий алгоритм проведення тестування на проникнення

У загальному випадку порядок проведення робіт показаний на рис. 1.23).

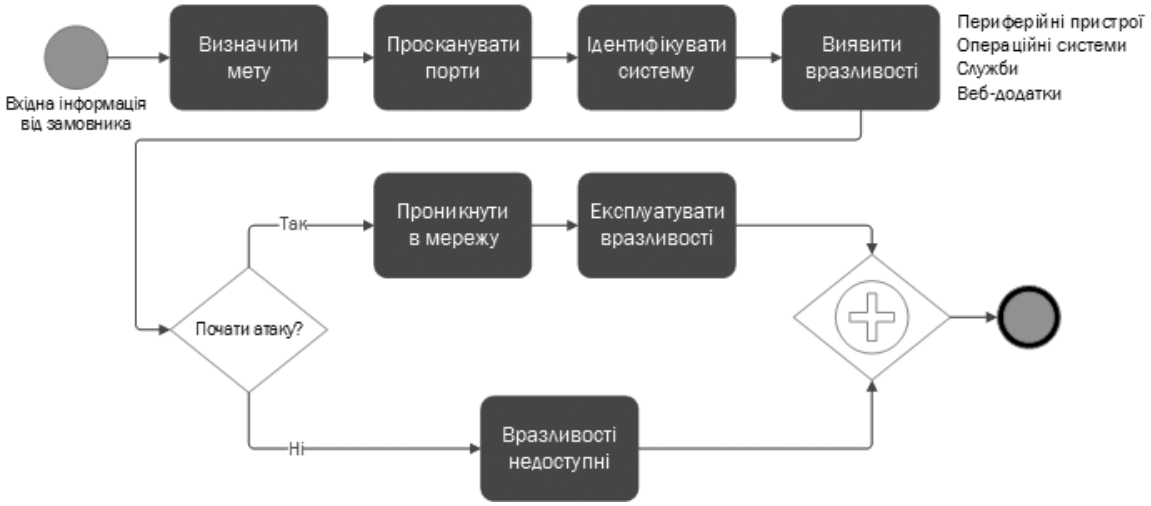


Рис. 1.23. Розширений алгоритм проведення тестування на проникнення

1. *Отримання попередньої інформації* про мережу замовника та планування проведення тесту на проникнення. Для цього можуть бути використані як пасивні (Google Hacking, Google Cache, WHOIS інформація, Shodan, Wayback Machine); офіційний сайт компанії; публікації про компанію та її співробітниках у ЗМІ; сайти пошуку роботи; прес-релізи інтеграторів; сторінки співробітників у соціальних мережах; блоги та форуми; пошук у фізичному мусорі компанії – dumpster diving тощо), так і активні (ping sweep, fingerprint, сканування портів, аналіз банерів мережевих служб, сканування NetBios, SNMP, LDAP, NTP, SMTP, DNS, соціальна інженерія тощо) методи.

Як результат – формування карти мережі, визначення типів пристроїв, ОС, додатків по реакції на зовнішній вплив.

2. *Пошук та ідентифікація уразливостей* мережевих служб і додатків. Може проводитися як вручну, так і з використанням різних сканерів від компаній Max-Patrol, Nessus, OpenVAC та ін.

Перевіряється наявність і можливість використання вразливих місць, а саме:

SQL-ін’єкції (SQL injection);

виконання довільного коду (source code injection);

виконання команд ОС (OS commanding);

атаки на клієнтів (client-side attacks);

міжсайтового виконання сценаріїв (cross-site scripting, скор. XSS);

підміни вмісту (content spoofing);

переповнення буфера (buffer overflow);

механізмів авторизації та аутентифікації і інше.

За даними компанії Positive Technologies [46] в ході проведення тестування на проникнення для тестів часто використовуються уразливості наведені на рис. 1.24.

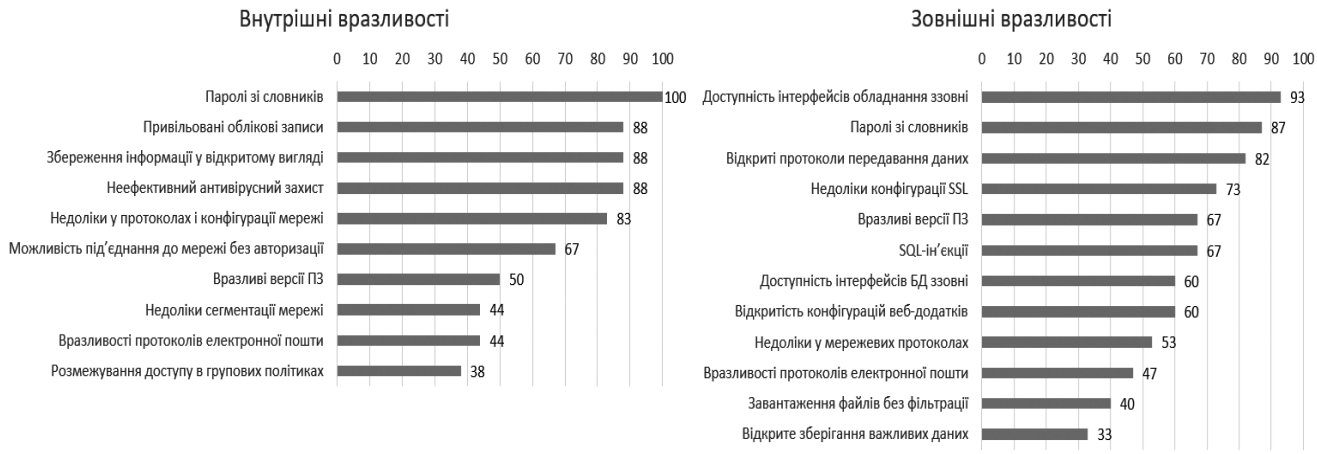


Рис. 1.24. Вразливості, характерні для проведення тестів на проникнення

3. *Експлуатація уразливостей.* Отримавши перелік можливих уразливостей аудитор проводить їх експлуатацію. Методи та інструментарій вибираються при цьому індивідуально для кожного типу уразливості. Особлива увагу приділяється: підбору паролів до різних мережевих сервісів; проведенню атак типу «людина посередині» для перехоплення паролів користувачів тощо.

Атаки типу «людина посередині» (man-in-the-middle) полягають у перехопленні зловмисником каналу зв'язку між двома системами, отриманні доступу до ресурсів мережі та активному втручанні в протокол передавання інформації з метою її крадіжки, знищення, фальсифікації або модифікації.

З цією метою аудиторами використовується як інструментарій власної розробки, так і загальнодоступні утиліти такі, як експлойти: *www.exploit-db.com*, *www.rapid7.com/db/*, *ru.0day.today*, *www.ussrback.com* тощо, а також фреймворки: Metasploit; Cobalt Strike; Core Impact; Immunity CANVAS. Після отримання доступу до будь-якої системи аудитор намагається максимально розширити свої привілеї й отримати доступ до інших систем, а також скомпрометувати максимальну кількість облікових записів користувачів.

За погодженням із замовником при цьому може проводитися перевірка:

базових робіт з контроля захищеності безпроводових мереж;

зовнішнього периметру і відкритих ресурсів на DoS (DDoS) атаки, а також оцінки ступеня стійкості мережевих елементів і можливого збитку при їх проведенні;

стійкості мережі, шляхом моделювання атак на протоколи канального рівня STP, VTP, CDP, ARP;

стійкості маршрутизації, шляхом моделювання фальсифікації маршрутів і проведення DoS (DDoS) атак проти використовуваних протоколів маршрутизації;

мережевого трафіку, з метою отримання важливої інформації (паролі користувачів, конфіденційні документи та ін.);

можливості отримання зловмисником НСД до конфіденційної інформації або інформації обмеженого доступу замовника. Проводиться перевіркою прав доступу до різних IP замовника з привілеями, отриманими на різних етапах тестування.

4. Отримана в ході аналізу уразливостей і спроб їх експлуатації *інформація документується та аналізується* з метою вироблення рекомендацій у формі звіту, що спрямований на поліпшення захищеності IT-систем (мереж). Практика ведення бізнесу в Україні показує, що найбільш оптимальною структурою звіту є його розбиття на три рівні: для вищого керівництва, для менеджерів ІБ і для технічних фахівців.

Після проведення тесту можливі залишкові сліди тесту, так звані артефакти, які необхідно усунути. Наприклад, якщо був отриманий доступ до якої-небудь системи, то необхідно провести зміну паролів для всіх її користувачів. У разі використання вірусів їх також необхідно видалити, і т. ін. Логічним продовженням тесту на проникнення можуть бути роботи з проектування та впровадження системи управління рівнем захищеності, моніторингу захищеності периметра корпоративної мережі, розробки програми підвищення обізнаності в області ІБ та впровадження СУІБ.

Критеріями завершення тесту на проникнення є отримання:

доступу до внутрішньої мережі з боку інтернету;

доступу до певного сегменту мережі (наприклад, сегмент АСУТП);

привілеїв в основних інфраструктурних та інформаційних системах/сервісах (active directory, мережеве обладнання, СУБД, ERP і т. ін.);

доступу до певних інформаційних ресурсів;

доступу до певної інформації (наприклад, електронна пошта директора);

всього, до чого вдасться дотягнутися за певний час;

першого серйозного збою, викликаного діями аудитора.

Якщо ж компанія звертається за проведенням інформаційного аудиту всього інформаційного середовища, сума може досягати сотень тисяч, а для початкового корпоративного сайту – тисяч доларів і тривати до місяця (табл. 1.8).

Таблиця 1.8

Тривалість злому різних сайтів і сервісів

Послуга	Термін виконання, доба
Аналіз відкритої інформації про організацію	7–21
Вивчення базової інформації про мережеву інфраструктуру	7
Аналіз соціальних мереж	3
Аналіз вакансій, резюме на HR-сайтах	1–2
Аналіз форумів	10
Сканування портів	1–2
Визначення додатків і веб додатків	<5
Визначення операційних систем	9
Ідентифікація мережевих маршрутизаторів і міжмережевих екранів	2–3
Пошук вразливостей (автоматизовані сканування і ручний аналіз)	5–10
Аналіз отриманої інформації і розробка сценаріїв злому	2–3
Проведення атак на компоненти IT інфраструктури	30
Визначення взаємодії додатків і підтвердження вразливостей	5–10
Оформлення та презентація звіту	1–3

Отримавши перелік можливих вразливостей аудитор проводить їх експлуатацію. Методи та інструментарій вибираються при цьому індивідуально для кожного типу вразливості. Особлива увага приділяється питанню перехоплення паролів користувачів шляхом їх підбору до різних мережевих сервісів [47], проведення атак типу «людина посередині» і ін.

В ході тестування на проникнення вдається, як правило, отримати доступ до: вебсайтів – в 50% випадків; електронній пошті – в 40%; бізнес-програмам – в 35%; IP-телефонії – в 10%; систем дистанційного банківського обслуговування – в 29%. Повний контроль над інфраструктурою може бути отриманий ними не більше ніж в 25% проектів, а в 5% – тестувальникам взагалі не вдається подолати периметр.

До найпопулярніших вразливостей експерти в області інформаційної безпеки останнім часом відносять: міжсервісне виконання сценаріїв (50%); наявність інтерфейсів віддаленого керування (47%); доступна інформація про додатки (45%); вбудовування SQL-коду (63%).

Найпопулярнішою вразливістю за висновками експертів зараз є прості паролі адміністраторів. Вони зустрічаються в 80% проектів, іноді навіть в тих випадках, коли в організаціях були впроваджені політики щодо забезпечення складності паролів для рядових користувачів. Уразливості веб-додатків і некоректно налаштоване обладнання несуть за собою значно менші ризики, і тому є ключем до злому

відповідно в 46 і 38% випадках. Відсутність оновлень сприяє успішному проведенню тестових атак в 25% компаній, а недоліки архітектури – в 9%.

З огляду на таке, саме проведення тестування на проникнення дозволить:

дізнатися можливості здійснення загроз безпеки інформації;

оцінити наслідки спрямованої хакерської атаки;

визначити уразливості в захисті інформаційної системи;

оцінити ефективність засобів захисту інформації;

оцінити ефективність менеджменту інформаційної безпеки;

оцінити можливий рівень кваліфікації порушника для успішної реалізації атаки;

отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ;

виробити список контрзаходів, з тим щоб знизити можливість реалізації атак.

За погодженням із замовником при тестуванні на проникнення, додатково, може проводитися перевірка [48–50]: базових робіт по контролю захищеності безпроводових мереж; зовнішнього периметра і відкритих ресурсів на можливість DoS атак, а також оцінки ступеня стійкості мережевих елементів і можливого збитку при їх проведенні; стійкості мережі, шляхом моделювання атак на протоколи канального рівня STP, VTP, CDP, ARP; стійкості маршрутизації, шляхом моделювання фальсифікації маршрутів і проведення DoS (DDoS) атак проти використовуваних протоколів маршрутизації; мережевого трафіку, з метою отримання, наприклад, паролів користувачів, конфіденційних документів тощо; можливості отримання зловмисником несанкціонованого доступу до конфіденційної інформації або інформації обмеженого доступу замовника (проводиться перевіркою прав доступу до різних IP-адрес замовника з привілеями, отриманими на різних етапах тестування) і т. ін.

Не дивлячись на досить часту критику тестування на проникнення, технологія реалізації якого не може гарантувати замовнику того, що: тестувальник виявив все «дірки» в системі безпеки замовника; знайдені тестувальником «дірки» не згодом використані для заволодіння інформацією, що належить замовнику; діяльність тестувальника може бути замовником повністю проконтрольована; в умовах сучасної інформаційної і кібервійни, яка ведеться проти нашої країни, завдання щодо забезпечення безпеки інформаційних систем на об’єктах інформаційної діяльності та, перш за все, IT-систем (мереж) органів влади і критичних інфраструктур (соціальних фондів і різних державних реєстрів), а також об’єктивної оцінки рівня безпеки цих структур без проведення тестування на проникнення практично нездійсненна [51].

1.3.2. Технології підвищення захищеності безпроводових мереж

Через легкість застосування і доступність апаратного забезпечення розвиток і поширення безпроводових мереж у декілька наступних років залишатимуться актуальними. За даними неприбуткової організації Wi-Fi Alliance, яка займається сертифікацією обладнання для Wi-Fi мереж, у світі вже розповсюджено приблизно 1 мільярд пристроїв з Wi-Fi модулями і окремих Wi-Fi модулів [52]. А за статистичними даними компанії ABI Research, яка досліджує тенденції у телекомунікаціях і новітніх технологіях, розвиток світового ринку Wi-Fi на період до 2014 року характеризується щорічним збільшенням реалізації Wi-Fi обладнання на 100 мільйонів пристроїв на рік.

Крім того у даний час Wi-Fi Alliance разом з Wireless Gigabit Alliance займаються розробкою нових стандартів для пристроїв зі швидкість на порядок більшою за існуючі аналоги (технологія WiGig) [53], а разом з ZigBee Alliance – економічних методів передачі даних у безпроводових мережах (технологія Smart Grid). Таке широке розповсюдження, зацікавленість виробників апаратного забезпечення світового масштабу і інвестиції у розробки нових Wi-Fi технологій означає, що найближчим часом треба очікувати появу нових стандартів передачі і покращення існуючих.

В [54] розглядалися загальні питання захищеності Wi-Fi мереж, а в даній роботі зроблено спробу детально розглянути протоколи шифрування і авторизації, зміни у способах шифрування ТБД на відміну від 2008 року, з метою вдосконалення захищеності Wi-Fi мереж.

Для аналізу проведений експеримент зовнішнього моніторингу (див. [55]), в експерименті інформація отримана за допомогою вбудованого Wi-Fi приймача на мікросхемі серії RaLink RT2860. Прийом та аналіз даних проводився за допомогою Wi-Fi драйвера rt2800pci (ОС Gentoo Linux, версія ядра 2.6.34-r1) та аналізатора пакетів Aircrack-ng (версії 1.0). Підчас експерименту було отримано інформацію від 1906 унікальних ТБД і від 540 клієнтських машин. Координати прийнятих сигналів отримано за допомогою GPS-приймача на мікросхемі SiRFstar III через послідовний інтерфейс PXA-serial версія ядра ОС Gentoo Linux 2.6.27 [56].

Стабільність сигналу залежить від багатьох факторів, які впливають на зону прийому і швидкість передачі даних. Важливим показником стабільності роботи Wi-Fi мереж є пропускна здатність каналу, яка визначається:

максимально можливою швидкістю роботи ТБД (в даному випадку швидкість 11 Мбіт/с за стандартом 802.11b підтримують 1,8% і 54 Мбіт/с за стандартом 802.11g – 97,6%);

залежністю потужності передавача до швидкості передачі;

залежністю чутливості приймача до швидкості прийому;

потужністю роботи ТБД і клієнтів, так на рис. 1.25 зображені розподіли потужностей для ТБД чорною кривою і клієнтів пунктирною кривою, перший максимум потужності в обох кривих припадає на мінус 72 дБмВт (63 пВт), а другий – на мінус 70 дБмВт (100 пВт);

конфігурацією антени і наявністю додаткового підсилювача;

присутністю або відсутністю шифрування;

віддаленістю клієнтів від ТБД (принцип «останньої милі»);

перешкодами, які призводять до втрати пакетів і потребі у їх повторному пересиланні;

активністю клієнтів, яку складно спрогнозувати.

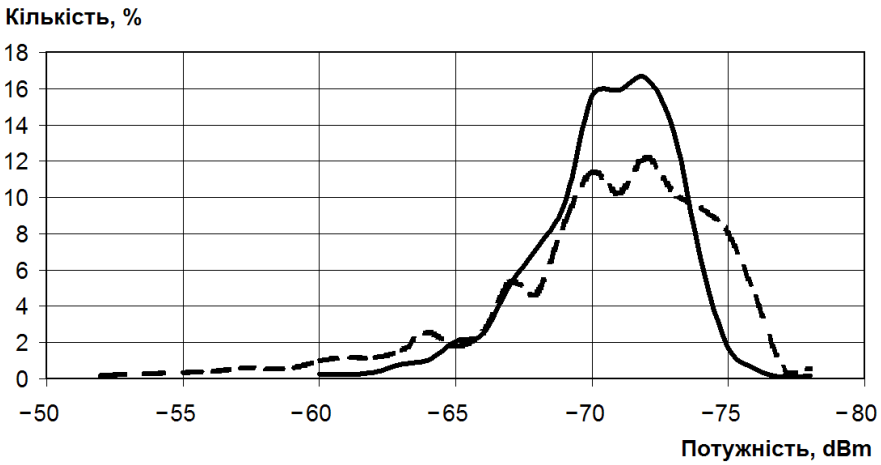


Рис. 1.25. Графік розподілу потужності

З аналізу факторів, які впливають на пропускну здатність, можна зробити висновок, що для стабільної роботи треба враховувати усі зазначені вище фактори і конфігурувати мережу у відповідності до індивідуальних потреб.

Через значну кількість параметрів, від яких залежить завантаженість каналу, для кожного моменту часу активність буде змінюватися. Але при перегляді великої кількості ТБД можна побудувати усереднений графік активності (див. рис. 1.26), при побудові якого не враховувались ECHO-пакети, кількість яких залежить лише від налаштувань ТБД. Так умовно можна поділити всі ТБД на малоактивні (<1 пакет/с) і активні (>2 пакет/с). Середній нормований розмір пакету становить 1,5 кБ.

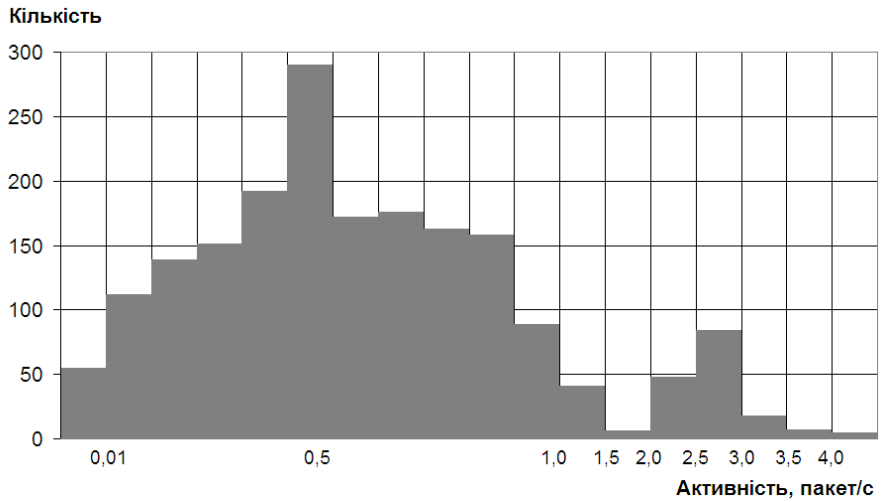


Рис. 1.26. Графік активності ТБД

У порівнянні з 2008 роком [54] кількість захищених мереж збільшилася, а найголовніше доля шифрування WPA і WPA2 збільшилася на 13% (див. рис. 1.27).

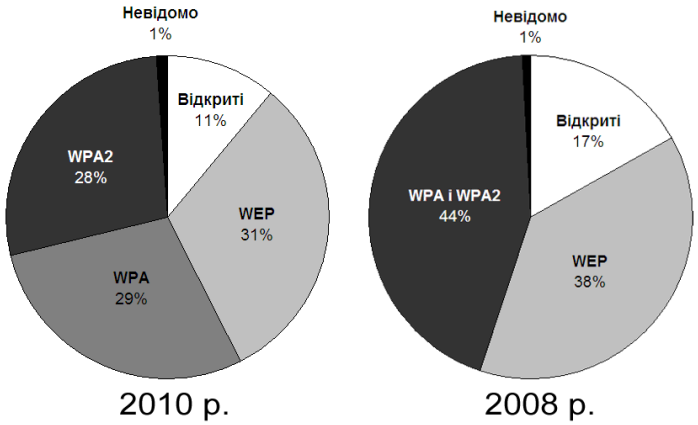


Рис. 1.27. Діаграма шифрування ТБД у відсотках за 2008 і 2010 рр.

Якщо розглянути четвірку найширше представлених на ринку виробників, то видно, що D-Link і Cisco лишилися фаворитами, а TP-Link і Asus замінили Motorola і ZyXEL. Дані отримані з MAC-адрес ТБД за переліками: унікальних ідентифікаторів організацій OUI (organizationally unique identifier) [57] і індивідуальних блоків адрес IAB (individual address block) [58]. В табл. 1.9 приведено дані про зміни у протоколах шифрування. Видно, що збільшення частки WPA і WPA2 для лідерів ринку складає в середньому 18,7%.

Усі виробники, що входять до четвірки лідерів за 2008 і 2010 роки, є або спонсорами, або постійними членами організації Wi-Fi Alliance.

На сучасних ТБД встановлюють функцію заміни і клонування MAC-адреси. Але такою функцією для побудови безпроводових мереж користується незначна

кількість адміністраторів (ця функція дуже зручна при роботі зі стаціонарною мережею, коли треба замінити обладнання, що вийшло з ладу або застаріло, без зміни конфігурації мережі). Похибка становить 4,2%.

Таблиця 1.9

Виробники ТБД, найширше представлені на ринку

Спосіб шифрування	Частка від загальної кількості*, %							
	D-Link		Cisco		TP-Link		Asus	
	2010 р. (717)**	2008 р. (626)	2010 р. (345)	2008 р. (219)	2010 р. (287)	2008 р. (16)	2010 р. (118)	2008 р. (42)
WEP	↓ 29,15	43,29	↓ 21,74	29,22	↑ 53,31	50,00	↓ 13,56	40,48
WPA/WPA2	↑ 64,02	44,89	↑ 60,87	46,58	↑ 40,42	31,25	↑ 79,66	47,62
Без шифрування	6,83	11,82	17,39	24,20	6,27	18,75	6,78	11,90

* Стрілки ↑ і ↓ вказують на динаміку у порівнянні з попереднім вимірюванням.

** В дужках вказана загальна кількість ТБД даного виробника за відповідний рік.

Якщо розглянути обладнання клієнтів, то четвірка найбільш розповсюджених виробників буде значно відрізнятися від лідерів виробників обладнання для ТБД. Так з табл. 1.9 і 1.10 видно, що у обидві четвірки входить лише D-Link, це пояснюється широким асортиментом і порівняно низькою ціною мережних пристроїв D-Link на ринку (хоча стабільність роботи пристроїв цього бренду визиває нарікання у користувачів). Компанія Hon Hai Precision (торгівельна марка Foxconn) виробляє модулі і закінчені пристрої для компаній Apple, Dell і Hewlett Packard, тому важко визначити під яким саме брендом було продане обладнання. З іншого боку видно, що серед стаціонарних (десктопів) і мобільних пристроїв (лептопів) переважає Intel, а серед портативних пристроїв – Apple.

Таблиця 1.10

Виробники клієнтського обладнання, найширше представлені на ринку

Виробник клієнтського обладнання	Кількість	
	абсолютна, од.	відносна, %
Intel	111	20,6
Hon Hai Precision (Foxconn)	96	17,8
Apple	56	10,4
D-Link	56	10,4

При шифруванні за допомогою WPA і WPA2 використовуються два типи протоколів: шифрування й аутентифікації. Детальніше протоколи описані в [54] і [59]. Так протокол цілісності тимчасового ключа TKIP (temporal key integrity protocol) звичайно використовується для WPA, а протокол блочного шифрування CCMP (counter mode with cipher block chaining message authentication code protocol) – для WPA2 як альтернатива TKIP, але специфікація дозволяє використ-

товувати у WPA і WPA2 будь-який протокол: TKIP або CCMP (а також і деякі інші), або декілька одночасно в залежності від клієнтського забезпечення.

Аутентифікація проводиться за попередньо розподіленими ключами PSK (pre-shared keys), де на клієнт і ТБД попередньо встановлюють ключі, які пізніше використовуються для з'єднання, або через виділений сервер аутентифікації 802.1x або RADIUS-сервер (remote authentication in dial-in user service) [60].

У дослідженні було виявлено 1077 ТБД з WPA або WPA2 (деякі ТБД можуть підтримувати одночасно два способи, але для спрощення враховується лише протокол за яким проводилася передача даних в момент прийому). Як видно з попередньої діаграми (рис. 1.27) різниця в використанні WPA і WPA2 складає 1%. В табл. 1.11 приведені відомості про протоколи, які використовуються для шифрування і аутентифікації. Так з таблиці видно, що TKIP найчастіше використовується у WPA, а CCMP – у WPA2, також пізніший WPA2 у 2,6 рази частіше підтримує обидва протоколи шифрування. Для аутентифікації в більшості випадків використовуються протокол за попередньо розподіленими ключами (>96%).

Таблиця 1.11

Розподіл протоколів шифрування і аутентифікації для WPA і WPA2

	Спосіб шифрування			
	WPA		WPA2	
Кількість ТБД з протоколами шифрування, од.				
TKIP	386	}110	56	}286
CCMP	39		192	
Інші	8		0	
Кількість ТБД з протоколами аутентифікації, шт.				
PSK	526		525	
802.1x	17		9	
Всього:	543		534	

За отриманими координатами ТБД можна побудувати інтегральну діаграму розподілу відповідно до відстані. Сумарна відстань дослідження склала майже 45 км, а точність вимірювання складає 1 м через обмеження GPS-системи загального користування. Також не вдалося визначити вірні координати для приблизно 1% ТБД через перешкоди: будинки, дерева тощо, такі ТБД не враховані на діаграмі (див. рис. 1.28). На діаграмі окремо показані розподіли для відкритих ТБД (рис. 1.28а), з WEP (рис. 1.28б) і WPA/WPA2 (рис. 1.28в) шифруванням. Діаграма з інтегральною потужністю дозволяє отримати уявлення про щільність покриття.

Щільність потоку потужності визначається за наступною формулою [61]:

$$W = \frac{P}{N_{\text{ККД}} \cdot \Delta S \cdot \Delta f}, \tag{1.17}$$

де P – потужність, Вт; $N_{ККД}$ – коефіцієнт корисної дії антени; ΔS – площа охоплення антени, м^2; Δf – ширина каналу, МГц. Тоді для конкретного випадку щільність потоку потужності для кожного протоколу шифрування, де коефіцієнт корисної дії не враховується, так як потужність вже виміряна з врахуванням ККД, дорівнює:

$$W^* = \frac{1}{\Delta S \cdot \Delta f}\sqrt{\frac{1}{n^*}\sum_{i=1}^{n^*} P_i^2}, \tag{1.18}$$

де n^* – кількість ТБД з заданим типом шифрування, а потужності вимірюється, дБмВт.

Для нашого випадку ΔS = 0,022 м^2 (площа контуру навколо 8,9-дюймового монітору) і Δf = 20 МГц (для стандарту 802.11b ширину каналу становить 22 МГц, а для 802.11g – 20 МГц, як показано раніше, другий стандарт використовують 97,6% ТБД, тому вибираємо відповідну ширину каналу). Тоді щільності потоків потужності складають:

$$\begin{aligned} W_{\text{відкр}} &= (160{,}0 \pm 2{,}3)\,\frac{\text{дБмВт}}{\text{м}^2\cdot\text{МГц}}, \\ W_{\text{WEP}} &= (160{,}7 \pm 2{,}3)\,\frac{\text{дБмВт}}{\text{м}^2\cdot\text{МГц}}, \quad , \\ W_{\text{WPA/WPA2}} &= (160{,}2 \pm 2{,}3)\,\frac{\text{дБмВт}}{\text{м}^2\cdot\text{МГц}}, \end{aligned} \tag{1.19}$$

різниця між якими не перевищує значення похибки вимірювання: для всіх протоколів шифрування середній рівень щільності потоків потужності один й той самий. А також з розрахунку видно, що значення не перевищують норми (потужність ТБД повинна бути меншою за 100 мВт, знаходитися виключно всередині будівель і щільність потоку потужності на відстані 100 м від зовнішніх фасадних стін будівель не перевищує мінус 110 дБмВт/м^2/МГц).

З діаграми (рис. 1.28) видно, що максимуми відкритих мереж відповідають мінімумам мереж з WEP шифруванням. Що пояснюється застарілим обладнанням, яке підтримує вибір тільки цих двох режимів, і одночасно несерйозним відношенням користувачів до питань захищеності мереж, так як у більшості випадків можна встановити програну реалізацію WPA/WPA2 шифрування. Похибку вносить присутність навмисно відкритих мереж, наприклад, в закладах громадського харчування. З іншого боку закриті мережі з WPA/WPA2 шифруванням розподіляються рівномірно.

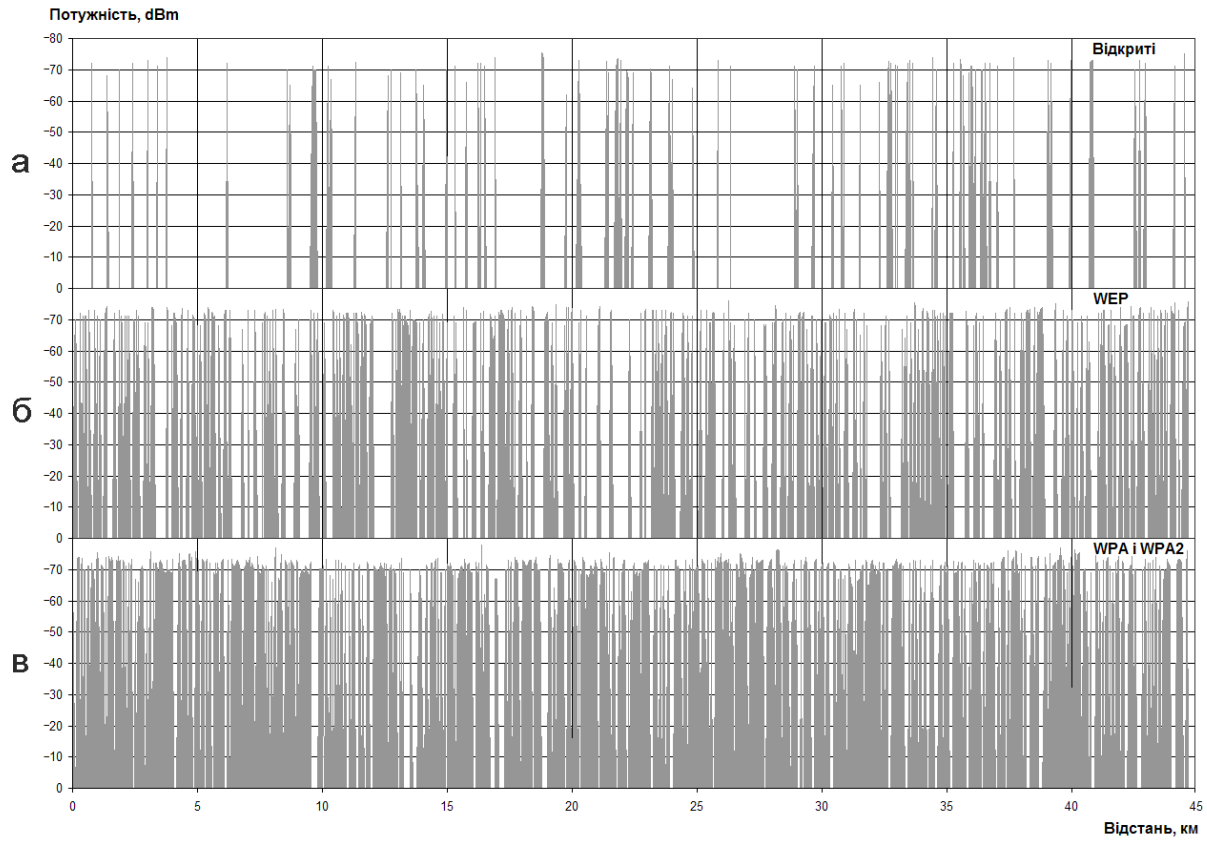


Рис. 1.28. Діаграма розподілу ТБД відповідно до відстані

За результатами дослідження видно, що більшість ТБД і клієнтів працюють на оптимальній потужності мінус (70÷72) дБмВт, а переважна більшість пристроїв підтримує стандарт 802.11g (сучасніший стандарт передачі даних). Більшість ТБД знаходиться у режимі очікування. Й хоча кількість відкритих мереж і зменшується у відсотковому еквіваленті, але абсолютна кількість зростає через зростаючу популярність мобільних пристроїв. Цьому сприяє високий енергетичний потенціал радіоліній [64], помітний внесок у який дають антени передавального і приймального обладнання

$$P_{\text{пр}} = \frac{G_{\text{пер}} \cdot A_{\text{еф.пл.пр}} \cdot \eta}{4\pi \cdot \gamma \cdot R_{\text{зв}}^2} P_{\text{пер}}, \tag{1.20}$$

де $G_{\text{пер}}$ – коефіцієнт підсилення антени передавача; $A_{\text{еф.пл.пр}}$ – ефективна площа антени приймача, яка може бути визначена через довжину хвилі λ і коефіцієнт підсилення антени приймача $G_{\text{пр}}$

$$A_{\text{еф.пл.пр}} = \frac{\lambda^2 \cdot G_{\text{пр}}}{4\pi}; \tag{1.21}$$

η – коефіцієнт узгодження за поляризацією; γ – коефіцієнт розрізнення; $R_{\text{зв}}$ – дальність зв'язку; $P_{\text{пер}}$ – потужність передавача. (Мається на увазі, що антени орієнтовані максимумами ДС одна на одну).

Підвищення коефіцієнтів підсиленні антени можна досягти збільшенням геометричних розмірів і застосуванням рівномірних амплітуд розподілів струмів. Щоправда, при використанні спрямованих антен може виникнути ситуація, коли енергія поля за межами будівель буде перевищувати норми, встановлені законодавчо [62]. Також з огляду на резолюцію ПАРЄ щодо впливу УКХ випромінювання на живі організми [14], постає завдання по зменшенню неспрямованого випромінювання і використання передавачів зі зниженою потужністю. Між тим, застосування суто спрямованих антен у телекомунікаційних системах вступає у протиріччя з основною вимогою до таких систем: забезпечити зв'язок із заданою кількістю абонентських терміналів незалежно від їх азимутального (і частково кутомісного) розташування, що потребує використання неспрямованої антени і позбавляє необхідності орієнтувати за кутами абонентське обладнання.

Певним кроком для розв'язання цього протиріччя є застосування додаткової фокусуючої лінзи, яка буде вирівнювати фронт хвилі, збільшуючи таким чином щільність потоку електромагнітної хвилі в певному напрямку. Такий підхід не потребує конструктивної зміни існуючого обладнання, а лінза є автономним доповненням. Перевагу доцільно віддати прискорюючій лінзі (ПЛ), яка легка і проста у виготовленні порівняно з уповільнюючою. З одного боку, ПЛ може застосувати абонент, який потребує підвищення відношення сигнал/шум на вході свого приймача в умовах високого рівня шумового фону або збільшення максимальної відстані у відповідності до (1.20). Абоненту лише потрібно зорієнтувати у напрямку ТБД систему: штатна антена з ПЛ. З іншого боку, ПЛ можна застосувати у складі ТБД для підвищення якості зв'язку з окремим абонентом за рахунок фокусування енергії в його напрямку (наприклад, у корпоративних мережах для покриття віддалених або важко доступних частин будівлі). Звичайно, в цьому випадку також потрібно орієнтувати ПЛ в необхідному напрямку, але в теоретико-прикладному плані у цій ситуації гостріше постає потреба у визначенні впливу ПЛ на ДС антени, тобто визначення просторової ДС системи із штатної антени ТБД і ПЛ. Нижче приведені деякі результати теоретичних і експериментальних досліджень щодо використання ПЛ.

На фізичному рівні можна виділити декілька шляхів розвитку ПЛ:

вибір і адаптація конструкції до конкретного частотного діапазону [66];

виявлення і усунення конструктивних недоліків [67];

застосування багатопроменевих або багатоканальних систем [68];

узгодження антенних систем передавача і приймача за напрямком головного пелюстка, поляризацією тощо [69].

Висновки до першого розділу

В Україні та всьому світі розповсюдження Wi-Fi мереж ґрунтується на відповідних законодавчих ініціативах. З подальшим повсюдним переходом на стандарт 802.11n з максимальною швидкістю передачі 300 Мбіт/с можна прогнозувати стрімкий перехід провайдерів на безпроводові методи надання телекомунікаційних послуг. Разом з тим, поширеність безпроводових технологій, навіть коли користувачі працюють за стаціонарними робочими станціями, але в мережу входить один або декілька безпроводових сегментів та неспроможність традиційних засобів захисту протидіяти сторонньому кібернетичному впливу останнім часом, по-перше, вимагає захисту в тому числі і віддалених користувачів й, по-друге, ставить під загрозу інформацію, та власне самі безпроводові мережі в яких інформації циркулює.

Для кожного з існуючих типів безпроводових мереж (домашніх, загальнодоступних і корпоративних) характерними є як власна модель загроз, так і власне дерево атак. Дерева атак в сукупності з ТБД-приманками (AP Honeypots), спеціальним скануючим обладнанням, а також SSL і SSH використовуються для своєчасного виявлення та ідентифікації категорії нападу на безпроводові мережі.

Зважаючи на таке, при створенні безпроводових мереж пропонується дотримуватись певних правил для забезпечення їх функціональної безпеки та живучості, а також покращення якості прийому і/або розширення зони покриття, а саме:

1) застосовувати віртуальні канали, RADIUS-сервери і мережеві екрани;

2) використовувати електромагнітну прискорюючу металопластинчасту циліндричну лінзу [63–65];

3) проводити планове оновлення ПЗ і мікропрограм мережевого апаратного забезпечення;

4) не використовувати (по можливості) DHCP-сервери і стандартні засоби для зберігання даних.

Це дозволить, застосовуючи аналізатори спектра з роздільною здатністю зіставною з шириною підканалів, оперативно збирати дані (для цього з метою дослідження певного каналу достатньо не більше 1 хв.) та оперативно протидіяти виявленим атакам (на пізніх стадіях враховуючи, що швидкість протидії повинна бути порівняна з швидкістю атаки, у адміністратора на протидію залишатиметься приблизно в півтора рази більше часу). При цьому в процесі завантаження спектру можуть виникнути два можливих варіанти рішень: проводити перевірку у певний момент часу для короткочасного сеансу або вибирати частоти стаціонарної ТБД.

Їх порівняння може бути проведене за рахунок використання різних моделей OFDM-сигналу, які характеризуються інтегральною потужністю, врахуванням додаткових вузлів передавача, середовища і приймача або математичним описом.

Список використаних джерел у першому розділі

1. Степашкин М. В. Модели и методика анализа защищенности компьютерных сетей на основе построения деревьев атак : дис. канд. тех. наук : 05.13.11, 05.13.19. Санкт-Петерб. инст. инф. и автом. РГН, 2007.196 с.

2. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Київ : Департамент спеціальних телекомунікаційних систем та захисту інформації, 1999. 53 с. (Служба безпеки України).

3. Основи інформаційної безпеки / Андрєєв В. І. та ін. ; за ред. В. О. Хорошка. 2-е вид. Київ, 2009. 292 с.

4. Гордейчик С. Безопасность беспроводных LAN. *Беспроводные технологии*. 2004. №2. С. 51–52.

5. Филиппов М. Г. Вопросы обеспечения безопасности корпоративных беспроводных сетей стандарта 802.11. Специфика России. *Сети*. 2003. №7.

6. Деева Д. А. Методы обеспечение безопасности сетей стандарта 802.11. *Актуальные проблемы современной науки и образования: Естественные науки* : материалы Всеросс. научн.-практ. конф., февраль 2010 г. Уфа : РИЦ БашГУ, 2010. С. 161–164.

7. Соколов В. Ю. Підвищення захищеності Wi-Fi мереж: пошук триває. *Зв'язок*. 2011. №1 (93). С. 53–57.

8. Атаки на беспроводные сети. Часть 1. 2004. URL: https://www.securitylab.ru/analytics/216360.php (дата звернення: 29.03.2019).

9. Защита от DDoS атак. 2012. URL: http://www.digilex.ru/ (дата звернення: 29.03.2019).

10. Бандурян А. Анализ угроз для беспроводных сетей. *Компьютерное обозрение*. 2010. №12 (723). С. 21–25.

11. Червяков А. С. Угрозы и риски безопасности сетей стандарта Wi-Fi. *Высокие интеллектуальные технологии и инновации в образовании и науке* : материалы XVII Межд. научн.-метод. конф., 11–12 февраля 2010 г. С-Пб.: Изд-во Политех. ун-та, 2010. С. 131,132.

12. Уязвимости корпоративных информационных систем. 2017. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/Corp-Vulnerabilities-2017-rus.pdf (дата звернення: 29.03.2019).

13. IP Spoofing: An Introduction. 2003. URL: http://www.symantec.com/connect/articles/ip-spoofing-introduction (дата звернення: 29.03.2019).

14. Петренко С. А., Беляев А. В. Безопасная беспроводная корпоративная сеть. *Wireless Ukraine*. 2009. №2–3 (3). С. 20–24.

15. Wireless Attacks Primer. 2003. URL: http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html (дата звернення: 29.03.2019).

16. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. Москва, 2010. 232 с.

17. Соколов В. Ю., Карацюба К. І. Використання дерев атак для аналізу захищеності безпроводових технологій стандарту IEEE 802.11. *Вісник ДУІКТ*. 2012. Т. 10, №1. С. 42–49.

18. Шварцман В. О. Количественная оценка защищенности информации и сетей связи от несанкционированных действий. *Электросвязь*. 2008. №5. С. 5–8.

19. Нечунаев В. М. Оценка рисков информационной безопасности корпоративной информационной системы. *Доклады ТУСУРа*. 2009. №1 (19), ч. 2. С. 51–53.

20. Давыдов И. В., Шелупанов А. А. Формализация модели совершения киберпреступлений, совершаемых с использованием вредоносных кодов. *Известия Томского политехн. ун-та*. 2006. Т. 309, №8. С. 126–129.

21. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. Київ, 2001. 688 с.

22. Чипига А. Ф., Пелешенко В. С. Оценка эффективности защищенности автоматизированных систем от несанкционированного доступа. *Вестник СевКавГТУ*. 2004. №1 (8). С. 40.

23. Проблеми забезпечення контролю захищеності корпоративних мереж та шляхи їх вирішення / Бурячок В. Л. та ін. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. №3. С. 48–61.

24. Соколов В. Ю. Порівняння можливих підходів щодо розробки низькобюджетних аналізаторів спектру для сенсорних мереж діапазону 2,4–2,5 ГГц. *Кібербезпека: освіта, наука, техніка*. 2018. №2. С. 31–46. DOI: 10.28925/2663-4023.2018.2.3146.

25. Соколов В. Ю. Порівняння математичних і функціональних моделей широкосмугових сигналів з ортогональним частотним розділенням. *Управління розвитком складних систем*. 2010. №4. С. 109–113.

26. Бурячок В. Л. Застосування бездротових мереж в ході організації та проведення розвідки систем телекомунікацій. *Захист інформації*. 2013. Т. 15. №4. С. 284–291. DOI: 10.18372/2410-7840.15.5711.

27. Некоторые улучшения OCG и работа с ними. 2012. URL: http://www.radioscanner.ru/info/article220/ (дата звернення: 29.03.2019).

28. LabVIEW Modulation Toolkit OFDM Example. 2006. URL: http://zone.ni.com/devzone/cda/epd/p/id/3456 (дата звернення: 29.03.2019).

29. Understanding an OFDM Transmission. 2008. URL: http://www.dsplog.com/2008/02/03/understanding-an-ofdm-transmission/ (дата звернення: 29.03.2019).

30. IEEE 802.11-2007. IEEE Standard for Information Technology. Telecommunications and Information Exchange between Systems. Local and Metropolitan Area Networks. Specific Requirements, 2007. 1232 p. (IEEE Computer Society).

31. Про затвердження Плану використання радіочастотного ресурсу України від 9 червня 2006 р. №815. URL: https://zakon.rada.gov.ua/laws/show/815-2006-%D0%BF (дата звернення: 29.03.2019).

32. Ларин В. Ю., Хандильды А. В., Купцов В. И. Исследование модели генератора группового спектра сигнала. *Вісник інженерної академії України*. 2008. №3–4. С. 115–119.

33. Banitsas K. A., Song Y. H., Owens T. OFDM over IEEE 802.11b Hardware for Telemedical Applications. 2004. 18 p.

34. Selby S., Amini A., Edelman C. Simulating Interference Issues between Bluetooth PANs and 802.11 b and 802.11g WLANs. 2008. 15 p.

35. AirView Spectrum Analyzer. 2014. URL: https://dl.ubnt.com/datasheets/airmax/UBNT_DS_airView.pdf (дата звернення: 29.03.2019).

36. Open Flash Chart 2. 2018. URL: http://teethgrinder.co.uk/open-flash-chart-2/ (дата звернення: 29.03.2019).

37. Статистика : Підручник / С. С. Герасименко та ін. 2-е вид. Київ, 2000. 467 с.

38. Соколов В. Ю. Принципи реалізації систем роумінгу у мережах стандарту IEEE 802.11. *Світ інформації і телекомунікацій – 2012*: матеріали IX Міжнар. наук.-техн. конф., 17, 18 травня 2012 р. Київ : ДУІКТ, 2012. С. 84,85.

39. Скворцов А. В. Триангуляция Делоне и ее применение. Томск, 2002. 128 с.

40. Скворцов А. В. Комплексное исследование и разработка эффективных вычислительно устойчивых алгоритмов вычислительной геометрии и их реализация в геоинформационной системе: автореф. док. тех. наук : 05.13.18. Том. ун-т, 2002. 40 с.

41. Соколов В. Ю. Застосування діаграм Вороного для побудови безпроводових мереж стандарту IEEE 802.11 з роумінгом. *Сучасні тенденції розвитку в інфокомунікаціях та освіті* : матеріали VIII Наук. конф., 24, 25 лист. 2011 р. Київ : ДУІКТ, 2011. С. 359,360.

42. Статистика уязвимостей web-приложений за 2008 год. URL: https://www.ptsecurity.com/ru-ru/download/WASS-SS-2008-ru.pdf (дата звернення: 29.03.2019).

43. Безопасность АСУ ТП в цифрах. 2016. URL: https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf (дата звернення: 29.03.2019).

44. Каталков Д. Уязвимости корпоративных информационных систем в 2015 году. 2016. URL: https://www.ptsecurity.com/ru-ru/ics/Webinar_14042016.pdf (дата звернення: 29.03.2019).

45. Бурячок В. Л., Козачок В. А., Складанний П. М. Пентестінг як інструмент комплексної оцінки ефективності захисту інформації в розподілених корпоративних мережах. *Сучасний захист інформації*. 2015. №3. С. 4–12.

46. Positive Technologies MaxPatrol. URL: ftp://public.dhe.ibm.com/software/security/products/qradar/documents/iTeam_addendum/m_vuln_MaxPatrol.pdf (дата звернення: 29.03.2019).

47. Бурячок В. Л., Борсуковський Ю. В., Складанний П. М. Аналіз сучасних вимог до створення парольних політик корпоративних користувачів. *Сучасний захист інформації*. 2016. №3. С. 72–76.

48. Впровадження європейської кібербезпеки: загальний огляд. 2014. URL: http://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf (дата звернення: 29.03.2019).

49. Дорофеев А. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? *Защита информации. Инсайд*. 2010. №6 (36). С. 72-73.

50. Лепихин В. Б. Сравнительный анализ сканеров безопасности. Pentest. Москва, 2008. 50 с.

51. Бурячок В. Л., Соколов В. Ю. Технологія забезпечення об’єктивного контролю захищеності корпоративних інформаційно-телекомунікаційних систем і ме-

реж. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : матеріали Всеукр. наук.-практ. конф., 23 лист. 2018 р. Харків : ХНУВС, 2018. С. 242–247.

52. WiGig Alliance promotes faster short range WiFi. 2010. URL: https://www.techworld.com/news/data/wigig-alliance-promotes-faster-short-range-wifi-3222952/ (дата звернення: 29.03.2019).

53. Wi-Fi Alliance and WiGig sync up for 60GHz WiFi. 2010. URL: http://www.engadget.com/2010/05/10/wi-fi-alliance-and-wigig-sync-up-for-60ghz-wifi/ (дата звернення: 29.03.2019).

54. Богуш В. В., Соколов В. Ю. Дослідження захищеності Wi-Fi мереж. *Зв'язок*. 2009. №4 (88). С. 29–31.

55. Соловьев В. Р., Богуш В. В., Соколов В. Ю., Соловьева М. В. К вопросу о совершенствовании методики защиты информации от помех и вирусных атак в системах подвижной связи. Системный подход. *Зв'язок*. 2010. №1 (89). С. 54–61.

56. WiFi на Asus P535. 2010. URL: https://www.kaa.org.ua/ru/23-asusp535/49-wifi-%D0%BD%D0%B0-asus-p535.html (дата звернення: 29.03.2019).

57. IEEE. Organizationally Unique Identifier. 2019. URL: http://standards-oui.ieee.org/oui/oui.txt (дата звернення: 29.03.2019).

58. IEEE. Individual Address Block. 2019. URL: http://standards-oui.ieee.org/iab/iab.txt (дата звернення: 29.03.2019).

59. Мартынюк И. В. Безопасность – это процесс. *Компьютерное обозрение*. 2005. №26. С. 30–33.

60. Airodump-ng. 2018. URL: http://www.aircrack-ng.org/doku.php?do=show&id=airodump-ng (дата звернення: 29.03.2019).

61. Белоцерковский Г. Б. Основы радиотехники и антенны. Ч. II. Антенны. Москва, 1969. 328 с.

62. Про затвердження Переліку радіоелектронних засобів та випромінювальних пристроїв від 4 лют. 2010 р. №51. URL: https://zakon.rada.gov.ua/laws/show/z0201-15 (дата звернення: 29.03.2019).

63. Радиоэлектронные системы: основы построения и теория. Справочник / Ширман Я. Д. и др. Москва, 1998. 828 с.

64. Заикин И. П., Тоцкий А. В., Абрамов С. К. Проектирование антенных устройств систем связи. Учебное пособие. Харьков, 2007. 78 с.

65. Шифрин Я. С. Антенны. Харьков, 1976. 408 с.

66. Астапеня В. М., Соколов В. Ю. Використання прискорювальної лінзи для підвищення ефективності та завадозахищеності мереж IEEE 802.11b. *Зв'язок*. 2012. №2 (98). С. 33–37.

67. Astapenya V. M., Sokolov V. Yu. Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane. *Antenna Theory and Techniques (ICATT'2017)* : in XI Int. Conf., 24–27 May 2017. Kyiv : IEEE, 2017. P. 389–391. DOI: 10.1109/icatt.2017.7972671.

68. Астапеня В. М., Соколов В. Ю. Підвищення доступності інформації у бездротових системах на основі використання прискорюючої металопластинчастої лінзи. *Сучасні інформаційно-комунікаційні технології (COMINFO'2015)* : матеріали IX Міжнар. наук.-техн. конф., 17–20 лист. 2015 р. Київ : ДУТ, 2015. С. 67–71.

69. Астапеня В. М., Соколов В. Ю. Підвищення пропускної здатності безпроводових каналів зв'язку на основі поляризаційних ефектів у мережах IEEE 802.11. *Зв'язок*. 2012. №3 (99). С. 36–41.

Розділ 2

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ТА ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БЕЗПРОВОДОВОЇ ІНФРАСТРУКТУРИ

Розвиток і широке поширення безпроводових технологій призводить до постійного зростання кількості користувачів і пристроїв. При цьому збільшення кількості безпроводових мереж веде до взаємного впливу мереж одна на одну, а зростання кількості безпроводових користувачів в обмеженому частотному діапазоні – до міжканальної і просторової інтерференції. Це в кінцевому результаті впливає на пропускну здатність безпроводових каналів і навіть на їх працездатність в цілому, а також на ступень захисту безпроводових мереж від проявів стороннього кібернетичного впливу.

2.1. Методи забезпечення гарантоздатності безпроводових мереж

На стан безпеки систем безпроводового зв’язку останнім часом суттєво впливає збільшення кількості мобільних пристроїв та вбудованих систем, які можуть бути використані, в разі потреби, як ТБД (наприклад, модулі сімейства ESP8266 та ESP32). З динамікою зростання кількості ТБД і їх потенційно можливою кількістю в найближчому майбутньому (на рис. 2.1 теоретична крива показана штриховим пунктиром, а реальна – суцільною лінією) можна за результатами аналізу статистичних даних з 2001 по 2016 роки, що були зібрані та оприлюднені компанією Wireless Geographic Logging Engine [1].

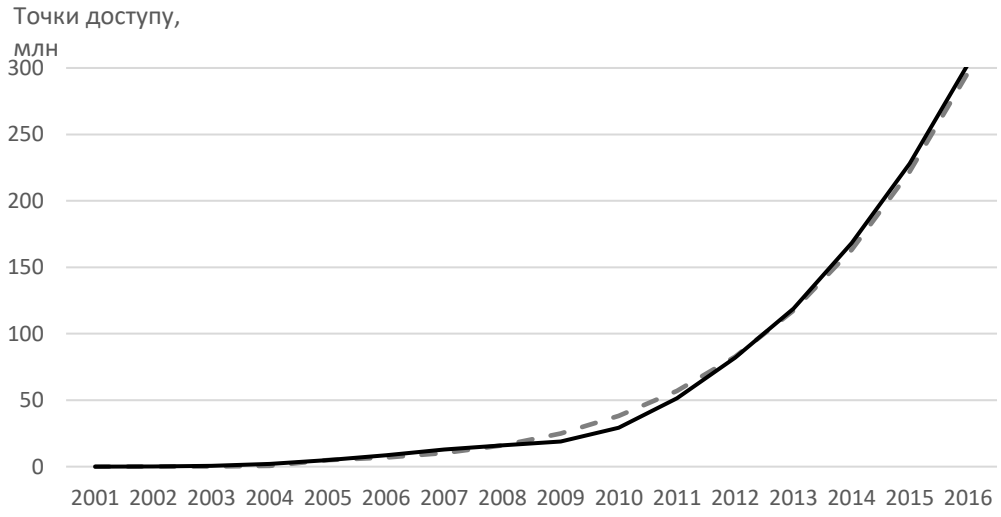


Рис. 2.1. Зростання кількості ТБД

Процес росту кількості ТБД на кінець кожного року може бути описаний ступеневою функцією:

$$N(Y) = (Y - 2000)^{4,54} + 3450, \quad (2.1)$$

де Y – обліковий рік. Екстраполюючи графік, так до початку 2018 року слід очікувати майже 400 млн ТБД.

Такий стан справ може кінець-кінцем негативно вплинути на розподіл та використання частотного ресурсу, врегулювати які ані централізованим плануванням безпроводової інфраструктури, ані регуляторним моніторингом та адаптацією систем вручну, ані введенням адаптивних систем налаштування на рівні протоколів, моніторингу та автокорегування на рівні приймального тракту, застосуванням додаткових пристроїв для збирання інформації про стан безпроводової системи, – зробити буде просто неможливо.

2.1.1. Метод модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж

Прямокутна квадратурна амплітудна модуляція не є енергетично найбільш ефективним методом кодування цифрових 2^k-послідовностей, але вона отримала поширення через відносну простоту реалізації, в результаті чого прийнята у стандартах IEEE 802.11a і 802.16 (Wi-Fi і WiMAX). Існує декілька шляхів зменшення впливу широкосмугових каналів, які працюють в одній частотній смузі: максимальне рознесення несучих частот або мереж, використання направлених антен і кодів згортки. Всі ці методи не вирішують головної проблеми невірно переданих слів (для 2^k-QAM кожне слово складається з k бітів), а лише зменшують кількість помилок (symbol error rate, SER).

Для ефективного використання смуги частот потрібно модифікувати існуючу прямокутну квадратурну амплітудну модуляцію за простими правилами і досягти найбільшої евклідової метрики (дистанції) між базовим і модифікованим векторам (довжина вектору помилки).

Для синхронізації передавача і приймача використовуються службові підканали, на яких можна передавати інформації і про вид вектору: базовий або модифікований. Кожний вид повинен бути внесено до стандарту, і тільки в такому випадку використання модифікованого векторного простору можливе для розповсюдження у промислових масштабах для безпровідних мереж.

Розглянемо можливі варіанти модифікації базового простору комплексних векторів підканалів. В якості основних параметрів системи будемо розглядати евклідову відстань між векторами всередині векторного базового і модифікованого простору. Вектор задається у вигляді:

$$R = Q + i \cdot I, \tag{2.2}$$

де Q – дійсна координата, а I – уявна.

Для базового векторного простору мінімальна відстань між векторами становить $r_{\text{вн}} = 2{,}000$ для векторних просторів, які стандартно використовується для 2^k-QAM, а зовнішня – $r_{\text{зовн}} = 0{,}000$. Тому віддалення складає:

$$\Delta_{\text{ном}} = r_{\text{вн}} - r_{\text{зовн}} = 2{,}000, \tag{2.3}$$

що означає максимальне перекриття при використанні двох систем з базовим векторним простором. Чим менше віддалення, тим стабільніше будуть працювати обидві системи.

Для векторного простору також визначається коефіцієнт нормування (scaling factor) для нормалізації середньої енергії до одиниці (іноді використовується обернений запис коефіцієнта нормування). Цей коефіцієнт вказує на енергетичну оптимальність векторного простору, чим коефіцієнт менший, тим оптимальніше використовується енергія сигналу. Порівнювати можна лише коефіцієнти, які відносяться до одного виду модуляції.

Базовий векторний простір можна описати $R = \{\pm(2m-1) \pm (2m-1)i\}$, $m \in Z$, $m \in \overline{1,a}$, де $a = {\sqrt{2^k}}/{2} = 2^{\frac{k-2}{2}}$ – кількість разів, яку використовується проекція кожної амплітуди вектору на дійсну і уявну вісі, яка з фізичної точки зору представляє собою половину сторони квадратного векторного простору.

Для базового векторного простору коефіцієнт нормування становить [2,3] (так як середня енергія дійсної і уявної проекцій однакова для симетричного векторного простору, то уявна частина буде дорівнювати дійсній):

$$\begin{gathered} k_s = \sqrt{E_{\text{сер}}[|R|^2]} = \sqrt{E_{\text{сер}}[\text{Re}|R|^2] + E_{\text{сер}}[\text{Im}|R|^2]} = \sqrt{2E_{\text{сер}}[\text{Re}|R|^2]} = \\ = \sqrt{2 \cdot \frac{a}{n}\sum_{m=1}^{a}(2m-1)^2} = \sqrt{2 \cdot \frac{a}{n} \cdot \frac{1}{3} \cdot a \cdot (4a^2-1)} = \sqrt{\frac{2}{3} \cdot \frac{a^2}{n} \cdot (4a^2-1)} = \\ = \sqrt{\frac{2}{3} \cdot \frac{2^{\frac{k-2}{2} \cdot 2}}{2^{k-2}} \cdot \left(4 \cdot 2^{\frac{k-2}{2} \cdot 2} - 1\right)} = \sqrt{\frac{2}{3}(2^k - 1)}, \end{gathered} \tag{2.4}$$

де $n = {2^k}/{4} = 2^{k-2}$ – кількість точок в кожному квадранті; таблична сума ступенів натуральних чисел є $\sum_{m=1}^{a}(2m-1)^2 = \frac{1}{3}\cdot a\cdot(4a^2-1)$ [4].

Тоді для двох видів модуляції маємо $k_s^{16\text{QAM}} = \sqrt{10} \approx 3{,}162$ і $k_s^{64\text{QAM}} = \sqrt{42} \approx 6{,}481$.

Найпростіше перетворення отримується обертанням базового простору на 45° (див. рис. 2.2а для 16-QAM, квадратами вказано базовий векторний простір, а ромбами – його модифікація), перетворення проводиться за системою:

$$\begin{cases} Q = \sqrt{Q_0^2 + I_0^2}\cos\left(\alpha \pm \frac{\pi}{4}\right), \\ I = \sqrt{Q_0^2 + I_0^2}\sin\left(\alpha \pm \frac{\pi}{4}\right), \end{cases} \tag{2.5}$$

де (Q_0, I_0) – початкові координати вектору; $\text{tg}\alpha = \frac{I_0}{Q_0}$ для $\alpha \le 2\pi$ (знак «+» означає обертання проти, а «–» – за годинниковою стрілкою).

В даному випадку мінімальна відстань між векторами залишається незмінною $r_{\text{вн}} = 2{,}000$, зовнішня мінімальна відстань для 16-QAM – $r_{\text{зовн}}^{16\text{QAM}} = \sqrt{2(10-7\sqrt{2})} \approx 0{,}448$, а для 64-QAM – $r_{\text{зовн}}^{64\text{QAM}} = \sqrt{2(58-41\sqrt{2})} \approx 0{,}186$. Тобто $\Delta_{\text{об}}^{16\text{QAM}} \approx 1{,}552$ і $\Delta_{\text{об}}^{64\text{QAM}} \approx 1{,}814$, що вказує на часткове перетинання векторних просторів. При обертанні змінюється лише поляризація векторного простору, а коефіцієнт нормування залишається таким самим, як і у базового простору.

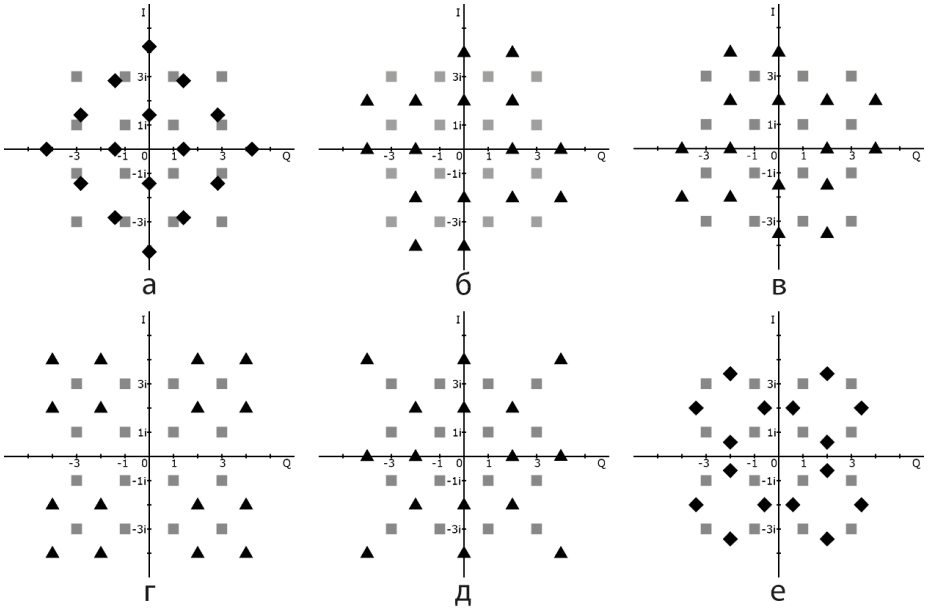


Рис. 2.2. Модифікація векторного простору для 16-QAM: обертання на 45° (а); зміщення проти (б) та за (в) годинникової стрілки; нормальне (г) та компактне (д) віддалення від початку координат; обертання групи на 45° (е)

В першому випадку симетрію в кожному із квадрантів було збережено, але якщо знехтувати симетрією можна отримати два перетворення: зміщення проти і за годинниковою стрілкою (див. рис. 2.2б і 2.2в, квадратами вказано базовий векторний простір, а трикутниками – його модифікація). Для кожного з квадрантів при зміщені (перший знак у відповідає зміщенню проти годинникової стрілки, а другий – за) маємо сукупність виду:

$$\begin{matrix}[\mathrm{I}]\\[\mathrm{II}]\\[\mathrm{III}]\\[\mathrm{IV}]\end{matrix}\begin{cases}R = R_0 + (\mp 1 \pm i),\\ R = R_0 + (\mp 1 \mp i),\\ R = R_0 + (\pm 1 \mp i),\\ R = R_0 + (\pm 1 \pm i).\end{cases} \tag{2.6}$$

Для визначення коефіцієнта нормування приведемо координати векторів для першого квадранта (для зміщення проти годинникової стрілки, але для обох варіантів значення коефіцієнтів однакові):

$$\begin{gathered}16\mathrm{QAM}: \{2i; 4i; 2+2i; 2+4i\};\\ 64\mathrm{QAM}: \begin{Bmatrix} 2i; 4i; 6i; 8i\\ 2+2i; 2+4i; 2+6i; 2+8i\\ 4+2i; 4+4i; 4+6i; 4+8i\\ 6+2i; 6+4i; 6+6i; 6+8i \end{Bmatrix},\end{gathered} \tag{2.7}$$

Тоді з (2.4) визначаються коефіцієнти нормування:

$$\begin{aligned} k_{s\,\text{зм}}^{16\mathrm{QAM}} &= \sqrt{\tfrac{1}{2^{4-2}}[2^2 + 4^2 + 2^2 + 2^2 + 2^2 + 4^2]} = 2\sqrt{3} \approx 3{,}464,\\ k_{s\,\text{зм}}^{64\mathrm{QAM}} &= \sqrt{\tfrac{1}{2^{6-2}}[8\cdot 2^2 + 8\cdot 4^2 + 8\cdot 6^2 + 4\cdot 8^2]} = 2\sqrt{11} \approx 6{,}633. \end{aligned} \tag{2.8}$$

Аналогічно для збереження симетрії можна побудувати віддалення від початку координат (див. рис. 2.2г) за правилом:

$$\begin{matrix}[\mathrm{I}]\\[\mathrm{II}]\\[\mathrm{III}]\\[\mathrm{IV}]\end{matrix}\begin{cases}R = R_0 + (+1 + i),\\ R = R_0 + (-1 + i),\\ R = R_0 + (-1 - i),\\ R = R_0 + (+1 - i).\end{cases} \tag{2.9}$$

Для всіх трьох випадків мінімальна відстань між векторами становить $r_{\text{вн}} = 2{,}000$, а зовнішня – $r_{\text{зовн}} = \sqrt{2} \approx 1{,}414$. Віддалення становить $\Delta_{\text{зм}} \approx 0{,}586 > \Delta_{\text{об}}^{16\mathrm{QAM}} > \Delta_{\text{об}}^{64\mathrm{QAM}} > \Delta_{\text{ном}}$, що набагато краще, ніж у випадку обертання навколо початку координат.

Аналогічно до зміщень проти і за годинниковою стрілкою визначаються коефіцієнти нормування віддалення від центру. Координати векторів для першого квадранта:

$$\begin{gathered}16\text{QAM}: \{2+2i; 2+4i; 4+2i; 4+4i\}; \\ 64\text{QAM}: \begin{Bmatrix} 2+2i; 2+4i; 2+6i; 2+8i \\ 4+2i; 4+4i; 4+6i; 4+8i \\ 6+2i; 6+4i; 6+6i; 6+8i \\ 8+2i; 8+4i; 8+6i; 8+8i \end{Bmatrix},\end{gathered} \tag{2.10}$$

Тоді з (2.4) визначаються коефіцієнти нормування:

$$\begin{gathered}k_{s\ \text{від}}^{16\text{QAM}} = \sqrt{\frac{1}{2^{4-2}}\left[4 \cdot 2^2 + 4 \cdot 4^2\right]} = 2\sqrt{5} \approx 4{,}472, \\ k_{s\ \text{від}}^{64\text{QAM}} = \sqrt{\frac{1}{2^{6-2}}\left[8 \cdot 2^2 + 8 \cdot 4^2 + 8 \cdot 6^2 + 8 \cdot 8^2\right]} = 2\sqrt{15} \approx 7{,}746.\end{gathered} \tag{2.11}$$

Крім простого зміщення можна використовувати компактні модифікації зміщення, приклад якого показаний на рис. 2.2д, але вони складні в реалізації. Координати векторів для першого квадранта компактного віддалення:

$$\begin{gathered}16\text{QAM}: \{2i; 4i; 2+2i; 4+4i\}; \\ 64\text{QAM}: \begin{Bmatrix} 2i; 4i; 6i; 8i \\ 2+2i; 2+4i; 2+6i \\ 4+2i; 4+4i; 4+6i; 4+8i \\ 6+2i; 6+4i; 6+6i \\ 8+6i; 8+8i \end{Bmatrix},\end{gathered} \tag{2.12}$$

Тоді з (2.4) визначаються коефіцієнти нормування:

$$\begin{gathered}k_{s\ \text{від.комп}}^{16\text{QAM}} = \sqrt{\frac{1}{2^{4-2}}\left[3 \cdot 2^2 + 3 \cdot 4^2\right]} = \sqrt{15} \approx 3{,}873, \\ k_{s\ \text{від.комп}}^{64\text{QAM}} = \sqrt{\frac{1}{2^{6-2}}\left[7 \cdot 2^2 + 9 \cdot 4^2 + 7 \cdot 6^2 + 5 \cdot 8^2\right]} = \sqrt{\frac{93}{2}} \approx 6{,}819.\end{gathered} \tag{2.13}$$

Але в кожному попередньому випадку потрібне збільшення максимальної амплітуди окремих векторів. Запропонована схема має навіть меншу максимальну амплітуду (на $7\sqrt{2} - \sqrt{2\left(37 + 6\sqrt{2}\right)} \approx 0{,}361$), залишається симетричною і не потребує складного перетворення. Так як базовий векторний простір складається з квадратних елементів, то кожний елемент можна обертати на 45° окремо від інших (див. рис. 2.2е, квадратами вказано базовий векторний простір, а ромбами – його модифікація). Рівняння перетворення має вигляд:

$$\begin{cases} Q = Q_{\text{ц}} + r \cdot \cos\left(\alpha \pm \frac{\pi}{4}\right), \\ I = I_{\text{ц}} + r \cdot \sin\left(\alpha \pm \frac{\pi}{4}\right), \end{cases} \tag{2.14}$$

де $(Q_{\text{ц}}, I_{\text{ц}})$ і (Q_0, I_0) – центр обертання і початкові координати вектору, $\text{tg}\alpha = \frac{I_0 - I_{\text{ц}}}{Q_0 - Q_{\text{ц}}}$ для $\alpha \leq 2\pi$, $r = \sqrt{2}$ – радіус обертання (знак «+» означає обертання проти, а «–» – за годинниковою стрілкою).

Для всіх трьох випадків мінімальна відстань між векторами становить $r_{\text{вн}} = 2\left(2 - \sqrt{2}\right) \approx 1{,}172$, а зовнішня – $r_{\text{зовн}} = \sqrt{r_{\text{вн}}} = \sqrt{2\left(2 - \sqrt{2}\right)} \approx 1{,}082$. Віддалення становить $\Delta_{\text{об.гр}} \approx 0{,}090 > \Delta_{\text{зм}} > \Delta^{16\text{QAM}} > \Delta^{64\text{QAM}} > \Delta_{\text{ном}}$, що є найкращим результатом у порівнянні з модифікаціями, розглянутими раніше.

Координати векторів для першого квадранта обертання групи на 45°:

$$\begin{gathered} 16\text{QAM}: \left\{2 + \left(2 \pm \sqrt{2}\right)i; \left(2 \pm \sqrt{2}\right) + 2i\right\}; \\ 64\text{QAM}: \begin{Bmatrix} 2 + \left(2 \pm \sqrt{2}\right)i; \left(2 \pm \sqrt{2}\right) + 2i \\ 2 + \left(6 \pm \sqrt{2}\right)i; \left(2 \pm \sqrt{2}\right) + 6i \\ 6 + \left(2 \pm \sqrt{2}\right)i; \left(6 \pm \sqrt{2}\right) + 2i \\ 6 + \left(6 \pm \sqrt{2}\right)i; \left(6 \pm \sqrt{2}\right) + 6i \end{Bmatrix}, \end{gathered} \tag{2.15}$$

Тоді з (2.21) визначаються коефіцієнти нормування:

$$\begin{gathered} k_{s\ \text{об.гр}}^{16\text{QAM}} = \sqrt{\frac{2^2 + \left(2+\sqrt{2}\right)^2 + 2^2 + \left(2-\sqrt{2}\right)^2}{2^{4-2}}} = \sqrt{10} \approx 3{,}162, \\ k_{s\ \text{об.гр}}^{64\text{QAM}} = \sqrt{\frac{8 \cdot 2^2 + 8 \cdot 6^2 + 4 \cdot \left(\left(2+\sqrt{2}\right)^2 + \left(2-\sqrt{2}\right)^2 + \left(6+\sqrt{2}\right)^2 + \left(6-\sqrt{2}\right)^2\right)}{2^{6-2}}} = \\ = \sqrt{\frac{85}{2}} \approx 6{,}519. \end{gathered} \tag{2.16}$$

Теоретичний виграш при заміні двох систем на базовому векторі, двома системами на базовому і модифікованому векторах становить:

$$\delta = \frac{\Delta_{\text{б}} - \Delta_{\text{м}}}{\Delta_{\text{б}}} \cdot 100\%, \tag{2.17}$$

де $\Delta_{\text{б}}$ і $\Delta_{\text{м}}$ – віддалення для базового і модифікованого векторних просторів.

Результати розрахунків коефіцієнтів нормування приведені в табл. 2.1, звідки видно, що з усіх видів зміщення (віддалення) краще використовується енергія спектру у віддаленні з оптимізацією. Запропонований метод обертання групи по-

казав незначне погіршення енергетичних характеристик у порівнянні з базовим векторним простором, і лише при використанні 64-QAM.

Таблиця 2.1

Коефіцієнти нормування k_s, віддалення Δ і виграш δ

Векторний простір:	$k_s^{16\text{QAM}}$	$k_s^{64\text{QAM}}$	$\Delta^{16\text{QAM}}$	$\Delta^{64\text{QAM}}$	$\delta^{16\text{QAM}}$,%	$\delta^{64\text{QAM}}$,%
Базовий	3,162	6,481	2,000		–	
Обертання на 45°	3,162	6,481	1,552	1,814	22,4	9,3
Зміщення	3,464	6,633	0,586		70,7	
Віддалення	4,472	7,746				
Компактне віддалення	3,873	6,819				
Обертанням групи на 45°	3,162	6,519	0,090		95,5	

При збільшенні рівня завад збільшується кількість помилок підчас приймання сигналу. Можна зменшити селективність фільтра для кожного вектору, але таке зменшення призведе до збільшення кількості помилок від модифікованого простору векторів. Рішенням є переналаштування на модуляцію з меншим коефіцієнтом *k*.

До того ж не обов'язково переналаштовуватися обом системам: наприклад, простори векторів базового 16-QAM і модифікованого 64-QAM також не перетинаються [5].

З розглянутих модифікацій найкращою можна вважати обертання групи, так як в даному випадку зберігається симетрія, максимальна амплітуда майже не змінюється, використовую досить просте перетворення, досить рівномірно розподіляється у просторі і залишає місце для третьої модифікації базового простору. З точки зору енергетичної ефективності обертання групи майже не відрізняється від базового векторного простору, тому при реалізації на практиці можна не змінювати коефіцієнти підсилення вхідних ланок.

Наступним кроком з оптимізації смуги частот може бути побудова простору векторів третього і вищих порядків. Запропонована схема також являється актуальною для менш розповсюджених 256-QAM (*k* = 8) і 1024-QAM (*k* = 10).

2.1.2. Метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру

Одним із методів вирішення зазначеної проблеми в безпроводових мережах може бути адаптивний підбір вільних каналів передавання даних. Багато виробників безпроводового обладнання застосовують для цього вбудовані алгоритми автоматичного вибору вільних каналів. Але такий підхід дозволяє сканувати спектр лише в

області розташування ТБД, не враховуючи при цьому особливості розташування клієнтів (частотну обстановку в місці розташування всіх або вибіркових користувачів). ТБД починає працювати на самому вільному каналі в місці її розташування (див. рівні якості в табл. 2.2), що в певній мірі покращує роботу всієї мережі, але не робить її оптимальною (так як неможливо врахувати всі параметри в ad hoc мережі: поляризацію, висоту розташування, екранування, перевідбивання і переміщення користувача).

Для гарантованого вибору оптимального частотного каналу передавання даних наряду з вже існуючими безпроводовими адаптерами, область видимості яких часто обмежена лише мережами стандарту IEEE 802.11 (а деякі карти навіть не бачать «прихованих» мереж), доцільним є використання системи додаткових незалежних пристроїв (аналізаторів спектру). Така система складатиметься з ТБД (або в деяких системах з роумінгу) клієнтів і аналізаторів спектру, які підключаються до контролера або до клієнта через провідні зв'язки (з PoE).

Таблиця 2.2

Рівні якості сигналу для ТБД

Рівень сигналу, дБмВт	Якість	Технічні характеристики
менше –90	Неприпустима	Близький до шуму обладнання та фону. Будь-яка робота малоймовірна
від –90 до –81	Погана	Мінімальний рівень сигналу для підтримки цілісності мережі. Доставка пакетів може бути ненадійним
від –80 до –71	Прийнятна	Мінімальний рівень сигналу для надійної доставки пакетів, наприклад, електронної пошти, мережі
від –70 до –67	Дуже добра	Сила сигналу для програм, що вимагають дуже надійної, своєчасної доставки пакетів даних, наприклад, VoIP, потокове відео
більше –67	Відмінна	Максимально досяжний сигнал. Клієнт знаходиться в декількох метрах від передавача. Нетипова ситуація

Схема, показана на рис. 2.3, може або не може містити аналізатор спектру на стороні ТБД. Пунктирна лінія відображає аналізатор спектру, який або з'єднаний з ТБД, або є її частиною.

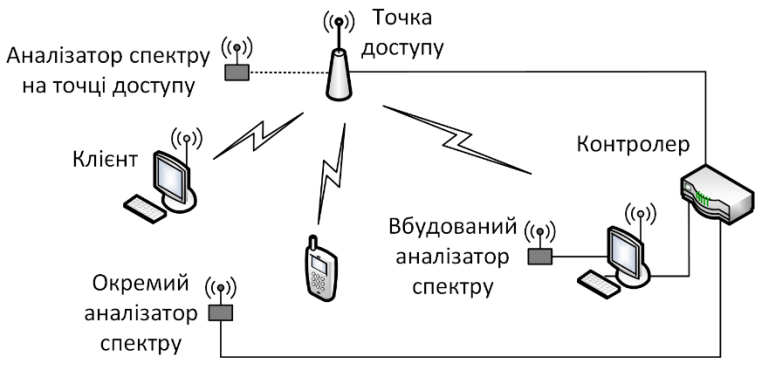


Рис. 2.3. Схема з аналізаторами спектру

Схема складається з:

контролеру, який розподіляє канали і навантаження в мережі, керуючи інфраструктурою безпроводового зв'язку;

ТБД, яка перемикається в тихий режим, дані збираються з доступних аналізаторів спектру або внутрішнього безпроводового інтерфейсу, зібрані дані надсилаються контролеру, ТБД може бути декілька;

клієнта, який збирає дані зі своєї власної безпроводової мережевої карти або з вбудованого аналізатора спектру і відправляє їх до контролера;

окремого аналізатора спектру, який має Ethernet-інтерфейс і передає дані безпосередньо до контролера.

Контролер отримує інформацію двох типів: від аналізаторів спектру, кожен із яких залежно від важливості розташування має власний ваговий коефіцієнт і від мережевих карт (формат вхідних даних відрізняється, але для кінцевого результату достатньо передати в контролер список каналів з мінімальним рівнем сигналу). Контролер вибирає вільний канал для кожної ТБД до мережі й ініціалізує передачу по новому каналу. Процес сканування повторюється. Алгоритм збору даних показаний на рис. 2.4.

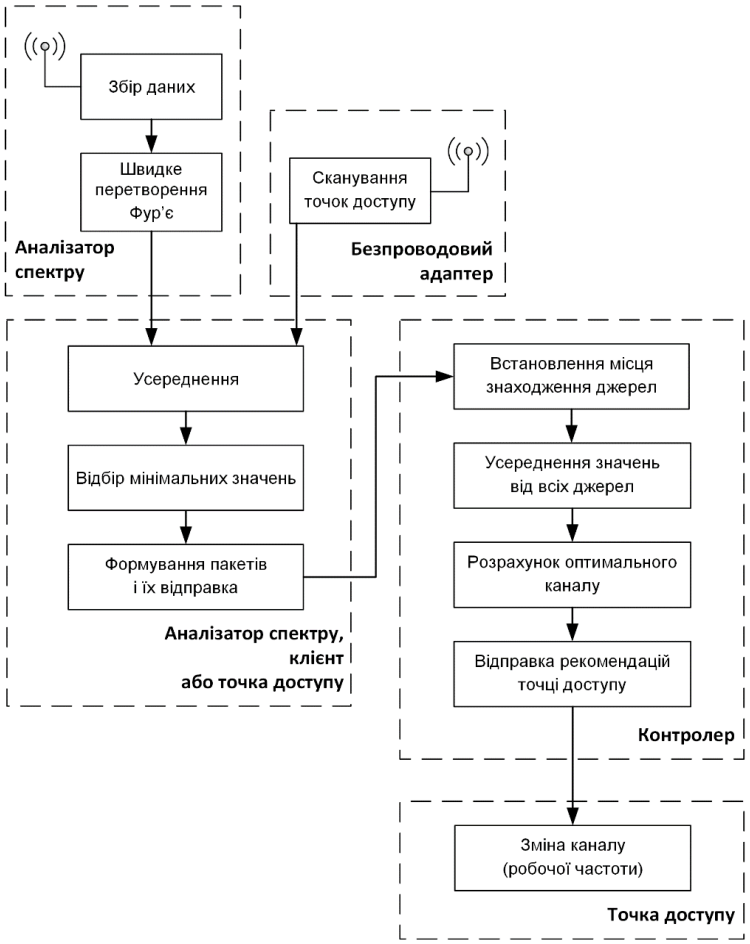


Рис. 2.4. Алгоритм динамічного розподілу каналів

Рівень сигналу в каналі *j* може бути обчислений при цьому за формулою:

$$L_j^{\text{ch}} = \frac{1}{N}\sum_{i=1}^{N} L_{ij}, \tag{2.18}$$

де індекс ch – номер каналу; *N* – кількість точок, що належать одному каналу; L_{ij} – вимірювання в *i*-й точці для *j*-го каналу, дБмВт. За один цикл вимірювання рекомендується проводити опитування в кожній точці приблизно в 100 разів, тому що замість L_i краще використовувати середнє значення для числа вимірювань.

Середній рівень сигналу від усіх зовнішніх пристроїв дорівнюватиме:

$$\bar{L}_{\text{зовн}}^{\text{ch}} = \frac{1}{M}\sum_{j=1}^{M} \mu_j L_j^{\text{ch}}, \tag{2.19}$$

де *M* – кількість спектроаналізаторів; μ_j - зважування важливості конкретного пристрою; L_j^{ch} – середній рівень сигналу для конкретного пристрою з (2.18).

Середній рівень сигналу від вбудованого безпроводового адаптеру, що надходить лише через рівні каналів (і лише для пристроїв, які працюють за одним стандартом) визначатиметься за формулою:

$$\bar{L}_{\text{вн}}^{\text{ch}} = \frac{1}{H}\sum_{j=1}^{H} \mu_j \sum_{k=1}^{K} \nu_k^{\text{ch}} L_k, \tag{2.20}$$

де *H* – кількість вбудованих безпроводових адаптерів; *K* – кількість сканованих ТБД; ν_k^{ch} – коефіцієнт перетину каналів через ширину каналу 20 МГц і інтервал між каналами – 5 МГц (див. табл. 2.3); L_k – рівні сигналу до *k*-ї безпроводової мережі.

Таблиця 2.3

Коефіцієнти перетину каналів

$\|ch–k\|$	0	1	2	3	>4
ν_k^{ch}	1	¾	½	¼	0

Розглянемо три варіанти створення портативних аналізаторів спектру:

1. Приймач і блок управління (відокремлені і на одному чіпі).
2. Приймач з визначеним рівнем сигналу на двох станах і блоці управління.
3. Інтегровані клієнтські безпроводові карти.

Оскільки в системі можуть бути присутні різні типи обладнання з різними операційними системами, з різною швидкістю і з різною точністю вимірювання, уніфікація повинна проводитися на етапі збору інформації, а саме в аналізаторах спектру з розділеним приймачем і модулем управління з USB, з вбудованим приймачем і модулем управління з USB та з розділеним приймачем і модулем управління з Ethernet. Перші два

типи аналізаторів спектра можуть працювати разом з клієнтом, з ТБД або окремо. Третій тип призначений для використання окремо.

Побудуємо аналізатор спектру для окремої схеми. Блок керування реалізуємо на Arduino Nano (версії 3.0 з живленням 3,3 В) та приймачеві – на TI CC2500+PA+LNA модуль із зовнішньою антеною [6]. Схема оснащена OLED 0,96" 128×64 SSD1306 (через I^2C або SPI) для візуалізації миттєвого значення. ПЗ написане в IDE Arduino і зкомпільована з GCC. На рис. 2.5 і 2.6 показано схему підключення модуля і живлення пристрою. Цей пристрій може працювати з контролером, який приймає дані через USB-інтерфейс. На двох екранах відображається діапазон від 2400,01 до 2503,40 МГц з інтервалом в 405,5 кГц. Було виявлено, що для керування пам'яттю блоку управління недостатньо (2 Кб) для аналізу доступних каналів. Крім того, цей пристрій не відповідає одному з вимог – повинен бути ненаправленою антеною, а напівхвильовий диполь має чітку поляризацію.

Для реалізації спектрального аналізатора на єдиному чіпі був обраний Pololu Wixel, розмір оперативної пам'яті якого 4 КБ, ненаправлена антена, в п'ять разів менше споживання енергії, майже в півтора рази краще дозвіл і SDK з детальною документацією [7].

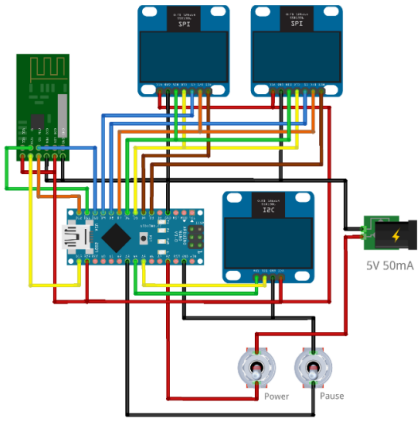


Рис. 2.5. Принципова схема розділеного приймача і блоку управління

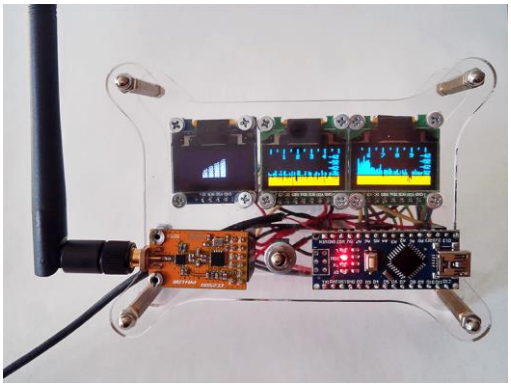


Рис. 2.6. Відокремлений приймач із зовнішньою антеною і блоком управління

На рис. 2.7 і 2.8 показано схему з’єднання модуля і живлення пристрою. На двох екранах відображається діапазон 2403,47–2476,50 МГц з інтервалом в 286,4 кГц, а також інформація про рекомендованих каналах Wi-Fi і ZigBee, обчислена за формулою (2.14). На рис. 2.9 показано приклад складання пристрою відображення в прозорому корпусі з додатковим перемикачем для режиму паузи.

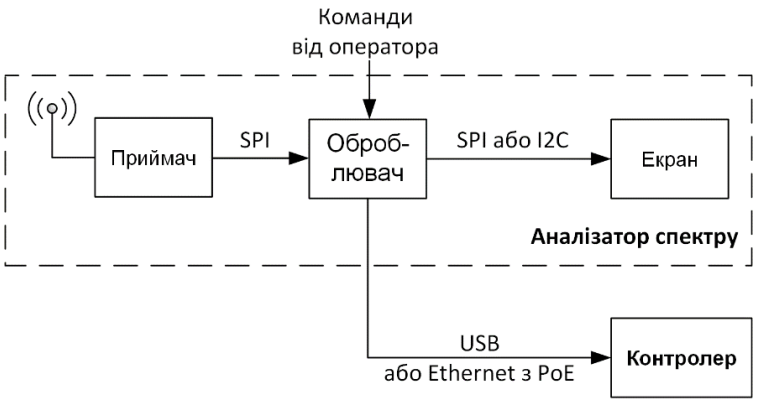


Рис. 2.7. Принципова схема розділеного приймача і блоку управління

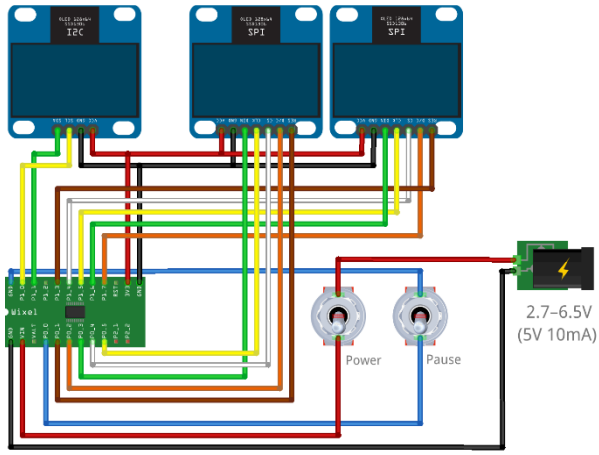


Рис. 2.8. Принципова схема приймача і блоку управління на одному чіпі

Він також може бути використаний для оцінки потужності сигналу і модуля, в якому рівень сигналу визначається оцінкою непрямих методів. На модулі nRF24L01 (або його модифікації з потужними і малошумними підсилювачами) базу в ОС Raspbian для вбудованих систем платформи Raspberry Pi. Вибраний як прототип спектрального аналізатора, який був пристосований для мікроконтролера Broadcom BCM2837 SoC (ядро ARM Cortex A53 CPU) ядро з прапорами -march = armv8-a + crc -mtune = cortex-a53 -mfpu = neon-fp-armv8. Для ініціалізації пристрою в операційній системі використовується стороннє ПЗ бібліотеки RF24.

Особливістю прийому даних з мікроконтролера nRF24L01 є той факт, що це лише один прапор (_NRF24_RPD), що вказує, що рівень прийнятого сигналу вище

або нижче рівня мінус 64 дБмВт. Змініть режим роботи програми з урахуванням змін у бібліотеці bcm2835 (версії 1.50). Сканування виконується кожні 976,5625 кГц, таким чином, охоплює діапазон 2,400–2,525 ГГц (128 точок вимірювання).

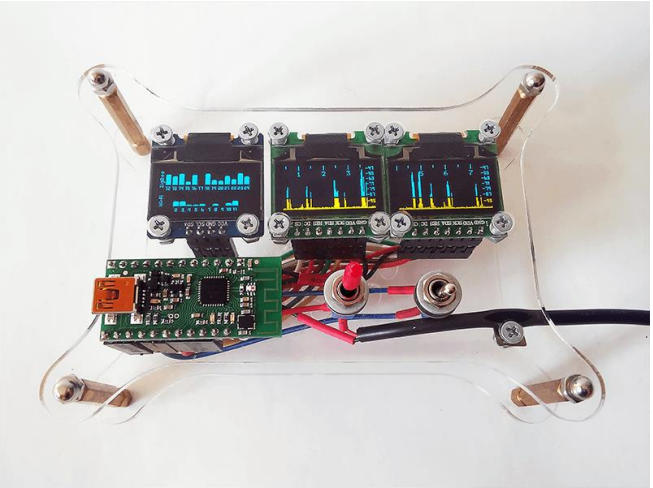


Рис. 2.9. Приймач і блок управління на одному чіпі

Що стосується частоти чутливості приймача мінус 85 дБмВт [8], то при отриманні 200 вимірювань рівень сигналу в i-й точці обчислюється за формулою:

$$P_i = L_{\min} + \frac{2(L_{\text{сер}} - L_{\min})}{N} \sum_{j=1}^{N} p_{ij}, \tag{2.21}$$

де $L_{\min}$ – мінімальний рівень, дБмВт; $L_{\text{сер}}$ – рівень тригера прапора, дБмВт; N – кількість вимірювань; p_{ij} – результат одиночного вимірювання (може приймати два значення: 0 або 1).

З (2.21) маємо особливий випадок для цього виміру:

$$P_i = -85 + 0{,}21 \sum_{j=1}^{200} p_{ij}. \tag{2.22}$$

На екрані відображаються результати реалізації розрахунку точок вимірювання. У нашому випадку ми мали 128 точок вимірювання, і ми побачимо масив з 128 значень у командному рядку.

На модулі була зібрана повномасштабна модель, яка показана на рис. 2.10. Arduino Nano (версія 3) використовується як система управління, і дані виводяться на OLED SSD1306. Щоб прискорити обробку, процес може бути паралелізований [9,10].

Таким чином, система адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру може містити кілька сегментів, які розділені каналами та/або фізично розділені.

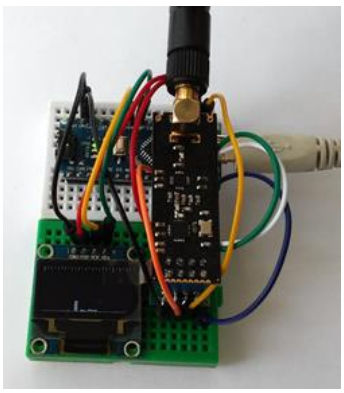


Рис. 2.10. Приймач nRF24L01 з блоком управління Arduino Nano

Це дозволить легко масштабувати систему за допомогою роумінгу й разом з тим накладає ряд обмежень:

1. Сегменти системи можуть стаціонарно розташовуватися в ключових точках інфраструктури в місцях розташування користувачів.

2. ДС антени повинна наближатися до сферичної.

3. Для передачі результатів повинні використовуватися безпроводові або проводові канали зв'язку, які виходять за межі об'єкту сканування частотного діапазону.

4. Мінімальне енергоспоживання (для можливості автономного живлення) [11,12].

На основі схеми та алгоритму, наведеного в [9] реалізуємо підсистему аналізу даних для безпроводової системи стандарту IEEE 802.11 (рис. 2.11).

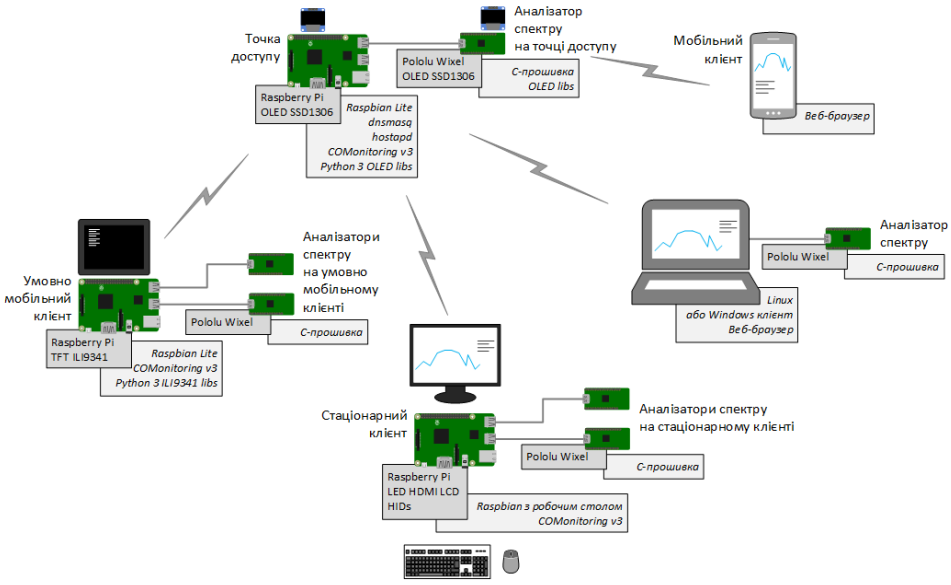


Рис. 2.11. Інфраструктура підсистеми системи моніторингу

Безпроводова система може знаходитися в трьох станах:

режимі регулярної роботи;

критичному режимі;

відмові в обслуговуванні.

Введення у безпроводову систему підсистеми з аналізаторами спектрів призводить до того, що настання критичного режиму роботи менш ймовірно, так як абоненти на перевантажених ТБД перенаправляються на сусідні ТБД не тільки за максимальним рівнем сигналу, але алгоритми розподілення навантаження можуть бути значно складнішими [7].

Визначимо коефіцієнт ефективності для безпроводової системи:

$$K = {}^{E}/_{C}, \tag{2.23}$$

де E – ефективність, а C – вартість.

Визначимо вартість звичайної безпроводової системи:

$$C = P_{\text{інф}} + P_{\text{обсл}}, \tag{2.24}$$

де $P_{\text{інф}}$ – вартість інфраструктури; $P_{обсл}$ – вартість обслуговування.

А вартість системи з мініатюрними аналізаторами спектру, з урахуваннями (2.24):

$$C_{sa} = P_{\text{інф}} + P_{\text{обсл}} + P_{\text{АС}} = C + P_{\text{АС}}, \tag{2.25}$$

де $P_{\text{АС}}$ – вартість підсистеми з аналізаторами спектру. Вартість обслуговування формується в обох випадках з постійної заробітної плати обслуговуючого персоналу, тому лишається незмінною.

Безпроводових абонентів підприємства або організації при цьому можна поділити на три категорії: рухомі (стільникові телефони, планшети тощо); умовно рухомі (ноутбуки) та нерухомі (стаціонарні персональні комп'ютери). Визначимо кількість рухомих як $N_{\text{рух}}$, умовно рухомих – $N_{\text{умов}}$ і нерухомих – $N_{\text{нерух}}$. Кількість рухомих приблизно дорівнює сумарній кількості умовно рухомих і нерухомих, бо практично кожний робітник має особистий мобільний термінал (якщо правилами внутрішнього розпорядку не передбачені обмеження на використання корпоративної мережі):

$$N_{\text{рух}} \approx N_{\text{умов}} + N_{\text{нерух}}. \tag{2.26}$$

Вартість підсистеми з аналізаторами спектру становить:

$$P_{\text{АС}} = \left(N_{\text{умов}} + N_{\text{нерух}}\right)P^{*}_{\text{АС}} + P_{\text{конт}}, \tag{2.27}$$

де $P^{*}_{\text{АС}}$ – вартість одного аналізатора спектру, $P_{\text{конт}}$ – вартість контролера, який відповідає за збір, аналіз даних з усіх аналізаторів спектру та виробляє поради для основного контролера безпроводової мережі. Кількість рухомих абонентів не враховується, так як на них встановити додаткове обладнання досить складно.

Вартість інфраструктури залежить від кількості абонентів:

$$P_{\text{інф}} \sim N_{\text{рух}} + N_{\text{умов}} + N_{\text{нерух}} + N_{\text{гост}}, \tag{2.28}$$

де $N_{\text{гост}}$ – кількість гостьових абонентів.

Введемо показник відкритості σ безпроводової системи:

$$N_{\text{гост}} = \sigma N_{\text{рух}}. \tag{2.29}$$

Тоді з (2.26), (2.28) і (2.29) маємо повну кількість абонентів:

$$N \approx (2 + \sigma)(N_{\text{умов}} + N_{\text{нерух}}). \tag{2.30}$$

Ефективність звичайної безпроводової мережі прямо пропорційна мінімальному часу доступу абонента до ресурсів ТБД:

$$E \sim T_{\text{a}}^{\min} = \frac{\Delta T}{N^{\max}}, \tag{2.31}$$

де ΔT – розмір часового вікна передавання, $N^{\max}$ – максимально можлива кількість абонентів на одну ТБД (в залежності від виробника становить від 30 до 50).

Ефективність безпроводової мережі з аналізаторами спектру:

$$E_{\text{АС}} \sim \frac{N_{\text{ТБД}}}{N} \Delta T, \tag{2.32}$$

де $N_{\text{ТБД}}$ – кількість ТБД.

Оцінити якість роботи можна за відношенням коефіцієнтів ефективності [10]:

$$\frac{K}{K_{\text{АС}}} = \frac{E \cdot C_{\text{АС}}}{E_{\text{АС}} \cdot C} = \frac{N}{N_{\text{ТБД}}} \cdot \frac{1}{N^{\max}} \cdot \left(1 + \frac{P_{\text{АС}}}{P_{\text{інф}} + P_{\text{обсл}}}\right). \tag{2.33}$$

2.2. Метод підвищення функціональної безпеки безпроводової інфраструктури для прискорюючих лінз

Приклад розташування циліндричної ПЛ показаний на рис. 2.12, яка працює з вертикальним несиметричним вібратором. В даному випадку розташування пластин буде паралельним площині поляризації хвилі.

Частотний діапазон для стандарту IEEE 802.11b/g (/n частково) припадає на (2,4000..2,4835) ГГц, для якого середня довжина хвилі становить $\lambda_{\text{сер}}$ = 0,123 м.

Рис. 2.12. Схематичне взаєморозташування антени і ПЛ (вид зверху), де F – фокусна відстань, $t = t' + t''$ – максимальна довжина профілю, d – ширина, a – відстань між окремими профілями

Відстань між профілями (пластинами):

$$a = \frac{\lambda_{\text{сер}}}{2\sqrt{1-n^2}} \approx 0{,}077\text{м}, \tag{2.34}$$

де n – коефіцієнт заломлення ПЛ, який повинен бути нижчим за 1 і з рекомендацій прийнятий рівним 0,6 [13]. Також відстань відповідає умові: $\lambda/2 < a < \lambda$. Через невелику точність виготовлення ПЛ допуск відповідає 1 мм (мінімальна ціна поділки дорівнює максимальному викривленню профілю і складає 1 мм). Із заданою точністю можна виготовити дві ПЛ, які потрапляють у вибраний діапазон і відповідають двом каналам: 5-му (f_5 = 2,4334 ГГц і $a_5 \approx 0{,}077$ м) і 12-му (f_{12} = 2,4654 ГГц і $a_{12} \approx 0{,}076$ м).

Ширина ПЛ для кожного каналу:

$$\begin{aligned} d_5 &= 7a_5 = 0{,}539\text{м}, \\ d_{12} &= 7a_{12} = 0{,}532\text{м}. \end{aligned} \tag{2.35}$$

Фокусна відстань ПЛ для кожного каналу:

$$\begin{aligned} F_5 &\approx d_5 = 0{,}539\text{м}, \\ F_{12} &\approx d_{12} = 0{,}532\text{м}. \end{aligned} \tag{2.36}$$

Згідно з рекомендаціями, приведеними в [14], приймаємо $F \approx d$. Глибину елементів буде розраховуватися за формулою:

$$t'_n = a_n \left| \frac{1}{n+1} - \sqrt{\frac{1}{(n+1)^2} + \frac{1}{4\cdot(1-n^2)}} \right|, \tag{2.37}$$

звідки отримуємо повний профіль $t = t' + t''$ (де t'' = 0,045 м, що забезпечує мінімальну жорсткість конструкції):

$$
\begin{aligned}
t'_{1(5-\text{й канал})} \approx t'_{1(12-\text{й канал})} = 0{,}010\text{м} \Rightarrow t_1 = 0{,}055\text{м},\\
t'_{2(5-\text{й канал})} \approx t'_{2(12-\text{й канал})} = 0{,}030\text{м} \Rightarrow t_1 = 0{,}075\text{м},\\
t'_{3(5-\text{й канал})} \approx t'_{3(12-\text{й канал})} = 0{,}050\text{м} \Rightarrow t_1 = 0{,}095\text{м},\\
t'_{4(5-\text{й канал})} \approx t'_{4(12-\text{й канал})} = 0{,}070\text{м} \Rightarrow t_1 = 0{,}115\text{м}.
\end{aligned}
\tag{2.38}
$$

Похибка виготовлення становить $\delta_{\text{виг}} = \frac{\Delta t\prime_{\text{з}}}{t\prime_{\text{зсер}}} \approx 2\%$, а похибка округлення при розрахунках – $\delta_{\text{окр}} = \frac{\Delta t_{\text{окр}}}{t\prime_{\text{зсер}}} = \frac{0{,}0005}{0{,}050} = 1\%$, що в сумі дає максимальну похибку в 3%.

З іншого боку похибка, яка залежить від вибору каналу передавання у межах діапазону $\delta_{\text{окр}} = \frac{\Delta a}{a_{\text{сер}}} = \frac{0{,}0026}{0{,}0767} \approx 3\%$, що близько до $(\delta_{\text{виг}} + \delta_{\text{окр}})$ [15].

Максимальний радіус першої зони Френеля:

$$
R_{\text{зФ}} = \sqrt{\frac{r_{\text{пер}} \cdot r_{\text{пр}}}{r_{\text{пер}} + r_{\text{пр}}} \lambda_{\max}} = \frac{1}{2}\sqrt{L \cdot \lambda_{\max}} = \frac{1}{2}\sqrt{\frac{c \cdot L}{f_{\min}}},
\tag{2.39}
$$

де $r_{\text{пер}}$ і $r_{\text{пр}}$ – відстані від передавача і приймача до можливої перешкоди, $\lambda_{\max}$ – максимальна довжина хвилі діапазону ($f_{\min}$ – відповідна мінімальні частота, c – швидкість світла у повітрі). Приймаємо повну відстань між приймачем і передавачем за $L = r_{\text{пр}} + r_{\text{пер}} = 2r$. Максимальний вплив перешкоди певної висоти у діапазоні робочих частот буде найбільшим при мінімальній частоті і рівновіддаленості від передавача і приймача, тобто $r = r_{\text{пр}} = r_{\text{пер}} = ½L$ [16–18].

2.2.1. Адаптація прискорюючих лінз до багатопроменевих систем

Складніше застосовувати ПЛ для систем зв’язку з рознесеними передавальними і приймальними антенами (multiple input multiple output, MIMO), в яких використовуються дві антени (і більше). При цьому виникає проблема вибору параметрів ПЛ, які дозволяли б підвищити показники доступності інформації в обох каналах, антени яких мають поперечний просторовий рознос і не можуть розташовуватися у фокусі ПЛ. Вирішення цієї проблеми може досягатися двоякий про: збільшенням фокусної відстані ПЛ; модифікацією профілю ПЛ таким чином, щоб він задовольняв вимогу однакового положення ДС, формованих при використанні зміщених як вліво, так і вправо від фазового центру ПЛ, випромінювачів.

ПЛ зі зміщеними відносно фокуса опромінювача розглянута в [13], але для цілей сканування ДС і без вказівки методики обчислень профілю ПЛ і фазового розподілу (ФР) в апертурі. У нашому випадку вимога протилежна: ДС повинні

мінімально відхилятися і мінімально спотворюватися при використанні кожного з опромінювачів. Тому була розроблена методика розрахунків спотворень ФР в розкриві циліндричної ПЛ і відхилення максимуму ДС, обумовлених зміщенням положення опромінювачів щодо фазового центра ПЛ перпендикулярно осі в горизонтальній площині (див. рис. 2.13).

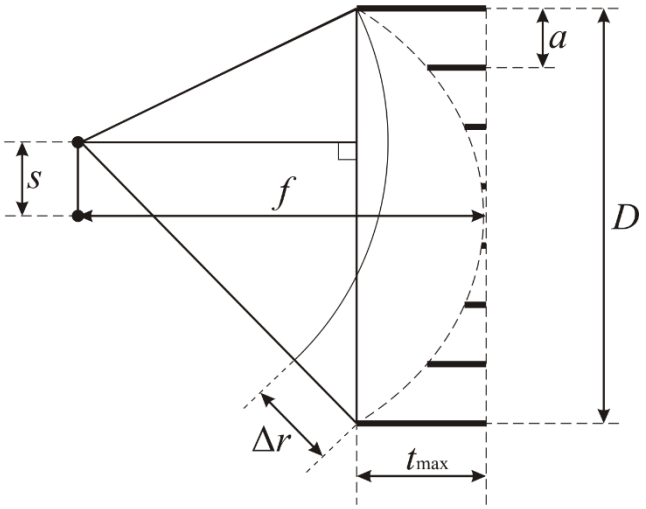


Рис. 2.13. Зсув випромінювача з фокусу ПЛ

Для ПЛ з класичним їм профілем (при розташуванні опромінювача у фокусі), оцінювалося відміну в геометричному шляху (Δr) хвилі від зміщеного вліво на величину s вібратора до опромінюваної поверхні ПЛ за формулою:

$$\Delta r(d) = \sqrt{\left(f - t(d)\right)^2 + (d-s)^2} - \sqrt{(f - t_{\max})^2 + \left({}^{D}/_{2} - s\right)^2}, \qquad (2.40)$$

де f – фокальна відстань; D – розкрив ПЛ; d – поточний розкрив, $d \in \left[-{}^{D}/_{2}; +{}^{D}/_{2}\right]$; s – зміщення опромінювача від фокуса; $t_{\max}$ – максимальна глибина ПЛ. Профіль ПЛ t являє собою функцію від положення пластини в розкриві d, яка відрізняється від класичної (2.38):

$$t(d) = \frac{f}{n+1} - \sqrt{\left(\frac{f}{n+1}\right)^2 - \frac{d^2}{1-n^2}}, \qquad (2.41)$$

де n – коефіцієнт заломлення [18,19].

На протилежній зміщенню випромінювача стороні апертури ПЛ має місце відставання по фазі, що приводить до зміщення максимуму ДС в сторону, протилежну зсуву опромінювача. При двох опромінювачах (один зміщений вліво, а другий – вправо) система матиме два максимуми ДС, зміщені, відповідно, вправо і вліво. Величина Δr є визначальною для оцінки зсуву максимуму ДС.

У рамках другого підходу було проведено обчислення профілів ПЛ для лівого і правого опромінювача окремо, вважаючи їх розташованими у фокусах відповідних ПЛ. Після цього виконано усереднення глибин окремих пластин. Відносний зсув ПЛ в поперечній площині становив 2*a*.

Для ПЛ з усередненням профілю величини відхилень середнього значення від необхідних класичних профілів для правого і лівого опромінювача порівнювався з допустимою помилкою вибору глибини ПЛ.

Виявилося, що зазначені відхилення сумісні або менші за допустиму величину для ПЛ з фокусною відстанню $f = 3D$, при $n = 0{,}5$. При $f = 1{,}6D$ тільки для першої від центру пластини. Тобто, зі збільшенням фокусної відстані ПЛ з усередненим профілем стає менш чутлива до помилок вибору профілю ПЛ.

Для обох типів ПЛ в межах випромінюючої поверхні ФР виявилося нелінійним з увігнутістю. На рис. 2.14 показані профілі ПЛ та ФР, побудовані за формулами (2.40) і (2.41). На всіх рисунках суцільні лінії відносяться до ПЛ з класичним профілем, а пунктирні – для ПЛ з усередненим профілем [19,20].

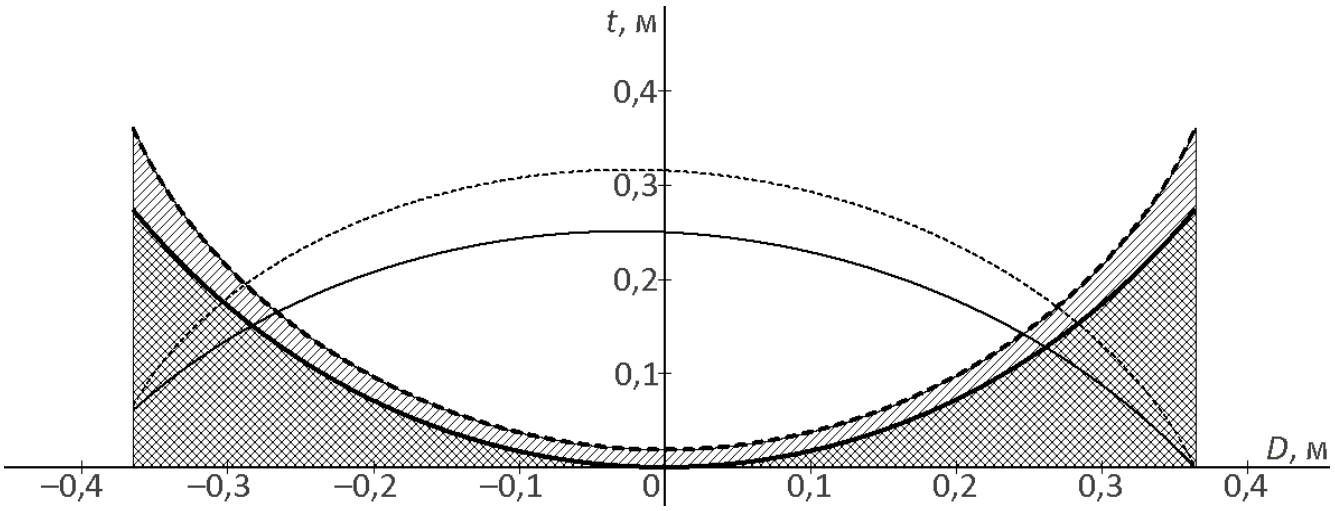


Рис. 2.14. Профілі ПЛ: класичної (суцільна лінія) і з усередненням (пунктирна), а також ФР в розкриві

2.2.2. Вплив поляризаційних властивостей багатопроменевих систем на цілісність інформації та її доступність

Поляризаційні параметри (характеристики) електромагнітних хвиль поряд з іншими параметрами сигналів, які можуть змінюватись у результаті модуляції при формуванні та випроміненні або під впливом взаємодії хвилі з об’єктами та середовищем при розповсюдженні, є інформативними або такими, що проявляються у якості мультипликативних завад. Теоретичні передумови врахування поляриза-

ційних параметрів радіосигналів для підвищення інформативності систем і пропускної здатності каналів зв'язку розглянуті у ряді праць. На наш погляд найбільш ґрунтовно це зроблено у [21–25]. Відомі приклади практичного втілення поляризаційної обробки в оптичних системах, у радіолокації при визначенні властивостей та ознак об'єктів (літаків, бойових головок балістичних ракет, супутників і т. ін.) [22,23], супутникових системах зв'язку, де поляризація змінюється при проходженні хвиль через іоносферу, у декаметрових радіолініях, де поляризація залежить від умов розповсюдження на ділянці іоносферної рефракції. Між тим практичне застосування поляризаційної обробки, особливо її найбільш досконалої форми – адаптивної поляризаційно-просторової та поляризаційно-часової обробки, яка передбачає також придушення завад, що мають поляризаційні відмінності від корисного сигналу, у системах зв'язку здебільше обмежується узгодженням за поляризацією приймальної антени з хвилею, що приймається, або використанням приймальних антен, інваріантних до випадкової або еліптичної поляризації хвилі у супутникових та декаметрових каналах (спіральні та турнікетні антени). У системах мобільного зв'язку та мобільного інтернету стандартів IEEE 802.11n (Wi-Fi), 4G, 3GPP LTE, WiMAX і HSPA+ врахування поляризаційної структури поля поки що не здобуло помітного поширення. Зрозуміло, що це обумовлено значними труднощами: по-перше, певними обмеженнями на конструкцію та складність передавальних і приймальних антен, по-друге, складною поляризаційною структурою поля, особливо у приміщеннях, яку важко моделювати, а експериментальні результати дослідження її напевно важко узагальнювати. Хоча актуальність пошуку нових підходів до збільшення кількості одночасно працюючих користувачів (ущільнення сигналів) та підвищення пропускної здатності каналів (або хоча б запобігання зниженню пропускної здатності) згаданих систем зростає [26].

Відомо, що одним з вирішальних факторів, який обумовлює принципову можливість функціонування багатоканальних і багатостанційних систем, таких як супутникові або наземні системи мобільного зв'язку, а також сучасні системи дистанційного доступу до мережі інтернету, є забезпечення ортогональності сигналів окремих користувачів [27]. На сучасному етапі це вирішується на основі частотного, часового, кодового поділу (розділення) або застосування певної комбінації цих методів. Дуже обмеженими є можливості застосування просторового рознесення з використанням фазованих антенних решіток (особливо у Wi-Fi мережах). Між тим стрімке зростання кількості користувачів таких систем та їх щільне розташування у просторі у межах прямої видимості потребує пошуку шляхів по-

долання проблеми перевантаження системи на основі поділу одночасно працюючих абонентів та запобігання суттєвого зниження якості (швидкості) інформаційного обміну (зниження пропускної здатності каналів). Існуючі протоколи, які ґрунтуються на часовому поділі пакетів, як показує досвід, майже вичерпали свої можливості [26].

Додатковим ступенем свободи для ортогоналізації сигналів з метою поділу абонентів у системах, які використовують радіоканали, може бути поляризація електромагнітної хвилі. З теоретичної точки зору ортогоналізація сигналів за поляризацією у лінійному або круговому базисі не викликає сумнівів [21,24,25] коли йдеться про більш-менш прості умови на трасі: відкрита місцевість, мала кількість відбиваючих об’єктів, однорідне та ізотропне середовище. Умови, у яких функціонують мережі стандарту IEEE 802.11, як правило, віднести до таких важко.

Певні спроби використати поляризаційні ефекти у MIMO системах відомі [28–31], але автори обмежились лише аналізом впливу ступеня узгодженості поляризації передавальних і приймальних антен на рівень прийнятого сигналу, не торкаючись інформаційних показників систему у цілому.

Розглянемо два із можливих напрямків використання поляризаційних властивостей хвиль для підвищення інформаційних можливостей радіосистем типу IEEE 802.11n у приміщеннях. Перше: застосування поляризаційного поділу сигналів, тобто ущільнення каналу (на першому етапі з використанням лінійного поляризаційного базису; у подальшому заплановано дослідити круговий базис), що в решті решт веде до підвищення пропускної здатності системи у цілому. Друге: застосування поляризаційного рознесення для підвищення пропускної здатності окремого каналу в умовах невизначеності поляризаційної структури поля. Основна увага приділена експериментальним дослідженням та їх інтерпретації відповідно до умов розповсюдження хвиль при використанні антен з лінійною поляризацією – несиметричних вібраторів.

Для виявлення зміни рівнів сигналів в залежності від розташування приймальної і передавальної антен передавача і приймача було побудовано експериментальний канал зв’язку. На рис. 2.15 показані схеми експериментів. В якості передавача використовувалася ТБД типу TP-LINK TL-WR340G (апаратна версія 4 на мікроконтролері Atheros AR2317, 200 МГц) зі стандартною прошивкою Stock 4.18.19.110701. В якості приймача використовувався зовнішній безпроводовий пристрій Linksys WUSB54G (апаратна версія 4 на мікроконтролері Ralink RT2500USB). Обидві сторони були переобладнані однаковими чвертьхвильовими

вібраторами з поворотним механізмом. Відстань між передавальною і приймальною антенами відповідає дальній зоні, а вимірювання проводяться у першій зоні Френеля. Аналіз рівнів сигналів проводився за допомогою програмного аналізатора спектру NetStumbler (версії 0.4.0).

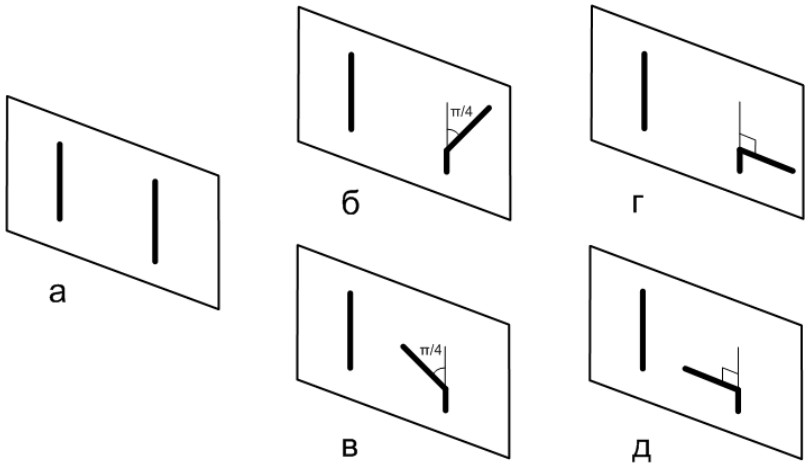


Рис. 2.15. Схеми експериментів з антенами в площині розповсюдження хвилі:
а – паралельне; б, в – під кутами ±π/4; г, д – перпендикулярне розміщення

В якості базового обране паралельне розташування вібраторів на одній висоті, при якому кожен має максимальну узгодженість (при відсутності землі) за вертикальною поляризацією (рис. 2.15а). В базовому випадку рівень сигналу становить мінус 18 дБмВт (по відношенню до рівня сигналу в антені 1 мВ, див. табл. 2.4).

Таблиця 2.4

Рівні сигналів в залежності від взаємного кута розташування, дБмВт

Типи приміщень	Кути між антенами, рад			
	0	π/4	–π/4	±π/2
Без перевідбиття	–18	–16	–22	–33
З перевідбиттям		–20	–20	–22

При розташуванні антени під –π/4 (рис. 2.15б) рівень сигналу збільшується до мінус 16 дБмВт, а при π/4 (рис. 2.15в або 2.15г) зменшується до мінус 22 дБмВт. При проведені моделювання у програмному комплексі Mmana-Gal basic (версії 3.0.0.15) отримуємо ДС для вертикальної поляризації, показану на рис. 2.16. З ДС видно, що різниця рівнів сигналів між кутами розташування ±π/4 становить близько 6 дБмВт, що відповідає результатам отриманим в експерименті.

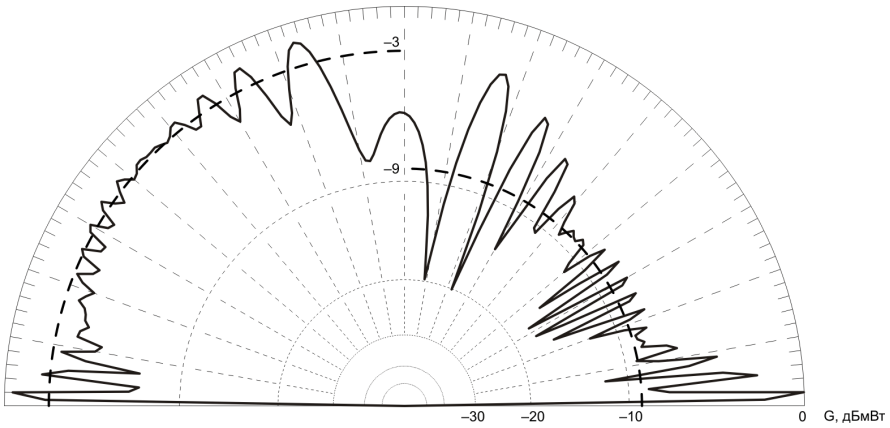


Рис. 2.16. ДС антени під ±π/4 з урахуванням землі

При проведені експериментів у приміщенні з великою кількістю перевідбиттів зменшення рівня сигналу відповідає 2 дБмВт при нахиленні на кожні 45°, що підтверджується у попередніх дослідженнях [28].

В наступному випадку перевірявся вплив ортогоналізації за поляризацією приймальної антени на рівень сигналу (див. рис. 2.17). При повороті на π/4 рівень сигналу становить в середньому мінус 23 дБмВт, а π/2 – мінус 31 дБмВт. Під час експерименту антена поверталася в два боки, але рівень сигналу лишався без змін, що опосередковано свідчить про відсутність впливу перевідбиттів. При проведенні експерименту у приміщенні з перевідбиттями жодної зміни при повороті антени в перпендикулярній площині не було помічено, що можна пояснити наявністю складових поля з різноманітною орієнтацією вектору напруженості електричного поля з приблизно однаковою інтенсивністю.

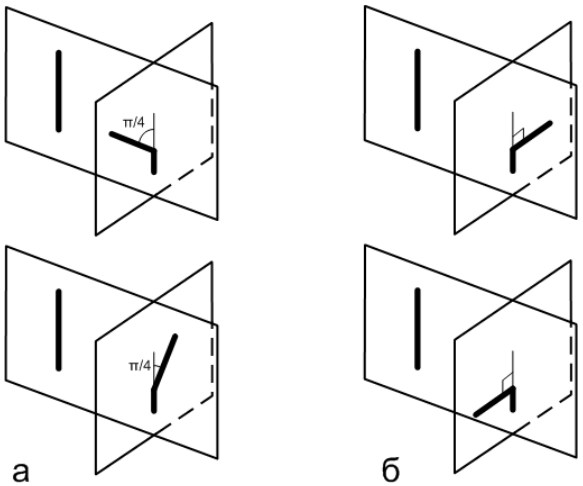


Рис. 2.17. Схеми експериментів з антенами в ортогональних площинах під π/4 (а) і під π/2 (б)

У багатоканальних системах (наприклад, MIMO) поряд з використанням дублювання пакетів для підвищення якості зв’язку можна застосовувати поляриза-

ційні ефекти. У діапазоні ультрависоких частот такі системи рекомендовано використовувати у приміщеннях зі складною геометрією і на невеликих відстанях. Для опису таких систем використовується канальна матриця $\boldsymbol{H}$, розмірність якої визначається кількістю передавальних і приймальних антен [30,31]. У експерименті використовувалися дві ТБД типу TP-Link TL-WR1043ND, які підтримують режим роботи MIMO 3×3. Канальна матриця для даного випадку буде квадратною розмірністю $N = 3$:

$$\boldsymbol{H} = \begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & h_{33} \end{bmatrix}. \tag{2.42}$$

За результатами першого етапу експериментальних досліджень знайдемо коефіцієнти узгодження для всіх випадків взаємного розташування антен і вільних роз'ємів, які призводять до паразитного випромінювання і впливають на канальну матрицю на малих відстанях. В експерименті роз'єми типу SMA Plug (Male) випромінювали в напрямку приймальної антени (рис. 2.18).

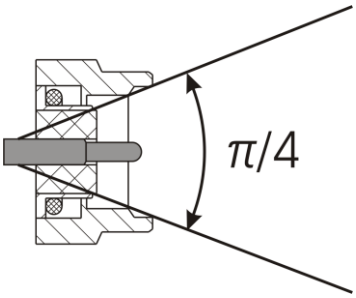


Рис. 2.18. Кут випромінювання SMA-роз'єму

Максимальна відстань, при якій два роз'єми забезпечують передавання за рахунок паразитного випромінювання, визначається [26]:

$$d_{\max} < \frac{c}{2\pi f_{\text{сер}}} 10^{\frac{P_{\text{пр}} - P_{\text{пер}} + P_{\text{роз}}}{20}}, \tag{2.43}$$

де c – швидкість світла; $f_{\text{сер}}$ – середня частота у діапазоні роботи; $P_{\text{пр}}$ – максимальна чутливість приймача, $P_{\text{пер}}$ – максимальна потужність приймача, $P_{\text{роз}}$ – коефіцієнт ослаблення роз'єму (для найгірших зразків відповідає мінус 40 дБмВт). Після розрахунку отримуємо максимальну відстань у 2,5 м, а відстань у експерименті склала 8,36 м, тому взаємним впливом двох роз'ємів можна знехтувати.

Елементи канальної матриці визначається за формулою:

$$h_{\text{ij}} = \frac{P_{\text{п}}}{P_{\text{б}}} = \sqrt[10]{10^{p_{\text{п}} - p_{\text{б}}}}, \tag{2.44}$$

де $P_{\text{п}}$ і $P_{\text{б}}$ – рівні сигналів у двох положеннях (поточному і базовому), мВт; $p_{\text{п}}$ і $p_{\text{б}}$ – рівні сигналів, дБмВт.

Після розрахунків за (2.42) отримуємо коефіцієнти узгодження, приведені в табл. 2.5.

Таблиця 2.5

Коефіцієнти узгодження

Варіанти розміщення антен	h_{ij}
Паралельні антени	1,00
Антени під кутами ±π/4	0,32
Перпендикулярні антени	0,05
Антена до вільного роз'єму	0,01
Два вільні роз'єми	$10^{-9}…10^{-8}$

В експерименті розглядалися різні варіанти взаємного розташування антен, для кожного з яких розраховувалася канальна матриця. Приклад взаємного розташування антен приведено на рис. 2.19.

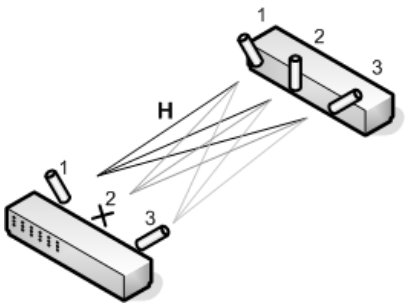


Рис. 2.19. Приклад взаємного розташування

Після розрахунку за формулами (2.42) і (2.44) канальна матриця для даного розташування має вигляд:

$$\boldsymbol{H} = \begin{bmatrix} 1{,}00 & 0{,}32 & 0{,}05 \\ 0{,}01 & 0{,}01 & 0{,}01 \\ 0{,}05 & 0{,}32 & 1{,}00 \end{bmatrix}. \tag{2.45}$$

У [32] і [33] приведена модифікація теореми Шеннона-Хартлі, за якою розраховується інформаційна пропускна здатність каналу (із розрахунку на один герц):

$$C = \log_2 \det\left(I_N + \frac{\rho}{N} \cdot \boldsymbol{H}\boldsymbol{H}^T\right), \tag{2.46}$$

де I_N – одинична матриця розмірністю N; ρ – відношення сигнал/шум; $\boldsymbol{H}^T$ – транспонована канальна матриця. Відношення сигнал/шум розраховується за формулою:

$$\rho = \frac{P_{\text{сигн}}}{P_{\text{шум}}} = \sqrt[10]{10^{p_{\text{сигн}} - p_{\text{шум}}}}, \tag{2.47}$$

де $P_{сигн}$ і $P_{шум}$ – рівні корисного сигналу і шуму, мВт; $p_{сигн}$ і $p_{шум}$ – рівні сигналів, дБмВт. В даному випадку за рівень сигналу $p_{сиг}$ прийнято рівень сигналу при паралельному розташуванні антен, а за рівень шуму $p_{шум}$ прийнято мінімальний робочий рівень приймача мінус 68 дБмВт для режимів передачі (54÷270) Мбіт/с, на яких проводилася експериментальне передавання даних.

В табл. 2.6 приведені результати розрахунків за формулами (2.46) і (2.47) інформаційної пропускної здатності безперервного каналів, з якої видно, що вона залежить в першу чергу від взаємного розташування передавальної і приймальної антен, а не від їх кількості. В досліджені розглядалися не усі можливі варіанти, а лише найбільш типові. Середні результати приходяться на взаємно паралельну орієнтацію антен (в таблиці помічені зіркою) з пропускною здатністю близько 16 біт у розрахунку на символ, найкращі (~35 біт) результати показали варіанти з нахиленим розташуванням антен (в таблиці помічені двома зірками) [34–36].

Таблиця 2.6

Пропускна здатність в залежності від орієнтації антен

Кількість антен	Взаємне розташування антен	Пропускна здатність, біт	Кількість антен	Взаємне розташування антен	Пропускна здатність, біт
1 (1:0)	| : ×	3,4594	6 (3:3)	|/ : |||	16,8784
2 (2:0)	|| : ×	4,3923	4 (2:2)	|| : ||	17,0253
2 (2:0)	\/ : ×	4,3923	5 (3:2)	||| : ||	17,6097
3 (3:0)	||| : ×	4,9542	4 (3:1)	|/ : |	17,9065
3 (3:0)	|/ : ×	4,9542	5 (3:2)	|/ : ||	18,1249
3 (2:1)	\/ : |	12,7500	6 (3:3)	||| : |||	18,1946
4 (2:2)	\/ : ||	13,7432	4 (2:2)	\/ : \/	30,0445
2 (1:1)	| : |	15,0272	5 (3:2)	|/ : \/	30,8029
3 (2:1)	|| : |	16,0260	6 (3:3)	|/ : |/	44,4410
4 (3:1)	||| : |	16,6099			

2.3. Метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз

З метою підвищення достовірності оцінки стану систем захисту безпроводових мереж, отриманої з використанням методу, описаного у розділі 1.1.4. Відомо, що будь-яка загроза характеризується набором характеристик. Враховуючи, що висновки експертів будуть корелюватися через суб’єктивність, а оцінки гарантоздатності і функціональної безпеки будуть взаємопов’язані, визначимо функцію цих характеристик від характеристики експерта.

Для цього використаємо нормовану характеристику S^* і одночасно розглянемо суб'єктивні оцінки гарантоздатності та функціональної безпеки i-ї характеристики:

$$\begin{cases} W_i = f_W(x_i), \\ G_i = f_G(x_i); \end{cases} \tag{2.48}$$

де f_W і f_G – функції гарантоздатності та функціональної безпеки від суб'єктивної оцінки окремого експерта x_i.

Загальна формула для монотонної f_W і непевної функції f_G має вигляд:

$$S^* = \frac{1}{N}\sum_{i=1}^{N} W^*(x_i) \cdot G^*(x_i), \tag{2.49}$$

де $W^*(x_i)$ – нормований коефіцієнт вагомості суб'єктивної оцінки від значення параметру x_i:

$$W^*(x_i) = \left|\frac{f_W(x_i)}{\max[f_W(x_i)]}\right|, \tag{2.50}$$

а $G^*(x_i)$ – нормоване бальне значення функції:

$$G^*(x_i) = \left|\frac{G_i^{\Sigma}}{G_{i\,\max}^{\Sigma}}\right|. \tag{2.51}$$

Проміжні значення якої визначаються як інтегральні характеристики:

$$\begin{cases} G_i^{\Sigma} = \int_{x_i^{\text{кін}}}^{x_i^{\text{поч}}} f_G(x)dx\,, \\ G_{i\,max}^{\Sigma} = \int_{x_i^{\min}}^{x_i^{\max}} f_G(x)dx; \end{cases} \tag{2.52}$$

де $x_i^{\text{поч}}$ і $x_i^{\text{кін}}$ – початок і кінець інтервалу значень для заданої характеристики, яка існує і неперервна на проміжку від $x_i^{\min}$ до $x_i^{\max}$.

Зважаючи, що в приведеному випадку необхідно оперувати з результатами, отриманими за допомогою експертної оцінки, перед початком обробки даних з використанням елементів *функціонально-вартісного аналізу* оцінимо адекватність експертної групи. Для цього припустимо, що довільна система характеризується N суттєвими характеристиками, які входять до множини X всіх її характеристик: $[x_1, x_2 \dots x_N] \in X$. Дослідним або аналітичним шляхом визначимо інтервали значень для всіх характеристик (мінімальне і максимальне значення), а також середнє значення (яке не обов'язково буде співпадати з середнім арифметичним мінімального і максимального значень).

В знайдених інтервалах експертами мають бути визначені бальні значення кожної характеристики G_i та побудовані графіки $G_i = f_G(x_i)$:

$$\begin{cases} G_1 = f_G(x), x = \overline{x_1^{\min}, x_1^{\text{сер}}, x_1^{\max}} \\ G_2 = f_G(x), x = \overline{x_2^{\min}, x_2^{\text{сер}}, x_2^{\max}} \\ \dots \\ G_N = f_G(x), x = \overline{x_N^{\min}, x_N^{\text{сер}}, x_N^{\max}} \end{cases} \quad (2.53)$$

Вагомість параметрів визначаємо методом розстановки пріоритетів, згідно з яким пріоритети характеристик визначає експертна група (M – кількість експертів), а за результатами складається табл. 2.7, в якій середня оцінка приводиться до числової форми за принципом: «>» відповідає 1,5; «=» – 1,0 і «<» – 0,5.

Таблиця 2.7

Приклад порівняння даних експертів

Параметри	Експерти					Середня оцінка	Числове значення
	1	2	3	…	M		
$x_1 \mid x_2$	=	=	>	…	>	>	1,5
$x_1 \mid x_i$	>	>	>	…	>	>	1,5
…	…	…	…	…	…	…	…
$x_{N-1} \mid x_N$	>	>	>	…	>	>	1,5

За отриманими даними заповнюється табл. 2.8 пріоритетів характеристик (для пар $x_i \mid x_i$ приймається коефіцієнт 1,0).

Таблиця 2.8

Пріоритети характеристик

	Характеристики						Важливість		Вагомість	
	x_1	x_2	…	x_i	…	x_N	b_i	φ_i	b_i'	$W_i = \varphi_i'$
x_1	1,0	1,5	…	1,5	…	1,5	7	0,28	34	0,292
x_2	0,5	1,0	…	1,5	…	1,5	5	0,2	22,5	0,193
…	…	…	…	…	…	…	…	…	…	…
x_i	0,5	0,5	…	1,0	…	1,5	4,5	0,18	20,5	0,176
…	…	…	…	…	…	…	…	…	…	…
x_N	0,5	0,5	…	0,5	…	1,0	3	0,12	14	0,12
Σ								1,0		1,0

Ступінь важливості φ_i кожного параметру:

$$\varphi_i = \frac{b_i}{\sum_{i=1}^{N} b_i}, \quad (2.54)$$

$$b_i = \sum_{j=1}^{N} a_{ij}, \quad (2.55)$$

де b_i – вага i-го параметру по результатам експертних оцінок; a_{ij} – числове значення пріоритету.

Коефіцієнт W_i вагомості i-го параметра визначається на другому кроці:

$$W_i = \dot{\varphi}_\iota = \frac{\dot{b_\iota}}{\sum_{i=1}^{N} \dot{b_\iota}}, \tag{2.56}$$

$$\dot{b_\iota} = \sum_{j=1}^{N} a_{ij} \cdot b_j. \tag{2.57}$$

Оцінка адекватність експертної групи проводиться після визначення залежності бального значеннями кожної характеристики від самої характеристики; функція з дискретної приводиться в неперервну з (2.53).

Сума рангів кожного параметра:

$$R_i = \sum_{j=1}^{M} r_{ij}, \tag{2.58}$$

де r_{ij} – ранг i-ї характеристики, визначений j-м експертом.

Перевірка загальної суми рангів, яка має дорівнювати:

$$R_{ij} = \frac{1}{2} \cdot M \cdot N \cdot (N+1). \tag{2.59}$$

Середня сума рангів $R_{\text{сер}}$:

$$R_{\text{сер}} = \frac{1}{N} \cdot R_{ij}. \tag{2.60}$$

Відхилення суми рангів для кожної i-ї характеристики від середньої суми (сума відхилень за всіма характеристиками повинна дорівнювати нулю):

$$\Delta_i = R_i - R_{\text{сер}}. \tag{2.61}$$

Загальна сума квадратів відхилень Δ_i^2:

$$S = \sum_{i=1}^{N} \Delta_i^2. \tag{2.62}$$

Коефіцієнт конкордації Кендалла:

$$W = \frac{12 \cdot S}{M^2 \cdot (N^3 - N)}. \tag{2.63}$$

Коефіцієнт конкордації може приймати значення: $0 \le W \le 1$. У випадку повної узгодженості поглядів експертів коефіцієнт становить: $W = 1$. Якщо $W \ge W_{норм.}$ визначені дані заслуговують на довіру и придатні для використання. Для засобів обчислювальної техніки прийнято $W_{норм.} = 0{,}67$, те саме значення можна використовувати і для розподілених систем безпроводого зв'язку [37–39]:

$$W_{розпод.\ сист.\ рух.\ зв'язку} \ge 0{,}67. \tag{2.64}$$

Зважаючи на те, що у приведеному випадку нормований ступень забезпечення систем захисту завжди буде $S^* \le 1$ (S^* – абсолютно захищена система, коли розгля-

нуті усі існуючі характеристики x_i) модифікований метод оцінки стану систем захисту безпроводових мереж від впливу техногенних та антропогенних загроз дозволить отримувати нормовану оцінку стану забезпечення безпеки для будь-яких систем безпроводого зв'язку та проводити порівняльний аналіз таких систем з різним набором (але не менше 3) характеристик.

Висновки до другого розділу

Для забезпечення функціональної безпеки та живучості безпроводових мереж, а також покращення якості прийому і/або розширення зони покриття, в розділі подальшого розвитку отримав метод оцінки стану систем захисту безпроводових мереж, метод модуляцій сигналів і адаптивного підбору вільних каналів передавання даних, а також метод підвищення цілісності та доступності інформації у безпроводових системах.

Вперше розроблено метод модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж, *що дозволило* за рахунок модифікації області амплітудно-фазового сузір'я сигналів *покращити* електромагнітну сумісність точки безпроводового доступу з абонентом та, на відміну від існуючих, *забезпечити* підвищення максимальної теоретичної просторової розв'язки сусідніх сузір'їв на 4,5%.

Вперше формалізовано метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру, *що дозволило* шляхом додавання аналізаторів спектру до існуючої безпроводової мережі *отримувати* оперативну інформацію про стан безпроводового ефіру, *виявляти* в режимі реального часу завади і сторонній кібернетичній вплив та, на відміну від існуючих, *забезпечувати* зростання стійкості безпроводових систем до такого впливу.

Вперше впроваджено метод підвищення функціональної безпеки безпроводової інфраструктури, *що дозволило* за рахунок адаптації конструкції прискорюючої лінзи до багатопроменевих систем та з урахуванням впливу їх поляризаційних властивостей на цілісність інформації та її доступність *узгодити* антенні систем передавача і приймача за поляризацією та, на відміну від існуючих, *забезпечити* збільшення потужності електромагнітної хвилі в точці прийому до 7 дБмВт, а пропускну здатність – до 4%.

Удосконалено метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз, *що дозволило* шляхом врахування залежності коефіцієнтів вагомості та бального значення кожної з характеристик (як функцій від самої характеристики) *забезпечити* підвищення достовірності оцінки стану систем захисту безпроводових мереж із значенням коефіцієнта конкордації експертів не нижче 0,67.

В сукупності зазначені методи складають підґрунтя для реалізації комплексного підходу до організації безпроводових мереж (як з роумінгом, так і без нього) підприємства: на фізичному (пункти 2.1.1 і 2.2), канальному (пункт 2.1.2), транспортному (пункт 2.1.2) і представницькому (2.3) рівнях OSI-моделі.

Список використаних джерел у другому розділі

1. Wireless Geographic Logging Engine Database. 2019. URL: https://wigle.net/graph-large.html (дата звернення: 29.03.2019).

2. Sankar K. Scaling Factor in QAM. 2007. URL: http://www.dsplog.com/2007/09/23/scaling-factor-in-qam/ (дата звернення: 29.03.2019).

3. Pillai K. Symbol Error Rate for M-QAM Modulation. 2008. URL: http://www.eetimes.com/design/signal-processing-dsp/4017648/Symbol-error-rate-for-M-QAM-modulation (дата звернення: 29.03.2019).

4. Градштейн И. С., Рыжик И. М. Таблицы интегралов, сумм, рядов и произведений. 4-е изд. Москва, 1963. 1100 с.

5. Соколов В. Ю. Модифікація прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу двох безпроводових систем. *Зв'язок*. 2012. №4 (100). С. 50–57.

6. CC2500 Low-Cost Low-Power 2.4 GHz RF Transceiver / Texas Instruments. 2016. 97 p.

7. Bogachuk I., Sokolov V. Yu., Buriachok V. Monitoring Subsystem for Wireless Systems based on Miniature Spectrum Analyzers. *Problems of Infocommunications. Science and Technology (PIC S&T'2018)* : in V Int. Sc. and Pract. Conf., 9–12 Oct. 2018. Kharkiv : IEEE, 2018. P. 581–585. DOI: 10.1109/infocommst.2018.8632151.

8. nRF24L01 Single Chip 2.4GHz Transceiver Product Specification / Nordic Semiconductor ASA. Ver. 2.0. 2007. 74 p.

9. Sokolov V. Yu., Carlsson A., Kuzminykh I. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network. *Problems of Infocom-*

munications. Science and Technology (PIC S&T'2017) : in IV Int. Sc. and Pract. Conf., 10–13 Oct. 2017. Kharkiv : IEEE, 2017. P. 564–568. DOI: 10.1109/infocommst.2017.8246463.

10. Buryachok V. L., Sokolov V. Yu. Low-Cost Spectrum Analyzers for Channel Allocation in Wireless Networks 2.4 GHz Range. *World Science*. 2018. No. 3 (31). Vol. 1. P. 9–16. DOI: 10.5281/zenodo.2528801. arXiv: 1902.08434.

11. Buriachok V., Sokolov V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors. *Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń*. Kharkiv : NU-CPU, 2019. P. 283–297. ISBN: 978-83-63680-28-2.

12. Астапеня В. М., Соколов В. Ю. Методы и средства контроля доступности в беспроводных сетях. *Сучасний захист інформації*. 2017. №3. С. 28–35.

13. The Potential Dangers of Electromagnetic Fields and Their Effect on the Environment on 27 May 2011. Prov. ed. No. 1815.

14. Шифрин Я. С. Антенны. Харьков, 1976. 408 с.

15. Соколов В. Ю. Розрахунок прискорюючої лінзи для стандарту IEEE 802.11. *Світ інформації і телекомунікацій – 2011* : матеріали VIII Міжн. наук.-техн. конф., 27–28 квітня 2011 р. Київ : ДУІКТ, 2011. С. 70–71.

16. Радиоэлектронные системы: основы построения и теория. Справочник / Ширман Я. Д. и др. Москва, 1998. 828 с.

17. Астапеня В. М., Соколов В. Ю. Використання прискорювальної лінзи для підвищення ефективності та завадозахищеності мереж IEEE 802.11b. *Зв'язок*. 2012. №2 (98). С. 33–37.

18. Metallic lens antenna : pat. US2576463A, USA. Kock W. E. 11.27.1951.

19. Astapenya V. M., Sokolov V. Yu. Modified Accelerating Lens as a Means of Increasing the Throughput, Range and Noise Immunity of IEEE 802.11 Systems. *Antenna Theory and Techniques (ICATT'2015)* : in X Anniversary Int. Conf., 21–24 Apr. 2015. Kharkiv : IEEE, 2015. P. 267–269. DOI: 10.1109/icatt.2015.7136852.

20. Астапеня В. М., Соколов В. Ю. Підвищення доступності інформації у бездротових системах на основі використання прискорюючої металопластинчастої лінзи. *Сучасні інформаційно-комунікаційні технології (COMINFO)* : матеріали IX Міжнар. наук.-техн. конф., 17–20 лист. 2015 р. Київ : ДУТ, 2015. С. 67–71.

21. Гусев В. Г., Филатов А. Д., Сополев А. П. Поляризационная модуляция. Москва, 1974. 288 с.

22. Канарейкин Д. Б., Павлов Н. Ф., Потехин В. А. Поляризация радиолокационных сигналов. Москва, 1966. 440 с.

23. Козлов А. И., Логвинов А. И., Сарычев В. А. Поляризация радиоволн. Поляризационная структура радиолокационных сигналов. Москва, 2005. 704 с.

24. Поздняк С. И., Мелитицкий В. А. Введение в статистическую теорию поляризации радиоволн. Москва, 1974. 480 с.

25. Родимов А. П., Поповский В. В. Статистическая теория поляризационно-временной обработки сигналов и помех. Москва, 1984. 272 с.

26. Соколов В. Ю. Електромагнітна сумісність транспортних мереж і мереж доступу технологій IEEE 802.11g і 802.15.1. *Зв'язок*. 2011. №2 (94). С. 67–70.

27. Радиосистемы передачи информации / Калмыков В. В. и др. Москва, 2005. 472 с.

28. Extended Ellipse Model for Multi-Polarized MIMO Antennas / Kwon S. et al. *Int. Symp. on Antennas and Propagation*. 2006. P. 1–5.

29. Oestges C., Guillaud M., Debbah M. Multi-Polarized MIMO Communications: Channel Model, Mutual Information and Array Optimization. *Wireless Communications and Networking Conf.*. 2007. P. 1057–1061.

30. Gonzalez A. N. Dual Polarized Omnidirectional Array Element for MIMO Systems. *KTH Signals Sensors and Systems*. Stockholm, 2005. 67 p.

31. Simulation of MIMO Channel Capacity with Antenna Polarization Diversity / Dong L. Et al. *IEEE Transactions on Wireless Communications*. 2005. Vol. 4. No. 4. P. 1869–1873.

32. Jensen M. A., Wallace J. W. MIMO Wireless Channel Modeling and Experimental Characterization / ed. A. B. Gershman, N. D. Sidiropoulos. 2005. 39 p.

33. Tse D., Viswanath P. Fundamentals of Wireless Communication. Cambridge, 2005. 564 p.

34. Астапеня В. М., Соколов В. Ю. Підвищення пропускної здатності безпроводових каналів зв'язку на основі поляризаційних ефектів у мережах IEEE 802.11. *Зв'язок*. 2012. №3 (99). С. 36–41.

35. Astapenya V. M., Sokolov V. Yu. Research Results of the Impact of Spatial and Polarization Value of the Antennas on Network Capacity of Wireless Channels Standard IEEE 802.11. *Antenna Theory and Techniques (ICATT'2013)* : in IX Int. Conf., 16–20 Sept. 2013. Odessa : IEEE, 2013. P. 172–174. DOI: 10.1109/icatt.2013.6650715.

36. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. *Сучасний захист інформації*. 2016. №2. С. 60–68.

37. Методичні вказівки до виконання організаційно-економічного розділу дипломних проектів / за ред. А. Т. Чернявського. Київ : НТУУ «КПІ», 1999. 66 с.

38. Методические указания к использования ФСА при разработке программного продукта / Чернявский А. Т. и др. Киев : НТУУ «КПИ», 1990. 69 с.

39. Соколов В. Ю. Кількісні показники оцінювання захищеності і ризиків від порушення безпеки у розподілених системах рухомого зв'язку. *Захист інформації*. 2010. №3 (48). С. 19–34. DOI: 10.18372/2410-7840.12.1957.

Розділ 3
ТЕХНІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ЖИВУЧОСТІ БЕЗПРОВОДОВИХ МЕРЕЖ

3.1. Взаємний вплив безпроводових мереж на забезпечення їх функціональної безпеки та живучості

Розглянемо варіант взаємного впливу двох мереж (шум зовнішнього середовища мінімізований за рахунок віддалення місця проведення експерименту від інших безпроводових мереж, екранування місця проведення експерименту та проведення замірів в нічний час): транспортної мережі з передачею даних на максимально можливій швидкості та мережі доступу з імітацією роботи користувача (передача IP-пакетів з максимальною довжиною в 64 кБ із заповненням каналу на 40–60% від максимуму).

Проведемо експеримент, в якому мережа доступу працюватиме в режимі точка-точка (peer to peer або ad hoc) з базовим набором послуг (independent basic service set, IBSS), а транспортна мережа – в режимі інфраструктури (infrastructure mode) з розширеним набором послуг (extended service set, ESS). При цьому транспортна мережа буде імітувати передачу зі швидкістю 54 Мб/с (стандарт 802.11g) з OFDM та часом тривалості одного символу разом з охоронним інтервалом 3,2 мкс. Отже, частота проходження імпульсів дорівнюватиме 312,5 кГц. Враховуючи, що в кожному з підканалів кодується по одному символу, а всього таких підканалів $M_{\text{роб}} = 48$ (і $M_{\text{сл}} = 4$ – службових підканали), отримаємо сумарне заповнення каналами: (48 + 4) × 312,5 кГц = 6,25 МГц < 22 МГц – ширини каналу передачі. Загальна кількість переданої інформації за один такт дорівнює [*б·такт*$^{-1}$]:

$$N = \nu_{\text{згор}} \cdot n \cdot M_{\text{роб}} = 216, \qquad (3.1)$$

з урахуванням швидкості згортального кодування $\nu_{\text{згор}} = ¾$ (на кожні три інформаційних біта додається один службовий); $n = \log_2 R = 6$ – кількість біт на символ (для швидкості 54 Мб/с використовується 64-QAM, що дає $R = 64$ можливих станів сигналу) [1].

Для побудови транспортної мережі використаємо технологію безпроводового розподілу даних (WDS) на двох ТБД D-Link DIR-320 з прошивкою від DD-WRT mini-usb-ftp v24-sp2.13064 [2], що працюють у режимі релейних станцій (wireless

bridging). ТБД знаходилися на відстані 3 м. Так як діапазон робочих частот маршрутизатора підтримує максимум 11 каналів (2,400–2,462 ГГц), то в якості робочої оберемо частоту в 2,442 ГГц (7-го каналу), яка знаходиться посередині зарезервованого діапазону. На максимальній швидкості каналу 54 Мб/с (режим 802.11g) максимальна вихідна потужність передавача ТБД складатиме (13±2) дБмВт, а чутливість приймача – мінус 68 дБмВт.

У мережі доступу ТБД використаємо в якості постачальника послуг і клієнта. Обрана ТБД D-Link DIR-300 зі стандартною прошивкою 1.05.a319 [3] підтримує діапазон робочих частот на 13 каналів (2,400–2,483 ГГц), чого достатньо для перегляду всього дозволеного діапазону (14-й канал з частотою 2,484 ГГц формально виходить за межі дозволеного інтервалу частот, тому їм можна знехтувати). На максимальній швидкості каналу 54 Мб/с (режим 802.11g) максимальна вихідна потужність передавача ТБД складатиме 12 дБмВт, а чутливість приймача – мінус 65 дБмВт. Клієнт працював на безпроводовому адаптері Atheros AR9285 з максимальною вихідною потужністю передавача (24±1,5) дБмВт і чутливістю приймача мінус 73 дБмВт (для швидкості 54 Мб/с) [4].

До кожної з ТБД необхідно підключити дипольну антену для використання всередині приміщень з коефіцієнтом підсилення 2 дБмВт. Між антенами ТБД 1 і ТБД 2 транспортної мережі на рівному видаленні від кожної розташуємо антену ТБД 3 мережі доступу, клієнтський термінал розташуємо за півметра від його антени, як показано на рис. 3.1.

Виміри рівня сигналу на ТБД 1 і ТБД 2 транспортної мережі будемо проводи з інтервалом в 1 с протягом однієї хвилини, змінюючи при цьому частоту (номер каналу передачі) у мережі доступу, і процедуру вимірювання рівня сигналу.

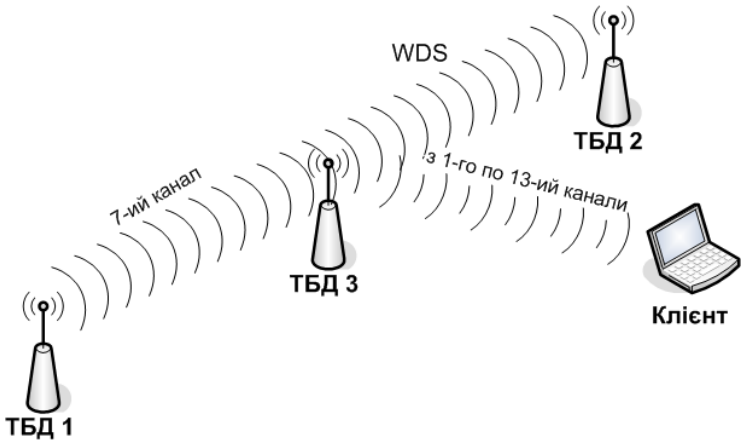


Рис. 3.1. Схема експерименту

Обчислимо теоретичну потужність сигналу

$$P_{\text{теор}} = P_{\text{прд}} + P_{\text{ант}} - P_{\text{срд}}, \tag{3.2}$$

де $P_{\text{прд}} \approx 13$ дБмВт – потужність передавача; $P_{\text{ант}} = 2$ дБмВт – підсилення антени; $P_{\text{срд}}$ – втрати в середовищі. Втрати потужності в середовищі для 7-го каналу становлять:

$$P_{\text{срд}} = 20\lg\left(\frac{4\pi d}{c}\sqrt{f_{\text{н}} \cdot f_{\text{в}}}\right), \tag{3.3}$$

де $d = 3$ м – відстань від приймача до передавача; c – швидкість світла в повітрі; $f_{\text{н}} = 2{,}431$ ГГц і $f_{\text{в}} = 2{,}453$ ГГц – нижня і верхня межі частотного діапазону [5].

В результаті потужність сигналу без зовнішніх перешкод складає $P_{\text{теор}} = (-34{,}7 \pm 2{,}0)$ дБмВт, що і підтверджується в експерименті $P_{\text{експ}} > P_{\text{теор}}$.

За діаграмою усереднених результатів експерименту на рис. 3.2 видно, що завади від каналів з різними частотами один на одного відрізняються.

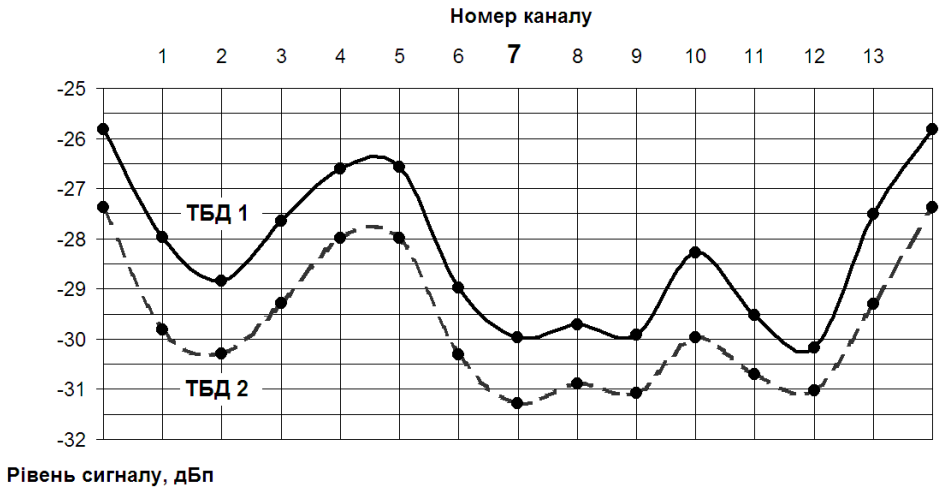


Рис. 3.2. Залежність рівня сигналу від вибору каналу

Так найбільше зниження сигналу спостерігається під час спільної роботи пристроїв на 7-му каналі. Наступні два мінімуми сигналу припадають на 2-му і 12-му канали, хоча ці канали і не пересікаються з 7-м.

Для обчислення похибки вимірювання середньої потужності сигналу $P_{\text{сер}}$ приймемо довірчу ймовірність рівною $\gamma = 0{,}95$ і число ступенів свободи – $\varphi \approx 60$ (так як кожне вимірювання проводилося протягом однієї хвилини з інтервалом в одну секунду). Тоді коефіцієнт Стьюдента $t_{0{,}95;60} = 2{,}000$ [6].

Виходячи з формули:

$$\Delta P_{\text{сер}} = t_{\gamma;\varphi}\sqrt{\frac{\sum_{i=1}^{\varphi+1}\left(P_i - P_{\text{сер}}\right)^2}{\varphi(\varphi+1)}}, \tag{3.4}$$

визначимо значення похибки для кожного виміру. За результатами експерименту максимальна похибка склала 0,19 дБмВт для ТБД 1 і 0,24 дБмВт для ТБД 2, а середня відносна похибка вимірювань становила 0,4% для ТБД 1 і 0,5% для ТБД 2.

Не зважаючи на те, що передавач мережі доступу був розміщений нами рівновіддалено від обох ТБД, рівень сигналу на другий ТБД виявився в середньому на 1,42 дБмВт нижчим, що не перевищує абсолютної похибки вихідної потужності передавача (1,42 дБмВт < 2 дБмВт).

Під час експерименту реальна швидкість передачі даних не перевищувала 10 Мб/с (при максимальній теоретичній – 54 Мб/с). При розгляді часової діаграми (рис. 3.3) явно видно зміну у швидкості передачі при перемиканні між каналами. Результати порівняння даної діаграми з рис. 3.2 показують, що рівень сигналу і швидкість передачі пов’язані обернено пропорційно. Дві півхвилинні ділянки з максимальною швидкістю відповідають періодам перемикання між каналами, тобто на них перешкода від мережі доступу була відсутня. У момент включення нового каналу (западини після максимальних рівнів сигналу) передається максимальна кількість широкомовних пакетів і відбувається обмін даними службовими підканалами.

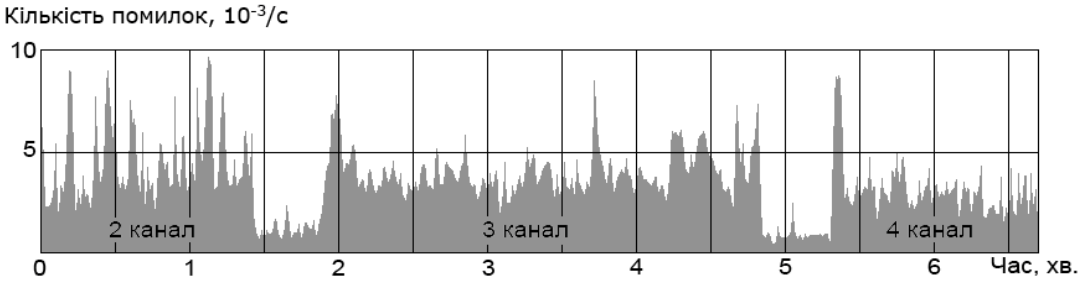


Рис. 3.3. Оцінка електромагнітної сумісності мереж на близьких частотах

Для всіх вимірювань рівень шуму склав менше мінус 92 дБмВт. Шифрування не впливає на втрати пакетів і зниження загальної швидкості передачі. Воно призводить лише до зниження переданого обсягу даних за рахунок самих протоколів шифрування. Значний вплив шифрування спостерігається лише при передачі потокових даних з програмним шифруванням/розшифрування на процесорах з частотами нижче 1,5 ГГц. Діапазони частот для Bluetooth і Wi-Fi збігаються 2,4008–2,4835 ГГц, таким чином, починає проявляється взаємний вплив між пристроями [7]. Враховуючи таке, крім дослідження взаємного впливу Wi-Fi мереж, доцільним виявилось розглянути варіант розташування двох Bluetooth пристроїв між транспортними ТБД та виміряти рівень сигналу в транспортній Wi-Fi мережі.

Для вирішення даного завдання оберемо Bluetooth (версії 2.0), які відносяться до першого класу (з максимальною потужністю передачі 20 дБмВт), підтримують технологію підвищення швидкості передачі даних (enhanced data rate, EDR) і в яких використовується інтелектуальна вибірка частот для передачі даних. Як показано на рис. 3.4, під час експерименту рівень сигналу знизився до (–30,48±0,25) дБмВт на першій ТБД і до (–28,92±0,22) дБмВт на другій. Зниження рівня сигналу склало при цьому близько 10%; що порівняно з даними [8] для Bluetooth (версії 1.1) на 5% менше при аналогічній відстані між ТБД.

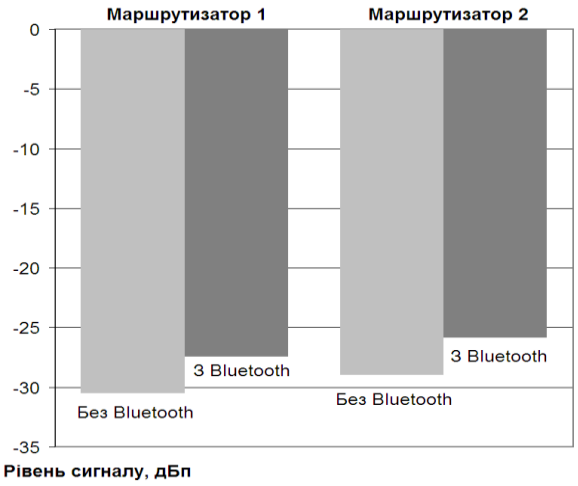


Рис. 3.4. Залежність роботи Wi-Fi від присутності Bluetooth

Так як канал в Bluetooth змінюється з частотою 1600 разів/с за технологією стрибкоподібно перебудови робочої частоти (frequency-hopping spread spectrum, FHSS), то вплив на 7-й канал транспортної Wi-Fi мережі розмивається на всьому діапазоні частот. На рис. 3.5 показано момент включення передачі у Bluetooth каналі, що мало відрізняється від форми сигналу при накладенні двох Wi-Fi каналів (див. рис. 3.3). Слід зауважити, що при включенні Wi-Fi під час роботи Bluetooth каналу, останній зависає на кілька секунд, адаптуючись до нової завади.

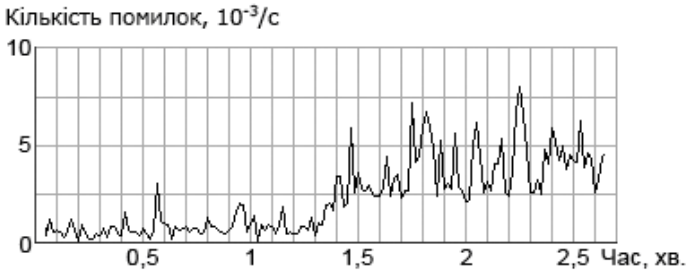


Рис. 3.5. Оцінка електромагнітної сумісності мереж
на однакових частотах для 802.11g і 802.15.1

Результати експерименту наочно продемонстрували, що для поліпшення сумісності Wi-Fi і Bluetooth мереж доцільно використовувати режим спільної роботи (Bluetooth coexistence mode) на Wi-Fi ТБД (відомий також під назвою «listen before transmit»). Але, нажаль, дана технологія підтримується тільки при автоматичному виборі каналів і означає попереднє сканування ТБД сигналів Bluetooth. Після аналізу потужності сигналів у всьому діапазоні вибирається оптимальний канал з мінімальними перешкодами [9].

3.2. Дослідження технології взаємного впливу безпроводових мереж з використанням сучасних спектроаналізаторів

Для проведення натурного експерименту, який дозволив би підтвердити працездатність модифікованого методу адаптивного підбору вільних каналів передавання даних в безпроводових мережах було обрано аналізатори спектру з трансиверами від компаній Texas Instruments (TI), Cypress та Nordic. Найбільш вдалими серед них є трансивери фірми TI і Cypress. Модуль Nordic nRF24L01 порівняно з ними має надто малий діапазон виміру потужності сигналу і через це досить малі межі застосування.

Зважаючи на таке в ході експерименту зосередимо увагу на порівняні роботи трасиверів тільки двох фірм, таких як TI і Cypress. З цією метою розглянемо чотири апаратні реалізації аналізаторів спектру на базі: мікроконтролера CC2500 (з USB-інтерфейсом); модуля CC2500 (USB); модуля CYWUSB6935 (LPT); модуля CYWUSB6935 (USB).

3.2.1. Програмно-апаратна реалізація технології взаємного впливу на базі мікроконтролера CC2500, мікрозбірок MD7105-SY і CYWUSB6935

Для аналізу цілісності передавання даних використаємо апаратний аналізатор спектру, який побудовано на радіочастотному трансивері, а саме Chipcon CC2500. Схему пристрою показано на рис. 3.6, а перелік електронних компонентів – в табл. 3.1.

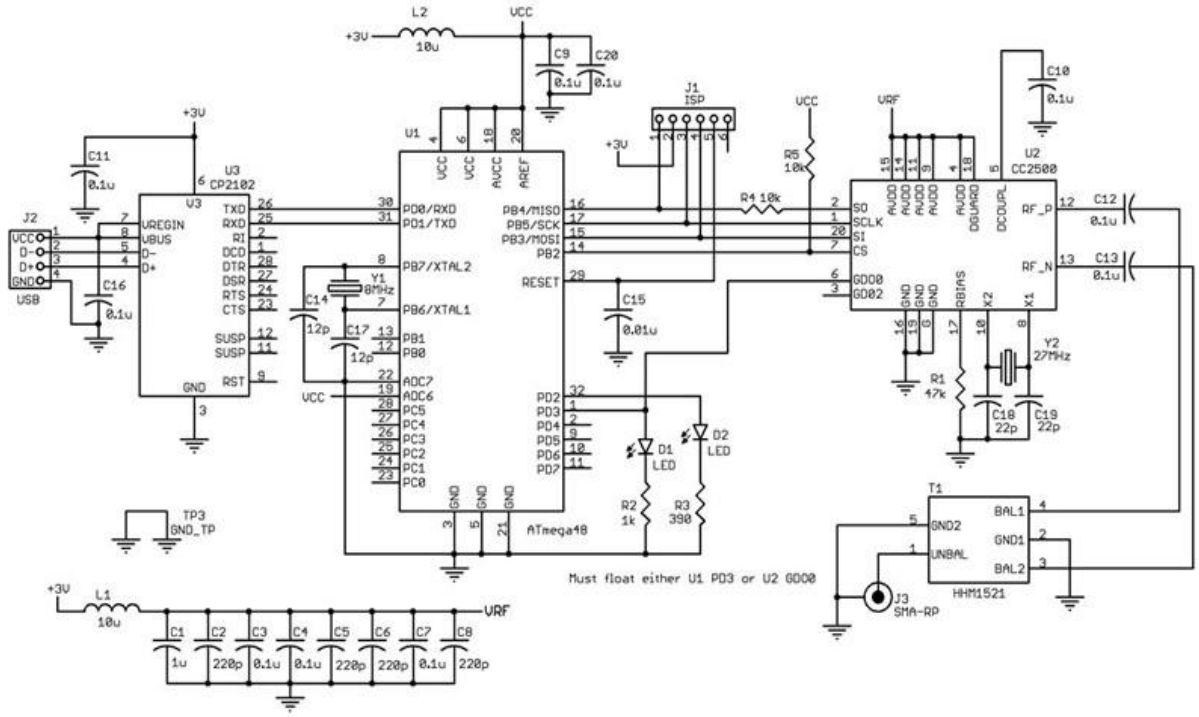


Рис. 3.6. Електрична принципова схема аналізатора спектру на Chipcon CC2500

Таблиця 3.1

Список електронних компонентів до аналізатора спектру на Chipcon CC2500

Позначення	Значення	Опис	Кількість
C1	1 мкФ	конденсатор	1
C2, C5, C6, C8	220 пФ	конденсатор	4
C3, C4, C7, C9–C11, C16, C20	100 нФ	конденсатор	8
C12, C13	100 пФ	конденсатор	2
C14, C17	12 пФ	конденсатор	2
C15	10 нФ	конденсатор	1
C18, C19	22 пФ	конденсатор	2
J1	ISP	6-контактний з’єднувач	1
J2	USB	USB-роз’єм	1
J3	SMA	SMA-з’єднувач	1
L2, L1	10 мкГн	індуктивність	2
R1	47 кОм	резистор	1
R2	1 кОм	резистор	1
R3	390 Ом	резистор	1
R4, R5	10 кОм	резистор	2
T1	HHM1521	трансформатор 2,4 ГГц	1
U1	ATmega48	ATmega48 TQFP	1
U2	CC2500	CC2500 трансивер	1
U3	CP2102	USB-UART контролер	1
Y1	8 МГц	кварц	1
Y2	27 МГц	кварц	1

Згідно схеми, приведеної на рис. 3.6, розробимо друковану двосторонню плату (рис. 3.7а).

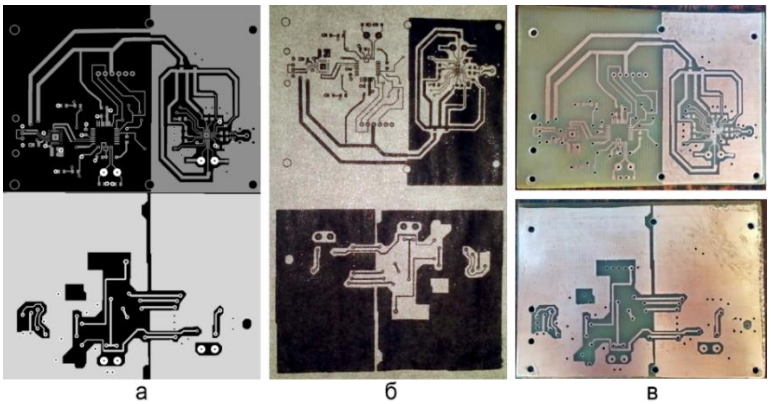


Рис. 3.7. Друкована плата аналізатора спектру на Chipcon CC2500:
а – проект в графічному редакторі; б – термопапір з надрукованою платою;
в – витравлена плата

На рис. 3.7б продемонстровано термопапір з надрукованою платою. Плата виконана на склотекстоліті розмірами 96×71 мм і товщиною 1 мм. Плата, повністю готова для монтування елементів, подана на рис. 3.7в.

Після монтажу елементів за допомогою USB-програматора для AVR (на рис. 3.8) проведемо програмування мікроконтролера Atmega48 [10,11].

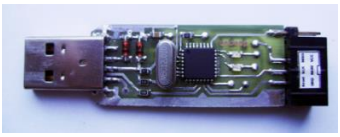


Рис. 3.8. Програматор для AVR мікроконтролерів

На рис. 3.9 подано запрограмовану друковану плату аналізатора спектру на Chipcon CC2500 повністю готову до застосування з вмонтованими елементами.

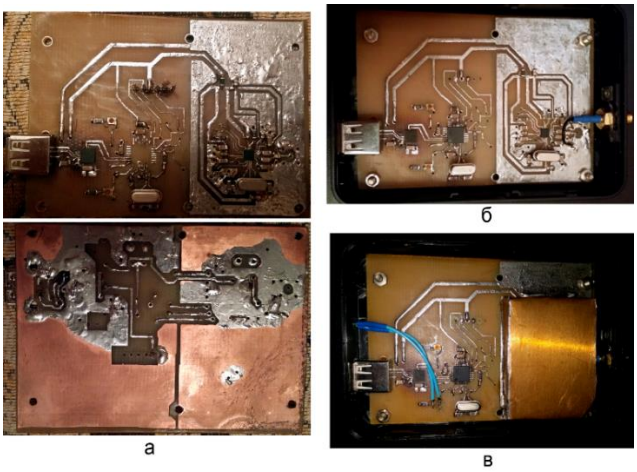


Рис. 3.9. Прототип аналізатора спектру на Chipcon CC2500:
а – із змонтованими елементами; б – встановлена в корпус; в – з екраном

Результати роботи аналізатора спектру представлені на рис. 3.10.

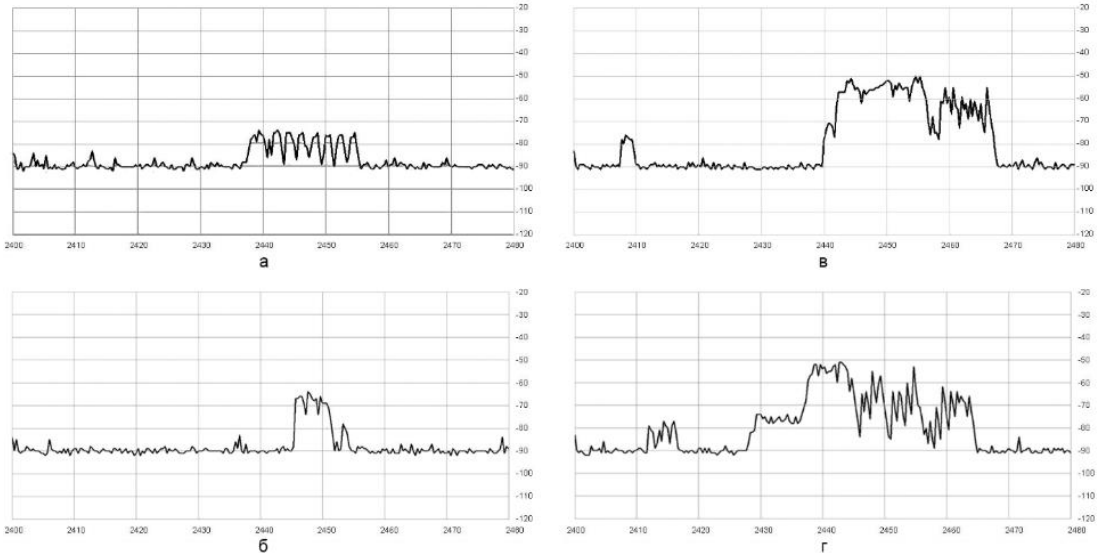


Рис. 3.10. Аналіз спектру, отриманого від Chipcon CC2500:
а – без використання антени і екрану; б – з використанням екрану, але без антени;
в – з використанням антени, але без екрану; г – з використанням антени і екрану

Для реалізації аналізатора спектру зі змінним трансивером задіємо мікрозбірки MD7105-SY, A7105 або їхні аналоги (рис. 3.11).

Рис. 3.11. Зовнішні вигляд модуля трансивера MD7105-SY

Процес виготовлення друкованої плати порівняно з попереднім зразком змінено і подано на рис. 3.12.

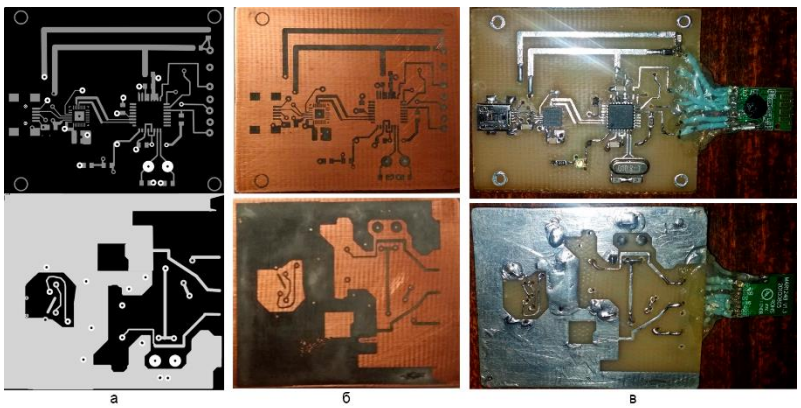


Рис. 3.12. Друкована плата аналізатора спектру на модулі MD7105-SY:
а – проект в графічному редакторі; б – витравлена; в – у готовому пристрою

Для реалізації аналізатора спектру за супергетеродинним принципом використано мікрозбірку Cypress CYWUSB6935 [12]. На рис. 3.13 показано принципову схему, в табл. 3.2 – перелік компонентів, а на рис. 3.14 – зібраний на монтажній платі перехідник.

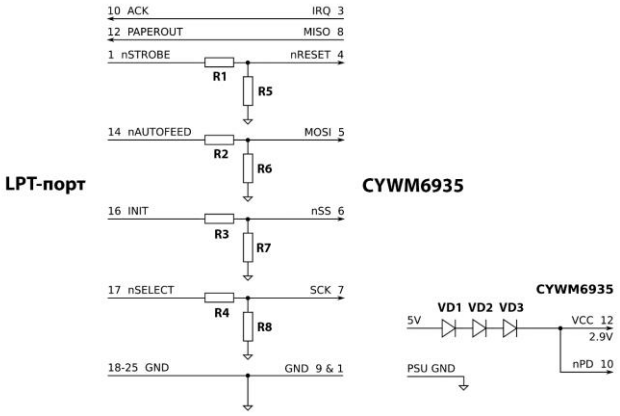


Рис. 3.13. Електрична принципова схема під’єднання до модуля CYWUSB6935

Таблиця 3.2

Список електронних компонентів до USB-аналізатора на модулі CYWUSB6935

Позначення	Значення	Опис	Кількість
R1–R4	10 кОм	резистор	1
R5–R8	15 кОм	резистор	4
VD1–VD3	1N4001	діод	3

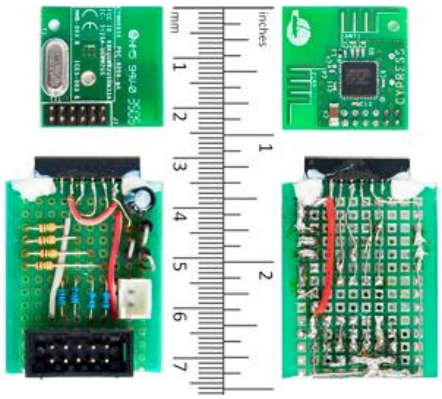


Рис. 3.14. Зовнішній вигляд готового LPT-аналізатора спектру
на модулі CYWUSB6935

При зчитуванні напряму з LPT-порта отримано данні в наступному вигляді (частина пакетів з рівнем RSSI):

frame:

[0,0,1,1,0,0,2,1,0,2,0,0,4,31,30,29,0,0,0,0,0,3,0,0,0,0,0,0,0,0,0,0,1,1,0,0,0,1,0,2,0,
0,0,0,0,0,0,1,0,0,2,0,0,0,2,0,0,0,1,0,4,5,1,1,0,0,1,1,0,1,1,1,0,0,0,0,3,2,1,0,0,0,0,1,]

Після збору даних отримано результуючу картинку спектру (рис. 3.15).

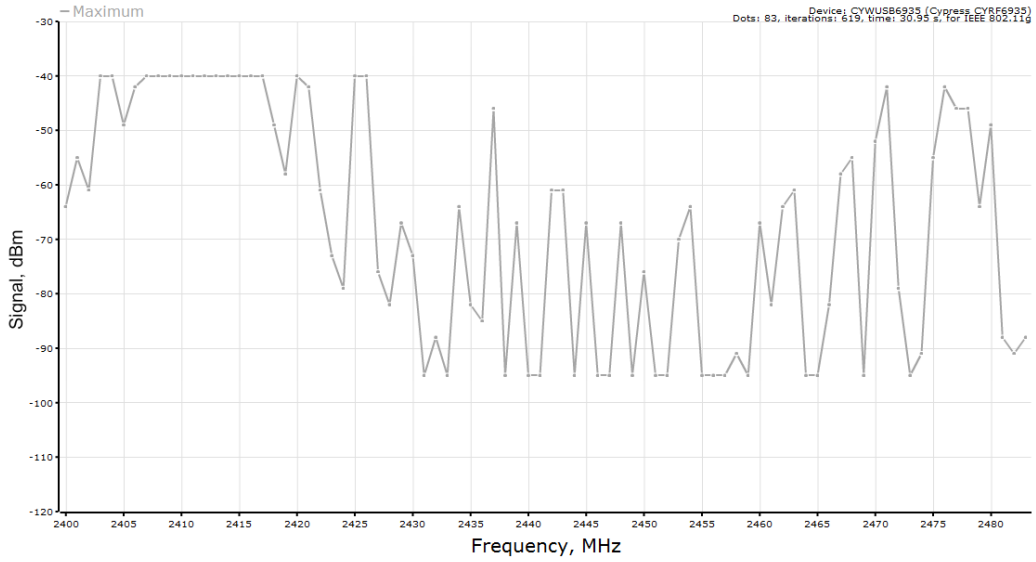


Рис. 3.15. Результат аналізу даних від аналізатора спектру на модулі CYWUSB6935

Конструкція має суттєвий недолік – робота на застарілому LPT-інтерфейсі, який нечасто зустрічається в сучасних комп'ютерах. Крім того, потрібне додаткове живлення. В даному випадку застосовувалось живлення від USB-порта послідовно підключеними трьома діодами для зниження напруги.

Принципову схему аналізатора спектру зображено на рис. 3.16. Оскільки мікроконтролер має в собі все необхідне для USB, в тому числі стабілізатор напруги 3,3 В, буфер пам'яті і приймач, все що потрібно зробити – підключити USB-кабель до виходів 15 і 16 мікроконтролера і конденсатор до виводу 14 для фільтрації напруги 3,3 В від вбудованого стабілізатора.

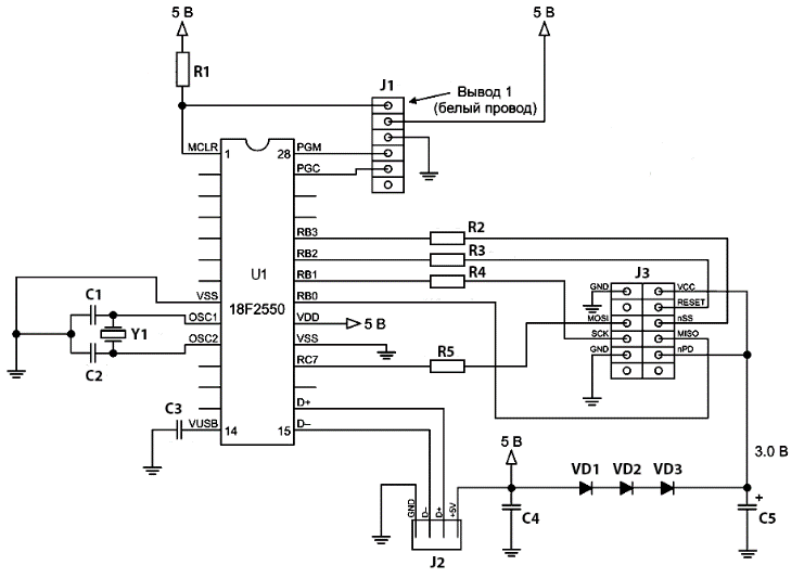


Рис. 3.16. Електрична принципова схема керування модулем CYWUSB6935

Тактування мікроконтролера здійснювалось від кварцового резонатора 20 МГц з двома навантажувальними конденсаторами 15 пФ. Внутрішній дільник мікроконтролера ділить при цьому тактову частоту на 5, щоб отримати значення частоти 4 МГц, яка буде використовуватися для фазового автопідлаштування частоти, що працює на частоті 48 МГц. Це основна тактова частота, на якій працюють USB інтерфейс і ядро. Резистор номіналом 10 кОм, підключений до виводу 1 мікроконтролера, підтягує вивід MCLR (скидання) до високого рівня.

Живлення сканер отримує від інтерфейсу USB, так як схема споживає незначний струм. Для живлення радіомодуля необхідно напругу від 2,7 до 3,6 В. Напругу порядку 3,0 В можна отримати від шини 5 В, включивши послідовно 3 діода типу IN4001 (на кожному діоді падіння напруги близько 0,7 В). Це, звичайно ж, найпростіший і дешевий, але разом з тим цілком надійний спосіб.

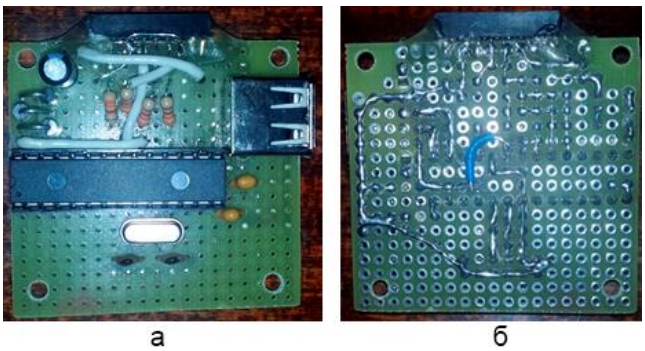
CYWUSB6935 має на входах захисні діоди. Це означає, що для керування можна використовувати 5-вольтові логічні сигнали мікроконтролера, включивши послідовні резистори для обмеження струму. В ході експерименту було обрано резистори з опором 3,3 кОм. Перелік компонентів представлений в табл. 3.3.

Таблиця 3.3

Список електронних компонентів до LPT-аналізатора на модулі CYWUSB6935

Позначення	Значення	Опис	Кількість
C1, C2	15 пФ	конденсатор	2
C3	220 нФ	конденсатор	1
C4	100 нФ	конденсатор	1
C5	100 мкФ	конденсатор	1
J1	ISP	6-контактний з’єднувач	1
J2	USB	USB-роз’єм	1
J3	ISP	10-контактний з’єднувач	1
R1	10 кОм	резистор	1
R2–R5	3,3 кОм	резистор	4
U1	PIC18F2550-I/SP	мікроконтролер	1
VD1–VD3	1N4001	діод	3
Y1	20 МГц	кварц	1

Так як схема є не надто складною, для складання пристрою оберемо найпростіший шлях: макетна плата (див. рис. 3.17). Для підключення радиомодуля використаємо спеціальний багатопіновий USB-роз’єм [11].



а б

Рис. 3.17. Готовий пристрій

Через програматор (рис. 3.18) запрограмуємо мікроконтролер PIC18F2550-I/SP.

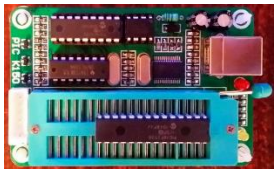


Рис. 3.18. Програмування мікроконтролера

3.2.2. Порівняльний аналіз сучасних спектроаналізаторів та їх програмного забезпечення

Програма аналізатору спектру Low-Cost Spectrum Analyzer (LCSA) – це 32-бітний додаток для ОС Windows XP (не вимагає встановлення). При роботі з ОС Windows 7 потрібно встановити VP Windows XP Mode, щоб усунути проблему з драйверами. Перед першим використанням ПЗ, необхідно встановити драйвер для мікросхеми адаптера COM2USB Silicon Labs CP2102. Після підключення аналізатора спектру, встановлення драйвера для CP2102 і запуску LCSA, ПЗ повинно негайно розпочати збір даних і в режимі реального часу демонструвати ISM-діапазон спектру на 2,4 ГГц. На вкладці *View* доступні такі функції: утримання піку, заморожування піку, а також вибір фонів (чорного або білого). На вкладці *Plotting Options* є функції для налаштування амплітуди і частоти.

При роботі з віртуальними COM-портам може виникнути ситуація, коли потрібно задавати вручну номер порту в реєстрі системи:

```
REGEDIT4
[HKEY_LOCAL_MACHINE\HARDWARE\DEVICEMAP\SERIALCOMM]
"\\device\\slabser0"="COM20"
```

Наочно ПЗ продемонстроване на рис. 3.19.

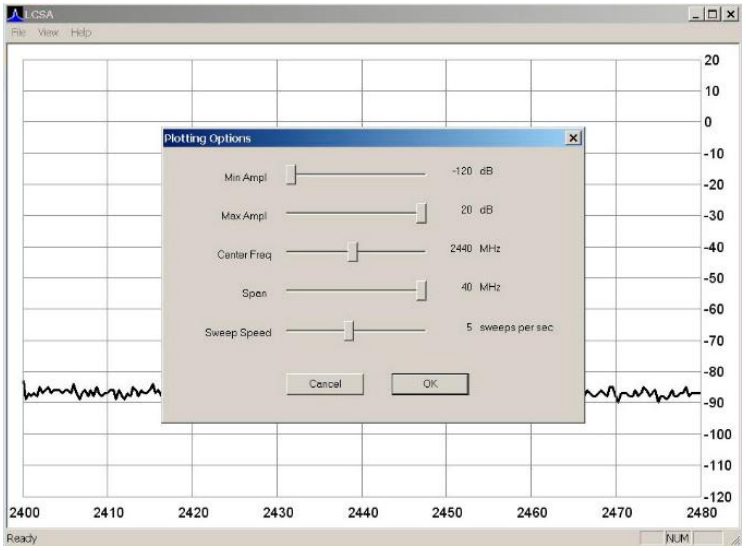


Рис. 3.19. Головні функції ПЗ LCSA

Використовуючи стандартний USB-інтерфейс підключимося до будь-якого комп'ютера, на якому встановлена ОС Windows XP/Vista/7. Перед тим як підключати пристрій до комп'ютера перевіримо апаратну частину (монтаж і підключення USB-кабелю), потім встановимо ПЗ, разом з яким буде встановлено і драйвер сканера. Тільки після цього сканер можна підключати до комп'ютера. У диспетчері пристроїв, в розділі *Інші пристрої*, можна побачити підключений в системі сканер ISM-діапазону.

Кнопка *Export* призначена для експорту поточних відліків в файл **.csv*, який може бути завантажений в програму Excel для обробки і побудови графіків.

При запуску ПЗ потрібно перевірити, що пристрій підключений: «Connected to Geoff's 2.4 GHz Scanner». Повідомлення «Scanner not found» означає, що пристрій або не підключений, або не працює.

При запуску ПЗ і підключенні сканера до USB в основному вікні програми можна побачити спектр сигналу діапазону 2,4 ГГц. Якщо поблизу немає безпроводових пристроїв ISM-діапазону, спектр буде відображати фоновий шум і шум радіочастотної частини CYWUSB6935.

Вертикальна шкала (рівень сигналу) не відкалібрована, вона має відносний характер, оскільки відображає рівень сигналу, який посилає радіомодуль. Спектр сигналу (рис. 3.20) відображає роботу ТБД Wi-Fi маршрутизатора (стандарту IEEE 802.11n), налаштованого на 8-й канал з центральною частою 2,447 ГГц і розташованого на відстані у 10 м.

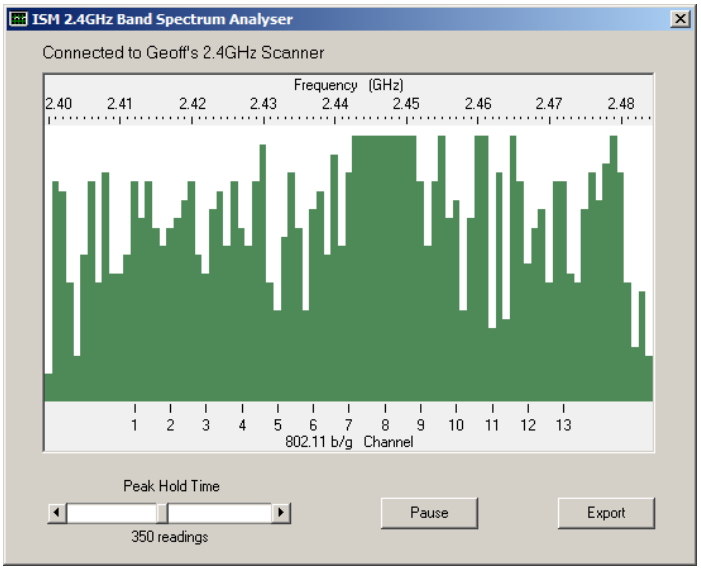


Рис. 3.20. Спектр сигналу безпроводового маршрутизатора IEEE 802.11n

На рис. 3.21а і 3.21б представлено результати прийому при розташуванні аналізатора спектру в ближній зоні передавача для передача даних по безпроводовому каналу Bluetooth, а на рис. 3.21в і 3.21г – Wi-Fi діапазону 2,4 ГГц. З рисунків легко бачити, що суцільна збірка показала набагато якісніші результати через те, що в ній якісніше проведена збірка, використаний екран і зовнішня антена.

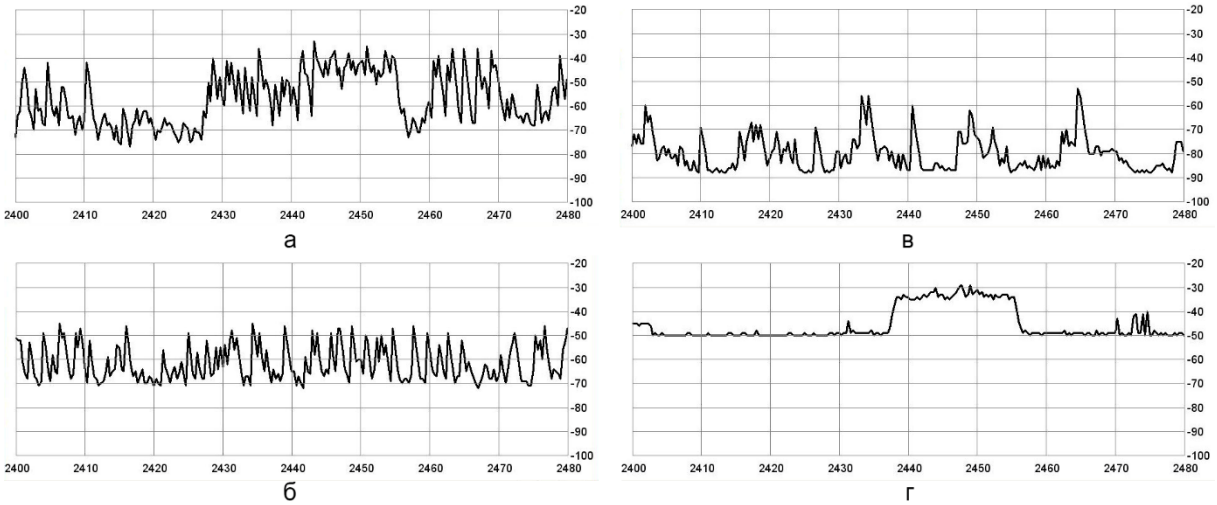


Рис. 3.21. Приклади спектрів для різних збірок:
а – Bluetooth для модульної; б – Bluetooth для суцільної;
в – Wi-Fi для модульної; г – Wi-Fi для суцільної

Після закінчення збірки, тестування і налагодження пристрої готові для використання як у технічний, так і у наукових задачах. Загальний вигляд усіх трьох пристроїв показано на рис. 3.22 [13].

Рис. 3.22. Загальний вигляд усіх приладів

В [14–17] наведені інші приклади реалізації аналізаторів спектру.

3.3. Дослідження технології моніторингу вільних каналів передавання даних в безпроводових мережах

Надійність системи моніторингу в ході натурного експерименту вимірювалась за такими критеріями:

кількість критичних помилок під час безперервної роботи системи, протягом 10 годин;

кількість невдалих динамічних відключень модулів протягом 30 спроб;

кількість невдалих динамічних підключень модулів протягом 30 спроб.

За своєю суттю систему моніторингу можна віднести до сенсорної безпроводової мережі. Такі системи повинні безперервно працювати значну кількість часу, яка вимірюється в роках. Саме тому, необхідно забезпечити надійну роботу системи на протягом тривалого часу.

Виходячи з такого було прийнято рішення, опиратись на значення в 10 годин, яке є, як на наш погляд, самим оптимальним часом в режимах активної розробки. Як результат, всі три версії системи успішно пройшли тестування. За весь час роботи, не було виявлено жодної помилки, зв’язаної з процесом роботи системи. Певні острахи були пов’язані лише модулями Pololu Wixel, коли система інколи на деякий час призупиняла роботу, а потім в довільному режимі її знову продовжувала. Є припущення, що таку ситуацію міг спричинити неправильно закритий порт модуля під час зчитування даних, в результаті, ПЗ могло довго чекати на повторне з’єднання з цим модулем, адже в другій версії не використовується таймаут на очікування під час з’єднання.

З іншими тестами перша версія (рис. 3.23) системи моніторингу впоралась також аж занадто добре.

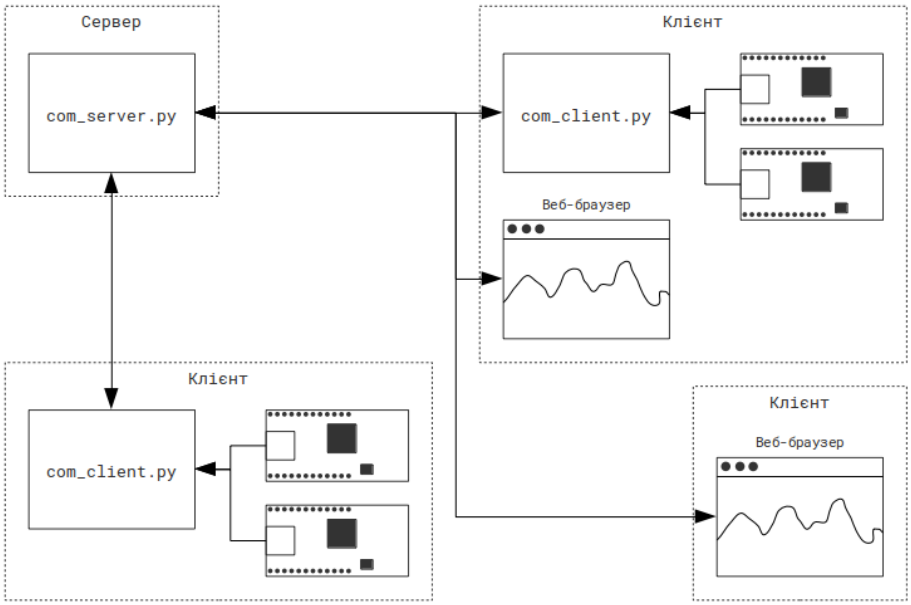


Рис. 3.23. Інфраструктура першої версії системи моніторингу

Завдяки функціонуючій в системі моніторингу схемі зупинки роботи з модулями, було регламентовано процес одночасного безпечного під'єднання/від'єднання модулю(-ів) до/від системи. Як результат, не було отримано помилок для жодної з операцій. Варто зазначити, що це не зовсім коректний тест саме для першої версії, адже вона не надавала можливості динамічного від'єднання та приєднання модулів.

Друга версія зазнала великої невдачі протягом наступних тестів (рис. 3.24).

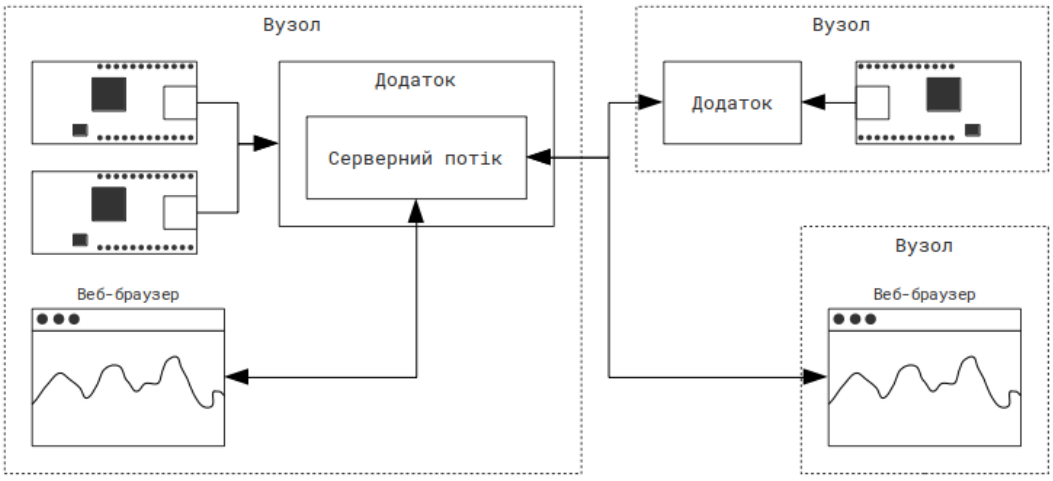


Рис. 3.24. Веб-інтерфейс першої версії системи моніторингу

Приблизно 90% спроб динамічно від’єднати модуль закінчувались критичною помилкою з подальшою зупинкою роботи вузла. Трохи кращим виявився результат для зворотної операції, приблизно в 25% спроб, виникали такі ж критичні помилки. Однак обидва результати були неприпустимі для надійної системи моніторингу. Джерелом проблеми виявилась некоректна обробка виключень в коді.

Як і перша версія, програмна реалізація третьої версії впоралась з наступними тестами відмінно. Завдяки тому, що використовувались потоки для роботи з кожним модулем, помилки, що в них виникали, не загрожували функціонуванню системи в цілому. Як результат, в ході 30 спроб для кожної з операцій від’єднання та приєднання модулів не було виявлено жодної помилки.

Додатково був проведений тест для третьої версії системи моніторингу (рис. 3.25). Так як, дана реалізація відповідала поставленим вимогам при початковій постановці завдання, необхідно було протестувати, наскільки система є відмовостійкою та перевірити її децентралізовану архітектуру. Суть тесту – впевнитись, що відключення вузла від системи обробляється коректно і не викликає помилок. Як результат, система успішно виконала дану операцію, а час на реагування становив приблизно 1–4 с.

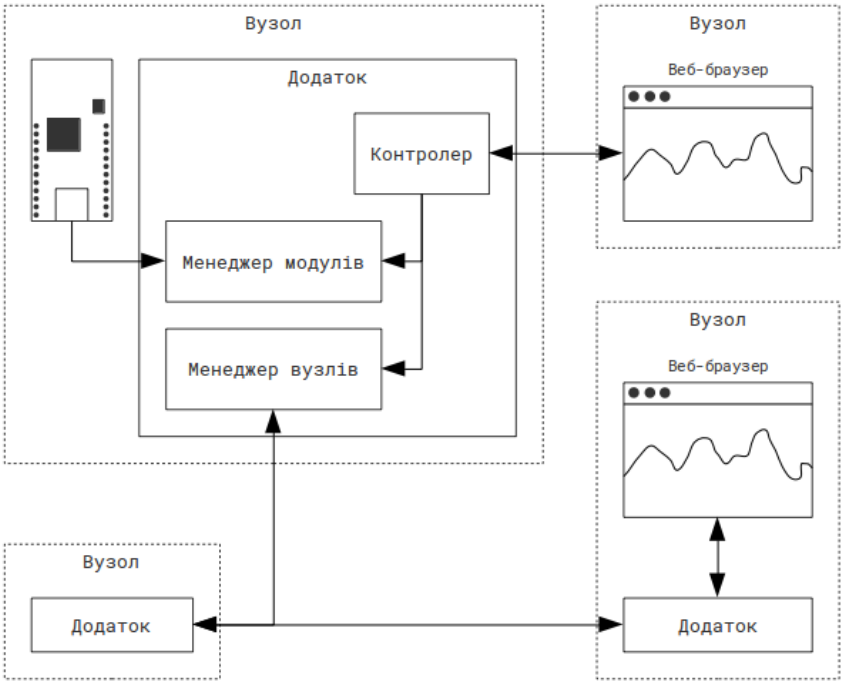


Рис. 3.25. Схема роботи третьої версії

За допомогою цих тестів було встановлено, що перша версія, не дивлячись на невдалу архітектуру і логіку роботи, все ж впоралась з завданням досить на пристойному рівні. Друга версія показала стабільність тривалої роботи без динамічного під'єднання та від'єднання модулів, що потребувало значних змін та вдосконалень. Третя версія із навантаженнями і збоями робити датчиків впоралась найкраще. Система стала працювати стабільно та очікувано. Децентралізована архітектура системи реалізована за простою схемою, що підвищує її надійність та відмовостійкість.

В ході роботи, система повинна бути готова підтримувати значну кількість як вузлів, так і модулів на кожному з них. В залежності від площі об'єкта моніторингу та складності мережі, може використовуватись різна конфігурація інфраструктури системи моніторингу. Тут головне забезпечити гнучкість системи, надати змогу легко допрацювати необхідний функціонал або швидко налагодити параметри системи для різних умов. Іншим важливим параметром є навантаження на апаратні ресурси. На жаль, під час розробки кожної із версій систем, проводився свій набір тестувань, використовуючи доступні апаратні засоби. Тобто, під час розробки першої та другої версії системи моніторингу, ми не мали змоги використати мікрокомп'ютери Raspberry Pi, тестування проводилось на комп'ютерах (рис. 3.26).

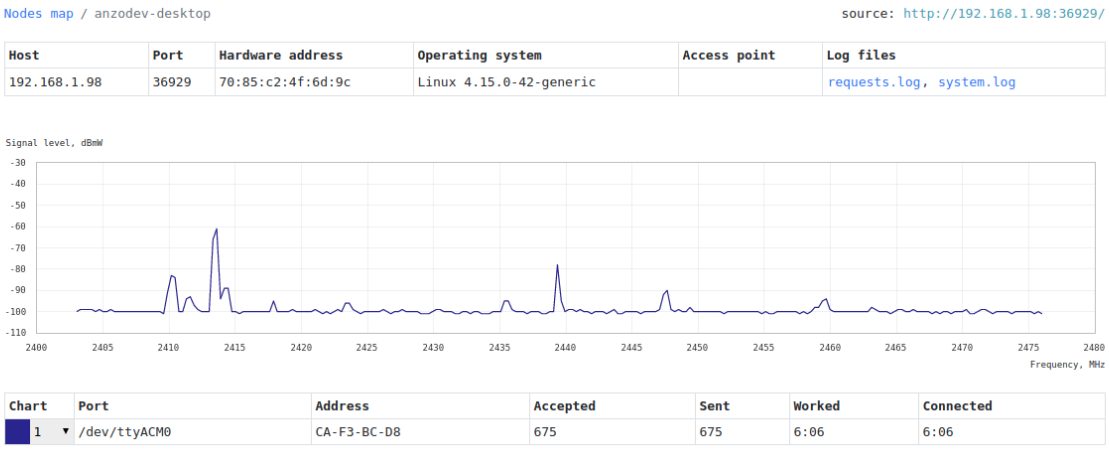


Рис. 3.26. Веб-інтерфейс третьої версії системи моніторингу

Для першої версії було поставлено вимоги підтримувати одночасно до 5 клієнтських додатків та до 5 модулів на кожному з них. Через проблеми в архітектурі та погано продуманій логіці, з 10 спроб під'єднати клієнтський додаток, 7–9 із них закінчувались критичною помилкою разом із зупинкою сервера. Однак, завдяки простій послідовній схемі роботи з модулями ми легко могли підтримувати

5 і більше модулів на одному клієнті, щоправда, це не несло особливого сенсу. Стосовно навантаження, інтерпретатор Python займає приблизно 9 МБ ОЗП. Разом з мікрофреймворком flask, це значення зростає до 20. Отже серверний додаток використовував приблизно 25 МБ ОЗП в процесі своєї роботи, при обробці запитів могла використовуватись додаткова пам'ять в розмірі 3–5 МБ. Клієнтський додаток не перевищував позначки у 15 МБ. Тестування навантаження проводилось на процесорі Intel Core i5 3317U. Це мобільний процесор, побудований за 22 нм технологією, що має базову тактову частоту 1,7 ГГц. Серверний додаток, в середньому, створював навантаження в межах 2–6% при роботі з 1 клієнтом. Клієнтський додаток міг навантажити процесор на 30–40%, іноді значення сягало 80%. Таке навантаження спричиняв не ефективний спосіб зчитування даних з модулів. З точку зору використання пам'яті система моніторингу має прийнятні показники. Однак, система створює значне навантаження, навіть на досить продуктивній апаратній частині, як для такого рівня ПЗ. В результаті тестування, можна зробити висновок, що система позбавлена можливості масштабування, а значне навантаження на центральний процесор не дозволить працювати системі на мікрокомп'ютерах.

Друга версія системи моніторингу, має повністю аналогічні показники для того ж набору тестувань. Однак, на вузлах, в яких працював серверний потік витрата пам'яті була значно більшою. Вузли без серверного потоку займали приблизно 20 МБ ОЗП в ході роботи. Додаток з сервером після запуску займав 30–35 МБ ОЗП. Це також було обумовлено тим, що працював новий функціонал зі збереженням значень рівня сигналу. В ході тривалої роботи було помічено, що витрата пам'яті зростає лінійно. Через 4–5 годин безперервної роботи, додаток міг використовувати 45–50 МБ пам'яті. Ця ситуація була досить дивною, адже Python має вбудований функціонал для збору сміття (автоматичне очищення пам'яті від ресурсів, що більше не використовуються), тобто, витік пам'яті вкрай малоймовірний. На жаль, в той момент часу ми не змогли найти відповідь на це питання, але факт того, що система мала проблеми з використанням пам'яті, на практиці робило другу версію системи менш ефективною ніж перша, не дивлячись на більш примітивну реалізацію. Все це сприяло тому, щоб створити нову систему, яка була б позбавлена минулих проблем.

Під час розробки третьої версії ми могли використовувати мікрокомп'ютери Raspberry, тому тестування проводилось саме на них. На цей раз нам вдалося створити інфраструктуру, що успішно підтримувала одночасну роботу більше,

ніж 4 вузлів. Тепер подальше масштабування залежало від продуктивності ТБД та мережевого обладнання. З цим завданням система впоралась, вона може функціонувати з величезною кількістю вузлів одночасно. Стосовно використання оперативної пам’яті, під час тривалої роботи, додаток стабільно витрачає 22–26 МБ. Це досить припустиме значення навіть для вибагливих до ресурсів систем. Завдяки новому методу збору даних з модулів, ми досягли того, що знизили навантаження на центральний процесор до значень 0–4%. Використовуючи більш потужні системи, на кшталт стаціонарних комп’ютерів або ноутбуків, цей показник не перевищує 2%. Варто зазначити, таке навантаження зберігається для будь якої кількості одночасно підключених модулів до вузла. З точки зору горизонтального масштабування, система використовує апаратні ресурси надзвичайно ефективно без негативного впливу на надійність системи. Навантаження може зрости, якщо до вузла будуть надходити запити з веб браузерів. Наприклад, якщо три різні клієнтські веб-браузери, одночасно почнуть надсилати запити на отримання даних про рівень сигналу, навантаження на процесор не перевищує 8–10%. На нашу думку, це чудовий результат, враховуючи те, що система працює на мікрокомп’ютерах. Можливо використання протоколу WebSocket зможе покращити цей результат. Підводячи підсумок, в третій версії ми досягли максимально ефективної продуктивності з точки зору використання ресурсів. Система чудово масштабується, що в рази підвищує захищеність та потужність інфраструктури. Маючи такі результати, система все одно надає можливість подальшого вдосконалення [18].

3.4. Дослідження технології підвищення захищеності безпроводових мереж з використанням прискорюючих лінз

3.4.1. Перевірка роботи прискорюючою лінзи у діапазоні 2,4–2,5 ГГц

Для виявлення впливу ПЛ, розташованої на боці приймача було побудовано експериментальний канал зв’язку між передавачем і приймачем. На рис. 3.27 показана схема експерименту. В якості передавача використовувалася ТБД Asus RT-N16 (на мікроконтролері Broadcom 4718A, 533 МГц) з прошивкою DD-WRT v24-sp2 mega і несиметричним вібратором в якості неспрямованої антени. Макет ПЛ побудовано з картону, вкритого алюмінієвою фольгою, на пінополістероловому каркасі. В якості приймача використано зовнішній безпроводовий пристрій Wiflycity IDU-2850UG-G2000 (на мікроконтролері Realtek RTL8187L) з неспрямованою

антеною. Аналіз спектру сигналу проводився за допомогою аналізатора спектру Ubiquiti AirView2.

Характеристики сигналу: ширина спектру 10 МГц, схема модуляції за допомогою додаткового коду (complementary code keying, CCK) з однією несучою за стандартом 802.11b.

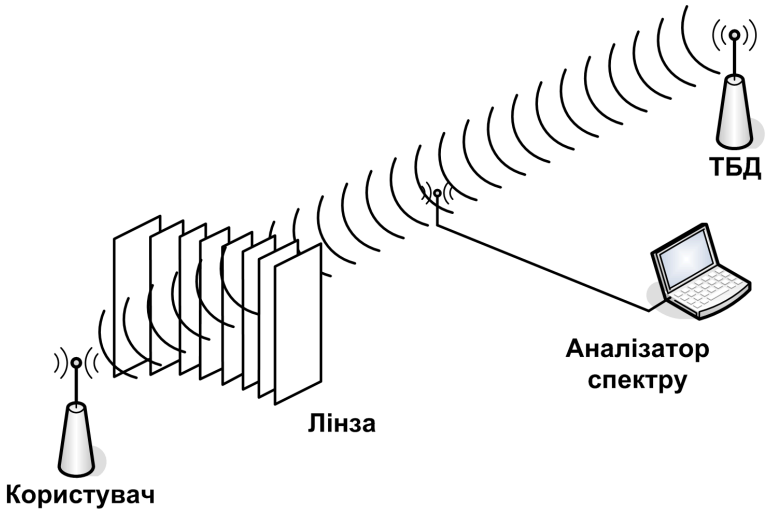


Рис. 3.27. Схема експерименту з ПЛ на боці користувача

Так згідно з (2.40) для відстані $R_{зв}$ = 11 м максимальний радіус першої зони Френеля становить $R_{зФ1}$ = 0,586 м. З цієї зони було вилучено усі зайві предмети.

ПЛ була встановлена на стороні користувача (але її можна встановлювати і на ТБД з неспрямованою антеною для фокусування в вибраному напрямку).

Дані про рівень сигналу отримані за методикою, описаною в [19], та представлені на рис. 3.28. При розгляді кривої з максимальними значеннями видно, що у сигналах можна виявити нестаціонарні завади (найбільші на частотах 2,417 і 2,452 ГГц), а при розгляді кривої з медіанними значеннями – стаціонарні завади (найбільші на частотах 2,400 і 2,448 ГГц).

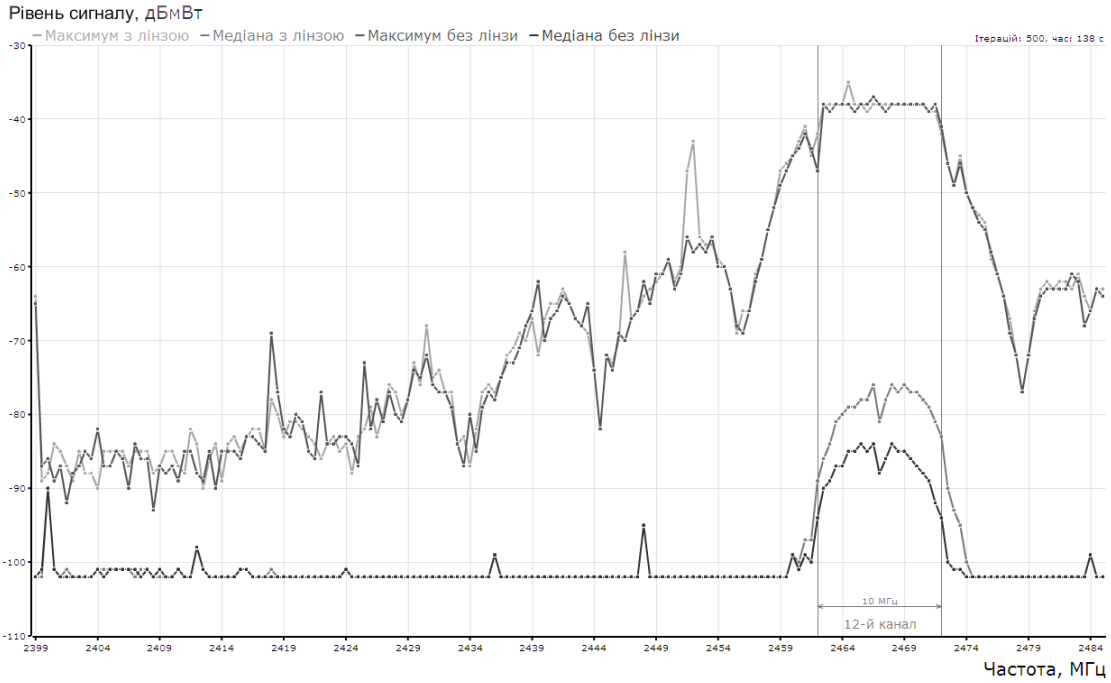


Рис. 3.28. Спектр сигналів з ПЛ і без

З кривої з медіанними значеннями видно, що середнє підсилення сигналу в полосі передавання (10 МГц) становить 5–7 дБ. Таке покращення рівня сигналу дозволяє покрити важко доступні ділянки, віддалені від основної зони покриття у 1,8–2,2 рази. Крім того при передаванні одного і того самого потоку даних з ПЛ і без змінювалася швидкість передавання даних:

без ПЛ середній рівень сигналу становить мінус 85 дБмВт, а середня швидкість передавання 680 кб/с;

з ПЛ – мінус 78 дБмВт і 710 кб/с відповідно.

Тобто введення ПЛ в робочу систему в проведеному експерименті покращило швидкісні показники на 4%.

З іншого боку, було досліджено вплив ПЛ на дальність прийому при граничній відстані між передавачем і приймачем. На передавальній стороні (ТБД) було встановлено неспрямовану антену з підсиленням у 5 дБ, а на приймальній стороні (користувач) – спрямовану антену у 10 дБ. На рис. 3.29 показано схему експерименту.

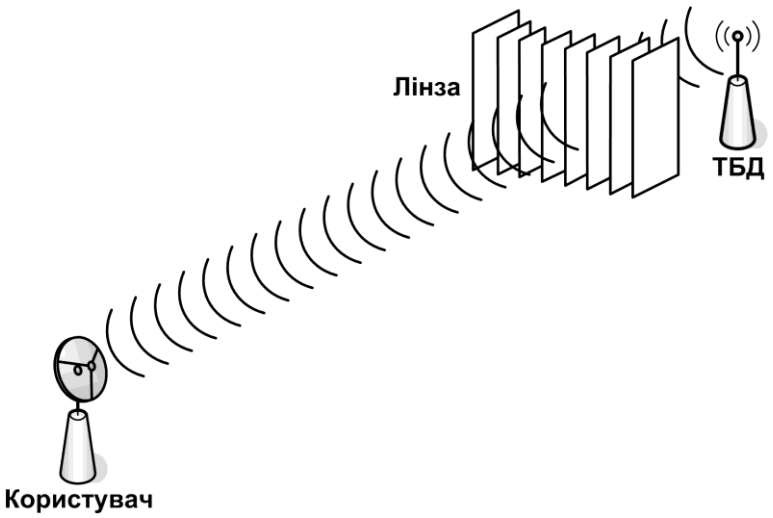


Рис. 3.29. Схема експерименту з ПЛ на боці ТБД

В експерименті передавач був розташований на висоті h_1 = 8 м, а приймач – h_2 = 2 м, довжина хвилі для 5-го каналу становила λ = 0,123 м, а відстань було обрано за результатами приблизної інженерної формули:

$$P'_{\text{пр}} = -175 + 20\lg R_{\text{зв}} + P'_{\text{пер}} + G'_{\text{пр}} + G'_{\text{пер}} + \Delta'_{\max}, \tag{3.5}$$

де $P'_{\text{пр}}$, $P'_{\text{пер}}$, $G'_{\text{пр}}$ і $G'_{\text{пер}}$ – чутливість приймача, потужність передавача, коефіцієнт підсилення антени приймача і передавача в децибелах (характеристики приладів див. нижче); $\Delta'_{\max}$ = 1 дБ – максимальна можлива похибка виготовлення антен.

Враховуючи таке інтервал відстаней, при яких буде спостерігатися зрив зв'язку, згідно формули (3.5) становитиме 168..188 м. Приймаємо відстань в середині інтервалу $R_{зв}$ = 175 м. Номінальна потужність передавача ТБД Asus RT-N16 становить 19,5 дБмВт (з технічної документації виробника), підсилення стаціонарної антени – 5 дБ, а підсилення ПЛ з отриманих раніше результатів – 6 дБ. Тоді з формули Введенського [20] потужність випромінювання на приймачі в децибелах з урахуванням впливу землі:

$$\begin{gathered} P'_{\text{пр}} = P'_{\text{пер}} + G'_{\text{пр}} + G'_{\text{пер}} - K'_{\text{Землі}} = \\ = P'_{\text{пер}} + G'_{\text{пр}} + G'_{\text{пер}} - 20\lg\frac{V}{R_{\text{зв}}} - 20\lg f_{\text{сер}} - 93 = \\ = P'_{\text{пер}} + G'_{\text{пр}} + G'_{\text{пер}} - 20\lg 4\pi\frac{h_1 \cdot h_2}{\lambda \cdot R_{\text{зв}}^2} - 160{,}75, \end{gathered} \tag{3.6}$$

де $K'_{\text{сер}}$ – зниження потужності випромінювання за рахунок впливу землі і відстані між передавачем і приймачем; $f_{\text{сер}}$ = 2,442 ГГц – середня частота; $V = 4\pi\frac{h_1 \cdot h_2}{\lambda \cdot R_{\text{зв}}}$ – коефіцієнт Введенського, в якому враховані h_1 і h_2 – висоти передавача і приймача відносно землі, λ – довжина хвилі, на якій проводилося вимірювання.

Із загальної формули (3.6) отримуємо потужність без ПЛ і з нею:

$$P'_{\text{пр}} = (-96{,}8 \pm 0{,}2)\ \text{дБмВт},$$
$$P'_{\text{пр.лінза}} = (-90{,}8 \pm 0{,}2)\ \text{дБмВт}.$$

Максимальна чутливість приймача на RTL8187L становить $P'_{\text{пр.max}}$ = –91 дБмВт (з технічної документації виробника для стандарту 802.11b), а з розрахунків спрямованої приймальної антени отримано максимальний коефіцієнт підсилення 14 дБ. Тому без ПЛ маємо $P'_{\text{пр}} < P'_{\text{пр.max}}$ – зв'язок неможливий, а з ПЛ – $P'_{\text{пр.лінза}} < P'_{\text{пр.max}}$ – можливий.

За результатами вимірювання отримано графік зриву передавання (див. рис. 3.30) для трьох випадків:

спрямованої антени з коефіцієнтом підсилення 10 дБ без ПЛ;

спрямованої антени з коефіцієнтом підсилення 10 дБ з ПЛ;

неспрямованої антени з коефіцієнтом підсилення 5 дБ з ПЛ, для якою зв'язок без ПЛ неможливий.

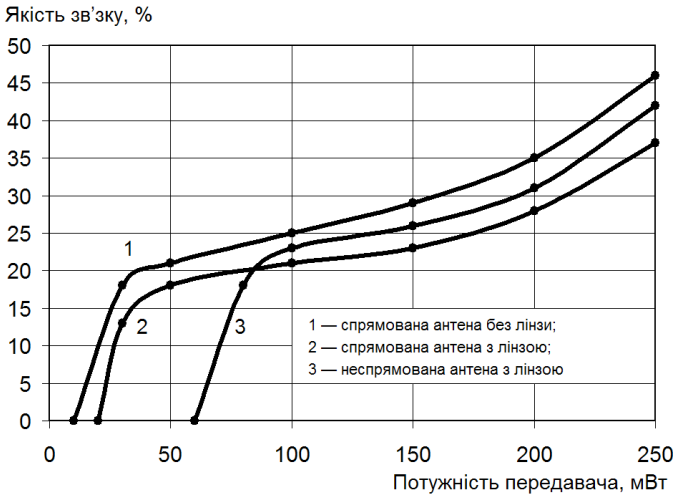


Рис. 3.30. Залежність якості зв'язку до потужності передавача

Відомо, що якість зв'язку визначається відношенням кількості прийнятих пакетів даних до кількості відправлених. З графіків на рис. 3.30 видно, що через недосконаліть виготовлення ПЛ крім вирівнювання фази на виході також спостерігається ефект часткового екранування і розсіювання. Так передавання зі спрямованою антеною на 10 дБ дає кращі результати, ніж використання неспрямованої антени на 5 дБ з ПЛ на 6 дБ (на рис. 3.31 показано ДС даної антенної системи, отриманої у програмному комплексі для моделювання антен Mmana-Gal basic версії 3.0.0.15).

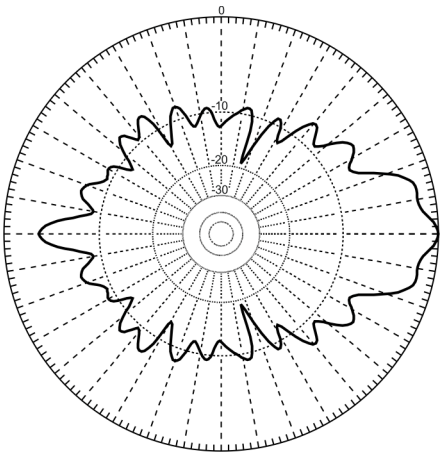
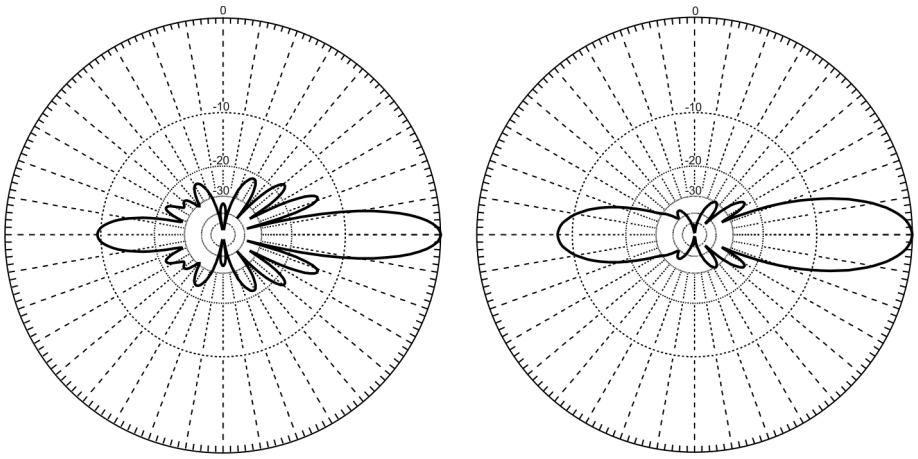


Рис. 3.31. ДС лінзової антени з несиметричним вібратором в горизонтальній площині

Між тим зрив передавання спрямованої антени з ПЛ починається навіть раніше, ніж у неспрямованою. Цей ефект крім екранування і розсіювання (особливо горизонтально поляризованого випромінювання) пояснюється також нерівномірністю розподілу амплітуд струмів у розкриві ПЛ. Початковий розрахунок ПЛ був проведений для неспрямованою антени, тому при використанні спрямованої розподіл буде наближатися до косінусоїдального. На рис. 3.32 показані ДС для двох видів розподілу.



Рівномірний розподіл Косінусодальний розподіл

Рис. 3.32. Порівняння ДС для рівномірного і косінусоїдального розподілу амплітуд в горизонтальній площині

З ДС видно, що має місце зменшення підсилення антенної системи з косінусоїдальним розподілом і при цьому збільшується задній пелюсток. З моделі абсолютне підсилення у напрямі головного пелюстка складає $\Delta G = G_{\text{рівн}} - G_{\text{кос}} = 15{,}85 - 14{,}58 \approx 1{,}3$ дБ [21,22].

Не менш цікавими є результати експериментального дослідження структури поля в азимутному секторі (до 60°) від осі ПЛ, орієнтованої на пріоритетного абонента. Його метою було визначення впливу «затемнення» ПЛ на абонентів, що знаходяться на інших азимутальних напрямках. Для цього було розроблено і виготовлено макет, який включає УМЛ; пристрій формування пакета даних і випромінювання сигналу; набір прийомних датчиків; необхідне обладнання і ПЗ для збору та обробки результатів.

Приймальні датчики розташовувалися по дузі радіуса 6,5 метрів (в далекій зоні лінзової антени), кутове розташування яких показано на рис. 3.33. Кут 30° був вибраний виходячи з розташування фокуса ПЛ і поперечних розмірів розкриву ПЛ як межа «геометричній» тіні. Розташування датчиків вибиралося з міркувань передбачуваної ширини ДС, положення провалів і бічних пелюсток. Розташування датчика в напрямку 60° вибрано для того, щоб оцінити вклад бічної пелюстки.

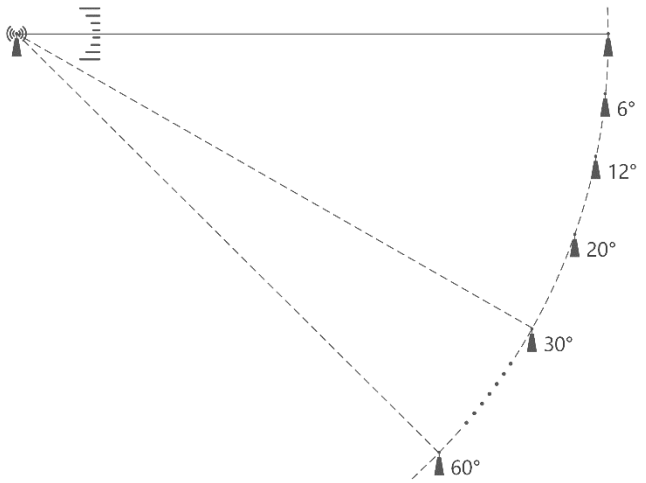


Рис. 3.33. Розташування елементів макета (в масштабі)

Металопластинчата ПЛ була розрахована за методикою з пункту 2.4.1 для частоти 2,45 ГГц. За результатами розрахунків зібрана нова (в порівнянні з [23]) циліндрична ПЛ, пластини якої виготовлені з діелектрика, покритого алюмінієвою фольгою. Каркас – з спіненого полістиролу. Поперечний розмір розкриву ПЛ – 52 см, висота – 33,5 см.

Частота передавача 2449,58 МГц (162-й ZigBee канал) обрана виходячи з мінімальної зайнятості спектра. Ширина спектра сигналу становить 600 кГц. Як приймач і передавач використовуються модулі Popolu Wixel на базі мікросхеми TI CC2511F32, яка працює за стандартом IEEE 802.15.4 з MSK. У передавальних і прийомних модулях вбудовані планарні антени.

Пристрій формування пакета даних і випромінювання сигналу включав передавач, що працює незалежно від приймаючої сторони. Приймачі підключені через USB (емуляція віртуального COM-порту) до одноплатного комп'ютера на базі Raspberry Pi. Прошивки для передавача і приймача різні, завдяки чому один модуль налаштований тільки на передачу, а решта - на прийом, і написані на діалекті мови C# для компілятора SDCC. Автоматичний пошук підключених датчиків, ініціалізація і збір даних проводився за допомогою скриптів на мові Python (версія 3). Зібрані дані передавалися на персональний комп'ютер по провідній мережі і оброблювалися за допомогою PHP скриптів (див. рис. 3.34).

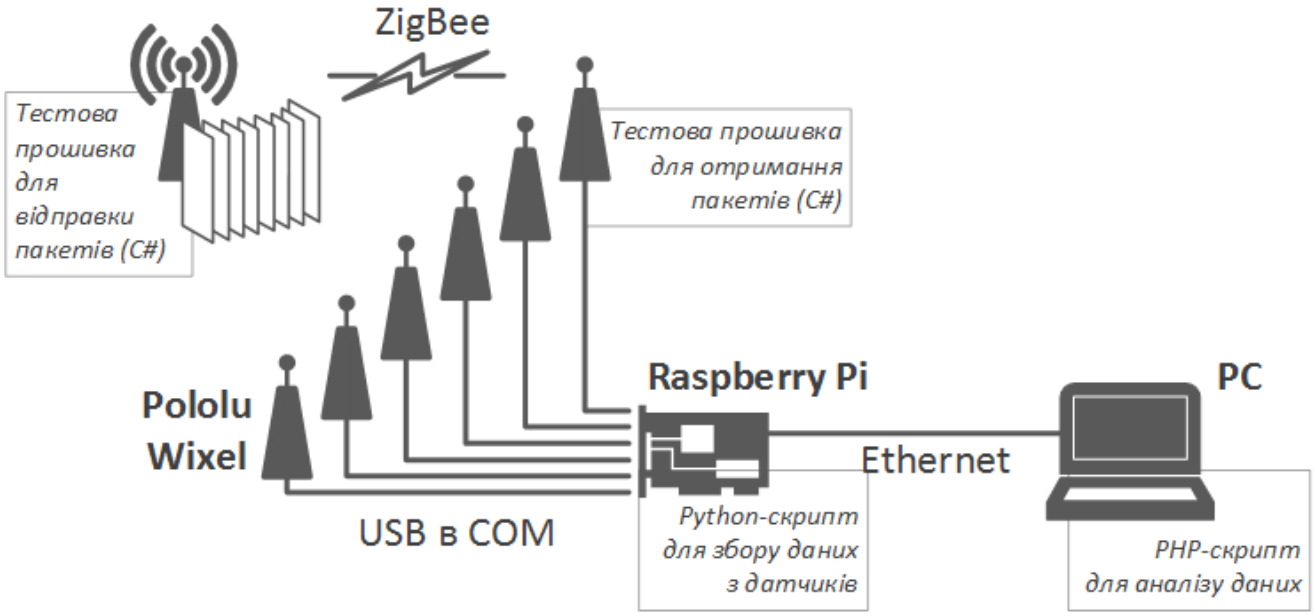


Рис. 3.34. Апаратно-програмний експериментальний макет

Експеримент проводився в офісному приміщенні у позаробочий час, щоб забезпечити мінімальний вплив безпроводових користувачів на результати експерименту. Було проведено десять сеансів прийому з використанням ПЛ і п'ять – без неї, кожен тривалістю в одну хвилину. За один сеанс відправлялося 350 пакетів. Тестовий ZigBee пакет (аналог UDP пакету) показано на рис. 3.35.

10	01	261B	45464748494A4B4C4D4E4F5051
Префікс	CRC	Лічільник	Дані (в ASCII – "EFGHIJKLMNOPQ")

Рис. 3.35. Структура тестового пакету

Лічильник в пакеті змінювався з інкрементом, тому можна однозначно ідентифікувати пакет, отриманий на різних пристроях.

Приклад такого пакета:

```
/dev/ttyACM2: 13-B5-6F-CC ?&?EFGHIJKLMNOPQ    -69  -85 1001261B45464748494A4B4C4D4E4F5051 162
/dev/ttyACM4: 2F-E1-FE-2B ?&?EFGHIJKLMNOPQ    -74  -96 1001261B45464748494A4B4C4D4E4F5051 162
/dev/ttyACM0: 74-95-F4-DB ?&?EFGHIJKLMNOPQ    -74  -99 1001261B45464748494A4B4C4D4E4F5051 162
/dev/ttyACM1: 88-5B-12-6F ?&?EFGlHJKLMNOPQ !  -76  -89 1001261B4546476C484A4B4C4D4E4F5051 162
/dev/ttyACM5: A9-FA-F5-78 ?&?EFGHIJKLMNOPQ    -71  -93 1001261B45464748494A4B4C4D4E4F5051 162
/dev/ttyACM3: 80-BB-85-9C ?&?EFGHIJKLMNOPQ    -76  -87 1001261B45464748494A4B4C4D4E4F5051 162
```

Зазначені датчики дозволили визначити в кожній точці усереднений рівень сигналу разом з шумом (щодо 1 мВт) за час прийому пакета. Також вимірювався усереднений рівень шуму за час паузи між пакетами (щодо 1 мВт). Це дозволило визначити показник відношення суми сигналу S і шуму N до шуму (далі – *SNNR*, порівн. *SNR*):

$$SNNR = 10\lg\frac{S+N}{N} = 10\lg(SNR+1), \tag{3.6}$$

Дані оброблялися по кожному пакету окремо. Якщо в момент початку або закінчення реєстрації даних деякі пакети не були отримані на всіх пристроях або були отримані з помилками, то такі пакети відфільтровувались. Тому усереднення в кожному кутовому напрямку вироблялося лише для пакетів без помилок, отриманих усіма пристроями.

На графіку (рис. 3.36) показана залежність від азимутального напрямку величини *SNNR* і для наочності вказано усереднений рівень *SNNR* (близько 9 дБмВт), отриманий при відсутності ПЛ.

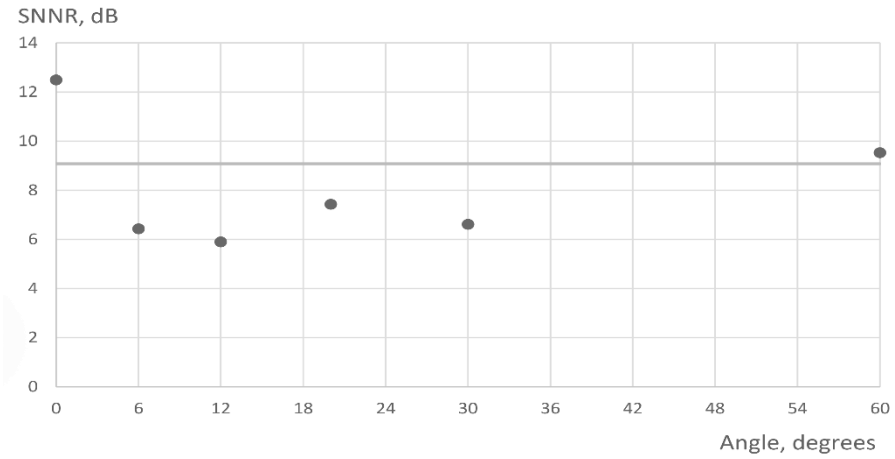


Рис. 3.36. Розподіл *SNNR* за кутовими напрямками

Крім того, оцінювалася (у відсотках) частка пакетів, отриманих з помилками у відповідних кутових напрямках за всі сеанси, в яких використовувалася ПЛ. Ця залежність по кутах показана на рис. 3.37.

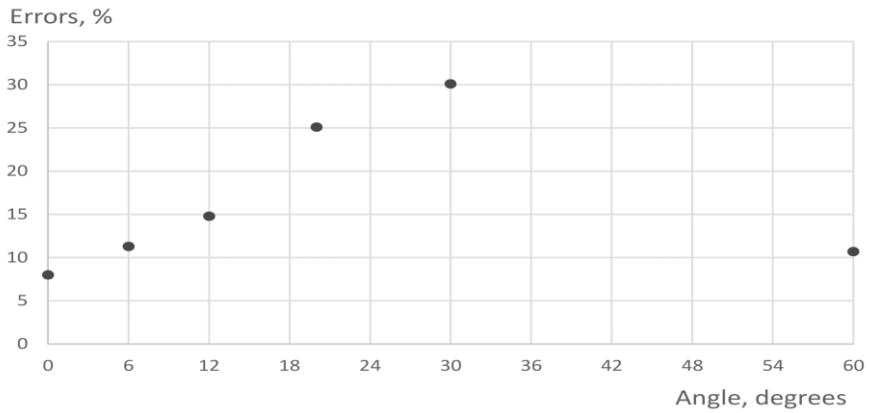


Рис. 3.37. Розподіл помилок за кутовими напрямками

На рис. 3.38 приведено ДС для антенної системи з точкового випромінювача і ПЛ без урахування впливу елементів перевідбивання, яка була отримана в програмному середовищі для моделювання антен Mmana-Gal basic (версії 3.0.0.15). Сірий сектор ДС вказує на кут в 6°, отриманий в результаті експерименту.

В межах кута у 30° існує другий мінімум ДС. Саме у цьому напрямку експериментальні дані вказують на низький рівень *SNNR*. В напрямку 60°, де ДС системи має максимум чотири пелюстки, спостерігається близькість величини *SNNR* при відсутності, так і при наявності ПЛ.

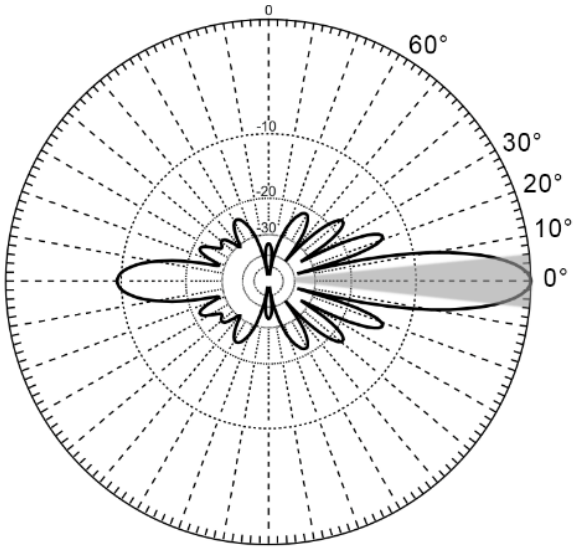


Рис. 3.38. Теоретична ДС

Аналіз отриманих даних показує, що в межах головної пелюстки ДС ПЛ *SNNR* вище, ніж в області бічних пелюсток. Такий же висновок можна зробити й за результатами порівняння роботи частотного діапазону 2,4–2,5 ГГц у випадку відсутності ПЛ.

У зоні кутів понад 60° відношення суми сигналу *S* і шуму *N* до шуму за результатами натурного експерименту виявилося дуже схожим як для випадку використання ПЛ, так і без неї (рис. 3.36). Відповідно, кількість пакетів з помилками

є мініальною в межах головної пелюстки і, навпаки, максимальною в зоні ближніх бічних пелюсток.

Сектор «затінення» також оцінювався за рівнем *SNNR* при наявності ПЛ та без неї (рис. 3.36). Цей сектор починається приблизно з 6° щодо осі ПЛ і закінчується на 30°. Початок сектора для даної ПЛ (в припущенні рівномірного амплітудного розподілу) відповідає спадаючій зоні головної пелюстки ДС [22]. Права межа сектора відповідає напівширині кутового розміру ПЛ щодо фокусу. За межами цього кутового сектора кількість виявлених помилок в пакетах практично однаково як для випадку використання ПЛ, так і без неї. Якщо в секторі «затінення» користувачів немає, то ПЛ можна розташовувати близько до ТБД. В іншому випадку ПЛ рекомендується доповнювати обладнання користувача. Однак при цьому складніше витримати вимоги по взаємному розташуванню приймального обладнання абонента і ПЛ, а також їх орієнтації щодо ТБД [24].

3.4.2. Перевірка конструктивних і поляризаційних властивостей багатопроменевих систем на цілісність інформації та її доступність

Виходячи з розрахунку у пункті 2.4.2, на рис. 3.39 наведено графіки зміщення максимуму ДС від нормалі, а на рис. 3.40 – максимум увігнутості ФР в залежності від фокусної відстані ПЛ і коефіцієнта заломлення.

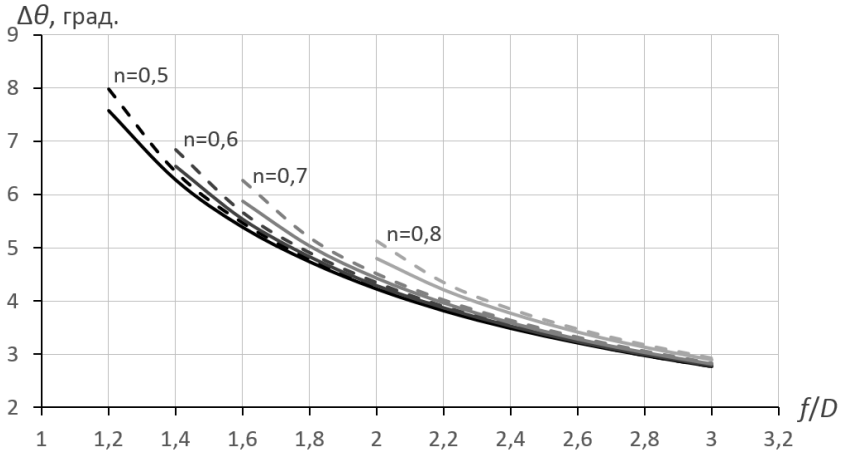


Рис. 3.39. Зсув максимуму ДС від нормалі

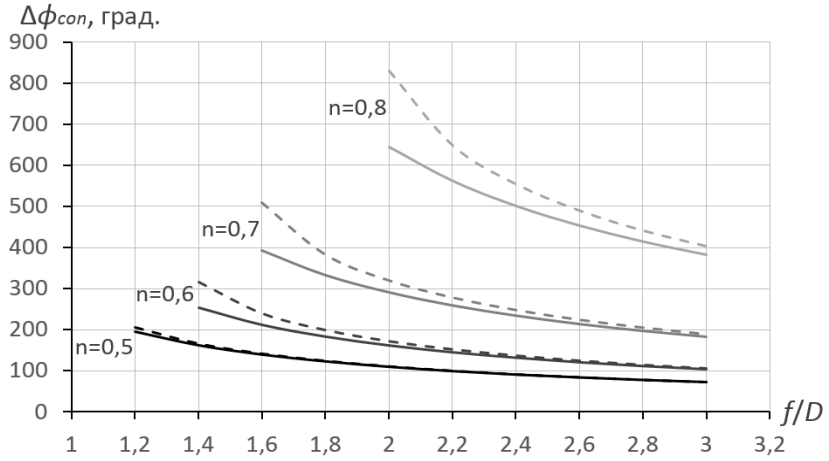


Рис. 3.40. Максимум увігнутості ФР

З графіків (рис. 3.40) випливає, що із збільшенням відношення *f/D* зменшуються кутові зсуви максимумів ДС, тобто зростає рівень сигналів, прийнятих абонентом від кожної антени ТБД (абонент знаходиться на лінії, що збігається з віссю ПЛ). Зменшенню кутових зсувів ДС також сприяє зменшення коефіцієнта заломлення. Особливо це відчутно при малих значеннях *f/D*. Така закономірність зберігається і для ПЛ з усередненим профілем. При цьому як відхилення ДС, так і увігнутість ФР для ПЛ з усередненим профілем мають великі значення. Це вказує на недоцільність вибору усередненого профілю.

При $f/D = 1{,}2$ відхилення ДС не перевищує 8 град. (що є максимальним значенням для рекомендованого діапазону коефіцієнта заломлення ПЛ $0{,}5 \le n \le 0{,}7$). Для ПЛ з $D = 7a$ ширина ДС може складати близько 20 град. У такому (гіршому) випадку зазначене зсув максимуму ДС призведе до зниження коефіцієнта підсилення (КП) в рівносигнальному напрямку (у місці розташування абонента) менш, ніж на 3 дБ. При $f/D = 2$ відхилення не перевищує 5 град., що призведе до зниження КП не більше, ніж на 2 дБ. Якщо абонент знаходиться на деякому відхилення від осі ПЛ, то він буде в кращому ступені приймати сигнал від одного випромінювача. При цьому кутове відхилення його місця розташування від осі ПЛ не повинно перевищувати величини відхилення ДС. Така ситуація буде близька до випадку роботи в одному каналі.

Наявність увігнутого ФР, близького до симетричного по відношенню до нахилу ФР, призводить до звуження головної пелюстки ДС. Графіки (рис. 3.40) показують, що у всьому діапазоні умов як по *n*, так і по *f/D* зазначена увігнутість має глибину більше $\pi/8$, тобто знехтувати нею не можна. Лише при $n = 0{,}5$ і $f/D = 3$ увігнутість становить не більше 90 град., що несуттєво звужує ДС. В якості міри

подолання зазначеного недоліку профіль ПЛ бажано робити більш плоским (глибину ПЛ зменшувати в порівнянні з класичною).

Для поліпшення діапазонних властивостей ПЛ доцільно її зонування. Це, у свою чергу, може компенсувати увігнутість ФР. Останнє вимагає подальшого детального опрацювання [25]. Для цього необхідна розробка нової, набірної ПЛ з окремих елементів та її опромінювання за допомогою двох з трьох антен промислової ТБД Asus RT-N16 (2×3:2 MIMO), які вийняті з корпусу і додатково рознесені на відстань 2*a*. При цьому ТБД має бути попередньо модифікована. До неї має бути доданий внутрішній жорсткий накопичувач, система охолодження та інші незначні модифікації, а стандартна прошивка замінена на DD-WRT K2.6 Big Generic (ревізія 14896). В якості приймального обладнання доцільним є використання мережевої карти на основі безпроводового контролеру Atheros AR9287 (2×2:2 MIMO), а в ролі датчиків поля – Popolu Wixel (на мікроконтролері TI CC2511F32). Дані будуть оброблятися за допомогою спеціального ПЗ MDRV, яке збирає дані з датчиків і в режимі реального часу відображає результат у зведеній формі.

Таким чином, наявність, наприклад, двох випромінювачів в системах MIMO призводить до складнощів в частині застосування ПЛ для поліпшення доступу віддаленого абоненту.

В якості рекомендованого заходу, що сприятиме досягненню позитивного ефекту від застосування ПЛ в системі MIMO, слід вважати збільшення відношення *f/D*. Це призведе до зменшення відхилення ДС від нормалі і зменшення угнутості ФР. Зі збільшенням фокусної відстані профіль ПЛ стає ближче до плоского, що, як результат, полегшить конструктивне виконання такої ПЛ та в подальшому її використання. Крім того, збільшення *f/D* сприятиме зменшенню сектору затінення інших користувачів, що надасть доступ більшому числу абонентів. Але при цьому користувачі, що знаходяться в області бічних пелюсток ПЛ, будучи формально поза області тіні, можуть опинитися в ситуації, коли сигнал буде приходити до них по двох шляхах: прямим і від бічної пелюстки ПЛ. Тобто, буде мати місце двопроменевий прийом, який обумовлений саме наявністю ПЛ. Особливо це відчуватиметься у приміщеннях і на місцевості, де присутні так чи інакше відображатимуть площини, що, в свою чергу, певною мірою ускладнюватиме інтерференційну картину [26,27].

В ході експериментальних досліджень було перевірено декілька, на наш погляд, характерних ситуацій, в яких розглядалися різні варіанти застосування антен

з досить вираженою поляризацією, а саме несиметричних вібраторів та визначався вплив поляризації на рівні сигналів приймальних і передавальних у двох типах приміщень:

по-перше, у порівняно однорідних та малонасичених перевипромінюючими елементами приміщеннях, у яких, крім того, присутній невисокий рівень сторонніх випромінювань у робочому діапазоні;

по-друге, у неоднорідних приміщеннях, з великою кількістю металевих предметів і конструкцій (приладів, корпусів, устаткування, елементів несучих конструкцій, стінових і стельових покриттів тощо).

За результатами експерименту отримано графік відношення інформаційної швидкості передавання даних до пропускної здатності безперервного каналу, показаний на рис. 3.41. З графіку видно, що суттєве збільшення інформаційної швидкості проявляється при повороті антен на π/4.

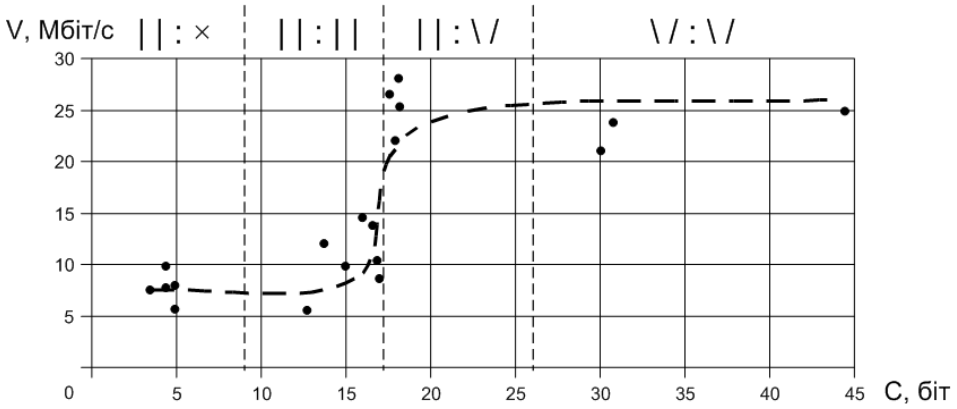


Рис. 3.41. Відношення інформаційної швидкості до пропускної здатності

В експерименті ТБД знаходилися у прямій видимості і помилки в каналі зникали вже при підключенні хоча б по одній антені з кожного боку, забезпечуючи при цьому передавання на мінімальній швидкості.

На рис. 3.42 показане відношення кількості помилок від пропускної здатності безперервного каналу. Як видно, підвищення інформаційної швидкості на графіку пояснюється передусім збільшенням розмірності кодового сузір’я і зменшенням надлишковості кодів згортки, що обумовлено зростанням відношення потужності сигналу до потужності шуму у наслідок наявності поляризаційного рознесення антен, яке дозволило приймати хвилі при їх різній поляризації [28,29].

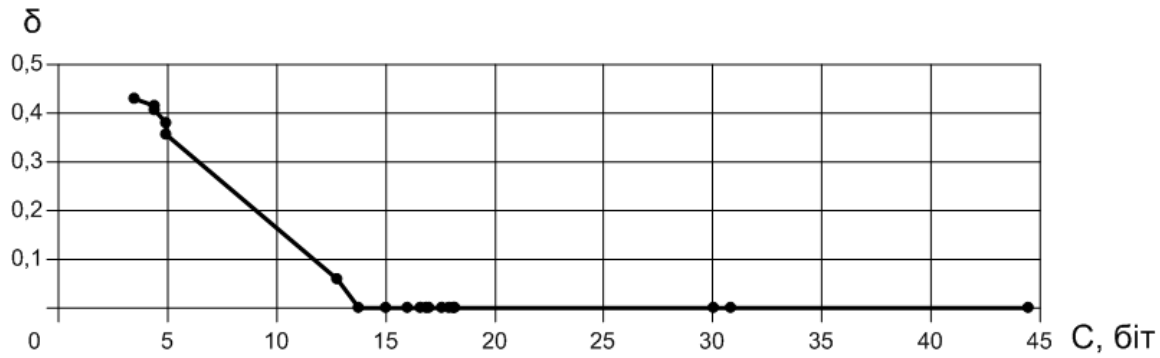


Рис. 3.42. Відношення кількості помилок до пропускної здатності

Висновки до третього розділу

Подальше зростання кількості безпроводових мереж і потужності передавачів може призвести до різкого зростання рівня перешкод, особливо в густонаселених районах. Частковим вирішенням проблеми накладення частот є розширення діапазонів загального користування на державному рівні, а також впровадження нових методів стиснення і кодування інформації у вже існуючому діапазоні. При цьому кількість одночасно працюючих каналів, які не пересікаються, може бути не більше трьох. І хоча загальновідомо, що найменший вплив один на одного надають найбільш віддалені канали, наприклад, 1–7–13 (або хоча б не пересічні, наприклад, 1–6–11, якщо обладнання підтримує тільки 11 каналів), проте, як показало дослідження, найменший вплив один на одного надали канали, що відстають один від одного на 3–4 канали, замість 5–6. Цей результат означає, що рекомендовану кількість каналів можна збільшити, довівши до 4 каналів: 1–5–8–13.

В розділі представлено результати проектування і виготовлення аналізаторів спектру на готових компонентах (мікросхеми-трансивери для стандарту IEEE 802.15.4/ZigBee). Детально описано процес проектування і виготовлення друкованих плат, збір приладів і програмування мікроконтролерів. Проведено тестування і внесення вдосконалень у існуючі прилади. При розводці плат виявлено залежність якості роботи приладу від якості його збірки, наявності електромагнітного екрану і типу антени. Для аналізу даних, зібраних с різних аналізаторів спектру в роботі використано як стороннє ПЗ, так і розроблене на кафедрі інформаційної та кібернетичної безпеки Київського університету імені Бориса Грінченка [30].

Отримані результати вказують на те, що існує можливість підвищення енергетичних характеристик та інформаційної пропускної здатності систем безпроводового зв’язку. Це покращення може бути досягнуто порівняно простим методом з використанням автономної приставки, в першу чергу, для неспрямованої антени

користувача (а в деяких випадках і ТБД) у вигляді ПЛ та розширення її частотного діапазону, а також ортогоналізації приймальних і передавальних антен та їх поляризаційного рознесення. Це дозволить збільшити потужність електромагнітної хвилі в точці прийому в середньому на 5–7 дБ, а пропускну здатність – на 4%, а також підвищити доступність інформації в системах безпроводового доступу, що експериментально проявляється у збільшенні дальності зв'язку при його фіксованій якості в 1,8–2,2 рази.

Як результат, розроблені технології можуть бути інтегрованими в програмний комплекс ситуаційного центру, який консолідує в собі роботу з різними низькобюджетними моделями аналізаторів спектру заданого частотного діапазону.

Список використаних джерел у третьому розділі

1. Зайка В. А., Абрамцев А. С. Технологии беспроводных локальных сетей (Wi-Fi). Физический уровень. *Электроника инфо*. 2006. №7 (31). С. 50–54.

2. D-Link DIR-320 A1/A2. 2019. URL: https://dd-wrt.com/support/router-database/?model=DIR-320_A1/A2 (дата звернення: 29.03.2019).

3. D-Link DIR-300(Bx)/DIR-600(Bx). 2019. URL: https://openwrt.org/toh/d-link/dir-300revb (дата звернення: 29.03.2019).

4. ZCN-1523H-2-8. Skyport ZCN-1523H-2-8 2.4Ghz Outdoor CPE. Data Sheet, 2011. 4 p. (Zcomax Technologies).

5. Беспроводная технология Ultra WideBand. 2005. URL: https://compress.ru/article.aspx?id=10841 (дата звернення: 29.03.2019).

6. Баронов С. Б. Расчет погрешностей при обработке результатов измерений. 2013. URL: http://www.students.chemport.ru/materials/deviations.htm (дата звернення: 29.03.2019).

7. Широкополосные беспроводные сети передачи информации / Вишневський В. М. та ін. Москва, 2005. 592 с.

8. Немного об устранении радиопомех. 2015. URL: https://web.archive.org/web/20140918030854/http://connect-portal.info/radio_ystr_pomeh.html (дата звернення: 29.03.2019).

9. Соколов В. Ю. Електромагнітна сумісність транспортних мереж і мереж доступу технологій IEEE 802.11g і 802.15.1. *Зв'язок*. 2011. №2 (94). С. 67–70.

10. Armitage S. Low-Cost 2.4-GHz Spectrum Analyzer. *Circuit Cellar*. 2006. Iss. 189., P. 18–22.

11. Graham G. 2.4 GHz WiFi & ISM Band Scanner. 2007 URL: http://geoffg.net/ISM_Scanner.html (дата звернення: 29.03.2019).

12. Cypress Perform CYRF6935 : Datasheet / Cypress Semiconductor. 2010. 36 p.

13. Соколов В. Ю. Порівняння можливих підходів щодо розробки низькобюджетних аналізаторів спектру для сенсорних мереж діапазону 2,4–2,5 ГГц. *Кібербезпека: освіта, наука, техніка*. 2018. №2. С. 31–46. DOI: 10.28925/2663-4023.2018.2.3146.

14. Buryachok V., Gulak G., Sokolov V. Building Secure Communication Channels based on the IEEE 802.15.4 Standard. *Actual Problems of Science and Technology*, in I Int. Sc.-Tech. Conf., 22 Oct. 2015. Kyiv : ESIIS SUT, 2015. P. 263.

15. Buryachok V., Gulak G., Sokolov V. Miniaturization of Wireless Monitoring Systems 2.4–2.5 GHz Band. *Actual Problems of Science and Technology*, in II Int. Sc.-Tech. Conf., 20 Dec. 2015. Kyiv : ESIIS SUT, 2015. P. 41.

16. Buryachok V., Gulak G., Sokolov V. Construction of the Spectrum Analyzers Network 2.4–2.5 GHz Band. *Actual Problems of Science and Technology*, in III Int. Sc.-Tech. Conf., 19 May 2016. Kyiv : ESIIS SUT, 2016. P. 32.

17. Buriachok V., Sokolov V. Increase the Speed of Spectrum Analyzers based on Atmel Atmega328 and ARM Cortex-M3 RISC Processors. *Bezpieczeństwo w Cyberprzestrzeni Społeczna Przestrzeń Internetu w Kontekście Wartości i Zagrożeń*. Kharkiv : NU-CPU, 2019. P. 283–297. ISBN: 978-83-63680-28-2.

18. Bogachuk I., Sokolov V., Buriachok V., Korzhenko O. Development and Operation Analysis of Spectrum Monitoring Subsystem 2.4–2.5 GHz Range. *Data-Centric Business and Applications – Evolvements in Business Information Processing and Management (DCBA)*. Springer. 2019. 32 p. (Препринт).

19. Соколов В. Ю. Порівняння математичних і функціональних моделей широкосмугових сигналів з ортогональним частотним розділенням. *Управління розвитком складних систем*. 2010. №4. С. 109–113.

20. Марков Г. Т., Петров Б. М., Грудинская Г. П. Электродинамика и распространение радиоволн : Учебное пособие для вузов. Москва, 1979. 376 с.

21. Соколов В. Ю., Астапеня В. М. Вплив прискорюючої лінзи на якість каналу зв’язку у безпроводових мережах стандарту IEEE 802.11b. *Сучасні інформаційно-комунікаційні технології (COMINFO’2011)* : матеріали VII Міжнар. наук.-техн. конф., 10–14 жовтня 2011 р. Київ : ДУТ, 2011. С. 212–215.

22. Астапеня В. М., Соколов В. Ю. Використання прискорювальної лінзи для підвищення ефективності та завадозахищеності мереж IEEE 802.11b. *Зв'язок*. 2012. №2 (98). С. 33–37.

23. Astapenya V. M., Sokolov V. Yu. Research Results of the Impact of Spatial and Polarization Value of the Antennas on Network Capacity of Wireless Channels Standard IEEE 802.11. *Antenna Theory and Techniques (ICATT'2013)* : in IX Int. Conf., 16–20 Sept. 2013. Odessa : IEEE, 2013. P. 172–174. DOI: 10.1109/icatt.2013.6650715.

24. Astapenya V. M., Sokolov V. Yu. Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane. *Antenna Theory and Techniques (ICATT'2017)* : in XI Int. Conf., 24–27 May 2017. Kyiv : IEEE, 2017. P. 389–391. DOI: 10.1109/icatt.2017.7972671.

25. Кюн Р. Микроволновые антенны / под ред. М. П. Долуханова. Ленинград, 1967. 520 с.

26. Астапеня В. М., Соколов В. Ю. Підвищення доступності інформації у бездротових системах на основі використання прискорюючої металопластинчастої лінзи. *Сучасні інформаційно-комунікаційні технології (COMINFO'2015)* : матеріали IX Міжнар. наук.-техн. конф., 17–20 лист. 2015 р. Київ : ДУТ, 2015. С. 67–71.

27. Бурячок В. Л., Астапеня В. М., Соколов В. Ю. Способы повышения доступности информации в беспроводных системах стандарта IEEE 802.11 с MIMO. *Сучасний захист інформації*. 2016. №2. С. 60–68.

28. Астапеня В. М., Соколов В. Ю. Підвищення пропускної здатності безпроводових каналів зв'язку на основі поляризаційних ефектів у мережах IEEE 802.11. *Зв'язок*. 2012. №3 (99). С. 36–41.

29. Астапеня В. М., Соколов В. Ю. Використання поляризації радіохвиль для підвищення пропускної здатності та завадостійкості безпроводових каналів зв'язку мереж стандарту IEEE 802.11. *Сучасні інформаційно-комунікаційні технології (COMINFO'2012)* : матеріали VIII Міжнар. наук.-техн. конф., 1–5 жовтня 2012 р. Київ : ДУТ, 2012. С. 230–232.

30. Buriachok V., Sokolov V. Implementation of Active Learning in the Master's Program on Cybersecurity. *Computer Science, Engineering and Education Applications (ICCSEEA'2019)* : in II International Conference, 26,27 Jan. 2019. Kiev : Springer, 2019. P. 610–624. DOI: 10.1007/978-3-030-16621-2_57.

Розділ 4

ПРАКТИЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ БЕЗПРОВОДОВИХ ТЕХНОЛОГІЙ

На рівні персональних радіо мереж на даний момент найактивніше розвивається інтернет речей (Internet of things, IoT). Він щільно пов'язаний з хмарними технологіями і є надзвичайно вразливим до проявів стороннього кібернетичного впливу. Враховуючи, що в IoT використовуються, як правило, дані від зовнішніх сервісів всіх трьох моделей хмарних сервісів: ПЗ (Software-as-a-Service, SaaS), платформи (Platform-as-a-Service, PaaS) та інфраструктури (Infrastructure-as-a-Service, IaaS) як сервісів, – кількість вразливостей (див. рис. 4.1) інфраструктури інтернету речей зростає експоненційно.

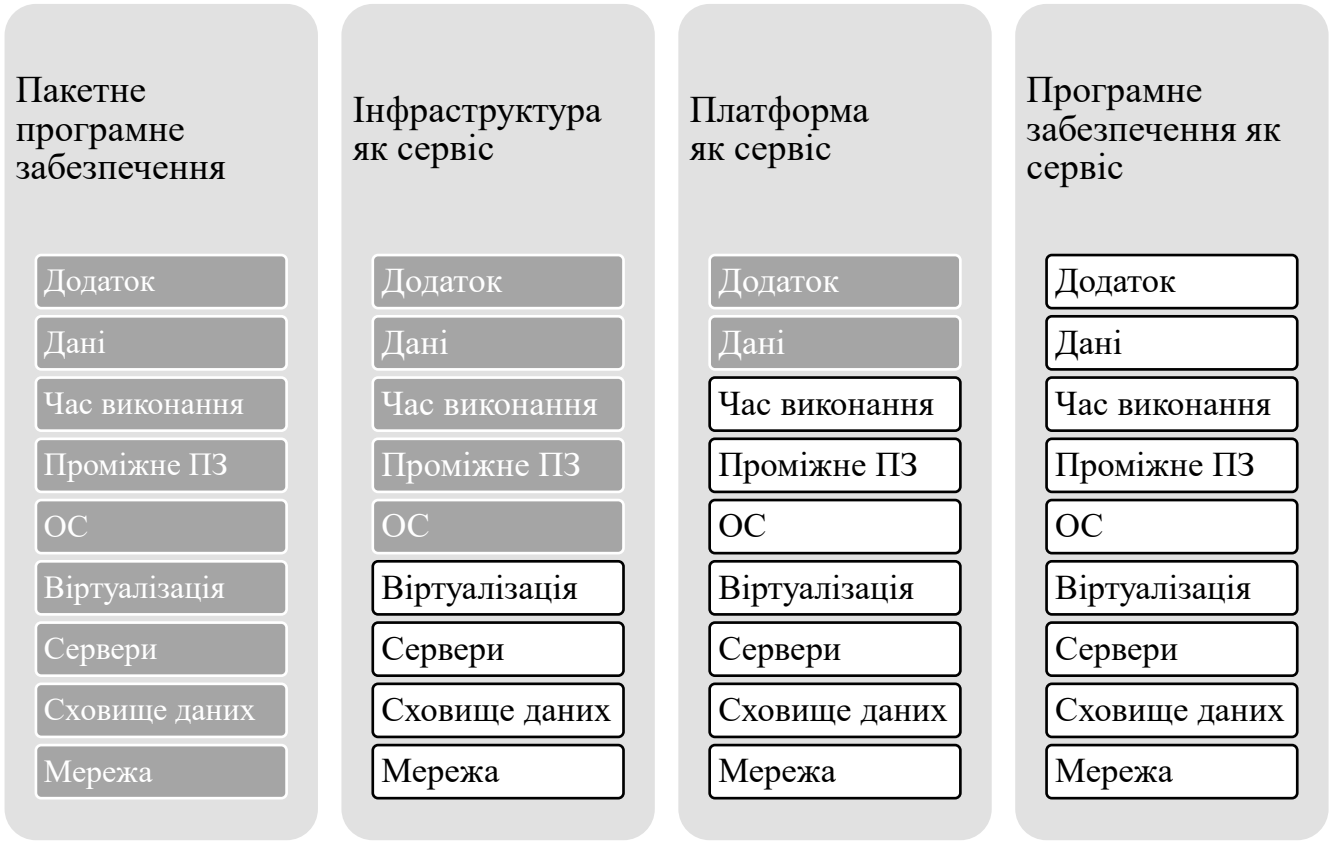
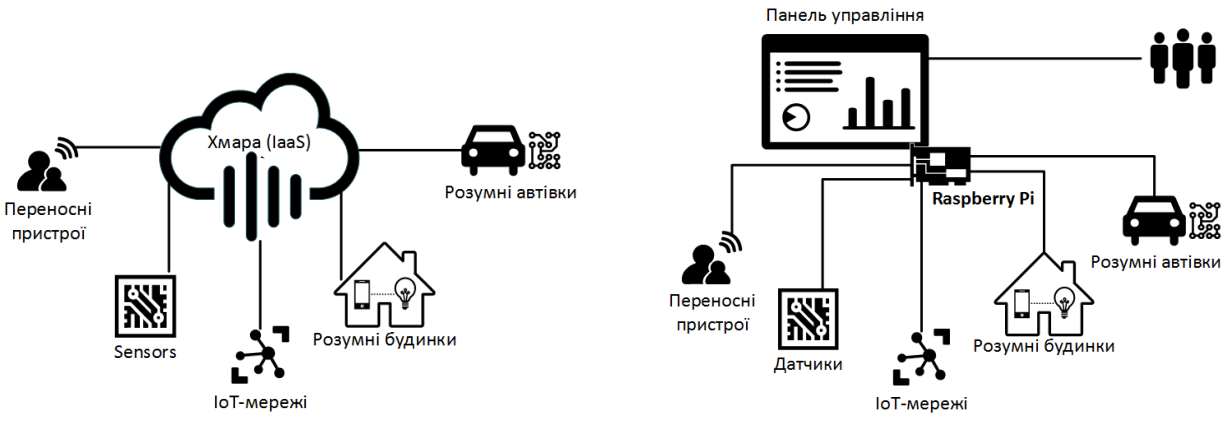


Рис. 4.1. Порівняння хмарних моделей для інтернету речей

Зважаючи на таке, використання хмари як інфраструктури для обробки даних практично неможливе без шифрування відповідних каналів передачі даних. Вирішити цю проблему можливо, наприклад, за рахунок використання IaaS-сервісів (рис. 4.2а) [1], які на відміну від PaaS блокують незадекларовані інтерфейси у ПЗ.

Але, оскільки здатності та потреби пристроїв, які підключаються до державних та приватних IoT-систем постійно збільшуються, змусити їх безпосередньо спілкуватися з системами доволі часто є неможливим. Це пояснюється здебільшого тим, що деякі датчики та контролери не підтримують енергоємні протоколи, такі як Wi-Fi або Bluetooth; деякі пристрої об'єднують дані так, що вони є переважними та неоціненними у незаповненому вигляді, тощо.

Разом з цим, проблему захисту каналів передачі даних від датчиків до хмари можна вирішити, як це показано на рис. 4.2б, й за рахунок використання IoT-шлюзу.



а б

Рис. 4.2. Схеми IoT-системи:
а – класична; б – з шлюзом і хмарною інфраструктурою

Шлюз IoT виконує кілька критичних функцій від перекладних протоколів до шифрування, обробки, керування, фільтрації даних. Його відмінними якостями є:

висока масштабованість (шлюз IoT здатен приймати інтелектуальні дані з центрів обробки даних або хмар і натискати на поле або краю мережі);

вплив на вартість кінцевих пристроїв (шлюз IoT нівелює потреби кінцевих пристроїв у високих обчислювальних потужностях, пам'яті тощо);

швидке виробництво (технологічний цикл виробництва шлюзів IoT максимально зменшений);

скорочення комунікаційних витрат (застосування шлюзів IoT сприяє зменшенню обсягу мережі та трафіку передачі даних);

пом'якшення ризиків (шлюзи IoT можуть ізолювати пристрої та датчики, які не працюють, перш ніж вони спричинять проблеми для виробничої лінії).

Таким чином, постійне збільшення кількості пристроїв і датчиків безпроводових мереж потребує нових підходів до забезпечення безпеки зв'язку між «речами», шлюзом та хмарою передусім в IoT системах, що реалізується, як правило, за допомогою

інфраструктури відкритих ключів. Саме завдяки цьому кожній «речі», що зв'язується, надається ідентичність, тобто пара криптографічних ключів (або цифрового сертифіката), що й дозволяє шифрувати зв'язок [2].

Нижче приведено два приклади атак на безпроводову мережу на кшталт перехоплення безпроводових пакетів (за допомогою радіо з програмним керуванням) та атаки типу «відмова в обслуговуванні» (з відправкою службових деавторизаційних пакетів за допомогою безпроводового ботнета).

4.1. Організація перехоплення безпроводових пакетів BLE і ZigBee

4.1.1. Вибір апаратної платформи SDR

Перехоплення безпроводових пакетів для Bluetooth Low Energy (BLE) і ZigBee на фізичному рівні проведемо, як приклад, за допомогою радіо з програмним керуванням (software-defined radio, SDR). Теоретичні засади для таких SDR-пристроїв [3] разом з групою IEEE P1900.1 розробили фахівці безпроводового інноваційного форуму. SDR забезпечує ефективне та порівняно недороге рішення для багаторежимного, багатоканального та/або багатофункціонального безпроводового пристрою, який може розширити за допомогою оновлення ПЗ (табл. 4.1).

Таблиця 4.1

Основні характеристики радіо з програмним керуванням

Назва	Вартість, дол.	Частотний діапазон, МГц	Розрядність АЦП, біт	Макс. полоса пропускання, МГц	Режими роботи
R820T RTL2832U	10–22	24–1766	8	3,2	тільки RX
Airspy R2	169	24–1750	12	10,0	тільки RX
HackRF One	299	1–6000	8	20,0	напівдуплекс
LimeSDR	299	0,1–3800	12	61,4	напівдуплекс
BladeRF	420–650	300–3800	12	28,0	дуплекс

SDR визначає набір апаратних і програмних технологій, де деякі або всі операційні функції радіо (також називаються обробкою фізичного рівня) реалізуються за допомогою модифікованого ПЗ. Ці пристрої включають в себе програмовані польові матриці (FPGA), цифрові процесори сигналів (DSP), процесори загального призначення (GPP), програмовані системи на чіпі (SoC) або інші програмовані процесори. Використання цих технологій дозволяє додати до існуючих радіосистем нові безпроводові функції та можливості, не вимагаючи нового обладнання.

Одним з найкращих зразків SDR є HackRF One (рис. 4.3), який має потужний набір функцій та широко підтримується різноманітним ПЗ з відкритим вихідним

кодом на більшості стандартних комп'ютерних платформ. Найбільш помітними серед них є широкий діапазон частот і підтримка до 20 млн вимірів на секунду.

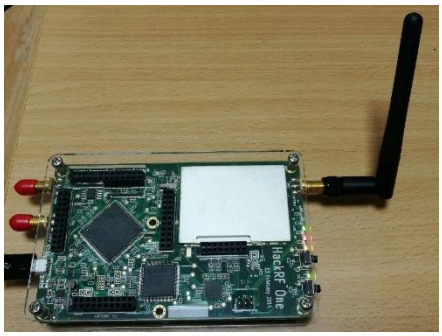


Рис. 4.3. Загальний вигляд використовуваної HackRF One

4.1.2. Огляд інструментів SDR

В даний час існують десятки таких програмних пакетів для роботи з SDR. Розглянемо декілька з них.

SDR# (SDR sharp) є найпопулярнішим безкоштовним ПЗ, сумісним з RTL-SDR, що використовується на даний момент для ОС Windows. Він порівняно простий у використанні в порівнянні з іншими програмами SDR і має просту процедуру налаштування. SDR# має модульну архітектуру і багато додатків від сторонніх розробників (рис. 4.4) [4,5].

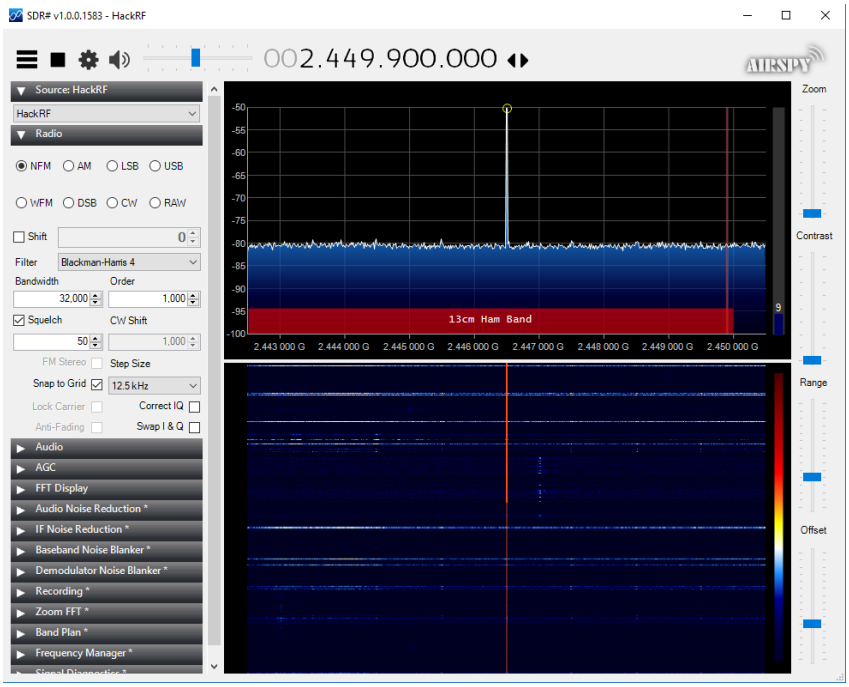


Рис. 4.4. Головне вікно SDR#

GQRX є безкоштовним простим у використанні SDR приймачем, який працює на ОС Linux і Mac. Він схожий на SDR# з точки зору можливостей і простоти

використання. GQRX поставляється зі стандартним спектром FFT і дисплеєм водоспаду і рядом загальних налаштувань фільтра (рис. 4.5).

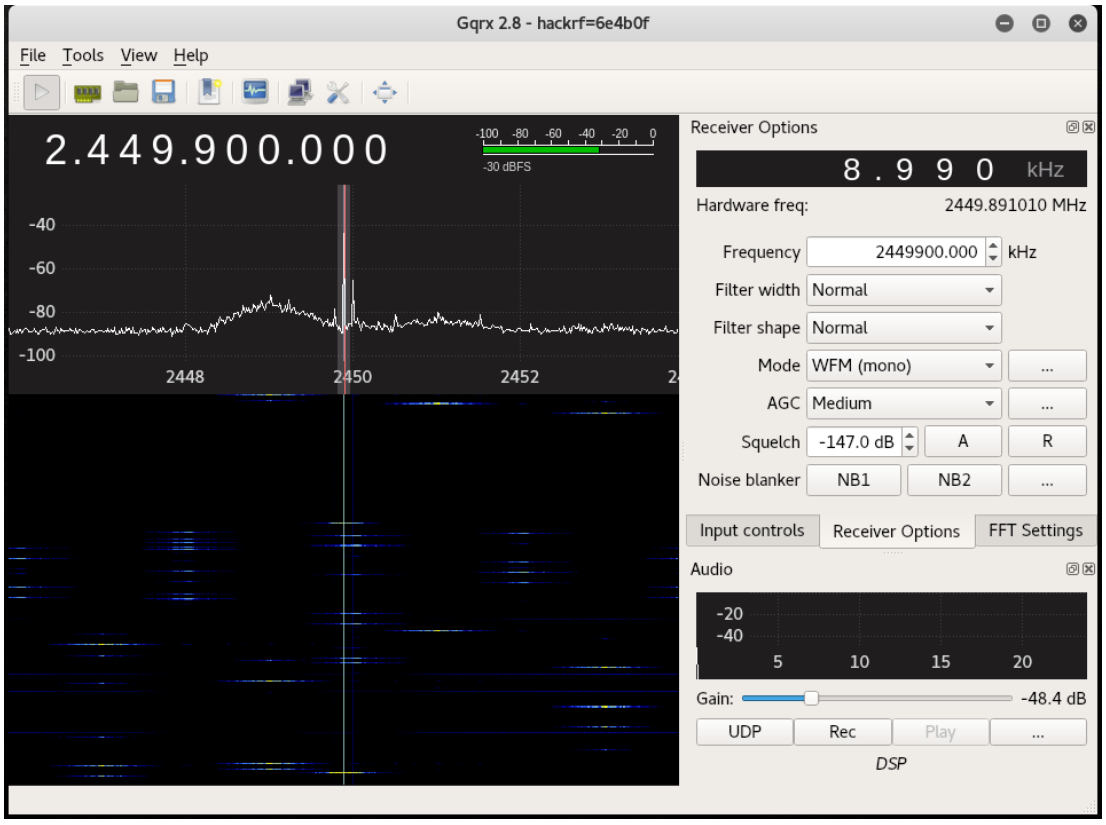


Рис. 4.5. Головне вікно GQRX

GNU Radio виконує всю обробку сигналів. Її можна використовувати для запису додатків для прийому та передачі даних з радіомережею, або для створення повністю заснованих на моделюванні програм. GNU Radio має фільтри, коди каналів, елементи синхронізації, еквалайзери, демодулятори, вокодери, декодери і багато інших типів блоків, які зазвичай знаходяться в системах обробки сигналів. Більш важливо, що він включає в себе спосіб підключення цих блоків і потім керує тим, як передаються дані з одного блоку в інший. Розширення GNU Radio також досить просте; якщо ви знайдете певний блок, який відсутній, його можна швидко створити та додати.

ПЗ для GNU Radio може бути написане або на мові програмування C++, або на мові Python, в той час як критичний шлях обробки сигналів реалізований у C++ за допомогою розширень з плаваючою точкою, якщо такі є. Це дозволяє розробнику реалізовувати радіосистеми високої пропускної здатності в режимі реального часу у простій у використанні середовищі швидкого розробки додатків.

4.1.3. Перехоплення BLE-пакетів

Для захоплення BLE частотного стрибкоподібного зв’язку необхідно пройти кілька кроків, показаних на рис. 4.6.

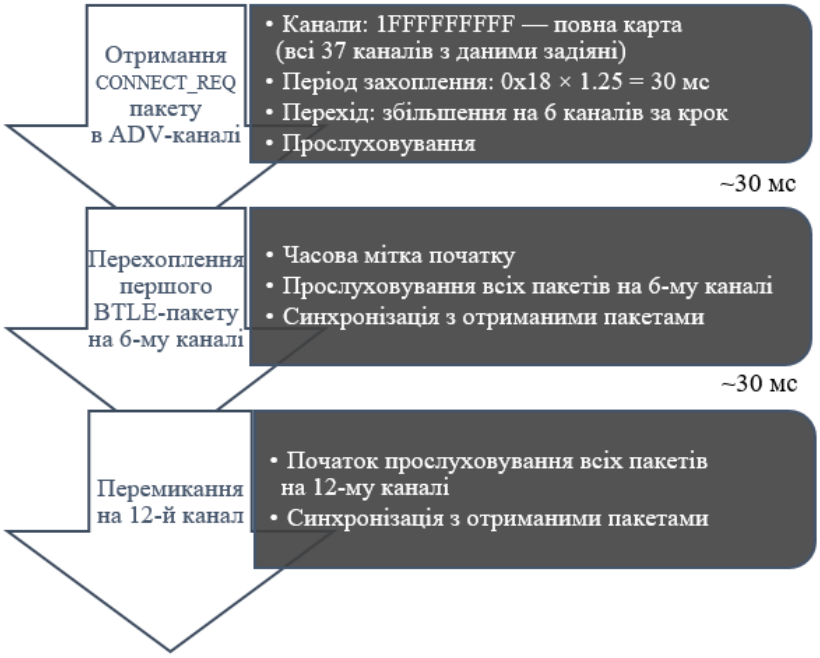


Рис. 4.6. Етапи для стрибкоподібного зв’язку для BLE

Створимо пакет iBeacon (на каналі 37) і передамо його командою ./BLE_rx –g 0. В результаті отримаємо відповідь показаний нижче:

163342us Pkt192 Ch37 AA: 8e89bed6 A DV_PDU_t2: ADV_NONCONN_IND T1 R0 PloadL25 AdvA: 41e0302e6669

Дані: 0303aafe0e16aafe10bb0074616a64696e690a CRC0

BLE є частиною специфікації Bluetooth (версії 4.0), яка була випущена ще в 2010 році. Вона виникла в 2006 році в Nokia як Wibree, але з тих пір була об’єднана в Bluetooth. Це інший набір протоколів, ніж «класичний» Bluetooth, а пристрої не є зворотно-сумісними. Отже, в ході проведення натурних експериментів можна скористатися трьома типами пристроїв:

Bluetooth (підтримує тільки «класичний» режим);

Bluetooth Smart Ready (підтримує як класичний, так і BLE режим);

Bluetooth Smart (підтримує тільки режим BLE).

Новіші смартфони, ноутбуки, планшети, всі оснащені повним Bluetooth 4.0 і, отже, Smart Ready. З іншого боку, маяки підтримують лише протоколи з низькою енергією (що дозволяє їм працювати на одному акумуляторі протягом тривалого часу) і, отже, реалізують Bluetooth Smart. Старі пристрої, такі як периферійні при-

строї, автомобільні системи та старі телефони, зазвичай підтримують лише класичний протокол Bluetooth.

У центрі уваги в BLE, звичайно, низьке споживання енергії. Наприклад, деякі маяки можуть передавати сигнал протягом 2 років на батареї однієї комірки (батареї, як правило, не замінюються; ви, мабуть, просто заміните маяк, коли вони перестануть працювати). І класичний, і BLE використовують один і той же спектр (2,4000–2,4835 ГГц). Протокол BLE має більш низькі швидкості передачі даних, однак це не призначено для потоку великої кількості даних, а скоріше для виявлення і простого зв'язку. З точки зору дальності, як BLE, так і «класичний» Bluetooth сигнал може досягати до 100 метрів.

BLE-комунікація складається з двох основних частин: анонсу і підключення. Анонс – це механізм одностороннього виявлення. Пристрої можуть передавати пакети даних з інтервалами від 20 до 10 000 мс (чим коротший інтервал, тим менший час роботи акумулятора, але чим швидше буде виявлений пристрій). Пакети можуть мати довжину до 47 байт (рис. 4.7) і складатися з:

преамбула (1 байт);

адреса доступу (4 байти);

рекламний канал PDU (2–39 байтів);

CRC (3 байти).

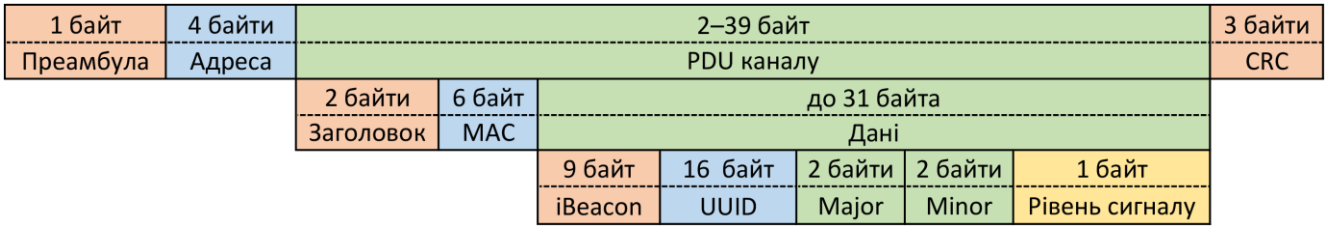


Рис. 4.7. Формат пакетів BLE

Для рекламних каналів зв'язку адреса доступу завжди дорівнює 0×8E89BED6. Для каналів даних він відрізняється для кожного з'єднання.

PDU в свою чергу має свій власний заголовок (2 байти: розмір корисного навантаження і його тип – чи підтримує пристрій з'єднання тощо) і фактичне корисне навантаження (до 37 байт). Нарешті, перші 6 байтів корисного навантаження є MAC-адресою пристрою, і фактична інформація може мати до 31 байт.

Пристрої BLE можуть працювати в нез'ємному для реклами режимі (де вся інформація міститься в рекламі), але вони також можуть дозволяти з'єднання (і зазвичай роблять). Після виявлення пристрою можна встановити з'єднання. Потім можна прочитати послуги, які пропонує пристрій BLE, і для кожної служби свої

характеристики. Кожна характеристика надає деяке значення, яке може бути прочитане, написане або те й інше. Наприклад, інтелектуальний термостат може виставляти одну послугу для отримання поточних показників температури/вологості (як характеристики цієї послуги) і іншої служби і характеристики для встановлення бажаної температури. Однак, оскільки маяки не використовують з'єднання [6].

4.1.4. Перехоплення ZigBee-пакетів

Для перехоплення одного ZigBee-пакета в секунду зі статичними даними (в нашому випадку «FFEEFFEE» на 2,4499 ГГц) доцільно використовувати модуль Pololu Wixel як ZigBee Rx/Tx.

Як згадувалося в стеку протоколу ZigBee, кадр рівня MAC ZigBee складається з заголовка MAC, корисного навантаження MAC і FCS. На діаграмі нижче зображено загальний формат кадру MAC, прийнятий в технології ZigBee на рівні MAC. Ця частина також називається MPDU або блоком даних протоколу MAC.

За допомогою апаратного передавача (а) і приймача (б), реалізованих на моделі Pololu Wixel з OLED (рис. 4.8) можна без перерви надсилати та отримувати пакети з приблизно 7% помилок.

а б

Рис. 4.8. Апаратний передавач (а) і приймач (б) на моделі Pololu Wixel з OLED

Після кешування цих сигналів за допомогою HackRF One їх можна відправити повторно, як клони пакетів. Для цього можна використати просту діаграму, як це показано на схемі (рис. 4.9) в GNU Radio для кешування сигналів і збереження їх у двійковому файлі.

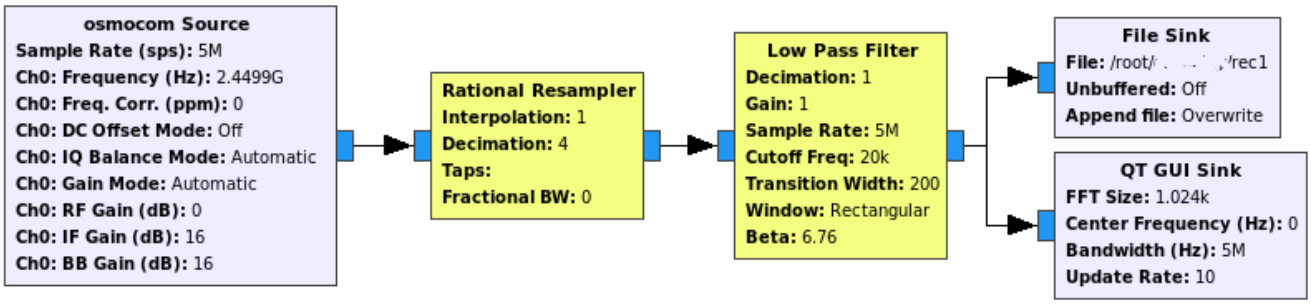


Рис. 4.9. Схема радіоприймача

Схема приймача, застосування якого дозволить відправити точно такі ж сигнали, закешовані в двійковому файлі, показана на рис. 4.10.

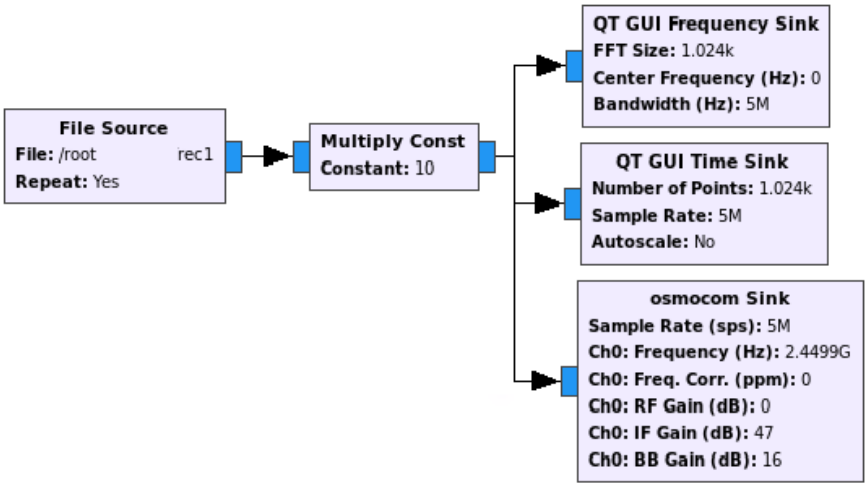


Рис. 4.10. Схема радіопередавача

Результатом експерименту стало отримання більше 50% сигналів без помилок. Це означає, що з 7% завідомо втрачених пакетів, після їх перехоплення з HackRF One і відправлення наново – було втрачено 43% більше пакетів.

За результатами експериментів видно, що використання SDR доцільно для проведення експериментів з атаками на проникнення, а також для емуляції приймачів і передавачів для протоколів BLE і ZigBee [7].

4.2. Реалізація атаки «відмова в обслуговуванні» за допомогою ботнета

4.2.1. Принципи організації ботнета

На рис. 4.11 зображена типова схема організації ботнета. Перш за все, зловмисник знаходить вразливі вузли в інтернеті і розгортає на них засоби атаки – агенти. Машини, на яких встановлені агенти називаються ботами. Ці боти запускають прихований канал для зв’язку з сервером команд і управління – обробни-

ком, який контролює зловмисник. Після цього зловмисник поширює атакуючу команду з обробників ботам, інструктуючи ботів про те, кого, коли і як атакувати. Починаючи з заданого часу атаки, боти генерують атакуючий трафік для здійснення атаки [8].

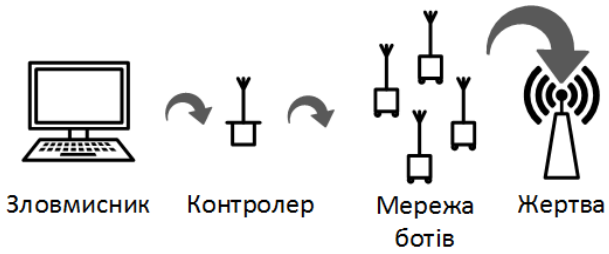


Рис. 4.11. Типова схема структури ботнета

4.2.2. Програмні компоненти і алгоритм роботи ботнета

В програмній частині натурного експерименту із дослідження роботи ботнета доцільно використати ESP8266 SDK та Arduino API для ESP8266, як основні інструменти розробки ПЗ для ESP8266. При цьому SDK дає великий вибір інструментарію, а Arduino API – зручне та безпечне використання цих інструментів.

ESP8266 SDK (software development kits) – сукупність інструментів для розробки додатків IoT, розроблена Espressif Systems. Включає в себе бібліотеку базових функцій для взаємодії з апаратним та програмним забезпеченням ESP8266 та приклади проектів, що можна реалізувати, використовуючи їх. В залежності від того, засновані вони на операційній системі, чи ні, SDK можна класифікувати на два типи: Non-OS SDK та RTOS SDK.

Non-OS SDK не засноване на операційній системі, підтримує AT команди. Використовує таймери та колбеки, як основний засіб виконання різних функцій – вкладених подій, функцій, що викликаються певними умовами. Використовує мережевий інтерфейс espconn; користувачам необхідно розробляти свої програми у відповідності за правилами використання інтерфейсу espconn.

RTOS SDK засноване на FreeRTOS та має відкритий програмний код на Github. FreeRTOS SDK заснований на FreeRTOS, багатозадачній ОС. Ви можете використовувати стандартні інтерфейси для реалізації управління ресурсами, затримки виконання, міжпроцесну передачу взаємодію і синхронізацію та інші рішення, орієнтовані на виконання певних завдань. RTOS SDK надає пакет, який забезпечує інтерфейс BSD Socket API. Користувачі можуть безпосередньо використовувати Socket API для розробки програмних додатків; переносити додатки з інших платформ, що викорис-

товують Socket API на ESP8266, знижуючи витрати на навчання, що виникають через зміну платформи. RTOS SDK включає бібліотеку cJSON, функції якої спрощують обробку JSON пакетів. RTOS сумісний з non-OS SDK в інтерфейсах Wi-Fi та системних інтерфейсах, але не підтримує AT-команди.

Arduino API для ESP8266 була розроблена на основі ESP8266 SDK, використовуючи згоду щодо імен та загальну функціональну концепцію бібліотеки Arduino. Ця API складається з декількох бібліотек, кожна з яких покликана спростити розробку ПЗ для ESP8266, логічно об'єднує низькорівневі функції SDK. Таким чином Arduino API для ESP8266 значно спрощує та прискорює розробку ПЗ для ESP8266, об'єднуючи в собі низькорівневі дії.

Ботнет буде мати структуру типового ботнету, який приведено на рис. 4.11, за одним виключенням – в нашому ботнеті буде всього один обробник, який буде взаємодіяти з усіма ботами.

Суб'єкти, що були задіяні в здійсненні атаки на відмову в обслуговуванні:

обробник – основний елемент бот-мережі, який буде сканувати доступні ТБД та надавати адміністратору можливість вибрати мережу, на яку необхідно здійснювати атаку, а також буде збирати всю необхідну для здійснення атаки інформацію про ТБД та передавати її ботам;

бот – пристрій, що буде здійснювати атаку; після отримання інформації від обробника, він має підготувати кадри деавтентифікації та почати розсилати їх, а також підробні кадри Beacon, щоб при спробі повторно підключитися, клієнт не мав правильної інформації про ТБД;

адміністратор – людина, що керує обробником (роль адміністратора – вибрати мережу, на яку буде здійснено атаку);

клієнт – пристрій, що підключений до ТБД який буде отримувати від ботів підробні кадри деавтентифікації від імені ТБД.

ТБД в процесі роботи ботнету не бере участі [9].

В загальному вигляді алгоритм роботи складається з наступних етапів:

знаходження ТБД у зоні досяжності обробника;

вибір ТБД, на яку буде здійснена атака;

виявлення пристроїв, що підключені до вибраної ТБД;

передача інформації про ТБД та її клієнтів, а також додаткової інформації ботам;

формування ботами кадрів деавтентифікації.

Циклічне відправлення пакетів деавтентифікації та підробних кадрів Beacon.

4.2.3. Апаратні компоненти і алгоритм роботи ботнета

В якості апаратної платформи для ботів доцільно використати Espressif Systems ESP8266 (ESP-01) (див. рис. 4.12).

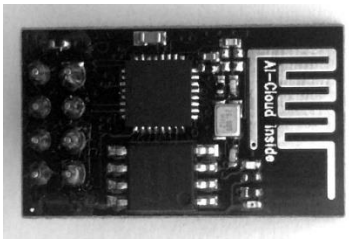


Рис. 4.12. ESP8266 ESP-01

ESP8266 ESP-01 – Wi-Fi модуль, використовується в проектах, де потрібна швидкісна безпроводова передача даних між різними об'єктами проекту по Wi-Fi, наприклад, між контролером і датчиком, який знаходиться на відстані або у важкодоступному місці тощо. Може використовуватися в системах безпеки, системах віддаленого контролю, системах домашньої автоматизації, системи телеметрії. ESP-01 обладнана планарною антеною, дальність прийому/передачі може сягати 400 м. Так, як необхідна для модуля напруга – 3,3В, якщо подати напругу вище, модуль вийде з ладу. Тому, для використання модуля потрібно спочатку підключити лінійний стабілізатор живлення AMS1117 на 3,3 В (див рис. 4.13).

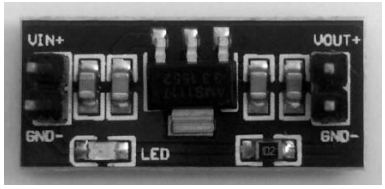


Рис. 4.13. AMS1117 на 3,3В

Схема підключення ESP-01 до AMS1117 показана в табл. 4.2.

Таблиця 4.2

Схема підключення ESP-01 до AMS1117

ESP-01	AMS1117
GND	GND
CH_PD	V_{out}
V_{cc}	V_{out}

В якості обробника була обрана платформа для створення пристроїв IoT на основі Wi-Fi модуля ESP8266 (ESP-12E). NodeMCU (див. рис. 4.14) має інтегровані інтерфейси GPIO, PWM, I^2C, 1-Wire, ADC. Присутній конвертер USB-UART, що дозволяє програмувати плату за допомогою Arduino IDE або Lua.

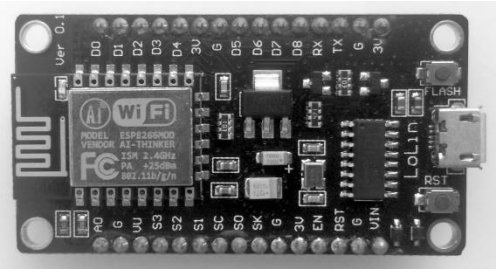


Рис. 4.14. NodeMCU

4.2.4. Реалізація атаки «відмова в обслуговуванні»

Для того, щоб розпочати атаку необхідно підключити обробник та ботів до живлення. Треба зауважити, що можна включити їх заздалегідь, боти після включення будуть очікувати з'єднання з обробником.

З самого початку обробник створює ТБД, до якої підключається адміністратор та боти, які згодом отримають завдання від обробника. Після цього обробник запускає простий веб-сервер, використовуючи який адміністратор зможе вибрати ТБД для атаки. Для кожного запиту, який потрібно буде обробляти, необхідно задати окрему функцію.

Адміністратор може підключитися до ТБД, створеної обробником (за замовченням – esp_ap) та перейти в браузері на 192.168.4.1 [9]. В результаті, адміністратор побачить сторінку, подібну рис. 4.15.

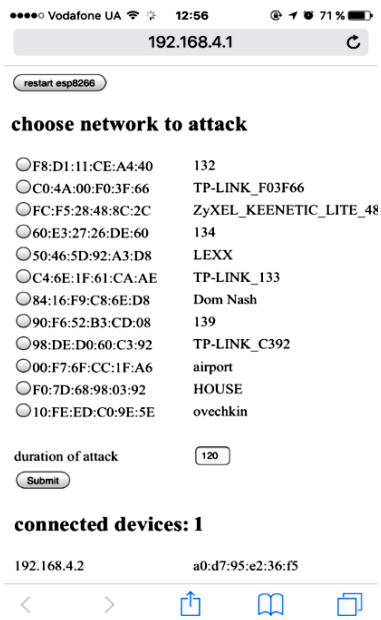


Рис. 4.15. Сторінка для вибору ТБД, на яку буде здійснюватися атака

Для того, щоб знайти клієнтів ТБД, нам необхідно перевести обробник в режим монітору. Зробити це можливо за допомогою функції wifi_promiscuous_enable,

і, хоча в назві написано, що вона активує нерозбірливий режим, вона активує режим монітора. Також, перед тим, як активувати цей режим, нам необхідно задати функцію, що буде викликатися, коли обробник буде захоплювати пакет даних. Вона буде перевіряти отриманий пакет і додасть адресата у список клієнтів тільки у випадку, якщо пакет задовольняє наступні умови: його відправила ТБД, він направлений не в broadcast та не в multicast [10–13].

Коли сканування завершиться, отримуємо список клієнтів у clients_list для формування завдання для ботів. Після того, як обробник сформував список клієнтів ТБД, йому необхідно передати ботам всю інформацію, що необхідна їм, щоб розпочати атаку. Відправка цієї інформації здійснюється використовуючи UDP, так як це найпростіший спосіб передати простий текст між пристроями в одній мережі. Формувати пакет з інформацією про атаку будемо використовуючи шаблон, що показаний на рис. 4.16.

channel len	channel	time len	time	clients num len	clients num	SSID len	SSID	MAC AP	MAC 1	…

Рис. 4.16. Структура UDP пакета, що відправляється ботам

Пакет складається з наступних елементів:

channel – номер каналу, на якому працює ТБД;

channel len – кількість символів в полі «channel»;

time – тривалість атаки в секундах;

time len – кількість символів в полі «time»;

clients num – кількість клієнтів;

clients num len – кількість символів в полі «clients num»;

SSID – назва мережі;

SSID len – кількість символів в SSID;

MAC AP – MAC-адреса ТБД;

MAC – MAC-адреса клієнта.

Весь цей час боти чекали, поки обробник відправить їм пакет з інформацією, необхідною для здійснення атаки. Після отримання цього пакета, кожний бот розбирає його та формує такий самий список клієнтів ТБД, що був у обробника. Далі, на основі цього списку, кожний бот формує новий, в якому вже зберігаються не MAC-адреси, а кадри деавтентифікації, що будуть відправлятись клієнтам від імені ТБД. Формуються кадри деавтентифікації функцією deauth_frame. Також,

разом за кадром деавтентифікації, боти відправляють підробні кадри Beacon, що генеруються з використанням SSID ТБД, а решта інформації генерується випадково. Для формування кадра Beacon використовується функція sendBeacon.

Таким чином, якщо користувач деаутентифікованого пристрою спробує знову підключитися до ТБД, він буде мати невірну інформацію про неї, отже він не зможе підключитися заново. Для перевірки працездатності ботнету було створено тестовий стенд, також на основі NodeMCU та OLED дисплея SSD1306. Даний стенд може працювати в якості повторювача побудови або тестування стабільності безпроводових систем IoT. Він з'єднується з ТБД, параметри якої задані заздалегідь. Якщо з'єднання немає, тестовий стенд просто відображає підключені до нього пристрої в режимі реального часу. Вся інформація виводиться на підключений OLED дисплей, як показано на рис. 4.17.

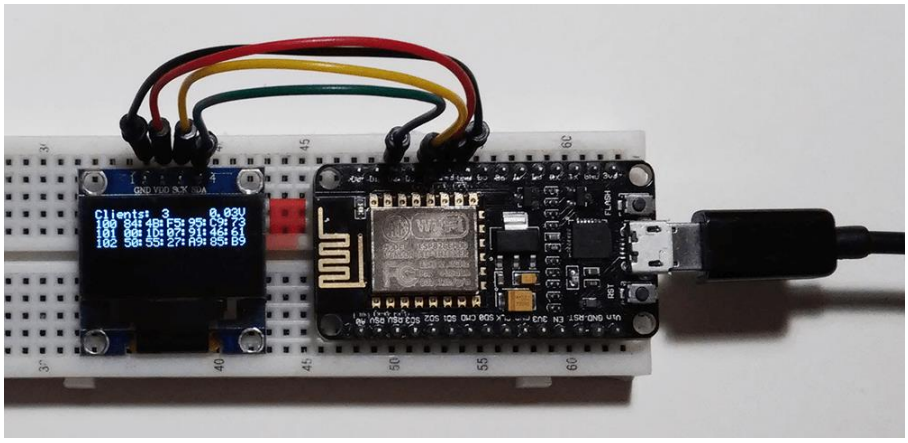


Рис. 4.17. Тестовий стенд контролера ботнета

У сучасних реаліях дуже важливо приділяти особливу увагу комп'ютерній безпеці незалежно від того, чи є ви адміністратором великої корпоративної мережі або ж простим комп'ютерним користувачем. Технології, націлені на викрадення конфіденційних даних або порушення нормальної роботи різноманітних сервісів розвиваються швидше, ніж засоби їх захисту; зловмисники не підкорюються жодним правилам, не дотримуються стандартів, вони домагаються своїх цілей будь-якими способами. Перехід від одиночних атак на відмову в обслуговуванні до розподілених є цьому відмінним доказом: хакери захоплюють чужі пристрої і використовують їх у своїх цілях без згоди власників. Отже, щоб захиститися від такого ворога слідувати базовим правилам захисту комп'ютерних систем недостатньо, необхідно забезпечити комплексний захист своєї системи [14].

4.3. Соціальний інжиніринг у безпроводовій інфраструктурі

Алгоритм застосування соціального інжинірингу до безпроводової інфраструктури поєднує в собі декілька взаємопов'язаних кроків, а саме:

1) формуємо мету впливу на жертву;

2) збираємо інформацію про об'єкт, з метою виявлення найбільш зручних мішеней впливу;

3) створюємо необхідні умови для впливу на об'єкт – атракцію [15].

Детальніше порядок дій соціального інженера при рішенні зазначеної вище задачі приведений на рис. 4.18.

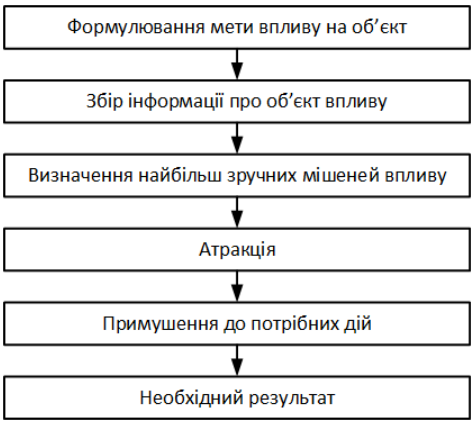


Рис. 4.18. Основна схема впливу в соціального інжинірингу

4.3.1. Апаратно-програмне забезпечення підробної точки доступу

З появою Wi-Fi мереж більшість з них (наприклад, Wi-Fi мережі готелів, аеропортів тощо) для зручності людей залишаються відкритими. Це робить їх гарним місцем для проведення різноманітних атак [16], спрямованих, наприклад, на збирання інформації про потенційних жертв атаки й, навпаки, для виявлення серед великої скупченості людей потенційного терориста тощо.

Натурний експеримент, який було проведено, полягав в тому, щоб створивши відкриту Wi-Fi мережу, збирати дані з жертв за рахунок:

надання можливості бажаючим підключитися до безпроводової мережі;

створення псевдо-інтерфейсу для реєстрації користувача в мережі;

налаштування обладнання до роботи в автономному режимі;

розміщення обладнання в місцях скупчення людей.

Це дозволило, як результат, збирати дані про жертви включаючи як ті, що вони нам нададуть самостійно, так й ті, які ми отримаємо від браузерів жертв, а

саме User-Agent та Cookies для домену на який жертви хотіли б зайти, а також використовувати автентифікацію жерт на даних доменах.

В експерименті було задіяне наступне апаратне забезпечення:

мініатюрний одноплатний енергоефективний комп'ютер на базі архітектури ARM з можливістю підключення пристроїв по інтерфейсу USB;

кабель для подачі живлення типу USB-MicroUSB;

портативний акумулятор (power bank) ємністю в 10 А·год. з USB-інтерфейсом;

безпроводовий мережевий адаптер стандарту 802.11n з інтерфейсом USB та зовнішньою антеною;

подовжувач USB-USB для зручності розташування елементів;

карта пам'яті MicroSDHC 10-го класу об'ємом 16 ГБ.

На рис. 4.19 зображено тестовий стенд у зібраному та увімкненому вигляді.

Рис. 4.19. Зовнішній вигляд тестового стенду

Для реалізації підробної ТБД та фішингового інтерфейсу на ній було визначено наступний інструментарій ПЗ:

hostapd – сервіс Wi-Fi ТБД;

dnsmasq – сервер DHCP та DNS;

lighttpd – веб-сервер;

PHP – мова програмування зі сторони веб-серверу;

стек *HTML*, *CSS* та *JavaScript* для представлення в браузері;

SQLite – база даних для зберігання даних.

В рамках проведення експерименту було вибрано три профілі закладів вищої освіти (ЗВО):

технічний (Державний університет телекомунікацій, м. Київ);

гуманітарний (Київський університет імені Бориса Грінченка, м. Київ);

змішаний (Національний університет «Львівська політехніка», м. Львів).

Відповідно до кожного з них було розроблено окрему фішингову веб-сторінку (на рис. 4.20 показаний приклад сторінки).

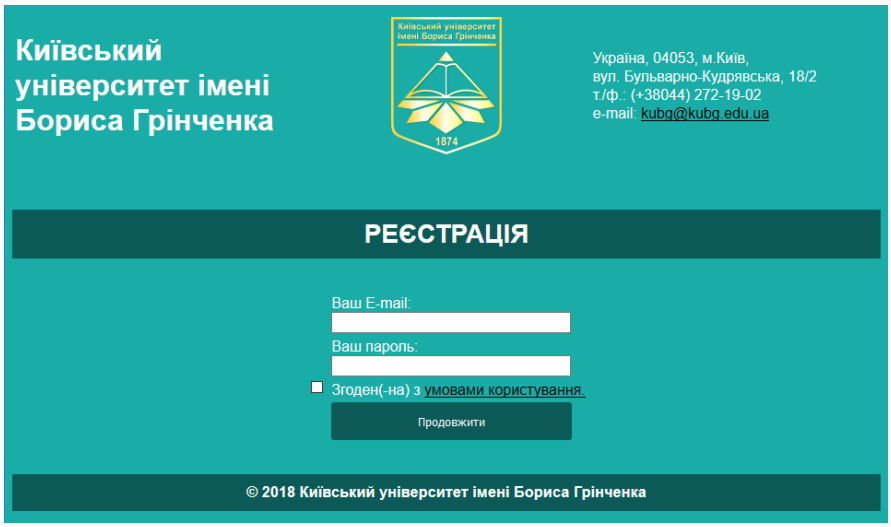


Рис. 4.20. Приклад підробленої веб-сторінки
для Київського університету імені Бориса Грінченка

Для законності даного дослідження було розроблено умови користування сервісом (політику конфіденційності). Погодження з політикою конфіденційності сервісу користувачем перед відправленням даних надає організатору законні підстави на зберігання, обробку та публікацію цих даних. ТБД не мала доступу до інтернету, тому дані збиралися лише підчас першого підключення, дані зберігалися лише у вигляді статистики.

4.3.2. Аналіз результатів емуляції підробної точки доступу

Під час аналізу результатів виникла необхідність в автоматизації процесу обробки інформації та знаходження зв’язків між даними. З цією метою для створення відповідностей між MAC та IP-адресами та діями на веб-сервері, на C#/.NET v. 4.5 було створено відповідне ПЗ.

За результатами експерименту було отримано: технічні дані (операційна система, версія браузеру, виробник мобільного пристрою тощо), дані поведінки (повторне підключення) і дані користувача (електронна пошта, паролі, кукі, запит до сайту-цілі). Найбільшу цінність для дослідження соціального інжинірингу серед

них мають лише дані про поведінку користувачів і персональні дані, якими користувачі погодилися поділитися самі.

Якісним показником доступності інтернету є відсоток повторних підключень. З діаграми (рис. 4.21) видно, що кількість спроб повторного підключення не залежить від профілю вищого навчального закладу, а лише від доступності альтернативних безпроводових мереж.

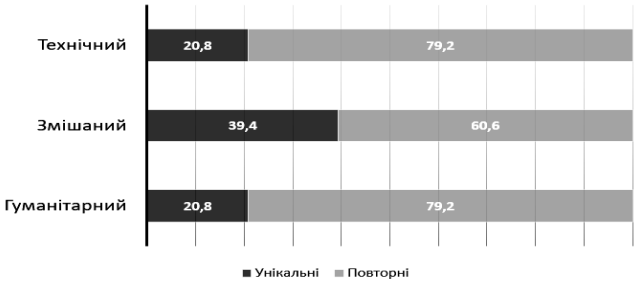


Рис. 4.21. Статистика підключень

Статистика того, з якою легкістю користувачі діляться своєю електронною адресою і навіть паролями, приведена на рис. 4.22. Результати статистики показують збільшення відсотку наданих персональних даних (електронної пошти і пароля) студентами гуманітарного профілю та все ж таки досить високу до невідомих відкритих мереж й серед студентів технічних ЗВО. Це можна пояснити як на наш погляд введенням неіснуючих паролів.

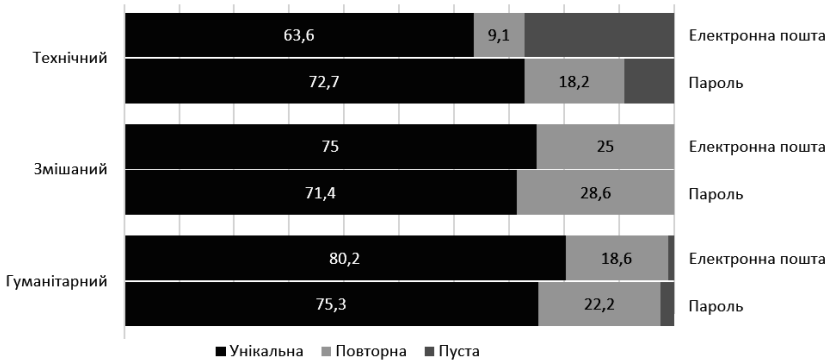


Рис. 4.22. Статистика введення персональних даних (електронної пошти і пароля)

Осторонь стоїть питання відкритості кукі, бо для отримання більшого функціоналу від веб-ресурсів більшість користувачів дозволяють обмінюватися цими даними без окремих запитів на передавання даних. З рис. 4.23 видно, що кількість користувачів, які відкривають доступ до кукі лише частково залежить від профілю ЗВО. Тому питання відкритості кукі скоріш треба розглядати як загальну небезпеку обміну даними, а не тільки як аспект соціального інжинірингу [17,18].

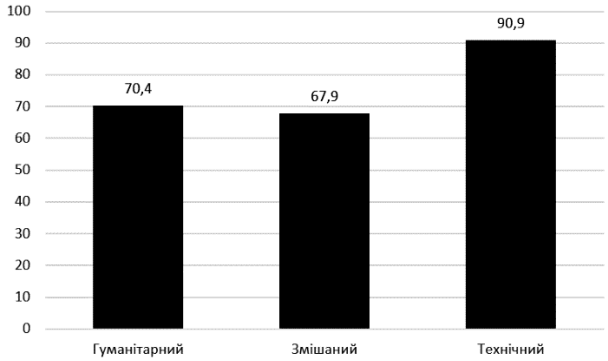


Рис. 4.23. Статистика по дозволу роботи з кукі

4.4. Апробація результатів

Основні положення роботи доповідались та обговорювались:

на VI, VIII і IX Міжнародних науково-технічної конференції студентства і молоді ДУІКТ (м. Київ, 2009, 2011, 2012 рр.);

на VII і VIII Наукових конференціях «Сучасні тенденції розвитку в інфокомунікаціях та освіті» (м. Київ, 2010, 2011 рр.);

на VII, VIII і IX Міжнародних науково-технічних конференціях «Сучасні інформаційно-комунікаційні технології» (COMINFO, м. Київ, 2011, 2012, 2015 рр.);

на IX, X і XI Міжнародних конференціях з теорії і техніки антен (International Conference on Antenna Theory and Techniques, ICATT, м. Одеса, 2013 р., м. Харків, 2015 р., м. Київ, 2017 р.);

на I, II і III Міжнародних науково-технічних конференціях з актуальних проблем науки і техніки (International Scientific-Technical Conference on Actual Problems of Science and Technology, м. Київ, 2015, 2016 рр.);

на IV і V Міжнародних науково-практичних конференціях «Проблеми інфокомунікацій. Наука і техніка» (International Scientific and Practical Conference Problems of Infocommunications. Science and Technology, PIC S&T, м. Харків, 2017 і 2018 рр.);

на II Міжнародній науково-практичній конференції «Міжнародні тенденції в галузі науки і техніки» (International Trends in Science and Technology, стендова доповідь, м. Варшава, 2018 р.);

на презентації програми дисципліни «Методи та засоби забезпечення безпеки безпроводових і мобільних мереж» (м. Карлскрона, 2017 р.);

на конференції країн Європи і СНД «ALERT Cyber Drill» (ALERT cyber drill for Europe and CIS Regions, м. Кишинів, 2017 р.);

на IV Міжнародній науково-практичній конференції «Інноваційні технології в науці» (Innovative Technologies in Science, стендова доповідь, м. Дубай, 2018 р.);

на регіональному семінарі Міжнародного союзу електрозв'язку для країн Європи і СНД «Цифрове майбутнє на основі 4G/5G» (Regional Workshop of the International Telecommunication Union for Europe and CIS Region "Digital Future Powered by 4G/5G", м. Київ, 2018 р.);

на круглому столі «Кібербезпека: освітній аспект» (м. Київ, 2018 р.); на всеукраїнській науково-практичній конференції «Актуальні питання протидії кіберзлочинності та торгівлі людьми» (м. Харків, 2018 р.);

на всеукраїнській науково-практичній конференції здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації» (м. Кропивницький, 2018 р.);

на II міжнародній конференції з комп'ютерних наук, інженерії та освітніх програм (International Conference on Computer Science, Engineering and Education Applications, ICCSEEA2019, м. Київ, 2019 р.).

Практичні результати роботи частково представлені в навчальному посібнику «Інформаційні системи і технології» [19], які були розширені лабораторним практикумом «Безпека безпроводових і мобільних мереж» (на українській мові) [20] і «Wireless and Mobile Security» (на англійській мові) [21] для студентів університету освітнього рівня «магістр» за спеціальністю 125 «Кібербезпека» для курсу дисципліни «Методи та засоби забезпечення безпеки безпроводових і мобільних мереж», який був розроблений в рамках Темпус-проекту №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR «Підготовка наступного покоління експертів з кібербезпеки: нова визнана ЄС магістерська програма» (ENGENSEC), яка фінансувалася Європейським Союзом.

Висновки до четвертого розділу

За результатами проведення натурного експерименту в розділі було розглянуто одну з головних загроз безпеки в інтернеті – відмову в обслуговуванні. З цією метою було проведено всебічний огляд і класифікацію DoS-атак та види контрзаходів, а також розроблено безпроводовий ботнет для реалізації атак на відмову в обслуговуванні, що складався з декількох ботів.

Результати експерименту показали, що кількість ботів можна збільшувати або зменшувати, залишивши лише один. При цьому у випадку, якщо один чи декілька бо-

тів залишаться поза зоною досяжності обробника під час атаки, це не вплине на роботу інших ботів та обробника (вони чекатимуть на підключення). Також результати експерименту показали, що під час атаки можна одну ТБД змінити на іншу й розпочати нову атаку. Однак в цьому випадку, якщо на момент сканування та пошуку ТБД клієнтів вони не ведуть активного обміну даними, наприклад, якщо це смартфон, що знаходиться в режимі очікування, то деякі пристрої можуть залишитися не поміченими обробником. Тести показали, що чим активніший обмін даними ТБД з пристроєм, тим більша ймовірність того, що пристрій буде відключено від ТБД.

В ході натурного експерименту було також виявлено та усунуто низку проблем в конфігурації ПЗ lighttpd. За замовчуванням, даний веб-сервер не використовує логування усіх звернень до нього, на відміну від Apache httpd. Тому такі статистичні дані, як виробники пристроїв, з пристроїв, що надавали дані вебсерверу, виявились недоступними для місця проведення збору інформації в Державному університеті телекомунікацій. Даний факт був взятий до уваги і кількість місць збору інформації було збільшено до трьох. Також під час роботи було вирішено ряд проблем, пов’язаних із логуванням, автоматизацією аналізу та обробки даних, налаштуванням адресації IPv4 мережі, перехоплення усіх запитів від користувачів, та інші.

Як результат, можна констатувати, що обізнаність користувачів як гуманітарних, так і технічних та змішаних напрямків підготовки щодо соціотехнічних атак в цілому недостатня. Це вимагає приділення окремої уваги до розробки методик підвищення рівня обізнаності користувачів та зменшення кількості потенційних атак на об’єкти інформаційної діяльності.

Список використаних джерел у четвертому розділі

1. Akrivopoulou C. M., Garipidis N. Human Rights and the Impact of ICT in the Public Sphere: Participation, Democracy, and Political Autonomy. 2014. 371 p.

2. Taj Dini M., Sokolov V. Yu. Internet of Things Security Problems. *Сучасний захист інформації*. 2017. №1. С. 120–127. DOI: 10.5281/zenodo.2528814. arXiv: 1902.08597.

3. What is Software Defined Radio? 2018. URL: https://wirelessinnovation.org/Introduction_to_SDR (дата звернення: 29.03.2019).

4. Shen D. GNU Radio Installation Guide : Step by Step. 2005. 6 p.

5. IEEE 802.15.4 and ZigBee / Heile B. et al. Lexington, 2015. 34 p.

6. Fähnle M. Software-Defined Radio with GNU Radio and USRP/2 Hardware Frontend: Setup and FM/GSM Applications. Ulm, 2010. 92 p.

7. Taj Dini M., Sokolov V. Yu. Penetration Tests for Bluetooth Low Energy and ZigBee using the Software-Defined Radio. *Сучасний захист інформації*. 2018. №1. С. 82–89. DOI: 10.5281/zenodo.2528810. arXiv: 1902.08595.

8. Singh R., Kaur A., Sethi S. Attacks at Data Link Layer of OSI Model: An Overview. *Int. Journal of Advanced Techn. in Eng. and Sc.* 2015. No. 3. P. 501–509.

9. Sokolov V. AP on ESP8266 Module with I2C OLED SSD1306 and Battery. 2017. URL: https://github.com/Oestoidea/IoT/tree/master/ESP8266_oled_AP_ssd1306 (дата звернення: 29.03.2019).

10. Multi Target De-Auth Attack Implementation for ESP8266 Module. 2016. URL: https://github.com/RandDruid/esp8266-deauth (дата звернення: 29.03.2019).

11. ESP8266 Packet Injection/Sniffer Example. 2016. URL: https://github.com/willemwouters/esp8266-injection-example (дата звернення: 29.03.2019).

12. Wifi Hacking with a 4 Dollar Microcontroller. 2016. URL: https://github.com/markszabo/Hacktivity2016 (дата звернення: 29.03.2019).

13. Fake Beacon ESP8266. 2016. URL: https://github.com/markszabo/FakeBeaconESP8266 (дата звернення: 29.03.2019).

14. Buryachok V. L., Sokolov V. Yu. Using 2.4 GHz Wireless Botnets to Implement Denial-of-Service Attacks. *Web of Scholar*. 2018. No. 6 (24). Vol. 1. P. 14–21. DOI: 10.31435/rsglobal_wos/12062018/5734. arXiv: 1902.08425.

15. Дашко Д. А., Мешков В. И. Социальная инженерия с точки зрения информационной безопасности. *ІТБтаЗ* : матеріали V Всеукр. конф., 4 квітня 2013 р. Киев : ДВНЗ «НГУ», Салвей, 2013. С. 1,2.

16. Давидюк А. В., Петрик В. М. Протидія автоматизованим засобам використання соціальної інженерії. *Актуальні проблеми управління інформаційною безпекою держави* : матеріали IX Всеукр. наук.-практ. конф., 30 бер. 2018 р. Київ : НАСБУ, 2018. С. 346,347.

17. Sokolov V. Y., Korzhenko O. Y. Analysis of Recent Attacks based on Social Engineering Techniques. *Комп'ютерна інженерія і кібербезпека: досягнення та інновації* : матеріали Всеукр. наук.-практ. конф., 27–29 лист. 2018 р. Кропивницький : ЦНТУ, 2018. С. 361–363. DOI: 10.5281/zenodo.2575459. arXiv: 1902.07965.

18. Соколов В. Ю., Курбанмурадов Д. М. Методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності. *Кібербезпека: освіта, наука, техніка*. 2018. №1. С. 6–16. DOI: 10.28925/2663-4023.2018.1.616.

19. Соколов В. Ю. Інформаційні системи і технології : Навчальний посібник. Київ, 2010. 138 с. ISBN: 978-966-8546-95-2.

20. Sokolov V., Taj Dini M., Buryachok V. Wireless and Mobile Security : Laboratory Workshop. Kyiv, 2017. 124 p. DOI: 10.5281/zenodo.2528820.

21. Соколов В. Ю., Тадж-Діні М. М. Безпека безпроводових і мобільних мереж : Лабораторний практикум / за ред. перекл. О. П. Райтер. Київ, 2018. 122 с. DOI: 10.5281/zenodo.2528822.

НАУКОВЕ ВИДАННЯ

Володимир Леонідович БУРЯЧОК
Володимир Юрійович СОКОЛОВ

МЕТОДИ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ І ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ БЕЗПРОВОДОВОЇ ІНФРАСТРУКТУРИ НА ОСНОВІ АПАРАТНОГО РОЗДІЛЕННЯ АБОНЕНТІВ

Монографія

(українською мовою)