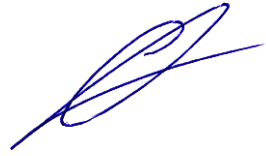


МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ І ГЛОБАЛЬНОГО
ІНФОРМАЦІЙНОГО ПРОСТОРУ НАН УКРАЇНИ

СОКОЛОВ Володимир Юрійович



УДК 004.056:621.396

**МЕТОДИ І ЗАСОБИ ПІДВИЩЕННЯ
ІНФОРМАЦІЙНОЇ ТА ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ
БЕЗПРОВОДОВИХ МЕРЕЖ ПЕРЕДАВАННЯ ДАНИХ**

05.13.06 — «Інформаційні технології»

Автореферат
дисертації на здобуття наукового ступеня
кандидата технічних наук

Київ – 2019

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційної та кібернетичної безпеки факультету інформаційних технологій та управління Київського університету імені Бориса Грінченка Міністерства освіти і науки України.

Науковий керівник: доктор технічних наук, професор
Бурячок Володимир Леонідович,
Київський університет імені Бориса Грінченка
завідувач кафедри інформаційної
та кібернетичної безпеки
факультету інформаційних технологій та управління

Офіційні опоненти: доктор технічних наук, професор
Юдін Олександр Костянтинівич,
Київський національний університет
імені Тараса Шевченка,
професор кафедри кібербезпеки та захисту інформації
факультету інформаційних технологій

доктор технічних наук, професор
Рудницький Володимир Миколайович,
Черкаський державний технологічний університет,
завідувач кафедри
інформаційної безпеки та комп'ютерної інженерії
факультету інформаційних технологій і систем

Захист відбудеться «29» жовтня 2019 р. о 13⁰⁰ на засіданні спеціалізованої вченої ради Д 26.255.01 при Інституті телекомунікацій і глобального інформаційного простору НАН України за адресою:
03186, м. Київ, бул. Чоколівський, 13, ауд. 601.

З дисертацією можна ознайомитись у бібліотеці Інституту телекомунікацій і глобального інформаційного простору НАН України за адресою:
03186, м. Київ, бул. Чоколівський, 13.

Автореферат розісланий «27» вересня 2019 р.

Вчений секретар
спеціалізованої вченої ради
к. т. н.



О. Г. Лебідь

ВСТУП

Обґрунтування вибору теми дослідження. Події кінця ХХ – початку ХХІ 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. Для передачі інформації між її користувачами все частіше застосовуються безпроводові мережі. Вони розгортаються, як правило, в аеропортах, університетах, готелях, ресторанах, на підприємствах та слугують для підключення користувачів до мереж провайдерів інтернет-послуг (замість використання виділених проводових ліній або застарілого модемного з'єднання), а також об'єднання просторово рознесених підмереж в одну загальну мережу – тобто там, де кабельне з'єднання підмереж неможливе або небажане.

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. Це стосується і безпроводового зв'язку, активне поширення послуг якого (оскільки комунікаційні сигнали при їх розповсюдженні через радіоефір легкодоступні для перехоплення) вивело на перший план питання забезпечення захисту безпроводових мереж та способи захисту даних в них. Зважаючи, що основи такої діяльності на даний час формалізовано недостатньо, питання щодо забезпечення інформаційної та функціональної безпеки (доступності та цілісності) безпроводових мереж (з одночасним підвищенням їх ефективності при передаванні інформації) є надзвичайно актуальними.

Відомо, що вирішенню проблеми інформаційної та функціональної безпеки в цілому, та безпроводових мереж зокрема, присвячено праці відомих вітчизняних та закордонних вчених та їх наукових шкіл: Д. В. Агеєва, В. М. Астапені, В. М. Богуша, В. Л. Бурячка, В. В. Домарева, А. Карлсона, О. Г. Корченка, Г. Т. Маркова, М. В. Степашкина, С. В. Толюпи, В. О. Хорошка та Я. С. Шифрина та багатьох ін. **Науково-прикладною задачею**, яка вирішується в дисертаційній роботі, є забезпечення інформаційної та функціональної безпеки безпроводових мереж передавання даних, що, в свою чергу, потребує створення науково обґрунтованих методів підвищення ефективності при передаванні інформації в безпроводових системах в умовах існуючих **об'єктивних протиріч** між динамічними змінами сучасного світу при одночасному збільшенні кількості безпроводових технологій і мереж, та недосконалістю, а подекуди й відсутністю методології побудови інформаційно і функціонально захищених безпроводових систем з іншого. Наявність даних протиріч і обумовлює **актуальність теми дисертації**, а тому вирішення пос-

тавленої науково-прикладної задачі забезпечення інформаційної та функціональної безпеки безпроводових мереж має важливе наукове та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційна робота виконана у рамках науково-дослідної роботи «Розробка методів та заходів підвищення живучості інформаційно-комунікаційних систем в умовах впливу кібернетичних атак» (шифр «Захист ІКС», № д/р 0114U000391), а також міжнародної дослідницько-навчальної програми ВТН №90520 «Computer Science: Master Programs for the Swedish Institute Study Scholarships» за фінансованої підтримки Технологічного інституту Блекінге (Швеція).

Мета і задачі дослідження. Метою дисертаційної роботи є забезпечення інформаційної і функціональної безпеки (доступності та цілісності) безпроводових мереж з підвищенням їх ефективності при передаванні інформації.

Досягнення поставленої мети вимагає вирішення таких **завдань**:

- проведення аналізу існуючих загроз і атак на безпроводові технології (на передавач, приймач і середовище передавання інформації), побудову дерева атак на безпроводові мережі, визначення критеріїв загроз у безпроводових технологіях, оцінювання вразливостей у безпроводових мережах;

- розроблення концепції порівняння моделей побудови безпроводових мереж, проаналізувати спектри сигналів в безпроводових мережах, дослідження технології побудови безпроводових мереж, моделювання безпроводової мережі з ортогональним частотним розділенням каналів;

- удосконалення підходів щодо захисту безпроводових мереж за рахунок технології забезпечення об'єктивного контролю захищеності безпроводових мереж і технології підвищення захищеності безпроводових мереж;

- розроблення методу модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж;

- розроблення методу адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру;

- розроблення методу підвищення функціональної безпеки безпроводової інфраструктури з використанням прискорюючих лінз (в тому числі і поляризаційних властивостей);

- розроблення методу оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз;

- дослідження взаємного впливу безпроводових мереж на забезпечення їх функціональної безпеки та живучості (з використанням спектроаналізаторів);

- дослідження технології моніторингу вільних каналів передавання даних в безпроводових мережах та технології підвищення захищеності безпроводових мереж з використанням прискорюючих лінз і її поляризаційні властивості.

Зважаючи на таке **об'єктом дослідження** в роботі є процес забезпечення інформаційної і функціональної безпеки в безпроводових мережах. **Предметом дослідження** – методи та моделі забезпечення інформаційної та функціональної безпеки в безпроводових мережах на основі апаратного розділення абонентів.

Методи дослідження. Проведені дослідження ґрунтуються на теоретично обґрунтованих та практично апробованих методах теорії інформації (для модифікації теореми Шеннона-Хартлі), теорії інформаційної безпеки (для побудови де-

рев атак), теорії національної безпеки (для опису методів оцінки ймовірності відмови в обслуговуванні, очікуваного збитку і стану систем захисту безпроводових мереж), теорії ймовірності (для оцінки адекватності експертної групи, коефіцієнтів конкордації і Стьюдента), теорії обробки сигналів (для отримання швидкого перетворення Фур'є для сигналів з нульовим середнім каналом), електронної теорії дисперсії світла (для розрахунку зон Френеля), теорії множин (для діаграм Вороного у системах з роумінгом), теорії функцій дійсної змінної (для розрахунку функцій Уолша), теорії мереж Петрі (для моделювання мережі Петрі-Маркова), теорії систем та системного аналізу (для побудови моделі «зомбування», «чорної» скриньки і для проведення функціонально-вартісного аналізу) і міжнародних стандартів BSI, PCI DSS, ISSAF, PTES, OSSTMM, OWASP, NIST SP 800-115 і ISO 17799 в сфері безпеки (для проведення тестування на проникнення).

Наукова новизна отриманих результатів полягає в подальшому розвитку теоретичних і практичних методів та моделей забезпечення інформаційної та функціональної безпеки в безпроводових мережах на основі апаратного розділення абонентів. Новими результатами, отриманими в дисертаційній роботі, є:

– вперше розроблений метод модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж, **впровадження якого** за рахунок модифікації амплітудно-фазового сузір'я сигналів **дозволило: покращити** електромагнітну сумісність точки безпроводового доступу (ТБД) з абонентом та, на відміну від існуючих, **забезпечити** підвищення максимальної теоретичної просторової розв'язки сусідніх сузір'їв на 4,5%;

– вперше розроблений метод підвищення функціональної безпеки безпроводової інфраструктури, **впровадження якого** за рахунок адаптації конструкції прискорюючої лінзи до багатопроменевих систем та з урахуванням впливу їх поляризаційних властивостей на цілісність інформації та її доступність **дозволило: узгодити** антенні системи передавача і приймача за поляризацією та, на відміну від існуючих, **забезпечити** збільшення потужності електромагнітної хвилі в точці прийому до 7 дБмВт, а пропускної здатності – до 4%;

– удосконалений метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах, **впровадження якого** шляхом додавання окремо розташованих аналізаторів спектру до існуючої безпроводової мережі **дозволило: отримувати** оперативну інформацію про стан безпроводового ефіру; **виявляти** в режимі реального часу завади і сторонній кібернетичний вплив та, на відміну від існуючих, **забезпечити** зростання стійкості та інформаційної безпеки безпроводових систем до такого впливу;

– удосконалений метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз, **впровадження якого** шляхом врахування інформаційної та функціональної безпеки кожної з характеристик (як функцій від самої характеристики) **дозволило забезпечити** підвищення достовірності оцінки стану систем захисту безпроводових мереж із значенням коефіцієнта конкордації експертів не нижче 0,67.

Практичне значення отриманих результатів у сукупності складає підґрунтя для побудови захищеної безпроводової корпоративної системи, в якій автоматизо-

вано процеси збору інформації з аналізаторів спектру та її обробки, а також впроваджено дієву та ефективну підсистему моніторингу для адміністраторів безпеки.

Практична цінність отриманих результатів полягає у такому:

1) розроблено мікропрограму на мові програмування C (під компілятор SDCC 3.6.0) для аналізатора спектру на базі Pololu Wixel;

2) розроблено програмний додаток на базі бібліотеки Open Flash Chart для порівняння зібраних даних з мініатюрних аналізаторів спектру CYW6935, WIdetector, TI eZ430-RF2500, Ubiquiti AirView2, Metageek Wi-Spy 2.4x і Pololu Wixel;

3) розроблено експериментальний макет аналізатора спектру на радіомодулі TI CC2500+PA+LNA, контролері Arduino Nano 3.0 і з дисплеєм OLED SSD1306 та програмне забезпечення на мові програмування C (під компілятор GCC 5.4.0);

4) розроблено експериментальні макети для аналізу спектру та моніторингу:

– на базі приймача D-Link DIR-320 (прошивка DD-WRT mini-usb-ftp v24-sp2.13064) і приймача D-Link DIR-300 (прошивка 1.05.a319);

– на базі приймача на мікросхемі RaLink RT2860 (драйвер rt2800pci, ОС Gentoo Linux 2.6.34-r1) та аналізатора пакетів Aircrack-ng 1.0;

– на базі передавача Asus RT-N16 (мікроконтролер Broadcom 4718A, прошивка DD-WRT v24-sp2 mega), приймача Wifly-city IDU-2850UG-G2000 (мікроконтролер Realtek RTL8187L) та аналізатора спектру Ubiquiti AirView2;

– на базі передавача Asus RT-N16 (прошивка DD-WRT K2.6 14896), приймача Atheros AR9287 та аналізаторів спектру Pololu Wixel (TI CC2511F32);

– на базі передавача TP-LINK TL-WR340G (мікроконтролер Atheros AR2317, прошивка Stock 4.18.19.110701), приймача Linksys WUSB54G (мікроконтролер Ralink RT2500USB) та аналізатора спектру NetStumbler 0.4.0;

5) розроблено програмний макет системи моніторингу аналізаторів спектру на базі мікрофреймворка flask на мові програмування Python 3.7.2 для одноплатного комп'ютера на базі Raspberry Pi 3B.

Результати дисертаційного дослідження впроваджено у навчальний процес Державного університету телекомунікацій і Київського університету імені Бориса Грінченка в рамках магістерського курсу «Методи та засоби забезпечення безпеки безпроводових і мобільних мереж» (акт впровадження №20-н від 15.04.2019), у міжнародному Темпус-проекті №544455-TEMPUS-1-2013-1-SE-TEMPUS-JPCR ENGENSEC «Підготовка наступного покоління експертів з кібербезпеки: нова визнана ЄС магістерська програма» в рамках магістерського курсу «Wireless and Mobile Security» (диплом впровадження від 12.11.2017), при розгортанні чотирьох віртуальних платформ «Навчальний кіберполігон» (Державний університет телекомунікацій, Київський університет імені Бориса Грінченка, Національний університет «Львівська політехніка» і Харківський національний університет радіоелектроніки), а також в практичній діяльності ТОВ «Автор» (акт впровадження від 23.04.2019), ТОВ «ХЕЛСІ ЮА» (акт впровадження від 13.04.2019), ТОВ «Система Трейд» (акт впровадження від 14.03.2019) і ТОВ «Домофон-Південь» (акт впровадження від 16.02.2019).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [1,2,19,30,32,33] – підходи щодо роз-

робки низькобюджетних аналізаторів спектру; [3,23,24] – метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру і організація ботнетів; [4,5,8,9] – дослідження захищеності та електромагнітної сумісності безпроводових мереж; [6] – модифікований метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз; [7,13] – метод модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж; [10,34] – використання дерев атак для аналізу захищеності безпроводових технологій; [11,21,22,25,26,31] – метод підвищення цілісності та доступності інформації у безпроводових системах з використанням прискорюючих лінз; [12,14,16,20,29] – підвищення пропускну здатності безпроводових каналів зв'язку на основі поляризаційних ефектів; [15,17] – застосування SDR для тестування на проникнення IoT-пристроїв стандартів IEEE 802.15.4 і 802.16.4; [18,35] – методика протидії соціальному інжинірингу на об'єктах інформаційної діяльності; [27,28] – застосування діаграм Вороного для безпроводових мереж з роумінгом.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на наукових конференціях та семінарах, серед яких: VI, VIII і IX міжнар. н.-т. конф. студентства і молоді ДУІКТ (м. Київ, 2009, 2011, 2012 рр.); VII і VIII наук. конф. «Сучасні тенденції розвитку в інфокомунікаціях та освіті» (м. Київ, 2010, 2011 рр.); VII, VIII і IX міжнар. н.-т. конф. «Сучасні інформаційно-комунікаційні технології» (COMINFO, м. Київ, 2011, 2012, 2015); IX, X і XI міжнар. конф. 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.); I, II і III міжнар. н.-т. конф. з актуальних проблем науки і техніки (International Scientific-Technical Conference on Actual Problems of Science and Technology, м. Київ, 2015, 2016 рр.); IV і V міжнар. н.-пр. конф. «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.); II міжнар. н.-пр. конф. «Міжнародні тенденції в галузі науки і техніки» (International Trends in Science and Technology, стендова доп., м. Варшава, 2018 р.); презентація програми дисципліни «Методи та засоби забезпечення безпеки безпроводових і мобільних мереж» (м. Карлскрона, 2017 р.); конф. країн Європи і СНД «ALERT Cyber Drill» (ALERT cyber drill for Europe and CIS Regions, м. Кишинів, 2017 р.); IV міжнар. н.-пр. конф. «Інноваційні технології в науці» (Innovative Technologies in Science, стендова доп., м. Дубай, 2018 р.); регіон. семінар Міжнар. 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.); круглий стіл «Кібербезпека: освітній аспект» (м. Київ, 2018 р.); всеукр. н.-пр. конф. «Актуальні питання протидії кіберзлочинності та торгівлі людьми» (м. Харків, 2018 р.); всеукр. н.-пр. конф. здобувачів вищої освіти й молодих учених «Комп'ютерна інженерія і кібербезпека: досягнення та інновації» (м. Кропивницький, 2018 р.); II міжнар. конф. з комп. наук, інженерії та освітніх програм (International Conference on Computer Science, Engineering and Education Applications, ICCSEEA2019, м. Київ, 2019 р.).

Публікації. Основні положення дисертаційної роботи опубліковані у 35 наукових працях, з яких: 1 публікація – розділ колективної монографії [1]; 18 – у закордонних [2,3] і вітчизняних [4–19] фахових наукових виданнях, які входять до міжнародних наукометричних баз даних (*Index Copernicus, CORE, BASE, DBLP, arXiv, DiVA2, ResearchBib, PKP, OCLC* тощо); 5 – публікацій у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science* [20–24] та 11 тез доповідей [25–35]. Без співавторів – опубліковано 6 наукових статей і 3 тези доповідей.

Обсяг і структура дисертації. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, трьох розділів, загальних висновків, списків використаних джерел (в кінці кожного розділу основної частини дисертації) і має 161 сторінок основного тексту, 89 рисунків, 22 таблиці. Список використаних джерел містить 123 унікальні найменування і займає 14 сторінок. Загальний обсяг дисертаційної роботи – 182 сторінки.

ОСНОВНИЙ ЗМІСТ

У **вступі** показано актуальність напряду досліджень, відбито зв'язок дисертаційної роботи з науковими програмами, планами та темами, сформовано мету і завдання дослідження, наведено основні положення, які виносяться на захист і практичну цінність роботи, наведено відомості про апробацію результатів і їх впровадження.

У **першому розділі:**

1. Досліджено суперечності, що впливають на безпроводову інфраструктуру та мають місце між безпроводовими мережами при їх розгортанні і підтримуванні їх працездатності та безпроводовими технологіями при їх використанні для забезпечення потреб бізнесу і персоналій, що дозволило, як результат, сформуванати наукове завдання дослідження і його загальну концепцію (рис. 1).

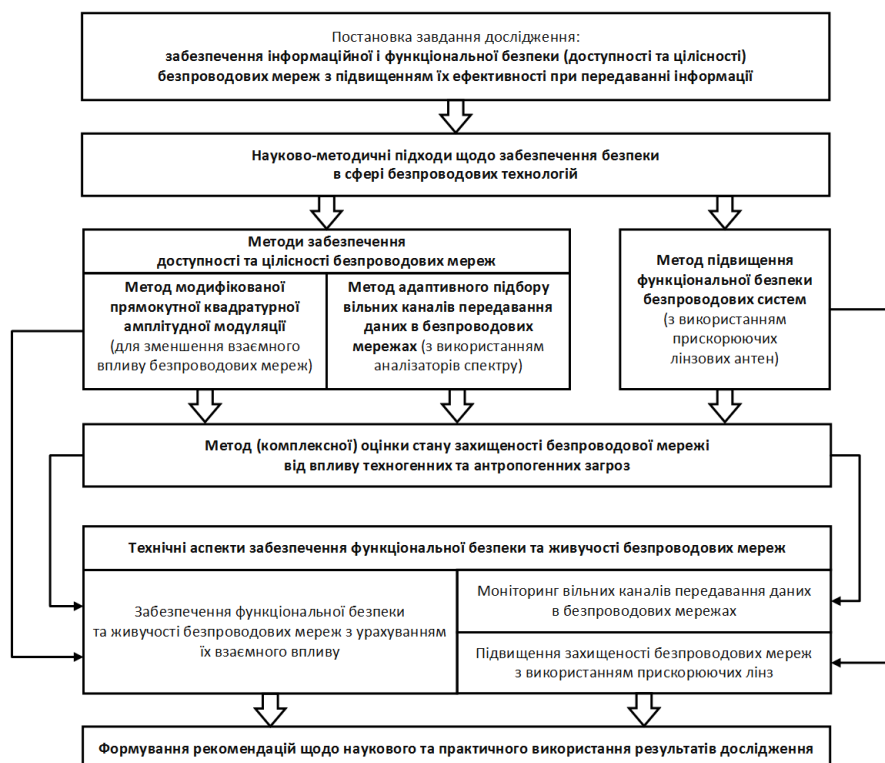


Рис. 1. Загальна концепція дисертаційного дослідження

2. Проведено, використовуючи технологію побудови дерева атак, аналіз існуючих загроз та атак на безпроводову інфраструктуру, а також розглянуто шляхи щодо послаблення їх впливу. Констатовано, що найбільш критичною для безпроводової інфраструктури є DoS-атаки на службові канали зв'язку.

3. Сформовано основні напрями проведення дослідження, вирішуючи які доцільно виходити з того, що нині з розширенням покриття безпроводових технологій виникає проблема системного підходу до захисту всієї безпроводової інфраструктури, а не лише окремих ТБД. Ця проблема ускладнюється легкістю доступу до середовища передавання даних та відсутністю універсального інструментарію для виявлення сучасних загроз і атак на безпроводову інфраструктуру.

В другому розділі показано, що динаміка зростання кількості ТБД є ступеневою функцією:

$$N(Y) = (Y - 2000)^{4,54} + 3450, \quad (1)$$

де Y – обліковий рік.

Дана функція отримана за результатами аналізу статистичних даних компанії Wireless Geographic Logging Engine (рис. 2, де теоретична крива показана штриховим пунктиром, а реальна – суцільною лінією).

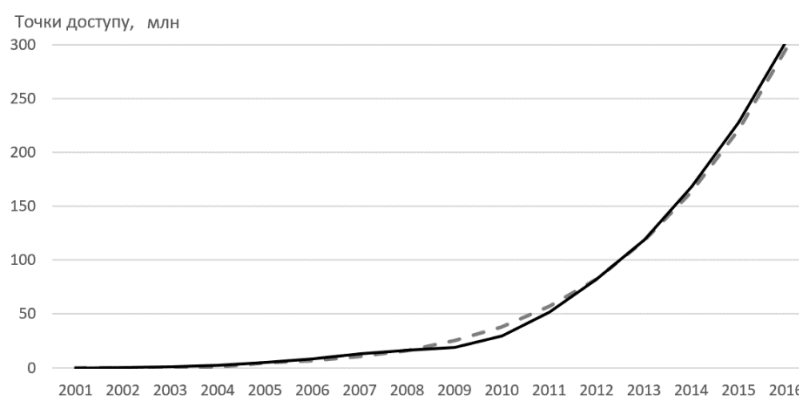


Рис. 2. Зростання кількості точок безпроводового доступу

Таке стрімке зростання приводить до ускладнення роботи кількох безпроводових мереж в одному і тому самому частотному діапазоні.

З метою нівелювання цієї проблеми та забезпечення ущільнення амплітудно-фазового сузір'я сигналів, зменшення взаємного впливу безпроводових мереж та забезпечення їх інформаційної безпеки, в роботі використовуючи прості правила для досягнення найбільшої евклідової метрики (дистанції) між базовим і модифікованим векторам (довжина вектору помилки) розроблено **метод модифікованої прямокутної квадратурної амплітудної модуляції**.

Для базового векторного простору мінімальна внутрішня відстань між векторами становить $r_{вн} = 2,000$ для векторних просторів, які стандартно використовуються для 2^k -QAM, а зовнішня – $r_{зовн} = 0,000$. Віддалення складає при цьому $\Delta_{ном} = r_{вн} - r_{зовн} = 2,000$. Це означає максимальне перекриття при використанні двох систем з базовим векторним простором. Тобто, чим менше віддалення, тим стабільніше будуть працювати обидві системи.

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

Тоді для базового векторного простору коефіцієнт нормування становить:

$$\begin{aligned} \bar{k} &= \sqrt{E_{\text{сеп}}[|R|^2]} = \sqrt{2E_{\text{сеп}}[\text{Re}|R|^2]} = \sqrt{2 \cdot \frac{a}{n} \sum_{m=1}^a (2m - 1)^2} = \\ &= \sqrt{\frac{2}{3} \cdot \frac{a^2}{n} \cdot (4a^2 - 1)} = \sqrt{\frac{2}{3} \cdot \frac{2^{\frac{k-2}{2} \cdot 2}}{2^{k-2}} \cdot (4 \cdot 2^{\frac{k-2}{2} \cdot 2} - 1)} = \sqrt{\frac{2}{3} (2^k - 1)}, \end{aligned} \quad (2)$$

де $n = 2^k/4 = 2^{k-2}$ – кількість точок в кожному квадранті; таблична сума ступенів натуральних чисел $\in \sum_{m=1}^a (2m - 1)^2 = \frac{1}{3} \cdot a \cdot (4a^2 - 1)$. Тоді для двох видів модуляції маємо $\bar{k}^{16\text{QAM}} = \sqrt{10} \approx 3,162$ і $\bar{k}^{64\text{QAM}} = \sqrt{42} \approx 6,481$.

В роботі введено і перевірено гіпотезу, згідно якої зміна правил побудови сигнального простору дозволить ущільнити кілька ТБД в одному частотному діапазоні та розглянуто п'ять основних модифікацій: обертання на 45° (рис. 3а); зміщення (рис. 3б і 3в); нормальне (рис. 3г) та компактне (рис. 3д) віддалення від початку координат; обертання групи на 45° (рис. 3е).

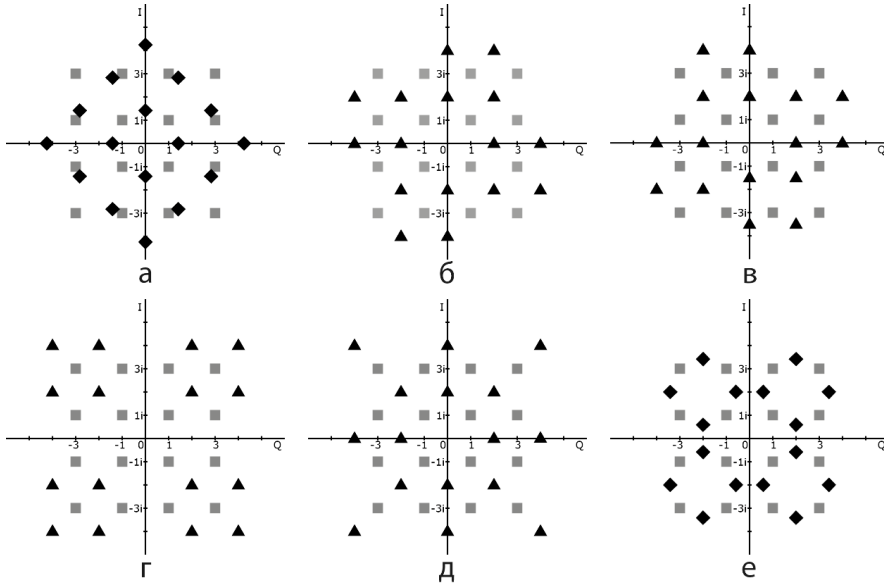


Рис. 3. Модифікація векторного простору для 16-QAM: обертання на 45° (а); зміщення проти (б) та за (в) годинникової стрілки; нормальне (г) та компактне (д) віддалення від початку координат; обертання групи на 45° (е)

Доведено, що найпростіше перетворення отримується обертанням базового простору на 45° (рис. 3а, де для 16-QAM, квадратами вказано базовий векторний простір, а ромбами – його модифікація). Таке перетворення проводиться за наступною схемою:

$$\begin{cases} Q = \sqrt{Q_0^2 + I_0^2} \cos\left(\alpha \pm \frac{\pi}{4}\right), \\ I = \sqrt{Q_0^2 + I_0^2} \sin\left(\alpha \pm \frac{\pi}{4}\right), \end{cases} \quad (3)$$

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

В даному випадку мінімальна внутрішня відстань між векторами залишається незмінною $r_{\text{вн}} = 2,000$, мінімальна зовнішня 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.

Якщо знехтувати симетрією можна отримати два перетворення: зміщення проти і за годинниковою стрілкою (рис. 3б і 3в, де квадратами вказано базовий векторний простір, а трикутниками – його модифікація). Для кожного з квадрантів при зміщенні (перший знак у відповіді вказує на зміщення проти годинникової стрілки, а другий – за) маємо сукупність виду:

$$\begin{aligned} \text{[I]} & \left\{ R = R_0 + (\mp 1 \pm i), \right. \\ \text{[II]} & \left\{ R = R_0 + (\mp 1 \mp i), \right. \\ \text{[III]} & \left\{ R = R_0 + (\pm 1 \mp i), \right. \\ \text{[IV]} & \left\{ R = R_0 + (\pm 1 \pm i). \right. \end{aligned} \quad (4)$$

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

$$\begin{aligned} 16\text{QAM}: & \{2i; 4i; 2 + 2i; 2 + 4i\}; \\ 64\text{QAM}: & \left\{ \begin{array}{l} 2i; 4i; 6i; 8i \\ 2 + 2i; 2 + 4i; 2 + 6i; 2 + 8i \\ 4 + 2i; 4 + 4i; 4 + 6i; 4 + 8i \\ 6 + 2i; 6 + 4i; 6 + 6i; 6 + 8i \end{array} \right\}, \end{aligned} \quad (5)$$

Тоді з (2) визначаються коефіцієнти нормування:

$$\begin{aligned} k_{S_{3M}}^{16\text{QAM}} &= \sqrt{\frac{1}{2^{4-2}} [2^2 + 4^2 + 2^2 + 2^2 + 2^2 + 4^2]} = 2\sqrt{3} \approx 3,464, \\ k_{S_{3M}}^{64\text{QAM}} &= \sqrt{\frac{1}{2^{6-2}} [8 \cdot 2^2 + 8 \cdot 4^2 + 8 \cdot 6^2 + 4 \cdot 8^2]} = 2\sqrt{11} \approx 6,633. \end{aligned} \quad (6)$$

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

$$\delta = \frac{\Delta_{\text{б}} - \Delta_{\text{м}}}{\Delta_{\text{б}}} \cdot 100\%, \quad (7)$$

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

Результати розрахунків коефіцієнтів нормування для інших модифікацій приведено в табл. 1. З таблиці видно, що з усіх видів зміщення (віддалення) краще використовується енергія спектру у віддаленні з оптимізацією (розроблений метод обертання групи показав незначне погіршення енергетичних характеристик у порівнянні з базовим векторним простором, і лише при використанні 64-QAM).

Коефіцієнти нормування k_s , віддалення Δ і вигравш δ

Векторний простір:	k_s^{16QAM}	k_s^{64QAM}	Δ^{16QAM}	Δ^{64QAM}	$\delta^{16QAM},\%$	$\delta^{64QAM},\%$
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	0,090		95,5	
Обертанням групи на 45°	3,162	6,519				

При збільшенні рівня завад збільшується кількість помилок під час приймання сигналу. Селективність фільтра для кожного вектору можна зменшити, але це призведе до збільшення кількості помилок від модифікованого простору векторів. Одним із варіантів рішень саме й стало переналаштування на модуляцію з меншим коефіцієнтом k . Це дозволило за рахунок модифікації області амплітудно-фазового сузір'я сигналів покращити електромагнітну сумісність ТБД з абонентами та, на відміну від існуючих, забезпечити підвищення максимальної теоретичної просторової розв'язки сусідніх сузір'їв на 4,5%. Разом з тим питання щодо забезпечення стійкості та інформаційної безпеки безпроводової інфраструктури залишились невирішеними й такими, що й нині потребують свого розв'язку.

З метою забезпечення стійкості та інформаційної безпеки безпроводової інфраструктури в умовах стороннього кібернетичного впливу в реальному часі в роботі розроблено метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру. Він дозволив, застосовуючи систему додаткових незалежних пристроїв (аналізаторів спектру), вирішити задачу гарантованого вибору оптимального частотного каналу передавання даних наряду з вже існуючими безпроводовими адаптерами, область видимості яких часто обмежена лише мережами одного стандарту (так деякі карти навіть не бачать «прихованих» мереж). Схема, подана на рис. 4, показує розподілену підсистему з аналізаторами спектру.

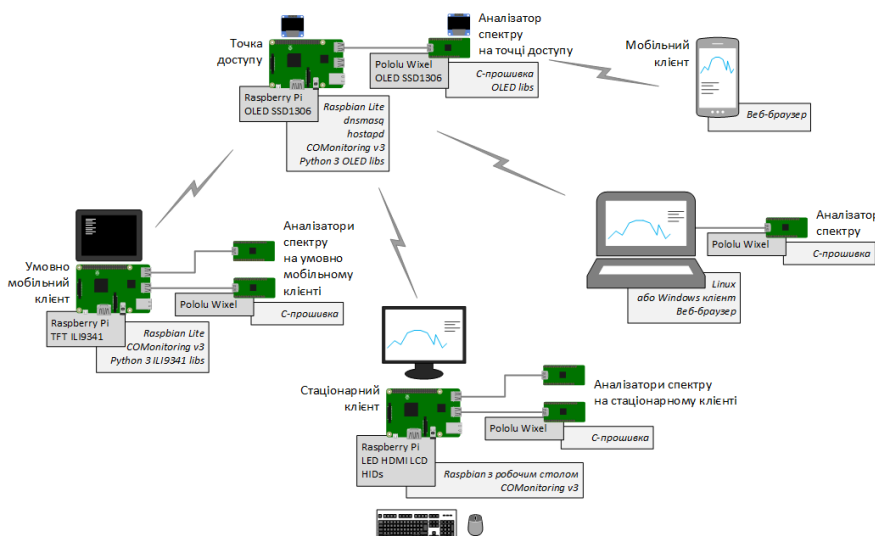


Рис. 4. Схема з аналізаторами спектру

Схема складається з контролера, який розподіляє канали і навантаження в мережі, керуючи інфраструктурою безпроводового зв'язку; ТБД; клієнтів з аналі-

заторами спектру і окремих аналізаторів спектру, розташованих у ключових точках. Алгоритм збору даних показано на рис. 5.

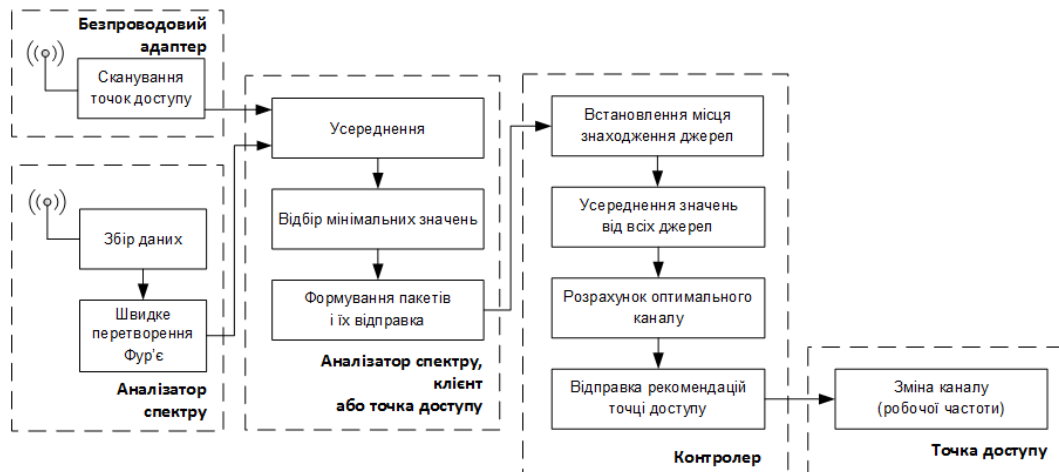


Рис. 5. Алгоритм динамічного розподілу каналів

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

$$L_j^{\text{ch}} = \frac{1}{N} \sum_{i=1}^N L_{ij}, \quad (8)$$

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:

$$\bar{L}_{\text{зовн}}^{\text{ch}} = \frac{1}{M} \sum_{j=1}^M \mu_j L_j^{\text{ch}}, \quad (9)$$

де M – кількість спектроаналізаторів; μ_j – зважування важливості конкретного пристрою; L_j^{ch} – середній рівень сигналу для конкретного пристрою з (8).

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:

$$\bar{L}_{\text{вн}}^{\text{ch}} = \frac{1}{H} \sum_{j=1}^H \mu_j \sum_{k=1}^K \nu_k^{\text{ch}} L_k, \quad (10)$$

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 (табл. 2); L_k – рівні сигналу до k -ї безпроводової мережі.

Таблиця 2

Коефіцієнти перетину каналів

$ ch-k $	0	1	2	3	>4
ν_k^{ch}	1	$\frac{3}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	0

В роботі досліджено три варіанти створення портативних аналізаторів спектру: приймач і блок управління (відокремлені і на одному кристалі, див. рис. 6); приймач з визначеним рівнем сигналу на двох станах і блоці управління; інтегровані клієнтські безпроводові карти.

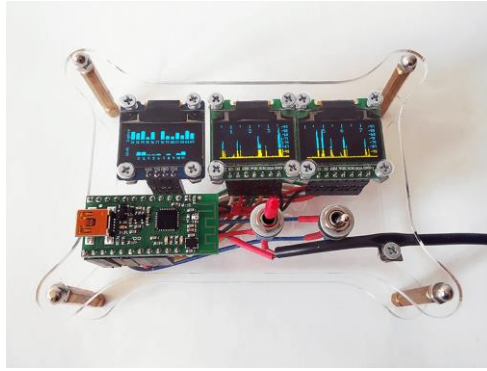


Рис. 6. Приклад однокристалного аналізатору спектру на Pololu Wixel

Їх введення в безпроводову систему призводить до того, що настання критичного режиму роботи стає менш ймовірним. Це пояснюється передусім тим, що абоненти на перевантажених ТБД за максимальним рівнем сигналу та складними алгоритмами розподілення навантаження перенаправляються на сусідні ТБД. При цьому для аналізаторів спектру з двома станами рівню сигналу (наприклад, Nordic nRF24L01) рівень сигналу в i -й точці може бути обчислений за формулою:

$$P_i = L_{\min} + \frac{2(L_{\text{сеп}} - L_{\min})}{N} \sum_{j=1}^M p_{ij}, \quad (11)$$

де L_{\min} і $L_{\text{сеп}}$ – мінімальний рівень і рівень тригера прапора, дБмВт; M – кількість вимірювань; p_{ij} – результат одиночного вимірювання (приймає значення 0 або 1).

Оцінити якість роботи безпроводової мережі з аналізаторами спектру можна за відношенням коефіцієнтів ефективності:

$$\frac{K}{K_{\text{АС}}} = \frac{E \cdot C_{\text{АС}}}{E_{\text{АС}} \cdot C} = \frac{N}{N_{\text{ТБД}}} \cdot \frac{1}{N^{\max}} \cdot \left(1 + \frac{P_{\text{АС}}}{P_{\text{інфр}} + P_{\text{обсл}}} \right), \quad (12)$$

де $E_{\text{АС}}$ – ефективність мережі з аналізаторами спектру, $E_{\text{АС}} \sim \frac{N_{\text{ТБД}}}{N} \Delta T$;

E – ефективність звичайної безпроводової мережі прямо пропорційна мінімальному часу доступу абонента до ресурсів ТБД, $E \sim T_a^{\min} = \frac{\Delta T}{N^{\max}}$;

ΔT – розмір часового вікна передавання;

N^{\max} – максимально можлива кількість абонентів на одну ТБД (від 30 до 50);

$N_{\text{ТБД}}$ – кількість ТБД;

N – повна кількість абонентів, $N \approx (2 + \sigma)(N_{\text{умов}} + N_{\text{нерух}})$;

$N_{\text{умов}}$ – кількість умовно рухомих абонентів;

$N_{\text{нерух}}$ – кількість нерухомих абонентів;

$P_{\text{обсл}}$ – вартість обслуговування;

$P_{\text{інфр}}$ – вартість інфраструктури, $P_{\text{інфр}} \sim N_{\text{рух}} + N_{\text{умов}} + N_{\text{нерух}} + N_{\text{гост}}$;

$N_{\text{рух}}$ – кількість рухомих абонентів, $N_{\text{рух}} \approx N_{\text{умов}} + N_{\text{нерух}}$;

$N_{\text{гост}}$ – кількість гостей, $N_{\text{гост}} = \sigma N_{\text{рух}}$;

σ – показник відкритості безпроводової системи;

$P_{\text{АС}}$ – вартість системи спектроаналізаторів, $P_{\text{АС}} = (N_{\text{умов}} + N_{\text{нерух}})P_{\text{АС}}^* + P_{\text{конт}}$;

$P_{\text{АС}}^*$ – вартість одного спектроаналізатору;

$P_{\text{конт}}$ – вартість контролера для збору і аналізу даних від аналізаторів спектру;

C – вартість звичайної безпроводової системи, $C = P_{\text{інфр}} + P_{\text{обсл}}$;

$C_{\text{АС}}$ – вартість безпроводової системи з аналізаторами спектру,

$$C_{\text{АС}} = P_{\text{інфр}} + P_{\text{обсл}} + P_{\text{АС}} = C + P_{\text{АС}}.$$

Застосування підсистем з аналізаторами спектру *дозволило* шляхом їх додавання до існуючої безпроводової мережі *отримувати* оперативну інформацію про стан безпроводового ефіру, *виявляти* в режимі реального часу завади і сторонній кібернетичний вплив та, на відміну від існуючих, *забезпечувати* зростання стійкості та інформаційної безпеки безпроводових систем до такого впливу.

Враховуючи, що наряду із забезпеченням інформаційної безпеки не менш важливими показниками функціонування безпроводової інфраструктури є забезпечення доступності та цілісності інформації, що циркулює в безпроводових мережах, в роботі розроблено **метод підвищення функціональної безпеки безпроводової інфраструктури**. Метод базується на модифікованих прискорюючих лінзових антенах, які застосовуються, зокрема, й для багатопроменевих систем типу МІМО. Для визначення діаграми спрямованості модифікованої прискорюючої лінзової антени в роботі було проведено розрахунки спотворень фазового розподілу в розкритті циліндричної прискорюючої лінзи і відхилень максимуму діаграми спрямованості, обумовлених зміщенням положення опромінювачів щодо фазового центра лінзи перпендикулярно осі в горизонтальній площині (рис. 7).

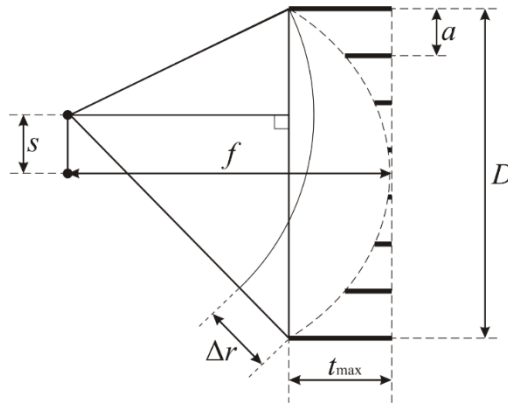


Рис. 7. Зсув випромінювача з фокусу прискорюючої лінзи (вид зверху)

Для прискорюючої лінзи з класичним профілем (при розташуванні опромінювача у фокусі) геометричний шлях (Δr) хвилі від зміщеного вліво на величину s вібратора до опромінюваної поверхні лінзи можна обчислити за формулою:

$$\Delta r(d) = \sqrt{(f - t(d))^2 + (d - s)^2} - \sqrt{(f - t_{\max})^2 + (D/2 - s)^2}, \quad (13)$$

де f – фокальна відстань; D – розкриття прискорюючої лінзи; d – поточний розкриття, $d \in [-D/2; +D/2]$; s – зміщення опромінювача від фокуса; t_{\max} – максимальна глибина прискорюючої лінзи. Профіль t являє собою функцію від положення пластини в розкритті d , яка відрізняється від класичної:

$$t(d) = \frac{f}{n+1} - \sqrt{\left(\frac{f}{n+1}\right)^2 - \frac{d^2}{1-n^2}}, \quad (14)$$

де n – коефіцієнт заломлення.

На протилежній зміщенню випромінювача стороні апертури прискорюючої лінзи має місце відставання по фазі, що приводить до зміщення максимуму діаграми спрямованості в сторону, протилежну зсуву опромінювача. При двох опромінювачах (один зміщений вліво, а другий – вправо) система матиме два максимуми діаграми спрямованості, зміщені, відповідно, вправо і вліво.

У рамках другого підходу було проведено обчислення профілів лінзи для лівого і правого опромінювача окремо, вважаючи їх розташованими у фокусах від-

повідних лінз. Після цього виконано усереднення глибин окремих пластин. Виявилось, що зазначені відхилення сумісні або менші за допустиму величину для лінзи з фокусною відстанню $f = 3D$, при $n = 0,5$. При $f = 1,6D$ тільки для першої від центру пластини. Тобто, зі збільшенням фокусної відстані лінзи з усередненим профілем стає менш чутлива до помилок вибору профілю лінзи.

Для підвищення якості зв'язку у багатоканальних системах поряд з використанням дублювання пакетів було застосовано поляризаційні ефекти. Елементи каналної матриці \mathbf{H} , що використовується для опису таких систем визначимо за формулою:

$$h_{ij} = \frac{P_{\text{п}}}{P_{\text{б}}} = \sqrt[10]{10^{p_{\text{п}} - p_{\text{б}}}}, \quad (15)$$

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.

В якості прикладу у роботі було досліджено взаємне розташування антен, що показано на рис. 8.

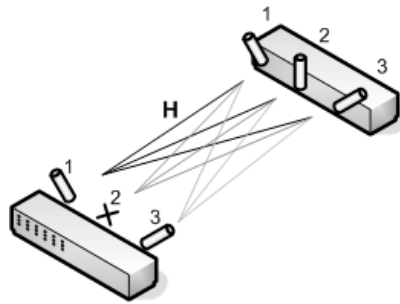


Рис. 8. Приклад взаємного розташування антен

Канальна матриця для даного розташування має вигляд:

$$\mathbf{H} = \begin{bmatrix} 1,00 & 0,32 & 0,05 \\ 0,01 & 0,01 & 0,01 \\ 0,05 & 0,32 & 1,00 \end{bmatrix}. \quad (16)$$

З модифікованої теореми Шеннона-Хартлі маємо інформаційну пропускну здатність каналу (із розрахунку на один герц):

$$C = \log_2 \det \left(I_N + \frac{\rho}{N} \cdot \mathbf{H}\mathbf{H}^T \right), \quad (17)$$

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

$$\rho = \frac{P_{\text{сигн}}}{P_{\text{шум}}} = \sqrt[10]{10^{p_{\text{сигн}} - p_{\text{шум}}}}, \quad (18)$$

де $P_{\text{сигн}}$ і $P_{\text{шум}}$ – рівні корисного сигналу і шуму, мВт; $p_{\text{сигн}}$ і $p_{\text{шум}}$ – рівні сигналів, дБмВт. В табл. 3 приведено результати розрахунків за формулами (17) і (18) інформаційної пропускну здатності безперервного каналу в залежності від орієнтації антен. З наведених даних видно, що пропускну здатність залежить, насамперед, від взаємного розташування передавальної і приймальної антен, а не від їх кількості.

Адаптація конструкції прискорюючої лінзи *дозволила* з урахуванням впливу їх поляризаційних властивостей на цілісність інформації та її доступність *узгодити* антенні системи передавача і приймача за поляризацією та, на відміну від існуючих, *забезпечити* збільшення потужності електромагнітної хвилі в точці прийому до 7 дБмВт, а пропускну здатності – до 4%.

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			

З метою отримання інтегральної оцінки підвищення інформаційної і функціональної безпеки в роботі було удосконалено **метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз**. Відомо, що будь-яка загроза характеризується набором характеристик. Враховуючи, що висновки експертів будуть корелюватися через суб'єктивність, а оцінки інформаційної 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 інформаційної та функціональної безпеки i -ї характеристики:

$$\begin{cases} W_i = f_W(x_i), \\ G_i = f_G(x_i); \end{cases} \quad (19)$$

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

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

$$S^* = \frac{1}{N} \sum_{i=1}^N W^*(x_i) \cdot G^*(x_i), \quad (20)$$

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

$$W^*(x_i) = \left| \frac{f_W(x_i)}{\max[f_W(x_i)]} \right|, \quad (21)$$

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

$$G^*(x_i) = \left| \frac{G_i^\Sigma}{G_{i \max}^\Sigma} \right|. \quad (22)$$

Проміжні значення функції $G^*(x_i)$ визначаються як інтегральні характеристики:

$$\begin{cases} G_i^\Sigma = \int_{x_i^{\text{кін}}}^{x_i^{\text{поч}}} f_G(x) dx, \\ G_{i \max}^\Sigma = \int_{x_i^{\text{мін}}}^{x_i^{\text{макс}}} f_G(x) dx; \end{cases} \quad (23)$$

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 $x_i^{\text{мін}}$ до $x_i^{\text{макс}}$.

Зважаючи, що в приведеному випадку необхідно оперувати результатами експертної оцінки, 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 знай-

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

$$\begin{cases} G_1 = f_G(x), x = \overline{x_1^{\min}, x_1^{\text{cep}}, x_1^{\max}} \\ G_2 = f_G(x), x = \overline{x_2^{\min}, x_2^{\text{cep}}, x_2^{\max}} \\ \dots \\ G_N = f_G(x), x = \overline{x_N^{\min}, x_N^{\text{cep}}, x_N^{\max}} \end{cases} \quad (24)$$

Вагомість функціональної безпеки визначаємо методом розстановки пріоритетів. Згідно з ним пріоритети характеристик визначає експертна група, для якої розраховується коефіцієнт конкордації Кендала. Для розподілених систем безпроводого зв'язку він становить $W_{\text{розпод. сист. рух. зв'язку}} \geq 0,67$.

Зважаючи на те, що нормований ступень забезпечення систем захисту має бути $S^* \leq 1$, модифікований метод оцінки стану систем захисту безпроводової інфраструктури 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. Це, як наслідок, дозволить шляхом врахування інформаційної та функціональної безпеки кожної з характеристик *забезпечити* підвищення достовірності оцінки стану систем захисту безпроводових мереж.

В **третьому розділі** приведено експериментальну перевірку запропонованих методів, а саме:

1) досліджено взаємний вплив безпроводових мереж на забезпечення їх функціональної безпеки та живучості. Результати перевірки електромагнітної сумісності мереж IEEE подано на рис. 9;

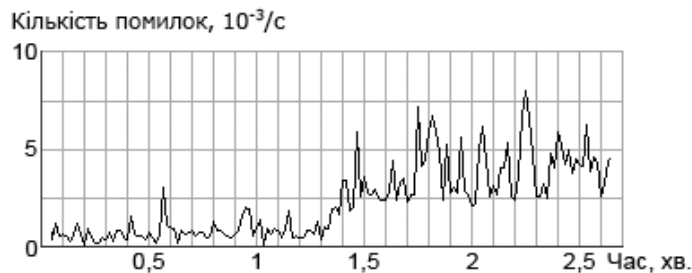


Рис. 9. Електромагнітна сумісність мереж IEEE 802.11 і 802.15.1

2) досліджено взаємний вплив безпроводових мереж з використанням сучасних спектроаналізаторів на базі мікроконтролера CC2500, мікробірок MD7105-SY і CYWUSB6935. Розроблене і вдосконалене програмне і апаратне забезпечення для сучасних спектроаналізаторів;

3) проведено моніторинг вільних каналів передавання даних в безпроводових мережах. З цією метою в роботі розроблене відповідне програмне забезпечення;

4) досліджено захищеність безпроводових мереж, в яких застосовуються прискорюючі лінзи. З цією метою в роботі проведено експериментальне підтвердження якості дії прискорюючою лінзи для частотного діапазону 2,4–2,5 ГГц. Введено показник відношення суми сигналу S і шуму N до шуму:

$$SNNR = 10 \lg \frac{S+N}{N} = 10 \lg(SNR + 1); \quad (25)$$

5) проведено перевірку конструктивних і поляризаційних властивостей багатопромених лінзових систем на цілісність інформації та її доступність. Результати перевірки подано відповідно на рис. 10 та рис. 11.

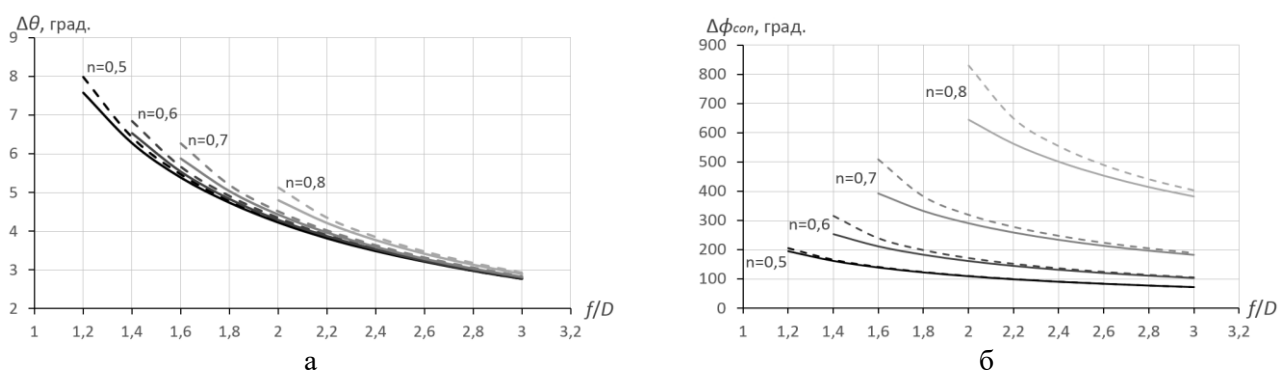


Рис. 10. Характеристики багатопроменевих лінзових систем: а – зсув максимуму діаграми спрямованості; б – максимум увігнутості фазового розподілу

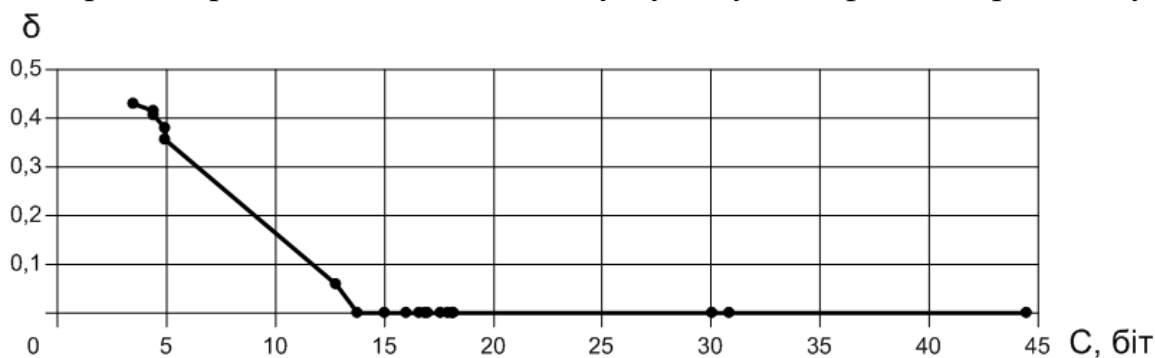


Рис. 11. Відношення кількості помилок до пропускної здатності

ВИСНОВКИ

Результатом виконаної роботи є вирішення актуальної і важливої науково-прикладної задачі розробки методів забезпечення інформаційної і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів, що сприятиме підвищенню рівня захищеності безпроводової інфраструктури від загроз безпеці різноманітного характеру.

У процесі виконання дисертаційної роботи отримано такі основні результати:

1. Розроблено метод модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж, що забезпечило підвищення максимальної теоретичної просторової розв'язки сусідніх сузір'їв на 4,5%.

2. Розроблено метод підвищення функціональної безпеки безпроводової інфраструктури, що забезпечило збільшення потужності електромагнітної хвилі в точці прийому до 7 дБмВт, а пропускної здатності – до 4%.

3. Удосконалено метод адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру, що забезпечило зростання стійкості та інформаційної безпеки безпроводових систем до кібернетичного впливу.

4. Удосконалено метод оцінки стану систем захисту безпроводової інфраструктури від впливу техногенних та антропогенних загроз, що забезпечило підвищення достовірності оцінки стану систем захисту безпроводових мереж із значенням коефіцієнта конкордації експертів не нижче 0,67.

5. Розроблено мікропрограми для аналізаторів спектру на базі Pololu Wixel та експериментальні макети для аналізу спектру та моніторингу: на базі приймачів D-Link DIR-300, D-Link DIR-320, мікросхеми RaLink RT2860 та аналізатору пакетів Aircrack-ng 1.0; на базі передавача Asus RT-N16, приймача Wifly-city IDU-2850UG-G2000 та аналізатора спектру Ubiquiti AirView2; на базі передавача Asus RT-N16, приймача Atheros AR9287 та аналізаторів спектру Pololu Wixel; на базі

передавача TP-LINK TL-WR340G, приймача Linksys WUSB54G та аналізатора спектру NetStumbler 0.4.0.

б. Розроблено програмні додатки для порівняння даних з аналізаторів спектру і для системи моніторингу аналізаторів.

Результати експериментів впроваджено у навчальний процес українських та іноземних закладів вищої освіти, в тому числі розгорнуто чотири віртуальні платформи «Навчальний кіберполігон» для відпрацювання механізмів безпеки. Таким чином, запропоновані методи і отримані результати їх експериментального підтвердження дозволяють забезпечити інформаційну і функціональну безпеку безпроводової інфраструктури, отримати ефективну безпроводову мережу та забезпечити вирішення проблеми «останньої милі» для абонентів зі складним розташуванням.

У своїй сукупності отримані в роботі наукові результати утворюють нову інформаційну технологію підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Колективна монографія в іноземному науковому виданні:

1. 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.

Статті в іноземних наукових виданнях:

2. 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/c4xx.

3. 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/cvnd.

Статті у наукових фахових виданнях України:

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

5. Соловьев В. Р., Богущ 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.

6. **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/cvds.

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

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

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

11. 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.

12. 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.

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

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

15. Taj Dini M., **Sokolov V. Yu.** Internet of Things Security Problems. *Сучасний захист інформації*. 2017. №1. С. 120–127. DOI: 10/c56m.

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

17. 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/c4xz.

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/c4xr.

19. **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/c4xp.

Публікації у наукометричних базах Scopus i Web of Science:

20. 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)* : in IX Int. Conf., 16–20 Sept. 2013. Odessa : IEEE, 2013. P. 172–174. DOI: 10/cvdr. (*Scopus*).

21. 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)* : in X Anniversary Int. Conf., 21–24 Apr. 2015. Kharkiv : IEEE, 2015. P. 267–269. DOI: 10/cvdq. (*Scopus, WoS*).

22. Astapenya V. M., **Sokolov V. Yu.** Experimental Evaluation of the Shading Effect of Accelerating Lens in Azimuth Plane. *Antenna Theory and Techniques* : in XI Int. Conf., 24–27 May 2017. Kyiv : IEEE, 2017. P. 389–391. DOI: 10/cvdp. (*Scopus, WoS*).

23. **Sokolov V. Yu.**, Carlsson A., Kuzminykh I. Scheme for Dynamic Channel Allocation with Interference Reduction in Wireless Sensor Network. *Problems of Informatics. Science and Technology (PIC S&T)* : in IV Int. Sc. and Pract. Conf., 10–13 Oct. 2017. Kharkiv : IEEE, 2017. P. 564–568. DOI: 10/gc8w52. (*Scopus, WoS*).

24. 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)* : in V Int. Sc. and Pract. Conf., 9–12 Oct. 2018. Kharkiv : IEEE, 2018. P. 581–585. DOI: 10/c4xt. (*Scopus, WoS*).

Тези наукових доповідей:

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

26. **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)* : матеріали VII Міжнар. н.-т. конф., 10–14 жовтня 2011 р. Київ : ДУТ, 2011. С. 212–215.

27. **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.

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

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* : матеріали VIII Міжнар. н.-т. конф., 1–5 жовтня 2012 р. Київ : ДУТ, 2012. С. 230–232.

30. 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 : ESIS SUT, 2015. P. 164.

31. 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. н.-т. конф., 17–20 лист. 2015 р. Київ : ДУТ, 2015. С. 67–71.

32. 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 : ESIS SUT, 2015. P. 41.

33. 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 : ESIS SUT, 2016. P. 32.

34. Бурячок В. Л., **Соколов В. Ю.** Технологія забезпечення об'єктивного контролю захищеності корпоративних інформаційно-телекомунікаційних систем і мереж. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : матеріали Всеукр. н.-пр. конф., 23 лист. 2018 р. Харків : ХНУВС, 2018. С. 242–247.

35. **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. н.-пр. конф., 27–29 лист. 2018 р. Кропивницький : ЦНТУ, 2018. С. 361–363. DOI: 10/c4xs.

АНОТАЦІЯ

Соколов В. Ю. **Методи і засоби підвищення інформаційної та функціональної безпеки безпроводових мереж передавання даних.** – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.13.06 «Інформаційні технології». Інститут телекомунікацій і глобального інформаційного простору НАН України, Київ, 2019.

Дисертація робота присвячена вирішенню актуальної науково-практичної проблеми розробки методів забезпечення інформаційної і функціональної безпеки безпроводової інфраструктури на основі апаратного розділення абонентів для підвищення рівня її захищеності від загроз безпеці різноманітного характеру, що полягають у розроблених теоретичних основах, методах, моделях та засобах забезпечення надійної роботи безпроводових систем та мереж.

У роботі запропоновано методи модифікованої прямокутної квадратурної амплітудної модуляції для зменшення взаємного впливу безпроводових мереж, адаптивного підбору вільних каналів передавання даних в безпроводових мережах з використанням аналізаторів спектру, підвищення функціональної безпеки безпроводової інфраструктури і комплексної оцінки стану систем її захисту від впливу техногенних та антропогенних. Проведено експериментальні дослідження сучасного стану безпроводових технологій, взаємний вплив безпроводових мереж, ефективності мініатюрних аналізаторів спектру та роботоспроможності прискорюючої лінзи для багатопробенеєвих систем, а також її затемнення і поляризаційні властивості. Розроблені нові моделі аналізаторів спектру, система моніторингу вільних каналів, прискорююча лінзова антена для багатопробенеєвих систем.

Ключові слова: безпроводова інфраструктура, інтернет речей, сигнальне сузір'я, електромагнітна сумісність, адаптивний підбір каналів, аналізатор спектру, надійність, доступність, цілісність, ефективність, прискорююча лінза, поляризація, пропускна здатність, інформаційна безпека, функціональна безпека.

ABSTRACT

Sokolov V. Yu. Methods and Means of Enhancing Information and Functional Security of Wireless Data Networks. – Manuscript.

The dissertation for the degree of a candidate of technical sciences on the specialty 05.13.06 "Information technologies." Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, Kyiv, 2019.

The dissertation is devoted to the actual scientific and practical problem of developing methods for guaranteeing the reliability and functional safety of wireless infrastructure on based on hardware division of subscribers to increase its level of protection against security threats of diverse nature consisting of the developed theoretical foundations, methods, models and means of reliable wireless systems and networks.

The dissertation proposes methods of modified rectangular quadrature amplitude modulation to reduce the mutual influence of wireless networks, adaptive selection of free transmission channels in wireless networks using spectrum analyzers, increase of functional security in wireless infrastructure and a comprehensive assessment of the state of its protection systems against the anthropogenic effects. Experimental studies of the current state of wireless technologies, the mutual influence of wireless networks, the efficiency of miniature spectrum analyzers and the efficiency of the accelerating lens for multiprocessing systems, as well as its dimming and polarization properties have been carried out. New models of spectrum analyzers, free channel monitoring system, accelerating lens antenna for multiprocessing systems have been developed.

Keywords: wireless infrastructure, internet of things, constellation diagram, electromagnetic compatibility, adaptive channel selection, spectrum analyzer, reliability, availability, integrity, efficiency, accelerating lens, polarization, bandwidth, informational security, functional security.

Підписано до друку 16.09.2019. Папір офсетний. Ум.-др. арк. 0,9.
Формат 60×90/16. Наклад 110 прим. Замовлення №1561.

Суб'єкт видавничої діяльності занесено до державного реєстру №620049 від 13.10.2008
ПРІНТЦЕНТР, м. Київ, вул. Політехнічна, 16