ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Мухаммед Кадім Абдул-Хуссейн

УДК 621.396

РОЗВИТОК МЕТОДІВ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ Wi-Fi КАНАЛІВ ЗВ'ЯЗКУ НА ФІЗИЧНОМУ РІВНІ

05.12.17 – радіотехнічні та телевізійні системи

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2013

Дисертацією є рукопис.

Роботу виконано в Харківському національному університеті радіоелектроніки Міністерства освіти і науки України.

Науковий керівник: кандидат технічних наук, доцент **Стрельницький Олексій Олександрович**, Харківський національний університет радіоелектроніки МОН України, доцент кафедри основ радіотехніки

Офіційні опоненти: доктор технічних наук, професор **Обод Іван Іванович**, Національний технічний університет «ХПІ» МОН України, професор кафедри систем інформації

кандидат технічних наук, доцент **Чесановський Іван Іванович**, Хмельницький національний університету МОН України, доцент кафедри радіотехніки та зв'язку

Захист відбудеться "10" грудня 2013 р. о 15:00 годині на засіданні спеціалізованої вченої ради Д 64.052.03 в Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, проспект Леніна, 14, ауд. № 13.

З дисертацією можна ознайомитись у бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, проспект Леніна, 14.

Автореферат розіслано "8" листопада 2013 року.

Вчений секретар
спеціалізованої вченої ради, проф., д.т.н. _____ Безрук В.М.

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Сучасне людство будує глобальну інформаційну спільноту, матеріальним носієм якої є інформаційно-комунікаційні технології та системи, включаючи безпроводові системи зв'язку. У зв'язку з цим, питання безпеки каналів зв'язку в цих системах виходять на перший план при подальшому розвитку безпроводових технологій. Для безпроводових цифрових систем передачі інформації (ЦСПІ), таких як IEEE 802.11x (Wi-Fi), основними проблемами безпеки є: моніторинг та перехоплення трафіку, атаки типу «відмова в обслуговуванні», підключення до мережі неавторизованих клієнтів. Сервіс хмарних обчислень може стати дуже потужним засобом для злому найбільш захищених безпроводових мереж. Важко обмежити фізичний доступ зловмисників до мережі через те, що неможливо ефективно екранувати всі приміщення, в яких встановлені точки доступу Wi-Fi, тому частково мережі діють і ззовні. Все це – негативні сторони безпечного використання Wi-Fi технологій, що ставить під загрозу безпеку безпроводових мереж як окремих компаній, так і домашніх користувачів.

У роботі під легітимним розуміється такий канал зв'язку, який утворений передавачем та приймачем системи зв'язку. Під відвідним – канал зв'язку, утворений передавачем системи зв'язку та приймачем-виявником. Під захищеністю каналів зв'язку матимемо на увазі енергетичну прихованість та завадозахищеність. Захищеність каналів з квазістатичним загасанням досліджувалась в роботах вчених НТУУ «КПІ», Прінстонського університету, Санкт-Петербурзького державного університету телекомунікацій та Массачусетського університету, де як критерії оцінки рівня прихованості використовувалась ймовірність виявлення легітимного каналу та гранична секретна продуктивність (різниця продуктивності в легітимному та продуктивності в відвідному канал зв'язку). Однак у публікаціях цих вчених викладено моделі аналізу захищеності, які не враховують вплив на її рівень електродинамічних характеристик антен та розсіювачів легітимного та відвідного каналів, а також різноманітність механізмів поширення радіохвиль (ПРХ). Наближений характер носить і метод побудови зони виявлення, величина площі якої є загальноприйнятою мірою прихованості легітимного каналу, що перешкоджає розробці ефективних способів забезпечення захищеності каналів зв'язку на фізичному та канальному рівнях моделі OSI. Такі способи в даний час відомі, але для їх практичного здійснення потрібно залучення протоколів вищих рівнів, що надто ускладнює завдання підвищення захищеності. Отже, відсутність цілісної теорії, яка дозволяє визначити можливості та раціональні шляхи побудови релеєвських каналів зв'язку з високим рівнем енергетичної прихованості, є стримуючим фактором у їх розвитку.

Тому актуальною є тема дисертаційних досліджень, спрямованих на розробку методів підвищення захищеності Wi-Fi каналів зв'язку на фізичному рівні, які враховують вплив електродинамічних характеристик антен та механізмів ПРХ на рівень ймовірності виявлення та граничної секретної продуктивності.

Зв’язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження пов'язані з виконанням госпдоговірної НДР, що виконувалась згідно з тематичним планом МОН України: №260 «Дослідження потенційних можливостей

ефективного функціонування мережних реконфігурованих інформаційно-вимірювальних систем екологічного моніторингу», № ДР 0111U002903.

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення захищеності Wi-Fi каналів зв'язку за рахунок застосування моделей та методів, що більш повно враховують особливості функціонування релеєвських радіоканалів на першому та другому рівнях моделі OSI.

Для досягнення поставленої мети вирішуються такі наукові завдання:

– удосконалення моделей каналу зв'язку для оцінки рівня захищеності за величинами ймовірності виявлення та секретної продуктивності з урахуванням впливу електродинамічних характеристик антен та розсіювачів легітимного і нелегітимного каналів, та механізмів поширення в них радіохвиль в будь-якій із зон випромінювання;

– проведення чисельних експериментів за допомогою удосконалених моделей, визначення раніше невідомих характеристик прихованості реальних релеєвських каналів з технологією Wi-Fi, експериментальний доказ достовірності розроблених моделей;

– розробка методу побудови зон виявлення (ЗВ) із застосуванням удосконалених моделей та його верифікація, чисельні дослідження ЗВ релеєвських Wi-Fi каналів з різноманітними середовищами ПРХ;

– розробка із застосуванням запропонованих моделей та методу нового способу роботи легітимного каналу під «штучним шумом» з метою збільшення його захищеності на фізичному та канальному рівнях моделі OSI без застосування криптоалгоритмів.

Об’єктом дослідження є процес прихованого передавання мультимедійної інформації релеєвським каналом зв'язку з квазістатичним загасанням.

Предметом дослідження є методи та засоби підвищення захищеності релеєвських каналів зв'язку локальних мереж.

Методи досліджень – при вирішенні поставлених задач використовувались основні положення теорії поширення радіохвиль і цифрового зв'язку, методи математичного моделювання, а також методи експериментальних досліджень радіоканалів ЦСПІ. Експериментально перевірялась і можливість застосування на практиці запропонованого способу роботи каналу під «штучним шумом». В основу запропонованих досліджень покладено концепцію відвідного каналу Вайнера.

Наукова новизна отриманих результатів полягає в наступному:

1. Розроблено нову модель релеєвських каналів зв'язку для визначення рівня їх прихованості та завадозахищеності, в якій вперше, виходячи з поняття секретної продуктивності, отримано аналітичний вираз для розрахунку імовірності виявлення легітимного каналу ЦСПІ. На відміну від відомих, у виразі враховано зв'язок ймовірності виявлення з розмірами апертур антен каналів зв'язку, їх взаємного розташування та залежність від того чи іншого механізму поширення радіохвиль.

2. Набув подальшого розвитку теоретико-експериментальний метод побудови зон виявлення, характерною особливістю якого є розрахунок за розробленою моделлю, кривої постійної ймовірності виявлення в координатах радіус – кут при відомих характеристиках каналів зв'язку.

3. Вперше запропоновано та теоретично обґрунтовано новий метод підвищення рівня прихованості каналів зв'язку за рахунок їх роботи під «штучним шумом». На відміну від відомих, розроблений метод не використовує криптоалгоритми, а базується на застосуванні в генераторах шуму антен, що створюють «нуль» випромінювання в напрямку легітимного модему та максимальну інтенсивність шуму у всіх інших напрямках.

Практичне значення отриманих результатів

1. Отримано нові експериментальні дані про кутові залежності інтенсивності поля антен ряду Wi-Fi пристроїв (точок доступу, клієнтських адаптерів і т.д.), які можуть бути використані при практичній розробці радіоканалів з Wi-Fi технологією.

2. Виміряно раніше невідомі дані про ймовірності виявлення легітимних Wi-Fi каналів у приміщенні та на відкритому просторі в ближній, проміжній і дальній зонах.

3. Розроблено та експериментально випробувано пристрій, що реалізує запропонований метод роботи системи під «штучним шумом». Результати вимірювань запроваджені в ТОВ «ТК АЙ ПІ СИСТЕМС», яке надає послуги доступу до мережі Інтернет, при частотно-територіальному плануванні мережі рівня LAN у м. Харкові (є відповідний акт впровадження). Крім того, матеріали дисертації використовуються в навчальному процесі кафедри ОРТ ХНУРЕ. На основі дисертації написано конспект лекцій та поставлено цикл лабораторних робіт з курсу «Захист інформації в системах з радіодоступом» для магістрів та спеціалістів випуску 2013р. (є акт про впровадження).

Обґрунтованість та достовірність результатів дисертаційної роботи зумовлена коректним використанням апробованих математичних методів теорії електродинаміки, поширення радіохвиль та цифрового зв'язку, а також позитивними результатами порівняння даних натурних експериментів та розрахунків за запропонованими аналітичними співвідношеннями.

Особистий внесок здобувача. Основні наукові результати, наведені в дисертаційній роботі, отримані здобувачем самостійно. У роботах, опублікованих у співавторстві, здобувачем виконано такі дослідження: запропоновано підхід до моделювання і принцип вимірювання загасань та характеристик спрямованості антен в радіоканалах локальних систем зв’язку [1, 4, 10]; запропоновано варіант моделі розрахунку ймовірності виявлення радіоканалу локальної мережі зв’язку [2, 6, 14]; проведено чисельні та натурні експерименти [3, 7, 11, 12, 13]; створено експериментальні установки [5, 8, 9].

Апробація результатів дисертації. Результати дисертації представлені та обговорені на таких конференціях міжнародного та республіканського рівня: 6-а Міжнародна науково-практична конференція «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій» (м. Запоріжжя, 2012 р.); 12-а, 13-а Міжнародні науково-технічні конференції «Сучасні інформаційні та електронні технології» (м. Одеса, 2011, 2012 рр.); IV-й Міжнародний радіоелектронний Форум (МРФ-2011) «Прикладна радіоелектроніка. Стан та перспективи розвитку» (м. Харків, 2011 р.); 11-та Міжнародна науково-технічна конференція «Сучасні проблеми радіоелектроніки, телекомунікації та комп’ютерної інженерії (TCSET’2012)» (м. Львів, 2012 р.).

Публікації. Матеріали дисертаційної роботи опубліковано в 7 статтях, виданих у збірниках, що входять до переліку ВАК України, а також у 7-ох тезах доповідей Міжнародних конференцій.

Структура дисертаційної роботи. Дисертація складається із вступу, 4 розділів, висновків, списку використаних джерел 74 найменувань і додатку. Повний обсяг роботи становить 132 сторінки, у тому числі: 82 рисунки (з них рисунки на окремих сторінках займають 15 сторінок), 5 таблиць, список використаних джерел на 9 сторінках і додаток на 2 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі обґрунтовано актуальність теми дисертації, сформульовано мету та задачі досліджень. Визначено наукову новизну роботи та її практичне значення. Наведено дані про особистий внесок автора в роботах, виконаних у співавторстві, апробацію результатів дисертації та відомості про публікації за темою дисертації.

У першому розділі дисертації проведено аналітичний огляд існуючих методів аналізу рівня прихованості багатопроменевих каналів зв'язку рівня LAN. Викладено основну суть двох відомих підходів до оцінки рівня енергетичної прихованості, що базуються на критеріях Неймана-Пірсона, та нульовій секретній продуктивності. Останній з них, як більш адекватний обраній теоретичній основі роботи – концепції відвідного каналу, більш детально описано як для SISO, так і для MIMO технологій.

З представленого огляду зроблено такі висновки: безпроводові канали рівня LAN є багатопроменевими та описуються релеєвською моделлю квазістатичного загасання; найбільш придатною для подальших досліджень та удосконалень є модель, котра грунтується на концепції відвідного каналу; наразі слабо розвинені методи технічного захисту інформації в безпроводових каналах, а відомі методи роботи «під шумом» складні в реалізації та для їх широкого практичного застосування потребують спрощення. Вихід із цього становища полягає в необхідності розробки власної наближеної математичної моделі та технічного рішення, які при незначних часових та фінансових витратах дозволять підвищити захищеність Wi-Fi мереж на фізичному рівні.

У **другому розділі** запропоновано удосконалені моделі аналізу рівня енергетичної скритності SISO релеєвського каналу зв'язку. На початку розділу запропоновано варіант моделі розрахунку ймовірності виявлення радіоканалу локальної мережі зв'язку.

На рис. 1 представлена ЦСПІ з відвідним каналом (ВК) у вигляді трьох взаємодіючих апертур. Дві з них утворюють легітимний багатопроменевий канал. Передавальна апертура є сферою з діаметром a, всередині якої знаходяться як випромінювачі, так і розсіювачі. Наявність розсіювачів дозволяє збільшити кількість каналів передавання інформації в MIMO системах. Приймальна апертура легітимного каналу має розмір $a_л$. Відвідний багатопроменевий канал розташовується по відношенню до осі легітимного каналу під кутом γ і має приймальну апертуру з розміром $a_о$. У легітимному каналі апертури віддалені на відстань $r_л$, а у відвідному – на відстань $r_о$.

Для такої системи отримано вираз, що визначає ймовірність виявлення $P_{об}$:

$$P_{об} = 1 - \frac{(S/N)_л}{(S/N)_л + 2^{R_s}\cdot(S/N)_o}\cdot e^{-\frac{2^{R_s}-1}{(S/N)_л}} = 1 - \frac{1}{1+2^{R_s}\cdot(S/N)_o/(S/N)_л}\cdot e^{-\frac{2^{R_s}-1}{(S/N)_л}}, \quad (1)$$

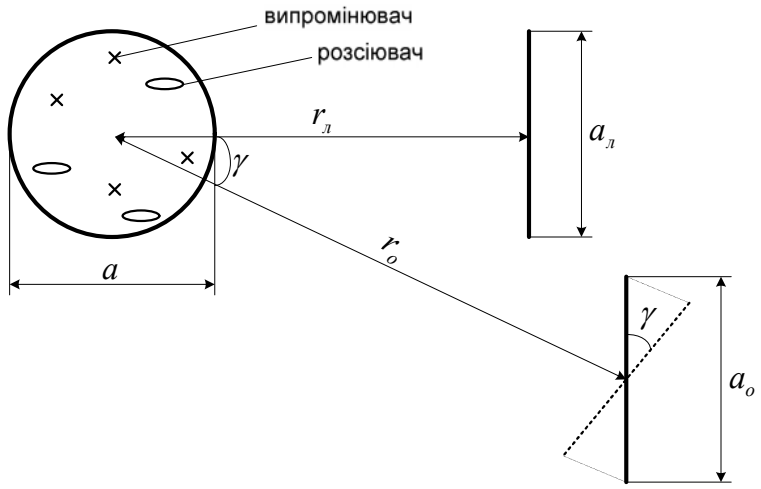

Рис. 1. Еквівалентне подання ЦСПІ з ВК

де $(S/N)_л$ і $(S/N)_o$ – відношення сигнал / шум в легітимному та відвідному каналу відповідно, R_s – секретна швидкість, нормована до продуктивності каналу з білим шумом при заданому середньому значенні сигнал/шум.

З формули Найквіста та теореми Шеннона отримано співвідношення для визначення кількості просторових каналів, необхідних при передаванні інформації із заданим відношенням *S/N*:

$$C = 2\cdot\log_2 M, \quad (2) \qquad C = \log_2(1+SNR), \quad (3)$$

де C – продуктивність ЦСПІ, M – кількість дискретних сигналів, необхідних для передавання інформації із заданою продуктивністю. Далі вважалося, що для передавання M дискретних сигналів потрібно M помітних просторових каналів. На цій підставі, прирівнявши праві частини виразів (2) та (3) отримано рівняння: $S/N = M^2 - 1,$ яке дозволяє визначити необхідне число M при заданій величині *S/N*. Числа $M_л$ й M_o для легітимного та відвідного каналів можна записати через геометричні параметри ЦСПІ:

$$M_л = (\ /\ _л)\cdot(\ _л/\lambda), \quad (4) \qquad M_o = (\ /\ _o)\cdot(\ _o/\lambda)\cdot\cos\gamma, \quad (5)$$

де λ – довжина хвилі.

Тепер з (4-5) маємо такі співвідношення:

$$(S/N)_л = \left[(\ /\ _л)\cdot(\ _л/\lambda)\right]^2 - 1, \quad (6) \qquad (S/N)_o = \left[(\ /\ _o)\cdot(\ _o/\lambda)\cdot\cos\gamma\right]^2 - 1. \quad (7)$$

Підставивши вирази (6) та (7) у формулу (1), було отримано:

$$P_{об} = 1 - \left(1\Big/1 + 2^{R_s}\frac{\left(a\cdot a_o\cdot\cos\gamma/r_o\cdot\lambda\right)^2 - 1}{\left(a\cdot a_л/r_л\cdot\lambda\right)^2 - 1}\right)\cdot e^{\left[-\frac{2^{R_s}-1}{(a\cdot a_л/r_л\cdot\lambda)^2-1}\right]}. \quad (8)$$

Формули (6)-(8) у явному вигляді відображують залежність параметрів *(S/N)* та $P_{об}$ від геометричних розмірів апертур антен ЦСПІ *a, $a_л$* і відвідного каналу a_o, а також їх взаємного розташування (розміри $r_л$, r_o і кут γ). Аналізуючи вираз (6) неважко зробити такі рекомендації. Необхідне співвідношення сигнал/шум у легітимному каналі забезпечується вибором відповідних розмірів приймальної апертури $a_л/\lambda$ та величини заповнення траси радіоканалу розсіювачами, тобто залежить від відношення $a/r_л$. З погляду зловмисника ефективна робота відвідного каналу також забезпечується наявністю великої кількості розсіювачів уздовж траси завдовжки r_o та значними розмірами апертури відвідного каналу a_o/λ.

Викликає практичний інтерес вивчення впливу відношення $r_o/r_л$ на величину $P_{об}$. Вважаючи, що виконуються такі нерівності:

$$\left((a/r_o)\cdot(a_o/\lambda)\cdot\cos\gamma\right)^2 >> 1, \qquad (9) \qquad \left((a/r_л)\cdot(a_л/\lambda)\right)^2 >> 1, \qquad (10)$$

формулу (8) можна записати в такому вигляді:

$$P_{об} = 1 - \frac{1}{1+2^{R_s}\cdot\left(\frac{r_o}{r_л}\right)^{-1}\cdot\frac{a_o}{a_л}\cos\gamma}\cdot e^{\left[-\frac{2^{R_s}-1}{\left(\frac{a}{r_л}\right)^2\cdot\left(\frac{a_л}{\lambda}\right)^2-1}\right]} = 1 - \frac{1-\left[\left(2^{R_s}-1\right)\Big/\left(\frac{a\cdot a_л}{r_л\cdot\lambda}\right)^2\right]}{1+2^{R_s}\cdot\left(\frac{r_o}{r_л}\right)^{-1}\cdot\frac{a_o}{a_л}\cos\gamma}. \qquad (11)$$

Останній запис у виразі (11) отримано в результаті подання $\exp(\bullet)$ у вигляді суми перших двох членів ряду Тейлора. З аналізу виразу (11) виходить, що при виконанні умови (10) величина заповнюваності розсіювачами траси уздовж легітимного каналу $a/r_л$ практично не позначується на значенні $P_{об}$ і одним з основних факторів, що визначають величину ймовірності виявлення, є відношення $r_o/r_л$. Цей висновок підтверджений результатами розрахунків. Якщо прийняти, що впевнене виявлення сигналів ЦСПІ можливе при $P_{об} \ge 0,7$, то можна провести такий аналіз отриманих результатів. Сигнали ЦСПІ можуть бути виявлені при секретній швидкості $R_s \ge 2$ практично при будь-яких співвідношеннях $r_л/r_o$. При цьому розміри апертури випромінювача відвідного каналу a_o мають бути не менше 4λ, а співвідношення $a/r_o > 0,35$.

Ступінь безпеки функціонування Wi-Fi радіоканалів оцінюється ймовірністю виявлення $P_{об}$ за допомогою приймача-виявляча зловмисника. У працях багатьох вчених показано, що величина $P_{об}$ залежить від умов поширення радіохвиль. Однак при моделюванні в них використовувалася степенева модель ПРХ, яка не враховує специфіки роботи Wi-Fi радіоканалів. У роботі описуються результати теоретичних та експериментальних досліджень, що доводять можливість застосування наближених моделей, котрі грунтуються на відбивному трактуванні, для прогнозування загасань широкосмугових сигналів у будь-якій зоні випромінювання багатопроменевих радіоліній як для закритого приміщення, так і для відкритого простору.

У виразі (1) співвідношення сигнал/шум було представлено в наступному вигляді:

$$(S/N)_л = S(r_л, \theta_1, \theta_2)/N(r_л, \theta_2), \qquad (12) \qquad (S/N)_o = S(r_o, \theta_1, \theta_3)/N(r_o, \theta_3), \qquad (13)$$

де $r_л$, r_o – відстань від антени передавача до антен приймачів легітимного та відвідного каналів відповідно, θ_1, θ_2, θ_3 – кути напрямку максимумів кутової інтенсивності напруженості поля передавальної антени $F_П(r_л,\theta_1)$ і приймальних антен легітимного $F_л(r_л,\theta_2)$ та відвідного $F_o(r_л,\theta_3)$ каналів.

Тоді вирази (12) та (13) було записано так:

$$S(r_л, \theta_1, \theta_2)/N(r_л, \theta_2) = S(r_э)/N(r_э)\cdot\alpha\left(r_э/r_л\right)\cdot F_П^2(r_л, \theta_1)\cdot F_л^2(r_л, \theta_2), \qquad (14)$$

$$S(r_o, \theta_1, \theta_3)/N(r_o, \theta_3) = S(r_э)/N(r_э)\cdot\alpha\left(r_э/r_o\right)\cdot F_П^2(r_o, \theta_1)\cdot F_o^2(r_o, \theta_3). \qquad (15)$$

Далі було припущено, що при будь-яких відстанях $r_л$, $r_о$. інтенсивності $F_П(r_л,\theta_1)$, $F_л(r_л,\theta_2)$, $F_о(r_л,\theta_3)$ не залежать від кутових координат. Тоді вираз (1) було перетворено до наступного вигляду:

$$P_{об} = 1 - \left(\exp\left[-2^{R_s} - 1/(S/N)_л \right] \Big/ 1 + 2^{R_s} \cdot (\alpha_о / \alpha_л) \right). \qquad (16)$$

Вираз (16) дозволяє досліджувати залежність величини $P_{об}$ від значень $a_о$ й $a_л$, тобто і від умов ПРХ у легітимному та відвідному каналах. За її допомогою було проведено розрахунки, результати яких представлені на рис. 2. Тут показано залежності $P_{об}(R_s)$ при $(S/N)_л = 20$ дБ і різних значеннях $r_л/r_о$ для відкритого простору та приміщення. З наведених даних виходить, що у випадку приміщення умови виявлення погіршуються й критерій $P_{об}$ >0,7 реалізується при більших значеннях $r_л/r_о$, ніж у далекій зоні, при тих самих величинах R_s. Отже, чим далі знаходиться приймач-виявляч від передавача порівнянно з легітимним приймачем, тим при рівних значеннях $r_л/r_о$ та R_s у близькій зоні відкритого простору співвідношення $a_о/a_л$ буде більше, ніж у далекій зоні, а значить і величина $P_{об}$ буде більше. З цього виходить, що відмінності в умовах ПРХ суттєво впливають на величину $P_{об}$.

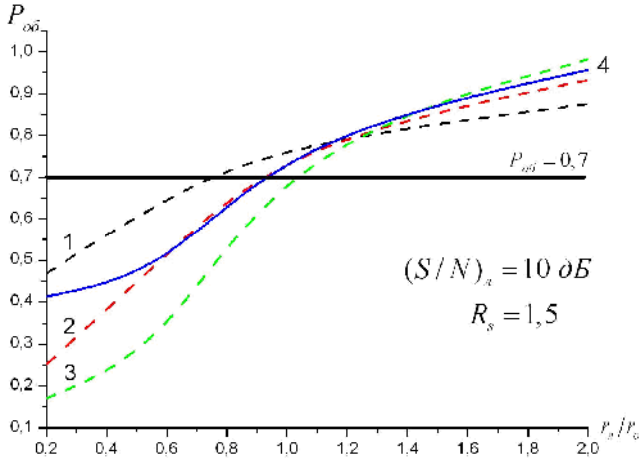

Рис. 2. Результати числових досліджень $P_{об}$

Це наочно проілюстровано на рис. 2. Криві 1-3 відповідають умовам ПРХ на відкритому просторі (1 – у далекій зоні, 2 – у проміжній зоні, 3 – у близькій зоні), крива 4 – у приміщенні. Отримані дані є новими та дозволяють визначити умови, при яких $P_{об} \geq 0,7$, що відповідає критерію впевненого виявлення сигналів ЦСПІ. З метою доказу вірогідності розробленої моделі виявлення проводились експериментальні дослідження. Порівнювались розрахункові значення $P_{об}$ та виміряні. Експериментальні величини $P_{об}$ були отримані на підставі вимірювання рівнів сигналів $P_л$ і $P_о$ в легітимному та відвідному каналах і підстановки їх у вираз

$$P_{об} = 1 - \left(\exp\left[-2^{R_s} - 1/(S/N)_л \right] \Big/ 1 + 2^{R_s} \cdot (\ _о / \ _л) \right). \qquad (17)$$

Вираз (17) отримано із (14) у припущенні, що шуми в легітимному та відвідному каналах однакові. Для вимірювання величин $P_л$ і $P_о$ використовувалося Wi-Fi обладнання, а для представлення інформації про рівні сигналів використовувалося спеціалізоване програмне забезпечення. У тих самих умовах вимірювання проводилися десять разів із наступним обробленням (визначення середнього значення й довірчих інтервалів). Для оброблення отриманих даних використовувався розподіл Стьюдента при довірчій імовірності $p = 0,95$. Спочатку досліди виконувалися в лабораторії ХНУРЕ. Результати вимірювань і розрахунків кривих $P_{об}(r_л/r_о)$ для випадку приміщення наведено на рис. 3. Вимірювання проводилися при $R_s = 2$, $r_л = 6$ м і $(S/N)_л = 32$ дБ.

Аналогічні вимірювання були проведені й на відкритому просторі. Досліди виконувалися на стадіоні університету. З аналізу представлених результатів можна зробити наступне. Теоретичні криві в основному знаходяться в границях кривих довірчих інтервалів. Однак самі границі, розраховані при ймовірності 0,95, досить широкі (через малу кількість вимірювань), що дозволяє зробити висновок про те, що розроблені моделі можна використовувати лише для оцінки, а не точного визначення ймовірності виявлення функціонування каналу зв'язку.

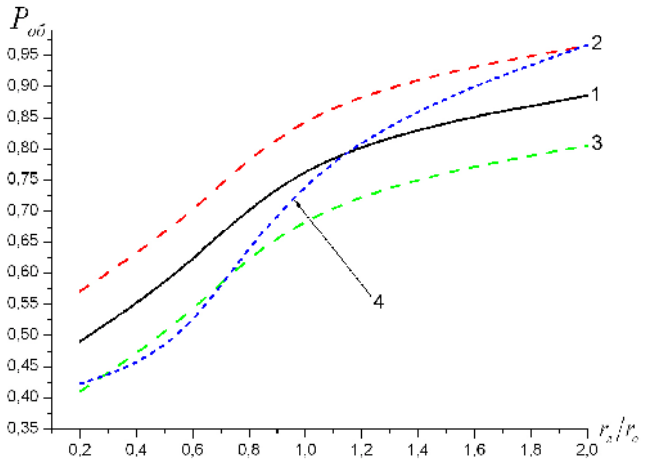

Рис. 3. Результати вимірювання величини $P_{об}$ у приміщенні (1 – виміряна крива; 2, 3 – довірчий інтервал; 4 – теоретична крива)

У літературі показано, що при заданій ймовірності виявлення $P_{об}$ гранична секретна продуктивність $C_{пр}$ визначається в такий спосіб:

$$C_{пр}(\ _{об}) = \log_2\left(\left[(\overline{\ } / \overline{\ })_л \cdot\ _{об} + 1\right] \Big/ \left[(\overline{\ } / \overline{\ })_o \cdot (1 -\ _{об}) + 1\right]\right). \qquad (18)$$

Використовуючи формули (2), (3), вираз (18) для $C_{пр}$ було записано з урахуванням впливу розмірів та взаємного розташування апертур антен легітимного і відвідного каналів на граничну секретну продуктивність:

$$C_{пр}(\ _{об}) = \log_2\left(\left[\left(\frac{a \cdot a_л}{r_л \cdot \lambda}\right)^2 - 1\right] \cdot\ _{об} + 1 \Big/ \left[\left(\frac{a \cdot a_o}{r_o \cdot \lambda} \cdot \cos\gamma\right)^2 - 1\right] \cdot (1 -\ _{об}) + 1\right). \qquad (19)$$

Розрахунки за формулою (19) при $P_{об} = 0{,}7$ дали результати, з аналізу яких можна визначити умови, при яких ЦСПІ стає розсекреченою. Одна з таких умов – це $a_o \approx 1{,}5 \cdot a$ при $\gamma = 0^\circ$ та $a_o \approx 2 \cdot a$ при $\gamma = 40^\circ$. Інша умова – $r_л \approx 1{,}5 \cdot r_o$ при $\gamma = 0^\circ$ та $r_л \approx 2 \cdot r_o$ при $\gamma = 40^\circ$.

Третій розділ присвячено методу розрахунку границь зон виявлення функціонування релеєвського радіоканалу з квазістатичними завмираннями за двома критеріями: $P_{об} = 0{,}7$ та $C_{пр} = 0$. Метод базується на застосуванні моделей, описаних у розділі 2. В ньому наводяться приклади розрахунків границь зон виявлення багатопроменевого каналу Wi-Fi при його роботі як на відкритому просторі, так і в приміщенні.

Співвідношення сигнал/шум у формулі (1) було представлено в наступному вигляді: $(S/N)_л = S(r_л, \theta_1, \theta_2)/N(r_л, \theta_2)$ та $(S/N)_o = S(r_o, \theta_1, \theta_3)/N(r_o, \theta_3)$, де $r_л$, r_o – відстань від антени передавача до антен приймачів легітимного та відвідного каналів відповідно, θ_1, θ_2, θ_3 – поточні кути відліків значень ненормованих кутових інтенсивностей напруженості поля передавальної антени $F_П(r_л, \theta_1)$ та приймальних антен легітимного $F_л(r_л, \theta_2)$ та відвідного $F_o(r_o, \theta_3)$ каналів у місцевій системі координат. Тоді:

$$S(r_л, \theta_1, \theta_2)/N(r_л, \theta_2) = S(r_э)/N(r_э) \cdot \alpha\left(r_н/r_л\right) \cdot F_П^2(r_л, \theta_1) \cdot F_л^2(r_л, \theta_2), \quad (20)$$

$$S(r_o, \theta_1, \theta_3)/N(r_o, \theta_3) = S(r_э)/N(r_э) \cdot \alpha\left(r_н/r_o\right) \cdot F_П^2(r_o, \theta_1) \cdot F_o^2(r_o, \theta_3), \quad (21)$$

де $S(r_э)/N(r_э)$ – експериментально виміряне на еталонній відстані $r_э$ співвідношення сигнал/шум в максимумі інтенсивності випромінювання; $\alpha\left(r_н/r_л\right), \alpha\left(r_н/r_o\right)$ – функціональні залежності загасання сигналу в легітимному та відвідному каналах: через $r_н$ у виразах (20), (21) позначено відстань $r_э$, $r_в$ – відстань, з якої починає виконуватися формула Введенського. Вирази (20), (21) записано з урахуванням спрощуючого припущення, що при всіх значеннях r та θ_2, θ_3 шумова температура антен не змінюється і приблизно дорівнює $290^\circ K$.

Відомо, що зі зміною відстані r в межах ближньої зони та зони Френеля змінюються і кутові залежності інтенсивностей полів $F_л^2(r_л, \theta_2), F_o^2(r_o, \theta_3)$. Ця обставина суттєво ускладнює процес визначення відношення S/N. Для його спрощення пропонувалося застосувати ще одне наближення, суть якого полягає в тому, що в межах кожної із зон випромінювання кутові залежності інтенсивності поля (КЗІП) приймаються постійними. Введене наближення дозволило значно спростити вирази (20), (21). З урахуванням зроблених наближень остаточний вираз для розрахунку ймовірності виявлення набуло такого вигляду:

$$P_{об} = 1 - \left[\exp\left(-\frac{2^{R_s} - 1}{(S/N)_л} \right) \Big/ \left(1 + 2^{R_s} \cdot \frac{\alpha_o}{\alpha_л} \cdot \frac{F_o^2(r_o, \theta_3) \cdot F_П^2(r_o, \theta_1)}{F_л^2(r_л, \theta_2) \cdot F_П^2(r_л, \theta_1)} \right) \right]. \quad (22)$$

Скориставшись поняттям кривих постійної ймовірності виявлення $P_{об}(r, \theta) = const$ та застосувавши вираз (22) були побудовані зони виявлення ЦСПІ. Вони обмежують двовимірний простір на площині (r, θ_3), всередині й на границі якого $P_{об}(r, \theta) \geq 0,7$. Будувалися криві постійної ймовірності виявлення у такий спосіб. Спочатку за формулою (22) розраховувались криві $P_{об} = f(r)$ при різних кутах θ_{3i}. Розраховані криві апроксимувались поліномами, які прирівнювались до заданого значення $P_{об}=0,7$. Для кожного з цих рівнянь знаходились корені $r_1, r_2, r_3, \ldots r_n$. Крива, що проходить через точки $(r_1, \theta_{31}), (r_2, \theta_{32}), \ldots (r_n, \theta_{3n})$, і є кривою постійної ймовірності виявлення.

Викладеним методом можна скористатися і для побудови границі зони виявлення за критерієм $C_{пр} = 0$. Границя цієї зони виявлення обмежує простір, на площині (r, θ_3) всередині й на границі якого радіоканал ще не може бути виявлений. При побудові зон виявлення за критерієм $C_{пр} = 0$ використовувались ті самі наближення, що й при побудові зон виявлення за критерієм $P_{об} = 0,7$.

Правомочність застосування цих наближень обговорюється нижче. Було проведено дослідження, які полягали в експериментальному визначенні КЗІП точок доступу і терміналів ЦСПІ. Значення КЗІП входять до виразу (22), однак визначити їх можна лише експериментально. Це було показано на прикладі КЗІП обладнання Wi-Fi радіоканалу, експерименти проводилися у антенній лабораторії ХНУРЕ. З отриманих результатів стало ясно, що всі КЗІП мають дуже нерівномірну характеристику як у вертикальній, так і у горизонтальній площині. Також спостерігалась суттєва зміна форми КЗІП та рівня сигналу при переході від одного

частотного каналу до іншого. Чим вище частота робочого каналу, тим сильніше виражена нерівномірність і тим менше абсолютний рівень сигналу. Слід зазначити, що у вертикальній площині провали в діаграмі досягали рівня порядку -70 дБм. Це ставить під сумнів можливість організації роботи мережі при довільному розташуванні її терміналів. У результаті проведених вимірювань зроблено наступні висновки: всі виміряні КЗІП сильно відрізнялися від всеспрямованих; КЗІП точки доступу та ноутбука, схожі за будовою, мали майже рівну кількість пелюсток та «провалів»; ноутбук забезпечував більшу чутливість порівняно з комунікатором та радіокартою. Однак останні мали найменшу нерівномірність КЗІП. Проведені експерименти підтвердили, що КЗІП всіх типів обладнання Wi-Fi каналу мають досить складну конфігурацію і теоретично не можуть бути розраховані. Отримані експериментальні результати були використані при дослідженні зон виявлення легітимного Wi-Fi каналу за критеріями $P_{об} = 0,7$ и $C_{пр} = 0$.

Шляхом чисельних експериментів, з описаною ЦСПІ, досліджувалось питання, як саме орієнтація КЗІП антени приймача-виявляча впливає на розміри зони виявлення за критерієм $P_{об} = 0,7$? Для цього моделювалася ЦСПІ, у якої за передавач та приймачі обох каналів зв'язку використовувалися нетбуки. Передбачалося, що КЗІП антен, що утворюють легітимний канал, були спрямовані один на одного своїми максимумами. Антена відвідного каналу розташовувалася по відношенню до осі легітимного каналу так, що під кутом $\gamma = 30^\circ$ (рис. 1) на передавач був спрямований або максимум, або мінімум її КЗІП. При розрахунках приймалося, що: $(S/N)_л = 20$ дБ, $R_s=2$, $r_л = 12$ м.

У реальних умовах виявлення антена приймача відвідного каналу може перебувати в довільному положенні щодо антени передавача, як за дальністю, так і за кутом. Про вплив місця розташування антени приймача-виявляча на розмір та форму зони виявлення можна судити з порівняння результатів розрахунків, наведених на рис. 4. Тут крива 1 обмежує область виявлення за критерієм $P_{об} = 0,7$ при орієнтації максимуму КЗІП антени відвідного каналу (ВК) на передавач під кутом $\gamma = 30^\circ$. Крива 2 відповідає орієнтації мінімуму її КЗІП на передавач ($\gamma = 30^\circ$). Розрахунки проводилися для реальних умов поширення радіохвиль в умовах приміщення та потужності передавача Wi-Fi $P_\Sigma = 100$. Значення $(S/N)_л$ показані на полях рис. 4. Там само вказані значення довжини траси легітимного каналу $r_л$. Крім того, на полях рисунку наведені відношення площ зон виявлення при орієнтації на передавач максимуму КЗІП антени ВК ($S_{\max}$) та її мінімуму ($S_{\min}$). Площі $S_{\max}$ та $S_{\min}$ визначалися інтегруванням кривих $r(\theta_3)$ в прямокутній системі координат. З порівняння даних, наведених на рис. 4, виходить, що збільшення нерівномірності КЗІП антени приймача-виявляча призводить і до збільшення різниці Δr_o між максимальною та мінімальною відстанню r_o.

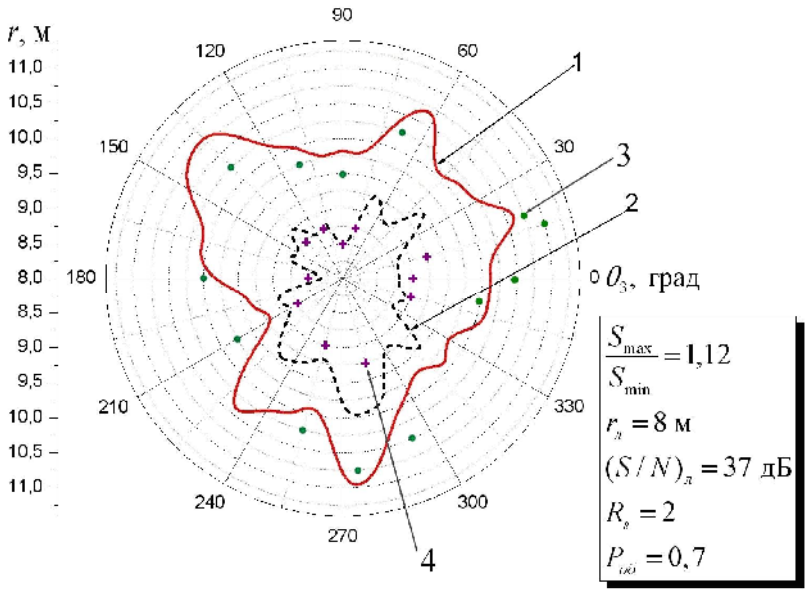

Рис. 4. Зони виявлення ЦСПІ для випадку приміщення та ближньої зони за критерієм $P_{об} = 0,7$

Проаналізувавши всі результати чисельних експериментів, зроблено висновок, що у разі застосування у відвідному каналі слабоспрямованих антен площі зон виявлення при орієнтації на передавач максимуму КЗІП антени ВК ($S_{\max}$) або її мінімуму ($S_{\min}$), сильно не відрізняються. На підставі цього факту зроблено висновок про те, що орієнтація антени відвідного каналу слабо впливає на розміри зони виявлення.

Достовірність викладеного методу побудови зон виявлення за критерієм $P_{об} = 0,7$ перевірялась експериментально. За допомогою ноутбуків було виміряно декілька значень $P_{об}(r,\theta_3)$, які нанесені на рис. 4. На рис. 4 точками 3 позначені результати вимірювань $P_{об}(r,\theta_3)$ при спрямуванні максимуму КЗІП антени відвідного каналу на передавач, хрестиками 4 – оцінка $P_{об}(r,\theta_3)$ при спрямуванні на передавач її мінімуму. Між кривими постійної продуктивності та даними натурного експерименту спостерігалася гарна узгодженість. На підставі цього факту зроблено висновок, що розроблений метод можна застосовувати при проектуванні ЦСПІ із заданим рівнем ймовірності виявлення.

Далі в роботі проведено розрахунки за допомогою запропонованого в розділі методу границі зон виявлення за критерієм $C_{пр} = 0$. Розглядалися ті самі приклади багатопроменевих каналів, для яких досліджувалися і зони виявлення за критерієм $P_{об} = 0,7$. Розрахунки проводилися для реальних умов поширення радіохвиль в умовах приміщення та відкритого простору. З порівняння отриманих результатів стало ясно, що площа зони виявлення у випадку використання критерію $C_{пр} = 0$ значно більша, ніж у випадку застосування критерію $P_{об} = 0,7$. Таким чином, критерій $C_{пр} = 0$ є більш «м'яким» і найкраще на практиці використовувати критерій $P_{об} = 0,7$, щоб уникнути помилок виявлення.

У **четвертому розділі** дано теоретичне обґрунтування простого методу роботи легітимного каналу (ЛК) під «штучним шумом», який відрізняється від відомих використанням протоколів тільки першого та другого рівнів моделі OSI. Проведено чисельні експерименти, які довели можливість реалізації легітимного каналу з гарною прихованістю в усьому навколишньому просторі, крім головної пелюстки ДС передавальної антени легітимного модему при достатній завадозахищеності приймача ЛК. Розроблено експериментальну установку та проведено досліди, що підтверджують плодотворність висловленої ідеї роботи ЛК під «штучним шумом».

Суть запропонованого способу (рис. 5) полягає в наступному. У точках А та В розташовані модеми легітимного каналу з антенами, що характеризуються діаграмами спрямованості ДС1. У цих самих точках знаходяться і генератори штучного шуму, забезпечені антенами, у яких діаграма спрямованості ДС2 - кардіоїда.

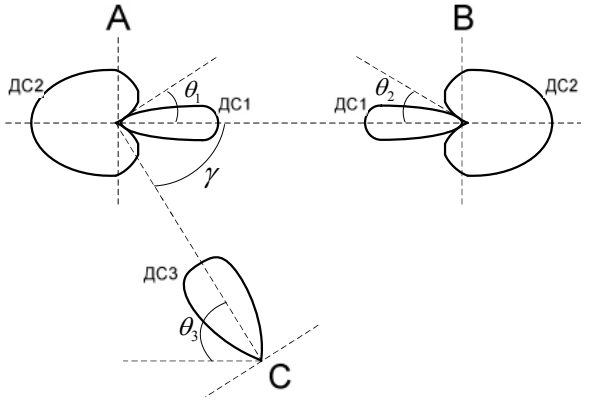

Рис. 5. Схема розташування антен легітимного і відвідного каналів

При орієнтації антен модемів максимумами ДС1 один на одного, а антен генераторів штучного шуму мінімумом ДС2 на максимум ДС1, на входах приймачів модемів в ідеальному випадку буде виділятись тільки інформаційний сигнал. Штучний шум впливатиме лише на вхід приймача-виявляча, що знаходиться в точці С. Його антена має діаграму спрямованості ДС3. При цьому умови виявлення легітимного каналу суттєво погіршуються. Це було показано шляхом розрахунків, взявши за основу формулу для імовірності виявлення $P_{об}$:

$$P_{об} = 1 - \left(1/1 + 2^{R_s} \cdot (S/N)_o/(S/N)_л\right) \cdot e^{\left[-2^{R_s}-1/(S/N)_л\right]}, \qquad (23)$$

де $(S/N)_o$, (S/N) – середні значення сигнал/шум у відвідному та легітимному каналах, R_S – секретна швидкість передавання інформації, при якій система зв'язку вважається секретною (не виявляється).

В (23) зроблено такі перетворення:

$$(S/N)_л = \left(S/N + J \cdot G_{TJ} \cdot f_{TJ}^2(\theta_1)\right) \cdot \alpha\left(r_э/r_л\right) \times G_{TS} \cdot f_{TS}^2(r_л, \theta_1) \cdot G_{RЛ} \cdot f_{RЛ}^2(r_л, \theta_2), \qquad (24)$$

$$(S/N)_o = \left(S/N + J \cdot G_{TJ} \cdot f_{TJ}^2(\gamma)\right) \cdot \alpha\left(r_э/r_o\right) \times G_{TS} \cdot f_{TS}^2(r_o, \gamma) \cdot G_{RO} \cdot f_{RO}^2(r_o, \theta_3), \qquad (25)$$

де S – потужність передавача; J – потужність генератора штучного шуму; G_{TJ}, G_{TS}, $G_{RЛ}$, G_{RO} – коефіцієнти підсилення антен передавача штучного шуму, передавача сигналу, антен легітимного та відвідного каналу відповідно, а f_{TJ}, f_{TS}, $f_{RЛ}$, f_{RO} – їхні нормовані кутові залежності інтенсивності поля; γ – кут приходу завади.

У роботі наведено результат розрахунку ймовірності виявлення для випадку, коли в генераторі шуму Wi-Fi каналу використовується антена з кардіоїдною ДС, а ДС модемів легітимного каналу та приймача-виявляча є неспрямованими. У цьому випадку канал можна було виявити ($P_{об} > 0{,}7$) тільки в невеликому секторі кутів. Фактично тоді, коли приймач-виявляч знаходився на осі легітимного каналу. Використовуючи вібраторні антени з довжиною пліч $> 0{,}5\lambda$, можна реалізувати ДС з кількістю максимумів більше двох, що дозволяє забезпечити роботу базової станції під шумом від трьох до шести абонентів. Про ефективність запропонованого способу забезпечення безпечної роботи легітимного Wi-Fi каналу зв'язку можна судити з розгляду показаних на рис. 6 зон виявлення при вимкненому (крива 1) та включеному (крива 2) генераторі штучного шуму.

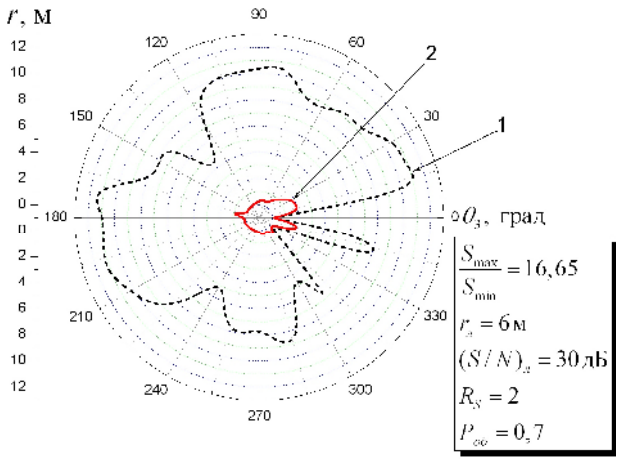

Рис. 6. Зони виявлення Wi-Fi каналу

Під зоною виявлення мається на увазі площа, обмежена кривою постійної ймовірності виявлення $P_{об}(r,\theta) = 0,7$. На полях рис. 6 показано відношення площ зон виявлення при вимкненому – S_{max} та включеному – S_{min} генераторі шуму. Легко побачити, що площі S_{max} та S_{min} відрізняються більш ніж у 10 разів для всіх розглянутих випадків. Причому, з переходом від ближньої зони до дальньої відношення S_{max}/S_{min} зменшується, що зумовлено різними умовами ПРХ в цих зонах.

Отже з'ясовано, що при роботі під «штучним шумом» основний позитивний ефект полягає в зменшенні площі зони виявлення S_{min} більш ніж у 10 разів, порівняно з площею S_{max}. Ця обставина суттєво спрощує організацію контролю несанкціонованого доступу до інформації, що передається по легітимним каналом. З результатів чисельних досліджень можна зробити висновок, що запропонований спосіб забезпечення безпечної роботи легітимного Wi-Fi каналу може бути реалізований на практиці, якщо завадозахищеність легітимних приймачів буде достатньою.

Про рівень завадозахищеності приймачів модемів можна судити за величиною ймовірності бітової помилки.

$$P_B = \frac{1}{2}\cdot\left[1 - \sqrt{\frac{(S/N)\cdot\alpha\left(r_J/r_S\right)^n\cdot\left[G_{TS}\cdot f_{TS}^2(\theta_1)\cdot G_R \cdot f^2 / G \cdot f^2(\theta_1)\right]}{\left((S/N)\cdot\alpha\left(r_J/r_S\right)^n\cdot\left[G_{TS}\cdot f_{TS}^2(\theta_1)\cdot G_R \cdot f^2 / G \cdot f^2(\theta_1)\right]\right)+1}}\right], \quad (26)$$

де (S/N) – середні значення сигнал/шум в каналі зв'язку α – функціональна залежність загасання сигналу; r_S, r_J – відстань (рознесення) між передавальними та приймальними антенами відповідно до даної системи зв'язку та постановника завад; n – показник ступеня загасання.

Результати розрахунків ймовірності бітової помилки представлені в дисертації. Значення ймовірності бітової помилки виявилися незадовільними ($>10^{-4}$) у всіх випадках ДС за винятком невеликого сектора кутів поблизу $\theta = 0^\circ$. Зі зменшенням співвідношення S/N сектор кутів θ, у межах яких відбувається передавання інформації з високою якістю ($P_B = 10^{-4} \div 10^{-6}$), звужується, але залишається достатнім для впевненої роботи легітимного каналу. Висловлена ідея перевірялася експериментально. Структурну схему експериментальної установки показано на рис. 7. Установу було зібрано на основі Wi-Fi обладнання робочого діапазону 2,45 ГГц. Використовувалися нетбуки з підтримкою протоколу IEEE 802.11n, внутрішніми модемами та внутрішніми антенами A1 з неспрямованими діаграмами спрямованості.

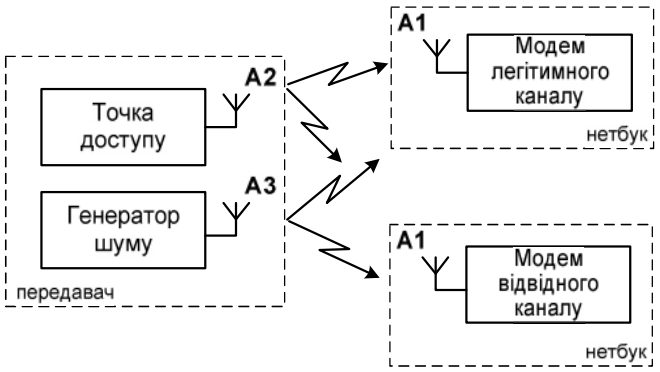

Рис. 7. Структурна схема експериментальної установки

Ці нетбуки спільно з точкою доступу утворювали легітимний та відвідний канали. Як генератор шуму застосовувався стандартний генератор Г4-79, котрий створює одночастотну заваду. При створенні експериментальної установки вирішувалося питання про вибір типів антен А1, А2, А3 та, в результаті, антенну систему передавача було виконано з двох антен: антени А2 «подвійний квадрат» над екраном, підключеної до точки доступу та укороченого симетричного вібратора А3, з'єднаного з генератором шуму.

Подальші експерименти щодо вимірювання рівня сигналу на вході модему легітимного приймача при включеному генераторі шуму підтвердили правильність висловленої ідеї роботи під «штучним шумом». Генератор Г4-79 при цьому створював «вузькосмуговий» шум на одній частоті Wi-Fi діапазону. Аналізуючи отримані дані було встановлено, що значний рівень сигналу спостерігався лише в секторі кутів $\Delta\theta \approx \pm 30^{\circ}$. Як з'ясувалося в процесі експерименту, вплив вузькосмугового шуму не повністю блокує роботу відвідного каналу, оскільки в сучасних Wi-Fi системах використовується технологія адаптивного прийому, і інформація, що передається в легітимному каналі, може бути виявлена. Для усунення цього недоліку було запропоновано застосувати генератор, що створює шум в усій смузі Wi-Fi. Такий генератор був спроектований на кафедрі ОРТ ХНУРЕ.

Результати експерименту зі створеним генератором шуму наведено на рис. 8. Тут сектор, обмежений кривою 2, відповідає випадку встановлення зв'язку в каналі, тобто підключенню до точки доступу. Заштрихований сектор, крива 1 – це сектор передавання інформації з високою якістю. Щоб цілком упевнитися в можливості роботи легітимного каналу при передаванні відеоінформації та функціонуванні широкосмугового генератора шуму, проводився дослід з безпроводовою IP-камерою.

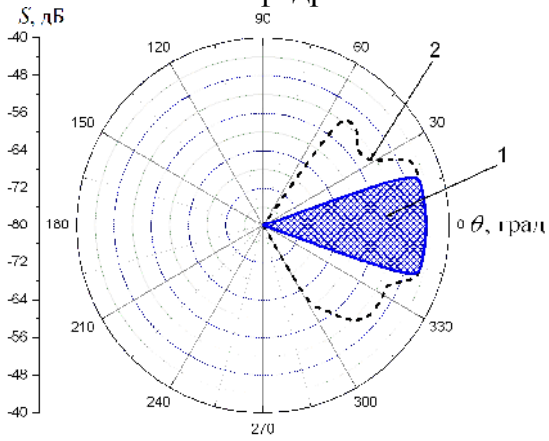

Рис. 8. Результати вимірювань рівня сигналу при роботі широкосмугового генератора шуму

Вихідне зображення на екрані приймача легітимного каналу при включеному генераторі шуму не змінилося, а відсутність зображення на екрані приймача в відвідному каналі було свідченням того, що ВК був повністю подавлений завадою і не функціонував.

Проведені досліди свідчать про високу ефективність запропонованого методу підвищення прихованості легітимного каналу при його роботі під «штучним шумом», створюваним широкосмуговим генератором.

ВИСНОВКИ

В результаті дисертаційних досліджень одержано нове вирішення актуальної науково-практичної задачі підвищення захищеності Wi-Fi каналів зв'язку за рахунок застосування нових моделей та методів, які більш повно враховують особливості функціонування релеєвських каналів зв’язку на першому та другому рівнях моделі OSI. Для цього одержано аналітичні вирази, що враховують вплив на рівень ймовірності виявлення та граничної секретної продуктивності електродинамічних характеристик антен і розсіювачів легітимного та відвідного каналів, а також різноманітності механізмів поширення радіохвиль. Також запропоновано метод побудови зон виявлення, який дозволяє проектувати безпроводові цифрові системи передавання інформації із заданим рівнем ймовірності виявлення. У результаті нового вирішення задачі отримано позитивний ефект, що полягає в зменшенні площі зони виявлення більш ніж у 10 разів, що істотно полегшує організацію контролю несанкціонованого доступу до інформації, що передається Wi-Fi каналами зв'язку і не потребує застосування криптоалгоритмів.

У процесі досліджень отримано такі основні результати:

1. Удосконалено модель для визначення рівня прихованості релеєвських каналів зв'язку. Розроблено математичну модель, що пов'язує ймовірність виявлення каналу ЦСПДІ та його секретну продуктивність з розмірами апертур антен легітимного каналу, апертур антен відвідного каналу та їх взаємним розташуванням. Показано, що основними факторами, які впливають на ефективність виявлення, є віддалення приймальних апертур легітимного та відвідного каналу від апертури системи випромінювачів та розсіювачів джерела інформації, а також величина секретної швидкості.

2. Наведено результати чисельних експериментів, з яких виходить, що відмінності в умовах ПРХ суттєво впливають на величини $P_{об}$ і $C_{пр}$. Отримані дані є новими та дозволяють визначити умови, за яких $P_{об} < 0,7$ та $C_{пр} = 0$, що відповідає критерію безпечної роботи багатопроменевих радіоканалів.

3. Виведено нові вирази, що визначають залежність величини $P_{об}$ та $C_{пр}$ від різних умов поширення радіохвиль. Запропоновано методи розрахунку зон виявлення радіоканалу за критеріями $P_{об} = 0,7$ і $C_{пр} = 0$. Показано, що при розрахунках виникає необхідність використовувати експериментальні кутові залежності інтенсивності поля.

4. З'ясовано, що при слабкій нерівномірності границі зони виявлення розрахунки можна спростити, не вдаючись до пошуку коренів рівняння $P_o = f(r)$, при $\theta_{3i} = const$, а побудувавши сімейство кривих $P_{об}(\theta_3)$, – при різних значеннях r_o.

5. Отримано нові конкретні кількісні дані про розміри апертур легітимного та відвідного каналів, а також про їх взаємне розташування, при яких сигнали ЦСПІ можна виявити напевно.

6. З'ясовано, що у разі застосування в відвідних каналах слабкоспрямованої антени її орієнтація що до передавача мало впливає на розмір зони виявлення; рекомендовано на практиці при побудові границі зони виявлення використовувати критерій $P_{об} = 0,7$, як більш «жорсткий».

7. Виміряні раніше невідомі дані про ймовірності виявлення легітимних Wi-Fi каналів у приміщенні й на відкритому просторі в ближній, проміжній та дальній зонах.

8. Експериментальні дослідження, проведені з метою доказу достовірності розробленої моделі аналізу ймовірності виявлення, показали, що створена модель може бути використана лише для наближеного, а не точного визначення ймовірності виявлення функціонування каналу зв'язку.

9. Науково обґрунтовано метод роботи легітимного каналу під «штучним шумом», який базується на застосуванні в передавачі легітимного каналу генератора шуму та додаткової антени з нулем діаграми спрямованості у напрямку легітимного модему та інтенсивним випромінюванням у напрямку антени відвідного каналу. Шляхом розрахунків показано, що при описаному принципі роботи факт функціонування легітимного каналу може бути виявлений лише в межах головної пелюстки діаграми спрямованості легітимного передавача. При цьому на стороні приймача в достатньому для практики секторі кутів забезпечується приймання інформації з високою якістю ($P_B = 10^{-4} \div 10^{-6}$).

10. Створено експериментальну установку та проведено досліди, в результаті яких встановлено, що повне подавлення роботи відвідного каналу можливе лише при застосуванні широкосмугових генераторів шуму, що працюють у всій смузі Wi-Fi точок доступу.

11. Отримано нові експериментальні дані про кутові залежності інтенсивності поля антен ряду Wi-Fi пристроїв (точок доступу, клієнтських адаптерів і т.д.), які можуть бути використані при практичній розробці радіоканалів з Wi-Fi технологією.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Основні результати дисертації опубліковані в таких роботах:

1. Абдул-Хуссейн, М.К. Метод расчета радиоканала цифровых систем передачи информации с заданной вероятностью обнаружения [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, А.Е. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Радиотехника: Всеукраинский межведомственный научно-технический сборник. – 2011. – Вып. № 165. – С. 107-111.

2. Абдул-Хуссейн, М.К. Моделирование и экспериментальное определение вероятности обнаружения функционирования Wi-Fi радиоканала [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.А. Назаренко, В.М. Шокало, Е.В. Ягудина // Научный вестник Черновицкого университета. – 2011. – Том 1, выпуск 1. Физика. Электроника. – С. 13-16.

3. Абдул-Хуссейн, М.К. Метод расчета границы зоны обнаружения рэлеевского Wi-Fi радиоканала с квазистатическими замираниями [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Известия вузов. Радиоэлектроника: Международный ежемесячный научно-технический журнал. – 2012. – Том 55, №10. – С. 26-34.

4. Абдул-Хуссейн, М.К. Усовершенствованная модель расчета предельной секретной производительности Wi-Fi канала связи [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Радиотехника: Всеукраинский

межведомственный научно-технический сборник. – 2012. – Вып. № 169. – С. 190-195.

5. Абдул-Хуссейн, М.К. Простой способ обеспечения скрытности каналов связи уровня LAN [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Науково-технічний журнал «Сучасний захист інформації». – Київ: ДУІКТ, 2012. – Спеціальний випуск. – С. 26-31.

6. Abdul-Hussein, M.K. Refined model for calculation of limiting secret efficiency of Wi-Fi communication channel [Текст] / M.K. Abdul-Hussein, O.O. Strelnitskiy, V.M. Shokalo, E.V. Yagudina // International journal «Telecommunication and Radio Engineering». – Begell House, 2012. – Vol. 71(16). – P. 1465-1473.

7. Abdul-Hussein, M.K. Method of calculating the detection zone boundaries of the rayleigh Wi-Fi wireless channel with quasi-static fading [Текст] / M.K. Abdul-Hussein, O.O. Strelnitskiy, V.M. Shokalo, E.V. Yagudina // International journal «Radioelectronics and Communications Systems. – Allerton Press, 2012. – Vol. 55, Number 10. – P. 452–457.

8. Абдул-Хуссейн, М.К. Усовершенствование метода повышения скрытности легитимного канала связи за счет работы под «искусственным шумом» [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Тези доповідей VI Міжнародної науково-практичної конференції «Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій». – Запоріжжя: ЗНТУ, 2012. – С. 118-119.

9. Abdul-Hussein, M.K. Improving random keys of WLAN security algorithms [Текст] / M.K. Abdul-Hussein, O.O. Strelnitskiy // Труды 12-й Международной научно-технической конференции «Современные информационные и электронные технологии». – Одесса: ОНПУ, 2011, – С. 165.

10. Абдул-Хуссейн, М.К. Учет влияния на скрытность Wi-Fi каналов связи их электродинамических характеристик и условий распространения радиоволн [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина // Сборник научных трудов 4-го Международного радиоэлектронного форума «Прикладная радиоэлектроника. Состояние и перспективы развития». Конференция «Телекоммуникационные системы и технологии» /МРФ’2011/. – Том II. – Харьков: ХНУРЭ, 2011. – С. 404-407.

11. Abdul-Hussein, M.K. The method of calculating detection areas of digital communication systems [Текст] / M.K. Abdul-Hussein, O.O. Strelnitskiy, V.M. Shokalo, E.V. Yagudina / Матеріали 11-ої Міжнародної науково-технічної конференції «Сучасні проблеми радіоелектроніки, телекомунікації та комп’ютерної інженерії»/TCSET’2012/ – Львів - Славсько: НУ “ЛП”, 2012, – С. 268.

12. Абдул-Хуссейн, М.К. Метод построения зон обнаружения Wi-Fi каналов связи [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.М. Шокало, Е.В. Ягудина// Труды 13-й Международной научно-технической конференции «Современные информационные и электронные технологии». – Одесса: ОНПУ, 2012. – С. 139.

13. Абдул-Хуссейн, М.К. Нові результати досліджень зон виявлення релеєвських каналів зв'язку [Текст] / М.К. Абдул-Хуссейн, О.О. Стрельницкий, В.М. Шокало, О.В. Ягудина // Праці І-ї Міжнародної науково-технічної конференції

«Захист інформації і безпека інформаційних систем». – Львів: НТУ «ЛП», 2012. – С. 56-57.

14. Абдул-Хуссейн, М.К. Моделирование и экспериментальное определение вероятности обнаружения функционирования Wi-Fi радиоканала [Текст] / М.К. Абдул-Хуссейн, А.А. Стрельницкий, В.А. Назаренко, В.М. Шокало, Е.В. Ягудина // Матеріали І-ої Всеукраїнської науково-практичної конференції «Фізико-технологічні проблеми радіотехнічних пристроїв, засобів телекомунікацій, нано- та мікроелектроніки». – Чернівці: ЧНУ, 2011. – С. 48-51.

АНОТАЦІЯ

Мухаммед Кадім Абдул-Хуссейн. Розвиток методів підвищення захищеності Wi-Fi каналів зв'язку на фізичному рівні. - Рукопис .

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи. – Харківський національний університет радіоелектроніки, Харків, 2013.

В результаті дисертаційних досліджень отримано нове вирішення актуальної науково-практичної задачі підвищення захищеності Wi-Fi каналів зв'язку за рахунок застосування нових моделей та методів, які більш повно враховують особливості функціонування релеєвських каналів зв’язку на першому та другому рівнях моделі OSI. Для цього отримано аналітичні вирази, що враховують вплив на рівень ймовірності виявлення та граничної секретної продуктивності електродинамічних характеристик антен і розсіювачів легітимного та відвідного каналів, а також різноманітності механізмів поширення радіохвиль. Крім того, запропоновано метод побудови зон виявлення, який дозволяє проектувати безпроводові цифрові системи передавання інформації із заданим рівнем ймовірності виявлення. У результаті нового вирішення задачі отримано позитивний ефект, котрий полягає у зменшенні площі зони виявлення більш ніж у 10 разів, що істотно полегшує організацію контролю несанкціонованого доступу до інформації, що передається по Wi-Fi каналах зв'язку і не потребує залстосування криптоалгоритмів.

Практична цінність роботи визначається, перш за все, багатим експериментальним матеріалом про кутові залежності інтенсивності поля антен ряду Wi-Fi пристроїв і раніше невідомих даних про ймовірності виявлення легітимних Wi-Fi каналів в приміщенні та на відкритому просторі в ближній, проміжній і дальній зонах.

Проведені експерименти підтвердили достовірність розроблених в дисертації наукових положень та принципів. Її результати впроваджені при частотно-територіальному плануванні безпроводової мережі рівня LAN у м. Харкові та в навчальному процесі ХНУРЕ.

Ключові слова: ймовірність виявлення, секретна продуктивність, захищеність, прихованість, завадозахищеність, цифрові системи передавання інформації, загасання, радіоканал, моделі, експеримент.

АННОТАЦИЯ

Мухаммед Кадим Абдул-Хуссейн. Развитие методов повышения защищенности Wi-Fi каналов связи на физическом уровне. – Рукопись.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.17 – радиотехнические и телевизионные системы. – Харьковский национальный университет радиоэлектроники, Харьков, 2013.

В результате диссертационных исследований получено новое решение актуальной научно-практической задачи повышения защищенности Wi-Fi каналов связи за счет применения новых моделей и методов, более полно учитывающих особенности функционирования рэлеевских связных каналов на первом и втором уровнях модели OSI. Для этого получены аналитические выражения, учитывающие влияние на уровень вероятности обнаружения и предельной секретной производительности электродинамических характеристик антенн и рассеивателей легитимного и отводного каналов, а также разнообразия механизмов распространения радиоволн. Также предложен метод построения зон обнаружения, который позволяет проектировать беспроводные цифровые системы передачи информации с заданным уровнем вероятности обнаружения. В результате нового решения задачи получен положительный эффект, состоящий в уменьшении площади зоны обнаружения более чем в 10 раз, что существенно облегчает организацию контроля несанкционированного доступа к информации, передаваемой по Wi-Fi каналам связи и не требует применения криптоалгоритмов.

Практическая ценность работы определяется, прежде всего, богатым экспериментальным материалом об угловых зависимостях интенсивности поля антенн ряда Wi-Fi устройств и ранее неизвестных данных о вероятностях обнаружения легитимных Wi-Fi каналов в помещении и на открытом пространстве в ближней, промежуточной и дальней зонах.

Проведенные эксперименты подтвердили достоверность разработанных в диссертации научных положений и принципов. Ее результаты внедрены при частотно-территориальном планировании беспроводной сети уровня LAN в г. Харькове и в учебном процессе ХНУРЭ.

Ключевые слова: вероятность обнаружения, секретная производительность, защищенность, скрытность, помехозащищенность, цифровые системы передачи информации, затухание, радиоканал, модели, эксперимент.

ABSTRACT

Mohammad Kadhim Abdul-Hussein. Development of Methods for Improving the Physical Security of Wi-Fi Communication Channels. – Manuscript.

Thesis for the degree of Candidate of Engineering Sciences (PhD in Engineering) majoring in 05.12.17 – Radio and Television Systems. – Kharkov National University of Radio Electronics, Kharkov, 2013.

As a result of the thesis research there has been obtained a new solution of an urgent theoretical and practical problem of increasing the security of Wi-Fi communication channels with the help of the new models and methods, which more comprehensively take into account the peculiarities of Rayleigh communication channels on the first and the second levels of the OSI model. In order to achieve this there have been obtained analytical expressions that take into account the impact of the limit of secret performance of electodynamic characteristics of antennas, the disperser of the legitimate and diverting

channels and the diversity of radio waves propagation mechanisms on the detection probability level. Also there has been provided a detection zone construction method, which allows to design wireless digital systems of information transmission with a given level of detection probability. As a result of the new solution to the problem there has been obtained a positive effect of 10-time decreasing the area of the detection zone, which greatly facilitates the organization of control of an unauthorized access to information transmitted using Wi-Fi communication channels, and does not require encryption algorithms.

The practical effect of the research consists, first and foremost, in extensive experimental materials on angular dependence of field intensity of antennas of a number of Wi-Fi devices and in the previously unknown data on probabilities of detection of legitimate Wi-Fi channels indoors and on the open space in the near, intermediate and far field zones.

The experiments evidenced validity of scientific postulates and principles elaborated in the thesis. Its results were implemented for frequency territorial planning of wireless network of LAN level in Kharkov and in the KhNURE's training process.

Key words: probability of detection, secret efficiency, security, interference immunity, digital information transmission systems, fading, radio channel, models, experiment.

Підп. до друку 06.11.13. Формат 60х841/16. Спосіб друку – ризографія.
Умов. друк. арк. 1,2. Тираж 100 прим.
Зам. № 2-353. Ціна договірна.

??????????????????????????????????????

Віддруковано в