Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

ВАСИЛЕНКО ТЕТЯНА ОЛЕКСАНДРІВНА

УДК 621.396.2

МЕТОДИ РОЗПІЗЗНАВАННЯ WI-FI ПРИСТРОЇВ ШЛЯХОМ ВРАХУВАННЯ ЇХ ІНДИВІДУАЛЬНИХ ОЗНАК ДЛЯ ПІДВИЩЕННЯ ЗАХИЩЕНОСТІ МЕРЕЖІ

05.12.17 – радіотехнічні та телевізійні системи

Автореферат дисертації на здобуття наукового ступеня
кандидата технічних наук

Харків – 2021

Дисертацією є рукопис

Робота виконана у Харківському національному університеті радіоелектроніки Міністерства освіти і науки України

Науковий керівник: доктор технічних наук, професор
Антіпов Іван Євгенійович,
Харківський національний університет
радіоелектроніки, завідувач кафедри комп'ютерної
радіоінженерії та систем технічного захисту інформації

Офіційні опоненти: доктор технічних наук, старший науковий співробітник
Костиря Олександр Олексійович,
Харківський національний університеті
Повітряних Сил імені Івана Кожедуба,
начальник науково-дослідної лабораторії факультету
радіотехнічних військ протиповітряної оборони;

кандидат технічних наук
Нарєжній Олексій Павлович,
Харківський національний університет імені В. Н. Каразіна,
доцент кафедри безпеки інформаційних систем і технологій

Захист відбудеться « 6 » травня 2021 року о 15:00 годині на засіданні спеціалізованої вченої ради Д 64.052.03 у Харківському національному університеті радіоелектроніки за адресою: 61166, м. Харків, проспект Науки, 14, ауд.13.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету радіоелектроніки за адресою: 61166, м. Харків, проспект Науки, 14.

Автореферат розіслано «___» квітня 2021 року.

Вчений секретар
спеціалізованої вченої ради  В.М. Безрук

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Масовому поширенню Wi-Fi мереж сприяє простота їх розгортання, висока швидкість, універсальність і зручність використання. Розвиток і поширення цих мереж триває, незважаючи на наявність ряду недоліків. Одним з недоліків Wi-Fi мереж є їх вразливість до різних видів атак, у тому числі, основаних на підробці (імітації) ідентифікаційних даних.

Для захисту бездротових мереж від цих атак застосовуються системи виявлення вторгнень (СВВ). Вони здатні виявляти і запобігати атакам шляхом обмеження доступу до мережі або зміни конфігурації комунікаційного обладнання. Ознаками атак в існуючих СВВ являються параметри мережевого трафіку (мережева активність вузла, мережеве налаштування вузла, дані про файли та процеси) тобто, ознаки канального, мережевого та більш високих рівнів моделі OSI. Такий підхід повністю виправданий в провідних чи оптоволоконних мережах, де фізичне підключення до мережі для зловмисників є складним, а тому ідентифікація обладнання, як така відсутня (здійснюється тільки аутентифікація користувача). Втім підключення ж до Wi-Fi мережі на фізичному рівні не є проблемою для зловмисників через відритий радіоінтерфейс.

Спроби збільшення кількості аналізованих ознак на високих рівнях моделі OSI для протидії новим видам атак ведуть до ускладнення СВВ, уповільнення їх роботи і великої кількості помилкових спрацьовувань. Крім того, ряд цих ознак може бути імітовано зловмисниками.

Разом з тим існують ознаки фізичного рівня, знання яких розширює уявлення про стан мережі, може сприяти підвищенню надійності ідентифікації абонентів мережі і таким чином запобіганню ряду атак. Але ці ознаки не враховуються в СВВ, через відсутність теоретичного і практичного обґрунтування можливості їх застосування.

Тому науково-прикладну задачу ідентифікації пристроїв бездротових мереж шляхом врахування ознак фізичного рівня з метою підвищення безпеки бездротових мереж слід вважати **актуальною.**

Зв'язок роботи з науковими програмами, планами, темами

Дисертаційні дослідження пов'язані з виконанням держбюджетної НДР, що виконувалася відповідно до тематичного плану МОН України: № 260-5 «Розробка методів моделювання інформаційних мереж, побудованих на основі реконфігурованих антен» (№ ДР 011U002903), у якій здобувачка була співвиконавцем.

Мета і задачі дослідження. Метою дисертаційної роботи є підвищення захищеності бездротової Wi-Fi мережі шляхом обґрунтованого врахування ознак її стану на фізичному рівні.

Для досягнення поставленої мети вирішуються наступні **наукові задачі:**

– проаналізувати роботу бездротової Wi-Fi мережі, визначити коло загроз і вразливостей та сучасного стану її захищеності;

– розробити метод ідентифікації пристрою користувача по спектральним характеристикам випромінювання передавача;

– експериментально перевірити можливості ідентифікації пристрою в мережі по спектральним характеристикам випромінювання передавача;

– виробити пропозицій щодо врахування місцеположення пристрою як ознаки при виявленні атак на бездротову мережу.

Об'єкт дослідження – процес захисту бездротової Wi-Fi мережі.

Предмет дослідження – параметри оцінки бездротової мережі, на основі яких приймається рішення про її аномальний стан[1].

Методи дослідження. При розробці методу ідентифікації по спектру використовувалися методи спектрального аналізу і метод порівняння. При розробці методу ідентифікації за місцем розташування використовувався метод порівняння. При розробці обох методів застосовувалася експериментальна перевірка. Для оцінки ефективності методів використовувалося математичне моделювання.

Наукова новизна отриманих результатів:

Головний науковий результат дисертації – це розроблені і експериментально перевірені методи ідентифікації пристроїв в бездротовій мережі, що відрізняються від раніше відомих тим, що в них використовуються ознаки стану мережі на фізичному рівні, що дозволяє виявляти і спільно з системами виявлення вторгнень запобігати ряду атак і тим самим підвищувати безпеку Wi-Fi мереж .

У рамках головного отримано ряд окремих **наукових результатів**:

1. Вперше запропоновано метод ідентифікації користувачів Wi-Fi мереж, відмінною особливістю якого є детальний аналіз спектральних характеристик випромінювання їх пристроїв, що дозволяє виявляти спроби втручання в мережу шляхом імітації роботи авторизованих користувачів.

2. Розроблено новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв, відмінною особливістю якого є обчислення середнього квадрату різниці відповідних спектральних відліків з урахуванням різниці в середній потужності різних сигналів, що дозволяє порівнювати спектри, отримані в різних умовах, з еталонним.

3. Запропоновано новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом оцінки коефіцієнта асиметрії взаємокореляційної функції спектру Wi-Fi пристроїв.

4. Отримав подальший розвиток метод виявлення атак на бездротову мережу, що полягає у використанні даних про місцеположення користувачів в мережі, які визначаються за рівнем RSSI з використанням радіовідбитків, що дозволяє виявляти атаки, що не виявляються за іншими ознаками.

5. Розроблено нову модель, що імітує спектр сигналу Wi-Fi мережі в умовах впливу шуму, що дозволяє оцінити ефективність розроблених методів в реальних умовах і виробити рекомендації щодо їх практичного застосування.

Примітка: [1)] під аномальним станом бездротової мережі Wi-Fi в даній роботі будемо розуміти нетипову активність мережі (велика кількість трафіку, кількість абонентів, місцеположення абонентів, швидкість передачі даних, неспівпадання спектрів пристроїв і т. д.) не властиву їй для конкретного періоду часу.

Практичне значення отриманих результатів:

1. Експериментально встановлено схожість спектрів Wi-Fi сигналів одного і того пристрою в різних положеннях та виявлено істотну різницю в спектрах випромінювання різних пристроїв, що може бути використано для їх ідентифікації.

2. Розроблено методику визначення місцеположення абонента бездротової мережі за рівнем RSSI з використанням методу радіовідбитків. Показано, що похибка у визначенні місцеположення становить 2.5 м при застосуванні детермінованого (евклідова відстань) підходу визначення координат в закритому приміщенні.

3. Запропонований в роботі алгоритм аналізу стану Wi-Fi мережі дозволяє більш адекватно приймати рішення про аномальний стан мережі за рахунок врахування ознак, які не враховуються в діючих СВВ.

4. Результати дисертаційної роботи прийняті до використання виробничим підрозділом «Харківське відділення» філії «Головний інформаційно-обчислювальний центр» АТ «Укрзалізниця» при аналізі стану захищеності інформаційних ресурсів для підвищення безпеки систем бездротового зв'язку (Акт від 10.02.2021р., м. Харків, Україна). Крім того, матеріали дисертаційної роботи використовуються в освітньому процесі Харківського національного університету радіоелектроніки на кафедрі комп'ютерної радіоінженер та систем технічного захисту інформації в курсі лекцій з дисципліни «Обробка сигналів в системах ТЗІ» і при підготовці магістерських атестаційних робіт, про що є відповідній акт впровадження. (Акт від 18.02.2021р., м. Харків, Україна).

Особистий внесок здобувача. Дисертаційна робота є результатом наукових досліджень автора. Основні наукові результати, які наведені у дисертаційній роботі, отримані здобувачем самостійно і досить повно викладені в 15 наукових роботах, опублікованих здобувачем у співавторстві і самостійно. Особистий внесок здобувача в роботах, опублікованих у співавторстві, полягає в наступному. В роботі [1] здобувач запропонував алгоритм аналізу станів Wi-Fi мережі на основі нечіткої логіки, що дозволяє більш адекватно приймати рішення щодо аномального стану бездротової мережі. У роботі [2] дисертант розглядає можливість застосування теорії гри для захисту бездротової Wi-Fi мережі. У матеріалах роботи [3] здобувачем створена нова модель, реалізована у вигляді комп'ютерної програми, що імітує роботу Wi-Fi мережі, яка дозволяє врахувати можливість вторгнень, збоїв та перешкод в режимі Point Coordination Function. Матеріали публікації [4] є продовженням теми наукових досліджень [3], де дисертант доповнив модель, що імітує роботу Wi-Fi мережі режимом розподіленої координації Distributed Coordination Function. В статті [5] здобувач брав участь у дослідженнях ефективності технології MIMO. У статті [6] здобувач розробив методику визначення місцезнаходження абонентів бездротової мережі за методом RSSI з використанням методу радіовідбитків. В статті [7] здобувач розробив метод обробки результатів вимірювання спектрів випромінювання мобільних Wi-Fi пристроїв шляхом обчислення середнього квадрата різності відповідних спектральних відліків.

Апробація результатів дисертації. Основні результати роботи представлені та обговорювалися на таких науково-технічних конференціях: 23-й Міжнародній Кримській конференції «СВЧ-техніка і телекомунікаційні технології» (Севастопіль, 2013 ро-

ку); 15, 16, 17, 18, 19, 22, 24 Міжнародних молодіжних форумах «Радіоелектроніка та молодь у XXI столітті» (Харків, 2011, 2012, 2013, 2014, 2015, 2018, 2020).

Публікації. За темою дисертації загалом опубліковано 15 наукових робіт, у тому числі 6 статей у провідних наукових фахових виданнях, затверджених ВАК України та одна стаття, що індексується у світових наукометричних базах даних Scopus, 8 тез доповідей на міжнародних наукових конференціях (в тому числі Scopus).

Структура та обсяг дисертації. Дисертація складається із вступу, чотирьох розділів, висновків, списку використаних джерел, який складається з 82 найменувань та 3 додатків. Обсяг дисертаційної роботи 145 сторінок., 48 рисунків, 17 таблиць.

ОСНОВНИЙ ЗМІСТ РОБОТИ

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

У першому розділі «Безпека бездротових мереж як багатофакторна задача» проведено огляд технології Wi-Fi, сучасного стану її захищеності, визначено спектр загроз та вразливостей. Здійснено аналіз засобів щодо її захисту.

Суттєвий недолік технології Wi-Fi – це потенційна вразливість мереж до різних видів атак. Вона обумовлена тим, що Wi-Fi мережа на фізичному рівні доступна всім (всі обмеження доступу до неї тільки програмні), а самі протоколи передачі даних і обладнання, часто містять в собі «слабкі місця» і залишають можливості для втручання.

Існуючі методи захисту не досконалі. Методи ідентифікації ненадійні, як і криптографічні алгоритми, які успішно зламуються. А роботу мережі можна порушити і не знаючи алгоритми і ключі шифрування. Міжмережеві екрани мають безліч недоліків і не захищають внутрішню мережу. Через складність структури і алгоритмів СОВ, їх робота супроводжується великою кількістю помилкових спрацьовувань, або вони не здатні виявляти раніше невідомі атаки.

Причиною недоліків є те, що при забезпеченні захисту Wi-Fi мереж не враховуються параметри мережі фізичного рівня, знання яких розширює уявлення про його стан.

Таким чином, сформульовано мету та задачі дослідження, обґрунтовано наукове завдання дисертаційної роботи, яке полягає в підвищенні безпеки бездротових мереж, шляхом врахування ознак фізичного рівня.

Другий розділ дисертації «Ідентифікація користувачів Wi-Fi мереж по спектрам їх пристроїв». У розділі розглянуто новий метод ідентифікації, оснований на аналізі спектральних характеристик сигналів, що випромінюються абонентськими пристроями, його теоретичне обґрунтування, експериментальна перевірка і способи порівняння.

Оскільки наявні методи ідентифікації в бездротових мережах, основані на перевірці MAC-адрес, IP, SSID є вразливими до атак, то було вирішено звернути увагу на такі параметри Wi-Fi обладнання, які з одного боку є його невід'ємними властивостями, піддаються вимірюванню і перевірці, а з іншого, їх досить складно підробити (імітувати).

Одним з таких параметрів є спектральний склад сигналу. Порівняння виміряного спектра абонентського пристрою з його шаблоном і зіставлення з MAC-адресою дозволить ідентифікувати абонентів, і здійснювати наступні заходи щодо забезпечення безпеки бездротових мереж.

1. Здійснювати контроль доступу. Обмеження з'єднання до мережі тільки пристроїв, зареєстрованими в мережі, що захищається, блокувавши підключення пристроїв, що не зберігаються в базі конкретної мережі.

2. Мінімізувати зловмисні дії, вчинені шляхом підключення до мережі під чужим ім'ям (MAC, IP). Спектр пристроїв підробити не так просто як MAC або IP.

Прийнято вважати, що спектр випромінювання Wi-Fi пристроїв визначений відповідним стандартом є незмінним, але вимірювання реальних спектрів показали, що це не так.

Всі вимірювання проводилися за допомогою спектрального аналізатора Signal Hound USB-SA44B при передачі одних і тих же даних від однієї і тієї ж точки доступу при сталості температури та відстаней. В ході досліджень з'ясувалося, що стандартом визначаються тільки граничні рівні і середні значення спектральної щільності потужності, а кожен пристрій має індивідуальні особливості спектра, приклади яких наведені на рис. 1.

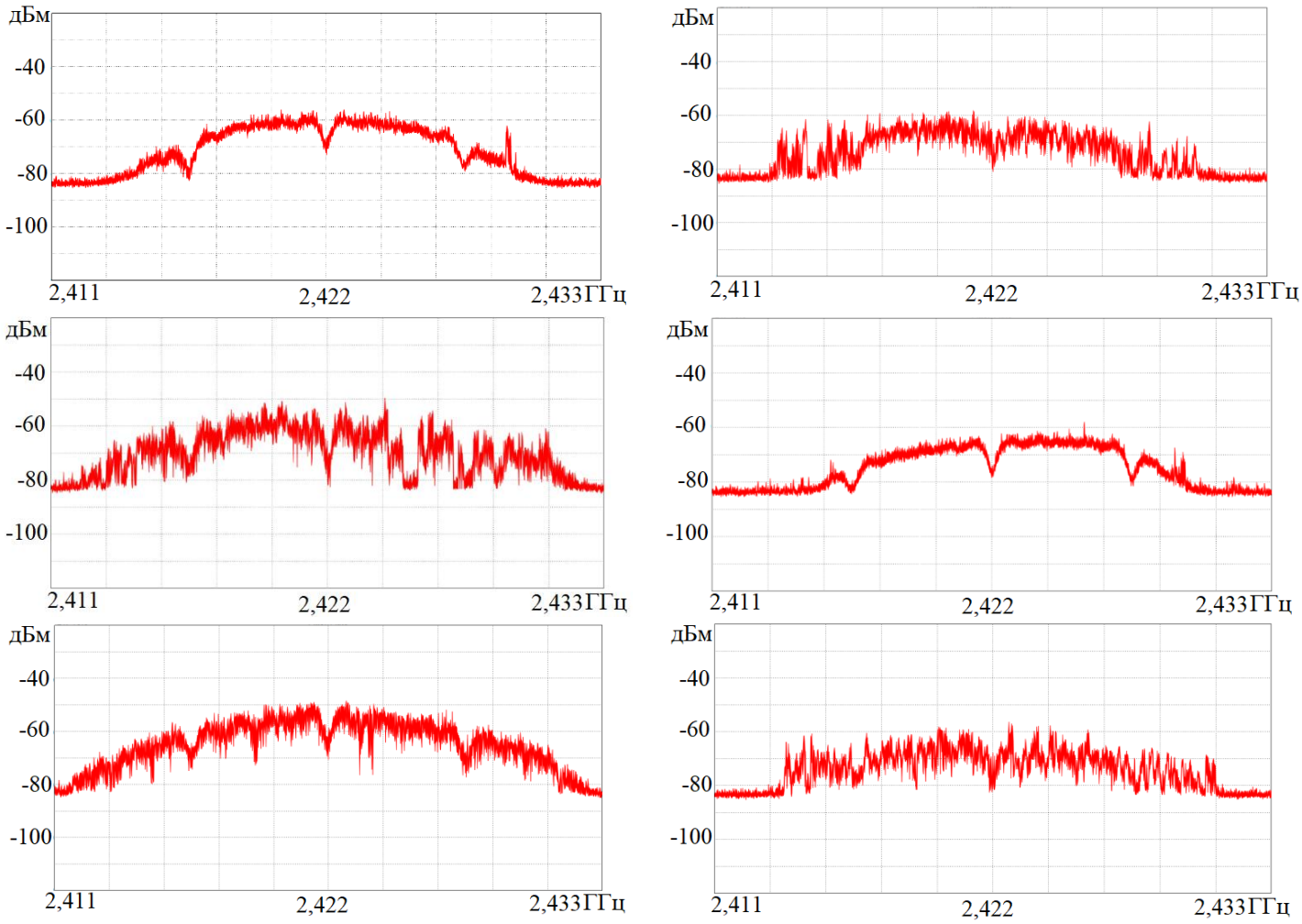


Рис. 1

Виявлено, що на вигляд спектра випромінювання впливає положення пристрою відносно прийомної антени, тому всі вимірювання проводилися в чотирьох різних положеннях. Подібність спектрів для різних положень зберігається, а потужність змінюється.

Також експериментально показано, що спектри відрізняються навіть у різних екземплярах однієї і тієї ж моделі пристрою, що показано на рис.2.

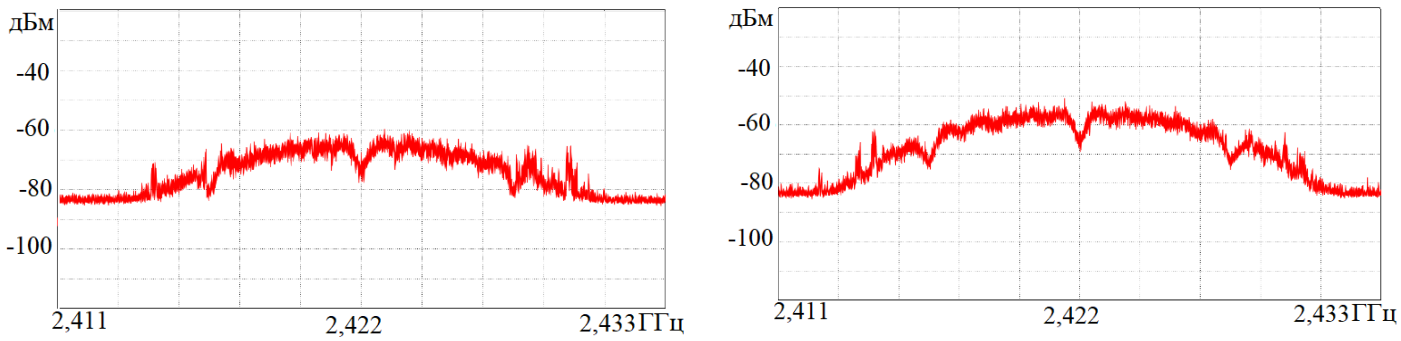


Рис. 2

Для реалізації процедури ідентифікації було розглянуто два методи.

Перший оснований на обчисленні середнього квадрата різниці (СКР) між виміряними і шаблонними спектральними відліками з поправкою на різницю в їх середньої потужності:

$$D_{L,L0} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(P_L(f_n) - P_{L0}(f_n) - P_0)^2} \qquad (1)$$

де N – кількість частот, $P_L(f_n)$ – значення потужності кожного з виміряних спектральних відліків, $P_{L0}(f_n)$ – значення потужності шаблонних спектральних відліків, P_0 – поправка на різницю середніх потужностей виміряного і шаблонного спектру. (Всі обчислення виконуються у відносних одиницях дБ).

Шаблонні значення спектра (рис.3) отримані шляхом усереднення спектральних характеристик по чотирьом різним положенням пристрою. Літерні позначення відповідають різним моделям смартфонів А –RedmiNote 4X; В –RedmiNote 4X (аналогічний «А», але інший екземпляр); Г –Meizu M5 Note; Д – Honor 09 Lite; Е –Meizu M6 Note. Алгоритм порівняння спектрів yfdtltybq на рис. 4.

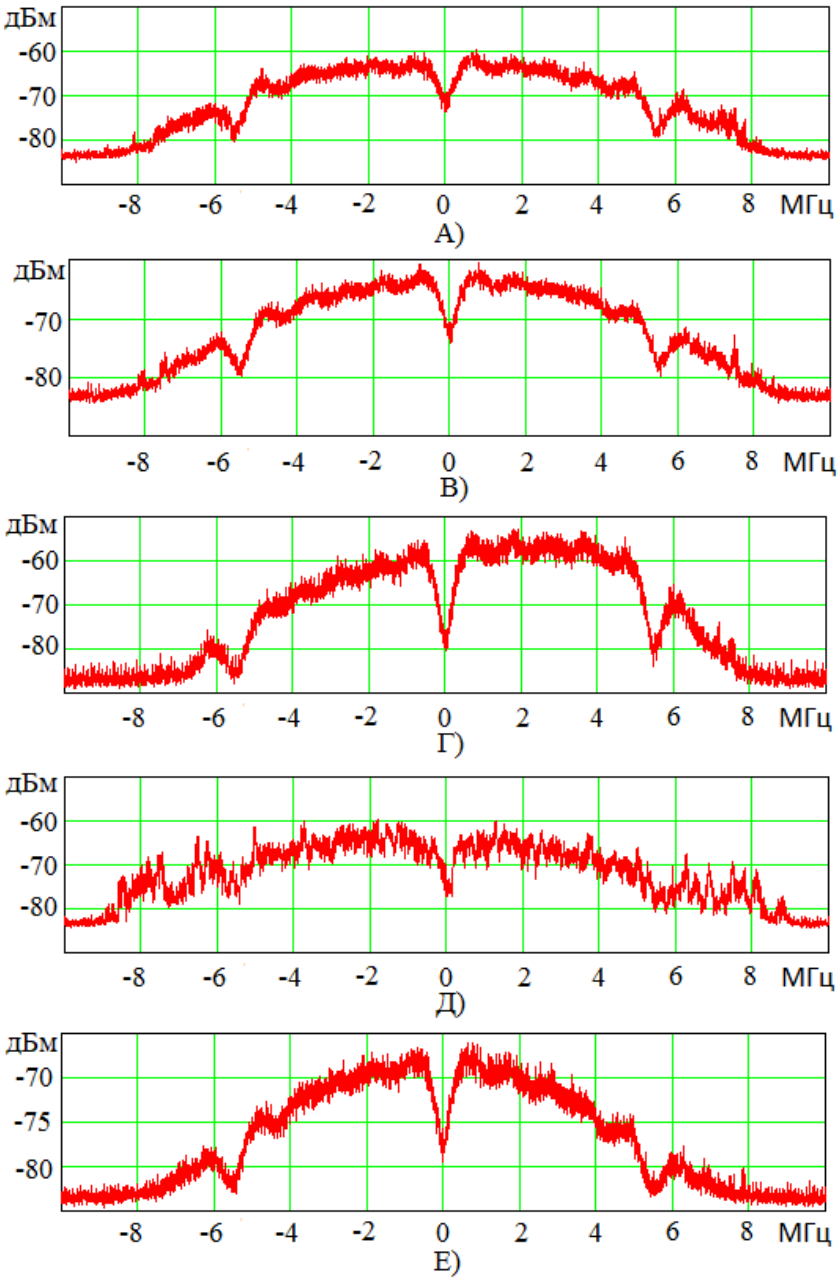


Рис.3

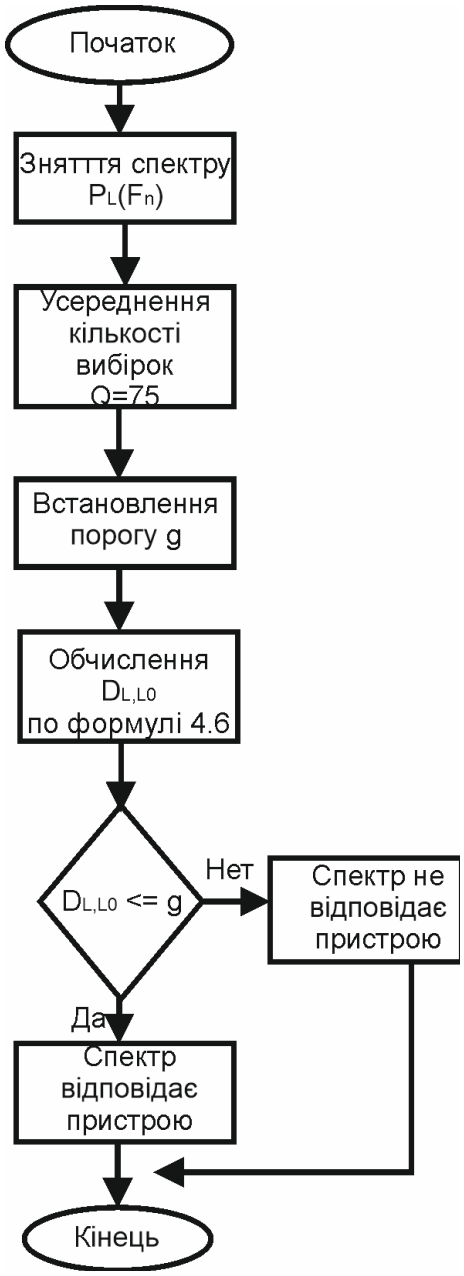


Рис.4

Таблиця 1 – Результати обчислень (1)

		Спектри пристроїв				
		А	В	Г	Д	Е
Шаблони пристроїв	А	0,7	0,9	2,2	3,5	1,4
	В	1,0	0,5	2,0	3,4	1,2
	Г	2,1	1,7	1,1	3,8	2,2
	Д	2,9	2,8	3,4	2,2	2,3
	Е	1,9	1,6	2,7	3,4	1,3

Результати обчислень СКР розраховані по (1) наведені в табл.1.

Як видно з таблиці, цифрові значення є мінімальними для шаблону і власного пристрою.

Якщо в (1) замість шаблонного спектра підставляти виміряні значення спектральних відліків інших пристроїв, то можна знайти СКР між спектрами окремих пристроїв:

$$D_{L1,L2} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(P_{L1}(f_n) - P_{L2}(f_n) - P_0)^2} \qquad (2)$$

Результати (2) наведені в табл. 2 і в графічному вигляді на рис 5, де темні плями, відповідають максимальному збігу для однакових пристроїв (мінімуму СКР).

Таблиця 2 – Результати обчислень (2)

	А	**В**	**Г**	**Д**	**Е**
А	1,1	1,2	2,3	3,5	1,7
В	1,2	0,6	2,0	3,5	1,4
Г	2,3	2,0	1,2	3,8	2,5
Д	3,6	3,5	3,8	2,4	3,1
Е	1,7	1,4	2,5	3,1	1,0

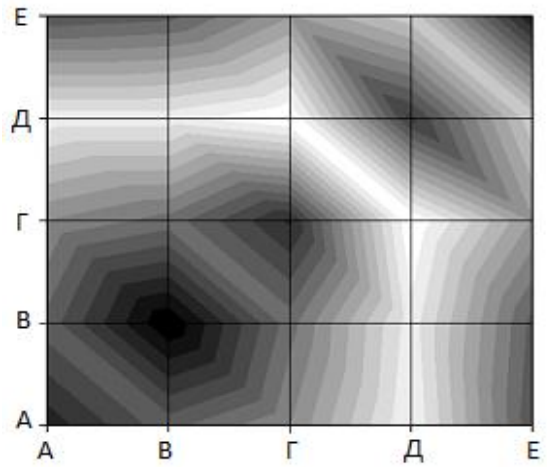


Рис. 5

Для реалізації другого методу були побудовані автокореляційні функції (АКФ) шаблонів і взаємокореляційні функції (ВКФ) шаблонів з різними пристроями згідно:

$$B(j) = \frac{1}{N}\sum_{n=0}^{N-1} P_{L1}(f_n) \cdot P_{L2}(f_{n+j}). \qquad (3)$$

Аналіз отриманих функцій не виявив залежності середньоквадратичного відхилення ВКФ, різниці в ширині ВКФ за рівнем 0,5 та істотного зсуву частоти. Різниця спектрів була зафіксована тільки в параметрах третього порядку, а саме в коефіцієнті асиметрії, який обчислювався як:

$$\mathrm{A} = \frac{\frac{1}{(2k+1)\cdot B(j)_{cp}}\sum_{j=-K}^{K}(j - j_{cp})^3 \; B(j)}{\left(\sqrt{\frac{1}{2K \cdot B(j)_{cp}} \cdot \sum_{j=-K}^{K}(J^2 \cdot \; B(j))}\right)^3}. \qquad (4)$$

Таблиця 3 – Результати обчислень (4)

Шаблоны Устройств	Спектры устройств				
	А	В	Г	Д	Е
А	0,0057	0,007	0,07	0,06	0,03
В	0,008	0,0048	0,074	0,07	0,04
Г	0,07	0,07	0,0055	0,025	0,09
Д	0,06	0,07	0.04	0,01	0,06
Е	0,024	0,03	0,09	0,07	0,016

Результати (4) наведені в табл. 3. Мінімальне значення коефіцієнту асиметрії зберігається при порівнянні шаблону з різними положеннями власного пристрою.

Проведені вимірювання та обробка їх результатів двома методами дозволяють зробити наступні висновки:

– експериментально встановлено візуальну схожість спектрів одного і того ж пристрою та суттєві відмінності у спектрах різних пристроїв;

– розглянута оцінка порівняння спектрів може бути використана для ідентифікації Wi-Fi пристроїв.

У третьому розділі дисертації «Ідентифікація користувачів Wi-Fi мережі по місцеположенню їх пристроїв» розглядається можливість використання місцеположення користувача мережі, як одну з ідентифікуючих ознак.

Само по собі місцеположення не є інформативним. Якщо цю ознаку використовувати спільно з системами захисту,наприклад такими як системи виявлення вторгнень. Це дозволить істотно розширити можливості таких систем та дозволить здійснювати наступні заходи щодо забезпечення безпеки бездротових мереж:

1. Здійснювати контроль доступу. Обмеження з'єднання до мережі лише межами фізичного периметра, блокувавши спроби підключення з територій, що знаходяться за межами фізичного периметра, навіть якщо підключається цілком легальний користувач.

2. Здійснювати контроль стаціонарного обладнання. Забезпечить повний контроль стаціонарного бездротового обладнання (комп'ютери, камери, принтери і т. д.). Зміна місця розташування стаціонарних пристроїв свідчить про неправомірні дії (крадіжки).

3. Визначення місцеположення джерела несанкціонованих дій. Для мінімізації ризиків витоку конфіденційної інформації сервіс визначення місцеположення дозволить швидко визначити джерело несанкціонованих дій та застосувати відповідні дії, відновивши нормальне функціонування бездротової мережі.

Виходячи з суті та принципів організації різних видів атак на бездротові мережі, показано, що знання місцеположення абонента, дозволяє виявляти атаки виду: «абонент-шахрай»; «помилкова точка доступу»; «man in the middle» і допомагає визначити джерело при атаці «глушіння».

За результатами аналізу методів визначення місцеположення пристроїв абонентів для застосування в бездротових Wi-Fi мережах найбільш доцільним є метод оцінки потужності сигналів опорних вузлів. У порівнянні з іншими, він показує високу точність позиціонування в тому числі, в закритих приміщеннях. Для його реалізації найкраще підходить одна з різновидів методу, а саме так званий метод радіовідбитків (заснований на побудові радіокарти).

Похибка методу радіокарт була оцінена експериментально.

Для приміщення були отримані три радіокарти від трьох точок доступу (рис.6).

Рис. 6

Показано, що рівні сигналу від кожної з точок доступу в одній і тій же опорній точці значно відрізняються. Положення дверей і вікон практично не впливає на рівень сигналу. Найбільш істотно впливає поворот приймача навколо осі. Можлива похибка тут становить близько 5 дБ, що дозволяє оцінити похибку у визначенні відстані в 2,5 метри для однієї ТД, або 1,3 м для трьох точок доступу. На межах зон обслуговування через велику протяжність зон зі слабким сигналом похибка може збільшуватися до 3..5 м.

На підставі експериментальних даних і результатів їх обробки можна зробити висновок, що

– місцеположення служить ідентифікуючою ознакою;

– знання місцеположення дозволяє запобігти ряду атак;

– для визначення місцеположення може бути використаний метод радіовідбитків.

Четвертий розділ дисертації присвячений ефективності запропонованих методів порівняння спектра при наявності шума. У ньому також висловлені рекомендації щодо практичного використання запропонованих методів.

Основна частина роботи була проведена експериментально, але при великому відношенні сигнал/шум. Для перевірки того, наскільки шум впливає на можливість ідентифікації по спектру, було застосовано моделювання. Воно дозволило оцінити ймовірні характеристики запропонованого методу в самих різних умовах, що для реального експерименту було б складно.

Була створена математична модель шуму та імітація його додавання до експериментально отриманих спектрів. У моделі виходили з того, що в кожній частотній смузі відбувається векторне додавання сигнальної $\overrightarrow{S(fi)}$ та шумової $\overrightarrow{n(fi)}$ складових:

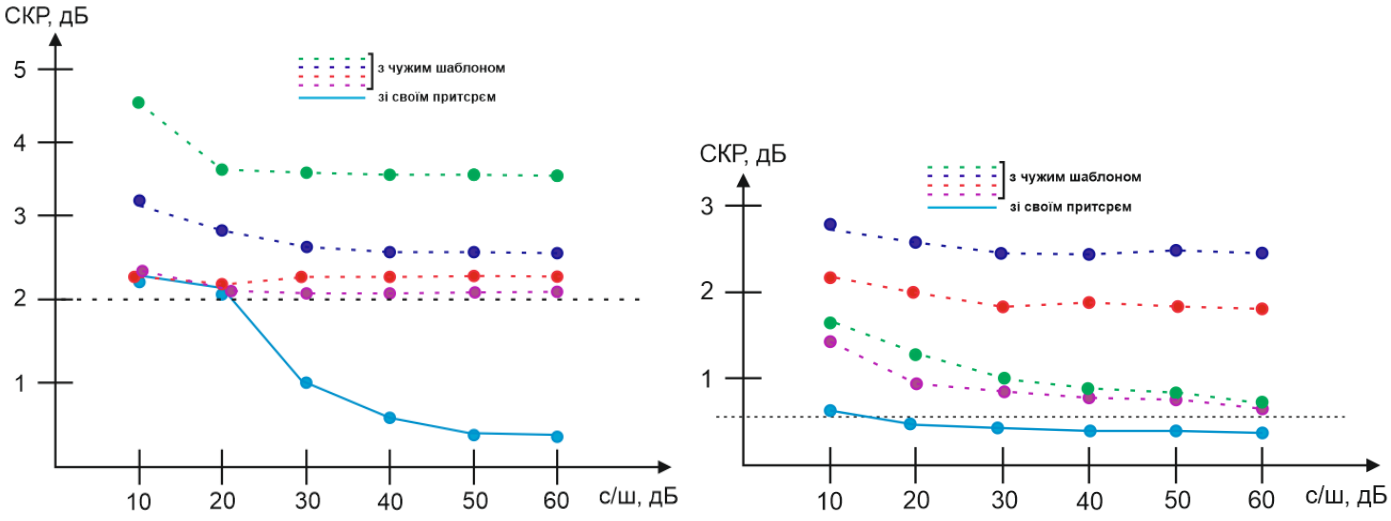
$$\overrightarrow{S`(f_i)} = \overrightarrow{KS(f_i)} + \overrightarrow{n(f_i)}, \qquad (5)$$

де K – коефіцієнт, що визначає відношення сигнал/шум.

При такому додаванні може відбуватися як збільшення модуля (потужності) спектральної вибірки, так і її зменшення. Значення фази сигналу при моделюванні невідоме і приймається рівним нулю. Тоді значення модуля знаходимо як:

$$|S`(f_i)| = \sqrt{(KS(f_i) + n(f_i)\cos\varphi(f_i))^2 + (n(f_i)\sin\varphi(f_i))^2}. \qquad (6)$$

Для методу, що ґрунтується на розрахунках СКР результати вимірювань по відношенню до одного з шаблонів наведені на рис.7 (а – по відношенню до шаблону Г; б – по відношенню до шаблону В).



а) в)

Рис. 7

З графіків можна зробити наступні висновки:

– СКР спектральних відліків для «свого» пристрою і шаблону залишається мінімальним при будь-якому відношенні сигнал/шум;

– при зменшенні відношення сигнал/шум абсолютне значення СКР росте;

– при зменшенні відношення сигнал/шум, відмінності між різними СКР зменшуються, що теж цілком закономірно, оскільки чим більший шум, тим в більше згладжуються відмінності між спектрами, «стираються» їх індивідуальні особливості.

Наведені графіки дозволяють оцінити значення порогу на рівні 0,6 … 2 дБ, але не дають можливості зробити висновок про ймовірність помилкової тривоги або правильного виявлення. Графічним представленням щодо розрізнення результатів при малих відношеннях сигнал/шум можуть служити гістограми, показані на рис. 8. Вони отримані в ході багаторазової імітації різних шумових реалізацій і при різних варіантах повороту порівнюваного пристрою.

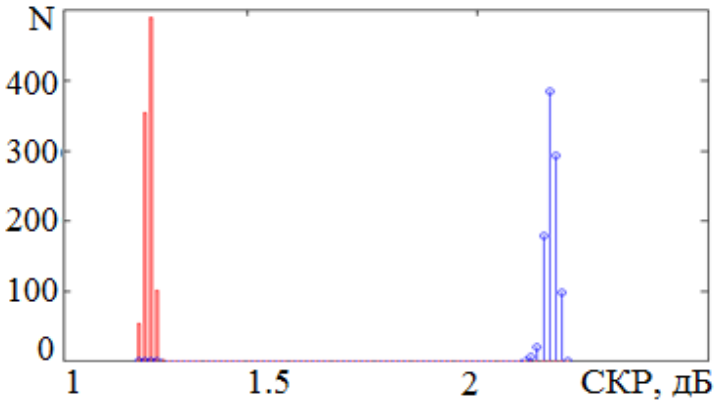


Рис. 8

При зменшенні відношення сигнал/шум від 25 дБ і менше, починають виникати помилки. Графічним представленням результатів при великих відношеннях сигнал/шум можуть бути гістограми, показані на рис. 9.

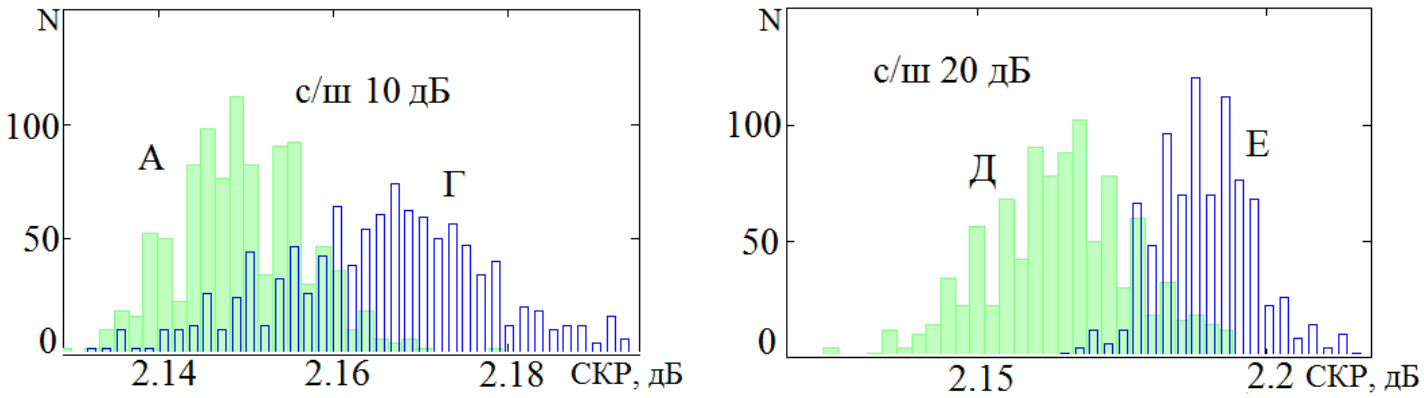


Рис. 9

Були досліджені залежності ймовірності пропуску цілі $P_{ПЦ}$ (помилки першого роду) та помилкової тривоги $P_{ЛТ}$ (помилки другого роду). На рис. 10 показані ймовірності для відношення сигнал/шум 10, 20 і 25 дБ.

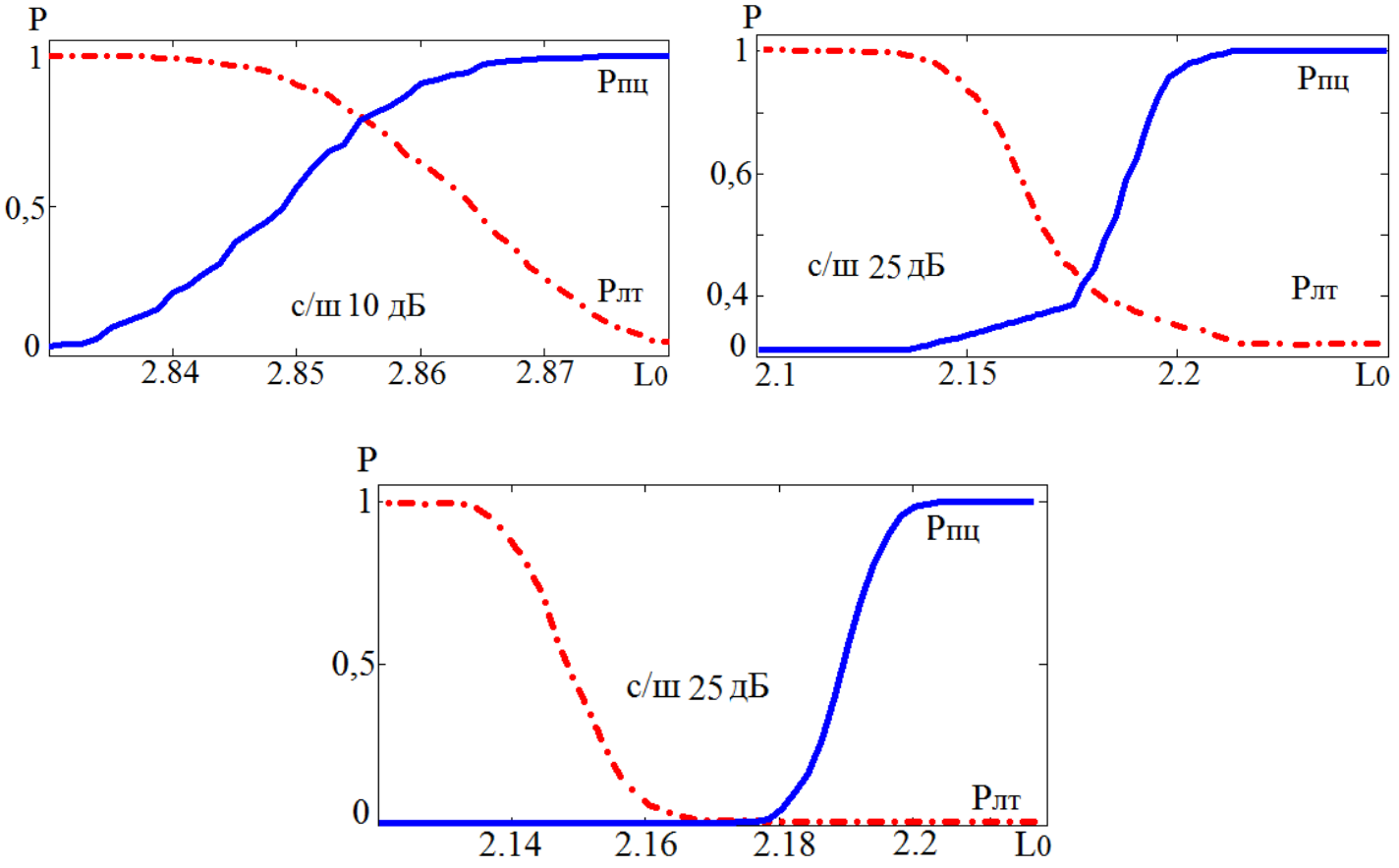


Рис. 10

При малих відношеннях сигнал/шум і особливо при початковій схожості спектрів, помилки ідентифікації при строго встановлених порогах неминучі. Для таких випадків запропоновано ввести два пороги (сіру зону) і оцінювати її за допомогою елементів нечіткої логіки.

Для методу основаного на розрахунках коефіцієнта асиметрії результати вимірювань по відношенню до одного з шаблонів представлені рис. 11 (а – по відношенню до шаблону Г; б – по відношенню до шаблону А).

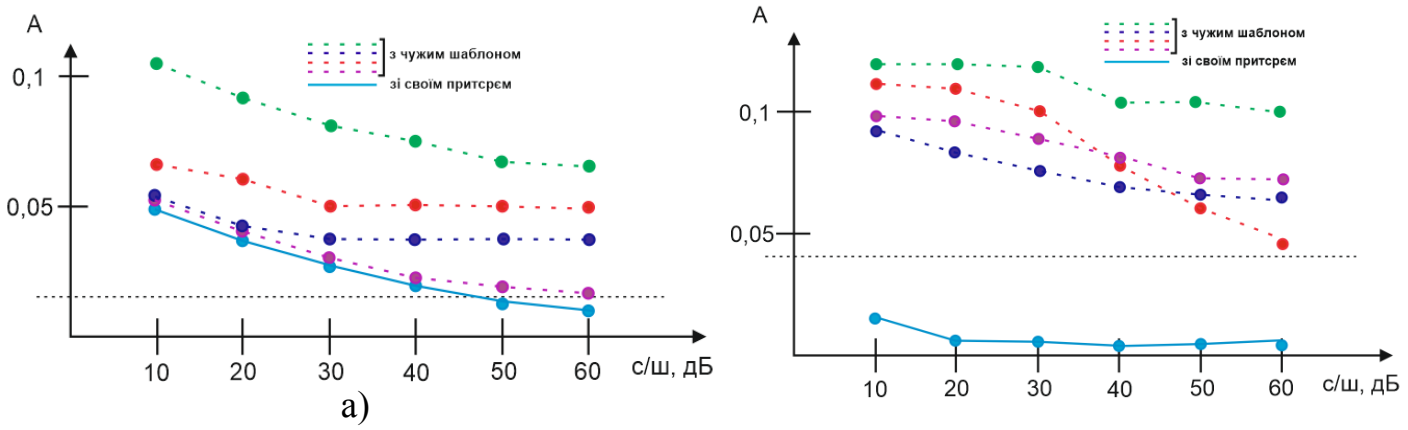


Рис.11

З графіків можна зробити наступні висновки:

– коефіцієнт асиметрії для різних пристроїв значно відрізняється, що дозволяє оцінити значення порогу однозначно;

– при зменшенні відношення сигнал/шум абсолютне значення коефіцієнту асиметрії росте;

– при порівнянні двох різних пристроїв однакової моделі значення коефіцієнтів асиметрії дуже близькі вже при відношенні сигнал/шум 40 дБ.

При відношенні сигнал/шум від 40 дБ і менше, для пристроїв однакових моделей починають виникати помилки. Графічним представленням результатів служить гістограма, на рис. 12. Залежності ймовірності пропуску цілі $P_{ПЦ}$ та помилкової тривоги $P_{ЛТ}$ наведені на рис. 13 для відношення сигнал/шум 40 дБ. Дані залежності зберігаються при відношенні сигнал/шум 30, 20 та 10 дБ.

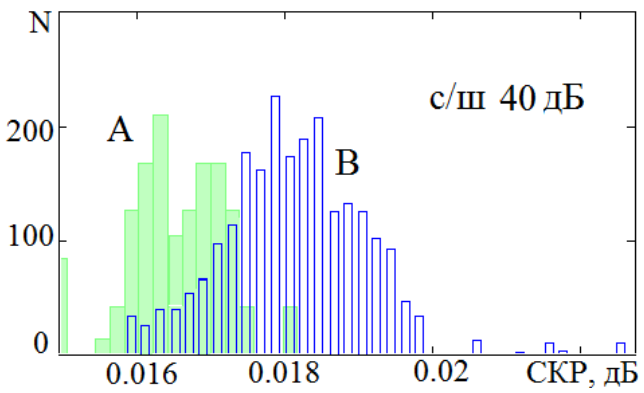


Рис. 12

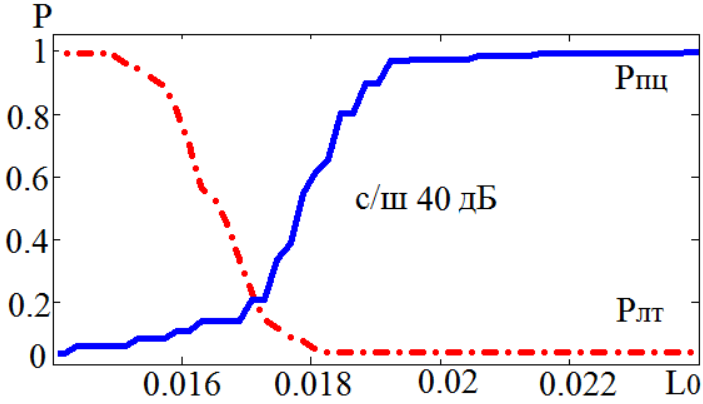


Рис. 13

Виходячи з суті та принципів організації різних видів атак на бездротові мережі, у роботі показано, що при наявності ідентифікації абонентів по спектру, можна виявити атаки типу «man in the middle», «абонент-шахрай», «помилкова точка доступу» і «глушіння» де класичні методи захисту не завжди справляються.

ВИСНОВКИ

У дисертаційній роботі вирішена актуальна науково-практична задача ідентифікації пристроїв бездротових мереж шляхом врахування ознак фізичного рівня мереж з метою підвищення їх безпеки.

В ході вирішення вказаної задачі отримані такі науково-практичні результати:

1. Вперше запропоновано метод ідентифікації користувачів Wi-Fi мереж, відмінною особливістю якого є детальний аналіз спектральних характеристик випромінювання їх пристроїв, що дозволяє виявляти спроби втручання в мережу шляхом імітації роботи авторизованих користувачів.

2. Розроблено новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв, відмінною особливістю якого є обчислення середнього квадрату різниці відповідних спектральних відліків з урахуванням різниці в середній потужності різних сигналів, що дозволяє порівнювати спектри, отримані в різних умовах, з еталонним.

3. Запропоновано новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом оцінки коефіцієнта асиметрії взаємокореляційної функції спектру Wi-Fi пристроїв.

4. Отримав подальший розвиток метод виявлення атак на бездротову мережу, що полягає у використанні даних про місцезнаходження користувачів в мережі, які визначаються за рівнем RSSI з використанням радіоовідбитків, що дозволяє виявляти атаки, що не виявляються за іншими ознаками.

5. Розроблено нову модель, що імітує спектр сигналу Wi-Fi мережі в умовах впливу шуму, що дозволяє оцінити ефективність розроблених методів в реальних умовах і виробити рекомендації щодо їх практичного застосування.

Основний науковий результат полягає в розробці та експериментальній перевірці методів ідентифікації пристроїв в бездротові мережі, що відрізняються від раніше відомих тим, що в них використовуються ознаки стану мережі на фізичному рівні, що дозволяють виявляти і спільно з системами виявлення вторгнень запобігати ряду атак і тим самим підвищувати безпеку Wi-Fi мереж .

Практична цінність роботи полягає в експериментально встановленій схожості спектрів Wi-Fi сигналів одного і того пристрою в різних положеннях та виявлено істотну різницю в спектрах випромінювання різних пристроїв, що може бути використано для їх ідентифікації. Розроблено методику визначення місцезнаходження абонента бездротової мережі за рівнем RSSI з використанням методу радіоовідбитків. Показано, що похибка у визначенні місцеположення становить 2.5 м при застосуванні детермінованого (евклідова відстань) підходу визначення координат в закритому приміщенні. В

ході моделювання встановлено, що можливість розпізнавання спектрів різних пристроїв по значенню СКР зберігається до відношення сигнал/шум 20 дБ. При відношенні сигнал/шум 30 дБ і більше спектри пристроїв розрізняються з ймовірністю, вище ніж 0,999 (жодної помилки на 1000 випробувань). При оцінюванні по значенню коефіцієнтів асиметрії для різних пристроїв розпізнавання спектрів зберігається до відношення сигнал/шум 10 дБ. Виняток складають пристрої однакової моделі, де помилки можуть виникати при відношенні сигнал/шум 40 дБ.

Використання результатів дисертаційних досліджень підтверджується трьома актами впровадження.

СПИСОК ПУБЛІКАЦІЙ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Василенко Т. А. Применение нечеткой логики для повышения безопасности сетей на основе технологии Wi-Fi / И. Е. Антипов, Т. А. Василенко, Нух Таха Насиф // Межведомственный научно-технический сборник «Радиотехника». – 2011. – Вып. 165. – С. 103 – 106.

2. Василенко Т. А. Применение теории игр для защиты беспроводных Wi-Fi сетей / И. Е. Антипов, Т. А. Василенко, В. С. Вовченко // Межведомственный научно-технический сборник «Радиотехника». – 2013. – Вып. 173. – С. 204 – 207.

3. Василенко Т. А. Разработка модели Wi-Fi сети с целью предотвращения вторжений / И. Е. Антипов, Т. А. Василенко, И. В. Михеев // Восточно-Европейский журнал передовых технологий. – 2014. – Т.1 № 9 (67). – С. 4 – 8.

4. Василенко Т. А. Совершенствование модели Wi-Fi сети с целью предотвращения вторжений / И. Е. Антипов, Т. А. Василенко, Е. Ю. Бондар // Межведомственный научно-технический сборник «Радиотехника». – 2014. – Вып. 177. – С. 60 – 63.

5. Василенко Т. А. Применение шумоподобных сигналов в радиолокации / Т. А. Василенко, В. С. Вовченко, Е.В. Шарапова // Межведомственный научно-технический сборник «Радиотехника». – 2014. – Вып. 179. – С. 18 – 22.

6. Василенко Т.А. Improving the model of decision making about abnormal network state using a positioning system / И. Е. Антипов, Т. А. Василенко // Восточно-Европейский журнал передовых технологий. – 2019. – Т.1 № 9 (97). – С. 4 – 8. (Scopus)

7. Василенко Т. А. Идентификация мобильных устройств по особенностям спектров их сигналов / И. Е. Антипов, Т. А. Василенко // Межведомственный научно-технический сборник «Радиотехника». – 2020. – Вып. 179. – С. 91 – 97.

8. Василенко Т.А. Применение Применение нечеткой логики для повышения безопасности Wi-Fi сети / Т.А. Василенко // Сборник научных трудов по материалам XV международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», апрель 2011г. – Харьков, Украина. – 2011. – Т.3. – С. 277 – 278.

9. Василенко Т.А. Применение нечеткой логики для анализа состояний радиотехнических систем / Т.А. Василенко // Сборник научных трудов по материалам XVI международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», апрель 2012г. – Харьков, Украина. – 2012. – Т.3. – С. 214 – 215.

10. Василенко Т.А. Применение нечеткой логики для повышения безопасности сетей на основе технологии Wi-Fi / И. Е. Антипов, Т.А. Василенко // Сборник научных трудов по материалам 23- Международной Крымской конференция «СВЧ-техника и телекоммуникационные технологии», 9-13 сентября 2013г. – Севастополь, Украина. – 2013.– С. 472 – 473. (Scopus)

11. Василенко Т.А. Применение теории игр для анализа состояния радиотехнических систем / Т.А. Василенко // Сборник научных трудов по материалам XVII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», апрель 2013г. – Харьков, Украина. – 2013. – Т.3. – С. 165 – 166.

12. Василенко Т.А. Математическое моделирование для анализа безопасности беспроводных сетей / Т.А. Василенко // Сборник научных трудов по материалам XVIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», 14-16 апреля 2014г. – Харьков, Украина. – 2014. – Т.3. – С. 203 – 204.

13. Василенко Т.А. Совершенствование модели Wi-Fi сети с целью предотвращения вторжений / Т.А. Василенко // Сборник научных трудов по материалам XVIIII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», апрель 2015г. – Харьков, Украина. – 2015. – Т.3. – С. 115 – 116.

14. Василенко Т.А. Радиотехнические методы идентификации абонентов в сетях IEEE 802.11 / Т.А. Василенко // Сборник научных трудов по материалам XXII международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», апрель 2018г. – Харьков, Украина. – 2018. – Т.3. – С. 117 – 118.

15. Василенко Т.А. Экспериментальное исследование спектров Wi-Fi передатчиков / Т.А. Василенко // Сборник научных трудов по материалам XXIV международного молодежного форума «Радиоэлектроника и молодежь в XXI веке», 2020г. – Харьков, Украина. – 2020. – Т.3. – С. 132 – 133.

АНОТАЦІЯ

Василенко Тетяна Олександрівна. Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі. – На правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук за спеціальністю 05.12.17 – радіотехнічні та телевізійні системи. Харківський національний університет радіоелектроніки, Харків 2021.

У дисертаційній роботі вирішена актуальна науково-практична задача ідентифікації пристроїв бездротової мережі шляхом врахування ознак фізичного рівня мереж з метою підвищення їх безпеки.

В ході огляду зроблено висновок, що існуючі системи захисту бездротових мереж не можуть забезпечити необхідного рівня безпеки, в тому числі тому, що в них не використовуються параметри фізичного рівня моделі OSI.

Для врахування параметрів фізичного рівня в роботі пропонується спільно з системами виявлення вторгнень використовувати метод ідентифікації користувачів мережі

за спектрами їх пристроїв та за рівнем потужності, що дозволить виявити атаки типу «man in the middle», «абонент-шахрай» і «помилкова точка доступу », а так само сприяє визначенню місцеположення джерела при атаці« глушіння ».

В ході дослідження виявлено, що спектри різних мобільних пристроїв є в значній мірі унікальними, що може служити ідентифіуючою ознакою.

Для практичної реалізації ідентифікації розроблені методи порівняння спектрів різних пристроїв, основані на обчисленні середнього квадрату різниці і на обчисленні коефіцієнтів асиметрії їх кореляційних функцій. За результатами розрахунку показано, що середній квадрат різниці спектральних відліків для шаблону і відповідного йому пристрою істотно менше, ніж для чужих пристроїв, а коефіцієнт асиметрії однозначно розрізняє різні пристрої при будь-якому відношенні сигнал/шум, але допускає помилки при порівнянні пристроїв однакових моделей.

Для практичної реалізації визначення місцеположення запропоновано використовувати радіокарти. Експериментально показано, що похибка даного методу становить 2,5 метра.

В дисертації показано результати моделювання шумового середовища, що дозволило порівняти спектри приладів у близьких до реальних умовах. Для методу СКР спектри різних пристроїв відрізняються з імовірністю 0,999 (із відношенням сигнал/шум 30 дБ або більше.) Для методу, основаного на коефіцієнті асиметрії, здатність розпізнавання підтримується до відношення сигнал/шум 10 дБ з тією ж ймовірністю.

Отримані результати свідчать про можливість застосування розглянутих методів на практиці, що дозволить запобігати цілому ряду атак.

Ключові слова: захищеність Wi-Fi мереж, ознаки фізичного рівня, спектральна характеристика, мысцеположення, ідентифікація.

АНОТАЦИЯ

Василенко Татьяна Александровна. Методы распознавания Wi-Fi устройств путем учета их индивидуальных признаков для повышения защищенности сети. – На правах рукописи.

Диссертация на соискание ученой степени кандидата технических наук по специальности 05.12.17 – радиотехнические и телевизионные системы. Харьковский национальный университет радиоэлектроники, Харьков 2021.

В диссертационной работе решена актуальная научно-практическая задача идентификации устройств беспроводной сети путем учета признаков физического уровня сетей с целью повышения их безопасности.

В ходе обзора сделан вывод, что существующие системы защиты беспроводных сетей не могут обеспечить необходимого уровня безопасности, в том числе потому, что в них не используются параметры физического уровня модели OSI.

Для учёта параметров физического уровня в работе предлагается совместно с системами обнаружения вторжений использовать метод идентификации пользователей сети по спектрам их устройств и по уровню мощности, что позволит выявить атаки ти-

па «man in the middle», «абонент-мошенник» и «ложная точка доступа», а так же способствует определению местоположения источника при атаке «глушение».

В ходе исследования обнаружено, что спектры различных мобильных устройств являются в значительной мере уникальными, что может служить идентифицирующим признаком.

Для практической реализации идентификации разработаны методы сравнения спектров разных устройств, основанные на вычисления среднего квадрата разности и на вычислении коэффициента асимметрии их корреляционных функций. По результатам расчета показано, что средний квадрат разности спектральных отсчетов для шаблона и соответствующего ему устройства существенно меньше, чем для чужих устройств, а коэффициент асимметрии однозначно различает разные устройства при любом соотношении сигнал/шум, но допускает ошибки при сравнении устройств одинаковых моделей.

Для практической реализации определения местоположения предложено использовать радиокарты. Экспериментально показано, что погрешность данного метода составляет 2,5 метра.

Проведено моделирование шумовой обстановки в сети, что позволило сравнить спектры устройств в условиях близким к реальным. Для метода СКР спектры различных устройств отличаются с вероятностью 0,999 (с соотношением сигнал/шум 30 дБ и более.) Для метода, основанного на коэффициенте асимметрии, способность распознавания поддерживается в отношение сигнал/шум 10 дБ с той же вероятностью.

Полученные результаты свидетельствуют о применимости рассмотренных методов на практике, что позволит предотвращать целый ряд атак**.**

Ключевые слова: защищенность Wi-Fi сетей, признаки физического уровня, спектральная характеристика, местоположение, идентификация.

ABSTRACT

Vasilenko T. A. Methods for the Wi-Fi devices recognizing by its individual signs for the network security improving. – Manuscript.

The thesis for the degree of Technical Sciences Candidate (equivalent of Ph. D. degree). Speciality 05.12.17 – radio and television systems. – National university of radioelectronics, Kharkov, 2021.

In this work, an urgent scientific and practical problem, which is the identification of wireless network devices based on the characteristics of the physical layer of networks in order to increase their security, is solved.

Based on the review, it was concluded that the existing systems for protecting wireless networks do not provide the required level of security. This is because they do not use the physical layer parameters of the OSI model.

The dissertation proposes to take into account the parameters of the physical layer (such as spectrum and power level) and use them in combine with Intrusion Detection System to identify network users. This will detect attacks such as "man-in-the-middle", "rogue subscrib-

er", "fake access point" and will help to determine the location source of a jamming attack. Experimental measurements have shown that the spectra of various mobile devices are largely unique and can serve as a distinguishing feature.

For practical identification, methods for comparing the spectra of different devices have been developed. The methods are based on calculating the mean square of the difference and calculating the coefficient of asymmetry of their correlation functions.

Calculations have shown that the root-mean-square difference of spectral readouts for the template and the corresponding device is significantly less than for extraneous devices. Also, calculations have shown that the asymmetry coefficient uniquely determines different devices at any signal-to-noise RMS ratio, but makes mistakes when comparing devices of the same model.

For the practical implementation of the location determination method, it is proposed to use radio maps. It has been shown experimentally that the error of this method is 2.5 meters.

The dissertation shows the results of modeling a noise environment, which made it possible to compare the devices spectra in close to real conditions.

For the RMS difference method, the spectra of different devices differ with a probability of 0.999 (with a signal-to-noise ratio of 30 dB or more.) For the method based on the asymmetry coefficient, the recognition capability is maintained up to a signal-to-noise ratio of 10 dB with the same probability.

The obtained results show that the considered methods can be applied in practice to prevent several types of attacks.

Keywords: security of Wi-Fi networks, signs of the physical layer, spectral characteristics, location, identification.

Підп. До друку 31.03.21 Формат 60×84 1/16. Спосіб друку – ризографія
Умов. друк. арк. 1,2 Тираж 100 прим.
Зам. № 2-198 Ціна договірна.

ХНУРЕ, 61166, Харків, просп. Науки, 14

Віддруковано в редакційно-видавничому відділі ХНУРЕ
Харків, просп. Науки, 14