МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ РАДІОЕЛЕКТРОНІКИ

Кваліфікаційна наукова
праця на правах рукопису

ВАСИЛЕНКО ТЕТЯНА ОЛЕКСАНДРІВНА

УДК 621.396.2

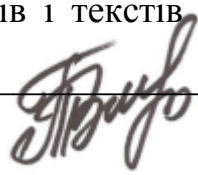
ДИСЕРТАЦІЯ

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

05.12.17 – радіотехнічні та телевізійні системи

Подається на здобуття наукового ступеня кандидата технічних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело



_____ Т.О. Василенко

Науковий керівник Антіпов Іван Євгенійович, доктор технічних наук, професор

Харків – 2021

АНОТАЦІЯ

Василенко Т.О. Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата технічних наук (доктора філософії) 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 (фальшива) точка доступу », а так само сприяє визначенню місця розташування 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, засновані на обчисленні середнього квадрату різниці і на обчисленні коефіцієнта асиметрії їх кореляційних функцій. За результатами розрахунку показано, що середньоквадратична різниця спектральних відліків для шаблону і відповідного йому пристрої істотно менше, ніж для

чужих пристроїв, а коефіцієнт асиметрії однозначно розрізняє різні пристрої при будь-якому співвідношенні 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 співвідношенням сигнал/шум 30 дБ або більше.) Для методу, заснованого 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, місцеположення, ідентифікація.

Список публікацій здобувача:

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.

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 subscriber", "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.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АКФ – автокореляційна функція

ВКФ – взаємокореляційна функція

СКВ – середньоквадратичне відхилення

СКР – середній квадрат різності

СВВ – системи виявлення вторгнень

BPSK – binary phase-shift keying

DBPSK – differential binary phase-shift keying

DCF – distributed coordination function

DoS – denial of service

DQPSK – differential quadrature phase shift keying

DSSS – sequence spread spectrum

HCF – hybrid coordination function

IDS – Intrusion Detection System

IEEE – institute of electrical and electronics engineers

IoT – internet of things

IP – internet protocol

LLC – logical link control

MAC – media access control

MIMO – multiple-input multiple-output

MU-MIMO – multi user multiple-input multiple-output

NGFW – next generation firewall

OFDM – Orthogonal frequency-division multiplexing

OSI – open system interconnection

PCF – point coordination function

PHY – physical layer protocol

PLCP – physical layer convergence procedure

PMD – physical medium dependent

QAM – Quadrature Amplitude Modulation

QoS – quality of service

QPSK – quadrature phase shift keying

RSSI – received signal strength indicator

SC – single carrier

SISO – single input single output

SQPS – staggered quadrature phase shift keying

SU-MIMO – single user multiple-input multiple-output

CSMA/CA – carrier sense multiple access / collision avoidance

TBTT – set of target beacon transmission time

TLS/SSL – transport level security / secure sockets layer

WIDS – wireless intrusion detection system

Wi-Fi – wireless fidelity

WIPS -wireless intrusion prevention system

ВСТУП

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].

Примечание:

[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.

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 підвищує безпеку Wi-Fi мереж .

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

1. Вперше запропоновано метод ідентифікації користувачів Wi-Fi мереж на основі детального аналізу 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 шляхом 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.

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, 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.

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 та1 систем технічного захисту інформації (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 рівнем RSSI з використанням методу радіовідбитків. В статті [7] здобувач розробив метод обробки результатів вимірювання спектрів випромінювання мобільних Wi-Fi пристроїв шляхом обчислення середнього квадрата різниць 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 року); 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, включених до переліку наукових фахових видань України, затвердженого Міністерством освіти і науки України та 1 стаття, що індексується в 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.

РОЗДІЛ 1
БЕЗПЕКА БЕЗДРОТОВИХ МЕРЕЖ ЯК БАГАТОФАКТОРНА ЗАДАЧА

У першому розділі розглянуто бездротову технологію стандарту IEEE 802.11 з точки зору захисту інформації, що передається по каналу зв'язку. У ньому викладено принцип передачі інформації за допомогою бездротової технології, загрози і вразливості, що є невід'ємною частиною технології Wi-Fi, у зв'язку з недоліками процесу функціонування, властивостями архітектури мережі, протоколами обміну та інтерфейсами, програмним забезпеченням, що застосовується та апаратною платформою, умовами експлуатації та розташування. Зроблено огляд основних методів захисту та їх недоліків. Розглянуто приклади існуючих засобів захисту бездротових Wi-Fi мереж.

1.1 Технологія Wi-Fi.

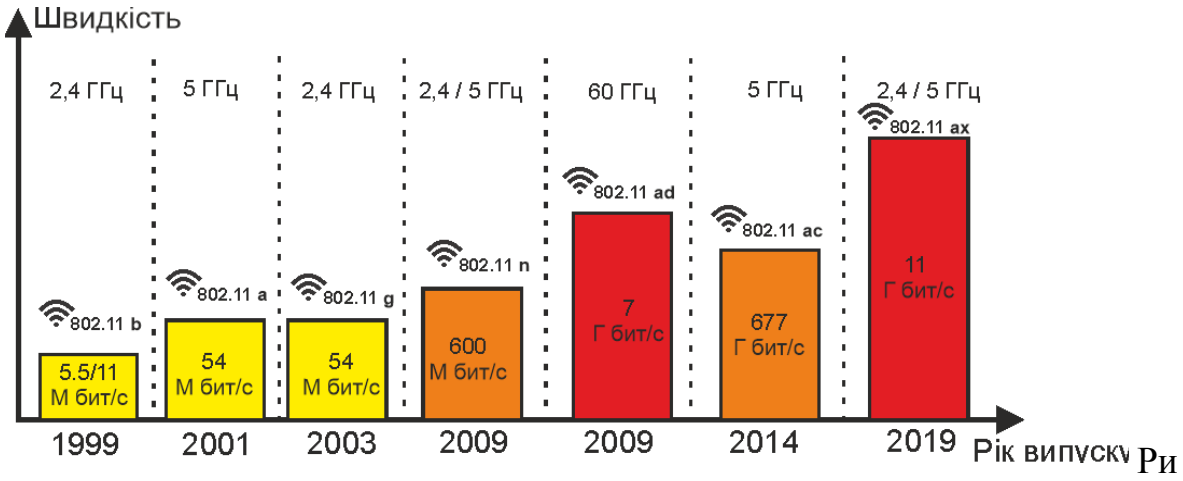
Wi-Fi (Wireless Fidelity) – це сімейство протоколів бездротової передачі даних IEEE 802.11x (802.11a, 802.11b, 802.11g, 802.11n и т. д.) [16]. Комітет по стандартам IEEE (Institute of Electrical and Electronic Engineers, Міжнародний інститут інженерів електротехніки та електроніки) сформував робочу групу по стандартам для бездротових локальних мереж 802.11 в 1990 році.

Стандарт бездротової мережі 802.11x, який є складовою частиною стандартів локальних мереж IEEE 802.x, охоплює тільки два нижніх рівні у семирівневій моделі OSI (Open System Interconnection) – фізичний і канальний, найбільшою мірою відображають специфіку локальних мереж. Бездротові мережі відрізняються від кабельних мереж на фізичному і частково на канальному (MAC) – рівнях моделі взаємодії OSI.

Різні версії бездротових локальних мереж стандарту IEEE 802.11 регламентують передачу даних в діапазонах 2,4 і 5 ГГц (за виключення стандарту 802.11ad, який працює на частоті 60 ГГц).

Сімейство стандартів 802.11 включає в себе сім основних стандартів, які використовуються для організації передачі даних, що показано на рисунку 1.1 [17]. У табл. 1.1 наведені їх основні характеристики [18, 19].

У табл. 1.1 наведені їх основні характеристики [18, 19].



сунок 1.1 – Еволюція стандартів групи IEEE 802.11

Через зростання кількості мобільних користувачів, потрібне ефективне здійснення комунікацій між ними. У зв'язку з цим відбувається інтенсивний розвиток технологій бездротових комунікацій. Особливо це актуально щодо бездротових Wi-Fi мереж.

Перевагами Wi-Fi-мереж в порівнянні зі звичайними кабельними мережами є:

– швидке розгортання;

– мобільність користувачів в рамках діючих зон мережі;

– високі швидкості передачі даних;

– сумісність з кабельними мережами.

– єдиним виходом, коли немає можливості прокласти кабель для звичайної мережі.

Таблиця 1.1

Стандарт	802.11 b	802.11 a	802.11 g	802.11 n	802.11 ad	802.11 ac	802.11 ax
Частотний діапазон, ГГц	2,4	5	2,4	2,4 / 5	60	5	2,4 / 5
Технологія формування сигналів	DSSS	DSSS, OFDM	DSSS, OFDM	OFDM	SC, OFDM	OFDM	OFDM
Швидкість, біт/с	5,5/11 М	54 М	54 М	600 М	7 Г	6,77 Г	11 Г
Метод полосової модуляції	DBPSK, DQPSK	BPSK, QPSK, 64-QAM	BPSK, QPSK	BPSK, 64-QAM	SQPS, QPSK, QAM,	256-QAM	1024-QAM
Ширина каналів, МГц	20	20	20	20, 40	до 2 ГГц	20,40,80, 160, 80+80	20,40,80, 160, 80+80
Антенні технології	SISO	SISO	SISO	SU-MIMO	SISO	MU-MIMO	MU-MIMO
Дальність зв'язку в приміщенні, м	30		20-50	50-100	2-10	50-100	50-100
Дальність зв'язку поза приміщенням, м	125	150	250	500	2-10	300-500	300-500

Серед великої кількості переваг Wi-Fi-мереж існує вагомий недолік – безпека даних мереж, пов'язана з передачею даних через радіо ефір.

Для того щоб зрозуміти суть проблеми забезпечення безпеки, при передачі інформації по бездротових каналах зв'язку, більш детально розберемося в принципі дії самих Wi-Fi-мереж.

1.1.1 Частотні канали Wi-Fi

Більшість Wi-Fi пристроїв працюють в двох частотних діапазонах 2,4 ГГц (802.11 b/g/n) и 5 ГГц (802.11 a/n/ac).

В діапазоні 2,4 ГГц стандартами визначено 14 каналів. В Україні дозволено використовувати тільки 13 каналів. Кожен канал займає ширину в 20 (40) МГц. Номери каналів і їх центральні частоти наведені на рис. 1.2 [17].

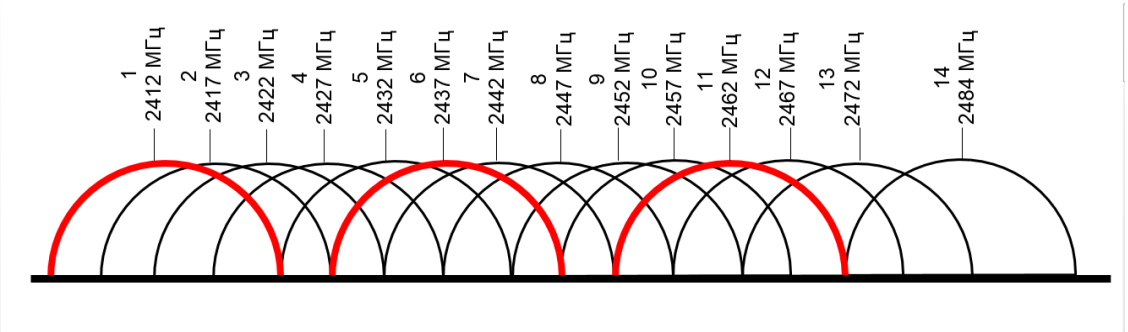


Рисунок 1.2 – Канали Wi-Fi в діапазоні 2.4 ГГц

Канали з номерами 1, 6 і 11 вважаються повністю непересічними по частотах. Але, якщо точки доступу будуть розташовані близько один до одного, то і непересічні канали стають пересічними, що показано на рисунку 1.3 [17].

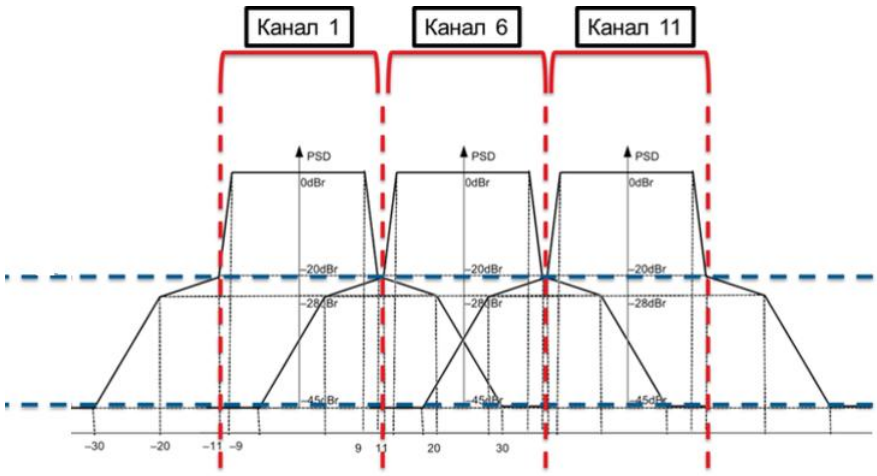


Рисунок 1.3 – Непересічні канали Wi-Fi в діапазоні 2.4 ГГц

Одним з недоліків діапазону 2,4 ГГц є його висока завантаженість і мала кількість каналів. Перешкоди для Wi-Fi-мережі можуть створювати не тільки Wi-Fi-пристрої, але і Bluetooth-пристрої, бездротові камери, побутова техніка, що працюють в цьому ж частотному діапазоні. Для мінімізації взаємних впливів потужність Wi-Fi-передавачів строго обмежена і регламентована.

Діапазон частот варіюється від 5, 170 ГГц до 5,905 (19 непересічних каналів). Зі збільшенням частоти збільшується і швидкість передачі даних, але

росте загасання. Для збільшення швидкості передачі даних в цьому діапазоні використовують технологію MIMO [5]. Дану частоту частіше використовують в невеликому радіусі. Наприклад, для підключення телевізора, комп'ютера або ноутбуку поблизу роутера.

Також великим мінусом цього діапазону являється його нестійкість до завад. Сигнал сильно затухає: від стін, скла, металу, дерев – чим 2.4 ГГц.

1.1.2 Топологія бездротових мереж

Мережі стандарту 802.11 можуть будуватися по кожній із наступних топологій [16]:

- однорангова;
- інфраструктурна;
- розподілена.

Розглянемо докладніше кожну з існуючих топологій побудови бездротових мереж стандарту IEEE 802.11.

Однорангова топологія мережі (рис. 1.4) ще має назву ad-hoc (незалежна базова зона обслуговування). Станції зв'язуються безпосередньо одна з одною без використання однієї точки доступу. Розподіл часу (timing) здійснюється нецентралізовано. Клієнт, який розпочинає передачу, задає сигнальний (маячковий) інтервал (beacon interval) для створення набору моментів часу передачі маячкового сигналу (set of target beacon transmission time, TBTT). Коли завершується TBTT, кожен клієнт виконує наступне:

- призупиняє всі неспрацьовані таймери затримки (backoff timer) з попереднього TBTT;
- визначає нову випадкову затримку.

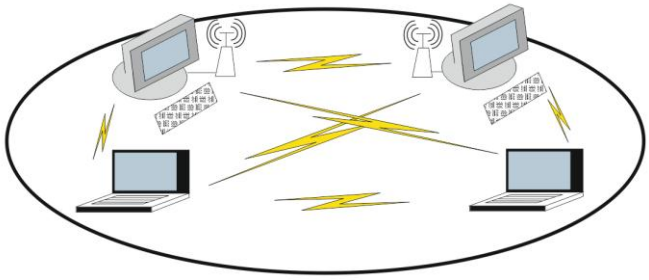


Рисунок 1.4 – Однорангова топологія мережі

Перевагою однорангової топології є простота організації, яка не потребує додаткового обладнання. Недоліком являється той факт, що дана топологія дозволяє встановити з'єднання на швидкості не більше 11 Мбіт/с, яка рівномірно ділиться на кількість підключених пристроїв [20].

Інфраструктурна топологія мережі передбачає спілкування підключених пристроїв через точку доступу, яка сама направляє передані дані станції-адресату (рис. 1.5). Точка доступу може мати порт висхідного каналу, через який базова зона обслуговування підключається до дротової мережі.

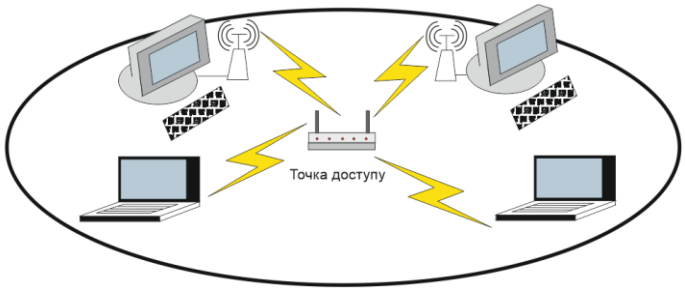


Рисунок 1.5 – Інфраструктурна бездротова локальна топологія мережі

Кілька інфраструктурних бездротових мереж можуть бути з'єднані через їх інтерфейси висхідного каналу, утворюючи при цьому розподілену топологію мережі (розширену зону обслуговування), що показано на рисунку 1.6. Топологія організації мереж в даному режимі аналогічна звичайним провідним топологіям [21].

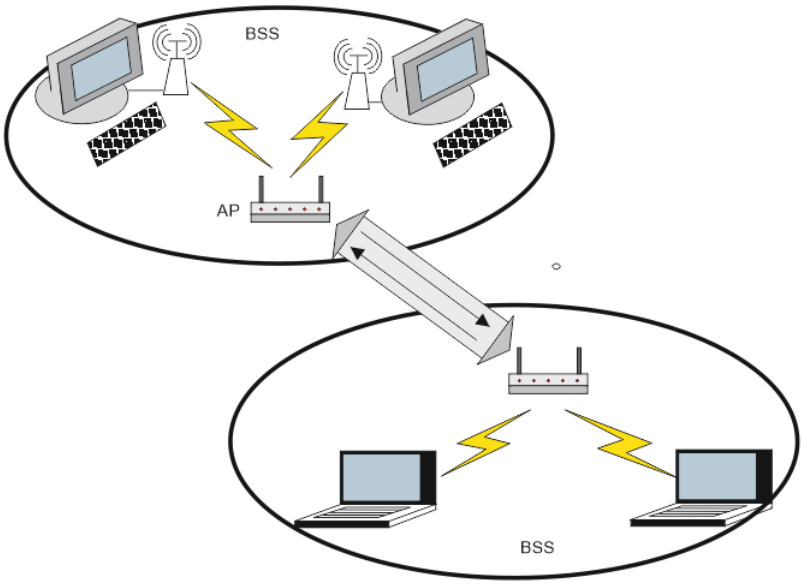


Рисунок 1.5 – Розподілена топологія мережі

1.1.3 Управління доступом до середовища стандарту IEEE 802.11

Стек протоколів стандартів IEEE 802.11 складається з фізичного рівня і канального рівня з підрівнями управління доступом до середовища MAC (Media Access Control) і логічної передачі даних LLC (Logical Link Control) (рис. 1.6). Набір стандартів 802.11 визначає цілий ряд технологій реалізації фізичного рівня (Physical Layer Protocol, PHY), які можуть бути використані підрівнями 802.11 MAC. Кожен з фізичних рівнів стандарту 802.11 має два підрівні [20].

– Physical Layer Convergence Procedure (PLCP). Процедура визначення стану фізичного рівня;

– Physical Medium Dependent (PMD). Підрівень фізичного рівня, який залежить від середовища передачі.

Рисунок 1.6 – Підрівні рівня PHY

На MAC рівні використовується два основних механізми регламентованого колективного доступу PCF (режим централізованої координації) і DCF (режим розподіленої координації). Так само існує гібридна функція координації HCF.

У режимі PCF на центр координації покладається задача управління колективним доступом всіх інших вузлів мережі до середовища передачі даних на основі певного алгоритму опитування або виходячи з пріоритетів вузлів мережі. Центр координації опитує всі вузли мережі, внесені в його список, і на підставі цього опитування організовує передачу даних між усіма вузлами мережі. Важливо відзначити, що такий підхід повністю виключає конкуруючий доступ до середовища і робить неможливе можна виникнення колізій.

Функція DCF заснована на методі колективного доступу з виявленням несучої і механізмом уникнення колізій (Carrier Sense Multiple Access / Collision Avoidance, CSMA / CA). При такій організації кожен вузол, перш ніж почати передачу, «прослуховує» ефір, і тільки за умови відсутності сигналу інших абонентів, може почати передачу своїх даних. Режим DCF є більш вра-

зливим з точки зору несанкціонованого доступу до неї, так як при цьому абоненти спілкуються між собою, минаючи точку доступу.

Wi-Fi – середовище з загальним доменом колізій. Тобто, чим більше пристроїв працюють на одному каналі (± 2 сусідніх), тим вище імовірність колізії – одночасної спроби передачі пакета. Кожна така колізія вимагає затримки перед повторною спробою передачі і зменшує сумарну швидкість всього каналу. При цьому неважливо, до однієї або декількох точках доступу підключені клієнти, домен колізій один на канал. Втрати сумарної пропускної спроможності зазвичай приймаються як 3-5% на кожен наступний пристрій в тому ж або в сусідніх каналах.

Оскільки для передачі інформації використовують радіохвилі, то. Wi-Fi мережа доступна в межах можливого радіусу їх поширення (з іншого поверху або навіть з сусіднього будинку, і т. д.). Будь-який бездротовий пристрій здатний «бачити» всіх користувачів мережі. Єдиним фізичним кордоном бездротової мережі є рівень самого сигналу.

1.2 Загрози інформаційної безпеки бездротових мереж

Під загрозою інформації розуміється сукупність умов і факторів, що створюють потенційну небезпеку, пов'язану з витоком інформації і/або несанкціонованими та/або ненавмисними діями на неї [22].

1.2.1 Класифікація загроз інформаційної безпеки

У документах міжнародних організацій по стандартизації виділено кілька способів класифікації загроз безпеки систем зв'язку, розділених за типами, видами і категоріями. Загроз безпеці, що підлягають аналізу на етапі проектування архітектури безпеки конкретної бездротової мережі, є безліч з багатьма елементами, що створює складність при виборі заходів захисту від загроз. Щоб полегшити рішення цього завдання, доцільно згідно з документом ETSI

ETR 332 згрупувати загрози безпеки по категоріям [23], що показано на рисунку 1.7.

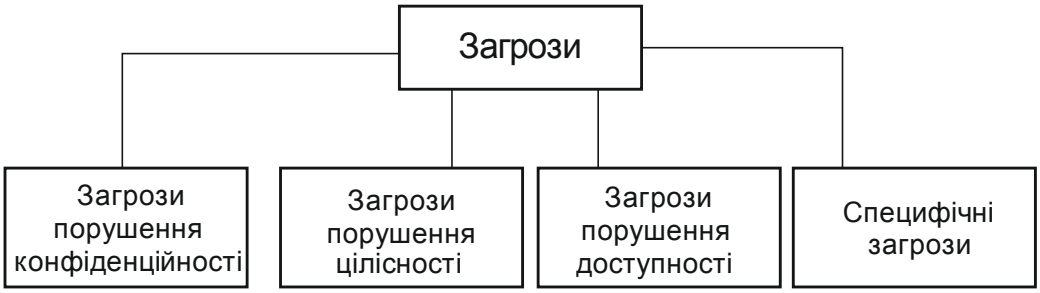


Рисунок 1.7 – Класифікація загроз

Загрози порушення конфіденційності включають в себе [24]:

– порушення конфіденційності інформації шляхом перехоплення бездротового трафіку;

– несанкціонований доступ до інформації та сервісів сегментів провідних мереж, з якими працює користувач, використовуючи вільний бездротовий доступ;

– розкриття параметрів бездротової мережі або сегментів провідної мережі, з якими працює користувач, використовуючи провідний доступ, за межами контрольованої зони;

– розголошення інформації про налаштування системи захисту бездротової мережі.

Загрози порушення цілісності включають в себе:

– спотворення циркулюючої в мережі інформації;

– знищення інформації, що зберігається в сегментах провідних мереж, з якими працює користувач, використовуючи бездротовий доступ;

– розсилка пакетів не за адресою, втрата пакетів, невірна збірка пакетів, їх підміна;

– втручання в роботу точок доступу;

– руйнування власного програмного забезпечення точок доступу.

Загрози порушення доступності включають в себе:

– втручання в процес обміну повідомленнями по мережі;

– блокування прийнятих, або переданих повідомлень на рівні користувачів або точок доступу;

– впровадження несанкціонованого бездротового трафіку;

– виведення з ладу точки доступу разом з усіма підключеними користувачами;

– зменшення швидкості роботи, неадекватна реакція на команди оператора.

Специфічні загрози включають в себе:

– несанкціоноване, анонімне використання трафіку Інтернет;

– протиправні анонімні дії від імені користувача бездротової мережі;

– розкрадання клієнтських пристроїв або точок доступу з метою отримання інформації про налаштування системи захисту бездротової мережі;

– установка несанкціонованих точок доступу і клієнтських мережевих карт;

– перешкоджання зміні параметрів засобів захисту бездротової мережі;

– несанкціоноване підключення до бездротової мережі;

– помилки персоналу;

– відмови програмного забезпечення.

Загрози, як можливі небезпеки вчинення будь-яких дій, спрямованих проти об'єкта захисту, виявляються не самі по собі, а через вразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформації [25]. Тому далі розглянемо вразливості бездротових Wi-Fi мереж.

1.2.2 Спектр вразливостей бездротових мереж

Вразливості властиві бездротовим мережам стандарту IEEE 802.11, невіддільні від них. Джерела загроз можуть використовувати вразливості для порушення безпеки інформації, отримання незаконної вигоди (нанесення

шкоди власнику, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз щодо активізації тих чи інших вразливостей, що завдають шкоди.

Для бездротових мереж стандарту IEEE 802.11 характерні наступні види вразливостей [19]:

1) вразливості, обумовлені середовищем передачі і діапазоном робочих частот;

2) вразливості системи аутентифікації;

3) вразливості криптографічних протоколів;

4) вразливості програмного забезпечення, що використовується;

5) вразливість, обумовлена людським фактором.

Розглянемо докладніше кожен з цих видів.

1. Діапазон робочих частот є не ліцензованим. В діапазоні робочих частот працюють деякі моделі радіотелефонів, побутові пристрої, протокол Blutooth, які створюють завади. Інформація, що циркулює в бездротових мережах схильна до перехоплення. Це пояснюється тим, що переносником інформації є радіохвилі.

2. Відкрита аутентифікація не дозволяє точці радіодоступу визначити, чи є абонент легітимним чи ні. Порушник може підмінити свій MAC-адрес на легітимний.

3. У багатьох організаціях всі користувачі працюють з одним ключем. Цей ключ зберігається в кожному комп'ютері і пристрої. Секретний ключ шифрування WEP може бути обчислений з використанням певних кадрів, пасивно зібраних через бездротову локальну мережу. Відсутні дієві засоби контролю цілісності повідомлень.

4. Драйвери бездротових пристроїв розробляються без належної уваги до безпеки, і нові функції додаються в поспіху заради конкуренції. В даний час існує безліч інструментів, що дозволяють використовувати вразливість драйверів бездротових адаптерів.

5. Виявляється в небажанні або невмінні користувачів бездротових мереж захищатися від несанкціонованого доступу. Прикладом вразливості може слугувати втрата одного мережевого інтерфейсу і несвоєчасне повідомлення адміністратору.

Вищеописані вразливості розкривають величезний спектр атак, спрямований на бездротові мережі Wi-Fi.

1.2.3 Різновиди атак на бездротову мережу

При проведенні атак на бездротову мережу характерна така послідовність дій [26]:

1) вивчення мережі і зони її покриття;

2) планування методики огляду місця розгортання і проведення атаки;

3) збір, підготовка та конфігурація обладнання та програмного забезпечення;

4) огляд місця розгортання мережі, визначення її кордонів і рівня сигналу уздовж периметра;

5) аналіз трафіку в мережі і подолання виявлених заходів протидії;

6) підключення до бездротової мережі та аналіз її структури;

7) пасивний аналіз трафіку і оцінка безпеки протоколів;

8) проведення активних атак;

9) вихід в інтернет або іншу мережу через виявлені шлюзи.

Атаки, відповідні вразливостям, можна розділити як [19]:

1. Атаки з використанням вразливості середовища передачі і діапазону робочих частот:

– атаки, що експлуатують налаштування деяких параметрів канального рівня в мережах IEEE 802.11;

– Dos-атаки, що використовуються як один з етапів проникнення в мережу або для реалізації загроз доступності шляхом глушіння пристроїв бездротової мережі.

2. Атаки на систему аутентифікації:

– атака на фільтрацію MAC-адрес;

– атака на фільтрацію протоколів;

– атака «людина посередині»

3. Атаки на криптографічні протоколи:

– пасивні мережеві атаки

– статистичний метод обчислення ключа;

– активні мережеві атаки;

– індуктивне обчислення ключа.

4. Атаки на програмне забезпечення, що використовується. Драйвери бездротових пристроїв розробляються без належної уваги до безпеки, і нові функції додаються в поспіху заради конкуренції, тому код часто наповнений помилками і небезпечний.

5. Атаки, обумовлені людським фактором. Для цієї загрози схильні мережі, власники яких використовують короткі паролі або паролі, що складаються з поширених фраз.

За підсумками матеріалів розглянутих в даному підрозділі, можна зробити висновок, що існує багато різних типів мережевих атак, класифікувати їх непросто, так як лише небагато є достатньо загальними і найчастіше використовуються. Виділимо сім основних видів атак, специфічних для бездротових Wi-Fi мереж [3]:

– підслуховування;

– DoS атака (Denial of Service - відмова в обслуговуванні);

– глушіння;

– вторгнення та модифікація даних;

– атака «man in the middle»;

– абонент-шахрай;

– помилкова (фальшива) точка доступу.

1.3 Аналіз методів забезпечення безпеки бездротових Wi-Fi мереж

Якщо не використовувати який-небудь механізм захисту, будь-яка станція стандарту 802.11 зможе обробити дані, надіслані по бездротовій локальній мережі, якщо тільки її приймач працює в тому ж радіодіапазоні. Забезпечити захист пристрою бездротового доступу і, відповідно, звести до мінімуму пов'язаний з цим видом доступу ризик можна за допомогою міжмережевих екранів (firewall), шифрування і систем виявлення вторгнень.

1.3.1 Міжмережеві екрани

Міжмережевий екран або мережевий екран (рис.1.6) [27] – комплекс апаратних або програмних засобів, що здійснює контроль і фільтрацію мережевих пакетів, що приходять через нього за заданими правилами.

Основною задачею мережевого екрану є захист комп'ютерних мереж або окремих вузлів від несанкціонованого доступу. Також мережеві екрани часто називають фільтрами, так як вони призначені не пропускати (фільтрувати) пакети, що не підходять під критерії, визначені в конфігурації.

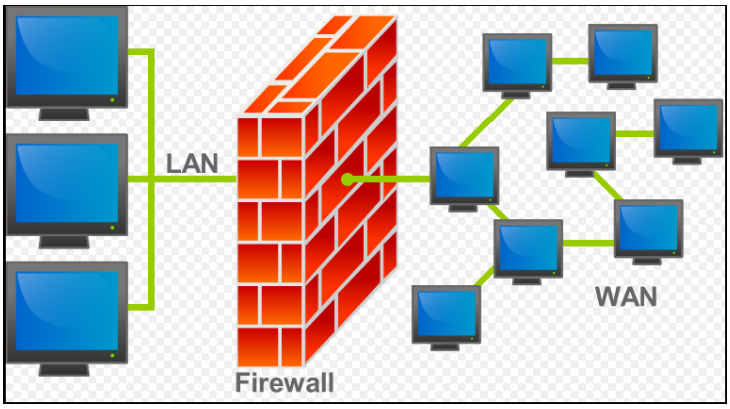


Рисунок 1.6 – Міжмережевий екран

Загальноприйнятої класифікації міжмережевих екранів не існує. Залежно від реалізації за моделлю OSI, міжмережеві екрани можна розділити на керо-

вані комутатори; пакетні фільтри; шлюзи сенсорного рівня; посередники прикладного рівня та інспектори стану.

Незважаючи на всі переваги міжмережевих екранів, вони не можуть забезпечити захист від внутрішніх загроз. Хоча їх можна розробити так, щоб запобігти отриманню конфіденційних даних зовнішніми порушниками, вони все одно не заборонить внутрішнім користувачам копіювати дані. Крім цього, мережеві екрани не зможуть захистити об'єкт від проникнення через «люки», так звані «Back doors». Так якщо на об'єкт, захист якого здійснює мережевим екраном, дозволяється необмежений модемний доступ, зловмисники можуть обійти його.

Останнім часом з'явилося нове покоління міжмережевих екранів NGFW. У цих пристроях додана тісна інтеграція додаткових можливостей, таких як вбудована глибока перевірка пакетів, запобігання вторгнень і перевірка трафіку на рівні додатків. Деякі NGFW також включають перевірку зашифрованого трафіку TLS / SSL, фільтрацію веб-сайтів, управління пропускною спроможністю і QoS, антивірусну перевірку та інтеграцію зі сторонніми системами управління ідентифікацією, такими як LDAP, RADIUS і Active Directory. Такий підхід призводить до неузгодженості політик безпеки і не дозволяє вирішити проблему моніторингу та управління трафіком додатків, при цьому виникає проблема в неточній або неповній класифікації трафіку, складних процедурах управління та додаткових затримках, викликаних безліччю процесів сканування.

1.3.2 Стандарти шифрування

WEP – перший стандарт захисту Wi-Fi. Розшифровується як Wired Equivalent Privacy, використовує два види шифрів [28]:

– потоковий (груповий) шифр;

– блоковий шифр.

Шифри обох типів працюють, генеруючи ключовий потік (key stream), що отримується на основі значення секретного ключа. Ключовий потік змішується з даними, або відкритим текстом, в результаті чого виходить закодований вихідний сигнал, або зашифрований текст. Названі два види шифрів відрізняються за обсягом даних, з якими вони можуть працювати одночасно.

Основна проблема WEP – у фундаментальній помилці проектування. Шифрування потоку робиться за допомогою тимчасового ключа. WEP фактично передає кілька байт цього самого ключа разом з кожним пакетом даних. Таким чином, незалежно від складності ключа розкрити будь-яку передачу можна просто маючи достатню кількість перехоплених пакетів [28, 29].

Стандарт WEP має безліч недоліків і зламується безліччю різних способів, що через відстані, що покривається передавачем, робить дані більш уразливими [28, 29]. Його потрібно уникати майже так само, як і відкритих мереж – безпеку він забезпечує тільки на короткий час. Можливо повністю розкрити данні незалежно від складності пароля. Ситуація ускладняється тим, що паролі в WEP – це або 40, або 104 біта, що є вкрай короткою комбінацією і підібрати її можна за секунди (це без урахування помилок в самому шифруванні).

Щоб усунути недоліки WEP, WPA (Wi-Fi Protected Access) був розроблений як новий стандарт безпеки для бездротових протоколів. Відмінними рисами WPA є [28]:

– вдосконалена схема шифрування;

– обов'язкова аутентифікація;

– система централізованого управління безпекою.

Для забезпечення цілісності повідомлень він використовував протокол цілісності TKIP або Temporal Key Integrity. Це було відмінним від WEP в деякому сенсі, який використовував CRC (Cyclic Redundancy Check). Вважалося, що TKIP набагато сильніше, ніж CRC. Його використання забезпечувало передачу кожного пакету даних за допомогою унікального ключа шифрування.

Комбінація клавіш збільшила складність декодування ключів і тим самим зменшила кількість вторгнень ззовні.

У 2008 році на конференції PacSec був представлений спосіб, що дозволяє зламати ключ TKIP. У 2009 році фахівцями з Університету Хіросіми і Кобе був розроблений метод злому будь-якої мережі, де WPA зламується за одну хвилину. У більшості випадків WPA можна зламати за допомогою звичайного перебору всіх можливих варіантів (брут-форс).

Таким чином, WPA було розширено в WPA 2, який визначається технічною характеристикою IEEE 802.11i. У ньому реалізовано CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol, протокол блочного шифрування з кодом автентичності повідомлення та режимом зчеплення блоків і лічильника) та шифрування AES (Advanced Encryption Standard, симетричний алгоритм блочного шифрування). Підтримка WPA2 є обов'язковою умовою для всіх сертифікованих Wi-Fi пристроїв з 2006 року.

У 2010 році була опублікована інформація про вразливість в протоколі WPA2, виявленої співробітниками компанії Air Tight Networks, що отримала назву Hole196. Використовуючи цю вразливість, авторизований в мережі зловмисник може розшифрувати дані інших користувачів, використовуючи свій закритий ключ. У 2017 році зведена група дослідників з Левенського католицького університету, яку очолювали Меті Ванхоф та Франк Піссенс, розкрила інформацію про комплекс вразливостей в WPA2, що отримав назву KRACK.

На початку 2018 року міжнародний альянс Wi-Fi Alliance анонсував новітній протокол бездротової безпеки – WPA3. Основними доповненнями, реалізованими в цьому протоколі, стануть: вбудований захист від брутфорс-атак; індивідуальне шифрування даних для посилення конфіденційності користувачів у відкритих Wi-Fi мережах; спрощене налаштування IoT-пристроїв; вдосконалений криптографічний стандарт для мереж Wi-Fi – «192-розрядний пакет безпеки» [30].

На початку 2019 року Меті Ванхоф та його колега Еял Ронен оприлюднили деталі про інший комплекс проблем, що отримав ім'я DragonBlood – «в честь» уразливого Dragonfly механізму, за допомогою якого клієнти проходять аутентифікацію на пристроях з підтримкою нового стандарту WPA3. До недавнього часу цей механізм «рукостискання» вважався більш безпечним, але тепер Ванхоф та Ронен довели, що і це не так. Під назвою DragonBlood об'єдналися п'ять вразливостей, включаючи відмову в обслуговуванні, дві проблеми, що призводять до side-channel витокам, і ще дві проблеми, пов'язані з даунгрейдом з'єднань. В результаті DragonBlood дозволяє атакуючому, що знаходиться в зоні доступу Wi-Fi мережі, відновити паролі жертви і проникнути в мережу [31].

Таким чином, можна сказати, що шифрування в тій чи іншій мірі захищає дані, що передаються по мережі. Але методи дешифрування розвиваються не менш успішно, ніж методи шифрування, безпека мереж не зводиться тільки до захисту процесу передачі даних. Алгоритми шифрування не захищають самі мережі від специфічних загроз викликаними вразливостями середовища передачі інформації Wi-Fi мереж, що наведені в п.1.2.3, так як працездатність мережі можна порушити, не знаючи алгоритмів шифрування і ключів.

1.3.3 Системи виявлення вторгнень

Системи виявлення вторгнень (СВВ, IDS - Intrusion Detection System) – це системи, які збирають інформацію з різних точок корпоративної мережі (комп'ютерної системи, що захищається) і аналізують цю інформацію для виявлення не тільки спроб, але і реальних порушень захисту (вторгнень) [32, 33].

СВВ є програмними або програмно-апаратними системами, що дозволяють автоматизувати процес вивчення подій, виникаючих в комп'ютерній мережі або окремо взятій системі, аналізують їх з точки зору безпеки та приймають дії. З урахуванням постійного зростання кількості мережевих атак системи СВВ стають важливим доповненням інфраструктури безпеки мережі.

Дані системи дозволяють автоматизувати процес моніторингу та аналізу подій, які відбуваються в мережі або окремо взятому вузлі (системі) з метою виявлення атаки або проникнення.

1.3.3.1 Класифікація систем виявлення вторгнень

Існує кілька способів класифікації СВВ, кожен з яких заснований на різних характеристиках СВВ. За способом моніторингу СВВ можна класифікувати:

– **Мережеві** (Network-Based IDS, NIDS). Перевіряють мережевий трафік (підключаючись до хабу або світчу, налаштованому на віддзеркалення портів, або мережевий TAP пристрій) та ведуть спостереження за декількома хостами.

– **Вузлові** (Host-Based IDS, HIDS). Система (або агент), розташована на хості. Відстежують вторгнення, використовуючи аналіз системних викликів, логів додатків, модифікацій файлів (виконуваних, файлів паролів, системних баз даних), стану хоста та інших джерел.

За способом аналізу:

– **Виявлення сигнатур** (Signature Detection), також називається виявленням зловживань (Misuse Detection). Відповідність зразка відомій атаці називається сигнатурою. Детектори сигнатур аналізують діяльність системи, аналізуючи подію або безліч подій на відповідність наперед визначеним зразком, який описує відому атаку. Найбільш загальна форма визначення сигнатур, яка використовується в комерційних продуктах, специфікує кожен зразок подій, відповідний атаці, як окрему сигнатуру. Проте існує кілька більш складних підходів для виконання визначення сигнатур (званих state-based технологіями аналізу), які можуть використовувати єдину сигнатуру для визначення групи атак.

– **Виявлення аномалій** (Anomaly Detection). Детектори аномалій визначають ненормальну (незвичайну) поведінку на хості або в мережі. Вони припускають, що атаки відрізняються від "нормальної" (законної) діяльності та

можуть бути визначені системою, яка вміє відслідковувати ці відмінності. Детектори аномалій створюють профілі, що представляють собою нормальну поведінку користувачів, хостів або мережевих з'єднань. Ці профілі створюються, виходячи з даних історії, зібраних в період нормального функціонування. Потім детектори збирають дані про події і використовують різні метрики для визначення того, що аналізована діяльність відхиляється від нормальної.

Метрики і технології, що використовуються при визначенні аномалій, включають [34]:

– визначення допустимого порогу. У цьому випадку основні атрибути поведінки користувача і системи виражаються в кількісних термінах. Для кожного атрибута визначається деякий рівень, який встановлюється як допустимий. Такі атрибути поведінки можуть визначати число файлів, доступних користувачеві в даний період часу, число невдалих спроб входу в систему, кількість часу центрального процесору, що використовується процесом і т.п. Даний рівень може бути статичним або евристичним – наприклад, може визначатися зміною аналізованих значень.

– статистичні метрики: параметричні, при яких передбачається, що розподіл атрибутів профілю відповідає конкретному зразку, і непараметричні, при яких розподіл атрибутів профілю є "навчаючим" виходячи з набору значень історії, що спостерігалося за певний період часу.

– метрики, засновані на правилах, які аналогічні непараметричним статистичними метрикам в тому, що дані за якими спостерігають визначають допустимі зразки для використання, але відрізняються від них в тому, що ці зразки специфіковані як правила, а не як чисельні характеристики.

– інші метрики, включаючи нейромережі, генетичні алгоритми та моделі імунних систем.

Тільки перші дві технології використовуються в сучасних комерційних СВВ. На жаль, детектори аномалій і СВВ, засновані на них, часто створюють

велику кількість помилкових повідомлень, так як зразки нормальної поведінки користувача або системи можуть бути дуже невизначеними. Незважаючи на цей недолік, дослідники припускають, що СВВ, засновані на аномаліях, мають можливість визначати нові форми атак, на відміну від СВВ, заснованих на сигнатурах, які покладаються на відповідність зразку минулих атак.

Залежно від реагування на виявлені атаки СВВ діляться на [35]:

– **Активні** (Active IDS), також відомі як система попередження вторгнень (IPS – Intrusion Prevention system). Ведуть відповідні дії на порушення (збір додаткової інформації, зміна оточення, виконання дії проти атакуючого). Дії у відповідь можуть проводитися автоматично або по команді оператора.

– **Пасивні** (Passive IDS). При виявленні порушення безпеки, інформація про порушення записується в лог додатку, а також сигнали небезпеки відправляються на консоль і / або адміністратору системи.

У суперечках, що краще IPS і IDS, відповідь очевидна і те й інше. Тому в останні роки ринок пропонує механізми захисту, які містять в собі обидва механізму, що отримало назву IDPS (Intrusion Detection Prevention System).

Архітектура СВВ зазвичай включає в себе [35]:

– сенсорну підсистему, призначену для збору інформації про події, пов'язані з безпекою мережі, що захищається;

– підсистему аналізу, призначену для виявлення мережевих атак і підозрілих дій;

– сховище, в якому накопичується інформація про первинні події і результати аналізу;

– консоль управління, що дозволяє конфігурувати СВВ, спостерігати за станом захищається системи і СОВ, переглядати виявлені підсистемою аналізу інциденти.

Доцільно розрізняти локальну і глобальну архітектуру. В рамках локальної архітектури реалізуються елементарні складові, які потім можуть бути об'єднані для обслуговування корпоративних систем [35, 36].

Основні елементи локальної архітектури та зв'язку між ними показані на рисунку 1.7. Первинний збір даних здійснюють агенти, що називаються ще сенсорами. Реєстраційна інформація може вилучатись з системних або прикладних журналів, або добуватися з мережі за допомогою відповідних механізмів активного мережного обладнання або шляхом перехоплення пакетів за допомогою встановленої в режим моніторингу мережевої карти.

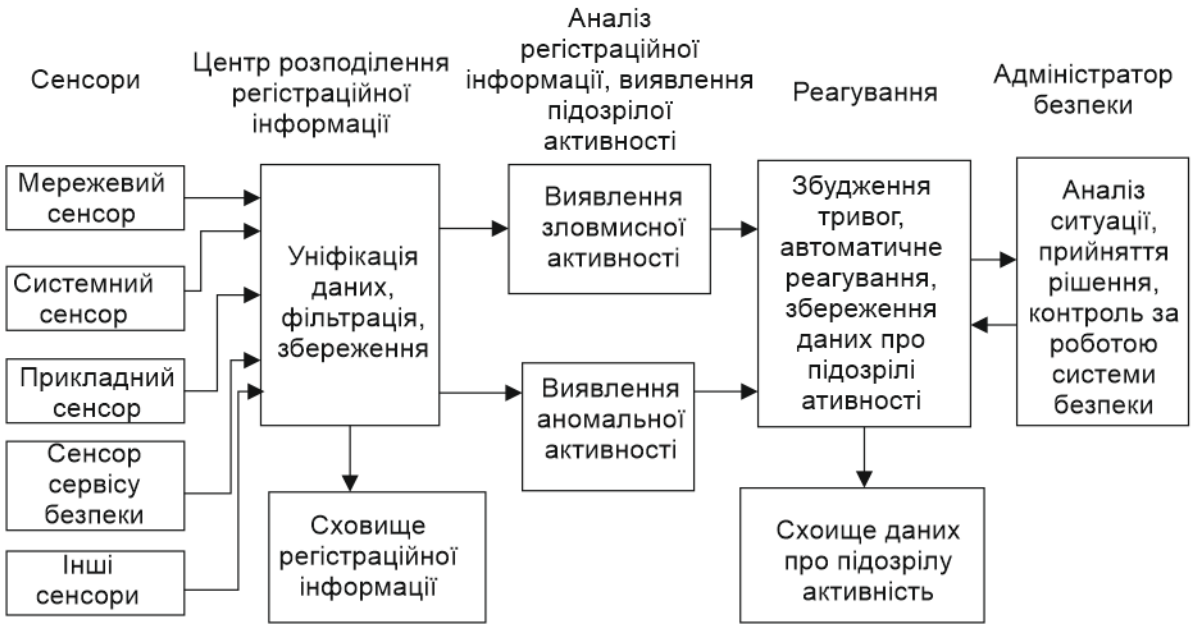


Рисунок 1.7 – Основні елементи локальної архітектури систем виявлення вторгнень

Глобальна архітектура організовує тимчасові і різнорангові зв'язки між локальними системами виявлення вторгнень (рис. 1.8) [35, 36]. На одному рівні ієрархії розташовуються компоненти, що аналізують підозрілу активність з різних точок зору. Наприклад, на хості можуть розташовуватися підсистеми аналізу поведінки користувачів та додатків.

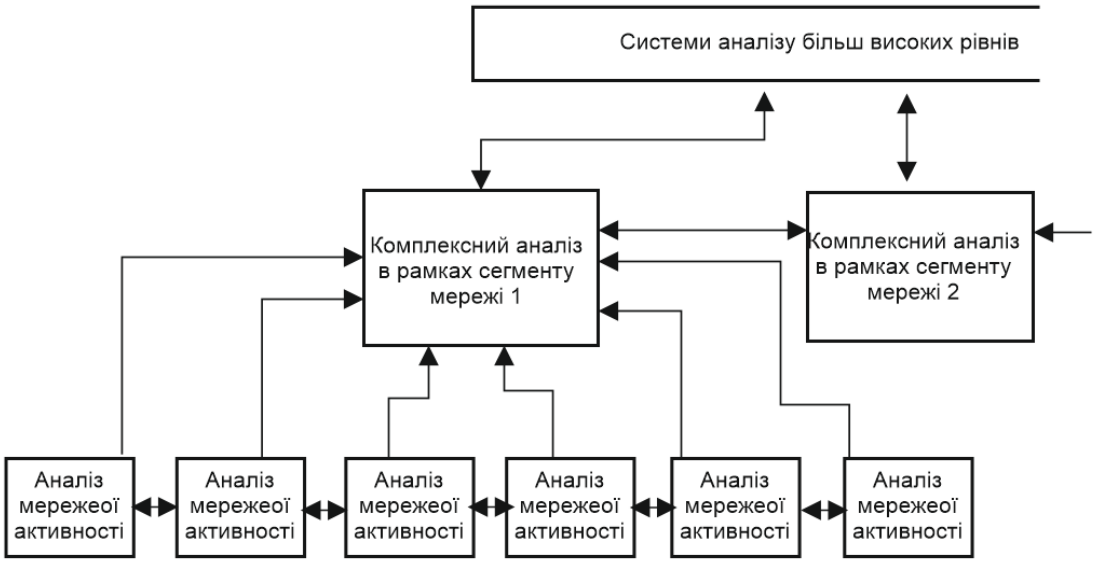


Рисунок 1.8 – Глобальна архітектура систем виявлення вторгнень

1.3.3.2 Бездротові СВВ

Існує безліч загроз безпеки мережі, що не виявляються традиційними системами IDS/IPS, оскільки їх можна виявити на канальному або фізичному рівнях. Через вже вказану відкритість Wi-Fi мережі, обумовлену природою поширення радіохвиль, мережі можуть бути схильні до атак з боку зловмисників. Тому безпеці бездротових мереже слід приділяти особливу увагу. Для вирішення проблем безпеки в бездротових локальних мережах, багато організацій розгортають бездротові системи запобігання вторгнень (WIDPS).

WIDPS – це система, яка здійснює моніторинг навколишнього радіоефіру за допомогою сенсорів (зазвичай ними є ті ж самі точки доступу, що і роздають Wi-Fi), аналізує отриману інформацію про джерела радіосигналу, їх взаємодію і аномальні (незвичайні) активності та запобігає діям, що суперечать налаштованій політиці запобігання вторгнень.

WIDPS націлені на шахрайські бездротові пристрої (виявлення і запобігання використання несанкціонованих бездротових пристроїв), а не на події безпеки. Основна ідея полягає у тому, щоб виділити деякі точки доступу в інфраструктуру, налаштовану в режимі WIDPS. Ці точки доступу попередньо сконфігуровані для певного частотного каналу, і вони просто постійно слуха-

ють частотний спектр в пошуках аномалій. Різні типи аномалій, які можна побачити, це: потік кадрів деаутентифікації або потік кадрів дисоціації, виявлення бездротових локальних мереж, що транслюються точками доступу з невідомим BSSID, і т. д. Глибока перевірка пакетів або виявлення шкідливого коду повинні бути виявлені в кабельній мережі.

Як і в провідних мережах, в бездротових рішеннях для реалізації захисту існують компоненти, які виконують функції безпеки. Контролер бездротових рішень виконує стандартні функції управління бездротовою мережею (точками доступу), а також реалізує додаткові можливості по аутентифікації користувачів. Сканери мережевої безпеки нагадують собою точки доступу, але призначені виключно для мережевого моніторингу та передачі інформації на контролер або пристрій СВВ. Точки доступу служать в якості станцій для підключення пристроїв користувачів, але в деяких випадках можуть одночасно виступати сканерами мережевої безпеки. Пристрій СВВ аналізує дані сканерів мережевої безпеки і точок доступу та надає команди контролеру для запобігання вторгнень в разі їх виявлення. У складі СВВ може бути представлено окремий пристрій або в складі бездротового контролера.

Існує кілька способів впровадження СВВ в бездротові мережі: оверлейная (накладена) модель; інтегрована (вбудована) модель і гібридна модель [37].

Оверлейная модель (рис. 1.9) – використовує спеціальні сенсори і систему управління для створення СВВ над існуючою бездротовою мережею. Сенсорами є пасивні точки доступу, які контролюють навколишнє середовище на наявність ознак атаки.

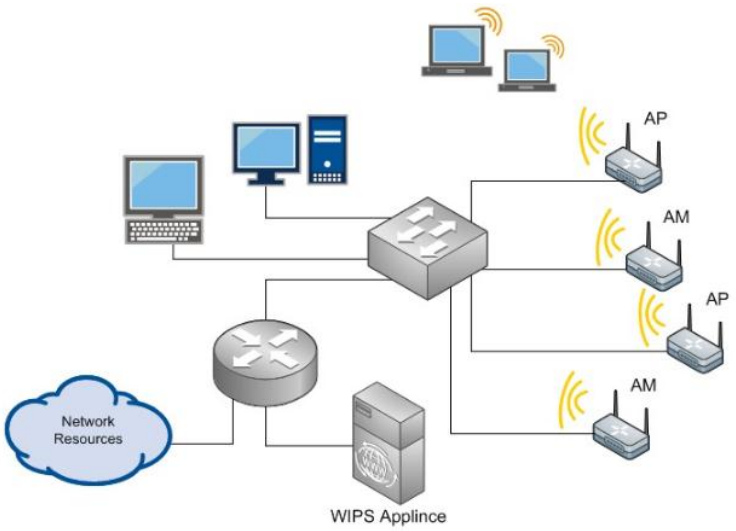


Рисунок 1.9 – Структура оверлейної моделі

Інтегрована модель використовує одну консоль управління для бездротової мережі і СВВ. Сенсорами виступає обладнання (точки доступу), що обслуговує користувачів мережі, без залучення додаткового обладнання.

Гібридна модель моніторингу використовує в собі сильні сторони двох попередніх моделей. Можна використовувати звичайні точки доступу і посилити захист, доповнивши пасивними точками доступу.

На жаль, часто можна спостерігати, як бездротові атаки залишаються непоміченими досить тривалий час, будучи замаскованими під нестійке підключення або перевантаження середовища передачі.

До недоліків СОВ можна віднести [35]:

– неприпустимо високий рівень помилкових спрацьовувань і пропусків атак;

– слабкі можливості по виявленню нових атак;

– більшість вторгнень неможливо визначити на початкових етапах;

– важко, іноді неможливо, визначити атакуючого;

– відсутність оцінок точності і адекватності результатів роботи;

– неможливо визначати «старі» атаки, що використовують нові стратегії;

– складність виявлення вторгнень в реальному часі;

– слабкі можливості з автоматичного виявлення складних координованих атак;

– значне перевантаження систем, в яких функціонують СВВ, при роботі в реальному часі.

1.4 Огляд існуючих бездротових систем виявлення і запобігання вторгнень

Незважаючи на те, що перелік загроз, з якими намагаються боротися різні WIDPS приблизно однаковий, алгоритми виявлення «порушників» і механізми запобігання їх діяльності абсолютно різні. Ухвалення рішення про безпеку будь-якої мережевої активності в комерційних продуктах реалізується за допомогою закритих алгоритмів, принцип роботи яких становить комерційну таємницю. При цьому заявлена кількість і види загроз, що виявляються у різних продуктів відрізняються, хоча в дійсності вони належать одному типу атак, що пояснюється відсутністю стандартів в області бездротових атак.

За визначенням Gartner, WIDPS-системи повинні реагувати на такі сценарії нападу, як «Злий двійник» (підміна точки доступу), «Посередник» (таємне втручання в канал зв'язку з метою перехоплення) та DDoS; блокувати проникнення через вразливості, наприклад, викликані неправильним конфігуруванням точок доступу або слабким захистом для користувача пристроїв; здійснювати моніторинг працездатності WLAN; нарешті, при необхідності – взагалі забороняти бездротовий доступ на тій чи іншій території. WIDPS моніторить спектр (бажано весь, тому що чужі точки доступу можуть «ховатися» між стандартними каналами), візуалізує на карті розташування легальних і сторонніх користувачів та вживає заходів проти зловмисників (блокування з'єднань, примусове відключення). Серед відомих виробників, в сегменті WIDPS [38], за останні 5 років (2015 – 2020 рр.) Можна виділити: Cisco, IBM, Check Point, HP, Netscout, AirWave (Aruba), Extreme Networks, Fortinet, ForeScout, WatchGuard, Venustech, Topsec і Qihoo 360.

Сучасні контролери бездротових мереж на базі бездротових комутаторів можуть самостійно виконувати ті чи інші функції захисту. Однак надійність виявлення вторгнень, кількість видаваних тривожних повідомлень і характер зроблених ними дій виглядають досить блідо на тлі спеціалізованих продуктів WIDPS. Вони працюють в режимі 24/7 і, як правило, не вимагають управління або участі адміністратора.

Виробники WIDPS не надають докладний опис того, які методи використовуються при блокуванні тієї чи іншої атаки. І навіть якщо б були, то буде потрібно багато часу і зусиль, щоб роздивитися всі варіанти і оцінити сильні і слабкі сторони кожного з них. Більш реально оцінити статистику з офіційних джерел і відгуки користувачів, які використовують ці системи.

За прогнозом Gartner [39], до кінця 2021 роки 70% нових автономних систем виявлення і запобігання вторгнень будуть розміщуватися не традиційно, за фаєрволом, а в хмарі (публічному або приватному).

Точка доступу UniFi AP XG [40] в реальному часі показує інформацію про стан радіочастотного спектру. Забезпечує неперервне управління загрозами, працюючи в якості бездротової системи запобігання вторгнень (Wireless Intrusion Prevention System, WIPS) і бездротової системи виявлення вторгнень (Wireless Intrusion Detection System, WIDS). Заявлені характеристики говорять про дієвість програмного інструменту, але виявляє він тільки такі загрози як шкідливі фрейми і "підроблені" точки доступу [40].

У своїй публікації [41] автор робить огляд продукту Cognitive Wi-Fi від Mojo Networks. Дана система являє собою хмарну систему, яка добре себе показала при тестуванні. Її не можна назвати легкою і зрозумілою. Панель моніторингу містить величезну кількість взаємозалежної інформації, але все ж це складна ієрархічна система, в якій непросто розібратися. Доступ до аккаунту через стандартну авторизацію «ім'я користувача/пароль» вразливий до цілеспрямованих атак хакерів. Автора дослідження також відзначають недостатню, на їхню думку, підтримку рішенням можливостей множинної адресації. Ще

одним недоліком є те, що деякі зміни конфігурації точок доступу можуть зайняти до декількох десятків хвилин від клацання по миші, щоб підтвердити нові налаштування, до фактичної їх доступності. Як відзначають автори дослідження, одночасне застосування множинних змін конфігурації точок доступу може призвести до того, що вся бездротова Wi-Fi інфраструктура буде недоступна протягом двадцяти хвилин. Слід відзначити, що не дуже добре працює протидія DoS, відбуваються збої в системі. При протидії стандартним атакам виду connection flood, forced disconnectioni т.п. погіршення пропускної можності мережі все одно помітне. Але знайти джерело все-таки стає простіше.

Висновки по розділу 1

На підставі огляду, виконаного в першому розділі, можна зробити такі висновки:

1. На сьогоднішній день бездротові мережі передачі даних Wi-Fi продовжують стрімко розвиватися, і в майбутньому сфери їх застосування будуть тільки розширюватися. Найчастіше безпека в даних мережах не відповідає необхідному рівню, так як об'єкти бездротової інфраструктури мають вразливості та схильні до різних мережевих атак, що пов'язано зі специфікою поширення радіохвиль і особливостями обладнання, що використовується.

2. В якості основних механізмів захисту бездротових мереж від вторгнень є шифрування та системи виявлення вторгнень. Однак вони не можуть забезпечити потрібну ступінь безпеки. Шифрування не вирішує завдання безпеки, оскільки, по-перше, методи де-шифрування розвиваються не менш успішно, ніж методи шифрування, а по-друге, безпека мереж не зводиться тільки до захисту процесу передачі даних, а працездатність мережі можна порушити не знаючи алгоритмів шифрування і ключів. Системи виявлення вторгнень дозволяють в доповнення до інших засобів виявляти вторгнення. Однак дані си-

стеми мають ряд недоліків, до яких відносяться, в першу чергу, великі ймовірності помилкових тривог і пропуску вторгнень при непередбачуваній активності користувачів. Так само варто відмітити що основна задача бездротових систем виявлення схожа з провідними системами і спрямована на моніторинг трафіку і фактично не враховує область поширення інформації в бездротових мережах.

3. Задача забезпечення безпеки є складною, багаторівневою, багатофакторною, тому для її вирішення потрібно застосування допоміжних методів аналізу, а так само розширення спектра ознак, що розглядаються при визначенні несанкціонованого доступу, специфічних безпосередньо для бездротових Wi-Fi мереж. Для вирішення поставленої задачі пропонується:

– розробити метод ідентифікації користувачів Wi-Fi мереж на основі детального аналізу спектральних характеристик випромінювання підключених пристроїв.

– розглянути позиціонування в бездротовій Wi-Fi мережі, як один з критеріїв оцінки несанкціонованого доступу, провести експериментальні дослідження і показати ефективність даного застосування.

РОЗДІЛ 2
ІДЕНТИФІКАЦІЯ КОРИСТУВАЧІВ WI-FI МЕРЕЖ ПО СПЕКТРАМ ЇХ ПРИСТРОЇВ

Методи ідентифікації користувачів в Wi-Fi мережах добре відомі і описані в [42, 43]. Також добре, на жаль, відомі і методи «злому», підробки, імітації і т. д. даних, на підставі яких відбувається ідентифікація [44, 45]. Способи захисту постійно удосконалюються, але разом з ними вдосконалюються і способи її подолання. В даному розділі розглянуто запропоновані автором методи ідентифікації, основані на аналізі спектральних характеристик сигналів, що випромінюються абонентськими пристроями. Цей параметр, по-перше, складно імітувати, а по-друге, більшості сучасних фахівців з інформаційних технологій він маловідомий. Застосування цих методів спільно з іншими сприятиме підвищенню безпеки Wi-Fi мережі.

Матеріали розділу викладені в [12, 14, 15].

2.1 Існуючі методи ідентифікації в бездротових Wi-Fi мережах

Перш ніж перейти до розгляду запропонованого методу, коротко зупинимося на існуючих методах ідентифікації обладнання в Wi-Fi мережах і вкажемо їх вразливості.

Стандартними ідентифікаторами бездротової Wi-Fi мережі є MAC (Media Access Control), IP (InternetProtocol) і SSID (ServiceSetIdentifier).

MAC адреса (фізична адреса) використовується для унікальної ідентифікації пристроїв у локальній мережі. Він має розмірність 6 або 8 байт (згідно MAC-48, EUI-48, або EUI-64). Така розмірність дозволяє сформувати кількасот трильйонів унікальних номерів. MAC адреса записується на заводі-виробнику в постійну (енергонезалежну) пам'ять всіх Wi-Fi пристроїв, мережевих карт, маршрутизаторів, абонентських терміналів, IoT пристроїв. Його

можна було б вважати свого роду паспортом обладнання, якби не простота його підміни. Існує можливість зміни MAC-адреси програмним шляхом, так як його значення, вказане через драйвер, має більш високий пріоритет, ніж «зашите» в плату [46].

Крім того, деякі виробники пристроїв виставляють останні три байта MAC адреси в випадкове число, швидше за все, після кожного перезавантаження пристрою.

Також слід вказати, що в складі кожного пакету в ефір передається MAC адреса, причому, в незашифрованому вигляді. Це дозволяє зловмисникам здійснити перехоплення і подальшу заміну MAC-адреси.

Тому ідентифікація за допомогою MAC адреси не може вважатися надійною.

IP-адреса – це унікальний 4-х або 6 байтний ідентифікатор пристрою, підключеного до мережі. Адреса має ієрархічну структуру і в більшій своїй частині не є випадковою. Мережеве обладнання автоматично або користувач вручну визначає, як правило, тільки останній байт цієї адреси. На відміну від MAC адреси, IP-адреса змінюється при підключенні до різних мереж. Його основне призначення – визначення маршруту передачі пакетів. Через те, що дана адреса може здаватися вручну, він також не може служити надійною ідентифікуючою ознакою.

SSID – це символьна назва бездротової точки доступу Wi-Fi, що слугує для ідентифікації її серед інших. Він являє собою рядок, розміром до 32 байт, який регулярно передається широкомовно в ефір точкою доступу. Його перехоплення і модифікація теж не складає труднощів для технічно грамотного зловмисника.

Перераховані способи ідентифікації схематично показані на рис. 2.1.

Рисунок 2.1 – Схематичне представлення способів ідентифікації пристроїв в Wi-Fi мережах

Паролі, клавіатурний почерк та інші біометричні ознаки, які ідентифікують певного користувача, в рамках даної роботи не розглядалися.

Таким чином, існуючі способи ідентифікації обладнання є недостатньо надійними і можуть бути обійдені зловмисниками.

2.2 Розпізнавання джерел випромінювання за особливостями їх сигналів

Крім методів ідентифікації, передбачених стандартними протоколами бездротового зв'язку, можна вказати і інші.

Методи розпізнавання джерел радіовипромінювання по часовими та частотними особливостями їх сигналів давно застосовуються в системах радіомоніторингу, радіо- і радіотехнічної розвідки. Для кожного радіотехнічного засобу (і свого, і потенційного противника), відомі робочі частоти, типові параметри випромінювання. За цими параметрами оператор, або автоматизована система визначає, які радіоелектронні засоби працюють в зоні спостереження [47, 48].

Розглянемо ряд прикладів використання таких методів.

Фахівцям з технічного захисту інформації добре відомі демаскуючі ознаки так званих «закладних пристроїв» – мініатюрних радіопередавачів, що використовуються для підслуховування. У цих передавачів дуже нестабільна несуча (середня) частота спектра – вона змінюється в залежності від температури навколишнього середовища і напруги живлення [49]. Це пояснюється відсутністю кварцової стабілізації частоти в подібних пристроях

Іншою відмітною ознакою «закладного пристрою» є наявність вищих гармонік в спектрі сигналу (як правило, другої та третьої). Це викликано тим, що в таких пристроях, зібраних в кустарних умовах, не використовуються фільтри гармонік. Цей приклад показує, що спектральні та часові характеристики сигналів дозволяють визначити лише тип джерела радіовипромінювання, але не конкретний його екземпляр. Але на цьому можливості спектрального аналізу не вичерпуються.

При вивченні метеорного поширення радіохвиль було необхідно не тільки зафіксувати факт прийому віддаленого телецентру по метеорному радіоканалу, але й ідентифікувати його. Автором [50] була розроблена експериментальна установка, яка дозволяла вимірювати значення частоти прийнятих станцій з точністю до восьмого десяткового знаку. Всі розглянуті в роботі [50] телецентри працюють на одному частотному каналі, але частота на восьмому десятковому знаку була унікальною для кожної зі станцій, що давало можливість їх ідентифікувати.

Це дослідження, яке схематично показано на рис. 2.2, проводилось в Харківському національному університеті радіоелектроніки на кафедрі Комп'ютерної радіоінженер і систем технічного захисту інформації. При проведенні вимірювань гетеродин приймача був синхронізований з виходом термостатичного опорного джерела частоти (опорне джерело синтезатора частоти Ч6-31, нестабільність 10^{-8} (1 Гц на 100 МГц).

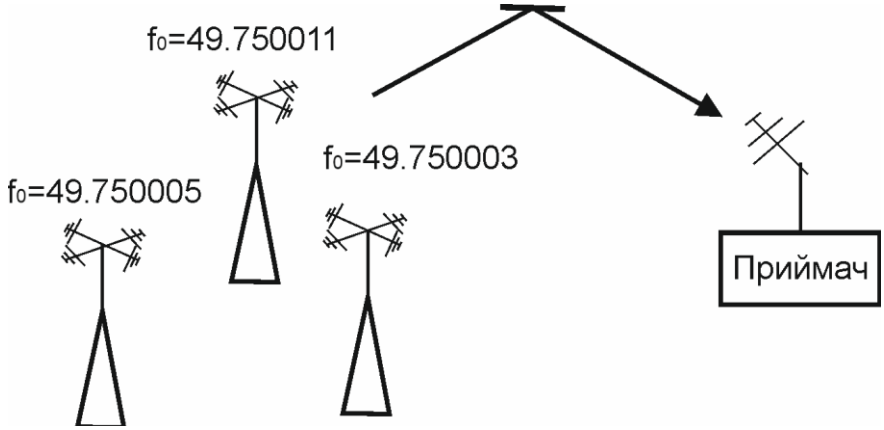


Рисунок 2.2 – До питання про ідентифікацію телецентр по точному значенню частоти

Ще одним прикладом використання особливостей спектра для задач класифікації (фактично, ідентифікації) є розробка корпорації Cisco [51]. Вона інтегрувала запатентоване апаратне і програмне забезпечення Clean Air для обробки спектра, спеціально розроблене для проведення аналізу завад, і випустила набір мікросхем для створення бездротових мереж корпоративного класу. Технологія Cisco Clean Air класифікує і визначає місце розташування окремих джерел завад та інформує про те, як вони впливають на продуктивність і безпеку мережі.

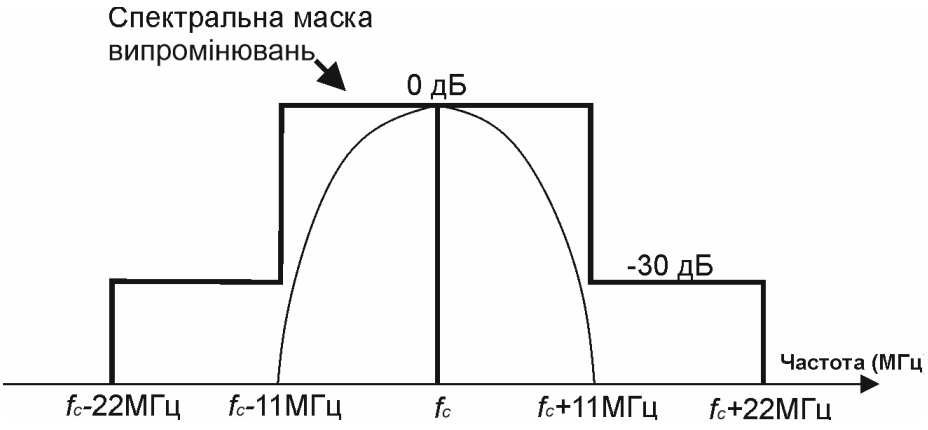
Засоби аналізу спектра дозволяють виявляти всі пристрої, щоспільно використовують смугу частот: як пристрої Wi-Fi, так і джерела завад, відмінні від Wi-Fi пристроїв. Для кожного пристрою, що працює в не ліцензованій смузі частот, засоби аналізу спектру можуть визначити тип пристрою, а також як цей пристрій впливає на мережу Wi-Fi. Управління радіосередовищем основане на інтенсивному використанні даних, що надаються засобами аналізу спектру.

Таким чином, показано, що особливості сигналів можуть бути використані для ідентифікації джерел випромінювання. Застосувавши подібну технологію для аналізу спектрів безпосередньо абонентів бездротових Wi-Fi мереж, а не перешкод, можна було б ідентифікувати всіх абонентів по радіочастотному спектру їх пристроїв.

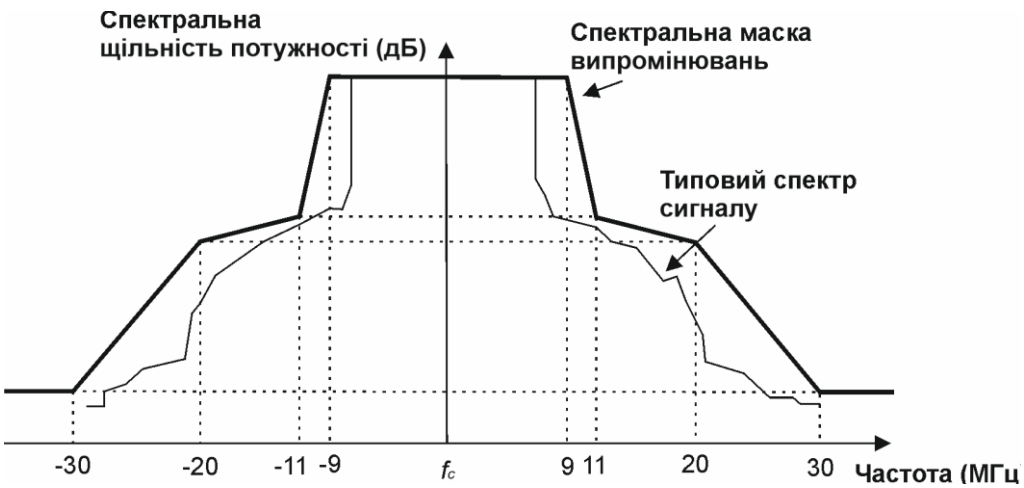
2.3 Особливості спектрального складу Wi-Fi сигналу для ідентифікації абонентів бездротової мережі

Розглянемо, що являє собою Wi-Fi сигнал зі спектральної точки зору.

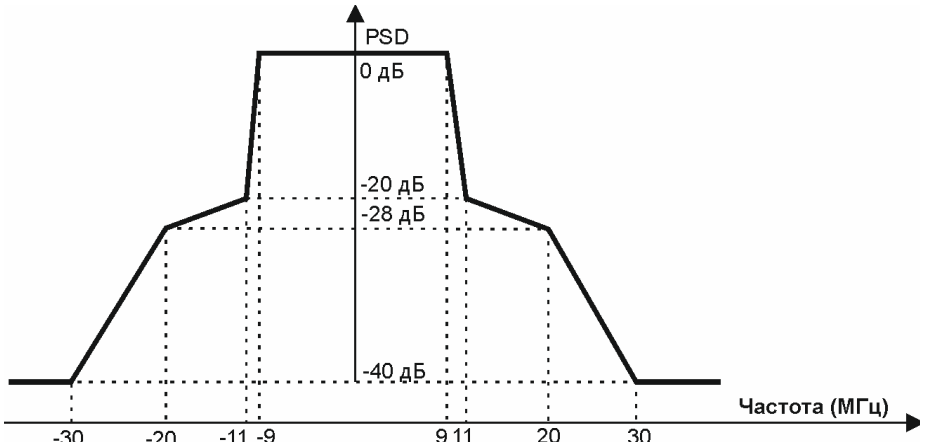
Стандарт IEEE 802.11 визначає параметри спектра Wi-Fi каналу так, як показано на рис. 2.3 [52].



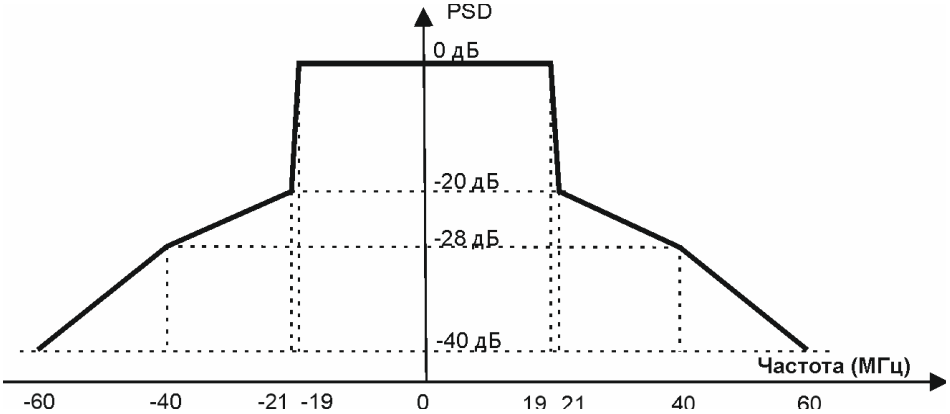
а)



б)



в)



г)

Рисунок 2.3 – Маска спектру сигналу для стандарту:
а) 802.11b; б) 802.11g; 802.11a; в) 802.11n (ширина каналу 20 МГц);
г) 802.11n (ширина каналу 40 МГц)

За результатами [53] ідеальний OFDM спектр виходить таким, як показано на рис. 2.4. З цього рисунка видно, що спектр є:

– симетричним відносно середньої частоти;

– практично рівномірним в межах певної смуги частот поблизу центральної частоти;

– різко спадаючий за межами певної смуги частот.

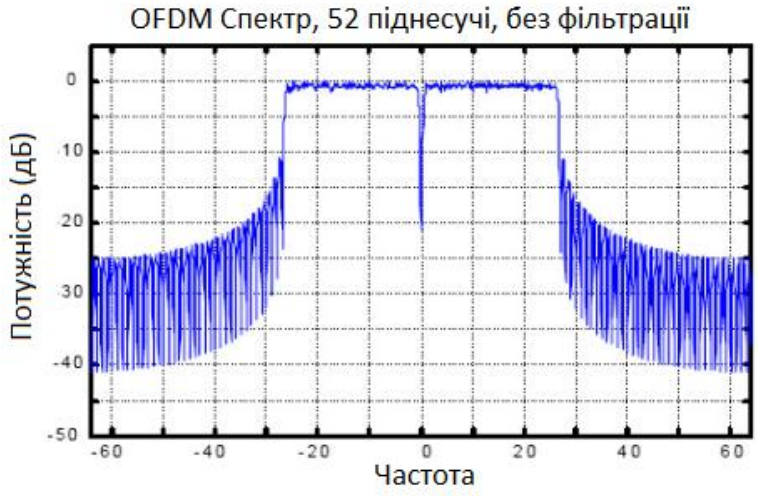


Рисунок 2.4 – Спектр OFDM сигналу

Але обладнання пристрою що входить до складу Wi-Fi (генератор частот, модулятор, радіопередавач, фільтр, антено-фідерна система) можуть мати свої особливості. Такими особливостями можуть бути

– близьке розташування різних електричних ланцюгів, обумовлене малими розмірами пристроїв, що може викликати паразитні зв’язки;

– взаємний вплив різних вузлів схеми по ланцюгах живлення;

– неідентичність елементів схем, різні затримки в них;

– залежності параметрів схем від напруги живлення і температури;

– особливості схем вихідних каскадів передавачів і вихідних фільтрів;

– особливості програмного коду, що реалізує модуляцію;

– відмінності в конструкціях антен і корпусів обладнання.

Всі перераховані вище фактори можуть впливати на спектр випромінюваного сигналу. Причому, внесок кожного з них може бути незначним, але всі разом вони можуть надавати досить істотний вплив, який робить кожен спектр унікальним.

Це може призводити до наступних відхилень:

– несиметричності спектра;

– нестабільності середньої частоти сигналу;

– виникнення аномалій в спектрі у вигляді «горбів» або «провалів»;

– виникнення вищих гармонік і інших позасмугових випромінювань.

2.4 Експериментальні дослідження з вимірювання спектра пристроїв

2.4.1 Апаратура і методика вимірювань

Для перевірки гіпотези про унікальність спектрів пристроїв, підключених до бездротової мережі Wi-Fi, в рамках дисертаційної роботи були проведені експериментальні дослідження.

Вони проводилися на кафедрі Комп'ютерної радіоінженерії та систем технічного захисту інформації Харківського національного університету радіое-

лектроніки. Для вимірювань були взяті декілька різних мобільних пристроїв, які підключалися до однієї і тієї ж точки доступу. На кожному з пристроїв запускався один і той же додаток (web-браузер) і одна й та сама задача – програвання одного і того ж відеофайлу з Інтернету.

Реєстрація проводилася на аналізаторі спектра Signal Hound USB-SA44B, підключеному до комп'ютера, на якому встановлено програмне забезпечення Spike (VSG version 1.0.4; Spikeversion 3.2.3). Розміщення обладнання схематично показано на рис. 2.5.

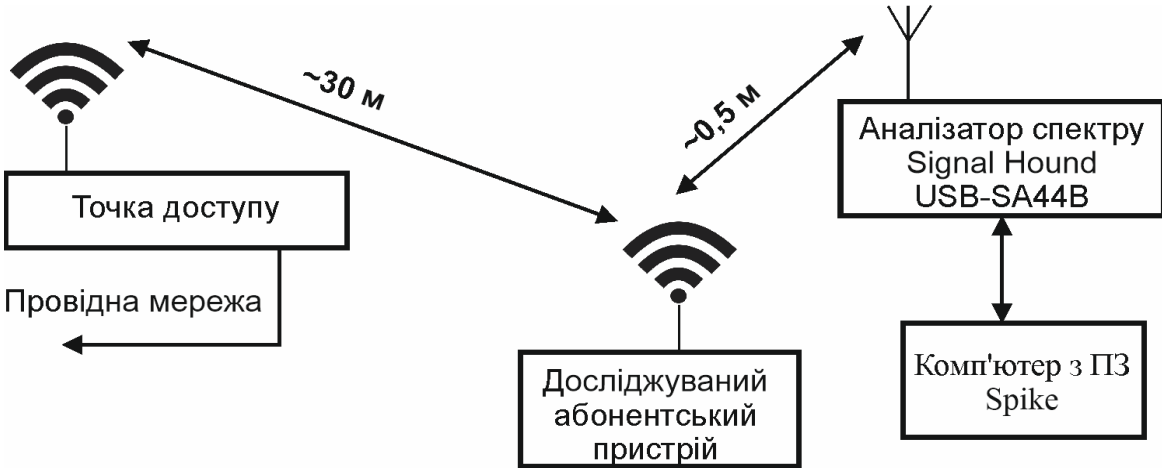


Рисунок 2.5 – Схема проведения эксперименту

Діапазон робочих частот аналізатора спектра від 1 Гц до 4.4 ГГц з максимальною пропускною здатністю в 5 МГц. Відносна похибка складає $\pm 1 \cdot 10^{-6}$. Діапазон ослаблення вхідного атенюатора від 0 до 15 дБ з кроком 5 дБ. Усереднений рівень власних шумів, нормалізований до смуги пропускання 1 Гц (ослаблення вхідного атенюатора 0 дБ), без підсилювача на частотах від 2,6 до 3,3 ГГц не більше -135 дБм з підсилювачем не більше -151 дБм. Межі похибки вимірювання потужності при опорному рівні <0 дБм ± 1,5 дБ, при опорному рівні понад 0 дБм ± 2,0 дБ. Похибка в режимі вимірювального приймача ± 0,25 дБ. Приймає до 2 МБ квадратурних даних кожну секунду, які потім можуть бути відображені в графічному вигляді. Подавлення дзеркального каналу

виконується змішуванням верхньої і нижньої бічної смуг та подальшою математичною обробкою.

Програмне забезпечення Spike підтримує операційні системи Windows 7, 8, 10. Потрібен двоядерний процесор Intel з мінімальною оперативною пам'яттю 4 ГБ (рекомендується 8 ГБ).

Для кожного з мобільних пристроїв відбувалися вимірювання у чотирьох положеннях відносно приймальної антени (рис. 2.6). Кожне вимірювання (накопичення) спектральних відліків продовжувалося близько 3 хвилин. Таким чином для п'яти мобільних пристроїв було виконано 80 вимірювань загальною тривалістю близько 4 годин. В даному дослідженні не ставилося за мету дослідити якомога більше спектрів мобільних пристроїв. Задача роботи показати, що вони розрізняються.

1 2 3 4

Рисунок 2.6 – Положення пристроїв відносно приймальної антени

Всі вимірювання проводилися при кімнатній температурі і при температурі +5 ^{0}C. Серії вимірювань для різних пристроїв були позначені:

А – Смартфон Redminote 4X;

Б – Смартфон Redminote 4X (той же «А», але при температурі +5 ^{0}C.);

В – Смартфон Redminote 4X, аналогічний «А», але другий екземпляр;

Г – Смартфон MeizuM5 Note;

Д – Смартфон Honor 09 Lite;

E – Смартфон MeizuM6 Note;

За допомогою програми Spike були записані всі проведені експериментальні результати з розширенням «.bbr», яке дозволяє повторно відтворювати робочу сесію для подальшого детального аналізу зі збереженням всієї функціональності програмного забезпечення, що і під час самого експерименту. Також всі отримані дані були записані в двійковому форматі і в текстовому файлі з розширенням «.csv», який можна використовувати в сторонніх програмах таких як Labview, Matlab, Excel. Як приклад в Додатку Б наведено один з отриманих спектрів в форматі * .csv.

Вимірювання проводилися в режимі свіпуючого аналізатора спектра (Swept Analysis). Цей режим дозволяє встановити бажану смугу огляду і провести в ній вимірювання. Смуга огляду Wi-Fi сигналу дорівнює ширині каналу і в нашому випадку становить 22 МГц. Це значно більше миттєвої смуги аналізатора спектра, тому програмне забезпечення проводить кілька сканувань в смузі огляду, а потім «склеювання» результатів проводиться за допомогою швидкого перетворювання Фур'є для кожного зі сканувань.

2.4.2 Результати вимірювань для різних пристроїв

В результаті кожного вимірювання програма формувала файл даних $P_L(f)$, f = 2,411...2,433 (третій канал Wi-Fi сигналу) з кроком 2 кГц. Значення потужності на кожній частоті виражалося в одиницях дБм. На рис. 2.7 наведені результати вимірювань для двох пристроїв при кімнатній температурі в різних положеннях.

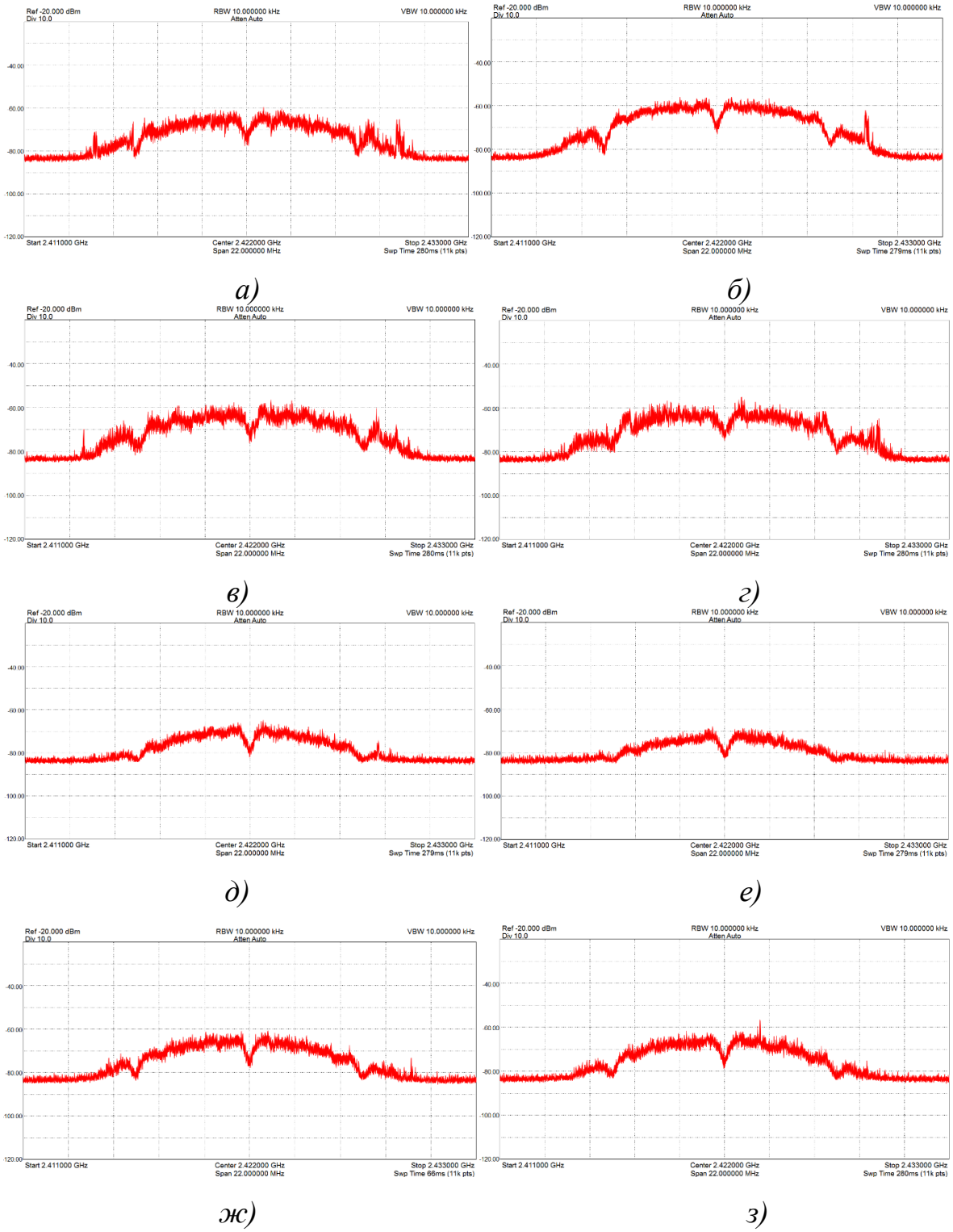
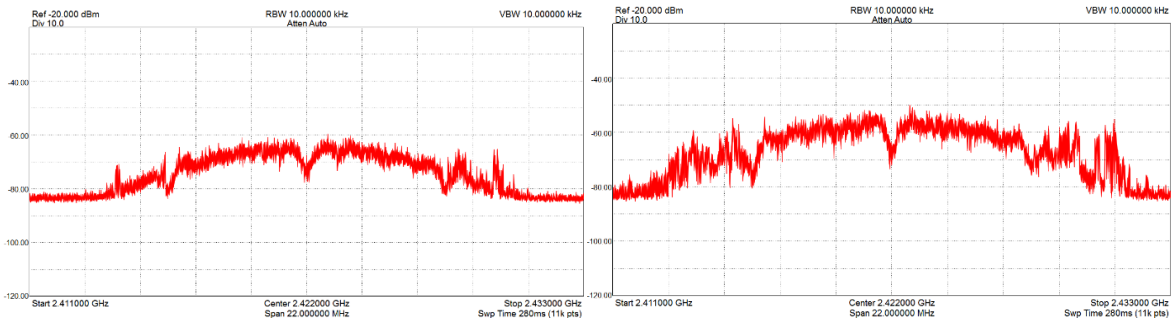


Рисунок 2.7 – Результати вимірювань для двох пристроїв в різних положеннях: *а)* пристрій А в положенні 1, *б)* пристрій А в положенні 2, *в)* пристрій А в положенні 3, *г)* пристрій А в положенні 4, *д)* пристрій Д в положенні 1, *е)* пристрій Д в положенні 2, *ж)* пристрій Д в положенні 3, *з)* пристрій Д в положенні 4.

2.4.3 Вимірювання при різних температурах

В роботі було досліджено вплив температури на спектр випромінювання мобільних пристроїв. Передбачалося, що при зміні температури навколишнього середовища будуть змінюватися частоти кварцових генераторів, і спектр буде зміщуватися.

На рисунку 2.8 наведені спектри одного і того ж смартфону при кімнатній температурі і при температурі +5 ^{0}C.



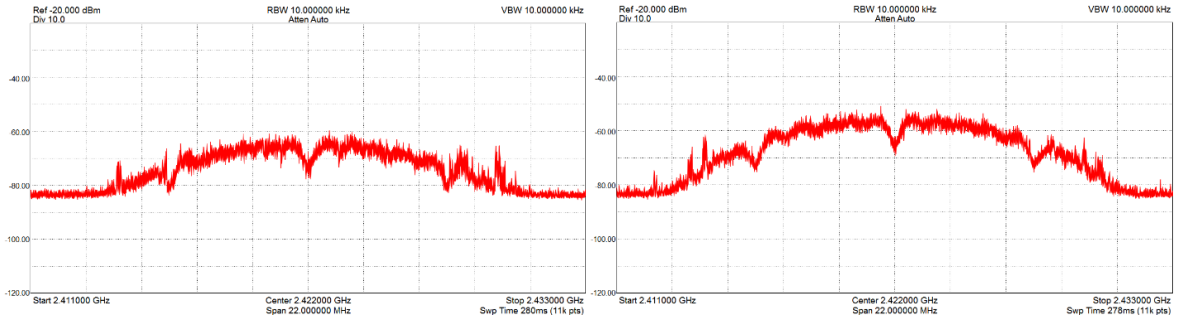
а) *б)*

Рисунок 2.8 – Результати вимірювань для пристрою А в положенні 1 *а)* при кімнатній температурі, *б)* при температурі +5 ^{0}C.

Як видно з рисунків, зниження температури призводить до зміни виду спектральної характеристики, але не до його зміщення. Мабуть, від температури змінюються характеристики елементів схеми передавача. Чисельний аналіз температурних змін наведено в п. 2.7.

2.4.4 Вимірювання для різних екземплярів однієї моделі

Безумовний інтерес представляє питання про те, чи розрізняються між собою спектри випромінювання різних екземплярів одного і того ж мобільного пристрою. В ході роботи було проведено таке дослідження. Результати вимірювань пнаведені на рисунку 2.9 демонструють спектри мобільних пристроїв для різних телефонів, але однією і тієї ж моделі.



а) *б)*

Рисунок 2.9 – Результати вимірювань в положенні 1

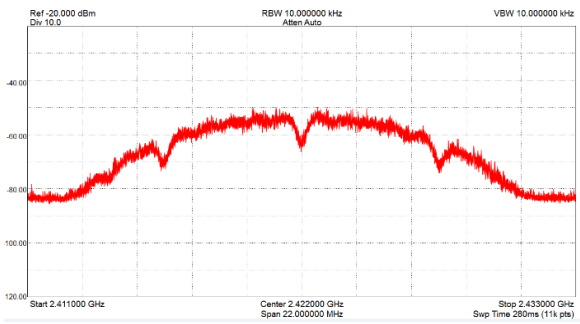
а) пристрою А, *б*) пристрою Б

Як видно з рисунка, навіть між різними екземплярами однієї моделі є відмінності. Їх чисельна оцінка наведена в п. 2.7.

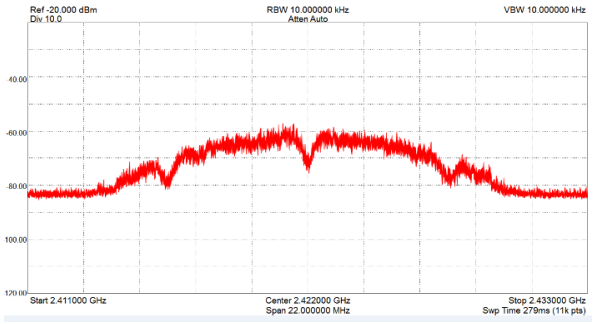
2.4.5 Вимірювання при повороті пристрою

Так само були проведені вимірювання спектра для пристрою А при повному повороті по колу (360°). Виміри проводилися при повороті на 45° (8 положень). Першим положення (0°) вважаємо положення мобільного пристрою по відношенню до антени аналізатора спектра, показане на рисунку 2.10. Обертання проводилося за годинниковою стрілкою. Отримані спектри показано на рисунку 2.11.

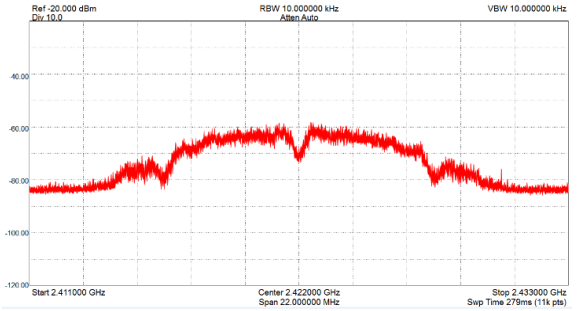
Рисунок 2.10 – Положення мобільного пристрою (0°)



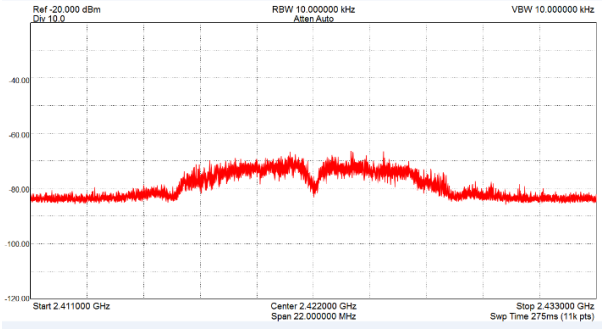
0°



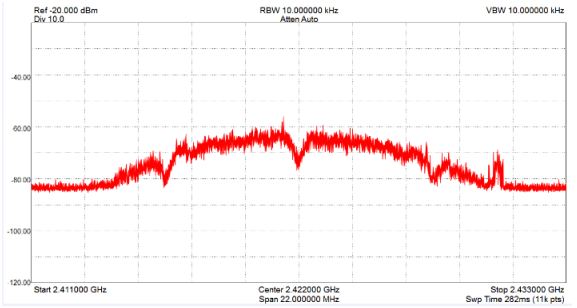
45°



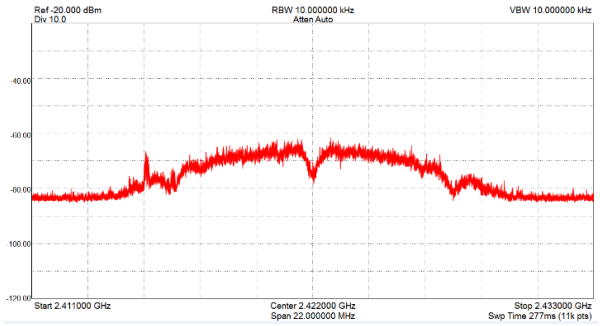
90°



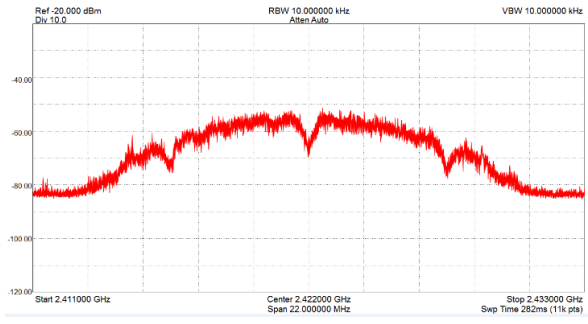
135°



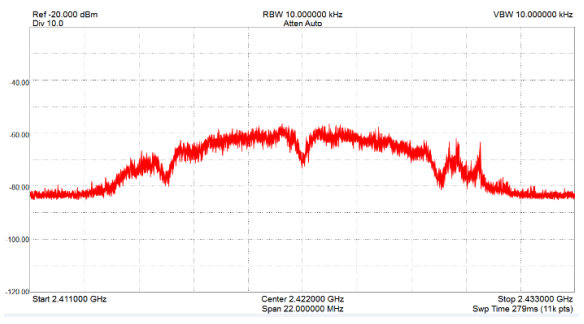
180°



225°



270°



315°

Рисунок 2.11 – Спектри пристрою А при обертанні

Навіть при візуальному аналізі рис. 2.7 – 2.11. можна зробити висновок, що спектр випромінювання у одного і того самого пристрою, хоч і змінюється при його повороті, але несуттєво (в більшій мірі змінюється потужність). Разом з тим спектри випромінювання у різних пристроїв помітно відрізняються (рис.2.7).

2.4.6 Вимірювання вищих гармонік

У більшості радіопередавальних пристроїв, крім основного (корисного) радіовипромінювання, на виході антени присутні неосновні (небажані) випромінювання. Його рівень залежить від особливостей схеми передавача, якості фільтрації вихідних ланцюгів, робочого режиму активних приладів та ін. Ці фактори також можуть бути унікальними для кожного з пристроїв, отже, і позасмугове випромінювання буде унікальним.

Пошук таких випромінювань проводився на частотах 2-ї та 3-ї гармонік і на інших частотах, згідно [54] (рис. 2.12).

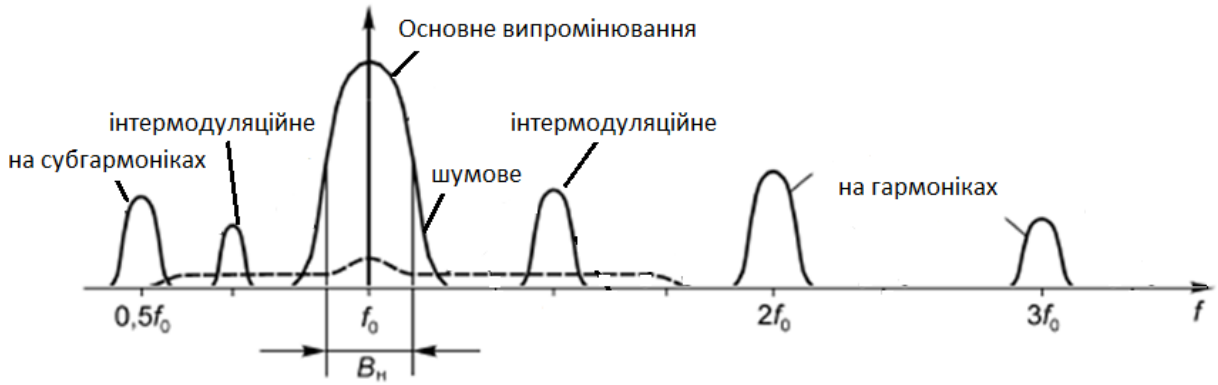


Рисунок 2.12 – Спектр щільності потужності радіовипромінювання радіопередаючого пристрою

Але експериментальні дослідження не виявили позасмугових випромінювань ні на гармоніках, ні на субгармоніках, ні на будь-яких інших частотах, у всякому разі, придатного для вимірювань рівня.

Таким чином, в ході експериментальних досліджень отримані спектри різних мобільних пристроїв в різних умовах. Це дає можливість перейти до їх докладного аналізу.

2.5 Методи обробки отриманих результатів

2.5 1 Аналіз існуючих методів обробки та порівняння спектрів сигналу

Експериментально отримані спектри при візуальному аналізі (при простому розгляді рисунків) мають щось спільне, а в чомусь різняться. Але для задачі ідентифікації потрібен об'єктивний метод, який дозволить в реальних умови ідентифікувати користувачів бездротових мереж за спектральними характеристиками їх пристроїв. Розглянемо існуючі методи порівняння сигналів, що застосовуються для задач ідентифікації.

Огляд [55 – 58] показав, що досить розвинена теорія розрахунку спектрів за неповними часовими рядами, з використанням різних віконних функцій, різні методи їх усереднення і згладжування. Зокрема, методи Бартлетта, Уелча, Блекмена-Тьюки, модифікованих періодограмм та інші. Вони можуть використовуватися для виявлення слабких частотних компонентів в сигналі, або смуг, де зосереджена його максимальна енергія, а також для інших подібних задач.

Для аналізу сигналів має велике практичне застосування кореляційний статистичний аналіз експериментальних даних. Суть кореляційного аналізу зводиться до встановлення рівняння регресії (алгебраїчного рівняння), тобто виду прямолінійного або криволінійного зв'язку між величинами, оцінці тісноти (сили) зв'язків і достовірності результатів вимірювань [82].

Але для задач порівняння вже отриманих спектрів необхідно застосовувати інші методи. Аналогічні рішення були знайдені в сфері голосової ідентифікації.

В роботі [59] автори пропонують спосіб виявлення умови, що дозволяє оцінити властивості «схожості – відмінності» спектрів сигналів по середньоквадратичному відхиленню. Але метод, що розглядають автори дозволяє розділити тільки спектри, що суттєво відрізняються, для спектрів які є досить подібними дана методика не працює.

Тут можна виділити безліч різних способів для визначення належності голосу конкретної людини, в тому числі ідентифікація по спектру. В [60] розглядається спектральна щільність потужності звукової хвилі різних дикторів. Автор пропонує порівнювати отриманий спектр з еталонними зразками в базі. Основним параметром, використовуваним для ідентифікації, є міра подібності двох звукових фрагментів. Для її обчислення необхідно порівняти спектрограми цих фрагментів. При цьому спочатку порівнюються спектри, отримані в окремому вікні, а потім обчислені значення усереднюються. Автор припускає, що X [1..N] і Y [1..N] – масиви чисел, однакового розміру N, що містять значення спектральної потужності першого і другого фрагментів відповідно. Ступінь подібності між ними пропонується обчислювати за такою формулою:

$$f_{xy} = \left| \frac{\sum_i (x_i - M_x)(y_i - M_y)}{\sqrt{\sum_i (x_i - M_x)^2}\sqrt{(y_i - M_y)^2}} \right|, \qquad (2.1)$$

де M_x и M_y– математичне сподівання для масивів X [] и Y [] відповідно, обчислюється за формулою:

$$M_z = \frac{1}{N}\sum_1^N z_i. \qquad (2.2)$$

Автор [60] вважає, що даний спосіб обчислення схожості двох фрагментів, представлених у вигляді спектра, є найкращим для задачі ідентифікації

людини по його голосу. В роботі [61] стверджується, що спектральний аналіз голосу може навіть застосовуватися для діагностики порушень голосової функції.

2.5.2 Розробка методу на основі середніх квадратів різниці

Спектральні характеристики випромінювання різних Wi-Fi пристроїв, отримані при експериментальних вимірах (рис. 2.7) містять в собі інформацію, що ідентифікує пристрій також, як спектральний склад голосу ідентифікує людину в розглянутому вище прикладі. Отже, для ідентифікації необхідно створити базу даних спектрів всіх пристроїв, які можуть підключатися до ТД. Але, на форму спектра можуть впливати:

– розташування пристрою (антени пристрою) відносно приймаючої антени;

– потужність пристрою, яка може адаптивно змінюватися в залежності від дальності до ТД;

– шум та перешкоди від інших пристроїв.

При обробці спектрів необхідно виключити вплив зазначених чинників на ідентифікацію пристрою.

Розглянемо вплив повороту антени.

Спектр Wi-Fi сигналу можна вважати досить вузькосмуговим, (відношення $\Delta f / f_0 = 0.01$), тому характеристики антени можна вважати незмінними. Отже, поворот пристрою буде супроводжуватися лише зміною рівня потужності. Це підтверджується експериментальними вимірами – як видно з рис. 2.7, спектри сигналів, знятих при різних положеннях джерела відносно приймної антени за формою однакові.

Якщо ж результати вимірювання представити в логарифмічній формі, як це зроблено на рисунку 2.7 (в дБ), то відрізнятися буде тільки середній рівень сигналу.

В рамках даної роботи не проводилося вивчення впливу потужності передавача на форму його спектра. Будемо вважати, що передавач є лінійним пристроєм і зміна його потужності через зміну відстані до ТД не призведе до змін в його спектрі.

Вплив шуму розглянемо в розділі 4.

Виходячи з того, що потужність кожної спектральної складової $P_L(f_n)$ при вимірюванні буде відрізнятися від її шаблонної потужності $P_{L0}(f_n)$ (що зберігається в базі) на величину P_0:

$$P_L(f_n) = P_{L0}(f_n) + P_0. \quad (2.3)$$

Тут і надалі всі операції з потужністю виконуються в логарифмічному масштабі. Величина P_0 може мати як додатне, так і від'ємне значення, але воно однакове для всіх спектральних складових. При різних вимірюваннях величина P_0, звісно, може бути різною.

Також додатне чи від'ємне значення може мати різниця виміряного і шаблонного значень, обумовлена природними відмінностями в спектрах при різних вимірах:

$$DP(f_n) = (P_L(f_n) - P_{L0}(f_n)) - P_0. \quad (2.4)$$

Аналогічно буде обчислюватися різниця для двох різних пристроїв.

Для порівняння двох спектрів знайдемо квадрат різниці:

$$\left(DP(f_n)\right)^2 = (P_L(f_n) - P_{L0}(f_n) - P_0)^2. \quad (2.5)$$

Щоб порівнювати не кожне спектральне значення, а всю їх сукупність, знайдемо середній квадрат різниці (СКР):

$$D_{L,L0} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(P_L(f_n) - P_{L0}(f_n) - P_0)^2}\,, \qquad (2.6)$$

де N– кількість частот.

По (2.6) можна порівняти не тільки шаблонне та виміряне значення, а й два виміряних значення $P_{L1}(f_n)$ та $P_{L2}(f_n)$ для того, щоб визначити, наскільки вони відрізняються. Алгоритм порівняння спектрів наведений на рис. 2.13. Шаблонні значення спектра отримуються шляхом усереднення спектральних характеристик за різними положеннями пристроїв, отриманих окремо для різних положень пристрою.

Абонент, підключений до мережі, спочатку проходить ідентифікацію пристрою за стандартними параметрами (MAC-адреса, пароль, ім'я та т. д). Для кожного пристрою в базі зберігається шаблон спектра. Спектр $P_L(f_n)$ сигналу пристрою підключеного до бездротової Wi-Fi мережі проводиться в режимі реального часу. Після зняття спектра обчислюється СКР від шаблону за виразом 2.6, при осередненні вікон по 75 елементів (по ковзному середньому). Коли СКР виявляється менше порогу, то приймається рішення, що спектр відповідає пристрою. Коли це значення перевищує поріг, відбувається перевірка подібності в різних положеннях. Якщо відбувся хоча б один збіг, приймається рішення, що спектр відповідає пристрою. Якщо по всім порівнянням поріг перевищено, то приймається рішення, що спектр не відповідає пристрою.

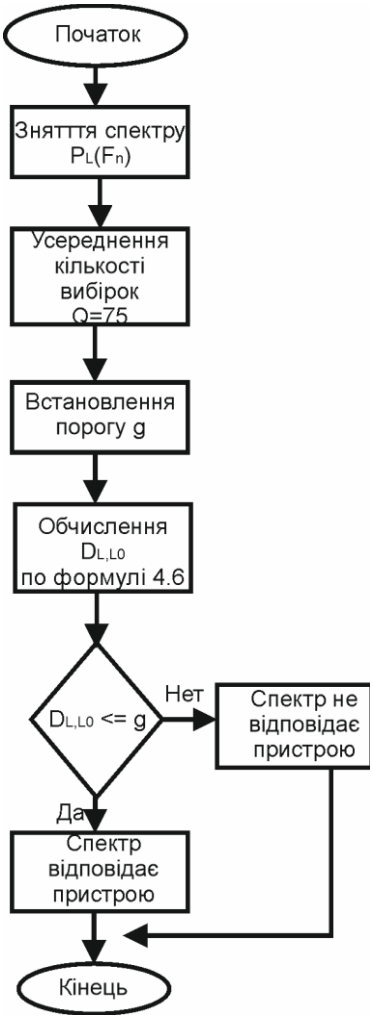


Рисунок 2.13 – Алгоритм порівняння спектрів

2.5.3 Аналіз отриманих результатів

Застосуємо розроблену методику до експериментальних даних, наведених в п. 2.4.

Для цифрових даних, отриманих спектральним аналізатором і записаних у вигляді файлу, за виразом 2.6 рахуємо СКР для кожного пристрою в кожному його положенні та іншими пристроями в кожному їхньому положенні. При цьому мінімізуємо вплив зміни рівня потужності сигналу при переміщенні пристрою за допомогою величини P_0.

Результати вимірювань наведені в таблиці 2.1. У цій таблиці, а також в інших таблицях і на рисунках зберігаються ті ж позначення пристроїв та їх положень, які були прийняті в підрозділі 2.4.

Таблица 2.1

	А1	А2	А3	А4	В1	В2	В3	В4	Г1	Г2	Г3	Г4	Д1	Д2	Д3	Д4	Е1	Е2	Е3	Е4
А1	0	1,6	1,4	1,4	1,3	1,0	1,0	1,0	2,1	2,5	2,0	2,2	2,3	2,5	3,8	3,7	1,2	1,8	1,1	1,2
А2	1,6	0	1,5	1,3	1,2	1,0	1,2	1,4	2,7	3,1	1,9	1,8	3,8	3,1	4,7	4,7	2,1	2,9	1,4	1,3
А3	1,4	1,4	0	1,3	1,1	1,0	1,1	1,1	2,3	2,6	2,0	2,1	3,3	2,7	4,1	4,1	1,8	2,3	1,4	1,3
А4	1,4	1.4	1,3	0	1,3	1,3	1,2	1,3	2,6	3,0	2,2	2,4	3,2	3,0	4,1	4,1	1,8	2,4	1,4	1,3
В1	1,3	1,2	1,1	1,3	0	0,9	1,0	1,1	2,2	2,6	2,0	2,0	3,2	2,4	4,2	4,2	1,7	2,4	1,3	1,2
В2	1,0	1,0	1,0	1,3	0,9	0	0,5	0,7	2,0	2,5	1,6	1,7	3,4	2,7	4,2	4,1	1,5	2,1	1,0	1,0
В3	1,0	1,2	1,1	1,2	1,0	0,5	0	0,5	1,8	2,3	1,6	1,7	3,2	2,6	4,0	3,8	1,2	1,8	1,0	1,0
В4	1,0	1,4	1,1	1,3	1,1	0,7	0,5	0	1,8	2,2	1,8	2,0	3,1	2,6	3,8	3,7	1,0	1,6	1,1	0,9
Г1	2,1	2,7	2,2	2,6	2,2	2,0	1,8	1,8	0	0,6	1,9	2,1	3,5	2,8	4,0	3,9	2,0	1,9	2,5	2,4
Г2	2,5	3,1	2,6	3,0	2,6	2,5	2,3	2,2	0,6	0	2,2	2,4	3,6	3,0	4,1	4,0	2,4	2,3	2,9	2,8
Г3	2,0	1,9	2,0	2,2	2,0	1,6	1,6	1,8	1,9	2,2	0	0,6	4,0	3,3	4,7	4,7	2,5	2,9	2,4	2,3
Г4	2,2	1,8	2,1	2,4	2,0	1,7	1,7	2,0	2,1	2,4	0,6	0	4,2	3,3	5,0	5,0	2,7	3,2	2,5	2,4
Д1	2,3	3,8	3,3	3,2	3,2	3,4	3,2	3,1	3,5	3,6	4,0	4,2	0	2,5	3,6	3,4	3,0	2,9	3,1	3,2
Д2	2,5	3,1	2,7	3,0	2,4	2,7	2,6	2,6	2,8	3,0	3,3	3,3	2,5	0	4,0	2,9	2,7	2,9	2,6	2,7
Д3	3,8	4,7	4,1	4,1	4,2	4,2	4,0	3,8	4,0	4,1	4,7	5,0	3,6	4,0	0	3,1	3,5	3,1	3.7	3,8
Д4	3,7	4,7	4,1	4,1	4,2	4,1	3,8	3,7	3,9	4,0	4,7	5,0	3,4	2,9	3,1	0	3,2	2,7	3,7	3,7
Е1	1,2	2,1	1,8	1,8	1,7	1,5	1,2	1,0	2,0	2,4	2,5	2,7	3,0	2,7	3,5	3,2	0	1,0	1,2	1,1
Е2	1,8	2,9	2,3	2,4	2,4	2,1	1,8	1,6	1,9	2,3	2,9	3,2	2,9	2,9	3,1	2,7	1,0	0	1,9	1,9
Е3	1,1	1,4	1,4	1,4	1,3	1,0	1,0	1,1	2,5	2,9	2,4	2,5	3,1	2,6	3,7	3,7	1,2	1,9	0	0,7
Е4	1,2	1,3	1,3	1,3	1,2	1,0	1,0	0,9	2,4	2,8	2,3	2,4	3,2	2,7	3,8	3,7	1,1	1,9	0,7	0

У таблиці міститися значення СКР в дБ, розраховані по (2.6) для кожного пристрою в кожному його положенні по відношенню до інших пристроїв в кожному їхньому положенні. Наприклад, на перетині А1 і А1 стоїть «0»– звісно, так як між одним і тим же значенням різниці немає. На перетині А1 і А3 стоїть значення «1,4» – це означає що СКР спектрів для першого і третього положення пристрою А (відповідно до рисунка 2.6) відповідає значенню 1,4 дБ. На перетині А1 і Д3 ми бачимо значення «3,8», що означає СКР спектрів пристрою А в першому положенні та пристрою Д в третьому положенні.

В цілому таблиця 2.1 досить складна для сприйняття в чисельному вигляді, тому отримані значення СКР були усереднені по всіх чотирьом положенням, для всіх досліджених пристроїв та наведені в табл. 2.2. Наприклад, на перетині А і А має значення «1,1». Дане значення було отримане шляхом суми всіх пересічних значень СКР (з таблиці 2.1) для пристрою А в положеннях А1, А2, А3 і А4 і розділене на їх кількість. Відповідно перетин В і Г означає суму всіх СКР пристрою В для чотирьох положень пересічні в табл.2.1 з усіма положеннями пристрою Б і поділені на кількість отриманих порівнянь СКР.

Отримані результати показують схожість спектрів одного і того ж пристрою в різних положеннях і різницю між спектрами інших пристроїв.

Графічне представлення результатів табл. 2.2 продемонстровані на рисунку 2.14. На рисунку добре проглядаються темні плями, що відповідають максимальному збігу для однакових пристроїв (мінімуму СКР). Чим далі від перетинів, тим світліше простір, що означає велику різницю СКР розглянутих спектрів мобільних пристроїв.

Таблиця 2.2

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

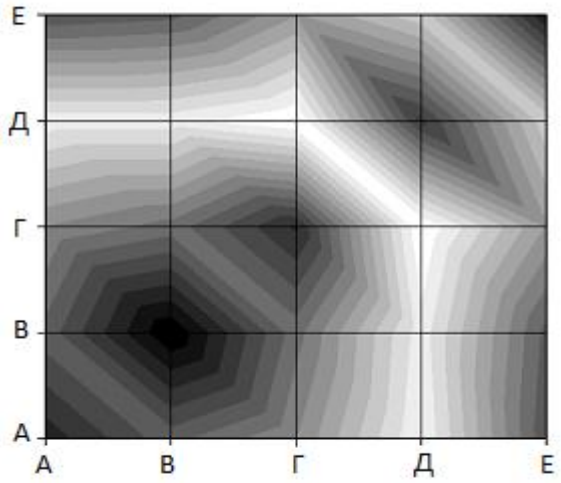


Рисунок 2.14 – Графічне представлення результатів табл. 2.2

Пристрій, що досліджується, може перебувати в будь-якому положенні, в тому числі, в проміжних, для яких дані не знімалися. Тому для подальшого аналізу було запропоновано застосовувати усереднене значення його спектра по всім чотирьом положенням, яке в подальшому будемо називати шаблоном спектра. Ці шаблонні значення навіть візуально відрізняються один від одного, що показано на рисунку 2.15.

Далі в роботі були розглянуті значення СКР шаблонів в дБ, одного пристрою до різних положень інших. Результати отриманих даних наведені в таблицях 2.3 – 2.7. Нижній рядок під кожною таблицею – це середнє значення СКР за всіма положеннями (всім значенням даного стовпця).

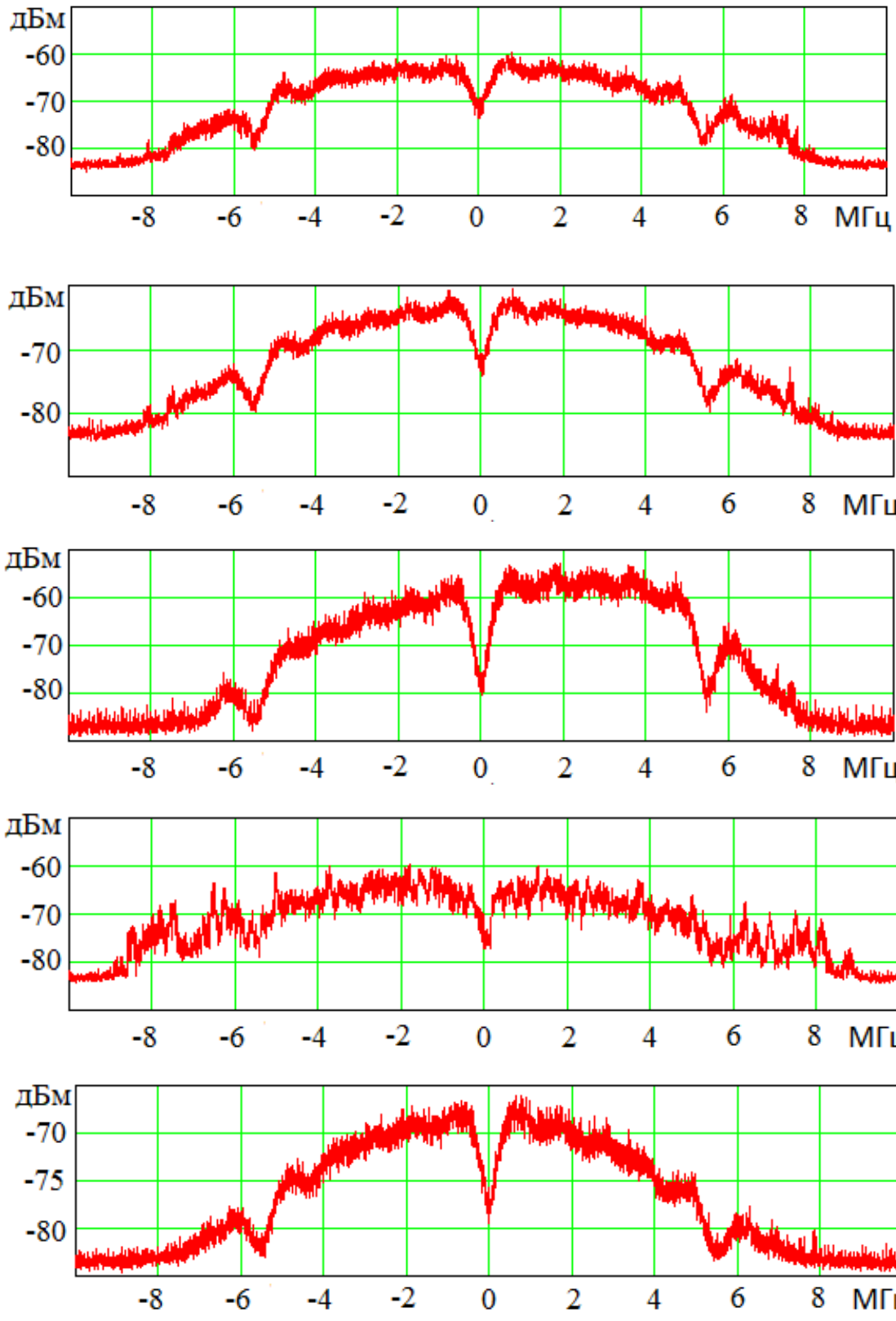


Рисунок 2.15 – Шаблони спектрів пристроїв з відповідними літерними позначеннями

Таблиця 2.3

Шаблон пристрою А									
А1	0,8	**В1**	0,9	**Г1**	2,2	**Д1**	3,2	**Е1**	1,5
А2	0,6	**В2**	0,9	**Г2**	2,7	**Д2**	2,7	**Е2**	2,2
А3	0,7	**В3**	0,8	**Г3**	1,8	**Д3**	4,1	**Е3**	1,0
А4	0,8	**В4**	0,8	**Г4**	1,9	**Д4**	4,1	**Е4**	0,9
Ср.	0,7	**Ср.**	0,9	**Ср.**	2,2	**Ср.**	3,5	**Ср.**	1,4

Таблиця 2.4

Шаблон пристрою В									
В1	0,8	**А1**	0,8	**Г1**	2,0	**Д1**	3,2	**Е1**	1,3
В2	0,4	**А2**	1,1	**Г2**	2,4	**Д2**	2,6	**Е2**	1,9
В3	0,4	**А3**	1,0	**Г3**	1,7	**Д3**	4,0	**Е3**	0,9
В4	0,5	**А4**	1,2	**Г4**	1,8	**Д4**	3,9	**Е4**	0,8
Ср.	0,5	**Ср.**	1,0	**Ср.**	2,0	**Ср.**	3,4	**Ср.**	1,2

Таблиця 2.5

Шаблон пристрою Г									
Г1	1,1	**А1**	1,9	**В1**	2,0	**Д1**	3,7	**Е1**	2,1
Г2	1,4	**А2**	2,2	**В2**	1,6	**Д2**	3,1	**Е2**	2,3
Г3	0,8	**А3**	2,0	**В3**	1,5	**Д3**	4,3	**Е3**	2,3
Г4	1,1	**А4**	2,3	**В4**	1,6	**Д4**	4,2	**Е4**	2,2
Ср.	1,1	**Ср.**	2,1	**Ср.**	1,7	**Ср.**	3,8	**Ср.**	2,2

Таблиця 2.6

Шаблон пристрою Д									
Д1	1,9	**А1**	2,4	**В1**	2,9	**Г1**	2,9	**Е1**	2,2
Д2	2,4	**А2**	3,5	**В2**	2,9	**Г2**	3,1	**Е2**	1,9
Д3	2,3	**А3**	2,9	**В3**	2,7	**Г3**	3,6	**Е3**	2,5
Д4	2,0	**А4**	2,9	**В4**	2,5	**Г4**	3,9	**Е4**	2,6
Ср.	2,2	**Ср.**	2,9	**Ср.**	2,8	**Ср.**	3,4	**Ср.**	2,3

Таблиця 2.7

Шаблон пристрою Е									
Е1	1,0	**А1**	1,4	**В1**	2,0	**Г1**	2,5	**Д1**	3,3
Е2	1,5	**А2**	2,1	**В2**	1,6	**Г2**	3,0	**Д2**	3.2
Е3	1,3	**А3**	2,0	**В3**	1,4	**Г3**	2,5	**Д3**	3,6
Е4	1,3	**А4**	1,9	**В4**	1,3	**Г4**	2,7	**Д4**	3,3
Ср.	1,3	**Ср.**	1,9	**Ср.**	1,6	**Ср.**	2,7	**Ср.**	3,4

Аналіз показує, що відмінність між шаблоном і різними положеннями «свого» пристрою в цілому менше, ніж між шаблоном і різними положеннями інших пристроїв (за винятком ситуації, коли порівнюються два різних пристрої однієї й тієї ж моделі). Але слід враховувати, що алгоритмом (рис. 2.13) не передбачено порівняння виміряного спектру з кожним шаблоном – порівняння відбувається тільки зі «своїм».

Вищевказаним алгоритмом передбачено порівняння отриманого значення СКР з порогом (перевірка на потрапляння в «зону допуску», обмежена деякою пороговою величиною). Як видно з табл. 2.3 – 2.7, значення цих порогів будуть різними для різних пристроїв. Для розглянутих пристроїв значення порогів наведені в табл. 2.8.

Таблиця 2.8

Пристрій	А	В	Г	Д	Е
Поріг g, дБ	0,9	0,8	1,4	2,4	1,5

Розглянемо тепер вплив температури. У таблиці 2.9 порівнюються спектри одного і того ж смартфону при кімнатній температурі і при температурі +5 ^{0}C.

Таблиця 2.9

	Б1	Б2	Б3	Б4
А1	1,8	1,2	1,6	1,8
А2	2,2	1,9	1,4	1,3
А3	2,2	1,6	1,5	1,6
А4	2,2	1,7	1,6	1,7

Результати порівняння спектрів з поправкою на зміну температури і без показали, що значення середнього квадрата різниць незначно змінюється тіль-

ки в другому та третьому десяткову знаку, при цьому підсумкові результати (округлені по першому десяткову знаку) не змінюються. На рисунку 2.16 показані два спектра в першому положенні. Верхній спектр належить пристрою А, при кімнатній температурі, а нижній, того ж пристрою, тільки при температурі +5 ^{0}С.

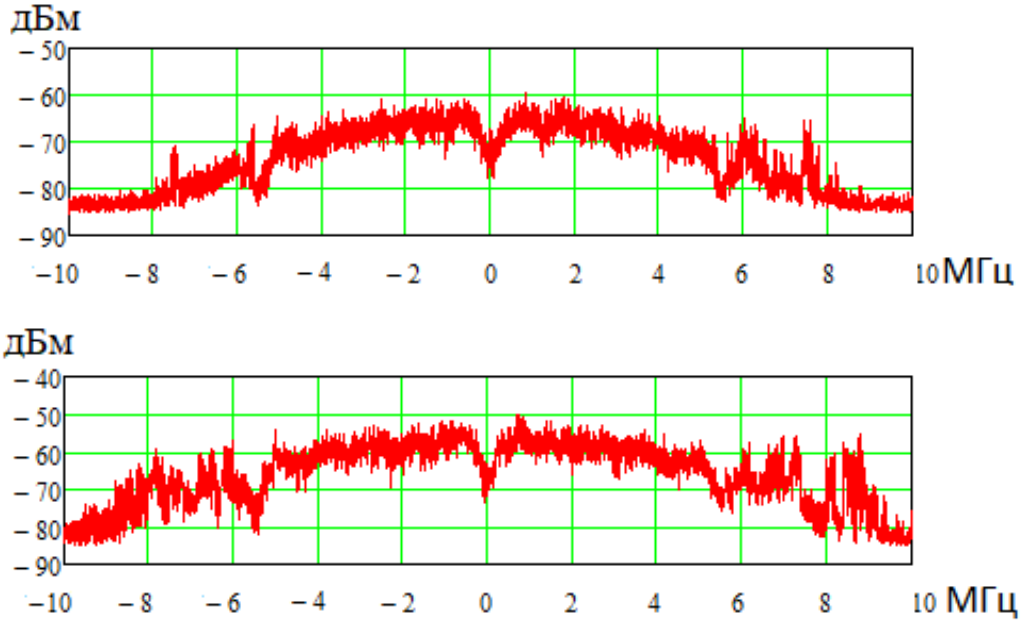


Рисунок 2.16 – Спектри пристроїв з відповідними літерними позначеннями в першому положенні

На рисунку 2.17 наведені результати порівняння пристрою А при кімнатній температурі і при зниженні температури пристрою до +5 ^{0}С (позначено як пристрій Б).

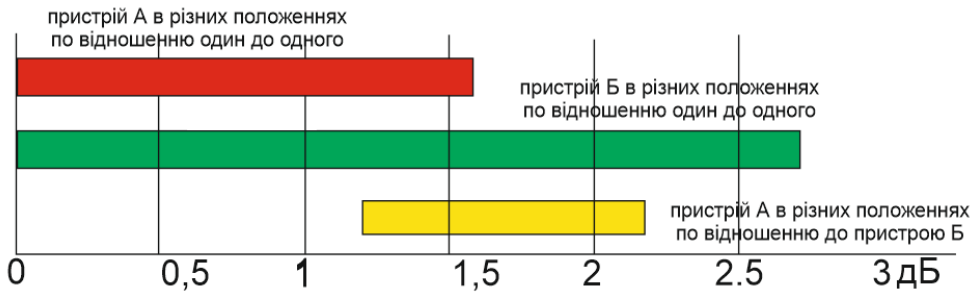


Рисунок 2.17 – Результати порівняння пристрою А при знижені температури

Рисунок показує, що для коректного розпізнавання пристрою при зміні температури необхідно змінювати область допуску, що може значно погіршити точність розпізнавання. Тому на даному етапі можна сказати лише те, що облік температурних змін спектрів вимагає додаткового дослідження.

Узагальнені результатів вимірювань для всіх пристроїв, що беруть участь в експериментах, показані у вигляді діаграми на рис. 2.18.

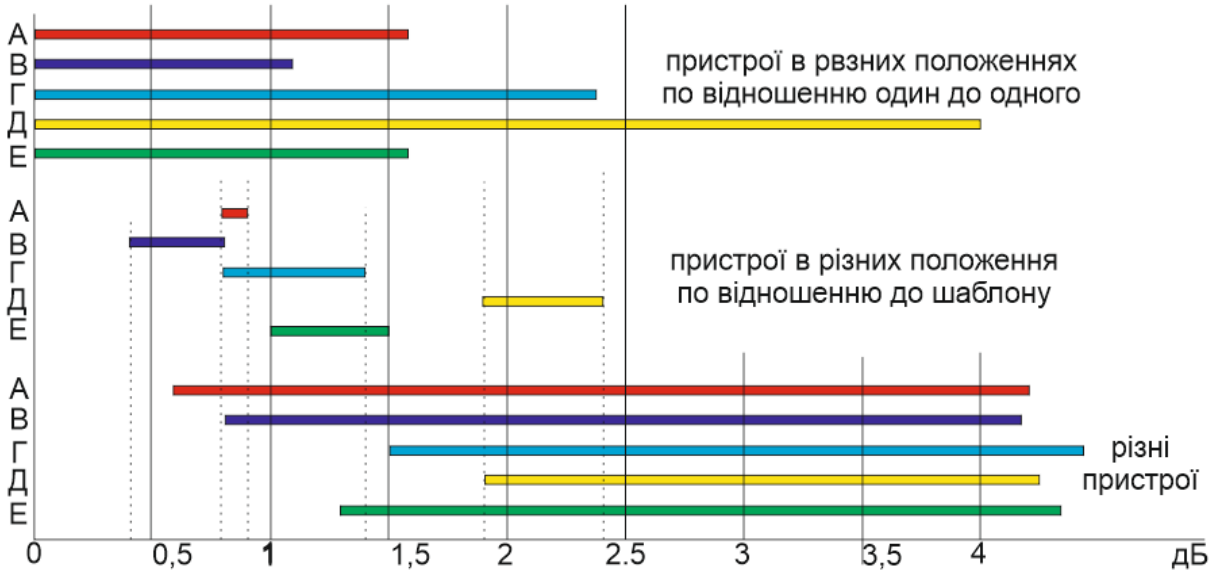


Рисунок 2.18 – Результати вимірів

На діаграмі показані діапазони значень, які можуть мати середні квадрати різниць спектральних відліків для різних пристроїв. З рисунка видно, що значення шаблонів та інших пристроїв практично не перетинаються. Великі похибки в даних дослідженнях показали однакові моделі мобільних пристроїв. Також схожість показали пристрої Д і Е, причому, тільки в одному з положень. Але вони мають абсолютно різні спектри, що видно на рисунку 2.15 і що може бути виявлено більш детальним їх аналізом.

Розвитком запропонованого методу може стати розподіл аналізуючих спектрів на кілька окремих смуг (наприклад, на 2, 4 або більше) і обчислення СКР для кожної з них. Таким чином, кожна різниця спектрів буде описуватися

вже не одним числом, а низкою чисел. Це дозволить виявляти відмінності, які «випадають» при повному осередненні всіх значень.

Так як різниця в деяких випадках (наприклад два пристрої однакової моделі) можуть показувати близькі результати розглянемо можливість застосування ще одного методу основаного на кореляційній обробці.

2.5.4 Розробка методу на основі кореляційної обробки

У підрозділі 2.4 дисертаційної роботи розглянуті експериментально отримані спектри пристроїв, підключених до бездротової мережі, два з яких наведені на рис. 2.19. Застосуємо до вказаних залежностей взаємно-кореляційну обробку.

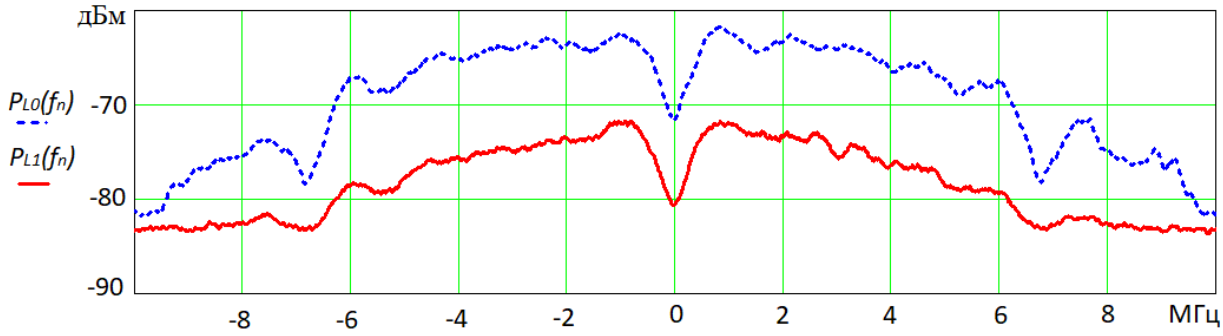


Рисунок 2.19 – Спектри пристроїв

Як відомо, для кількісної оцінки ступеня відмінності сигналу S(t) та його зміщеної копії S(t-τ) використовується автокореляційна функція (АКФ) сигналу S(t), що дорівнює скалярному добутку сигналу та його копії:

$$B(\tau) = \int_{-\infty}^{\infty} S(t) \cdot S(t-\tau) dt. \qquad (2.7)$$

Застосуємо вираз (1) для порівняння спектрів:

$$B(j) = \frac{1}{N}\sum_{n=0}^{N-1} P_{L1}(f_n) \cdot P_{L2}(f_{n+j}), \qquad (2.8)$$

де $P_L(f_n)$ – потужність кожної спектральної складової; N – кількість спектральних складових. Причому, вказаний вираз буде застосовуватися для розрахунку кореляції шаблону (автокореляційна функція, АКФ) та спектра шаблону зі спектрами «чужих« пристроїв» (ВКФ). Розрахунки були виконані для всіх пристроїв в різних положеннях. На рисунку 2.20 показані деякі з них.

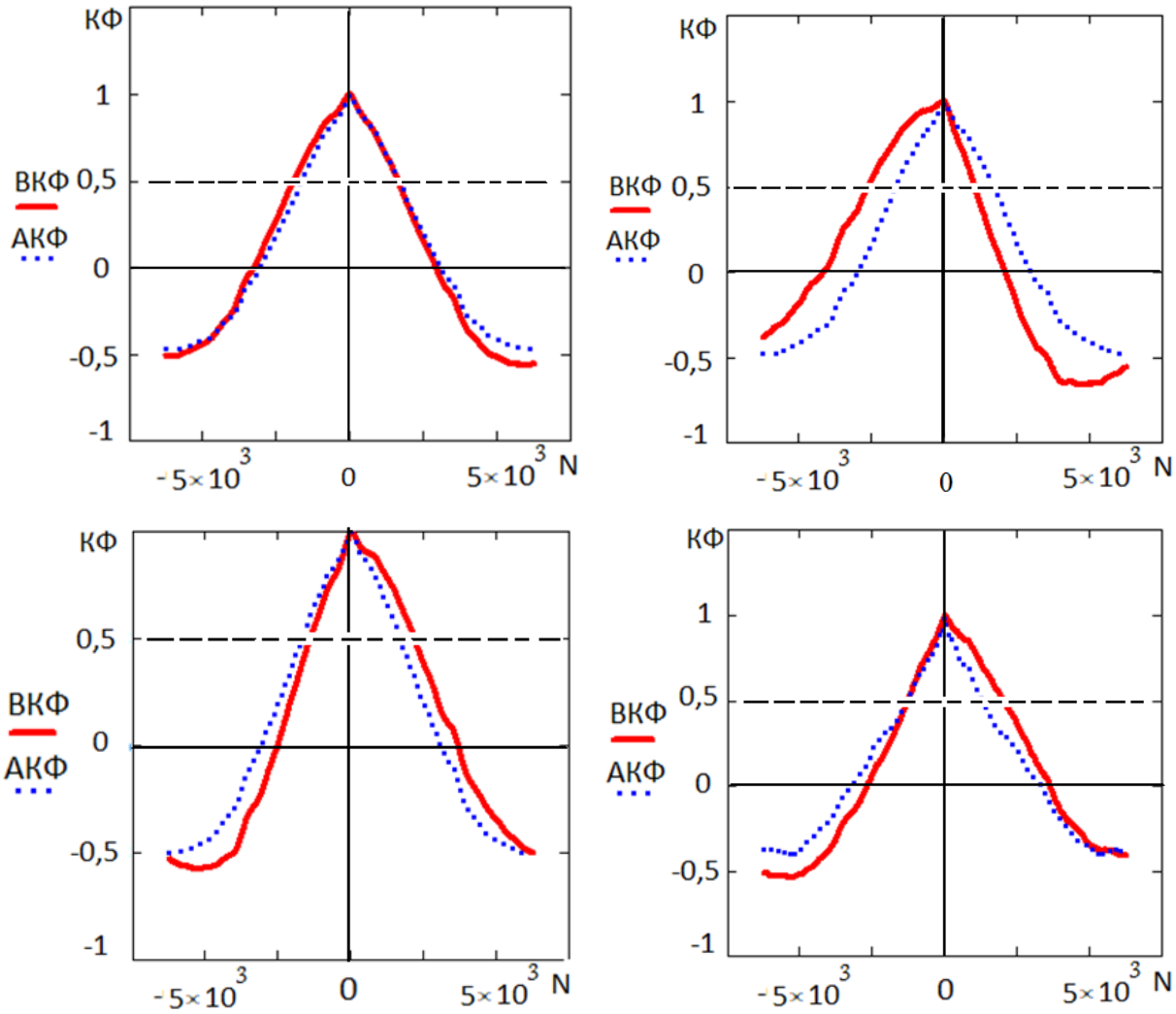


Рисунок 2.20 – АКФ и ВКФ

Істотної різниці в наведених на рис. 2.20 залежностях не спостерігається. Тому було розраховано середньоквадратичне відхилення (СКВ) для всіх отриманих функцій:

$$\sigma = \sqrt{\frac{1}{2K \cdot B(j)_{cp}} \cdot \sum_{j=-K}^{K} (J^2 \cdot B(j))}, \qquad (2.9)$$

де j – елементи ряду; $B(j)_{cp}$ – середнє значення АКФ:

$$B(j)_{cp} = \frac{1}{2K+1} \sum_{j=-K}^{K} B(j)\,). \qquad (2.10)$$

Результати розрахунку σ для одного з шаблонів (А) по відношенню до різних положень пристроїв наведені в таблиці 2.10.

Таблиця 2.10

	А1	А1	А3	А4	В1	В2	В3	В4	Г1	Г2	Г3	Г4	Д1	Д2	Д3	Д4
σ	945	943	940	937	937	949	952	952	955	953	942	943	944	954	940	932

Також була виміряна ширина (в кількості відліків) АКФ для шаблонів та ВКФ для всіх пристроїв по відношенню до шаблону на рівні 0.5. Результати розрахунку для одного з шаблонів наведені в таблиці 2.11.

Таблиця 2.11

	Ширина АКФ (ВКФ) по рівню 0,5					
Положення	Шаблон А	А	В	Г	Д	Е
1	2650	2655	2715	2864	2701	2929
2	2650	2688	2726	2879	2833	2937
3	2650	2675	2796	2817	2588	2844
4	2650	2635	2796	2785	2459	2807
Середнє	2650	2663	2758	2836	2645	2879

З таблиці видно, що ширина ВКФ чужих пристроїв може бути вужчою за АКФ.

На підставі виконаних розрахунків можна сказати, що:

– різниці в середньоквадратичному відхиленні ВКФ для шаблону зі своїм пристроєм і чужими не виявлено;

– різниці в ширині ВКФ за рівнем 0,5 також не виявлено. При нормуванні всі функції практично ідентичні;

– істотного зсуву центральної частоти в ВКФ також не спостерігається.

Таким чином, параметри до другого порядку включно не дозволяють виявити різницю між двома спектрами. Але з рис. 2.11 видно, що ВКФ мають певний «перекос», який може характеризуватися коефіцієнтом асиметрії. Як відомо, коефіцієнт асиметрії розраховується як:

$$A = \frac{m_3}{\sigma^2}, \qquad (2.11)$$

де, σ – СКВ; m_3 – центральний емпіричний момент третього порядку, який обчислювався за формулою:

$$m_з = \frac{1}{(2k+1)\cdot B(j)_{ср}} \sum_{j=-K}^{K} (j - j_{ср})^3 \; B(j). \qquad (2.12)$$

Стосовно до нашого випадку асиметрія розраховувалася:

$$\mathrm{A} = \frac{\frac{1}{(2k+1)\cdot B(j)_{ср}} \sum_{j=-K}^{K} (j - j_{ср})^3 \; B(j)}{\left(\sqrt{\frac{1}{2K \cdot B(j)_{ср}} \cdot \sum_{j=-K}^{K} (J^2 \cdot \; B(j))}\right)^3}, \qquad (2.13)$$

У таблиці 2.12 наведені результати отриманих за (2.13) коефіцієнтів асиметрії. Середнє значення коефіцієнта асиметрії обчислювалося при підсумовуванні кожного елемента за значенням модуля.

Виходячи з таблиці можна зробити висновок, що мінімальне значення коефіцієнта асиметрії при порівнянні шаблону з різними положеннями власного пристрою. Отже, ця ознака також може бути використана для ідентифікації Wi-Fi пристроїв.

Слід зазначити, що розглянуті методи на основі аналізу взаємної кореляційної функції і середнього квадрату різниці дали практично однакові результати. Однак метод аналізу заснований на СКР набагато простіше і швидше в плані обчислень.

Таблиця 2.12

		Шаблони пристроїв									
		А	**$А_{ср}$**	**В**	**$В_{ср}$**	**Г**	**$Г_{ср}$**	**Д**	**$Д_{ср}$**	**Е**	**$Е_{ср}$**
Пристрої в різних положеннях	**А1**	0,013	0,0057	0,008	0,007	-0,07	0,07	0,075	0,06	0,038	0,03
	А2	0,002		-0,005		-0,07		0,06		0,03	
	А3	0,004		-0,007		-0,07		0,06		0,029	
	А4	0,004		-0,008		-0,066		0,059		0,017	
	В1	0,005	0,008	-0,007	0,0048	-0,066	0,074	0,049	0,07	0,026	0,04
	В2	0,003		-0,0004		-0,076		0,074		0,038	
	В3	0,016		0,011		-0,075		0,087		0,046	
	В4	0,006		0,0007		-0,079		0,077		0,036	
	Г1	0,077	0,07	0,079	0,07	-0,008	0,0055	0,057	0,025	0,093	0,09
	Г2	0,077		0.08		0,011		-0,002		0,065	
	Г3	0,063		0,067		-0,002		0,022		0,093	
	Г4	0,064		0,069		0,001		0,017		0,094	
	Д1	-0,077	0,06	-0,083	0,07	0,038	0.04	-0,023	0,01	-0,08	0,06
	Д2	-0,07		-0,075		-0,039		0,016		-0,05	
	Д3	-0,051		-0,057		-0,056		0,012		-0,049	
	Д4	-0,048		-0,022		-0,022		0,002		-0,068	
	Е1	-0,012	0,024	-0,022	0,03	-0,098	0,09	0,08	0,07	0,016	0,016
	Е2	-0,012		-0,019		-0,114		0,08		0,022	
	Е3	-0,038		-0,044		-0,078		0,052		-0,014	
	Е4	-0,038		-0,045		-0,078		0,051		-0,012	

Висновки по розділу 2

1. Експериментально встановлено візуальну схожість спектрів Wi-Fi сигналів одного і того ж пристрою в різних положеннях та суттєві відмінності в спектрах випромінювання у різних пристроїв, що може бути використано для їх ідентифікації.

2. Запропоновано новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом 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. Показано, що СКР спектральних відліків та коефіцієнт асиметрії ВКФ для шаблону та відповідного йому пристрою істотно менше, ніж для шаблону та іншого пристрою, що може слугувати ідентифікуючою ознакою.

5. Встановлено діапазон значень середніх квадратів різниць спектральних відліків та коефіцієнтів асиметрії, які можуть відповідати як одному й тому ж пристрою в різних положеннях, так і різним пристроям. Для ідентифікації пристроїв в цьому діапазоні необхідно здійснювати більш детальний аналіз спектра.

6. Встановлено, що суттєва зміна температури пристрою може змінювати форму його спектра настільки, що його коректне розпізнавання запропонованим методом може бути ускладнене.

Таким чином, форма спектра сигналу, випромінюваного Wi-Fi пристрою, може слугувати одним з ідентифікуючих ознак.

РОЗДІЛ 3
ІДЕНТИФІКАЦІЯ КОРСТУВАЧІВ WI-FI МЕРЕЖІ ПО МІСЦЕПОЛОЖЕННЮ ЇХ ПРИСТРОЇВ

Визначення місцеположення джерела випромінювання – класична радіотехнічна задача. На шляху її вирішення існує великий досвід та публікації [62-68]. Але коли джерелом радіосигналу є абонентський Wi-Fi пристрій, вимірювальні прилади базуються на типових точках доступу WI-FI мережі, а середовищем поширення радіохвиль є міська забудова, житлові, офісні та виробничі потужності, то виникають особливості реалізації класичних методів, які необхідно враховувати.

В даному розділі розглянуто можливість використання місцезнаходження пристрою бездротової мережі, як один з ідентифікуючих ознак.

Матеріали розділу опубліковані в розділі [3, 4, 6, 12, 13].

3.1 Місцеположення як ідентифікуюча ознака.

Wi-Fi – це бездротова технологія, але часто використовується для зв’язку зі стаціонарними об'єктами, такими як: веб-камери, платіжні термінали, стаціонарні комп'ютери, стаціонарні пристрої «розумного будинку» та інші. За даними джерела [69] до 2030 року кількість пристроїв Інтернету речей виросте до 125 мільярдів (сьогодні близько 30 мільярдів). Це говорить про те, що більшу частину пристроїв Wi-Fi будуть займати стаціонарні об'єкти.

Навіть якщо пристрій потенційно мобільний (ноутбук, планшет, смартфон і т. д.), для більшості користувачів є область простору або типовий маршрут, в межах якого вони найчастіше використовують свої пристрої.

Тому моніторинг розташування пристроїв користувачів бездротових Wi-Fi мереж може бути одним з додаткових ознак для виявлення несанкціонова-

ного доступу і виявлення зловмисника. Виявлення такого пристрою в невластивому йому місці може бути ознакою:

– викрадення пристроїв;

– нехарактерної (зловмисної) поведінки користувача;

– того, що зловмисник працює під його ім'ям (MAC, IP).

Wi-Fi мережа зазвичай забезпечує зв’язок і за межами того простору, для якого вона призначена (на сусідніх поверхах, і навіть за межами будівель і територій, що охороняються). Спроби використання мережі поза межами можуть бути обмежені, якщо відоме місцеположення користувача.

В останній час позиціонування об'єктів стало невід'ємною частиною торгівлі та логістики (з використанням FRID технологій), сфера застосування стрімко розширюється [70]. Такого роду рішення прискорюють процес торгівлі та відстеження продукції. Технологія Wi-Fi сама по собі вже має базові функції FRID, тому використання розгорнутої мережі Wi-Fi для моніторингу підключених користувачів, зіграло б позитивну роль в забезпеченні безпеки підприємств та офісів.

Контроль місцеположення має вирішальне значення для підвищення безпеки, що дає можливість аналізувати дії співробітників і виявляти порушення в роботі за допомогою різноманітних програмних засобів.

Впровадження систем контролю місцеположення – це довгострокове вкладення. Компанії витрачають багато часу і грошей на захист своїх підприємств, але, незважаючи на це, за даними [71], за 2018 рік майже половина українських організацій постраждали від економічних злочинів і шахрайства за останні два роки. У більшості випадків шахрайство було скоєно самими співробітниками.

Відкритість і простота підключення до бездротових мереж, які швидкими темпами впроваджуються повсюдно, можуть значно полегшити задачу зловмисникам. Можливість контролювати місцеположення користувачів бездро-

тових мереж в поєднанні з іншими заходами захисту допоможе значно скоротити відсоток несанкціонованих дій на території що захищається.

3.2 Аналіз методів визначення місцеположення абонента

Спочатку розглянемо класичні методи визначення місцеположення джерела радіовипромінювання стосовно нашої задачі і визначимо ті з них, які можуть бути застосовані для прийняття рішень про аномальний стан Wi-Fi мережі.

Методи позиціонування можна класифікувати за параметрами, що використовуються для розрахунку координат пристроїв, що випромінює радіосигнал. Існує чотири основні методи:

– метод, заснований на вимірюванні напрямку сигналу (AoA – Angle of Arrival або кутовий метод) [62, 64];

– метод, заснований на вимірюванні абсолютного значення затримки приймання сигналу (ToA – Time of Arrival або далекомірний метод) [62, 65, 66];

– метод, заснований на вимірюванні різниць в затримках прийому сигналів (TDoA – TimeD ifference of Arrival або різницево-далекомірний метод) [62, 65, 66];

– метод, заснований на вимірюванні рівня потужності прийнятого сигналу (RSSI – Received Signal Strength Indicator) [67, 68].

Також можуть використовуватися комбінації цих методів.

Коротко розглянемо їх.

3.2.1 Кутовий метод

Для реалізації цього методу необхідно як мінімум три стаціонарних приймальних пунктів, координати яких точно відомі. У кожному з цих пунктів має вимірюватися кут (напрямок) на джерело радіовипромінювання. Знан-

ня трьох кутів у просторі дозволяє однозначно визначити точку, в якій знаходиться джерело.

Цей метод на перший погляд видається досить простим. Серед його переваг можна виділити наступне:

– для «плоского» випадку (коли наперед відомо, що всі можливі джерела сигналу знаходяться в одній площині, наприклад, в площині землі або одного поверху) досить використовувати всього два приймальних пункту;

– похибка вимірювання для практичних задач цілком допустима;

– для здійснення вимірів не вимагається синхронізація або знання про затримки.

Але при реалізації даного методу на основі існуючого (типового) Wi-Fi обладнання неминуче виникнуть труднощі. Так, для визначення напрямку прийому сигналу необхідно застосовувати гостроспрямовані антени, які в типовій комплектації відсутні. Крім того, необхідно передбачити функцію повороту цих антен, програмне керування поворотом та вимірювання рівня сигналу як функцію від кута повороту. Причому, вимірювання необхідно здійснювати узгоджено на двох (або трьох) точках доступу.

Не варто забувати, що при всьому цьому точки доступу мають виконувати свою головну задачу – забезпечити зв’язок всім абонентам мережі.

Звичайно, вказані складності не є непереборними: існують ФАР з електронним управлінням діаграм направленості, існують точки доступу з можливістю формування декількох променів, зв'язок з кожним абонентом здійснюється пакетами, тому її короткочасне переривання може бути цілком природним, якщо вимірювання провести досить швидко.

Але, крім вищеназваних недоліків, необхідно враховувати ще одну обставину. Кутомірний метод добре застосовувати на відкритому просторі, де поширення радіохвиль прямолінійно. А в умовах міської забудови, особливо в приміщеннях, можливе виникнення перевідбитків від стін, металевих предметів і т. д. Причому, не виключені ситуації, коли відбитий сигнал в точці при-

йому може виявитися сильнішим за «прямий». Це може серйозно вплинути на результати вимірювань.

Тому ці труднощі, на нашу думку, не дозволяють вважати кутовий метод простим і придатним для нашої задачі.

3.2.2 Далекомірний метод

Метод ToA оснований на вимірюванні часу поширення сигналу від джерела до приймача.

При вирішенні нашої задачі слід пам'ятати, що абонентський пристрій є не радіолокаційною ціллю (пасивним відбивачем), а активним джерелом сигналу. І випромінює воно відповідно до свого алгоритму роботи. Точка доступу може ініціювати відповідь абонентського пристрою на свій запит, але в цьому випадку час від посилання запиту до прийому відповіді буде включати не тільки час поширення сигналу в обидві сторони, але і затримку на обробку запиту в абонентському пристрої.

Для реалізації далекомірного методу в нашому випадку необхідно, щоб абонентський пристрій послідовно підключався до кожної з трьох точок доступу і відповідав на запит кожної з них. При цьому немає ніякої впевненості, в тому що затримка між запитом і відповіддю в кожному випадку буде однаковою. Як зазначається в роботі [3] «... в процедурі роботи з точкою доступу передбачені наступні операції: етап звернення до точки доступу; затримка часу DIFS; формування маячка; передача маячка; очікування затримки SIFS і передача управління...»

При цьому «тривалість часових інтервалів становить: ASK (підтвердження) = 304 мкс; DATA (дані) – 937 мкс; DIFS (часовий інтервал) – 100 мкс; SIFS (часовий інтервал) – 10 мкс; CRS (контрольна сума) – 304 мкс; POLL (запит) 352 мкс» (рис. 3.1.) [3]

У режимі колективного доступу DCF [4, 13] (рис. 3.2) всі абоненти мережі, перед тим як почати передачу даних, перевіряють вільне середовище чи ні.

Якщо середовище виявляється вільним, абоненти вичікують протягом певного проміжку часу, який є випадковим і складається з двох складових: обов'язкового проміжку DIFS і проміжку зворотного відліку (Backoff time), що обирається випадковим чином.

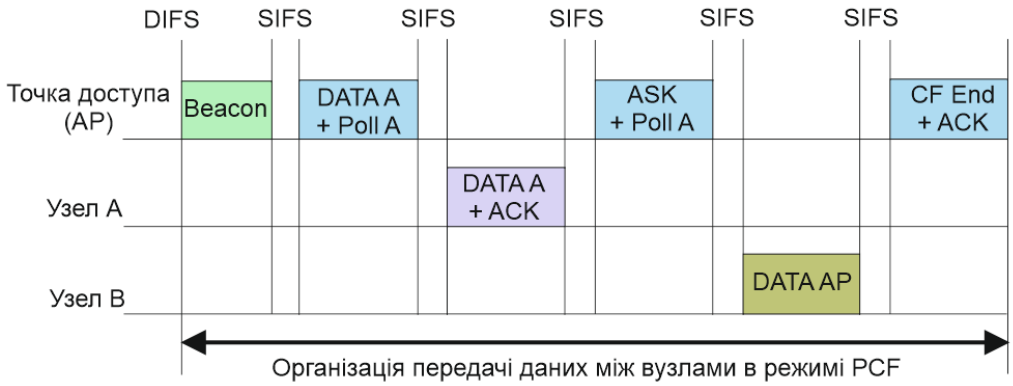


Рисунок 3.1 – Організація передачі даних між вузлами в режимі PCF

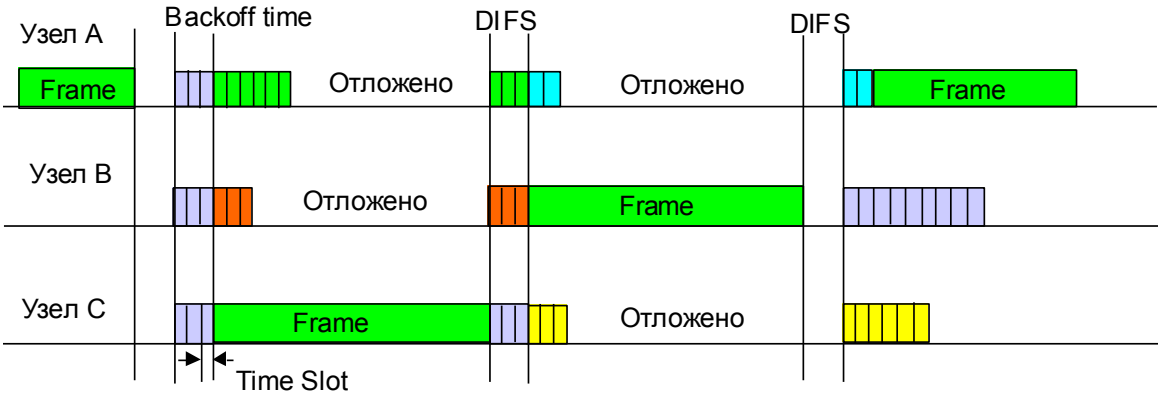


Рисунок 3.2 – Організація передачі даних між вузлами в режимі DCF

Таким чином, виходить, що при дальності від ТД до АУ 10...50 м час затримки на поширення радіохвиль складе від 33 ... 166 нс, а можливі варіації з затримкою між запитом і відповіддю може перевищувати десятки мікросекунд.

Як бачимо, для реалізації далекомірного методу не потрібно гостроспрямованих антен та іншого складного обладнання – всі необхідні вимірювання можуть виконуватися програмно. Але затримки, зумовлені алгоритмом роботи

Wi-Fi мережі, зводять нанівець ці переваги. Тому навіть виконання безлічі вимірів з наступним усередненням не забезпечить прийнятної похибки.

3.2.3 Різницево-далекомірний метод

У різницево-далекомірному методі (TDoA) не потрібно знати абсолютне значення затримок, потрібні тільки їх відмінності. Місцеположення джерела радіовипромінювання визначається як точка перетину двох гіпербол на площині або точка перетину трьох гіперболоїдів обертання з фокусами в точках розташування пунктів прийому в тривимірному просторі [72, 73].

Точність визначення місцеположення зростає зі збільшенням відстані між пунктами прийому. Найбільш висока точність оцінки координат забезпечується в тому випадку, якщо лінії положення перетинаються під кутами, близькими до 90 градусів [74]. Навіть в цьому випадку, результатом буде не точка, а область перетину (рис. 3.3).

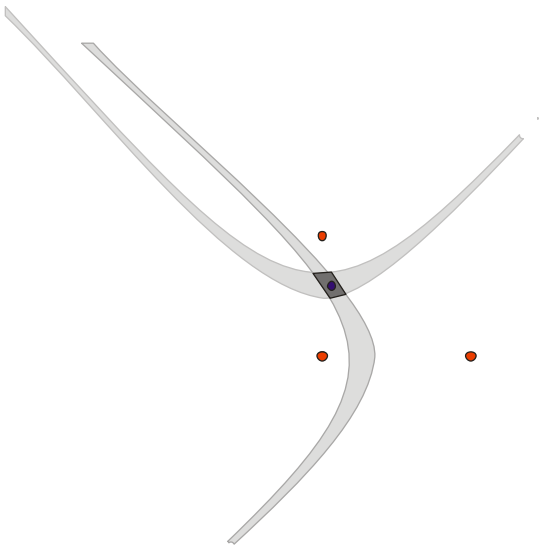


Рисунок 3.3 – Похибка різницево-далекомірного методу

Основна складність реалізації даного методу полягає в необхідності високоточної синхронізації.

Часто автори використовують кілька методів одночасно, як в [75] розглядають знаходження місцеположення мобільного телефону комбінуванням

двох методів AoA і TDoA. В останньому вимірюється час поширення від передавача до приймача і назад по годинниках передавача, тобто не потрібно синхронізації годинників. Недоліком даного методу є необхідність застосування додаткового обладнання та його висока вартість.

3.2.4. Метод RSSI

Одним з найпоширеніших методів позиціонування в Wi-Fi мережі є метод RSSI (Received Strength Signal Indication), описаний в [67, 68] та багатьох інших джерелах, оснований на оцінці відстані між мобільним об'єктом і точкою доступу по потужності сигналу.

$$RSSI_d = RSSI_d - 10Lg\left(\frac{d}{d_o}\right), \tag{3.1}$$

де $RSSI_0$ – потужність сигналу на відстані d, d_0 – калібрована відстань, $RSSI_d$ – потужність сигналу в дБм на калібрувальної відстані, n – коефіцієнт втрат при поширенні сигналу.

Потужність прийнятого радіосигналу зменшується зі збільшенням відстані, і приймач може виміряти це затухання на основі RSSI для того, щоб оцінити відстань до відправника. RSSI вимірює потужність сигналу на приймачі. Таким чином значення RSSI може бути переведене в оцінку відстані.

Проте цьому методу притаманний ряд суттєвих обмежень, оскільки рівень сигналу є досить мінливим параметром через вплив наступних факторів:

– швидкі та повільні завмирання сигналів на трасі через зміну умов поширення радіохвиль;

– багатопроменеве поширення внаслідок відбиття від різних предметів;

– великий діапазон вихідної потужності передавачів та чутливості приймачів;

– вплив орієнтації антен через нерівномірність діаграми спрямованості.

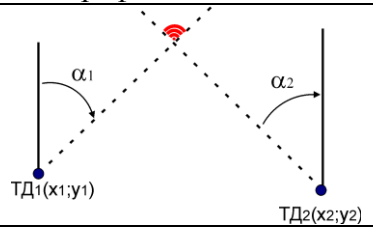
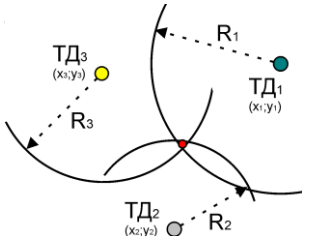
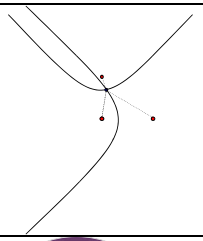
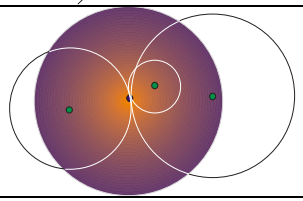
Через вплив зазначених факторів реальна залежність потужності від відстані виявляється нелінійної і непостійною в часі, внаслідок чого точність вимірювань швидко падає з ростом відстані.

3.2.5 Вибір методу для визначення місцеположення абонента в мережі

Результати аналізу методів визначення місцеположення абонента наведені в табл. 3.1. З її розгляду можна зробити висновок, що для застосування в бездротових Wi-Fi мережах найбільш придатний є метод оцінки потужності сигналів опорних вузлів. На користь використання методу RSSI також те, що при передачі даних в Wi-Fi мережах паралельно передається інформація про рівень сигналу. Технічна реалізація методу RSSI має економічні переваги по відношенню до решти розглянутих варіантів виявлення місцеположення об'єктів у бездротових мережах передачі даних.

У порівнянні з іншими, він показує високу точність позиціонування об'єктів в бездротових мережах передачі даних. Цього методу немає серед «класичних» методів позиціонування, але для Wi-Fi мереж, розгорнутих на обмеженій території, він виявляється найбільш простим та ефективним.

Таблица 3.1

Метод	Необхідне обладнання/інформація	Недоліки	Графічне подання	Переваги
AoA (кутомірний)	Як мінімум два вимірювальних пункти з гостроспрямованими поворотними антенами або ФАР	Низька точність позиціонування всередині приміщення через вплив перевідбитків, складна антенна система		Потенційно висока точність позиціонування на відкритому просторі
ToA (далекомірний)	Як мінімум три вимірювальних пункти, працюючих в режимі прийому і передачі з можливість підключення абонента до кожного з них. Потрібна інформація про затримку в абонентських пристроях.	Складність реалізації спільної роботи з трьома пунктами одночасно, вплив невідомої затримки в абонентському пристрої		Ніяких спрямованих антен або іншого складного обладнання не потрібно, всі необхідні вимірювання можна зробити програмним забезпеченням
TDoA (різницево-далекомірний)	Як мінімум три вимірювальних пункти з можливість прийому сигналу в кожному з них. Потрібна точна синхронізація годинників в усіх приймальних пунктах.	Складність обладнання, складність вимірювання і обробки.		Стійкий до перешкод, викликаних повторним впливом вимірюваль-них акустичних імпу-льсів від навколишніх об'єктів
RSSI (за рівнем потужності)	Кілька приймальних пунктів (чим більше, тим краще). Необхідна модель поширення радіохвиль	Вплив геометричної орієнтації абонентського пристрою		Висока точність в приміщенні, не вимагає додаткових витрат

3.3 Особливості реалізації методу RSSI в Wi-Fi мережах

Ослаблення потужності електромагнітного поля у вільному просторі, як відомо, описується виразом Фріїса [76]:

$$\frac{P_R}{P_T} = G_T G_R \left(\frac{\lambda}{4\pi R}\right)^2, \tag{3.2}$$

де R – відстань в метрах між передавачем і приймальною антеною; P_T – потужність передавача антени на відстані d, в дБМ; P_R – потужність, що приймається антеною в дБм; G_T – коефіцієнт посилення передавальної антени; G_R – коефіцієнт посилення приймальної антени; λ – довжина хвилі в метрах, що відповідає частоті передачі.

З виразу (3.2) виводимо формулу для визначення відстані від об'єкта до точки доступу:

$$R = \frac{\lambda}{4\pi}\sqrt{\frac{P_T G_T G_R}{P_R}}. \tag{3.3}$$

Але Wi-Fi- мережі рідко організовуються на відкритому просторі. Як правило вони використовуються всередині будівель.

Вирішити задачу визначення відстані між приймачем і кожною точкою доступу, використовуючи дані про рівні сигналу, можна за допомогою моделі поширення сигналу всередині будівлі. Існують емпіричні і теоретичні (розрахункові) моделі розповсюдження сигналу.

Серед емпіричних моделей можна виділити 2 групи: статистичні моделі – вимагають тільки загального опису типу будівлі; одно- або багатопроменеві моделі – оцінюють рівень сигналу, що приймається і засновані на врахуванні втрат на всіх перешкодах на шляху проходження сигналу.

Для реалізації даного методу необхідно змоделювати поширення сигналу всередині будівлі. Найчастіше використовують *рекомендовану* Міжнародним союзом електрозв'язку статистичну модель ITUR P1238 [77]. Вона була розроблена для розрахунків всередині будівель та приміщень:

$$L = 20\,log\,f + N\log d + P_f(n) - 28, \tag{3.4}$$

де, d в метрах, f в мегагерц.

N – коефіцієнт втрати потужності сигналу з відстанню.

n – кількість перешкод (стін) між приймачем і передавачем.

Pf (n) – параметр втрати потужності сигналу при проходженні через перешкоди. Визначається емпірично і залежить від кількості пройдених перешкод.

Але поширення радіосигналів всередині будівлі являє собою результат дії механізмів багатопроміневості, заломлення, дифракції та дифузії. В результаті формується складна інтерференційна картина, яка не завжди адекватно описується навіть найдосконалішою моделлю.

Альтернативою математичним алгоритмам поширення сигналу є метод радіовідбитків (Fingerprinting) [78]. Він ґрунтується на побудові радіокарти в приміщенні та має дві стадії реалізації. Перша стадія передбачає збір інформації про RSSI безлічі опорних точок від базових станцій (не менше трьох) і формування бази даних зберігання цих точок, а також план приміщення. Потужність від доступних точок доступу Wi-Fi повинна бути прив'язана до координат приміщення. Друга стадія полягає в постійному моніторингу RSSI обладнання користувачів і порівняння їх з наявною базою даних, для пошуку збігів або найближчого значення.

Даний метод забезпечує високу точність визначення місцеположення за підтримки радіокарти в актуальному стані.

3.4 Експериментальні дослідження з визначення похибки місцеположення абонента в захищеному приміщенні

Для прикладу реалізації методу радіовідбитків розглянемо трикімнатну квартиру панельного будинку площею 70 м² з трьома точками доступу (ТД1, ТД2, ТД3), план приміщення і розміщення точок доступу вказано на рис. 3.4. Так само на плані вказані опорні точки, в яких проводилися вимірювання рівня сигналу.

Точки доступу розміщені по периферії зони покриття, на різних рівнях, що надає хороші дані про пристрої, які в іншому випадку виглядали б рівновіддаленими з усіх інших точок доступу. Зроблено радіообстеження приміщення з метою розподілу каналів і регулювання потужності в діапазоні по точках доступу.

Виходячи з отриманих даних, можна зробити висновок, що трьох точок доступу достатньо для площі до 100 м². У разі використання більшої кількості точок, обладнання буде заважати роботі один одного (що пов'язано з особливістю технології Wi-Fi), а використання меншої кількості призведе до зниження точності визначення місцеположення.

Для експерименту використовувалися три однакових маршрутизатора Asus RT-N10E Wireless N Router з технічними параметрами: робоча частота – 2,412 ГГц; посилення антени – 2 дБі; потужність передавача – 19 дБм. Смартфон Lenovo S898t+. В ході експерименту з'ясувалося, що в залежності від орієнтації мобільного пристрою (фактично, його антени) вимірювана потужність змінюється, тому радіокарти складалися виходячи з середньої потужності на висоті 1 метр, протягом 60 секунд для шести різних положень мобільного пристрою (по вертикалі – положення вгору і вниз; по горизонталі – 0º, 90º, 180º, 270º), що показано на малюнку 4, по 10 секунд в кожному з них. Результати експерименту наведені в табл. 3.2.

Рисунок 3.4 – Положення смартфону по відношенню до роутеру:
а – вверх; *б* – вниз; *в* – 0º; *г* – 180º; д – 90º; *е* – 270º

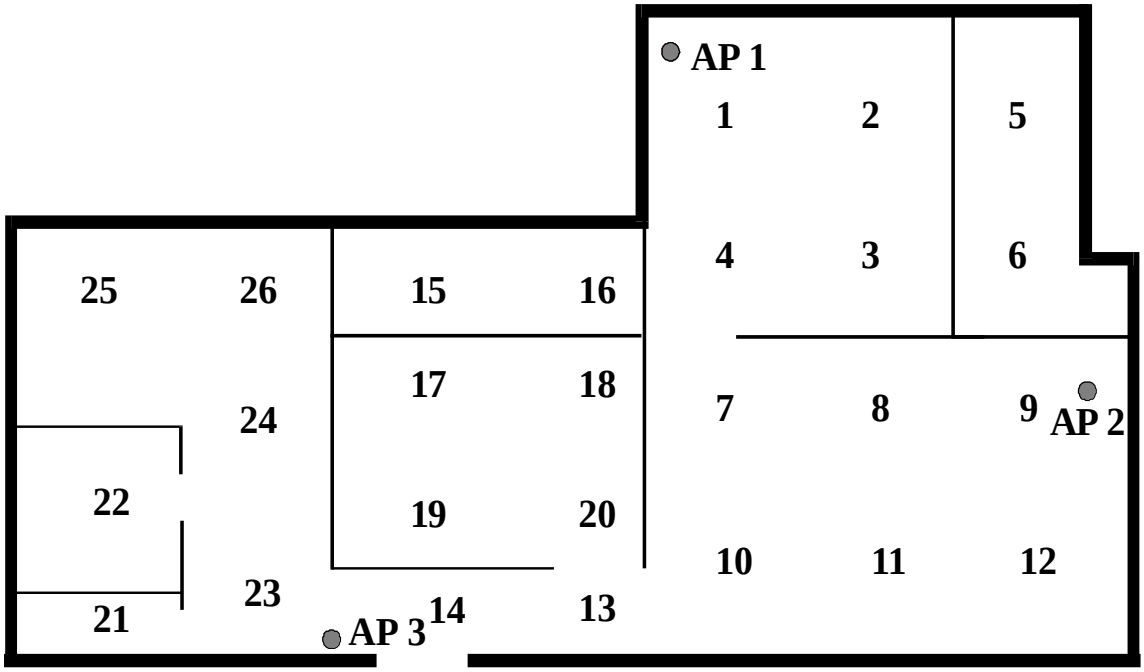


Рисунок 3.5 – План приміщення з розміщенням опорних точок та точок доступу

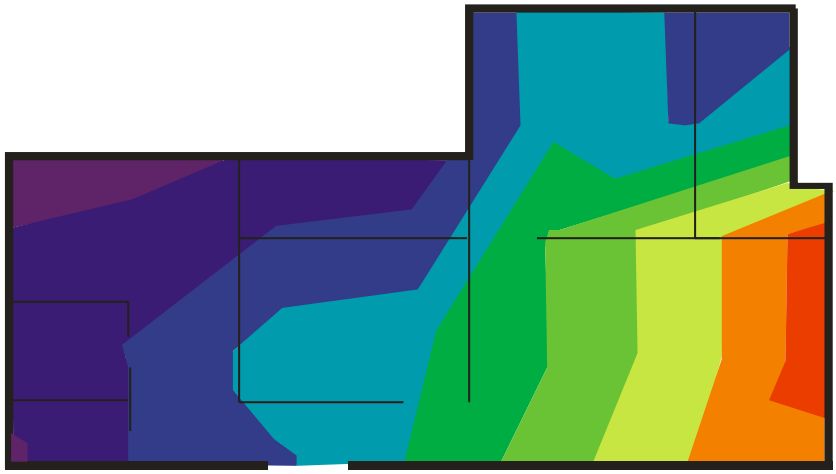
Таблиця 3.2

№ точки	TD1, середній рівень RSSI, дБм		TD2, середній рівень RSSI, дБм		TD3, середній рівень RSSI, дБм	
	Вікна/двері зачинені	Вікна/двері відкриті	Вікна/двері зачинені	Вікна/двері відкриті	Вікна/двері зачинені	Вікна/двері відкриті
1	–36,9	–36,1	–60,3	–62,1	–71,5	–69,0
2	–43,0	–44,0	–61,0	–62,4	–68,4	–67,4
3	–42,0	–43,7	–65,7	–64,1	–72,4	–72,5
4	–43,0	–44,6	–61,4	–58,0	–64,5	–64,9

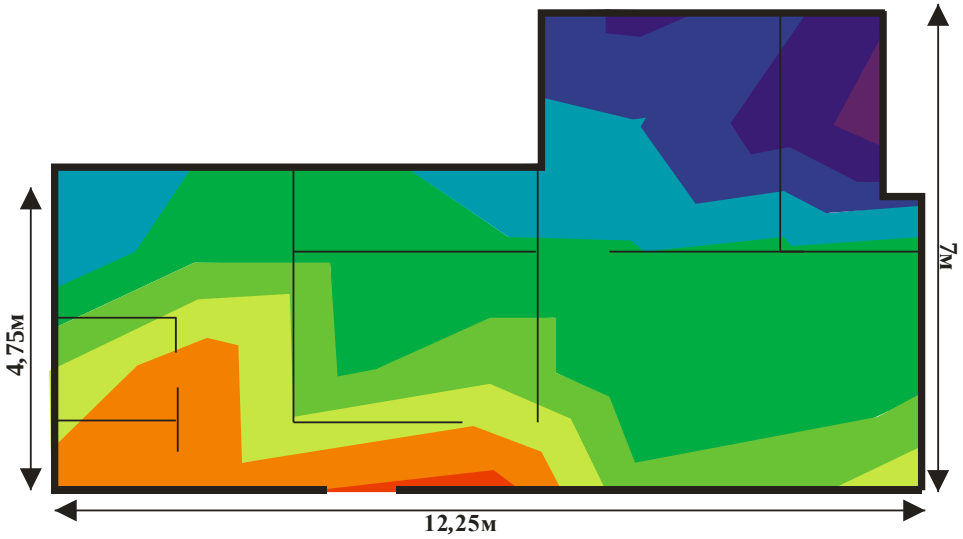
№ точки	TD1, середній рівень RSSI, дБм		TD2, середній рівень RSSI, дБм		TD3, середній рівень RSSI, дБм	
	Вікна/двері зачинені	Вікна/двері відкриті	Вікна/двері зачинені	Вікна/двері відкриті	Вікна/двері зачинені	Вікна/двері відкриті
5	–53,5	–52,2	–65,8	–65,1	–76,0	–75,0
6	–49,2	–48,6	–59,3	–58,4	–79,1	–74,9
7	–54,0	–53,4	–54,7	–54,4	–59,5	–57,4
8	–58,0	–59,4	–47,4	–46,3	–58,4	–48,7
9	–69,8	–67,8	–36,8	–35,3	–57,0	–54,5
10	–61,0	–59,0	–52,0	–53,6	–53,4	–43,1
11	–63,0	–64,2	–44,7	–43,0	–52,2	–51,8
12	–59,2	–61,1	–41,5	–39,6	–45,1	–52,3
13	–68,2	–66,3	–59,2	–58,1	–37,7	–40,4
14	–78,4	–77,5	–65,6	–64,2	–38,8	–37,5
15	–67,4	–68,9	–75,9	–76,0	–60,3	–63,3
16	–59,9	–60,1	–76,2	–77,9	–62,5	–63,7
17	–66,4	–66,5	–69,7	–69,0	–56,5	–56,2
18	–68,2	–66,7	–68,5	–67,2	–59,3	–62,6
19	–74,0	–73,0	–62,7	–63,1	–55,8	–53,2
20	–70,2	–69,8	–60,8	–60,6	–51,4	–52,5
21	–81,8	–78,3	–75,9	–74,4	–42,1	–41,7
22	–78,2	–78,4	–73,6	–74,0	–49,2	–46,7
23	–78,4	–81,1	–69,4	–68,6	–40,8	–38,5
24	–75,2	–73,5	–73,1	–74,1	–56,0	–56,2
25	–78,9	–79,9	–74,7	–77,0	–61,9	–60,6
26	–75,8	–76,3	–78,0	–76,3	–61,0	–60,6

На рис. 3.6 наведено графічне представлення експериментальних вимірювань поширення Wi-Fi сигналу, що доводить правильність розміщення бездротового обладнання. Рівні сигналу в одній і тій же опорній точці від трьох точок доступу значно відрізняються.

а)



б)



в)

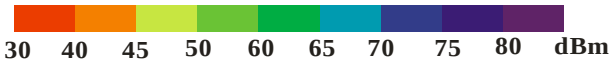


Рисунок 3.6 – Карта поширення сигналу: *а*– ТД1; *б*– ТД2; *в*– ТД3

Виходячи з даних табл. 3.2, можна зробити висновок, що рівень сигналу практично не залежить від положення дверей і вікон, що знаходяться в приміщенні (похибка становить 1 – 2 дБ). У процесі формування карти радіовідбитків в різних положеннях результати відрізнялися від 3 дБ до 10 дБ. Максимальне відхилення фіксоване тільки в п'ятьох точках, в інших опорних точка різниця в вимірюваних рівнях сигналу не перевищувала 5 дБ. Як бачимо з рис. 3.6, похибка в визначенні потужності в 5 дБ еквівалентна похибці у визначенні місцеположення в $\pm$ 2,5 м при застосуванні детермінованого (евклідова відстань) підходу визначення координат. Точність об'єкта визначення місцеположення за допомогою радіокарти можна порівняти з ринковими системами позиціонування. Для підвищення точності результатів кількість опорних точок можна збільшити.

Визначення місцеположення за межами території, що охороняється також можливо. Для цього потрібно попередньо заміряти рівні сигналу на цій території і включити її в карту радіовідбитків. Якщо з якихось причин це зробити неможливо (наприклад, там «чужа» територія, що охороняється), оцінку рівня сигналу можна виконати розрахунковим шляхом, використовуючи наявні дані і вирази (3.4).

Визначити місцеположення абонента за межами території, що охороняється можливо також за допомогою методів латерації. Цей метод не дасть точних результатів, але, якщо абонент потрапляє в радіус дії хоча б однієї або двох точок доступу, можна визначити радіус його знаходження і напрямок.

3.5 Прийняття рішень про аномальний стан бездротової мережі з урахуванням місцеположення абонента

Само по собі місцеположення пристроїв не є інформативним – крім як знання координат користувачів мережі, більше ні про що не говорить. Якщо цю ознаку використовувати спільно з системою захисту, такою як системи ви-

явлення вторгнень або системи запобігання вторгнень, описаними в п. п. 1.3.3-1.4 даної роботи, це дозволить істотно розширити можливості таких систем і дозволить здійснювати наступні заходи щодо забезпечення безпеки бездротових мереж.

1. Здійснювати контроль доступу. Місцеположення, наприклад з системою виявлення вторгнень, дозволить обмежити з'єднання до мережі тільки межами фізичного периметра, блокувавши спроби підключення з територій, що знаходяться за межами фізичного периметра, навіть якщо підключається цілком легальний клієнт.

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 (наприклад, крадіжки).

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

За підсумками матеріалів розглянутих в пункті 1.2, можна зробити висновок, що при забезпеченні захисту бездротової мережі Wi-Fi особливо варто виділити наступні атаки: прослуховування, DoS атака, глушіння, вторгнення та модифікація даних, атака «man in the middle», абонент-шахрай та помилкова (фальшива) точка доступу (рис. 3.7 [12]).

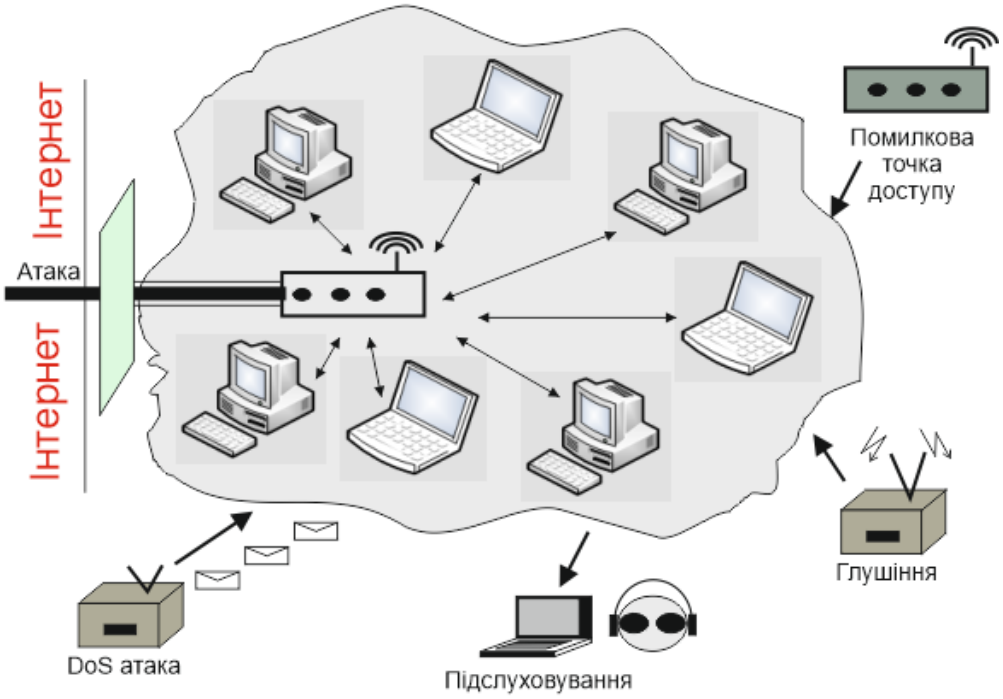


Рисунок 3.7– Атаки на бездротову мережу

Далі в табличній формі (таблиця. 3.3) [3] наведені ці загрози з коротким їх описом та поданням про можливість їх виявлення і блокування при наявності можливості моніторингу місця розташування користувачів мережі на базі інших систем захисту, таких як системи виявлення або запобігання вторгнень.

Таблиця 3.3

Вид атаки	**Що потрібно для здійснення атаки**	**Характерні ознаки ідентифікації атаки**	**Опис дій зловмисника**	**Що дозволяє місцезнаходження**
Прослуховування	Приймач розташований поблизу передавача	Ідентифікувати практично неможливо	Перехоплення радіосигналу і (при необхідності) дешифрування даних, що передаються	Не впливає
DoS атака (Denial of Service - відмова в обслуговуванні)	Створюється пристрій, який заповнює весь спектр на частоті 2.4 ГГц перешкодами і нелегальним трафіком	Відбуваються регулярні помилки при отриманні пакетів даних, іноді - неможливість підключитися	Точка доступу перевантажується багатьма безглуздими пакетами, внаслідок чого обслуговування мережі, практично, припиняється	Не впливає

Вид атаки	Що потрібно для здійснення атаки	Характерні ознаки ідентифікації атаки	Опис дій зловмисника	Що дозволяє місцезнаходження
Глушіння	Пристрій для постановки перешкод у всьому спектрі частот, даної бездротової мережі	до мережі	Генерується радіошум на частоті роботи бездротової мережі. Розрізняють глушіння клієнтів і глушіння базової станції	Дозволяє визначити джерело зловмисних дій, якщо він знаходиться в радіусі дії мережі
Вторгнення і модифікація даних	Знання протоколу і параметрів мережі, володіння приймачем, розташованим в радіусі дії мережі	Користувачам відмовлено в доступі до мережі.	Додається інформація до існуючого потоку даних. Можливо втручання на рівні пакетів (модифікація даних користувачів), або на рівні керівників команд, (аж до від'єднання користувачів від мережі)	Не впливає
Атака «man in the middle»	Зловмиснику потрібно детальна інформація про мережу	Наприклад, виявлення точки доступу з SSID корпоративної мережі, але відсутня у списку легальних пристроїв, може бути ознакою такої атаки	Може використовувати всі перераховані атаки	Сприяє виявленню атаки і подальшого її блокування
Абонент-шахрай	Знання протоколу і параметрів мережі		Імітація клієнтського профілю абонента для отримання доступу до мережі від його імені. (Може здійснюватися шляхом викрадення абонентського пристрою)	За нетипового знаходженню користувача атака виявляється і блокується
Помилкова (фальшива) точка доступу	Знання протоколу і параметрів мережі, власна точка доступу з імітацією мережевих ресурсів	В радіусі дії даної мережі, з'являється сигнал, від ще однієї точки доступу	Організація фальшивої точки доступу з імітацією мережевих ресурсів для перехоплення, наприклад автентифікаційної інформації абонентів	Блокуються всі точки доступу, що знаходяться не на своєму місці

Розглянемо вплив сервісу позиціонування більш докладно.

Атака «прослуховування» пов'язана з вразливістю самої бездротової мережі, і всі користувачі в зоні дії, здатні прослуховувати ефір. Якщо це робить легальний користувач (співробітник в свій робочий час) то виявити це практично неможливо.

Стандартні заходи безпеки здатні виявити факт вторгнення при атаці "глушіння", але не можуть ідентифікувати джерело атаки. З огляду на той факт, що дана атака відбувається в основному в радіусі дії мережі, що атакується. Знаючи розташування всіх абонентів в короткі терміни, можна виявити джерело зловмисних дій і блокувати його. Так як точки доступу мережі працюють на різних каналах, заглушити всі одночасно, навряд чи вийде, і якась із точок зафіксують нападника, що дозволить виявити його місцеположення. Сама по собі ця атака фактично не використовується, за нею зазвичай слідує атака «помилкова (фальшива) точка доступу» або DoS атака. Тому запобігши, подібного роду атак, можна вберегти мережу від продовження зловмисних дій у вигляді інших атак.

Атака «помилкова (фальшива) точка доступу». Суть цієї атаки зводиться до блокування легальної точки Wi-Fi мережі, щоб перенаправити клієнтів мережі на свою точку доступу. Знаючи точне місцеположення легальної точки доступу, всі інші з такими ж параметрами будуть миттєво блоковані.

Знання місцеположення, при DoS атаці здатне допомогти, тільки в тому випадку якщо атака відбувається всередині мережі. Але практично завжди даний вид атак відбувається віддалено і виявити джерело не є можливим.

Запобігти атаку «вторгнення і модифікація даних» місцеположення допоможе, тільки в тому випадку, якщо атакуючий буде «чужий». Коли цю атаку здійснює внутрішній співробітник, на своєму робочому місці, то виявити її не вийде.

У випадку атаки «man in the middle» (В канал зв'язку між роутером і комп'ютером жертви з’являється зловмисник і прослуховує їх, представляючись для кожного співрозмовника іншою стороною) класичні методи не тільки не можуть виявити джерело радіовипромінювання, але і сам факт вторгнення в мережу до того моменту поки зловмисник не переходить до активних дій. Наявність можливості відстеження місцеположення допомагає вирішити про-

блему виявлення даної атаки і дає можливість приймати швидкі заходи по блокуванню.

Атака «абонент-шахрай» свідчить про крадіжку обладнання або його глушіння. В такому випадку атака буде відбуватися в нетиповому даному користувачеві місці. При наявності позиціонування ця атака швидко блокується, шляхом відключення користувача.

При реалізації даних атак завжди використовується обладнання, яке має координати, що кардинально відрізняються від легальних абонентів. Таким чином, врахування місцеположення при захисті бездротових мереж дозволяє виявляти більшу кількість атак на бездротові мережі, ніж без функції виявлення місцеположення.

Результати експериментальних вимірювань RSSI, наведені в табл. 3.2, а карти поширення сигналу, що побудовані за методом радіовідбиткі, наведені на рис. 3.6. Отримані карти говорять про можливість застосування даного методу для знаходження місцеположення всередині приміщення. Данні табл. 3.2 підтверджують, що трьох точок доступу для досліджуваного приміщення є достатнім, щоб визначити місцеположення бездротового пристрою, так як рівні RSSI в одній і тій же точці від трьох різних джерел істотно відрізняються. Тому використовуючи дані методи, можна отримати точність знаходження місцеположення в 2,5 м. без істотних витрат.

Облік розташування в алгоритмах захисту бездротової мережі дозволяє зменшити ризики несанкціонованих дій серед персоналу. Подібна методика наведена в роботі [75], але на відміну від методу TDoA, яку пропонують автори, метод радіовідбитків не вимагає встановлення додаткового обладнання і купівлі дорогих датчиків, а також забезпечує точність позиціонування вище більш ніж в два рази.

Слід зазначити, що дана методика знаходження місцеположення справедлива тільки для класичних пристроїв, які для реалізації своїх цілей не використовують зовнішні спрямовані антени для великих відстаней. Щоб захисти-

тися від подібного роду атак також необхідно використовувати гостронаправлені антени з посиленням на кожній точці доступу. Однак розглянуті методи можна застосовувати, для виявлення місцеположення об'єктів із заздалегідь невідомими параметрами, такими як IP-адреса або MAC-адреса та нетиповим місцеположенням внутрішніх користувачів, що допоможе підвищити рівень захищеності в комплексі з іншими заходами захисту.

Висновки до розділу 3

1. В рамках другого розділу дисертаційної роботи обраний спосіб визначення місцеположення користувачів бездротової Wi-Fi мережі по радіокартам, як ознака для прийняття рішень про аномальний стан мережі.

2. Експериментально показано, що похибки у визначенні місцеположення в умовах закритого приміщення становить 2,5 м при застосуванні детермінінованого (евклідова відстань) підходу визначення координат. У процесі формування карти радіовідбитків в опорних точка різниця в вимірюваних рівнях сигналу не перевищувала 5 дБ для різних положень. Зроблено висновок, що рівень сигналу практично не залежить від положення дверей та вікон, що знаходяться в приміщенні (похибка становить 1-2 дБ). Це дозволяє стверджувати, що запропонований метод ефективно вирішує свою задачу без витрат на дороге обладнання.

3. Виходячи з суті та принципів організації різних видів атак на бездротові мережі, показано, що знання місцеположення абонента, дозволяє, виявляти атаки типу «man in the middle», «абонент-шахрай» і «помилкова (фальшива) точка доступу», а також допомагає визначити місцеположення джерела при атаці «глушіння» що класичні методи захисту не можуть.

РОЗДІЛ 4
ПРАКТИЧНЕ ВИКОРИСТАННЯ ЗАПРОПОНОВАНИХ МЕТОДІВ

У заключному розділі показано, наскільки ефективний запропонований метод порівняння спектра при наявності шуму, а також висловлені рекомендації щодо практичного використання запропонованих методів.

Матеріали розділу частково викладені в [1, 2, 8-11].

4.1 Моделювання різних умов прийому

У попередніх розділах запропоновані два нових методи ідентифікації абонентського обладнання. Основна частина роботи була проведена експериментально, але при великому відношенні сигнал/шум. При практичній реалізації запропонованих методів доведеться мати справу зі значно гіршими умовами прийому. Для перевірки того, наскільки вплине шум на можливість ідентифікації по спектру, було вирішено застосувати моделювання.

Це вимушений крок, оскільки проводити експериментальні дослідження при значній відстані приймача від передавального пристрою наявна вимірювальна апаратура не дозволяла. Крім того, вимірювання в діючій мережі повинні виконуватися з урахуванням часового поділу абонентів. Але, з іншого боку, моделювання дозволило оцінити ймовірні характеристики запропонованого методу в самих різних умовах, що для реального експерименту було б важко.

В рамках роботи була створена математична модель шуму та імітації його додавання з експериментально отриманими спектрами.

4.1.1 Модель шуму

Як відомо, тепловий шум в часовій області являє собою нормальний випадковий процес, який складається з корисним сигналом. Але в нашому випа-

дку ми маємо справу з сигналом в спектральній області. Відновлення його в часовій області неможливо, так як спектр енергетичний, інформації про фазовий спектр немає. Тому додавання сигналу та шуму доведеться здійснювати в частотної області.

Розглянемо шум в кожній частотній смузі спектраналізатору як вузькосмуговий випадковий процес. Згідно [79], закон розподілу інтенсивності шуму в частотній області описується законом Релея:

$$p(A) = \frac{A}{\sigma_A^2} \exp\left(-\frac{A^2}{2\sigma_A^2} \right), \tag{4.1}$$

а початкова фаза кожної його складової розподілена рівномірно в діапазоні:

$$0 \le \varphi < 2\pi . \tag{4.2}$$

Згідно [80], спектральна щільність теплового шуму становить -174 дБм/Гц, а інтенсивність інших шумів в діапазоні 2,4 ГГц (атмосферних, промислових) становить -20 дБм від рівня теплового шуму. Це дозволить нам в першому наближенні знехтувати цими шумами. В даному частотному діапазоні більший вплив можуть надавати завади від сусідніх Wi-Fi та інших пристроїв, але їх аналіз виходить за межі нашої роботи.

Смуга частот смугового фільтра, що входить до складу аналізатора спектра становить 2 кГц. Отже, потужність теплового шуму в цій смузі складе -141 дБм.

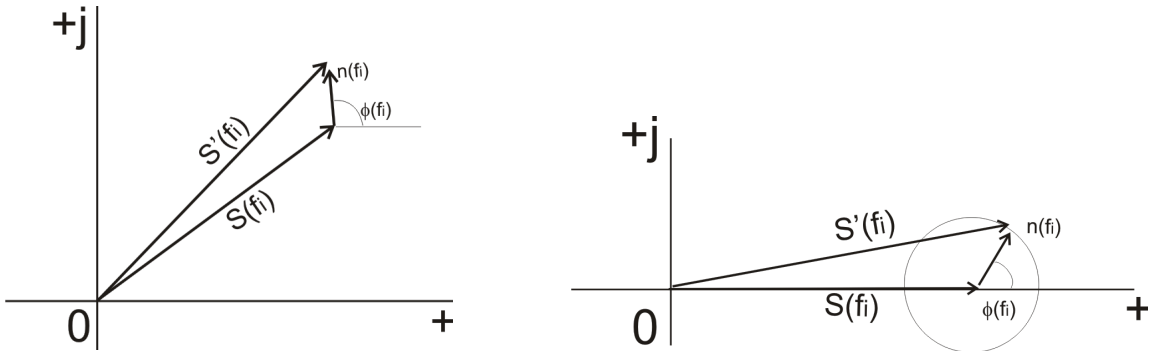
При створенні моделі виходили з того, що в кожній частотній полосі при векторному додаванні с сигнальної $\overrightarrow{S(fi)}$ та шумової $\overrightarrow{n(fi)}$ складових (рис. 4.1, а):

$$\overrightarrow{S'(f_i)} = \overrightarrow{KS(f_i)} + \overrightarrow{n(f_i)}, \tag{4.3}$$

де К – коефіцієнт, що визначає співвідношення сигнал/шум. При складанні може відбуватися як збільшення модуля (потужності) спектральної вибірки, так і її зменшення, що цілком природно.

Значення фази сигналу при моделюванні невідомо і приймається рівним нулю (рис. 4.2 б). Тоді значення модуля знаходимо як:

$$\left|S'(f_i)\right| = \sqrt{\left(KS(f_i) + n(f_i)\cos(\phi(f_i))\right)^2 + \left(n(f_i)\sin(\phi(f_i))\right)^2} \tag{4.4}$$



а) б)

Рисунок 4.1 – До розрахунку суми сигналу та шуму в частотній області

4.1.2 Процедура моделювання

Для порівняння можливості ідентифікації пристрою по його спектру проводиться імітаційне моделювання. Порядок дій при моделюванні графічно наведений на рис. 4.2 за аналогією зі структурою програми, що реалізує модель.

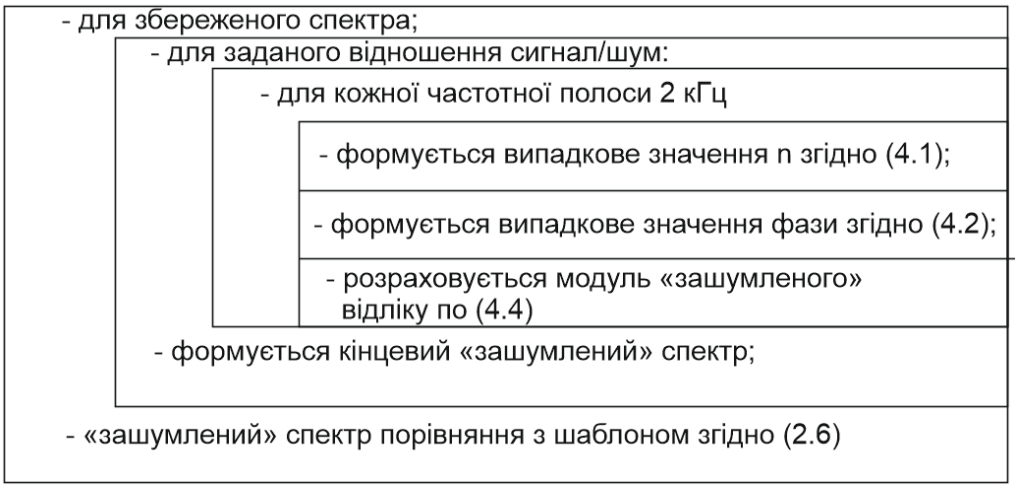
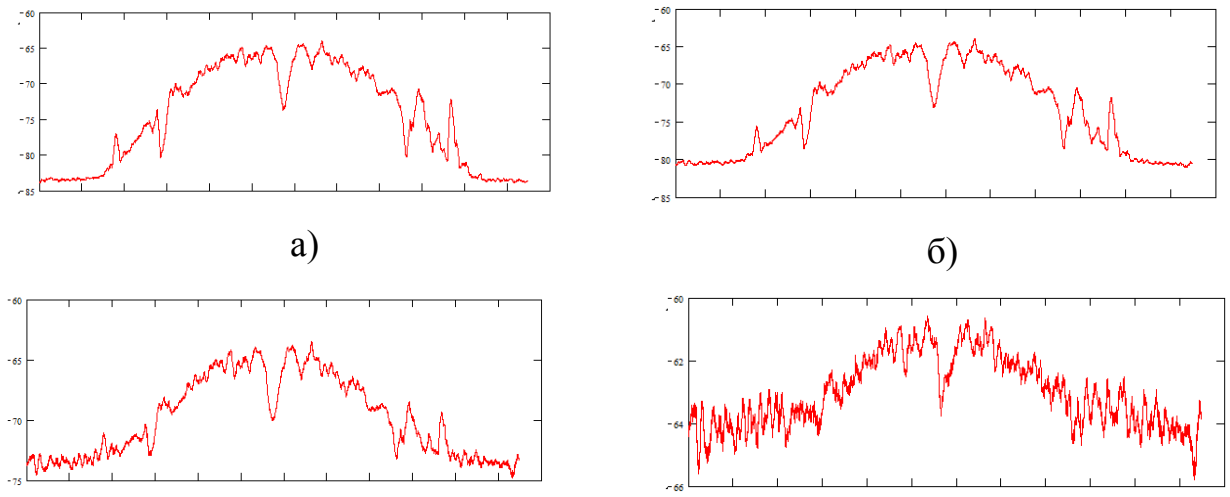


Рисунок 4.2 – Порядок дій при імітаційному моделюванні

На рисунку 4.3 наведені експериментально отримані спектри для одного з аналізованих Wi-Fi пристроїв, до якого додано змодельований шум. Результати показані при різних відношеннях сигнал/шум.



а) б)

в) г)

Рисунок 4.3 – Спектри сигналів при відношенні сигнал/шум
а) 60 дБ (шаблон), б) 40 дБ, в) 20 дБ, г) 10 дБ.

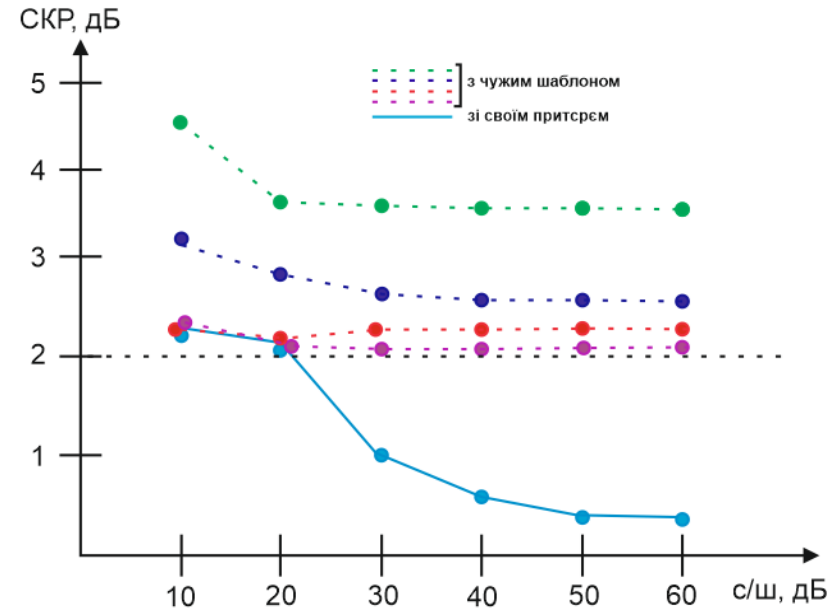
Кілька слів про абсолютні значеннях виміряних та модульованих рівнях сигналу та шуму.

При вимірюванні спектрів в п. 2, рівень сигналу на відстані 0,5 м від джерела становив ~ -60 дБм в смузі 2 кГц, що відповідає -20 дБм в смузі частот 20 МГц. За даними [81] прийом Wi-Fi сигналу може здійснюватися при потужності сигналу до -75 дБм, що відповідає результатам вимірювань в п. 3 (-70 ... -43 дБм). Якщо спектральна щільність шуму -174 дБм/Гц, то в смузі Wi-Fi каналу шириною 22 МГц його потужність складе ~ -100 дБм. Це означає, що граничне відношення сигнал/шум, при якому можлива підтримка зв'язку, становить ~ 25 дБ.

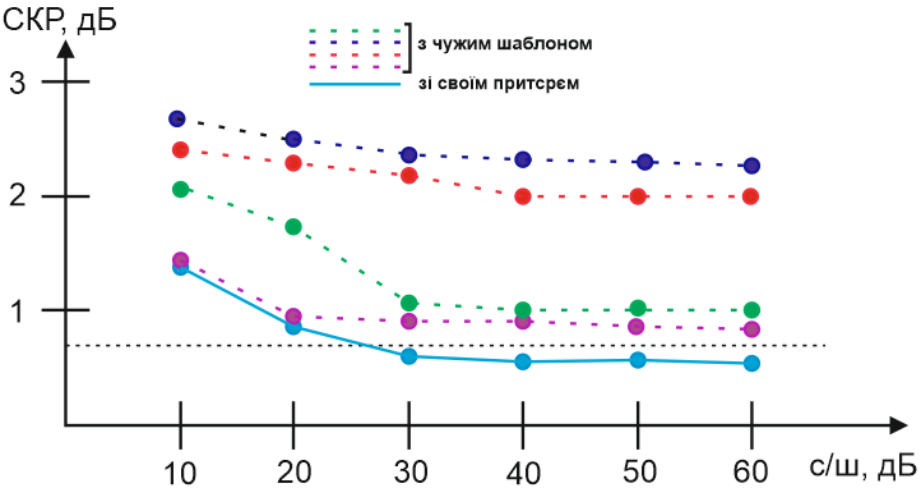
В процесі моделювання було встановлено, що використовувати всю смугу частот 22 МГц при наявності шуму недоцільно. Слабка спектральна потужність на краях смуги піддається впливу шуму в значно більшій мірі, ніж середня частина, що знаходиться в межах +/- 6 МГц від центральної частоти. Саме ця ділянка спектру і використовувалась надалі для аналізу. Більш широку смугу можна використовувати лише при відношенні сигнал/шум > 40 дБ.

4.2 Результати моделювання та їх аналіз для СКР

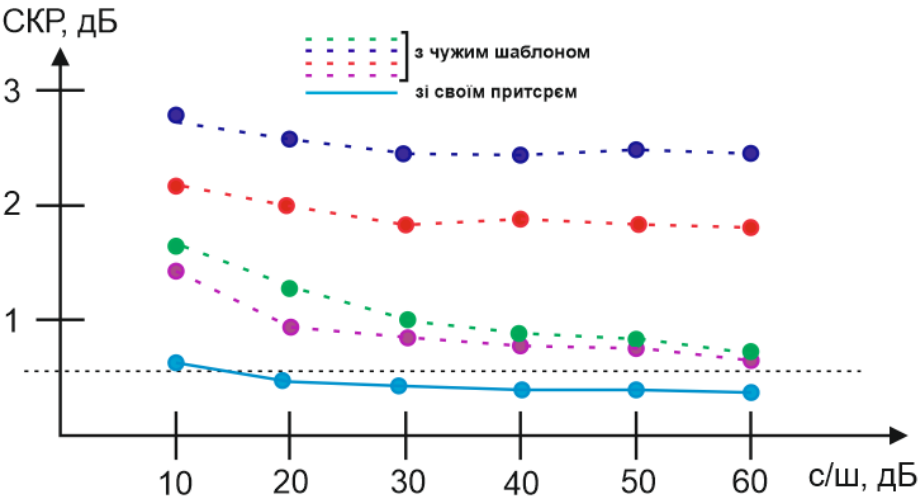
Наведений на рис. 4.2 алгоритм в процесі моделювання застосовувався неодноразово до різних пар спектрів, які були отримані в ході попередніх вимірювань. Для більшості значень було виконано по 1000 операцій додавання випадкового шуму. Результати наведені рис.4.4.



а)



б)



в)

Рисунок 4.4 – Залежність СКР різних спектрів від відношення сигнал/шум: а) по відношенню до шаблону Г; б) по відношенню до шаблону А; в) по відношенню до шаблону В

Синьою лінією на графіках (пряма лінія) наведені залежності СКР від відношення сигнал/шум для шаблону та його пристрою. Іншими кольорами (пунктиром) позначено пристрої, які не належать даному шаблоном.

З графіків можна зробити наступні висновки:

1) середній квадрат різниці значень спектральних відліків для «свого» пристрою і шаблону залишається мінімальним при будь-якому відношенні сигнал/шум;

2) по мірі зменшення відношення сигнал/шум абсолютне значення СКР росте. Це цілком закономірно, тому що чим більше шум, тим в меншій мірі зашумлений спектр залишається схожим на своє шаблонне значення;

3) по мірі зменшення відношення сигнал/шум, відмінності між різними СКР зменшуються, що теж цілком закономірно, тому що чим більше шум, тим в більшій мірі згладжуються відмінності між спектрами, «стираються» їх індивідуальні особливості.

Наведені графіки дозволяють оцінити значення порога на рівні 0,6 ... 2 дБ, але не дають можливість зробити висновок про ймовірність помилкової тривоги або правильного виявлення.

Графічним представленням розрізнення результатів при малих відношеннях сигнал/шум можуть служити гістограми, показані на рис. 4.5. Вони отримані в ході багаторазової імітації різних шумових реалізацій і при різних варіантах повороту порівнюваного пристрою.

На рисунках по горизонталі значення СКР, отримане за результатами моделювання, а висота кожного стовпчика гістограми відповідає кількості значень СКР, що опинилися в заданому діапазоні. Для кожної з розглянутих пар спектрів розраховувалося по декілька тисяч значень, що дозволяє говорити про деяку статистику.

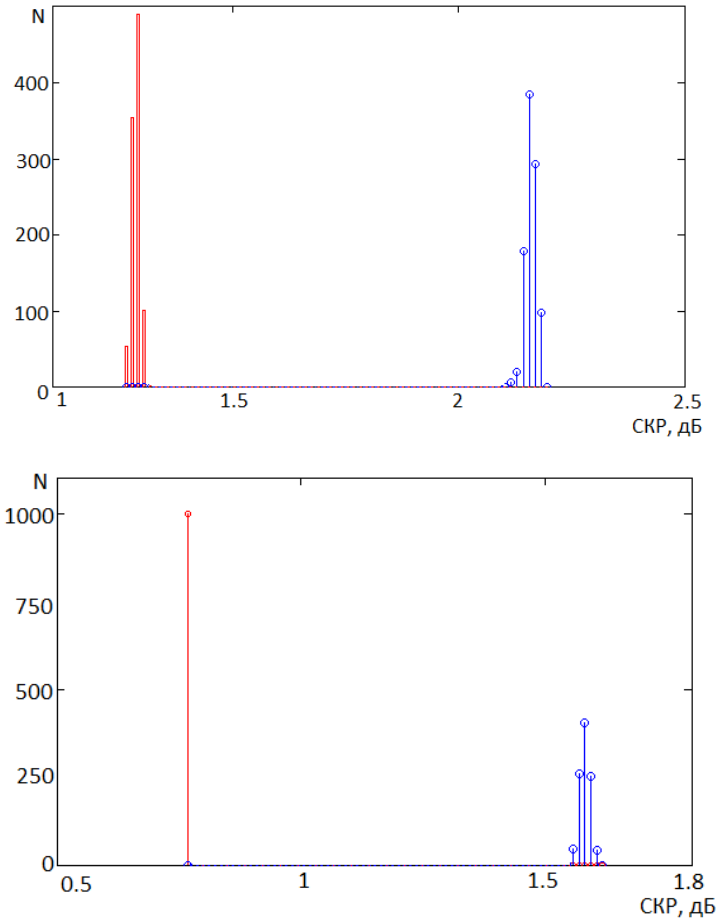
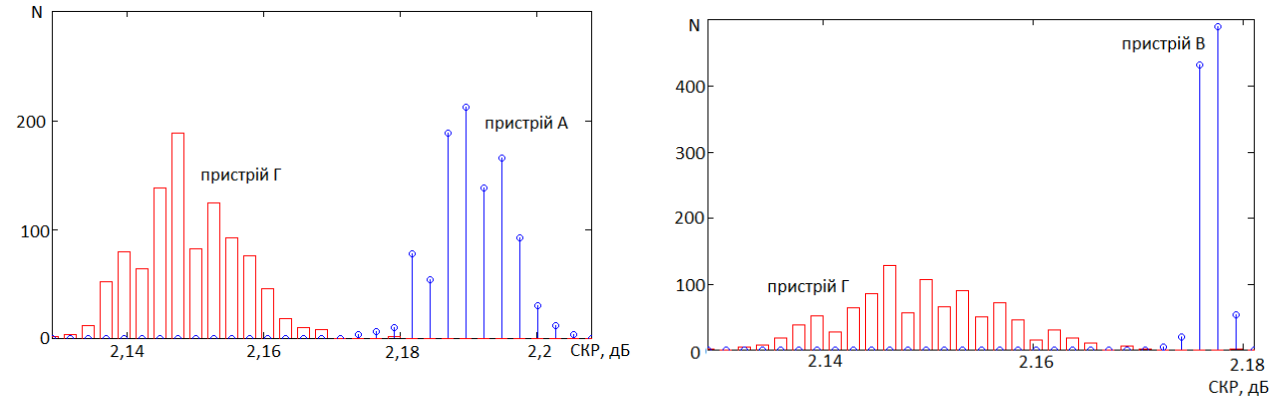


Рисунок 4.5 – Діапазон значень СКР при співвідношенні сигнал/шум 30 дБ для різних пристроїв

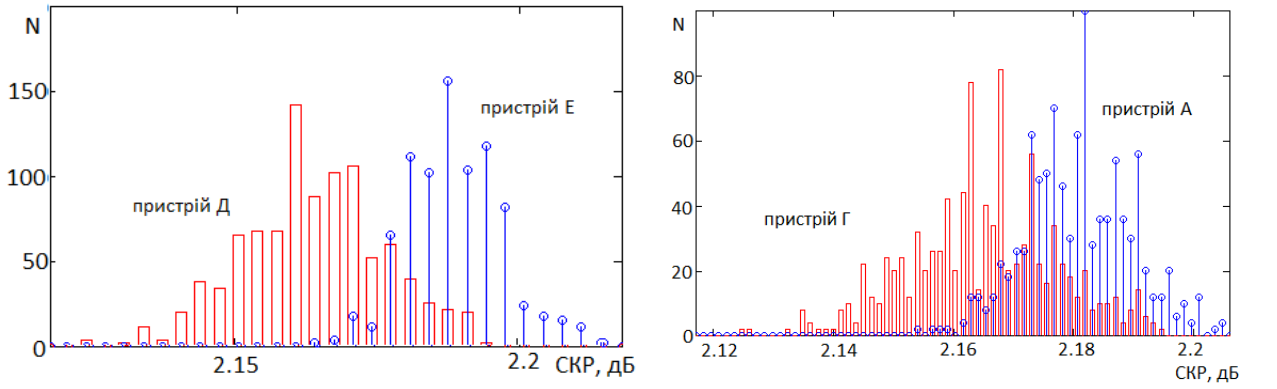
При зменшенні відношення сигнал/шум від 25 дБ і менше, починають виникати помилки. Графічним представленням результатів при великих відношеннях сигнал/шум можуть служити гістограми, показані на рис. 4.6.

Як видно з рисунків, для відношення сигнал/шум краще, ніж 30 дБ питання про відмінність «своїх» і «чужих» спектрів взагалі не виникає. Вони розрізняються однозначно.

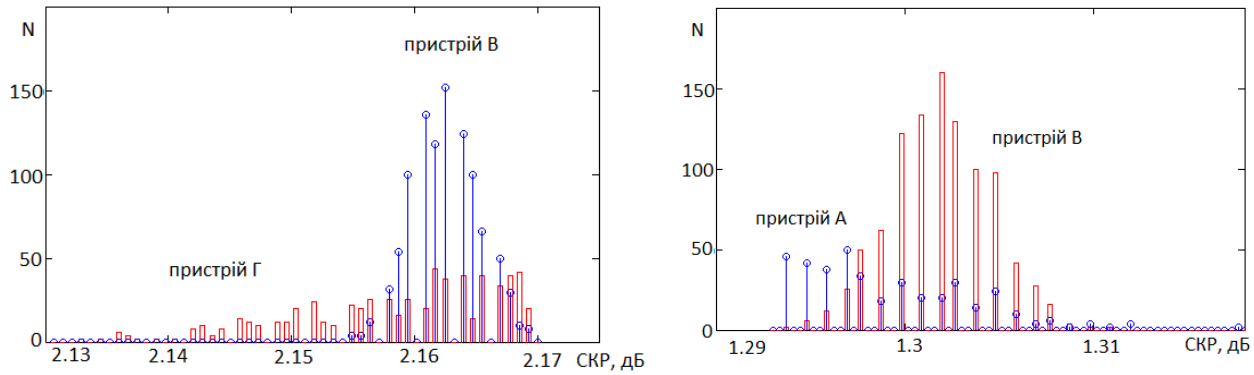
За отриманими даними були побудовані графіки залежностей ймовірності пропуску цілі $P_{пц}$ (помилки першого роду) та хибної тривоги $P_{лт}$ (помилки другого роду), що показано на рис. 4.7



а)

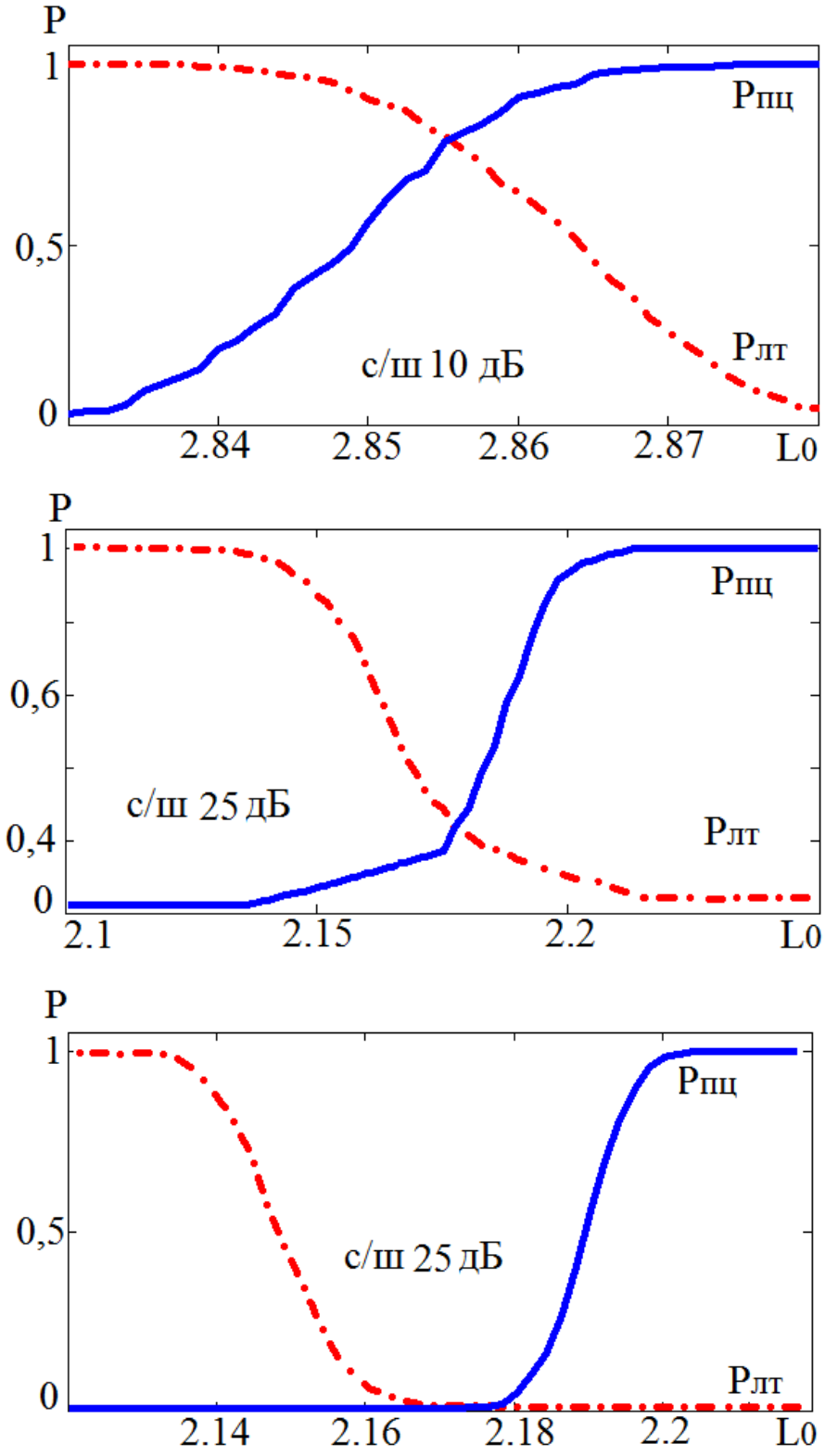


б)



в)

Рисунок 4.6 – Діапазон значень СКР для різних пристроїв: а) при співвідношенні сигнал/шум 25 дБ; б) при співвідношенні сигнал/шум 20 дБ; в) при співвідношенні сигнал/шум 10 дБ;



а)

б)

в)

Рисунок 4.7 – Залежність ймовірності помилкової тривоги і пропуску цілі від установленого порогу для співвідношення сигнал/шум:

а) 10 дБ; б) 20 дБ; в) 25 дБ

4.3 Результати моделювання та їх аналіз для коефіцієнта асиметрії

Для моделювання впливу шуму на результати ідентифікації з використанням коефіцієнта асиметрії використовувався розглянутий раніше алгоритм (рис. 4.2).

Для більшості значень було виконано по 1000 операцій додавання випадкового шуму. Результати розрахунків наведені рис.4.8.

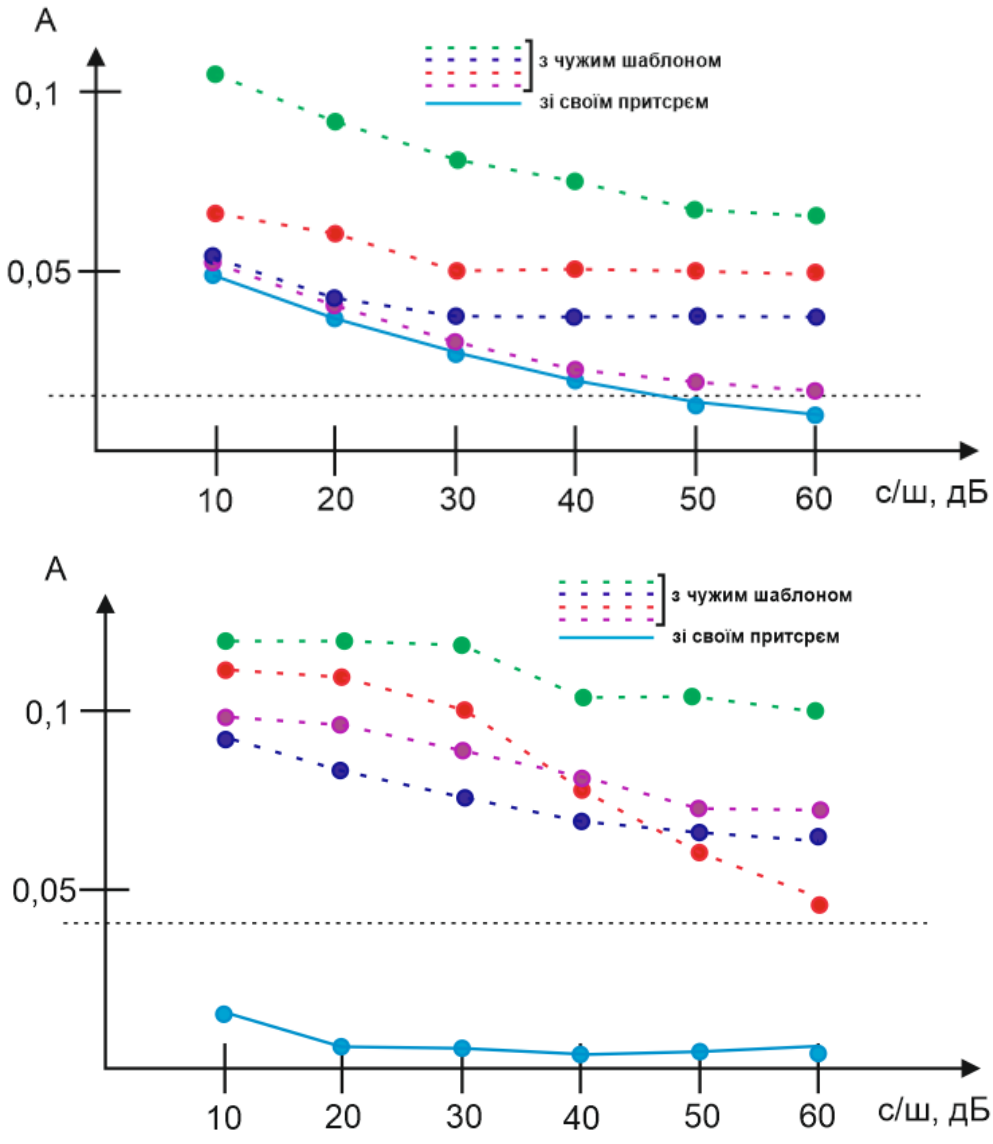


Рисунок 4.8 – Залежність коефіцієнта асиметрії різних спектрів від відношення сигнал/шум: а) по відношенню до шаблону А; б) по відношенню до шаблону Г

З графіків можна зробити наступні висновки:

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

– по мірі зменшення 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 однакових пристроїв починають виникати помилки. Графічним представленням результатів являється гістограма, на рисунку 4.9. Вони отримані в ході багаторазової імітації різних шумових реалізацій і при різних варіантах повороту, пристроїв що порівнюються.

На рисунках по горизонталі значення коефіцієнту асиметрії, отримане за результатами моделювання, а висота кожного стовпчика гістограми відповідає кількості значень коефіцієнтів асиметрії, що опинилися в заданому діапазоні.

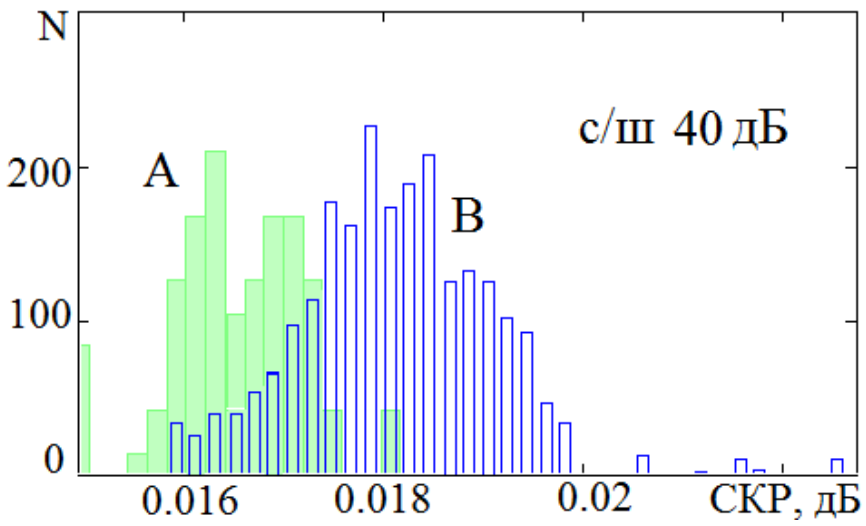


Рисунок 4.9 – Діапазон значень коефіцієнту асиметрії для однакових пристроїв при співвідношенні сигнал/шум 40 дБ

Залежності ймовірності пропуску цілі $P_{ПЦ}$ та помилкової тривоги $P_{ЛТ}$ наведені на рисунку 4.10 для відношення сигнал/шум 40 дБ. Дані залежності зберігаються при відношенні сигнал/шум 30, 20 та 10 дБ.

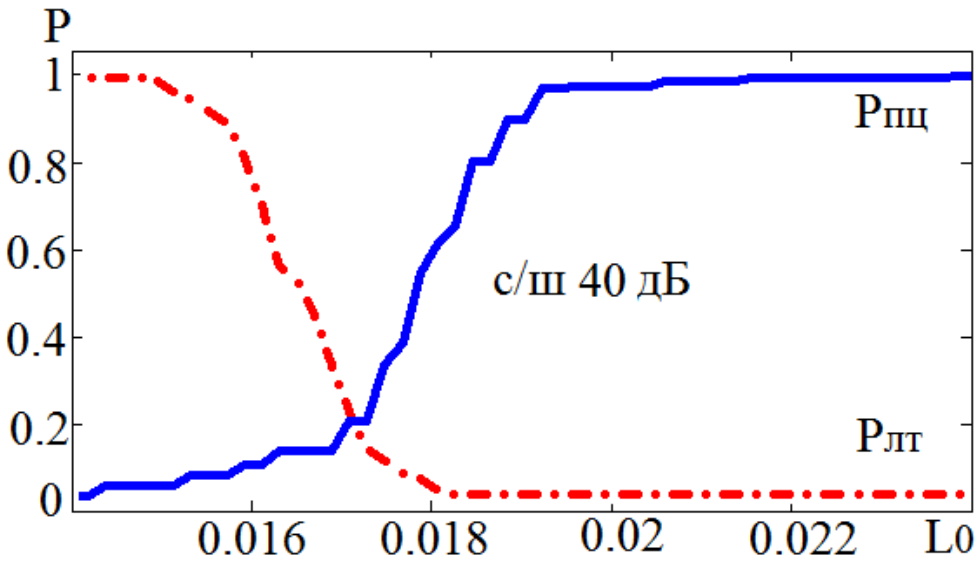


Рисунок 4.10 – Залежність ймовірності помилкової тривоги і пропуску цілі від установленого порогу для співвідношення сигнал/шум 40 дБ для однакових моделей пристрою

4.4 Застосування двох порогів для порівняння спектрів

При малому відношенні сигнал/шум і, особливо при первісній схожості двох спектрів, помилки ідентифікації при чітко встановлених порогах неминучі. Тому варто розглянути принципи роботи СВВ, основані на нечітких ознаках і ввести два пороги. За результатами експериментів, наведених в даному розділі, можна говорити про те, що при відношенні сигнал/шум менше 30 дБ (для методу основаного на розрахунках СКР) або для різних пристроїв однакових моделей (для методу основаного на розрахунках коефіцієнтів асиметрії), утворюються деякі «сірі» зони значень, які не дозволяють однозначно ідентифікувати пристрій (рис.4.11):

$$L_1 < CKP < L_2 \tag{4.5}$$

У цьому випадку доцільне подальше застосування алгоритмів, основаних на нечіткій логіки, які розглянуті в [1, 2, 8-11]. І остаточне рішення буде прийматися СВВ за сукупністю ознак.

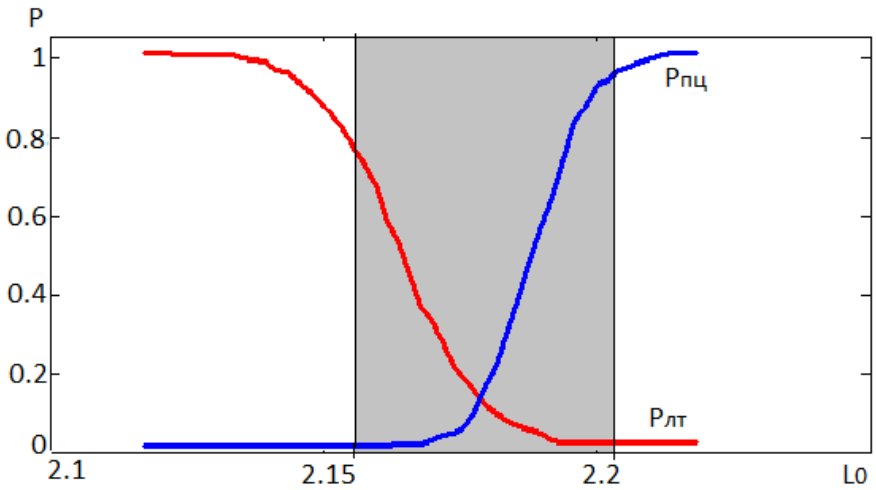


Рисунок 4.11 – До поясненням двох порогів

Суть алгоритму, що включає в себе елементи нечіткої логіки, полягає в тому, що значення одного з ознак порівнюються з базовим значенням, характерним для певного періоду часу. Потім отримані значення виражаються за допомогою лінгвістичних величин нечіткої логіки (висока аномальність мережі, нормальна робота мережі, низька аномальність мережі і т. д.) Аналогічні операції порівняння з базою даних та перетворення в значення нечіткої логіки необхідно виконати для всіх аналізованих ознак, що характеризують роботу бездротової мережі Wi-Fi.

Оцінка параметрів здійснюватися комплексно: як по кожній ознаці окремо, так і по їх сукупності. Для оцінки по сукупності ознак, отримані значення лінгвістичних змінних з урахуванням вагових коефіцієнтів потрібно скласти.

Значно впливають на роботу мережі завади, тому їх також потрібно враховувати при аналізі бездротової мережі. У прийнятті кінцевого рішення враховується база даних по попереднім вторгненням.

Така система може працювати як в автоматичному режимі (сама приймати рішення) так і за допомогою оператора (експерт, проаналізувавши отримані дані, сам приймає рішення).

Структура моделі прийняття рішення про аномальність мережі може мати вигляд, показаний на рисунку 4.12.

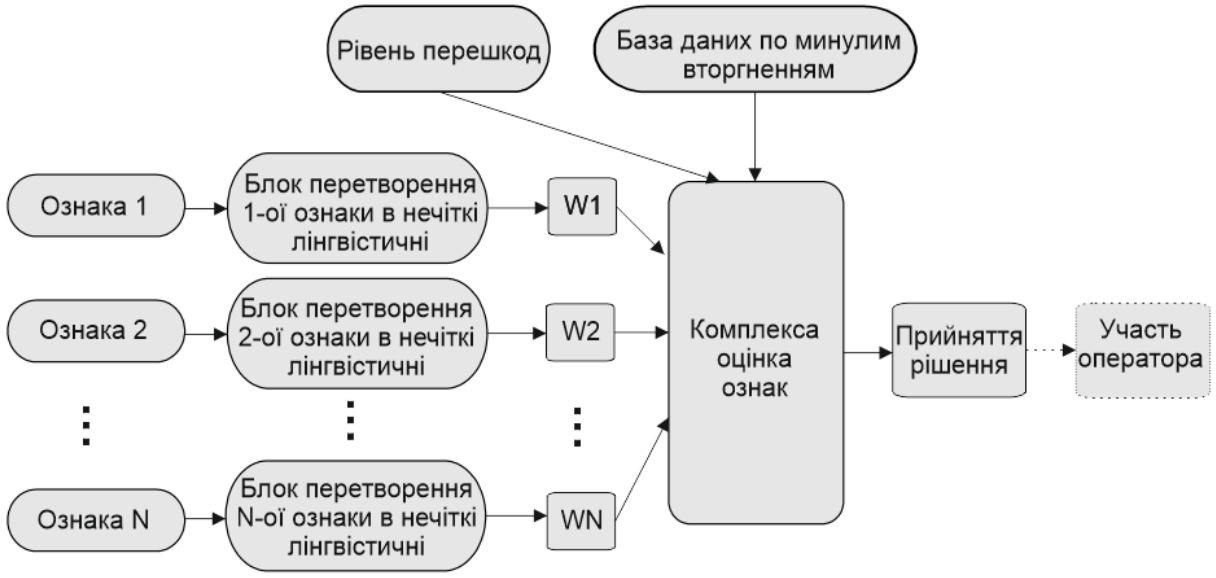


Рисунок 4.12 – Структурна схема, яка реалізує функції аналізу мережі з використанням нечіткої логіки

Такий спосіб визначення аномального стану в мережі при низькому відношенні сигнал/шум, де великі ймовірності помилок, сприяє більш адекватному прийняттю рішень. Застосування декількох порогів дає можливість коригувати рішення в залежності від зміни умов функціонування мережі.

Дійсно, якщо розташування аналізованого пристрою збігається з передбаченим, його трафіком й інші ознаки поведінки за даними СВВ не дає підс-

тав для занепокоєння, то потрапляння СКР (коефіцієнта асиметрії) його спектра в зону невизначеності не повинно бути приводом для його блокування.

Разом з тим, нетипове розташування, нетиповий трафік і «сіре» значення СКР (коефіцієнта асиметрії) спектра має стати приводом для відповідної реакції СВВ.

4.5 Прийняття рішень про аномальний стан бездротової мережі з урахуванням спектрального аналізу пристроїв

Основні загрози, специфічні для бездротових Wi-Fi мереж, описані в п. 3.5. У табл. 4.1 наведені ці загрози з коротким їх описом та можливістю їх виявлення і блокування при наявності ідентифікації абонентів по спектру. Так само як і у випадку з ознакою про місцеположення користувачів, дана ознака повинна бути частиною системи захисту, наприклад такої як системи виявлення вторгнень.

Розглянемо вплив наявності ідентифікації по спектру при захисті бездротових мереж.

Контроль спектру пристроїв співробітників при атаці «глушіння», дозволяє ідентифікувати атаку. Так як мережа може перестати працювати від різних причин, знаючи спектральну обстановку виявляється даний вид атак. Крім виявлення самої атаки це дозволить виявити «чистий» частотний канал. Як говорилося раніше, сама по собі ця атака фактично не використовується, за нею зазвичай йде атака «помилкова (фальшива) точка доступу» або DoS атака та інші. Запобігши, подібного роду атак, можна вберегти мережу від продовження зловмисних дій у вигляді інших атак.

Таблиця 4.1

Вид атаки	Що дозволяє місцеположення	Що дозволяє ідентифікація по спектру	ІТОГО
Глушіння	Дозволяє визначити джерело зловмисних дій, якщо він знаходиться в радіусі дії мережі	Дозволяє ідентифікувати атаку, виявити «чистий» частотний канал.	+
Вторгнення та модифікація даних	Не впливає	Дозволяє уникнути атаки ззовні	+
Атака «man in the middle»	Сприяє виявленню атаки і подальшого її блокування	Сприяє виявленню атаки	+
Абонент-шахрай	За нетиповим місцеположенням користувача атака виявляється і блокується	Дозволяє ідентифікувати чужі пристрої	+
Помилкова (фальшива) точка доступу	Блокуються всі точки доступу, що знаходяться не на своєму місці	Дозволяє ідентифікувати чужі пристрої	+
Прослуховування	Не впливає	Не впливає	–
DoS атака (Denial of Service – відказ в обслуговування)	Не впливає	Не впливає	–

Якщо вести спектральний контроль не тільки підключених користувачів, а й найближчих точок доступу, то це буде сприяти виявленню атаки «помилкова (фальшива) точка доступу». Суть цієї атаки зводиться до блокування легальної точки Wi-Fi мережі, щоб перенаправити абонентів мере-

жі на свою точку доступу. А це означає, що спектральна характеристика точки доступу поміняє свій вигляд.

Запобігти атаці «вторгнення і модифікація даних» стає можливим в тому випадку, якщо дану атаку здійснює не легітимний користувач мережі.

У разі атаки «man in the middle» (в канал зв'язку між роутером і комп'ютером жертви з’являється зловмисник і прослуховує їх, представляючись для кожного співрозмовника іншою стороною) класичні методи не тільки не можуть виявити джерело радіовипромінювання, але і сам факт вторгнення в мережу до того моменту поки зловмисник не переходить до активних дій. Знаючи спектральні особливості користувачів мережі, представитися «чужим ім'ям» не вийде, власне як і при атаці «абонент-шахрай».

Атаку «прослуховування» за допомогою ідентифікації по спектру запобігти не вийде, так як і при DoS атаці.

При реалізації даних атак в більшості випадків використовується обладнання, що не належать до мережі. Відповідно спектри пристроїв, у них будуть відмінні від легітимних. Таким чином, ідентифікація абонентів мережі по спектру дозволяє виявляти більшу частину атак на бездротові мережі, які в класичних системах часто пропускаються або не виявляються зовсім.

Висновки по розділу 4

За результатами даного розділу можна зробити наступні висновки:

1. Розроблено модель, що імітує шумову обстановку та дозволяє порівнювати спектри в умовах, близьких до реальних.

2. В ході моделювання для методу на основі СКР встановлено, що:

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

– по мірі зменшення відношення сигнал/шум абсолютне значення СКР росте;

– по мірі зменшення відношення сигнал/шум, відмінності між різними СКР зменшуються.

3. В ході моделювання для методу на основі кореляційної обробки встановлено, що:

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

– по мірі зменшення відношення сигнал/шум абсолютне значення коефіцієнту асиметрії росте;

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

3. Для методу основаного на СКР при співвідношенні сигнал/шум 30 дБ і більше спектри пристроїв розрізняються з ймовірністю, вище ніж 0,999 (жодної помилки на 1000 випробувань). Це дозволяє стверджувати, що метод може практично використовуватися.

3. Для методу основаного на кореляційній обробці спектри різних моделей пристроїв розрізняються з ймовірністю, вище ніж 0,999 (жодної помилки на 1000 випробувань) при любому відношенні сигнал/шум. Це дозволяє стверджувати, що метод може практично використовуватися.

4. Для методу на основі СКР при відношенні сигнал/шум менше 30 дБ та для однакових моделей пристроїв, при використанні методу на основі кореляційної обробки, можливі помилки в ідентифікації. Для зменшення впливу цих помилок на кінцеве рішення СВВ по ідентифікації пристрою пропонується застосувати алгоритм з елементами нечіткої логіки, шляхом введення двох порогів.

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

ВИСНОВКИ

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 вирішення вказаної задачі отримані такі науково-практичні результати:

1. Вперше запропоновано метод ідентифікації користувачів Wi-Fi мереж на основі детального аналізу спектральних характеристик випромінювання їх пристроїв, що дозволяє виявляти спроби втручання в мережу шляхом імітації роботи авторизованих користувачів.

2. Запропоновано новий метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом 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 розробленні 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 дозволяє виявляти і спільно з системами виявлення вторгнень запобігати ряду атак і тим самим підвищує безпеку Wi-Fi мереж .

Практична цінність роботи полягає в експериментально встановленій схожості спектрів Wi-Fi сигналів одного і того пристрою в різних положеннях та 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. Використання результатів дисертаційних досліджень підтверджується трьома актами впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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.

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.

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. 214 – 215.

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 XVIII 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.

16. Педжман Р. Основы построения беспроводных локальных сетей стандарта 802.11 / Р. Педжман, Д. Лиери. – М.: Вильямс, 2004. – 294 с.

17. Денисов Д. Обзор технологии Wi-Fi [Электронной ресурс] / Дмитрий Денисов // nag. – 2019. – Режим доступа до ресурса: https://nag.ru/articles/reviews/104595/obzor-tehnologii-wi-fi.html.

18. Современные беспроводные сети: состояние и перспективы развития / И. А.Гепко, В. Ф. Олейник, Ю. Д. Чайка, А. В. Бондаренко. – К.: ЕКМО, 2009. – 672 с.

19. Щербаков В. Б. Безопасность беспроводных сетей стандарта IEEE 802.11 / В. Б. Щербаков, С. А. Ермаков. – М.: РадиоСофт, 2010. – 255 с.

20. Гейер Д. Беспроводные сети. Первый шаг. / Пер. с англ / Дж. Гейер. – М.: Вильямс, 2005. – 192 с.

21. Феллинг Д. Точки доступа стандарта 802.11g / Д. Феллинг. // Windows IT Pro. – 204. – №4. – С. 17–23.

22. Приходько А. Я. Словарь-справочник по информационной безопасности / А. Я. Приходько. – М.: Синтег, 2001. – 124 с.

23. ETSI ETR 332: Security techniques advisory group (STAG). // Security requirements capture 1996.

24. Совлук Я. Безопасность внутриофисных сетей Wi-Fi / Я. Совлук. // Информационная безопасность: научный журнал. ВГТУ. – Воронеж. – 202. – №2. – С. 7–10.

25. Новиков А. А. Уязвимость и информационная безопасность телекоммуникационных технологий. Учебное пособие для вузов / А. А. Новиков, Г. Н. Устинов. – М.: Радио и связь, 2003. – 296 с.

26. Владимиров А. А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А. А. Владимиров. – М.: НТ-Пресс, 2005. – 463 с.

27. Межсетевые экраны [Электронной ресурс] // Компьютерные сети и технологии. – 2020. – Режим доступа до ресурса: http://www.xnets.ru/plugins/content/content.php?content.273.

28. Кухта А. И. Анализ методов защиты беспроводной сети Wi-Fi / А. И. Кухта. // Молодой исследователь Дона. – 2020. – №2 (23). – С. 48.

29. Милосердов А. Тестирование на проникновение с помощью Kali Linux 2.0 / А. Милосердов., 2015. – 348 с.

30. Барретт Б. The Next Generation of Wi-Fi Security Will Save You From Yourself [Электронной ресурс] / Брайан Барретт // WIRED. – 2018. – Режим доступа до ресурса: https://www.wired.com/story/wpa3-wi-fi-security-passwords-easy-connect/.

31. Vanhoef M. Dragonblood: Analyzing the DragonflyHandshake of WPA3 and EAP-pwd [Электронной ресурс] / M. Vanhoef, E. Ronen – Режим доступа до ресурса: https://papers.mathyvanhoef.com/dragonblood.pdf.

32. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин. – М.: ИД «ФОРУМ»: ИНФРА-М, 2008. – 416 с.

33. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, 1997. – 368 с.

34. Лекция 4: Intrusion Detection Systems (IDS) [Электронной ресурс] // НОУ ИНТУИТ – Режим доступа до ресурса: https://intuit.ru/studies/professional_retraining/966/courses/20/lecture/631?page=4.

35. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии). Учебное пособие для вузов / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова. – М.: Горячая линия – Телеком, 2013. – 221 с. 36. Бобров А. Системы обнаружения вторжений [Электронной ресурс] / Артем Бобров // Институт механики сплошных сред – Режим доступа до ресурса: http://www2.icmm.ru/~masich/win/lexion/ids/ids.html.

37. Беспроводная система предотвращения вторжений (WIPS) [Электронной ресурс] // Allta – Режим доступа до ресурса: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/wips.

38. Предотвратить и защитить [Электронный ресурс] // «Открытые системы» open System Publications. – 2018. – Режим доступа до ресурса: https://www.osp.ru/lan/2018/05/13054245.

39. Market Guide for Intrusion Detection and Prevention Systems [Электронный ресурс] // Gartner. – 2019. – Режим доступа до ресурса: https://www.gartner.com/en/documents/3945589.

40. Точка доступа предназначена для высокоплотных мест и работает по технологии Wave 2 802.11ac [Электронный ресурс] // Ubiquiti Networks – Режим доступа до ресурса: http://www.ubiquiti.by/katalog/unifi/unifi-ac.

41. Обзор системы обнаружения вторжений Cognitive WiFi от Mojo Networks [Электронный ресурс] // NetworkGuru – Режим доступа до ресурса: https://networkguru.ru/wips-mojo-networks-cognitive-wifi/.

42. Семенов Ю. А. Телекоммуникационные технологии / Ю. А. Семенов. – Москва: ГНЦ ИТЭФ, 2014. – 600 с.

43. Технологии современных беспроводных сетей Wi-Fi. Учебное издание Компьютерные системы и сети / [Е. В. Смирнова, А. В. Пролетарский, Е. А. Ромашкина та ін.]. – Москва: МГТУ им. Н.Э. Баумана, 2017. – 448 с.

44. Информационные операции в сети интернет / Под общ. ред. А.Б. Михайловского. – М.: АНО ЦСОиП, 2014. – 128 с.

45. Linux глазами хакера – СПб.: БХВ-Петербугр, 2019. – 416 с. – (5).

46. Сетевые средства Linux. / Перевод с английского и редакция В. В. Вейгпмана. – М.: Издательский дом "Вильяме", 2003. – 672 с.

47. Безрук В. Обнаружение и распознавание радиоизлучений при автоматизированном радиоконтроле / В. Безрук, Г. Певцов, О. Лебедев. // Комп'ютерні технології друкарства. – 2011. – №25. – С. 164–175.

48. Лазоренко О. В. Сверхширокополосные сигналы и физические процессы. 2. Методы анализа и применение / О. В. Лазоренко, Л. Ф. Черногор. // Радиофизика и радиоастрономия. – 2008. – №4. – С. 270–322.

49. Олейніков А. Н. Методи та засоби захисту інформації: Навчальний посібник для студентів вищих навчальних закладів / А. М. Олейніков. – Харків: НТМТ, 2014. – 298 с.

50. Кукуш В. Д. Совершенствование метеорной радиотехнической системы мониторинга динамических параметров атмосферы Земли по сигналам телевизионного вещания : дис. канд. техн. наук : 05.12.17 / Кукуш В. Д. – Харьков, 2012. – 165 с.

51. Основы спектрального мониторинга, радиочастотного регулирования и геолокации источников радиоизлучения [Электронной ресурс] // Agilent Technologies. – 2009. – Режим доступа до ресурса: https://radiorf.ru/wp-content/uploads/2014/10/adiolajn_spektralnyj_monitoring_
Agilent.pdf

52. Рішення НКРЗІ від 12.01.2012 № 18 [Електронний ресурс] // Національна комісія, що здійснює державне регулювання у сфері зв`язку та інформатизації офіційний веб-портал. – 2012. – Режим доступу до ресурсу: https://nkrzi.gov.ua/images/upload/256/5810/UUZ_stanom_na_26_09_2017.pdf

53. Бернгардт, А. С. Теория электрической связи [Электронной ресурс] / А. С. Бернгардт, // Тусур, РТФ – Режим доступу до ресурсу: https://slide-share.ru/1-117505.

54. Управление радиочастотным спектром и электромагнитная совместимость радиосистем. Учебн. пособие / [А. Л. Бузов, М. А. Быховский, Н. В. Васехо та ін.]. – М.: Эко-Трендз, 2006. – 376 с.

55. Шахтарин Б. И. Сравнение методов оценки энергетического спектра / Б. И. Шахтарин, Д. В. Бурляев. // Научный вестник МГТУ ГА. – 2010. – №158. – С. 27–43.

56. Денисенко А. Н. Сигналы. Теоретическая радиотехника. Справочное пособие / А. Н. Денисенко. – М.: Горячая линия - Телеком, 2005. – 704 с.

57. Надольський А. Н. Теоретические основы радиотехники: Учебное пособие для студентов специальности «Радиотехника», «Радиоинформатика» и «Радиотехнические системы» всех форм обучения. / А. Н. Надольський. – МН.: БГУИР, 2005. – 232 с.

58. Воробьев В. И. Теория и практика вейвлет-преобразования / В. И. Воробьев, В. Г. Грибунин. – СПб.: ВУС, 1999. – 203 с.

59. Горшенков А. А. Некоторые закономерности идентификационных измерений спектров сигналов / А. А. Горшенков, Ю. Н. Кликушин. // Журнал радиоэлектроники. – 2011. – №2.

60. Желтов А. Идентификация пользователя по голосу [Электронной ресурс] / Антон Желтов // Хабр. – 2012. – Режим доступу до ресурсу: https://habr.com/ru/post/144580/.

61. Спектральный компьютерный анализ голоса – метод ранней и дифференциальной диагностики нарушений голосовой функции [Электронной ресурс] / Ю. С.Василенко, А. П. Мещеркин, О. Г. Павлихин, С. Г. Романенко // ГБУЗ НИКИО им. Л.И. Свержевского ДЗМ – Режим доступу до ресурсу: https://nikio.ru/спектральный-анализ-голоса/

62. Теоретические основы радиолокации. Учебное пособие для вузов / [Я. Д. Ширман, В. Н. Голиков, И. Н. Бусыгин та ін.]. – М.: Советское радио, 1970. – 562 с.

63. Гоноровский И. С. Радиотехнические цепи и сигналы. Учебник для вузов. Издание 3-е, переработанное и дополненное / И. С. Гоноровский. – М.: Советское радио, 1977. – 608 с.

64. Niculescu D. Ad hoc positioning system (APS) using AOA / D. Niculescu, B. Nath. // Proceedings of the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications; San Francisco, CA, USA. 30 March–3 April. – 2003. – С. 1734–1743.

65. An asynchronous time-based location determination system / [M. Youssef, A. Youssef, C. Rieger та ін.]. // Proceedings of the 4th International Conference on Mobile Systems, Applications and Services; Uppsala, Sweden. 19–12 June. – 2006. – С. 165–176.

66. Cong L. Hybrid TDOA/AOA mobile user location for wideband CDMA cellular systems / L. Cong, W. H. Zhuang. // IEEE Trans. Wirel. Commun. – 2002. – С. 439–447.

67. Bargshady N. Precise Tracking of Things via Hybrid 3-D Fingerprint Database and Kernel Method Particle Filter / N. Bargshady, G. Garza, K. Pahlavan. // IEEE Sens. J. – 2016. – С. 8963–8971.

68. Atia M. Dynamic Propagation Modeling for Mobile sers' Position and Heading Estimation in Wireless Local Area Networks / M. Atia, A. Noureldin, M. Korenberg. // IEEE Wireless Communication Letters. – 2012. – №99. – С. 1–4.

69. The Internet of Things: a movement, not a market [Електронний ресурс] // IHS Markit. – 2020. – Режим доступу до ресурсу: https://cdn.ihs.com/www/pdf/IoT_ebook.pdf.

70. Зиборов И. А. Применения RFID технологий в деятельности различных субъектах хозяйствования / И. А. Зиборов. // Молодой ученый. – 209. – №12 (12). – С. 17–22.

71. Всесвітнє дослідження економічних злочинів та шахрайства 2018: результати опитування українських організацій [Електронний ресурс] // PwC

Україна. – 2018. – Режим доступу до ресурсу: https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf.

72. Кондратьев В. С. Многопозиционные радиолокационные системы / В. С. Кондратьев, А. Ф. Котов, Л. Н. Марков. – М.: Радио и связь, 1986. – 264с.

73. Отчет МСЭ-R SM.2211-1. Сравнение методов определения географического местоположения источника сигнала, основанных на разнице во времени прихода и угле прихода сигнала. Международный союз электросвязи. − июнь 2014. – 32 с.

74. Ворошилин Е. П. Определение координат источников радиоизлучения разностно-дальномерным методом с использованием группировки низкоорбитальных малых космических аппаратов / Е. П. Ворошилин, М. В. Миронов, В. А. Громов. // ТУСУРа. – 2010. – С. 23 –28.

75. Юркин Д. В. Системы обнаружения вторжений в сетях широкополосного радиодоступа стандарта IEEE 802.11 / Д. В. Юркин, В. Н. Никитин. // Информационно-управляющие системы. – 2014. – С. 44–49.

76. Saunders S. R. Antennas and propagation for wireless communication systems, 2nd Edition / S. R. Saunders, A. Aragon-Zavala., 2007. – 546 с.

77. ITU-R P.1238-9. Propagation data and prediction methods for the planning of indoor radio communication systems and the radio local area networks in the frequency range 300 MHz to 100 GHz, **G**eneva: ITU-R Recommendations, 2017.

78. Миниахметов Р. М. Обзор алгоритмов локального позиционирования для мобильных устройств / Р. М. Миниахметов, А. А. Рогов, М. Л. Цымблер. // Вестник ЮУрГУ. Сер. Вычислительная математика и информатика Т. 2. № 2 – 2013. – С. 83–96.

79. Гоноровский И. С. Радиотехнические цепи и сигналы / И. С. Гоноровский. – М.: Советское радио, 1977. – 608 с.

80. РЕКОМЕНДАЦИЯ МСЭ-R P.372-13 [Електронний ресурс] // МСЭ-R. – 2016. – Режим доступу до ресурсу: https://www.itu.int/dms_pubrec/itu-r/rec/p/R-REC-P.372-13-201609-S!!PDF-R.pdf.

81. Характеристики WiFi оборудования [Електронний ресурс] // © LanTorg. – 2015. – Режим доступу до ресурсу: https://lantorg.com/article/harakteristiki-wifi-oborudovaniya.

82. Сиденко В. М. Основы научных исследований / В.М. Сиденко, И.М. Грушко. – Харьков: Выща школа, 1978. – 200 с.

Додаток А

Акти впровадження результатів дисертаційних досліджень

«ЗАТВЕРДЖУЮ»
Головний інженер виробничого підрозділу
«Харківське відділення» філії «Головний
інформаційно-обчислювальний центр»
АТ «Укрзалізниця»

_____ І.В.Давидов

«10» 02 2021

АКТ

Про використання результатів дисертаційної роботи
Василенко Тетяни Олександрівни
на тему **«Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі»**

Цим актом підтверджуємо, що результати дисертаційної роботи Василенко Т.О. 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.

Вважаємо теоретично обґрунтованими та практично підтвердженими такі результати згаданої дисертаційної роботи:

1. Розроблено метод ідентифікації користувачів Wi-Fi мереж на основі детального аналізу спектральних характеристик випромінювання їх пристроїв, що дозволяє виявляти спроби втручання шляхом імітації роботи авторизованих користувачів в мережу.
2. Запропоновано метод обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом обчислення середнього квадрата різниці відповідних спектральних відліків з урахуванням різниці в середній потужності різних сигналів, що дозволяє порівнювати з еталонним спектри, отримані в різних умовах.
3. Опрацьовано метод виявлення атак на бездротову мережу, що полягає у використанні даних про місцеперебування користувачів в мережі, які визначаються за RSSI, з використанням індивідуальних «радіовідбитків», що дозволяє виявляти атаки, які не виявляються за іншими ознаками.
4. Розроблено модель, що імітує спектр сигналу Wi-Fi мережі в умовах впливу шуму, яка дозволяє оцінити ефективність розроблених методів в реальних умовах і виробити рекомендації щодо їх практичного застосування.

Начальник сектору захисту
інформації та безпеки інформаційних систем Є.Ю.Жевага

Адміністратор 2 категорії відділу
телекомунікаційних систем і
мереж передачі даних І.Ю.Семиренко

«ЗАТВЕРДЖУЮ»
Перший проректор
Харківського національного
університету радіоелектроніки

_____ Рубан І.В.

«__» _____ 2021

АКТ

Про впровадження результатів дисертаційної роботи Василенко Тетяни Олександрівни «Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі».

Комісія в складі голови комісії зав. каф. КРіСТЗІ проф. д.т.н. Антіпова І.Є. членів комісії: доц. каф. КРіСТЗІ к. ф-м. н. Лихограєм В.Г та доц. каф. КРіСТЗІ к.т.н Щербиною О.О. підтверджує, що результати четвертого розділу дисертаційної роботи Василенко Тетяни Олександрівни, а саме розробка моделі Wi-Fi мережі по запобіганню вторгнень з елементами нечіткої логіки, були використані при виконанні держбюджетної НДР, фінансованою МОН України: №260-5 «Розробка методів моделювання інформаційних мереж, побудованих на основі реконфігурованих антен».

Голова комісії
Зав. каф. КРіСТЗІ, д. т. н., проф. І.Є. Антіпов

Члени комісії:

Доц. каф. КРіСТЗІ, к. ф-м. н. В.Г. Лихограй

Доц. каф. КРіСТЗІ, к. т. н О.О. Щербина

«ЗАТВЕРДЖУЮ»
Перший проректор
Харківського національного
університету радіоелектроніки

_____ Рубан І.В.

«__17__» _____2021

АКТ

Про використання результатів дисертаційної роботи Василенко Тетяни Олександрівни «Методи розпізнавання Wi-Fi пристроїв шляхом врахування їх індивідуальних ознак для підвищення захищеності мережі».

Ми, що нижче підписалися, завідувач кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації професор Антіпов І. Є., професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Должиков В.В., професор кафедри Комп'ютерної радіоінженерії та систем технічного захисту інформації Олейніков А.М., склали даний акт про те, що результати дисертаційної роботи Василенко Тетяни Олександрівни використовувались в освітньому процесі на кафедрі Комп'ютерної радіоінженерії та систем технічного захисту інформації.

Результати дисертаційної роботи, пов'язані з використанням методу ідентифікації користувачів Wi-Fi мереж на основі детального аналізу спектральних характеристик випромінювання їх мобільних пристроїв та методу обробки результатів вимірювання спектрів випромінювання Wi-Fi пристроїв шляхом обчислення середнього квадрата різниці (розділ 2) використовуються в курсі лекцій по дисципліні «Обробка сигналів в системах ТЗІ».

Результати дисертаційної роботи по використанню спектрального аналізу пристроїв Wi-Fi мережі для їх ідентифікації (розділ 2. 4) використовувались при підготовці магістерських атестаційних робіт студентів спеціальності «Системи технічного захисту інформації, автоматизація її обробки», що проходять підготовку на кафедрі Комп'ютерної радіоінженерії та систем технічного захисту інформації

Голова комісії
Зав. каф. КРіСТЗІ, д. т. н., проф. І.Є. Антіпов

Члени комісії:

Проф. каф. КРіСТЗІ, д. ф-м. н В.В. Должиков

Проф. каф. КРіСТЗІ, к. т. н. А.М. Олейніков

Додаток Б

Спектр пристрою у форматі * .csv

-84.0093 2411.002262 -83.4015 2411.004166 -82.7608 2411.006071 -81.9897 2411.007976 -82.1799 2411.009881 -81.7077 2411.011785 -83.3834 2411.013690 -83.5052 2411.015595 -83.0422 2411.017500 -83.5850 2411.019404 -83.4556 2411.021309 -82.4256 2411.023214 -83.0263 2411.025119 -83.7401 2411.027024 -83.7984 2411.028928 -84.3100 2411.030833 -84.9672 2411.032738 -83.4306 2411.034643 -83.7245 2411.036547 -84.7687 2411.038452 -85.0005 2411.040357 -84.0994 2411.042262 -84.5566 2411.044166 -84.6061 2411.046071 -84.8271 2411.047976 -84.7328 2411.049881 -83.7147 2411.051785 -82.5278 2411.053690 -83.1520 2411.055595 -84.5267 2411.057500 -84.3861 2411.059404 -83.7983 2411.061309 -84.6117 2411.063214 -84.5192 2411.065119 -83.9071 2411.067024 -83.4849 2411.068928 -84.1285 2411.070833 -84.4609 2411.072738 -84.3953 2411.074643 -84.2188 2411.076547 -84.2767 2411.078452 -83.6007 2411.080357 -84.4716 2411.082262 -84.0312 2411.084166 -83.6678 2411.086071 -83.5564 2411.087976 -83.6415 2411.089881 -82.7999 2411.091785 -83.5229 2411.093690 -84.5011 2411.095595 -84.6146 2411.097500 -83.7181 2411.099404 -83.6060 2411.101309 -82.9345 2411.103214 -83.2734 2411.105119 -82.3549 2411.107024 -81.8117 2411.108928 -82.1962 2411.110833 -83.0970 2411.112738 -83.9764 2411.114643 -83.9591 2411.116547 -84.3356 2411.118452 -83.9255 2411.120357 -84.0690 2411.122262 -84.2841 2411.124166 -83.5631 2411.126071 -83.6593 2411.127976 -84.0943 2411.129881 -84.3438 2411.131785 -84.4814 2411.133690 -82.7991 2411.135595 -83.7579 2411.137500 -84.3253 2411.139404 -84.2440 2411.141309 -84.4652 2411.143214 -83.7278 2411.145119 -83.5454 2411.147023 -83.4399 2411.148928 -83.6316 2411.150833 -84.4840 2411.152738 -84.0134 2411.154643 -83.5421 2411.156547 -82.8757 2411.158452 -83.6320 2411.160357 -82.8364 2411.162262 -83.0381 2411.164166 -84.4662 2411.166071 -84.1108 2411.167976 -82.3156 2411.169881 -81.7851 2411.171785 -82.0133 2411.173690 -83.0189 2411.175595 -84.0085 2411.177500 -83.2538 2411.179404 -82.9671 2411.181309 -83.0112 2411.183214 -84.1201 2411.185119 -83.8087 2411.187023 -82.9292 2411.188928 -82.8774 2411.190833 -82.9704 2411.192738 -83.6612 2411.194643 -84.8014 2411.196547 -83.6397 2411.198452 -83.9763 2411.200357 -83.0525 2411.202262 -81.8248 2411.204166 -82.8116 2411.206071 -83.9275 2411.207976 -83.4292 2411.209881 -82.8095 2411.211785 -82.3528 2411.213690 -83.3478 2411.215595 -83.0744 2411.217500 -82.1277 2411.219404 -82.4203 2411.221309 -83.5092 2411.223214 -83.0041 2411.225119 -83.2301 2411.227023 -83.0293 2411.228928 -83.7076 2411.230833 -84.0961 2411.232738 -83.0762 2411.234643 -84.1403 2411.236547 -83.4560 2411.238452 -83.2730 2411.240357 -84.3981 2411.242262 -84.6228 2411.244166 -83.6834 2411.246071 -82.9531 2411.247976 -82.7486 2411.249881 -83.5590 2411.251785 -83.9938 2411.253690 -84.3297 2411.255595 -84.5775 2411.257500 -83.9382 2411.259404 -82.6065 2411.261309 -83.5549 2411.263214 -84.5979 2411.265119 -85.1196 2411.267023 -84.6783 2411.268928 -84.2378 2411.270833 -83.8607 2411.272738 -83.2574 2411.274643 -84.1160 2411.276547 -84.1731 2411.278452 -85.1241 2411.280357 -84.6796 2411.282262 -84.5276 2411.284166 -84.1901 2411.286071 -83.8202 2411.287976 -83.7201 2411.289881 -83.5903 2411.291785 -83.3460 2411.293690 -84.5369 2411.295595 -84.4697 2411.297500 -83.3582 2411.299404 -82.3250 2411.301309 -82.2456 2411.303214 -83.2154 2411.305119 -83.4426 2411.307023 -83.4759 2411.308928 -82.3759 2411.310833 -82.6733 2411.312738 -83.2687 2411.314643 -83.7795 2411.316547 -83.8138 2411.318452 -84.4406 2411.320357 -83.7356 2411.322262 -83.7670 2411.324166 -84.1126 2411.326071 -82.5775 2411.327976 -81.9341 2411.329881 -82.2849 2411.331785 -83.1229 2411.333690 -83.9297 2411.335595 -83.9764 2411.337500 -83.0162 2411.339404 -82.5419 2411.341309 -84.4094 2411.343214 -83.7300 2411.358452 -85.1176 2411.360357 -84.4458 2411.362262 -84.4230 2411.364166 -84.2795 2411.366071 -84.4731 2411.367976 -84.20912411.369881 -82.9818 2411.358452 -85.1176 2411.360357 -84.44582411.362262 -84.4230 2411.364166 -84.2795 2411.366071 -84.4731 2411.367976 -84.2091 2411.369881 -82.9818 2411.371785 -82.2346 2411.373690 -83.1588 2411.375595 -83.6393 2411.377500 -83.5180 2411.379404 -82.3791 2411.381309 -82.5635 2411.383214 -83.39922411.385119 -83.5845 2411.387023 -82.8325 2411.388928 -83.0439 2411.390833 -83.7817 2411.392738 -83.7158 2411.394642 -83.4130 2411.396547 -83.4972 2411.398452 -83.3032 2411.400357 -83.5652 2411.402262 -82.1927 2411.404166 -82.5922 2411.406071 -83.0459 2411.407976 -84.0113 2411.409881 -82.8684 2411.411785 -81.8413 2411.413690 -82.1836 2411.415595 -81.8033 2411.417500 -82.9898 2411.419404 -84.2229 2411.421309 -83.7261 2411.423214 -82.9060 2411.427023 -82.5400 2411.428928 -83.0212 2411.430833 -83.1968 2411.432738 -83.1217 2411.434642 -83.7261 2411.423214 -82.6624 2411.440357 -83.1928 2411.442262 -83.3741 2411.444166 -83.8182 2411.446071 -83.2284 2411.447976 -84.2746 2411.449881 -82.9558 2411.451785 -82.2178 2411.453690 -82.5745 2411.455595 -82.1583 2411.457500 -84.0021 2411.459404 -84.5309 2411.461309 -84.6801 2411.463214 -84.1356 2411.465119 -84.0011 2411.467023 -83.8224 2411.468928 -83.9331 2411.470833 -84.2325 2411.472738 -84.3762 2411.474642 -83.2769 2411.476547 -83.6462 2411.478452 -82.9703 2411.480357 -83.4270 2411.482262 -83.7866 2411.484166 -83.7473 2411.486071 -83.8677 2411.487976 -83.7348 2411.489881 -83.9090 2411.491785 -82.1531 2411.493690 -82.1139 2411.495595 -83.5611 2411.497500 -83.8721 2411.499404 -83.3359 2411.501309 -83.5488 2411.503214 -83.6969 2411.505119 -84.1449 2411.507023 -83.4202 2411.508928 -83.7664 2411.510833 -83.7202 2411.512738 -83.6047 2411.514642 -83.5189 2411.516547 -83.3484 2411.518452 -83.8744 2411.520357 -83.2547 2411.522261 -82.6598 2411.524166 -82.5576 2411.526071 -83.6463 2411.527976 -83.6840 2411.529881 -83.8168 2411.531785 -83.7379 2411.533690 -83.4947 2411.535595 -83.7214 2411.537500 -83.3121 2411.539404 -82.6156 2411.541309 -83.9382 2411.543214 -83.2212 2411.545119 -82.1064 2411.547023 -83.2641 2411.548928 -82.6539 2411.550833 -81.4603 2411.552738 -82.1204 2411.554642 -83.5826 2411.556547 -82.5053 2411.558452 -81.9113 2411.560357 -81.8279 2411.562261 -82.3155 2411.564166 -82.8297 2411.566071 -81.2582 2411.567976 -81.2672 2411.569881 -81.0713 2411.571785 -81.1020 2411.573690 -81.9540 2411.575595 -83.7892 2411.577500 -84.3719 2411.579404 -83.4289 2411.581309 -84.1932 2411.583214 -84.2168 2411.585119 -84.0692 2411.587023 -84.3037 2411.588928 -84.2426 2411.590833 -84.4849 2411.592738 -84.0627 2411.594642 -84.0565 2411.596547 -83.8651 2411.598452 -84.0212 2411.600357 -82.1290 2411.602261 -83.1605 2411.604166 -82.8984 2411.606071 -83.0795 2411.607976 -83.5068 2411.609881 -83.2478 2411.611785 -82.6131 2411.613690 -82.6232 2411.615595 -83.3845 2411.617500 -83.0075 2411.619404 -84.0449 2411.621309 -83.1861 2411.623214 -82.2353 2411.625119 -81.9717 2411.627023 -82.8009 2411.628928 -83.1761 2411.630833 -83.1296 2411.632738 -83.9936 2411.634642 -82.7198 2411.636547 -82.9768 2411.638452 -84.4197 2411.640357 -84.6473 2411.642261 -84.9403 2411.644166 -84.9606 2411.646071 -83.8399 2411.647976 -81.8368 2411.649881 -81.3650 2411.651785 -82.1039 2411.653690 -83.6915 2411.655595 -85.2399 2411.657500 -83.9568 2411.659404 -83.4887 2411.661309 -83.9557 2411.663214 -83.7109 2411.665119 -84.1535 2411.667023 -84.2127 2411.668928 -84.3851 2411.670833 -83.4874 2411.672738 -82.5493 2411.674642 -82.7708 2411.676547 -84.2269 2411.678452 -83.9350 2411.680357 -84.2438 2411.682261 -83.2683 2411.684166 -83.0208 2411.686071 -82.3080 2411.687976 -82.2011 2411.689881 -82.9342 2411.691785 -82.9753 2411.693690 -82.7661 2411.695595 -83.5516 2411.697500 -83.8428 2411.699404 -82.0692 2411.701309 -81.5750 2411.703214 -82.9320 2411.705119 -83.4267 2411.707023 -84.5316 2411.708928 -84.3655 2411.710833 -83.9369 2411.712738 -84.3954 2411.714642 -84.8415 2411.716547 -83.6900 2411.718452 -84.1964 2411.720357 -84.0645 2411.722261 -83.9584 2411.724166 -83.1654 2411.726071 -83.9323 2411.727976 -83.1872 2411.729880 -83.2688 2411.731785 -83.7855 2411.733690 -83.4429 2411.735595 -83.8339 2411.737500 -84.2387 2411.739404 -83.7040 2411.741309 -84.1077 2411.743214 -83.5114 2411.745119 -83.1967 2411.747023 -83.3012 2411.748928 -84.0564 2411.750833 -84.8649 2411.752738 -83.7321 2411.754642 -83.2750 2411.756547 -83.4458 2411.758452 -82.6561 2411.760357 -82.1527 2411.762261 -82.8577 2411.764166 -84.2916 2411.766071 -83.9715 2411.767976 -84.1440 2411.769880 -83.3443 2411.771785 -83.1853 2411.773690 -82.6020 2411.775595 -82.8363 2411.777500 -83.2729 2411.779404 -83.8701 2411.781309 -83.3779 2411.783214 -84.1581 2411.785119 -83.9604 2411.787023 -83.7813 2411.788928 -82.9089 2411.790833 -82.1256 2411.792738 -83.0839 2411.794642 -84.1825 2411.796547 -83.5761 2411.798452 -83.7018 2411.800357 -82.7130 2411.802261 -82.2407 2411.804166 -82.2188 2411.806071 -82.1701 2411.807976 -82.6515 2411.809880 -82.8929 2411.811785 -82.2696 2411.813690 -81.5246 2411.815595 -81.8330 2411.817500 -82.8741 2411.819404 -83.0592 2411.821309 -84.3459 2411.823214 -83.9188 2411.825119 -83.0198 2411.827023 -83.8944 2411.828928 -84.3984 2411.830833 -82.7975 2411.832738 -82.7365 2411.834642 -83.1594 2411.836547 -83.7397 2411.838452 -82.6109 2411.840357 -82.7901 2411.842261 -83.3750 2411.844166 -83.2615 2411.846071 -83.3645 2411.847976 -84.7725 2411.849880 -84.1633 2411.851785 -83.3855 2411.853690 -83.6498 2411.855595 -82.9220 2411.857500 -82.5244 2411.859404 -83.1961 2411.861309 -83.5291 2411.863214 -83.8082 2411.865119 -83.5534 2411.867023 -83.6053 2411.868928 -84.6827 2411.870833 -84.6677 2411.872738 -84.6677 2411.874642 -83.5689 2411.876547 -84.1904 2411.878452 -83.7439 2411.880357 -84.0749 2411.882261 -83.2728 2411.884166 -84.0613 2411.886071 -84.2014 2411.887976 -83.8260 2411.889880 -83.5201 2411.891785 -84.0431 2411.893690 -84.1352 2411.895595 -83.3013 2411.897499 -83.0729 2411.899404 -83.5080 2411.901309 -83.6481 2411.903214 -83.0701 2411.905119 -83.7589 2411.907023 -83.2717 2411.908928 -82.6188 2411.910833 -83.6274 2411.912738 -84.1011 2411.914642 -84.2788 2411.916547 -84.0221 2411.918452 -83.9176 2411.920357 -83.1859 2411.922261 -83.8871 2411.924166 -83.0159 2411.926071 -82.1366 2411.927976 -81.8824 2411.929880 -82.9235 2411.931785 -83.2709 2411.933690 -83.3959 2411.935595 -83.0880 2411.937499 -83.9626 2411.939404 -83.2718 2411.941309 -84.9860 2411.943214 -84.7162 2411.945119 -83.3889 2411.947023 -83.4410 2411.948928 -83.7865 2411.950833 -84.5691 2411.952738 -84.1951 2411.954642 -84.9541 2411.956547 -84.6216 2411.958452 -84.1414 2411.960357 -84.3182 2411.962261 -83.3697 2411.964166 -82.9834 2411.966071 -83.5102 2411.967976 -83.7114 2411.969880 -83.2697 2411.971785 -83.1293 2411.973690 -83.6149 2411.975595 -83.8493 2411.977499 -84.2361 2411.979404 -84.9545 2411.981309 -85.2753 2411.983214 -85.0302 411.985119 -83.2836 2411.987023 -84.0759 2411.988928 -83.7780 2411.990833 -82.8785 2411.992738 -82.4942 2411.994642 -82.4671 2411.996547 -83.5279 2411.998452 -83.1608 2412.000357 -83.2720 2412.002261 -83.1182 2412.004166 -82.4718 2412.006071 -82.3839 2412.007976 -82.2221 2412.009880 -82.4741 2412.011785 -83.6957 2412.013690 -84.1215 2412.015595 -82.6708 2412.017499 -82.1744 2412.019404 -83.0751 2412.021309 -82.3930 2412.023214 -82.2987 2412.025119 -82.8887 2412.027023 -83.4462 2412.028928 -84.0447 2412.030833 -84.3253 2412.032738