УДК 004.056.053
DOI: 10.31673/2409-7292.2019.022531

О.А. Лаптєв

МЕТОДИКА ВИЯВЛЕННЯ І ЛОКАЛІЗАЦІЇ ЗАСОБІВ НЕГЛАСНОГО ОТРИМАННЯ ІНФОРМАЦІЇ, ЯКІ ПРАЦЮЮТЬ У ЦИФРОВОМУ ДІАПАЗОНІ Wi-Fi

Проведено аналіз частотного діапазону Wi-Fi щодо завантаженості різноманітними приладами та пристроями. Наведено спектрограми реальних сигналів цифрового діапазону які доводять неможливість виявлення, розпізнання та локалізацію засобів негласного отримання інформації. Проаналізовано перелік сучасних засобів отримання інформації (ЗНОІ), які можуть бути використані у якості пристроїв отримання інформації по мережі Wi-Fi. Запропонована удосконалена методика пошуку цифрових засобів негласного отримання інформації в діапазоні Wi-Fi, яка дає змогу, додатково до класичних методів пошуку, додатково аналізувати MAC-адреси засобів. Розроблено методичні рекомендації щодо створення сучасного програмно-апаратного комплексу аналізу пошуку засобів негласного отримання інформації, які працюють під прикриттям радіомереж Wi-Fi. Приведені реальні спектрограми та проведено натурне модулювання виявлення, розпізнавання та локалізації ЗНОІ що працює у діапазоні Wi-Fi. Отримані результати (теоретичні та графічні) цілком підтверджують розроблену нами методику пошуку ЗНОІ, які працюють у цифровому діапазоні.

Ключові слова: діапазон Wi-Fi, спектр, засоби негласного отримання інформації, MAC-адрес, методика

Вступ

Розглядаючи історію виникнення Wi-Fi, слід зазначити що абревіатура Wi-Fi є скороченою назвою зареєстрованої торгової марки «Wi-Fi AUiance». Технологія Wi-Fi була розроблена у 1991 році фірмою NCR Corporation (яка на той час була поглинена компанією AT&T, а з 1997 року знову стала самостійною) і спочатку призначалася для використання в торгових касових апаратах. [1] В основу технології лягла методика передачі даних по радіоканалу на частоті 2,4 ГГц з використанням кодування сигналу робочими частотами і спеціальними додатками. Технологія Wi-Fi використовується для організації високошвидкісних бездротових локальних мереж, які працюють у міжнародному неліцензованому діапазоні частот (ISM) 2,4 ГГц і 5 ГГц. [2] Галузь застосування цієї технології пов'язані з мережами для виходу в Інтернет, бездротовою передачею аудіо- та відеоінформації, промислової телеметрією, транспортними локальними бездротовими мережами.

Основною перевагою Wi-Fi перед іншими технологіями є висока швидкість передачі інформації-до 1300 Мбіт/с. Тому ця технологія набула розвитку в таких галузях побутової електроніки, як бездротовий доступ до Інтернету, цифрове телебачення та ін. Широко застосовується Wi-Fi в різних бездротових телеметричних системах на транспорті. Практично всі бездротові відеокамери та реєстратори швидкості, встановлені на автомагістралях, використовують Wi-Fi. Також ця технологія використовується для організації локальних мереж між будівлями і промисловими об'єктами. Слід підкреслити, що діапазон Wi-Fi 5 ГГц є найкращим для організації промислових локальних мереж в умовах перешкод високого рівня.

На даний час важко знайти іншу подібну по активності використовувану ділянку радіочастотного спектру, як діапазон Wi-Fi. У цьому діапазоні працюють пристрої таких стандартів Wi-Fi, Bluetooth, DECT, аналогові та цифрові відеопередавачі, системи дистанційного керування та доступу, та багато іншого. Звісно чим більше використовуваним є ділянку радіочастотного спектру, тим складніше його контролювати і аналізувати. Ця обставина є найбільш вагомим фактором для вибору зловмисниками середовища з метою маскування роботи своїх засобів негласного отримання інформації (ЗНОІ), призначених для перехоплення інформації обмеженого доступу. Виходячи з вищевикладеного пошук ЗНОІ в діапазоні роботи Wi-Fi є особливо важливим, а розробка методики пошуку таких ЗНОІ є актуальною.

Аналіз останніх досліджень і публікацій

Завданням щодо пошуку ЗНОІ, присвячено значну кількість публікацій. Так у [4] розглядаються питання аналізу систем радіоконтролю (радіомоніторингу) з різними

технічними параметрами, які об'єднує тільки одне - вони можуть тільки показувати та (в кращому випадку) зберігати панорами спектрів сигналів в радіоефірі. Завдання аналізу цифрових легальних каналів зв'язку вони у взагалі не вирішують. У [6] Розглядається Wi-Fi, який застосовується у різних бездротових телеметричних системах на транспорті. Діапазон Wi-Fi 5 ГГц є найкращим для організації промислових локальних мереж при наявності перешкод високого рівня. Доведено, що «класичним» методом пошуку проаналізувати цей частотний діапазон неможливо. Тобто для пошуку ЗНОІ, потрібні інші методи. У [8] розглядається комплекс радіомоніторингу «Delta», якій продовжує перелік самих передових та технологічних рішень в галузі радіомоніторингу. Комплекс «Delta» надає широкі можливості для виявлення та ідентифікації джерел сигналів. Недоліком цього комплексу відсутність можливості автоматично локалізувати цифрові ЗНОІ.

З аналізу сучасної літератури можна зробити висновок, що універсальних пристроїв (приладів, автоматизованих програмних комплексів) для аналізу цифрових пакетів, стосовно завдань пошукового радіоконтролю, зараз практично немає. Тому задача виявлення ЗНОІ які працюють в діапазоні Wi-Fi – є дуже важливою.

Постановка проблеми

Головною перевагою Wi-Fi перед іншими технологіями є висока швидкість передачі інформації, ця технологія розвивається дуже швидко, тому ця ділянка радіочастотного діапазону, швидко заповнюється. Виходячи з цього цей частотний діапазон становиться складніше контролювати і аналізувати. Ця обставина часто є вирішальним фактором при виборі зловмисниками середовища для варіанту маскування роботи своїх засобів негласного отримання інформації, які призначені для перехоплення інформації обмеженого доступу. Виходячи з вищевикладеного пошук ЗНОІ в діапазоні роботи Wi-Fi є особливо важливим, а розробка методики пошуку таких ЗНОІ є актуальної.

Виклад основного матеріалу

Використовуючи для роботи ЗНОІ сильно завантажені частотні діапазони, зловмисник має намір максимально ускладнити їх виявлення, логічне використовувати для цього загальноприйняті і поширені в цих діапазонах стандарти зв'язку. Стосовно до технології Wi-Fi це істотно спрощує виробництво ЗНОІ, тому що застосовуються поширені, доступні та недорогі компоненти (електронні радіодеталі та модулі), відпрацьовані інженерні рішення.

Але найголовніше – важко відрізнити один від одного роботу двох пристроїв, що використовують один і той же цифровий стандарт зв'язку, без виявлення їх унікальних ID (ідентифікаторів). У випадку з Wi-Fi, таким ідентифікатором є MAC-адреса (MAC-адреса - це унікальний ідентифікатор мережевого інтерфейсу (зазвичай мережевої карти) для реалізації комунікації пристроїв в мережі на фізичному рівні. Це унікальний номер, який зберігається у пам'яті, що доступна тільки для читання, призначена мережевій карті її виробником). або LLC (Logical link control - підрівень керування логічним зв'язком - за стандартом IEEE 802 - верхній підрівень канального рівня моделі OSI, здійснює управління передачею даних та забезпечує перевірку і правильність передачі інформації по з'єднанню). У даній статті ми не будемо торкатися питання безпеки легальних мереж Wi-Fi, це окрема тема. У даному випадку нас цікавить використання технології Wi-Fi, яка полягає у основі виготовлення ЗНОІ, а також вимоги, які необхідно пред'являти до сучасних засобів аналізу мереж Wi-Fi стосовно області пошуку і локалізації ЗНОІ для запобігання витоку інформації по частотному радіоканалу Wi-Fi.

Актуальність вищевикладеного підтверджується крім теоретичного обґрунтування ще й прикладом, протягом однієй години поїздки в травні цього року за маршрутом Майдан Незалежності-вул. Велика Житомирська-Львівська площа вул. Січових стрільців (м.Київ), фахівцями було зафіксовано 947 унікальних MAC-адреси. У їх числі 552 точок доступу і 395 пристроїв в черговому режимі без поточного підключення (в основному це смартфони, власники яких не вимикають Wi-Fi далеко від зареєстрованих точок доступу). Реальні спектрограми доводять неможливість визначення ЗНОІ які працюють у цифровому діапазоне існуючими методами приведені на рис.1 та рис.2.

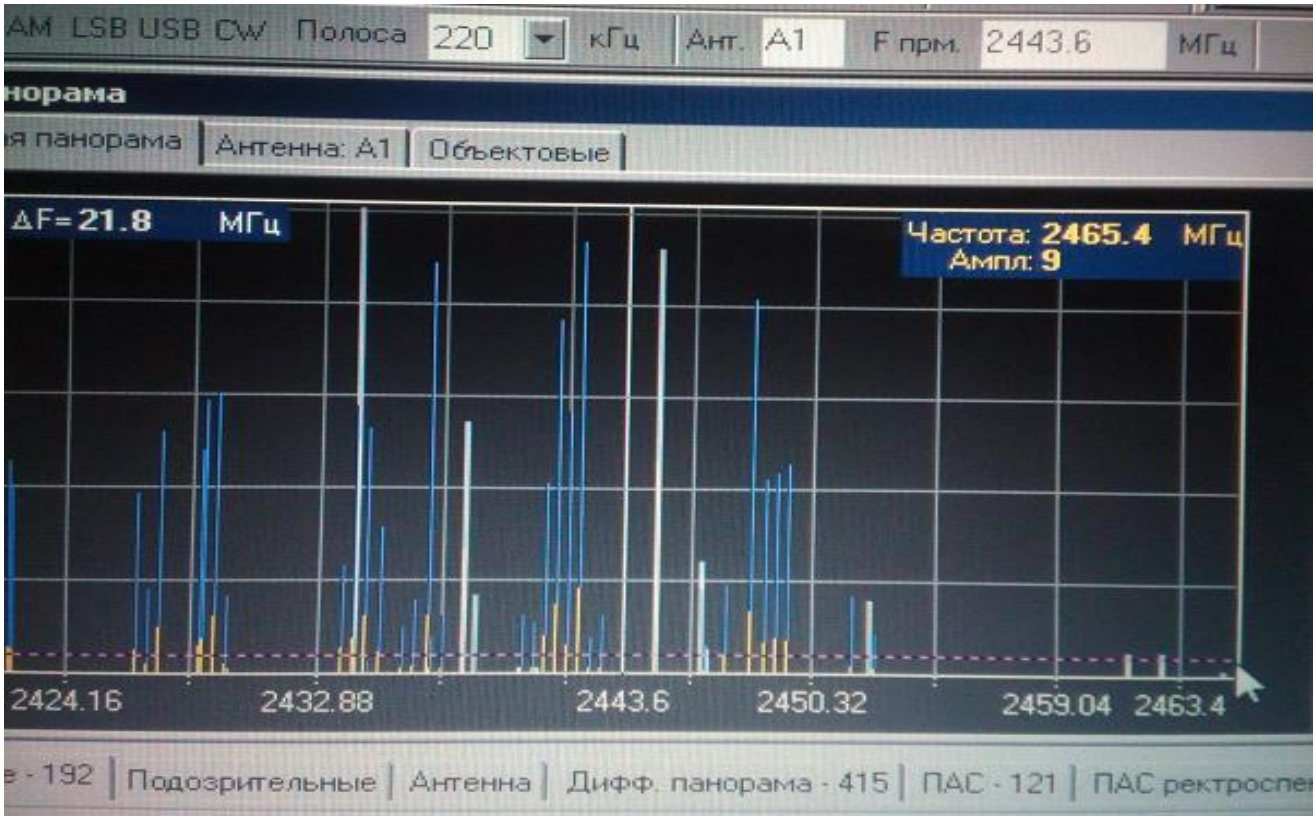

Рис. 1. Спектр сигналів діапазону Wi-Fi

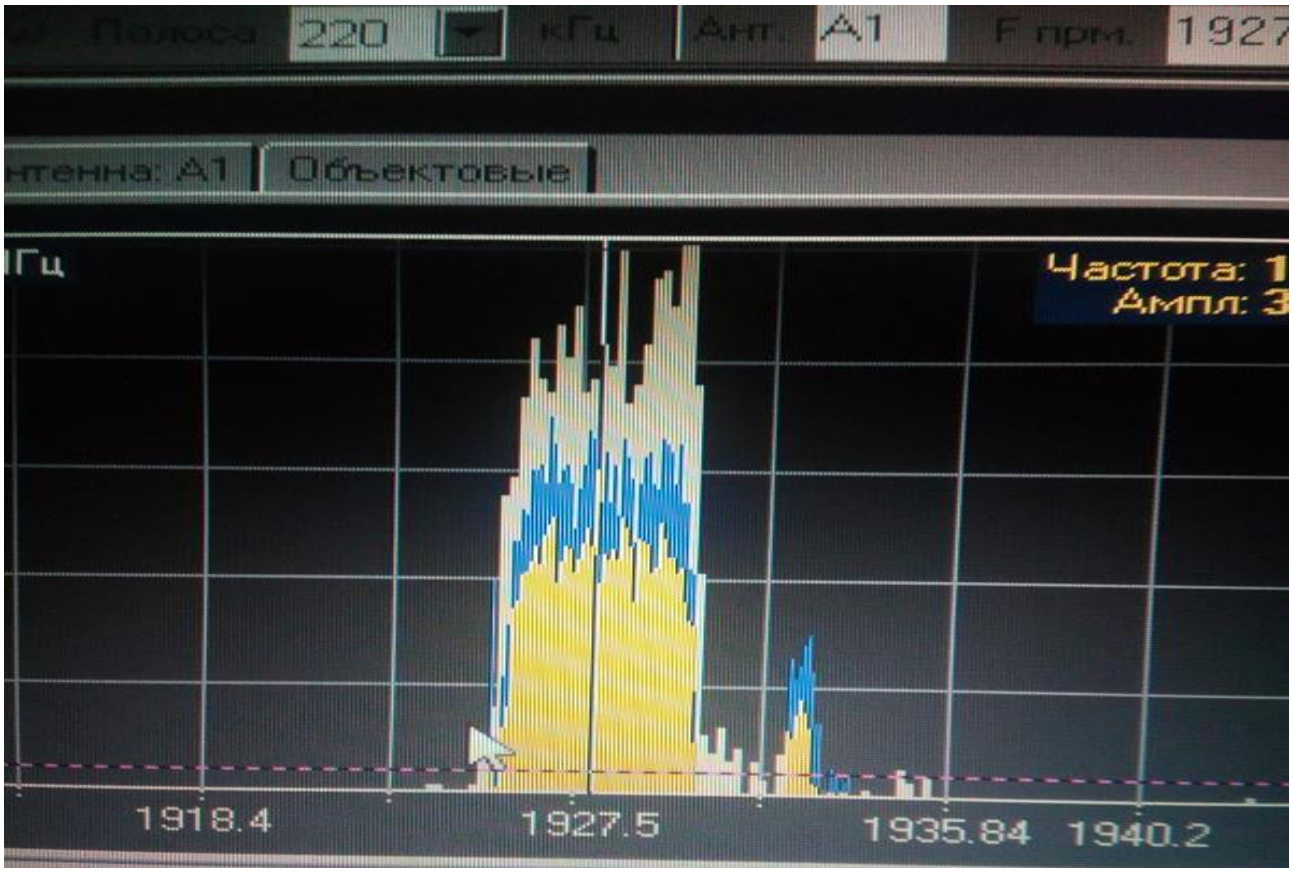

Рис. 2. Спектр сигналів діапазону базових станцій GSM2

З рис. 1 та рис. 2 видно, що виявити та розпізнати сигнал який не належить до легальних сингалів неможливо. Якщо аналоговий сигнал можливо виявити за речовим відгуком, встановити сканер на частоту та отримати речовий відгук, то цифровий сигнал так виявить неможливо, тому що він закодований. Тому, при отримані речового дискретного сигналу, неможливо здійснити його розпізнання при виконанні робіт по пошуку ЗНОІ. Закодований цифровій сигнал розпізнати можливо однак це потребує багато обчислювальних ресурсів та часу якого при пошуку ЗНОІ не вистачить.

Отже, сканування цифрового радіапазону не дозволить остаточно виявити, а тім більш розпізнати сигнал ЗНОІ.

Якщо брати до уваги, що ринок зараз наповнюється високоякісними міні диктофонами з вбудованим Wi-Fi передавачем, який поєднує в собі диктофон та передатчик Wi-Fi, то завантаження добового аудіо спостереження, при якісному Wi-Fi з'єднанні, займає всього декілька хвилин. Беручи до уваги, що у комплекті з Micro Wi-Fi диктофоном «MicroWi» поставляється міні маршрутизатор. Диктофон можна конфігурувати таким чином, щоб він автоматично виявляв мережу міні маршрутизатора, підключався до неї і виробляв завантаження аудіозаписей. В такому режимі, оператору досить наблизитися з ноутбуком з підключеним маршрутизатором на відстань дії мережі Wi-Fi (до 50 метрів в приміщеннях), щоб завантажити всю накопичену інформацію. Виявити цій пристрій дуже складно.

У зв’язку з тім, що зовсім не виявлених передавачів Wi-Fi не існує, тому даний пристрій у момент передачі виявити можливо, також можливо виявити його по побічному електромагнітному випромінюванню (далі – ПЕМВ),коли він працює у режимі запису. Однак по цей ознаки його навряд чи зможуть ідентифікувати більшість фахівців з радіоконтролю.

Отже, виявити пристрій найбільш ймовірно саме у момент передачі накопиченої інформації по мережі Wi-Fi.

Після тестування даного диктофона в реальних умовах можна підтвердити основні ТТХ та відмітити такі особливості:

1. Диктофон може бути виявлено в мережі як точка доступу, причому SSID (SSID - англ. Service Set Identifier - унікальне найменування безпроводової мережі, що відрізняє одну мережу Wi-Fi від іншої. У налаштуваннях всіх пристроїв, які повинні працювати в одній безпроводовій мережі, повинен бути зазначений однаковий SSID) можливо привласнювати будь-яке ім‘я.

2. Передача півгодинної записи розмови здійснюється за 30 секунд

Це дуже важливий сигнал щодо необхідності повного перегляду концепції моніторингу мереж Wi-Fi. Постійний і безперервний у часі аналіз мереж Wi-Fi тепер стає актуальним, як і постійний радіомоніторинг на об'єктах з наявністю інформації обмеженого доступу.

На нашу думку, велику загрозу уявляють також Wi-Fi-камери. В якості прикладу, розглянемо доступну модель Defender MULTICAM WF-10HD. Достатньо розглянути її ТТХ, щоб зрозуміти, що для досвідченого зловмисника цей пристрій цілком може стати суттєвою проблемою для фахівців із захисту інформації. Прикладом може бути налагодження з можливістю доступу до камери з будь-якої точки світу через спеціалізований ресурс. В даному випадку головним є можливість підключення камери до мережі Інтернет, що на теперішній час не є складністю. Модифіковані зразки такого типу відеокамер можуть робити за аналогією приведеного вище диктофону, тобто використовувати передачу по Wi-Fi у ближньому полі.

Проблема виявлення таких ЗНОІ виникає виходячи з можливостей сучасних аналізаторів Wi-Fi, які зазвичай використовуються пошуковими бригадами при проведенні пошукових заходів і моніторингу контрольованих об'єктів. Більшість гарних аналізаторів мають досить великі габарити і прив'язані до комп'ютера. Якщо зазначений і існує, то в кращому випадку він розміщений на посту контролю, який може бути значно віддалений від контрольованого приміщення, де зазвичай немає можливості встановити окремий аналізатор.

На підставі вищевикладеного, а також аналізу нових загроз можна сформувати методику пошуку за допомогою нового автоматизованого програмного комплексу (АПК) аналізу мереж Wi-Fi. Для виявлення цифрових ЗНОІ необхідно:

1. Неперервно (цілодобово) за допомогою АПК, контролювати мережі Wi-Fi всіх стандартів (IEEE 802.11 a/b/g/n), з прив'язкою всіх вимірювань на часі.

2. Пошукові модулі АПК повинні бути розміщені, безпосередньо в контрольованих приміщеннях (без необхідності установки в приміщенні додаткових ПК) та пов'язаних в єдину мережу.

3. Оператор повинен здійснювати пошукові роботи-мобільно, без необхідності підключення до ПК, накопичений архів даних повинен зберігатися тривалий час.

4. АПК повинен вести список легальних MAC-адрес для швидкого виявлення та ідентифікації нових передавачів Wi-Fi, та виявляти усі MAC адреси усіх приладів.

5. Для остаточного виявлення та локалізації цифрових ЗНОІ оператору потрібно мати легкий, мобільний та економічний приймальний пеленгаційний модуль. Цей модуль потрібен для вирішення оперативних завдань.

Для постійного ведення роботи з протидії незаконним методам отримання інформації необхідна наявність мережевого програмного забезпечення, підтримка зонального розміщення необхідної кількості пошукових модулів які будуть виконувати задачі по пошуку цифрових ЗНОІ на постійній основі.

З метою підтвердження вищевикладеного нами було проведено натурне моделювання пошук ЗНОІ у цифровому діапазоні. Автор використав мережеве програмне забезпечення, встановили імітатори сканерів (точки доступу Wi-Fi які були переведені у режим сканування) у приміщенні (рис. 4).

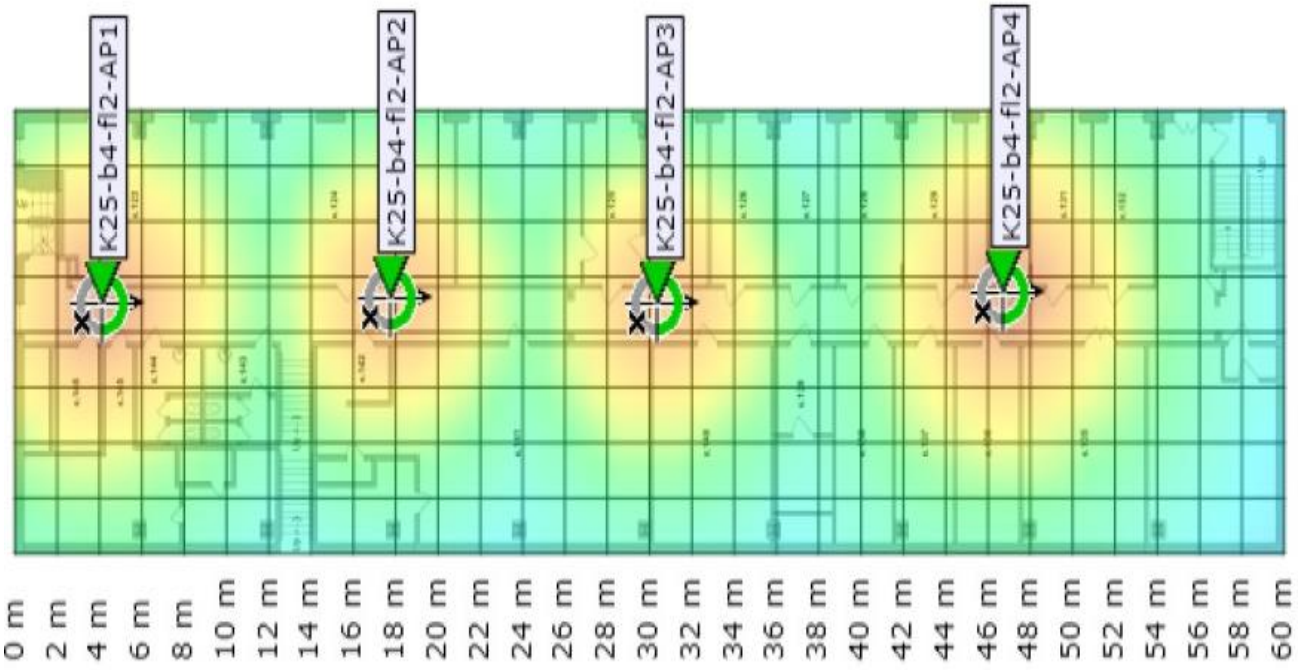

Рис. 4. Приміщення з розташованими точками сканування

Далі було встановлено нештатний пристрій Wi-Fi, на рис.5 приведено реальна робота нашої методики та програмного засобу виявлення, розпізнання та локалізації імітатора ЗНОІ.

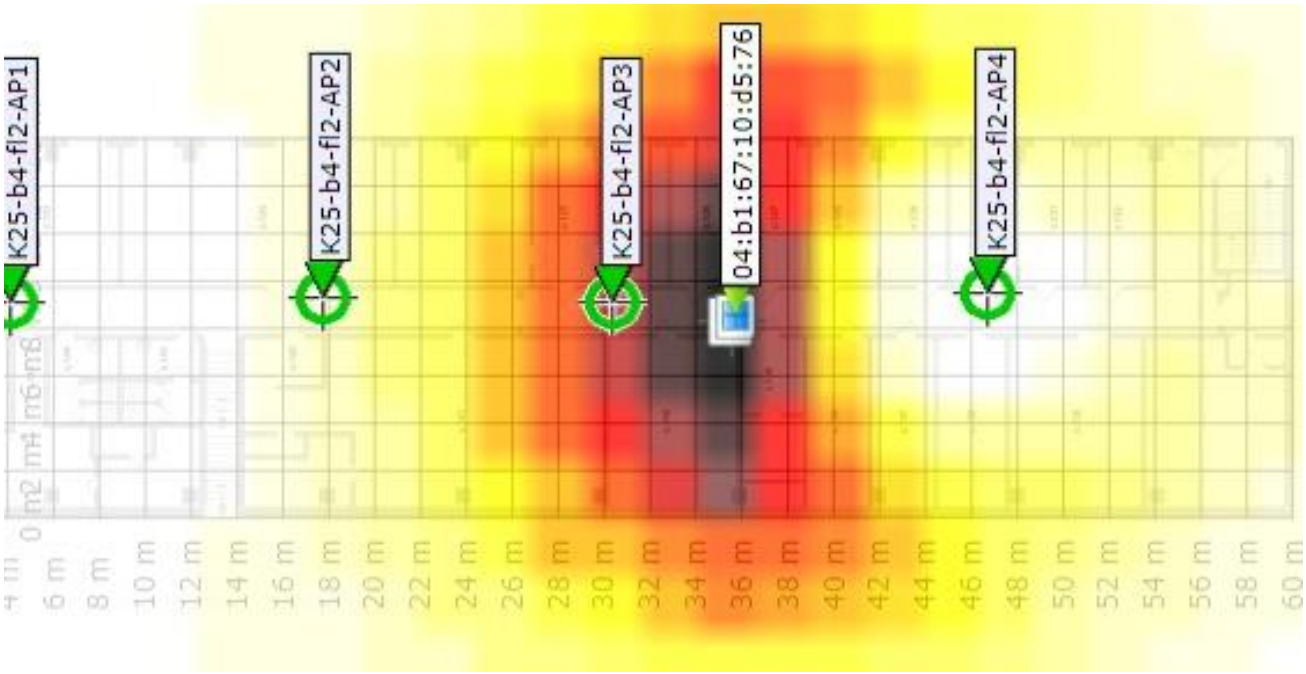

Рис. 5. Діаграма виявлення імітатора ЗНОІ з використанням запропонованій методиці

На рис. 5 темним кольором позначено місце локалізації імітатора ЗНОІ.

Таким чином, отримані результати які цілком підтверджують запропоновану нами методику пошуку ЗНОІ у цифровому діапазоні.

Саме таким чином, згідно з запропонованою методикою та за допомогою нових розроблених АПК, які можуть виконувати ці завдання, можливо виявити та локалізувати цифрові ЗНОІ, що працюють під прикриттям легального частотного діапазону Wi-Fi.

Напрямки подальших досліджень

Подальші дослідження доцільно спрямувати на удосконалення програмних засобів для автоматизованого програмного комплексу, з метою можливості автоматизованого розпізнавання та локалізації ЗНОІ, що працюють у комп'ютерної мережі, мережі Bluetooth та DECT приватного підприємства чи державної установи

Висновки

Проведений аналіз частотного діапазону Wi-Fi, показав найбільшу завантаженість, різними приладами та пристроями, цього частотного діапазону. У перспективі ці прилади будуть тики розвиватися, та ще більш завантажити цей частотний діапазон.

Оглянуті найбільш ймовірні по застосуванню, засоби негласного отримання інформації , які працюють у цифровому діапазоні частот, одним з яких є діапазон частот Wi-Fi.

Приведено реальні спектрограми та проведено натурне модулювання визначення, розпізнавання та локалізації ЗНОІ що працює діапазону Wi-Fi. Отримані результати (теоретичні та практичні) цілком підтверджують розроблену нами методику пошуку ЗНОІ, що працюють у цифровому діапазоні.

Список використаної літератури

1. Постанова Кабінету Міністрів України від 14 травня 2015 р. № 295 «Про внесення змін до Плану використання радіочастотного ресурсу України».

2. IEEE Standard for Information technology — Telecommunications and information exchange between systems. Local and metropolitan area networks. Specific requirements. Part 11: Wireless LAN Medium Access Control and Physical Layer (PHY) Specifications.

3. Захаров А.В. Требования к перспективному анализатору сетей Wi-Fi [Електронний ресурс]Режим доступу: http://www.analitika.info/stati3.php?page=1&full=block_article241 (25.05.2019).

4. Ананский Е.В.что такое радиозакладки и как их обнаружить? (часть2)/журнал «Служба безопасности» [Электронный ресурс] режим доступ: http://www.kvirin.com/articles/267/

5. Власов А. Беспроводные офисная связь: DECT и Wi-Fi. [Электронный ресурс]. — Режим доступа: http://www.dect.ru/dect.html (05.05.2016)

6. Поисковые комплексы . [Электронный ресурс]. https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (03.05.2019)

7. Лаптєв О.А. Грозовський Р.І. Аналіз та тенденції розвитку засобів пошуку цифрових радіозакладок //Сучасні інформаційні технології у сфері безпеки та оборони: науковий журнал, К.: УНО України імені Івана Черняховського, (2)35,2019, С 35-41.

8. Лаптєв О. А., Федоренко Р. М., Берестов Д. С. Удосконалення методики пошуку цифрових радіозакладок в діапазоні Wi-Fi //, Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, №2(66),2019., С102-107.

9. Барабаш О.В., Лаптєв О.А., Мусієнко А.П., Собчук В.В. Методика виявлення несанкціонованого доступу до інформаційній системи підприємства у цифровому діапазоне // Науково-практичний журнал «Зв'язок». К.: ДУТ,2019. №7(137), С.45-52.

Надійшла: 30.05.2019 Рецензент: д.т.н., проф. Вишнівський В.В.