УДК 004.056

Лаптєв О. А., канд. техн. наук, ст. наук. співроб.[1] **(ORCID : 0000-0002-4194-402X);**
Федоренко Р. М., канд. екон. наук[2] **(ORCID: 0000-0003-2929-3495);**
Берестов Д. С., канд. техн. наук[3] **(ORCID 0000-0002-3918-2978)**

[1] - Державний університет телекомунікацій, Київ;
[2] - Київський національний університет імені Тараса Шевченка, Київ;
[3] – Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського, Київ

Удосконалення методики пошуку цифрових радіо закладок в діапазоні Wi-Fi

Резюме. Проведено аналіз частотного діапазону Wi-Fi щодо завантаженості різноманітними приладами та пристроями. Наведено удосконалену методику пошуку цифрових засобів негласного отримання інформації в діапазоні Wi-Fi, яка дає змогу, крім 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.

Ключові слова: діапазон Wi-Fi; диктофон; засоби негласного отримання інформації; радіочастотний спектр; Wi-Fi-камери; MAC-адреса.

Постановка проблеми. З огляду на 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 момент 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, що працюють в міжнародному неліцензованому діапазоні частот (ISM) 2,4 ГГц і 5 ГГц. [2] Основною перевагою Wi-Fi перед іншими технологіями є висока швидкість передачі (до 1300 Мбіт/с). Області застосування цієї технології пов’язані з мережами для виходу в Інтернет, бездротовою передачею аудіо- та відеоінформації, войсковою телеметрією, контролю доступу до військових об’єктів, локальними бездротовими мережами.

Командування Армії США вирішило перевести всі свої командні пункти у всьому світі з провідних мереж на бездротовий зв’язок стандарту IEEE 802.11, або інакше Wi-Fi. Це робиться тому, що за оцінкою військових, використання бездротових роутерів дасть змогу приєднати більшість обчислювальних систем до мережі протягом декількох хвилин з початку розгортання командного пункту, що дає змогу отримати значну перевагу під час ведення військових дій. До того ж виникає актуальне завдання щодо захисту та запобігання витоку інформації у діапазоні Wi-Fi. З огляду на викладене, проблема пошуку радіозакладок у діапазоні Wi-Fi, для запобігання витоку інформації є актуальною.

Майже всі бездротові відеокамери, які встановлені для контроля військових об’єктів, використовують Wi-Fi. Також ця технологія використовується для організації локальних мереж між будівлями та промисловими об’єктами. Слід підкреслити, що діапазон Wi-Fi 5 ГГц є найкращим для організації промислових локальних мереж за наявності перешкод високого рівня.

На сьогодні важко знайти іншу таку активно використовувану ділянку радіочастотного спектра як 2,4 ГГц. У цьому діапазоні працюють пристрої стандартів Wi-Fi, системи дистанційного керування безпілотними літальними апаратами, аналогові та цифрові відеопередавачі, системи контролю доступу до військових об’єктів, сучасні командні пункти та багато іншого. Природно, що чим більше використовуваною є ділянка радіочастотного спектра, тим складніше її контролювати і аналізувати. Ця обставина часто є вирішальною під час вибору зловмисниками середовища для варіанта маскування роботи своїх *засобів негласного отримання інформації* (ЗНОІ), призначених для перехоплення інформації обмеженого доступу. Зважаючи на викладене

пошук ЗНОІ в діапазоні роботи Wi-Fi є особливо важливим, а розроблення методики пошуку таких ЗНОІ є актуальним завданням.

Аналіз останніх досліджень і публікацій. Завданням пошуку засобів негласного знімання інформації присвячена значна кількість публікацій. У роботі [4] розглядаються питання аналізу систем радіоконтролю (радіомоніторингу) з різними технічними параметрами, які об'єднує те, що вони можуть тільки показувати та (у кращому разі) зберігати панорами спектрів сигналів у радіоефірі. Завдання аналізу цифрових легальних каналів зв'язку вони не вирішують взагалі.

У [6] розглядається Wi-Fi, який застосовується в різних бездротових телеметричних системах на транспорті. Діапазон Wi-Fi 5 ГГц є найкращим для організації промислових локальних мереж за наявності перешкод високого рівня. Доведено що "класичним" методом пошуку цей частотний діапазон проаналізувати неможливо. Тобто для пошуку ЗНОІ, потрібні інші методи.

У [8] розглядається комплекс радіомоніторингу "Delta", якій продовжує лінійку самих передових і технологічних рішень в області радіомоніторингу. Комплекс надає широкі можливості з виявлення та ідентифікації джерел сигналів. Недоліком його можливо вважати відсутність можливості ідентифікування ЗНОІ та автоматичної їх локалізації.

З аналізу сучасної літератури можна дійти висновку, що універсальних пристроїв (приладів, програмних комплексів) для аналізу цифрових пакетів щодо завдань пошукового радіоконтролю зараз практично немає. Отже задача виявлення ЗНОІ, що працюють у діапазоні Wi-F, є актуальною.

Мета статті - на основі аналізу частотного діапазону Wi-Fi та реальних спектрограм, визначити ознаки виявлення ЗНОІ та удосконалити методику пошуку цифрових ЗНОІ, що працюють у діапазоні Wi-Fi.

Виклад основного матеріалу. Використовуючи для роботи ЗНОІ сильно завантажені частотні діапазони, зловмисник має намір максимально ускладнити їх виявлення, розумно використовуючи для цього загальноприйняті та поширені в цих діапазонах стандарти зв'язку. Для діапазону Wi-Fi це істотно спрощує виробництво ЗНОІ, оскільки використовуються поширені, доступні та недорогі компоненти (електронні радіодеталі та модулі) і добре відпрацьовані інженерні рішення.

Але найголовніше – важко відрізнити один від одного роботу двох пристроїв, що використовують однаковий цифровий стандарт зв'язку, без виявлення їх унікальних ідентифікаторів (ID). У випадку з Wi-Fi таким ідентифікатором є MAC-адреса або LLC. У цій статті не розглядається питання безпеки легальних мереж Wi-Fi. Розглянемо використання технології Wi-Fi, яка використовується в основі виготовлення ЗНОІ, та вимоги, які необхідно пред'являти до сучасних засобів аналізу мереж Wi-Fi щодо області пошуку і локалізації ЗНОІ для запобігання витоку інформації по частотному радіоканалу Wi-Fi.

Розглянемо високоякісний мінідиктофон з вбудованим Wi-Fi передавачем, який поєднує в собі диктофон і передатчик Wi-Fi (рис. 1) та модуль Wi-Fi GEM-atom (рис. 2), як приклад використання ЗНОІ, що здійснюють передачу інформації в діапазоні частот Wi-Fi. Дані про ці пристрої на сайті фірми Acustek Ltd [3]. Wi-Fi диктофон Micro Wi-Fi – унікальний пристрій для прихованого аудіоспостереження, що сполучає переваги і позбавлене недоліків диктофонів і радіопередавачів. На відміну від звичайних диктофонів, для прочитання записів з MicroWi-Fi диктофона з Wi-Fi передавачем не потрібен фізичний доступ до диктофона. Диктофону з Wi-Fi передавачем достатньо декілька хвилин на день роботи радіо, щоб передати записану інформацію. Тому такий диктофон складно виявити як детектором поля, так і системами радіомоніторінгу. Розміри Wi-Fi диктофона не перевищують двох складених разом запальничок.

Wi-Fi диктофон підтримує змінні Micro SD-карти. Підтримуваний обсяг пам'яті дає змогу вести запис протягом 300 годин. Вбудований акумулятор забезпечує диктофону до 120 годин автономної роботи. Завантаження добового аудіоспостереження під час якісного Wi-Fi з'єднання займає всього декілька хвилин. У комплекті з Micro Wi-Fi-диктофоном поставляється мінімаршрутизатор. Wi-Fi-диктофон можна конфігурувати у так, щоб він автоматично виявляв мережу мінімаршрутізатора, підключався до неї і виробляв завантаження аудіозаписей. У такому режимі, оператору досить наблизитися з ноутбуком із підключеним маршрутизатором на відстань дії мережі Wi-Fi (до 50 метрів у приміщеннях), щоб завантажити всю накопичену інформацію. Диктофон також можна налаштувати для роботи в звичайній

(наприклад, офісній) мережі Wi-Fi. У такому разі, Micro Wi-Fi може завантажувати на віддалений комп'ютер накопичену аудіоінформацію за графіком користувача.

Рис. 1. Диктофон MicroWi-Fi

Рис. 2. Модуль Wi-Fi GEM-atom

З огляду на викладене можна виділити основні особливості засобів негласного отримання інформації в діапазоні Wi-Fi:

можливість цифрового аудіозапису зі збереженням на micro SD-карту;

стандартний розмір диктофона - сірникова коробка;

вбудований мікрофон дає змогу вести запис на відстані до 10 м;

наявність входу для підключення зовнішнього мікрофона;

наявність режимів активації запису за графіком і по голосу;

автономна робота на одній зарядці акумулятора - до 120 годин;

віддалене управління і пересилання записів, використовуючи з'єднання Wi-Fi;

завантаження 24 годин запису займає всього близько 5 хвилин;

використання гнучкого графіку включення/вимикання Wi-Fi-передавача;

можливість аудіомоніторингу в режимі реального часу через з'єднання Wi-Fi;

можливість автоматичного розпізнавання і завантаження записів під час появи в зоні дії (до 50 м) мобільної точки доступу;

можливість підключення до будь-якої стаціонарної точки доступу Wi-Fi.

Засоби негласного отримання інформації можна знайти в момент передачі даних, проте в режимі тільки запису виявити такий диктофон за допомогою засобів радіоконтролю важко, його *побічне електромагнітне випромінювання* (ПЕМВ) навряд чи зможуть ідентифікувати більшість фахівців з радіоконтролю. Нижче наведено приклад ПЕМВ досліджуваного диктофона в режимі запису, який можна виявити тільки на дуже чутливій апаратурі та на відстані декількох сантиметрів (рис. 3). Спектр ПЕМВ зафіксовано за допомогою комплексу радіоконтролю і цифрового аналізу сигналів "Кассандра-К21" [6].

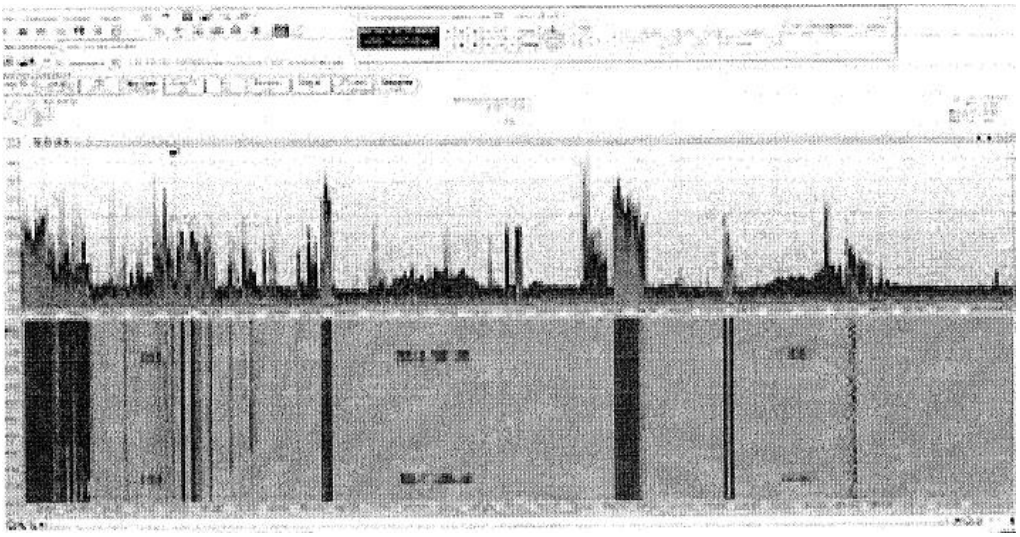

Рис. 3. Побічне електромагнітне випромінювання диктофону в режимі тільки запису

Отже виявити пристрій найімовірніше саме в момент передачі накопиченої інформації по мережі Wi-Fi (передача півгодинної записи розмови здійснюється за 30 секунд (рис. 4) [3]). Диктофон може бути виявлено в мережі як точка доступу, причому унікальному ідентифікатору бездротової мережі (SSID англ. Service Set Identifier) можливо привласнити будь-яке ім'я. Після тестування цього диктофона в реальних умовах можна визначити його основні ТТХ.

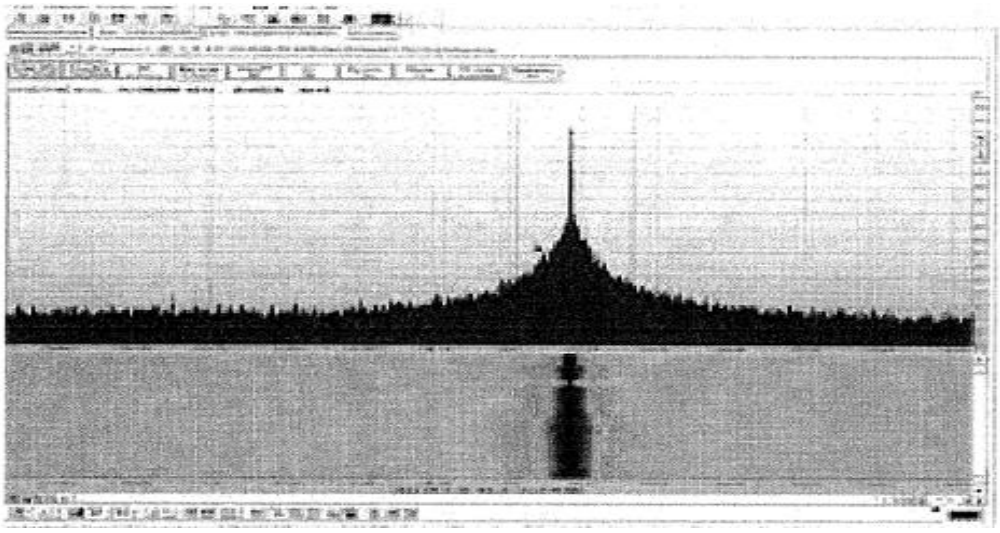

Рис. 4. Фіксація передачі запису інформації диктофоном Wi-Fi

Унікальний ідентифікатор бездротової мережі (SSID) – 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 радіомоніторинг на об'єктах з наявністю інформації обмеженого доступу.

Тепер для порівняння уявіть собі, наприклад, військовий заклад, військовий командний пункт або пункти управління, де встановлені кілька пов'язаних в загальну мережу точок доступу, що мають однаковий SSID. Нині на деяких об'єктах одночасно приймаються вже сотні пристроїв Wi-Fi (рис. 5).

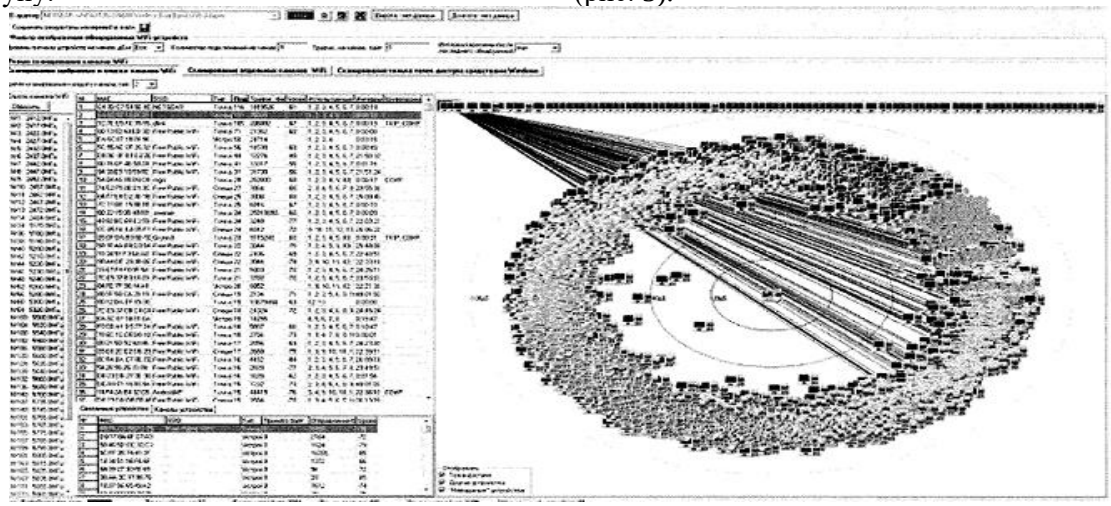

Рис. 5. Векторний аналіз пристроїв Wi-Fi великого офісного центру

На рис. 5 наведено результати векторного аналізу, який здійснено пошуковим комплексом в умовах реальної роботи учбового командного пункту.

У навчальному командному пункти проводились планові заходи щодо виявлення засобів негласного знімання інформації. Одним з пунктів пошукового заходу було визначення Wi-Fi пристроїв, що знаходяться в самому командному пункті, а також визначення загальної картини роботи Wi-Fi пристроїв у діапазоні роботи пошукового комплексу.

Кругова діаграма показує загальну картину роботи реальних пристроїв Wi-Fi у всіх приміщеннях, на всіх поверхах та найближчому оточенні командного пункту. Лінії вказують напрямки на пристрої Wi-Fi конкретного приміщення учбового командного пункту.

У таких умовах дуже важко помітити появу ще однієї точки доступу з тією ж назвою і таку, що має майже однаковий з іншими рівень сигналу. Без знання MAC-адрес всіх своїх пристроїв ніхто не в змозі зрозуміти легальність точки доступу.

На підставі викладеного та аналізу нових загроз можна сформувати удосконалену методику пошуку ЗНОІ та аналізу мереж Wi-Fi. Для виявлення цифрових радіозакладок необхідно:

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

2. Пошукові модулі MAC-адрес мають бути розміщені, безпосередньо в контрольованих приміщеннях (без необхідності установки в приміщенні додаткових ПК) та пов'язані в єдину мережу.

3. Аналіз має поводитися без необхідності підключення до ПК для зберігання архіву накопичених даних за тривалий час.

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

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

Для постійного ведення роботи з протидії засобам технічної розвідки необхідна наявність мультисерверного ПЗ, підтримка зонального розміщення великої кількості пошукових модулів (серверів), які виконуватимуть задачі з пошуку цифрових радіозакладок на постійній основі. Саме так, згідно із запропонованою методикою та за допомогою АПК, який може виконувати ці завдання, можливо виявити та локалізувати цифрові радіозакладки, що працюють під прикриттям частотного діапазону Wi-Fi, тобто виконувати роботи в області протидії засобам технічної розвідки.

Висновки

1. Проведено аналіз частотного діапазону Wi-Fi, який показав велику завантаженість різними приладами та пристроями, які в перспективі розвиватимуться і ще більш завантажувати цей частотний діапазон.

2. Розглянуто найімовірніші за застосуванням у приміщеннях командних пунктів пристрої знімання інформації, які працюють в діапазоні частот Wi-Fi.

3. Наведено реальні спектрограми та результати векторного аналізу ЗНОІ, що працює, діапазону Wi-Fi, виявлені найоптимальніші умови їх виявлення.

4. Удосконалено методику пошуку цифрових ЗНОІ, яка дає змогу виявляти цифрові радіо закладки, що працюють у діапазоні Wi-Fi для виключення витоку інформації з командного пункту у рамках протидії засобам технічної розвідки.

Подальші дослідження доцільно спрямувати на удосконалення ПЗ для АПК, для можливості автоматизованої локалізації пристроїв, що мають MAC-адреси, які не належать комп'ютерній мережі перевіреного приміщення.

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. Сайт фирмы Acustek Ltd https / [Електронний ресурс]- Режим доступу: //www.acustek.com/en (05.06.2019).
4. 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).
5. Ананский Е. В.что такое радиозакладки и как их обнаружить? (часть2)/журнал "Служба безопасности" [Электронный ресурс] режим доступ: http://www.kvirin.com/articles/267/.
6. А. В. Кривцун Использование новых возможностей комплекса радиомониторинга и цифрового анализа сигналов «Кассандра-М» для обнаружения современных специальных технических средств с передачей информации по радиоканалу [Электронный ресурс] /А. В. Кривцун А. В. Захаров режим доступа: http://www.inspectorsoft.ru/article.php?id=388 (24.05.2019).
7. Власов А. Беспроводные офисная связь: DECT и Wi-Fi. [Электронный ресурс]. - Режим доступа: http://www.dect.ru/dect.html (05.05.2016).
8. Поисковые комплексы. [Электронный ресурс]: https://www.das-ua.com/documents/catalog/search-appliances/search-complexes/page-01.php (03.05.2019).

Стаття надійшла до редакційної колегії 22.02.2019

Лаптев А. А., канд. техн. наук, ст. науч. сотрудник[1]**;**
Федоренко Р. Н., канд. экон. наук[2]**;**
Берестов Д. С., канд. техн. наук[3]

[1] – Государственный университет телекоммуникаций, Київ;
[2] – Киевский национальный университет имени Тараса Шевченко, Киев;
[3] – Центр военно-стратегических исследований Национального университета обороны Украины имени Ивана Черняховского, Киев

Усовершенствование методики поиска цифровых радиозакладок в диапазоне Wi-Fi

Резюме. Проведен анализ частотного диапазона Wi-Fi по загруженности различными приборами и устройствами. Приведена усовершенствованная методика поиска цифровых средств негласного получения информации в диапазоне Wi-Fi, которая позволяет, помимо классических методов поиска, дополнительно анализировать MAC-адреса устройств. Разработаны методические рекомендации по созданию современного программно-аппаратного комплекса анализа поиска средств негласного съема информации, которые работают под прикрытием радиочастотного диапазона сетей Wi-Fi.

Ключевые слова: диапазон Wi-Fi; диктофон; радиочастотный спектр; Wi-Fi-камеры; MAC-адрес.

O. Laptev, PhD (Technical), senior researcher[1]**;**
R. Fedorenko, Ph.D (Economic)[2]**;**
D. Berestov, Ph.D (Technical)[3]

[1] – State University of Telecommunications, Kyiv;
[2] –Taras Shevchenko National University of Kyiv, Kyiv;
[1] – Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Chernyhovskyi, Kyiv

Improvements in Wi-Fi digital radio bookmarks search

Resume. The Wi-Fi Frequency Band analysis of various types of devices and devices is carried out. The advanced method of searching digital means of the tacit reception of information in the Wi-Fi range is given, which allows, in addition to the classic search methods, to further analyze the MAC addresses of the means. The methodical recommendation for the creation of a modern software and hardware complex for the analysis of the search for tacit reception of information that works under cover of Wi-Fi networks is developed.

Keywords: Wi-Fi range; voice recorder; radio frequency spectrum; Wi-Fi camera; MAC address.