УДК 621.39
DOI: 10.31673/2409-7292.2022.040010

Воронін М.О.

МЕТОДИ ВИЯВЛЕННЯ РАДІОВИПРОМІНЮВАНЬ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Розглянуто загрозу перехоплення радіозакладними пристроями конфіденційної акустичної мовленнєвої інформації на об'єктах інформаційної діяльності та методи виявлення радіовипромінювань цих пристроїв за допомогою засобів радіоконтролю. Наводяться основні принципи побудови систем радіомоніторингу електромагнітних випромінювань, їх функціональні можливості, алгоритм методики виявлення активованих радіозакладних пристроїв.

Ключові слова: конфіденційна акустична інформація, перехоплення інформації, радіоканали витоку інформації, джерело радіовипромінювання, радіозакладні пристрої, радіомоніторинг.

Вступ

В умовах глобальної інформатизації суспільства реальна безпека держави багато в чому залежить від безпеки її інформаційних ресурсів і технологій. У загальній проблемі забезпечення безпеки інформації питання захисту конфіденційної інформації є одним із найважливіших. Це пояснюється, зокрема, тим, що частка конфіденційної інформації в загальному інформаційному потоці являє собою значну частину [3].

Захист національної конфіденційної інформації став одним із головних пріоритетів державної політики, у тому числі й у нашій країні. Важливим завданням на об'єктах інформаційної діяльності є забезпечення захисту конфіденційної акустичної інформації [4-5].

Одним з найбільш поширених технічних засобів, що використовуються для перехоплення конфіденційної акустичної інформації, є радіозакладні пристрої (РЗП), які використовують радіоканал, як середовище передачі небезпечних сигналів [7].

Основним місцем встановлення радіозакладних пристроїв є внутрішні приміщення як державних об'єктів і закладів, так і комерційних структур. Виявлення і вилучення цих пристроїв являє собою окрему і досить складну задачу в системі заходів захисту конфіденційної акустичної інформації [8].

Основна частина

Класифікацію радіоканалів витоку інформації за походженням, діапазоном випромінювання та середовищем поширення наведено на рис.1.

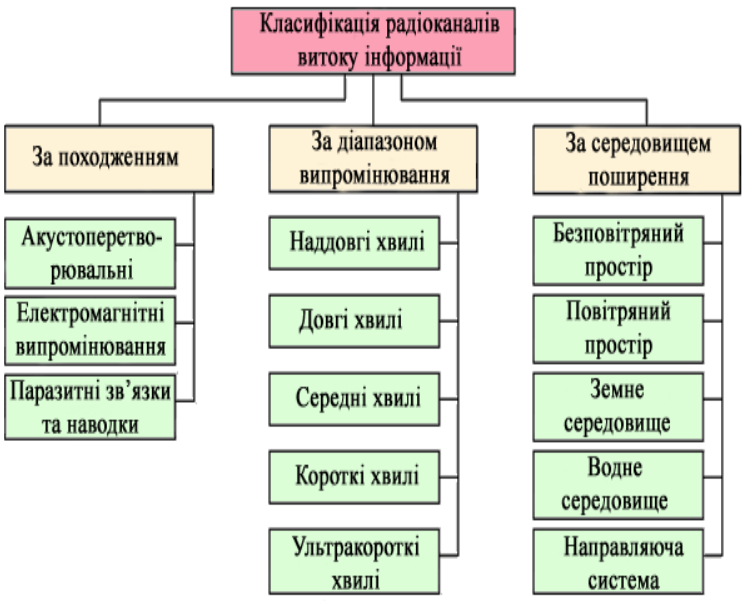

Рис.1 Класифікація радіоканалів витоку інформації

Існує велике різноманіття радіозакладних пристроїв. Це пояснюється, з одного боку, простотою та ефективністю використання таких пристроїв, а, з другого боку, постійним удосконаленням методів їх знешкодження.

Всі методи виявлення РЗП як джерел радіовипромінювання можна поділити на два підвиди, які доповнюють один одного.

Перший, найбільш ефективний – постійний ***радіомоніторинг електромагнітного спектру частот*** на об'єктах інформаційної діяльності. Метод полягає у постійній перевірці радіовипромінювань та виявленні нових складових у рисунку спектру (тобто, нових частот випромінювання), шляхом порівняння з попереднім. При появі у контрольованій області спектру нових частотних складових проводять пошук передавача. Для цього використовують спеціальні прилади та методи пошуку, які складають сутність другого підвиду.

Але якщо перший підвид вимагає, в разі появи нових спектральних складових, застосувати інший, то останній може бути використаний автономно. Це метод періодичних оглядів, який застосовується на об’єктах, де відсутня апаратура для постійного контролю [8].

Головним приладом, що входить до системи радіомоніторингу електромагнітного спектру частот, є скануючий приймач, наприклад, AR-2700, AR-3000A, AR-8000, AR-8200 або відповідні їм за технічними характеристиками. Найбільш досконалі серед них – сканери “AR-8200” та “AR-8600” [2]. Такі приймачі мають вихід на ПЕОМ (другий елемент системи), з якого за допомогою спеціальної програми (третій елемент системи) провадиться керування режимами роботи сканера. Сканер може перенастроюватися із заданим кроком дискретності по частоті. Він може працювати з сигналами, які мають різний вид модуляції та в різних смугах частот прослуховування (широкій та вузькій) на певній частоті, має індикацію режиму, і може працювати без підключення до ПЕОМ, що і використовується при пошуку РЗП.

Програма моніторингу побудована таким чином, що запам’ятовує спектр просканованої ділянки електромагнітного радіовипромінювання та використовує його як еталон при порівнянні з наступними вимірюваннями. Результати пошуку виводяться на монітор. В разі виявлення нових частотних складових у контрольованій зоні ПЕОМ видає сигнал тривоги. Система може працювати і в автоматичному режимі [8].

Зараз багатьма фірмами розроблено декілька таких програм. Принцип їх побудови однаковий, хоча вони можуть бути різними за вартістю і точністю роботи.

Зараз подібні програми розроблені й в Україні. Це програма “DigiScoun”, яку слід відмітити серед багатьох програм, розроблених для автоматичного сканування електромагнітного радіовипромінювання.

Робота комплексу з цією програмою побудована за принципом порівняння параметрів акустичних сигналів і працює таким чином:

1. На першому етапі вимірюється та запам’ятовується спектр радіосигналів по всьому діапазону роботи сканера. Одночасно встановлюється вид модуляції для кожного сигналу, випромінювання якого зафіксовано.

2. На другому етапі на кожній з виявлених частот комплекс випромінює у повітря декілька складних акустичних сигналів, які сприймаються ним через коло зворотного зв’язку, а саме – через радіоканал (приймач сканера) на тій частоті, що перевіряється. Якщо в приміщенні є РЗП, то параметри сигналу, продетектованого з радіо випромінювання, співпадуть з параметрами сигналу, що випромінювався у оточуючий простір приміщення. Для забезпечення однозначності сигналів, що сприймаються радіозакладним пристроєм, в сигнал, що випромінюється комплексом, додається акустичний сигнал з приміщення (шум, розмови тощо) через коло зворотного зв’язку (мікрофон, підсилювач та змішувач сигналів) [10].

Серед сучасних вітчизняних автоматизованих комплексів виявлення електромагнітних випромінювань слід відзначити комплекси “АКОР” та РІАС-РДм “DigiScan EX” [10].

Особливість цих комплексів полягає у тому, що вони, по-перше, здатні виявляти наявність радіозакладних пристроїв з шумоподібною та випадковою несучою і, по-друге, локалізувати місце знаходження РЗП. Для цього у комплекси введено ряд додаткових пристроїв та програм. Крім того, такі комплекси використовуються для перевірки відповідності рівня захисту об'єкту технічним вимогам та надійності блокування каналів витоку акустичної інформації. Ці комплекси розроблені в Україні та пройшли відповідну атестацію. Вони є офіційними приладами захисту інформації у нашій країні.

На рис.2 показано зовнішній вигляд та інтерфейс апаратно-програмного комплексу PIAC-РДм "DigiScan EX", на рис.3 – "АКОР".

Рис. 2 Зовнішній вигляд та інтерфейс апаратно-програмного комплексу PIAC-РДм "DigiScan EX"

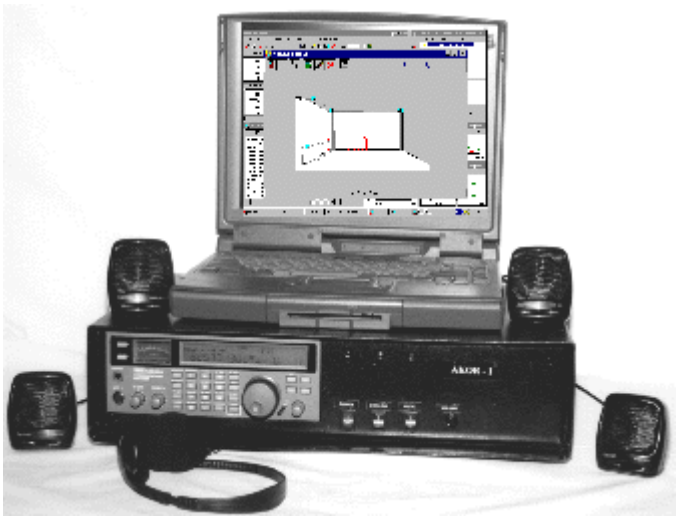

Рис. 3 Зовнішній вигляд та інтерфейс апаратно-програмного комплексу "АКОР"

Крім того, при використанні додаткового конвертору наднизьких частот DS-LINE програма може виявляти підслуховувальні пристрої, що використовують кабельні комунікації для передавання ***звукової інформації*** з приміщення у діапазоні частот від 5 кГц до 2 МГц (мережа 220 В, телефонні кабелі, проводи сигналізації) [1].

Панорамні приймачі дозволяють контролювати великий спектр частот, причому робити це має або одночасно у всьому діапазоні, або переходячи від значення до значення за гранично малий інтервал часу. Можливості панорамних приймачів значною мірою

визначаються методом аналізу частотного діапазону [9]. Від нього повністю залежить і вид структурної схеми приймача. Розрізняють методи паралельного й послідовного аналізу спектра.

При паралельному аналізі всі сигнали, що перебувають у певній смузі частот, що називається смугою огляду, виявляються одночасно. Структурну схему такого приймача наведено на рис.4.

Тут ВЧ-фільтр *1* формує необхідну смугу огляду, у якій ведеться виявлення сигналів; змішувач *2* виконує лінійне перенесення спектра прийнятого випромінювання в низькочастотну область радіодіапазону; смугові фільтри *3* здійснюють частотний поділ сигналів. Вихідний підсилювач *4* забезпечує необхідний рівень сигналу, достатній для нормальної роботи аналізуючого пристрою *5*.

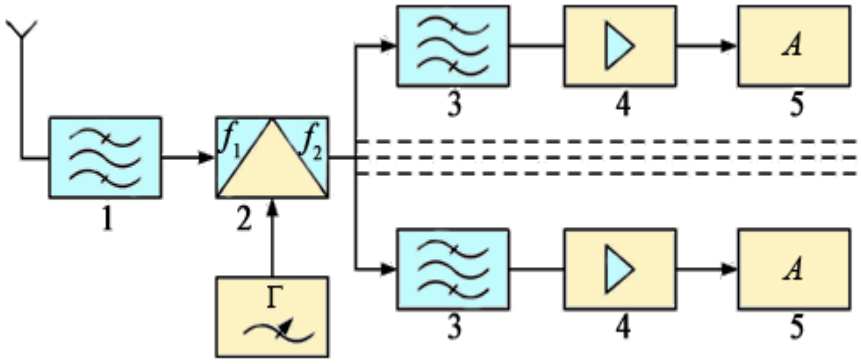

Рис. 4 Структурна схема панорамного приймального пристрою з паралельним аналізом спектра сигналів

У радіоприймачі послідовного аналізу, відповідно, здійснюється послідовна зміна частот в смузі огляду й виявлення сигналу. Спрощену структурну схему пристрою подібного типу показано на рис. 5.

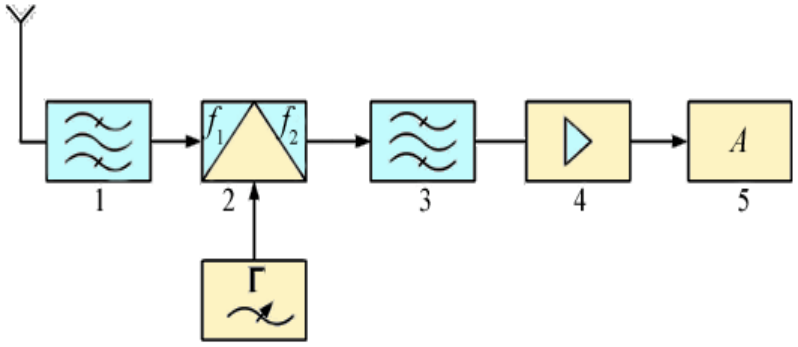

Рис. 5 Структурна схема панорамного радіоприймального пристрою з послідовним аналізом спектра сигналів

ВЧ-фільтр *1* має смугу пропускання, що дорівнює смузі огляду, а гетеродин *2* забезпечує перетворення приймача в заданій смузі. Проміжна частота – фіксована. Після селекції фільтром 3 і посилення підсилювачем *4* виявлений сигнал надходить у пристрій *5* для аналізу. При автоматичній зміні частоти приймач сканує частотний діапазон, звідси і його вживана назва – сканер. Термін не зовсім точний, але досить поширений.

Прикладами приймачів можуть служити AR-8000 і IC-PCR1000 [10].

Подальшим кроком на шляху вдосконалення процедури пошуку РЗП є застосування програмно-апаратних комплексів радіоконтролю й виявлення каналів витоку інформації,

оскільки їхні можливості значно ширші порівняно зі сканувальними приймачами. У найбільш загальному вигляді ці можливості полягають у наступному:

1. Виявлення випромінювань радіозакладних пристроїв.
2. Пелентування радіозакладних пристроїв у реальному часі.
3. Визначення дальності до джерел випромінювання.
4. Аналого-цифрова обробка сигналів з метою визначення їх приналежності до випромінювання радіозакладними пристроями.
5. Контроль силових, телефонних, радіотрансляційних та інших мереж.
6. Робота в режимі, що дозволяє обробляти кілька об'єктів одночасно.
7. Постановка прицільних завад на частотах випромінювання радіозакладних пристроїв тощо [8].

Блок-схему алгоритму методики виявлення радіозакладних пристроїв перехоплення акустичної мовленнєвої інформації на об'єктах інформаційної діяльності подано на рис. 6.

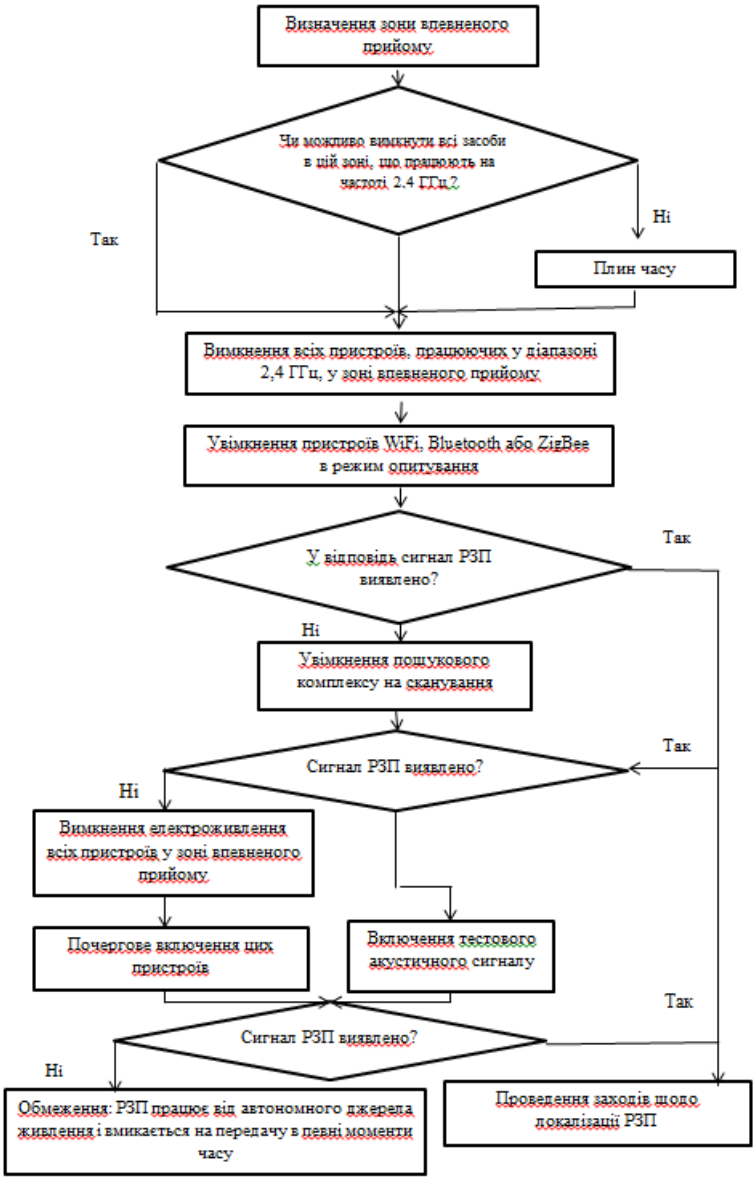

Рис. 6 Блок-схема алгоритму методики виявлення РЗП на об'єктах інформаційної діяльності

Ґрунтуючись на аналізі протоколів бездротового зв'язку, а також демаскуючих ознак пристроїв, побудованих на їх основі, були розроблені технічні заходи щодо виявлення пристроїв перехоплення акустичної мовленнєвої інформації, побудованих на базі засобів бездротового зв'язку, серед яких заходи щодо виявленню Wi-Fi, Bluetooth та ZigBee пристроїв. Технічні заходи спрямовані на те, щоб змусити РЗП відправити в радіоефір сигнал, яким оператор зможе виявити його пошуковим комплексом.

Висновки

Розглянута методика виявлення радіозакладних пристроїв на об’єктах інформаційної діяльності не є універсальною. Залежно від меж контрольованої зони, а також від типу пристрою, у методики існують обмеження, що роблять її непридатною для застосування в деяких випадках або застосовною, але з деякими застереженнями. Знання конструктивних особливостей та схемних рішень побудови закладних пристроїв дозволяє виявити їх сильні та слабкі сторони та вибрати оптимальні способи протидії.

Радіозакладні пристрої, які працюють від автономного джерела живлення та здійснюють передавання перехопленої інформації лише в заздалегідь налаштовані зловмисником моменти часу, можуть бути виявлені тільки випадково. Також, легальні пристрої, що функціонують у зоні впевненого прийому, і вимкнути які немає можливості, можуть завадити виявленню активованого радіозакладного пристрою.

Для гарантованого виявлення та ідентифікації небезпечних сигналів у конкретних ситуаціях потрібне чітке уявлення про моделі небезпечного сигналу, методи пошуку джерел поширення таких сигналів та обробки їх основних показників, а також методи виявлення можливих каналів витоку інформації.

Перелік посилань

1. Телекомунікаційні системи та мережі. Структура й основні функції. Том 1 Автори: Поповський В.В, Лемешко О.В.; Ковальчук В.К.; Плотніков М.Д.; Картушин Ю.П.; Попонін О.М.; Агєєв Д.В.; Сабурова С.О., Олійник В.Ф., Персиков А.В.; Лошаков В.А. Селіванов К.О. // https://ice.nure.ua/ua/books-and-tutorials/multymedijnyj-pidruchnyk-telekomunikatsijni-systemy-ta-merezhi-2/
2. Хорошко В. А., Чекатков А. А. “Методы и средства защиты информации” Юниор 2003г.
3. Закон України « Про державну таємницю».
4. Положення про технічний захист інформації в Україні. Затвердженно Указом Президента України від 27 вересня 1999 року № 1229
5. Закон України «Про основи національної безпеки України».
6. Закон України «Про інформацію».
7. Закон України «Про захист інформації в інормаційно-телекомунікаційних системах».
8. ДСТУ 3396.0-96.
9. ДСТУ 3396.1-96.
10. ДСТУ 3396.2-97.

Надійшла: 01.12.2022 Рецензент: д.т.н., професор Крючкова Л.П.