

[DOI 10.28925/2663-4023.2026.35.1459](https://doi.org/10.28925/2663-4023.2026.35.1459)

УДК 004.056:621.396

Опірський Іван Романович

доктор технічних наук, професор, завідувач кафедри «Захист інформації»

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0000-0002-8461-8996

ivan.r.opirskyi@lpnu.ua**Стефанків Артем Вікторович**

аспірант кафедри «Захист інформації»

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0009-0006-8851-8358

artem.v.stefankiv@lpnu.ua**Лобан Георгій Антонович**

аспірант кафедри «Захист інформації»

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0009-0003-4862-8729

heorhii.loban.asp.2025@lpnu.ua**Гимза Олександр Анатолійович**

студент кафедри «Захист інформації»

Національний університет «Львівська політехніка», Львів, Україна

ORCID: 0009-0009-7928-7545

oleksandr.hymza.mkbasp.2025@lpnu.ua**РОЗРОБКА КОНЦЕПЦІЇ ІНТЕГРОВАНОЇ СИСТЕМИ АКТИВНОГО ВИЯВЛЕННЯ
РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ЗА ДОПОМОГОЮ ЗГОРТКОВИХ НЕЙРОННИХ МЕРЕЖ ТА
SDR-ПРИЙМАЧІВ**

Анотація. Сучасні засоби радіочастотного виявлення закладних пристроїв переважно пасивні: вони фіксують появу нових випромінювань у спектрі, але не можуть спровокувати передавання пристроїв, що активуються за подією – голосом (VOX-активація), рухом чи за розкладом, а комерційні системи ідентифікації за радіочастотними відбитками (RFFI) не розкривають своїх алгоритмів. Метою статті є розробка концепції архітектури інтегрованої системи виявлення пристроїв на основі доступного обладнання, яка поєднує пасивну RFFI з модулями випромінювачів стимуляційних сигналів. Аналіз публікацій показав, що стимуляційний вплив та ідентифікація джерела відгуку досі розглядаються окремо. Запропоновано класифікацію цілей виявлення за доменами зібраної інформації та за поведінковими характеристиками (постійне передавання, внутрішня, зовнішня та часова активація), розглянуто особливості двох поколінь засобів радіочастотного виявлення. Розроблено апаратну архітектуру системи, що включає SDR-приймач із режимами огляду спектра та цільового захоплення I/Q-відліків, випромінювачі акустичних, ультразвукових, інфрачервоних і радіочастотних стимулів з інтерфейсним модулем фіксації міток часу та модуль антенного перемикача. Запропоновано процедуру обстеження, за якої стимули подаються за псевдовипадковим розкладом, а рішення ґрунтується на двох ознаках: кореляції моментів появи випромінювання з розкладом стимулів і невідповідності радіочастотного відбитка базі легітимних пристроїв. Програмну архітектуру побудовано на згортковій нейронній мережі, яка використовується як екстрактор ознак для класифікації на відкритому наборі. Імітаційне моделювання показало, що за шести стимулів пристрій із VOX-активацією виявляється з імовірністю 0,93 за імовірності хибної тривоги не більше 0,01 на сеанс тривалістю близько 2 хв за умови повторного огляду частоти не рідше ніж раз на 0,5 с, а захоплення сигналу, синхронізоване зі стимулом, підвищує якість ідентифікації аналогових передавачів (площа під ROC-кривою 0,75 проти 0,59 за відношення сигнал/шум 20 дБ). Водночас за досягнутої якості ідентифікації злиття ознак не зменшує кількості хибних тривог, тому підвищення надійності RFFI визначено ключовим напрямом подальших досліджень.



Ключові слова: виявлення закладних пристроїв; технічний захист інформації; радіочастотний моніторинг; ідентифікація за радіочастотними відбитками; SDR-приймач; VOX-активація; стимуляційні сигнали; згорткові нейронні мережі; класифікація на відкритому наборі.

ВСТУП

Постановка проблеми. Сучасні апаратно-програмні комплекси виявлення пристроїв переважно покладаються на моніторинг радіочастотного спектра з метою виявлення нових сигналів або визначення протоколів передавання даних. Системи з аналізом фізичних особливостей сигналу, такі як Acustek SigDNA, є закритими та використовують невідомі алгоритми і процедури. Додатково, існуючі комплекси є пасивними та не мають можливості створювати стимуляційні сигнали, наприклад, для виявлення пристроїв з активацією за голосом. Значна частина цільових пристроїв побудована за схемою активації, тобто передача даних не відбувається постійно. Джерелом активаційного сигналу може бути зовнішня команда, голосова активність або будь-яка інша активність в обстежуваному приміщенні.

Аналіз останніх досліджень і публікацій.

Проблема побудови інтегрованих систем виявлення пристроїв досліджується переважно в плані об'єднання декількох пристроїв різних категорій в один пристрій. Так, система виявлення акустичних закладних пристроїв, запропонована Самосуд [1], поєднує скануючий приймач, набір акустичних систем, імпульсний генератор, пристрій вимірювання затримок та індикаційну систему з метою виявлення точного розташування закладних пристроїв із голосовою активацією методом триангуляції за часовими затримками. За оцінкою авторки, запропонований комплекс демонструє ефективність не нижчу, ніж у комерційних аналогів, зокрема DigiScan EX, проте авторка дослідження залишає питання оптимізації експлуатаційних характеристик пристрою для подальших досліджень.

Близький підхід описано в праці Вороніна [2]: після формування переліку виявлених радіосигналів на кожній знайденій частоті система випромінює в приміщення складний акустичний тестовий сигнал і порівнює його з демодульованим радіосигналом, а збіг сигналів свідчить про наявність каналу витоку акустичної інформації. Проте, автор зазначає, що методика не є універсальною, оскільки пристрої з автономним живленням, які передають накопичену інформацію за розкладом, виявляються випадково, а легітимні випромінювання в зоні впевненого приймання ускладнюють аналіз. Клименко та ін. [3] запропонували загальну класифікацію засобів негласного отримання інформації, зокрема за способом активації (від голосу, руху, таймера чи дистанційної команди), та включили до підготовчого етапу обстеження вибір способів активації і тестових сигналів. Апаратна реалізація таких заходів у праці не розглядається.

Принцип керованого впливу на пристрій застосовують і в інших доменах. Конотопець та ін. [4] для виявлення оптико-електронних засобів запропонували двоканальну схему спостереження з повторною ініціалізацією пристрою шляхом керованої періодичної зміни світлового потоку та кореляцією з базою шумових характеристик сенсорів; експериментальної перевірки підходу в праці не наведено. Sami та ін. [5] реалізували активне виявлення прихованих камер за допомогою ToF-сенсора смартфона: лазерне випромінювання сенсора відбивається від лінзи камери, а злиття даних про відстань та інтенсивність відбиття з подальшою фільтрацією методами комп'ютерного зору забезпечило частку виявлення 88,9 % проти 46,0 % під час огляду неозброєним оком. Водночас метод має обмежене поле зору ($\pm 10^\circ$) і потребує ручного сканування оператором. Протилежний, суто пасивний підхід реалізовано в системі Ghostbuster [6], яка виявляє приховані радіоприймачі за витоком випромінювання їхнього гетеродина: на відстані до 5 м точність виявлення перевищує 95 %, однак система не відрізняє легітимний приймач від стороннього і потребує значних обчислювальних ресурсів.

Методи ідентифікації за радіочастотними відбитками (RFFI) систематизовано в оглядах Jagannath та ін. [7] і Liu та ін. [8]. Традиційні методи будують ознаки на основі модуляційних спотворень, статистичних характеристик сигналу, перехідних процесів увімкнення передавача чи вейвлет-перетворення, сучасні – використовують глибинне навчання (згорткові та рекурентні мережі, генеративно-змагальні мережі). Для методів на основі перехідних процесів наведено точність 99,9 % для 7 Bluetooth-пристроїв, 97,7 % для 8 пристроїв IEEE 802.11b і 100 % для 8 GSM-телефонів [7]. Водночас автори обох оглядів виокремлюють невирішені проблеми: залежність відбитка від приймача та каналу поширення, розпізнавання невідомих пристроїв (задача класифікації на відкритому наборі), стійкість до підробки сигналу та брак відкритих наборів даних. Слід зауважити, що більшість досліджень RFFI стосується стандартних протоколів (Wi-Fi, Bluetooth, LoRa, ADS-B), тоді як даних про аналогові або нестандартні передавачі, характерні для закладних пристроїв, у розглянутих джерелах немає.



Апаратні засоби широкосмугового моніторингу спектра розвиваються в напрямі перенесення первинної обробки на програмовані логічні інтегральні схеми (ПЛІС). Flak [9] реалізував на приймачі LimeSDR-USB апаратне обчислення спектральної густини потужності методом Велча та апаратне керування перестроюванням, що дало змогу досягти смуги аналізу в реальному часі до 96 МГц і швидкості огляду менше 1 мс на 1 ГГц у діапазоні 100 кГц – 3,6 ГГц. McTaggart та ін. [10] на платформі RFSoc побудували поліфазний каналізатор на 106 каналів шириною 3,84 МГц із розсиленням результатів за схемою «видавець-підписник» (ZeroMQ). Обидва рішення передають до блоку обробки лише оцінки потужності, тому для RFFI, якому потрібні I/Q-відліки, вони без доопрацювання непридатні. Ває та ін. [11] запропонували інший компроміс: детектор CA-CFAR у ПЛІС кожного приймача ADALM-PLUTO пересилає лише ті фрагменти I/Q-потоків, що містять сигнал, разом із метаданими (ідентифікатор приймача, частота, мітка часу). У випробуваннях із кабельним підключенням генератора за коефіцієнта заповнення 10 % обсяг даних зменшився на 88 %, а ймовірність виявлення становила 96,26 % за відношення сигнал/шум (ВСШ) близько 13 дБ. Саме такий принцип виявлення на рівні спектра, зі збереженням I/Q-відліків лише для виявлених подій, доцільно покласти в основу системи, що поєднує огляд спектра та RFFI.

Для локалізації джерел і злиття рішень від різномірних сенсорів важливими є праці Bhattacharya та ін. [12], де локалізацію передавача сформульовано як задачу перевірки гіпотез, а вибір підмножини сенсорів розв'язано жадібними алгоритмами з гарантованою точністю наближення (виграш до 50–60 % порівняно з базовими методами в моделюванні), та Svanström та ін. [13], де злиття рішень інфрачервоного, видимого та акустичного каналів за правилом зваженого голосування підвищило частку виявлень дрона з 67 % (найкращий окремий сенсор) до 78 % і усунило хибні спрацювання під час тестового прогону. Серед комерційних засобів найближчою до задачі ідентифікації пристроїв є платформа Acustek SigDNA [14], що заявляє про атрибуцію пристроїв за сигнатурою випромінювання, проте виробник не розкриває алгоритмів її роботи.

Підсумовуючи, відомі праці розглядають стимуляційний вплив і аналіз радіочастотного відгуку окремо. Системи зі стимуляцією [1, 2, 4, 5] аналізують відгук на енергетичному рівні або за змістом демодульованого сигналу і не ідентифікують його джерело, а методи RFFI [7, 8] і комерційні засоби [14] є пасивними та не впливають на поведінку пристроїв, що активуються за подією. Невирішеною залишається задача поєднання цих підходів в одній архітектурі, побудованій на доступному обладнанні.

Мета статті. Метою статті є розробка концепції архітектури системи виявлення пристроїв на основі доступного обладнання, зокрема SDR-приймачів та модулів випромінювачів стимуляційних сигналів.

ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Класифікація цілей виявлення. Для цілей радіочастотного виявлення доцільно використовувати класифікацію пристроїв за доменами зібраної інформації та за поведінковими характеристиками, які визначають часові шаблони передачі інформації за межі контрольованої зони.

За доменами зібраної інформації пристрої можна поділити на акустичні, видові та телекомунікаційні [3]. На додачу до запропонованих трьох видів доцільно ввести четвертий – змішаний. Пристрої змішаного типу поєднують збір і передачу декількох видів інформації одночасно. Наприклад, таким пристроєм може бути прихована відеокамера, яка одночасно передає як відеосигнал, так і акустичний сигнал.

За поведінковими характеристиками всі пристрої можна поділити на чотири категорії: з постійним передаванням, із внутрішньою активацією, із зовнішньою активацією та із часовою активацією.

Перший клас пристроїв є найпростішим і найлегшим для виявлення. Інформаційний сигнал випромінюється постійно, а тому його виявлення можливе навіть за допомогою засобів радіочастотного виявлення першого покоління. Енергоефективність пристроїв цього класу є мінімальною, тому час їхньої роботи є доволі невеликим (у разі батарейного живлення).

Другий клас пристроїв у переважній більшості складають акустичні закладні пристрої з активацією за голосом (VOX-активацією) та приховані відеокамери з сенсором руху. Передача в таких пристроях активується у разі перевищення встановленого порогового значення сигналу з мікрофона. Експлуатаційним недоліком таких пристроїв з точки зору особи, яка здійснює негласне зняття інформації, є втрата інформації безпосередньо в момент активації закладного пристрою.

Третій клас пристроїв функціонально є схожим на другий, проте активація передавання ініціюється не за допомогою внутрішнього правила, а оператором пристрою, що перебуває поза межами контрольованої зони.

Пристрої четвертого класу є найбільш складними з технічної точки зору, оскільки їхня конструкція передбачає наявність запам'ятовувального пристрою, годинникового генератора та мікропроцесора.

Активация таких пристроїв відбувається за встановленим графіком, а передаваний сигнал є доволі короткочасним і складається зі стиснених даних, записаних в інтервалі між активаціями. Саме короткочасність сигналу робить пристрої даного класу найскладнішими для виявлення, оскільки система радіочастотного виявлення може сканувати частотний діапазон, який відрізняється від частотного діапазону пристрою саме в момент передачі зібраної інформації.

Цільові пристрої виявлення можуть поєднувати ознаки кількох класів. Наприклад, акустичний закладний пристрій може одночасно працювати за активацією за голосом та мати засоби накопичення та високошвидкісної передачі, що робить його більш ефективним та малопомітним.

Часові шаблони передавання пристроїв кожного класу схематично показані на Рисунку 1. Для пристроїв II класу характерні затримка активації t_a , протягом якої інформація втрачається, та час утримання t_h , протягом якого передавач залишається увімкненим після зникнення сигналу активації. Для пристроїв IV класу ймовірність виявлення визначається збігом короткого сеансу передавання з вікном сканування на відповідній частоті, тому навіть повний цикл огляду діапазону не гарантує їхнього виявлення.

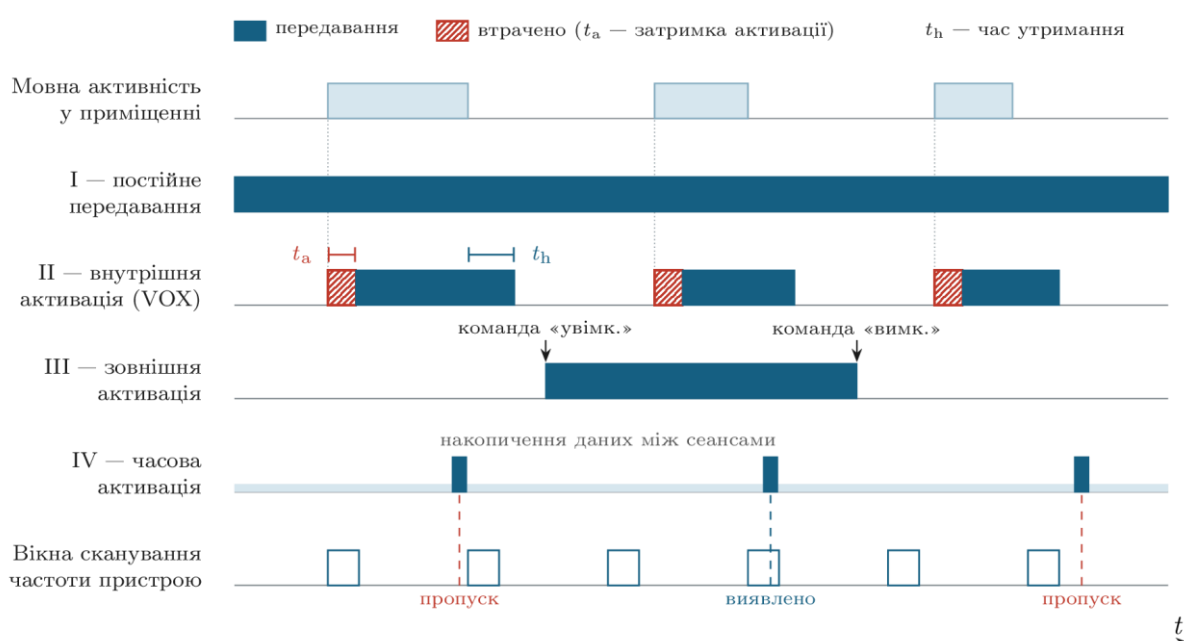


Рис. 1. Часові шаблони передавання пристроїв різних поведінкових класів (схематично).

Загальна архітектура засобів радіочастотного виявлення пристроїв.

В загальному випадку засоби радіочастотного виявлення пристроїв складаються з антено-фідерного пристрою, приймача та блоку обробки даних.

Антено-фідерний пристрій (далі – АФП) виконує функцію перетворення електромагнітних хвиль в просторі в електричний сигнал, придатний до подальшого аналізу. Характеристики АФП повинні відповідати характеристикам цільового сигналу – його частоті та потужності. Оскільки налаштування АФП під конкретні сигнали є витратним, переважно використовуються широкосмугові АФП, центральним компонентом яких є відповідна широкосмугова антена. Така антена забезпечує прийнятні показники узгодження на достатньо широкому діапазоні частот. Найбільш поширеними широкосмуговими антенами, які використовуються для цих видів задач, є біконічні, диско-конусні антени та їхні варіації.

Прийнятий за допомогою АФП електромагнітний сигнал подається на вхід приймача, який виконує його відбір, демодуляцію та перетворення в необхідний для аналізу формат. Сучасні системи використовують програмно визначені радіоприймачі (SDR-приймачі), в яких обробка сигналу максимально перенесена з апаратної площини в програмну, що значно підвищує гнучкість та якість роботи. Саме завдяки використанню SDR-приймачів стало можливим не тільки виявляти нові сигнали в часі, а й будувати вектори ознак цих сигналів з метою їх класифікації в просторі «свій-чужий», тобто реалізовувати технології ідентифікації за радіочастотними відбитками (RF Fingerprint Identification). Використання SDR-приймачів також збільшує швидкість сканування – розробник утиліти `hackrf_sweep` [15] заявляє про максимальну швидкість сканування до 8 ГГц/с на сумісних приймачах серії HackRF.



Блок обробки даних (переважно – персональний комп'ютер) виконує процеси обробки, візуалізації даних та взаємодії з оператором системи. Обчислювальні характеристики блоку обробки даних повинні забезпечувати достатню продуктивність під час обробки великих обсягів даних у реальному часі, зокрема під час ширококутового сканування зі встановленою частотою оновлення.

Покоління засобів радіочастотного виявлення пристроїв та їхні особливості.

Засоби виявлення пристроїв першого покоління використовують загальну архітектуру, описану в попередньому розділі, з можливими незначними варіаціями. Пристрої даного покоління розроблялися з середини 1980-х до 2000-х років, коли скануючі приймачі були витіснені більш компактними та технологічно досконалішими SDR-приймачами. Підключення приймача до блоку обробки даних у системах першого покоління відбувається окремими каналами керування (переважно - RS-232) та даних (звуковим каналом). В якості приймачів використовувалися ширококутові сканери, наприклад, AOR AR8200, Icom IC-PCR1500 та інші. Тривалість циклу сканування діапазону 50-3000 МГц в таких системах становить близько 20 хвилин у разі використання приймача AOR AR8200 та 7 хвилин для Icom IC-PCR1500 (на прикладі однієї з найбільш поширених систем першого покоління DigiScan EX [16]). Можливості систем першого покоління є доволі обмеженими порівняно з наступними: визначення нових пристроїв виконується на енергетичному рівні, а алгоритми ідентифікації є доволі базовими. Проте системи першого покоління забезпечували прийнятну точність виявлення протягом свого активного етапу розвитку.

Засоби виявлення пристроїв другого покоління почали активно розроблятися з популяризацією та здешевленням SDR-систем, таких як Ettus Research USRP, Great Scott Gadgets HackRF One, NI ADALM-PLUTO, LimeSDR та інші. Архітектурно, SDR-приймачі складаються з блоків приймального тракту, аналого-цифрового перетворювача та цифрового сигнального процесора (як правило, на основі програмованої логічної інтегральної схеми). Обробка сигналів при цьому переноситься з апаратного рівня за допомогою фільтрів та демодуляторів на програмний рівень. Передача даних у вигляді I/Q-відліків дозволяє програмному комплексу виконувати обробку сигналів у найбільш наближеному до реального вигляді, а також спрощує глибокий аналіз сигналів, зокрема методами машинного та глибинного навчання. Власне, засоби виявлення пристроїв другого покоління використовують більш просунуті методи аналізу сигналів, що дозволяють значно підвищити точність і швидкість виявлення. Найбільш відомим та просунутим представником засобів даного покоління є раніше згаданий Acustek SigDNA.

Платформа SigDNA [14] побудована на захищеному планшетному комп'ютері Durabook U11I і доповнена портативним пристроєм Vector для пошуку джерел на близькій відстані. За даними виробника, вона забезпечує ширококутове приймання з прямою оцифровкою радіосигналу в діапазоні 30 МГц – 11 ГГц, пасивний моніторинг мереж Wi-Fi (2,4, 5 і 6 ГГц, зокрема Wi-Fi 7), Bluetooth/BLE (включно з Bluetooth 6.0), стільникових мереж 2G–5G NR і протоколів IoT, ширококутовий огляд з автоматичною класифікацією сигналів, а також локалізацію джерел за кутом приходу з оцінкою відстані. Ключовою заявленою функцією є атрибуція на рівні пристрою - розпізнавання конкретного апаратного засобу за «сигнатурою передавання», зокрема за умов приховування або рандомізації MAC-адрес. Додатковий модуль Recall забезпечує безперервний запис радіообстановки для подальшого аналізу. Водночас виробник не розкриває ні ознак, ні алгоритмів атрибуції, ні показників точності, що унеможливує їхню незалежну перевірку. Крім того, система позиціонується як повністю пасивна, тобто не має засобів активації пристроїв, що передають інформацію лише за подією.

Стимуляційні сигнали та модулі.

З метою виявлення пристроїв класів II, III та комбінованих з ними класів II-IV та III-IV, пропонується використовувати стимуляційні сигнали. Такими сигналами, зокрема, можуть виступати звукові сигнали (для пристроїв акустичного домену), ультразвукове випромінювання (для пристроїв акустичного чи видового домену з активацією за допомогою ультразвукового сенсора руху), інфрачервоне випромінювання (для пристроїв акустичного та видового доменів з активацією за допомогою PIR-сенсора) або радіосигнали (для пристроїв усіх доменів з активацією за допомогою радіосигналу). Стимуляційні сигнали повинні повторювати характеристики дійсних інформаційних сигналів, що викликають активацію пристроїв. Так, мовний сигнал, який випромінюється системою виявлення, повинен складатися з записів живої чи штучно згенерованої мови; рівень гучності сигналу не повинен перевищувати гучності природного мовлення середньостатистичної людини, але також не повинен бути занадто тихим, щоб активація пристрою відбувалася з достатньою ймовірністю; за змістом повідомлення не повинні кардинально відрізнятися від типових розмов у приміщенні, оскільки оператор може запідозрити факт перевірки приміщення у разі використання сигналу іншої природи.

Організація переміщення об'єктів усередині приміщення під час сканування, зокрема в неробочий час, є доволі складною технічною задачею, а тому штучна активація сенсорів руху є виправданою.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Апаратна архітектура інтегрованої системи моніторингу. Запропонована архітектура інтегрованої системи виявлення пристроїв складається з блоку обробки даних, SDR-приймача, інтерфейсного модуля взаємодії з випромінювачами стимуляційних сигналів, самих модулів випромінювачів стимуляційних сигналів та антенно-фідерного комплексу, який може розширюватися за допомогою модуля антенних перемикачів і відповідного інтерфейсного модуля. Архітектуру комплексу зображено на Рисунку 2. Функції основних модулів системи є аналогічними до попереднього опису. Інтерфейсний модуль взаємодії з випромінювачами відповідає за передачу команд та даних зворотного зв'язку. Модуль антенного перемикача може бути використаний у разі необхідності перемикання між декількома ширококутовими антенами або вибору антени для роботи в певному частотному діапазоні.

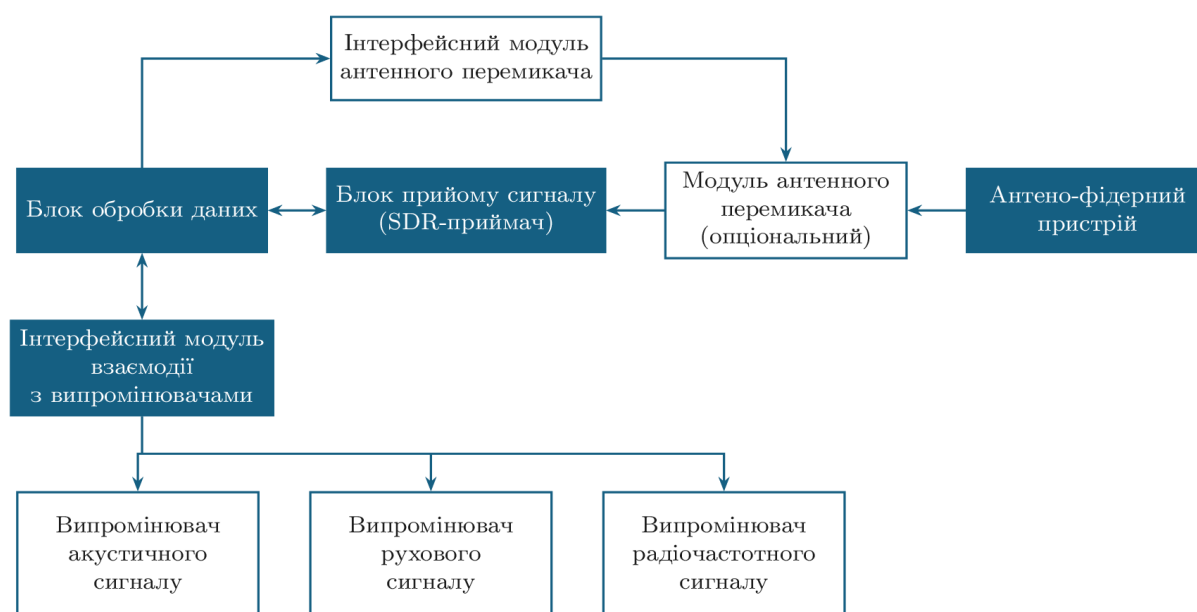


Рис. 2. Блок-схема архітектури інтегрованої системи виявлення пристроїв.

Ключовою вимогою до SDR-приймача є можливість передавати до блоку обробки даних необроблені I/Q-відліки, оскільки саме вони містять інформацію про апаратні особливості передавача, необхідну для RFFI. Рішення, що передають лише оцінки спектральної густини потужності [9, 10], забезпечують високу швидкість огляду, але унеможливають подальшу ідентифікацію. Тому приймач у запропонованій архітектурі працює у двох режимах: режимі огляду, у якому діапазон частот послідовно переглядається з обчисленням спектра та виявленням нових випромінювань (наприклад, за алгоритмом CFAR), і режимі цільового захоплення, у якому після виявлення події приймач перемикається на її частоту та записує фрагмент I/Q-потoku тривалістю $T_{\text{зах}}$. Такий розподіл узгоджується з підходом [11], за яким передаванню підлягають лише фрагменти потоку, що містять сигнал.

Інтерфейсний модуль взаємодії з випромінювачами доцільно реалізувати на мікроконтролері, підключеному до блоку обробки даних через USB або UART. Окрім трансляції команд, модуль повинен фіксувати фактичні моменти ввімкнення та вимкнення кожного стимулу і повертати їх у вигляді міток часу, узгоджених із часовою шкалою SDR-приймача. Саме спільна часова база дає змогу оцінювати затримку між початком стимулу та появою випромінювання, тобто встановлювати причинно-наслідковий зв'язок між стимулом і відгуком.

Випромінювач акустичного стимуляційного сигналу складається з модуля відтворення записів мовлення, підсилювача потужності та акустичної системи з каліброваним рівнем звукового тиску. Випромінювач рухового стимуляційного сигналу об'єднує ультразвуковий випромінювач для сенсорів руху доплерівського типу та джерело інфрачервоного випромінювання для PIR-сенсорів. Оскільки PIR-сенсори реагують на зміну теплового потоку, а не на його наявність, джерело ІЧ-випромінювання повинно працювати в імпульсному режимі або імітувати переміщення теплового об'єкта. Випромінювач радіочастотного стимуляційного сигналу призначений для імітації можливих команд активації пристроїв III класу; його застосування повинне здійснюватися з урахуванням вимог законодавства щодо

користування радіочастотним ресурсом, а його активація повинна узгоджуватися зі скануванням основним приймачем з метою уникнення хибних записів.

Модуль антенного перемикача, окрім вибору антени для певного діапазону частот, дає змогу почергово підключати спрямовані або рознесені в просторі антени та за співвідношенням рівнів прийнятого сигналу здійснювати грубу локалізацію джерела. У разі масштабування системи до кількох приймальних позицій для вибору оптимальної підмножини сенсорів можуть бути застосовані методи [12].

Взаємодію апаратних модулів під час обстеження ілюструє часова діаграма на Рисунку 3. Стимули подаються не періодично, а за псевдовипадковим розкладом із різною тривалістю увімкнення та тривалістю пауз. Пристрій з VOX-активацією починає передавання із затримкою t_a після початку стимулу і завершує його через час утримання t_h після закінчення стимулу, тоді як легітимні джерела випромінюють сигнали незалежно від розкладу. Тому повторюваний збіг моментів появи випромінювання з розкладом стимулів є ознакою, що відрізняє пристрій, активований стимулом, від легітимних джерел, навіть коли за енергетичними ознаками вони не відрізняються. Крім того, оскільки момент активації наперед відомий з точністю до t_a , приймач може розпочати цільове захоплення так, щоб у записаний фрагмент потрапив перехідний процес увімкнення передавача, який вважається одним із найінформативніших джерел ознак у методах RFFI [7]. Цей запропонований підхід відрізняється від пасивного моніторингу, за якого момент увімкнення пристрою є випадковим.

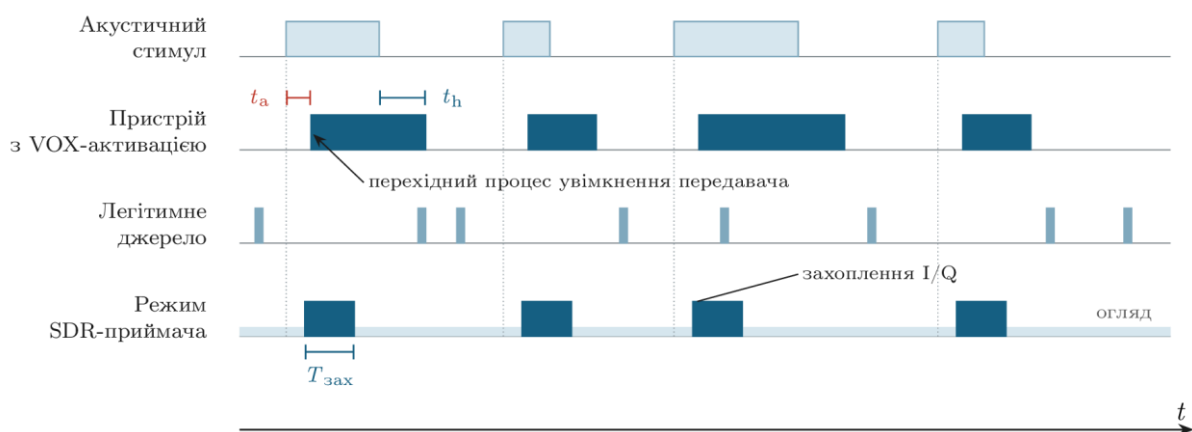


Рис. 3. Часова діаграма циклу «стимул–відгук» у запропонованій системі (схематично).

Узагальнена процедура обстеження приміщення включає такі етапи:

- 1) базове пасивне обстеження: реєстрація радіообстановки та формування бази еталонних відбитків легітимних пристроїв об'єкта;
- 2) формування псевдовипадкового розкладу стимулів для кожного типу випромінювачів;
- 3) подання стимулів з одночасним оглядом спектра та фіксацією моментів появи нових випромінювань;
- 4) цільове захоплення I/Q-фрагментів випромінювань, що виникли в інтервалі очікуваного відгуку;
- 5) ідентифікація джерел методами RFFI та оцінка кореляції моментів їхньої появи з розкладом стимулів;
- 6) локалізація підозрілих джерел за допомогою модуля антенного перемикача та формування звіту.

Програмна архітектура інтегрованої системи моніторингу.

Процеси виявлення та ідентифікації пристроїв запропонованою системою можна представити у вигляді задачі класифікації на відкритому наборі: навчання моделі відбувається на множині легітимних пристроїв, а основною задачею під час роботи системи є виявлення пристроїв, які не належать до легітимних. Для цього в запропонованій архітектурі будуть використані методи глибинного навчання, зокрема згорткові нейронні мережі (CNN).

Програмне забезпечення системи складається з чотирьох підсистем (Рис. 4). Підсистема керування сеансом формує псевдовипадковий розклад стимулів, передає команди апаратним модулям і веде журнал стимулів із мітками часу. Підсистема обробки сигналів виконує огляд спектра, виявляє нові випромінювання, ініціює цільове захоплення I/Q-фрагментів та їхню попередню обробку (виділення фронту сигналу, нормування амплітуди). Підсистема ідентифікації формує вектори ознак за допомогою

CNN і порівнює їх з базою еталонних відбитків легітимних пристроїв. Модуль прийняття рішень поєднує результат ідентифікації з оцінкою кореляції «стимул–відгук» і формує повідомлення для оператора.

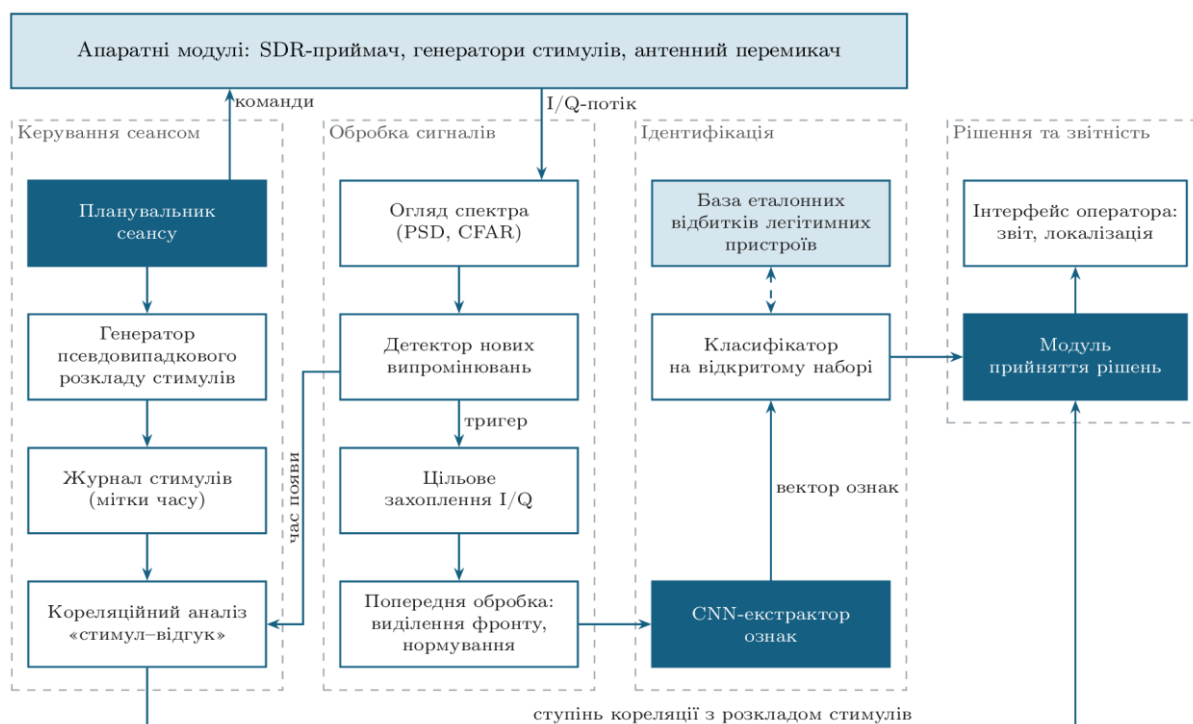


Рис. 4. Програмна архітектура інтегрованої системи виявлення пристроїв.

Вибір згорткових нейронних мереж зумовлений тим, що апаратні недосконалості передавача - дисбаланс квадратурних складових, зсув несучої частоти, нелінійність підсилювача потужності, особливості перехідних процесів - проявляються як локальні повторювані шаблони в часовій області сигналу. Згорткові шари по суті є набором фільтрів, параметри яких підбираються під час навчання, тому мережа сама визначає ознаки, що розрізняють пристрої, без ручного конструювання ознак. На вхід мережі подається фрагмент I/Q-сигналу у вигляді двоканальної послідовності розміром $2 \times N$ або його часово-частотного представлення (спектрограма). Так, у праці Sankhe та ін. [17] одновимірні CNN з I- та Q-складовими як двома вхідними каналами розрізняла 16 однотипних радіомодулів USRP X310 з точністю близько 98,6 % за квазістатичного каналу; водночас для 50 комерційних Wi-Fi-пристроїв точність під час тестування на даних, записаних в інший день, знижувалася до 46 %, що свідчить про чутливість таких моделей до зміни умов поширення.

Звичайний CNN-класифікатор із вихідним шаром softmax відносить будь-який вхідний сигнал до одного з відомих класів, тобто сигнал стороннього пристрою буде помилково віднесено до одного з легітимних класів. Тому в запропонованій архітектурі CNN використовується як екстрактор ознак: вихід передостаннього шару розглядається як вектор ознак z , а рішення приймається на основі відстані $d_{\min}$ від z до найближчого еталона в базі легітимних пристроїв. Якщо $d_{\min}$ не перевищує порогу τ , пристрій вважається легітимним, інакше - невідомим, що є підставою для тривоги. Навчання екстрактора доцільно виконувати методами метричного навчання, як у праці Shen та ін. [18], де такий підхід дав змогу додавати нові легітимні пристрої до бази без перенавчання мережі та виявляти сторонні пристрої (експеримент на 60 пристроях LoRa). Hanna та ін. [19] порівняли кілька архітектур для задачі на відкритому наборі (бінарний дискримінатор, мережі «один проти всіх», OpenMax, автокодувальник) і показали, що за наявності 10 авторизованих і 50 відомих неавторизованих Wi-Fi-передавачів точність виявлення сторонніх пристроїв становить близько 98 % на даних того ж дня, але знижується до 80 % на даних іншого дня. Поріг τ визначає компроміс між імовірністю пропуску стороннього пристрою та частотою хибних тривог і підлягає налаштуванню для кожного об'єкта.

Важливо, що рішення в запропонованій системі не ґрунтується лише на результаті класифікатора: модуль прийняття рішень також враховує ступінь кореляції між появою випромінювання та розкладом стимулів. Поєднання двох незалежних ознак «невідомий відбиток» і «відгук на стимул» потенційно може зменшити кількість хибних тривог, спричинених обмеженою стійкістю моделей RFFI [17, 19], однак, як



показують наведені нижче результати моделювання, лише за достатньої якості ідентифікації. Відкритими питаннями, які потребують експериментальної перевірки, залишаються формування навчальних наборів даних для аналогових і нестандартних передавачів, характерних для закладних пристроїв, а також стійкість ознак до зміни каналу поширення.

Імітаційне моделювання роботи системи.

З метою перевірки працездатності запропонованої логіки прийняття рішень та архітектури системи виконано імітаційне моделювання ключових складових архітектури: кореляційного аналізу «стимул-відгук» (модель А), ідентифікації передавачів за РЧ-відбитками в межах задачі ідентифікації на відкритому наборі (модель Б) та злиття двох ознак у модулі прийняття рішень (модель В). Моделі реалізовано мовою Python з використанням бібліотек NumPy [20], SciPy [21] та PyTorch [22]. Основні параметри моделей наведено в Таблиці 1. Значення параметрів моделей (зокрема параметрів VOX-активації та апаратних недосконалостей передавачів) обрано на основі припущень, оскільки експериментальних даних про них у відкритих джерелах немає. У зв'язку з цим, результати моделювання слід розглядати виключно як оцінку працездатності архітектури.

Таблиця 1

Основні параметри імітаційних моделей

Модель	Параметр	Значення
А	Розклад стимулів	Тривалість $U(2; 6)$ с, пауза $U(8; 20)$ с; кількість стимулів $K = 1 \dots 15$
А	VOX-пристрій	$p_{\text{акт}} = 0,5; 0,7; 0,9$; $t_a \sim U(0,05; 0,5)$ с; $t_h \sim U(1; 5)$ с; фонові акустичні події — $0,3 \text{ хв}^{-1}$
А	Легітимні джерела	30 ; інтенсивність появи випромінювань $0,1\text{--}6 \text{ хв}^{-1}$ (логарифмічно рівномірний розподіл)
А	Огляд спектра	$T_{\text{огл}} = 0,5$ с ($0,05\text{--}4$ с в окремому досліді); вікно відгуку $t_{a,\text{max}} + T_{\text{огл}}$
А	Правило рішення	Біноміальний тест, $\alpha = 0,01$ на сеанс, поправка Бонферроні; 2000 сеансів на точку
Б	Передавачі	ЧМ, девіація 5 кГц ; частота дискретизації 1 МГц ; захоплення 1024 відліки; 10 відомих і 20 невідомих пристроїв
Б	Апаратні недосконалості	Зсув частоти $U(-20; 20) \text{ кГц}$ з дрейфом ($\sigma = 1 \text{ кГц}$) і похибкою оцінки $U(-2; 2) \text{ кГц}$; дисбаланс I/Q ($\sigma = 3 \text{ \%, } 2^\circ$); постійна складова
Б	Перехідний процес	Наростання $10\text{--}60 \text{ мкс}$; викид $5\text{--}30 \text{ \%$ ($5\text{--}40 \text{ кГц}$); встановлення частоти до $\pm 30 \text{ кГц}$ ($50\text{--}200 \text{ мкс}$); джиттер $5 \text{ \%$
Б	Канал	Випадкова фаза; двопробневий ($\beta \leq 0,3$); адитивний білий гаусів шум, ВСШ $0\text{--}30 \text{ дБ}$
Б	Попередня обробка	Вирівнювання фази за відліком з найбільшою амплітудою; канали I, Q , миттєва амплітуда, миттєва частота
Б	CNN	5 згорткових блоків ($32\text{--}128$ фільтрів), вектор ознак 64 , косинусний класифікатор; 300 захоплень на пристрій, 20 епох; 3 реалізації
В	Склад сеансу	22 (L1), 3 (L2), 5 (L3) легітимних джерел і 1 закладний пристрій; $K = 6$; ВСШ 20 дБ ; 2000 сеансів

У моделі А стимули подаються за псевдовипадковим розкладом, VOX-пристрій активується на кожен стимул з імовірністю $p_{\text{акт}}$ і затримкою t_a , а момент появи його випромінювання фіксується під час найближчого відвідування частоти оглядом спектра з періодом $T_{\text{огл}}$. Легітимні джерела випромінюють незалежно від розкладу. Для кожного джерела підраховується кількість стимулів, після яких у вікні очікуваного відгуку зафіксовано появу випромінювання, і обчислюється р-значення біноміального тесту відносно фонові інтенсивності появ цього джерела, оціненої поза вікнами відгуку. Як видно з Рис. 5, а, одного стимулу недостатньо для прийняття рішення із заданим рівнем хибних тривог, однак уже за $K = 4$ імовірність виявлення становить $0,80$ для $p_{\text{акт}} = 0,7$ і $0,96$ для $p_{\text{акт}} = 0,9$, а за $K = 6$ — $0,93$ і $0,998$ відповідно;

навіть за $p_{\text{акт}} = 0,5$ імовірність виявлення 0,94 досягається за $K = 10$. Тривалість сеансу з шістьма стимулами становить у середньому близько 2,0 хв, з десятима — близько 3,2 хв. Імовірність хибної тривоги на сеанс в усіх випадках не перевищила 0,01.

Для порівняння розглянуто правило одного стимулу, за яким підозрілим вважається будь-яке джерело, випромінювання якого з'явилося у вікні відгуку після стимулу; таке правило відповідає аналізу відгуку на енергетичному рівні. Воно забезпечує імовірність виявлення 0,69 за імовірності хибної тривоги на джерело 0,024, що за наявності 30 легітимних джерел дає хибну тривогу в 52 % сеансів. Натомість площа під ROC-кривою, AUROC (Рис. 5, б), зростає з 0,83 за $K = 1$ до 0,98 за $K = 3$ і понад 0,99 за $K \geq 5$. Отже, саме повторення стимулів за псевдовипадковим розкладом забезпечує відокремлення пристрою, активованого стимулом, від легітимних джерел.

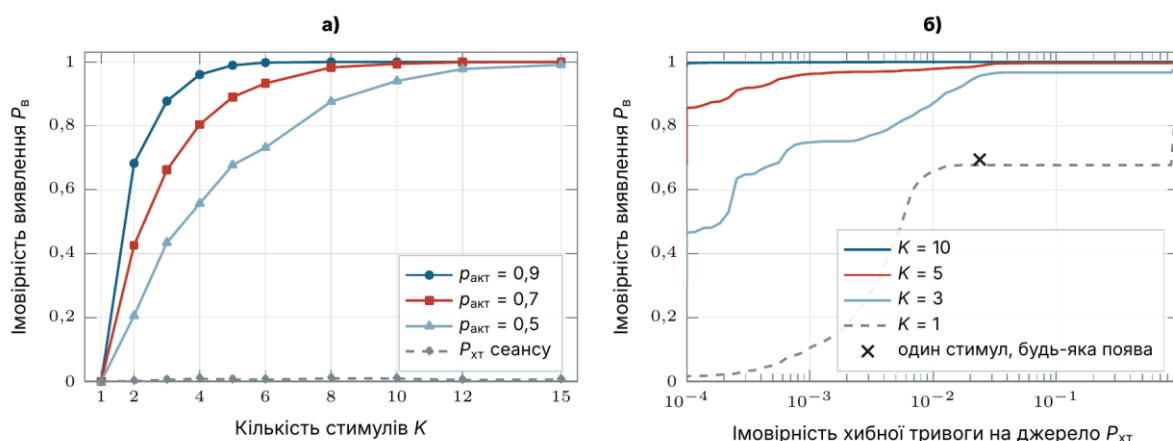


Рис. 5. Результати моделювання методу кореляції «стимул–відгук»: а) імовірність виявлення VOX-пристрою та імовірність хибної тривоги на сеанс залежно від кількості стимулів ($\alpha = 0,01$, 30 легітимних джерел); б) ROC-криві на рівні окремого джерела ($p_{\text{акт}} = 0,7$)

Результати дослідження впливу періоду огляду частоти (Рис. 6, а) показують, що за $T_{\text{огл}} \leq 0,5$ с імовірність виявлення практично не змінюється (0,94–0,96 за $K = 6$), а за $T_{\text{огл}} = 1, 2$ і 4 с знижується до 0,90, 0,84 і 0,78 відповідно. Зниження пояснюється тим, що разом із періодом огляду зростає вікно очікуваного відгуку, а отже, й імовірність випадкового збігу появи випромінювання з вікном, тому той самий збіг стає менш значущим. За $T_{\text{огл}} = 4$ с імовірність хибної тривоги на сеанс (0,019) перевищує заданий рівень. Причина в тому, що фонові інтенсивності появ кожного джерела оцінюються за коротшим інтервалом поза вікнами відгуку, і похибка цієї оцінки робить тест наближеним: за відомої фонові інтенсивності за тих самих умов імовірність хибної тривоги становить лише 0,002. Отже, до підсистеми огляду висувається вимога повторного відвідування частоти не рідше ніж раз на 0,5 с. Її можна забезпечити широкополосним захопленням у реальному часі або апаратно прискореним оглядом [9, 11], але не засобами першого покоління, тривалість циклу сканування яких становить кілька хвилин.

У моделі Б синтезовано сигнали 30 аналогових передавачів із частотною модуляцією (ЧМ) з індивідуальними апаратними недосконаlostями та перехідним процесом увімкнення. CNN навчалася на захопленнях 10 відомих (легітимних) пристроїв, а під час тестування до них додавалися 20 невідомих. Перед поданням до мережі кожне захоплення поверталася на кут фази відліку з найбільшою амплітудою, а I/Q-відліки доповнювалися миттєвою амплітудою та миттєвою частотою; таке подання інваріантне до випадкової початкової фази сигналу. Порівнювалися два режими: захоплення, синхронізоване зі стимулом, яке містить фронт увімкнення передавача, і захоплення в довільний момент усталеного передавання, характерне для пасивного моніторингу. Перевага синхронізованого захоплення виявилася суттєвою за ВСП ≥ 10 дБ: за 20 дБ точність розпізнавання відомих пристроїв становить 0,96 проти 0,69, а AUROC розділення відомих і невідомих пристроїв — 0,74 проти 0,59 (Рис. 6, б). За ВСП ≥ 15 дБ AUROC синхронізованих захоплень становить 0,70–0,75, тоді як для захоплень у довільний момент не перевищує 0,59, тобто наближається до рівня випадкового вгадування. Причина в тому, що в усталеному режимі ЧМ-передавача з постійною огибаючою інформативними залишаються лише зсув частоти, який змінюється від захоплення до захоплення, та слабкі прояви дисбалансу I/Q, тоді як перехідний процес увімкнення містить виразні індивідуальні ознаки. Отже, синхронізація захоплення зі стимулом є не лише засобом підтвердження відгуку, а й умовою ефективної ідентифікації аналогових передавачів.

Водночас навіть синхронізоване захоплення не забезпечує розділення, достатнього для самостійного прийняття рішення: за частки хибних тривог 5 % виявляється лише 36–38 % невідомих пристроїв (ВСПШ 20–30 дБ). Це узгоджується з даними [17, 19] щодо обмеженої стійкості RFFI і підтверджує необхідність поєднання ідентифікації з іншими ознаками.

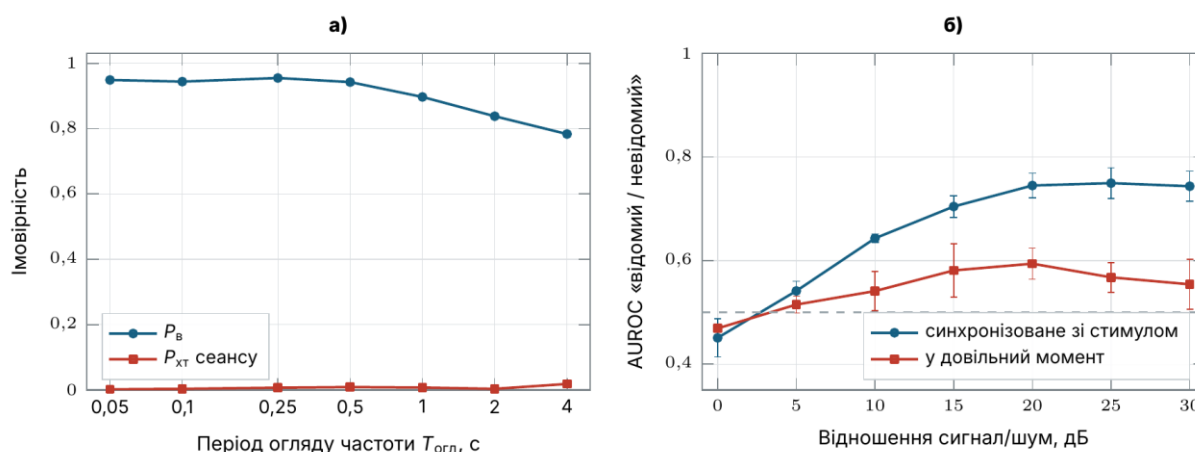


Рис. 6. Результати моделювання: а) вплив періоду огляду частоти на імовірність виявлення та хибної тривоги ($K = 6$, $p_{\text{акт}} = 0,7$); б) AUROC розділення відомих і невідомих передавачів залежно від ВСПШ (середнє $\pm$ СКВ за трьома реалізаціями)

У моделі В у кожному сеансі разом із закладним пристроєм присутні 30 легітимних джерел трьох категорій: внесені до бази пристрої, що не реагують на стимул (L1); внесені до бази пристрої, що реагують на мовлення, наприклад голосові асистенти (L2); нові пристрої, не внесені до бази (L3). Оцінка RFFI для кожного джерела усереднювалася за всіма захопленнями його фронту увімкнення протягом сеансу. Злиття виконувалося за кон'юнктивним правилом, за яким тривога формується лише тоді, коли значущими є обидві ознаки, у двох варіантах: зі спільним порогом для обох р-значень, тобто за оцінкою $S = -\lg \max(p_{\text{кор}}, p_{\text{RF}})$, де $p_{\text{кор}}$ і p_{RF} — р-значення кореляційної ознаки та ознаки невідомого відбитка, та з окремими порогоми, підібраними для мінімізації кількості хибних тривог за $P_v = 0,9$ на тих самих даних (оптимістична оцінка). Для порівняння також розглянуто метод Фішера. Результати наведено на Рис. 7 та в Таблиці 2.

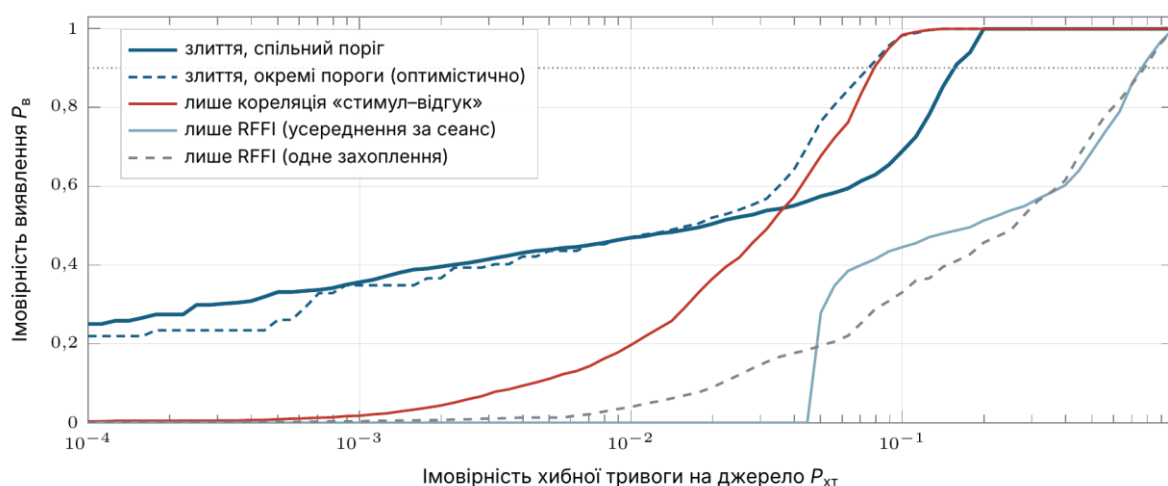


Рис. 7. ROC-криві виявлення закладного пристрою серед легітимних джерел різних категорій ($K = 6$, ВСПШ 20 дБ)

Показники виявлення закладного пристрою за $P_b = 0,9$ (модель В)

Ознака	AUROC	Хибних тривог на сеанс	Частка тривог L1 / L2 / L3
Кореляція «стимул–відгук»	0,962	2,37	< 0,01 / 0,79 / 0
RFFI, одне захоплення	0,675	23,52	0,76 / 0,76 / 0,90
RFFI, усереднення за сеанс	0,688	22,41	0,72 / 0,71 / 0,89
Злиття (метод Фішера)	0,966	2,38	< 0,01 / 0,73 / 0,04
Злиття (обидві ознаки, спільний поріг)	0,942	4,66	0,09 / 0,71 / 0,11
Злиття (обидві ознаки, окремі порогови)*	—	2,29	< 0,01 / 0,76 / < 0,01

* Пороги підбрано на тих самих даних; оцінка оптимістична, площа під ROC-кривою не визначається.

Отже, результати моделювання підтверджують працездатність основного механізму запропонованої архітектури. Повторювана стимуляція за псевдовипадковим розкладом забезпечує виявлення пристроїв з VOX-активацією за кілька хвилин із контрольованим рівнем хибних тривог за умови повторного відвідування частоти не рідше ніж раз на 0,5 с, а синхронізація захоплення зі стимулом суттєво покращує ідентифікацію аналогових передавачів порівняно із захопленням у довільний момент. Водночас за досягнутої в моделі якості ідентифікації злиття ознак не зменшує кількості хибних тривог, основним джерелом яких залишаються легітимні пристрої, що реагують на мовлення. Тому підвищення надійності ідентифікації (обсяг і різноманітність навчальних даних, стійкі до каналу поширення ознаки) є ключовою умовою реалізації переваг злиття. Обмеженнями моделювання є синтетичний характер сигналів одного типу передавачів, припущення про незалежність легітимних джерел від стимулів (окрім категорії L2) та відсутність протидії з боку порушника; перевірка отриманих оцінок на реальних пристроях є предметом подальших досліджень.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

В результаті проведеного дослідження було запропоновано концепцію інтегрованої системи виявлення пристроїв, яка поєднує пасивну ідентифікацію джерел за радіочастотними відбитками та активне виявлення шляхом створення стимуляційних сигналів. Аналіз попередніх досліджень показав, що ці два напрями виявлення пристроїв розвиваються окремо: засоби зі стимуляцією використовують виявлення за енергетичним рівнем або за змістом демодульованого сигналу, а більш просунуті методи RFFI залишаються пасивними та не впливають на поведінку досліджуваних пристроїв.

Запропоновано класифікацію цілей виявлення (пристроїв) за поведінковими характеристиками: з постійним передаванням (клас I), з внутрішньою (клас II), зовнішньою (клас III) та часовою (клас IV) активаціями. Показано, що ймовірність виявлення пристроїв класів II, III та IV пасивними засобами визначається випадковим збігом часу сеансу передавання з вікном сканування робочої частоти пристрою. Визначено, що найбільш доцільним методом підвищення ймовірності виявлення даних пристроїв є застосування стимуляційних сигналів.

Розроблено апаратну архітектуру системи виявлення пристроїв на основі обладнання, доступного для вільного продажу. До складу системи входять SDR-приймач, що працює в режимах огляду спектра та цільового захоплення I/Q-відліків, випромінювачі стимуляційних сигналів з інтерфейсним модулем, який фіксує мітки часу стимулів у спільній з приймачем часовій шкалі, та опціональний модуль антенного перемикача. Обґрунтовано необхідність передавання необроблених даних для застосування RFFI.

Розроблено програмну архітектуру системи, у якій виявлення сторонніх пристроїв сформульовано як задачу класифікації на відкритому наборі. Згортова нейронна мережа використовується для екстракції ознак, а рішення про ідентифікацію приймається на основі відстані вектора ознак до найближчого еталонного вектора в базі легітимних пристроїв об'єкта спостереження.

Імітаційне моделювання показало, що за шести стимулів пристрій із VOX-активацією виявляється з імовірністю 0,93 за імовірності хибної тривоги не більше 0,01 на сеанс, а захоплення сигналу, синхронізоване зі стимулом, суттєво підвищує якість ідентифікації аналогових передавачів порівняно із захопленням у довільний момент. Водночас за досягнутої в моделі якості ідентифікації злиття ознак не зменшує кількості хибних тривог, тому підвищення надійності RFFI є ключовим напрямом подальших досліджень.



Новизна запропонованої концепції полягає у псевдовипадковому розкладі подачі стимуляційних сигналів та поєднанні методів RFFI з активними методами виявлення пристроїв. Використання псевдовипадкового розкладу дає дві незалежні ознаки для прийняття рішення: збіг моментів появи випромінювання з розкладом стимулів та невідповідність радіочастотного відбитка жодному з легітимних пристроїв. Перша ознака відрізняє пристрої, активовані стимулом, від легітимних джерел за умови однакових енергетичних характеристик сигналів. Поєднання обох ознак потенційно дає змогу зменшити кількість хибних спрацювань, проте, як показало моделювання, лише за достатньої якості ідентифікації. Крім того, керований момент активації дозволяє спрямовано захоплювати перехідний процес увімкнення передавача, який є одним із найінформативніших джерел ознак для RFFI.

Практичне значення роботи полягає в тому, що запропоновану архітектуру можна реалізувати на доступних у вільному продажу серійних SDR-приймачах та відносно простих випромінювачах стимулів (динаміки, інфрачервоні світлодіоди, ультразвукові випромінювачі тощо). Водночас, запропонована концепція потребує експериментального підтвердження та перевірки ефективності.

Перспективними напрямками подальших досліджень є:

1. Експериментальне визначення параметрів VOX-активації типових закладних пристроїв (порогу спрацювання, затримки активації, часу утримання) та обґрунтування на цій основі вимог до рівня, спектрального складу й тривалості акустичних стимулів;

2. Розроблення методу формування псевдовипадкового розкладу стимулів та статистичного критерію оцінювання кореляції «стимул–відгук» із заданою ймовірністю хибної тривоги, а також визначення мінімальної кількості циклів стимуляції, достатньої для прийняття рішення;

3. Формування набору даних радіочастотних відбитків аналогових і нестандартних передавачів, характерних для закладних пристроїв, і порівняльна оцінка архітектур CNN та методів метричного навчання для задачі класифікації на відкритому наборі на цих даних;

4. Дослідження стійкості відбитків до зміни каналу поширення, температури, напруги живлення та положення пристрою, а також до зміни приймача, зокрема методами доповнення даних і формування канално-незалежних ознак;

5. Обґрунтування правила злиття рішень класифікатора й кореляційного аналізу та вибору порогу τ з урахуванням радіообстановки конкретного об'єкта;

6. Реалізація макета системи та його експериментальне порівняння з пасивними засобами за ймовірністю виявлення пристроїв II–IV класів, частотою хибних тривог і тривалістю обстеження;

7. Розширення системи до багатопозиційної конфігурації з точнішою локалізацією джерел і оптимальним вибором приймальних позицій, а також розроблення стимулів для пристроїв відеодомену й пристроїв із зовнішньою активацією з урахуванням вимог законодавства щодо користування радіочастотним ресурсом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Самосуд, З. О. (2015). Пошук закладних пристроїв за допомогою акустичної локації. *Ukrainian Scientific Journal of Information Security*, 21(3), 263–268. <https://doi.org/10.18372/2225-5036.21.9689>
2. Voronin, M. O. (2022). Methods of detecting radio broadcast at objects of information activity. *Modern Information Security*, 52(4). <https://doi.org/10.31673/2409-7292.2022.040010>
3. Klymenko, K. O., Kostenko, O. V., & Ilchenko, O. M. (2020). General classification of means of covert obtaining of information and methods of their detection. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*, 1(6), 6–15. <https://doi.org/10.32838/tmu-2663-5941/2020.6-1/02>
4. Конотопець, М. М., Смольков, О. Ю., & Пшенична, Ю. О. (2025). Підвищення можливостей пошукових комплексів щодо виявлення оптико-електронних елементів засобів негласного отримання інформації на об'єктах інформаційної діяльності. *Сучасні інформаційні технології у сфері безпеки та оборони*, 53(2), 60–69. <https://doi.org/10.33099/2311-7249/2025-53-2-60-69>
5. Sami, S., Tan, S. R. X., Sun, B., & Han, J. (2021). LAPD: Hidden Spy Camera Detection using Smartphone Time-of-Flight Sensors. *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 288–301. <https://doi.org/10.1145/3485730.3485941>
6. Chaman, A., Wang, J., Sun, J., Hassanieh, H., & Roy Choudhury, R. (2018). Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, MobiCom '18*, 337–351. <https://doi.org/10.1145/3241539.3241580>
7. Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. *Computer Networks*, 109455. <https://doi.org/10.1016/j.comnet.2022.109455>



8. Liu, Y., Wang, J., Li, J., Niu, S., & Song, H. (2021). Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey (Версія 1). arXiv. <https://doi.org/10.48550/ARXIV.2101.10181>
9. Flak, P. (2022). Hardware-Accelerated real-time spectrum analyzer with a broadband fast sweep feature based on the cost-effective SDR platform. IEEE Access, 10, 110934–110946. <https://doi.org/10.1109/access.2022.3215800>
10. McTaggart, B., Maclellan, A., Atimati, E., Nyasulu, L. B. T., Crockett, L. H., Crawford, D., & Stewart, R. W. (2026). A reconfigurable rfsoc-based spectrum sensing platform using a polyphase channeliser and distributed publisher-subscriber framework. Y ICC 2026 - IEEE international conference on communications (c. 1–6). IEEE. <https://doi.org/10.1109/icc59461.2026.11586939>
11. Bae, Y., Lee, H., Park, H., Jang, W.-h., & Jang, B.-J. (2026). Edge CA-CFAR Data Reduction for Bandwidth-Efficient Real-Time Wideband Spectrum Sensing on Low-Cost SDRs. Sensors, 26(14), 4468. <https://doi.org/10.3390/s26144468>
12. Bhattacharya, A., Zhan, C., Maji, A., Gupta, H., Das, S. R., & Djuric, P. M. (2021). Selection of sensors for efficient transmitter localization. IEEE/ACM Transactions on Networking, 1–13. <https://doi.org/10.1109/tnet.2021.3104000>
13. Svanstrom, F., Englund, C., & Alonso-Fernandez, F. (2021). Real-Time drone detection and tracking with visible, thermal and acoustic sensors. Y 2020 25th international conference on pattern recognition (ICPR). IEEE. <https://doi.org/10.1109/icpr48806.2021.9413241>
14. Acustek. (2026). SigDNA - universal RF TSCM & attribution platform | acustek. <https://acustek.com/product/tscm/sigdna>
15. Great Scott Gadgets. (2017). Release 2017.02.1 · greatscottgadgets/hackrf. GitHub. <https://github.com/greatscottgadgets/hackrf/releases/tag/v2017.02.1>
16. DigiScan-Labs. (2009). DigiScan (EX, версія 2.4) [Комп'ютерне програмне забезпечення].
17. Sankhe, K., Belgiovine, M., Zhou, F., Angioloni, L., Restuccia, F., D'Oro, S., Melodia, T., Ioannidis, S., & Chowdhury, K. (2020). No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments. IEEE Transactions on Cognitive Communications and Networking, 6(1), 165–178. <https://doi.org/10.1109/tccn.2019.2949308>
18. Shen, G., Zhang, J., Marshall, A., & Cavallaro, J. R. (2022). Towards scalable and channel-robust radio frequency fingerprint identification for lora. IEEE Transactions on Information Forensics and Security, 17, 774–787. <https://doi.org/10.1109/tifs.2022.3152404>
19. Hanna, S., Karunaratne, S., & Cabric, D. (2020). Open set wireless transmitter authorization: Deep learning approaches and dataset considerations. IEEE Transactions on Cognitive Communications and Networking, 1. <https://doi.org/10.1109/tccn.2020.3043332>
20. Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., ... Oliphant, T. E. (2020). Array programming with NumPy. Nature, 585(7825), 357–362. <https://doi.org/10.1038/s41586-020-2649-2>
21. Virtanen, P., Gommers, R., Oliphant, T. E., Haberland, M., Reddy, T., Cournapeau, D., Burovski, E., Peterson, P., Weckesser, W., Bright, J., van der Walt, S. J., Brett, M., Wilson, J., Millman, K. J., Mayorov, N., Nelson, A. R. J., Jones, E., Kern, R., Larson, E., ... van Mulbregt, P. (2020). SciPy 1.0: Fundamental algorithms for scientific computing in Python. Nature Methods, 17(3), 261–272. <https://doi.org/10.1038/s41592-019-0686-2>
22. Paszke, A., Gross, S., Massa, F., Lerer, A., Bradbury, J., Chanan, G., Killeen, T., Lin, Z., Gimelshein, N., Antiga, L., Desmaison, A., Kopf, A., Yang, E., DeVito, Z., Raison, M., Tejani, A., Chilamkurthy, S., Steiner, B., Fang, L., ... Chintala, S. (2019). PyTorch: An Imperative Style, High-Performance Deep Learning Library. Y H. Wallach, H. Larochelle, A. Beygelzimer, F. d'Alché-Buc, E. Fox, & R. Garnett (Ред.), Advances in Neural Information Processing Systems (T. 32). Curran Associates, Inc. https://proceedings.neurips.cc/paper_files/paper/2019/file/bdbca288fee7f92f2bfa9f7012727740-Paper.pdf

**Ivan Opirskyy**

D.Sc., Professor,
Head of the Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8461-8996
ivan.r.opirskyy@lpnu.ua

Artem Stefankiv

PhD Student,
Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0006-8851-8358
artem.v.stefankiv@lpnu.ua

Heorhii Loban

PhD Student,
Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0003-4862-8729
heorhii.loban.asp.2025@lpnu.ua

Oleksandr Hymza

Master's Student,
Department of Information Protection
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0009-7928-7545
oleksandr.hymza.mkbasp.2025@lpnu.ua

**DEVELOPMENT OF A CONCEPT FOR AN ACTIVE INTEGRATED RADIO COVERT DEVICE
DETECTION SYSTEM BASED ON CONVOLUTIONAL NEURAL NETWORKS AND SDR
RECEIVERS**

Abstract. Modern radio frequency means of detecting covert listening devices are predominantly passive: they register new emissions in the spectrum but cannot provoke transmission by devices that are activated by an event, such as voice (VOX activation), motion or a schedule, while commercial radio frequency fingerprint identification (RFFI) systems do not disclose their algorithms. The aim of the article is to develop a concept for the architecture of an integrated device detection system, based on affordable equipment, that combines passive RFFI with stimulus-signal emitter modules. The literature review shows that stimulation and identification of the responding source are still treated separately. A classification of detection targets by the domain of collected information and by behavioural characteristics (continuous transmission, internal, external, and time-based activation) is proposed, and the features of two generations of radio-frequency detection means are considered. A hardware architecture is developed that includes a software-defined radio (SDR) receiver with spectrum survey and targeted I/Q capture modes; acoustic, ultrasonic, infrared, and radio-frequency stimulus emitters with an interface module that records stimulus timestamps; and an antenna switch module. An inspection procedure is proposed in which stimuli are applied according to a pseudo-random schedule, and the decision is based on two features: the correlation between emission onsets and the stimulus schedule and the mismatch between the radio-frequency fingerprint and the database of legitimate devices. The software architecture uses a convolutional neural network as a feature extractor for open-set classification. Simulation shows that with six stimuli a VOX-activated device is detected with a probability of 0.93 at a false alarm probability of no more than 0.01 per session lasting about 2 minutes, provided that each frequency is revisited at least every 0.5 s, and that stimulus-synchronised capture improves the identification of analogue transmitters (area under the ROC curve of 0.75 versus 0.59 at a signal-to-noise ratio of 20 dB). However, given the model's current identification quality, fusing the two features does not reduce the number of false alarms; improving the reliability of RFFI is therefore identified as the key direction for further research.



Keywords: covert device detection; technical security countermeasures; radio frequency monitoring; radio frequency fingerprint identification; software-defined radio; VOX activation; stimulus signals; convolutional neural networks; open-set classification.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Samosud, Z. O. (2015). Bugs detection using acoustic location. *Ukrainian Scientific Journal of Information Security*, 21(3), 263—268. <https://doi.org/10.18372/2225-5036.21.9689>
2. Voronin, M. O. (2022). Methods of detecting radio broadcast at objects of information activity. *Modern Information Security*, 52(4). <https://doi.org/10.31673/2409-7292.2022.040010>
3. Klymenko, K. O., Kostenko, O. V., & Ilchenko, O. M. (2020). General classification of means of covert obtaining of information and methods of their detection. *Scientific Notes of Taurida National V.I. Vernadsky University. Series: Technical Sciences*, 1(6), 6–15. <https://doi.org/10.32838/tnu-2663-5941/2020.6-1/02>
4. Konotopets, M. M., Smolkov, O. Yu., & Pshenychna, Yu. O. (2025). Enhancing the capabilities of search complexes in detecting optoelectronic elements of covert information gathering devices at information activity sites. *Modern Information Technologies in the Sphere of Security and Defence*, 53(2), 60–69. <https://doi.org/10.33099/2311-7249/2025-53-2-60-69>
5. Sami, S., Tan, S. R. X., Sun, B., & Han, J. (2021). LAPD: Hidden Spy Camera Detection using Smartphone Time-of-Flight Sensors. *Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems*, 288—301. <https://doi.org/10.1145/3485730.3485941>
6. Chaman, A., Wang, J., Sun, J., Hassanieh, H., & Roy Choudhury, R. (2018). Ghostbuster: Detecting the Presence of Hidden Eavesdroppers. *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking, MobiCom '18*, 337—351. <https://doi.org/10.1145/3241539.3241580>
7. Jagannath, A., Jagannath, J., & Kumar, P. S. P. V. (2022). A comprehensive survey on radio frequency (RF) fingerprinting: Traditional approaches, deep learning, and open challenges. *Computer Networks*, 109455. <https://doi.org/10.1016/j.comnet.2022.109455>
8. Liu, Y., Wang, J., Li, J., Niu, S., & Song, H. (2021). Machine Learning for the Detection and Identification of Internet of Things (IoT) Devices: A Survey (Version 1). *arXiv*. <https://doi.org/10.48550/ARXIV.2101.10181>
9. Flak, P. (2022). Hardware-Accelerated real-time spectrum analyzer with a broadband fast sweep feature based on the cost-effective SDR platform. *IEEE Access*, 10, 110934–110946. <https://doi.org/10.1109/access.2022.3215800>
10. McTaggart, B., Maclellan, A., Atimati, E., Nyasulu, L. B. T., Crockett, L. H., Crawford, D., & Stewart, R. W. (2026). A Reconfigurable RFSoc-Based Spectrum Sensing Platform Using a Polyphase Channeliser and Distributed Publisher-Subscriber Framework. *ICC 2026 - IEEE International Conference on Communications*, 1—6. <https://doi.org/10.1109/ICC59461.2026.11586939>
11. Bae, Y., Lee, H., Park, H., Jang, W.-h., & Jang, B.-J. (2026). Edge CA-CFAR Data Reduction for Bandwidth-Efficient Real-Time Wideband Spectrum Sensing on Low-Cost SDRs. *Sensors*, 26(14), 4468. <https://doi.org/10.3390/s26144468>
12. Bhattacharya, A., Zhan, C., Maji, A., Gupta, H., Das, S. R., & Djuric, P. M. (2021). Selection of sensors for efficient transmitter localization. *IEEE/ACM Transactions on Networking*, 1–13. <https://doi.org/10.1109/tnet.2021.3104000>
13. Svanstrom, F., Englund, C., & Alonso-Fernandez, F. (2021). Real-Time Drone Detection and Tracking With Visible, Thermal and Acoustic Sensors. *2020 25th International Conference on Pattern Recognition (ICPR)*, 7265—7272. <https://doi.org/10.1109/ICPR48806.2021.9413241>
14. Acustek. (2026). SigDNA - universal RF TSCM & attribution platform | acustek. <https://acustek.com/product/tscm/sigdna>
15. Great Scott Gadgets. (2017). Release 2017.02.1 · greatscottgadgets/hackrf. *GitHub*. <https://github.com/greatscottgadgets/hackrf/releases/tag/v2017.02.1>
16. DigiScan-Labs. (2009). DigiScan (EX, version 2.4) [Computer software].
17. Sankhe, K., Belgiovine, M., Zhou, F., Angioloni, L., Restuccia, F., D'Oro, S., Melodia, T., Ioannidis, S., & Chowdhury, K. (2020). No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments. *IEEE Transactions on Cognitive Communications and Networking*, 6(1), 165–178. <https://doi.org/10.1109/tccn.2019.2949308>
18. Shen, G., Zhang, J., Marshall, A., & Cavallaro, J. R. (2022). Towards scalable and channel-robust radio frequency fingerprint identification for lora. *IEEE Transactions on Information Forensics and Security*, 17, 774–787. <https://doi.org/10.1109/tifs.2022.3152404>



19. Hanna, S., Karunaratne, S., & Cabric, D. (2020). Open set wireless transmitter authorization: Deep learning approaches and dataset considerations. *IEEE Transactions on Cognitive Communications and Networking*, 1. <https://doi.org/10.1109/tccn.2020.3043332>
20. Harris, C. R., Millman, K. J., van der Walt, S. J., Gommers, R., Virtanen, P., Cournapeau, D., Wieser, E., Taylor, J., Berg, S., Smith, N. J., Kern, R., Picus, M., Hoyer, S., van Kerkwijk, M. H., Brett, M., Haldane, A., del Río, J. F., Wiebe, M., Peterson, P., ... Oliphant, T. E. (2020). Array programming with NumPy. *Nature*, 585(7825), 357–362. <https://doi.org/10.1038/s41586-020-2649-2>
21. Virtanen, P., Gommers, R., Oliphant, T. E., Haberland, M., Reddy, T., Cournapeau, D., Burovski, E., Peterson, P., Weckesser, W., Bright, J., Van Der Walt, S. J., Brett, M., Wilson, J., Millman, K. J., Mayorov, N., Nelson, A. R. J., Jones, E., Kern, R., Larson, E., ... Vázquez-Baeza, Y. (2020). SciPy 1.0: Fundamental algorithms for scientific computing in Python. *Nature Methods*, 17(3), 261–272. <https://doi.org/10.1038/s41592-019-0686-2>
22. PyTorch: An imperative style, high-performance deep learning library. (2019). In *Proceedings of the 33rd International Conference on Neural Information Processing Systems*. Curran Associates Inc.

Отримано редакцією журналу / Received: 06.09.26

Прорецензовано / Revised: 18.09.26

Схвалено до друку / Accepted: 26.10.26



This work is licensed under Creative Commons Attribution-noncommercial-sharealike 4.0 International License.