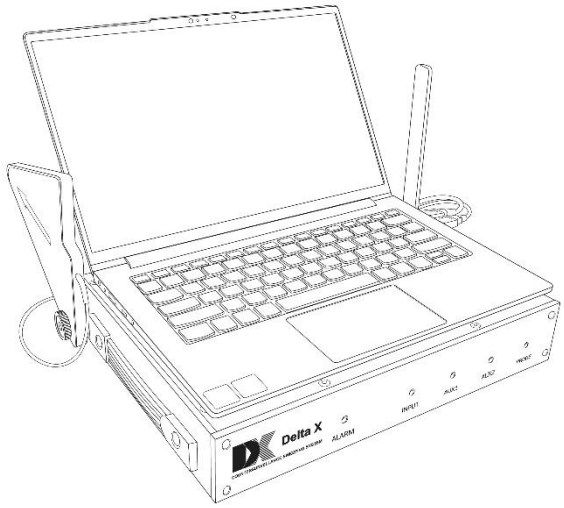


Комплекси пошуку закладних пристроїв «Delta S V3» та «Delta X G3/12»

(з програмним забезпеченням «Breeze RF»)

НАСТАНОВА КОРИСТУВАЧА

Зміст

Про системи

Ласкаво просимо у світ професійного пошуку! Аналізатори Delta S і Delta X нового покоління зроблять виявлення закладних пристроїв швидким і легким, забезпечуючи надзвичайно надійні результати. Їхнє сучасне апаратне забезпечення гарантує високу швидкість вимірювань, а вбудована система перемикання антен дозволяє досягти максимальної чутливості у всьому діапазоні частот.

На відміну від інших аналізаторів спектра, Delta S і Delta X зберігають здатність виявляти сигнали у повному діапазоні незалежно від того, яку саме смугу відображено на графіку спектра. Поки оператор перевіряє підозрілий сигнал, аналізатор продовжує фіксувати загрози в усьому спектрі частот та цілодобово охороняти ваше приміщення.

Delta S і Delta X автоматично ділять спектр на діапазони відповідно до місцевого розподілу частот, інформуючи оператора про ймовірний тип джерела — будь це 4G, 5G, Wi-Fi, Bluetooth чи інший передавач.

Унікальною особливістю Delta S і Delta X є можливість сканувати лише обраний набір діапазонів, оминаючи ділянки, які не викликають інтересу під час виконання поточної задачі. Наприклад, для виявлення автомобільних маячків (трекерів) достатньо сканувати мобільні діапазони, а для дослідження Wi-Fi — лише відповідні канали Wi-Fi. Налаштовуйте розклад сканування самостійно та отримуйте унікальні можливості, недоступні для інших аналізаторів спектра.

Важливою перевагою Delta S і Delta X є їхня висока чутливість та стійкість до перешкод. У той час як звичайні приймачі та детектори ближнього поля значно або повністю втрачають ефективність поблизу потужних джерел (веж стільникового зв’язку, антен, радіостанцій, точок доступу Wi-Fi тощо), Delta S і Delta X стабільно виявляють радіочастотні закладні пристрої з великої відстані.

Існує клас закладок, які не транслюють інформацію безперервно, а накопичують її та передають за зовнішнім запитом або за розкладом. Для виявлення таких прихованих загроз необхідний тривалий радіомоніторинг із повною реєстрацією ефіру та подальшим аналізом. Delta S і Delta X здатні цілодобово контролювати радіочастотне середовище, безперервно записуючи дані на SSD-накопичувач ноутбука або планшета.

Сучасні технології Wi-Fi та Bluetooth Low Energy (BLE) використовують спільні частотні канали, що в умовах насиченого радіоефіру суттєво ускладнює ідентифікацію окремих джерел. BLE-трекери або «мітки» (на кшталт AirTag) мають низьку потужність, виходять в ефір вкрай рідко та «маскуються» серед звичайних гаджетів. Це робить їх виявлення портативними детекторами поля майже неможливим, а для звичайних аналізаторів спектра — надзвичайно складним. Своєю чергою, протокол Wi-Fi дозволяє приховати небезпечне джерело всередині каналу «мирної» точки доступу або навіть використовувати її для негласної передачі даних. За таких умов критично важливою стає здатність виявляти та локалізувати кожен окремий Wi-Fi та BLE пристрій. Для цього нові покоління пошукових систем Delta X G3 та Delta S V3 оснащені додатковими модулями, які сканують бездротові мережі паралельно зі спектральним аналізом.

Загальні характеристики

- **Легка в освоєнні та водночас потужна** пошукова система.
- Швидко та надійно виявляє **всі види радіочастотних пристроїв** негласного зняття інформації в діапазоні до 6 ГГц (12 ГГц). Сюди входять аналогові й цифрові передавачі, що працюють постійно або періодично, транслюють аудіо чи відео, з шифруванням або без нього.
- Виявляє, ідентифікує та дозволяє локалізувати закладні пристрої, які використовують **цифрові стандарти GSM, 3G, 4G/LTE, 5G, Bluetooth, Wi-Fi, DECT** та інші протоколи в діапазоні до 6 ГГц (12 ГГц).
- Виявляє, ідентифікує та дозволяє локалізувати **пристрої Bluetooth Low Energy** (зокрема «мітки» типу AirTag та аналоги) у режимі реального часу, паралельно з основним радіочастотним скануванням. Система записує історію активності кожного гаджета і класифікує об'єкти за категоріями: «Всі», «Tags» (мітки) та «Beacons» (навігаційні маяки).
- Виявляє, ідентифікує та дозволяє локалізувати **пристрої Wi-Fi** у режимі реального часу паралельно з основним скануванням. Система реєструє історію активності кожного пристрою та класифікує їх за категоріями: «Точки доступу», «З'єднані станції (клієнти)» та «Нез'єднані станції». Дозволяє аналізувати взаємодію між пристроями завдяки зручній навігації між пов'язаними вузлами.
- Забезпечує спектральний аналіз та вимірювання рівня сигналу **на каналах окремих протоколів** для точної локалізації джерела (BLE, Bluetooth, Wi-Fi).
- Виявляє **радіочастотні глушники (блокіратори, джамери)** в усіх діапазонах, зокрема на частотах мобільного зв'язку (Uplink та Downlink), Глобальної навігаційної супутникової системи (GPS, GLONASS, GALILEO тощо), Wi-Fi/Bluetooth тощо.
- Спектральний аналіз забезпечує **надвисоку чутливість і велику дальність виявлення**, що в 10–20 разів перевищує показники типових РЧ-детекторів та приймачів ближнього поля.
- Функція **маскування фону** дозволяє відсіяти безпечні сигнали (телебачення, радіомовлення, базові станції зв'язку, службовий радіозв'язок тощо) та зосередитися на пошуку локальних джерел загрози.
- **Цілодобовий моніторинг радіоефіру (24/7)** з повною реєстрацією даних (спектральні траси, тривоги, BLE, Wi-Fi). Кількість журналів не обмежена, і кожен із них може містити нескінченну історію подій.
- Швидке налаштування під **частотний розподіл країни використання** (мобільний зв'язок, діапазони для бездротових пристроїв).
- **Гнучкі пошукові режими**: «Всі сигнали», «Мобільні/GPS-трекери», «Бездротові/ISM», «Низхідні/Навігація» та «Користувач», а також два додаткові режими дослідження діапазону та сигналу для локалізації.
- Кілька **антенних входів** та вбудований антенний перемикач забезпечують максимальну чутливість в усьому робочому діапазоні.
- **Ергономічна мобільна конструкція**: система працює в парі з ноутбуком або планшетом і живиться безпосередньо від нього. Головний блок оснащений зручною магнітною системою кріплення для гаджета, що забезпечує надійне з'єднання під час переміщення та локалізації джерел.
- **Зручність транспортування**: бічні ручки використовуються для зручного перенесення, всі антени кріпляться безпосередньо до блока, а захисний кейс уже входить до комплекту постачання.

Додаткові можливості

- **Маркери небезпеки «Threat Marks»** наочно відображають виявлені загрози безпосередньо на графіку спектра.
- **Функція «Burst Hunt» (Пріоритет коротких сигналів)** суттєво покращує фіксацію та візуалізацію короткочасних (імпульсних) сигналів, таких як Wi-Fi, Bluetooth, 5G тощо.
- **Функція «Звукова тривога»** попереджає користувача про наявність загрози звуковим сигналом, інтенсивність якого змінюється залежно від потужності сигналу.
- **Функція «Атенюатор»** спрощує локалізацію закладок під час пошуку поблизу потужних легальних передавачів, запобігаючи перевантаженню тракту.
- **Функція «Утримання максимальної небезпеки»** автоматично фіксує та виводить на екран найбільш небезпечний діапазон або сигнал, миттєво привертаючи увагу оператора до появи нової загрози.
- **Функція демодуляції AM/FM** дозволяє прослуховувати аналогові сигнали в реальному часі для швидкої аудіоідентифікації джерела.

Відмінності між системами

Система **Delta X G3/12** має такі особливості:

- **Розширений діапазон частот:** від 9 кГц до 12 ГГц.
- **Універсальний провідний та ІЧ-моніторинг:** виявляє несанкціоновану передачу інформації в мережах змінного струму, телефонних лініях, Ethernet-кабелях, сигналізаціях та інших дротових комунікаціях, а також в інфрачервоному діапазоні за допомогою багатофункціонального зонда, що входить до комплекту.
- **Професійна точність:** створена на базі повноцінного відкаліброваного аналізатора спектра, який забезпечує точні вимірювання фізичних рівнів сигналів в одиницях дБм (dBm).
- **Еталонний динамічний діапазон:** завдяки 14-розрядному АЦП аналізатора спектра система здатна одночасно фіксувати надслабкі сигнали та працювати поблизу потужних джерел без перевантаження вхідного тракту.
- **Апаратна індикація:** світлодіодний індикатор тривоги безпосередньо на передній панелі приладу.
- **Рекомендований сценарій використання:** безкомпромісний пошук та локалізація всіх без винятку типів закладних пристроїв (зокрема низькочастотних дротових та високочастотних понад 6 ГГц)

Система **Delta S V3** має такі особливості:

- **Базовий діапазон частот**: від 60 МГц до 6 ГГц.
- **Оптимальна архітектура**: створена на базі сучасного програмно-визначеного приймача (SDR) від Analog Devices, що дозволило суттєво знизити вартість та вагу комплексу без критичних втрат у точності вимірювань.
- **Збалансований динамічний діапазон:** 12-розрядний АЦП забезпечує високу лінійність тракту, а за потреби динамічний діапазон гнучко розширюється за допомогою вбудованого атенюатора.

- **Ефективне виявлення**: поєднання високої чутливості та швидкості сканування гарантує надійну фіксацію всіх актуальних типів радіозагроз у межах робочого діапазону.
- **Рекомендований сценарій використання:** довготривалий радіомоніторинг на об'єкті, виявлення автомобільних трекерів/маяків та оперативний контроль ефіру.

Специфікація

Спектральний аналіз

	Delta S V3	**Delta X G3/12**
Діапазон частот	60 - 6000 МГц	9 кГц – 12000 МГц
Швидкість сканування спектра - з функцією Burst Hunt - без Burst Hunt	 8 ГГц/с 10 ГГц/с	 7 ГГц/с 11 ГГц/с
Розрядність АЦП	12 біт	14 біт
Роздільна здатність спектра	11 кГц / 21.9 кГц	9.8 кГц
Чутливість - стандартне підсилення - високе підсилення	 -85 дБ -95 дБ	 -85 дБм -95 дБм
Динамічний діапазон	72 дБ	84 дБ
Відображуваний діапазон рівня сигналу - стандартне підсилення - високе підсилення	 -90…-20 дБ -100…-20 дБ (до 0 дБ в «авто»)	 -90…-20 дБм -100…-20 дБм (до 0 дБм в «авто»)
Полоса пропускання реального часу (RTBW)	24 / 27 МГц	27 МГц
Пошукові режими (час оновлення)	• Всі сигнали (~0.8 с) • Мобільні/GPS-трекери (~0.2 с) • Бездротові/ISM (~0.3 с) • "Низхідні/Навігація" (~0.3 с) • Дослідження діапазону/сигналу (~0.1-0.2 с)	• Всі сигнали (~0.9-1.1 с) • Мобільні/GPS-трекери (~0.2 с) • Бездротові/ISM (~0.3 с) • "Низхідні/Навігація" (~0.3 с) • Дослідження діапазону/сигналу (~0.1-0.2 с)
Відображувана смуга графіку спектра	Від 1 до 6000 МГц	Від 1 до 12000 МГц
Режим пікової траси	Вимкн., швидко, помірно, повільно, безкінечно	
Режим «Real-Time»	Так	

Аналіз Wi-Fi

	Delta S V3	**Delta X G3/12**
Діапазон частот	2400 - 2484 MHz, 5180 - 5885 MHz	
Сумісність зі стандартами	IEEE 802.11 b/g/n/a/ac/ax (Wi-Fi 6)	
Середня чутливість	-88 dBm	

Режими роботи	Пошук всіх пристроїв, аналіз окремого пристрою
Класифікація та фільтрація пристроїв	«Точки доступу», «З'єднані станції (клієнти)», «Нез'єднані станції»
Основні дані по пристрою	MAC-адреса, виробник, SSID, спосіб автентифікації
Статистичні дані по пристрою	Максимальний накопичений рівень, канали, лічильник пакетів по каналах, перше виявлення передачі, останнє виявлення передачі, перше виявлення прийому, останнє виявлення прийому
Додаткові дані	Таблиця взаємодіючих пристроїв
Дані користувача по пристрою	Коментар, статус «Верифікований», верифікований поріг
Сортування	RSSI, перше виявлення, лічильник кадрів

Аналіз Bluetooth Low Energy (BLE)

	Delta S V3	**Delta X G3/12**
Діапазон частот	2402 - 2484 MHz	
Чутливість	-99 dBm	
Режими роботи	Пошук всіх пристроїв, аналіз окремого пристрою	
Класифікація та фільтрація пристроїв	«Всі», «Tags» (мітки), «Beacons» (навігаційні маяки)	
Основні дані по пристрою	MAC-адреса, виробник та додаткові деталі, отримані з пакета оголошення	
Статистичні дані по пристрою	Максимальний накопичений рівень, лічильник пакетів, перше виявлення, останнє виявлення	
Додаткові можливості	Виділення ідентичних пристроїв, Таблиця ідентичних пристроїв, Відбір нових екземплярів	
Дані користувача по пристрою	Коментар, статус «Верифікований», верифікований поріг	
Сортування	RSSI, перше виявлення, лічильник пакетів	

Загальні параметри

	Delta S V3	**Delta X G3/12**
Конструкція	Портативний блок	Портативний блок
Платформа	SDR від Analog Devices	Аналізатор спектра
Антенні входи	INPUT 1, INPUT 2, BLUETOOTH, Wi-Fi	INPUT, AUX1, AUX2, BLUETOOTH, Wi-Fi
Елементи відображення (панелі)	«Рівень», «Спектр», «Тривоги», «Wi-Fi», «BLE»	
Демодуляція	AM, FM зі смугою 5, 15, 30, 100 та 200 кГц (в діапазоні 70-6000 МГц)	AM, FM, CW, USB, LSB зі смугою 2, 5, 15, 50, 100 та 200 кГц
Вимоги до ноутбука / планшету	Діагональ екрану: 12-14" Процесор: Intel Core i3 / AMD Ryzen 3 або вище (рекомендовано Intel Core i5 / AMD Ryzen 5) Не менше 2 портів USB: 1) «USB 3.1» або «USB-C»; 2) «USB-C» RAM: 8 Gb або більше SSD: 256 Gb чи більше Операційна система: Windows 11	

Живлення	Від USB порту ноутбука / планшету	
Час автономної роботи	1-1.5 год	
Час роботи від електромережі	Необмежений	
Мова інтерфейсу	Українська, Англійська	
Діапазон температур	-5°C…+45°	
Розміри блоку (без антен)	33.5 x 26 x 6 см	
Розміри в упаковці	50 x 40 x 20 см	
Вага головного блоку з антенами (без комп'ютеру)	3 кг	3.5 кг
Вага в упаковці	8.5 кг	10.5 кг

Режими та функції

Режими пошуку

- **У режимі «Всі сигнали»** система аналізує спектр у всьому доступному діапазоні частот та фіксує радіовипромінювання будь-яких типів. Окрім мобільних та бездротових стандартів, комплекс успішно виявляє закладні пристрої, що працюють поза ними — наприклад, радіомікрофони VHF/UHF, бездротові відеокамери аналогових та цифрових форматів (900/1200 МГц) та будь-які інші РЧ-пристрої з частотою до 6/12 ГГц. Паралельно з цим виконується виявлення пристроїв Wi-Fi та пристроїв Bluetooth Low Energy.
- **У режимі «Мобільні/GPS-трекери»** система зосереджується на виявленні стільникових пристроїв усіх поколінь, зокрема GPS-маяків, які встановлюються на транспортні засоби для відстеження координат та передають дані через мобільний ефір. Режим гарантує швидке та надійне виявлення прихованих мікрофонів і відеокамер, що транслюють інформацію через мережі GSM, 3G, 4G/LTE та 5G (до 6/12 ГГц). За потреби користувач може додатково активувати паралельне виявлення пристроїв Wi-Fi та Bluetooth Low Energy.
- **У режимі «Бездротові/ISM»** Delta S / Delta X оперативно виявляє сигнали Wi-Fi, Bluetooth, ZigBee, DECT, LoRa та інші радіочастотні засоби, що функціонують у загальнодоступних ISM-діапазонах (наприклад, пульти дистанційного керування, компоненти систем «розумний дім», бездротові датчики сигналізації тощо). Паралельно з цим виконується виявлення пристроїв Wi-Fi й Bluetooth Low Energy.
- **У режимі «Низхідні/Навігація»** система сканує низхідні канали базових станцій мобільного зв'язку (Downlink) та діапазони Глобальних навігаційних супутникових систем (GNSS: GPS, GLONASS, GALILEO тощо). За умови активації функції «Виявляти РЧ глушники», будь-які завади та аномалії, що створюються генераторами шуму (джамерами), будуть миттєво виявлені та відображені на додатковій графічній шкалі, а програмне забезпечення увімкне особливий тональний сигнал попередження.

Виявлення пристроїв Wi-Fi

- **Комплексне виявлення:** Пошук точок доступу та клієнтських пристроїв у режимі реального часу паралельно з основним радіочастотним скануванням.
- **Інтелектуальний аналіз:**
  - Класифікація об'єктів: «Точки доступу», «З'єднані станції (клієнти)» та «Нез'єднані станції».

    - Аналіз взаємодій між пристроями зі зручною навігацією між пов’язаними вузлами.
- **Глибока деталізація:** Вичерпні дані по кожному джерелу: MAC-адреса, виробник, SSID, канали, кількість кадрів (фреймів) та часові мітки.
- **Контроль рівнів сигналу:** Візуалізація поточного, пікового та максимального накопиченого рівня RSSI для оцінки відстані до джерела та його фізичного пошуку.
- **Додатковий спектральний аналіз каналу:** система дозволяє швидко перейти до аналізу окремого каналу Wi-Fi для пришвидшення локалізації
- **Візуалізація на спектрі** дозволяє суміщати спектральну картинку з піктограмами пристроїв
- **Тривалий моніторинг:** Запис повної історії активності для кожного пристрою з візуалізацією на графіку тривог.
- **Швидка локалізація:** Спеціальний режим аналізу окремого пристрою для його точного фізичного пошуку.
- **Система сповіщень:** Налаштування індивідуальних порогів тривоги та окрема звукова індикація.
- **Зручне керування базою:**
    - Створення «білого списку» для верифікованих пристроїв
    - Можливість додавання текстових коментарів безпосередньо в таблиці результатів.
    - Фільтрація та сортування результатів.
- **Апаратна оптимізація:** Зовнішня направлена антена суттєво прискорює фізичний пошук джерела сигналу

Виявлення пристроїв Bluetooth Low Energy (BLE)

- **Комплексне виявлення:** Пошук пристроїв BLE у режимі реального часу паралельно з основним радіочастотним скануванням.
- **Інтелектуальна ідентифікація:**
    - **Класифікація об'єктів** за категоріями: «Всі», «Tags» (мітки) та «Beacons» (навігаційні маяки).
    - **Унікальні функції:** «Виявлення ідентичних пристроїв» та «Нові екземпляри» дозволяють локалізувати пристрій навіть в умовах постійної динамічної зміни MAC-адреси та корисного навантаження а також відслідковувати історію на довгих проміжках часу
- **Глибока деталізація:** Повна інформація по кожному джерелу: поточна MAC-адреса, виробник, кількість кадрів (фреймів), точні часові мітки та корисне навантаження (payload).
- **Контроль рівнів сигналу:** Візуалізація поточного, пікового та максимального накопиченого рівня RSSI для оцінки наближення до джерела.
- **Додатковий спектральний аналіз каналів:** дозволяє виявляти та локалізувати пристрої які не визначаються шляхом сканування пакетів Advertising (пристрої BLE у з’єднаному стані, пристрої Bluetooth Classic)
- **Візуалізація на спектрі** дозволяє суміщати спектральну картинку з піктограмами пристроїв
- **Тривалий моніторинг:** Запис детальної історії активності кожного пристрою з відображенням на графіку тривог
- **Швидка локалізація:** Спеціальний режим аналізу конкретного пристрою для його точного фізичного пошуку на об'єкті.

- **Система сповіщень:** Гнучке налаштування порогів тривоги та окрема звукова індикація при появі підозрілих BLE-сигналів.
- **Зручне керування базою:**
    - Формування «Білого списку» для довірених пристроїв.
    - Система фільтрації, сортування та можливість додавання текстових коментарів до будь-якого знайденого об'єкта.
- **Апаратна оптимізація**: Зовнішня направлена антена суттєво прискорює фізичний пошук джерела сигналу

Діапазони

- **Наочна індикація ефіру:** відображення поточної радіочастотної обстановки виконується за допомогою графічних шкал рівня, кожна з яких відповідає за свій частотний діапазон.
- **Автоматична сегментація:** за замовчуванням весь частотний проміжок розбитий на кілька базових піддіапазонів, до яких додається набір мобільних та бездротових каналів відповідно до регіонального плану розподілу частот.
- **Регіональна адаптація:** таблиця діапазонів швидко й легко налаштовується під частотний розподіл країни, де безпосередньо проводяться пошукові роботи.
- **Гнучке редагування:** користувач може самостійно редагувати існуючі або додавати нові діапазони (зокрема нові частоти 4G/LTE та 5G) у разі зміни локального частотного плану.
- **Індивідуальні пороги чутливості:** для кожного діапазону можна задати власний поріг спрацьовування, що дозволяє гнучко регулювати чутливість системи та дальність виявлення загроз.
- **Вичерпна інформативність:** по кожному діапазону в реальному часі відображаються його назва, межі частот, поточний, піковий та максимальний зареєстровані рівні, поточний поріг, кількість виявлених небезпечних сигналів та частота найбільш критичної загрози. За умови активації функції «Виявляти РЧ глушники», на шкалу також виводиться рівень навмисної завади.
- **Колірна індикація тривоги:** у разі перевищення встановленого порогу чутливості шкала рівня відповідного діапазону миттєво змінює свій колір на червоний.
- **Журналювання подій:** повна історія тривог по кожному з діапазонів автоматично зберігається в базі даних журналу і може бути детально проаналізована на графіках активності.
- **Оперативна локалізація:** оператор має можливість в один клік перейти до поглибленого дослідження конкретного діапазону, щоб переглянути детальний список сигналів та розпочати фізичний пошук і локалізацію передавача.

Сигнали

- **Автоматичне розпізнавання:** сигнали миттєво ідентифікуються безпосередньо в спектральних трасах, автоматично заносяться до загального списку та безперервно оновлюються в реальному часі.
- **Інтерактивний список:** повний перелік виявлених сигналів доступний для детального аналізу у спеціалізованому режимі дослідження обраного діапазону.
- **Повна технічна інформація:** по кожному сигналу оператор бачить точну частоту, смугу пропускання, номер каналу, а також поточний, піковий та максимальний зареєстрований рівень потужності.
- **Логування та графічний аналіз:** історія тривог і динаміка активності по кожному окремому сигналу автоматично фіксується в журналі подій та може бути детально вивчена на часовому графіку.

- **Цільова локалізація:** користувач може в будь-який момент перейти до поглибленого дослідження конкретного сигналу для його детального аналізу та точного визначення місця розташування передавача.

Маскування фону

- **Фільтрація зовнішнього середовища:** команда «Маскувати фон» дозволяє зафіксувати та занести до бази безпечних джерел зовнішні радіосигнали (телебачення, радіомовлення, ретранслятори мобільного зв’язку тощо). Це дає змогу оператору зосередитися виключно на пошуку локальних передавачів, розташованих усередині об'єкта.
- **Принцип спектральної маски:** зовнішні завади ігноруються на основі точного контуру спектральної маски. Це повністю унеможливлює пропуск підозрілих джерел, навіть якщо частоти їхнього випромінювання збігаються з діючими каналами теле- чи радіомовлення.
- **Цільове застосування:** процедура маскування є обов'язковою та необхідною лише для загального режиму пошуку «Всі сигнали».
- **Вибіркова фільтрація:** маскуванню підлягають лише ті сигнали, що розташовані поза межами стандартних мобільних та бездротових діапазонів.
- **Гнучке налаштування часу:** тривалість процедури вимірювання фону та накопичення трас вибирається оператором.
- **Багатоточкове вимірювання:** для підвищення точності сканування фону аналіз ефіру можна послідовно проводити в кількох різних точках за межами зони контролю.
- **Регулювання чутливості:** зміщення спектральної маски (загальний рівень допуску та чутливості до появи нових сигналів) гнучко регулюється за допомогою встановлення порогу.

Поріг та індикація тривоги

- **Індивідуальне налаштування:** кожен частотний діапазон має власний поріг чутливості, який гнучко задається користувачем під конкретні умови завадової обстановки.
- **Миттєва візуалізація:** колір графічної шкали діапазону автоматично змінюється на червоний у разі перевищення встановленого порогу потужності.
- **Автоматична фіксація:** будь-які сигнали, рівень яких перетинає межу порогу, миттєво розпізнаються системою як потенційні загрози та вносяться до бази даних.
- **Акустичний пошук джерела:** функція «Звукова тривога» вчасно попереджає оператора про небезпеку. Інтенсивність та частота звукового тону динамічно наростають у міру збільшення рівня сигналу, що значно полегшує локалізацію передавача методом наближення.
- **Графічна ретроспектива:** система автоматично веде хронологію подій для кожного діапазону та сигналу, зберігаючи повну історію тривог із можливістю її виведення на часовий графік.
- **Гнучкий аналіз журналу:** оператор може переглядати та аналізувати графік тривог за будь-який обраний проміжок часу та з необхідним ступенем деталізації (від хвилин до діб).

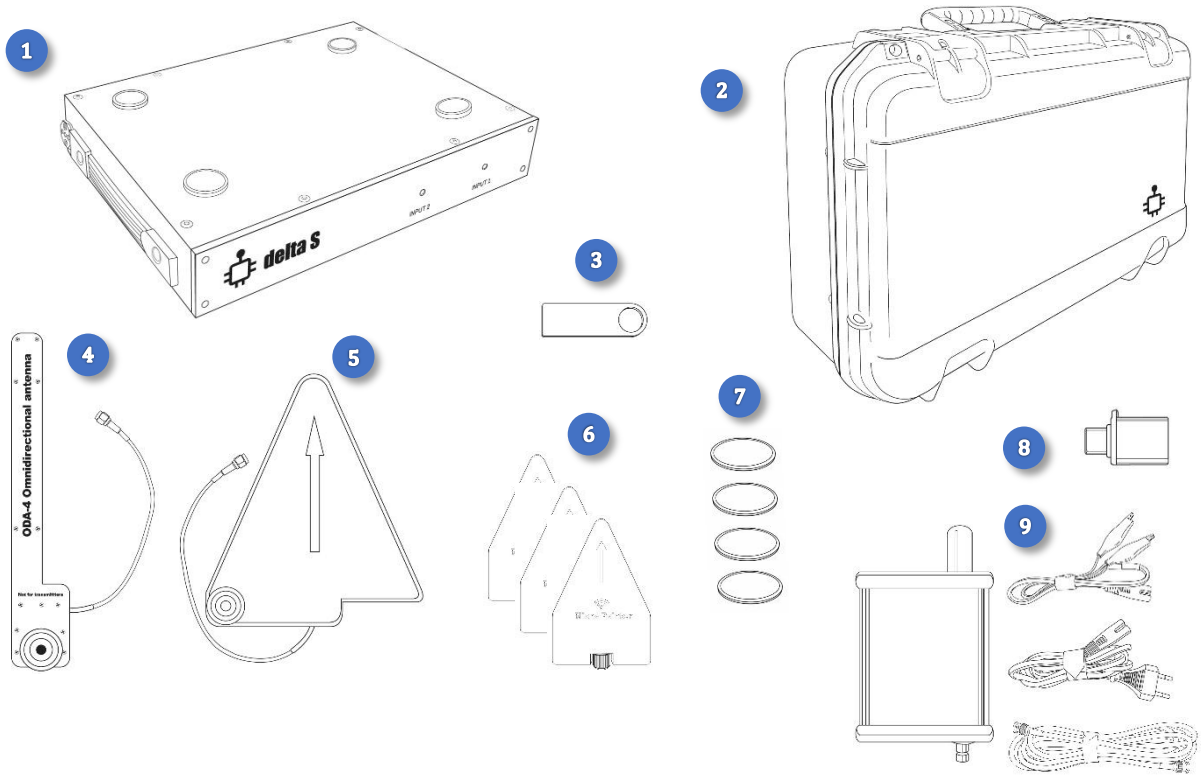
Відображення спектра

- **Багатошаровий графік:** одночасне виведення спектральних трас «Поточна» (живий ефір), «Пікова» (максимальні значення) та лінії «Поріг» для наочного моніторингу обстановки.

- **Режим «Постійність» (Persistence):** накопичення та колірна індикація частоти появи сигналів, що дозволяє візуально розділити постійні завади та короткочасні імпульсні випромінювання.
- **Інтерактивні маркери** на графіку спектра**:**
    - «ThreatMarks» **-** автоматичне маркування та підсвічування виявлених небезпечних сигналів
    - «Канали» - підсвічування смуги та рівня на каналах бездротових стандартів
    - «Пристрої» - відображення піктограм пристроїв BLE або Wi-Fi відповідно до їх каналу та рівня сигналу
- **Функція «Водоспад» (Waterfall):** тривимірне відображення історії спектра в часі, де потужність сигналу кодується кольором, що спрощує фіксацію періодичних або рухомих джерел.
- **Зручна навігація:** інтуїтивний скролінг (прокручування) та плавне масштабування графіка спектра для детального вивчення зацікавлених ділянок.
- **Оптимізація під сенсорні екрани:** повноцінна підтримка жестів керування (Touch Screen) для комфортної роботи на планшетах та польових ноутбуках.
- **Фоновий моніторинг при масштабуванні:** можливість детально збільшити будь-яку окрему ділянку спектра без зупинки фонового пошуку та аналізу загроз в усьому робочому діапазоні системи.
- **Швидка зміна масштабу екрана:** кнопки миттєвого вибору смуги відображення:
    - «Весь» — виведення повного робочого діапазону приладу;
    - «Діапазон» — фокусування на обраному частотному діапазоні;
    - «Сигнал» — максимальне наближення для дослідження конкретного сигналу.

Комплект постачання

	Найменування	**Delta S V3**	**Delta X G3/12**
1.	Головний блок	1	1
2.	Кейс транспортувальний	1	1
3.	USB-носій з програмою інсталяції та інструкцією з використання	1	1
4.	Широкодіапазонна антена ODA-4	1	1
5.	НВЧ антенна MWA-6	1	1
6.	НВЧ антенна LPDA-12	3	3
7.	Магнітна наклейка для ноутбука або планшета	4	4
8.	Адаптер USB-C–USB 3.1	1	1
9.	Багатофункціональний зонд з комплектом кабелів	-	1



Підготовка

Попередження про правила безпеки

- **Обмеження вхідної потужності:** категорично забороняється подавати на високочастотні входи пристрою по кабелю сигнали, рівень потужності яких перевищує **0 дБм (dBm)**.
- **Захист від потужних джерел випромінювання:** уникайте роботи в безпосередній близькості від потужних радіопередавачів (радіостанцій, ретрансляторів) або локаторів нелінійних переходів (NLJD), і ніколи не спрямовуйте на них антени пристрою.
- **Захист від стороннього випромінювання:** стежте за тим, щоб антени сторонніх потужних передавачів не були спрямовані безпосередньо на приймальний блок системи.
- **Електростатична безпека антен:** не використовуйте антени з пошкодженою ізоляцією або оголеними металевими частинами, які можуть стати джерелом накопичення та передачі електростатичного розряду (ESD).
- **Захист роз'ємів від статики:** уникайте будь-якого потрапляння електростатичних розрядів на відкриті вхідні високочастотні роз’єми пристрою.
- **Температурна акліматизація:** не вмикайте пристрій одразу після його тривалого зберігання або транспортування в умовах низьких температур. Перед запуском залиште прилад у теплому приміщенні на деякий час для повного випаровування можливого конденсату.

Вибір комп’ютера

Переконайтеся, що характеристики обраного ноутбука або планшета повністю відповідають специфікації, наведеній на початку цієї інструкції. Оскільки пошукова система виконує великий обсяг складних математичних обчислень та потребує високошвидкісної передачі даних в реальному часі, використання комп’ютера з нижчими технічними характеристиками може призвести до некоректної роботи або збоїв системи.

КРИТИЧНІ ВИМОГИ ДО АПАРАТНОГО ЗАБЕЗПЕЧЕННЯ:

- **Тип процесора:** підтримуються лише високопродуктивні процесори архітектури x86/x64 серій **Intel Core i** (Core i5, Core i7 тощо) або **AMD Ryzen** (Ryzen 5, Ryzen 7 тощо).
    - *Не підходять:* енергоефективні процесори типу **ARM** (наприклад, Qualcomm Snapdragon), які часто використовуються в мобільних планшетах.
    - *Не підходять:* слабкі серії процесорів Intel, такі як **Pentium, Celeron або серія Intel N** — вони не мають достатньої обчислювальної потужності.
- **Діагональ екрана:** для забезпечення сумісності з мобільною магнітною системою кріплення головного блока діагональ екрана **не повинна перевищувати 14"**.
- **Операційна система:** обов'язкова наявність ліцензійної ОС **Windows 10, Windows 11** або новішої версії.

Інсталяція

Інсталяція програмного забезпечення

1. **Встановлення ПЗ:** Підключіть USB-носій, що входить до комплекту поставки, та запустіть інсталятор програми **«Breeze RF»**. Для пошукових систем останнього покоління обов'язково використовуйте версію програмного забезпечення **1.026 або новішу**.
2. **Перезавантаження:** Дочекайтеся повного завершення процесу інсталяції та обов'язково перезавантажте ноутбук або планшет. Після перезапуску ярлик для запуску програми з'явиться на Робочому столі та в меню «Пуск».

Додаткові налаштування комп’ютера (рекомендовано):

- **Запобігання наводкам від бездротових пристроїв комп’ютера**
  Перед початком роботи переведіть комп’ютер в режим польоту та впевніться що на ньому вимкнено Wi-Fi та Bluetooth.

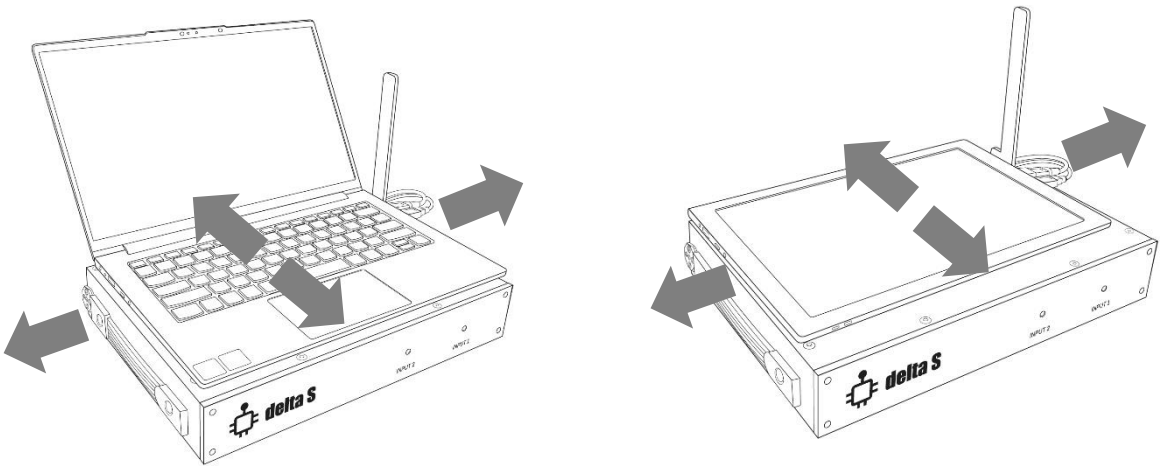
- **Налаштування електроживлення USB**
  Для забезпечення стабільного швидкісного обміну даними та запобігання раптовому вимкненню обладнання рекомендується вимкнути режим тимчасового вимкнення USB-портів (USB Suspend):
    - Натисніть комбінацію клавіш Win + R на клавіатурі (або скористайтеся пошуком на панелі завдань), введіть команду powercfg.cpl і натисніть **Enter**.
    - У вікні, що відкрилося, навпроти активної схеми живлення натисніть **«Змінити настроювання плану - «Змінити додаткові параметри живлення»**.
    - У списку знайдіть та розгорніть пункт **«Параметри USB»** - **«Параметр тимчасового вимкнення USB-порту»**.
    - Переведіть усі доступні режими (від мережі та від батареї) у стан **«Заборонено»** (або «Вимкнено») та натисніть **«Застосувати»**.

Кріплення ноутбука або планшета

Система Delta S / Delta X сконструйована у вигляді мобільного переносного блоку, який утримує ноутбук або планшет за допомогою магнітних тримачів. Магнітні стікери входять до комплекту поставки та мають бути наклеєні на нижню панель ноутбука або планшета перед початком експлуатації. Після встановлення магнітних стікерів ноутбук або планшет можна приєднувати та від'єднувати від головного блока будь-яку кількість разів.

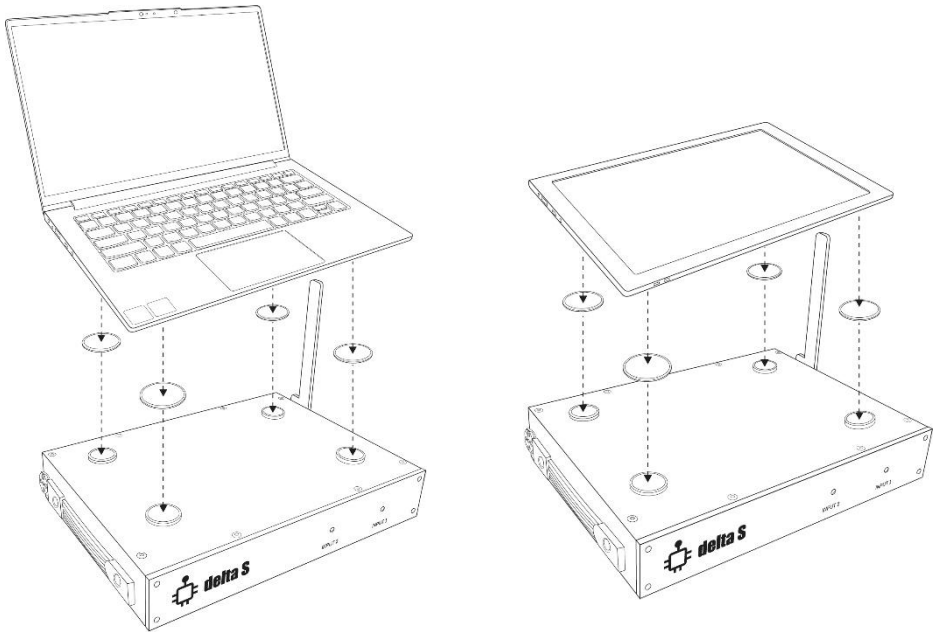
Порядок кріплення магнітних стікерів:

1. Очистіть та знежирте нижню панель ноутбука / планшета за допомогою очищувальної серветки.
2. Тимчасово прикрутіть широкодіапазонну антену ODA-4 до тримача на правій стороні головного блока.
3. Поставте ваш планшет або ноутбук на головний блок, підключіть до нього кабель живлення, інтерфейсні кабелі та адаптери USB, як описано в наступному розділі, та знайдіть оптимальне положення комп'ютера з урахуванням таких вимог:
    - Ноутбук або планшет не повинні виступати за габаритні краї головного блока.
    - Виступ USB-кабелів за межі головного блока можна мінімізувати, змістивши ноутбук або планшет у бік, протилежний до USB-роз'ємів.
    - Зміщуйте ноутбук або планшет вперед чи назад так, щоб підключені кабелі не впиралися в антени.
    - У разі використання планшета переконайтеся, що магнітні тримачі на головному блоці не викликають помилкового спрацьовування датчика Холла («закритої кришки») на планшеті. Якщо під час опускання планшета на магніти екран згасає або пристрій переходить у сплячий режим, необхідно підібрати інше положення (підніміть планшет, увімкніть екран і опустіть його знову, зміщуючи вліво-вправо або вперед-назад).
    - Ділянки поверхні на нижній панелі ноутбука, що торкаються магнітних тримачів, мають бути абсолютно рівними — без пластикових ніжок, ребер жорсткості чи вентиляційних отворів, оскільки саме на ці місця наклеюватимуться стікери. За потреби змініть положення ноутбука.



4. Запам'ятайте або позначте обране розташування і приберіть ноутбук / планшет з блока.

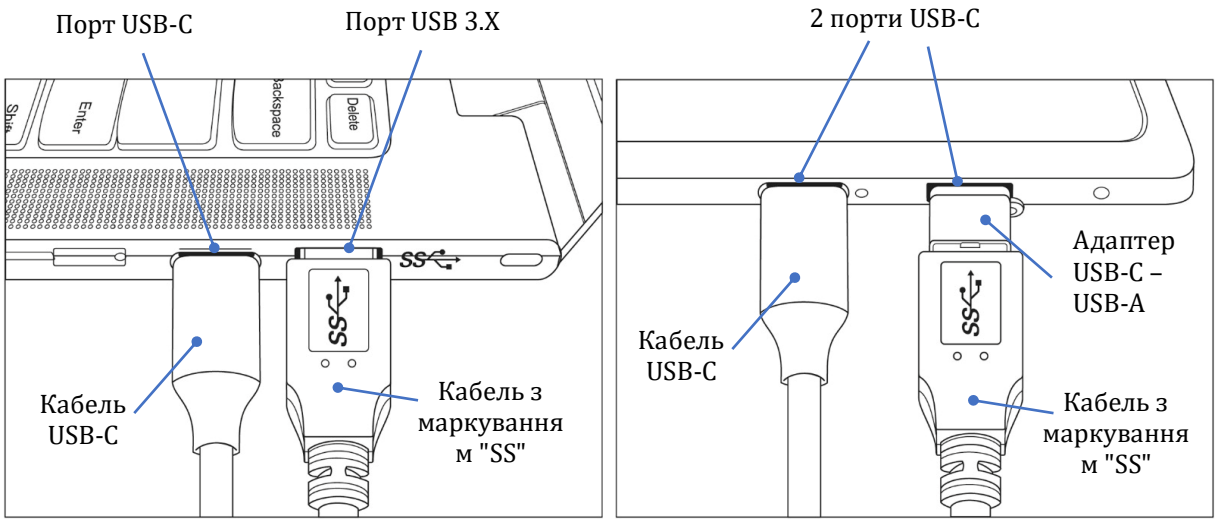
5. Розмістіть 4 магнітні стікери на магнітних тримачах клейкою стороною догори та зніміть із них захисну плівку. Вирівняйте стікери чітко по центру тримачів.
6. Зафіксуйте ноутбук / планшет над головним блоком в обраній раніше позиції, після чого рівно опустіть його і щільно притисніть до стікерів. Потримайте пристрій притиснутим протягом однієї-двох хвилин. Далі акуратно зніміть його, піднімаючи кути по черзі — стікери залишаться надійно приклеєними до нижньої панелі гаджета. Дайте клейовому шару остаточно полімеризуватися та уникайте багаторазового від'єднання пристрою від магнітів протягом перших 24 годин.



Підключення інтерфейсних кабелів

Система Delta S / Delta X оснащена двома USB-кабелями, які необхідно підключити до відповідних портів вашого ноутбука або планшета:

1. **Кабель із маркуванням «SS» (SuperSpeed):** призначений для керування системою та високошвидкісного обміну даними з аналізатором. Його необхідно підключати виключно до швидкісного порту USB 3.1 або USB 3.2, який має аналогічне маркування **«SS»** біля роз'єму на корпусі комп’ютера. Якщо такий порт формату USB-A відсутній, використовуйте комп'ютерний порт USB-C, підключивши кабель через перехідник (адаптер), що входить до комплекту поставки.
2. **Кабель USB-C:** призначений для додаткового живлення/інтерфейсу і має бути підключений до відповідного стандартного порту USB-C на вашому комп’ютері.



Підключення антен

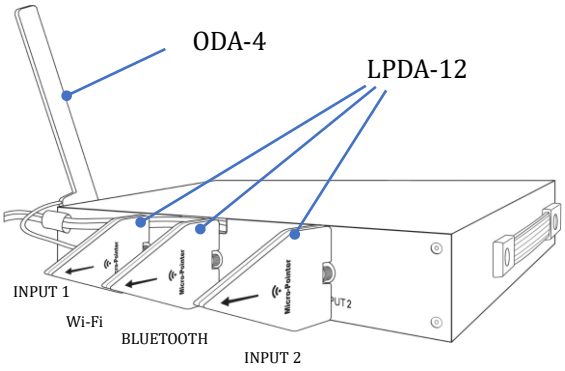
До комплекту поставки системи Delta S / Delta X входить набір спеціалізованих антен, кожна з яких оптимізована під конкретні завдання та частотні діапазони:

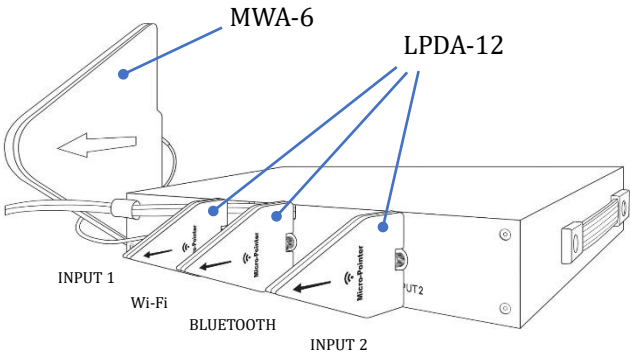
- **Антена ODA-4:** розроблена для покриття нижньої частини робочого діапазону. Вона має кругову (всеспрямовану) діаграму спрямованості, завдяки чому чудово підходить для загального моніторингу та ефективного використання в усіх режимах пошуку, зокрема в базовому режимі «Всі сигнали».
- **Антена MWA-6:** завдяки підвищеному коефіцієнту підсилення та високій чутливості в середній частині спектра (800–6000 МГц), ця антена є оптимальним вибором для сканування стільникових і бездротових стандартів. Вона демонструє високу ефективність у всіх режимах, і особливо в «Мобільні/GPS-трекери» та «Бездротові/ISM». Крім того, спрямований характер антени дозволяє значно прискорити процес точного визначення місця розташування (локалізації) передавача в режимах поглибленого дослідження діапазону або сигналу.
- **Антена LPDA-12:** працює в діапазоні 2–12 ГГц і використовується системою для сканування верхньої частини радіочастотного спектра, а також для паралельного аналізу бездротових мереж Wi-Fi та пристроїв Bluetooth Low Energy. Логоперіодична конструкція та чітка спрямованість цієї антени суттєво полегшують і прискорюють фізичний пошук і локалізацію прихованих джерел випромінювання.

Таблиця підключення антен:

Антена	**Delta S**	**Delta X**
ODA-4 – широкодіапазонна антена з круговою направленістю	INPUT 1	INPUT
MWA-6 – над-високочастотна направлена антена з діапазоном 800 МГц - 6 ГГц	INPUT 1	AUX1
LPDA-12 – над-високочастотна направлена антена з діапазоном 2-12 ГГц	INPUT 2	AUX2
LPDA-12 – над-високочастотна направлена антена з діапазоном 2-12 ГГц	BLUETOOTH	BLUETOOTH
LPDA-12 – над-високочастотна направлена антена з діапазоном 2-12 ГГц	Wi-Fi	Wi-Fi

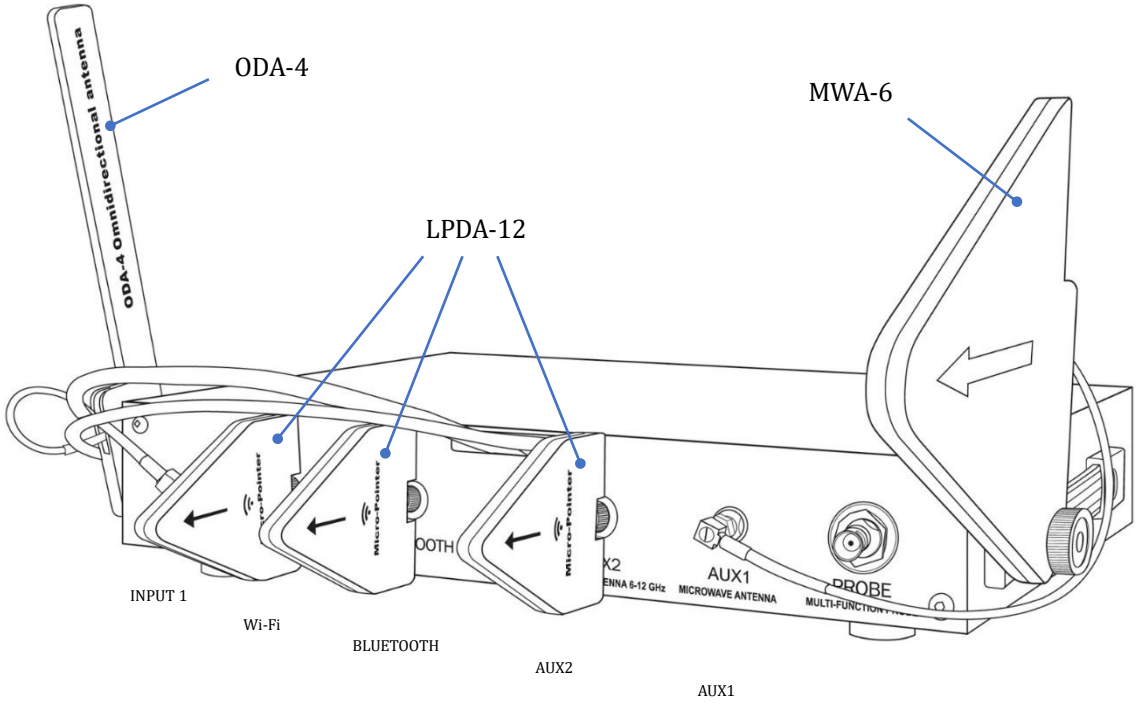
Підключення антен до Delta S V3





Вхід Delta S V3	**Антена**
INPUT 1	Залежно від поточного завдання оператор може підключити до входу INPUT 1 всеспрямовану антену ODA-4 або мікрохвильову антену MWA-6. Рекомендації щодо вибору антени: • Для пошуку в базовому режимі «Всі сигнали» використовується антена ODA-4. • Для режиму «Мобільні/GPS-трекери» антена обирається з огляду на габарити та конфігурацію зони пошуку. Наприклад, великогабаритні об'єкти (вантажні автомобілі, контейнери або масивні вантажі) ефективніше оглядати за допомогою спрямованої антени MWA-6, підключеної до цього входу. Порядок монтажу: Вибрану антену (ODA-4 або MWA-6) необхідно встановити вертикально на тримач із правого боку приладу та зафіксувати гвинтом. Після цього підключіть коаксіальний кабель антени до роз'єму INPUT 1
INPUT 2	Підключіть логоперіодичну антену LPDA-12 безпосередньо до високочастотного входу INPUT 2. Вона відповідатиме за сканування верхньої частини радіочастотного спектра
BLUETOOTH	Підключіть антену LPDA-12 безпосередньо до входу BLUETOOTH для забезпечення паралельного аналізу та локалізації пристроїв Bluetooth Low Energy.
Wi-Fi	Підключіть антену LPDA-12 безпосередньо до входу Wi-Fi для забезпечення фонового сканування та ідентифікації бездротових мереж Wi-Fi.

Підключення антен до Delta X G3/12



Вхід Delta X G3/12	Антена
INPUT	Широкосмугову антену ODA-4 необхідно встановити вертикально на тримач із правого боку пристрою та зафіксувати гвинтом. Підключіть коаксіальний кабель антени до роз'єму INPUT на задній панелі приладу.
AUX1	Прикрутіть мікрохвильову антену MWA-6 до тримача з лівого боку пристрою за допомогою гвинта. Під час встановлення розташуйте антену так, щоб її кабель був спрямований у бік оператора. Підключіть кабель антени до гнізда AUX1 на задній панелі.
AUX2	Прикрутіть логоперіодичну антену LPDA-12 безпосередньо (напряму) до високочастотного гнізда AUX2 на задній панелі пристрою.
BLUETOOTH	Підключіть антену LPDA-12 безпосередньо до входу BLUETOOTH для забезпечення сканування та локалізації пристроїв Bluetooth Low Energy.
Wi-Fi	Підключіть антену LPDA-12 безпосередньо до входу Wi-Fi для забезпечення сканування та локалізації пристроїв Wi-Fi.

Запуск програми

Запустіть програму «Breeze RF», скориставшись ярликом на Робочому столі або в меню «Пуск». Після відкриття головного вікна система автоматично розпочне пошук підключеного обладнання. Якщо обидва USB-кабелі підключені правильно, програма ідентифікує пристрій та запустить його ініціалізацію, перебіг якої відображатиметься на панелі статусу в нижній частині екрана.

Після успішної ініціалізації всі функції та режими програми стають повністю доступними. Якщо пристрій не підключено або не розпізнано, більшість елементів керування залишатимуться заблокованими.

Можливі причини проблем із розпізнаванням пристрою:

- **Проблеми з драйверами:** драйвери пристрою не встановлені або процес інсталяції програмного забезпечення було перервано чи завершено некоректно.
- **Помилка підключення USB:** високошвидкісний інтерфейсний кабель пристрою вставлений не до кінця або він підключений до звичайного повільного порту USB 2.0 замість швидкісного порту USB 3.x (з маркуванням «SS»).
- **Низький рівень живлення:** батарея ноутбука/планшета критично розряджена, через що операційна система може обмежувати живлення на USB-портах.
- **Невідповідність вимогам:** апаратна конфігурація комп'ютера (тип процесора або специфікація портів) не відповідає мінімальним технічним вимогам системи.

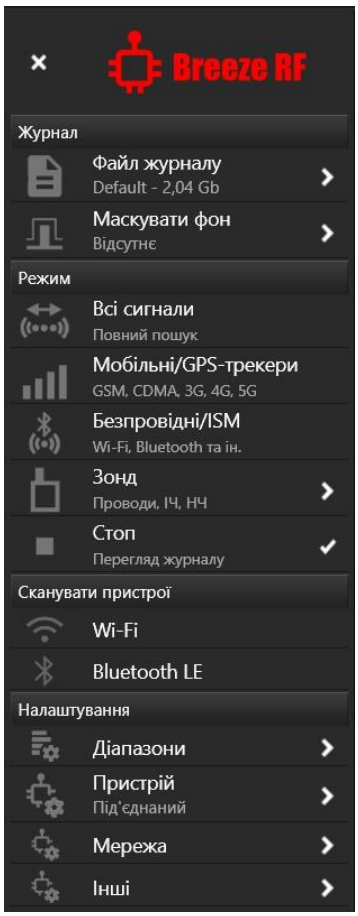
Обов'язкові налаштування під час першого запуску (виконуються ОДНОРАЗОВО):

1. **Вибір країни використання (для автоматичного налаштування таблиці діапазонів):**
   - Перейдіть у меню: **«Налаштування»** - **«Діапазони»** - **«Країна»**.
   - Виберіть потрібну країну зі списку та натисніть кнопку **«Застосувати»**. Примітка: обов'язково повторіть цю процедуру, якщо плануєте використовувати пошукову систему в іншій країні.
2. **Калібрування системи (процедура видалення власних шумів):**
   - Тимчасово від'єднайте всі антени від високочастотних входів пристрою.
   - Перейдіть у меню: **«Налаштування»** - **«Пристрій»** - **«Видалити шуми»**.
   - Натисніть кнопку **«Видалити шуми»** та дочекайтеся завершення процесу внутрішнього калібрування.

Функції програми та їх використання

Головне меню

Кнопка меню  у верхньому лівому кутку відкриває доступ до основних команд та інструментів налаштування системи:



«Журнал» - «Файл журналу»: керування збереженням даних, створення нових сесій, експорт та аналіз збережених результатів пошуку.

«Журнал» - «Маскувати фон»: процедура вимірювання та додавання поточної радіочастотної обстановки до активного журналу. Використовується для вилучення відомих безпечних сигналів (телебачення, радіомовлення тощо) з аналізу в режимах «Всі сигнали» або «Низхідні/Навігація».

«Режим»: вибір робочого режиму пошукової системи. Деякі режими (залежно від модифікації приладу) можуть активуватися та працювати одночасно.

«Сканувати пристрої»: ручне увімкнення або вимкнення фонового сканування бездротових мереж Wi-Fi та пристроїв Bluetooth Low Energy під час пошуку. У певних режимах ця функція активується автоматично.

«Налаштування» - «Діапазони»: керування конфігурацією частотних каналів — вибір регіонального розподілу під країну використання, ручне редагування меж діапазонів, зміна порогів чутливості тощо.

«Налаштування» - «Пристрій»: відображення поточної інформації про апаратний блок (серійний номер, версія прошивки), моніторинг його статусу та доступ до службових функцій (калібрування власних шумів).

«Налаштування» - «Мережа»: функція зарезервована розробником для майбутніх модифікацій і в поточних версіях Delta S / Delta X не використовується.

«Налаштування» - «Інші»: доступ до додаткових системних і користувацьких параметрів інтерфейсу та відображення даних.

Після вибору необхідних параметрів закрийте меню, щоб збільшити робочу зону екрана та розширити інформаційні панелі «Спектр» і «Тривоги».

Запис даних та робота з журналами

Файл журналу є єдиною базою даних поточної пошукової сесії, яка автоматично фіксує та зберігає таку інформацію:

- **Параметри фону:** збережену спектральну маску замаскованого фону.
- **Дані радіоефіру:** траси спектра за весь час моніторингу (історія для побудови графіка «водоспад»).
- **Аналітика сигналів:**
  - список виявлених сигналів у кожному діапазоні;
  - історію тривог для кожного окремого сигналу;

    - історію тривог для кожного частотного діапазону.
- **Моніторинг мереж Wi-Fi:**
    - точний список усіх виявлених пристроїв Wi-Fi;
    - історію активності кожного знайденого Wi-Fi пристрою;
    - лог взаємодії та зв'язків між пристроями всередині мережі Wi-Fi.
- **Моніторинг мереж Bluetooth Low Energy (BLE):**
    - список виявлених пристроїв;
    - історію активності для кожного знайденого пристрою.

Рекомендації щодо організації пошуку:

Рекомендується створювати **окремий файл журналу для кожного конкретного об'єкта** (приміщення, автомобіля тощо). У разі проведення повторного чи регулярного моніторингу цього ж об'єкта відкривайте той самий файл — це дозволить впорядковувати та порівнювати дані отримані під час різних сеансів.

Усі збережені спектральні траси можна згодом детально проаналізувати на графіках «Водоспад» (Waterfall) та «Спектр», а динаміку сплесків потужності — на графіку тривог.

Як активувати запис даних:

Накопичення та збереження інформації у файл журналу здійснюється двома способами:

1. **Автоматично:** якщо в налаштуваннях активовано функцію **«Автоматичний запис журналу»** (головне меню **«Налаштування»** - **«Інші»**).
2. **Вручну:** шляхом натискання кнопки **«Запис журналу»** на верхній інструментальній панелі інтерфейсу програми.

Як впевнитись що ведеться запис:

1. Поведінка графіка «Водоспад» (Waterfall)

Графік «Водоспад» безперервно накопичує спектральні дані під час пошуку, проте його поведінка кардинально змінюється залежно від режиму:

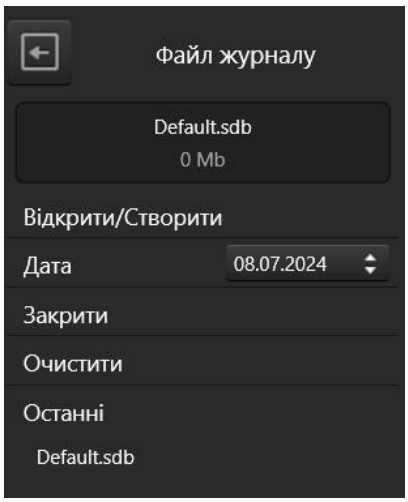
- Якщо запис НЕ ведеться: Графік повністю очищається щоразу, коли оператор прокручує або масштабує вікно спектра. Після цього «Водоспад» починає накопичувати траси спектра заново — і так до наступної зміни відображуваної ділянки.
- Якщо запис ВЕДЕТЬСЯ: Графік не стирається. Під час масштабування або прокручування він автоматично заповнюється даними спектра, які були збережені в журналі раніше.

2. Поведінка графіка «Тривоги» (Alarms)

Аналогічним чином поводиться й графік «Тривоги»:

- За активного запису: під час перемикання чи прокручування на інший часовий проміжок графік не очищається, а стабільно відображає всі збережені в журналі події та загрози, що відбулися у вказаний час.

Для вибору, створення нового або відкриття існуючого журналу перейдіть у головне меню: **«Журнал»** - **«Файл журналу»**. У цьому підменю зосереджені всі інструменти для керування базами даних пошукових сесій:



«Відкрити/Створити»: викликає діалогове вікно провідника. Для відкриття існуючого журналу виберіть потрібний файл на диску. Якщо необхідно створити новий файл — перейдіть у бажану папку, введіть у полі нову назву, і система запропонує автоматично створити чистий файл журналу.

Порада: Зберігайте всі файли журналів в постійній папці.

«Дата»: дозволяє вибрати та детально переглянути дані за певне число в режимі «Стоп» (аналіз архіву). Нові дати створюються в журналі автоматично, якщо під час проведення пошуку було активовано функцію запису.

«Закрити»: вивантажує поточний файл журналу з пам'яті програми. Коли файл журналу не відкритий, більшість аналітичних та пошукових функцій системи залишаються заблокованими.

«Очистити»: безповоротно видаляє всю накопичену інформацію (спектри, тривоги, логи BLE/Wi-Fi) з поточного відкритого файлу журналу, повністю звільняючи його для нового циклу вимірювань.

«Останні»: відображає список нещодавно відкриваних журналів, дозволяючи в один клік повернутися до аналізу попереднього об'єкта.

Натисніть кнопку зі стрілкою **"Назад"** щоб повернутись до головного меню.

Маскування фону

Маскування фону є однією з ключових і найважливіших операцій під час пошуку прихованих закладних пристроїв («жучків»). Ця процедура дозволяє вилучити з аналізу легальні зовнішні радіосигнали, такі як цифрове й аналогове телебачення, радіомовлення, службовий радіозв'язок, а також базові станції мобільного зв’язку. За звичайного моніторингу без використання маски ці «мирні» сигнали постійно викликають хибні спрацьовування, перевантажують таблицю тривог і відвертають увагу оператора від реальних загроз. Завдяки застосуванню маскування система Delta S / Delta X автоматично відфільтровує зовнішній радіофон і миттєво виявляє лише **локальні сигнали** — тобто ті, джерело яких розташоване безпосередньо всередині цільового приміщення. Саме такі сигнали становлять потенційну небезпеку, оскільки можуть здійснювати несанкціоновану передачу конфіденційної інформації за межі об'єкта.

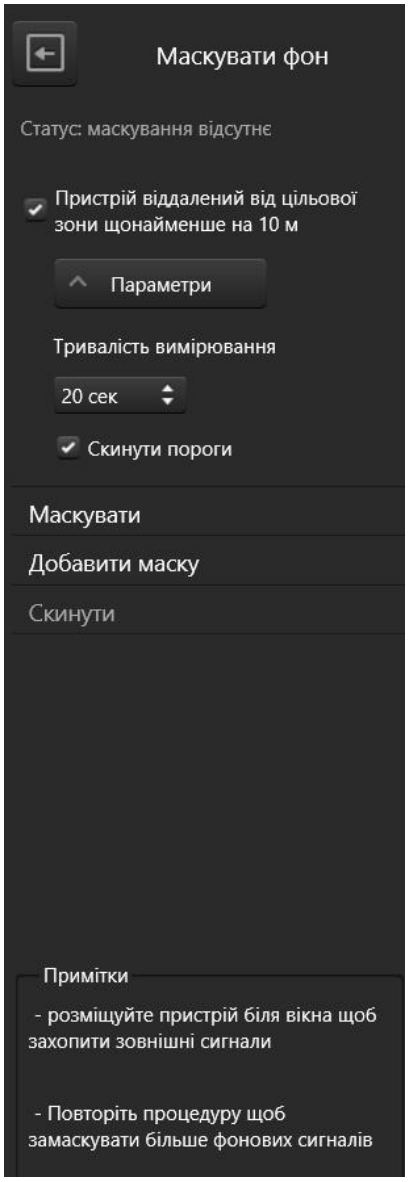
Коли необхідно виконувати маскування фону

- **Обов'язково:** Процедура виконується виключно перед початком роботи в режимах «Всі сигнали» та «Низхідні/Навігація».
- **Не потрібно:** Перед активацією режимів «Мобільні/GPS-трекери» та «Бездротові/ISM» маскування фону проводити не потрібно. У цих діапазонах виявлення та ідентифікація сигналів здійснюються за оптимізованим пороговим методом.

Порядок проведення процедури

Процедура маскування фону є швидкою та інтуїтивно зрозумілою. Загальний алгоритм дій:

1. **Вибір позиції для зняття фону:** До того як увійти з комплексом до цільового приміщення, розмістіть систему в точці, де забезпечується найкращий прийом зовнішніх міських радіосигналів, але на достатній відстані від об'єкта перевірки. **Оптимальні локації:** підвіконня у віддаленій кімнаті чи кінці коридору (на відстані **не менше 10 метрів** від цільового приміщення) або на вулиці біля будівлі (наприклад, у салоні автомобіля).
2. **Запуск вимірювання:** Перебуваючи у вибраній фоновій точці, увімкніть систему та активуйте процес створення маски через меню програми.



Перейдіть у головне меню: **«Журнал»** - **«Маскувати фон»**. Підтвердьте правильне розташування пошукового комплексу, активувавши галочку **«Пристрій віддалений від цільової зони щонайменше на 10 м»**. Після цього натисніть кнопку **«Маскувати»** та дочекайтеся завершення автоматичного процесу.

Функція **«Додати маску»** дозволяє накласти результати нового вимірювання на вже існуючу маску, суттєво підвищуючи точність фільтрації. Для досягнення максимального результату рекомендується проводити маскування в кількох різних точках ззовні об'єкта:

- У першій точці виберіть опцію **«Маскувати»** (створення базової маски).
- Перейдіть в іншу фонову точку і кілька разів скористайтеся функцією **«Додати маску».**

Після закінчення процедури створена спектральна маска автоматично збережеться в поточному файлі журналу. З цього моменту підготовку завершено: ви можете заходити в цільове приміщення та розпочинати сканування в режимі **«Всі сигнали»**.

«Скинути»: повністю видаляє поточні результати маскування фону та очищує спектральну маску в журналі.

Кнопка «Параметри»: відкриває доступ до налаштувань:

- **«Тривалість вимірювання»** — дозволяє збільшити час сканування радіофону. Більш тривалий аналіз дозволяє надійно зафіксувати та замаскувати непостійні (імпульсні або періодичні) сигнали, що мінімізує кількість хибних спрацювань під час пошуку.

«Скинути пороги» — автоматично повертає пороги чутливості для мобільних та бездротових діапазонів до заводських значень (за замовчуванням) під час виконання маскування.

Пошукові режими

Всі сигнали

Цей режим є основним і призначений для широкосмугового пошуку та виявлення всіх типів прихованих радіочастотних закладних пристроїв («жучків») у всьому робочому діапазоні частот системи.

Які сигнали виявляються:

- **Мобільні стандарти:** GSM, CDMA, 3G, 4G/LTE, а також найновіші мережі 5G.
- **Бездротові технології:** Wi-Fi (всі підтримувані діапазони), Bluetooth (включно з класичним та BLE), LoRa, DECT та ін.
- **Інші джерела випромінювання:** аналогові та цифрові радіомікрофони, бездротові приховані відеокамери, пульти дистанційного керування, компоненти систем «розумний дім», автомобільні сигналізації, радіостанції та будь-які інші локальні передавачі.

Під час роботи в цьому режимі система здійснює послідовне сканування та аналіз усіх категорій частотних розподілів: «Базові», «Мобільні», «Бездротові/ISM» та «Низхідні/Навігація» (якщо активно). Паралельно зі швидкісним спектральним аналізом програма виконує фонове виявлення пристроїв Bluetooth Low Energy (BLE) та Wi-Fi з логування їх активності.

Особливості відображення та логіка роботи

- **Категоризація сигналів:** Сигнали, що працюють усередині виділених стільникових або бездротових смуг, класифікуються та відображаються як «мобільні» або «бездротові» відповідно. Усі інші передавачі, що працюють на частотах поза цими специфічними стандартами, відображаються на шкалах і графіках «Базових» діапазонів.
- **Застосування маски:** Перед активацією режиму «Всі сигнали» **обов'язково необхідно виконати процедуру маскування фону**. Створена спектральна маска буде автоматично застосована до сегментів базових діапазонів (частот, які знаходяться поза межами мобільних та бездротових стандартів), що дозволить системі ігнорувати безпечні сигнали.

Налаштування чутливості та порогів

Радіус (відстань) виявлення та загальна чутливість системи задаються за допомогою порогів. Програма «Breeze RF» пропонує гнучку архітектуру налаштування:

- Поріг можна виставити індивідуально для кожного окремого діапазону.
- Можна встановити єдиний поріг для цілої категорії діапазонів (наприклад, окремо для всіх мобільних або всіх базових діапазонів).
- Можна змінити рівень чутливості глобально для всього спектра одночасно.
- **Принцип роботи для базових частот:** За умови наявності знятої маски фону, встановлені пороги базових діапазонів математично працюють як **зміщення (offset) маски**. Тобто лінія тривоги динамічно повторює форму амплітудного

рельєфу фону, піднімаючи або опускаючи загальну чутливість на задану оператором величину в децибелах (дБ).

Мобільні / GPS-трекери

Використання каналів стільникового зв'язку має суттєві переваги для організації прихованого стеження, що робить мобільні закладні пристрої вкрай небезпечними:

1. **Висока пропускна здатність:** швидкісні мобільні канали дозволяють передавати аудіо- та відеопотоки високої якості в реальному часі.
2. **Відсутність територіальних обмежень:** немає потреби розгортати пост контролю поблизу об'єкта стеження. Дані передаються через мережу Інтернет, зокрема із можливістю збереження у хмарних сховищах.
3. **Двосторонній зв'язок:** зловмисник може здійснювати гнучке дистанційне керування пристроєм (активація, зміна налаштувань тощо).
4. **Оптимальний канал для телеметрії:** мобільні мережі є ідеальною платформою для передачі координат транспортних засобів (GPS/ГЛОНАСС-трекери та маяки).
5. **Адаптивні режими передачі:** можливість накопичення інформації у внутрішню пам'ять пристрою («накопичувачі») з її подальшим швидкісним скиданням за розкладом або за запитом.
6. **Складність ідентифікації:** сигнал закладного пристрою повністю ідентичний трафіку звичайного смартфона, що дозволяє йому легко маскуватися під роботу телефонів сусідів або перехожих.

Особливості роботи режиму

Режим **«Мобільні / GPS-трекери»** оптимізований для цілеспрямованого пошуку мобільних пристроїв усіх типів та стандартів, включаючи GSM, CDMA, 3G, 4G/LTE та 5G на частотах до **6 ГГц** (або до **12 ГГц** залежно від апаратної модифікації комплексу). Під час його активації система зосереджує всі ресурси на скануванні та відображенні частотних діапазонів категорії «Мобільні».

- **Максимальна швидкість сканування:** Завдяки звуженню загального спектра аналізу та суттєвому зменшенню часового інтервалу (проміжку) вимірювань, система радикально збільшує швидкість роботи та ймовірність перехоплення надкоротких, імпульсних сигналів.
- **Сфера застосування:** Цей режим є рекомендованим для специфічних завдань, де пріоритетом є виявлення автомобільних GPS-трекерів (маячків) та прихованих відеокамер або мікрофонів що транслюють інформацію через мобільну мережу.

Налаштування чутливості

Дальність виявлення та спрацювання тривоги в цьому режимі регулюються за допомогою порогів:

- Можна налаштувати індивідуальний поріг чутливості для кожного конкретного мобільного діапазону.
- Можна встановити єдиний базовий поріг для всієї категорії «Мобільні» одночасно.

Детальні методики тактики пошуку та алгоритми локалізації стільникових пристроїв наведені в розділі «Рекомендації щодо пошуку».

Бездротові / ISM

Сучасні бездротові стандарти передачі даних та цивільні частотні діапазони ISM (Industrial, Scientific, Medical) часто використовуються зловмисниками для побудови прихованих каналів витоку аудіо- та відеоінформації.

Суттєві переваги бездротових закладних пристроїв:

1. **Доступність компонентів:** простота розробки та збирання «жучків» завдяки насиченості ринку готовими мініатюрними Wi-Fi, Bluetooth та ISM-модулями.
2. **Висока пропускна здатність:** ширина смуги частот бездротових стандартів є цілком достатньою для трансляції високоякісного цифрового звуку або відеопотоку в реальному часі.
3. **Гнучке керування:** можливість повноцінного дистанційного керування режимами роботи та налаштуваннями пристрою.
4. **Адаптивна передача (накопичувачі):** підтримка режимів накопичення інформації у внутрішній буфер із її подальшим швидкісним скиданням (пакетною передачею) за заданим розкладом або за запитом.
5. **Складність виявлення серед побутового шуму:** цифровий сигнал закладного пристрою повністю легальний за структурою, тому легко маскується під роботу звичайного домашнього/офісного Wi-Fi роутера, бездротової миші, смарт-годинника або інших побутових приладів.

Особливості роботи режиму

У режимі **«Бездротові / ISM»** система фокусує всі апаратні ресурси на скануванні частотних діапазонів лише однойменної категорії.

- **Максимальна ймовірність перехоплення:** Завдяки звуженню загальної смуги панорамного огляду, час повного циклу сканування критично зменшується. Це радикально підвищує ймовірність реєстрації та фіксації надкоротких, імпульсних і нестаціонарних сигналів.
- **Сфера застосування:** Режим рекомендовано використовувати у випадках, коли необхідно з максимальною точністю, швидкістю та надійністю виявити й локалізувати пристрої, що працюють за стандартами Wi-Fi, Bluetooth, LoRa, DECT, а також будь-які інші локальні передавачі на цих діапазонах.

Налаштування чутливості

Дальність виявлення та спрацювання тривоги регулюються за допомогою порогів:

- Програма дозволяє гнучко виставити індивідуальний поріг чутливості для кожного конкретного бездротового діапазону (наприклад, окремо для діапазону «ISM 2.4 ГГц»).
- Також можна встановити єдиний поріг для всієї категорії «Бездротові / ISM» загалом.

Детальні методики тактики тактичного пошуку та алгоритми локалізації пристроїв цієї категорії наведені в розділі «Рекомендації щодо пошуку».

Низхідні / Навігація

Цей режим призначений для виявлення та локалізації активних радіочастотних глушників (джамерів) мобільного зв'язку та навігаційних сигналів.

Принцип роботи РЧ-глушників:

- **Смуги мобільного зв'язку (Downlink):** Стільникові глушники створюють потужні загороджувальні перешкоди в діапазонах низхідної лінії зв'язку (Downlink) — тобто в тій частині спектра, де дані передаються від базової станції (вежі) на мобільний пристрій користувача.
- **Смуги навігації (GNSS):** Так звані «глушники GPS» генерують шум на частотах супутників, щоб маскувати легальні супутникові сигнали та перешкоджати навігаційним приймачам отримувати телеметрію, необхідну для точного розрахунку географічних координат.

Таким чином, для своєчасного виявлення та пошуку джерел штучних перешкод система здійснює постійний моніторинг смуг низхідної лінії мобільного зв'язку та глобальних навігаційних супутникових систем, таких як GPS, ГЛОНАСС, GALILEO та BeiDou.

Особливості активації режиму

Програмне забезпечення «Breeze RF» постачається із вбудованою базою даних, яка містить актуальний частотний розподіл для багатьох країн світу, зокрема специфікації низхідних каналів (Downlink) та діапазонів глобальних навігаційних супутникових систем (GNSS).

За замовчуванням під час первинного вибору країни діапазони низхідної лінії зв'язку та навігації автоматично **не додаються** до загального списку робочих діапазонів, щоб не перевантажувати інтерфейс під час стандартного пошуку закладних пристроїв.

Порядок активації режиму «Низхідні / Навігація»:

1. Перейдіть у головне меню: **«Налаштування»** - **«Діапазони»** - **«Країна»**.
2. Встановіть прапорці (галочки) напроти пунктів **«Низхідні лінії»** та **«Навігація»**.
3. Натисніть кнопку **«Застосувати»**, щоб система повторно сформувала та оновила список частот під ваші потреби.
4. Після виконання цих дій режим **«Низхідні / Навігація»** з'явиться в списку доступних режимів і стане активним для вибору.

Детальні методики протидії радіоелектронному придушенню та алгоритми локалізації джамерів наведені в розділі «Виявлення РЧ глушників та радіочастотних аномалій»

Користувач

Програмне забезпечення «Breeze RF» надає оператору можливість створювати необмежену кількість власних (кастомних) частотних діапазонів для їхнього вибіркового та цілеспрямованого сканування. Це дозволяє адаптувати систему під специфічні завдання радіомоніторингу або дослідження конкретних ділянок спектра.

Після активації режиму **«Користувач»** система повністю перемикає апаратні ресурси на сканування та відображення лише тієї категорії частот, яку сформував сам оператор. Усі інші стандартні діапазони тимчасово ігноруються, що суттєво підвищує швидкість аналізу заданих ділянок.

Цей режим з'являється в списку вибору та стає активним лише тоді, коли в загальному переліку частот присутній щонайменше один створений користувачем діапазон із міткою категорії «Користувач».

Як створити власний діапазон: Керування, додавання та редагування кастомних частотних смуг здійснюється через інженерне меню: **«Налаштування»** - **«Діапазони»**.

Зонд

Цей режим доступний виключно в пошукових комплексах серії Delta X.

У режимі **«Зонд»** система використовує спеціалізований пристрій для виявлення та локалізації дротових, оптичних та низькочастотних каналів витоку інформації. Комплекс дозволяє ідентифікувати такі типи загроз:

- **Дротові закладні пристрої:** стетоскопи та мікрофони, що здійснюють передачу перехопленої інформації високочастотним накладанням через силові лінії електромережі, слабкострумові телефонні лінії або структуровані кабельні системи Ethernet.
- **Оптичні канали витоку (ІЧ-передавачі):** приховані аудіо- та відеосистеми, які транслюють дані в невидимому для людського ока інфрачервоному (ІЧ) діапазоні спектра.
- **Низькочастотні аномалії (ПЕМВН):** побічні електромагнітні випромінювання та наведення від працюючої електронної апаратури та вузлів зв'язку в діапазоні низьких частот (НЧ), які можуть використовуватися для зняття інформації.

1. Детальний опис процедури підключення конвертерів, методики проведення перевірок сильних і слабкострумових мереж, а також тактика пошуку оптичних пристроїв наведені в розділі «Виявлення РЧ глушників та радіочастотних аномалій».

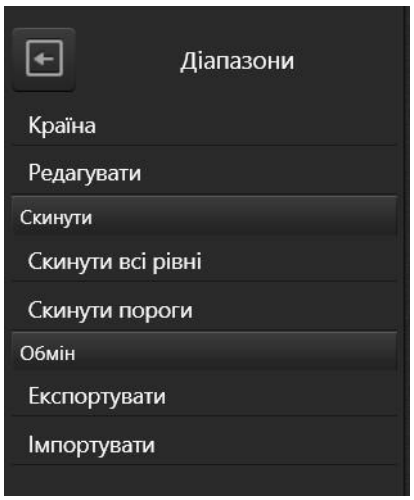
Режим "Стоп"

Цей режим є статичним (екранне оновлення спектра в реальному часі зупинено) і призначений для детального аналізу зібраних даних та адміністрування системи.
У режимі **«Стоп»** оператор може виконувати такі операції:

- **Робота з архівом журналу:** покроковий перегляд хронології подій, вивчення збережених спектральних трас на графіках «Водоспад» та аналіз таблиці виявлених сигналів чи пристроїв за будь-яку дату й час.
- **Зміна конфігурації:** редагування списку частотних діапазонів, встановлення індивідуальних або категорійних порогів чутливості, та ін.
- **Керування маскою:** запуск процедури маскування фону, накладання додаткових вимірів («Додати маску») або повне скидання поточних результатів маскування.
- **Пост-аналіз результатів:** ретельне вивчення графіків тривог, сортування та маркування сигналів за результатами пошукової сесії.

Налаштування – Діапазони

Для забезпечення максимальної точності та швидкодії системи вкрай важливо, щоб таблиця діапазонів у програмному забезпеченні повністю відповідала реальному частотному розподілу мобільного та бездротового зв’язку в регіоні проведення перевірки. Програмне забезпечення «Breeze RF» містить інтегровану базу даних з актуальними частотними планами для більшості країн та регіонів світу.



«Країна» - призначена для автоматичного заповнення таблиці робочих діапазонів відповідно до стандартів країни використання. Після активації цієї команди у верхній частині панелі «Рівень» з'явиться додаткова вкладка зі списком доступних країн. Оператору достатньо вибрати потрібну країну та натиснути «Застосувати».

Редагувати
Дозволяє увійти в режим редагування діапазонів (рекомендується для досвідчених користувачів).

Скинути пороги
Дозволяє скинути пороги всіх діапазонів до рівня за замовчуванням. Зазвичай ця команда виконується автоматично під час маскування фону.

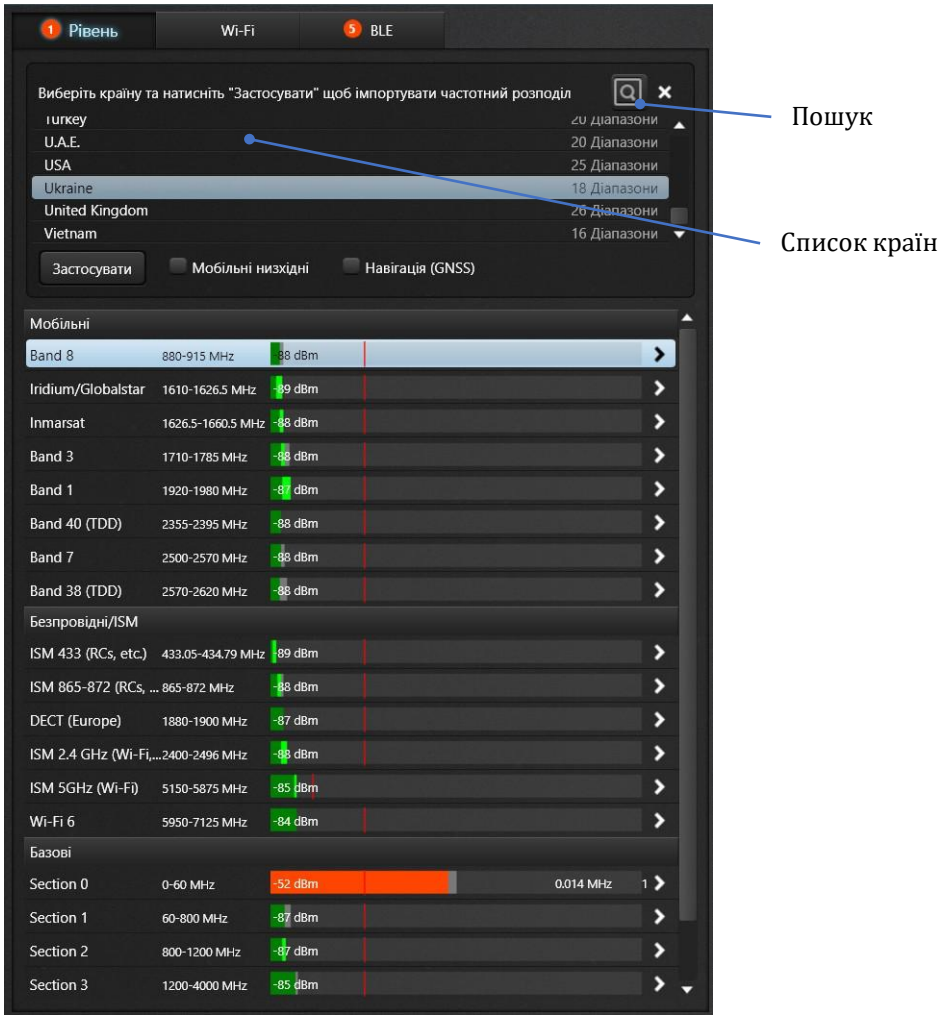
Експортувати
Дозволяє записати поточний список діапазонів у файл

Імпортувати
Дозволяє завантажити з файлу список діапазонів.

Вибір країни використання

Важливо: Виконуйте цю операцію під час першого запуску програми або у разі зміни країни, де система буде використовуватись.

Після вибору команди «Країна» у верхній частині панелі «Рівень» з'явиться додаткова вкладка зі списком доступних країн:

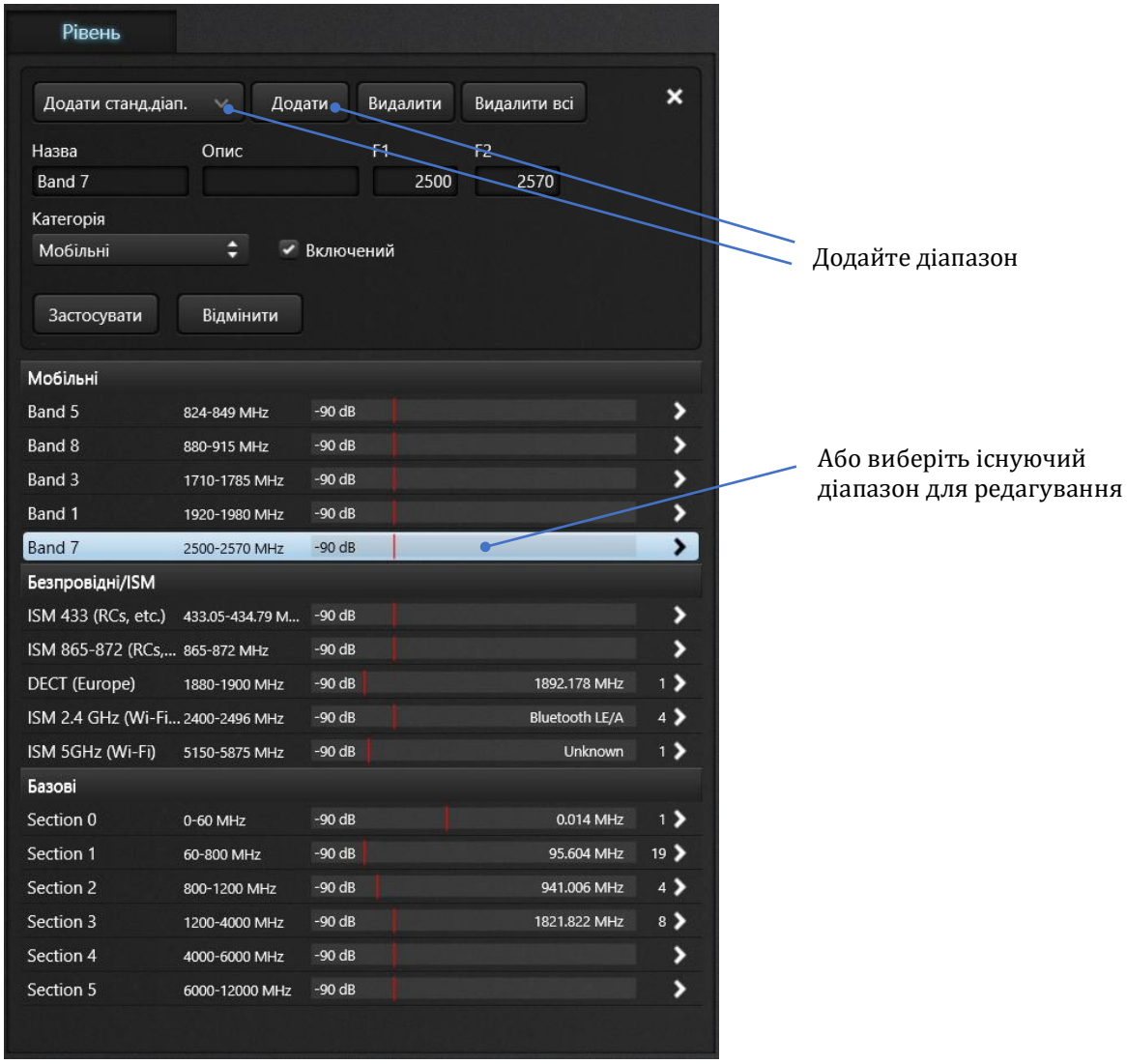


- Виберіть вашу **країну** у списку. За необхідності скористайтеся функцією пошуку
- Якщо ви плануєте використовувати режим «Низхідні/Навігація» (виявлення радіочастотних завад), встановіть галочку **«Мобільні низхідні»** та **«Навігація (GNSS)»**. За замовчуванням, ці два параметри відключені, тому вказані ділянки спектра не вносяться як окремі діапазони і аналізуються у складі базових діапазонів.
  Рекомендація: не додавайте ці діапазони без особливої необхідності
- Натисніть **«Застосувати»** або двічі клацніть на країну у списку. Таблиця діапазонів автоматично заповниться даними.

Якщо вашої країни немає у списку, виберіть варіант **«За замовчуванням (Default)»** та за потреби налаштуйте параметри вручну в режимі редагування. Щоб звірити актуальний розподіл частот мобільного зв'язку у вашому регіоні, скористайтеся відкритими інтернет-ресурсами, а потім внесіть відповідні зміни до таблиці діапазонів.

Редагування діапазонів

Щоб перейти до налаштувань, виберіть **«Редагувати»** в меню **«Діапазони»**. Керування діапазонами здійснюється за допомогою вкладеної панелі у верхній частині вікна **«Рівень»**.



Елементи керування та функції

- **Додати стандартний діапазон** — відкриває спливаюче меню зі списком усіх відомих стандартів мобільного та бездротового зв'язку (наприклад, діапазони 4G, 5G, Wi-Fi тощо). Знайдіть потрібний пункт, натисніть **«Додати»**, щоб внести його до загального переліку, або **«Закрити»** для скасування дії. Після цього натисніть **«Застосувати»**, щоб зберегти зміни.
  Порада: Додавайте лише ті діапазони, які дійсно використовуються у вашій країні.
- **Додати** — створює новий користувацький діапазон. Введіть назву, опис, частотні межі F1, F2 і натисніть **«Застосувати»**. За замовчуванням новий діапазон отримує категорію «Користувач», але за потреби її можна змінити.
- **Видалити** — вилучає поточний вибраний діапазон.
- **Видалити всі** — повністю очищає список діапазонів (усі елементи, крім базових, будуть видалені).
- **Застосувати** — підтверджує та зберігає всі поточні зміни.
- **Відмінити** — скасовує останні внесені зміни.

Параметри діапазону

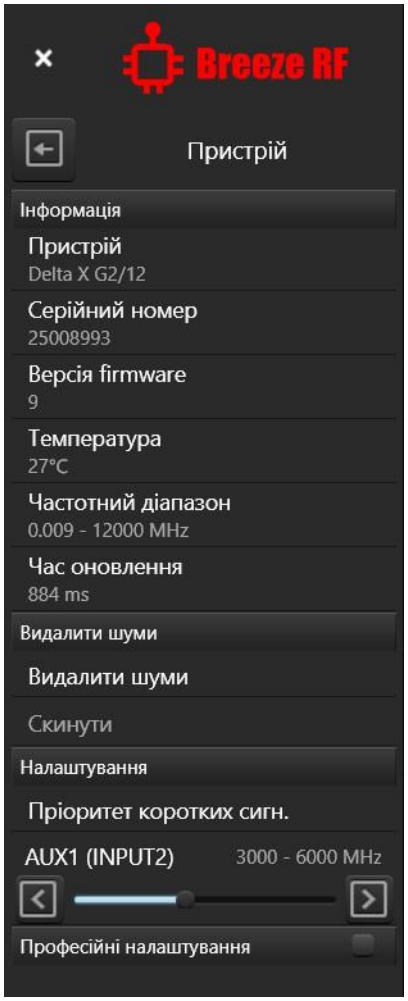
- **Назва**, **Опис** — текстові поля для ідентифікації діапазону. Вміст поля «Опис» відображається у списку в дужках.

- **F1, F2** — нижня та верхня частотні межі діапазону.
- **Категорія** — класифікація діапазону. Вибирайте значення «Користувач» під час створення власних, специфічних діапазонів.
- **Включений** — прапорець активації. Зніміть цю позначку для діапазонів, які ви хочете тимчасово пропустити під час пошуку, не видаляючи їх зі списку.

Важливо:

1. **Слідкуйте за тим, щоб мобільні та бездротові діапазони не накладалися один на один** (перетин із базовими діапазонами є нормою). За потреби скоригуйте частотні межі F1 та F2.
2. **Базові діапазони є вбудованими** в конфігурацію системи, тому вони не підлягають редагуванню чи видаленню.

Налаштування – Пристрій



Інформація
У цьому розділі відображається інформація про поточний стан та параметри підключеного обладнання:

- Назва підключеного пристрою
- Серійний номер
- Версія прошивки
- Температура
- Діапазон частот
- Час оновлення

Примітка: Час оновлення – це тривалість одного повного циклу сканування в поточному режимі пошуку. У режимі «Всі сигнали» час оновлення є найдовшим, оскільки система сканує весь доступний діапазон аналізатора. В інших (вужчих) режимах, а також під час перевірки окремого діапазону чи сигналу, смуга сканування звужується, завдяки чому час оновлення зменшується.

Видалити шуми – це функція, яка дозволяє пристрою мінімізувати власні шуми та компенсувати коливання динамічного діапазону. Таке калібрування робить спектральні траси більш плавними та легкими для аналізу. Видалення шуму достатньо виконати один раз для кожного комп'ютера, з яким використовується пошукова система.

Налаштування – Пріоритет коротких сигналів
Коли цю функцію увімкнено, суттєво підвищується ймовірність виявлення короткочасних пакетних (імпульсних) сигналів у мобільних та бездротових діапазонах. За увімкненої функції швидкість сканування спектра трохи знижується

Налаштування — AUX1 (INPUT2)
Цей параметр керує розподілом частот для другого антенного входу залежно від моделі пристрою:

- У **Delta X** другим входом є **AUX1** (комплектується спрямованою антеною **MWA-6**).
- У **Delta S** другим входом є **INPUT2** (комплектується спрямованою антеною **LPDA-12**).

Обидві ці антени є спрямованими. За замовчуванням система автоматично перемикається на вхід AUX1 / INPUT2 під час сканування ділянки спектра від 3 до 6 ГГц.

Навіщо змінювати частоту перемикання?

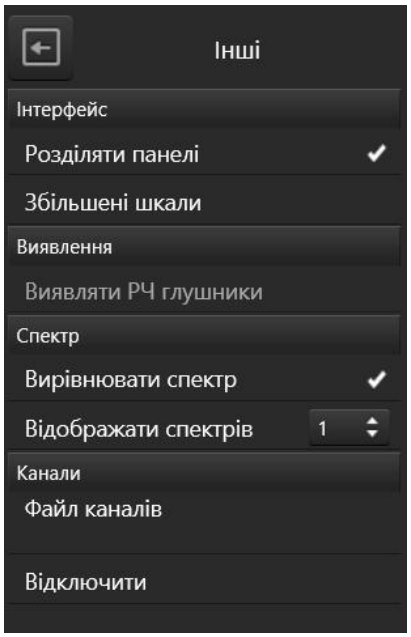
Інколи оператору необхідно змістити точку перемикання антен нижче 3 ГГц. Це дозволяє задіяти спрямовану антену на нижчих частотах і дає такі переваги:

- **Оптимізація діаграми спрямованості:** Використання спрямованої антени змінює зону охоплення та суттєво підвищує чутливість системи, що вкрай важливо під час огляду великогабаритних або протяжних об'єктів (наприклад, транспортних засобів).
- **Прискорення локалізації:** Спрямована антена дозволяє значно швидше й точніше визначити точне просторове розташування джерела загрози методом амплітудного пошуку (за напрямком максимального рівня сигналу).

Професійні налаштування
Ці параметри за замовчуванням приховані від користувача, щоб запобігти випадковій зміні критичних конфігурацій системи.

- **Високе підсилення (лише для Delta X)** — встановлює максимальну чутливість пристрою. Цей режим призначений виключно для специфічних експертних завдань. **Увага:** Увімкнення цієї функції може спричинити перевантаження вхідного тракту аналізатора. Активувати її у звичайних умовах не рекомендується — стандартної чутливості Delta X цілком достатньо для ефективного виконання будь-яких пошукових завдань.
- **Застосувати** — підтверджує та зберігає зміни, внесені у розділі професійних налаштувань.

Налаштування – Інші



Інтерфейс - розділяти панелі
Вибір варіанту відображення головного вікна програми.

- *З розділенням:* вікно розбивається на дві частини, що дозволяє одночасно бачити більше різнотипної інформації на одному екрані.
- *Без розділення:* панелі займають усю ширину вікна, забезпечуючи максимальну деталізацію вмісту та графіків.

Інтерфейс – збільшені шкали
Активує збільшений розмір шкал на панелі рівнів. Цей режим чудово підходить для моніторів із великою діагоналлю та високою роздільною здатністю (4K тощо).

Виявлення – Виявляти РЧ глушники
Вмикає додаткові індикатори «Рівень шуму» та особливий звуковий сигнал тривоги для фіксації роботи блокіраторів зв'язку (джамерів). Докладніші відомості та алгоритм роботи описано в спеціальному розділі «Виявлення РЧ глушників та радіочастотних аномалій».

Спектр – вирівнювати спектр
Активує додаткову цифровою обробку спектра, отриманого від приймача, для його більш згладженого та якісного відображення на графіку (лише Delta S).

Спектр – Відображати спектрів
Дозволяє оператору увімкнути одночасне відображення до 3 графіків спектра на відповідній панелі. Це рекомендовано для великих екранів високої роздільної здатності для одночасного візуального контролю декількох діапазонів.

Канали
Ця функція в поточних версіях систем **Delta S** та **Delta X** не використовується.

Панель інструментів

Панель інструментів розташована у верхній частині головного вікна та забезпечує швидкий доступ до ключових функцій системи.

Записувати журнал — активація функції безперервного запису поточної сесії (кнопка має бути в натиснутому стані).
Примітка: Ця кнопка приховується, якщо в налаштуваннях програми було увімкнено опцію **«Автоматичний запис журналу».**

Звукова тривога — звукове сповіщення оператора про виявлення загрози (перевищення встановленого порога чутливості). Інтенсивність звукового сигналу (частота клацання) автоматично зростає в міру наближення до джерела або збільшення потужності сигналу.

Утримання максимальної небезпеки — функція автоматично перемикає панель **«Рівень»** та графік спектра на **найнебезпечніший** діапазон або сигнал у цей момент.
Як це працює: Найнебезпечнішим система вважає той сигнал, який має найбільше перевищення порогу (надпороговий рівень). Це дозволяє миттєво реагувати на нові загрози.
Важливо: Не забудьте вимкнути цю функцію, якщо вам потрібно залишатися на одному діапазоні чи сигналі для його вивчення або налаштування його порогу.

Атенюатор — штучно знижує чутливість вхідного тракту для полегшення локалізації потужних джерел випромінювання.
Коли використовувати: Якщо рівень сигналу сягає -25.. 20 дБм і на сусідніх частотах з'являються видимі спотворення спектра (перевантаження).
Особливість: Функція доступна лише в режимах детального дослідження окремого діапазону чи сигналу й автоматично вимикається під час виходу з них.

Демодуляція — дозволяє прослуховувати аналогові сигнали (наприклад, FM-радіомовлення або аудіосупровід аналогового ТБ) в реальному часі. Функція доступна лише в режимах детального дослідження окремого діапазону чи сигналу й автоматично вимикається під час виходу з них.
Робота з цифровими сигналами: Цифрові стандарти (мобільний зв’язок, Wi-Fi тощо) декодувати звуком неможливо, проте в режимі AM вони мають характерне звучання (дзижчання, тріск).
Налаштування:

- **Режим** – вид демодулятора (AM, FM та ін.)
- **BW** —смуга пропускання демодулятора (можна регулювати в межах від 5 кГц до 200 кГц)
- **Вибір частоти** здійснюється за допомогою синього вертикального курсора що з’являється на графіку спектра в цьому режимі

Особливість: Функція активна тільки під час дослідження конкретного діапазону/сигналу й вимикається автоматично під час повернення до загального огляду.

Real-Time (Аналіз у реальному часі)
Real-Time переводить пристрій у режим безперервного аналізу у фіксованій смузі без перестроювання по частоті (сканування). Ширина ділянки, що аналізується одночасно, відповідає параметру Real-Time Bandwidth і становить від 24 до 27 МГц, в залежності від моделі обладнання. Функція доступна лише в режимах детального дослідження окремого діапазону чи сигналу й автоматично вимикається під час виходу з них.

Що забезпечує режим Real-Time?

На відміну від звичайного сканування, де аналізатор послідовно «перебирає» ділянки спектра й може пропустити швидку зміну ефіру, режим Real-Time здійснює безперервний захват усього зазначеного вікна. Це дає такі переваги:

- **Максимальна ймовірність фіксації:** дозволяє гарантовано виявляти надкороткі імпульсні загрози (short bursts), які звичайний режим сканування може пропускати.
- **Ефективний аналіз та локалізація:** забезпечує миттєве відображення зміни потужності сигналу під час фізичного пошуку джерел, що мають дуже короткий час існування в ефірі.

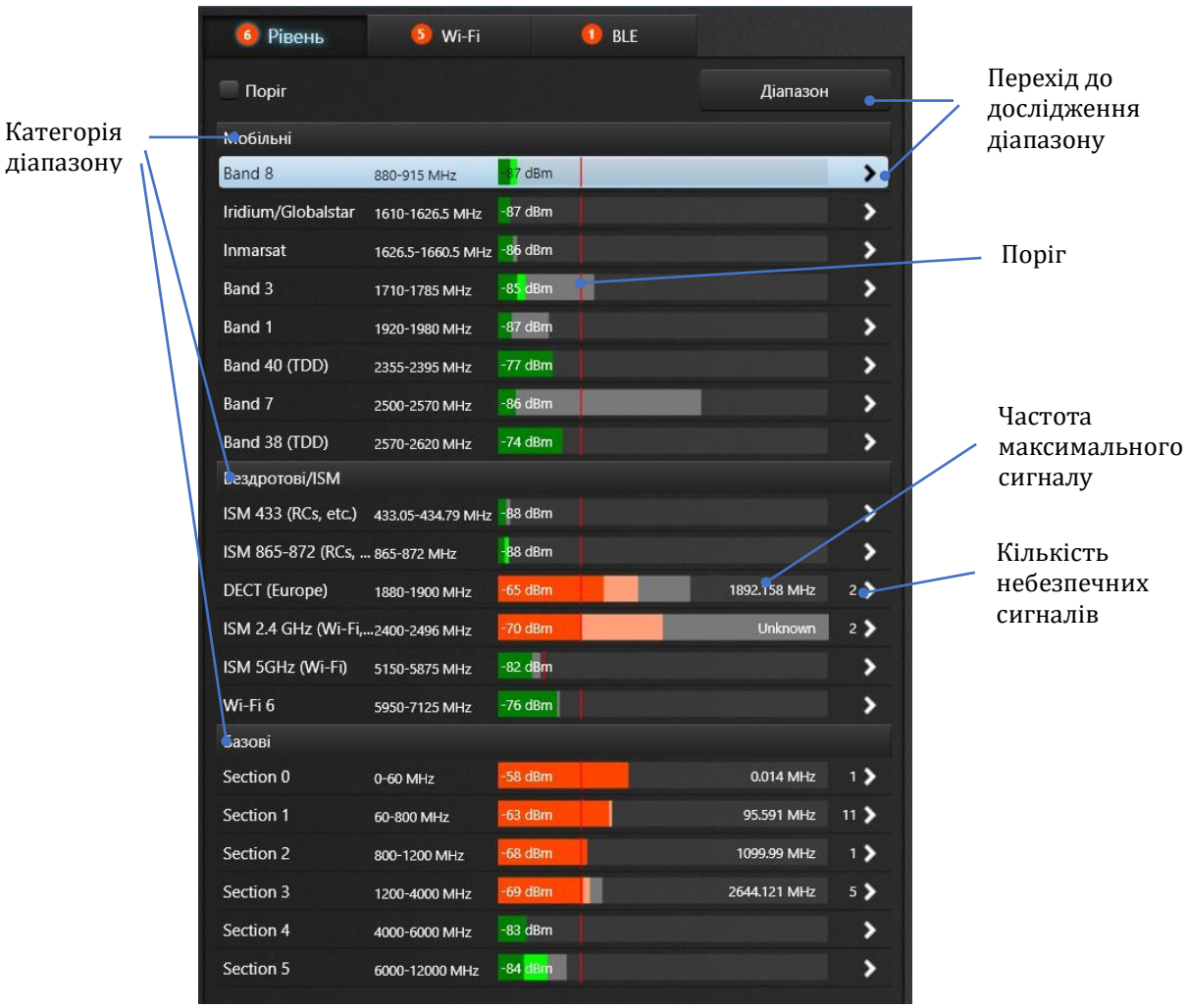
Коли використовувати режим Real-Time?
Під час **локалізації (фізичного пошуку)** окремих джерел випромінювання або конкретних каналів бездротового зв'язку: Wi-Fi, Bluetooth, 4G/5G, BLE-міток тощо.
Керування частотою: Вибір центральної частоти для аналізу в реальному часі здійснюється за допомогою **синього вертикального курсора**, який з'являється на графіку спектра після активації цього режиму. Встановіть його мишею або пальцем (якщо екран сенсорний) на потрібний сигнал.

Сервісні налаштування (права сторона панелі)

- **Віртуальна клавіатура** — якщо кнопку затиснуто, у разі активації будь-якого текстового поля на екрані автоматично з'являтиметься плаваюча клавіатура. Функція незамінна під час роботи із системою на планшетах (наприклад, для швидкого редагування назв діапазонів).
- **Тема** — швидке перемикання між темним та світлим режимами інтерфейсу. За замовчуванням встановлено темну тему, оскільки вона є менш обтяжливою для зору під час тривалого моніторингу.
- **Мова** — вибір мови інтерфейсу користувача.

Панель "Рівень"

Однією з головних переваг програмного забезпечення «Breeze RF» є автоматична обробка спектральних даних, які надходять від пристроїв Delta S та Delta X. Система самостійно розпізнає та зберігає сигнали, а також вимірює їхні рівні у відповідних діапазонах. Результати обробки спектра відображаються на панелі **«Рівень»** у вигляді наочного списку діапазонів із кольоровими шкалами. Це дозволяє оператору, не заглиблюючись у ручний аналіз радіоефіру, відстежувати загальну картину й миттєво реагувати на небезпечні ділянки.



Як працюють шкали та тривоги:

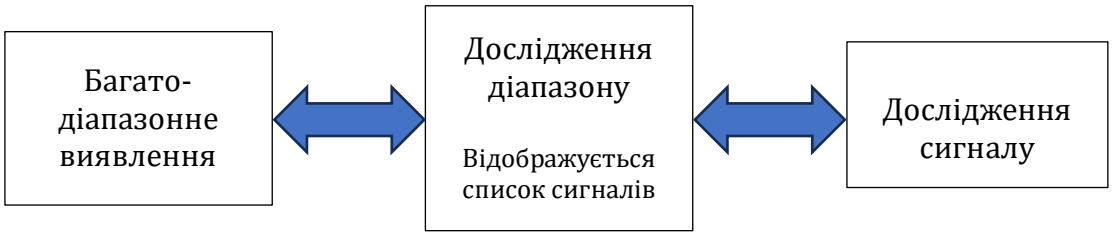
- **Зростання рівня:** Шкала автоматично збільшується, якщо в межах діапазону з'являється новий сигнал або пошуковий комплекс наближається до передавача.
- **Зміна кольору:** У разі перевищення встановленого порога колір шкали змінюється із **зеленого** на **червоний**.

Багаторівневий аналіз (ієрархія пошуку)

Програмне забезпечення підтримує три послідовні рівні деталізації ефіру, що дозволяє оператору ефективно звужувати зону пошуку:

- **Багатодіапазонне виявлення (загальний огляд):** Основний режим роботи системи, під час якого скануються всі вибрані частотні діапазони відповідно до поточного завдання. Оператор бачить загальну картину радіоефіру.
- **Дослідження діапазону (деталізація ділянки):** Оператор може детально перевірити підозрілий діапазон, натиснувши кнопку **«Діапазон»** або стрілку поруч із його назвою. У цьому режимі панель відображає інтегральний рівень усього діапазону та окремий список усіх сигналів усередині нього (кожен зі своєю шкалою рівня).
- **Дослідження сигналу (точковий аналіз):** Для перевірки конкретної частоти оператор переходить на найнижчий рівень, натиснувши кнопку **«Сигнал»** або стрілку поруч із ним. Панель фокусується виключно на параметрах та індикації рівня одного цього конкретного сигналу, що дозволяє розпочати його фізичну локалізацію.

Автоматичне фокусування: Під час переходу до конкретного діапазону або сигналу графік спектра автоматично масштабується, відображаючи саме цю частотну ділянку.



Розподіл сигналів в базових та мобільних діапазонах
Під час вимірювання рівня у **базових діапазонах** система автоматично ігнорує сигнали, які належать до мобільних, бездротових та інших «спеціалізованих» категорій.

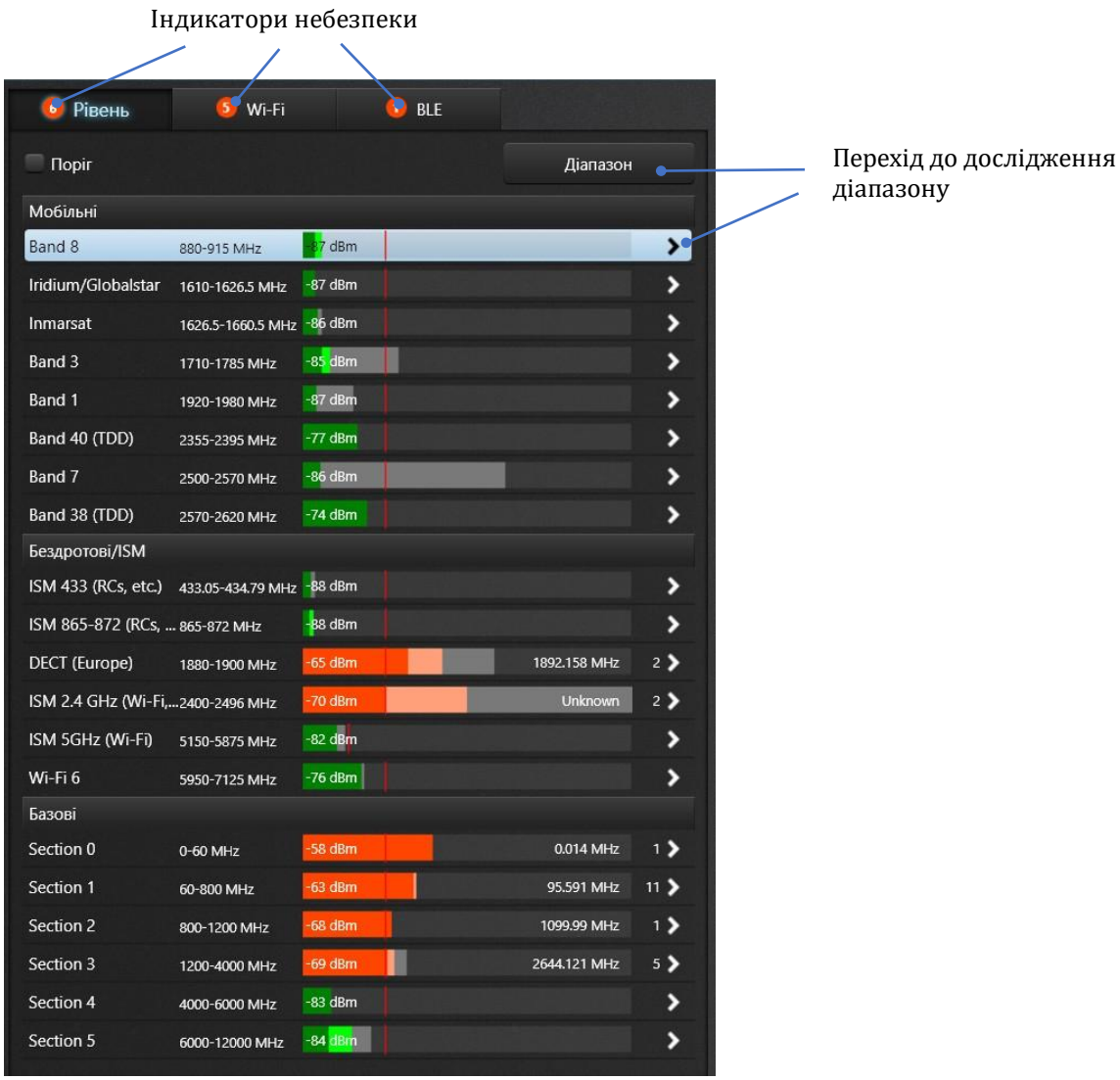
- Завдяки цьому сигнали стільникового зв'язку чи Wi-Fi не впливають на індикацію базових діапазонів і відображаються виключно у своїх профільних категоріях («Мобільні», «Бездротові/ISM» тощо).
- Шкали базових діапазонів фіксують сигнали лише поза межами відомих мобільних та бездротових стандартів, що критично важливо для виявлення «нестандартних» закладних пристроїв.

Типи вимірюваних рівнів
Для кожного діапазону та сигналу система одночасно розраховує та відображає три значення рівня:

1. **Поточний рівень** (миттєво зростає та миттєво спадає) — відображається **яскраво-зеленим** або **яскраво-червоним** кольором.
2. **Піковий рівень** (зростає миттєво, але згасає із затримкою) — відображається **світло-зеленим** або **світло-червоним** кольором. Допомагає фіксувати імпульсні сигнали.
3. **Максимальний зареєстрований рівень** (запам’ятовує найвище значення за всю сесію) — відображається **сірим** кольором.

Налаштування порога
Поріг спрацьовування тривоги для діапазону можна гнучко налаштовувати вручну в межах від
-85 до -20 дБм або від -95 до -20 дБм (діапазон налаштування залежить від вибраного рівня підсилення пристрою).

Мультидіапазонне вимірювання



Усі частотні діапазони відповідно до обраного режиму скануються та відображаються на інформаційній панелі. Для кожного діапазону зазначаються його назва, опис, робоча частота, рівні сигналів (поточний, піковий та максимальний зареєстрований), а також кількість загрожуючих сигналів та об'єкт із найвищим рівнем небезпеки. Діапазони згруповано за категоріями.

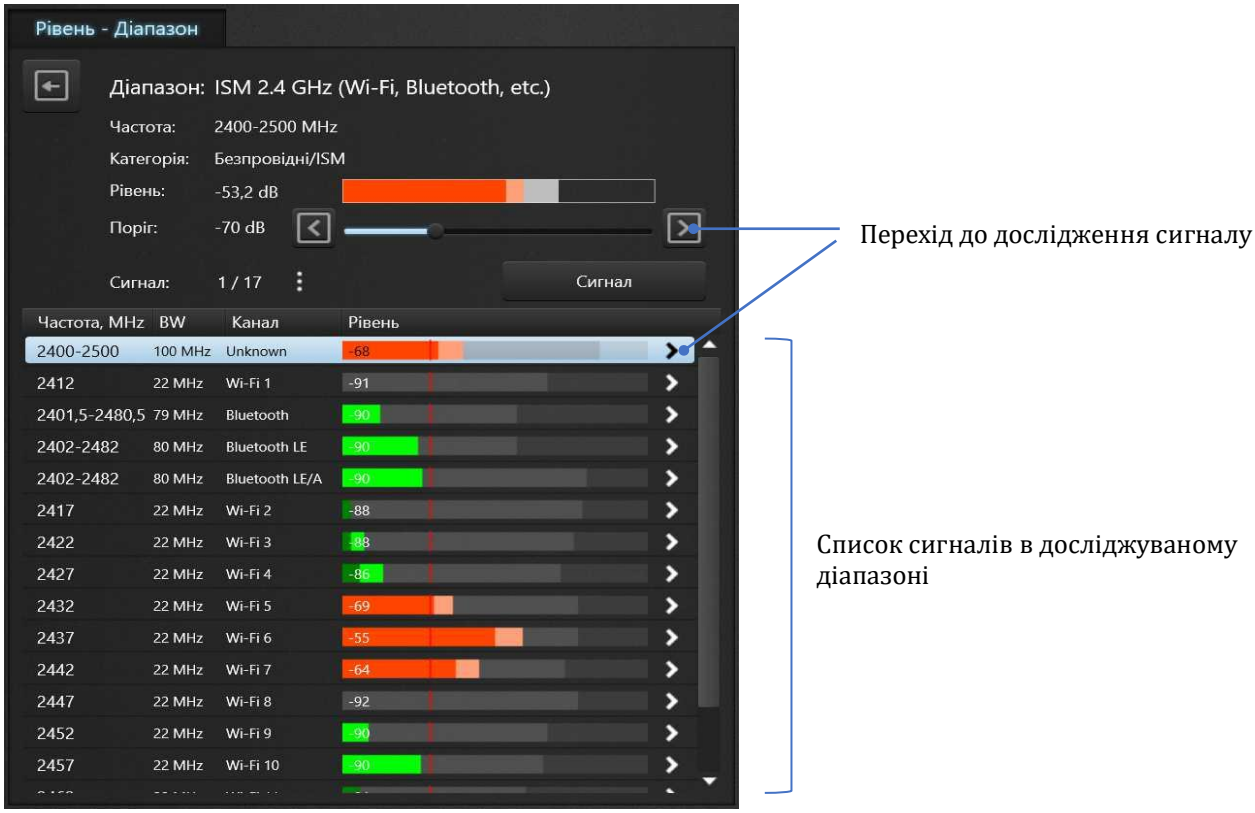
Індикатори небезпеки на вкладках показують кількість небезпечних записів в таблиці відповідної вкладки.

Подвійне клацання (клік) на рядку діапазону автоматично масштабує графік спектра для його детального аналізу.

Активуйте функцію **«Поріг»**, щоб налаштувати рівні спрацьовування. Параметри порога можна застосувати для окремого діапазону, певної категорії або для всіх діапазонів одночасно.

Дослідження діапазону

Виберіть потрібний діапазон і натисніть стрілку **«Зайти»** поруч із ним або скористайтеся кнопкою **«Діапазон»**, щоб перейти до режиму дослідження окремого діапазону. Панель **«Рівень»** набуде такого вигляду:



У цьому режимі система сканує виключно вибраний діапазон, відображаючи його параметри та детальний список сигналів. Для кожного сигналу зазначаються частота, смуга пропускання, назва каналу, а також поточний, піковий і максимальний зареєстрований рівні.

Використовуйте цей режим для точного визначення джерел загрози в межах діапазону та переходу до їх детального аналізу. Режим дослідження одного діапазону ефективний, якщо необхідно локалізувати кілька сигналів одночасно або коли сигнал постійно змінює частоту (скаче по діапазону). Оскільки в цьому разі аналізується значно менша ділянка спектра, швидкість сканування зростає, що суттєво підвищує ймовірність фіксації надкоротких (імпульсних) сигналів.

Одинарне клацання (клік) на сигналі — автоматично зсуває (центрує) графік спектра на частоту цього сигналу.

Подвійне клацання (клік) на сигналі — підлаштовує масштаб смуги відображення та фокусує графік спектра на вибраному сигналі.

За потреби ви можете відкоригувати рівень **порога** для поточного діапазону.

Над списком сигналів відображається інформація про номер поточного об'єкта та їх загальну кількість, а також кнопка виклику додаткового меню. У цьому меню доступні такі команди:

- **«Видалити сигнал»**
- **«Видалити всі сигнали в межах діапазону»**
- **«Видалити всі сигнали»**

Очищення списку сигналів може знадобитися для скидання результатів «злиття» сигналів, що виникає внаслідок роботи автоматичного алгоритму розпізнавання. Після видалення всі активні в цей момент сигнали будуть автоматично ідентифіковані та наново внесені до списку. Поводьтеся з цією функцією обережно, щоб випадково не втратити історію вимірювань підозрілого сигналу.

Натисніть кнопку **«Назад»**, щоб вийти з режиму дослідження та повернутися до загального списку.

Дослідження сигналу

Виберіть потрібний сигнал і натисніть стрілку **«Зайти»** поруч із ним або скористайтеся кнопкою **«Сигнал»**, щоб перейти до режиму дослідження сигналу. Панель **«Рівень»** набуде такого вигляду:

У цьому режимі оператор може детально вивчити окремий сигнал, конкретний канал (наприклад, 12-й канал Wi-Fi) або сітку каналів (наприклад, канали Bluetooth Low Energy).

Тут смуга вимірювання є мінімальною, завдяки чому швидкість сканування та ймовірність реєстрації короткочасних сигналів досягають свого максимуму. Режим

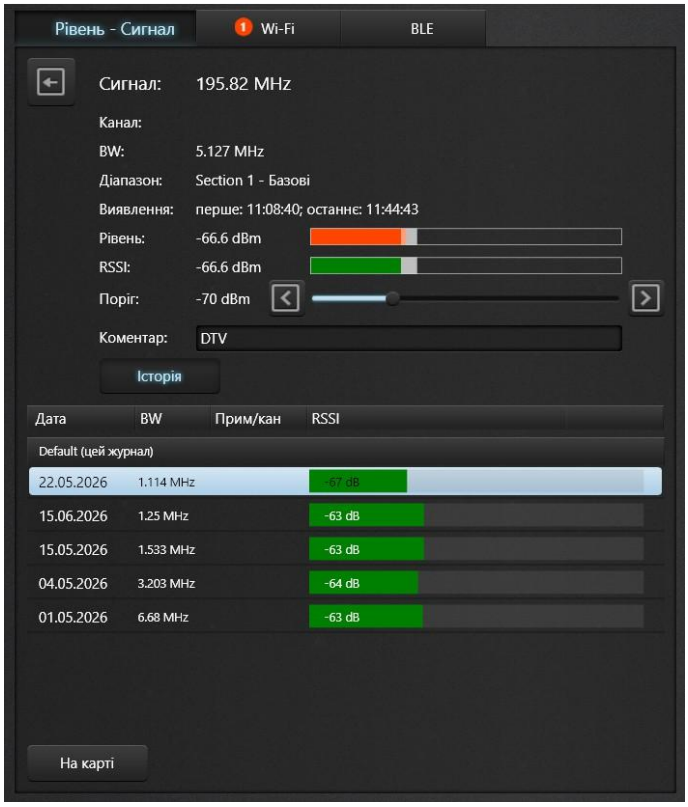
дослідження сигналу ідеально підходить для аналізу та локалізації імпульсних джерел випромінювання, таких як пристрої Wi-Fi, 4G/LTE, 5G тощо.

Параметри, що відображаються на панелі:

- **Сигнал** — центральна частота сигналу або початкова й кінцева частоти сітки каналів.
- **Канал** — назва каналу або сітки каналів.
- **BW (Bandwidth)** — значення смуги пропускання.
- **Діапазон** — назва діапазону, до якого входить поточний сигнал (канал).
- **Виявлення (перше, останнє)** — часові рамки першої та останньої реєстрації сигналу (каналу).
- **Рівень** — відносний рівень сигналу з урахуванням маскування фону.
- **RSSI** — абсолютний рівень сигналу (без урахування маскування).
- **Поріг** — дозволяє оперативно змінювати поріг діапазону безпосередньо під час локалізації сигналу.
- **Коментар** — поле для введення користувацького текстового коментаря до сигналу.
- **«Історія»** - призначена для перевірки появи поточного сигналу в інших базах даних (минулих сесіях моніторингу).

Робота з історією сигналу

Якщо кнопка **«Історія»** затиснута, у нижній частині панелі з’являється список журналів і дат, в яких фіксувався такий самий або схожий сигнал. Оператор може порівняти смугу сигналу (BW), коментар (канал) та його рівень RSSI. Для зручності аналізу дати групуються за журналами.



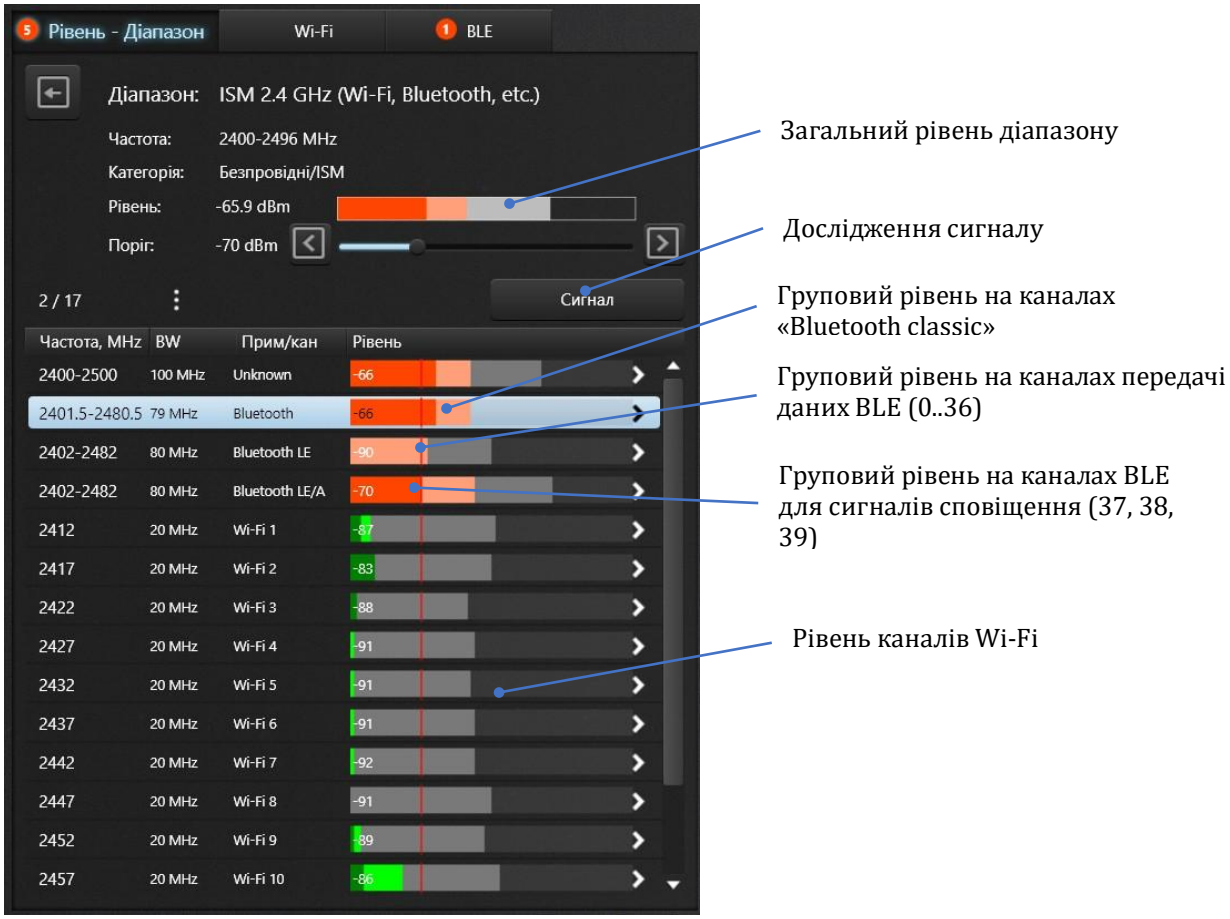
Рекомендація: Зберігайте всі файли журналів в одній спільній папці. У такому разі програма зможе автоматично просканувати їх та виявити аналогічну активність цього джерела в минулому.

Натисніть кнопку **«Назад»**, щоб вийти з режиму дослідження сигналу.

Використання панелі «Рівень» для пошуку бездротових сигналів

Алгоритм розпізнавання сигналів працює інакше в ISM-діапазонах «ISM 2.4 GHz (Wi-Fi, Bluetooth)» та «ISM 5 GHz (Wi-Fi)».

Для виявлення Bluetooth Low Energy, Bluetooth Classic та Wi-Fi використовуйте режим дослідження окремого діапазону «ISM 2.4 GHz» та «ISM 5 GHz»:



На відміну від стандартних діапазонів, де кожна окрема ділянка перевищення порога вважається самостійним сигналом, у цих ISM-діапазонах ідентифікація відбувається відповідно до вбудованої у програму сітки частот бездротових стандартів.

У разі виявлення сигналів, що використовують технологію швидкого перескоку частоти по сітці каналів — наприклад, Bluetooth Low Energy, — програма не створює окремий запис для кожного активного каналу. Замість цього система додає один загальний сигнал (наприклад, «Bluetooth LE») і надалі контролює його сумарний рівень по всій частотній сітці. Це суттєво знижує інформаційне навантаження на таблицю сигналів і значно спрощує локалізацію джерела загрози.

Специфіка групування бездротових стандартів у таблиці:

- **Сигнал «Bluetooth LE»** — це згруповані канали передачі даних стандарту BLE (з 0 по 36). Він відображає наявність та рівень сигналу з'єднаних BLE-пристроїв, що активно обмінюються даними.
- **Сигнал «Bluetooth LE/A»** — це згруповані канали сповіщення (Advertising) стандарту BLE (37, 38 і 39). Він інформує про наявність нез'єднаних BLE-пристроїв, які транслюють усеспрямовані пакети про свою присутність, а також показує їхній поточний рівень сигналу.
- **Сигнал «Bluetooth»** — це згруповані канали класичного стандарту Bluetooth Classic (з 0 по 78).
- **Сигнал «Wi-Fi ___»** — окремі канали Wi-Fi, що відображаються без групування (кожен канал окремим рядком).
- **Сигнал «Unknown»** — усі інші виявлені сигнали, параметри яких не відповідають критеріям жодного з наведених вище бездротових стандартів, подані у згрупованому вигляді.

Особливості відображення параметрів:

- **У разі групування каналів** (як для Bluetooth) у полі **«Частота»** відображаються початкова та кінцева частоти сітки відповідного стандарту, а в полі **«BW»** — смуга частот, що відповідає цій сітці.
- **Поле «Прим/кан» містить** назву бездротового стандарту та номер каналу або діапазон каналів (а також текстовий коментар оператора за його наявності).

Автоматичне розпізнавання бездротових сигналів та їхнє внесення до підсумкової таблиці відбувається лише за умови перевищення встановленого порогового значення. Своєчасно коригуйте рівень порога для забезпечення необхідної чутливості та відсікання фонових завад.

Порядок використання:

- Перейдіть до дослідження діапазону **«ISM 2.4 GHz (Wi-Fi, Bluetooth)»**, якщо під час загального пошуку в ньому зафіксовано підвищений рівень сигналу.
- Для підвищення надійності результату (враховуючи складність виявлення імпульсних сигналів у режимі широкодіапазонного аналізу) виконайте додатковий прохід приміщенням у режимі дослідження діапазону **«ISM 2.4 GHz (Wi-Fi, Bluetooth)»**, скануючи простір, конструкції та об'єкти більш детально.
- Переходьте до дослідження окремого сигналу в разі виявлення високого рівня випромінювання та виконуйте пошук джерела (локалізацію), орієнтуючись на амплітудні показники рівня.

У режимі **дослідження сигналу** шкали відображають параметри окремого сигналу/протоколу (поточний, піковий, максимальний та абсолютний RSSI). У разі групування, рівень сигналу вимірюється по сітці частот, за можливості обходячи сигнали інших протоколів які можуть виникати на тих же частотах.

Чутливість (дальність виявлення)

Оскільки одні й ті самі канали використовуються багатьма пристроями одночасно, дальність виявлення таких протоколів, як BLE (у з'єднаному стані) або Bluetooth Classic, безпосередньо залежить від наявності інших активних пристроїв у радіусі прийому. Ці пристрої, попри їхню безпечність, створюватимуть постійний підвищений рівень шуму

на шкалах та на графіку історії, змушуючи оператора піднімати поріг виявлення. Як наслідок, слабкі сигнали від небезпечних джерел виявлятимуться з меншої відстані.

Зважаючи на це, під час дослідження діапазону **«ISM 2.4 GHz»** рекомендується:

- Деактивувати (вимикати) всі безпечні джерела радіосигналу в зоні пошуку та навколо неї на час перевірки — зокрема Bluetooth усіх видів та інші бездротові девайси.
- Зміщувати нижню частоту перемикання на **AUX1 / INPUT 2** до значень нижче **2400 МГц**, щоб задіяти мікрохвильову (НВЧ) антену.
- Оглядати конструкції та предмети на мінімальній дистанції (50 см), постійно змінюючи просторову орієнтацію антени та уважно стежачи за рівнями протоколі
- Для тривалого радіомоніторингу залишати систему на певний час у режимі дослідження діапазону **«ISM 2.4 GHz»**, розміщуючи її якомога ближче до цільової зони та спрямовуючи на неї мікрохвильову антену.

Для розуміння дистанції огляду використовуйте наступні емпіричні дані щодо дальності виявлення BLE-пристрою у з’єднаному стані:

Умови навколишнього середовища	**Орієнтовна дальність виявлення**
Сільська місцевість (чистий ефір)	2-3 м
Міське середовище, низька насиченість гаджетами	1-2 м
Міське середовище, висока насиченість гаджетами (зашумлений ефір)	0.5 м

Нижче наведено приклад виявлення пристрою BLE у з’єднаному стані, який активно здійснює обмін даними (сигнал «Bluetooth LE»):

Панель **«Тривоги»** дозволяє чітко зафіксувати всі стадії процесу пошуку:

1. **Фіксація фону:** Постійний фоновий рівень сигналу **Bluetooth LE** становив близько **-60 дБм**.
2. **Локалізація джерела:** Під час переміщення системи в просторі було виявлено та локалізовано активний пристрій, що відобразилося у вигляді зростання рівня сигналу до **-26 дБм**.
3. **Продовження перевірки:** Пошук було продовжено у звичайному режимі, після чого рівень випромінювання знову впав до фонового значення (близько **-60 дБм**), що свідчить про віддалення від джерела.

Виявлення Wi-Fi та Bluetooth Low Energy

Пошукові комплекси останнього покоління дозволяють сканувати та виявляти пристрої на глибшому рівні шляхом аналізу окремих радіочастотних пакетів:

- **Wi-Fi** (точки доступу, нез'єднані та з'єднані клієнти).
- **Bluetooth Low Energy** (нез'єднані пристрої, що транслюють пакети сповіщення **Advertising**).

Таке сканування забезпечує вищу чутливість, збільшує дальність виявлення та надає можливість локалізувати кожен окремий пристрій. Детальнішу інформацію наведено в розділах **«**Виявлення пристроїв Wi-Fi**»** та **«**Виявлення пристроїв Bluetooth Low Energy**».**

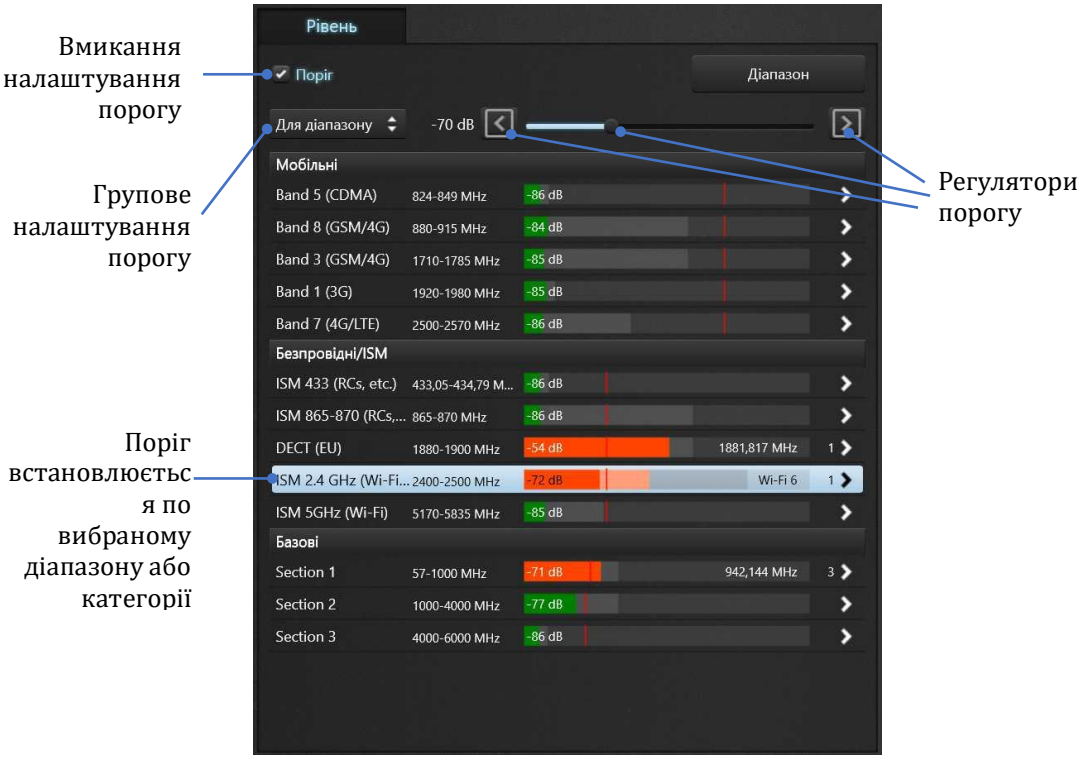
Використовуйте панель **«Рівень»** для виявлення інших протоколів або їхніх підвидів (зокрема Bluetooth Classic та BLE у з'єднаному стані).

Налаштування порогів діапазонів

Рівень порога діапазону визначає чутливість системи до виявлення сигналів. Коли поточний рівень сигналу перевищує встановлений поріг, система фіксує тривожну подію: графічна шкала стає червоною, вмикається звукова сигналізація, а інформація про подію автоматично реєструється в журналі.

Що нижчий поріг, то слабші (більш віддалені) сигнали здатна виявити система. Відповідно, зниження порога збільшує дальність виявлення, а його підвищення — зменшує її.

Система Delta S / Delta X дозволяє задавати індивідуальні пороги для кожного діапазону окремо, регулюючи дистанцію фіксації різних типів загроз. Допустимий діапазон значень: від -85 дБм до -20 дБм (і від -95 дБм до -20 дБм у режимі високого підсилення/High Gain).



Покрокова інструкція з налаштування порога:

1. Переконайтеся, що панель **«Рівень»** перебуває у стандартному режимі, та активуйте перемикач **«Поріг»** у її верхній частині.
2. Виберіть потрібний діапазон у списку на панелі.
3. Змінюйте значення порога за допомогою регулятора у верхній частині екрана.
4. Виберіть наступний діапазон і повторіть процедуру.
5. **Групове налаштування:** Ви можете змінити поріг одночасно для всієї категорії або для всіх діапазонів одразу. Для цього виберіть відповідний пункт у спадному списку поруч із регулятором.
6. Коли система працює в режимах **Дослідження діапазону** або **Дослідження сигналу**, регулятор порога постійно доступний у верхній частині робочої панелі.

Скидання до заводських параметрів:

Ви можете миттєво повернути пороги всіх діапазонів до початкових значень за допомогою команди **«Скинути пороги»** у меню «Налаштування» - «Діапазони».

Заводські налаштування є оптимальними для більшості завдань, забезпечуючи високу чутливість за мінімальної кількості хибних спрацювань від завад віддалених сигналів: -75 дБм для базових діапазонів та -70 дБм для всіх інших.

Практичні рекомендації:

- **Не встановлюйте занадто низький поріг (-85...-80 дБм):** Це призведе до надмірної кількості тривожних подій від передавачів, розташованих далеко за межами зони пошуку. Рекомендується тримати поріг вищим, щоб обмежити радіус виявлення кількома метрами й мінімізувати хибні спрацювання.
- **Не встановлюйте занадто високий поріг (-40...-20 дБм):** Це призведе до критичної втрати чутливості, і система не зможе зафіксувати навіть близькі джерела випромінювання.

Експериментальне визначення дальності виявлення
Оптимальне співвідношення між порогом і реальною відстанню до об'єкта можна встановити дослідним шляхом за допомогою звичайного мобільного телефона або тестової точки доступу Wi-Fi.
Поступово віддаляючись від тестового пристрою під час його активної передачі даних, ви побачите, як змінюється рівень сигналу на графіку, що дозволить точно підібрати необхідний поріг під габарити вашого приміщення.
Важливо: Під час тестування пристрій повинен безперервно транслювати сигнал. Для мобільного телефона надійним способом є активація вихідного голосового дзвінка або виклику через месенджер (наприклад, WhatsApp). Пам'ятайте: якщо на телефоні увімкнено Wi-Fi й виконано підключення до точки доступу, трафік піде через Wi-Fi. Якщо Wi-Fi вимкнути — телефон перейде на мобільний інтернет (3G/4G/5G).

Орієнтовна відповідність порога та відстані виявлення (для Wi-Fi або мобільного зв'язку):

Рівень сигналу (рівень порога)	**Орієнтовна відстань виявлення**
-80 dBm	5-20 метрів
-70 dBm	4-10 метрів
-60 dBm	3-8 метрів
-50 dBm	2-5 метрів
-40 dBm	1-3 метри
-30 dBm	<2 метрів

Пороги базових діапазонів (особливості роботи з маскуванням)
За умови активації функції маскування фону, пороги базових діапазонів працюють як математичне зміщення (offset) відносно лінії адаптивної маски, отриманої під час сканування безпечного оточення.

- **Збільшення порога** зміщує лінію маски вгору, відповідно зменшуючи чутливість системи до дрібних коливань ефіру.
- **Зменшення порога** опускає лінію маски ближче до рівня фону, що пропорційно підвищує чутливість пошукового комплексу.

Виявлення пристроїв Wi-Fi

Як зазначалося раніше, протокол Wi-Fi може використовуватися як канал передачі негласно отриманої аудіо-, відео- чи іншої інформації. Він забезпечує високу якість зв’язку, широку пропускну здатність, дуплексний канал та можливість дистанційного керування. У поєднанні з накопичувачем пам'яті це дозволяє створювати закладні пристрої високого професійного рівня.

Особливості загроз, пов'язаних зі стандартом Wi-Fi:

- **Режим радіомовчання (Stealth-mode):** можливість накопичувати інформацію в пам'яті та передавати її протягом коротких інтервалів часу.
- **Адаптивний вихід в ефір:** активація передачі лише тоді, коли заздалегідь визначений «отримувач» даних з’являється у зоні радіозв’язку.
- **Доступність приймального обладнання:** відсутність потреби у спеціальних засобах прийому — отримувачем може бути звичайний смартфон, планшет або комп’ютер.

- **Гнучкість топології мережі:** можливість роботи в режимах точки доступу (Access Point), станції (клієнта) або однорангової мережі (Ad-Hoc / Wi-Fi Direct).
- **Маскування в каналі:** робота в межах каналів наявних на об'єкті пристроїв Wi-Fi.
- **Маскування в радіочастотному полі:** фізичне розташування впритул до легальних пристроїв Wi-Fi компанії.
- **Імітація та підміна:** клонування наявних точок доступу з копіюванням їхніх MAC-адрес, SSID та інших атрибутів, або створення SSID, схожих на легальні.
- **Використання легальної інфраструктури:** у разі зламу або отримання пароля — використання корпоративної точки доступу для трансляції перехоплених даних.
- **Складність ідентифікації:** висока насиченість сучасних приміщень пристроями Wi-Fi та Bluetooth (зокрема BLE) ускладнює роботу звичайних радіочастотних детекторів або аналізаторів спектра. Працюючи в одному діапазоні, ці пристрої унеможливлюють локалізацію конкретного джерела енергетичним методом (за рівнем сигналу).

Зважаючи на такі технічні можливості, стандарт Wi-Fi є однією з пріоритетних загроз. Тому виявлення та аналіз кожного окремого пристрою Wi-Fi є критично важливою складовою пошукових робіт.

Вбудований бездротовий модуль Delta S / Delta X виконує сканування пристроїв Wi-Fi паралельно зі спектральним аналізом та дозволяє проаналізувати кожен окремий пристрій. Ця функція вмикається автоматично в режимах «Всі сигнали» та «Бездротові/ISM», а для інших пошукових режимів її можна активувати вручну.

Програмне забезпечення BreezeRF має вбудований **алгоритм визначення типу пристрою** (точка доступу, нез'єднана станція або з'єднаний клієнт) та постачається з файлами даних що забезпечують ідентифікацію виробника.

Антена, що відповідає за сканування Wi-Fi, розташована на задній панелі приладу та має відповідне маркування.

Реєстрація даних
Коли увімкнено запис журналу, система автоматично реєструє таку інформацію, отриману під час сканування Wi-Fi:
- таблицю виявлених пристроїв;
- таблицю взаємозв'язків між пристроями;
- історію активності для кожного пристрою.

Ці дані надійно зберігаються в журналі й можуть бути переглянуті або проаналізовані в будь-який момент.

Звукова тривога
Якщо на загальній інструментальній панелі активовано функцію **«Звукова тривога»**, у разі появи в ефірі Wi-Fi-пристрою з високим (небезпечним) рівнем сигналу програма сповістить оператора **особливим двотональним сигналом**.
Цей аудіосигнал суттєво відрізняється від стандартного «клацання», яке генерується під час тривожних подій у діапазонах спектрального аналізу, що дозволяє оператору на слух миттєво ідентифікувати активність саме в бездротових мережах.

Швидкість виявлення

Бездротовий модуль працює у двох режимах:

- **Виявлення всіх пристроїв** — режим, у якому відбувається послідовний моніторинг усіх каналів Wi-Fi із фіксованим часом перебування на кожному з них.

  Оскільки загальна кількість каналів у діапазонах 2.4 ГГц та 5 ГГц є значною, а модуль залишається на кожному каналі протягом обмеженого проміжку часу (ігноруючи інші канали в цей момент), ймовірність реєстрації поодинокого Wi-Fi-фрейма (кадра) є невисокою.

  Проте завдяки фоновому моніторингу Wi-Fi під час спектрального аналізу та збільшенню загального часу сканування, шанси на виявлення пристроїв суттєво зростають.

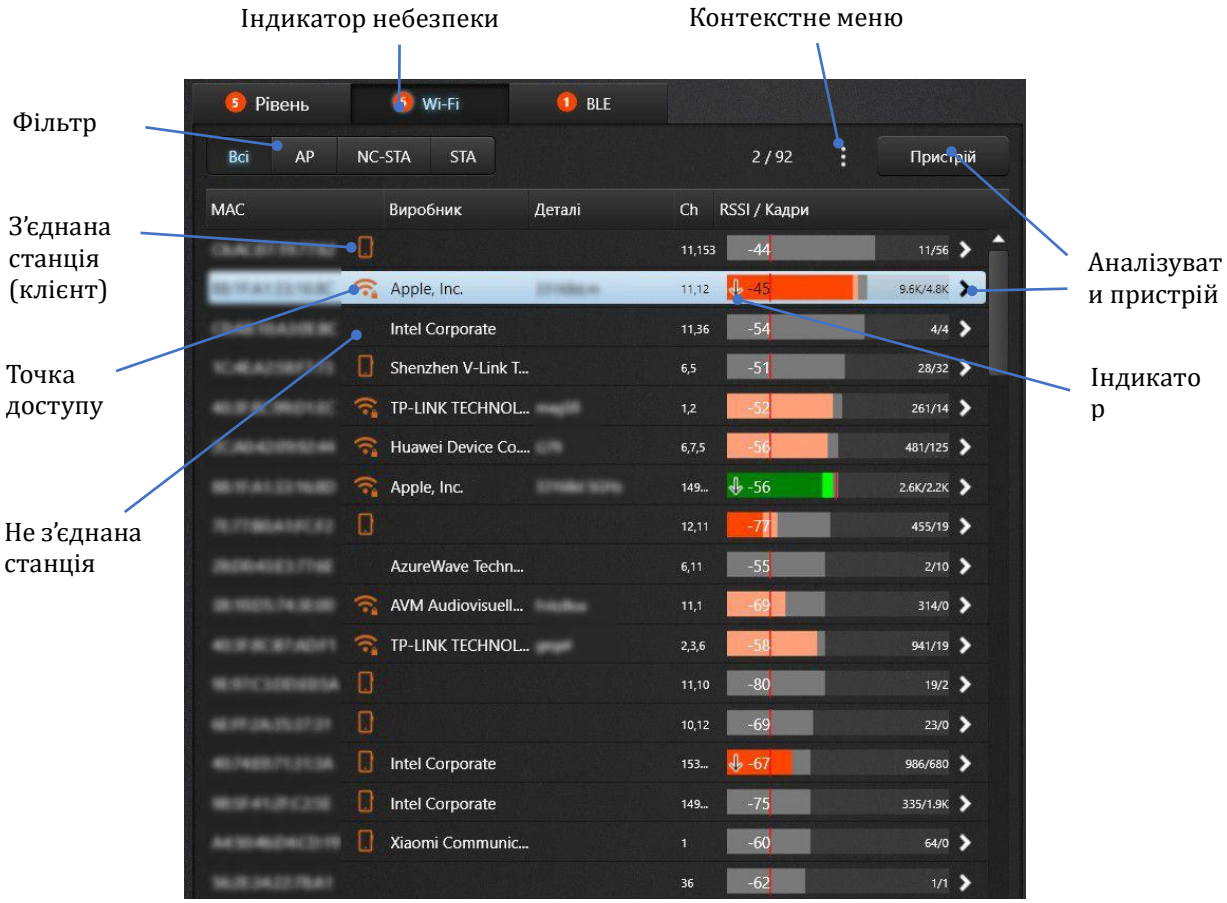
  Загальна швидкість виявлення об'єктів напряму залежить від інтенсивності обміну даними між ними:

  1) Інтенсивний обмін (наприклад, передача файлів або відеопотоку) — виявлення обох пристроїв (передавача та приймача) триває всього кілька секунд.
  2) Низька активність — для реєстрації факту зв'язку знадобиться більше часу.

  Рекомендація: Збільшуйте загальний час пошуку для підвищення надійності й повноти отриманих результатів.
- **Аналіз окремого пристрою** — режим, у якому моніторинг зосереджено лише на робочих каналах конкретного цільового пристрою (а також кількох сусідніх каналах). У цьому режимі ймовірність реєстрації кожної окремої події є значно вищою, що дозволяє швидко й ефективно локалізувати джерело сигналу.

Панель «Wi-Fi»

Панель **«Wi-Fi»** відображає список виявлених пристроїв і дозволяє детально проаналізувати кожен із них:



Індикатор небезпеки на вкладці відображає кількість пристроїв, які перевищують поріг. Він дозволяє слідкувати за станом ситуації коли панель (вкладка) «Wi-Fi» неактивна.

Фільтр дозволяє відбирати пристрої **за типом**:

- **Всі** — відображення всіх знайдених пристроїв.
- **AP** (Access Point) — тільки точки доступу.
- **NC-STA** (Not Connected Station) — нез'єднані станції (клієнти).
- **STA** (Station) — з'єднані станції (клієнти).

Таблиця пристроїв Wi-Fi відображує такі поля:

- **MAC** — унікальний апаратний ідентифікатор пристрою.
- **Тип пристрою** — графічне позначення типу пристрою:
  - Іконка «Wi-Fi з замком» - точка доступу з аутентифікацією
  - Іконка «Wi-Fi без замка» - точка доступу без аутентифікації
  - Іконка «Гаджет» - з'єднана станція / клієнт
  - Без іконки - нез'єднана станція / клієнт
- **Виробник** — назва виробника обладнання або чипсета, на якому побудовано пристрій (якщо його вдалося визначити за кодом OUI).
- **Деталі** — додаткова інформація про пристрій. Для точок доступу тут виводиться назва мережі (SSID). Також у цьому полі відображається текстовий коментар, доданий оператором вручну.

- **Ch (Канал)** — номер або список каналів, на яких було зафіксовано активність пристрою.
- **RSSI / Кадри** — поточний рівень сигналу (в dBm) та лічильник зареєстрованих кадрів (фреймів).

Відображення рівнів сигналу RSSI
Шкали рівня сигналу на панелі «Wi-Fi» відображають декілька значень:

1. **Поточний рівень** (миттєво зростає та миттєво спадає) — відображається **яскраво-зеленим** або **яскраво-червоним** кольором. Активується коли пристрій передає інформацію і спадає до мінімального значення коли пристрій перестає бути активним.
2. **Піковий рівень** (зростає миттєво, але згасає із затримкою) — відображається **світло-зеленим** або **світло-червоним** кольором. Активується коли пристрій передає інформацію і спадає до мінімального значення коли пристрій перестає бути активним.
3. **Максимальний зареєстрований рівень** (запам'ятовує найвище значення за всю сесію) — відображається **сірим** кольором. Ніколи не спадає.
4. **Індикатор прийому** (стрілка вниз) – активується коли реєструються кадри адресовані пристрою

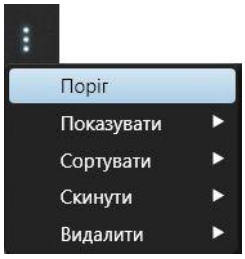
Лічильник кадрів веде роздільний облік кадрів, які були передані пристроєм (Tx), та кадрів, які були йому адресовані (Rx), і відображає їх у форматі «Tx / Rx».

- Збільшення лічильника Tx завжди супроводжується оновленням індикації RSSI для цього пристрою (оскільки він сам є джерелом радіовипромінювання в цей момент).
- Збільшення лічильника Rx не супроводжується оновленням індикації RSSI для цього пристрою

Пристрої без RSSI
До загальної таблиці заносяться як пристрої, що безпосередньо передають кадри, так і ті, яким ці кадри адресовані. У зв'язку з цим, якщо певний пристрій виступав тільки у ролі приймача (лічильник кадрів Tx дорівнює нулю), він буде зареєстрований у системі з відсутнім значенням RSSI.

Подвійник клік на пристрої в списку налаштовує вікно «Спектр» на відображення відповідного діапазону Wi-Fi.

Контекстне меню панелі «Wi-Fi» надає доступ до таких команд та налаштувань:



Поріг — відкриває налаштування порогового рівня сигналу (детальніше див. опис нижче).
Показувати — встановлює додатковий фільтр відображення пристроїв:

- **Неактивні** (увімкнено за замовчуванням) — відображає пристрої, які були зареєстровані, але вже не є активними та мають значення у полі «Час останнього виявлення», що перевищує допустимий інтервал.
- **Верифіковані** (увімкнено за замовчуванням) — відображає верифіковані пристрої.
- **Слабкі** (вимкнено за замовчуванням) — відображає пристрої з дуже слабким рівнем сигналу.

Сортувати — визначає спосіб сортування пристроїв у списку. Доступні варіанти:

- **RSSI** (за замовчуванням) — сортування за максимальним накопиченим рівнем RSSI.
- **Перше виявлення** — сортування пристроїв у порядку часу їхнього виявлення.
- **Лічильник кадрів** — сортування за лічильником кадрів (тобто за активністю пристроїв).

Скинути:

- **Максимальний RSSI** — дозволяє скинути максимальний накопичений рівень RSSI. Це корисно, коли необхідно пересортувати пристрої під час переміщення у просторі (щоб підняти найближчі пристрої вгору списку).
- **Пороги для верифікованих пристроїв** — дозволяє скинути пороги верифікованих пристроїв до поточного максимального накопиченого рівня RSSI. Це може бути корисно перед налаштуванням системи на довготривалий моніторинг. Детальніший опис наведено у розділі «Верифіковані пристрої Wi-Fi».

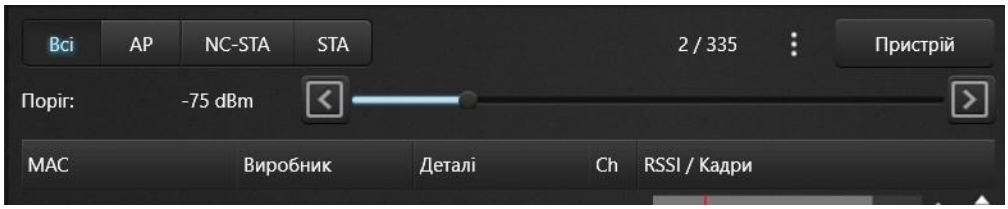
Видалити:

- **Пристрій** — видаляє вибраний пристрій зі списку.
- **Неактивні** — видаляє всі неактивні пристрої.
- **Слабкі** — видаляє пристрої з дуже низьким максимальним накопиченим рівнем RSSI.
- **Всі** — повністю очищає список пристроїв.

Кнопка **«Пристрій»**, а також **«стрілка вправо»** біля пристрою дозволяють перейти до аналізу одного окремого пристрою (дивіться опис нижче).

Поріг Wi-Fi

При увімкнутому пункті меню «Поріг» на інструментальній панелі «Wi-Fi» з'являється відповідний регулятор:



Як працює поріг

Поріг — це рівень сигналу від пристрою Wi-Fi, у разі перевищення якого пристрій класифікується як «потенційно небезпечний».
Вбудований бездротовий модуль здатний приймати навіть найслабші сигнали від віддалених пристроїв. Поріг використовується саме для того, щоб виділити із загального списку потенційно небезпечні джерела, які розташовані поблизу.
При перевищенні встановленого порогу шкала рівня RSSI змінює свій колір із зеленого на червоний, і система починає відтворювати звуковий сигнал тривоги (якщо активно). Таким чином, за допомогою порогу оператор може задати віртуальну «зону тривожної чутливості» навколо пошукової системи та миттєво локалізувати пристрої, що перебувають у цій зоні.
Значення порогу за замовчуванням становить **-75 дБм**, що є оптимальним для більшості пошукових задач.

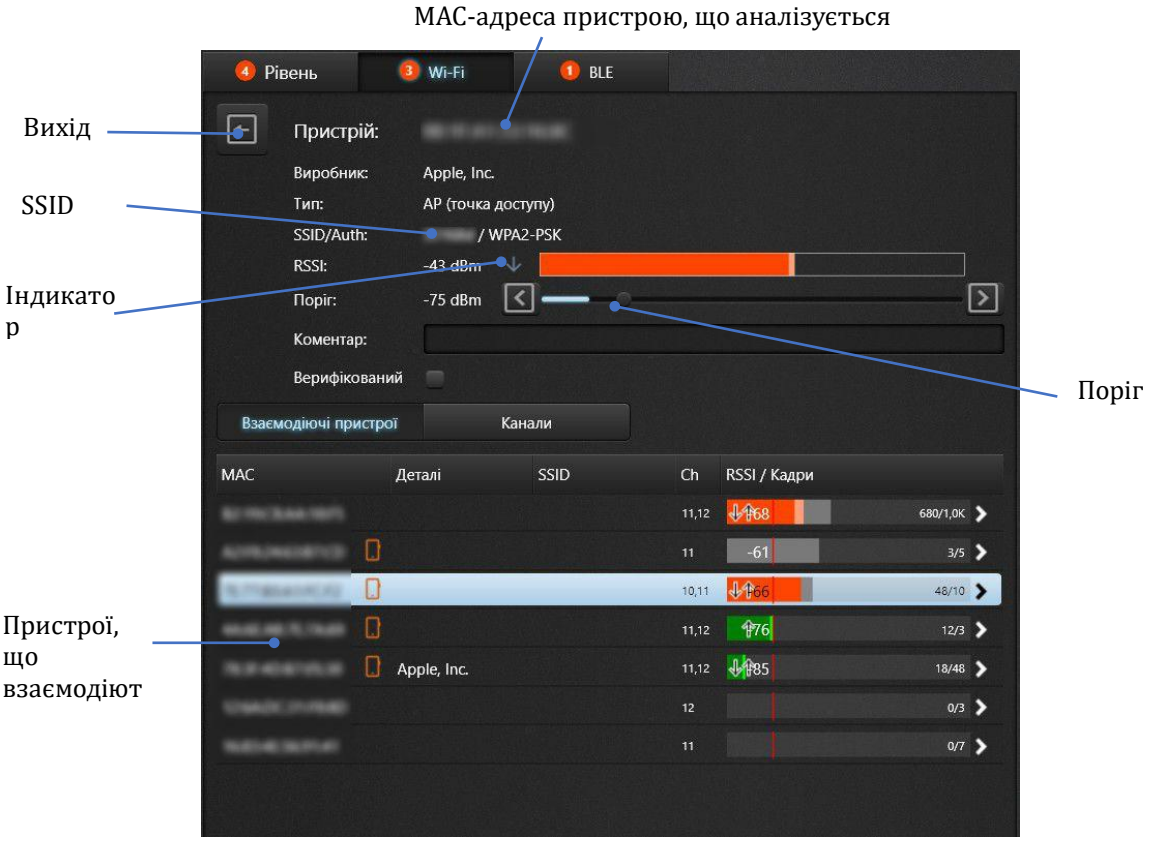
- **При підвищенні порогу** (наприклад, до -60 дБм) для спрацювання тривоги потрібен потужніший сигнал, тому чутливість до тривожних подій та радіус зони виявлення зменшуються.
- **При зниженні порогу** (наприклад, до -85 дБм) чутливість системи та радіус контрольованої зони, навпаки, зростають.

Емпірична відповідність рівня порогу та відстані тривоги у приміщенні:

Рівень порогу, дБм	**Точка доступу Wi-Fi (AP)**	**Клієнт Wi-Fi (STA / NC-STA)**
-75 (за замовчуванням)	5 - 12 м	3 – 6 м
-60	2 – 5 м	1.5 – 3 м
-45	до 1.5 м	до 1 м

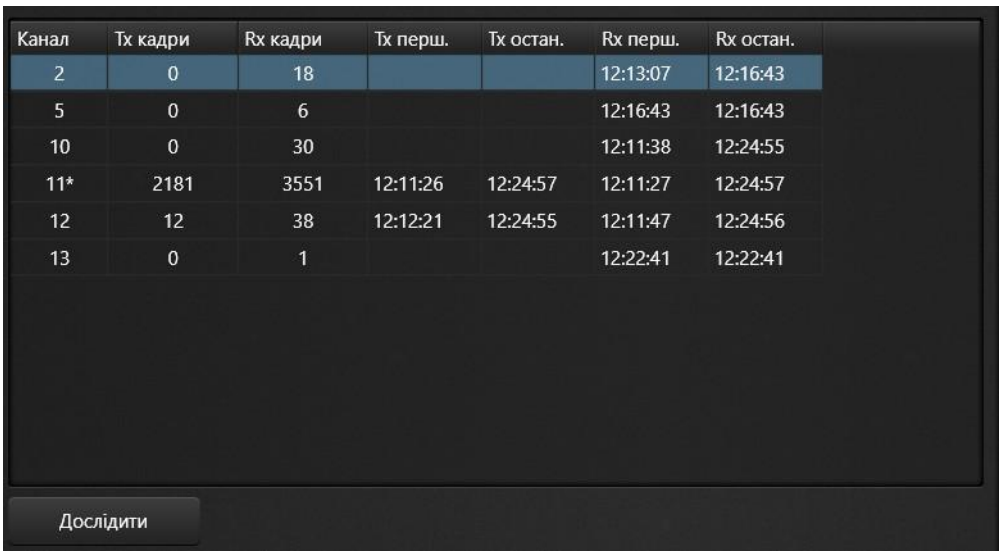
Аналіз окремого пристрою

У режимі аналізу окремого пристрою бездротовий модуль сканує **виключно ті канали, на яких працює цей пристрій**. Завдяки швидкій реакції на події цей режим чудово підходить для детального вивчення пристрою, аналізу його зв’язків та визначення його фізичного розташування (локалізації).



На панелі відображається така інформація про пристрій:

- **Пристрій** — унікальний апаратний ідентифікатор пристрою (MAC-адреса).
- **Виробник** — назва виробника обладнання або чипсета, на якому побудовано пристрій (якщо його вдалося визначити за кодом OUI).
- **Тип** — тип пристрою:
  - AP (Access Point — точка доступу);
  - NC-STA (Non-Connected Station — нез'єднаний клієнт/станція);
  - STA (Station — з'єднаний клієнт).
- **SSID/Auth** — назва мережі (SSID) та спосіб автентифікації (Auth) - відображаються лише для точок доступу (AP).
- **RSSI** — поточний рівень сигналу в dBm, індикатор прийому (стрілка вниз) та графічна шкала, яка відображає поточний, піковий та максимальний рівні (поточна та пікова шкала активні тільки коли пристрій передає кадри). **Зверніть увагу: індикатор прийому** активується тільки коли реєструються кадри адресовані пристрою
- **Поріг** — дублікат регулятора порогового рівня сигналу для зручності локалізації. Дозволяє оператору оперативно змінювати поріг під час наближення до джерела.
- **Коментар** – текстовий коментар оператора
- **Верифікований** — прапорець для присвоєння пристрою статусу «верифікований» (детальніше див. розділ нижче).
- **Вкладка «Взаємодіючі пристрої»** відображає список пристроїв, що взаємодіють із пристроєм, який аналізується (детальніше див. розділ нижче).
- **Вкладка «Канали»** дозволяє відстежувати поканальну активність пристрою із фіксацією часових відміток (у випадку аналізу точки доступу, її основний канал сповіщення відмічається зірочкою *):



- **Tx кадри** — лічильник зареєстрованих фреймів (кадрів), які були **відправлені** пристроєм.
- **Rx кадри** — лічильник зареєстрованих фреймів (кадрів), які були **адресовані** пристрою.
- **Tx перш.** — час першого зареєстрованого кадру **від** пристрою.
- **Tx остан.** — час останнього зареєстрованого кадру **від** пристрою.
- **Rx перш.** — час першого зареєстрованого кадру, що **адресований** пристрою.
- **Rx остан.** — час останнього зареєстрованого кадру, що **адресований** пристрою

Кнопка «Дослідити» на вкладці «Канали» дозволяє перевести спектральний аналіз в режим дослідження вибраного Wi-Fi-каналу (може бути корисним як додатковий інструмент при фізичній локалізації пристрою).

Натискайте кнопку **«Вихід»** для повернення до таблиці пристроїв та стандартного сканування.

Верифіковані пристрої

У сучасному міському середовищі система може виявляти велику кількість пристроїв Wi-Fi, і завданням оператора є аналіз та локалізація кожного з них. Після того як пристрій було фізично знайдено, вивчено та встановлено його безпечність, оператор має можливість позначити його як «Верифікований». Створення такого «білого списку» дозволяє:

- уникати спрацювань від перевіреного пристрою в подальшій роботі й зосередитися на аналізі інших джерел;
- чітко бачити, які пристрої в списку вже перевірені, а які ще ні;
- миттєво фіксувати появу нових пристроїв;
- уникати інформаційного перевантаження під час довготривалого моніторингу (щоб відомі «дружні» джерела не генерували тривожні події і будь-яке нове спрацювання могло швидко привернути увагу).

На відміну від звичайних пристроїв, тривога від яких виникає в разі перевищення загального порогу, небезпечність верифікованих пристроїв визначається на основі **індивідуального «верифікованого» порога**. Така організація дозволяє встановити вищий поріг для перевірених пристроїв і запобігти хибним спрацюванням від них.

Статус «Верифікований» можна встановити, коли панель «Wi-Fi» перебуває в режимі аналізу пристрою. Якщо цей прапорець увімкнено, поруч з ним з'являється регулятор рівня верифікованого порогу.

Рівень верифікованого порогу автоматично встановлюється відповідно до накопиченого максимального рівня пристрою з додаванням невеликого фіксованого значення. Це дозволяє уникнути спрацювань від пристрою майже в усіх локаціях, де до цього виконувалося його вимірювання. З цього моменту спрацювання від верифікованого пристрою можливе лише тоді, коли його RSSI-рівень перевищить цей індивідуальний поріг.
Коли пристрій має статус верифікованого, його шкала рівня набуває «мирного» зеленого кольору навіть у разі перевищення загального порогового рівня, оскільки тривожні події від нього не генеруються.

Порада: Разом із присвоєнням статусу «Верифікований» додавайте до пристрою текстовий коментар. У ньому варто зазначити тип обладнання, його призначення або місце розташування.
Приклади коментарів: «Основна точка доступу», «Принтер у кабінеті 5», «Телефон John Smith» тощо.
Ця інформація відображатиметься в загальному списку пристроїв, що значно полегшить сприйняття даних та аналіз радіообстановки.

Важлива примітка щодо безпеки

Ідентифікація пристроїв Wi-Fi пошуковими системами здійснюється виключно на основі апаратного ідентифікатора (MAC-адреси). Потрібно розуміти, що зловмисник або шпигунський Wi-Fi-пристрій може встановити будь-яку MAC-адресу й інші атрибути, зокрема й клонувати ваші наявні точки доступу або зробити дублікат MAC-адреси клієнта.
Не можна вважати якусь верифіковану MAC-адресу «назавжди безпечною», навіть якщо ви фізично перевірили джерело сигналу.

- Користуйтеся відміткою «Верифікований» з обережністю!
- Періодично повторюйте аналіз та локалізацію пристроїв.
- У разі довготривалого стаціонарного моніторингу стежте за аномаліями (зміною рівня сигналу) від верифікованих пристроїв на графіку тривог. У разі появи «клону» можливі відхилення рівня як у менший бік (клон розташований далі, ніж оригінал), так і в більший (клон розташований ближче).

Порада: Намагайтеся не встановлювати занадто високий верифікований рівень. Це дозволить вчасно помітити появу «клону», якщо його рівень перевищить поріг: у такому разі шкала набуде червоного кольору, увімкнеться звукова тривога, а графік тривог у режимі «Рівень небезпеки» відобразить подію від пристрою. Відділяйте пристрої які можуть рухатися разом зі своїм власником (телефони, плашети) від стаціонарних (точки доступу, комп'ютери, оргтехніка) та встановлюйте більший допуск порогу для пристроїв які переміщуються.

Скидання верифікованого порогу для пристроїв
Перед тривалим моніторингом, коли пошукова система працюватиме стаціонарно, ви можете скинути пороги всіх верифікованих пристроїв, щоб підвищити чутливість до

зміни RSSI. Це дозволить гарантовано зафіксувати появу «клону» точки доступу / клієнта, якщо такий клон буде розташований ближче до системи.

Порядок дій для скидання порогів:

1. Встановіть систему стаціонарно там де вона перебуватиме протягом наступних вимірювань
2. Переконайтеся, що панель **«**Wi-Fi**»** перебуває у звичайному режимі (не в режимі аналізу конкретного пристрою).
3. Відкрийте **контекстне меню** панелі.
4. Перейдіть у пункт **«Скинути»**.
5. Виберіть команду **«(Скинути) Максимальний RSSI»**
6. Почекайте декілька хвилин (або довше) щоб накопичився новий максимальний рівень RSSI
7. Виберіть команду **«(Скинути) Пороги для верифікованих пристроїв»**. Для всіх верифікованих пристроїв будуть встановлені пороги з накопиченого максимального рівня RSSI

Взаємодіючі пристрої

Під час пошукових робіт, окрім виявлення та аналізу самих пристроїв Wi-Fi є край важливим вивчення їх зв’язків. Це дозволяє систематизувати інформацію про бездротову мережу на об’єкті та швидше виявити підозрілі джерела.

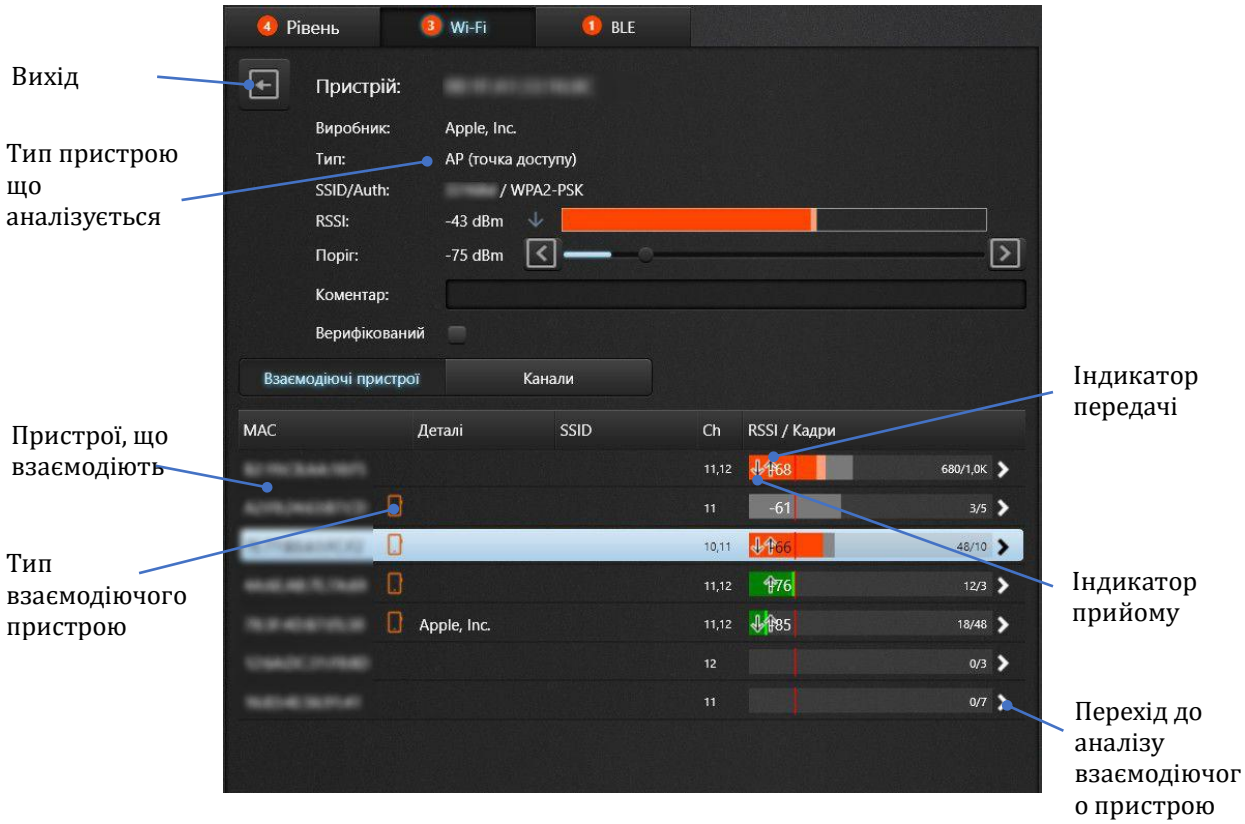
У режимі аналізу окремого пристрою пошукова система відображає його зв'язки з іншими об'єктами радіоефіру на вкладці **«Взаємодіючі пристрої».**

Кожен тип пристрою, що аналізується (точка доступу, з’єднаний клієнт або нез’єднана станція), має свій характерний паттерн поведінки та набір взаємодій:

- Коли аналізується **Точка доступу (AP — Access Point):**
  Вона активно взаємодіє з авторизованими в її мережі з’єднаними клієнтами (STA), здійснюючи постійний обмін даними (Data-кадри). Водночас вона періодично комунікує з нез’єднаними станціями (NC-STA), які проходять повз: отримує від них кадри управління Probe Request (запит на сканування) і відповідає кадрами Probe Response (відповідь на сканування).
  Примітка: З огляду на специфіку протоколу 802.11, для легітимної точки доступу є нормальним накопичення довгого списку нез’єднаних клієнтів із короткою історією обміну (низькі значення лічильників Rx / Tx). Якщо ж у списку взаємодій з'являється пристрій із аномально високим трафіком без переходу в статус з'єднаного, це може свідчити про спробу атаки на точку доступу або сканування її вразливостей.
- Коли аналізується **З’єднана станція (STA — Station):**
  Цей клієнт (наприклад, підключений до Wi-Fi смартфон чи ноутбук) веде активну взаємодію (двосторонній обмін даними) зі своєю точкою доступу. Паралельно пристрій може періодично взаємодіяти з іншими точками доступу, не з’єднуючись із ними (наприклад, надсилаючи запити для оцінки рівня сигналу сусідніх точок під час підготовки до роумінгу).
  Примітка: У списку взаємодій з’єднаного клієнта головна AP завжди матиме найбільші показники лічильників Rx / Tx та стабільний рівень RSSI. Поява в цьому списку інших точок доступу з високою активністю може вказувати на те, що пристрій намагаються перехопити за допомогою фейкової базової станції (атака типу Evil Twin).

- Коли аналізується **Нез'єднана станція (NC-STA — Non-Connected Station):** Це клієнтський пристрій, який наразі не підключений до жодної Wi-Fi мережі (наприклад, смартфон із увімкненим Wi-Fi, що шукає знайомі мережі). Він циклічно надсилає в ефір кадри управління типу Probe Request на різних каналах і фіксує відповіді Probe Response від усіх точок доступу в радіусі досяжності. **Примітка:** У вкладці взаємодій такого пристрою відображатиметься велика кількість різноманітних точок доступу, але лічильники кадрів для кожної з них будуть мінімальними. За специфікою цих запитів оператор може визначити, які саме мережі цей пристрій «шукає».

На скріншоті наведений приклад аналізу точки доступу, що має ідентифікованого виробника Apple, Inc. В списку взаємодіючих пристроїв присутній ряд з'єднаних та нез'єднаних станцій (клієнтів).



У списку взаємодіючих пристроїв відображається стандартна інформація: тип пристрою (іконка), MAC-адреса, SSID (для точок доступу), робочі канали (Ch), лічильник кадрів, шкала RSSI тощо.
Окрім цього, на комбінованій шкалі **«RSSI / Кадри»** відображаються додаткові динамічні індикатори, які деталізують напрямок трафіку:

- **Індикатор прийому** (стрілка вниз): спалахує, коли реєструються кадри, які пристрій, що аналізується, надсилає цьому взаємодіючому пристрою (тобто взаємодіючий пристрій працює на прийом).
- **Індикатор передачі** (стрілка вгору): спалахує, коли реєструються кадри, які взаємодіючий пристрій надсилає пристрою, що аналізується (тобто взаємодіючий пристрій працює на передачу).

Спільний аналіз індикаторів прийому/передачі та лічильників Rx / Tx дозволяє миттєво визначити паттерн поведінки взаємодіючого об'єкта (наприклад, чи це пасивний слухач, чи активний ініціатор обміну).

Навігація та перехід по дереву взаємозв'язків

Функція переходу по дереву взаємодіючих пристроїв дозволяє оператору миттєво перемикати фокус дослідження. Якщо у списку взаємодій виявлено підозрілий об'єкт, оператор може натиснути кнопку **«вправо» (стрілка переходу)** навпроти цього об'єкта.

У цей момент інтерфейс панелі «Wi-Fi» автоматично перебудовується:

1. Взаємодіючий пристрій стає новим головним об'єктом аналізу.
2. Система починає сканувати виключно його робочі канали.
3. Вкладка «Взаємодіючі пристрої» оновлюється й показує вже його власне оточення та зв'язки.

Перехід по дереву не просто перемикає екран, а створює ланцюжок дослідження (стек пам'яті):

- Оператор може заглиблюватися по дереву взаємозв'язків на кілька рівнів (наприклад: Точка доступу → З'єднаний смартфон → Інша точка доступу, яку цей смартфон шукає → Наступний клієнт цієї точки).
- Навігаційна кнопка «Вихід» працює за принципом повернення на один крок назад у зворотному порядку. Вона дозволяє крок за кроком повернутися до початкового об'єкта дослідження без втрати накопичених даних про його RSSI та кадри.

Ця функція незамінна для виявлення прихованих ретрансляторів, Wi-Fi мостів або несанкціонованих клієнтів, які намагаються маскуватися під легітимне обладнання, підключаючись через проміжні пристрої.

Історія активності

Якщо запис журналу увімкнений, програма Breeze RF реєструє історію активності по кожному виявленому Wi-Fi-пристрою з можливістю її перегляду на графіку панелі «Тривоги».

Якщо запис не активний, графік накопичує історію по вибраному пристрою але скидає її при виборі іншого та починає накопичення спочатку.

Щоб увімкнути перегляд історії на графіку необхідно вибрати пристрій в таблиці та встановити прапорець «Wi-Fi: XX:XX:XX:XX:XX» (MAC-адреса пристрою) на панелі «Тривоги».

Графік історії по вибраному пристрою буде відображатися напівпрозорим помаранчевим кольором:

При виборі іншого пристрою в таблиці графік буде автоматично налаштовуватись на відображення історії нового пристрою.

За допомогою функції масштабування (яка активується під час клацання мишкою на графіку) можна гнучко налаштувати часовий інтервал відображення даних:

- **Короткий інтервал (швидке оновлення часу)** — оптимізований для миттєвого відстеження змін рівня сигналу безпосередньо під час локалізації (пошуку) джерела.
- **Довгий інтервал (повільне накопичення)** — призначений для ретроспективного аналізу активності пристрою та виявлення паттернів його поведінки протягом тривалого часу.

Ви можете більш детально ознайомитись з роботою з графіком у розділі «Панель «Тривоги».

Відображення пристроїв на графіку спектра

Програма Breeze RF підтримує відображення іконок Wi-Fi пристроїв безпосередньо на графіку спектра. Вони розміщуються на відповідних частотних каналах із прив'язкою до їхнього поточного рівня сигналу (RSSI).

Візуальне поєднання спектрограми з даними сканування Wi-Fi дозволяє оператору наочно оцінювати радіообстановку під час огляду приміщення в режимі реального часу:

- **Наближення до об'єкта:** іконка пристрою, до якого наближається пошукова система, зміщуватиметься вгору (рівень RSSI зростає по вертикалі).
- **Віддалення від об'єкта:** іконка пристрою, від якого система віддаляється, зміщуватиметься вниз (рівень RSSI падає).

Як увімкнути відображення:

1. У меню панелі **«Спектр»** виберіть пункт **«Пристрої» → «Wi-Fi»**.
2. **Масштабуйте графік спектра** для відображення конкретного діапазону Wi-Fi — 2.4 ГГц або 5 ГГц. Зробити це швидко можна двома способами:
    - Перейдіть на панель «Рівень» і двічі клацніть на потрібний діапазон.
    - Двічі клацніть на будь-який пристрій у панелі «Wi-Fi», чиї робочі канали відповідають шуканому діапазону (канали 1–14 для 2.4 ГГц або канали 100+ для 5 ГГц).

Особливості режимів відображення:

- **Режим загального сканування:** за великої кількості виявлених точок доступу та клієнтів велика кількість іконок може візуально перевантажувати графік спектра.
- **Режим аналізу окремого пристрою:** на графіку відображається цільовий об'єкт, а також пов'язані з ним пристрої (наприклад, клієнти, підключені до аналізованої точки доступу). Це значно полегшує оцінку ситуації всередині конкретного бездротового кластера.

Виявлення пристроїв Bluetooth Low Energy

Протокол Bluetooth Low Energy (далі — BLE) був створений для передачі інформації з мінімальним енергоспоживанням. Як наслідок, закладні пристрої, що базуються на цій технології, відрізняються тривалим часом автономної роботи, низьким енергоспоживанням та складністю виявлення.

Особливості загроз, пов'язаних зі стандартом BLE:

- **Режим радіомовчання (Stealth-mode):** можливість накопичувати інформацію в локальній пам'яті та передавати її короткими імпульсними інтервалами часу.
- **Адаптивний вихід в ефір:** активація передавача лише тоді, коли заздалегідь визначений пристрій-«отримувач» даних з’являється в зоні радіозв’язку.
- **Доступність приймального обладнання:** відсутність потреби у спеціалізованих засобах прийому — отримувачем даних може бути звичайний смартфон, планшет або комп’ютер зловмисника.
- **Гнучкість топології мережі:** можливість роботи як у режимі «Периферія» (Peripheral — надавач послуги/даних), так і в режимі «Централь» (Central — користувач послуги/приймач).
- **Маскування в радіочастотному полі:** висока насиченість сучасних приміщень легітимними сигналами Wi-Fi та іншими побутовими пристроями Bluetooth ускладнює виявлення закладок за допомогою звичайних радіочастотних детекторів (індикаторів поля) або аналізаторів спектра.
- **Постійна зміна ідентифікаторів:** безперервна ротація MAC-адреси та структури корисного навантаження (Payload) під час роботи в режимі розсилання сповіщень (Advertising).
- **Прихованість у з’єднаному стані:** неможливість дешифрування ефіру, а також повна відсутність сигналів сповіщення (Advertising), коли «закладка» вже встановила безпосередній зв'язок з отримувачем і веде пряму передачу даних.

Основні види «шпигунського» обладнання, що використовує BLE:

- **Мікрофони:** призначені для негласного зняття акустичної інформації. Сучасні модулі BLE дозволяють здійснювати фонове накопичення аудіоданих та їхню періодичну пакетну трансляцію.
- **Пошукові мітки (трекери):** призначені для негласного визначення розташування рухомого об'єкта, транспортного засобу, вантажу чи людини (детальний опис наведено далі).
- **GNSS-трекери та інше обладнання:** BLE-канал може використовуватися як шлюз для прихованої передачі накопичених координатних даних та (або) для дистанційного керування пристроєм.

З огляду на високу небезпеку, під час проведення пошукових робіт **необхідно виявляти, фізично локалізувати та ідентифікувати в зоні контролю кожен пристрій BLE** всіма доступними методами.

Бездротовий модуль, вбудований у комплекси Delta S та Delta X останнього покоління, здатний виявляти пристрої BLE у нез'єднаному стані шляхом сканування їхніх сигналів сповіщення (Advertising-пакетів). Це дозволяє фіксувати приховані мікрофони, що очікують на з'єднання, всі види пошукових міток (оскільки в режимі нелегального стеження вони завжди залишаються в режимі сповіщення без постійного з'єднання) та інше небезпечне BLE-обладнання. Модуль здійснює сканування паралельно зі спектральним аналізом та дозволяє проаналізувати кожен окремий пристрій. Ця функція вмикається автоматично в режимах «Всі сигнали» та «Бездротові/ISM», а для інших пошукових режимів її можна активувати вручну.

Важливе зауваження: Вбудований бездротовий модуль Delta S / Delta X забезпечує сканування пристроїв BLE виключно в нез'єднаному стані (режим Advertising). Проте оператор має обов'язково здійснювати пошук пристроїв BLE, які вже перебувають у з'єднаному стані (Connected) та джерел що базуються на інших варіантах протоколу (Bluetooth Classic, або інші «кастомні» протоколи на діапазоні 2.4 ГГц). Для виявлення таких пристроїв використовуйте спектральный аналіз і режим дослідження частотного діапазону «ISM 2.4 GHz Wi-Fi/Bluetooth» (детальніше див. розділ «Використання панелі «Рівень» для пошуку бездротових сигналів»).

Класифікація пристроїв

Програмне забезпечення Breeze RF має вбудований алгоритми класифікації BLE-пристроїв на «Всі», «Tags» (мітки)» та «Beacons» (навігаційні маяки) та постачається з файлами даних що забезпечують ідентифікацію виробника.

Антена, що відповідає за сканування BLE, розташована на задній панелі приладу та має маркування «BLUETOOTH».

Реєстрація даних

Коли увімкнено запис журналу, система автоматично реєструє таку інформацію, отриману під час сканування BLE:

- таблицю виявлених пристроїв;
- історію активності для кожного пристрою.

Ці дані надійно зберігаються в журналі й можуть бути переглянуті або проаналізовані в будь-який момент.

Звукова тривога
Якщо на загальній інструментальній панелі активовано функцію **«Звукова тривога»**, у разі появи в ефірі BLE-пристрою з високим (небезпечним) рівнем сигналу програма сповістить оператора **особливим двотональним сигналом**.
Цей аудіосигнал суттєво відрізняється від стандартного «клацання», яке генерується під час тривожних подій у діапазонах спектрального аналізу, що дозволяє оператору на слух миттєво ідентифікувати активність саме в бездротових мережах.

Змінні ідентифікатори

Шпигунські BLE-пристрої, трекери (мітки), а також споживча електроніка (смартфони, навушники, смарт-годинники) захищені від відстеження шляхом постійної зміни своєї MAC-адреси та корисного навантаження. Для цього вони використовують криптографічний ротаційний ключ.
Така зміна (ротація) зазвичай відбувається кожні 10–15 хвилин, а в деяких випадках і частіше. Кожна нова ротація створює новий запис (екземпляр) у таблиці пристроїв Breeze RF, тоді як попередній екземпляр залишається в базі як неактивний.

Ця технологічна особливість створює суттєві труднощі під час радіомоніторингу BLE:

- **Тимчасовий ефект перевірки:** Неможливо ідентифікувати та верифікувати всі пристрої в приміщенні «раз і назавжди». Навіть після повної локалізації та аналізу кожного об'єкта вже за 15–30 хвилин ви отримаєте новий список «невідомих» пристроїв.
- **Марність статичних «білих списків» верифікованих пристроїв:** Створити постійний білий список дозволених девайсів неможливо (за винятком поодиноких девайсів, що не використовують ротацію адрес).
- **Перевантаження інтерфейсу:** Таблиця пристроїв безперервно наповнюється застарілими неактивними записами, що ускладнює оперативний аналіз радіообстановки.

Рекомендації щодо організації тривалого радіомоніторингу BLE

Зважаючи на динамічну зміну адрес, класичний підхід до моніторингу не працює. Ефективна стратегія виявлення BLE-загроз має базуватися на таких підходах та функціях Breeze RF:

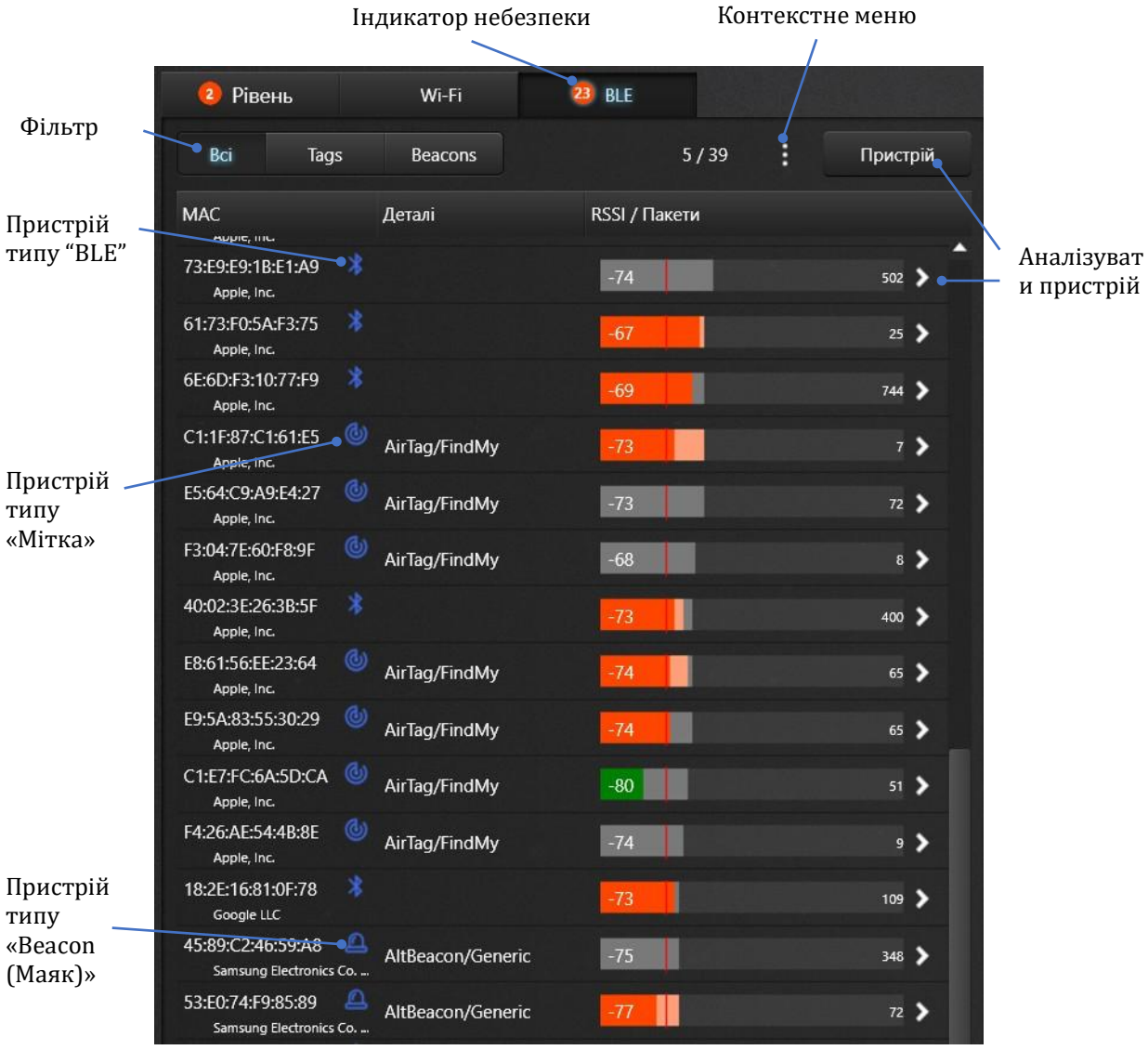
1. **Фільтрація застарілих даних:** Деактивуйте параметр **«Показувати неактивні»** в меню налаштувань. Це дозволить приховати старі «дублюючі» екземпляри пристроїв, які вже змінили адресу, і залишить на екрані лише актуальну картину ефіру.
2. **Звуження зони контролю за допомогою порогів:** Обмежуйте радіус виявлення пристроїв, встановлюючи вищий поріг рівня сигналу (RSSI). Це дозволить відсікти фонові пристрої за стінами або на вулиці й реагувати лише на ті девайси, що знаходяться безпосередньо в цільовій зоні.
3. **Використання функції «Ідентичні пристрої»:** Завжди застосовуйте цей інструмент для аналізу структури корисного навантаження пакетів. Він допомагає миттєво «зв'язувати» історію девайса до і після зміни MAC-адреси.
4. **Кореляція з фізичною присутністю людей:** Співвідносьте дані радіовиявлення BLE із графіком перебування відвідувачів або персоналу в приміщенні.
5. **Профілювання легітимних пристроїв:** Проаналізуйте BLE-сигнали постійних працівників (їхніх телефонів, гарнітур тощо) та зафіксуйте характерну структуру

їхніх пакетів. Це дозволить швидше помічати аномальні або нові невідомі сигнатури.

6. **Регулярний локальний пошук:** Поєднуйте безперервний фоновий моніторинг із періодичним цільовим пошуком (обходом території) у зонах найвищого ризику.
7. **Дистанційне керування (RDP):** Організуйте постійний моніторинг через віддалений робочий стіл (RDP). Це дозволить оператору безпечно й централізовано аналізувати накопичену статистику та графіки тривог в режимі 24/7 без фізичної присутності на об'єкті.

Панель «BLE»

Панель «BLE» відображає список виявлених пристроїв та інформацію про них:



Індикатор небезпеки на вкладці відображає кількість пристроїв, які перевищують поріг. Він дозволяє слідкувати за станом ситуації коли панель (вкладка) «BLE» неактивна.

Фільтр дозволяє класифікувати та відбирати BLE-пристрої за їхнім типом:

- **Всі** — повне відображення всіх зафіксованих у радіоефірі пристроїв.
- **Tags** — відображення виключно пошукових та персональних міток

- **Beacons —** відображення суто навігаційних маяків.

Зауваження: Визначення типу пристрою здійснюється автоматичним інтелектуальним алгоритмом програми шляхом глибокого аналізу корисного навантаження (Payload) пакетів сповіщення. Зважаючи на постійну появу нових брендів мікроелектроніки та використання розробниками нестандартних або зашифрованих протоколів трансляції даних, цей автоматичний алгоритм **не дає 100% гарантії** безпомилкової класифікації пристрою як «Tag» (мітка). Під час проведення професійної перевірки оператор обов'язково повинен додатково аналізувати загальну категорію «Всі», оскільки нові, модифіковані або специфічні BLE-пристрої можуть не потрапити у профільні фільтри й залишатися в загальному списку.

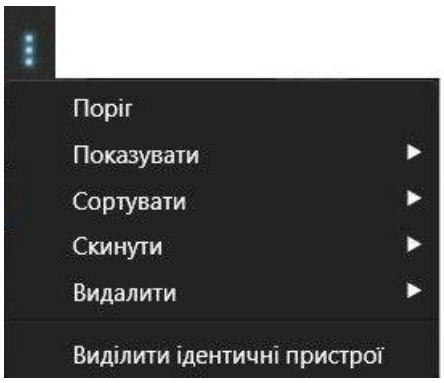
Таблиця пристроїв BLE відображує такі поля:
- **MAC —** апаратний ідентифікатор пристрою.
- **Тип пристрою —** графічне позначення типу пристрою:
  - Іконка «Локатор» позначає пристрої типу «Tag» (мітка)
  - Іконка «Маяк» - пристрої типу «Beacon» (маяки геопозиціювання)
  - Іконка «Bluetooth» - всі інші BLE-пристрої, не ідентифіковані як Tag чи Beacon
- **Виробник —** назва виробника обладнання, якщо його вдалося визначити за інформацією з корисного навантаження.
- **Деталі —** додаткова інформація про пристрій. Тут виводиться тип пристрою, якщо його було ідентифіковано, ім’я пристрою (якщо сповіщається) та інша інформація з корисного навантаження
- **RSSI / Пакети —** поточний рівень сигналу (в dBm) та лічильник зареєстрованих пакетів.

Відображення рівнів сигналу RSSI
Шкали рівня сигналу на панелі «BLE» відображають декілька значень:
1. **Поточний рівень** (миттєво зростає та миттєво спадає) — відображається **яскраво-зеленим** або **яскраво-червоним** кольором. Активується коли пристрій передає інформацію і спадає до мінімального значення коли пристрій перестає бути активним.
2. **Піковий рівень** (зростає миттєво, але згасає із затримкою) — відображається **світло-зеленим** або **світло-червоним** кольором. Активується коли пристрій передає інформацію і спадає до мінімального значення коли пристрій перестає бути активним.
3. **Максимальний зареєстрований рівень** (запам’ятовує найвище значення за всю сесію) — відображається **сірим** кольором. Ніколи не спадає.

Лічильник пакетів веде облік зареєстрованих пакетів від пристрою та дозволяє оцінити його активність (інтервал передачі).

Подвійник клік на пристрої в списку налаштовує вікно «Спектр» на відображення відповідного діапазону (2.4 GHz).

Контекстне меню панелі «BLE» надає доступ до таких команд та налаштувань:



Поріг — відкриває налаштування порогового рівня сигналу (детальніше див. опис нижче).
Показувати — встановлює додатковий фільтр відображення пристроїв:

- **Неактивні** (увімкнено за замовчуванням) — відображає пристрої, які були зареєстровані, але вже не є активними та мають значення у полі «Час останнього виявлення», що перевищує допустимий інтервал.
  Рекомендація: Вимикайте **«Показувати неактивні»** щоб приховати с старі неактивні екземпляри пристроїв, що періодично змінюють ідентифікатор, особливо після тривалого радіомоніторингу.
- **Верифіковані** (увімкнено за замовчуванням) — відображає верифіковані пристрої.
- **Слабкі** (вимкнено за замовчуванням) — відображає пристрої з дуже слабким рівнем сигналу.

Сортувати — визначає спосіб сортування пристроїв у списку. Доступні варіанти:

- **RSSI** (за замовчуванням) — сортування за максимальним накопиченим рівнем RSSI.
- **Перше виявлення** — сортування пристроїв у порядку часу їхнього виявлення.
- **Лічильник кадрів** — сортування за лічильником кадрів (тобто за активністю пристроїв).

Скинути:

- **Максимальний RSSI** — дозволяє скинути максимальний накопичений рівень RSSI. Це корисно, коли необхідно пересортувати пристрої під час переміщення у просторі (щоб підняти найближчі пристрої вгору списку).
- **Пороги для верифікованих пристроїв** — дозволяє скинути пороги верифікованих пристроїв до поточного максимального накопиченого рівня RSSI.

Видалити:

- **Пристрій** — видаляє вибраний пристрій зі списку.
- **Неактивні** — видаляє всі неактивні пристрої.
- **Слабкі** — видаляє пристрої з дуже низьким максимальним накопиченим рівнем RSSI.
- **Всі** — повністю очищає список пристроїв.

Виділити ідентичні пристрої - функція що дозволяє бачити в списку інші пристрої з аналогічною структурою корисного навантаження (див. розділ «Ідентичні пристрої та ідентифікація нового екземпляра»).

Кнопка **«Пристрій»**, а також **«стрілка вправо»** біля пристрою дозволяють перейти до аналізу одного окремого пристрою (дивіться опис нижче).

Поріг BLE

При увімкнутому пункті меню «Поріг» на інструментальній панелі «BLE» з'являється відповідний регулятор:

Як працює поріг

Поріг — це рівень сигналу від пристрою BLE, у разі перевищення якого пристрій класифікується як «потенційно небезпечний».
Вбудований бездротовий модуль здатний приймати навіть найслабші сигнали від віддалених пристроїв. Поріг використовується саме для того, щоб виділити із загального списку потенційно небезпечні джерела, які розташовані поблизу.
При перевищенні встановленого порогу шкала рівня RSSI змінює свій колір із зеленого на червоний, і система починає відтворювати звуковий сигнал тривоги (якщо активно). Таким чином, за допомогою порогу оператор може задати віртуальну «зону тривожної чутливості» навколо пошукової системи та миттєво локалізувати пристрої, що перебувають у цій зоні.
Значення порогу за замовчуванням становить **-75 дБм**, що є оптимальним для більшості пошукових задач.

- **При підвищенні порогу** (наприклад, до -60 дБм) для спрацювання тривоги потрібен потужніший сигнал, тому чутливість до тривожних подій та радіус зони виявлення зменшуються.
- **При зниженні порогу** (наприклад, до -85 дБм) чутливість системи та радіус контрольованої зони, навпаки, зростають.

Емпірична відповідність рівня порогу та відстані тривоги у приміщенні:

Рівень порогу, дБм	Пристрій BLE в прямій видимості	Пристрій BLE за стіною (міжкімнатна цегла)
-75 (за замовчуванням)	6 – 12 м	3 – 6 м
-60	2 – 4 м	1 – 2 м
-45	до 0.5 - 1.5 м	до 0.2 – 0.5 м

Як працюють BLE-мітки (Tags)

Ця технологія належить до класу «Геопозиціювання з використанням публічних мереж» (Crowdsourced Location Networks). Вона використовує мільярди сторонніх смартфонів і планшетів як анонімні ретранслятори для пошуку об'єктів.

Алгоритм роботи мітки

Процес пошуку та передачі координат складається з чотирьох основних етапів:

- **Крок 1: Трансляція сигналу (мітка передає дані в ефір).** Мітка не має вбудованого GPS-модуля і не підключена до інтернету. Вона працює виключно як автономний радіомаяк. Кожні кілька секунд пристрій надсилає через BLE свій унікальний ідентифікатор. Цей ідентифікатор постійно змінюється,

використовуючи криптографічний ротуючий ключ, щоб сторонні особи не могли відстежувати переміщення самої мітки в реальному часі.

- **Крок 2: Прийом смартфоном-ретранслятором.** Повз мітку проходить випадковий перехожий із увімкненим смартфоном (iPhone або Android з активними сервісами Google чи Samsung). Смартфон цієї людини у фоновому режимі «чує» BLE-сигнал мітки й миттєво фіксує координати свого власного GPS-модуля в цей конкретний момент.
- **Крок 3: Передача в хмару (анонімний рапорт).** Смартфон перехожого автоматично надсилає зашифрований пакет на сервери Apple, Google або Samsung (залежно від екосистеми мітки). Пакет містить лише два елементи: [ID мітки] + [GPS-координати смартфона-перехожого]. Передача відбувається абсолютно непомітно для власника телефона. Процес повністю анонімний і захищений наскрізним шифруванням (End-to-End Encryption): ані компанії Apple/Google, ані сам перехожий не знають, чию мітку було виявлено.
- **Крок 4: Сповіщення власника мітки.** Сервер приймає зашифровані дані. Оскільки розшифрувати геопозицію може тільки закритий ключ, який зберігається безпосередньо на смартфоні власника мітки, сервер просто пересилає цей пакет у додаток (наприклад, «Локатор» або «Find My Device»). Власник відкриває карту і бачить точку, де мітку востаннє зафіксував чийсь телефон.

Точний пошук (прибуття на місце)

Коли оператор чи власник приходить за координатами на карті, система переходить у режим ближнього пошуку. Смартфон зв'язується з міткою напряму через Bluetooth, після чого з’являється можливість увімкнути на ній звуковий сигнал.

Якщо смартфон та мітка підтримують технологію UWB (Ultra-Wideband), активується інтерфейс точного пошуку. Смартфон вимірює час проходження радіосигналу (Time-of-Flight) і за принципом радара веде користувача чітко до об'єкта, долаючи проблему «останнього метра» (наприклад, якщо трекер сховано глибоко в обшивці чи під панеллю приладів авто).

Найбільш відомі платформи

Екосистема	**Назва мітки**	**Мережа пошуку**
Apple	AirTag	Find My (локатор)
Android (Google)	Chipolo ONE Point, Pebblebee Clip, Moto Tag тощо	Find My Device
Samsung (Android)	Galaxy SmartTag / SmartTag2	SmartThings Find
Незалежні	Tile	Власна мережа Tile App

Захист від стеження

Оскільки мітка дозволяє визначати координати, має надзвичайно малі габарити та великий ресурс батареї, зловмисники можуть використовувати її як прихований трекер для нелегального стеження. Для захисту приватності компанії Apple та Google впровадили спільний стандарт безпеки:

1. Якщо чужа мітка переміщується за вами протягом певного часу, а її власника немає поруч, ваш смартфон (неважливо, iPhone це чи Android) видасть сповіщення: **«**Поруч виявлено невідома мітка».

2. Користувач може дистанційно змусити таку мітку подати звуковий сигнал або прочитати інструкцію, як вийняти батарейку для її повного вимкнення.

Джерело небезпеки: Приховані та модифіковані мітки
На жаль, побутовий автоматичний захист смартфонів безсилий проти професійних міток із модифікованою прошивкою (Stealth-трекери), які спеціально розроблені для обходу алгоритмів виявлення.
Як вони обходять захист:

- Замість стандартного інтервалу ротації публічного ключа (раз на 15–20 хвилин), хакерська прошивка змінює ключі значно частіше або хаотично, а також маскує інші параметри радіопакета.
- Оскільки хмара Apple чи Google не може деанонімізувати такий ланцюжок і пов'язати його з єдиним пристроєм, смартфон жертви сприймає ці сигнали як безліч різних випадкових Bluetooth-пристроїв (наприклад, як звичайний натовп чи чужі навушники у фоні).

Як наслідок, автоматична тривога на гаджеті особи, за якою ведеться стеження, не спрацьовує.

Як працюють навігаційні маяки (Beacons)

Навігаційні маяки дозволяють створювати системи внутрішньої навігації в приміщеннях, а також вони використовуються в маркетингу та логістиці.

Особливості:

- Маяк зазвичай жорстко закріплений на стіні, колоні, дверях чи стелі (на відміну від мітки яка рухається з людиною, транспортом або вантажем)
- MAC-адреса та UUID ніколи не змінюються (у мітки зміна відбувається постійно)
- Транслює відкриті стандартизовані дані (у міток вони зашифровані)

Приклади навігаційних маяків: iBeacon (Apple), Eddystone (Google) або AltBeacon.

Навігаційний маяк може транслювати таку інформацію в пакеті:

- **UUID (Універсальний ідентифікатор):** Загальний ID, який показує, якій системі чи будівлі належить маяк
- **Major ID (Головний параметр):** Визначає конкретну зону або поверх (наприклад, «2-й поверх»).
- **Minor ID (Другорядний параметр):** Визначає точну точку встановлення (наприклад, «Маяк №14 біля ліфта»).
- **Tx Power Level (Калібровочна потужність):** Значення RSSI на відстані 1 метра від маяка. Пристрій-користувач зчитує цей параметр, порівнює його з поточним рівнем сигналу і за формулою вираховує точну відстань до маяка (до сантиметрів).

Незмінні параметри маяків (в особливості MAC-адреса) дозволяють відмічати їх як «верифіковані» (перевірені безпечні пристрої) з ціллю більш зручного виявлення тільки нових сигналів.

Аналіз окремого пристрою

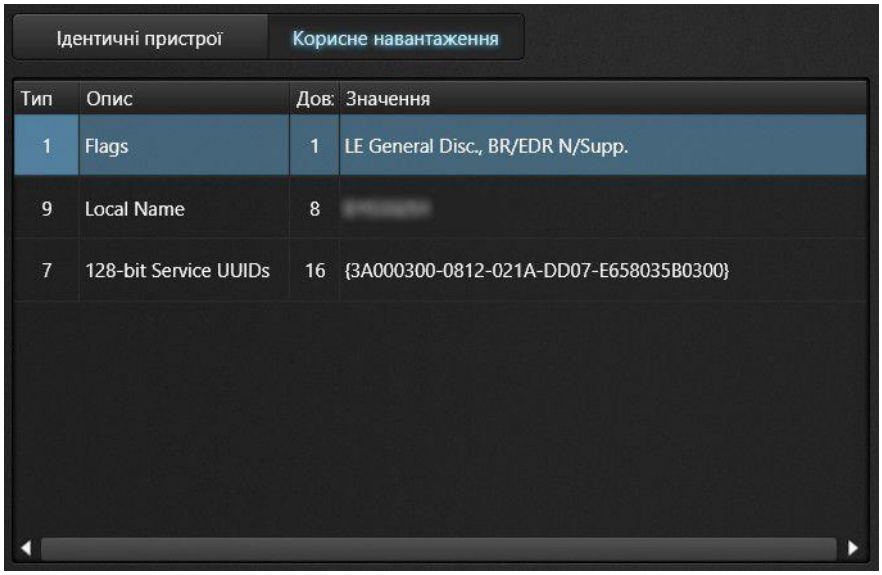
Використовуйте аналіз окремого пристрою для фізичної локалізації джерела та вивчення корисного навантаження що транслюється в пакеті.

На панелі відображається така інформація про пристрій:

- **Пристрій** — ідентифікатор пристрою (MAC-адреса).
- **Тип** — тип пристрою (за результатом роботи автоматичного алгоритму розпізнавання):
  - Tag - мітка
  - Beacon - маяк геопозиціювання
  - BLE - будь-який інший BLE-пристрій, не ідентифікований як Tag чи Beacon
- **Виробник** — назва виробника обладнання
- **Деталі** — додаткова інформація про пристрій. Тут виводиться тип пристрою, якщо його було ідентифіковано, ім’я пристрою (якщо сповіщається) та інша інформація з корисного навантаження
- **Активність:**
  - **First seen** – час першого виявлення
  - **Last seen** – час останнього виявлення
  - **Packets** – лічильник зареєстрованих пакетів
- **RSSI** — поточний рівень сигналу в dBm та графічна шкала, яка відображає поточний, піковий та максимальний рівні (поточна та пікова шкала активні тільки коли пристрій передає пакети).
- **Поріг** — дублікат регулятора порогового рівня сигналу для зручності локалізації. Дозволяє оператору оперативно змінювати поріг під час наближення до джерела.

- **Коментар** – текстовий коментар оператора
- **Верифікований** — прапорець для присвоєння пристрою статусу «верифікований» (детальніше див. розділ нижче).
- **Вкладка «Ідентичні пристрої»** відображає список пристроїв, що мають ідентичну структуру даних (детальніше див. розділ нижче).

Вкладка «Корисне навантаження» дозволяє переглядати корисне навантаження що транслюється пристроєм:



Тип – ідентифікатор типу поля.
Опис – опис поля
Дов – довжина поля (байт)
Значення – значення поля

Корисне навантаження пакетів сповіщення (Advertising Payload) може включати такі типи полів:

Тип (Десяткове значення)	**Опис поля**
1	Прапорці стану (Flags)
2 – 7	Ідентифікатори служб (UUID)
8, 9	Локальне ім’я пристрою (скорочене / повне)
10	Рівень потужності передавача (Tx Power Level)
13	Клас пристрою (Class of Device)
14, 15	Параметри з’єднання (Інтервали підключення)
16	Ідентифікатор безпеки / Сервісний UUID пристрою
18	Інтервал підключення Slave (Slave Connection Interval Range)
20, 21, 31	Список запитів на обслуговування (Service Solicitation UUIDs)
22	Сервісні дані (Service Data)
23	Публічна адреса цільового пристрою (Public Target Address)

24	Випадкова (рандомна) адреса цільового пристрою (Random Target Address)
25	Зовнішній вигляд / Категорія пристрою (Appearance)
26	Інтервал сповіщення (Advertising Interval)
27	Bluetooth-адреса пристрою LE (LE Bluetooth Device Address)
28	Роль пристрою LE (LE Role)
32, 33	Сервісні дані для 32/128-бітних UUID
36	Інформаційне URI-посилання (Uniform Resource Identifier)
255	Специфічні дані виробника (Manufacturer Specific Data)

Структура полів корисного навантаження може відрізнятися для BLE-пристроїв різних типів. Деякі з них передають відкриту інформацію, таку як Local Name (локальне ім’я пристрою), UUIDs (ідентифікатори служб) тощо, а інші — лише дані в закритому вигляді, використовуючи поле типу 0xFF (255) «Специфічні дані виробника» (Manufacturer Specific Data) або 0x16 (22) «Сервісні дані» (Service Data).

Ідентичні пристрої та ідентифікація нового екземпляра

Як зазначено вище, більшість BLE-пристроїв захищені від відстеження шляхом постійної зміни MAC-адреси та корисного навантаження за допомогою криптографічного ротаційного ключа. Така зміна може відбуватися кожні 10–15 хвилин, а в деяких випадках і частіше. Кожна нова ротація створює новий екземпляр у таблиці пристроїв Breeze RF, тоді як попередній запис залишається неактивним.

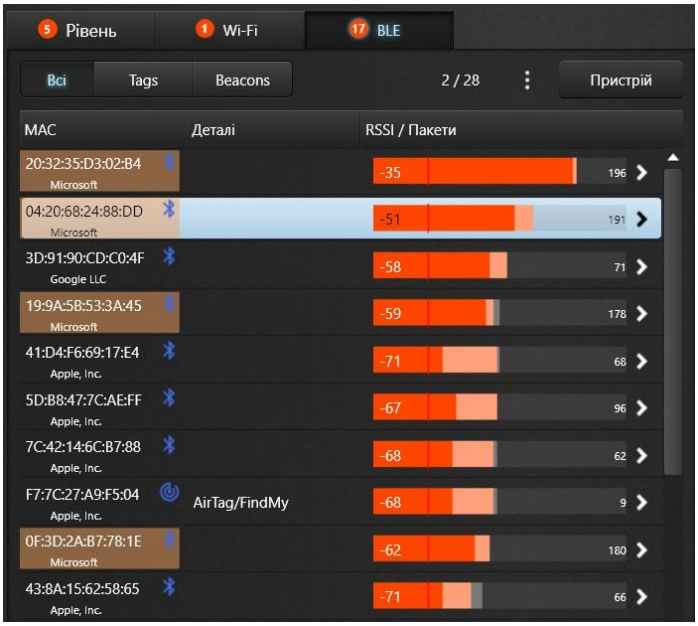
Функція виявлення ідентичних пристроїв дозволяє знаходити об'єкти з аналогічною структурою корисного навантаження і таким чином «зв’язувати» різні екземпляри одного фізичного девайса між собою. Завдяки цій функції ви можете продовжувати аналіз або локалізацію пристрою, який змінив ідентифікатор, швидко перейшовши до його нового екземпляра.

Звісно, багато однотипних пристроїв (наприклад, смартфони чи навушники Apple) можуть мати однакову структуру пакетів, залишаючись при цьому фізично різними девайсами. Щоб точно визначити, який саме об'єкт є новим екземпляром цільового пристрою, а який — чужим девайсом, використовуйте рівень сигналу RSSI, графік тривог та часові маркери (час першого й останнього виявлення). Для цього застосовуйте такі критерії:

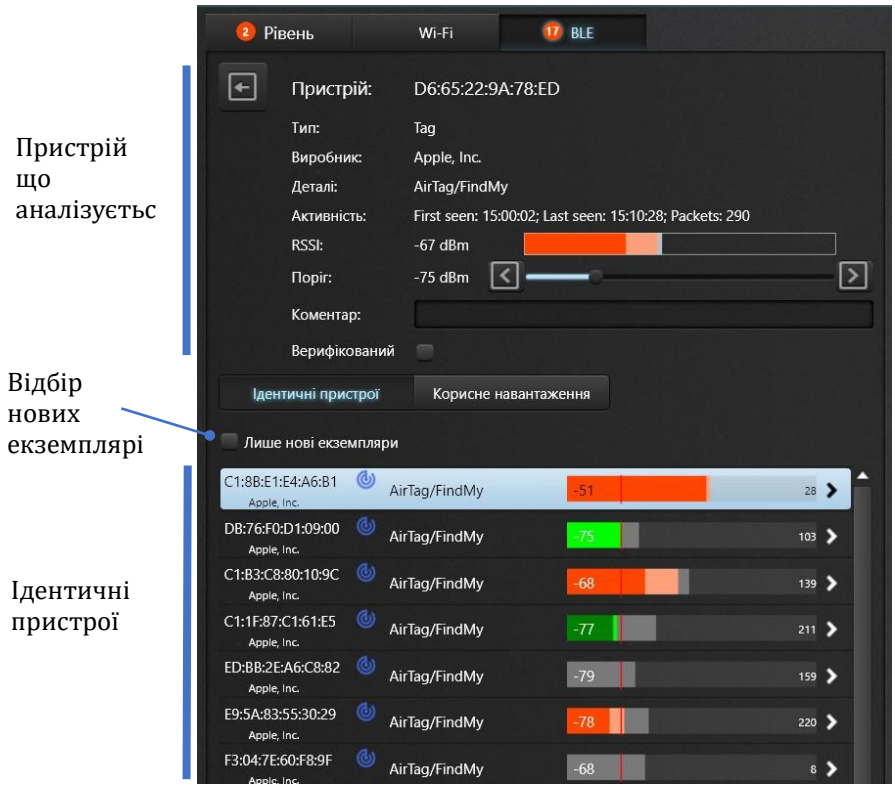
- **Максимальний накопичений рівень RSSI:** у фізично різних девайсів він зазвичай відрізнятиметься через різну відстань до приймача.
- **Часове перекриття:** активність фізично різних девайсів може **перетинатися в часі**.
- **Послідовність активації:** активність різних екземплярів одного й того самого девайса **ніколи не перетинається в часі**. Якщо ви аналізуєте активний пристрій, його старі екземпляри у списку ідентичних уже будуть неактивними. Щойно поточний пристрій зникне з ефіру (змінить адресу), новий екземпляр з’явиться у списку одразу після цього.

Доповнення: Один і той самий фізичний девайс може транслювати рекламні пакети кількох різних типів одночасно (наприклад, одночасно надсилати відкрите ім'я та зашифровану телеметрію виробника).

Коли панель «BLE» перебуває в стандартному режимі (відображення списку пристроїв): активуйте пункт меню «Виділити ідентичні пристрої», і всі схожі об'єкти підсвічуватимуться в списку золотавим кольором.



Коли панель «BLE» переведена в режим аналізу конкретного пристрою: у вкладці «Ідентичні пристрої» відображається їх повний список, а прапорець «Лише нові екземпляри» дозволяє відфільтрувати тільки ті об’єкти, що з’явилися в ефірі після деактивації поточного пристрою.



Як працює фільтр «Лише нові екземпляри»
Щойно пристрій змінює свій ідентифікатор (MAC-адресу), його старий екземпляр перестає бути активним. Програма порівнює значення в полях «Останнє виявлення» старого екземпляра та «Перше виявлення» потенційних нових кандидатів.
Завдяки цьому алгоритм відсікає пристрої, які працювали в ефірі паралельно, і виводить лише ті, що з’явилися після зникнення поточного об'єкта. Це суттєво звужує зону пошуку та дозволяє оператору миттєво перейти до аналізу нового актуального екземпляра.

Порада: Після фізичної локалізації пристрою та підтвердження його безпечності додавайте до нього текстовий коментар. У ньому варто вказати тип пристрою, його власника або місце розташування (наприклад: «Навушники Івана», «Телефон Андрія», «Принтер у кабінеті 4» тощо).
Ця інформація автоматично підтягуватиметься й відображатиметься в списку ідентичних пристроїв, що значно полегшить розпізнавання його нових екземплярів у майбутньому.

«Стрілка вправо» біля ідентичного пристрою дозволяють перейти до його аналізу.

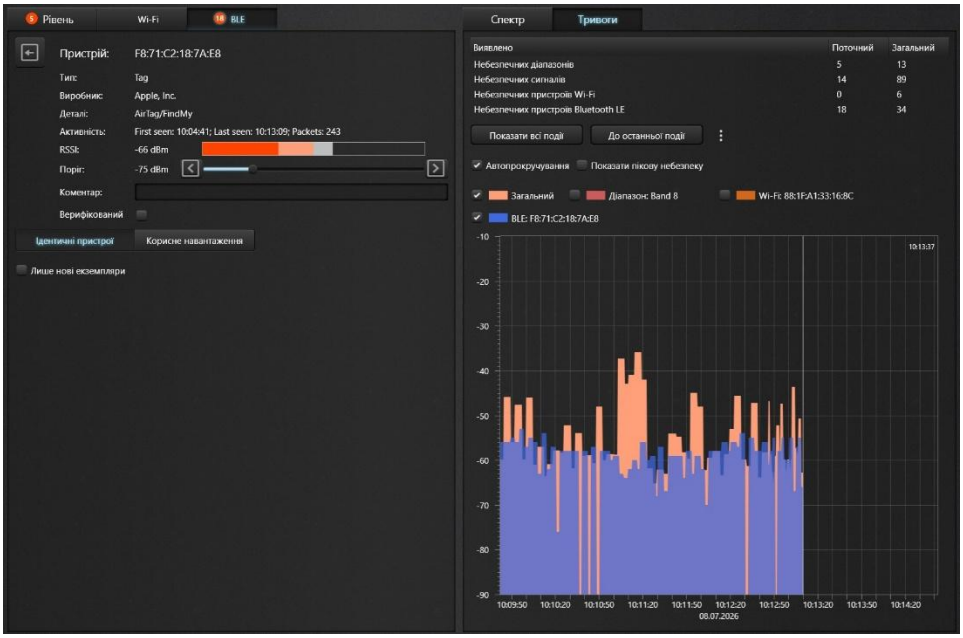
Історія активності

Якщо запис журналу увімкнений, програма Breeze RF реєструє історію активності по кожному виявленому BLE-пристрою з можливістю її перегляду на графіку панелі «Тривоги».

Якщо запис не активний, графік накопичує історію по вибраному пристрою але скидає її при виборі іншого та починає накопичення спочатку.

Щоб увімкнути перегляд історії на графіку необхідно вибрати пристрій в таблиці та встановити прапорець «BLE: XX:XX:XX:XX:XX» (MAC-адреса пристрою) на панелі «Тривоги».

Графік історії по вибраному пристрою буде відображатися напівпрозорим блакитним кольором:



Оскільки більшість екземплярів в таблиці будуть мати обмежений час існування, щоб знайти необхідний період на графіку буде необхідно користуватися перемоткою (скролінгом) та масштабуванням (зміна інтервалу). Час першого виявлення (First seen) та час останнього виявлення (Last seen), які відображуються в режимі аналізу окремого пристрою, дозволяють визначити необхідний період.

При виборі іншого пристрою в таблиці графік буде автоматично налаштовуватись на відображення історії нового пристрою.

За допомогою функції масштабування (яка активується під час клацання мишкою на графіку) можна гнучко налаштувати часовий інтервал відображення даних:

- **Короткий інтервал (швидке оновлення часу)** — оптимізований для миттєвого відстеження змін рівня сигналу безпосередньо під час локалізації (пошуку) джерела.
- **Довгий інтервал (повільне накопичення)** — призначений для ретроспективного аналізу активності пристрою та виявлення паттернів його поведінки протягом тривалого часу.

Ви можете більш детально ознайомитись з роботою з графіком у розділі «Панель «Тривоги».

Відображення пристроїв на графіку спектра

Програма Breeze RF підтримує відображення іконок BLE-пристроїв безпосередньо на графіку спектра. Вони розміщуються на частотних каналах сповіщення (Advertising) № 37, 38 та 39 із прив'язкою до їхнього поточного рівня сигналу (RSSI).

Примітка щодо візуалізації: Фізично BLE-пристрій дублює пакети сповіщення одночасно на всіх трьох каналах (37, 38 та 39). Проте для уникнення візуального нагромадження та покращення сприйняття програма відображає іконку пристрою лише на одному з цих каналів.

Візуальне поєднання спектрограми з даними сканування BLE дозволяє оператору наочно оцінювати радіообстановку під час огляду приміщення в режимі реального часу:

- **Наближення до об'єкта:** іконка пристрою, до якого наближається пошукова система, зміщуватиметься вгору (рівень RSSI зростає по вертикалі).
- **Віддалення від об'єкта:** іконка пристрою, від якого система віддаляється, зміщуватиметься вниз (рівень RSSI падає).

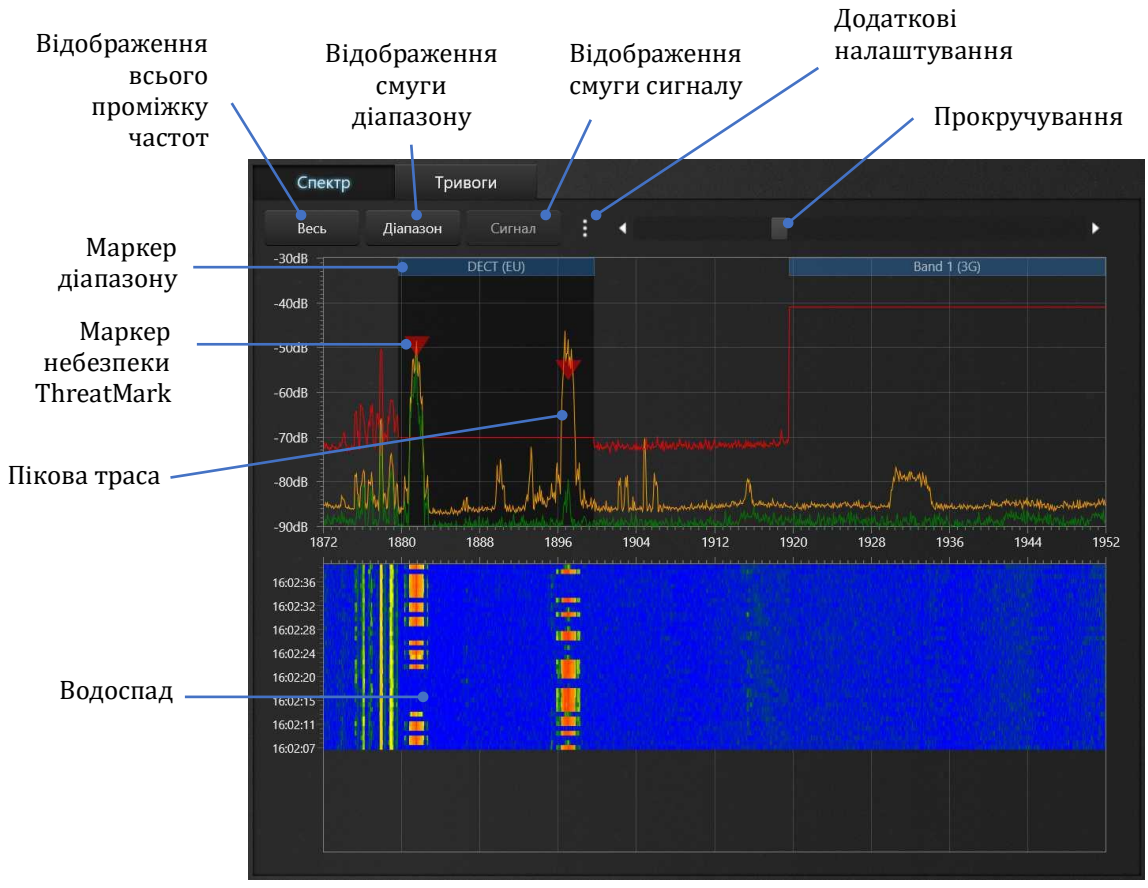
Як увімкнути відображення:

3. У меню панелі **«Спектр»** виберіть пункт **«Пристрої» → «Bluetooth LE»**.
4. **Масштабуйте графік спектра** для відображення діапазону 2.4 ГГц. Зробити це швидко можна двома способами:
    - Перейдіть на панель «Рівень» і двічі клацніть на діапазон «ISM 2.4 GHz».
    - Або двічі клацніть на будь-який об’єкт на панелі «BLE»

Особливості режимів відображення:

- **Режим загального сканування:** за великої кількості виявлених BLE-пристроїв велика кількість іконок може візуально перевантажувати графік спектра.
- **Режим аналізу окремого пристрою:** на графіку відображається виключно цільовий об'єкт, що дозволяє оператору повністю зфокусуватися на його локалізації.

Панель "Спектр"



Панель «Спектр» відображає графік спектра та графік «Водоспад». За допомогою цих інструментів користувач може досліджувати сигнали й отримувати інформацію про їхній рівень, періодичність появи, смугу частот, тривалість роботи тощо.

На графіку спектра можна переглядати будь-яку ділянку частот: наприклад, увесь частотний проміжок, що охоплюється пристроєм, конкретний діапазон або окремий сигнал.

Відображувані рівні сигналу становлять від -90 до -20 дБ або від -100 до -20 дБ залежно від обраного рівня підсилення.

Графік спектра може автоматично регулювати вертикальний масштаб до максимального рівня сигналу, який виявляється. У такому режимі можуть відображатися рівні до 0 дБм.

Одиниця вимірювання рівня сигналу залежить від моделі комплексу: «дБм» для Delta X та «дБ» для Delta S.

Кнопка «Весь» налаштовує графік на відображення всього частотного проміжку, який сканується.
Кнопка «Діапазон» перемикає графік на відображення смуги поточного виділеного діапазону.
Кнопка «Сигнал» фокусує графік на смузі поточного сигналу (доступна лише в режимах дослідження діапазону або сигналу).

Поточна (миттєва) траса спектра на графіку відображається **зеленим** кольором, а лінія порогу — **червоним**.

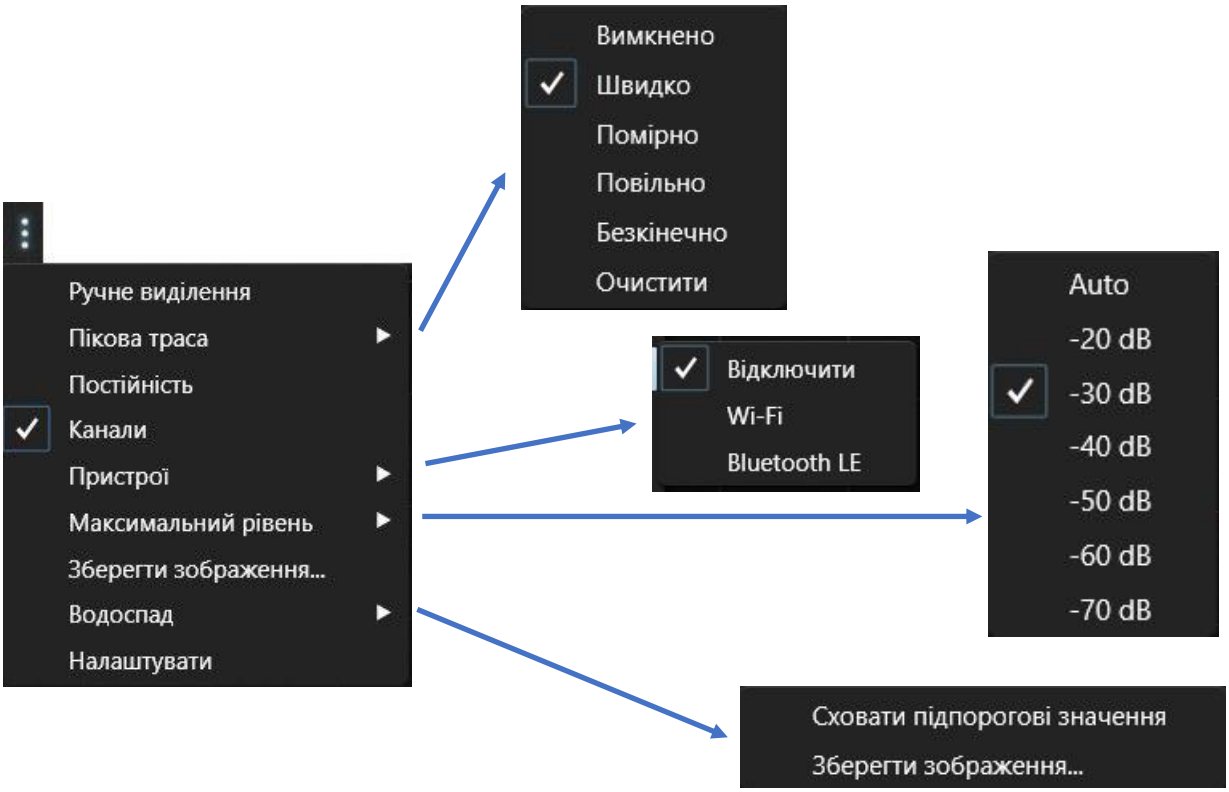
Графік спектра підтримує **прокручування**. Крім стандартної смуги прокручування, можна натиснути ліву кнопку миші над графіком і, не відпускаючи її, перетягнути зображення вліво або вправо. На пристроях із сенсорним екраном цю дію можна виконати, торкнувшись графіка спектра пальцем або стилусом.

Графік спектра підтримує зручне **масштабування**. Щоб змінити масштаб, клацніть на графіку мишкою (або торкніться екрана) та натисніть кнопку **«Збільшити»** або **«Зменшити»**. Також можна миттєво збільшити масштаб **до меж потрібного діапазону**, якщо виділити його заздалегідь.

Щоб **зробити виділення**, натисніть і утримуйте праву кнопку миші над початковою частотою, перемістіть курсор до кінцевої частоти, після чого відпустіть кнопку. Виділення конкретного сигналу також здійснюється автоматично під час подвійного кліку на нього на панелі «Рівень».

Водоспад займає нижню частину панелі та відображає історію спектральних вимірювань за певний проміжок часу. Кожна горизонтальна лінія в ньому представляє одну спектральну трасу. Рівень сигналу кодується кольором: **синій** — низький рівень, **зелений** — дещо вищий, **жовтий** — середній, а **червоний** — високий. Під час вимірювання старі траси зміщуються вниз, а нові з'являються вгорі. Мітки часу відображаються ліворуч. Оператор може використовувати Водоспад для виявлення непостійних (імпульсних) сигналів та відстеження їхньої частоти.

Кнопка додаткових налаштувань відкриває спливаюче меню:

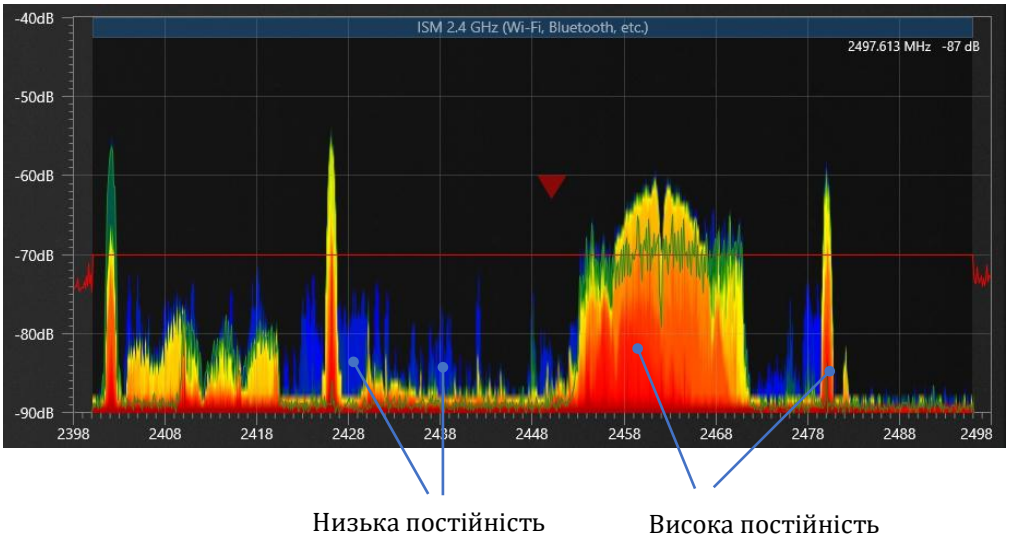


Ручне виділення: Дозволяє оператору виконувати виділення на графіку спектра за допомогою лівої кнопки миші, що особливо зручно на сенсорних екранах. За замовчуванням для вибору діапазону необхідно натиснути й утримувати праву кнопку.

Пікова траса: Завдяки властивості утримувати максимальне значення спектра, траса піків дозволяє оператору помічати будь-які короткочасні події від імпульсних сигналів. Крива піку позначається **помаранчевим** кольором на графіку спектра.

- Швидко, Помірно, Повільно, Безкінечно — вмикають пікову трасу та дозволяють встановити час інтеграції (накопичення). Режим «Безкінечно» запускає постійне накопичення даних.
- Вимкнено — повністю вимикає пікову трасу.
- Очистити — скидає поточну пікову трасу та перезапускає процес накопичення.

Постійність (Persistence): Ця функція використовує зміну кольорів для відображення сигналів із різним рівнем активності. Чим частіше з’являється сигнал у цій точці ефіру, тим у «тепліший» колір він фарбується на графіку. Одиничні появи сигналу відображаються **синім** кольором, частіша активність — **зеленим**, а регулярні або постійні сигнали — **жовтим** чи **червоним**.



Використовуйте цей режим для дослідження щільно завантажених діапазонів, де багато сигналів перекриваються (наприклад, ISM 2.4 ГГц).

Канали: Вмикає та вимикає функцію підпису каналів на спектрі з візуальним підсвічуванням їхньої смуги та рівня.

Пристрої: Вмикає відображення іконок пристроїв Wi-Fi / BLE безпосередньо на графіку спектра. Пристрої розміщуються на відповідних частотних каналах із прив'язкою до їхнього поточного рівня сигналу (RSSI). Для коректного відображення панель **«Спектр»** має бути налаштована на відповідну смугу частот.

Максимальний рівень: Встановлює верхню межу вертикального масштабу графіка спектра. Вибирайте вище значення для відображення потужних сигналів і нижче — для кращої візуальної ідентифікації слабких сигналів. Доступні значення: від -70 дБ до -20 дБ або **«Авто»**. У режимі **«Авто»** графік спектра автоматично регулює свій вертикальний масштаб.

Зберегти зображення...: Експортує поточний знімок графіка спектра у файл форматів .jpeg або .bmp.

Водоспад | Приховати підпорогові значення: Дозволяє приховати області «Водоспаду» з низьким рівнем шуму і таким чином чітко виділити сигнали, які перевищили встановлений поріг.

Водоспад | Зберегти зображення...: Експортує повне зображення історії «Водоспаду» у файл форматів .jpeg або .bmp.

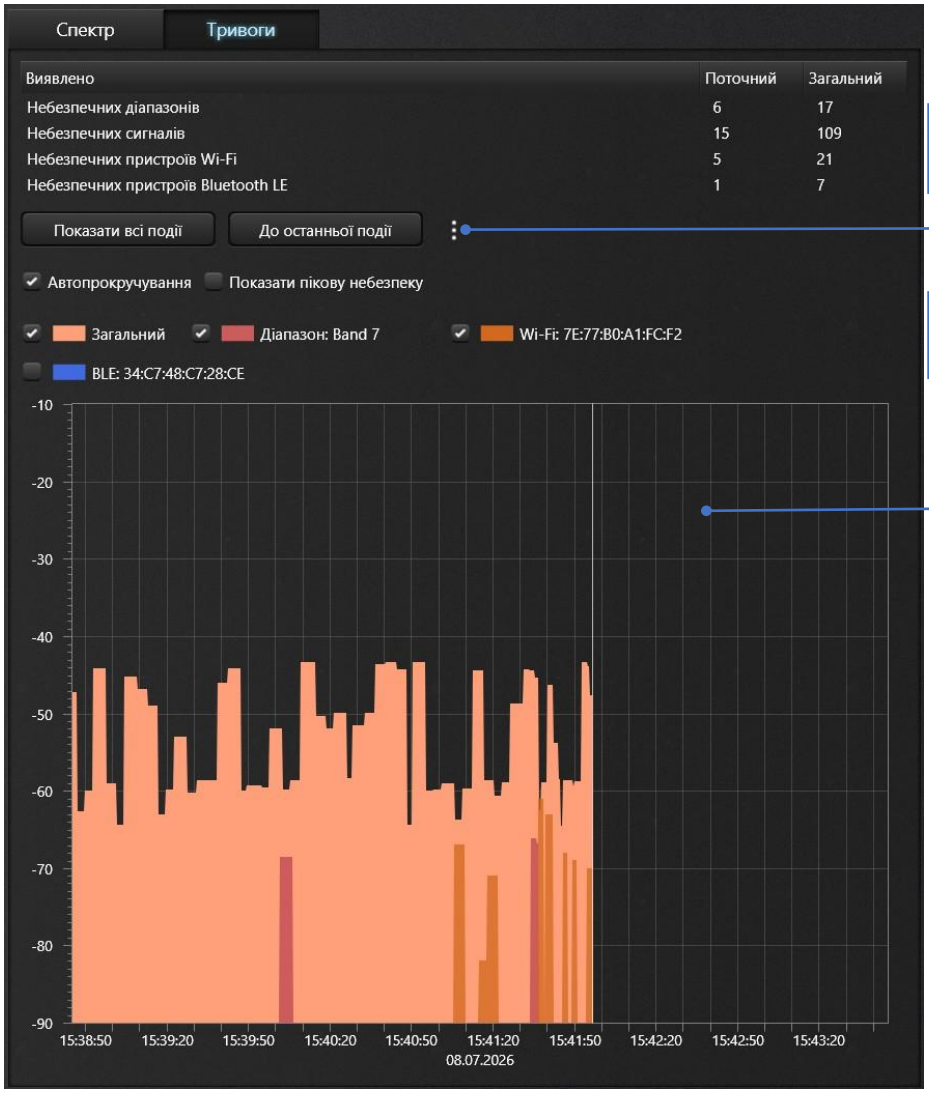
Налаштувати: Відкриває два додаткові елементи керування:

- **Вертикальний трекпад** (праворуч від графіка спектра) — допомагає налаштувати колірну гаму «Водоспаду» та графіка постійності. Зміщуючи рівень жовтого кольору, оператор регулює контрастність відображення ефіру.
- **Параметр «Пікселів на вимір»** (під «Водоспадом») — дозволяє встановити бажану кількість пікселів на одне спектральне вимірювання. Більші значення підвищують читабельність ліній, але призводять до того, що «Водоспад»

зміщуватиметься швидше та зберігатиме історію за менший проміжок часу. Значення за замовчуванням — 2.

Панель «Тривоги»

На цій панелі в режимі реального часу відображається інформація про виявлені загрози під час пошуку або в режимі «Стоп».



Статистика по небезпекам

Додаткові налаштування

Вибір даних для відображення

Клацніть мишкою щоб масштабувати або «тягніть» вліво-вправо для скролінгу

Таблиця статистики показує кількість небезпечних діапазонів, сигналів та пристроїв як у **поточний момент**, так і сумарно за весь період роботи (**загальний**).

Реєстрація даних у журнал відбувається за такою логікою:

- За результатами спектрального аналізу записуються **лише тривожні події** (коли рівень будь-якого сигналу перевищив встановлений поріг).
- Результати сканування **Wi-Fi** та **BLE** записуються **постійно**, незалежно від перевищення порогу.

Кількість подій за тривалий проміжок часу може бути значною, і **графік тривог** є зручним інструментом для їхньої візуалізації. Робота графіка тісно пов'язана із записом журналу. Коли ведеться запис, графік відображає як поточні дані, так і ті, що були збережені раніше. У разі зміни параметрів (прокручування, перехід до іншого діапазону чи сигналу) дані миттєво зчитуються з журналу. Якщо запис не ведеться, графік скидає дані щоразу, коли змінюються параметри відображення, і починає побудову заново.

Графік тривог може відображати дані в таких режимах (обирається в **меню додаткових налаштувань**):

- **Рівень dBm** — абсолютне значення рівня сигналу.
- **Рівень небезпеки** — надпорогове значення рівня сигналу (перевищення порогу).

Графік можна налаштувати на відображення таких параметрів:

- **Загальний** — сукупний рівень dBm / небезпеки за всіма діапазонами. Відображається світло-червоним кольором.
- **Вибраний діапазон** — рівень dBm / небезпеки для діапазону, що вибраний на панелі «Рівень». Відображається яскраво-червоним кольором.
- **Вибраний сигнал** — рівень dBm / небезпеки для сигналу, що вибраний на панелі «Рівень». Відображається темно-червоним кольором. Цей параметр стає доступним лише тоді, коли панель «Рівень» переведена в режим дослідження окремого діапазону чи сигналу.
- **Wi-Fi** — рівень dBm / небезпеки для пристрою, що вибраний на панелі «Wi-Fi».
- **BLE** — рівень dBm / небезпеки для пристрою, що вибраний на панелі «BLE».

«Автопрокручування» вмикає режим автоматичного зміщення графіка під час пошуку, щоб на екрані завжди відображалися останні результати вимірювань.

Якщо автопрокручування вимкнене, графік тривог можна перемотати на **будь-який момент часу**. Для цього клацніть лівою кнопкою миші на графіку і, не відпускаючи її, потягніть курсор вліво чи вправо. На пристроях із сенсорним екраном цю дію можна виконати пальцем або стилусом.

Якщо ви бажаєте змінити часовий період відображення (масштабувати графік), клацніть на ньому лівою кнопкою миші та використовуйте кнопки **«Збільшити»** або **«Зменшити»**. Також для масштабування можна використовувати коліщатко миші.
Примітка: Максимальний часовий інтервал, який здатний одночасно відобразити графік, становить **6 годин**.

Кнопка **«Показати всі події»** — автоматично налаштовує масштаб для відображення всіх наявних у журналі подій.
Кнопка **«До останньої події»** — виконує швидке прокручування до найновішої події в журналі.

У режимі «Стоп» (перегляд журналу) користувач має можливість аналізувати рівні діапазонів, сигналів та пристроїв на конкретний момент часу за допомогою кліку на потрібну точку графіка. При цьому шкали на панелях «Рівень», «Wi-Fi» та «BLE» миттєво відобразять рівні сигналів, що відповідають обраному часу, а «Водоспад» автоматично перемотається для показу спектральної історії цієї події.

Рекомендації щодо пошуку

Підготовка

Вибір режиму пошуку

Оберіть режим пошуку, який максимально відповідає вашому завданню:

- **«Всі сигнали»** — використовується для комплексної перевірки приміщень на наявність усіх видів закладних пристроїв.
- **«Мобільні/GPS-трекери»** — використовується для пошуку автомобільних маяків (трекерів).
- **«Низхідні/Навігація»** — використовується для виявлення навмисного глушіння радіосигналів (окремо або в поєднанні з іншими режимами).
- **«Бездротові/ISM»** — використовується для виявлення різних бездротових пристроїв, в т. ч. Wi-Fi, Bluetooth та ін.

Важливо:

- Намагайтеся завжди використовувати режим, який найкраще підходить для поточного завдання. Велика смуга сканування у режимі **«Всі сигнали»** суттєво знижує ймовірність виявлення короткочасних імпульсних сигналів. Тому наполегливо рекомендуємо уникати цього режиму під час цільового пошуку автомобільних маяків або бездротових пристроїв.
- Для підвищення надійності результату рекомендується додатково провести перевірку в режимах **«Мобільні/GPS-трекери»** та **«Бездротові/ISM»** після завершення загального сканування в режимі **«Всі сигнали»**. Це значно збільшить ймовірність виявлення складних мобільних та бездротових загроз.

Антени

Delta S	**Delta X**
Оскільки в комплекті постачання для входу **INPUT 1** передбачено дві антени на вибір, оберіть ту, яка відповідає вашому поточному завданню: • **ODA-4** — всеспрямована багатоцільова антена, яка підходить для всіх режимів пошуку, зокрема для комплексного режиму **«Усі сигнали»**. • **MWA-6** — спрямована мікрохвильова (НВЧ) антена. Вона забезпечує більшу дальність виявлення та спрощує локалізацію джерела завдяки своїй спрямованості, але має обмежений діапазон частот. Цій антені слід віддати перевагу під час перевірки	Під'єднайте всеспрямовану антену **ODA-4** до входу **INPUT**. Під'єднайте спрямовану антену **MWA-6** до входу **AUX1**. Підключіть антени **LPDA-12** до високочастотних входів **Wi-Fi**, **BLUETOOTH** та **AUX2**.

великогабаритного транспорту, вантажівок або протяжних вантажів у режимі **«Мобільні/GPS-трекери»** (де потрібна вузька спрямована діаграма виявлення), а також для тимчасового перемикання з метою точного виявлення місцезнаходження джерела. Підключіть антени **LPDA-12** до відповідних високочастотних входів **Wi-Fi**, **BLUETOOTH** та **INPUT 2**.	

За потреби змініть частоту розподілу сигналів між першим та другим антенними входами за шляхом: **«Налаштування»** → **«Пристрій»** → **«Частота AUX1 (INPUT2)»**.
За замовчуванням для першого входу призначено діапазон частот **до 3000 МГц**, а для другого — **3000–6000 МГц**.
Змінювати частоту розподілу **AUX1 (INPUT2)** доцільно в таких випадках:

- Коли оператор планує використовувати спрямовані властивості антени **MWA-6** для точного визначення місцезнаходження (локалізації) передавача на нижчих частотах.
- Коли під час тривалого моніторингу без переміщення комплексу в протяжних приміщеннях необхідно задіяти довшу діаграму спрямованості всеспрямованої антени.
- Під час огляду вантажних автомобілів або великогабаритних вантажів у режимі **«Мобільні/GPS-трекери»** для формування подовженої зони виявлення уздовж транспортного засобу.

Важливо: Мінімально допустиме значення частоти для порту **AUX1** становить **800 МГц**, що відповідає нижній робочій межі антени **MWA-6**.

Файл журналу

Створіть окремий **файл журналу** для запланованої локації пошуку. У разі проведення повторної перевірки на цьому самому об'єкті ви зможете відкрити цей файл знову, щоб дописувати в нього нові дані.

Маскування фону

Режими **«Всі сигнали»** та **«Низхідні/Навігація»** потребують попереднього маскування фону за межами цільового приміщення. Оберіть коректну точку розташування комплексу поза об'єктом та виконайте процедуру маскування. Для мінімізації хибних спрацювань задайте триваліший час накопичення спектра та повторіть маскування фону в кількох точках навколо цільової зони (але в жодному разі не всередині неї).

Примітка: Для режимів **«Мобільні/GPS-трекери»** та **«Бездротові/ISM»** процедура маскування фону не потрібна.

Пороги

Визначтеся з дальністю виявлення, якої ви прагнете досягти під час поточної перевірки. Системи **Delta S** і **Delta X** мають надзвичайно високу чутливість і здатні фіксувати

сигнали на відстані десятків і сотень метрів. Проте для завдань протидії негласному зніманню інформації рекомендується штучно обмежувати дальність виявлення. Це дозволить уникнути численних хибних тривог від зовнішнього ефіру та суттєво спростить процес локалізації. Ефективніше послідовно переміщуватися цільовою зоною, виявляючи та локалізуючи сигнали один за одним, ніж бачити десятки сигналів одночасно, не розуміючи джерела їхнього походження.
Програмне забезпечення **Breeze RF** встановлює оптимальні пороги діапазонів за замовчуванням. Вони забезпечують дальність виявлення в кілька метрів для мобільних і бездротових діапазонів (що ідеально для пошуку в кімнаті) та більшу дальність для інших сигналів поза межами цих діапазонів.

Коли потрібно ЗБІЛЬШИТИ пороги (зменшити дальність виявлення):
Збільшення порогів відсікає слабкі сигнали. Це необхідно в таких випадках:

- **Для захисту від завад із сусідніх приміщень:** щоб уникнути сигналів, які проникають крізь стіни (наприклад, Wi-Fi сусідів) і створюють хибні спрацювання.
- **Для селективного зниження чутливості:** коли необхідно загрубити чутливість на окремому складному діапазоні або на всіх частотах одночасно.
- **Під час фізичного пошуку (локалізації) передавача:** коли оператор наближається до передбачуваного джерела методом «гаряче/холодно» і крок за кроком підвищує пороги, щоб звузити зону пошуку до конкретного сантиметра.

Коли потрібно ЗМЕНШИТИ пороги (збільшити дальність виявлення):
Зменшення порогів підвищує чутливість системи до слабких сигналів. Це доцільно:

- Якщо ви плануєте проводити тривалий радіомоніторинг об'єкта без переміщення комплексу.
- Якщо необхідно охопити контролем велику відкриту територію (наприклад, залу засідань або склад) з однієї точки.
- Якщо ви виконуєте огляд транспортного засобу в режимі **«Мобільні/GPS-трекери»** за умови відсутності завад.

Додаткова інформація: Детальний опис процедури коригування наведено в розділах «Налаштування порогів діапазонів», «Поріг Wi-Fi» та «Поріг BLE».

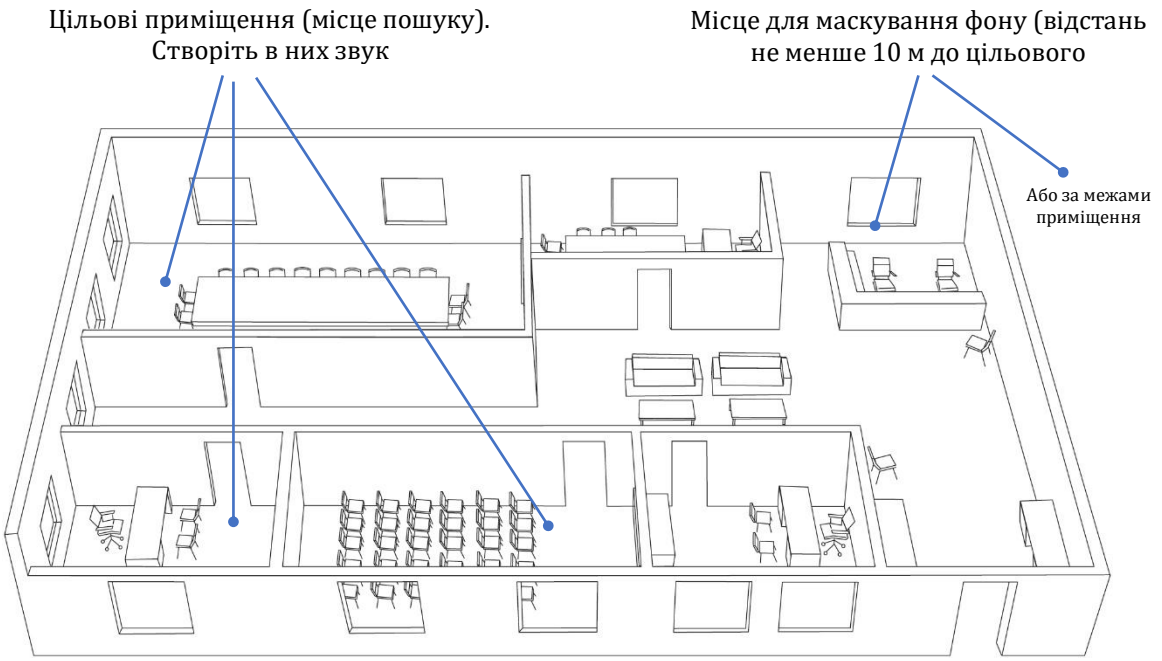
Запобігання хибним спрацюванням

Деактивуйте (вимкніть) усі санкціоновані радіочастотні засоби на локації, де проводиться пошук. Це стосується мобільних телефонів, комп’ютерів, точок доступу, бездротової периферії (гарнітур, навушників, смартгодинників тощо), а також будь-яких інших побутових пристроїв, що працюють за стандартами Wi-Fi та Bluetooth.

Мінімізація хибних спрацювань суттєво прискорить процес перевірки та зробить її результати максимально надійними.

Акустична активація (звуковий фон)

Деякі типи закладних пристроїв (зокрема з функцією **VOX** або акустичним пуском) переходять у режим передачі даних лише за наявності звукового фону в приміщенні. Щоб активувати такі пристрої та зафіксувати їхнє випромінювання, під час перевірки необхідно забезпечити постійне джерело звуку (наприклад, увімкнути тестовий аудіозапис, генератор шуму, тощо).



Пошук

Спектральний пошук

Запуск режиму: Активуйте обраний режим пошуку. Режими **«Мобільні/GPS-трекери»** та **«Бездротові/ISM»** можна вмикати одночасно.

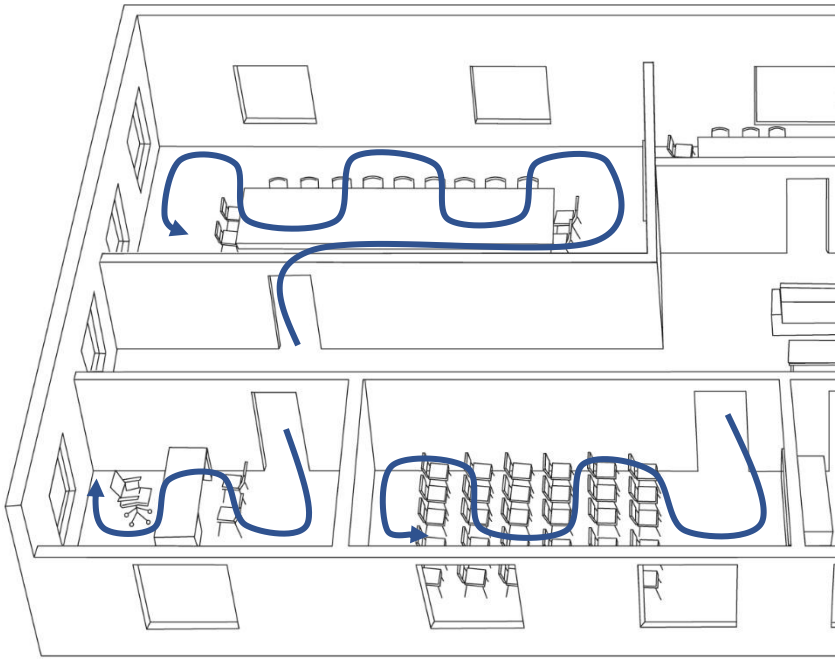
Активація журналу: Увімкніть фіксацію даних, натиснувши кнопку **«Запис журналу»** (якщо в налаштуваннях не активовано функцію автоматичного запису). Функція є активною, коли кнопка перебуває в натиснутому стані.

Налаштування сповіщень: Увімкніть звукову тривогу для зручності контролю поточної ситуації. Використовуйте функцію **«Утрим. макс. небезп.»** (Утримання максимальної небезпеки), щоб інтерфейс програми автоматично фокусувався на найбільш небезпечному діапазоні.

Тактика огляду приміщення: Перевіряйте об'єкт послідовно (наприклад, покімнатно). Скануйте кожну кімнату так, щоб забезпечити повне охоплення внутрішнього об’єму, враховуючи мінімальну дальність виявлення найслабшого сигналу, який потенційно може випромінюватися.

- Приклад траєкторії: Орієнтуючись на радіус виявлення **1 метр** навколо себе, рухайтеся «зигзагом» із кроком (відступом) **2 метри**.
- Швидкість руху: Переміщуйтеся зі швидкістю не більше ніж **0.5 м/с**, періодично спрямовуючи антенну систему в різні боки.

Контроль показників: Безперервно стежте за індикатором небезпеки й частотними діапазонами на панелі **«Рівень»**, а також за графіком історії та звуковими сигналами сповіщення.



Рівномірно оглядайте весь простір приміщення

Локалізація джерела (пошук місця розташування передавача)

Перехід до детального аналізу: На початку роботи панель **«Рівень»** перебуває в режимі моніторингу всіх частотних діапазонів. У разі виявлення загрози оператор переходить до дослідження конкретного небезпечного діапазону (входить у діапазон). Це звужує смугу сканування, суттєво підвищує швидкість роботи та ймовірність виявлення імпульсних сигналів. Для максимальної деталізації можна перейти до дослідження окремого сигналу, що ще більше звузить смугу аналізу.

Особливість мобільних мереж (динамічна зміна частот): Мобільні стандарти **LTE/4G** та **5G** здатні динамічно змінювати робочу частоту (діапазон) під час передачі даних. Якщо рівень сигналу в обраному діапазоні раптово впав, поверніть панель **«Рівень»** у режим моніторингу всіх діапазонів і зафіксуйте, де саме з’явився сплеск амплітуди. Після цього ви можете увійти в новий діапазон або продовжити локалізацію в режимі загального огляду **«Мобільні/GPS-трекери»**.

Пошук методом «гаряче/холодно»: Починайте локалізацію передавача. Для цього переміщуйте комплекс або змінюйте його просторову орієнтацію (крутіть), фіксуючи максимальний рівень сигналу. Стежте за шкалою рівня та вікном спектра, рухаючись у напрямку зростання амплітуди. Чим ближче антена до джерела випромінювання, тим вищим буде рівень сигналу. Світлодіодні індикатори на передній панелі приладу допоможуть визначити, яка саме антена активна в поточний момент. Під час наближення до джерела ви можете поступово **підвищувати поріг виявлення**, щоб штучно звузити радіус пошуку (після завершення локалізації обов'язково поверніть поріг до початкового значення).

Захист від перевантаження входу (Перевантаження тракту): Якщо рівень сигналу досягає критичних значень **-25...-20 дБм** і з’являється спотворення форми спектра (інтермодуляція) на сусідніх частотах, увімкніть внутрішній **атенюатор** (ослаблювач сигналів).

Фізичний догляд: Коли точку з максимальним рівнем радіовипромінювання чітко визначено, починайте ретельний фізичний та візуальний огляд меблів, конструкцій або предметів інтер'єру.
Ідентифікація зовнішніх завад: Пам'ятайте, що потужні сигнали з вулиці (наприклад, базові станції зв'язку) можуть спричиняти хибні спрацювання. Такі зовнішні завади зазвичай мають максимальний рівень біля вікон, зовнішніх стін, вентиляцій, підлоги чи стелі, а в міру заглиблення в приміщення їхній рівень стрімко падає.

Після завершення дослідження окремого діапазону чи сигналу обов'язково повертайте панель **«Рівень»** у стандартний режим моніторингу всього спектра.

Виявлення пристроїв Wi-Fi

Відкрийте панель **«Wi-Fi»**, де за час попереднього проходу вже накопичено список виявлених точок та клієнтів. Завданням оператора є ретельний **аналіз та локалізація** кожного пристрою Wi-Fi, зафіксованого в зоні пошуку (зокрема тих, чиї показники перевищують установлений поріг виявлення).

Переходьте до аналізу кожного окремого пристрою та виконуйте його фізичну локалізацію, орієнтуючись на амплітудний рівень **RSSI**.

Використовуйте функцію **«Верифікований»**, щоб позначити пристрій як безпечний (санкціонований), та додавайте до нього текстовий коментар для швидкої та легкої ідентифікації під час наступних перевірок.

Використовуйте функцію **«Взаємодіючі пристрої»** щоб виявляти зв’язки між точками доступу та клієнтами.

Виявлення пристроїв BLE в нез’єднаному стані

Відкрийте панель **«BLE»**, де за час попереднього проходу вже накопичено список зафіксованих пристроїв. Завданням оператора є ретельний **аналіз та локалізація** кожного пристрою BLE в зоні пошуку (зокрема тих, чиї показники перевищують установлений поріг виявлення).

Переходьте до аналізу кожного окремого пристрою та виконуйте його фізичну локалізацію, орієнтуючись на амплітудний рівень **RSSI**.

Особливість протоколу BLE (рандомізація MAC-адрес): Зважаючи на регулярну динамічну зміну ідентифікаторів (рандомізацію адрес) BLE-пристроями, можлива ситуація, коли список міститиме велику кількість уже неактивних засобів. У такому разі ви можете вимкнути відображення неактивних пристроїв за допомогою відповідного пункту в локальному контекстному меню та повторити прохід по приміщенню щоб накопичити пристрої, актуальні на даний момент.

Використовуйте функцію **«Верифікований»**, щоб позначити пристрій як безпечний (санкціонований), та додавайте до нього текстовий коментар для швидкої ідентифікації під час наступних перевірок (за умови, що цей пристрій зберігає постійний нерандомізований ідентифікатор).

Під час аналізу пристрою використовуйте функцію **«Ідентичні пристрої»**, щоб переглянути попередні екземпляри (історію виявлення) цього девайса або швидко перейти до аналізу його нового екземпляра, якщо зміна ідентифікатора (MAC-адреси) відбудеться безпосередньо під час сеансу аналізу.

Підготовка до довгострокового радіомоніторингу

Регламент підготовки до довгострокового радіомоніторингу:

1. Розміщення та доступ

- **Маскування та розташування:** Комплекс має бути розташований непомітно, але з урахуванням радіопрозорості конструкцій. Не ставте прилад у суцільні металеві шафи чи сейфи (це екранує антени).
- **Кабельний винос та затухання:** Якщо антени виносяться на кабелях (наприклад, для контролю суміжної кімнати), використовуйте тільки високоякісні коаксіальні кабелі з низькими втратами. Пам'ятайте, що на частотах понад 3 ГГц кожен метр дешевого кабелю критично знижує чутливість системи.
- **Мережева архітектура (RDP):** Для моніторингу тривалістю від кількох діб до тижня фізичний доступ до керуючого ПК зазвичай обмежений. Налаштуйте віддалений доступ через **RDP (Remote Desktop Protocol)** або спеціалізовані захищені канали. ПК повинен мати статичну IP-адресу, вимкнений режим сну (Sleep Mode) та активовану функцію автоматичного перезапуску в BIOS (Restore on AC Power Loss) на випадок збою електроживлення.

2. Попередній аудит та верифікація бездротового середовища

Сучасний офіс перенасичений легальними пристроями **Wi-Fi** та **Bluetooth Low Energy (BLE)**. Без попередньої зачистки ефіру журнал моніторингу буде перевантажений тисячами однотипних подій.

- **Вивчення бездротових мереж:** Перед стартом довгострокового моніторингу запустіть пошук у режимі **«Бездротові/ISM»** у робочий час (коли всі співробітники перебувають на робочих місцях), щоб накопичити дані на панелях **«Wi-Fi»** та **«BLE»**.
- **Маркування легальних пристроїв Wi-Fi:** Проаналізуйте ефір, локалізуйте джерела та переконайтеся в безпечності кожної корпоративної точки доступу, принтера, смарттелевізора, телефона чи ноутбука. Присвойте кожному санкціонованому об'єкту статус **«Верифікований»** та додайте чіткий текстовий коментар (наприклад, «Роутер Бухгалтерія» або «Телефон Івана»).
- **Ефект «Нового пристрою»:** Таке маркування дозволить системі під час тривалого моніторингу ігнорувати відомий санкціонований трафік і миттєво підсвічувати нові MAC-адреси, які з'явилися, наприклад, у нічний час або безпосередньо під час конфіденційних переговорів.
- **Аналіз BLE-патернів приміщення:** Зважаючи на постійну динамічну зміну ідентифікаторів BLE-пристроями та неможливість їхньої довгострокової прив’язки до конкретної MAC-адреси, раціонально аналізувати не кожну нову адресу окремо, а зміну загальної кількості та типів пристроїв у приміщенні (тобто фіксувати сталий патерн радіообстановки). Тим не менше, присвоєння санкціонованим об'єктам текстового коментаря додає зручності вставлення зв’язків нових екземплярів пристроїв з поточними під час майбутнього аналізу. В зв’язку з цим рекомендується виконати аналіз ефіру, локалізувати джерела, переконатись в безпечності кожного BLE-пристрою з цільовій зоні та присвоїти йому текстовий коментар, який їх ідентифікує.

Тактичний прийом: Встановіть вищий поріг виявлення, щоб обмежити зону контролю суто межами кабінету, і розмістіть антену **BLUETOOTH** максимально близько до цільової зони. Це дозволить отримати список пристроїв, який хоч і змінюватиметься за системними MAC-адресами, проте залишатиметься стабільним за специфікацією (типами) девайсів. Наприклад: за наявності керівника в кабінеті патерн виглядатиме як «смартфон + смартгодинник + ноутбук», а за його відсутності у активним залишатиметься тільки стаціонарний ноутбук. Будь-яке аномальне відхилення від цього патерна свідчитиме про появу стороннього BLE-джерела.

3. Конфігурація антенного перемикача AUX1 (INPUT2)
Залежно від геометрії приміщення необхідно оптимізувати роботу антенного входу.

- **Всеспрямований пошук (Стандарт):** За замовчуванням розподіл встановлено на рівні **3000 МГц**. Усе, що нижче, приймає всеспрямована антена ODA-4, що вище — антени MWA-6 та LPDA-12.
- **Спрямований пошук у протяжних зонах:** Якщо кімната довга (наприклад, коридор, зала засідань) або перевіряється довгастий вантаж, оператор може задіяти спрямовану антену **MWA-6** на нижчих частотах. Для цього частотну межу **AUX1 (INPUT2)** штучно занижують (мінімально до **800 МГц**). Це дозволить спрямованій антені «прострілювати» приміщення на більшу відстань у конкретному напрямку, фіксуючи мобільні стандарти або цифрові закладні пристрої.

4. Калібрування порогів та тестування ефіру

- **Тестова генерація сигналів:** Для встановлення реальної межі чутності комплексу проведіть натурний експеримент. Для цього використовуйте кілька тестових мобільних телефонів, що підключені до мереж різних стільникових операторів.
- **Імітація загрози мобільного зв'язку:** Розмістіть телефон із **вимкненим Wi-Fi** у найвіддаленішій точці кімнати або за природною перешкодою (наприклад, у шафі чи під столом) та послідовно ініціюйте:
    - Голосовий дзвінок — для тестування тривалого безперервного випромінювання та фіксації службових імпульсів керування.
    - Активну передачу даних (запуск утиліти Speedtest, завантаження важкого файлу або відеодзвінок у месенджерах WhatsApp/Telegram) — для тестування високошвидкісних пакетних режимів LTE.
- **Загальне коригування лінійного порогу:** Запустіть режим «Мобільні/GPS-трекери». Переконайтеся, що на панелі **«Рівень»** амплітуда цих тестових сигналів упевнено перетинає встановлену лінію порогу. Якщо система не фіксує сплески — опустіть лінію порогу нижче. Якщо лінія порогу постійно підсвічується червоним від фонового шуму приміщення — дещо підніміть її.
- **Калібрування порогу Wi-Fi:** Запустіть режим **«Бездротові/ISM».** Увімкніть Wi-Fi на тестовому телефоні та підключіть його до локальної точки доступу. Запустіть активне скачування даних (Speedtest) або відеодзвінок (WhatsApp/Telegram) — це дозволить оцінити рівень сигналу безпосередньо на панелі **«Wi-Fi»** та коректно виставити поріг для бездротових мереж.
- **Калібрування порогу BLE:** Увімкніть Bluetooth на телефоні, переконавшись, що в цей момент він **не з'єднаний** із жодним периферійним пристроєм (навушниками, смарт-годинником тощо). Телефон почне випромінювати рекламні пакети (Advertising), що дозволить точно відкалібрувати поріг виявлення на панелі **«BLE»** для нез'єднаних пристроїв.

5. Глибоке спектральне маскування фону

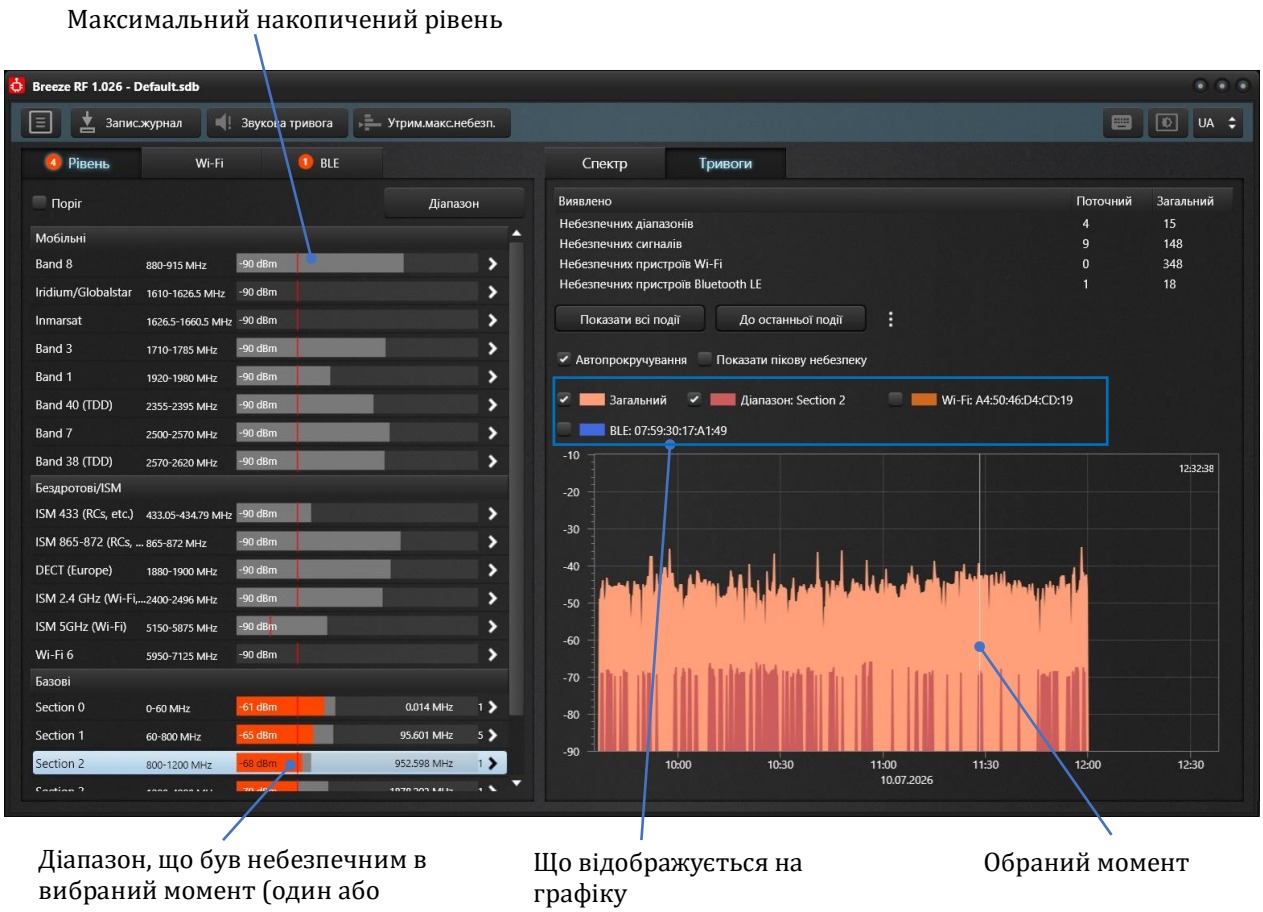
Маскування фону — це створення цифрового «зліпка» легального ефіру вашої локації.

- **Часовий регламент:** Для довгострокового моніторингу звичайне 5-хвилинне маскування не підходить. Задайте триваліший час накопичення спектра (**20 хвилин**)
- **Просторова тактика:** Проведіть маскування у кількох точках **навколо** цільового кабінету (коридор, сусідні кімнати поверхні вище/нижче, вулиця). Це сформує чітку картину зовнішнього фону.
- **Головне застереження:** У жодному разі не проводьте маскування всередині цільового приміщення, якщо є підозра, що закладний пристрій уже активний — інакше комплекс внесе сигнал «жучка» до білого списку (замаскує його), і ви його ніколи не знайдете.

6. Старт сеансу та верифікація запису

- **Перевірка дискового простору:** Переконайтеся, що на жорсткому диску ПК є достатньо вільного місця. За добу безперервного запису бази даних журналу Breeze RF можуть розростатися до значних розмірів (залежно від кількості та активності сигналів та пристроїв).
- **Активація фіксації подій:** Фізично розгорніть комплекс, підключіть усі інтерфейси та запустіть обраний режим пошуку (наприклад, **«Всі сигнали»** або комбінацію **«Мобільні/GPS-трекери» + «Бездротові/ISM»**).
- **Контроль працездатності:** Обов'язково перевірте, чи активована функція **«Запис журналу»** або **«Автоматичний запис журналу»** (індикатор кнопки має бути у втопленому/натиснутому стані, якщо автоматичний режим не активний. У разі активного автоматичного режиму кнопка «Запис журнал» приховується. Зробіть короткий тестовий дзвінок поруч із комплексом, щоб переконатися, що подія успішно записалася в таймлайн журналу. Після цього залиште комплекс працювати автономно.

Аналіз результатів спектрального моніторингу



Здійснюйте аналіз результатів в режимі «Стоп».

Вибір дати: У меню **«Файл журналу»** оберіть потрібну дату.

Аналіз результатів по діапазонам:

- Шкали на панелі **«Рівень»** будуть відображати максимальний накопичений рівень. Цей рівень інформує про наявність чи відсутність сигналів всередині діапазону за період перевірки. Високий рівень з перевищенням порогу означає наявність небезпеки в діапазоні
- Оберіть перший небезпечний діапазон на панелі **«Рівень»**, а потім на панелі **«Тривоги»** активуйте його відображення (встановіть маркер **«Діапазон: _____»**). Після цього на графіку тривог відобразиться рівень небезпеки суто за цим діапазоном, який підсвітиться яскраво-червоним кольором. Аналізуючи ізольований графік тривог окремого діапазону, ви зможете визначити, в який проміжок часу існував сигнал, наскільки високою була його амплітуда та як довго тривала передача даних. Під час перегляду даних на графіку користуйтесь масштабуванням та перемоткою, щоб переглядати весь період від початку до кінця.
- Перегляньте всі небезпечні діапазони по черзі

Аналіз результатів за допомогою графіка:

- Графік **«Загальний»** на панелі **«Тривоги»** (світло-червоний) відображує сукупний рівень небезпеки по всім діапазонам одночасно. Якщо клікнути мишкою на графіку, обравши момент з високим рівнем небезпеки, шкали на панелі **«Рівень»** відобразять рівень діапазонів, який вони мали в обраний момент. Як і під час реального пошуку, поруч зі шкалою відображатиметься кількість небезпечних сигналів та частота найнебезпечнішого з них.
- Переглядайте всі небезпечні діапазони по черзі, користуючись відображенням історії окремого діапазону на графіку («Вибраний діапазон»). Аналізуйте силу сигналу, час існування
- По черзі перевірте всі моменти з високим рівнем небезпеки на графіку тривог з переглядом всіх небезпечних діапазонів

Аналіз спектрограми (Водоспаду): Панель **«Спектр»** відображає записані траси спектра у вигляді 2D-растра («водоспаду»). Якщо двічі клікнути на діапазоні або сигналі на панелі **«Рівень»** у режимі **«Стоп»**, спектральний графік та водоспад автоматично налаштуються на відповідну смугу частот.

- Клікнувши на будь-яку подію на графіку тривог, оператор може автоматично прокрутити водоспад до моменту її виникнення. Це дозволяє детально вивчити структуру сигналу в обраний час.
- Ручне прокручування водоспаду здійснюється за допомогою вертикальної смуги прокручування, яка з’являється після кліку на полі графіка.
- Для перегляду миттєвого зрізу траси на графіку спектра досить клікнути на відповідну часову точку на водоспаді в режимі зупинки. Зелена траса відображатиме точний стан спектра, який існував саме в ту секунду.

Деталізація сигналів усередині діапазону: Ви можете увійти всередину обраного діапазону (дослідити діапазон) на панелі **«Рівень»**. Програма виведе список усіх сигналів, які існували в його межах. Сигнали, що становили небезпеку в обраний момент часу, матимуть червону шкалу рівня. Якщо вибрати такий сигнал і активувати маркер **«Сигнал: _____»** на панелі **«Тривоги»**, ви отримаєте ізольований графік тривог за цим конкретним сигналом для оцінки його потужності та тривалості роботи.

Тактичні рекомендації щодо локалізації прихованих загроз:
У разі виявлення підозрілого сигналу, який періодично з’являється у приміщенні, має стабільно високий рівень амплітуди та значну тривалість роботи, необхідно встановити точку його випромінювання:

- **Покімнатний моніторинг:** Досліджуйте об'єкт послідовно, залишаючи комплекс на добу в кожній кімнаті для накопичення чистої статистики та подальшого порівняння результатів.
- **Верифікація зовнішнього фону:** Переконайтеся, що сигнал не є хибним спрацюванням від зовнішнього джерела. Для цього виконайте контрольне вимірювання за межами цільового приміщення (на вулиці або в коридорі) — рівень локального «жучка» всередині будівлі має бути суттєво вищим, ніж ззовні.
- **Фокусування на частоті:** Ви можете залишити систему в режимі узгодженого дослідження конкретного підозрілого діапазону (наприклад «ISM 2.4 GHz». Це значно підвищить швидкість сканування та ймовірність повної реєстрації швидких або імпульсних подій у ньому.
- **Прогнозування та пошук:** Визначте кімнату, де зафіксовано максимальний рівень сигналу, та на основі графіка журналу спробуйте спрогнозувати точний час

наступного увімкнення передавача. Плануйте проведення фізичної локалізації («полювання») саме на цей прогнозований часовий проміжок.

Аналіз результатів моніторингу Wi-Fi

Після завершення пошуку на панелі «Wi-Fi» відобразиться список пристроїв та їхній максимальний накопичений рівень сигналу. Верифіковані точки доступу та клієнти матимуть індивідуальний поріг, який відрізняється від загального. Оператор повинен детально вивчити всі «підозрілі» пристрої, що з'явилися під час моніторингу. Критеріями «підозрілості» є перевищення встановленого порогу та високі показники лічильника кадрів, які свідчать про суттєву активність пристрою.

Примітка: Wi-Fi станції (клієнти), як-от мобільні телефони, постійно сканують ефір на наявність доступних точок доступу. Якщо такий пристрій просто «одноразово проходить» через зону сканування, система може зареєструвати його випромінювання, проте він відобразиться у списку з низьким значенням лічильника кадрів.

Оберіть перший «підозрілий» пристрій та перейдіть до його аналізу:

- Якщо пристрій досі активний, насамперед виконайте його **локалізацію**
- Вивчіть історію активності пристрою на вкладці **«Канали»**: лічильники кадрів, а також часові відмітки першого та останнього виявлення дозволяють оцінити, як довго працював цей пристрій та які обсяги даних він міг передати.
- Увімкніть відображення історії для обраного пристрою на панелі **«Тривоги»**. Під час перегляду даних на графіку використовуйте масштабування та прокручування (перемотку), щоб детально вивчити весь період активності від початку до кінця.

Вивчіть зв'язки «підозрілого» пристрою на вкладці **«Взаємодіючі пристрої»**. Виконуйте аналіз з огляду на тип об'єкта (точка доступу, нез'єднаний клієнт, з'єднаний клієнт).

За результатами дослідження присвоюйте пристрою текстовий коментар, який вказуватиме на ваші подальші дії. Наприклад:

! — дуже підозрілий, потребує постійного моніторингу;
? — потребує додаткового вивчення
ОК — безпечний/легітимний пристрій тощо.

Почергово перевірте всі виявлені небезпечні пристрої.

Додатковий моніторинг: Повторіть процедуру пошуку, якщо необхідно додатково зафіксувати та вивчити ті підозрілі пристрої, які виявилися неактивними на момент перегляду поточних результатів.

Аналіз результатів моніторингу BLE

Після завершення пошуку на панелі «BLE» відобразиться список пристроїв та їхній максимальний накопичений рівень сигналу. Зважаючи на постійну динамічну зміну ідентифікаторів BLE-пристроями та неможливість їхньої довгострокової прив'язки до конкретної MAC-адреси, раціонально аналізувати не кожну нову адресу окремо, а зміну загальної кількості та типів пристроїв у приміщенні (тобто фіксувати сталий патерн радіообстановки).

Для перегляду загального патерну скористайтеся графіком на панелі **«Тривоги»**:

- **Аналіз часових зрізів:** Клік на обраний час на графіку встановлює шкали пристроїв на той рівень, який вони мали в цей конкретний момент. Це дозволяє виявити пристрої, що були активними в обраний час (вони матимуть червону шкалу), та порахувати їхню кількість.
- **Додаткова ідентифікація:** Такі атрибути, як «Виробник» та «Деталі», залишаються сталими, тому їх можна використовувати для більш детальної ідентифікації пристроїв.
- **Порівняльний аналіз:** Клік на іншу часову точку показує пристрої, які були активними в цей новий проміжок часу.

Приклад аналітичної таблиці: Завдяки зіставленню даних у різні проміжки часу можна наочно виявити аномалії (наприклад, появу нових міток або різке зростання рівня сигналу):

Час	**Виробник**	**Тип**	**Деталі**	**Кількість**	**Макс.рівень**
10:00	Apple	мітка	AirTag/FindMy	3	-62
	Microsoft			5	-55
	Samsung			1	-65
10:30	Apple	мітка	AirTag/FindMy	5	-45 !аномалія
	Microsoft			5	-56
	Samsung			1	-66
…					

Порівняння з реальною обстановкою: Патерн приміщення завжди безпосередньо пов’язаний із фізичною обстановкою на об’єкті. Приклади типових сценаріїв:

- **Прибуття керівника/співробітників до кабінету:** Характеризується прогнозованим збільшенням кількості пристроїв (наприклад, додаються смартфон, смарт-годинник, бездротові навушники).
- **Завершення робочого дня або вихід із кабінету:** Характеризується зменшенням кількості активних BLE-пристроїв.

Важливо: Будь-яке стійке відхилення від зафіксованого раніше патерну (особливо поява нових невідомих пристроїв із високим рівнем сигналу за відсутності людей у кімнаті) є приводом для проведення ретельного фізичного пошуку та локалізації джерела.

Виявлення автомобільних GPS-трекерів (маяків)

Принцип роботи трекерів

За архітектурою та логікою передачі даних автомобільні GPS-трекери поділяють на три типи:

1. **Автономні реєстратори (логгери):** Накопичують координати у внутрішню пам'ять і взагалі не випромінюють радіосигналу. (Виявляються суто візуальним або магнітометричним оглядом).
2. **Запитові (непостійні) маяки:** Накопичують координати, але виходять у ефір лише за запитом оператора, по розкладу або у разі спрацювання якогось датчика
3. **Онлайн-трекери:** Регулярно або безперервно передають навігаційні дані на сервер моніторингу під час руху автомобіля.

4. **BLE-Tags/Мітки (нова технологія):** використовують навколишні телефони для трансляції свого ID та локації на сервер Apple, Google або Samsung.

Стандартний мобільний трекер (тип 2 та 3) — це пристрій, що поєднує в одному корпусі супутниковий **GNSS-приймач** (GPS/ГЛОНАСС/Galileo), модуль обробки й накопичення інформації (мікроконтролер), а також модуль мобільного зв'язку із SIM-карткою або eSIM. Алгоритм його роботи:

- Отримання поточних координат від супутникового угруповання.
- Запис та формування маршруту (треку) в буфері пам'яті.
- Передача пакетів даних на сервер через стільникову мережу.

Особливість: В окремих випадках, для контролю транспорту в зонах без покриття стільникових мереж (морські шляхи, пустелі, кар'єри, незаселені регіони) або для маскування, замість мобільних модулів використовуються термінали супутникового зв'язку **Iridium**, **Globalstar** або **Inmarsat**.

Методика виявлення

Щоб гарантовано зафіксувати сигнали від мобільних або супутникових модулів трекера, комплекс **Delta S / Delta X** має переміщуватися безпосередньо всередині транспортного засобу (ТЗ), який перебуває в русі та виконує маневри.

Важливо: Якщо тривалість перевірки перевищуватиме 1 годину, забезпечте стабільне живлення керуючого ноутбука та комплексу через автомобільний інвертор (12 В → 220 В) або потужний Power bank із підтримкою Power Delivery.

1. **Вибір локації для тесту:** Перевірку рекомендується проводити на місцевості з мінімальним рівнем радіочастотного шуму. Міське середовище критично насичене сигналами сотень сторонніх смартфонів та базових станцій, що унеможливлює правильну інтерпретацію результатів. Виїжджайте на порожню ділянку дороги в сільській місцевості — якомога далі від великих населених пунктів та іншого транспорту.
2. **Радіомовчання в салоні:** Повністю вимкніть усі санкціоновані радіочастотні пристрої в салоні: мобільні телефони (переведіть в авіарежим або вимкніть), бездротові гарнітури, смарт-годинники, ноутбуки та штатні точки доступу автомобіля. Деактивуйте інтегровані бездротові модулі ТЗ (**Wi-Fi**, **Bluetooth**, **CarPlay/Android Auto**).
3. **Розміщення комплексу:** Розмістіть пошукову систему всередині салону автомобіля (бажано ближче до центру для рівномірного зняття показників).
4. **Конфігурація антенного тракту:**
    - **Для комплексів Delta S:** Якщо необхідно забезпечити кругову (всеспрямовану) діаграму спрямованості, підключіть до входу **INPUT 1** антену ODA-4. Якщо перевіряється довгий або великогабаритний ТЗ (вантажівка, фура, тягач із причепом), використовуйте спрямовану антену MWA-6 на вході **INPUT 1** для формування подовженої зони чутливості. Вхід **INPUT 2** завжди працює в парі з ВЧ-антеною LPDA-12.
    - **Для комплексів Delta X:** Якщо потрібна розширена діаграма виявлення (наприклад, під час перевірки фури або автобуса), переналаштуйте розподіл частот антенного перемикача, призначивши антену MWA-6 для нижчих діапазонів. Для цього перейдіть: Налаштування → Пристрій → Налаштування → Частота AUX1 (INPUT2). Встановіть поріг частоти AUX1

(INPUT2) на значення **800 МГц**. Це гарантує використання спрямованої антени MWA-6, починаючи вже з частоти 800 МГц і вище.

5. **Ініціалізація бази даних:** Створіть новий файл журналу.
6. **Вибір режиму:** Активуйте цільовий пошуковий режим **«Мобільні/GPS-трекери»** та увімкніть **сканування пристроїв BLE**
7. **Пороги:** Встановіть індивідуальні рівні порогів для діапазонів або скиньте їх до базових значень за замовчуванням (дефолтних).
8. **Активація реєстратора:** Увімкніть запис даних, натиснувши кнопку **«Запис журналу»** (кнопка має залишатися в натиснутому стані), якщо не вибраний автоматичний запис
9. **Динамічний тест:** Запустіть двигун автомобіля та починайте рух. Оскільки багато засобів стеження програмуються на передачу даних за подіями (старт двигуна, зупинка, початок руху, поворот на кут понад **15°**), рухайтеся не менше ніж **30–40 хвилин**. Періодично змінюйте траєкторію, зупиняйтеся на узбіччі, глушіть та знову заводьте двигун. Безперервно стежте за графіком історії тривог, шкалами діапазонів на панелі «Рівень», шкалами на панелі «BLE» та звуковими сповіщеннями.
10. **Аналіз пакетних сигналів:** У режимі **«Мобільні/GPS-трекери»** комплекс сканує всі мобільні стандарти (2G/3G/4G/5G) та виводить інтегральний рівень небезпеки на графік тривог. Робота автомобільних трекерів характеризується дуже короткими, але потужними сплесками випромінювання (імпульсна пакетна передача). Графік історії дозволяє візуально зафіксувати ці короткочасні сигнали та вирахувати їхню циклічність.
11. **Кореляційний аналіз подій:** У разі виявлення підозрілого імпульсного сигналу спробуйте встановити чіткий зв’язок між його появою та фізичною поведінкою автомобіля. Перевірте, чи виникає сплеск чітко через 1 хвилину після старту двигуна, чи посилюється він під час набору швидкості чи зміни курсу ТЗ.
12. **Локалізація джерела:** Якщо підозрілий сигнал з'являється регулярно, переходьте до його безпосередньої локалізації. Повільно переміщуйте антенну систему всередині салону, підносьте її до торпеди, під сидіння, до блоків запобіжників та порогів. Зміна амплітуди на шкалі рівня дозволить точно визначити приховане місце монтажу трекера. Пам'ятайте, що рідкісні періодичні сигнали (наприклад, вихід в ефір раз на годину) потребують тривалішого спостереження.
13. **Аналіз BLE:** перевіряйте результати сканування пристроїв на панелі «BLE». У разі виявлення пристрою з високим рівнем, здійснюйте його фізичну локалізацію.

Виявлення РЧ глушників та радіочастотних аномалій

Правовий статус та ризики (за матеріалами FCC США)

На офіційному ресурсі Федеральної комісії зі зв’язку США (FCC) зазначається:
«Федеральний закон суворо забороняє експлуатацію, маркетинг, рекламу або продаж будь-якого типу обладнання для постановки завад (глушників), що навмисно створює перешкоди авторизованому радіозв’язку, зокрема стільниковому, персональному (PCS), супутниковому (GPS) зв'язку та роботі поліцейських радарів.
Пристрої радіопридушення (джамери) блокують можливість здійснення екстрених викликів на номери 9-1-1, створюють критичні ризики для каналів громадської безпеки та перешкоджають повсякденним формам комунікації.
Використання телефонних глушників, блокувальників GPS чи інших засобів пригнічення сигналів є правопорушенням. Жодних винятків для комерційного сектора,

приватного бізнесу, навчальних закладів, житлових зон чи транспортних засобів не передбачено. Місцеві правоохоронні органи не мають автономних повноважень на застосування таких засобів; у виняткових випадках це дозволено виключно окремим федеральним структурам відповідно до спеціальних нормативних актів».

Попри суворі заборони, нелегальні РЧ-глушники активно використовуються зловмисниками. Глушники стільникових мереж (GSM/3G/4G/5G) застосовуються для нейтралізації систем охоронної сигналізації під час проникнення на об'єкти або для викрадення автотранспорту. Портативними блокувальниками GPS/GNSS часто користуються водії, які прагнуть приховати маршрут руху від систем корпоративного трекінгу, а також автокрадії для придушення пошукових супутникових маяків.

Побутове використання джамерів створює серйозні проблеми для навколишньої інфраструктури: призводить до повної втрати або критичного погіршення якості мобільного зв’язку, падіння швидкості бездротового Інтернету, блокування навігації або генерації хибних GPS-координат.

Комплекси Delta S / Delta X під керуванням ПЗ Breeze RF є ефективним інструментом для детектування, ідентифікації та точної локалізації джерел таких радіочастотних завад і аномалій.

Фізика процесу глушіння

Глушники стільникового зв’язку спрямовують заваду на частотні діапазони Downlink (низхідної лінії зв’язку), тобто туди, де здійснюється передача даних від базової станції (БС) на мобільний термінал користувача. За наявності потужного стороннього шуму в цих смугах смартфон втрачає здатність детектувати сигнали БС і переходить у стан «Поза мережею».
Так звані «GPS-джамери» генерують загороджувальну чи прицільну заваду безпосередньо на частотах супутникових навігаційних систем, маскуючи слабкі сигнали з орбіти та перешкоджаючи приймачам отримати інформацію, необхідну для розрахунку координат.
Таким чином, для виявлення джерела перешкод система має безперервно контролювати діапазони Downlink мобільного зв’язку та частоти глобальних навігаційних супутникових систем (GPS, ГЛОНАСС, GALILEO, BeiDou). Фіксація аномального підняття рівня шумової полиці (Noise Floor) є прямим індикатором роботи глушника неподалік комплексу.

Покроковий алгоритм налаштування системи в ПЗ Breeze RF

Активація Downlink- та GNSS-діапазонів:
Програмне забезпечення Breeze RF постачається із вбудованою базою даних, яка містить актуальні частотні плани для більшості країн світу. За замовчуванням діапазони Downlink (від базової станції до телефона) та GNSS приховані зі стандартного списку, щоб не перевантажувати інтерфейс під час класичного пошуку закладних пристроїв.

- Щоб активувати їх, перейдіть: **Налаштування → Діапазони | Країна**.
- Встановіть прапорці (галочки) напроти пунктів **Низхідні** та **GNSS/Навігація**, після чого натисніть **«Застосувати»**.
- Після оновлення сітки частот у головному вікні програми стане видимим та активним цільовий режим **«Низхідні/Навігація»**.

Маскування фону та виявлення аномалій:
Перед початком пошуку рекомендується провести процедуру маскування ефіру у віддаленому, завідомо чистому від локальних завад місці. Результати цього маскування будуть експоновані на Downlink- та GNSS-діапазони. Це дозволить:

- **Уникнути хибних тривог:** Легальні потужні сигнали від розташованих поруч базових станцій чи супутників будуть внесені до «білого списку» і не викликатимуть постійного спрацювання системи.
- **Виявити РЧ-аномалії:** Комплекс миттєво зафіксує будь-які деструктивні зміни у спектрі. Аномалії можуть виникати як внаслідок технічних робіт провайдера, так і через несанкціоноване вторгнення в мережу за допомогою спецобладнання (радіоперехоплення, супутниковий спуфінг, робота фейкових базових станцій або **IMSI-catcher**).

Увімкнення виявлення:
Перейдіть у меню **Налаштування** → **Інші** та активуйте опцію **«Виявляти РЧ глушники»**. На головній панелі інструментів обов'язково увімкніть функцію **«Звукова тривога»**.

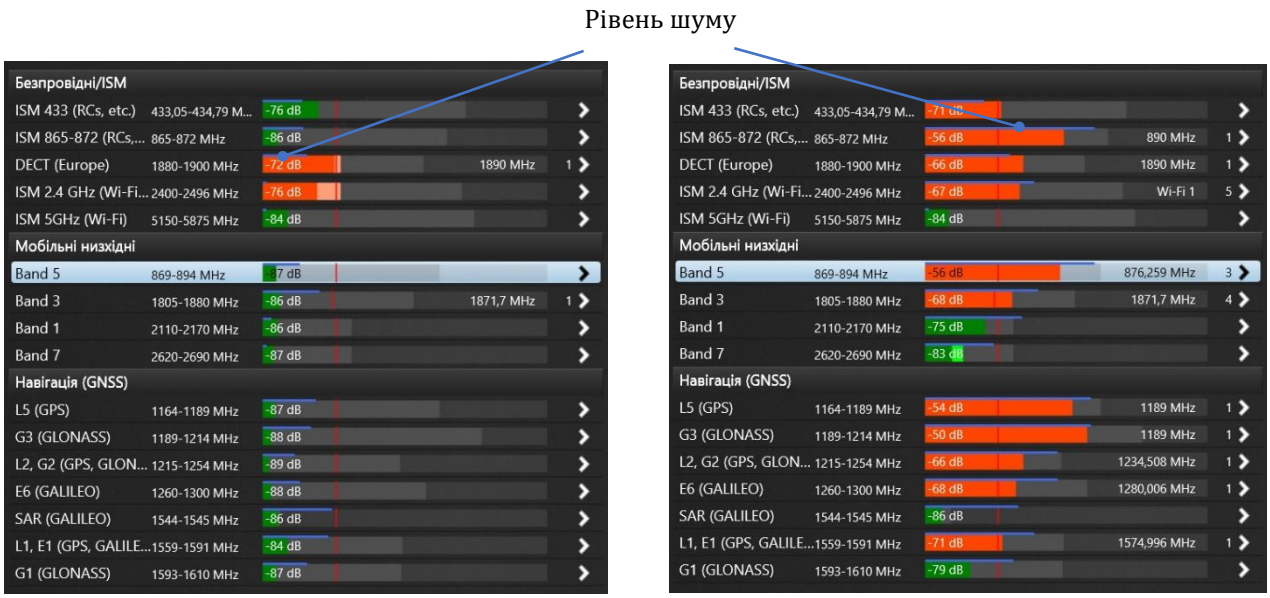
Вибір тактики сканування:

- Запустіть режим **«Низхідні/Навігація»**.
- Для максимального охоплення паралельно активуйте режим **«Мобільні/GPS-трекери»** — це дозволить сканувати специфічні мобільні діапазони, які не мають класичного розділення на Uplink/Downlink (наприклад, TDD-діапазони мереж 4G/5G, де прийом і передача відбуваються на одній частоті з розділенням у часі).
- Щоб виявляти глушники локальних мереж **Wi-Fi**, додатково увімкніть режим **«Wireless/ISM»**.
- Альтернатива: Можна запустити універсальний режим **«Всі сигнали»** — швидкість повного циклу сканування дещо знизиться, проте система аналізуватиме абсолютно всі частотні категорії одночасно.

Індикація та звукове сповіщення:
Коли алгоритм **«Виявляти РЧ глушники»** активний, на панелі **«Рівень»** поруч із кожним частотним діапазоном з'являється додатковий **синій вертикальний індикатор**. Він відображає поточний рівень інтегрального шуму (Noise Floor).

- За відсутності активних завад рівень шуму залишається стабільно низьким (зазвичай менше ніж **-70 дБм**), незалежно від амплітуди корисного сигналу базових станцій.
- У разі ввімкнення глушника синій стовпчик починає стрімко зростати. Щойно рівень шуму перетне встановлену лінію порогу, система ініціює спеціальний переривчастий звуковий сигнал тривоги (**«писк»**), сигналізуючи про присутність активного джерела РЧ-завад у ближній зоні.

Нижче наведено приклад виявлення багато-діапазонного глушника:



Без глушника

З працюючим глушником

Регулювання дальності перевірки: За допомогою коригування порогу оператор може гнучко керувати чутливістю системи та, відповідно, радіусом (дальністю) виявлення джерел випромінювання.

Локалізація РЧ-глушника (Пеленгація): У разі детектування сигналу завади оператор може встановити точне місце розташування передавача (глушника), орієнтуючись на синю шкалу інтегрального шуму та інтенсивність звукової сигналізації.

- **Методика пошуку:** Скануйте приміщення чи територію за стандартною тактикою «зигзага», як і під час пошуку класичних закладних пристроїв. У міру наближення антени до джерела завади синій стовпчик рівня шуму зростатиме, а інтервальний звуковий сигнал («писк») ставатиме частішим та інтенсивнішим.
- **Робота з атенюатором:** Якщо синій індикатор шуму заповнює шкалу більш ніж на **2/3** (відбувається насичення тракту), увійдіть у режим дослідження цього діапазону та увімкніть функцію **атенюатора**. Ослаблення сигналу знизить загальну чутливість комплексу, що дозволить звузити коло пошуку та підійти до джерела впритул.
- **Захист обладнання:** Зупиніть наближення до джерела випромінювання, якщо синій стовпчик рівня залишається критично високим навіть за умови активованого атенюатора. Надмірна потужність радіосигналу на ближній відстані є небезпечною і може спричинити апаратне пошкодження або вихід з ладу чутливих вхідних каскадів приймача комплексу.

Обробка та локалізація спектральних аномалій: Радіочастотні аномалії (різкі нетипові зміни у спектрі Downlink- та GNSS-діапазонів) викликатимуть стандартні сигнали тривоги, аналогічні до сигналів звичайних закладних пристроїв.

- **Індикація:** У разі перевищення встановленого порогу зелена шкала амплітуди почне стрімко зростати та змінить свій колір на червоний, а з динаміків (навушників) лунатиме стандартний акустичний сигнал сповіщення (клацання).
- **Аналіз та пошук:** Усі аномальні сигнали автоматично заносяться до робочого списку системи з можливістю їхнього подальшого детального аналізу в

режимі дослідження діапазону. Для визначення точного розташування джерела аномального сигналу виконайте стандартну процедуру локалізації методом оцінки максимального рівня амплітуди.

Багатофункціональний зонд (Delta X)

Дротові, оптичні та низькочастотні канали витоку інформації
Передача інформації через дротові лінії вважається одним із найбільш прихованих методів зняття інформації, оскільки в цьому разі відсутнє об'ємне радіовипромінювання, яке можна зафіксувати стандартними антенами. Практично будь-яка дротова лінія, що виходить із цільового приміщення або проходить крізь нього транзитом, може бути використана зловмисниками як провідний канал витоку. Провідна закладна система зазвичай складається з двох компонентів:

- **Передавач (мікрофон з модулятором):** Розташовується всередині цільової зони та підключається до обраної лінії. Він вловлює акустичні коливання в приміщенні, перетворює їх на високочастотний сигнал (для маскування під заваду) і транслює в лінію.
- **Приймач:** Підключається до цієї ж провідної лінії, але за межами контрольованої зони (у підвалі, на технічному поверсі або в розподільчій шафі). Він приймає ВЧ-сигнал з дроту, демонтує його та передає аудіопотік на диктофон або пост моніторингу.

Трансляція сигналу може здійснюватися через будь-які типи комунікацій (лінії охоронно-пожежної сигналізації, телефонні кабелі, проводи заземлення, радіоточки) без порушення їхньої основної функціональності.

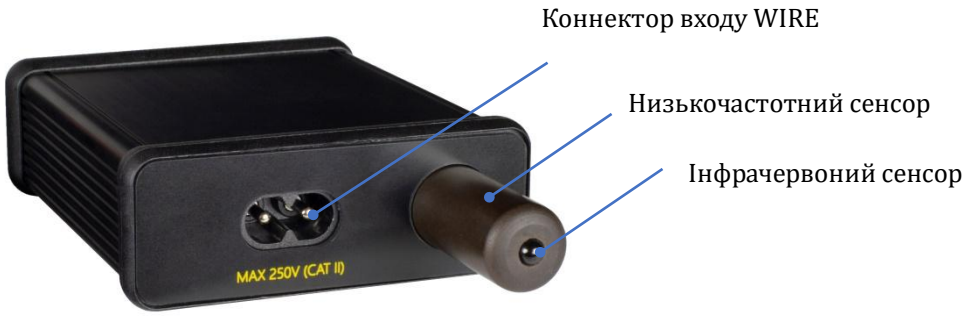
Використання побутових технологій (PLC / HomePlug)
Окрім спеціальних засобів, призначених для негласного зняття інформації, необхідно враховувати ризики використання цивільних побутових технологій у зловмисних цілях. Своєрідним прикладом є побудова комп'ютерних мереж через силову електромережу — **PLC (Power Line Communication)**.
Досить прихований провідний пристрій зняття інформації може бути зібраний зі звичайної компактної IP-відеокамери з мікрофоном та бюджетного адаптера «Ethernet через мережу 220 В». Цифровий потік (аудіо та відео) передаватиметься силовими проводами за межі кабінету і прийматиметься другим адаптером. Сучасні стандарти **HomePlug AV / AV2** забезпечують швидкість передачі даних до 500 Мбіт/с і займають широкий частотний діапазон 2–86 МГц.

Оптичний (ІЧ) та низькочастотний канали

- **Інфрачервоне випромінювання:** ІЧ-промені невидимі для неозброєного ока та здатні поширюватися на значні відстані в межах прямої видимості. Вони активно використовуються в оптичних каналах витоку для бездротової, але спрямованої передачі аудіоінформації через вікна приміщень.
- **Побічні електромагнітні випромінювання (ПЕМВІ):** Електронні компоненти багатьох закладних пристроїв (особливо блоки живлення від мережі 220 В, плати цифрових відеокамер тощо) під час роботи випромінюють специфічні низькочастотні електромагнітні хвилі, які можна зафіксувати в ближній зоні.

Пошуковий комплекс **Delta X** дозволяє оперативно виявляти, аналізувати та локалізувати всі зазначені типи прихованих загроз за допомогою

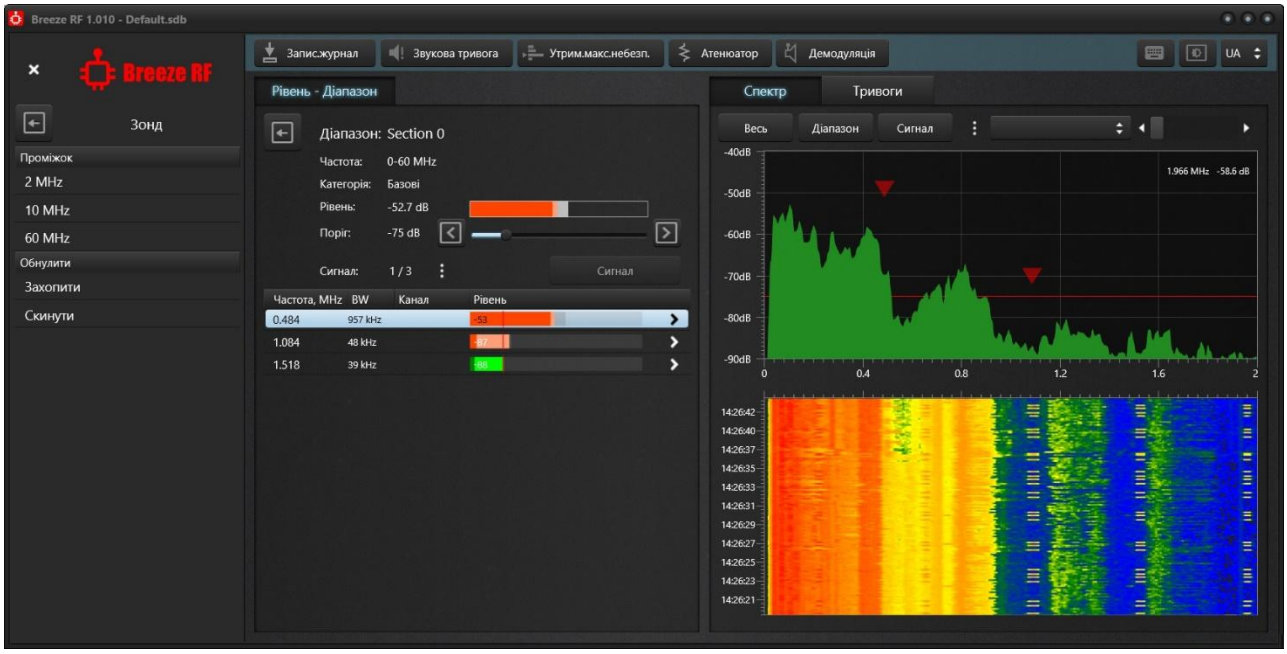
Багатофункціонального Зонда, який входить до базового комплекту постачання системи.



Багатофункціональний Зонд має 3 спеціалізовані входи (канали детектування), кожен з яких оптимізований під конкретну фізичну загрозу:

Вхід (Режим)	**Що виявляється (Об'єкти пошуку)**
IR	Приховані інфрачервоні (оптичні) передавачі нелегальних аудіо- та відеоканалів.
LF	Побічні низькочастотні електромагнітні випромінювання (ПЕМВІ) від внутрішніх плат «жучків», об'єктивів прихованих камер та блоків живлення.
WIRE	Закладні пристрої та високочастотні сигнали (зокрема HomePlug/PLC), що транслюють інформацію через провідні лінії: • Електромережу 220 В • Комп'ютерні кабелі Ethernet • Телефонні лінії • Кабелі охоронно-пожежної сигналізації • Інші низьковольтні та слабкострумові комунікації

Щоб ініціювати сеанс сканування провідних та оптичних каналів, натисніть кнопку **«Зонд»** у головному меню програми. Інтерфейс програмного забезпечення **Breeze RF** у режимі **«Зонд»** має такий вигляд:



Панель **«Рівень»** буде автоматично переведено в режим дослідження базового низькочастотного діапазону **«Section 0»**.

Оператор може оперативно обирати одну з трьох смуг огляду:

- **2 МГц:** рекомендовано для оптичного (**IR**) та низькочастотного (**LF**) входів;
- **10 МГц:** базовий режим, рекомендований для дротового входу (**WIRE**);
- **60 МГц:** розширений режим для входу **WIRE**, коли необхідно детально перевірити лінію у максимально широкому частотному діапазоні.

Функція **«Обнулити – Захопити»** призначена для фіксації та збереження поточної опорної траси спектра (референсного зліпка) з метою її подальшого віднімання (диференційного методу).

Функція **«Атенюатор»** використовується для штучного послаблення вхідного рівня, якщо в лінії виявлено надто потужний сигнал, що перевантажує тракт приймача.

Аналогічно до інших режимів роботи програми, подвійний клік на рядку сигналу в таблиці автоматично масштабує межі спектрального графіка для повного й детального відображення структури цього сигналу. Одне клацання миші просто виділяє сигнал у списку без зміни поточного масштабу графіка.

Функція **«Постійність»**, коли вона активна, дозволяє оператору наочно розрізняти безперервні (стаціонарні) сигнальні структури та непостійні (імпульсні, пакетні) сплески на екрані.

Моніторинг інфрачервоного спектра (IR)

Оскільки інфрачервоні промені мають чітко спрямований характер, оптична закладна система потенційно буде орієнтована безпосередньо у бік зовнішнього пункту прийому сигналу. Найімовірнішим вектором трансляції є зона біля вікон будівлі або віддалені кути кімнати з прямою видимістю на протилежні споруди.

Пошук необхідно здійснювати всередині кабінету, приділяючи особливу увагу зоні вікон. Під час сканування фотоприймач зонда має бути спрямований усередину приміщення, на віконні рами, укоси та область навколо них. Дальність детектування інфрачервоним оптичним датчиком залежить від потужності шпигунського передавача і зазвичай становить **1–5 метрів** за умови точного наведення на вісь променя.

Покроковий алгоритм проведення перевірки

1. **Підключення обладнання:** Підключіть Багатофункціональний Зонд до високочастотного гнізда **«PROBE»** на корпусі основного блока системи за допомогою коаксіального кабелю з комплекту постачання.
2. **Комутація датчика:** Перемкніть механічний селектор на самому зонді в положення **«IR»**.
3. **Ініціалізація ПЗ:** Оберіть режим **«Зонд»** у головному меню програми Breeze RF.
4. **Зачистка таблиці:** Очистіть поточний список сигналів. Для цього виконайте команду «Видалити всі сигнали в межах діапазону» в контекстному меню панелі **«Рівень»**.
5. **Акустична активація:** Створіть у приміщенні постійне джерело звуку (наприклад, увімкніть радіо, генератор шуму або тестовий аудіозапис), щоб змусити потенційні заклади з голосовою активацією (VOX) або амплітудні модулятори вийти в режим активної передачі.
6. **Сканування ліній:** Спрямуйте зонд на місця ймовірної інсталяції та вектори зняття інформації (проскануйте простір біля вікон, рухаючись уздовж рам та укосів у напрямку ззовні-всередину кабінету).
7. **Автоматична фіксація:** Якщо система виявить модульоване ІЧ-випромінювання, параметри цих сигналів будуть автоматично занесені до робочої таблиці.
8. **Пеленгація та локалізація джерела:** У разі появи сигналу тривоги плавно повертайте зонд у різних площинах, щоб зафіксувати максимальний рівень амплітуди. Пікове значення шкали означатиме, що оптична вісь зонда збіглася з променем передавача.
    - Повільно переміщуйте зонд ближче до передбачуваного джерела, контролюючи динаміку сигналу. Орієнтуйтеся на функцію **«Звукова тривога»**, яка під час наближення змінюватиме частоту й тональність звуку на інтенсивнішу.
    - У точці, де зафіксовано найвищий рівень небезпеки, зупиніть сканування та проведіть ретельний фізичний (візуальний) огляд конструкцій.
    - Якщо чітко вираженого локального джерела (фокуса) знайти не вдається, а стабільна загроза низького або середнього рівня фіксується по всій площі кімнати, це свідчить про наявність фонових завад від цивільних джерел штучного освітлення (наприклад, люмінесцентних ламп, плазмових панелей чи світлодіодних світильників із ШІМ-драйверами).
9. **Завершення сеансу:** Повторіть вищеописану процедуру перевірки біля кожного віконного прорізу та в усіх інших зонах приміщення, які мають пряму видимість із вулиці.

Моніторинг низькочастотного магнітного/електричного спектра (LF)

Низькочастотний сенсор (**Low Frequency**) Багатофункціонального Зонда дозволяє оператору детектувати побічні електромагнітні випромінювання (ПЕМВІ), які генерують електронні компоненти прихованих закладних пристроїв під час своєї

роботи (процесори, тактові генератори, цифрові шини даних, імпульсні перетворювачі напруги).
Ефективна дальність детектування у цьому режимі є дуже малою і становить **до 30 см**. Через це всі потенційно небезпечні предмети інтер'єру, оргтехніку та поверхні необхідно досліджувати методом ретельного контактного або безпосереднього сканування на мінімальній відстані.

Покроковий алгоритм проведення перевірки

1. **Підключення апаратури:** Підключіть Багатофункціональний Зонд до коаксіального гнізда **«PROBE»** на основному блоці пошукового комплексу за допомогою кабелю з базового комплекту.
2. **Комутація режиму:** Переведіть механічний перемикач на корпусі зонда в положення **«LF»**.
3. **Ініціалізація ПЗ:** Активуйте режим **«Зонд»** у головному вікні програми Breeze RF.
4. **Зачистка бази даних:** Очистіть поточну таблицю сигналів за допомогою команди «Видалити всі сигнали в межах діапазону» в контекстному меню панелі **«Рівень»**.
5. **Акустична активація:** Забезпечте наявність стабільного фонового звуку в кабінеті (наприклад, увімкніть звуковий генератор чи радіо). Це необхідно для активації мікрофонних ланцюгів та процесорів обробки звуку в закладному пристрої, що збільшить рівень його побічного ВЧ/НЧ-випромінювання.
6. **Контактний огляд об'єктів:** Почніть плавне та послідовне сканування елементів приміщення (елементів меблів, оргтехніки, розеток, вимикачів, елементів декору та плінтусів), утримуючи зонд на відстані не більше ніж **5–10 см** від об'єкта. Спостерігайте за динамікою індикаторів небезпеки. Функція **«Звукова тривога»** (якщо вона увімкнена) генеруватиме звуковий сигнал, тональність та частота якого змінюватимуться пропорційно до потужності зафіксованого поля.
7. **Автоматичний запис загрози:** Усі зафіксовані аномальні сплески спектра, які перетинають встановлену лінію порогу, будуть автоматично занесені до робочої таблиці сигналів. Їхні амплітудні значення динамічно оновлюватимуться в процесі переміщення зонда.
8. **Пеленгація та диференціація завад:** Намагайтеся локалізувати точку з максимальним рівнем сигналу, обережно змінюючи кут нахилу та просторову орієнтацію зонда.
    - **Ознака пристрою:** Активна електроніка формує на графіку спектра чіткі, стабільні гармонійні складові (піки) або характерні цифрові "гребінки".
    - **Природний фон:** Зверніть увагу, що масивні металеві предмети та будівельні конструкції (арматура, сейфи, металеві каркаси) під впливом потужних зовнішніх радіополів (наприклад, від міських телевеж або БС мобільного зв'язку) здатні вторинно пере-випромінювати РЧ-поля. Це призводить до локального підняття шкал небезпеки, що є нормальним фізичним явищем (ефектом перевідбиття), а не ознакою наявності шпигунської техніки.
9. **Акустичний аналіз та демодуляція:** Якщо ви виявили підозрілий стабільний сплеск, скористайтеся вбудованою функцією **акустичної демодуляції** для його ідентифікації. Оберіть потрібну частоту безпосередньо в таблиці або клікніть мишкою на пік спектральної лінії. Під час проведення прослуховування утримуйте Багатофункціональний Зонд нерухомо у точці максимального рівня сигналу.

Моніторинг силової мережі (WIRE)

Оскільки силова проводка мережі виконує роль величезної антени, вона природно накопичує велику кількість сторонніх радіочастотних завад та наводок, що присутні в сучасному міському середовищі.
Для уникнення труднощів під час сепарації шпигунських сигналів на тлі потужного мережевого шуму використовується **диференціальний метод аналізу**. За цієї методики комплекс **Delta X** фіксує та зберігає в пам'яті поточний стан радіочастотного фону в першій (референсній) розетці, а під час перевірки кожної наступної розетки автоматично віднімає цей базовий зліпок. В результаті оператор бачить на екрані суто математичну різницю спектрів.
Таким чином, якщо провідний закладний пристрій підключений до силової лінії, амплітуда його сигналу стрімко зростатиме в міру наближення оператора з зондом до місця його фізичного монтажу.
Важлива умова: Диференціальний метод коректно працює лише в тому разі, якщо група розеток підключена до однієї лінії (фази).

Покроковий алгоритм проведення перевірки

1. **Підключення зонда:** Підключіть Багатофункціональний Зонд до високочастотного гнізда **«PROBE»** на корпусі основного блока системи за допомогою коаксіального кабелю з комплекту постачання.
2. **Комутація датчика:** Перемкніть селектор на зонді в положення **«WIRE»**.
3. **Ініціалізація ПЗ:** Оберіть режим **«Зонд»** у головному меню програми Breeze RF.
4. **Комутація високої напруги:** Підключіть спеціальний **високовольтний кабель** із комплекту до відповідного роз'єму Багатофункціонального Зонда.

КРИТИЧНЕ ПОПЕРЕДЖЕННЯ З БЕЗПЕКИ:
НІКОЛИ НЕ ВИКОРИСТОВУЙТЕ НИЗЬКОВОЛЬТНИЙ КАБЕЛЬ ІЗ РОЗ'ЄМАМИ ТИПУ «КРОКОДИЛ» ДЛЯ ДІАГНОСТИКИ СИЛОВИХ МЕРЕЖ! ЦЕ СТВОРЮЄ НЕБЕЗПЕКУ УРАЖЕННЯ ЕЛЕКТРИЧНИМ СТРУМОМ.

5. **Акустична активація:** Створіть у приміщенні постійне джерело звуку (радіо, мовлення), щоб перевести заклади з голосовим керуванням (VOX) у режим активної трансляції та мати змогу чітко розпізнати звук кабінету під час демодуляції.
6. **Зняття опорного спектра:** Вставте вилку високовольтного кабелю в першу розетку (Розетка №1).
7. **Фіксація фону:** У вікні програми натисніть кнопку **«Обнулити – Захопити»**, щоб внести поточний шум мережі в пам'яті як базовий (нульовий) рівень.
8. **Очищення робочого простору:** Видаліть старі сигнали з таблиці за допомогою команди «Видалити всі сигнали в межах діапазону» в контекстному меню панелі **«Рівень»**.
9. **Послідовний перебір ліній:** Почергово підключайте високовольтний кабель до решти розеток у приміщенні, фіксуючи появу нових сигналів на графіку.
    - **Ознака побутових завад:** Побутові мережеві завади зазвичай мають розмитий спектр без чітко виражених піків, займають широку смугу частот і фіксуються в усіх розетках з приблизно однаковою амплітудою.
    - **Ознака закладного пристрою:** Сигнал від реального шпигунського передавача (або HomePlug-адаптера) матиме чітку форму, високу амплітуду й досягатиме максимуму лише в одній або кількох суміжних розетках.

10. **Аналіз та ідентифікація виявлених сигналів:**
    - Використовуйте одинарний або подвійний клік на підозрілому сигналі в таблиці для автоматичного фокусування та детального вивчення його спектрограми.
    - Переведіть систему в режим **«Демодуляція»**.
    - Послідовно клікайте на всі виявлені піки на графіку спектра для точного захоплення частоти й прослуховування аудіопотоку. Намагайтеся зафіксувати наявність акустичного фону кімнати. За потреби змінюйте тип демодуляції (**AM / FM**), коригуйте смугу пропускання фільтра та виконуйте точне підлаштування частоти (крок вгору/вниз).
    - Дії при виявленні загрози: У разі виявлення звуку приміщення в сигналі або фіксації сигналу з нетипово високим рівнем амплітуди — негайно припиніть сканування та розпочніть фізичний огляд і демонтаж елементів уздовж лінії проходження підозрілого кабелю.
11. **Захист від тактики маскування:** Щоб повністю виключити ризик того, що сам закладний пристрій перебуває безпосередньо всередині першої (референтної) розетки (через що його сигнал міг бути помилково прийнятий за фон і віднятий системою), обов'язково повторіть процедуру (кроки 7–10), обравши іншу розетку як базову розетку №1.

Моніторинг низьковольтних ліній (телефон, Ethernet, сигналізація)

Перевірка дротів та кабелів низької напруги здійснюється за допомогою спеціального **низьковольтного кабеля (кабеля низької напруги) з затискачами типу «крокодил»**, який входить до базового комплекту постачання системи.

Покроковий алгоритм проведення перевірки

1. **Підключення апаратури:** Підключіть Багатофункційний Зонд до високочастотного гнізда **«PROBE»** на корпусі основного блока системи за допомогою коаксіального кабелю з комплекту.
2. **Комутація режиму:** Переведіть механічний перемикач на корпусі зонда в положення **«WIRE»**.
3. **Ініціалізація ПЗ:** Оберіть режим **«Зонд»** у головному меню програми Breeze RF.
4. **Зачистка бази даних:** Очистіть поточну таблицю сигналів за допомогою команди «Видалити всі сигнали в межах діапазону» в контекстному меню панелі **«Рівень»**.
5. **Комутація тестового шлейфа:** Підключіть низьковольтний кабель з «крокодилами» до відповідного роз'єму Багатофункційного Зонда.
6. **Акустична активація:** Створіть у приміщенні постійне джерело звуку (наприклад, увімкніть радіо або тестовий аудіозапис), щоб активувати потенційні пристрої зняття інформації та легко розпізнати звук кабінету під час демодуляції.
7. **Комутація до лінії:** Почергово підключайте затискачі типу «крокодил» до оголених контактів, клемних колодок або окремих жил перевірюваного кабелю (телефонної лінії, шлейфа сигналізації чи комп'ютерного Ethernet-кабелю).
8. **Аналіз та локалізація:** Стежте за графіком спектра та появою нових сигналів у таблиці. У разі виявлення підозрілого сигналу використовуйте функцію **«Демодуляція»** (AM/FM) та прослухайте ефір лінії. Якщо в навушниках чітко чути звук із приміщення, це є прямим підтвердженням наявності провідного «жучка». Проведіть фізичний огляд лінії по всій її довжині для демонтажу пристрою.

Використання Внутрішньолінійного Модульного Адаптера

За наявності спеціалізованого **Внутрішньолінійного модульного адаптера** (Inline Modular Adapter) оператор має можливість безпечно та швидко підключатися до окремих жил кабельних ліній зі стандартизованими роз'ємами **RJ-11**, **RJ-12** та **RJ-45**. Як правило, цей адаптер постачається у комплекті зі спеціалізованим набором шлейфів та перехідників:

Тип лінії (кабелю)	**Тип інтерфейсу (роз'єму)**	**Необхідні аксесуари для підключення**	**Контакти адаптера (Pins)**
Аналоговий провідний телефон	RJ-11 (6 позицій, 4 контакти)	Витий кабель низької напруги, модульний адаптер, кабель 8 до 6, адаптер 8 до 6	1...4
Цифровий / Системний телефон	RJ-12 (6 позицій, 6 контактів)	Витий кабель низької напруги, модульний адаптер, кабель 8 до 6, адаптер 8 до 6	1...6
Комп’ютерний кабель Ethernet	RJ-45 (8 позицій, 8 контактів)	Витий кабель низької напруги, модульний адаптер, кабель 8 до 8, адаптер 8 до 8	1...8
Кабелі сигналізації	Пряме підключення	Низьковольтний кабель із затискачами типу **«крокодил»**	
Інші кабелі низької напруги	Пряме підключення	Низьковольтний кабель із затискачами типу **«крокодил»**	

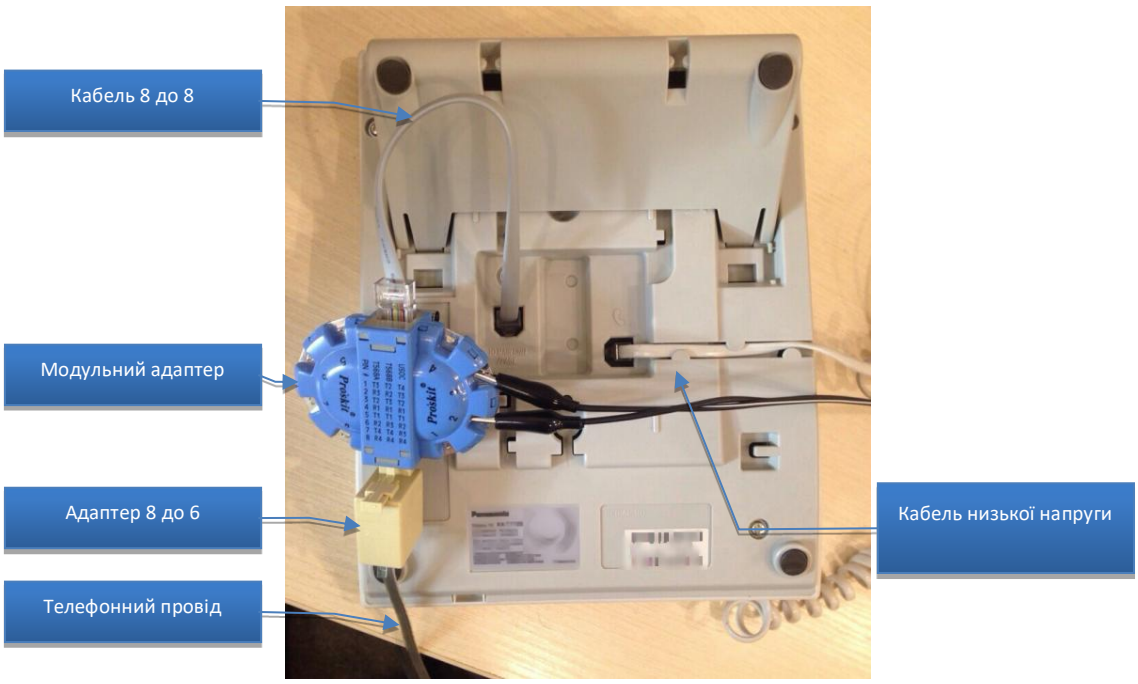
Перевірка стаціонарної телефонної лінії за допомогою модульного адаптера

Підключення до телефонної лінії для зняття спектральних показників можна виконати у будь-якій доступній точці комунікаційного шлейфа: або безпосередньо з боку телефонного апарату, або біля настінної розетки (залежно від умов доступу на об'єкті).

Порядок та особливості підключення:

1. Щільно та надійно зафіксуйте перехідник-адаптер типу «вилка-розетка» у гнізді Внутрішньолінійного модульного адаптера, щоб гарантувати безперервний та якісний електричний контакт.
2. Проведіть верифікацію лінії: обов'язково переконайтеся, що після підключення адаптера «у розрив» стаціонарний телефон продовжує функціонувати у штатному режимі (є тональний сигнал у слухавці, пристрій приймає та здійснює дзвінки). Це підтвердить, що комплекс не створює критичного шуму чи замикання в лінії.

Нижче наведено наочний приклад проведення інспекції та підключення пошукової системи безпосередньо біля телефонного апарату користувача.



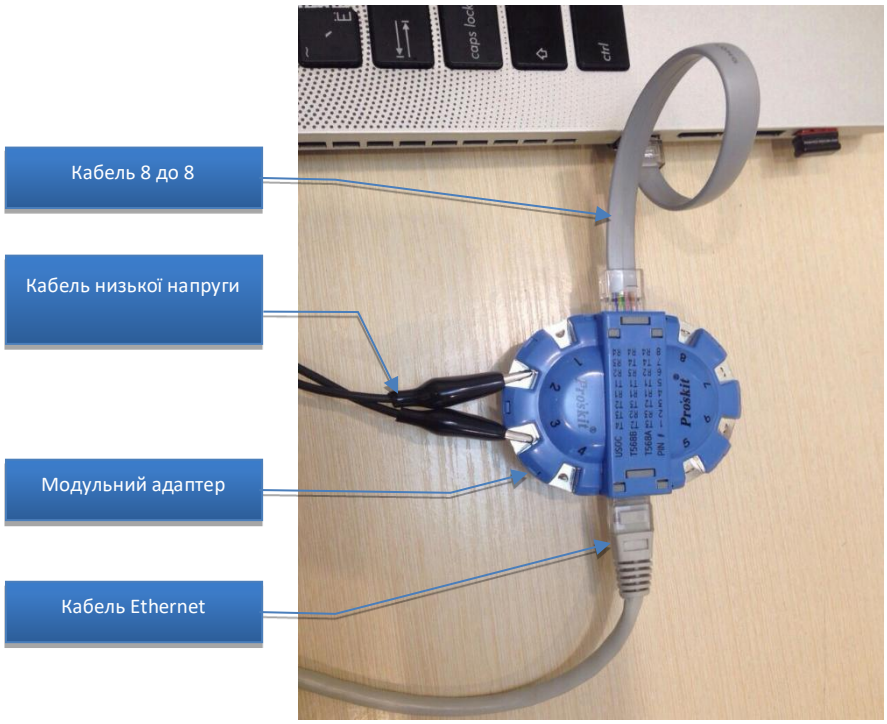
Перевірка ліній Ethernet за допомогою модульного адаптера

Підключення комплексу до мережі Ethernet можна виконати у будь-якій доступній і зручній точці комутаційного шлейфа: поруч із робочим комп'ютером (робочою станцією), біля настінної мережевої розетки або безпосередньо у серверній шафі біля активного мережевого обладнання (комутатора, маршрутизатора чи патч-панелі).

Порядок та особливості підключення:

1. Щільно та до упору вставте з'єднувальний кабель-перехідник типу «вилка-розетка» (RJ-45) у гніздо Внутрішньолінійного модульного адаптера, щоб гарантувати стабільний і надійний електричний контакт для зняття високочастотних показників.
2. Проведіть обов'язкову верифікацію лінії: переконайтеся, що комп'ютерна мережа та інтернет-з'єднання на цільовому пристрої продовжують функціонувати у штатному режимі після інтеграції адаптера в розрив лінії. Наявність лінку та мережевого обміну підтвердить, що комплекс підключено правильно і він не порушує узгодження хвильового опору кабелю.

Нижче наведено наочний практичний приклад проведення інспекції та підключення системи моніторингу до лінії Ethernet безпосередньо біля мережевої карти (мережевого порту) комп'ютера.

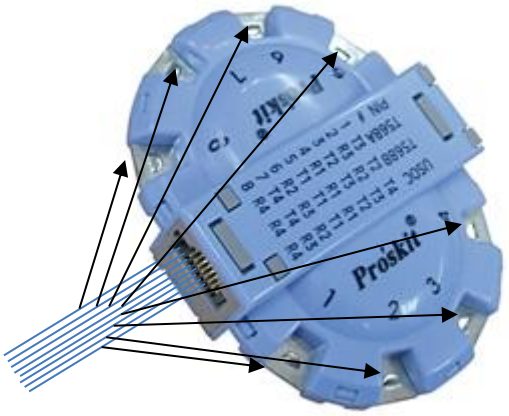


Перевірка шлейфів сигналізації та низьковольтних кабелів
Підключення до ліній низької напруги, зокрема до кабелів охоронно-пожежної сигналізації, виконується за допомогою низьковольтного кабелю та його затискачів типу **«крокодил»**.
Щоб отримати фізичний доступ до внутрішніх контактних клем, необхідно акуратно зняти кришку сповіщувача (наприклад, ІЧ-датчика руху). Також підключення можна виконати безпосередньо всередині головного приладу приймально-контрольного (ППК / централі).

Увага! Ризик тривоги: Сповіщувачі та блоки централей зазвичай захищені мікроперемикачами розкриття корпусу (тамперами). У разі спроби зняття кришки вони миттєво передають сигнал «Втручання» на пульт централізованого спостереження (ПЦС). Ця процедура має бути заздалегідь узгоджена з оператором охорони й проводитися виключно в присутності профільного інженера з обслуговування системи безпеки.

Покроковий алгоритм проведення перевірки

1. **Комутація жил та комбінаторний перебір:**
    - Підключіть затискачі типу «крокодил» до вихідних контактів на копусі Внутрішньолінійного модульного адаптера відповідно до кількості активних жил у лінії. Стаціонарні телефонні лінії зазвичай використовують 2, 4 або 6 жил, тоді як комп'ютерні мережі Ethernet (100Base-TX) задіюють 4 активні жили з 8 (дві пари в структурі крученої пари).
    - Послідовно підключайте «крокодили» до клем кабельної лінії.



Оскільки призначення жил часто невідоме або не має маркування, оператор повинен методично протестувати всі можливі комбінації пар: **1–2, 2–3, 3–4, 1–3, 1–4** тощо. У деяких парних комбінаціях спектральні картини можуть повністю збігатися.

2. **Запуск моніторингу:** Після фіксації «крокодилів» на парі дротів система автоматично розпочне вимірювання. Спектральні компоненти, що перетнуть лінію порогу, будуть автоматично внесені до робочої таблиці сигналів. За потреби активуйте опцію **«Звукова тривога»**.
3. **Аналіз та верифікація сигналів:**
    - Використовуйте одинарний або подвійний клік на сигналі в таблиці для фокусування та детального аналізу його спектрограми.
    - Активуйте інструмент **«Демодуляція»**.
    - Почергово натискайте на всі виявлені піки на Спектрограмі для точного захоплення частоти й прослуховування аудіопотоку. Намагайтеся зафіксувати наявність акустичного фону кімнати. За потреби змінюйте тип демодуляції (**AM / FM**), коригуйте смугу пропускання фільтра та виконуйте точне підлаштування частоти.

Оскільки будь-який довгий провід працює як антена, він природно приймає зовнішні ефірні радіочастотні сигнали (наводки від потужних радіостанцій, стільникових мереж тощо). Фіксація таких сторонніх сигналів у лінії є цілком нормальною ситуацією. Завдання оператора — ретельно дослідити всі позиції в таблиці, проаналізувати амплітуду, провести демодуляцію та прийняти рішення щодо безпеки чи небезпеки кожного джерела.

Дії при виявленні загрози: У разі детектування модульованого сигналу з чітким акустичним супроводом салону кімнати або сигналу з нетипово високим рівнем амплітуди — негайно зупиніть перевірку та розпочніть фізичний огляд уздовж усього кабельного треку.

4. **Тест телефонної лінії на розрив:** Якщо досліджується лінія стаціонарного зв'язку, проведіть вимірювання спочатку при покладеній слухавці (режим очікування, висока напруга в лінії), а потім — при знятій трубці (режим розмови, падіння напруги й активація шпигунських модулів із послідовним типом підключення).
5. **Циклічність процесу:** Повторіть вищеописаний тест для всіх можливих комбінацій контактних пар на модульному адаптері, за потреби перемикаючи «крокодили».
6. **Просторова сепарація ліній:** Проведіть аналогічні тестування для інших слабкострумових ліній та розеток, що присутні в цільовому кабінеті та суміжних з ним приміщеннях.

- **Поведінка завад:** Ефірні завади (інтерференційні сигнали) матимуть практично ідентичний вигляд спектра й однаковий рівень амплітуди на всіх лініях у межах будівлі. Натомість кабелі, в які реально інтегровано шпигунський пристрій, дадуть локальний сплеск амплітуди та унікальний профіль спектра лише в одній точці.
- **Особливість цифри:** Якщо закладний пристрій транслює інформацію в цифровому вигляді (наприклад, пакетні дані або зашифрований потік), виділити з нього первинний звук за допомогою стандартного аналогового демодулятора буде неможливо. Проте аномально високий рівень сигналу та характерний "прямокутний" або "гребінчастий" вигляд спектрального піка чітко вкажуть оператору на наявність загрози.

Компенсація фонового шуму (Диференціальний метод)
Оскільки в лініях Ethernet та телефонних мережах постійно присутні легальні високочастотні сигнали службового обміну, виявлення небезпечного шпигунського сигналу на їхньому тлі може бути серйозно ускладнене. Для спрощення цього завдання застосовується **диференціальний метод**. Він дозволяє математично усунути (компенсувати) легальні фонові компоненти, залишаючи на екрані для аналізу лише сторонні аномальні сплески.
Цей метод є максимально ефективним, якщо в кабінеті встановлено декілька однотипних телефонних або Ethernet-розеток, підключених до загального комутатора чи кросу.

Алгоритм компенсації:
1. Підключіть комплекс до першої (базової) розетки.
2. Натисніть кнопку **«Обнулити – Захопити»** — система внесе поточний спектр легального обміну лінії до буфера пам'яті як референсний нуль.
3. Перейдіть до наступних розеток і почергово зніміть показники. Програма автоматично вираховуватиме та відображатиме на екрані суто різницю спектрів.

Оскільки інформаційні кабелі містять багато провідників, переконайтеся, що порівняльні вимірювання на різних розетках проводяться суворо на **одній і тій самій парі жил** (наприклад, порівнюються пари 4–5 на першій та 4–5 на другій розетках).

Повна відсутність нових піків під час диференціального аналізу свідчить про чисту лінію та нормальну радіоелектронну обстановку. Натомість раптова поява нового чіткого сигналу на графіку — це пряма ознака аномалії. У такому разі оператор зобов'язаний провести детальне фізичне інспектування всієї кабельної траси та всього підключеного до неї кінцевого обладнання.