Міністерство освіти і науки України

Харківський національний університет радіоелектроніки

Факультет Центр після дипломної освіти

Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації

КВАЛІФІКАЦІЙНА РОБОТА

Пояснювальна записка

рівень вищої освіти другий (магістерський)

# Пошук радіозакладних пристроїв


Виконав: студентка групи СТЗІАздм-21-1

Сапоцька К.М.

Спеціальність 125 Кібербезпека

Тип програми освітньо-професійна

Освітня програма Системи технічного захисту інформації та автоматизація її обробки

Керівник доц. Ликов Ю.В.

(посада, прізвище, ініціали)


Допускається до захисту

Зав. кафедри _____ _Антіпов І.Є__

(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Центр після дипломної освіти

Кафедра Комп'ютерної радіоінженерії та систем технічного захисту інформації

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека

(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Системи технічного захисту інформації, автоматизація її обробки

(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____

(підпис)

«____»_____ 2024 р.

# ЗАВДАННЯ

НА КВАЛІФІКАЦІЙНУ РОБОТУ

Студентові Сапоцькій Катерині Миколаївні

(прізвище, ім'я, по батькові)

1. Тема роботи Пошук радіозакладних пристроїв

затверджена наказом університету від 06 грудня 2023 р. № 262 Стз .

2. Термін подання студентом роботи до екзаменаційної комісії 15 січня 2024 р.

3. Вихідні дані до роботи:

Об'єкт захисту – інформація в приміщені ОІД;

Канал витоку – акусторадіоелектроний;

Загроза – застосування зловмисником РЗП для прослуховування приміщення;

Тип РЗП – пасивні та активні.

4. Перелік питань, що потрібно опрацювати в роботі

Класифікація радіозакладних пристроїв. Загальна характеристика РЗП.

Огляд методів проведення пошукових заходів. Засоби виявлення РЗП. Експериментальне дослідження радіозакладних пристроїв (Опис експериментальної установки, результати експерименту). Провести аналіз отриманих експериментальних даних в результаті якого зробити висновок стосовно сигнальних демаскуючих ознак РЗП.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри)

Актуальність;
Класифікація радіозакладних пристроїв;
Класифікація методів виявлення РЗП;
Огляд засобів виявлення РЗП;
Результати експериментального дослідження радіозакладних пристроїв;
Висновки

## КАЛЕНДАРНИЙ ПЛАН

| № | Назва етапів роботи | Терміни виконання етапів | Примітка |
|---|---|---|---|
| 1. | Пошук літератури по темі кваліфікаційної роботи | 16.10.2023-1.11.2023 | Виконано |
| 2. | Написання оглядової частини роботи | 02.11.2023-1.12.2023 | Виконано |
| 3. | Проведення експериментального дослідження | 02.12.2023-20.12.2023 | Виконано |
| 4. | Оформлення пояснювальної записки | 21.12.2023-10.01.2024 | Виконано |
| | | | |
| | | | |

Дата видачі завдання 1 листопада 2023 р.

Студент _____ _____
(підпис)

Керівник роботи _____ доц. Ликов Ю.В.
(підпис) (посада, прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 89 с.,34 рис., 2 табл.,2 додатки, 18 джерел.

РАДІОЗАКЛАДНИЙ ПРИСТРІЙ, ЗАХИСТ ІНФОРМАЦІЇ, ПОШУК, СПЕКТР

Метою магістерської роботи є аналіз засобів та методів захисту інформації для їх подальшого застосування на об‘єктах інформаційної діяльності. Для досягнення мети у роботі були виконані наступні завдання:

- розглянуто основні поняття апаратних закладних пристроїв,
- канали несанкціонованого знімання інформації через закладні пристрої,
- організаційні заходи для не потрапляння закладних пристроїв на об’єкт інформаційної діяльності;
- аналіз засобів і методів які використовуються для виявлення апаратних закладних пристроїв;
- обґрунтування обраних засобів для виявлення апаратних закладних пристроїв.

Об’єктом магістерської роботи є захист інформації від витоку через радіозакладні пристрої. Предметом магістерської роботи є засоби і методи захисту інформації, що підлягає захисту.

# ABSTRACT

Explanatory note of qualification work: 89 p.,34 fig., 2 table., 2 appendice, 18 sources.

BUG DEVICE, INFORMATION PROTECTION, SEARCH, SPECTRUM

The purpose of the master's thesis is to analyze the means and methods of information protection for their further application at the objects of information activity. To achieve the goal, the following tasks were performed in the work:

- the basic concepts of hardware bug devices are considered,
- channels of unauthorized recording of information through bug devices,
- organizational measures to prevent embedded devices from entering the object of information activity;
- analysis of means and methods used to detect hardware bug devices;
- justification of the selected means for detecting hardware bug devices.

The object of the master's thesis is the protection of information against leakage through radio bug devices. The subject of the master's thesis is the means and methods of protecting information subject to protection.

ЗМІСТ

# ПЕРЕЛІК СКОРОЧЕНЬ

ЗП – Закладні пристрої

РЗП – Радіозакладний пристрій

ОТЗ – Об’єкт технічного захисту

ОІД – Об’єкт інформаційної діяльності

ІзОД – Інформація з обмеженим доступом

НД – Нормативний документ

ТЗІ – Технічний захист інформації

НЛ – Нелінійний локатор

# ВСТУП

Актуальність даної теми обумовлена тим, що сучасному світі, де технології постійно розвиваються, апаратні закладні пристрої стають все більшою загрозою для безпеки та приватності. Згідно з визначення НД ТЗІ 2.7-011-2012, закладний пристрій – потай встановлений технічний засіб, який створює загрозу для інформації [1]. Ці пристрої, такі як приховані камери, підслуховуючи пристрої, можуть бути розміщені у приміщеннях, транспортних засобах або навіть у пристроях, що здаються повністю безпечними, з метою отримання несанкціонованого доступу та віддаленого контролю.

Виявлення таких апаратних закладних пристроїв стає дедалі важливішою задачею для забезпечення безпеки та захисту інформації, що підлягає захисту. До цього часу, багато компаній застосовують різні методи виявлення та захисту від апаратних закладних пристроїв, однак їх ефективність може значно відрізнятись. Отже, доцільним є проведення аналізу цих методів та засобів з метою виявлення їх переваг та недоліків. Засоби та методи виявлення апаратних закладних пристроїв є важливою проблемою в галузі технічного захисту інформації. Аналіз наявних засобів та методів виявлення апаратних закладних пристроїв може допомогти збільшити ефективність захисту та зменшити ризики для організацій та установ.

Метою магістерської роботи є аналіз засобів та методів захисту інформації для їх подальшого застосування на об‘єктах інформаційної діяльності. Для досягнення мети дипломної роботи були виконані наступні завдання:

- розглянуто основні поняття апаратних закладних пристроїв,
- канали несанкціонованого знімання інформації через закладні пристрої,
- класифікацію заходів для не потрапляння закладних пристроїв на об’єкт інформаційної діяльності;
- аналіз засобів і методів які використовуються для виявлення апаратних закладних пристроїв;
- обґрунтування обраних засобів для виявлення апаратних закладних пристроїв.

Об’єктом магістерської роботи є захист інформації від витоку через радіозакладні пристрої. Предметом магістерської роботи є засоби і методи захисту інформації, що підлягає захисту.

# 1. ОГЛЯД ЗАКЛАДНИХ ПРИСТРОЇВ

## 1.1. Загальна характеристика закладних пристроїв та їх класифікація

Один з найбільш ефективних методів, який використовується в промисловому шпигунстві для незаконного отримання інформації, полягає в застосуванні так званих закладних пристроїв (ЗП), які приховано розміщуються в місцях проведення конференцій, розмов чи інших подібних заходів, або підключенні до каналів зв'язку, які використовуються конкурентами [2].

Для систематизації уявлення про закладні пристрої існують певні підходи до їх класифікації за різними ознаками (рис. 1.1). Розглянемо деякі з них більш детально.

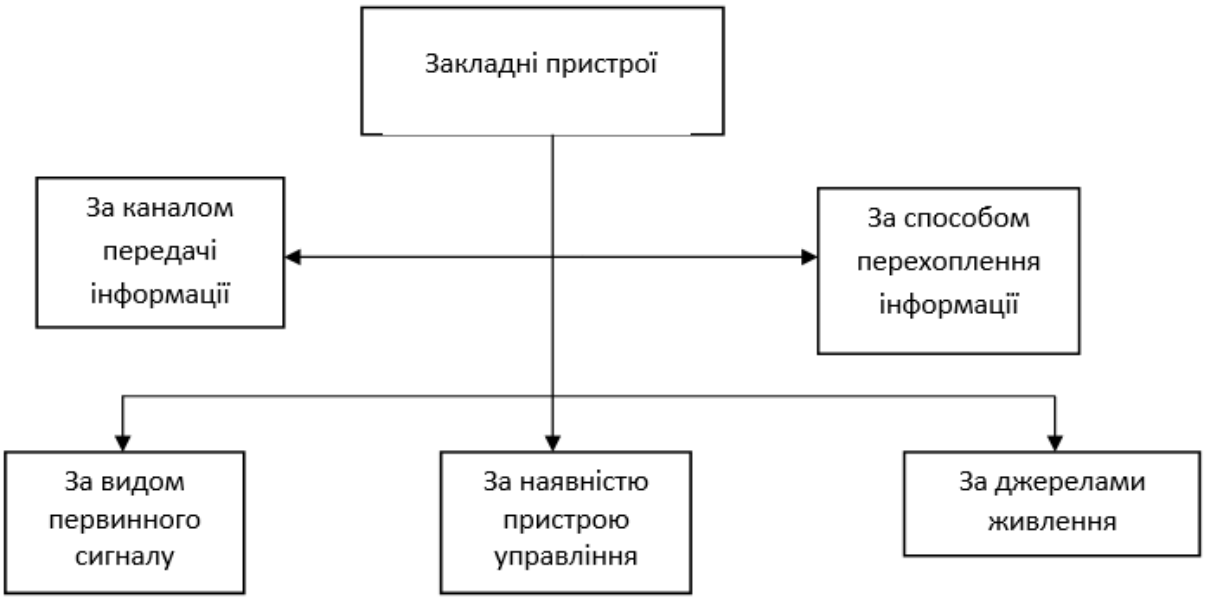


Рисунок 1.1 – Класифікація закладних пристроїв

Закладний пристрій – технічний засіб негласного отримання інформації, розміщений на об'єкті інформаційної діяльності з приховуванням від виявлення особою, яка не має відношення до застосування технічного засобу, факту його наявності та/або застосування, внаслідок чого створюється загроза витоку інформації з об'єкта інформаційної діяльності.

Сьогодні існує безліч різних видів таких пристроїв, що відрізняються принципом роботи, способом передачі інформації, дальністю дії, розмірами, зовнішнім виглядом, вартістю та іншими характеристиками. Деякі з

найменших ЗП можуть мати вагу всього близько 1,5 грама та розміри 2-5 міліметрів, що дуже небагато. Діапазон їх дії зазвичай не перевищує 10 метрів. Більш потужніші пристрої можуть мати розміри до декількох сантиметрів, але дозволяють отримувати сигнали з відстані декількох сотень до тисяч метрів або навіть більше. ЗП зазвичай встановлюються під одяг або камуфлюються під особисті речі шпигуна (наприклад, авторучку або дипломатичну сумку), а також можуть бути вбудовані в елементи конструкцій будівлі та декоративні предмети (наприклад, стільці, шафи, картини тощо). Щоб зробити класифікацію таких пристроїв більш зрозумілою та легкою для систематизації, розумно розподілити їх за кількома критеріями класифікації:

за каналом передачі даних;

за способом отримання інформації;

за наявністю пристрою керування;

за зовнішнім виглядом;

за застосованим джерелом живлення.

В залежності від каналу передачі інформації (виду носія інформації від закладних пристроїв до зловмисника) їх можна поділити на провідникові і випромінюючі (такі, що випромінюють електромагнітні коливання).

Для більш детального розуміння розглянемо кожен з критеріїв класифікації окремо (рис.1.2).

З приводу каналу передачі даних існують наступні типи ЗП: 1. Радіо-закладки; 2. Закладки з інфрачервоним зв'язком; 3. Закладні пристрої, що передають дані по провідникам; 4. Закладки з записом на магнітофони. Радіо закладні пристрої використовують електромагнітні хвилі, які не мають впливу на людські органи чуття, можуть пройти великі відстані та оминати перешкоди. Ці корисні властивості дозволяють здійснювати нагляд за об'єктом з віддалення на будь-якій точці розміщення. З технічної точки зору, закладні пристрої можуть працювати в різних діапазонах радіохвиль, але для зручності використання найчастіше використовують діапазон від 100 до 1000 МГц.

Інфрачервоні закладні пристрої використовують енергію електромагнітних хвиль, але в інфрачервоному діапазоні, який не видимий для ока людини. Завдяки малій довжині хвиль такі пристрої можуть передавати інформацію компактним пучком у заданому напрямку, що ускладнює їх пошук навіть з використанням спеціальної апаратури. Однак, висока прихованість таких пристроїв ускладнює їх застосування. Інфрачервона закладка повинна бути в прямій видимості приймача, а

потрапляння на шлях передачі будь-якого випадкового об'єкта може суттєво погіршити якість передачі або зовсім припинити її. Тому застосування інфрачервоних закладних пристроїв в промисловому шпигунстві обмежене.

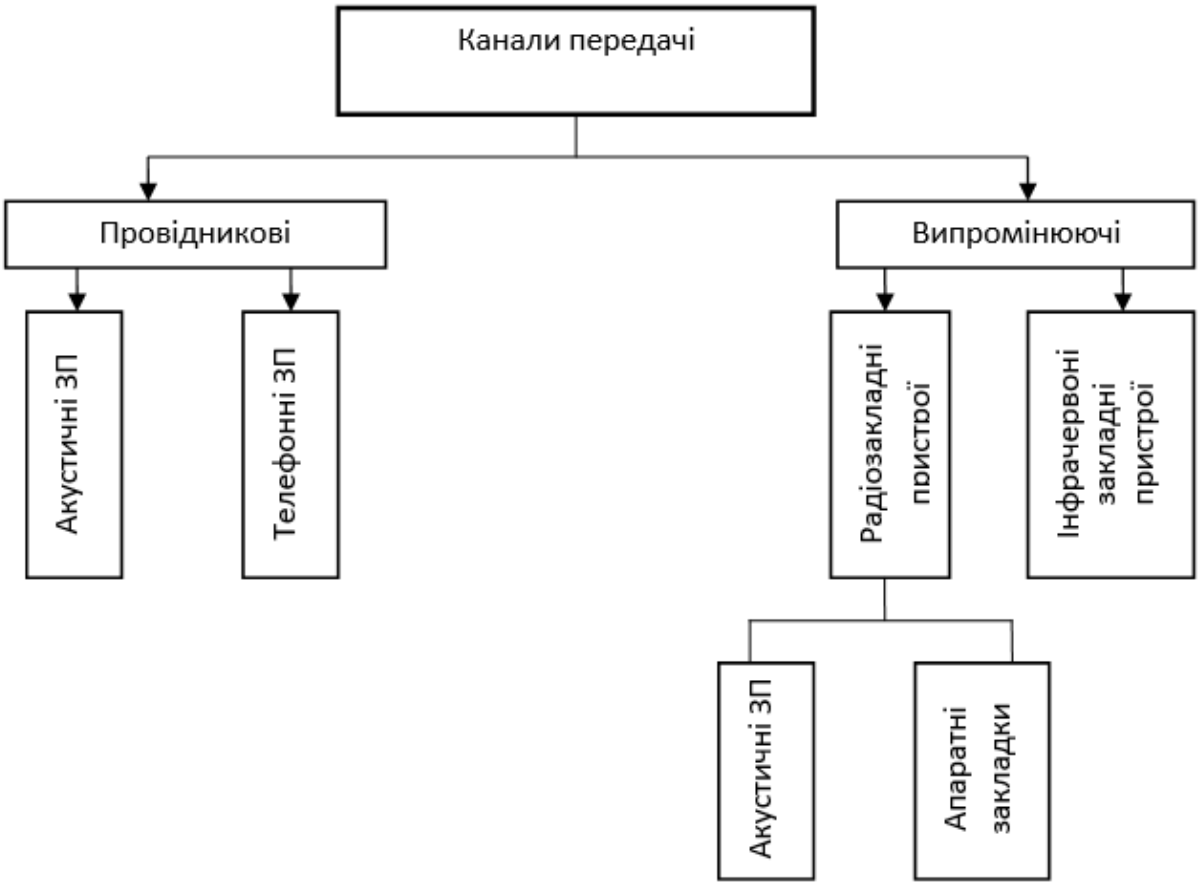


Рисунок 1.2 – Класифікація ЗП в залежності від каналу передачі інформації

Закладні пристрої для передачі даних по провідникам працюють на основі передачі електронних сигналів по провідникам на великі відстані. Цей метод має кілька переваг, включаючи високу прихованість передачі даних, відсутність потреби в додатковому живленні та велику дальність дії. Ці пристрої можуть використовувати окремі прокладені провідники або існуючі мережі, такі як мережа 220 В або слабо точні мережі, наприклад, телефонні лінії або пожежні. Вони можуть бути добре приховані на місці застосування, надійно маскуючись під елементи електронних ланцюгів та токові приймачі, такі як розетки, перехідники, настільні лампи та інші прилади.

Закладні пристрої з записом на магнітофон базуються на засадах записування сигналів на касетну стрічку чи будь-який інший носій. Застосовуються тоді, коли не потрібна негайна передача інформації в режимі

реального часу та існує ризик виявлення шпигунської апаратури під час передачі. Однак, слабким місцем цих пристроїв є необхідність періодично замінювати касети. Розглянемо різновиди ЗП в залежності від методу отримання інформації. Ці види можна класифікувати наступним чином:

1. ЗП мікрофонного типу
2. ЗП вібраційного типу
3. ЗП з підключенням до ліній комунікацій.

ЗП мікрофонного типу ґрунтується на перетворенні звукових коливань на електричний сигнал, який подальшим чином передається за допомогою одного з доступних методів передачі. ЗП вібраційного типу (такі як стетоскопи) дозволяють виявляти коливання на твердих поверхнях, що виникають внаслідок поширення акустичних хвиль на них ( рис. 1.3.). В якості чутливого елемента можуть використовуватися п'єзо мікрофони, електронні мікрофони або датчики акселерометричного типу, які найкраще реагують на коливання на тонких поверхнях, таких як скло, двері, міжкімнатні перегородки тощо.

ЗП мікрофонного типу ґрунтується на перетворенні звукових коливань на електричний сигнал, який подальшим чином передається за допомогою одного з доступних методів передачі. ЗП вібраційного типу (такі як стетоскопи) дозволяють виявляти коливання на твердих поверхнях, що виникають внаслідок поширення акустичних хвиль на них ( рис. 1.3). В якості чутливого елемента можуть використовуватися п'єзо мікрофони, електронні мікрофони або датчики акселерометричного типу, які найкраще реагують на коливання на тонких поверхнях, таких як скло, двері, міжкімнатні перегородки тощо.

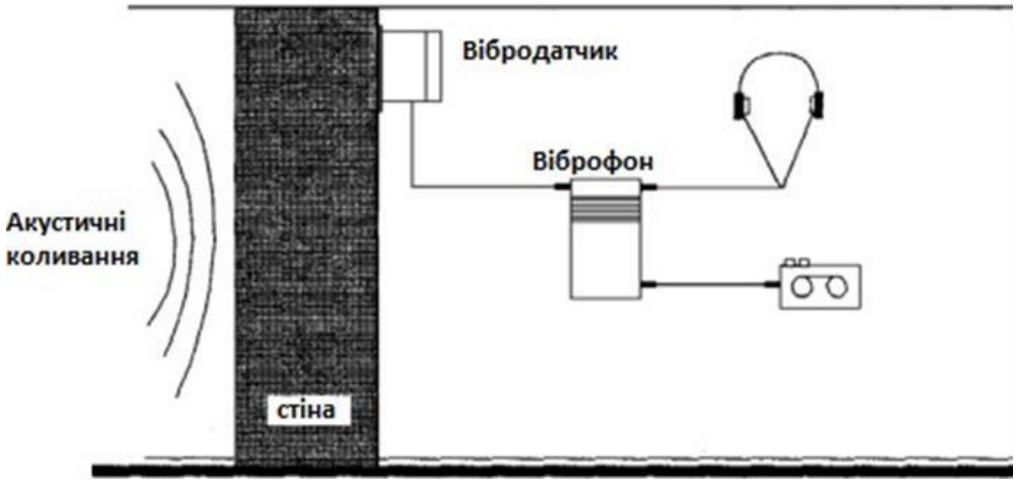


Рисунок 1.3 – Стетоскоп з передачею сигналу по провіднику

Існує також можливість передачі сигналу стетоскопа по радіоканалу, цей прилад називають радіо-стетоскоп ( рис 1.4).


Рисунок 1.4 – Радіо-стетоскоп

ЗП з підключенням до ліній комунікацій призначені для незаконного зняття корисної інформації з телефонних ліній або оптоволоконних кабелів. Ці пристрої дозволяють проводити скритий моніторинг телефонних розмов або навіть отримувати електронні повідомлення або факси. Для передачі інформації з таких пристроїв використовують радіоканал.

Існують два типи РЗП в залежності від способу підключення до ліній комунікацій: пряме підключення та індуктивне.

Існують два способи прямого підключення: паралельний та послідовний, як показано на рис. 1.5. (а) та (б) відповідно

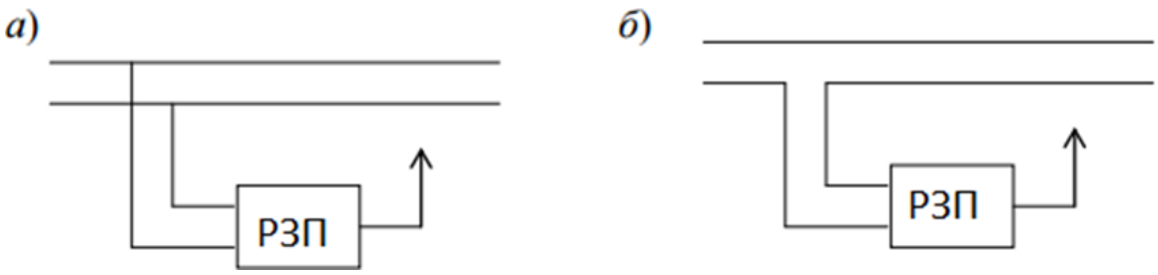


Рисунок 1.5 – Пряме підключення РЗП: а – паралельне, б – послідовне

Ці методи дають змогу отримувати високоякісний вхідний сигнал і живити сам пристрій без використання додаткових джерел живлення, проте такі закладки можуть бути виявлені через змінення параметрів в лінії.

Застосування ЗП з індуктивним підключенням дозволяє уникнути недоліків попереднього способу підключення, який використовує пряме підключення. (рис. 1.6.)

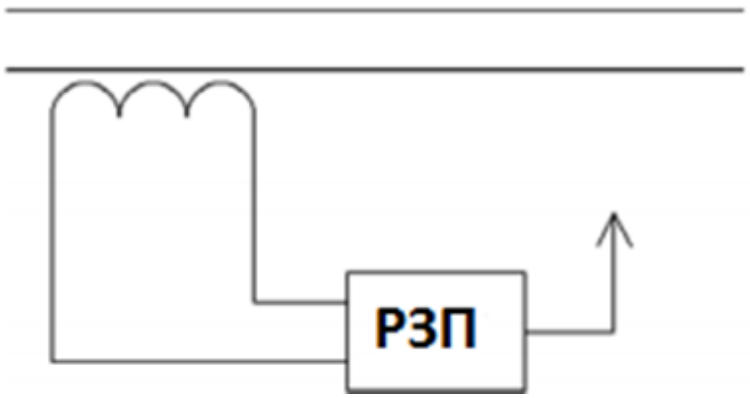


Рисунок 1.6 – Індуктивне підключення

В цих пристроях, основою є спеціальна антена, розташована якомога ближче до провідника, який сприймає електромагнітне поле. Це дозволяє визначити характер повідомлення, і в результаті, підсилювати токи та передавати їх далі до кінцевого користувача. У випадку з оптоволоконними провідниками, використовують спеціальні утискувачі провідника, які за допомогою інтерференційних явищ зчитують інформацію, що потім передається до фотоприймача.

Розрізняють три групи ЗП в залежності від наявності пристрою керування:

1. ЗП з неперервною передачею;
2. ЗП з дистанційним керуванням;
3. ЗП з автоматичним увімкненням при спрацюванні сигналу.

ЗП з неперервною передачею прості у виготовленні та економічно вигідні, працюють постійно при наявності живлення. Однак при використанні акумуляторів, їх час роботи буде дуже обмеженим через велику енерговитратність процесу передачі сигналу і зазвичай не перевищує 1-2 годин. Запуск пристрою здійснюється при підключенні батареї. Використання живлення з провідників розв'язує проблему обмеженого часу роботи. Однак, недоліком цих закладок є можливість їх виявлення через випромінювання. ЗП з дистанційним керуванням базується на тому, що закладка транслює інформацію лише тоді, коли на неї надходить команда, що значно збільшує тривалість її роботи від батареї та забезпечує додаткову конфіденційність через зменшення радіочастотних випромінювань. Крім того, можливо продовжити час роботи за рахунок стиснення інформації за допомогою відповідних систем. ЗП, які автоматично вмикаються при наявності сигналу, відомі як "акустомати", іноді їх також називають VAS чи VOX. Вони знаходяться в режимі очікування (моніторингу) на наявність акустичних сигналів, і коли такі сигнали з'являються, вони автоматично перемикаються в режим передачі. Зазвичай передача завершується через

декілька секунд після того, як "розмова" закінчилась. Недоліком цих пристроїв є можливість пропуску першого слова або кількох слів речення.

ЗП можна розподілити на дві категорії залежно від їх зовнішнього вигляду: звичайні та замасковані. Звичайні ЗП мають типовий корпус з металу або пластику та стандартну форму, що робить їх універсальними та придатними для використання у різних обставинах. З іншого боку, замасковані ЗП можуть бути приховані під одягом або предметами інтер'єру, такими як кошик для паперу, книжки, картини тощо, які дозволяють проходити акустичні та/або електромагнітні коливання. Замасковані ЗП використовуються лише для конкретних завдань, наприклад, для приховування електричних розеток, які мають ту ж форму та виробника, що й інші предмети, або для розміщення у предметах особистого користування, таких як авторучки, запальнички тощо.

Залежно від джерела живлення, ЗП можна розділити на дві категорії:

1. ЗП з власним джерелом живлення;

2. ЗП, які живляться від зовнішнього джерела.

До першої категорії відносяться ЗП, що працюють на акумуляторах або батарейках.

До другої - ті, що підключаються до електричної мережі (наприклад, 220В). Однією з переваг таких пристроїв є час роботи.

До ЗП з живленням від зовнішнього джерела відносяться ЗП з передачею інформації по струмопровідних лініях і ЗП з безпосереднім підключенням до комунікаційних ліній, що використовують енергію самої лінії. Час роботи таких пристроїв практично не обмежений. Широко застосовуються подібні закладні пристрої в телефонних апаратах, закамуфльовані під їх елементи (конденсатори, телефонні капсулі і ін.), у трійниках для підключення декількох приладів до однієї розетки електромережі.

За оцінками, у 75 % закладних пристроїв використовується автономне живлення, 8 % – живлення від мережі і 17 % – живлення від телефонної лінії. Слід зазначити, що застосовуються також пасивні закладки – без власних джерел електроживлення.

Для активізації вони опромінюються зовнішнім електромагнітним полем на частоті, що відповідає резонансній частоті коливального контуру закладки, утвореного елементами її конструкції. Модуляція радіосигналу відбувається в результаті впливу акустичної хвилі на частотнозадаючі елементи конструкції закладки.

Жорсткі вимоги до габаритів, маси, енергоспоживання ЗП обмежують потужність випромінювання їх передавачів. Найбільш часто (більше 80 %) застосовуються радіо-мікрофони, потужність випромінювання яких знаходиться в інтервалі 3–11 мВт, закладки з більшою потужністю випромінювання (до 22 мВт) становлять менше 10 %.

Зустрічаються закладки і більшої потужності випромінювання (до 200 мВт і більше), але їх частка вкрай незначна. Мала потужність випромінювання передавачів радіо-закладок визначає відносно невелику дальність прийому їх сигналів. Близько 75 % зразків забезпечує функціонування каналу на відстань 50 – 350 м, 16 % – на відстань 460 – 600 м, 7 % – на відстанях 740 – 800 м і лише близько 2 % – на відстань до 1000 м і більше.

В загальному випадку технічні дані ЗП знаходяться в наступних межах:

– частотний діапазон 27 – 900 МГц;

– потужність 0,2 – 500 мВт;

– дальність 10 – 150 м;

– час безперервної роботи від декількох годин до декількох років;

– габарити 1 – 8 дмз;

– вага 5 – 350 г.

За зовнішнім виглядом ЗП можуть бути у звичайному виконанні та у закамуфльованому вигляді. У звичайному виконанні пристрої мають, як правило, металевий корпус і форму паралелепіпеда. Вони досить універсальні і застосовуються в різних умовах обстановки. Маскуються одягом, предметами інтер’єру або місцевими предметами, які пропускають електричні і (або) електромагнітні коливання. У закамуфльованому вигляді ЗП застосовуються тільки у відповідності до конкретної обстановки. Так, наприклад, у вигляді силової або телефонної розетки тільки в тому випадку, якщо інші розетки, які не використовуються в приміщенні, мають такий же зовнішній вигляд; у вигляді особистих речей (запальничок, ручок, годинників тощо), якщо вони відповідають загальному іміджеві людини, яка їх використовує [2, 4].

## 1.2. Принципи побудови закладних пристроїв

Для ознайомлення з принципом роботи закладних пристроїв розглянемо два пристрої, схеми яких доступні у відкритих джерелах. Ці пристрої використовуються для проведення експериментальних досліджень з метою визначення їх технічних характеристик в різних умовах.

Перший зі створених пристроїв ЗП 1 має найпростішу схему конструкції (рис. 1.7.) [3]. Його особливість полягає в мінімальній кількості радіоелементів та легкості в реалізації.

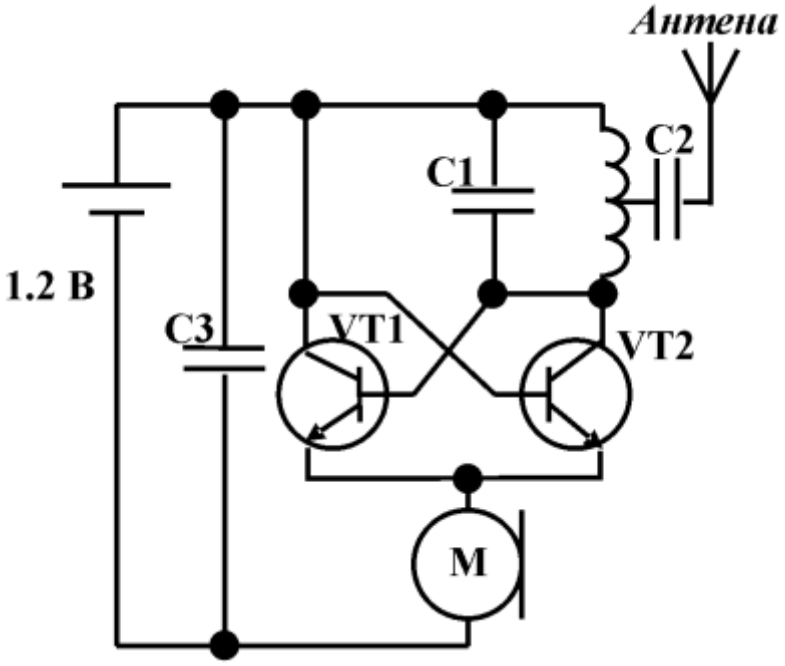


Рисунок 1.7. – Схема закладного пристрою №1

У ЗП_1, використовуються лише два транзистори типу КТ368, які регулюють частоту. Для мікрофону використовується стандартний гарнітурний мікрофон мобільного телефону, антена складається з мідного дроту, довжина якої складає 30 см, що намотана на гелеву ручку для зменшення розміру. Через дуже низький струм споживання, який складає всього 0,2 мА, для вимикання живлення не потрібен вимикач. Будучи настільки енергоощадним, пристрій може працювати на одній батарейці до місяця. Його головний недолік полягає у тому, що радіус прослуховування складає лише 10 метрів, але цього достатньо для прослуховування всього, що відбувається в сусідній кімнаті.

На рис.1.8. наведено схему побудови другого пристрою ЗП 2 [5]. Його особливість – значно менші розміри, порівняно із ЗП 1. Це відбувається завдяки використанню мініатюрних гальванічних елементів.

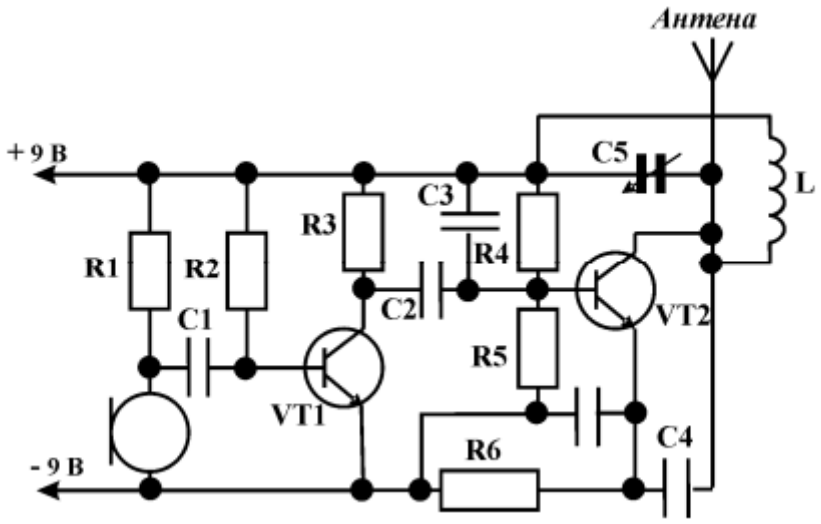


Рисунок 1.8 – Схема закладного пристрою №2

Схема ЗП 2 складається з мікрофонного підсилювача та передавача, що дозволяє досягти великої чутливості. Для мікрофона можна використовувати будь-який електронний мікрофон, включаючи цифровий мікрофон від мобільного телефона. Хоча чутливість мікрофона не є великою, у схемі використовується каскад підсилення мікрофона на одному транзисторі (S9014), хоча можна використовувати й інші транзистори малої потужності, такі як КТ315, КТ368, КТ3102, С9014/9018. Результати експериментальних випробувань закладних пристроїв за найбільш важливими характеристиками наведені в таблиці 1.1[6].

Таблиця 1.1 – Характеристики сконструйованих закладних пристроїв

| | Відстань прослухо-вування, м | | Часто-та, Гц | Струм спо-живання, мА | Жив-лен-ня, В | Час ро-боти, год | Чутли-вість мік-рофона, м | Габари-ти | Ва-га, г |
|---|---|---|---|---|---|---|---|---|---|
| | без шуму | зі шумом | | | | | | | |
| ЗП 1 | 2 | 5 | 99,6 | 0,2 | 1,5 | 360 | 1 | 6×3,5×2 | 40 |
| ЗП 2 | 50 | 60 | 103,4 | 30 | 9 | 6 | 5 | 4×2×1 | 14 |

Для вибору ефективного закладного пристрою необхідно провести порівняльний аналіз характеристик розроблених пристроїв. Після тестування ЗП 2 показав хороші результати, здатний прослуховувати на відстані більше 50 м без шуму та більше 60 м з незначним шумом. У порівнянні з ним, ЗП 1 значно відстає з цієї характеристики, здатний прослуховувати не більше 5 м.

Однак його дальність достатня для прослуховування сусідніх кімнат, а також цей пристрій важко виявити індикаторами поля, оскільки він випромінює слабкий сигнал. Частота передачі закладних пристроїв не відіграє великої ролі в прослуховуванні. Головне, щоб частота потрапляла в

діапазон FM приймача та не збігалася з частотою радіостанцій. Для ускладнення відстеження закладного пристрою підбирають частоту, яка наближена до частоти, на якій працюють інші пристрої, наприклад, Wi-Fi, мобільний телефон тощо. Час роботи закладних пристроїв залежить від їх споживання струму. ЗП 1 має дуже низьке споживання струму, тому може працювати значно довше. У порівнянні з ЗП 2, ЗП 1 має довший час роботи через мале споживання енергії. Живлення також впливає на розмір пристроїв - завдяки малому споживанню струму, ЗП 1 може використовувати менші батарейки, що знижує його розмір. На одному гальванічному елементі типу ААА, ЗП 1 може працювати близько місяця. ЗП 2 вимагає більше електроенергії через більшу кількість радіоелементів, тому має значно менший час роботи - близько 6 годин без заміни джерела живлення. Однією з найбільш важливих характеристик будь-якого закладного пристрою є його чутливість, оскільки вона визначає, наскільки чітко можна почути розмову. Чутливість ЗП 1 дорівнює всього одному метру, що є дуже низькою відстанню, тому пристрій повинен знаходитися поруч з розмовником, наприклад, на робочому столі, замаскований під звичайним предметом. Чутливість ЗП 2 достатня для підслуховування всієї кімнати.

Переваги і недоліки досліджуваних закладних пристроїв описано в табл. 1.2.[7]

Таблиця 1.2. Переваги та недоліки досліджуваних закладних пристроїв

| Переваги | Недоліки |
|---|---|
| ЗП 1 | |
| Низький споживаний струм і напруга живлення, довгий час автономної роботи і не випромінює радіохвиль, тому не перешкоджає роботі радіостанцій. Крім того, він має найменшу собівартість серед аналогів. | Закладний пристрій має обмежену чутливість мікрофона і може слухати лише на відносно близькій відстані, а також має досить великий розмір. |
| ЗП 2 | |
| Переваги | Недоліки |
| Значна зона прослуховування, компактні розміри, легкість та доступна ціна. | Частота близька до радіостанцій, високий струм споживання та напруга живлення, низька чутливість мікрофона та обмежений час роботи. |

Висновок до Розділу 1

У даному розділі розглянуто важливі аспекти, пов'язані з закладними пристроями та їх впливом на безпеку інформаційної діяльності. У розділі була представлена класифікація закладних пристроїв, що включає різноманітні типи пристроїв залежно від їх конструкції, розмірів, маскування та можливостей перехоплення інформації. Від маленьких прихованих мікрофонів і камер, які можуть бути встановлені у особистих речах, до більших пристроїв, розташованих у будівлях чи приміщеннях, класифікація допомагає краще розуміти різноманітність цих пристроїв та їх потенційні можливості.

З вивчення теоретичних аспектів виявлення закладних пристроїв можна зробити кілька висновків:

Закладні пристрої можуть бути встановлені в різних місцях та мати різні форми, що робить їх виявлення важким завданням.

- Для ефективного виявлення закладних пристроїв необхідно використовувати спеціальні прилади, такі як металошукачі, радіочастотні детектори та інші.

- Важливо знати особливості роботи закладних пристроїв, щоб можна було виявити їх присутність. Наприклад, деякі закладні пристрої можуть випромінювати радіосигнали, тоді як інші можуть реагувати на магнітні поля.

- При виявленні закладних пристроїв необхідно враховувати специфіку конкретної ситуації та можливість впливу зовнішніх факторів, таких як електромагнітні поля чи інші джерела перешкод.

Основними завданнями робіт з пошуку закладних пристроїв є виявлення, ідентифікація і локалізація закладних пристроїв. Перевірка проводиться їх використанням технічних засобів згідно з інструкціями щодо їх експлуатації, а також візуально.

У зв'язку з швидким розвитком технологій, закладні пристрої можуть мати більш високу технічну складність та прихованість, що потребує постійного оновлення методів та приладів для їх виявлення.

Також знання теоретичних основ закладних пристроїв, їх сутності і класифікації допомагає зрозуміти загрози, пов'язані з несанкціонованим зніманням інформації. Це важлива інформація для розробки та застосування заходів захисту, виявлення та запобігання використанню закладних пристроїв.

# 2. ЗАСОБИ ТА МЕТОДИ ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ

Роботи з виявлення закладних пристроїв проводяться з метою виявлення технічних каналів витоку інформації, що утворені за рахунок впроваджених технічних засобів негласного отримання інформації.

Основними завданнями робіт з пошуку закладних пристроїв є виявлення, ідентифікація і локалізація ЗП.

Перевірка проводиться із використанням технічних засобів згідно з інструкціями щодо їх експлуатації, а також візуально.

## 2.1. Огляд методів проведення пошукових заходів

Однією з важливих задач забезпечення конфіденційності та безпеки приміщень та об'єктів інформаційної діяльності є виявлення закладних пристроїв, які можуть бути використані для несанкціонованого отримання акустичної інформації. Для досягнення цієї мети існує ряд методів та приладів, які використовуються при проведенні пошукових заходів.

Вони включають в себе візуальний огляд, використання радіочастотних сканерів, акустичних аналізаторів, інфрачервоні сканери та детектори проводів [8]. Кожен з цих методів має свої особливості та можливості виявлення закладних пристроїв.

Вивчення та використання цих методів допоможе забезпечити ефективну облік та виявлення закладних пристроїв, що забезпечить захист конфіденційності та безпеки інформаційних ресурсів. Надалі будуть розглянуті деталі кожного з цих методів, їх принципи дії та можливості виявлення закладних пристроїв.

Методи проведення пошукових заходів для виявлення закладних пристроїв:

Візуальний огляд: Початковий етап пошукових заходів, який включає детальний огляд приміщень, меблів, електронних пристроїв і інших об'єктів з метою виявлення видимих ознак наявності закладних пристроїв. Це може включати перевірку наявності незвичайних деталей, кабелів, камер або мікрофонів.

Використання радіочастотних сканерів: Ці пристрої призначені для виявлення радіочастотних сигналів, які можуть бути випромінені закладними пристроями. Вони сканують радіочастотний спектр і сповіщають про наявність сигналів, що відрізняються від нормальних.

Використання акустичних аналізаторів: Ці пристрої виявляють незвичайні акустичні сигнали або звуки, що можуть свідчити про наявність закладних пристроїв. Вони можуть виявляти непередбачувані звукові сигнали, зміни в рівні шуму або частотному спектрі, які можуть бути пов'язані з прихованими пристроями.

Інфрачервоні сканери: ці пристрої виявляють теплове випромінювання, яке може бути випромінене закладними пристроями, такими як мікрокамери. Вони можуть виявити незвичайні джерела тепла або приховані пристрої, які можуть бути використані для несанкціонованого збору інформації.

Детектори проводів: Ці пристрої використовуються для виявлення прихованих кабелів або проводів, які можуть бути пов'язані з закладними пристроями. Вони можуть використовувати магнітні поля або імпульсну технологію для виявлення наявності проводів.

Візуальний огляд є одним з методів проведення пошукових заходів для виявлення закладних пристроїв. Цей метод базується на детальному огляді приміщень, об'єктів та електронних пристроїв з метою виявлення видимих ознак наявності закладних пристроїв.

Під час візуального огляду виконуються такі дії:

Огляд приміщень: Перевірка меблів, стін, стелі, підлоги та інших елементів приміщень на наявність незвичайних деталей, відкритих входів або прихованих пристроїв.

Електронні пристрої: Огляд усіх електронних пристроїв, таких як комп'ютери, телефони, роутери і т.д. Перевірка наявності незвичайних кабелів, непередбачуваних портів або змін у їх зовнішньому вигляді.

Розетки та світильники: Перевірка розеток, світильників та інших електричних точок на наявність додаткових елементів або змін, які можуть бути пов'язані з закладними пристроями.

Звуки та несподівані шуми: Слуховий аналіз приміщень з метою виявлення непередбачуваних звуків або несподіваних шумів, які можуть бути пов'язані з присутністю закладних пристроїв.

Використання технічних засобів: Використання спеціальних технічних пристроїв, таких як ендоскопи, мінікамери або теплові камери, для огляду складних або важкодоступних місць.

Візуальний огляд є важливим етапом виявлення закладних пристроїв, оскільки дозволяє звернути увагу на очевидні ознаки їх наявності. Однак, варто пам'ятати, що деякі закладні пристрої можуть бути досить хитро прихованими і вимагати використання інших спеціальних методів та приладів для виявлення.  Використання радіочастотних сканерів є одним із

методів пошуку закладних пристроїв. Ці сканери призначені для виявлення радіочастотних сигналів, які можуть бути випромінюваними закладними пристроями. Вони прослуховують електромагнітний спектр на наявність незвичайних сигналів у різних діапазонах частот. Під час використання радіочастотних сканерів проводиться наступна процедура [7]:

Сканування частот: Сканер прослуховує електромагнітний спектр у визначених діапазонах частот. Він реєструє присутність сигналів у цих діапазонах.

Виявлення незвичайних сигналів: Радіочастотний сканер аналізує знайдені сигнали та шукає ті, які відрізняються від типових сигналів, що можуть бути випромінюваними електронними пристроями.

Ідентифікація потенційних закладних пристроїв: Після виявлення незвичайних сигналів сканер аналізує їх характеристики та спробує ідентифікувати можливі закладні пристрої, засновуючись на відомих сигнатурах або характеристиках відомих пристроїв.

Використання радіочастотних сканерів є ефективним способом виявлення закладних пристроїв, особливо тих, які випромінюють радіочастотні сигнали.

Вони дозволяють оперативно виявити можливі загрози та забезпечити безпеку приміщень та об'єктів інформаційної діяльності.

Використання акустичних аналізаторів є ще одним методом пошуку закладних пристроїв. Ці аналізатори призначені для виявлення незвичайних звуків або акустичних сигналів, які можуть бути пов'язані з наявністю закладних пристроїв.

Процес використання акустичних аналізаторів для пошуку закладних пристроїв включає наступні кроки:

Збір акустичних даних: Акустичний аналізатор реєструє звуки, що присутні в приміщенні або на об'єкті. Він може записувати звукові сигнали або прослуховувати їх в реальному часі.

Аналіз звуків: Акустичний аналізатор аналізує зібрані акустичні дані з метою виявлення незвичайних звуків або акустичних сигналів, які можуть свідчити про наявність закладних пристроїв. Це можуть бути непередбачувані шуми, шурхоти, писк або будь-які інші незвичайні звуки.

Ідентифікація потенційних закладних пристроїв: Після виявлення незвичайних звуків акустичний аналізатор спробує ідентифікувати можливі закладні пристрої, враховуючи їх характеристики та відмінності від нормальних звуків, що очікуються.

Використання акустичних аналізаторів допомагає виявити закладні пристрої, основані на їх акустичних сигналах або звуках [8]. Цей метод є важливим для забезпечення конфіденційності та безпеки приміщень та об'єктів інформаційної діяльності, оскільки дозволяє виявити непередбачені пристрої, які можуть бути використані для незаконного отримання акустичної інформації. Інфрачервоні сканери є ще одним методом пошуку закладних пристроїв. Вони використовують інфрачервоне випромінювання для виявлення теплових змін або випромінювання, яке може бути пов'язане з наявністю закладних пристроїв. Основний принцип роботи інфрачервоних сканерів при пошуку закладних пристроїв наступний:

Збір інфрачервоних даних: Інфрачервоний сканер реєструє інфрачервоне випромінювання, що походить з поверхонь приміщення або об'єкта. Він виявляє теплові зміни або випромінювання, які можуть бути незвичайними.

Аналіз інфрачервоних даних: Інфрачервоний сканер аналізує зібрані інфрачервоні дані з метою виявлення зон зі збільшеною тепловою активністю або випромінюванням, які можуть вказувати на наявність закладних пристроїв.

Виявлення потенційних закладних пристроїв: Після аналізу інфрачервоних даних сканер спробує виявити можливі закладні пристрої, засновуючись на зоні зі збільшеною тепловою активністю або незвичайному випромінюванні.

Використання інфрачервоних сканерів дозволяє ефективно виявляти закладні пристрої, основані на їх теплових змінах або випромінюванні. Цей метод є корисним для забезпечення безпеки та конфіденційності приміщень та об'єктів інформаційної діяльності, оскільки дозволяє виявити приховані пристрої, які можуть використовуватися для несанкціонованого збирання акустичної інформації.

Детектори проводів є ще одним методом пошуку закладних пристроїв. Ці пристрої призначені для виявлення прихованих кабелів або проводів, які можуть бути пов'язані з закладними пристроями.

Основні принципи роботи детекторів проводів при пошуку закладних пристроїв наступні:

Використання магнітних полів: деякі детектори проводів використовують магнітні поля для виявлення проводів. Вони генерують магнітне поле, а потім спостерігають за будь-якими змінами в полі, що можуть виникнути внаслідок присутності прихованих проводів.

Використання імпульсної технології [9]: Інші детектори проводів можуть використовувати імпульсну технологію для виявлення проводів. Вони генерують короткі електричні імпульси, які відбиваються від проводів і повертаються до приладу. Прилад аналізує ці відбиті сигнали, що дозволяє виявити наявність проводів.

Перевірка розеток та світильників: Деякі детектори проводів можуть також перевіряти розетки та світильники на наявність прихованих проводів. Вони можуть виявити проводи, які підключені до розеток або світильників без дозволу.

Використання детекторів проводів дозволяє виявити наявність прихованих проводів, що можуть бути пов'язані з закладними пристроями.

Цей метод є важливим для забезпечення конфіденційності та безпеки приміщень та об'єктів інформаційної діяльності, оскільки дозволяє виявити потенційно шкідливі підключення.

## 2.2. Обладнання для виявлення закладних пристроїв

ПАК DigiScan є автоматизованим пошуковим програмно-апаратним комплексом, який складається з портативного комп'ютера, програмного забезпечення DigiScan-2000 та скануючого приймача AR 3000 A (рис. 2.1.). Його головна мета полягає в виявленні радіосигналів з закладних пристроїв шляхом визначення їх частоти, смуги пропускання, дослідження сигналів за допомогою кореляційних функцій, амплітудних і спектральних характеристик, виявлення гармонік сигналу, класифікації виявлених сигналів (дружніх або небезпечних) та занесення результатів до бази даних.


Рисунок 2.1 – ПАК DigiScan

Комплекс працює під керуванням універсального пошукового програмного забезпечення DigiScan-2000, яке впроваджує передові методи виявлення, зокрема:

Динамічний поріг: використовується для виявлення сигналів, які перевищують заданий рівень шуму.

Вимір смуги сигналу: дозволяє визначити ширину смуги, в якій присутній сигнал.

Перевірка наявності гармонік сигналу: дозволяє виявити наявність гармонійних складових у сигналі.

Пасивна кореляція: застосовується для порівняння отриманих сигналів з шаблонами та виявлення відповідностей.

Пасивна кореляція з зондуванням: використовується для виявлення сигналів з визначеними параметрами шаблону.

Активна амплітудна кореляція: дозволяє порівнювати амплітуди отриманих сигналів з встановленими значеннями.

Активна спектральна кореляція: використовується для порівняння спектральних характеристик сигналів та виявлення відповідностей.

Відбір сигналів по сумарному рівню небезпеки: використовується для класифікації сигналів на основі загального рівня небезпеки.

Ці методи дозволяють ефективно виявляти закладні пристрої та класифікувати їх рівень небезпеки. DigiScan-2000 має два режими роботи: режим пошуку та ручний режим. Після налаштування параметрів оператор може включити режим автоматичного сканування в заданому діапазоні. У режимі пошуку програма автоматично сканує встановлений діапазон, виявляє сигнали, що перевищують заданий поріг, та виконує тести, встановлені оператором. Якщо знайдено небезпечний сигнал, програма повідомляє оператора за допомогою звукового сигналу або виводить повідомлення на екран, а також розпочинає запис звукового зразка. Сигнал заноситься до розділу бази даних під назвою "Небезпечні". Всі інші сигнали, які не є небезпечними, заносяться до розділу бази даних "Нові". У розділ "Все" потрапляють всі сигнали, незалежно від їх небезпечності. Після кількох сканувань усього діапазону оператор зупиняє пошук та переходить в ручний режим.

У ручному режимі оператор має можливість проаналізувати результати пошуку або самостійно шукати нові сигнали. Для цього він поступово просувається по діапазону і проводить тести над виявленими сигналами. В ручному режимі також застосовується поріг, який оператор встановлює.

Оператор може переглядати осцилограму та спектр сигналів на дисплеях "Амплітуда" і "Спектр" (рис. 2.2) [8].


Рисунок 2.2 – Блок-схема алгоритму пошуку

Прилад ST 031 "Піранья" є багатофункціональним пошуковим засобом, призначеним для виявлення та локалізації спеціальних технічних засобів негласного знімання інформації, виявлення каналів витоку інформації, які можуть бути природними або штучно створеними, а також для контролю якості захисту інформації (рис. 2.3). Він забезпечує розв'язання контрольно-пошукових завдань в межах приміщення або в його непрямій близькості.

Рисунок 2.3 – ST 031 "Піранья"

У режимі високочастотного детектора-частотоміра прилад працює в наступний спосіб. Він приймає радіосигнали в діапазоні від 30 до 2500 МГц у ближній зоні, що охоплює об'єкт спеціальних робіт. Прилад детектує ці сигнали і виводить їх для слухового контролю та аналізу у вигляді змінних тональних посилок (клацань) або в явній формі фонограм. Їх можна прослуховувати як через вбудований динамік, так і через навушники.

У цьому режимі прилад постійно приймає й детектує найпотужніший радіосигнал у робочому діапазоні в конкретний момент часу на фоні реального завадного середовища. Рівень цього сигналу порівнюється з встановленим порогом детектора і відображається на дворядковому індикаторі з 40- сегментною шкалою на верхній частині рідкокристалічного дисплея.

У приладі використовуються дві шкали, і вони мають наступні відмінності: верхня шкала відображає середнє значення продетектованого сигналу, тоді як нижня шкала відображає його пікові значення. Відповідно, на верхньому рядку переважатимуть сигнали з постійною частотою без модуляції або частотно-модульовані сигнали, а на нижньому рядку будуть ближчі до імпульсних сигнали, наприклад, сигнали з амплітудною і імпульсною модуляцією. Якщо індикація відображається на обох шкалах, це означає, що сигнал має змішаний характер на вході детектора, наприклад, як телевізійний сигнал.

У випадку, коли прилад впевнено отримує сигнал із відомими параметрами, на дисплеї відображається ідентифікаційний напис сигналу під цифровою шкалою рівня сигналу. Зокрема, можлива індикація виявлення сигналів стандартів GSM (напис "GSM") та DECT (напис "DECT").

Залежно від умов і мети контрольно-пошукових робіт, оператор може вибрати й установити потрібний поріг детектора, який буде найбільш оптимальним.

Також на дисплеї одночасно відображаються поточні значення частоти прийнятого радіосигналу і визначається його найстабільніше значення для сигналів із постійною частотою. Ці значення представлені на екрані дисплея у явному вигляді.

Для якісної оцінки ступеня змінності частоти радіосигналу використовується спеціальний обчислювальний алгоритм, результати якого відображаються на екрані дисплея у вигляді тонкої горизонтальної лінії, яка динамічно змінюється в довжині над цифровими символами поточних значень частоти. Довжина цієї лінії пропорційна похідній від частоти прийнятого сигналу.

Детектор поля PROTECT 1203 розроблений для виявлення активних закладних пристроїв (рис. 2.4). Він призначений для перевірки приміщень, транспортних засобів, предметів інтер'єру і навіть людей з метою виявлення прихованих передавачів. PROTECT 1203 здатний працювати як у видимому, так і в прихованому режимі за допомогою вбудованого вібратора.

Рисунок 2.4 – Детектор поля PROTECT 1203

Цей прилад здатний виявляти працюючі мобільні телефони у співрозмовника, що дозволяє виявити наявність такого пристрою. Він може бути успішно застосований для забезпечення безпеки та виявлення незаконної або небажаної використовування мобільних пристроїв.

## 2.3. Аналізатор спектра

Згідно з "Класифікатором засобів технічного захисту інформації" (НД ТЗІ 1.5-002-2012), аналізатор спектру належить до класу засобів ТЗІ, який визначений як "Засоби аналізу радіочастотного спектра". Аналізатор спектра - це пристрій, що дозволяє вимірювати та візуалізувати спектр сигналу. Сам спектр сигналу являє собою набір синусоїдальних хвиль в певний момент часу і відображає розподіл енергії сигналу по частотах. Аналізатор спектра видає амплітудно-частотну характеристику (АЧХ) сигналу.

Аналізатор спектра є потужним інструментом, що допомагає виявити закладні пристрої шляхом аналізу радіочастотного спектра. Він прослуховує і записує радіочастотний діапазон і відображає його у вигляді графіка, де по горизонтальній осі відображається частота, а по вертикальній – сила сигналу.

Аналізатор спектра може допомогти виявити різні типи закладних пристроїв. Деякі з таких пристроїв включають:

Приховані мікрофони: Аналізатор спектра може виявити радіочастотні сигнали, що випромінюються прихованими мікрофонами. Це можуть бути пристрої, встановлені у приміщенні або в різних предметах, таких як меблі, розетки, підвісні стелі тощо.

Приховані камери: Аналізатор спектра може виявити радіочастотні сигнали, що випромінюються бездротовими камерами, які використовуються для нелегального відеоспостереження. Ці камери можуть бути приховані в різних предметах, які зазвичай знаходяться у приміщенні, наприклад, розетки, розсіювачі світла, димоходи тощо.

GPS-трекери: Аналізатор спектра може виявити радіочастотні сигнали, що випромінюються GPS-трекерами, які використовуються для стеження за місцезнаходженням транспортних засобів або осіб. Ці пристрої можуть бути приховані в автомобілях, рюкзаках, одязі тощо.

Основні принципи роботи

Сигнал надходить безпосередньо на вхід аналізатора спектра. Він також може надходити через спеціальний кабель або вловлювати приймальні антеною. Далі цей сигнал обробляється, і інформація про нього виводиться на дисплей у вигляді частотного спектру.

Зазвичай для візуалізації використовується дисплей з каліброваною сіткою. Цей дисплей має вертикальну шкалу, яка показує амплітуду кожного компонента сигналу, і горизонтальну шкалу, яка представляє смугу частот. Однак, сучасні пристрої також мають можливість зберігати спектрограму сигналу безпосередньо в своїй вбудованій пам'яті. Це дозволяє зберігати і аналізувати спектральні характеристики сигналу в майбутньому, а також проводити порівняння, виявляти патерни або відстежувати зміни в спектрі протягом часу.

Збереження спектрограми у вбудованій пам'яті також дозволяє здійснювати функцію історії та архівування, що є корисним для подальшого аналізу та обробки сигналу.

За принципом роботи аналізатори спектра поділяють на:

*Аналізатори спектру послідовного типу*

Дані аналізатори спектра працюють на базі супергетеродинів що автоматично перестоюються. Це такий тип радіоприймачів, які перетворюють сигнал що надходить, в сигнал фіксованої проміжної частоти та в подальшому посилюють її. Аналізатор спектра здійснює сканування частотної смуги з подальшим оцифровуванням даних.

При цьому компоненти спектра виділяються і аналізуються по черзі (послідовно). Такі аналізатори є найбільш простими в апаратній відношенні, однак, менш ефективними. Вони підходять тільки для аналізу періодичних сигналів. До їх переваг можна віднести більш широке вимір частотного діапазону.

*Аналізатори спектру паралельного типу*

Дані пристрої виконують аналіз, генеруючи еквівалент сигналу і обчислюючи спектр на основі алгоритмів швидкого перетворення Фур'є. Такі аналізатори мають набір резонаторів, налаштованих на певну частоту.

Аналізатори спектра паралельного типу відрізняються оперативною і ефективною роботою і здатні аналізувати імпульсні і одноразові сигнали. Їх недоліком є складність з точки зору апаратного забезпечення. Основні характеристики Аналізатори спектра мають наступні характеристики:

Частотний діапазон. Ця характеристика задає діапазон, в межах якого виконується аналіз спектра сигналу. Діапазон частот може мати під-діапазони.

Рівень власних шумів. Здається поріг, нижче якого прилад не сприймає шуми і сигнали.

Роздільна здатність. Ця характеристика являє собою мінімальний інтервал частот, при якому сусідні компоненти спектра можуть бути виділені і виміряні.

Час аналізу. Вказує на час, протягом якого можна провести аналіз сигналу в певному частотному діапазоні.

Похибка по частоті. Вказує на точність, з якою може бути визначений інтервал частот між компонентами спектра.

Похибка по амплітуді. Вказує на точність, з якою визначається амплітуда в залежності від інструментарію аналізатора.

Аналізатори спектра з вбудованими мікропроцесорами представляють собою сучасні пристрої, які здатні аналізувати різні параметри сигналів. Вони призначені для візуалізації та детального аналізу спектру сигналу. Ці пристрої також можуть бути інтегровані з іншими вимірювальними приладами та зовнішньою ЕОМ за допомогою відповідного інтерфейсу, що дозволяє включати їх до автоматизованих вимірювальних систем.

Прикладом аналізатору спектру є Signal Hound BB60C (рис. 2.5).

Signal Hound BB60C - це аналізатор спектра реального часу, який також є реєстратором високочастотних сигналів, є новим доповненням до лінійки продуктів Signal Hound. Завдяки використанню інтерфейсу USB 3.0, аналізатор спектру BB60C здійснює високошвидкісну передачу оцифрованого сигналу зі швидкістю 140 Мб/с. 14-бітний аналогово-цифровий перетворювач (АЦП) пристрою працює зі швидкістю 80 мільйонів вибірок за секунду, що забезпечує миттєву смугу 27 МГц.

Цей аналізатор спектра працює на основі власного прикладного програмного інтерфейсу (API), який забезпечує швидке виконання

перетворення Фур'є зі швидкістю до 1,2 мільйонів операцій в секунду. Через API спектральні дані передаються в реальному часі до графічного інтерфейсу користувача (GUI), який може бути реалізований з відкритим вихідним кодом або відповідним додатком.

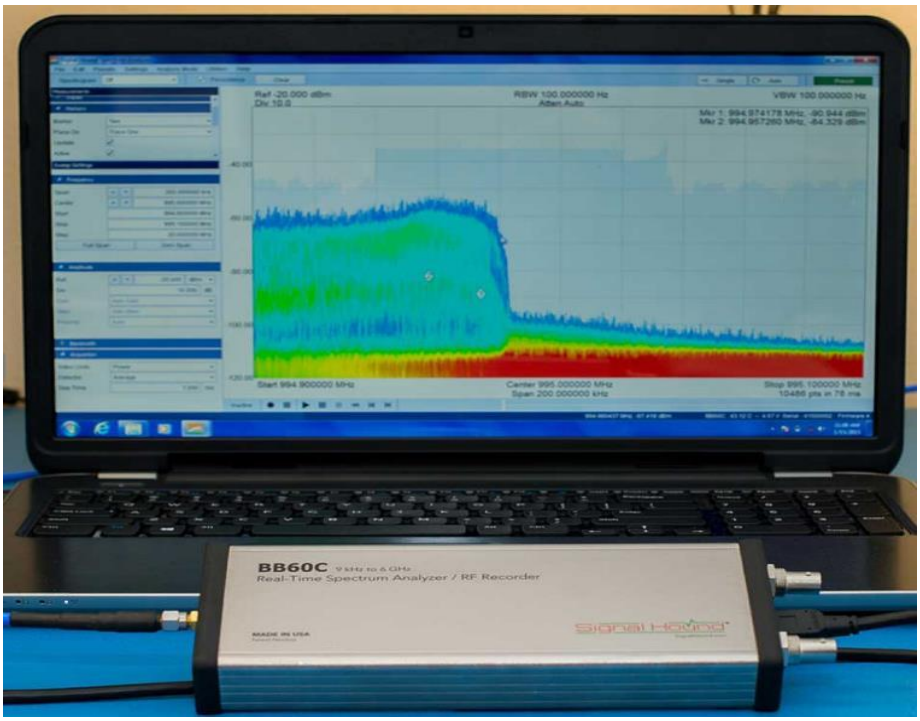


Рисунок 2.5 – Аналізатор спектра Signal Hound BB60C

Програмне забезпечення аналізатора дозволяє відображати спектр у двовимірному і тривимірному режимах. Також передбачений режим відображення спектра в часовій області з використанням насиченості, що зменшується. Цей режим зазвичай дозволяє легше відслідковувати окремі артефакти у спектрі сигналу.

Аналізатор РЧ-спектру BB60C працює в реальному часі і передає 140 МБ/с оцифрованого РЧ-сигналу на комп'ютер за допомогою USB 3.0. Він забезпечує миттєву пропускну здатність 27 МГц і швидкість розгортання 24 ГГц/с.

Аналізатор спектра BB60C має значні покращення у порівнянні з попередніми версіями. Він має покращений динамічний діапазон без паразитних складових (SFDR) на 20 дБ, згладження мінімального рівня шуму та смугових переходів більше ніж на 8 дБ. Також, робочий температурний діапазон був розширений від -40ºC до +65ºC, у порівнянні з попередньою моделлю, яка працювала від 0 ºC до +50 ºC. Конструкція BB60C була протестована і продемонструвала бездоганну роботу з високою точністю під

час 3-годинного випробування при температурі -40ºС, а також під час 24-годинного випробування при високій температурі +65ºС.

Ще одним досить гарним прикладом є аналізатора спектру є прилад RSA306B (рис. 2.6), він дозволяє виконувати аналіз спектру і глибокий аналіз імпульсних сигналів. Аналіз, запис і відтворення даних виконується на ПК, планшеті або ноутбуці. Робота комп'ютера окремо від системи захоплення дозволяє легко нарощувати потужність обробки і мінімізувати проблеми управління вимірювальною системою.

Tektronix RSA306 – компактний, портативний аналізатор спектру з малим енергоспоживанням. Він може працювати з ноутбуками і планшетами, оснащеними портом USB 3.0, і отримує живлення через цей інтерфейс (менше 4,5 Вт). Обробку, відображення і зберігання даних виконує комп'ютер, що дозволило зменшити розміри самого аналізатора. Однак малий розмір і мале енергоспоживання накладають свої обмеження на радіочастотні характеристики.

RSA306 є аналізатором спектру реального часу, що означає, що він здатен захоплювати сигнал за допомогою високошвидкісного дискретизатора і безперервно оновлювати спектр у зазначеній смузі захоплення шляхом використання перетворення Фур'є. Широкі смуги огляду реалізуються шляхом зміни частоти гетеродина та перемикання смуги приладу у вибраний частотний діапазон.

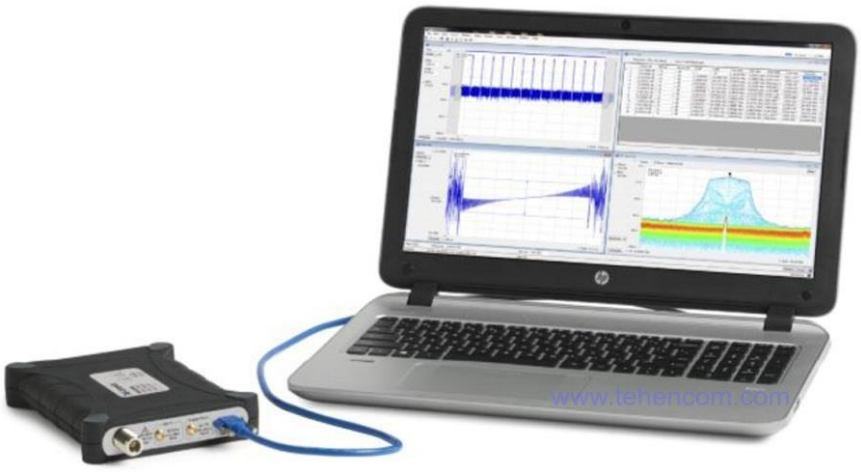


Рисунок 2.6 – Аналізатор спектру RSA306B

Можливості аналізатора спектру RSA306B:

- всеохоплюючий аналіз спектру з використанням ПЗ TektronixSignalVu-PC;

- 27 стандартних вимірювань для аналізу спектру і імпульсних сигналів;
- опції для пеленгації, аналізу модуляції, аналізу сигналів певних стандартів, імпульсних вимірювань і вимірювань часу встановлення частоти;
- відображення спектру / спектрограми в режимі реального часу для швидкого пошуку перехідних процесів і джерел перешкод;
- стандартний інтерфейс програмування для використання в середовищі Microsoft Windows.

Особливості аналізатора спектра RSA306B.

Аналізатор спектру RSA306 має компактний розмір та економне споживання енергії, що дозволяє йому отримувати живлення від порту USB 3.0. Однак, такий тип живлення накладає обмеження на конструкцію пристрою. При підключенні до порту USB, аналізатор споживає не більше 100 мА, а після установки з'єднання - не більше 900 мА при напрузі 5 В (з урахуванням падіння напруги на кабелі, що може знизитися до 4,5 В). Таким чином, пристрій має споживати не більше 4 Вт у всьому робочому діапазоні температур, який для RSA306 становить від -10 до +55 °C. З огляду на те, що робочий струм аналізатора RSA306 збільшується зі зростанням температури, для відповідності вимогам щодо живлення через порт USB 3.0, споживання струму пристрою при кімнатній температурі повинно бути менше на приблизно 30 мА.

Для порівняння: типова споживана потужність настільного аналізатора спектру становить від 100 до 400 Вт.

Цифрові схеми RSA306 (АЦП, ПЛІС, USB 3.0, ПЧ (підсилювач частоти), задаючий генератор) споживають приблизно 0,75 Вт з урахуванням втрат імпульсних перетворювачів живлення. Інша частина, включаючи РЧ-тракт, споживає приблизно 3,1 Вт.

РЧ-тракт (рис. 2.7) складається з вхідного атенюатора, який перемикається на зовнішній підсилювач, ступеневого атенюатора тонкого налаштування і додаткового каскаду з перемикаючим підсиленням (який налаштовується автоматично в залежності від встановленого опорного рівня, що дозволяє знизити шум і спотворення), за яким слідує один з семи аналогових попередніх фільтрів, який вибирається в залежності від вхідної частоти.

Потім сигнал надходить на перший змішувач, де перетворюється в одну з проміжних частот - 1190 МГц або 2440 МГц, яка обирається автоматично так, щоб мінімізувати рівень паразитних складових.

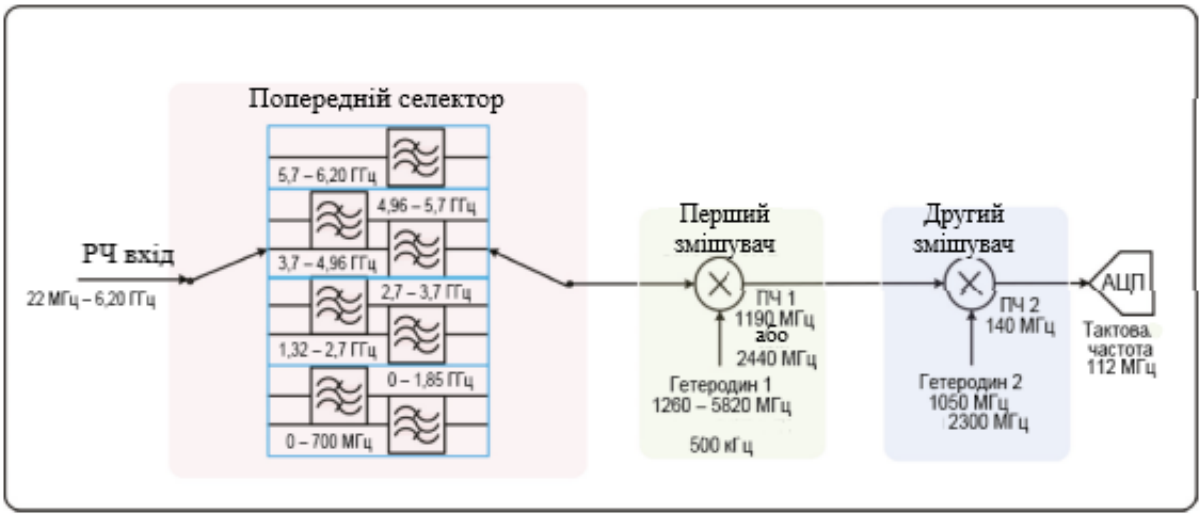


Рисунок 2.7 – Спрощена схема РЧ тракту аналізатора RSA306

Після фільтрації та посилення сигнал надходить на другий змішувач, де його частота знижується до другої проміжної частоти 140 МГц. Ця РЧ посилюється і пропускається через смуговий фільтр, 42 МГц ПАХ (на поверхневих акустичних хвилях), за яким слідує LC-фільтр сьомого порядку, і з виходу цього фільтра сигнал надходить на АЦП.

Характеристики РЧ-тракта сильно залежать від лінійності компонентів, яка перешкоджає виникненню паразитних складових в процесі посилення і змішання, а лінійність обох цих процесів, як правило, збільшується з ростом потужності. Тому для аналізатора ретельно відбираються компоненти, що володіють високою лінійністю і мінімальним шумом при малій потужності.

Фільтрація паразитних складових (гармонік і продуктів змішання, що виникають в результаті взаємодії вхідного сигналу, сигналів гетеродинів і тактових частот) дозволяє отримати вільний від паразитних складових динамічний діапазон з нижньою межею приблизно на 50 дБн нижче діапазону вхідного РЧ сигналу.

Для зменшення розміру і зниження ціни прилад зібраний на одній друкованій платі з мініатюрними екранами, яка встановлена в цілісний корпус з екструдованого профілю. На багатьох частотах динамічний діапазон досягає значення -65 дбн; проте основним чинником, що обмежує рівень паразитних складових, є рівень РЧ розв'язки між внутрішніми ланцюгами. Іншим важливим елементом конструкції є фільтри, які використовуються в тракті РЧ.

Недорогі ПАХ-фільтри з широкою смугою пропускання, малими пульсаціями та хорошим подавленням за межами смуги мають зазвичай і великі втрати в смузі пропускання. Це робить необхідністю додаткове

посилення, яке дає добавку споживаної потужності і вносить додаткові нелінійні спотворення.

Замість багатоконтурного синтезатора частоти в аналізаторі застосовані низьковольтні інтегральні синтезатори, що мають малі фазові шуми, що дозволило скоротити як розміри, так і вартість пристрою. Ці синтезатори тактуються високочастотним кварцовим генератором з малим джитером, який використовується і для тактування АЦП, що дозволяє отримати прийнятний фазовий шум, достатній для отримання EVM порядку 1%.

Динамічний діапазон і значення фазового шуму обмежені через обмеження по споживаній потужності від порту USB 3.0. Проте, комп'ютерні стандарти постійно розвиваються, і в недалекому майбутньому інтерфейс USB 3.1 обіцяє підвищені швидкості передачі даних і додаткову потужність.

А тим часом такі настільні прилади, як Tektronix RSA5k тта RSA6k, мають кращі РЧ-характеристики, оскільки споживана потужність для них – не проблема, і управляються вони тією ж програмою з тим ж інтерфейсом користувача.

На ринку виробників аналізаторів спектра спостерігаються певні тенденції. Деякі наведено нижче:

Зростання виробництва в Китаї. Китай став однією з провідних країн у виробництві аналізаторів спектра. Велика кількість китайських виробників пропонує широкий спектр продуктів з різними функціями та ціновими діапазонами.

Інновації та покращення продуктивності. Виробники аналізаторів спектра постійно прагнуть вдосконалювати свої продукти. Це охоплює покращення роздільної здатності, чутливості, швидкості вимірювання та інших характеристик. Використання новітніх технологій, таких як широкосмугові частотні перетворювачі та цифрові сигнальні процесори, дозволяє досягти кращих результатів.

Розширення функціональності. Сучасні аналізатори спектра включають додаткові функції, які дозволяють виконувати більше завдань.

Зниження вартості. Завдяки технологічному прогресу та конкуренції на ринку, середня ціна аналізаторів спектра знижується. Виробники шукають способи оптимізувати виробничі процеси та скоротити витрати, щоб зробити свої продукти доступнішими для широкого кола споживачів.

## 2.4. Ендоскопи

Говорячи про ендоскопи, не можна не згадати про важливість захисту інформації, що становить державну, комерційну чи іншу таємницю. Виявити різні закладні пристрої допоможе все той же ендоскоп у комплекті з відеомонітором або комп'ютером, здатний проникати у будь-які щілини та отвори.

Фізичний пошук засобів перехоплення інформації, який значно полегшується за допомогою ендоскопів, є важливою складовою пошукових заходів. Ендоскоп дозволяє якісно оглянути потенційні місця установки підслуховуючих та підглядуючих пристроїв, такі як порожнини і щілини у плінтусах, стінах, за батареями опалення, важкодоступні місця на шафах, карнизах, порожнини підвісної стелі тощо. Це дозволяє забезпечити більш ефективний пошук і виявлення потенційних загроз безпеці інформації.

Ендоскопи - волоконно-оптичні прилади, призначені для візуальногоконтролю важкодоступних зон, що характеризуються мінімальними розмірами вхідних отворів складними профілями та поганою освітленістю.

До складу приладу (рис. 2.8) входять:

1. потужне джерело світла;
2. світловод освітлення;
3. світловод зображення з об'єктивом 4;
5. окуляр з регулятором різкості 6;
7. маніпулятор гнучкої ділянки об'єднаної (робочої) частини світловодів 8.

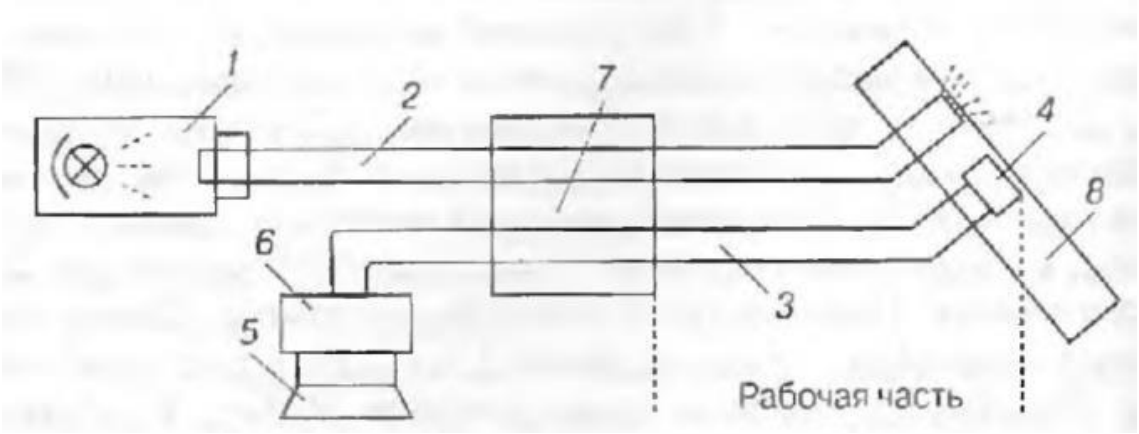


Рисунок 2.8 – Функціональна схема ендоскопа

В якості джерела світла 1 використовується галогенна лампа, з відбивачем з інтерференційним покриттям. Лампа та торцева частина

світловода освітлення охолоджуються повітряним потоком, створюваним вентилятором. По світловоду освітлення 2 світло передається у важкодоступну зону. Зображення, збільшене об'єктивом 4, передається світловодом 3 спостерігачеві. Якість зображення встановлюється регулятором різкості 6. Розрізняють жорсткі, гнучкі та напівжорсткі ендоскопи:

- Жорсткі ендоскопи є прямою металевою трубкою діаметром від 2,7 до 10 мм зі спеціальною лінзовою системою. Застосовуються такі ендоскопи досить рідко.

- В гнучких ендоскопах передача зображення здійснюється за допомогою оптоволоконного кабелю. Проте, при цьому відбуваються суттєві втрати світла, що обмежує довжину робочої частини до приблизно 1,5 метра. Проте, існують ендоскопи з довжиною близько 25 метрів, де передача зображення відбувається по радіоканалу, а оптоволокно використовується лише для підсвічування. Одна з особливостей гнучких ендоскопів - це можливість гнуття дистальної частини виробу на 180 градусів, що дозволяє отримати оглядовий кут усіх напрямків.

Зазвичай до комплекту поставки таких ендоскопів входить пристрій підсвічування, що дозволяє працювати без додаткового освітлення.

Ендоскопічні пошукові системи.

Серед широкого різноманіття пошуково-доглядових завдань, які вирішуються шляхом візуального контролю, зустрічаються такі, де доступ до об'єкта, що обстежується, може здійснюватися через отвори або щілини розміром близько 4 ... 12 мм.

Візуальний контроль:

- важкодоступних місць у різних будівельних конструкціях;
- порожнин кузовів транспортних засобів;
- внутрішнього утримання закритих контейнерів, невеликих будівель та будівель;

окремих предметів багажу, посилок та різних упаковок;

інших об'єктів, що мають порожнини з обмеженим доступом, здійснюється за допомогою ендоскопічних пошукових систем.

Ендоскопічні пошукові системи (ЕПС) – оглядові пристрої, побудовані на базі волоконної та лінзової оптики, малогабаритних телевізійних камер та механічних вузлів, укомплектовані джерелом світла або освітлювальним блоком.

Сучасні ендоскопи, що є основною частиною ЕПС, – це універсальні оптико-механічні пристрої, що забезпечують будь-який вид візуальної

діагностики та контролю усередині закритого простору на значну глибину (до кількох метрів).

Відмінною особливістю ендоскопів є велике відношення довжини робочої частини ендоскоп до її діаметра. До основних технічних параметрів будь-якого ендоскопа належать довжина робочої частини, її діаметр, кут спрямування спостереження від осі робочої частини, кут огляду.

Наявні на сьогоднішній день ендоскопи можна поділити на такі основні групи:

- жорсткі або лінзові;
- гнучкі чи волоконно-оптичні;
- комбіновані;
- відеоскопи (на основі компактних ТВ-камер).

Так як у більшості випадків освітленість у місцях огляду вкрай низька, то у складі ендоскопів зазвичай є освітлювальна система, що підключається до освітлювального блоку. Від освітлювального блоку по оптоволокну світло подається в зону контролю ЕПС, що дозволяє здійснювати контроль порожнин, що містять вибухо- та пожежно-небезпечні матеріали, рідини або гази. Джерелом світла зазвичай є галогенова лампа потужністю 20 - 150 Вт або потужний напівпровідниковий світлодіод, що розміщуються в окремому блоці, з'єднаному з ендоскопом світловолоконим кабелем зі спеціальним уніфікованим оптичним роз'ємом.

В даний час в системах освітлення все частіше застосовуються напівпровідникові випромінювачі. Вони використовуються у вбудованих підсвічуваннях, забезпечуючи задовільний рівень освітлення лише близько розташованих від торцевої поверхні ендоскопа предметів. При необхідності розглянути вміст відстані великих закритих обсягів (контейнер, бокс і т.п.) слід використовувати освітлювачі максимальної потужності. У телевізійних ЕПС в якості освітлювача іноді використовується джерело ІЧ-випромінювання, що в ряді випадків може виявитися єдиним варіантом вирішення пошукової задачі. Жорсткі ендоскопи призначені для огляду внутрішніх порожнин і виявлення дефектів у важкодоступних місцях, яких можливий прямолінійний доступ. Корпус приладу конструктивно виконується у вигляді жорсткої та міцної циліндричної трубки, усередині якої розташований оптичний канал спостереження та канал підсвічування (рис. 2.8).

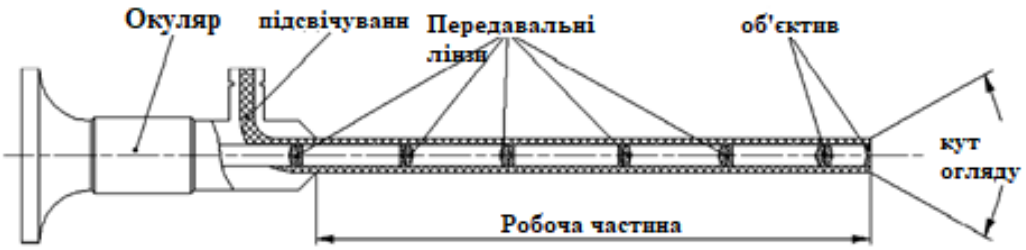


Рисунок 2.9 – Схема жорсткого ендоскопу

Оптичний канал спостереження є внутрішньою трубкою з розташованою в ній лінзовою або градієнтною оптикою. У лінзових ендоскопів краща роздільна здатність і світлосила, але мінімальний діаметр ендоскопа становить 4 мм, тоді як у градієнтного при дещо гіршій роздільній здатності – 1 мм. Для оператора на одному кінці встановлюється окуляр з діоптрійним підстроюванням. Канал підсвічування в ендоскопі виконаний з волоконно-оптичного джгута і розташований між внутрішньою трубкою та зовнішнім корпусом пристрою. Цей канал служить для передачі світла, необхідного для освітлення об'єкта, який досліджується. З одного боку каналу підсвічування розміщена кругова лінза, яка розсіює світло і створює пляму певного розміру, а з іншого боку є оптичний роз'єм для підключення до джерела світла. Деякі ендоскопи мають можливість обертання робочої частини для здійснення кругового огляду. На кінці робочої частини ендоскопа розташовуються спеціальні насадки, які можна змінювати для зміни кута спостереження та кута огляду на певні фіксовані значення. У деяких ендоскопах використовується хитаюча призма, яка дозволяє плавно змінювати кут спостереження в певному діапазоні за допомогою механічної тяги. Отже, ці технічні рішення забезпечують ендоскопам гнучкість та можливість регулювання кута спостереження, що робить їх універсальними для різних процедур візуальної діагностики та контролю всередині тілесних порожнин чи каналів. Довжина робочої частини жорстких ендоскопів зазвичай становить 100...500 мм, діаметр робочої. Необхідно, кут огляду 10…90₀ частини 1,7…16 мм, кут напряму спостереження 0 …120₀ пам'ятати, що з менших кутах огляду можливе виявлення дрібніших дефектів, але за цьому контролюється менша площа. Виведення сигналу на монітор під час використання ендоскопа має декілька переваг. Воно значно зменшує навантаження на зір оператора та його втомлюваність, що поліпшує якість і швидкість процедури обстеження. Крім того, за допомогою фототелевізійного тракту зображення може бути збережено в електронному вигляді для подальшої обробки та документування. Гнучкі волоконно-

оптичні ендоскопи призначені для огляду внутрішніх поверхонь та виявлення дефектів у важкодоступних місцях, де використання жорстких ендоскопів є неможливим. Основна відмінність гнучкого ендоскопа полягає в його здатності гнутися зі зменшеним радіусом, зазвичай 100-150 мм. Це досягається завдяки використанню волоконно-оптичного джгута у каналі спостереження. Джгут складається з окремих волокон діаметром 5-20 мкм, і їх кількість може сягати кількох десятків тисяч при загальному діаметрі 0,5-1,5 мм. Основна особливість джгута полягає в його впорядкованій структурі, яка забезпечує відтворення вихідного зображення з високою якістю ідентично вхідному. Проте в джгутах, які використовуються для підсвічування, така структура не є необхідною, і волокна укладаються безладно. Напівжорсткі ендоскопи – це гнучкі ендоскопи, у яких робоча частина виконана з металевого рукаву, який після вигину не займає початкове положення, а залишається в заданому. Закінчення робочої частини таких ендоскопів може бути виконане за аналогією з жорсткими або гнучкими ендоскопами. Робоча довжина таких ендоскопів зазвичай не перевищує 1.5 м.

Відео-ендоскопи призначені для оптико-візуального обстеження деталей та об'єктів у важкодоступних місцях механізмів, машин та обладнання, які не можуть бути оглянуті зовні. Відео-ендоскопи – це найсучасніші і в той же час найпростіші в експлуатації портативні прилади для візуально-вимірювального контролю в промисловості. Відео-ендоскопічні системи можуть використовуватися для дослідження віддалених до 30 метрів зон і дозволяють отримати високоякісне.

Відео-ендоскопи надають кольорове телевізійне зображення з високою якістю в широкому діапазоні освітлення. Вони дозволяють демонструвати зображення в реальному масштабі часу на екрані, що дозволяє багатьом спостерігачам одночасно спостерігати процес огляду. Зображення може бути записане в пам'ять відео-ендоскопа як фотографія або відео.

Відео-ендоскопи швидко набувають популярності як універсальні пристрої, що підходять для багатьох завдань візуального контролю. Вони використовують мініатюрну високороздільну камеру, розташовану за об'єктивом на кінці зонда, для створення телевізійного зображення. Це забезпечує високу якість і деталізацію ендоскопічного зображення. Однією з основних переваг таких ендоскопів є відсутність оптичного волокна в каналі спостереження, що усуває обмеження щодо його довжини. Роздільна здатність залежить від можливостей використовуваної відеокамери з об'єктивом. У таких ендоскопах може бути виключений оптоволоконний

канал підсвічування. Освітлення робочої зони може забезпечуватися за допомогою мініатюрних світловипромінюючих діодів, які зазвичай розміщуються навколо об'єктива телевізійної камери. Останнім часом стало можливим постачання відеоскопів, тобто ендоскоп з виведенням зображення на монітор. Відеоендоскоп Inskamв MS450- NTC (з двома камерами на зонді) (рис. 2.10.).


Рисунок 2.10 – Водонепроникний промисловий ендоскоп

Дві камери на зонді – фронтальна та бічна. Роздільна здатність зображення Full HD 1080. Запис відео на карту пам'яті. Жорсткий 5-метровий кабель. 4,5-дюймовий кольоровий екран IPS. Батарея ємністю 2500 мАп, автономність 3-4 години. Промисловий ендоскоп із двома об'єктивами підходить для всіх сценаріїв застосування, але особливо ефективний для інспектування вузьких просторів. Наприклад, труб, кабелів, рукавів високого тиску та інше. Все тому, що у цієї моделі дві камери. В даний час для візуального контролю важкодоступних місць розроблені та застосовуються мобільні телевізійні ендоскопи. Контроль та виявлення об'єктів здійснюється з використанням мініатюрних відеокамер та виведенням зображення на монітор Представником цих приладів є технічний відеоскоп IRIS40-6020Q (рис. 2.11), який є професійним рішенням для фахівців у галузі захисту інформації. Дозволяє оглядати важкодоступні місця – вентиляційні канали, меблі, ніші в конструкціях, ніші радіаторів опалення, простір підвісних стель тощо.

Керована камера з круговою артикуляцією забезпечує можливість огляду на всіх напрямках, а світлодіодне підсвічування з 7 рівнями яскравості дозволяє оглядати місця з різним рівнем освітлення. Глибина чіткості камери налаштована на більший діапазон відстаней відповідно до потреб пошукових завдань. Довжина зонда 2 м і товщина 6 мм дозволяють

проникати в найменші щілини і досягати найвіддаленіших місць під час проведення пошукових робіт.

*Тенденці, які проглядаються на ринку виробників ендоскопів:*

Збільшення якості зображення. Виробники ендоскопів намагаються покращити якість зображення, щоб забезпечити більш детальний та чіткий огляд внутрішніх структур. Мініатюризація та покращена маневреність.

Ендоскопи стають все більш компактними та маневреними. Застосування розширених функцій: Деякі ендоскопи включають додаткові функції, такі як оптична зумовленість, можливість реєстрації відео чи фотографій, а також можливість використання спеціальних додатків для аналізу зображень.

Рисунок 2.11 – Відеоскоп IRIS40-6020Q

2.5. Нелінійний локатор

Нелінійні локатори – це клас засобів ТЗІ, який у відповідності до «Класифікатору засобів технічного захисту інформації» (НД ТЗІ 1.5-002-2012) належить до групи засобів виявлення закладних пристроїв. Нелінійні локатори використовуються для виявлення радіоелектронних закладних пристроїв (РЗП), незалежно від їх стану (пасивного або активного).

До складу нелінійних локаторів належать: передавач, приймач, прийомно-передаюча антенна система, пристрої індикації. Здатність локатора виявляти об'єкти, що містять електронні компоненти, базується на наступному принципі. Радіоелектронне обладнання має друковані плати з провідниками (антенами), до яких підключені напівпровідникові елементи, такі як діоди, транзистори і мікросхеми. Ці елементи виступають як нелінійні

відбивачі для високочастотного зондувального сигналу локатора. При опроміненні цих антен наводяться змінні електрорушійні сили (ЕРС). Через нелінійну вольт-амперну характеристику цих елементів, зондувальний сигнал перетворюється на високочастотні сигнали кратних частот, відомі як гармоніки. Ці гармоніки випромінюються в простір. Прийомне обладнання локатора налаштоване на частоти гармонік другого або третього порядку, і отриманий перевипромінений сигнал сприймається ним. По наявності в спектрі прийнятого сигналу вищих гармонік частоти власного передавача встановлюється факт присутності в зоні зондування будь-якого радіоелектронного пристрою незалежно від того, включене воно або виключене. При використанні нелінійного локатора можуть виникати перешкоди від відбиття сигналу від металевих поверхонь, які торкаються одна одної. У таких місцях контакту металевих поверхонь може утворюватися самостійний напівпровідниковий нелінійний елемент зі структурою "метал-окисел-метал" (МОМ-діод), який має незбалансований "p-n" перехід. МОМ-структура перетворює спектр зондувального сигналу в частотний спектр, який відрізняється від спектра сигналу, що відбивається від електронного елемента. Відмінність обумовлена тимчасовою та механічною нестабільністю МОМ структури і виявляється у співвідношенні рівнів компонентів спектра, що є продуктами нелінійних перетворень другого і третього порядку. Джерелом перешкод можуть служити також і радіопередавачі, що працюють на частотах, близьких або кратних частоті зондувального сигналу. Головна перевага нелінійних локаторів - здатність виявляти електронні схеми як у включеному, так і виключеному стані, недолік - порівняно велике число «неправильних» виявлень природніх нелінійних відбивачів типу МОМ.

*Експлуатаційно-технічні характеристики локаторів*

Основними параметрами, використовуваними при порівнянні експлуатаційних якостей нелінійних локаторів, є:

режим роботи;

потужність і частота зондувального випромінювання передавача;

чутливість приймача;

точність приладів індикації;

сервісні можливості приладів.

Залежно від режиму роботи передавача розрізняють нелінійні локатори безперервного та імпульсного випромінювання. Коефіцієнт перетворення енергії зондувального сигналу в енергію вищих гармонік грає важливу роль у потужності випромінювання нелінійних локаторів. Підвищення потужності

сприяє покращенню характеристик локаторів, але одночасно збільшує небезпеку для оператора. Середня потужність локаторів безперервного випромінювання зазвичай становить від 0,3 до 3 Вт. Пікова потужність імпульсних нелінійних локаторів у різних режимах роботи може досягати від 150 до 400 Вт, що майже на 30 дБ перевищує потужність локаторів безперервного випромінювання. Оскільки ефективність перетворення залежить від пікового значення потужності випромінювання, дальність дії імпульсних локаторів значно перевищує дальність локаторів з безперервним випромінюванням за однакових умов. Зі збільшенням частоти випромінювання зменшуються геометричні розміри антенної системи, що полегшує роботу з локатором. Проте зі зростанням частоти згідно з експоненційним законом збільшується поглинання енергії матеріальним середовищем, що може маскувати радіоелектронні закладні. Також, при наближенні частоти випромінювання локатора до робочої частоти закладки, через білярезонансні явища зростає рівень перевідбитих сигналів, що збільшує імовірність виявлення радіоелектронних закладок. Сучасні нелінійні локатори здебільшого працюють у частотному діапазоні 680...1000 Мгц. Чутливістю приймача визначається максимальна дальність дії нелінійного локатора. Для сучасних приладів цей показник становить від -110 до -145 дб.

Передавальні пристрої локаторів, що генерують зондуючий сигнал, характеризуються:

- режимом роботи (безперервним або імпульсним);
- межами регулювання вихідної потужності, дБ;
- частотою безперервного випромінювання;
- частотою проходження і тривалістю радіоімпульсу, мкс.

Якість приймального пристрою, що реєструє перевипромінені сигнали, відображається такими показниками:

- частотами налаштування, МГц, на реєстровані гармоніки (2 і 3);
- реальною чутливістю при певному співвідношенні сигнал/шум дБ-Вт;
- межами регулювання чутливості, дБ.

Основними параметрами антенної системи, що випромінює зондувальні сигнали, що й зумовлює перевідбиті випромінювання на частотах вищих гармонік, є:

- коефіцієнт спрямованої дії;
- ширина головної пелюстки діаграми спрямованості за рівнем половинної потужності (град);

- рівень придушення задніх пелюсток діаграми спрямованості (дБ);
- коефіцієнт еліптичності (для антен із круговою поляризацією).

Для підвищення точності ідентифікації об'єкта в нелінійних локаторах передбачаються режими приймання на частотах 2 і 3 гармонік зондувального випромінювання, а також прослуховування сигналів, трансльованих засобами знімання за межі обстежуваного приміщення. Класифікація нелінійних локаторів в державі визначена нормативним документом системи ТЗІ НД ТЗІ 1.4-002-08 «Радіолокатори нелінійні. Класифікація. Рекомендовані методи та засоби випробувань».

Основними класифікаційними ознаками НЛ є:

- характер зондувального випромінювання сигналу;
- кількість гармонік зондувального сигналу, що аналізуються.

Нині на ринку засобів ТЗІ представлена широка номенклатура нелінійних локаторів як вітчизняних, так і імпортних. Прикладом сучасних нелінійних локаторів є: нелінійні радіолокатори NR-μ, NR-900EM, NR-900EMS, NR-2000, ORION 2.4 HX High Gain та інші. Компактний нелінійний радіолокатор NR 9000 (рис. 2.12) призначений для пошуку електронних приладів, що містять напівпровідникові компоненти.

Рисунок 2.12.– Компактний нелінійний радіолокатор NR 9000

Прилад застосовується для обстеження будь-яких, огороджувальних будівельних конструкцій, стін, меблів, предметів інтер'єру та виявлення електронних приладів негласного одержання інформації (радіо-мікрофонів, мікрофонних підсилювачів, диктофонів і т.п.) у різних режимах роботи: у режимі передачі, у виключеному або в сторожовому режимі (для приладів із дистанційним керуванням).

Відмінні риси:

- високий енергетичний потенціал;
- можливість пошуку електронних приладів за армуючою сіткою залізобетонних конструкцій;
- захист від перешкод GSM/DECT.
- режим виділення, що обгинає - "20К";
- можливість роботи з додатковим підсилювачем потужності;

Можливість візуалізації інформації щодо:

- значення атенюаторів приймачів;
- значення вихідної потужності приладу;
- напруги акумулятора.

Технічні характеристики та можливості нелінійного радіолокатора NR-900EM: Нелінійний радіолокатор NR-900EM (рис. 2.13) призначений для сканування елементів огороджувальних конструкцій і предметів інтер'єру. Його основне застосування полягає в виявленні та локалізації приховано встановлених пристроїв, які використовуються для негласного збирання інформації, таких як диктофони та інша апаратура, що містить напівпровідникові елементи. Цей локатор працює незалежно від того, чи перебувають ці пристрої в режимі передачі, вимкнення або сторожовому режимі.

Рисунок 2.13 – Нелінійний радіолокатор NR-900EM

Широкий енергетичний потенціал дозволяє використовувати нелінійний радіолокатор NR-900EM для дистанційного виявлення

саморобних вибухових пристроїв з пристроями дистанційного керування або електронними таймерами. Прилад має високу завадозахищеність, не чутливий до сигналів стільникового зв'язку будь-яких стандартів. Технічні характеристики та можливості нелінійного радіолокатора ORION 2.4 HX High Gain: Нелінійний локатор ORION 2.4 HX High Gain (рис. 2.14) є останньою розробкою в галузі нелінійної радіолокації та призначений для виявлення прихованих електронних пристроїв. Детектор жучків виявляє будь-які пристрої, які містять напівпровідникові компоненти, незалежно від того, чи вони перебувають у ввімкненому чи у вимкненому стані.


Рисунок 2.14 – Нелінійний локатор ORION 2.4 HX High Gain

Прилад дозволяє ефективно виявляти як великі, так і мініатюрні електронні компоненти та пристрої, у тому числі мобільні телефони, диктофони, мікрофони, Flash-карти, microSIM-картки. Має додатковий сенсорний екран керування та індикації, розширений набір функцій. Принцип роботи нелінійного локатора ORION 2.4 HX заснований на випромінюванні радіосигналу та аналізі відбитих від електронного пристрою (який містить напівпровідник) сигналів гармонік. Має додаткові можливості контролю та керування завдяки сенсорному екрану, розташованому на ручці. Сенсорний екран поєднує керування налаштуваннями та відображення інформації про роботу у графічному вигляді. Зображення екрана можна зберігати на карті пам'яті для документування обстеження. Методика практичної роботи з нелінійними локаторами. Загальний порядок виявлення ЗП та визначення місця його розташування. Нелінійний локатор виконує три основні функції:

- виявлення ЗП;
- визначення місця розташування ЗП;

- ідентифікація закладного засобу знімання інформації.

Зондувальне випромінювання локатора легко проникає крізь різні матеріали, воно може проходити (з ослабленням) через внутрішні перегородки приміщень, бетонні стіни та підлогу. Виявляюча характеристика нелінійного локатора нормується тільки для вільного простору. Тому в умовах пошуку схованих засобів знімання інформації мова йде не про дальність, а про максимальну глибину виявлення об'єктів в середовищі. Оцінка ведеться за рівнем відгуку, що збільшується при наближенні до об'єкта. Це дозволяє визначити точне місце розташування ЗП. При роботі на відкритих площах або у великих необладнаних приміщеннях локатор забезпечує більшу дальність виявлення, що дозволяє скоротити час обстеження. У офісах через насиченість виділеного і сусідніх приміщень електронною технікою та іншими контактними перешкоджаючими об'єктами, реальна дальність виявлення становить приблизно 0,5 м. Вона регулюється оператором з врахуванням перешкоджаючої обстановки шляхом зниження потужності передавача або загрубления чутливості приймача до межі, що дозволяє розрізняти, від якого об'єкта прийшов відгук. Дальність залежить від типу обладнання, що виявляється (наприклад, закладка з більшої по довжині антеною, як правило, виявляється на більш значній відстані) і умов його розміщення (у меблях, за перешкодами з дерева, цегли, бетону і т.д.). Для точного визначення місця розташування ЗП використовується метод поступового зменшення потужності й чутливості НЛ. Суть цього методу полягає в наступному. На першому етапу пошукових заходів виявлення ЗП операторові необхідно здійснити наступні операції:

Включивши нелінійний локатор, виявити та по можливості усунути джерела сигналів, що заважають;

Установити максимальний рівень чутливості прийомного обладнання й максимальний рівень потужності передавача зондувального сигналу;

Шляхом сканування огороджувальних конструкцій і предметів інтер'єру з відстані приблизно 1м провести контроль приміщення на наявність потужних перешкоджаючих об'єктів, як «корозійних», так і електронних (в основному електронну оргтехніку та радіоапаратуру).

При цьому призначення об'єктів повинне бути точно встановлене і вони повинні бути або вилучені із приміщення, або не братися до уваги при подальшому пошуку. Слід ураховувати, що такі перешкоджуючі об'єкти можуть перебувати в сусідніх кімнатах і на інших поверхах, які при необхідності й можливості доцільно оглянути;

Бажано видалити з кімнати джерела сильних перешкод та повторити огляд стін, стель, меблів і приладів з відстані 20 см і менше. У ході огляду відзначити підозрілі зони для більш досконалого огляду на другому етапи.

На другому етапі виявлення ЗП оператор керується наступним та здійснює пошукові роботи наступним чином:

Визначення місця можливого розташування ЗП здійснюється шляхом оцінки рівня й пеленга сигналу відгуку. Під пеленгом розуміється напрямок, відповідний до максимального рівня прийнятого сигналу [12]. Слід ураховувати, що зондувальні й відбиті сигнали перевідбиваються прилеглими об'єктами. Ефективними рефлекторами є дзеркала, металеві плити, сітки з арматури і т.д. При їхньому опроміненні можна реєструвати перевідбиті сигнали від нелінійних відбивачів, що перебувають за спиною оператора.

Для визначення точного місця розташування засобів знімання інформації необхідно:

Знизити рівень випромінюваної потужності й чутливість приймача;

- переміщаючи антену близько підозрілих зон, аналізувати показання світлового індикатору й частоту тонального сигналу в головних телефонах;
- визначити напрямок приходу відбитого сигналу максимального рівня, визначити точний пеленг по орієнтації антени;
- визначивши точне місце розташування, приступити до ідентифікації об'єкта.

При тривалій роботі, зручність використання відіграє немаловажну роль. Оператор повинен максимально використовувати особливості конструкції нелінійного локатора того типу, який використовується. Наприклад нелінійний локатор NR-9000 має телескопічну штангу, яка дозволяє без додаткового встаткування обстежувати досить високі стелі. Якщо конструкцією локатора такого зручного аксесуару не передбачено (приклад: нелінійний радіолокатор NR-2000), під час обстеження високих приміщень, знадобиться драбина и про це необхідно подбати завчасно. Якщо конструкцією приладу (наприклад, станція локатору NR-9000) передбачено ремінь для носіння приладу на плечі, то оператор повинен застосовувати таке приладдя, що буде виключати його стомлення після тривалого часу безперервної роботи. На ринку виробників нелінійних локаторів спостерігаються певні тенденції. Ось деякі з них:

- Розширення функціональності. Виробники нелінійних локаторів намагаються розширити можливості своїх продуктів. Вони вдосконалюють алгоритми виявлення нелінійних елементів та розробляють нові функції, такі

як вимірювання потужності сигналу, виявлення акустичних аномалій або ідентифікація типу нелінійного пристрою. Це дозволяє забезпечити більш точне та надійне виявлення закладних пристроїв.

- Мобільність та портативність. Тенденція до створення більш компактних та переносних нелінійних локаторів є досить актуальною. Виробники стараються зменшити розміри та вагу приладу, зберігаючи при цьому його функціональні можливості. Збільшення точності та швидкості виявлення. Виробники активно працюють над покращенням точності та швидкості роботи нелінійних локаторів. Вони використовують нові технології обробки сигналу, алгоритми виявлення та кращі антени для отримання більш точних і надійних результатів.

- Застосування інтегрованих рішень. Деякі виробники нелінійних локаторів вже почали виробляти інтегровані рішення, які поєднують функції нелінійного локатора з іншими засобами виявлення, наприклад металодетектор. Це дозволяє операторам отримати комплексну інформацію та забезпечує більш ефективний процес виявлення закладних пристроїв.

Висновок до Розділу 2

Загальний висновок до вищезгаданого полягає в тому, що існує ряд спеціальних пристроїв і приладів, призначених для пошуку, виявлення і контролю різних типів сигналів і пристроїв. Ці пристрої допомагають забезпечити безпеку, виявляти незаконне використання технічних засобів та забезпечувати якість захисту інформації. Вони можуть бути використані в різних сферах, включаючи приміщення, транспортні засоби та предмети інтер'єру. Деякі пристрої можуть працювати в прихованому режимі, а інші можуть надавати звукові або візуальні сигнали для повідомлення про виявлення сигналів. Застосування таких пристроїв сприяє підвищенню безпеки та ефективності контрольно-пошукових робіт.

Було розглянуто апаратні закладні пристрої, які в силу своєї великої різноманітності конструкцій і оперативного застосування створюють серйозні загрози безпеки мовної інформації під час розмов між людьми практично в будь-яких приміщеннях, в тому числі і на рухомих засобах пересування.

Більш детально оглянуто класифікацію закладних пристроїв за їх різними ознаками. Комбінація засобів дозволяє отримати більш повну та детальну інформацію при пошуку закладних пристроїв. Використовуючи аналізатор спектра, можна виявити незвичайні радіочастотні сигнали, які можуть свідчити про наявність закладних пристроїв. Нелінійний локатор доповнює цей процес, дозволяючи виявити нелінійні ефекти, які можуть вказувати на наявність закладних пристроїв. Ендоскоп же дозволяє проникнути всередину предметів і знайти приховані пристрої. Така комбінація засобів виявлення дозволяє знизити ймовірність пропуску закладних пристроїв, оскільки кожен інструмент виявляє їх на різних рівнях та з різних ракурсів. Поєднання їх можливостей забезпечує більш ефективне та точне виявлення потенційних загроз на об‘єктах інформаційної діяльності.

# 3. ЕКСПЕРИМЕНТАЛЬНЕ ДОСЛІДЖЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ ЗА ДОПОМОГОЮ СИСТЕМИ DELTA X

## 3.1. Опис комплексу

Експериментальна частина з пошуку закладних пристроїв проводилась за допомогою системи Delta X, яка забезпечує високий рівень надійності результатів.

Система побудована з використанням потужного аналізатора спектра, який гарантує надшвидку швидкість вимірювань з підвищеною чутливістю, в той час як вбудований радіочастотний перемикач розширює функціональні можливості.

На відміну від звичайних аналізаторів спектру, при роботі з якими потрібно окремо вивчати кожен частотний діапазон, система Delta X робить все автоматично. Сигнали розпізнаються в усьому частотному діапазоні і відображаються у постійно оновлюваному списку, з поділом на «Звичайні» та «Мобільні й безпровідні». Кожному сигналу присвоюється свій рівень небезпеки, що дозволяє оператору відрізняти підозрілі локальні передавачі від зовнішніх безпечних сигналів.

Великою перевагою системи Delta X є її висока чутливість і стійкість до завад. Звичайні пошукові прилади, такі як приймачі ближнього поля та РЧ-детектори, втрачають чутливість частково або повністю біля веж мобільного зв'язку, антен радіозв'язку, ретрансляційних станцій, точок доступу Wi-Fi, бездротових телефонів і т.д. Відстань виявлення Delta X залишається незмінною біля таких завад.

Можливості Delta X:

Швидко і надійно виявляє всі види радіочастотних пристроїв негласного зняття інформації, включаючи аналогові, цифрові, що працюють постійно й періодично, передають аудіо або відео, з шифруванням або без нього;

Знаходить підслуховуючі пристрої, що використовують цифрові стандарти GSM, 3G, 4G/LTE, 5G(<6ГГц), Bluetooth, Wi-Fi, DECT і т.д.

Виявляє приховану передачу інформації в мережі змінного струму, через дроти телефону, у проводах Ethernet, сигналізації та інших кабелях, а також перевіряє інфрачервоний діапазон за допомогою Багатофункціонального Зонду, що входить до комплекту поставки;

Може працювати в режимі миттєвого пошуку, безперервної охорони, локалізації та виявлення GPS-маяків;

Має в 20-50 разів більш високу чутливість, у порівнянні з радіочастотними детекторами та приймачами ближнього поля;

Може контролювати радіочастотну обстановку 24 години на добу, з реєстрацією даних;

Можливість виявлення прихованих підслуховуючих пристроїв з функцією накопичення, а також передавачів, захованих у спектрах інших сигналів;

Підтримує зберігання необмеженої кількості сигналів. Вся інформація зберігається в базі даних, з можливістю перегляду при виявленні або пізніше. Кількість баз даних, що підтримуються, – необмежена;

Демодуляція звуку в FM, AM, USB, LSB, CW (регульована смуга 3...240 кГц);

Система виконана в захищеному кейсі, що вміщає ноутбук з діагоналлю до 14 ".

Переваги **:**

Форм-фактор: портативна система під керуванням комп'ютера.

Висока місткість жорсткого диску комп'ютера дозволяє здійснювати реєстрацію радіочастотної обстановки протягом усього пошуку або цілодобово, в режимі безперервної охорони.

Ручний варіант використання антени є більш зручним для локалізації у важкодоступних місцях.

Обробка мобільних та безпровідних діапазонів GSM, CDMA, 3G, 4G/LTE, 5G(<6ГГц), DECT, Wi-Fi, Bluetooth, і т.д.

Мобільні та бездротові сигнали виявляються із застосуванням індивідуального для кожного діапазону порогу та відображаються окремо від інших сигналів.

Активності всередині кожного діапазону зберігаються як один сигнал з певним рівнем небезпеки, для зменшення кількості непотрібних записів у таблиці та можливості локалізації джерел з перескоком частоти.

На кожному циклі автоматично виконується додаткове зняття спектру на діапазонах з посиланнями особливо короткої тривалості, що збільшує ймовірність вимірювання таких сигналів, як GSM, 3G, 4G, 5G (<6ГГц) DECT, Wi-Fi, Bluetooth, і т.д.

Діапазони обстежуються одночасно з пошуком звичайних сигналів

Наведення від мобільних телефонів та сусідніх точок доступу Wi-Fi можуть бути легко усунені за допомогою порогів.

Багатофункціональний зонд виявляє електроніку, що випромінює електромагнітне поле, інфрачервоне випромінювання, а також несанкціоновану передачу інформації в мережі 110/220В (закладні пристрої з передачею по проводам, прихована комп'ютерна мережа в мережі живлення), Ethernet, телефонних лініях, проводах сигналізації і т.д.

Має 3 канали виявлення:

- IR - інфрачервоний (вбудований сенсор);
- LF - низькочастотний (вбудований сенсор);
- WIRE - високовольтні й низьковольтні дроти.

Діапазон частот:

- IR: 9 кГц - 4 МГц;
- LF: 9 кГц - 10 МГц;
- WIRE: 9 кГц - 100 МГц

WIRE: Максимальна напруга 250В (Категорія вимірювань II).

IR: спектральний діапазон чутливості: 740 ... 1080 нм.

Направленість сенсора:

- IR: 20 ° ;
- LF: всенаправлений 360°.

Рисунок 3.1 – Зовнішній вигляд пошукового комплексу Delta X

Комплектація комплексу Delta X:

1) Головний блок, виконаний у захисному кейсі, з вбудованим аналізатором спектра й радіочастотним перемикачем;
2) Програмне забезпечення Delta X на USB флеш-диску;
3) Всеспрямована широкодіапазонна антена (рис. 3.2);


Рисунок 3.2 – Всеспрямована широкодіапазонна антена ODA

4) НВЧ антена MWA-6 (рис. 3.3);


Рисунок 3.3 – антена MWA-6

5) Багатофункціональний зонд з кабелями (рис. 3.4);


Рисунок 3.4 – Багатофункціональний зонд

6) 5 м коаксіальний кабель з низькими затуханнями;
7) Внутрішньо-лінійний модульний адаптер;
8) Тринога, конвертована в рукоятку (рис. 3.5);

Рисунок 3.5 – Тринога

9) Набір аксесуарів (фіксатор кришки кейса, поворотні USB-адаптери, перехідники «BNC на SMA» та «SMA на BNC» НВЧ антена MWA-12.

## 3.2. Алгоритм роботи з пошуку закладних пристроїв системою Delta X

1. Підключення антен

Передня панель Delta X має 3 роз'єми:

- INPUT використовується для підключення широкодіапазонної антени (ODA-4) ;
- AUX в більшості випадків використовується для надвисокочастотної антени (MWA-6) ;
- PROBE використовується для підключення багатофункціонального зонда в режимі Зонд.

2. Запуск програмного забезпечення

Після запуску програми Delta X на екрані з'явиться вікно запуску, і буде виконана процедура знаходження підключеного обладнання.

Впевніться, що до роз'ємів INPUT, AUX та PROBE нічого не підключено та натисніть кнопку "Виконати калібрування". Процедура буде завершена протягом декількох хвилин. "Місцезнаходження – Країна" дозволяє системі правильно розпізнавати місцеві сигнали мобільного зв'язку, телебачення та радіомовлення відповідно до частотного розподілу. Вкажіть країну та слідуйте інструкціям.

Меню налаштування – «Діапазони».

Система Delta X ефективно виявляє підслуховуючі пристрої, які передають інформацію мобільними мережами або з використанням безпровідних стандартів. З цією метою програмне забезпечення обробляє мобільні й безпровідні діапазони особливим способом: усі активності всередині кожного діапазону групуються та виводяться як один сигнал з індивідуальним порогом. Завдяки цьому результати виявлення не містять

зайвої інформації, сигнали зі змінюваною частотою можуть бути локалізовані, а фонові завади можуть бути усунуті.

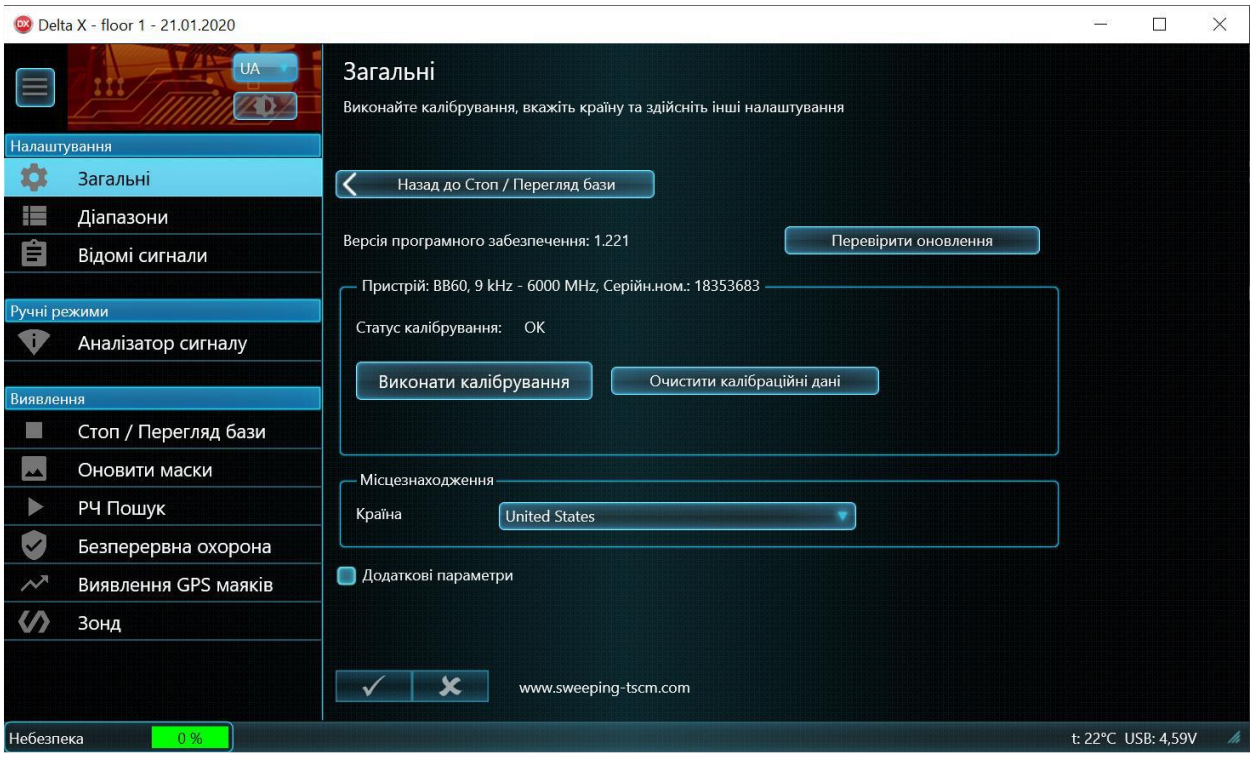


Рисунок 3.6 – Інтерфейс налаштувань ПЗ Delta X

Меню налаштування – «Автоналаштування».

Щоб забезпечити правильне виявлення, таблиця «Діапазони» повинна відповідати місцевому частотному розподілу. Система Delta X поставляється з файлами даних для різних країн, тому після вибору країни в «Налаштування – Загальні» система пропонує налаштувати таблицю «Діапазони» автоматично.

Існують наступні типи діапазонів:

- «Uplink (мобільні пристрої)»: Використовуються мобільними пристроями (терміналами) для передачі інформації на базові станції

- «Downlink (базові станції)»: Використовується базовими станціями для передачі даних на мобільні пристрої (термінали)

- «Shared (поділ частоти)»: Смуга використовується обома сторонами зв'язку одночасно. Ця технологія використовується деякими 4G/LTE/5G-діапазонами, Wi-Fi, Bluetooth, ZigBee й DECT.

«Поріг» визначає чутливість діапазону. При перевищенні порогу сигнал стає "небезпечним" та викликає спрацьовування тривоги. Поріг дозволяє оператору уникнути завад, що виникають від сусідніх мобільних

телефонів, точок доступу Wi-Fi та радіотелефонів, які не можуть бути вимкнені під час пошуку.

Оскільки завданням пошуку є виявлення локальних сигналів, пороги для мобільних пристроїв (uplinks, shared) повинні бути нижчими, а сигнали від базових станцій (downlink) повинні відсікатися за допомогою більш високих порогів. Пороги можуть налаштовуватися автоматично або вручну.

Параметр «Високий пріоритет» повинен бути встановлений для діапазонів «uplink» тих цифрових стандартів, які мають короткий час передачі або короткі часові інтервали (timeslots). Це GSM, 3G, 4G, 5G, DECT та Wi-Fi. При вимірюванні спектра система Delta X затримується на пріоритетних діапазонах, щоб «схопити» короткі сигнали.

Параметр «Виявлення автомобільних GPS-маячків» повинен бути встановлений для uplink-діапазонів мобільних мереж, щоб вони перевірялися в режимі Виявлення автомобільних GPS-маячків.

Якщо Автоналаштування було проведене успішно, система Delta X готова до пошуку. В цьому випадку можна обійти наступні розділи, що описують роботу з таблицею Діапазони.

Імпорт та експорт:

Якщо «Автоналаштування» не може знайти файл даних для обраної країни, таблиця «Діапазони» може бути заповнена вручну за допомогою кнопки «Імпорт/Експорт». Необхідні діапазони повинні бути імпортовані з зовнішніх файлів даних. Програмне забезпечення буде мати наступний вигляд, коли функція імпорту-експорту є активована.

Вміст зовнішнього файлу даних

Система Delta X поставляється з наступними файлами даних:

- GSM Bands (діапазони GSM) ;
- CDMA Bands (діапазони CDMA);
- 3G Bands (діапазони 3G);
- 4G (LTE) bands (діапазони 4G/LTE – співпадають з 5G до 6ГГц);
- Wireless Bands (безпровідні діапазони).

Поля та елементи керування:

«Показувати як» визначає представлення сигналів у таблиці. Режим «Центральна частота і смуга» підходить краще для вузькосмугових сигналів, таких як радіомовлення FM та радіозв'язок VHF/UHF. Режим «Початкова та кінцева частота» є більш інформативним при роботі з широкосмуговими телевізійними сигналами.

«Спектрограма» дозволяє переглядати спектр обраного відомого сигналу та виконувати операції з маскою цього сигналу (маска малюється синім кольором) (рис. 3.7).

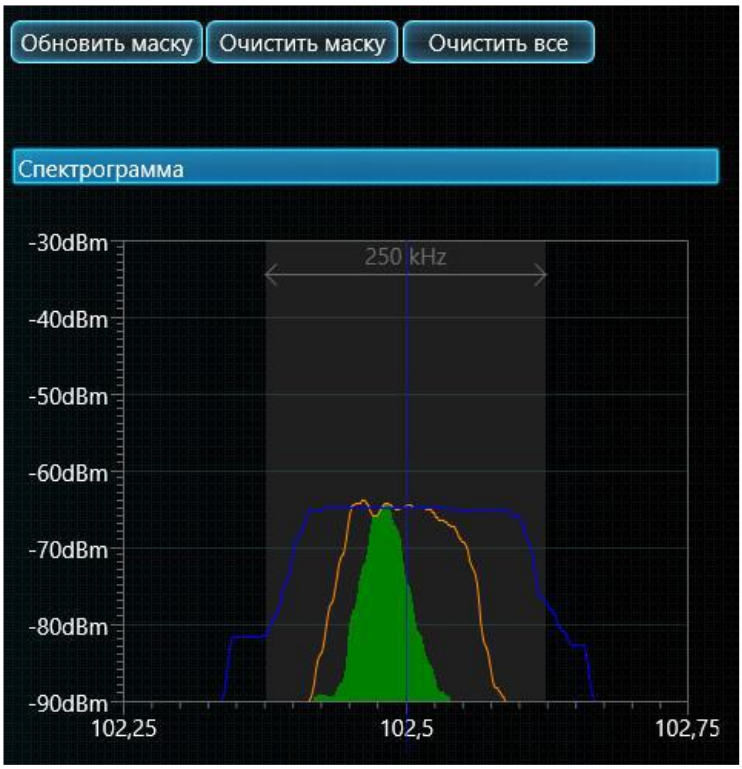


Рисунок 3.7 – Створення маски сигналу

Маска повторює спектр сигналу і дозволяє уникнути виникнення тривожних подій від цього сигналу під час пошуку. Кнопка «Оновити маску» оновлює маску поточного сигналу (синій колір) шляхом копіювання даних із траси «Максимуми» (помаранчевий колір). Кнопка «Очистити маску» очищає маску сигналу, а кнопка «Очистити все» видаляє маски усіх сигналів.

«Локатор» суттєво спрощує процес відслідковування результатів пошуку та фізичну локалізацію передавачів.

В той час як таблиця «Сигнали» містить всі зареєстровані сигнали, Локатор відображає лише ті небезпечні сигнали, які є активними в даний момент. Положення сигналу на колі локатора обирається залежно від рівня небезпеки. Близькі та потужні передавачі з рівнем небезпеки, близьким до 100%, розміщуються в центрі, в той час як слабкі й далекі сигнали з низьким рівнем небезпеки відображаються ближче до зовнішнього краю.

Завдяки візуальному ранжируванню сигналів оператор може легко розрізняти близькі й далекі джерела. Коли система Delta X або її антена

наближається до передавача, він зміщується до центру Локатора. Таким чином, оператор може виконати локалізацію.

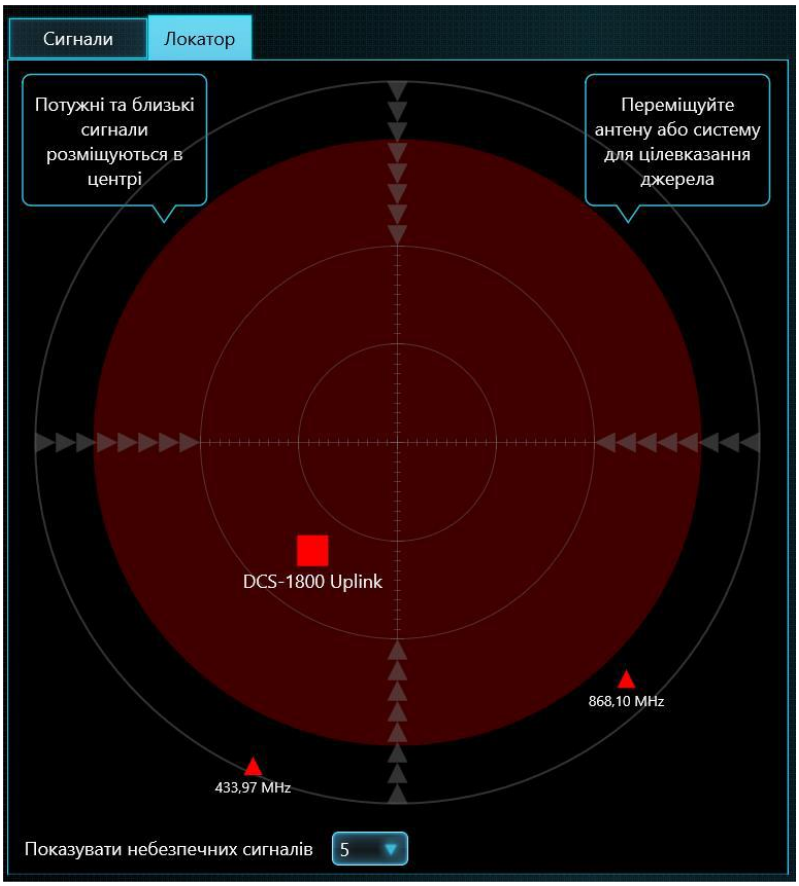


Рисунок 3.8 – Локалізація джерела випромінювання

Мобільні та безпровідні діапазони відображаються у вигляді червоних квадратів, а звичайні сигнали – у вигляді червоних трикутників.

Значки сигналів, які перевищують поріг тривоги і потрапляють до червоної зони, мають більший розмір (ознайомитися з порогом тривоги можна в наступному розділі "Детектор"). Сигнали нижче порогу тривоги відображаються меншим розміром.

Локатор може застосовуватися в усіх робочих режимах. У режимах РЧ-Пошук, Безперервна охорона або Виявлення GPS-маяків Локатор буде відображати декілька сигналів одночасно, в Аналізатор Сигналу – лише поточний обраний сигнал. В режимі Стоп/Перегляд бази Локатор відображає небезпеки, що існували в обраний момент.

«Детектор» створений для інформування оператора про виявлені спрацьовування (тривоги), а також для визначення місцезнаходження передавача. Він показує поточний рівень небезпеки на гістограмі та повідомляє оператора звуковим сигналом. Окрім того, Детектор відображає

історію спрацьовувань на графіку «Тривоги». Фізичне визначення місця розташування передавача здійснюється шляхом знаходження місця з найвищим рівнем небезпеки (Локатор і Детектор можуть використовуватися одночасно). При активації, функція звукової тривоги видає пропорційний звук.

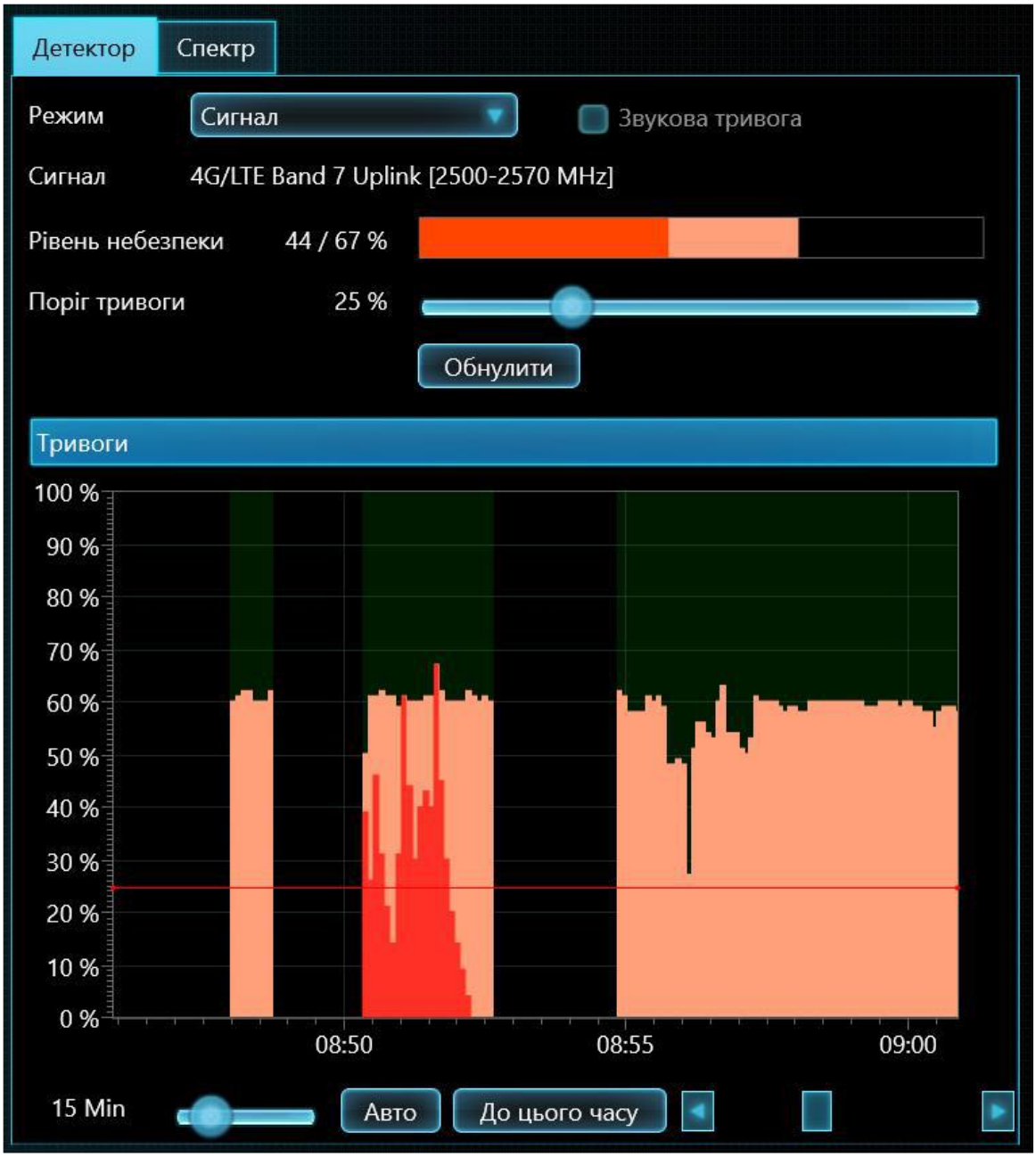


Рисунок 3.9 – Налаштування детектору

Детектор може працювати в 3-х режимах: «Широкодіапазонний», «Сигнал» та «Виділений діапазон».

У режимі «Широкодіапазонний» Детектор відстежує всі сигнали одночасно. Оператор може стежити за загальною радіочастотною

обстановкою в зоні пошуку, спостерігаючи за гістограмою та прослуховуючи звуковий сигнал тривоги. При появі нового небезпечного сигналу Детектор

негайно про це попередить. Використовуйте Локатор для спостереження за рівнем небезпеки окремих сигналів.

У режимі «Сигнал» Детектор відображає рівень небезпеки конкретного сигналу, який був обраний в даний момент у таблиці Сигнали (звичайний сигнал або діапазон). Режим є зручним для локалізації або для перегляду історії подій окремого сигналу.

У режимі «Виділений діапазон» Детектор відображає рівень небезпеки, що присутній у смузі частот, яка виділена в даний момент у Спектрограмі. Даний режим може бути корисний:

- для фізичної локалізації сигналів з перескакуванням частоти, завдяки можливості контролювати кілька каналів одночасно

- для фізичної локалізації вузькосмугових сигналів усередині мобільних/безпровідних діапазонів, наприклад, Bluetooth або Zigbee.

Коли увімкнена «Звукова тривога» і виявлена небезпека, детектор буде видавати попереджувальний звук у вигляді клацань. Інтенсивність клацань буде пропорційною до рівня небезпеки. Дана функція використовується для фізичної локалізації передавача.

«Поріг тривоги» дозволяє оператору регулювати рівень, при якому вмикається звукова тривога. Поріг дозволяє прибрати помилкові тривоги, викликані незначними змінами спектрів безпечних сигналів, і є зручним для процедури фізичної локалізації. Значення за замовчуванням встановлено на 25% в усіх режимах виявлення, за винятком «Виявлення GPS-маяків», де воно становить 10%.

Збільшення порога тривоги корисно використовувати при фізичної локалізації, оскільки це звужує область навколо передавача, в якій з'являється звуковий сигнал. Збільшуйте поріг крок за кроком, щоб більш точно визначити розташування передавача.

Також можна змінювати поріг, просто клацаючи по відсотковій шкалі графіка «Тривоги».

Кнопка «Обнулити» дозволяє оператору швидко встановити звуковий поріг, що відповідає поточному рівню небезпеки, і таким чином відкинути всі більш слабкі значення. Це також може бути корисним під час процедури фізичної локалізації.

Графік «Тривоги» відображає історію тривожних подій. Широкосмугові тривоги, тобто максимальний рівень небезпеки в кожний

момент, відображаються світло-червоним. Рівень небезпеки по обраному сигналу відображається насичено-червоним в режимі "Сигнал".

Налаштування часового періоду дозволяє оператору обрати відображуваний проміжок часу (при вимкненому «Авто»). Період можна також обирати за допомогою коліщатка миші або стандартних жестів «ближче/далі» на сенсорної панелі або екрані.

Кнопка «Авто» автоматично регулює проміжок часу, щоб відображалися всі зареєстровані тривожні події.

Кнопка «До поточного часу» прокручує до поточного часу.

Полоса прокрутки дозволяє оператору прокручувати час, щоб побачити події, які відбулися в певний момент (при вимкненому «Авто»).

Клацання на графіку Тривоги працює по-різному, в залежності від поточного режиму Delta X:

- У режимі «Стоп/Перегляд бази» клацання прокручує водоспад до відповідного часу, завантажує та відображає відповідний вимір (трасу) на спектрограмі, а також показує рівні dBm і небезпеки в таблиці «Сигнали», які існували в обраний момент. Локатор при цьому покаже небезпечні сигнали, що існували в обраний момент.

- В усіх інших режимах дозволяє прокрутити водоспад до відповідного часу.

Сторінка «Спектр» відображає графіки, які відповідальні за візуальне представлення спектра:

Спектрограма у верхній частині передає частоту по горизонтальній осі та рівень dBm по вертикальній осі.

Водоспад у нижній частині показує, як спектр змінюється в часі. По горизонтальній осі показана частота, по вертикальній – час, а колір пікселя відображає рівень dBm.

Спектрограма може відображати наступні графіки:

- «Постійність» – це спосіб візуалізації спектра за допомогою кольору, залежно від безперервності (постійності) сигналу.

- «Поточний» – поточна спектральна траса, отримана під час останнього оновлення. Показана зеленим кольором.

- «Макс.» – максимуми, які накопичені в ході поточної роботи. Показані помаранчевим кольором.

- «Поріг» – референтна траса, яка використовується алгоритмом виявлення для вибору сигналів зі спектра та оцінки рівня їх небезпеки. Показана червоним кольором.


Рисунок 3.9 – Відображення спектру сигналів

Клацання по спектрограмі в режимі «Аналізатор Сигналу» дозволяє оператору налаштуватися на потрібну частоту. Маркер (вертикальна лінія) покаже обрану частоту. Коли графік прокручується на інший діапазон, і маркер стає непомітним, кнопка «Перейти до маркера» повертає до нього.

Спектрограма дозволяє користувачу зробити виділення за допомогою лівої кнопки миші. Виділення можна наблизити за допомогою кнопки «Збільшити виділення». Таким чином можна швидко переглянути необхідний діапазон частот. Зверніть увагу, що при подвійному клацанні на сигналі в таблиці «Сигнали» вибір його діапазону в Спектрограмі здійснюється автоматично.

Відображуваний діапазон частот можна обрати за допомогою відповідного елемента керування. Можна обрати зручне значення від 0,5 МГц до 6000 МГц. Діапазон Спектрограми та Водоспаду обирається одночасно. Діапазон можна також обирати за допомогою коліщатка миші або стандартних жестів «ближче/далі» на сенсорної панелі або екрані.

«Постійність» – це спосіб візуалізації спектра за допомогою кольору, залежно від частоти існування сигналу. За допомогою даного відображення оператор може розрізняти постійні та переривчасті сигнали. Переривчасті сигнали, що рідко з’являються, будуть показані синім або зеленим кольором, в той час як більш постійні сигнали будуть відображатися жовтим або червоним.

## 3.3. Результати експериментального пошуку закладних пристроїв

Експериментальний пошук закладних пристроїв проводився 24.11.2023 року в приміщенні площею 15 кв м.

Під час експерименту було використано режим «РЧ-Пошук». Це основний режим виявлення, в якому Delta X виявляє сигнали, оцінює їх рівень небезпеки та попереджає оператора про появу тривоги. Сигнали, тривожні події та спектральні траси зберігаються в базі.

Режим «РЧ-Пошук» забезпечує надзвичайно високу чутливість завдяки здатності пропускати безпечні радіосигнали, що існують в зоні пошуку, та виявляти всі інші сигнали.

Режим підходить для виконання наступних завдань:

- Перевірка приміщень на наявність радіочастотних підслуховуючих/підглядаючих пристроїв (процедура пошуку);
- Перевірка автомобілів на наявність GPS-маячків та РЧ-закладок;
- Забезпечення безпеки під час переговорів та ін.

Перед початком «РЧ-Пошуку» необхідно провести наступну підготовку:

- Повинна бути вказана країна використання;
- Процедура «Оновити Маски» виконана;
- Для полегшення подальшої ідентифікації сигналів можна заранні наповнити таблицю "Відомі сигнали", під час оновлення масок або вручну (не обов'язково);
- Якщо функція «Сканувати безпровідні точки доступу 802.11 за допомогою безпровідного адаптера» активна, комп'ютер з Delta X повинен бути переведений у режим польоту;
- У приміщенні, що перевіряється, повинен бути створений звук, щоб активувати потенційні закладні пристрої та збільшити інтенсивність їх сигналів. Комп'ютер з Delta X може відтворювати музику або курс навчання іноземної мови.

Підключення антени: підключаємо антену з круговою направленістю ODA-4 безпосередньо до входу INPUT.

Після вибору режиму «РЧ-Пошук» задаємо початкові параметри.

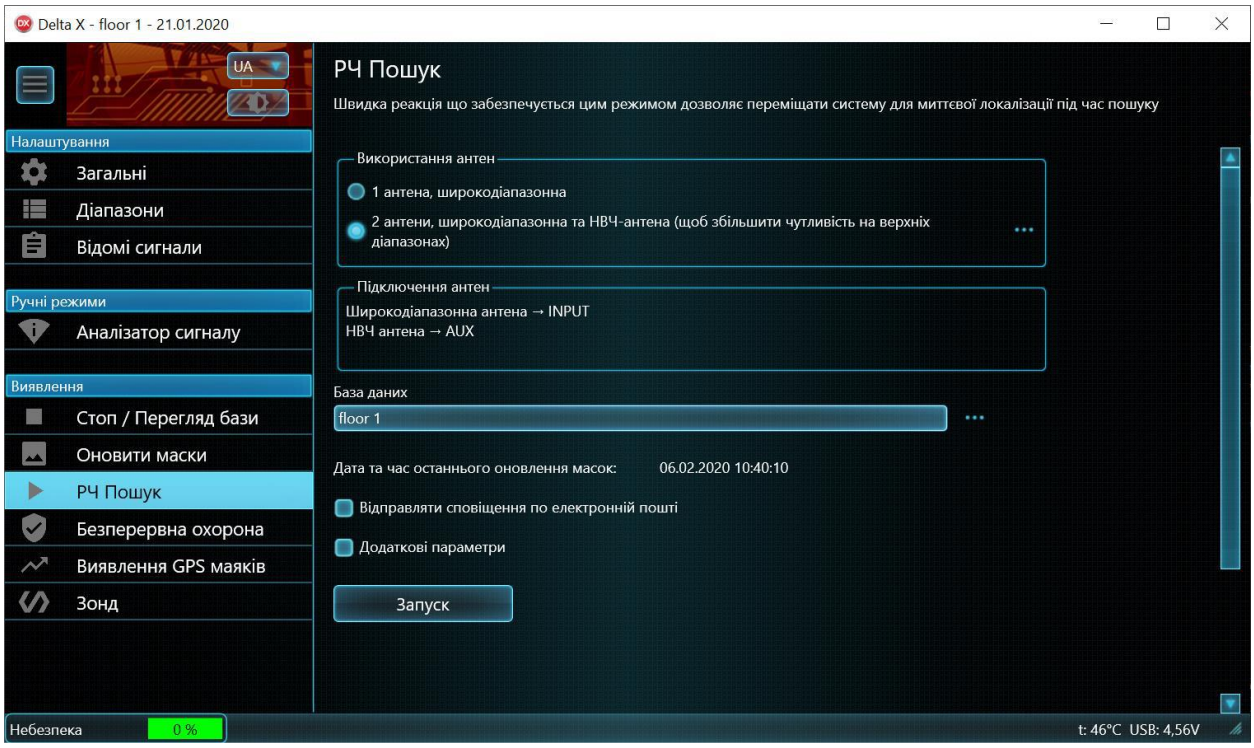


Рисунок 3.11 – Початкові параметри режиму «РЧ-Пошук»

"Використання антен" дозволяє вказати які саме антени будуть використовуватись під час пошуку:

- "1 антена, широкодіапазонна". Цей режим зручний для сканування кімнати антеною коли система стоїть на столі. Для подовження кабелю антени можна використати 5-метровий кабель та адаптери з комплекту поставки

- "2 антени, широкодіапазонна та НВЧ". Використання додаткової надвисокочастотної антени дозволяє компенсувати знижену чутливість широкодіапазонної антени на верхніх частотах. Можна переміщати всю систему Delta X або одну з антен (використовуючи 5-метровий кабель подовження). За замовчуванням, НВЧ антена застосовується для діапазону 3-6 ГГц, в той час як нижня частина спектра знімається з широкодіапазонної. Використовуємо НВЧ антени, які збільшують відстань виявлення таких сигналів як відеокамери та мікрофони що працюють через Wi-Fi 5ГГц. У контекстному меню (кнопка "...") можна налаштувати розподіл частот по антенам:

Рухаємо повзунок для зміни частоти, на якій відбувається перемикання між антенами. Відповідно до ефективного діапазону НВЧ антени мінімальне допустиме значення - 800 МГц.

Під час пошуку рекомендується враховувати спрямованість НВЧ антени. Дальність виявлення передавача буде змінюватися в залежності від того, чи спрямована на нього антена чи ні. Рекомендується міняти напрям НВЧ антени під час пошуку, щоб уникнути помилкових спрацьовувань і недостатньою дальності виявлення. Плавне обертання дозволить виявити сигнали у всіх напрямках навколо антени.

«Підключення антен» нагадує нам про правильне підключення антен згідно вибраного варіанту підключення.

«Дата і час останнього оновлення масок» попереджає, якщо зняття масок не проводилося або інформація застаріла.

«База даних» дозволяє нам обрати базу даних для запису даних. За необхідності натискаємо кнопку вибору бази даних. З’явиться спливаюче вікно вибору бази.

«Додаткові параметри» містять наступні налаштування:

«Діапазон частот» дозволяє вказати смугу частот, що перевіряється. Рекомендується використовувати значення за замовчуванням, але якщо є необхідність у моніторингу окремих сигналів, що займають певну смугу частот, то звуження смуги призведе до прискорення пошуку. Значення за замовчуванням встановлюються при кожному новому запуску Delta X.

Кнопка «Весь» встановлює максимально можливий діапазон. Кнопка «Оптимальний» обирає зменшену смугу до 6 ГГц, як найбільш ймовірну для використання пристроями зняття інформації.

«Встановити стан елементів керування» вмикає деякі функції в момент запуску виявлення.

Для того, щоб почати виявлення, натискаємо кнопку «Запуск».

Протягом декількох секунд після ініціалізації USB-з'єднання почнеться виявлення.

У режимі «РЧ-Пошук» програма автоматично розпізнає сигнали в спектральних трасах, додає розпізнані сигнали в таблицю «Сигнали» і оновлює їх рівні «dBm» та «Небезпека». Час вибірки спектральної траси залежить від використовуваної версії системи.

Сигнали підрозділяються на «Звичайні сигнали» та «Діапазони». Розділ «Діапазони» містить активності, які зареєстровані в мобільних та безпровідних діапазонах, в той час як інші сигнали розташовуються в категорії «Звичайні сигнали».

Перевищення порогу означає, що сигнал – місцевого походження (потенційно – підслуховуючий пристрій). Метою Delta X є виявлення всіх локальних передавачів, тому таким сигналам призначається більш високий

рівень небезпеки. Рівень розраховується за перевищенням порога. Під час розрахунку рівня небезпеки враховується як рівень dBm, так і смуга пропускання сигналу.

Рівень небезпеки показаний червоним кольором і відображає поточний рівень небезпеки. Пікове значення небезпеки відображається світло-червоним кольором. Він зберігає максимальний рівень небезпеки і не дає оператору можливість пропустити непостійні сигнали.

Фільтр «Небезпечні» дозволяє відібрати небезпечні сигнали, саме ті, у яких пікове значення небезпеки є більшим за 0%.

Детектор та функція «Звукова тривога» попереджає нас про виявлену небезпеку візуально і звуком. Інтенсивність звуку змінюється залежно від потужності сигналу, що дозволяє миттєво визначити місцезнаходження передавача. Детектор може працювати в широкодіапазонному режимі, інформуючи про всі сигнали одночасно, в режимі «Сигнал», з відображенням конкретного сигналу, а також в режимі «Виділений діапазон», показуючи тривоги, що виникають у певній смузі.

Локатор дозволяє нам під час пошуку закладних пристроїв стежити за декількома небезпечними сигналами відразу. Положення сигналу на колі Локатора змінюється залежно від рівня небезпеки, який, у свою чергу, залежить від відстані до передавача та його потужності. Наступний приклад демонструє 4 виявлених небезпечних сигналів: 3G (найближчий до центру, 3G-жучок із SIM-карткою), 5865,23 МГц (безпровідна відеокамера), 279,15 MHz (радіомікрофон) та 867.81 МГц (безпровідний датчик сигналізації).

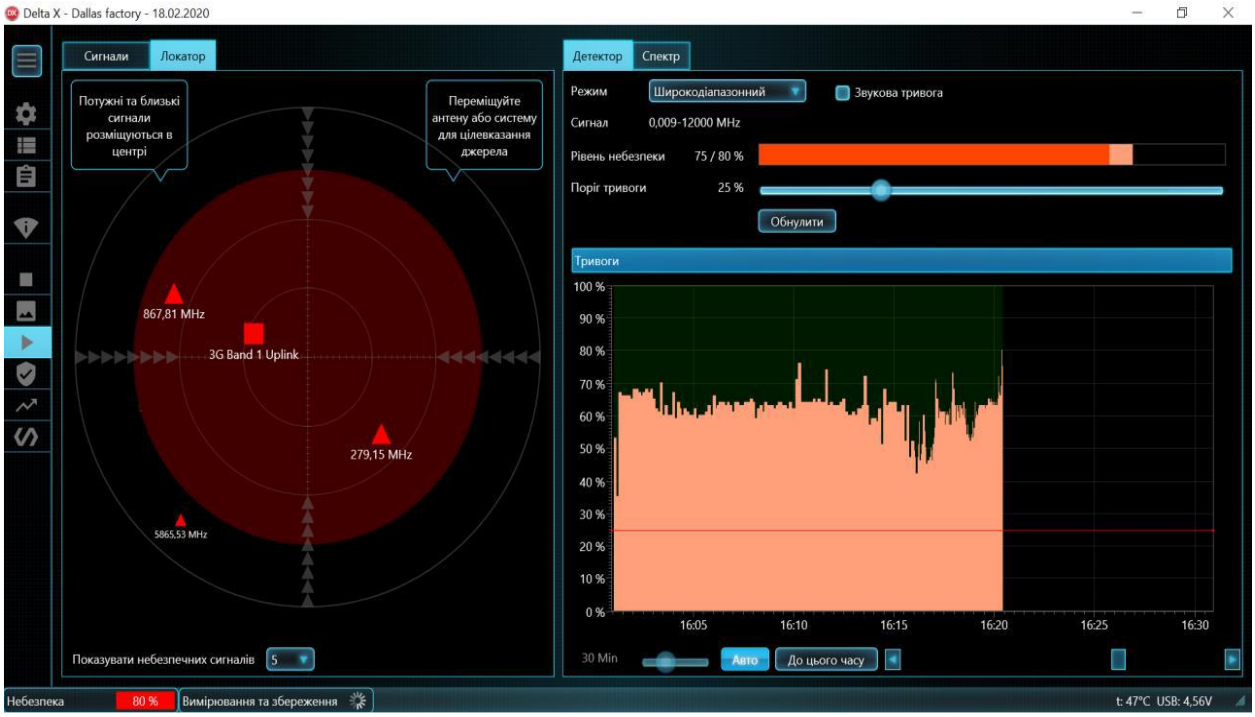


Рисунок 3.12 – Результат виявлення 4х джерел випромінювання

Червоне коло на Локаторі відображає обраний поріг.

У лівому нижньому кутку програми Delta X відображається статус небезпеки. Колір прямокутника змінюється залежно від ступеня небезпеки і буде зеленим для низьких значень, жовтим при середньому ступені небезпеки і ставати червоним, коли рівень буде підвищуватися.

Є ряд випадків, коли необхідно змінити чутливість на мобільних та безпровідних діапазонах:

- Щоб змінити відстань виявлення;
- Щоб переналаштувати чутливість у новому місці пошуку;
- Коли близько розташовані базові станції (downlink) перевищують поріг та мають рівень небезпеки більш 0;
- Коли фізично недоступні мобільні та безпровідні пристрої в сусідньому офісі або квартирі створюють завади (спрацьовування тривоги).

Відкриваємо панель інструментів діапазонів, натиснувши на заголовок «Діапазони», обираємо потрібний діапазон та відрегулюємо поріг, використовуючи повзунок:

Слідкуємо, що функція «Утрим.макс.небез.» не є активною.

Діапазони, які займаються базовими станціями (downlink), як правило, не повинні викликати спрацьовування і, отже, поріг для них повинен бути вище поточного рівня dBm. Пам'ятаємо, що не треба встановлювати занадто високе значення, щоб уникнути втрати чутливості.

Діапазони, що використовуються мобільними терміналами (uplink), та діапазони з розподілом частот (без позначки "uplink" або "downlink") повинні бути досить чутливими, щоб виявляти сигнали; тому їх пороговий рівень повинен бути нижчим. Не треба встановлювати його занадто низько, "на рівні шумів", оскільки діапазон буде постійно створювати тривожні події та ускладнювати процес виявлення.

У той час як для стандарту GSM необхідно, щоб поріг був вищим, щоб не захоплювати пристрої на відстані понад 5-10 метрів, для CDMA, 3G, 4G/LTE та 5G потрібно встановити більш низький поріг, оскільки вони мають більш низький рівень dBm та виявляються з ближчої відстані.

Зменшення чутливості може знадобитися, якщо Wi-Fi, стільникові або DECT-сигнали надходять із недоступних сусідніх приміщень. Чим вищим є поріг, тим меншою буде чутливість.

Поточний рівень небезпеки сигналу після зміни порога може зменшитися до нуля. Для скидання пікової небезпеки використовуємо команду «Обраний сигнал – Скинути небезпеку» зі спливаючого

контекстного меню в таблиці «Сигнали». В результаті діапазон буде видалений зі списку небезпечних сигналів.

Слід зауважити, що процедура «Оновити Маски» оновлює пороги автоматично, якщо увімкнений відповідний перемикач. Для збереження порогів, які налаштовані вручну, треба вимкнути цей параметр під час наступного оновлення масок.

## 3.4. Розробка рекомендацій щодо удосконалення роботи пошукової системи Delta X

Після проведення експериментального пошуку закладних пристроїв за допомогою системи Delta X виникає потреба в удосконаленні технічних характеристик пристрою:

1. Збільшення швидкості вимірювання до 2000-3000МГц/с;
2. Розширення діапазону частот 40 кГц-6000 МГц;
3. Зменшення часу реагування до 2-3 с;
4. Запровадження можливості миттєвого виявлення імпульсних цифрових сигналів;
5. Можливість одночасного виявляти і локалізувати передавач.
6. Збільшення ємності жорсткого диска комп'ютера, що дозволить здійснювати реєстрацію радіочастотної обстановки протягом всього пошуку або цілодобово в режимі охорони.

# 4. ОРГАНІЗАЦІЙНІ ЗАХОДИ ЗАХИСТУ ІНФОРМАЦІЇ

Канали витоку інформації на основі закладних пристроїв є штучними технічними каналами витоку, які призначені для несанкціонованого перехоплення, зняття або отримання інформації. Тому при їх встановленні вживаються заходи для маскування за різними способами. Маскування закладних пристроїв значно ускладнює їх пошук і затримку з витоку інформації. Для захисту інформації від витоку каналами на основні закладних пристроїв проводяться такі заходи [9]:

- Недопущення установки закладних пристроїв на ОІД;
- Виявлення та протидія роботі закладні пристроїв на ОІД.

Зазначені заходи розрізняють на організаційні та технічні.

Організаційні заходи включають:

- Організацію режиму роботи виділених приміщень та ОІД; Прикладом є розробка графіка роботи: Встановлення чіткого графіка роботи для виділених приміщень та об'єктів інформаційної діяльності (ОІД). Це може включати робочі години, періоди обслуговування, планові перерви та графіки технічного обслуговування.
- Встановлення чіткого графіка роботи для виділених приміщень та об'єктів інформаційної діяльності (ОІД). Це може включати робочі години, періоди обслуговування, планові перерви та графіки технічного обслуговування.
- Організацію контролю за доступом відвідувачів і співробітників, що мають обмеження за доступом.

Система ідентифікації та автентифікації: Встановлення системи ідентифікації та автентифікації для контролю доступу співробітників і відвідувачів, які мають обмеження за доступом. Це може включати використання ідентифікаційних карток, біометричних систем, паролів або комбінацій цих методів. Система дозволяє відстежувати та обмежувати доступ до виділених приміщень та ОІД.

- Організацію контролю роботи співробітників;
- Організацію перевірки приміщень об’єкта і техніки, що перебуває на ньому, на наявність закладних пристроїв, у тому числі і нової, що поступає.

Планування та проведення регулярних перевірок приміщень об'єкта і техніки з метою виявлення закладних пристроїв. Це може включати використання спеціальних пристроїв та технологій для пошуку та виявлення прихованих камер або пристроїв, які можуть здійснювати незаконний збір

інформації. Перевірки повинні бути проведені систематично згідно з планом, що охоплює всі приміщення та технічні засоби на об'єкті.

- Аналіз методів і способів установки закладних пристроїв, їхнього камуфляжу, конструкцій та технологій.

Аналіз таких факторів допомагає розробити ефективні стратегії та заходи для запобігання використанню закладних пристроїв у приміщеннях та об'єктах інформаційної діяльності.

Заходи з виявлення та протидії роботі закладних пристроїв.

Організаційні заходи включають:

- Аналітичні роботу з виявлення можливих місць установки закладних пристроїв ( з урахування особливостей їхньої роботи). Це може включати перевірку стін, підлоги, стелі, електричних розеток, комунікаційних кабелів та інших об'єктів, які можуть приховувати закладні пристрої. Застосування спеціалізованого обладнання, наприклад, радіочастотних детекторів або тепловізорів, може полегшити виявлення прихованих пристроїв.

- Організацію роботи служби безпеки по контролю випромінювань в ефірі, в мережах зв’язку, управління. Служба безпеки повинна регулярно перевіряти спектри частот та рівні сигналів у важливих зонах і поблизу ОІД. У разі виявлення незвичайних або підозрілих сигналів слід проводити подальший аналіз та вживати відповідних заходів.

- Аналіз частотного діапазону й способів роботи закладних пристроїв. Це дозволяє виявити характерні сигнали або виключити деякі частотні діапазони, які використовуються для роботи закладних пристроїв. Знання про типові частоти і способи роботи допомагає виявити аномальні сигнали або незвичайну активність в цих діапазонах, що можуть свідчити про наявність закладних пристроїв.

# ВИСНОВКИ

В магістерській роботі проведено аналіз загальної характеристики радіозакладних пристроїв, розглянуто важливі аспекти, пов'язані з закладними пристроями та їх впливом на безпеку інформаційної діяльності. Представлена класифікація закладних пристроїв, що включає різноманітні типи пристроїв залежно від їх конструкції, розмірів, маскування та можливостей перехоплення інформації. Класифікація допомагає краще розуміти різноманітність цих пристроїв та їх потенційні можливості.

З вивчення теоретичних аспектів виявлення закладних пристроїв можна зробити кілька висновків:

- Закладні пристрої можуть бути встановлені в різних місцях та мати різні форми, що робить їх виявлення важким завданням.

- Важливо знати особливості роботи закладних пристроїв, щоб можна було виявити їх присутність. Наприклад, деякі закладні пристрої можуть випромінювати помітні радіосигнали, тоді як інші можуть змінювати магнітні поля.

- При виявленні закладних пристроїв необхідно враховувати специфіку конкретної ситуації та можливість впливу зовнішніх факторів, таких як електромагнітні поля чи інші джерела перешкод.

- Для ефективного виявлення закладних пристроїв необхідно комплексно використовувати спеціальні прилади, які виявляють різні демаскуючі ознаки РЗП , наприклад комбінація: ендоскоп, аналізатор спектра, нелінійний локатор. Використовуючи аналізатор спектра, можна виявити незвичайні радіочастотні сигнали, які можуть свідчити про наявність закладних пристроїв. Нелінійний локатор доповнює цей процес, дозволяючи виявити нелінійні елементи, які можуть вказувати на наявність закладних пристроїв. Ендоскоп же дозволяє проникнути всередину предметів і знайти приховані пристрої. Така комбінація засобів виявлення дозволяє знизити ймовірність пропуску закладних пристроїв, оскільки кожен інструмент виявляє їх на різних рівнях та з різних ракурсів. Поєднання їх можливостей забезпечує більш ефективне та точне виявлення потенційних загроз на об‘єктах інформаційної діяльності.

Основними завданнями робіт з пошуку закладних пристроїв є виявлення, ідентифікація і локалізація закладних пристроїв. Перевірка проводиться з використанням технічних засобів згідно з інструкціями щодо їх експлуатації, а також візуально.

У зв'язку з швидким розвитком технологій, закладні пристрої можуть мати більш високу технічну складність та відповідно скритність, що потребує постійного оновлення методів та приладів для їх виявлення.

Також знання теоретичних основ закладних пристроїв, їх сутності і класифікації допомагає зрозуміти загрози, пов'язані з несанкціонованим зніманням інформації. Це важлива інформація для розробки та застосування заходів захисту, виявлення та запобігання використанню закладних пристроїв.

Проаналізували організаційні заходи для запобіганню потрапляння закладних пристроїв на об’єкт інформаційної діяльності.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. НД ТЗІ 2.7-011-2012 Захист інформації на об'єктах інформаційної діяльності. Методичні вказівки з розробки "Методики виявлення закладних пристроїв". URL: http://dstszi.gov.ua/dstszi/doccatalog/document?id=103 253 (дата звернення: 23.10.2023).

2. Івченко О.Б. Промислове (економічне) шпигунство: конкурентна розвідка й контррозвідка / О.Б. Івченко // Юридичний журнал. – 2003. – № 7. – С. 53-60.

3. Шпионские штучки. Радиомикрофоны. URL: http:// cxema.my1.ru/publ/zhuchok_na_350_m/6-1-0-4619 (дата звернення: 30.10.2023).

4. Омельченко Р. Проведення спеціального обстеження об'єктів з метою виявлення закладних пристроїв. URL: http://securepolicy.blogspot.com. (дата звернення: 08.11.2023).

5. Жучок своїми руками. URL: http://allhe.ru/publ/svoimi_rukami/ehlektronika/zhuchok_quot_kolibri_quot_svoimi_rukami (дата звернення: 13.11.2023).

6. Науковий Вісник НЛТУ України: Збірник науково-технічних праць.– Львів : РВВ НЛТУ України. – 2014. – Вип. 24.02. – 408 с.

7. Бландова,Є.С. Завадопоглинаючі вироби електронної техніки / Є.С. Бландова, Ю.І.Мещеряков, І.І. Сереженко //Електронна промисловість. - № 2. – 1997. – 44 - 48 с.

8. Вишня В. Б. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

9. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. Чинний від 01.01.1997 р. Вид. офіц. Київ : УкрНДНЦ, 1997. 6 с.

10. Михеев В.А. Основы построения подсистемы защиты информации многофункциональной информационной системы. URL: https://cyberleninka.ru/article/v/osnovy-postroeniya-podsistemy-zaschity-informatsii-mnogofunktsionalnoy-informatsionnoy-sitemy (дата звернення: 19.11.2023).

11. Ніколаєнко, Ю. С. Протидія радіотехнічній розвідці. Системи безпеки, зв'язку та телекомунікацій/ Ю.С. Ніколаєнко /Системи безпеки . - 1995. – №6. – С. 12 - 15. 17. Екранування і захист. URL:

http://www.elart.narod.ru/articles/article10/article10.htm (дата звернення: 26.11.2023).

12. Про затвердження Концепції технічного захисту інформації в Україні: Постанова Кабінету Міністрів України; Концепція від 08.10.1997 № 1126: станом на 13.10.2011 р. URL: https://zakon.rada.gov.ua/laws/show/1126-97-%D0%BF#Text (дата звернення: 15.11.2023).

13. Про затвердження Положення про державний контроль за станом технічного захисту інформації: Адміністрація Держспецзв'язку; Наказ від 16.05.2007 р. № 87: станом на 01.09.2021 р. URL: https://zakon.rada.gov.ua/laws/show/z0785-07#Text (дата звернення: 01.12.2023).

14. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР: станом на 01.07.2022 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 04.12.2023).

15. Про інформацію: Закон України від 02.10.1992 № 2657-XII: станом на 01.01.2023 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text (дата звернення: 04.12.2023).

16. Про Положення про технічний захист інформації в Україні: Указ Президента України від 27.09.1999 р. № 1229: станом на 04.05.2008 р. URL: https://zakon.rada.gov.ua/laws/show/1229/99#Text (дата звернення: 11.12.2023).

17. Технічні канали витоку інформації. Порядок створення комплексів технічного Захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗІ НТУУ «КПІ», 2016. – 104 с.

18. Технические средства защиты информации. URL: https://doklady.bsuir.by/m/12_104571_1_62726.pdf (дата звернення: 11.12.2023).